Network security applications

This section of the course covers the topic of network hardening and monitoring. Each device, tool, or security strategy put in place by security analysts further protects—or hardens—the network until the network owner is satisfied with the level of security. This approach of adding layers of security to a network is referred to as defense in depth.

In this reading, you are going to learn about the role of four devices used to secure a network—firewalls, intrusion detection systems, intrusion prevention systems, and security incident and event management tools. Network security professionals have the choice to use any or all of these devices and tools depending on the level of security that they hope to achieve.

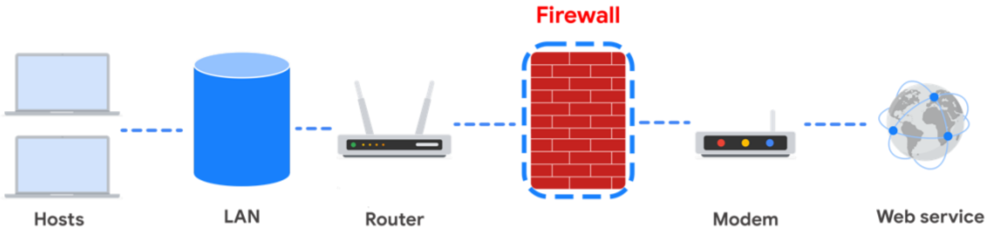
This reading will discuss the benefits of layered security. Each tool mentioned is an additional layer of defense that can incrementally harden a network, starting with the minimum level of security (provided by just a firewall), to the highest level of security (provided by combining a firewall, an intrusion detection and prevention device, and security event monitoring).

Take note of where each tool is located on the network. Each tool has its own place in the network's architecture. Security analysts are required to understand the network topologies shown in the diagrams throughout this reading.

Firewall

So far in this course, you learned about stateless firewalls, stateful firewalls, and next-generation firewalls (NGFWs), and the security advantages of each of them.

Most firewalls are similar in their basic functions. Firewalls allow or block traffic based on a set of rules. As data packets enter a network, the packet header is inspected and allowed or denied based on its port number. NGFWs are also able to inspect packet payloads. Each system should have its own firewall, regardless of the network firewall.

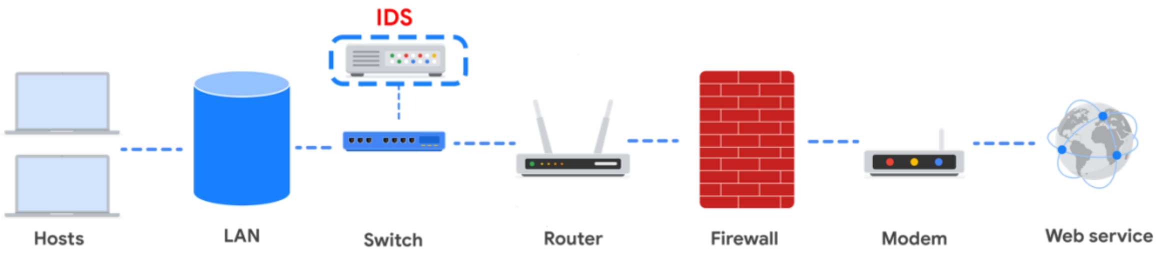


Intrusion Detection System

An **intrusion detection system** (IDS) is an application that monitors system activity and alerts on possible intrusions. An IDS alerts administrators based on the signature of malicious traffic.

The IDS is configured to detect known attacks. IDS systems often sniff data packets as they move across the network and analyze them for the characteristics of known attacks. Some IDS systems review not only for signatures of known attacks, but also for anomalies that could be the sign of malicious activity. When the IDS discovers an anomaly, it sends an alert to the network administrator who can then investigate further.

The limitations to IDS systems are that they can only scan for known attacks or obvious anomalies. New and sophisticated attacks might not be caught. The other limitation is that the IDS doesn't actually stop the incoming traffic if it detects something awry. It's up to the network administrator to catch the malicious activity before it does anything damaging to the network.

