Firewall Features and Functions

by Sophia

WHAT'S COVERED

In this lesson, you will learn about intrusion detection and prevention.

Specifically, this lesson will cover the following:

1. Intrusion Detection

REFLECT

If someone broke into your network, how would you know?

Attackers who break into networks often leave clues behind that can help you sleuth out their identities as well as how they gained access. A great tool for doing network detective work is known as an **intrusion detection system (IDS)**.

Firewalls are designed to block unauthorized traffic from entering your network, but an IDS is more of an auditing tool; it keeps track of all activity on your network so you can see if someone has been trespassing. Because the technology behind IDSes is fairly new, people are busy developing ways to combine IDS technology with existing firewalls.

BIG IDEA

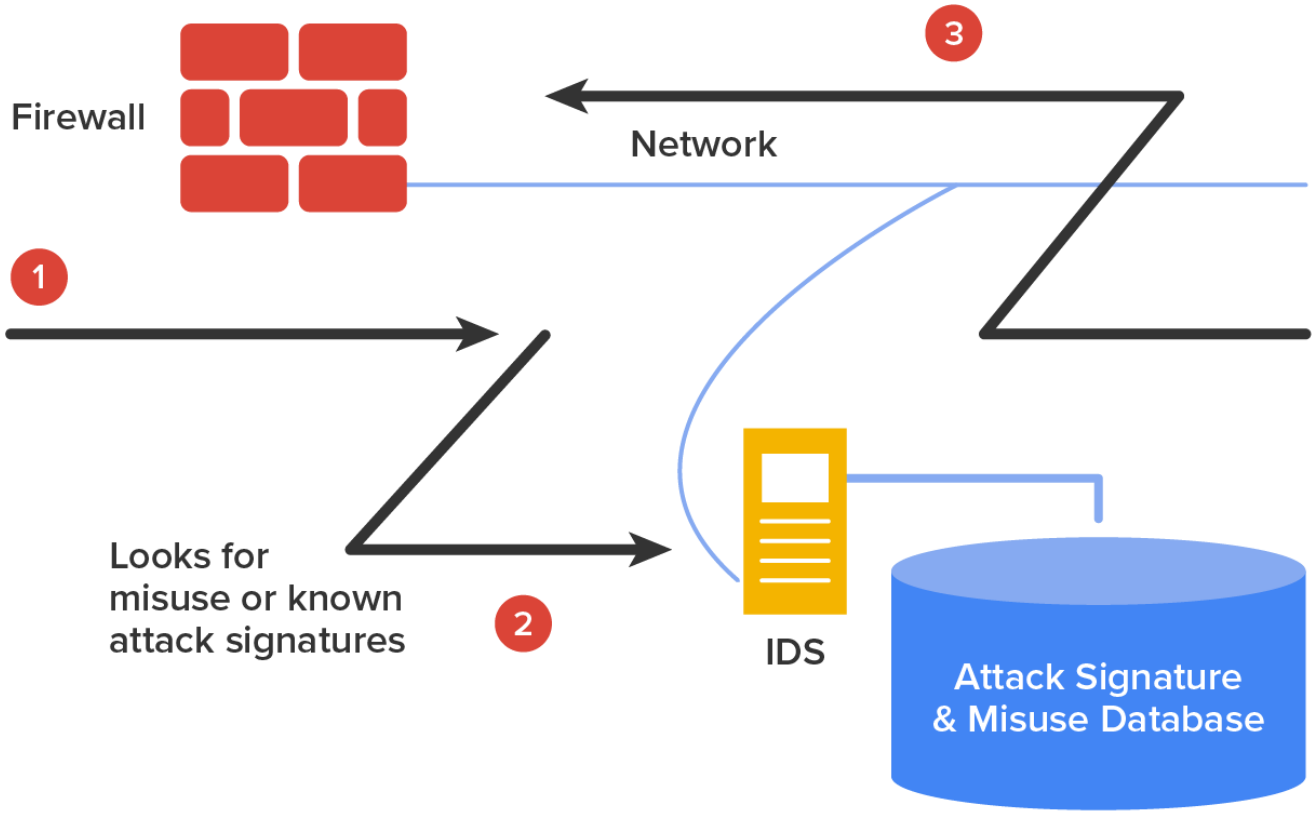
An intrusion detection system does NOT replace a firewall on your network!

