

THE ROLE OF IDS & ADS IN NETWORK SECURITY



The Role of IDS & ADS in Network Security

When it comes to security, most networks today are like an egg: hard on the outside, gooey in the middle. Once a hacker has penetrated the perimeter defenses, the typical network has few systems for intercepting malicious traffic and alerting administrators.

As IT managers grapple with network security in an increasingly sophisticated hacker environment, many are realizing that security is a complex problem that cannot be solved with a single technology. The current model of firewall protection is evolving into a layered approach that includes a hardened border supplemented by intrusion detection packet sniffing. How these systems are inter-related is very important for an effective implementation. This paper explains how the relationship between firewalls and intrusion detection systems can create hidden holes into the network and obscure data that would otherwise indicate an attack. Intrusion detection is not enough; attack detection external to the firewall must be part of the security fabric.

Layered Security

Typically, the first layer of defense is the firewall. Firewalls block suspicious traffic, using rules based on address source and the port destination.

To ensure that the firewall is working, many network administrators install an Intrusion Detection System (IDS). The IDS has the ability to “sniff” individual packets of network traffic for attack signatures, and alert the network administrator if intruders have slipped through the firewall. Also, most IDSs also report traffic patterns that differ from a pre-established norm. While the firewall looks outward, the IDS sits on the trusted side of the firewall, and can reveal suspicious activity originating from the network’s own users.

Some IDSs go a step further, and allow integration with firewall software, especially if the firewall software is offered by the same vendor. This enables the IDS to report blocked traffic and – in some cases – traffic abnormalities.

A few of the more comprehensive IDSs provide management reports for firewall activity on demand, or daily trend reports, often using ancillary software. Most systems, however, are capable only of outputting raw logs of firewall activity or static reports.

The IDS Can Report Only What the Firewall Allows To Pass Though It

The IDS is an important part of a network security program. However, the system can report only on the traffic that the firewall allows it to see. This limits the system's effectiveness for a number of reasons.

Firewalls have a pass/block approach to handling network traffic. The IDS never sees the traffic that the firewall blocks. Administrators should be concerned that the IDS is not sniffing the blocked packets. This is arguably the most suspicious traffic on the network. Denial of Service (DoS) attacks, for example, are often preceded by hacker probes, which are blocked at the firewall. What's worse, a manual review of pages and pages of firewall logs is impractical, so the administrator never sees patterns that may indicate an impending attack.

i-Trap commissioned a survey of the top 10 domestic firewall vendors. Roughly half of the firewalls report blocked traffic only as part of raw logs, and 70 percent require the user to purchase and install an additional software package to get detailed management reports. Generally, the information about which traffic was blocked is hidden in hard-to-read reports, which are typically little better than raw logs. See Figure 1.

Some IDSs offer more sophisticated reports, including analysis of the data supplied by the firewall logs. However, an IDS with sophisticated reporting capability is more expensive, easily costing \$14,000 plus the cost of an ancillary report software package if required. Even when the IDS offers useful reports, they may not be accurate because -- depending on the firewall's configuration -- the traffic data may have been altered in a number of ways:

Attachments. The firewall may remove certain types of attachments from inbound email. Certain types of attachments (file types such as .scr, .pif, .vbs) could indicate an attack. The IDS reports cannot show that these attachments were removed. This

problem is common with SMTP proxy available from major firewall manufacturers.

Source. To the IDS, it may look like the traffic was coming from the firewall. For example, if the firewall has been configured as a proxy server for inbound traffic, the traffic takes on the identity of the firewall, and the true source of the traffic on the Internet is lost, making tracking the source of traffic impossible.

Filters. If the firewall is configured to filter certain types of web traffic, such as certain header types or MIME types, then the firewall will remove these elements before the IDS can see them. Thus the firewall hides the attack attempts or removes the header while leaving the malicious content in the data.

