

# Intrusion Prevention Systems: the Next Step in the Evolution of IDS

Neil Desai 2003-02-27

## Intrusion Prevention Systems: the Next Step in the Evolution of IDS

by Neil Desai

last updated Feb 27, 2003

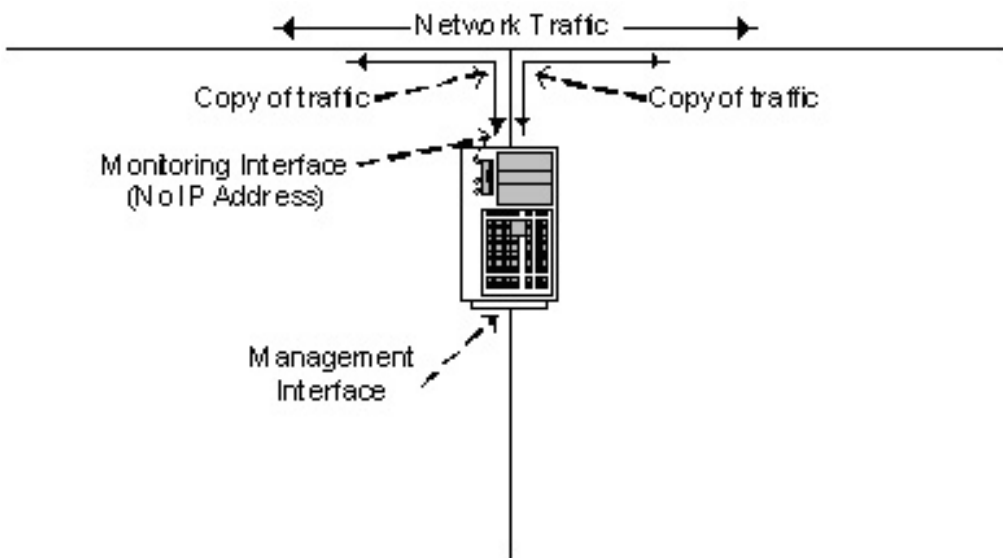
---

You blended your IDS with my firewall! No, you blended your firewall with my IDS! Either way, when you combine the blocking capabilities of a firewall with the deep packet inspection of an IDS, you get the new kid on the block: intrusion prevention systems or IPS.

So what exactly is an IPS? Like most terms, it depends on whom you ask. The definition of IPS that we are going to use is any device (hardware or software) that has the ability to detect attacks, both known and unknown, and prevent the attack from being successful. Now that firewalls can keep track of TCP sequence numbers and have the ability to block certain type of traffic (such as Code Red or Nimda) even they can act as intrusion prevention systems. However, this is not what we are going to look at. Rather, this discussion will look at five different categories of IPSs that focus on attack prevention at layers that most firewalls are not able to decipher, at least not yet. The five types of IPSs that we will look at are inline NIDS, application-based firewalls/IDS, layer seven switches, network-based application IDSs, and deceptive applications.

