# GLOSSARY

## IT Security Foundations: Network Security

Lisa Bock

Use these terms and definitions below to understand concepts taught in the course.

**Transcript Search:** Note that you can search for terms directly within the course. To search video text, switch to the *Transcripts* tab, then press Cmd/Ctrl + F on your keyboard to run a search within the active transcript.

| Term | Definition |
| --- | --- |
| **firewall** | A hardware or software-based mechanism that controls incoming and outgoing traffic based on a set of rules that permit or deny traffic on a network or host |
| **honeypot** | A system set up to lure a would-be attacker, with the goal of observing their behavior in order to learn attack methodologies to better protect the real network |
| **NAP** | Network Access Protection. A framework that uses a Network Policy Server to evaluate the health of client computers |
| **protocol spoofing** | When a malicious party impersonates another entity on the network with the objective of stealing data, spreading malware, or circumventing access controls |
| **server and domain isolation** | Provides an additional layer of protection by requiring IPSec authentication and encryption for communication within the domain |
| **user account control** | A feature in Windows that protects the security of the operating system |
| **VLAN** | Virtual Local Area Network. Removes the physical barrier and treats the host as if they were part of the same subnet while separating networks within networks |