Overflow Attacks. Another example of how the firewall will not provide attack information to the IDS is an overflow attack. Overflow attacks attempt to take control of a server or crash a server. The trick is to fill up the normal memory associated with an application so the server opens access to its overflow memory. If a hacker manages to load a program in overflow memory, the program will be able to run inside that server. In such a case, the firewall won't log the attack because it does not violate source and destination policies.

The Need for Attack Detection

An IDS and ADS (Attack Detection System) are very similar. Both are packet sniffers, but where they are placed on the network gives them different abilities. Figure 2. Because an ADS monitors traffic external to the firewall, it is able to see the traffic and suspicious patterns that the IDS system cannot. Unlike a firewall or IDS, the ADS enables the administrator see what the hacker is trying to do before it happens: i.e., download files, change appearance of web site, etc.

Many network managers have a false sense of security, because they assume that their firewalls are reliable and that their IDSs are providing good backup layers of security. However, by the time an IDS encounters an attack, the attack or misuse has

already occurred. The network needs an early warning system, and that is the role of the ADS.

There are several benefits to an ADS:

Devices Outside the Firewall. The ADS is essential for networks having a device located outside of the firewall. This is more common than people think. Bright.net estimates that up to 50 percent of companies deliberately place a workstation or a server (such as a web server) outside the firewall. This simplifies and reduces the cost of firewall implementation. Often the network administrator will deploy a firewall to protect desktop users, but not the web server. Therefore, an ADS will catch problems that the firewall cannot.

Attacks on the Firewall. The IDS sniffs only the traffic that passes through the firewall. If the firewall itself is attacked, the destination of the traffic is the firewall itself, and the IDS system will never see it. In the worst case example, a firewall may be completely compromised and the hacker has remote control of the firewall, able to evade attempts by the network manager to reconfigure his or her own firewall. Compared to the IDS, the ADS is a better monitor of the firewall, because it is able to detect an attack on the firewall itself.

Forensics. Because an ADS reports data that has not been changed by the firewall, its logs provide valuable forensic information after an attack has occurred. The network administrator can see the original Internet sources of the traffic, which kind of attack it was, on which ports, and assess the damage to the company. The ADS logs also aid in diagnosing which servers were affected, making it easy to find and fix the problem. Using this information, the network administrator can complain to his ISP, or even turn over the logs to law enforcement officials.

Application Examples

To fully understand the relationship between ADS, IDS, and firewalls, it is helpful to look at real world examples. The following three applications pose common security problems and explain how they would be solved using an attack detection system, such as i-Trap. The i-Trap system includes packet-sniffing probes on both sides of the firewall, one set for intrusion detection, the other set for attack detection. In addition, i-Trap integrates with the existing firewall. Logs from the firewall and probes are sent via a secure connection to the i-Trap Network Operations Center (NOC) where they are analyzed by software filters and NOC security experts who will alert the customer if needed. The system administrator can view detailed reports in near real time, via an encrypted browser connection.

1. Device Outside of Firewall

Overview:

In the case of a machine being placed outside of the company's firewall, there are obviously many ways to compromise and take control of that machine. In this example, we'll assume the machine is running Windows 2000, and is placed outside of a firewall because the firewall has no DMZ port available.

Being unprotected by a firewall, this machine can be scanned without triggering an alert. An attacker can see easily that this is a Microsoft Windows machine, and with little additional effort can determine the target is Windows 2000 specifically. Using widely available tools, the attacker can enable the FTP service on the system, create a user account, and store files to be downloaded by others.

ADS Role:

The ADS will allow several opportunities for alerting and intervention in this example. First, the i-Trap ADS would detect the scan of the machine. Once the attacker connects to the “Windows ports” to enable FTP and create accounts, i-TRAP would detect and alert to this as well. When files are being uploaded, the i-TRAP system would detect abnormal FTP traffic, as well as when other users connect to copy the files.

