**Network security**

From Wikipedia, the free encyclopedia

Jump to: [navigation](http://en.wikipedia.org/wiki/Network_security#mw-head), [search](http://en.wikipedia.org/wiki/Network_security#p-search)

**Network security**[[1]](http://en.wikipedia.org/wiki/Network_security#cite_note-1) consists of the provisions and [policies](http://en.wikipedia.org/wiki/Policies) adopted by a [network administrator](http://en.wikipedia.org/wiki/Network_administrator) to prevent and monitor [unauthorized](http://en.wikipedia.org/wiki/Unauthorized) access, misuse, modification, or denial of a [computer network](http://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.

|  |
| --- |
| **Contents**   * [1 Network security concepts](http://en.wikipedia.org/wiki/Network_security#Network_security_concepts) * [2 Security management](http://en.wikipedia.org/wiki/Network_security#Security_management)   + [2.1 Homes & Small Businesses](http://en.wikipedia.org/wiki/Network_security#Homes_.26_Small_Businesses)   + [2.2 Medium businesses](http://en.wikipedia.org/wiki/Network_security#Medium_businesses)   + [2.3 Large businesses](http://en.wikipedia.org/wiki/Network_security#Large_businesses)   + [2.4 School](http://en.wikipedia.org/wiki/Network_security#School)   + [2.5 Large government](http://en.wikipedia.org/wiki/Network_security#Large_government)   + [2.6 Types of Attacks](http://en.wikipedia.org/wiki/Network_security#Types_of_Attacks) * [3 See also](http://en.wikipedia.org/wiki/Network_security#See_also) * [4 References](http://en.wikipedia.org/wiki/Network_security#References) * [5 Further reading](http://en.wikipedia.org/wiki/Network_security#Further_reading) * [6 External links](http://en.wikipedia.org/wiki/Network_security#External_links) |

**Network security concepts**

Network security starts with [authenticating](http://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](http://en.wikipedia.org/wiki/Two-factor_authentication), something the user 'has' is also used (e.g. a [security token](http://en.wikipedia.org/wiki/Security_token) or 'dongle', an [ATM card](http://en.wikipedia.org/wiki/ATM_card), or a [mobile phone](http://en.wikipedia.org/wiki/Mobile_phone)); and with three-factor authentication, something the user 'is' is also used (e.g. a [fingerprint](http://en.wikipedia.org/wiki/Fingerprint) or [retinal scan](http://en.wikipedia.org/wiki/Retinal_scan)).

Once authenticated, a [firewall](http://en.wikipedia.org/wiki/Firewall_%28networking%29) enforces access policies such as what services are allowed to be accessed by the network users.[[2]](http://en.wikipedia.org/wiki/Network_security#cite_note-2) Though effective to prevent unauthorized access, this component may fail to check potentially harmful content such as [computer worms](http://en.wikipedia.org/wiki/Computer_worm) or [Trojans](http://en.wikipedia.org/wiki/Trojan_horse_%28computing%29) being transmitted over the network. [Anti-virus software](http://en.wikipedia.org/wiki/Anti-virus_software) or an [intrusion prevention system](http://en.wikipedia.org/wiki/Intrusion_prevention_system) (IPS)[[3]](http://en.wikipedia.org/wiki/Network_security#cite_note-3) help detect and inhibit the action of such [malware](http://en.wikipedia.org/wiki/Malware). An [anomaly-based intrusion detection system](http://en.wikipedia.org/wiki/Anomaly-based_intrusion_detection_system) may also monitor the network and [traffic](http://en.wikipedia.org/wiki/Deep_packet_inspection) for unexpected (i.e. suspicious) content or behavior and other anomalies to protect resources, e.g. from [denial of service](http://en.wikipedia.org/wiki/Denial_of_service) attacks or an employee accessing files at strange times. Individual events occurring on the network 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](http://en.wikipedia.org/wiki/Honeypot_%28computing%29), essentially [decoy](http://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](http://en.wikipedia.org/wiki/Exploit_%28computer_security%29) techniques. Such analysis may be used to further tighten security of the actual network being protected by the honeypot.[[4]](http://en.wikipedia.org/wiki/Network_security#cite_note-4)

**Security management**

Security management for networks is different for all kinds of situations. A home or small office may only require basic security while large businesses may require high-maintenance and advanced software and hardware to prevent malicious attacks from [hacking](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29) and [spamming](http://en.wikipedia.org/wiki/Spamming).

