# Network security

**Network security** consists of the [policies](https://en.wikipedia.org/wiki/Policies) adopted to prevent and monitor [unauthorized](https://en.wikipedia.org/wiki/Unauthorized) access, misuse, modification, or denial of a [computer network](https://en.wikipedia.org/wiki/Computer_network) and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs; conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

## Concepts

Network security starts with [authenticating](https://en.wikipedia.org/wiki/Authentication), commonly with a username and a password. Since this requires just one detail authenticating the user name—i.e., the password—this is sometimes termed one-factor authentication. With [two-factor authentication](https://en.wikipedia.org/wiki/Two-factor_authentication), something the user 'has' is also used (e.g., a [security token](https://en.wikipedia.org/wiki/Security_token) or '[dongle](https://en.wikipedia.org/wiki/Dongle)', an [ATM card](https://en.wikipedia.org/wiki/ATM_card), or a [mobile phone](https://en.wikipedia.org/wiki/Mobile_phone)); and with three-factor authentication, something the user 'is' also used (e.g., a [fingerprint](https://en.wikipedia.org/wiki/Fingerprint) or [retinal scan](https://en.wikipedia.org/wiki/Retinal_scan)).

Once authenticated, a [firewall](https://en.wikipedia.org/wiki/Firewall_(networking)) enforces access policies such as what services are allowed to be accessed by the network users.[[1]](https://en.wikipedia.org/wiki/Network_security#cite_note-1) Though effective to prevent unauthorized access, this component may fail to check potentially harmful content such as [computer worms](https://en.wikipedia.org/wiki/Computer_worm) or [Trojans](https://en.wikipedia.org/wiki/Trojan_horse_(computing)) being transmitted over the network. [Anti-virus software](https://en.wikipedia.org/wiki/Anti-virus_software) or an [intrusion prevention system](https://en.wikipedia.org/wiki/Intrusion_prevention_system) (IPS) help detect and inhibit the action of such [malware](https://en.wikipedia.org/wiki/Malware). An [anomaly-based intrusion detection system](https://en.wikipedia.org/wiki/Anomaly-based_intrusion_detection_system) may also monitor the network like wire shark [traffic](https://en.wikipedia.org/wiki/Deep_packet_inspection) and may be logged for audit purposes and for later high-level analysis.

Communication between two hosts using a network may be encrypted to maintain privacy.

[Honeypots](https://en.wikipedia.org/wiki/Honeypot_(computing)), essentially [decoy](https://en.wikipedia.org/wiki/Decoy) network-accessible resources, may be deployed in a network as surveillance and early-warning tools, as the honeypots are not normally accessed for legitimate purposes. Techniques used by the attackers that attempt to compromise these decoy resources are studied during and after an attack to keep an eye on new [exploitation](https://en.wikipedia.org/wiki/Exploit_(computer_security)) techniques. Such analysis may be used to further tighten security of the actual network being protected by the honeypot. A honeypot can also direct an attacker's attention away from legitimate servers. A honeypot encourages attackers to spend their time and energy on the decoy server while distracting their attention from the data on the real server. Similar to a honey pot, a honey net is a network set up with intentional vulnerabilities. Its purpose is also to invite attacks so that the attacker's methods can be studied and that information can be used to increase network security. A honey net typically contains one or more honeypots.

## Types of attacks

Networks are subject to [attacks](https://en.wikipedia.org/wiki/Attack_(computing)) from malicious sources. [Attacks](https://en.wikipedia.org/wiki/Attack_(computing)) can be from two categories: "Passive" when a network intruder intercepts data traveling through the network, and "Active" in which an intruder initiates commands to disrupt the network's normal operation.

Types of attacks include:

* Passive Network
  + - [Wiretapping](https://en.wikipedia.org/wiki/Telephone_tapping)
    - [Port scanner](https://en.wikipedia.org/wiki/Port_scanner)
    - [Idle scan](https://en.wikipedia.org/wiki/Idle_scan)
* Active
  + [Denial-of-service attack](https://en.wikipedia.org/wiki/Denial-of-service_attack)
  + [DNS spoofing](https://en.wikipedia.org/wiki/DNS_spoofing)
  + [Man in the middle](https://en.wikipedia.org/wiki/Man-in-the-middle_attack)
  + [ARP poisoning](https://en.wikipedia.org/wiki/ARP_poisoning)
  + [VLAN hopping](https://en.wikipedia.org/wiki/VLAN_hopping)
  + [Smurf attack](https://en.wikipedia.org/wiki/Smurf_attack)
  + [Buffer overflow](https://en.wikipedia.org/wiki/Buffer_overflow)
  + [Heap overflow](https://en.wikipedia.org/wiki/Heap_overflow)
  + [Format string attack](https://en.wikipedia.org/wiki/Format_string_attack)
  + [SQL injection](https://en.wikipedia.org/wiki/SQL_injection)
  + [Phishing](https://en.wikipedia.org/wiki/Phishing)
  + [Cross-site scripting](https://en.wikipedia.org/wiki/Cross-site_scripting)
  + [CSRF](https://en.wikipedia.org/wiki/CSRF)
  + [Cyber-attack](https://en.wikipedia.org/wiki/Cyber-attack)