2. Attack Through Intentionally Open Ports in the Firewall**Overview:**

In the case of a firewall with a DMZ port (or other comparable functionality), servers may be placed behind a firewall that prevents access to high-risk ports, while allowing access to ports necessary to its operation. Let’s consider a web server. This machine is protected by a firewall that allows access to ports 80 and 443 only.

An attack against such a machine could have several purposes. By gaining access, the attacker may be able to then access other machines inside of the company’s private network, to launch attacks against other systems, or to even disrupt services on the victim system.

ADS Role:

Many modern firewalls may include proxy services in an attempt to add an additional layer of security. Instead of the more traditional method of passing or blocking traffic based on ports and addresses, these firewalls pick apart the traffic and block certain patterns. The proxy service will block some attacks but the administrator must constantly update his or her policies as new attack methods are discovered. The action of these firewalls not only compromises the forensic value of computer logs, but also what an IDS sensor may pick up on. Being outside the firewall, the i-TRAP ADS sensor will have a full, unaltered copy of all traffic.

3. Attack Against the Firewall Itself

Overview:

In the case of an attack against the firewall itself, a traditional IDS system would have no purpose at all. The IDS examines traffic that makes it past the firewall only. If traffic terminates to the firewall, the IDS sensor will never see it.

The detail in logging for firewall-terminated traffic will vary greatly among different firewalls. Let's consider a firewall that is accessible for management via a web browser interface. If an attacker attempts to log into the firewall and fails to authenticate, generally one would see failed login attempts in the log. However if the attacker chooses to use any form of exploit against the firewall, logging may not be of value, if it occurs at all. Using a buffer overflow against the firewall's management port may cause disruption of the firewall's functionality or even provide access to the firewall for reconfiguration . This action may even produce no logs at all.

ADS role:

Not only will the i-TRAP alert the attempt of these attacks, but in absence of detailed firewall logs of the incident, the i-Trap report may be the only indication that an attempt was made. In the event that the firewall itself is compromised (and possibly reconfigured), the ADS sensor would provide a detailed account of what was done. This makes it possible to determine what was damaged and how to reverse what damage was done. It also enables planning to prevent similar incidents in the future.

Summary

CERT data indicates that hacker activity has doubled in the past two years, and is on pace to quadruple for next year. No network should be considered fully protected until it has layered security that is comprehensive in its scope.

The differences between intrusion detection and attack detection are clear: one watches for suspicious traffic inside the firewall, the other looks for suspicious activity outside of it. Both are needed for a complete network security solution.