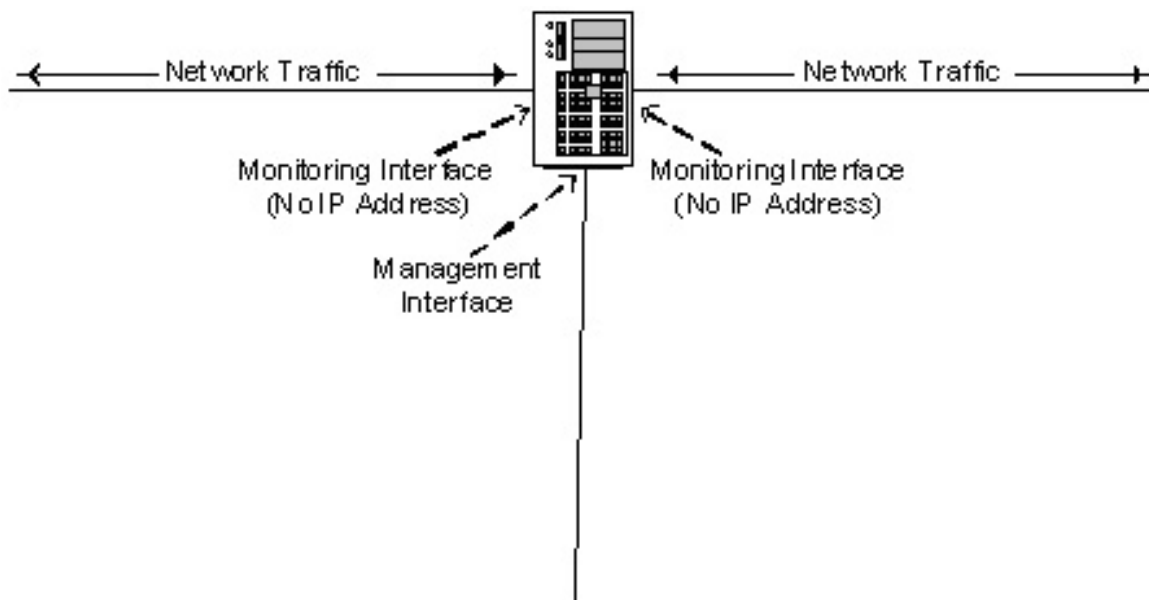
### Inline Network Intrusion Detection Systems

Most NIDS would be configured with two NICs, one for management and one for detection (Figure 1). The NIC that is configured for detection usually does not have an IP address assigned to it, making it a "stealth" interface. Since it does not have an IP address assigned to it no one can send packets to it or cause the NIDS to reply using that interface.



**Figure 1**

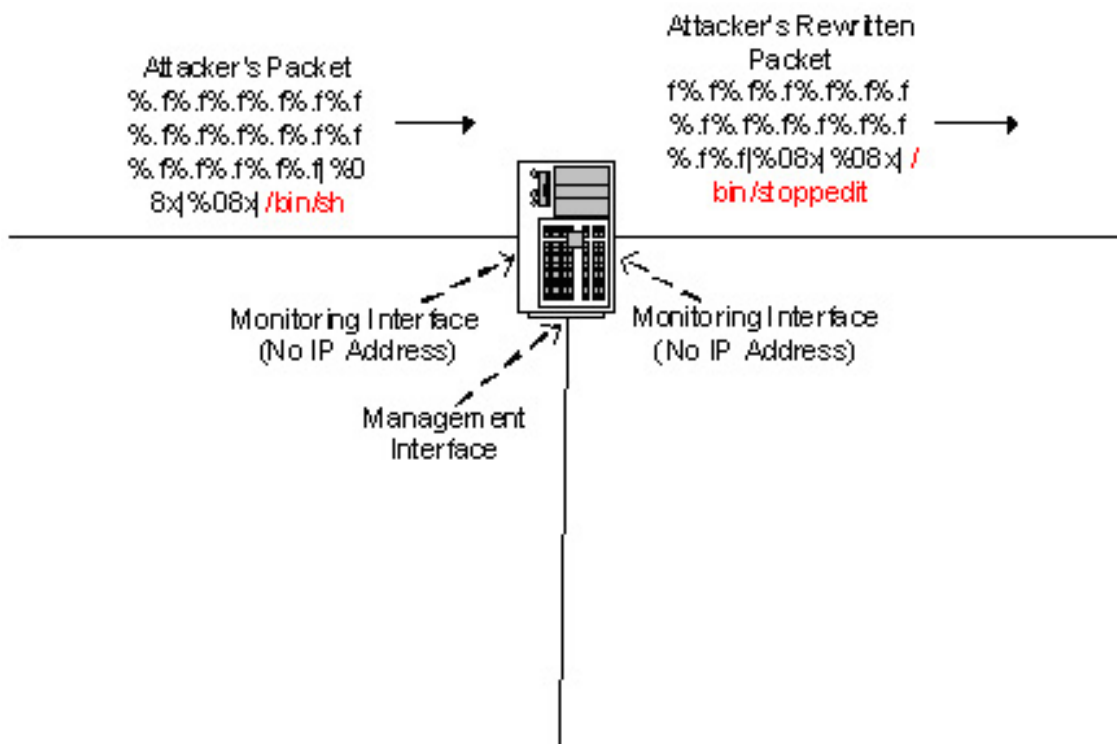
The inline NIDS works like a layer two bridge, sitting between the systems that need to be protected and the rest of the network (Figure 2).



