CS-048 · Network

Intrusion Prevention Systems (IPS)

In-line systems that detect attacks and actively block them in real time.

Executive Summary

An intrusion prevention system sits directly in the traffic path, inspects activity for signs of attack, and can block malicious traffic in real time. It is the active counterpart to an intrusion detection system, trading pure observation for the ability to stop threats. Because it can drop legitimate traffic if misconfigured, careful tuning is essential.

What It Is

An intrusion prevention system, or IPS, is a security control placed in line with network traffic so that every packet passes through it. Like an intrusion detection system it inspects activity using signatures of known attacks and anomaly models of unusual behavior, but unlike a detection-only system it can take action, such as dropping the offending packets, resetting the connection, or blocking the source. Because it is in the traffic path, an IPS can prevent an attack from reaching its target rather than merely reporting it afterward. Many modern security platforms, including next-generation firewalls, integrate IPS capabilities directly, and an IPS can also run on individual hosts.

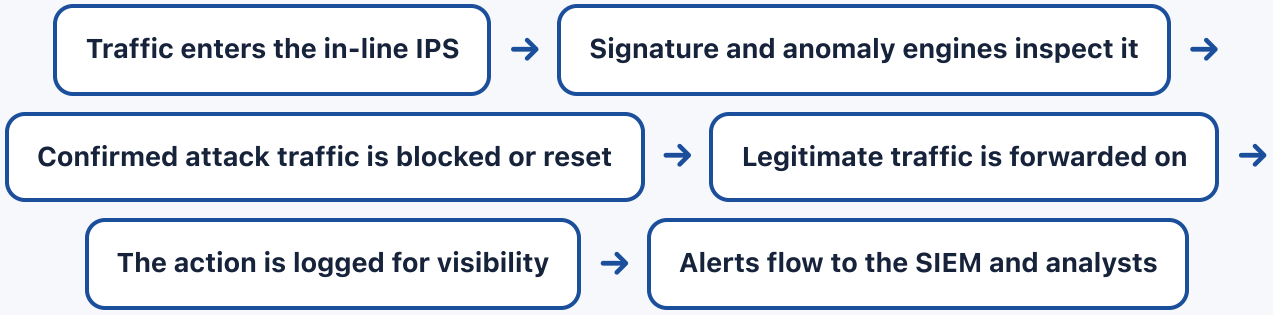
Why It Matters

Detection tells you an attack happened; prevention tries to stop it before it succeeds. For threats that move quickly, such as automated exploitation of a known vulnerability, blocking in real time can be the difference between a blocked probe and a breach. An IPS also buys time to patch, since it can shield a vulnerable service from known exploits while a fix is being deployed, a practice called virtual patching. The trade-off is that an in-line control can disrupt legitimate traffic if it blocks the wrong thing, so it carries operational risk that a passive sensor does not. Balancing protection against the risk of false blocks is a core skill for security engineers.

How It Works

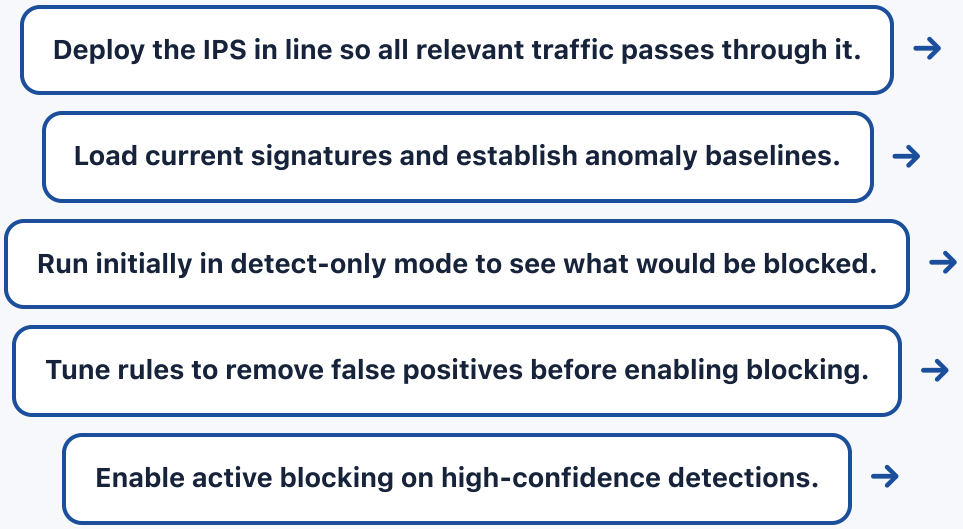
Because it is in line, an IPS evaluates each packet or session as it passes and decides whether to permit or block it. Signature-based prevention matches traffic against known attack patterns and drops matches, which is reliable for known threats. Anomaly-based prevention blocks activity that deviates sharply from a learned baseline, which can stop novel attacks but risks false positives that interrupt real users. To manage that risk, teams often deploy an IPS first in a detect-only mode to observe what it would block, tune the rules, and only then enable active blocking on high-confidence signatures. When it acts, the IPS logs the event so analysts retain full visibility, and its alerts typically feed a SIEM.