**Homes & Small Businesses**

* A basic [firewall](http://en.wikipedia.org/wiki/Firewall_%28computing%29) or a [unified threat management](http://en.wikipedia.org/wiki/Unified_threat_management) system.
* For Windows users, basic [Antivirus software](http://en.wikipedia.org/wiki/Antivirus_software). An anti-spyware program would also be a good idea. There are many other types of antivirus or anti-spyware programs available.
* When using a wireless connection, use a robust password. Also try to use the strongest security supported by your wireless devices, such as WPA2 with AES. TKIP may be more widely supported by your devices and should only be considered in cases where they are NOT compliant with AES.
* If using Wireless: Change the default SSID network name, also disable SSID Broadcast; as this function is unnecessary for home use. (Security experts consider this to be easily bypassed with modern technology and some knowledge of how wireless traffic is detected by software).[[5]](http://en.wikipedia.org/wiki/Network_security#cite_note-5)
* Enable MAC Address filtering to keep track of all home network MAC devices connecting to your router. (This is not a security feature per se; However it can be used to limit and strictly monitor your DHCP address pool for unwanted intruders if not just by exclusion, but by AP association.)
* Assign STATIC IP addresses to network devices. (This is not a security feature per se; However it may be used, in conjunction with other features, to make your AP less desirable to would-be intruders.)
* Disable ICMP ping on router.
* Review router or firewall logs to help identify abnormal network connections or traffic to the
* Use passwords for all accounts.
* For Windows users, Have multiple accounts per family member and use non-administrative accounts for day-to-day activities.
* Raise awareness about information security to children.[[6]](http://en.wikipedia.org/wiki/Network_security#cite_note-6)

**Medium businesses**

* A fairly strong [firewall](http://en.wikipedia.org/wiki/Firewall_%28computing%29) or [Unified Threat Management](http://en.wikipedia.org/wiki/Unified_Threat_Management) System
* Strong [Antivirus software](http://en.wikipedia.org/wiki/Antivirus_software) and Internet Security Software.
* For [authentication](http://en.wikipedia.org/wiki/Authentication), use strong passwords and change them on a bi-weekly/monthly basis.
* When using a wireless connection, use a robust password.
* Raise awareness about [physical security](http://en.wikipedia.org/wiki/Physical_security) to employees.
* Use an optional [network analyzer](http://en.wikipedia.org/wiki/Packet_analyzer) or network monitor.
* An enlightened administrator or manager.
* Use a VPN, or Virtual Private Network, to communicate between a main office and satellite offices using the Internet as a connectivity medium. A VPN offers a solution to the expense of leasing a data line while providing a secure network for the offices to communicate. A VPN provides the business with a way to communicate between two in a way mimics a private leased line. Although the Internet is used, it is private because the link is encrypted and convenient to use. A medium sized business needing a secure way to connect several offices will find this a good choice.[[7]](http://en.wikipedia.org/wiki/Network_security#cite_note-7)
* Clear employee guidelines should be implemented for using the Internet, including access to non-work related websites, sending and receiving information.
* Individual accounts to log on and access company intranet and Internet with monitoring for accountability.
* Have a back-up policy to recover data in the event of a hardware failure or a security breach that changes, damages or deletes data.
* Disable Messenger.
* Assign several employees to monitor a group like [CERT](http://en.wikipedia.org/wiki/CERT)[[8]](http://en.wikipedia.org/wiki/Network_security#cite_note-8) which studies Internet security vulnerabilities and develops training to help improve security.