**Figure 2**

All traffic will pass through the inline NIDS. Unlike a regular bridging device though, the inline NIDS will inspect the packet for any vulnerabilities that it is configured to look for. If a packet contains a piece of information that trips a signature the packet can be forwarded or dropped and either logged or unlogged. [Hogwash](#) can take it a bit further though: it has the added ability to rewrite the offending packet(s) to something that won't work, a procedure known as packet scrubbing (Figure 3). This type of IPS is useful if you don't want the attacker to know

that their attacks are unsuccessful or if you want the attacker to continue to attack one of your systems in an attempt to gather more evidence. It is also useful when deploying a [honeynet](#) so that only the outbound traffic, from the honeynet, is "scrubbed".



**Figure 3**

An inline NIDS offers the great capabilities of a regular NIDS with the blocking capabilities of a firewall. As with most NIDS, the user can monitor, in this case protect, many servers or networks with a single device. This can be both a blessing and a curse. If the system were to fail or crash the traffic would not get through the device. (ISS Guard actually fails open when the product crashes). If you are concerned about uptime and SLAs, this might cause a big issue for your network.

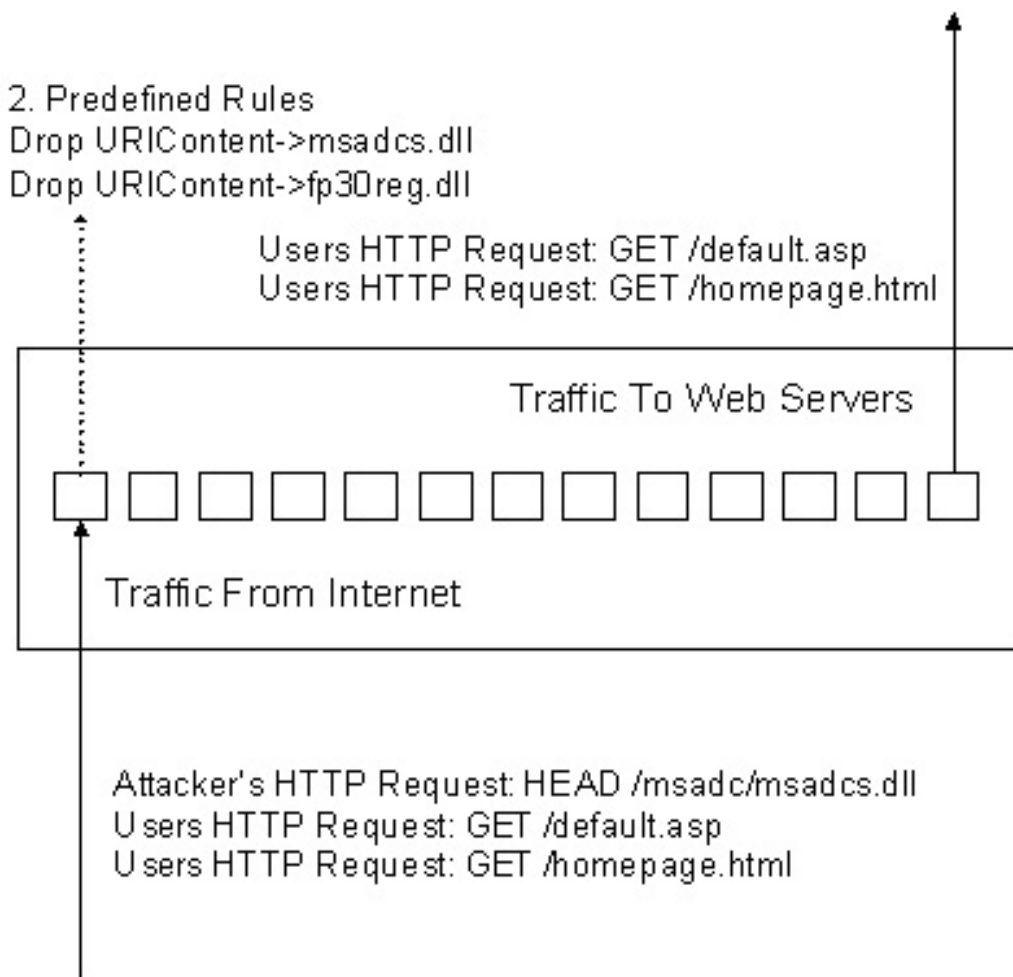
These IPSs will feel most comfortable in the hands of security teams that already deal with NIDS. Because these IPSs are variants of existing NIDS, writing rules for them is very easy and offers a way to catch new attacks. To block unknown attacks with a signature-based inline NIDS, you would have to have some generic rules, like looking for NOOP sleds. This does not, however, stop all new attacks. In the case of a protocol anomaly inline NIDS, it will be able to stop unknown attacks based on the protocols that it is able to decode, as well as the knowledge of those protocols. Both these systems have the drawback of only being able to protect certain applications that are in wide use (such as, IIS, Apache, etc.). If you have an application that