Architecture Diagram



An in-line IPS inspects each packet, blocks confirmed attacks, forwards legitimate traffic, and logs every decision.

Visual Workflow



Log all actions to a SIEM and review blocked events regularly.

Common Attacks

- Evasion through fragmentation or obfuscation to avoid signature matches
- Encrypted traffic that conceals attacks from inspection
- Triggering false-positive blocks to cause a self-inflicted denial of service
- Novel exploits with no signature that only anomaly logic might catch
- Overloading the in-line device to degrade or bypass inspection

Common Mistakes

- Enabling aggressive blocking before tuning, disrupting legitimate traffic
- Placing the IPS where it cannot see critical traffic
- Leaving signatures outdated so protection lags current threats
- Ignoring the availability risk of an in-line device failing or overloading
- Treating the IPS as complete protection and neglecting other layers

Best Practices

- Start in detect-only mode, then enable blocking after tuning
- Block on high-confidence signatures and monitor anomaly rules before enforcing
- Keep signatures and detection content current
- Plan for availability, including fail-open or fail-closed behavior on failure
- Use virtual patching to shield unpatched services while fixes are deployed

Quick Checklist

- [x] The IPS is placed in line with visibility into critical traffic
- [x] Blocking was enabled only after a tuning period
- [x] Signatures and detection content are up to date

- [x] Failure behavior (fail-open or fail-closed) is deliberately chosen
- [x] Blocked events are logged and reviewed for false positives

Recommended Tools

Network intrusion prevention appliance
Inspects and blocks malicious traffic in line

Next-generation firewall with IPS
Combines filtering and prevention in one platform

Host-based intrusion prevention agent
Blocks malicious behavior on an individual system

SIEM
Correlates IPS actions with broader security telemetry

Industry Standards

NIST SP 800-94
Guide to intrusion detection and prevention systems

MITRE ATT&CK
Frames the adversary techniques prevention should counter

PCI DSS
Calls for intrusion detection or prevention at network boundaries

Career Relevance

Deploying and tuning an IPS is a core responsibility for network security engineers and security engineers, who must balance protection against the risk of blocking legitimate traffic. SOC analysts investigate IPS actions, and cloud security engineers apply equivalent in-line protections in virtual environments. IDS and IPS concepts are staples of security interviews across the roles that AI-Governance-Jobs.com serves.

Interview Questions

- How does an IPS differ from an IDS in placement and action?
- Why is a false positive more serious for an IPS than for an IDS?
- What is virtual patching, and how does an IPS enable it?
- Why do teams often run an IPS in detect-only mode before enabling blocking?
- What is the difference between fail-open and fail-closed for an in-line device?

Related Certifications

CompTIA Security+ | GIAC Certified Intrusion Analyst (GCIA) | CompTIA CySA+

Further Reading

- NIST SP 800-94: Guide to Intrusion Detection and Prevention Systems
- MITRE ATT&CK
- CISA: Cybersecurity Best Practices

Key Takeaways

- An IPS sits in line and can block attacks, not just detect them.
- It is the active counterpart to a passive intrusion detection system.
- In-line blocking risks disrupting real traffic, so tuning is critical.
- Detect-only mode first, then blocking on high-confidence signatures, is the safe path.
- Virtual patching lets an IPS shield unpatched services temporarily.

FAQ

▶ **Should I use an IDS or an IPS?**

▶ **What is virtual patching?**

▶ **Can an IPS cause an outage?**

Related Careers

RELATED ROLES

- Network Security Engineer
- Security Engineer
- Soc Analyst

RELATED CERTIFICATIONS

- CompTIA Security+
- GIAC Certified Intrusion Analyst (GCIA)
- CompTIA CySA+

CURRENT OPENINGS

Live roles are on the job board.

Browse all jobs

GUIDES & SALARY

- Career guides
- Role roadmaps
- Salary data
- Career tools

SUGGESTED LEARNING PATH

1. Ground the basics with CS-001 Cybersecurity
2. Study this sheet: **Intrusion Prevention Systems (IPS)**
3. Go deeper: Intrusion Detection Systems (IDS)
4. Go deeper: Firewalls
5. Validate it: work toward **CompTIA Security+**
6. Find the role: browse current openings

RELATED SHEETS

- CS-047 Intrusion Detection Systems (IDS)
- CS-043 Firewalls
- CS-049 Proxy Servers
- CS-052 Wireshark
- CS-001 Cybersecurity