**Large businesses**

* A strong [firewall](http://en.wikipedia.org/wiki/Firewall_%28computing%29) and [proxy](http://en.wikipedia.org/wiki/Proxy_server), or [network Guard](http://en.wikipedia.org/wiki/Guard_%28information_security%29), to keep unwanted people out.
* A strong [Antivirus software](http://en.wikipedia.org/wiki/Antivirus_software) package and Internet Security Software package.
* For [authentication](http://en.wikipedia.org/wiki/Authentication), use strong passwords and change it on a weekly/bi-weekly basis.
* When using a wireless connection, use a robust password.
* Exercise [physical security](http://en.wikipedia.org/wiki/Physical_security) precautions to employees.
* Prepare a [network analyzer](http://en.wikipedia.org/wiki/Network_analyzer_%28electrical%29) or network monitor and use it when needed.
* Implement [physical security](http://en.wikipedia.org/wiki/Physical_security) management like [closed circuit television](http://en.wikipedia.org/wiki/Closed_circuit_television) for entry areas and restricted zones.
* [Security fencing](http://en.wikipedia.org/wiki/Security_fencing) to mark the company's perimeter.
* Fire extinguishers for fire-sensitive areas like server rooms and security rooms.
* [Security guards](http://en.wikipedia.org/wiki/Security_guards) can help to maximize physical security.

**School**

* An adjustable [firewall](http://en.wikipedia.org/wiki/Firewall_%28computing%29) and [proxy](http://en.wikipedia.org/wiki/Proxy_server) to allow authorized users access from the outside and inside.
* Strong [Antivirus software](http://en.wikipedia.org/wiki/Antivirus_software) and Internet Security Software packages.
* Wireless connections that lead to [firewalls](http://en.wikipedia.org/wiki/Firewall_%28computing%29).
* [Children's Internet Protection Act](http://en.wikipedia.org/wiki/Children%27s_Internet_Protection_Act) compliance. (Only schools in the USA)
* Supervision of network to guarantee updates and changes based on popular site usage.
* Constant supervision by teachers, librarians, and administrators to guarantee protection against attacks by both [internet](http://en.wikipedia.org/wiki/Internet) and [sneakernet](http://en.wikipedia.org/wiki/Sneakernet) sources.
* An enforceable and easy to understand acceptable use policy which differentiates between school owned and personally owned devices
* [FERPA](http://en.wikipedia.org/wiki/Family_Educational_Rights_and_Privacy_Act) compliance for institutes of higher education network

**Large government**

* A strong [firewall](http://en.wikipedia.org/wiki/Firewall_%28computing%29) and [proxy](http://en.wikipedia.org/wiki/Proxy_server) to keep unwanted people out.
* Strong [antivirus software](http://en.wikipedia.org/wiki/Antivirus_software) and Internet Security Software suites.
* Strong [encryption](http://en.wikipedia.org/wiki/Encryption).
* [Whitelist](http://en.wikipedia.org/wiki/Whitelist) authorized [wireless connection](http://en.wikipedia.org/wiki/Wireless_connection), block all else.
* All [network hardware](http://en.wikipedia.org/wiki/Network_hardware) is in secure zones.
* All [hosts](http://en.wikipedia.org/wiki/Host_%28network%29) should be on a [private network](http://en.wikipedia.org/wiki/Private_network) that is invisible from the outside.
* Host web servers in a [DMZ](http://en.wikipedia.org/wiki/Demilitarized_zone_%28computing%29), or a firewall from the outside and from the inside.
* [Security fencing](http://en.wikipedia.org/wiki/Security_fencing) to mark perimeter and set wireless range to this.
* Inventory controls of government owned mobile .

**Types of Attacks**

Networks are subject to [attacks](http://en.wikipedia.org/wiki/Attack_%28computing%29) from malicious sources. [Attacks](http://en.wikipedia.org/wiki/Attack_%28computing%29) 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.[[9]](http://en.wikipedia.org/wiki/Network_security#cite_note-9)

Types of attacks include:[[10]](http://en.wikipedia.org/wiki/Network_security#cite_note-10)