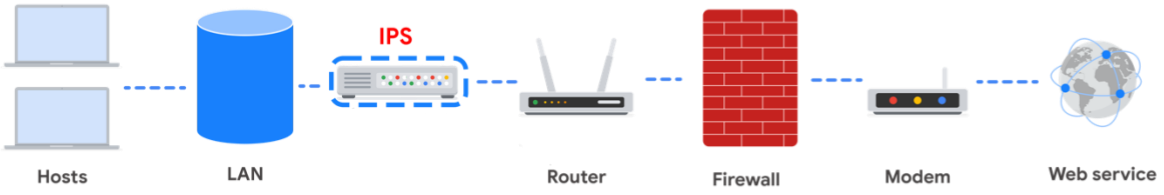


When combined with a firewall, an IDS adds another layer of defense. The IDS is placed behind the firewall and before entering the LAN, which allows the IDS to analyze data streams after network traffic that is disallowed by the firewall has been filtered out. This is done to reduce noise in IDS alerts, also referred to as false positives.

Intrusion Prevention System

An **intrusion prevention system (IPS)** is an application that monitors system activity for intrusive activity and takes action to stop the activity. It offers even more protection than an IDS because it actively stops anomalies when they are detected, unlike the IDS that simply reports the anomaly to a network administrator.

An IPS searches for signatures of known attacks and data anomalies. An IPS reports the anomaly to security analysts and blocks a specific sender or drops network packets that seem suspect.



The IPS (like an IDS) sits behind the firewall in the network architecture. This offers a high level of security because risky data streams are disrupted before they even reach sensitive parts of the network. However, one potential limitation is that it is inline: If it breaks, the connection between the private network and the internet breaks. Another limitation of IPS is the possibility of false positives, which can result in legitimate traffic getting dropped.

Full packet capture devices

Full packet capture devices can be incredibly useful for network administrators and security professionals. These devices allow you to record and analyze all of the data that is transmitted over your network. They also aid in investigating alerts created by an IDS.

Security Information and Event Management

A **security information and event management system (SIEM)** is an application that collects and analyzes log data to monitor critical activities in an organization. SIEM tools work in real time to report suspicious activity in a centralized dashboard. SIEM tools additionally analyze network log data sourced from IDSs, IPSs, firewalls, VPNs, proxies, and DNS logs. SIEM tools are a way to aggregate security event data so that it all appears in one place for security analysts to analyze. This is referred to as a single pane of glass.

Below, you can review an example of a dashboard from Google Cloud’s SIEM tool, Chronicle. **Chronicle** is a cloud-native tool designed to retain, analyze, and search data.

Splunk is another common SIEM tool. Splunk offers different SIEM tool options: Splunk Enterprise and Splunk Cloud. Both options include detailed dashboards which help security professionals to review and analyze an organization's data. There are also other similar SIEM tools available, and it's important for security professionals to research the different tools to determine which one is most beneficial to the organization.

A SIEM tool doesn’t replace the expertise of security analysts, or of the network- and system-hardening activities covered in this course, but they’re used in combination with other security methods. Security analysts often work in a Security Operations Center (SOC) where they can monitor the activity across the network. They can then use their expertise and experience to determine how to respond to the information on the dashboard and decide when the events meet the criteria to be escalated to oversight.

Key takeaways

Devices / Tools	**Advantages**	**Disadvantages**
Firewall	A firewall allows or blocks traffic based on a set of rules.	A firewall is only able to filter packets based on information provided in the header of the packets.
Intrusion Detection System (IDS)	An IDS detects and alerts admins about possible intrusions, attacks, and other malicious traffic.	An IDS can only scan for known attacks or obvious anomalies; new and sophisticated attacks might not be caught. It doesn’t actually stop the incoming traffic.
Intrusion Prevention System (IPS)	An IPS monitors system activity for intrusions and anomalies and takes action to stop them.	An IPS is an inline appliance. If it fails, the connection between the private network and the internet breaks. It might detect false positives and block legitimate traffic.

Devices / Tools	Advantages	Disadvantages
Security Information and Event Management (SIEM)	A SIEM tool collects and analyzes log data from multiple network machines. It aggregates security events for monitoring in a central dashboard.	A SIEM tool only reports on possible security issues. It does not take any actions to stop or prevent suspicious events.

Each of these devices or tools cost money to purchase, install, and maintain. An organization might need to hire additional personnel to monitor the security tools, as in the case of a SIEM. Decision-makers are tasked with selecting the appropriate level of security based on cost and risk to the organization. You will learn more about choosing levels of security later in the course.