

# Intrusion Detection Systems (IDS)

An Intrusion Detection System (IDS) detects network traffic that attempts to circumvent or destroy the security policy of a networked computer environment in attempt to deteriorate the integrity, confidentiality, and availability of computer resources.

## What does that mean to you?

The computers you have online to serve your business needs are potential targets for those who wish to use those systems for other purposes at your expense. Your best defense against these threats to your business is to set up levels of security to protect your online resources – patching the OS and its applications, limiting access to your systems with a firewall and implementing a well-managed IDS to detect threats.

## I have a firewall. Why do I need an IDS?

Network traffic is not always what it seems. An IDS looks at all the incoming traffic to your computers for thousands of known ways to bypass firewall and computer security. Just because traffic is coming in on TCP port 80 (standard web traffic) does not mean that it is coming from someone innocently attempting to view your webpage. It could be a carefully crafted string of binary code that tricks your webserver into installing a malicious application on your computer—a Trojan allowing administrative access to your system. The firewall did its job, but your system has now been compromised. Or, perhaps the attack is against the firewall itself. The variety of attacks is endless.

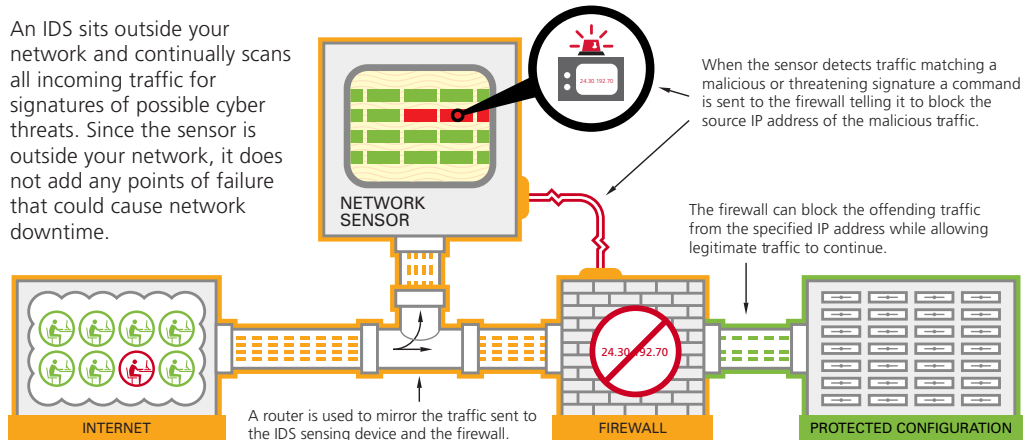
## Where does patching fit in?

Patching is your first level of defense for your operating system and applications; however, writing code to patch operating systems and applications can be a very complex and time-consuming process. An exploit for your online application can be created long before a patch is available to protect against it, but a signature to detect an exploit is relatively quite simple to create and implement. A signature can also detect entire families of exploits that all share similar characteristics, so your systems can be protected against many variations of the same attack.

## An IDS will help your bottom line.

An IDS has tremendous overhead to maintain effectively because it requires the attention of a high-level security engineer to update new exploit signatures and monitor its activity. By using a managed IDS solution at Rackspace, you are allowing us to distribute that cost over many systems and pass those savings along to you. According to SecurityFocus, the cost of administration of an IDS is over ten times the cost of the hardware per year. This makes an IDS solution at Rackspace one of the most cost-effective outsourcing decisions you can make for your business.

## How an Intrusion Detection System Protects Your Hosted Solution



MODIFIED DATE: 1-03-2008