JULY 2020

WHAT AN IPS IS,
AND WHAT AN IPS ISN'T

INTRUSION PREVENTION SYSTEM (IPS)

NETWORK BOX USA
cybersecurity done right

HOUSTON TX

2020

What an Intrusion Prevention System (IPS) is, and what it isn't

“

I recently discovered how, on the cyberfront, people frequently misunderstand what an Intrusion Prevention System (IPS) is and isn’t.

What it can and can’t do.

The level of protection it affords them.

It made me realize why so many companies do not have a Web Application Firewall (WAF) when they so very badly need it.

”

PIERLUIGI STELLA
chief technology officer

SO WHAT'S AN IPS?

FOR STARTERS

IPS is a layer 3 tool.

It monitors packets inbound and outbound, one packet at a time. That's very useful for deep packet inspection, but it does have limitations. The primary one being that it is what it is – a layer 3 tool. As such, it only understands packets, single packets. Not transactions. Not layer 7 protocols (i.e., HTTP), and definitely not applications.

But, that said, what an IPS isn't is equally as important as what an IPS is. It's **NOT** a proxy. It can't intercept traffic for proper scanning.

AN IPS SCANS "ON THE FLY".

Meaning decrypting encrypted traffic is not as simple as it might be for a proxy, and therefore, it may not be able to fully protect your server if port 443 is open from the Internet.

IPS is supposed to work at wire speed, without triggering a detectable latency in the data stream. Introducing decryption at the IPS level and still keeping acceptably undetectable latency would likely require massive hardware for small transactions.

WHY WE'RE #1

10K

we deploy 10,000 new signatures every day, all PUSHED to our devices within 3 seconds

99.78%

we catch spam with an impressive success rate of 99.78%, highest within the industry today

125

we partner with over 125 threat intelligence companies to create honey pots and collate data

INTRUSION
PREVENTION SYSTEM (IPS)

WHAT AN IPS ISN'T

When a browser connects to a server, the first thing to happen is the server issues a key for that session.

If the same user (from the same workstation, from the same browser even) opens a new session (new tab, new window), and connects to the same server, encryption of that new session is completely different from encryption of the previous session.

Essentially, each session is encrypted with its own key.

A unique key issued by the server.

EVERY SINGLE TIME A NEW SESSION IS INITIATED.

As such, deciphering and analyzing the data inside an HTTPS stream requires proper decryption. And this is only possible by undertaking a "man in the middle attack". Why? Because in order to open the encrypted traffic, you must have the key.

It's the nature of encryption.

Otherwise, if anyone could open that stream, what would be the point of having encryption in the first instance?

INTRUSION PREVENTION SYSTEM (IPS)

WHAT AN IPS ISN'T

So, your IPS simply cannot scan incoming encrypted traffic "attacking" your server.

It is incapable of scanning such traffic even if you're the client and the server is outside of your network. But for that, most of us (hopefully all) already have in place what we call an outbound proxy.

We use it for policy enforcement.

And if we have an updated one, we have a vendor-provided public certificate which is installed on our client, allowing the proxy to make outbound HTTPS connections on our behalf.

AND SCAN THAT TRAFFIC.

But when it comes to inbound traffic (when you have a server that's yours and it needs protection against internet attacks), it's a different story.

A regular proxy can't protect you since it's built to protect the client's browser from infections on the server.

Here, we're talking about quite the opposite. Protecting a server from attacks coming from a client. For this, you will need what is called an inbound proxy.

Or what's most commonly known as a WAF (Web Application Firewall).

SO WHAT'S A WAF?

FOR STARTERS

A WAF is a layer 7 tool.

A proxy that understands HTTP protocol.

A WAF is able to intercept browser calls to a web server in order to protect it from things like SQL Injections. A recent example is Citrix Vulnerability – CVE-2019-19781.

Citrix uses HTTPS.

An IPS that has the proper signature to block exploits to this vulnerability can't do its job properly because the traffic's encrypted.

A WAF INTERCEPTS THOSE CALLS.

A WAF would decrypt the traffic, pass it to the IPS, and together, they block the malicious traffic.

Major difference, as you can see.

WHY WE'RE #1

SRC

we have our own Security Response Center (SRC) and attained 3 ISO certifications (27001, 20000, 9001)

95%

we maintain a stellar client ticket response time of 7 minutes 19 second and a 95% client retention rate

16

we own and operate 16 security operations centers worldwide and have won over 140 global awards

INTRUSION
PREVENTION SYSTEM (IPS)

WHAT A WAF DOES

A WAF does a whole lot more to protect your servers.

But the main idea here is that most traffic is encrypted. And in order to scan for attacks, you'd need to decrypt it.

Only a layer 7 tool like the WAF can do that.

A WAF would be doing HTTPS offloading meaning you'd install the web server private CA, Certs and Keys on the WAF, and the remote browser would be talking to the WAF.

NEVER TO THE SERVER.

The WAF would then be able to decrypt the traffic, and analyze it for threats. If the traffic's deemed safe, then it'd re-encrypt it and pass it on to the server (actually, if the server's locally connected to the WAF, this second encryption may not even be necessary).

So next time you're installing a web server and someone says just an IPS is sufficient to protect it, you know now that is completely not true.

If you really want to protect a web server, you need a tool which understands the layer 7 protocols a particular server is currently using, and can decrypt the traffic in order to scan for threats.

And that tool is the WAF.

IS YOUR NETWORK SAFE?

DETECT . DIAGNOSE . DECIDE

Is your cybersecurity being done right? **Is your data protected?**

Cyber threats are **coming at you**, faster than ever before.

Are you equipped?

OUR STORY

Since we opened doors back in 2000, none of our clients have ever been breached.

NOT A SINGLE ONE.

It's not bragging if you can prove it.

And we can.

FULLY MANAGED

FULLY MONITORED

FULLY SCALEABLE

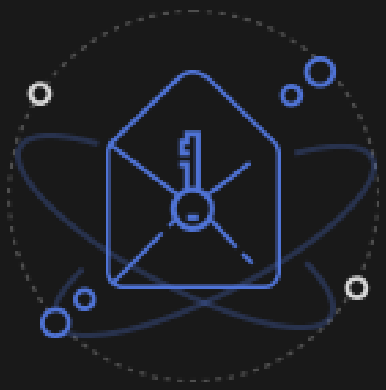
24/7/365

NETWORK BOX USA
cybersecurity done right
info@networkboxusa.com • www.networkboxusa.com

YOUR #1 MSSP PARTNER

OUR SOLUTIONS

> SIEM+
> SASE
> SD-Wan
> Zero Trust Assessment
> Managed Cloud Email Security
> Dark Web Monitoring
> IP & Domain Reputation Monitoring
> Web Browsing Protection
> Managed Cloud Proxy
> Web Application Firewall
> UTM
> Security Risk Assessment
> Vulnerability Assessment
> Penetration Testing
> Forensic Analysis
> Incident Response & Remediation
> ISP Brokerage



FREE DEMO?

info@networkboxusa.com

MORE DETAILS?

info@networkboxusa.com

ISO CERTIFICATIONS

NETWORK BOX USA
cybersecurity done right
info@networkboxusa.com • www.networkboxusa.com