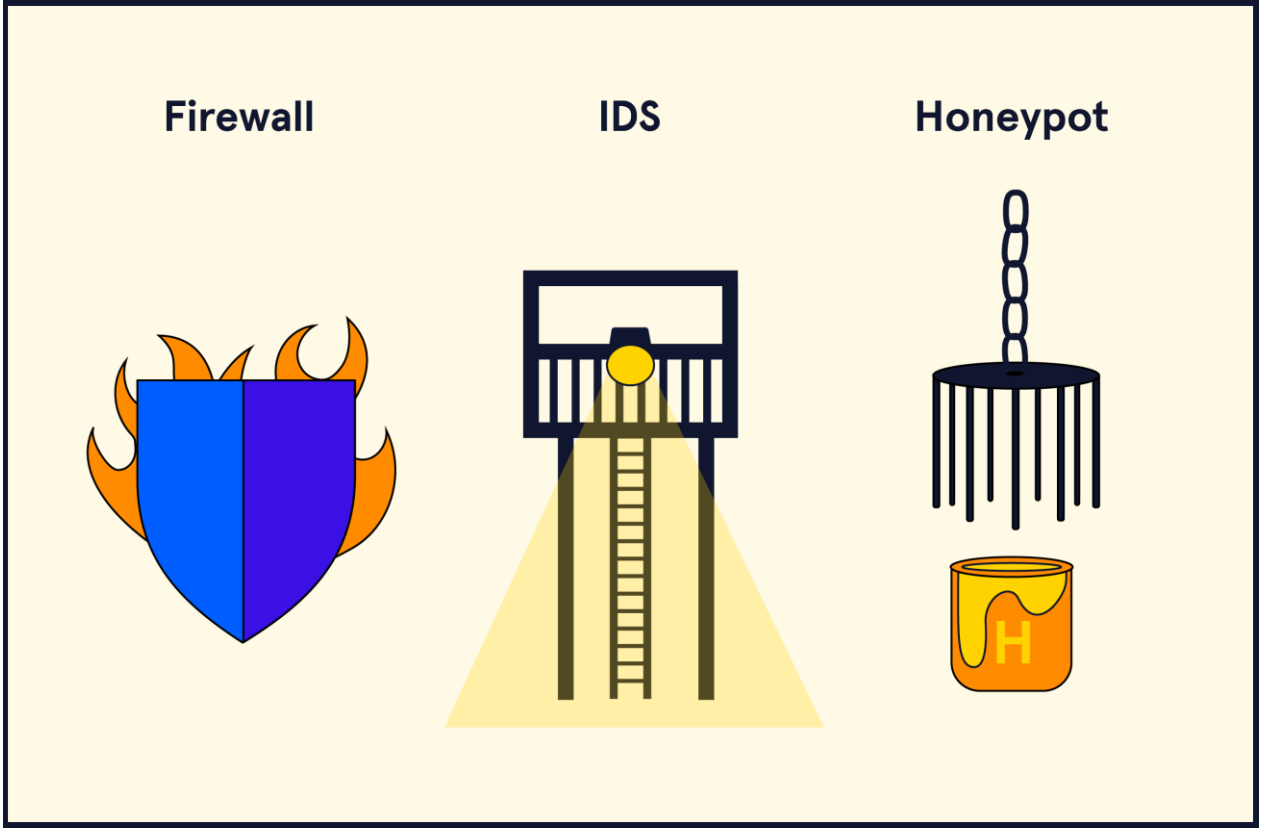
Evading Defensive Measures

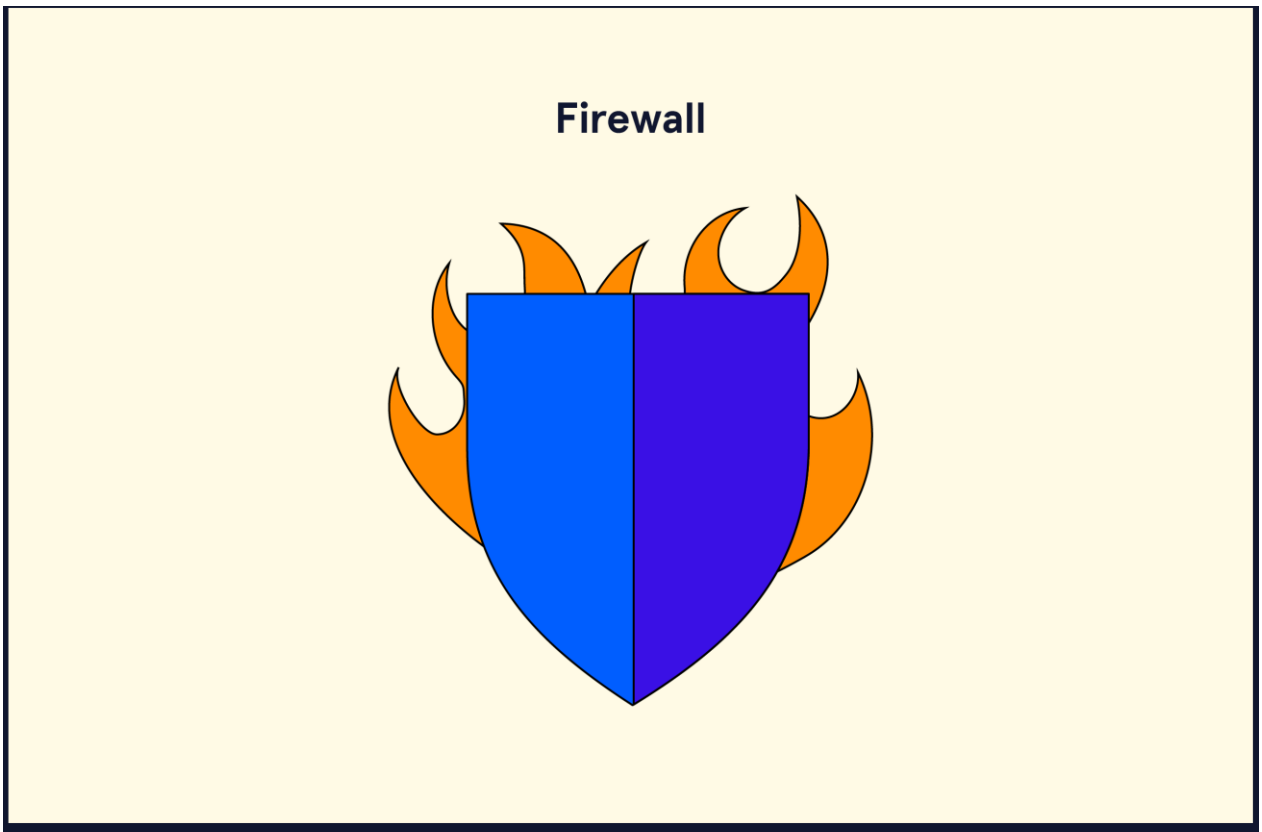
In this article, you'll learn about Firewalls, IDSs, and Honeypots. We'll discuss what they are, what their purpose is, and how they can be evaded.

What Are Firewalls, IDSs, and Honeypots?

Firewalls, IDSs, and Honeypots are all defensive tools for protecting a network. For defenders, they provide additional layers of security that can prevent or delay attacks and buy time and provide information to formulate a response. For attackers, they act as obstacles that must be overcome or avoided for an attack to be successful.



