**index**

Contents

|  |  |
| --- | --- |
| Contents | Page |
| Firewall | 2-3 |
| IDS vs IPS | 3-4 |
| Threat Intelligence | 4-6 |
| IT vs OT | 6-9 |

A **firewall** is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

**Firewalls** have been a first line of defense in network security for over 25 years. They establish a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks, such as the Internet

## Types of firewalls

**Firewalls** can either be software or hardware, though it’s best to have both. A software **firewall** is a program installed on each computer and regulates traffic through port numbers and applications, while a physical **firewall** is a piece of equipment installed between your network and gateway.

Packet-filtering **firewalls**, the most common type of **firewall**, examine packets and prohibit them from passing through if they don’t match an established security rule set. This type of firewall checks the packet’s source and destination IP addresses. If packets match those of an “allowed” rule on the **firewall**, then it is trusted to enter the network.

**Next-generation firewalls (NGFW)**combine traditional **firewall** technology with additional functionality, such as encrypted traffic inspection, intrusion prevention systems, anti-virus, and more. Most notably, it includes deep packet inspection (DPI). While basic firewalls only look at packet headers, deep packet inspection examines the data within the packet itself, enabling users to more effectively identify, categorize, or stop packets with malicious data

**Proxy firewalls** filter network traffic at the application level. Unlike basic **firewalls**, the proxy acts an intermediary between two end systems. The client must send a request to the **firewall**, where it is then evaluated against a set of security rules and then permitted or blocked. Most notably, proxy **firewalls** monitor traffic for layer 7 protocols such as HTTP and FTP, and use both stateful and deep packet inspection to detect malicious traffic

**Network address translation (NAT) firewalls**allow multiple devices with independent network addresses to connect to the internet using a single IP address, keeping individual IP addresses hidden. As a result, attackers scanning a network for IP addresses can't capture specific details, providing greater security against attacks. NAT **firewalls** are similar to proxy **firewalls** in that they act as an intermediary between a group of computers and outside traffic.

.

Briefly, an IDS platform can analyze network traffic for patterns and recognize malicious attack patterns. IPS combines the analysis functionality of an IDS with the ability to intervene and prevent the delivery of malicious packets. To put it simply, IDS systems detect, and IPS tools prevent.

An IDS program is a**diagnostic tool**that can recognize malicious network packets and create notifications, but it can’t block the unwanted packets from entering the network. An IPS is a **diagnostic and incident response tool**that can not only flag bad traffic but can also prevent that traffic from interacting with the network.

**What is an IDS and what does it do?**

The IDS monitors network traffic and sends an alert to the user when it identifies suspicious traffic. After receiving the alert the user can take action to find the root cause and remedy it. To detect bad traffic, IDS solutions come in two variations: a **Network Intrusion Detection System**(NIDS) and a**Host Intrusion Detection System** (HIDS)

A NIDS monitors network traffic for security threats through sensors, which are placed throughout the network. A HIDS monitors traffic on the device or system where it is installed. Both of these formats use two main methods of threat detection; **signature-based** and **anomaly-based**

## What is an IPS? and what does it do?

An IPS (also known as an intrusion detection prevention system or IDPS) is a software platform that analyses network traffic content to detect and respond to exploits. The IPS sits behind the firewall and uses**anomaly detection** or **signature-based detection** to identify network threats.

An IPS uses anomaly detection and signature-based detection similar to an IDS. With signature-based detection, the platform scans for patterns that indicate vulnerabilities or exploitation attempts

Likewise, anomaly detection analyses network traffic and identifies performance anomalies. When the system detects an anomaly it will follow up with an automated response.

These solutions also come with automated responses such as**blocking the traffic source address**, **dropping malicious packets**, and **sending alerts** to the user. Fundamentally, an IPS solution isn’t just a diagnostic tool that identifies network security threats but a platform that can respond to them as well.

## Which is better?

Which tool is better primarily depends on your needs. Both IDS and IPS solutions excel in different areas, but there is a strong argument that IPS is a much more comprehensive cybersecurity solution. Many companies are replacing IDS solutions in favor of the automated features that come with an IPS.

The reason why many companies are transitioning to IPS is that IDS solutions are good at raising the alarm during an attack but they can’t stop an attack. Instead, the user has to remediate the incident manually.

# What is Cyber Threat Intelligence?

Threat intelligence, or cyber threat intelligence, is information an organization uses to understand the threats that have, will, or are currently targeting the organization. This info is used to prepare, prevent, and identify cyber threats looking to take advantage of valuable resources.

The great unknown; it can be exciting in many situations, but in a world where any number of cyber threats could bring an organization to its knees, it can be downright terrifying. Threat intelligence can help organizations gain valuable knowledge about these threats, build effective defense mechanisms and mitigate the risks that could damage their bottom line and reputation. After all, targeted threats require targeted defense, and cyber threat intelligence delivers the capability to defend more proactively.

While the promise of cyber threat intel is alluring in itself, it is important to understand how it works so you can choose the right cyber threat tools and solutions to protect your business.

