The Truth about False Positives
Overview
In the security industry, many security analysts remark that Intrusion Detection Systems (IDS) are plagued by false positives. IDS operators spend too much time distinguishing events that require immediate attention from events that are lower priority or normal for a particular environment.

Many IDS sensors have less than a 5% rate of false positives. Why, then, do IDS operators report higher rates? It is important to distinguish between two concepts that are often merged together in this context: false positives and false alarms.

This paper describes the difference between false positives and false alarms and also provides methods to reduce their occurrence.

False Positives and False Alarms
False positives occur when an IDS sensor misinterprets one or more benign packets as an attack. False alarms are defined by the operator (and sometimes the IDS sensor) based on the context of the event. A false alarm happens when traffic fits a suspicious profile detected by a signature, even if that traffic is allowed or normal for a particular environment.

Example: In one environment, 100 syn packets without corresponding ack packets may mean that a synflood attack is in progress. However, if your company runs a very busy web server, this kind of traffic may be commonplace and would be considered a false alarm—the IDS sensor correctly identified the suspicious traffic, but it is not applicable in your environment.

False alarms include many scenarios, such as:

- **Unsuccessful attacks**—attacks against hosts that are not vulnerable to the attack, attacks that were stopped at the firewall, and so forth.
- **Non-critical events**—an event that is not important to the IDS operator (like HTTP GET), but is still reported as a suspicious event or an attack.

If you include the rate of false alarms in with the rate of false positives, it is easy to see why many security experts report that IDS sensors are so inaccurate.

Reducing False Positives
Perfecting signatures to reduce false positives is the responsibility of the IDS vendor. Therefore, the method for reducing false positives is simple: report false positives to the vendor and demand better signatures.

At Internet Security Systems, false positives are taken very seriously. Before releasing new signatures, ISS beta tests the signatures in our extensive Quality Assurance labs and through our 24 x 7 IDS managed security monitoring service. This comprehensive testing process has greatly reduced unexpected false positives by stress testing these signatures in multiple network environments.

However, it is difficult to predict all possible false positives due to the enormous variety and complexity of today’s networks. For this reason, IDS vendors rely on customer experience to help them identify and resolve unexpected false positive issues.

Reporting False Positives to Internet Security Systems
Reporting false positives to ISS is easy. Simply send a message to support@iss.net with a detailed description of the problem and a packet capture (using a utility like Network Monitor), if possible. Our X-Force™ research and development team reviews every false positive report and uses this information to improve the accuracy of all ISS signatures. Through our X-Press Update™ process, we have fixed false positive issues in the following signatures in response to customer requests:
- HTTP_Shells
- HTTP_Cisco_Catalyst_Exec
- Devil
- Email_Outlook_Date_Overflow
- Stream_DoS

Reference: For more information about reporting false positives, look up the false positives topic in the RealSecure™ Signatures Help available from the RealSecure Workgroup Manager Console.

Reducing False Alarms
For false alarms, IDS operators have the most control. The following section, “Methods to Reduce False Alarms,” describes some suggestions on how IDS operators can reduce false alarms.

Methods to Reduce False Alarms
This section briefly describes several methods to reduce false alarms caused by unsuccessful attacks and by non-critical events. The following list is an overview of the methods described in this section:

- Identify non-critical events by fine-tuning signatures and policies
- Identify unsuccessful events by identifying events that were stopped at the perimeter
- Take advantage of additional Internet Security Systems solutions

Identifying Non-critical Events
You can separate critical events from non-critical events by:

- Fine-tuning signatures
- Fine-tuning policies

Fine-tuning signatures
Many signatures, like synflood, are configurable. Often, the default setting for these signatures does not work for every network environment. Because they are not properly tuned, these signatures detect and notify you about normal network traffic. With some trial and error, you can tune these signatures so that they detect traffic that is abnormal on your network.