Firewalls

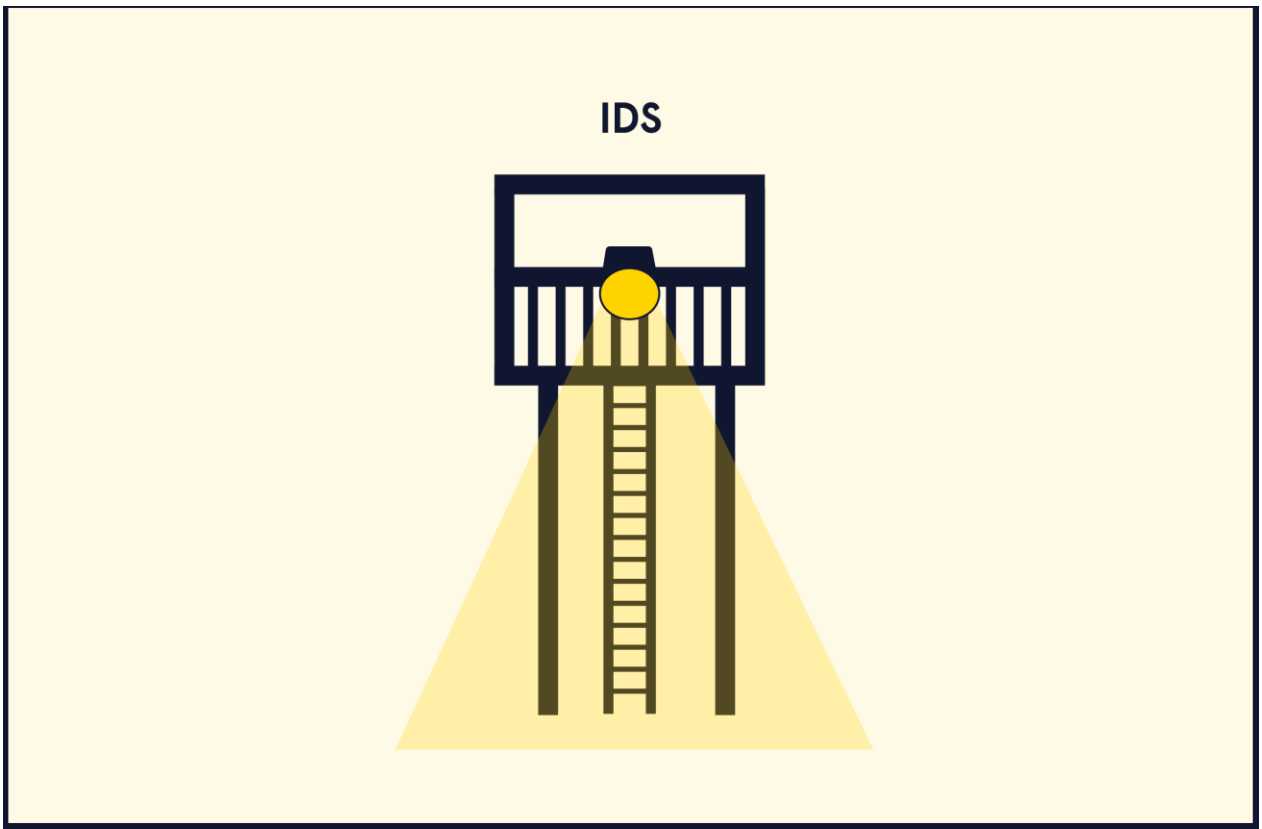


Firewalls are pieces of hardware or software that filter network traffic according to a set of rules. Packets that pass through a firewall are intercepted, inspected, and either passed on or discarded. It is also important to note that firewalls can be **stateless** or **stateful**.

Stateless firewalls look at individual packets of data in isolation.