There are two kinds of IDSs that can detect attacks or intrusions. The first, often referred to as a **misuse-detection IDS (MD-IDS)**, is based on the signature of an intrusion, and it works by looking for fingerprints, which in this case means strange or abusive use of the network. The IDS sends up an alarm only if it recognizes the fingerprints typical of attackers.

The second approach looks for anomalies in network activity, or an **anomaly-detection IDS (AD-IDS)**. An AD-IDS basically watches for anything out of the ordinary; if it discovers fingerprints where there should not be any, it will send out an alert.

HINT

An IDS learns on the go by keeping track of and building a history of network activity for norms to which you can compare unusual activity. Most IDSs today are a combination of two types of detection systems. The diagram below shows an MD-IDS in action.



1 Attack underway

2 IDS analysis

3 Response

KEY CONCEPT

An intrusion detection system cannot detect attacks within encrypted traffic.

An IDS is a system made up of several components, including one or more sensors to detect events, a console to control and configure the sensors and monitor events, and a database that records the events. These three elements can all be on the same device, or they can be implemented on multiple devices.

The two most common types of IDS implementations are network-based and host-based.

TERMS TO KNOW

Intrusion Detection System (IDS)

A device or software application that monitors a network or systems for malicious activity or policy violations.

Misuse-Detection IDS (MD-IDS)

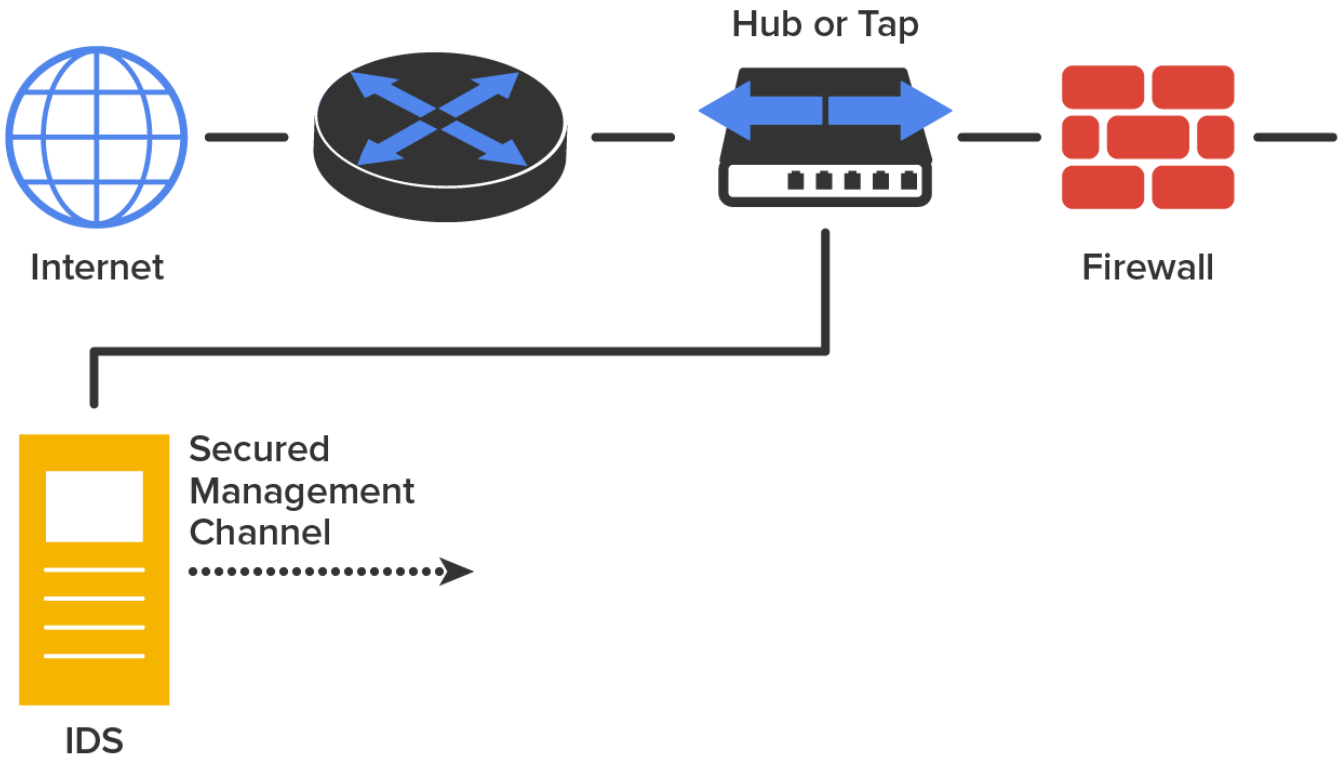
A device or software application that identifies an intrusion by looking for unauthorized use of the network.