### Why is threat intelligence important?

In a military, business or security context, intelligence is information that provides an organization with decision support and possibly a strategic advantage. Threat intelligence is a part of a bigger security intelligence strategy. It includes information related to protecting an organization from external and inside threats, as well as the processes, policies and tools used to gather and analyze that information.

### Types of threat intelligence

There are four varieties of threat intelligence: strategic, tactical, technical and operational. All four are essential to build a comprehensive threat assessment.

1. **Strategic threat intelligence.** This analysis summarizes potential cyberattacks and the possible consequences for nontechnical audiences and stakeholders, as well as decision-makers. It is presented in the form of white papers, reports and presentations, and is based on detailed analysis of emerging risks and trends from around the world. It is used to paint a high-level overview of an industry's or organization's threat landscape.
2. **Tactical threat intelligence.**Tactical intelligence provides information about the tactics, techniques and procedures (TTPs) that threat actors use. It is intended for those directly involved with protecting IT and data resources. It provides details on how an organization might be attacked based on the latest methods being used and the best ways to defend against or mitigate the attacks.
3. **Technical threat intelligence.** This information focuses on signs that indicate an attack is starting. These signs include reconnaissance, weaponization and delivery, such as spear phishing, baiting and social engineering. Technical intelligence plays an important role in blocking social engineering attacks. This type of intelligence is often grouped with operational threat intelligence; however, it adjusts quickly as hackers update their tactics to take advantage of new events and ruses.

## What is the difference between Information Technology (IT) and Operational Technology (OT)? In short, IT deals with information, while OT deals with machines. The former manages the flow of digital information (read: data), while the latter manages the operation of physical processes and the machinery used to carry them out.

## A good (though increasingly inaccurate) shorthand to represent this distinction is the office (IT) vs. the factory floor (OT). Another good (and perhaps even less accurate) juxtaposition would be that of software (IT) vs. hardware (OT).

## 

From power plants and oil rigs to manufacturing assembly lines and inventory management processes, OT is an essential part of some incredibly complex physical processes. It should come as no surprise, then, that some of the systems IT professionals invented to manage complexity are now being applied to operational technology. The same software and processes IT teams use to manage the flow of information are now being used to manage the flow of water, lubricating oil, heat, packing peanuts, and breakfast cereals.

Indeed, hardware (OT) and software (IT) now work hand-in-hand to monitor and regulate essential business processes outside of regular IT workflows. Although these processes will differ from one organization and one industry to the next, they have a central role to play in the success of many modern enterprises — and manufacturers in particular. Experts predict that the market for OT will expand to [more than $40 billion](https://www.marketsandmarkets.com/PressReleases/operational-technology.asp) by 2022.

## For these kinds of enterprises, whether public or private, it’s of vital importance that key decision-makers understand how IT and OT differ — in addition to how each discipline can (and should) interact. Given the rise of the Internet of Things (IoT) and its successful application across nearly every industry, now is the time for organizations with a stake in IT and OT systems and networks to invest in next-generation solutions that can bring these two distinct disciplines into ever-tighter partnership.

## Understanding IT

Most organizations understand the roles and functions of IT; but in the context of its relationship to OT, it is probably worth expanding. Put simply, IT refers to the application of network, storage, and compute resources toward the generation, management, storage, and delivery of data throughout and between organizations

## Understanding OT

Whether you’re new to OT or you’re just new to thinking about it in relation to IT, the next generation of connected operational technology demands that decision-makers understand OT in its traditional sense *and* as an area of exciting innovation. At the most basic level, OT refers to technology that monitors and controls specific devices and processes within industrial workflows.

## Compared with IT, OT is unique in that related hardware and software is usually (historically) designed to do specific things: control heat, monitor mechanical performance, trigger emergency shutoffs, etc. Typically, this is done through industrial control systems (ICS) and supervisory control and data acquisition (SCADA)

## Importantly, OT has typically required human oversight at key junctures — at least until recent years. If employees have seen fit to change the temperature on a factory floor, raise or lower humidity levels, or shut off machinery for a given reason, OT has provided a quick, clear way of making that happen — a physical switch, a steel lever, or a big red button. Conversely, IT systems have been able to perform key operations without constant human intervention — provided those workflows are within programmed functions

## Where We Go From Here

## While IT and OT have historically made up separate aspects of modern organizations, a phenomenon known as [IT-OT convergence](https://www.coolfiresolutions.com/blog/it-ot-convergence/) is changing that. Because IoT technology is taking assets not typically connected to the internet — such as assembly line machinery — and bringing them online, enterprises now have the opportunity to create new efficiencies by applying the intelligence of IT to the physical assets of OT systems

## For example, traditional temperature controls linked to OT systems would typically report readings by way of a closed-loop readout, enabling employees “on the floor” to see whether adjustments were necessary on their end. With IoT technology, however, those temperature sensors can be connected to IT networks, allowing them to communicate in real-time with other assets across facilities in order to optimize temperature levels *automatically* for maximum performance. AI and machine learning, of course, have a role to play here as well.