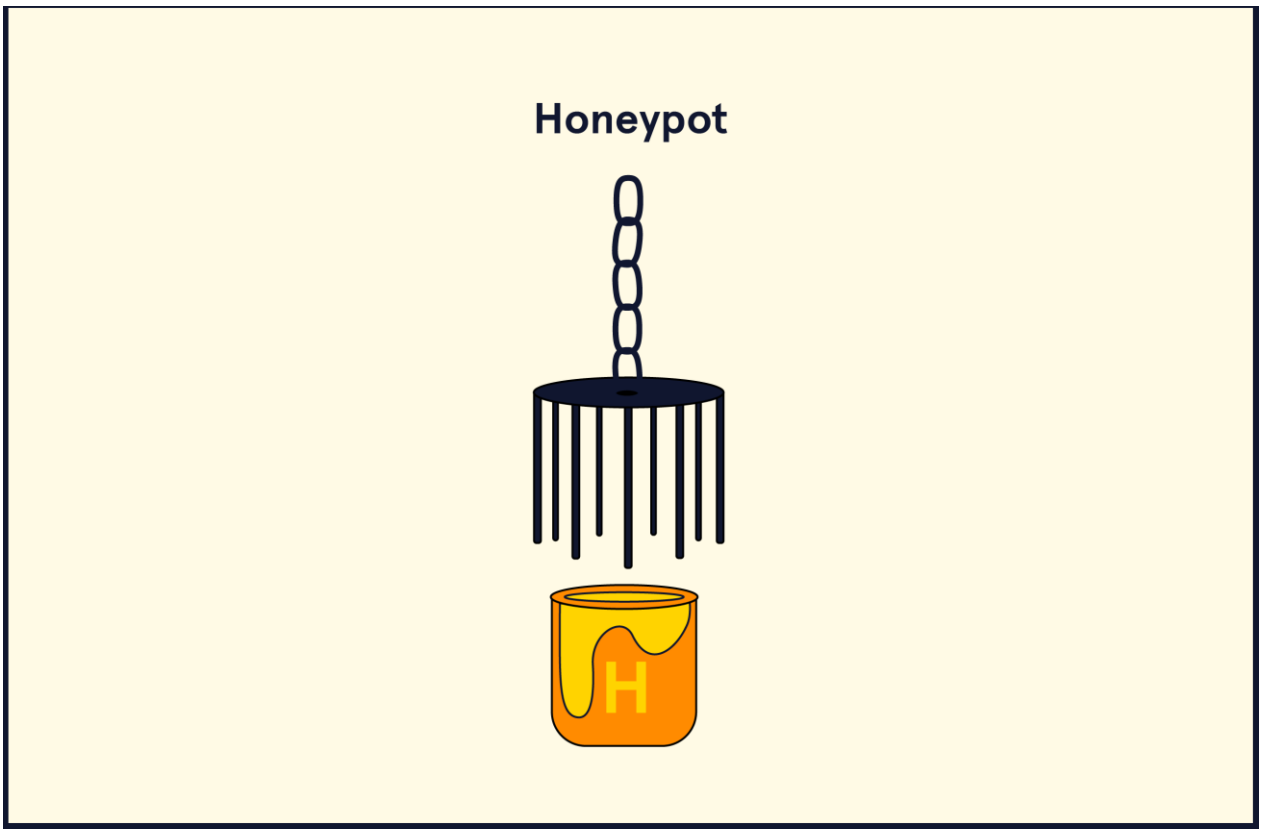
Stateful firewalls look at connections as a whole.

Intrusion Detection Systems



An Intrusion Detection System (IDS) is a piece of hardware or software that monitors activity on a network, looking for signs of malicious or prohibited activity. When it detects malicious or prohibited activity, it alerts the security team. IDSs do *not* take any action to stop the activity they detect; IDSs *just* report it to the security team. A related tool called an Intrusion Prevention System (IPS) is capable of taking action on its own.

Honeypots



A honeypot is a decoy computer or network (decoy networks are sometimes known as Honeynets) designed to entice and distract attackers while allowing defenders to gather intelligence on the attackers. Honeypots usually contain fake data that appears attractive to attackers, such as poorly encrypted password databases, trade secrets, financial or customers' data, and many more. Honeypots, by design, usually appear to have weaker security than other parts of the network but are heavily monitored to allow defenders to observe the attackers. Good honeypots keep attackers busy for long enough that defenders can formulate and execute a response.

Evading Defenses

Attack and defense are two sides of the same coin. If we know how to attack, we can use that knowledge when creating defenses and vice-versa. Competent defenders will try to anticipate the goals an attacker might have and methods they might use and plan their defensive measures accordingly. Competent attackers will try to anticipate the measures that defenders are likely to take and operate in a way that bypasses or subverts them.