Anomaly-Detection IDS (AD-IDS)

A device or software application that identifies an intrusion by looking for unusual activities on the network.

1a. Network-Based IDS

The most common implementation of a detection system is a **network-based IDS (NIDS)**, where the IDS is a separate device attached to the network via a machine like a switch or directly via a tap. Some IDSes are even capable of attaching to the network both outside and inside the firewall; this gives you the best security because you can see what is happening outside of your network and learn to recognize exactly what's getting through your defenses. The diagram below gives you an example of what a typical IDS setup can look like.



TERM TO KNOW

Network-Based IDS (NIDS)

An IDS that is a separate device attached to the network via a machine like a switch or directly via a tap.

1b. Host-Based IDS

In a **host-based IDS (HIDS)**, software runs on one computer to detect abnormalities on that system alone by monitoring applications, system logs, and event logs, and not by directly monitoring network traffic.

HINT

Systems like these are typically implemented on servers because they are challenging to manage if spread across several client computers on a network. Plus, if the IDS database is on the local computer and its data becomes compromised by an attack, the IDS data could be corrupted too.

STEP BY STEP

When your IDS detects an intrusion, it will respond to it either passively or actively. Passive responses are the easiest to configure and include the following:

1. **Logging**- All activity from the intrusion is logged. The information gathered can be used to foil future attacks of the same type. Intrusions should always be logged.
2. **Notification**- When an attack occurs, an IDS can send an alert to one or more administrators.
3. **Shunning**- Shunning is when you choose to just ignore an attack because it is possible it will not affect your network. For instance, if someone launches an attack designed to cripple a Microsoft Exchange

email server at a network that outsources its email service to a cloud-based email provider then your network is safe and you do not need to spend time mitigating the attack. However you should log the event for your records.

TERM TO KNOW

Host-Based IDS (HIDS)

