



# Intrusion Prevention Systems vs Application Firewalls

## Four Key Differences Your IPS Vendor Doesn't Want You to Know

Today's knowledgeable hackers have advanced well beyond scanning for open ports on network firewalls and are now targeting applications directly. They have devised sophisticated attacks that easily circumvent traditional intrusion detection systems (IDS) and network firewalls.

This trend has given rise to two different types of next-generation security products — Intrusion Prevention Systems (IPS) and Application Firewalls. Both IPS products and application firewalls are capable of blocking attacks that bypass traditional firewalls. And both have been successfully deployed in some of the largest networks in the world.

There are, however, some critical differences. To begin with, IPS products tend to focus their protection broadly across the network. As a result, they are primarily useful for holding off well-publicized network exploits while IT works to get the necessary patches in place.

Application firewalls, on the other hand, specialize in deep protection of mission-critical web applications. They arose from the realization that transactional web applications give anyone with a browser unprecedented access to critical business data — employee records, customer transactions, credit card

numbers, social security numbers and partner information to name just a few.

With millions of moving parts, *web applications are almost always the weakest link in any company's security strategy*, allowing anyone with a browser and a little time on his hands to access, view and even alter critical data without the company even knowing a compromise occurred.

Unlike most network-based attacks, which result in a temporary productivity loss, the damage from a single successful application attack can be devastating, exposing critical customer data, violating privacy laws and even exposing company executives to jail time.

Today's IPS products are clearly an improvement over their IDS predecessors and can be useful as part of an overall enterprise security strategy. Their superficial approach to application security, however, simply isn't sufficient when it comes to protecting mission-critical business data.

If you are considering an IPS product to protect mission-critical web applications, here are four important facts your IPS vendor probably doesn't want you to know.

## **Fact #1:** **IPS products have no knowledge of application state**

IPS products are network-level detection technologies that have no knowledge of application state. As a result, they are entirely incapable of blocking some of the most dangerous application attacks in existence.

Attacks such as cookie tampering, session hijacking, form field tampering and parameter tampering are exploits that simply cannot be blocked unless a security product has full knowledge of application state.

Application firewalls don't have this limitation because they fully terminate and proxy every connection, giving them complete visibility into each unique user session. As a result, they deliver full application state validation and policy enforcement, blocking all attack attempts, regardless of the specific method.

## **Fact #2:** **Most IPS products cannot handle encrypted or encoded traffic**

IPS vendors love to talk about stopping application attacks. What most fail to mention, however, is that any attack that is SSL encrypted or uses common encoding techniques will easily bypass their protection. Because most IPS products cannot see inside encrypted sessions or interpret application encoding schemes, they have zero ability to protect the most mission-critical applications in your network.

Good hackers know this and take full advantage of it. They love SSL because it hides their activities from the security snoops. Hackers also love encoding schemes like URL encoding, Unicode and hexadecimal because

they make it easy to disguise attacks that might otherwise be recognized.

When a hacker types %27 into his browser, for example, your application server instantly recognizes it as a tick [''] mark. Your app server also recognizes %2F as a [/], %2E as a [.] and %3D as an [=]. All of these characters can be used to launch dangerous attacks on backend data. Unfortunately, even basic encoding like this fools most IPS products, rendering their application protection useless against all but the simplest attacks.

Application firewalls, by contrast, were designed from the ground up with web applications in mind. As a result, they automatically decrypt and normalize all traffic before attempting any security inspection. This gives them complete visibility into both static and dynamic application content and allows them to perform deep inspection on the entire session payload, including headers, URLs, parameters and form fields.

## **Fact #3:** **IPS products only protect against well-known attack variants**

Most modern IPS products share a common heritage with signature-based IDS (intrusion detection system) solutions. They watch incoming network traffic and compare it against a database of signatures describing all previously known exploits. If a close match is discovered, the traffic is blocked.

Unfortunately, this signature-based approach, by definition, runs one step behind the hackers. To keep their protection current, IPS vendors must wait for each specific new threat to be discovered before they can begin building and distributing a new signature to detect it. To make matters worse, these signature-based

systems are often easily fooled by making changes to the pattern of known attacks. Switch a few bits around here and there, and your new attack variant will likely fly right past an IPS system because it's not a close enough match to any known exploit in its database.

While some IPS vendors have added basic "behavior" or "anomaly" detection to reduce the likelihood of missing new variants, they know that if they loosen the rules too much, they will fall victim to the same false positive problem that plagued their IDS predecessors. The fact remains that most IPS products are still highly dependent on a database of well-known attacks for their protection.

Application firewalls, by contrast, use a positive security model. Rather than trying to define every possible bad thing that could occur, they "learn" legitimate application behavior on-the-fly, ensuring that every user request conforms to expected application usage and that only valid traffic is passed to backend servers.

This breakthrough is accomplished by applying bi-directional deep inspection to all traffic. Unlike IPS systems which look only at *incoming* packets as they cross the wire, application firewalls have the ability to inspect all traffic going in *both directions*, giving them full, real-time visibility into what each application expects to see for each unique session.

This bi-directional inspection architecture gives application firewalls the unique ability to block both known and unknown application attacks with no signatures and no false positives.

## **Fact #4:** **IPS products cannot protect customized web applications**

IPS protection is also limited to well known applications and platforms. IPS products can be

useful, for example, in protecting unpatched vulnerabilities in widely-used platforms such as Microsoft, Oracle or Apache.

Unfortunately, as many as 75% of all attacks today target vulnerabilities in customized application code built on top of these platforms, not the lower-layer exploits in the platforms themselves. When it comes to customized application code, there ARE no signatures or patches. As a result, IPS products do nothing for custom apps.

This problem is often compounded by the fact that custom web applications themselves are dynamic and complex, so new holes are almost certain to open up the moment old ones are fixed. Most companies have countless web applications scattered throughout their IT environment, each connecting to mission-critical databases. Many were written by ex-employees, contractors or third-party outsourcers, most of whom have never had formal security training.

Because they learn legitimate application behavior in real time, application firewalls are able to block both known and unknown attacks in both known platforms and customized application code.

Bottom line — without an application firewall, your application code IS your perimeter. Unless you write and maintain perfect code, hackers can exploit those vulnerabilities to gain direct access to the crown jewels of your company.

## **About NetContinuum**

NetContinuum helps IT organizations secure and optimize the delivery of web applications. The company was founded in 1999 and is headquartered in Santa Clara, California. For more information, please call +1.408.961.5600 or visit [www.netcontinuum.com](http://www.netcontinuum.com).