uses either one of these Web servers, the inline NIDS will offer no protection for bad programming or misconfigurations. They provide a generic level of protection, but they still have a great place in protecting systems that are hard to protect (i.e. AS400, Tandem, mainframes). For many of these systems there is no other form of protection or monitoring.

## **Layer Seven Switches**

Traditionally switches were layer 2 devices. But now, with the high demands on networks and servers to deliver bandwidth intensive content, layer seven switches are on the rise. Network engineers mostly use these switches to load-balance an application across multiple servers. To do this they can inspect layer seven information (i.e. HTTP, DNS, SMTP) to make switching or routing decisions. In the case of a Web application, they can inspect the URL to direct particular request to specific servers based on predefined rules. The companies that make these devices have now started to add security features to their products, like DoS and DDoS protection.

These devices are built on custom hardware to deliver high performance, even in the most demanding networks. These systems can easily handle gigabit and multi-gigabit traffic. They work similarly to a signature-based inline NIDS when it comes to stopping attacks. Placing these devices in front of your firewalls would give protection for the entire network. That said, the drawbacks are similar to the inline NIDS. They can only stop attacks that they know about (Figure 4), but they do offer a way to write signatures just like a NIDS. The one attack that they can stop that most others can't are the DoS attacks. These devices have the horsepower to mitigate DoS attacks without affecting the rest of the network performance. They offer security as a byproduct of what they do in regards to inspecting layer seven content for routing/switching decisions.