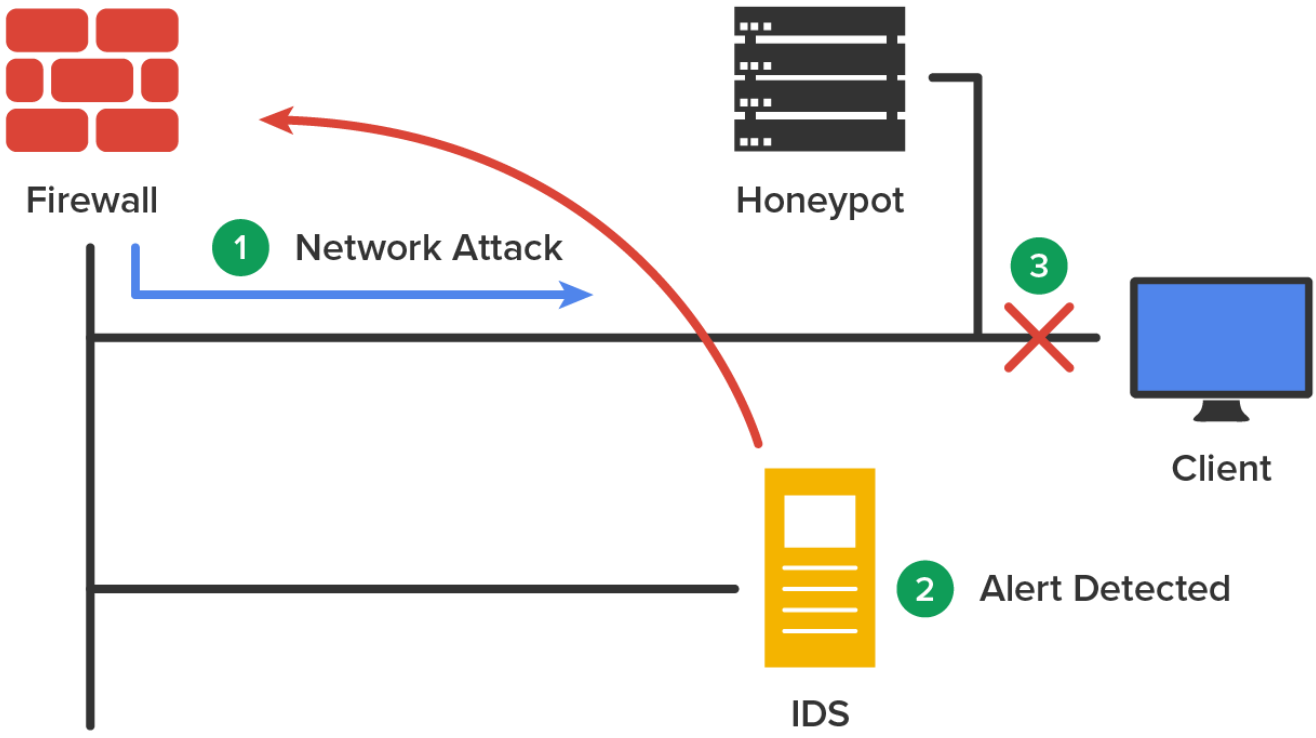
An IDS that is a software running locally on one computer to detect abnormalities on that system alone.

1c. Intrusion Prevention

Active responses mean taking immediate action. When an IDS moves to prevent an attack, it's often called a reactive system or an **intrusion protection system (IPS)**. Here are three common active responses:

- **Changing Network Configuration**: Let us say an attack comes in on port 21. Your IDS can close the port either temporarily or permanently. The downside is that if the IDS closes ports, legitimate traffic cannot get through either, but it will definitely stop the attack.
- **Terminating Sessions**: When the IDS detects an attack, it can force all sessions to close and restart, which will affect and delay legitimate traffic, too, but typically not for long.
- **Deceiving the Attacker**: This response tricks the attacker into thinking their attack is really working when it is not. The system logs information, trying to pinpoint who is behind the attack and which methods they are using. This response requires something called a **honeypot**, typically a server or group of servers (called honeynets) or maybe even access points, to which the hacker is directed; it is intended to keep their interest long enough to gather enough information to identify them and their attack method so you can prevent another attack in the future.

The diagram below demonstrates this.



1 Attack occurs 2 Analysis/response 3 Reroute network traffic

TERM TO KNOW

Intrusion Protection System (IPS)

A device or software application that proactively works to identify and prevent an attack in real time.

Honeypot

A server or access point to which the hacker is directed to keep their interest long enough to gather enough information to identify them and their attack method, to be used to prevent another attack in the future.

1d. Vulnerability Scanners

One of the most effective ways to determine if security holes exist in the network is to think like an attacker and attack your own network. Penetration testers often use the same tools that the hacker might use to identify network weaknesses.