Evading Firewalls

Firewalls usually consider various factors when deciding whether to block traffic. Here are some examples of common factors:

- Is this traffic coming from or going to an address known to be malicious?
- Is this traffic using non-standard ports or ports associated with insecure protocols?
- Does this traffic contain malformed or corrupted packets?
- Is this traffic coming from an address making a suspiciously large number of requests?

Evading firewalls is a matter of making our traffic look as legitimate as possible. This is where reconnaissance can be very useful. By looking at what traffic is normal for a given environment, we can try to disguise our traffic and blend it into the background. For example, in an environment where people regularly visit outside websites, HTTPS traffic would be a normal thing to see, but FTP traffic might raise red flags. Likewise, an outgoing connection to `google.com` is much less suspicious than an outgoing connection to somewhere like `malware.mal`.

Stateful firewalls can look at information about the connection as a whole, such as what protocol is actually being used, whether a connection is being created or already exists, or whether a packet is not part of a new or existing connection. This can complicate reconnaissance because the traffic generated by active reconnaissance tools should be highly suspicious to a stateful firewall.

Evading IDSs

IDSs look for *Indicators Of Compromise (IOCs)*; telltale signs that malicious activity is afoot. IOCs can be connections to certain IP addresses, unauthorized access to databases, suspicious data being sent over the network, an unusually large number of failed logins, etc. For example, transmitting the code of a known exploit in plaintext is a great way to get detected.

Using publicly available hacking tools increases our risk of detection. If it's publicly available for attackers, it's also publicly available for defenders. There are even services available that provide curated, regularly updated lists of IOCs so that security teams don't have to manage the lists themselves.

We won't always know when we've tripped an IDS. It's sometimes a better strategy for defenders to wait and gather information on an attacker rather than immediately trying to remove them from the network. Skilled defenders will give us no indication that we've been detected until it's too late.

Here are the three main ways of avoiding being detected by an IDS:

- *Don't let the IDS notice our traffic*. Transmit information slowly, split data into multiple packets, send packets out of order, etc.
- *Don't let the IDS figure out what our traffic is*. Even if the IDS notices our traffic and can scan it, we can take steps to avoid alerting the IDS: Obfuscate data by encrypting or encoding it. Use polymorphic code to transmit malware without it matching known signatures.
- *Don't let the IDS function*. The most direct way to prevent an IDS from detecting us is to render the IDS non-functional via denial-of-service attacks. Of course, this creates a whole new set of problems because the security team will probably start investigating why the IDS is getting attacked, but at least we can say we didn't get detected by the IDS.

Evading Honeypots

Honeypots are one of the many reasons why good reconnaissance is important. Understanding the layout of an environment before we start moving through it is important to avoid falling into a trap. Competent defenders don't just leave sensitive data lying around where it can be easily accessed or leave obvious vulnerabilities in internet-facing hosts. Of course, not all defenders are competent, and there are many stories of organizations having ludicrously poor security practices. Still, it's better to overestimate than underestimate our opponent.

Conclusion

In general, evading defenses is a matter of not arousing suspicion. It's better to take a slow and steady approach while we conduct reconnaissance and gather information to avoid setting off alarms. Consider what activity would look suspicious to defenders and what attack vectors have likely been anticipated.

Firewalls block suspicious traffic, and evading them means disguising our illegitimate traffic as legitimate traffic. IDSs scan for known indicators of compromise and are evaded by staying quiet and not creating signs of our presence. Honeypots lure in unsuspecting attackers and are avoided by working slowly and cautiously, conducting reconnaissance before acting.

Finally, it's important not to lose perspective, especially if we're in a role such as penetration testing that involves attempting to bypass defenses. The job of

a pentester isn’t to be an elite hacker but to test and help refine a client’s security. While successfully avoiding defenses is a useful skill, remember there’s no shame in getting caught. After all, it’s what the defenses were designed to do.