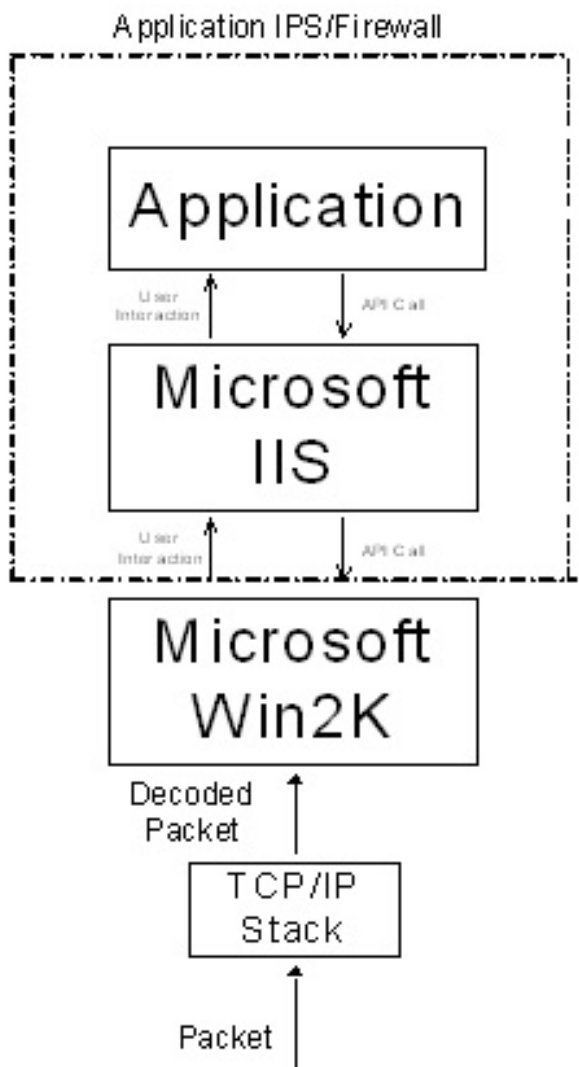
**Figure 4**

Layer seven switches also are configurable for redundancy. They can be configured in a hot standby mode or in a load-balancing mode. This feature is not found in any of the other IPSs. While their ability to stop attacks may not match up with the last two technologies that this article will discuss, they do offer many other features that can make them worth the money. Since most of these devices have origins in the networking world, they can load balance servers, firewalls and NIDS, route using BGP, OSPF and RIP and are geared towards guaranteeing speed and uptime. A lot of the security features offered are available as a software upgrade, so it may be possible to use an all ready existing switch that is used in the network.

## Application Firewalls/IDS

Application firewalls and IDSs are usually marketed as an intrusion prevention solution rather than a traditional IDS solution. These IPSs are loaded on each server that is to be protected.

While the overhead in management of this many IPSs could be daunting, it does pay off. These types of IPSs are customizable to each application that they are to protect. They don't look at packet level information; rather, they look at API calls, memory management (i.e. buffer overflow attempts), how the application interacts with the operating system, and how the user is suppose to interact with the application (Figure 5). This helps protect against poor programming and unknown attacks.



**Figure 5**

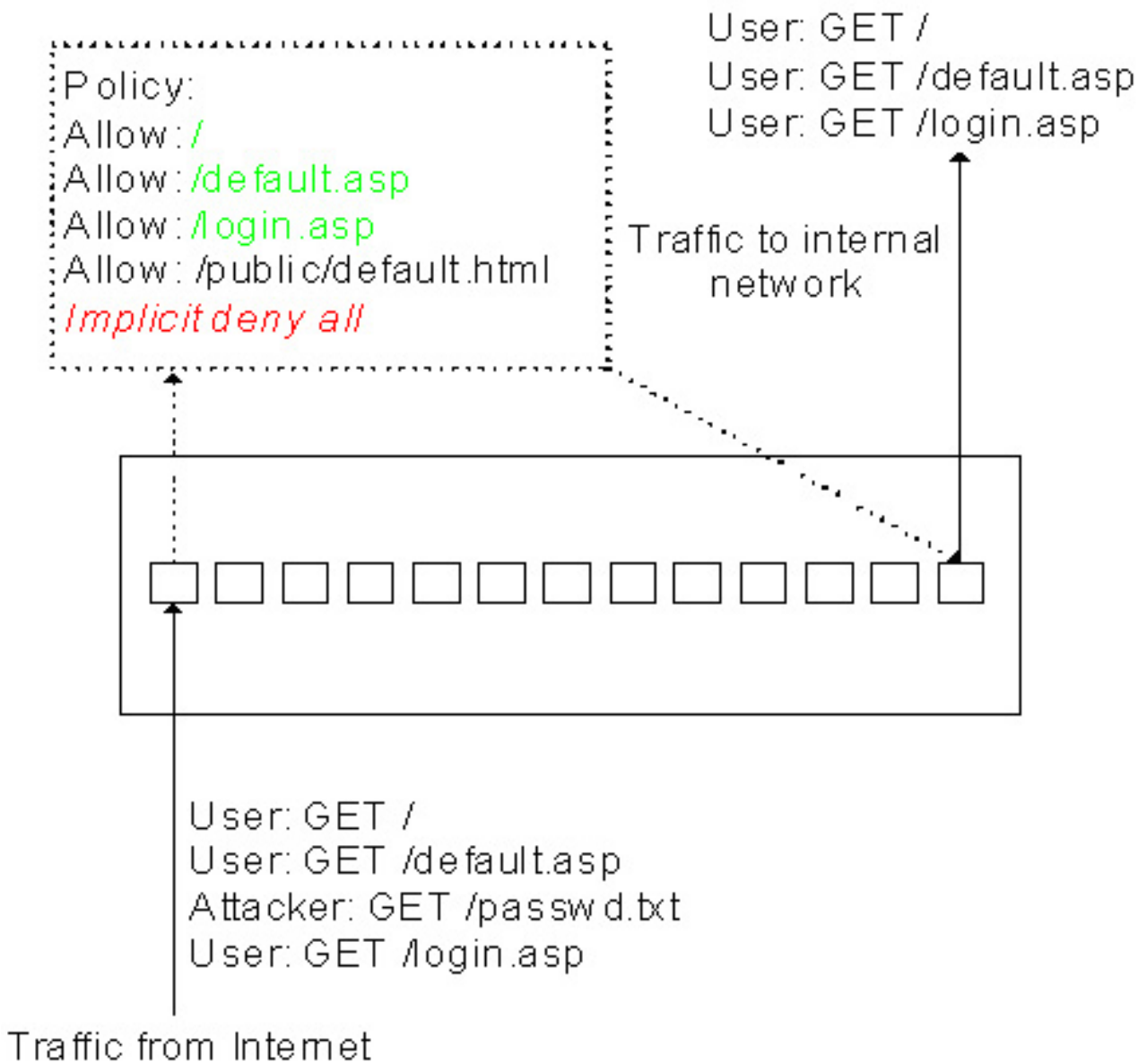
Application IPSs can profile a system before protecting it. During the profiling phase, the IPS can watch the user's interaction with the application and the applications interaction with the operating system to determine what legitimate interaction looks like. After the IPS has created a profile, or policy, of the application, it can be set to enforce it. Unlike the inline NIDS or the layer seven switch, the application layer IPSs are a "fail close" type of system, which means that if some action is attempted that is not predefined then the IPS will stop the action from taking place. One drawback of this type of system is that when an application is profiled, the