EXAMPLE If we wanted to verify the proper application of some ACLs to a firewall, we could do so with scanning services supplied by a vulnerability scanner. In the following sections, we will cover two of the most widely known and effective programs that can be used for this purpose.

IN CONTEXT

Nessus is a proprietary vulnerability scanning program that requires a license to use commercially yet

is the single most popular scanning program in use. It normally is executed from the command line because it can thus be included in batch files that can automate its operation on a schedule. Its output can be reported in a variety of formats, including plain text, HTML, and XML.

It operates by performing a port scan and then follows up with more specific tests and scans based on the ports open. It can identify a wide array of weaknesses, including the following:

- Unsecured access to sensitive data on a system
- Misconfigurations like open mail relay and missing patches
- Password issues such as the use of default passwords, common passwords, and blank passwords on system accounts

It can also perform an active attack such as denial of service or a dictionary attack.

Network Mapper (Nmap) was originally intended to simply identify devices on the network for the purpose of creating a network diagram. Its functionality has evolved, however, and now it can also do the following:

- Perform port scanning
- Identify versions of network services in operation on the network
- Identify operating systems

It can be used from the command line as with Nessus, but it also can be used with web-based interfaces to be controlled remotely.

TERMS TO KNOW

Nessus
A proprietary vulnerability scanning program.

Network Mapper (Nmap)
A program that creates network diagrams, performs port scanning, and identifies network services and operating systems running on a network.

1e. Unified Threat Management (UTM)

Unified threat management (UTM) devices perform multiple security functions within the same appliance:

- Network firewalling
- Network intrusion prevention
- Gateway antivirus
- Gateway anti-spam
- VPN
- Content filtering
- Load balancing
- Data leak prevention

- On-appliance reporting

While the advantage of unified security lies in the fact that administering multiple systems is no longer necessary, some feel that a single point of failure is created and creating multiple layers of devices is a more secure approach.