* Passive
  + Network
    - [wiretapping](http://en.wikipedia.org/wiki/Telephone_tapping)
    - [Port scanner](http://en.wikipedia.org/wiki/Port_scanner)
    - [Idle scan](http://en.wikipedia.org/wiki/Idle_scan)
* Active
  + [Denial-of-service attack](http://en.wikipedia.org/wiki/Denial-of-service_attack)
  + [Spoofing](http://en.wikipedia.org/wiki/Spoofing_attack)
  + [Man in the middle](http://en.wikipedia.org/wiki/Man-in-the-middle_attack)
  + [ARP poisoning](http://en.wikipedia.org/wiki/ARP_poisoning)
  + [Smurf attack](http://en.wikipedia.org/wiki/Smurf_attack)
  + [Buffer overflow](http://en.wikipedia.org/wiki/Buffer_overflow)
  + [Heap overflow](http://en.wikipedia.org/wiki/Heap_overflow)
  + [Format string attack](http://en.wikipedia.org/wiki/Format_string_attack)
  + [SQL injection](http://en.wikipedia.org/wiki/SQL_injection)
  + [cyber attack](http://en.wikipedia.org/wiki/Cyber_attack)

**See also**

* [Cloud computing security](http://en.wikipedia.org/wiki/Cloud_computing_security)
* [Crimeware](http://en.wikipedia.org/wiki/Crimeware)
* [Cyber security standards](http://en.wikipedia.org/wiki/Cyber_security_standards)
* [Data Loss Prevention](http://en.wikipedia.org/wiki/Data_Loss_Prevention)
* [Greynet](http://en.wikipedia.org/wiki/Greynet)
* [Information Leak Prevention](http://en.wikipedia.org/wiki/Information_Leak_Prevention)
* [Metasploit Project](http://en.wikipedia.org/wiki/Metasploit_Project)
* [Mobile security](http://en.wikipedia.org/wiki/Mobile_security)
* [Netsentron](http://en.wikipedia.org/wiki/Netsentron)
* [Network Security Toolkit](http://en.wikipedia.org/wiki/Network_Security_Toolkit)
* [TCP Gender Changer](http://en.wikipedia.org/wiki/TCP_Gender_Changer)
* [TCP sequence prediction attack](http://en.wikipedia.org/wiki/TCP_sequence_prediction_attack)
* [Timeline of hacker history](http://en.wikipedia.org/wiki/Timeline_of_hacker_history)
* [Wireless LAN Security](http://en.wikipedia.org/wiki/Wireless_LAN_Security)

**References**

* 1. [**^**](http://en.wikipedia.org/wiki/Network_security#cite_ref-1) Simmonds, A; Sandilands, P; van Ekert, L (2004). "An Ontology for Network Security Attacks". *Lecture Notes in Computer Science*. Lecture Notes in Computer Science **3285**: 317–323. [doi](http://en.wikipedia.org/wiki/Digital_object_identifier):[10.1007/978-3-540-30176-9\_41](http://dx.doi.org/10.1007%2F978-3-540-30176-9_41). [ISBN](http://en.wikipedia.org/wiki/International_Standard_Book_Number) [978-3-540-23659-7](http://en.wikipedia.org/wiki/Special:BookSources/978-3-540-23659-7).
  2. [**^**](http://en.wikipedia.org/wiki/Network_security#cite_ref-2) A Role-Based Trusted Network Provides [Pervasive Security and Compliance](http://newsroom.cisco.com/dlls/2008/ts_010208b.html?sid=BAC-NewsWire) - interview with [Jayshree Ullal](http://en.wikipedia.org/wiki/Jayshree_Ullal), senior VP of [Cisco](http://en.wikipedia.org/wiki/Cisco)
  3. [**^**](http://en.wikipedia.org/wiki/Network_security#cite_ref-3) Dave Dittrich, [*Network monitoring/Intrusion Detection Systems (IDS)*](http://staff.washington.edu/dittrich/network.html), University of Washington.
  4. [**^**](http://en.wikipedia.org/wiki/Network_security#cite_ref-4) ["''Honeypots, Honeynets''"](http://www.honeypots.net). Honeypots.net. 2007-05-26. Retrieved 2011-12-09.
  5. [**^**](http://en.wikipedia.org/wiki/Network_security#cite_ref-5) ["The six dumbest ways to secure a wireless LAN | ZDNet"](http://blogs.zdnet.com/Ou/index.php?p=43). Blogs.zdnet.com. Retrieved 2011-12-09.
  6. [**^**](http://en.wikipedia.org/wiki/Network_security#cite_ref-6) Julian Fredin, Social software development program Wi-Tech
  7. [**^**](http://en.wikipedia.org/wiki/Network_security#cite_ref-7) ["Introduction to Network Security"](http://www.interhack.net/pubs/network-security/network-security.html#SECTION00073000000000000000). Interhack.net. Retrieved 2011-12-09.
  8. [**^**](http://en.wikipedia.org/wiki/Network_security#cite_ref-8) ["Welcome to CERT"](http://www.cert.org). Cert.org. 2011-10-17. Retrieved 2011-12-09.
  9. [**^**](http://en.wikipedia.org/wiki/Network_security#cite_ref-9) Wright, Joe; Jim Harmening (2009) "15" Computer and Information Security Handbook Morgan Kaufmann Publications Elsevier Inc p. 257
  10. [**^**](http://en.wikipedia.org/wiki/Network_security#cite_ref-10) <http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf>