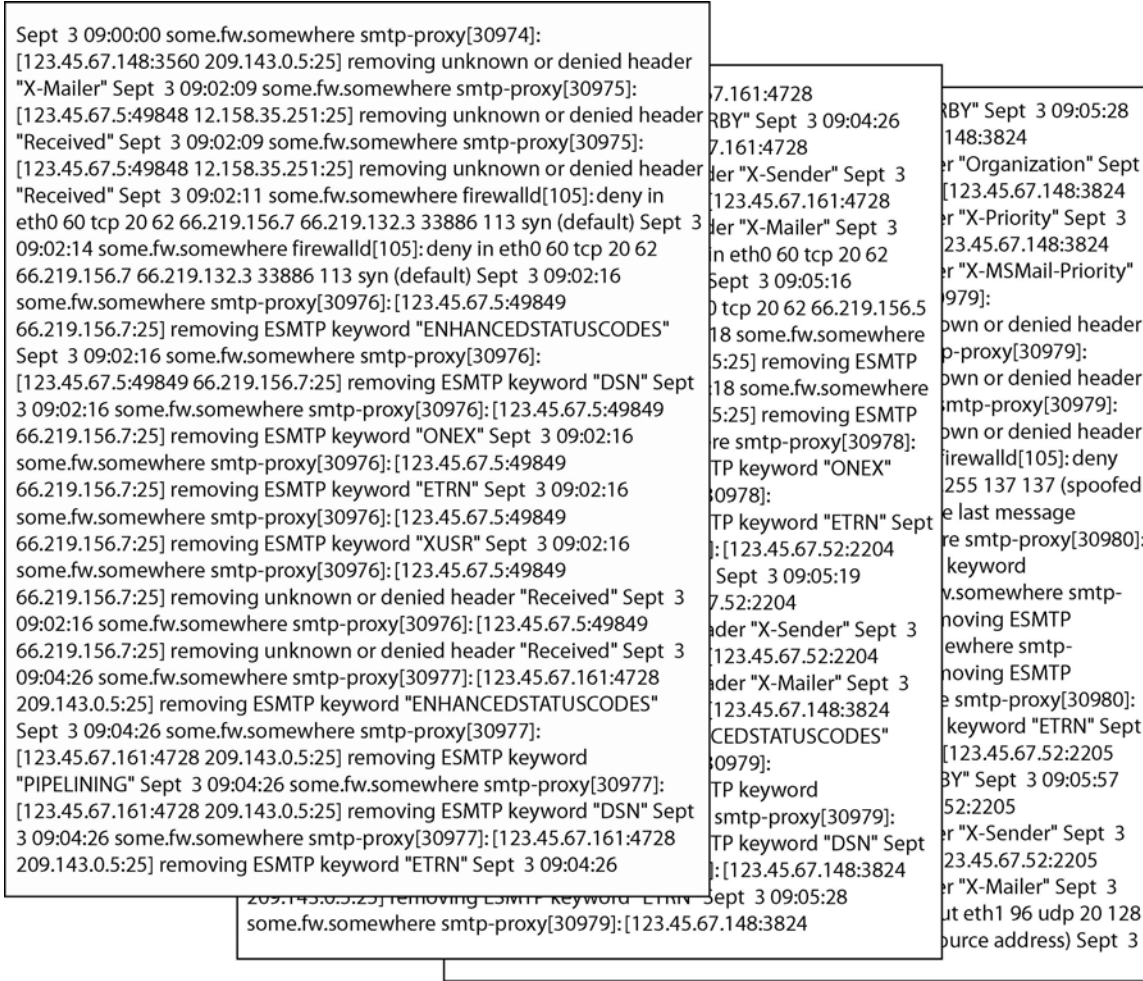
About I-Trap Internet Security Services

i-Trap Internet Security Services is a new venture formed by Bright.net. The i-Trap NOC is based on proven Bright.net experience in supporting more than 20,000 ISP customers. Bright.net is a wholly owned subsidiary of DCI Communications Incorporated (DCI), a 104-year old Ohio-based telecommunications company. DCI is a consortium that includes a local exchange and long distance telephone company, a cable television company, and Internet service providers.

About the i-Trap Attack and Intrusion Detection Solution

i-Trap is the first solution to combine an Intrusion Detection System (IDS) and external-to-the-firewall Attack Detection System for up to one-tenth the subscription price of current solutions. The i-Trap solution monitors corporate network traffic for a variety of hacker intrusions and attacks, and allows network administrators to verify that security firewalls and policies are working. For more information, visit www.i-trap.net or call 888-658-8727

Figure 1: Raw firewall logs make it difficult to spot patterns that could indicate hacker activity.