user needs to make sure that every aspect of the application is used so that the application IPS can see the interaction and write a rule for it. If thorough testing of the application is not carried out, then some parts of the application may not work. Another drawback is that when the application is updated it might have to be profiled again to ensure that the policy does not block legitimate use.

By profiling the application prior to enforcing the policy you can get very granular with the policies that are made. This type of IPS offers the one of the greatest amounts of protection for custom written applications. Since each application firewall/IPS is loaded on each physical server you can customize each policy so that it can offer the greatest amount of protection. Of the IPSs that are discussed in this paper, this one is the only one that looks at how the application interacts with the operating system and memory management on the server.

## **Hybrid Switches**

This type of technology is a cross between the host-based application firewall/IDS and the layer seven switch. These systems are hardware based in front of the servers(s), like the layer seven switch, but instead of using a regular NIDS type of rule set, hybrid switches use a policy similar to the application IDS/firewall (Figure 6). They inspect specific traffic for malicious content defined by the policy that is configured. Some of these companies offer application layer vulnerability assessment products that compliment their IPS. An application can be scanned with their vulnerability assessment product and the information from that scan can be imported into their IPS as a policy. This saves the security administrator a lot of time configuring the policy to defend the application.

**Figure 6**

The hybrid switch works in a similar manner to the layer seven switch, but instead of only having a handful of signatures that can block attacks aimed at the Web server, it can have detailed knowledge of the Web server and the application that sits on top of the Web server. It also fails close if the user's request does not match any of the permitted requests. If the application that is being protected receives a lot of traffic, the hybrid switch can be combined with a layer seven switch to offer even higher performance. The layer seven switch can be configured to send certain types of requests to the hybrid switch for further inspection, decreasing the amount of requests that the hybrid switch has to look at and increasing performance.

## Deceptive Applications

Now we will look at a type of technology that does things a bit differently. The methodology is not new, it was first discussed in 1998 at a RAID conference. This type of technology uses some deceptive practices. First, it watches all your network traffic and figures out what is good traffic (Figure 7), similar to the profiling phase of the application firewall/IDS. Then, when it sees attempts to connect to services that do not exist or at least exist on that server, it will send back a response to the attacker (Figure 8).