**Further reading**

* Cisco. (2011). What is network security?. Retrieved from [cisco.com](http://www.cisco.com/cisco/web/solutions/small_business/resource_center/articles/secure_my_business/what_is_network_security/index.html)
* [pcmag.com](http://www.pcmag.com/encyclopedia_term/0,2542,t=network+security&i=47911,00.asp)
* [Security of the Internet](http://www.cert.org/encyc_article/tocencyc.html) (*The Froehlich/Kent Encyclopedia of Telecommunications vol. 15*. Marcel Dekker, New York, 1997, pp. 231-255.)
* [*Introduction to Network Security*](http://www.interhack.net/pubs/network-security), Matt Curtin.
* [*Security Monitoring with Cisco Security MARS*](http://www.ciscopress.com/bookstore/product.asp?isbn=1587052709), Gary Halleen/Greg Kellogg, Cisco Press, Jul. 6, 2007.
* [*Self-Defending Networks: The Next Generation of Network Security*](http://www.ciscopress.com/bookstore/product.asp?isbn=1587052539), Duane DeCapite, Cisco Press, Sep. 8, 2006.
* [*Security Threat Mitigation and Response: Understanding CS-MARS*](http://www.ciscopress.com/bookstore/product.asp?isbn=1587052601), Dale Tesch/[Greg Abelar](http://www.ciscopress.com/authors/bio.asp?a=b411523c-c935-4708-a563-d24de8fcfc71), Cisco Press, Sep. 26, 2006.
* [*Securing Your Business with Cisco ASA and PIX Firewalls*](http://www.ciscopress.com/bookstore/product.asp?isbn=1587052148), [Greg Abelar](http://www.ciscopress.com/authors/bio.asp?a=b411523c-c935-4708-a563-d24de8fcfc71), Cisco Press, May 27, 2005.
* [*Deploying Zone-Based Firewalls*](http://www.ciscopress.com/bookstore/product.asp?isbn=1587053101), Ivan Pepelnjak, Cisco Press, Oct. 5, 2006.
* *Network Security: PRIVATE Communication in a PUBLIC World*, Charlie Kaufman | Radia Perlman | Mike Speciner, Prentice-Hall, 2002. ISBN .
* See How Security Alerts Help Manage Network Threats Retrieved from [AT&T security](http://www.business.att.com/enterprise/Portfolio/network-security/)
* [*Network Infrastructure Security*](http://www.springer.com/computer/communications/book/978-1-4419-0165-1), Angus Wong and Alan Yeung, Springer, 2009.

**External links**

* [Cyber Security Network](http://www.network.cyberwarzone.com)
* [Definition of Network Security](http://www.deepnines.com/secure-web-gateway/definition-of-network-security)
* [Cisco IT Case Studies](http://www.cisco.com/web/about/ciscoitatwork/case_studies/security.html) about Security and VPN
* [Firewall Security Case Study](http://www.business.att.com/enterprise/resource_item/Family/network-security/firewall-endpoint/Case_Study/armstrong_coal/)
* [Definition of Network Security](http://www.pcmag.com/encyclopedia_term/0,2542,t=network+security&i=47911,00.asp)
* Debate: The data or the source - which is the real threat to network security? - [Video](http://www.netevents.tv/docuplayer.asp?docid=102)
* OpenLearn - [Network Security](http://openlearn.open.ac.uk/course/view.php?id=2587)