Sept 3 09:00:00 some.fw.somewhere smtp-proxy[30974]: [123.45.67.148:3560 209.143.0.5:25] removing unknown or denied header "X-Mailer" Sept 3 09:02:09 some.fw.somewhere smtp-proxy[30975]: [123.45.67.5:49848 12.158.35.251:25] removing unknown or denied header "Received" Sept 3 09:02:09 some.fw.somewhere smtp-proxy[30975]: [123.45.67.5:49848 12.158.35.251:25] removing unknown or denied header "Received" Sept 3 09:02:11 some.fw.somewhere firewallld[105]:deny in eth0 60 tcp 20 62 66.219.156.7 66.219.132.3 33886 113 syn (default) Sept 3 09:02:14 some.fw.somewhere firewallld[105]:deny in eth0 60 tcp 20 62 66.219.156.7 66.219.132.3 33886 113 syn (default) Sept 3 09:02:16 some.fw.somewhere smtp-proxy[30976]:[123.45.67.5:49849 66.219.156.7:25] removing ESMTTP keyword "ENHANCEDSTATUSCODES" Sept 3 09:02:16 some.fw.somewhere smtp-proxy[30976]: [123.45.67.5:49849 66.219.156.7:25] removing ESMTTP keyword "DSN" Sept 3 09:02:16 some.fw.somewhere smtp-proxy[30976]:[123.45.67.5:49849 66.219.156.7:25] removing ESMTTP keyword "ONEX" Sept 3 09:02:16 some.fw.somewhere smtp-proxy[30976]:[123.45.67.5:49849 66.219.156.7:25] removing ESMTTP keyword "ETRN" Sept 3 09:02:16 some.fw.somewhere smtp-proxy[30976]:[123.45.67.5:49849 66.219.156.7:25] removing ESMTTP keyword "XUSR" Sept 3 09:02:16 some.fw.somewhere smtp-proxy[30976]:[123.45.67.5:49849 66.219.156.7:25] removing unknown or denied header "Received" Sept 3 09:02:16 some.fw.somewhere smtp-proxy[30976]:[123.45.67.5:49849 66.219.156.7:25] removing unknown or denied header "Received" Sept 3 09:04:26 some.fw.somewhere smtp-proxy[30977]:[123.45.67.161:4728 209.143.0.5:25] removing ESMTTP keyword "ENHANCEDSTATUSCODES" Sept 3 09:04:26 some.fw.somewhere smtp-proxy[30977]: [123.45.67.161:4728 209.143.0.5:25] removing ESMTTP keyword "PIPELINING" Sept 3 09:04:26 some.fw.somewhere smtp-proxy[30977]: [123.45.67.161:4728 209.143.0.5:25] removing ESMTTP keyword "DSN" Sept 3 09:04:26 some.fw.somewhere smtp-proxy[30977]:[123.45.67.161:4728 209.143.0.5:25] removing ESMTTP keyword "ETRN" Sept 3 09:04:26	7.161:4728 RBY" Sept 3 09:04:26 7.161:4728 er "X-Sender" Sept 3 123.45.67.161:4728 er "X-Mailer" Sept 3 in eth0 60 tcp 20 62 Sept 3 09:05:16 0 tcp 20 62 66.219.156.5 18 some.fw.somewhere 5:25] removing ESMTTP 18 some.fw.somewhere 5:25] removing ESMTTP re smtp-proxy[30978]: TP keyword "ONEX" 0978]: TP keyword "ETRN" Sept [123.45.67.52:2204 Sept 3 09:05:19 7.52:2204 ader "X-Sender" Sept 3 123.45.67.52:2204 ader "X-Mailer" Sept 3 123.45.67.148:3824 CEDSTATUSCODES" 0979]: TP keyword smtp-proxy[30979]: TP keyword "DSN" Sept [123.45.67.148:3824	BY" Sept 3 09:05:28 148:3824 er "Organization" Sept [123.45.67.148:3824 er "X-Priority" Sept 3 23.45.67.148:3824 er "X-MSMail-Priority" 979]: own or denied header p-proxy[30979]: own or denied header smtp-proxy[30979]: own or denied header firewallld[105]:deny 255 137 137 (spoofed e last message re smtp-proxy[30980]: keyword v.somewhere smtp- noving ESMTTP ewhere smtp- noving ESMTTP e smtp-proxy[30980]: keyword "ETRN" Sept [123.45.67.52:2205 BY" Sept 3 09:05:57 52:2205 er "X-Sender" Sept 3 23.45.67.52:2205 er "X-Mailer" Sept 3 ut eth1 96 udp 20 128 ource address) Sept 3
---	---	---

Figure 2: An Intrusion Detection System sits behind the firewall, and an Attack Detection System sits external to the firewall.