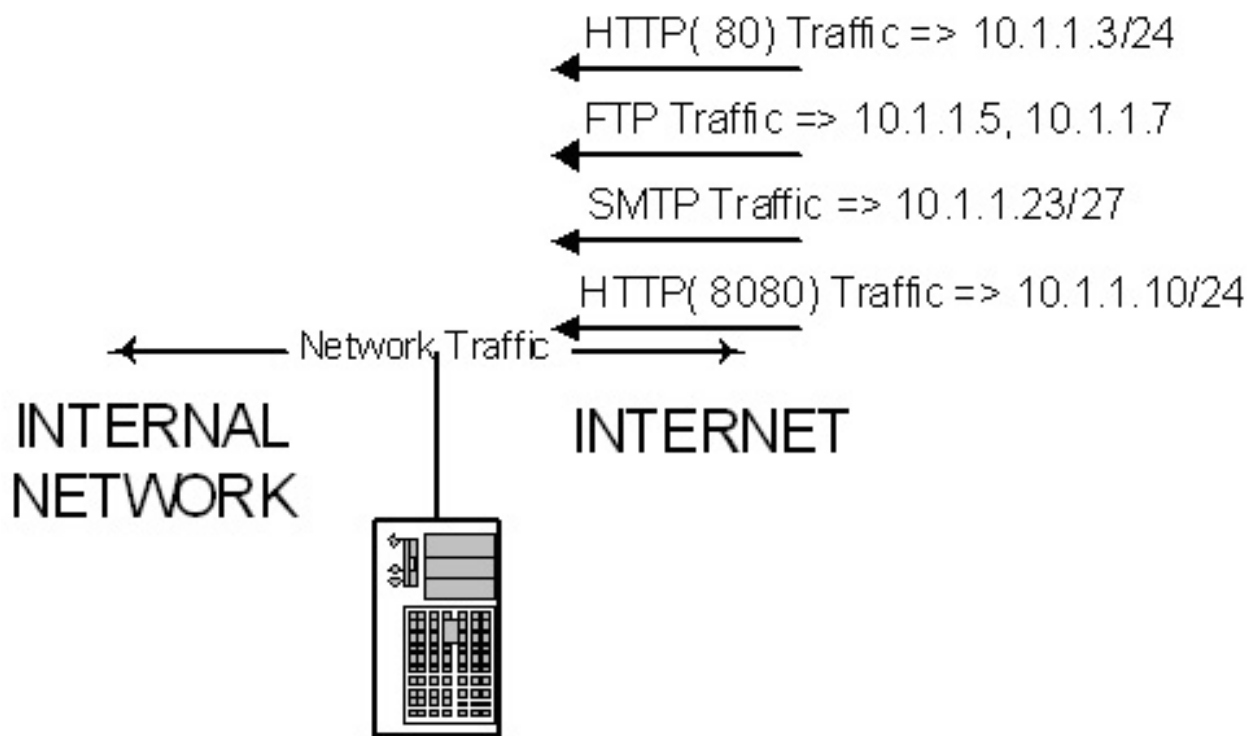
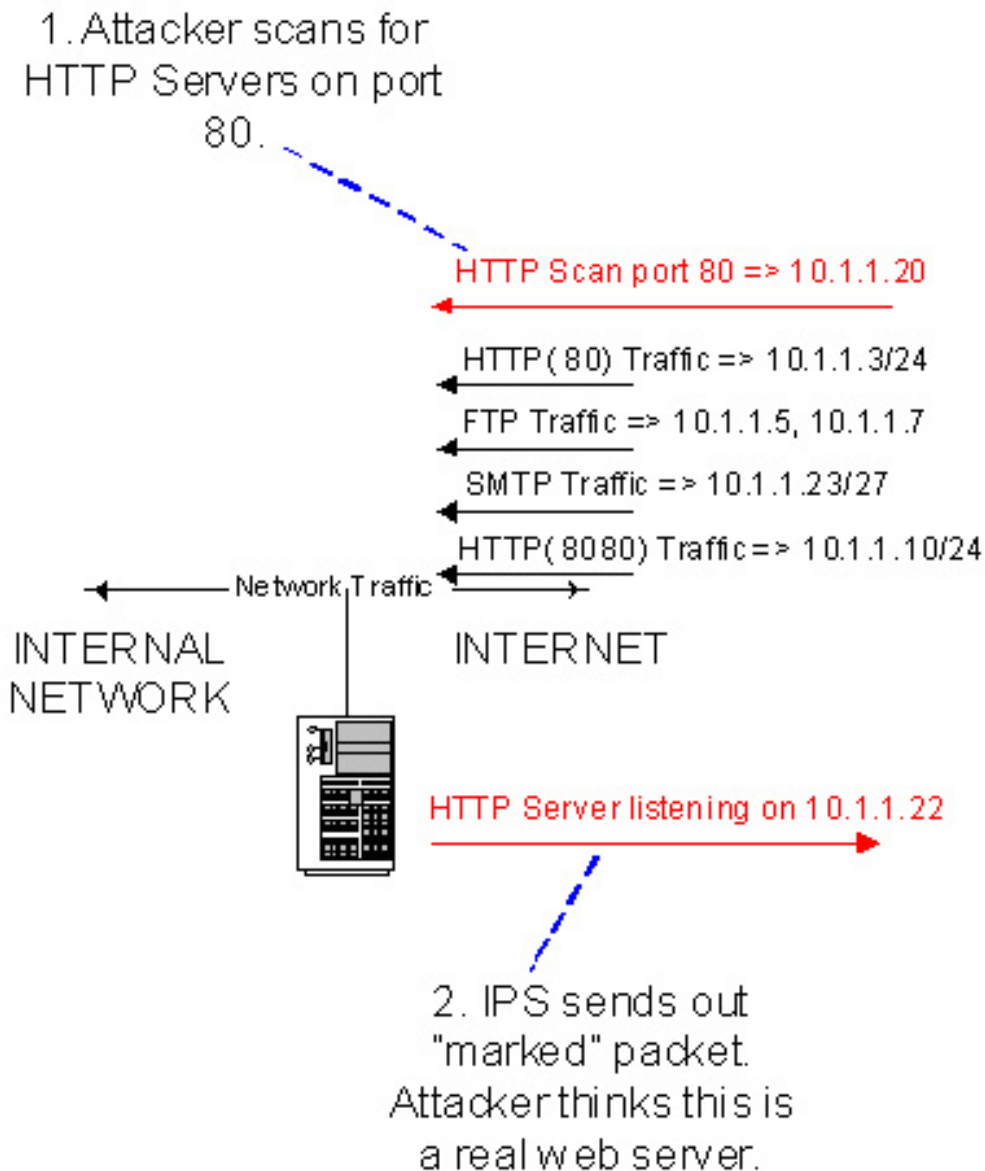


