Why Do You Need a SPI Firewall?

TechRounder PDF Edition

Live article: https://www.techrounder.com/security/why-do-you-need-a-spi-firewall/

By Vipin PG | Published February 15, 2022 | Updated January 4, 2026 | Format: Explainer | 4 min read

In brief

A firewall is one of the most important instruments for defending yourself against numerous web-based threats and viruses. Not all of them, however, are equally potent and safe.

A firewall is one of the most important instruments for defending yourself against numerous web-based threats and viruses. Not all of them, however, are equally potent and safe. One of the alternatives you have is to use SPI protection. Let’s look at how it functions and how effective it is.

What is SPI?

You may wonder: "What is SPI Firewall, and why do I need it?" An SPI (stateful packet inspection) firewall protects you by comparing incoming packets to existing connections.

On the other hand, a stateless firewall examines static values such as source or destination addresses. The packet’s connection traffic is not taken into account. It uses the same rules for all packets and does not know its connection.

These firewalls can’t be set up to open and close connections independently. They also don’t validate packets and can’t tell if they’re coming from a legitimate IP address. As a result, they are less secure than SPI security, but they are usually faster (learn more about a firewall).

How Does an SPI Firewall Do Its Job?

The properties of each connection can be remembered by an SPI protection firewall, which can then be used to determine the validity of a packet.

It keeps track of the data it gathers by analyzing packets and implementing rules. As a result, it sees the contents of a packet and its larger context.

The SPI firewall does not have to inspect every packet thoroughly because of its memory; hence it is faster than deep packet inspection (DPI).

The latter deconstructs the packets to see if they are correctly created and include any malicious content.

Network management, security, data mining, and internet control are just a few of the applications for DPI. It gives you security at the cost of quickness.

Traditional stateless firewalls defend your computer or network from malicious or superfluous network traffic, preventing data and third parties from gaining access to your personal data.

However, they are limited because they do not authenticate packets and hence cannot determine whether they originate from a real IP address.

Because it considers the nature of the incoming packet, including its origin, an SPI security firewall provides a better level of protection (within your network or from the Internet). It also keeps track of this data and creates custom rules to prevent illegal access to your network.

How can SPI Firewall Regulate Network Access

When an incoming packet attempts to acquire network access, an SPI firewall stores the identifiers of all the packets its network transmits, allowing it to determine whether it is a response to a packet sent from its network or if it is unsolicited.

An access control list, a database of trusted entities, and their network access privileges can all be used by an SPI firewall. When the SPI protection examines a packet, it can refer to the ACL to see if it came from a trusted source and, if so, where it should be routed inside the network.

How can an SPI Firewall Respond to Suspicious Traffic?

The SPI firewall can be configured to drop any packets delivered from sources not included in the ACL, preventing a denial-of-service attack in which an attacker floods the network with incoming traffic to saturate its resources and prevent it from responding to valid requests.

SPI firewalls can also examine packets for characteristics similar to those used in known hacking exploits, such as DoS attacks and IP spoofing, and drop any packet that it recognizes as potentially malicious, according to Netgear’s "Security: Comparing NAT, Static Content Filtering, SPI, and Firewalls" article.

What Are Some Benefits of an SPI Firewall and Why You Need It?

Adding hardware SPI protection to your business has numerous advantages. It can, for example, utilize an access control list, allow or deny connections based on a trusted user database, and restrict network privileges. Other advantages include:

- Its ability to monitor the status of several network connections, including TCP and UDP
- Its ability to inspect packet states, such as source, destination, and other data, to determine their authenticity.
- Its capacity to protect against malicious packets could lead to a data breach at a much higher level.
- In today’s world, an SPI firewall is a must-have for most enterprises. It can prevent unwanted remote access to LAN computers and warn employees about unusual worms, viruses, and DDoS attacks .

Setting up a hardware firewall, on the other hand, necessitates specialist expertise to arrange connections appropriately. You might begin the procedure by consulting an experienced IT specialist or a cybersecurity firm.

SPI firewalls are indispensable for internet users. Specifically, people with crucial business and other personal data on their systems. Therefore, it should be on the priority list of your IT team to set it up and monitor this SPI protection for you.

References

1. veepn.com - blog / what-is-spi-firewall - https://veepn.com/blog/what-is-spi-firewall/
2. imperva.com - learn / ddos - https://www.imperva.com/learn/ddos/denial-of-service/