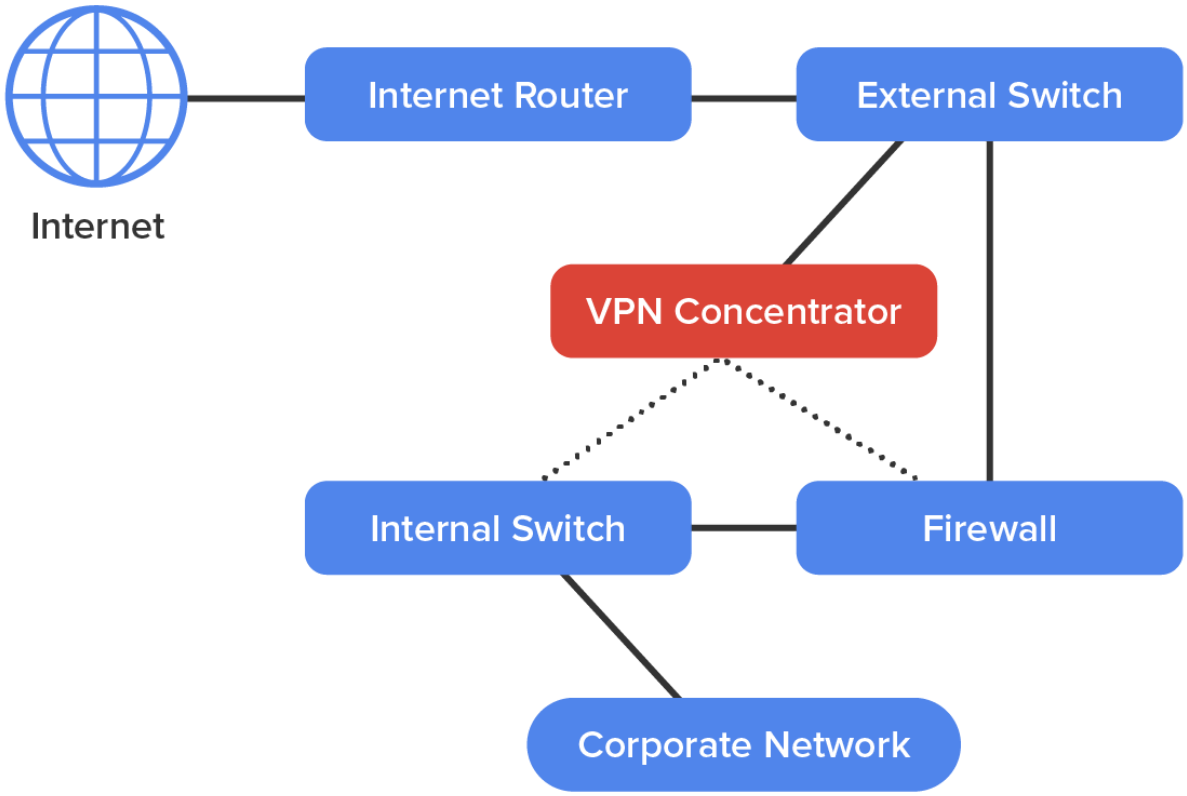
TERM TO KNOW

Unified Threat Management (UTM)

A device that performs multiple security functions within the same appliance.

1f. VPN Concentrators

A **VPN concentrator** is a device that creates remote access for virtual private networks (VPNs) either for users logging in remotely or for a large site-to-site VPN. In contrast to standard remote-access connections, remote-access VPNs often allow higher data throughput and provide encryption. Large enterprises may use concentrators that support anywhere from 100 users up to 10,000 simultaneous remote-access connections.



Encryption for a remote-access VPN through a concentrator is usually handled by Internet Protocol Security (IPSec) or by Secure Sockets Layer (SSL), and user authentication can be achieved via Microsoft's Active Directory, Kerberos, Remote Authentication Dial In User Service (RADIUS), Rivest, Shamir, and Adleman (RSA), and digital certificates. Many VPN concentrators also have a built-in authentication server and allow ACLs to be

implemented through them. In the diagram above you can see where VPN concentrators are usually placed within a network setup.

TERM TO KNOW

VPN Concentrator

A device that creates remote access for virtual private networks (VPNs) either for users logging in remotely or for a large site-to-site VPN.

SUMMARY

In this lesson, you learned about **intrusion detection** and prevention. Specifically, this lesson introduced network-based IDS, host-based IDS, intrusion prevention, vulnerability scanners Nessus and Nmap, unified threat management (UTM), and VPN concentrators.

Source: This content and supplemental material has been adapted from CompTIA Network+ Study Guide: Exam N10-007, 4th Edition. Source **Lammle: CompTIA Network+ Study Guide: Exam N10-007, 4th Edition - Instructor Companion Site (wiley.com)**

TERMS TO KNOW

Anomaly-Detection IDS (AD-IDS)

A device or software application that identifies an intrusion by looking for unusual activities on the network.

Honeypot

A server or access point to which the hacker is directed to keep their interest long enough to gather enough information to identify them and their attack method, to be used to prevent another attack in the future.

Host-Based IDS (HIDS)

An IDS that is a software running locally on one computer to detect abnormalities on that system alone.

Intrusion Detection System (IDS)

A device or software application that monitors a network or systems for malicious activity or policy violations.

Intrusion Protection System (IPS)

A device or software application that proactively works to identify and prevent an attack in real time.

Misuse-Detection IDS (MD-IDS)

A device or software application that identifies an intrusion by looking for unauthorized use of the network.

Nessus

A proprietary vulnerability scanning program.

Network Mapper (Nmap)

A program that creates network diagrams, performs port scanning, and identifies network services and operating systems running on a network.

Network-Based IDS (NIDS)

An IDS that is a separate device attached to the network via a machine like a switch or directly via a tap.

Unified Threat Management (UTM)

A device that performs multiple security functions within the same appliance.

VPN Concentrator

A device that creates remote access for virtual private networks (VPNs) either for users logging in remotely or for a large site-to-site VPN.