In the RealSecure network sensor, you can tune the following signatures to fit your environment:

- ARP
- BackOrifice
- Email_Qmail_Rcpt
- IPFrag
- IPHalfScan
- IPUnknownProtocol
- Loki
- Ping Flood
- Port_Scan
- RIPExpire
- ServiceScan
- Smurf
- Stream_DoS
- SYNflood
- TCP_Urgent_Data
- UDP_Port_Scan

Fine-tuning Policies
Many IDS sensors provide policies that detect events relevant to your corporate security policy. Some of these events are not critical attacks. Consider using one of the following solutions:

- Disable these signatures altogether.
- Create user-defined signatures to monitor more specific activity instead of using the signature.
- Set the signature responses to log only, so that you can access event data later, if necessary, without flooding the console with events.
Example: You may use the HTTP GET signature to monitor inappropriate web usage, like access to gambling sites, hacking sites, or pornographic content. The HTTP GET signature reports an event every time a user accesses any Web page, which can generate a lot of traffic. Consider setting up a custom signature to monitor HTTP URLs for specific words or locations instead of using the standard HTTP GET signature.

Identifying Unsuccessful Attacks
You can identify successful attacks from unsuccessful attacks by:

- Correlating assessment information
- Correlating firewall information

Correlating Assessment Information
Assessment products and other security assessment methods provide valuable information about your network. Cross-reference this information with your IDS system. For example, use this information to tune RealSecure policies and to analyze events as they occur.

Example 1—Using vulnerability assessment information: If you have no Solaris systems on your network, turn off signatures related to the Solaris platform, set them to log only, or simply reduce the priority setting so that they are not displayed as high priority events.

Example 2—Using security assessment information: Through a security assessment, identify known services that are secure and can be ignored for alerting purposes. For example, after a security assessment and penetration test has identified that a firewall is indeed configured properly and is blocking all the appropriate dangerous traffic, the IDS may be configured to log port scan events, but not alert on them. Port scanning on the Internet is very common. The organization may determine that these attacks are worthwhile to keep on record for evidence purposes, but with a properly installed and configured firewall, alerting and taking action on these attacks are not worthwhile.

Example 3—Referencing vulnerability information as attacks occur: Keep a list of vulnerable systems and refer to it when attacks occur. If you know your host is not vulnerable to a particular attack, you can rest assured that the attack was not successful.

Correlating Firewall Information
If you have only one sensor outside your firewall, consider installing another sensor inside the firewall so that you can focus on attacks that make it past your first layer of defense.

Alternatively, compare attacks to firewall logs to determine what attacks made it through. If you have the SAFEsuite® Decisions application, you can merge firewall logs with IDS data and use the standard reports to compare this information on a routine basis.

Internet Security Systems Solutions
One of the best ways to learn how to identify false alarms in your environment is to take advantage of several ISS solutions available to you. Use these resources to increase your company’s effectiveness in reducing false alarms:

- ISS SecureU offers educational classes on how to configure and tune your IDS. By participating in a class on IDS, you can take advantage of all the features and avoid the pitfalls of false alarms.
- ISS Consulting has an offering for doing a security assessment and configuring IDS deployments for optimal settings. With ISS consultants performing a security assessment and understanding the network layout, the IDS can be properly configured to only alert on what the organization considers serious, and thereby minimize false alarms.
- ISS Managed Security Services offers a 24 x 7 monitoring capability around IDS. If you do not have the resources to set up a 24 x 7 security operations center (SOC), this solution may be
optimal for you. ISS SOC operators monitor and analyze all malicious traffic. With their security expertise, they separate false alarms from real attacks and can help you respond appropriately when serious threats occur.

- The ISS Global Threat Operations Center (GTOC) continuously monitors the Internet. It globally correlates security threats to reduce false alarms and identify and escalate serious attack patterns that are affecting networks across the world. The center publishes the most current threat metrics, assessments, and forecasts on the ISS Web site so that you can stay current on threat incidents from all over the world. The address for this site is:

  https://gtoc.iss.net/secure/whatshot.php

**Conclusion**

IDS technology began with various methods of detecting attacks and generating alerts and responses. The IDS of the future is a total protection system that uses data from many sources, like vulnerability assessment and firewall data, to automatically reduce false positives and false alarms.

IDS are evolving beyond just intrusion detection and is becoming similar to comprehensive burglar alarm systems that monitor at various levels of applications, operating systems, and networks. Part of this evolution is that IDS technology is watching not only for intruders, but denial of service attacks, viruses, worms, Trojans, and backdoors.

Internet Security Systems is dedicated to helping you get the most out of your security dollars. Therefore, development on these technologies is already underway and could be available to you as early as the end of this year.

ISS hopes that the ideas and suggestions in this paper can help you reduce false alarms in your environment. For more information about other ISS services and solutions, contact sales@iss.net.