Figure 7



**Figure 8**

The response will be "marked" with some bogus data so that when the attacker comes back and tries to exploit the server the IPS will see the "marked" data and stop all traffic coming from the attacker. The attacker does not have to try to attack the fake web server to be detected. Based on the configuration of the product, there can be "marked" data within the packet data. This would catch an attacker even if he/she was to attack a legitimate web server.

## Conclusion

Each type of IPS offers a different level of protection, and each IPS has its pros and cons. By looking at the way that each IPS works, you should be able to figure out which solution would be best fitted for your needs. As is the case with most security technologies, there is no "one

size fits all" solution. You might even find yourself using more than one of the solutions that we looked at. For instance, you might use a layer seven switch in front of your Internet firewall to defend against DoS attacks and known attacks, using application layer firewalls/IPS software or hybrid switch to protect your Web servers and an inline NIDS to protect your AS400 or Tandems. This niche in the information security realm is relatively new so new technologies and products will be on the rise.

## Relevant Links

### Inline Network Intrusion Detection Systems

[ISS Guard](#)

[hogwash](#)

[Netscreen](#)

[TippingPoint](#)

[Intruvert](#)

### Layer Seven Switches

[Radware](#)

[TopLayer](#)

[Foundry](#)

### Application Firewalls/IDS

[Okena](#)

[Entercept](#)

### Hybrid Switches

[Appshild](#)

[Kavado](#)

### Deceptive Applications

[Forescout](#)

[Privacy Statement](#)

Copyright 2006, SecurityFocus