1. Nondiscretionary access controls (NDACs)	**2.** Discretionary access controls (DACs)
3. Access control	**4.** lattice-based access control (LBAC)
5. capabilities tables	**6.** role-based access controls (RBACs)
7. attributes	**8.** attribute-based access controls (ABACs)
9. task-based access controls (TBACs)	**10.** Mandatory access controls (MACs)

2.
Access controls that are implemented at the discretion or option of the data user.

1.
Access controls that are implemented by a central authority.

4.
A variation on the MAC form of access control, which assigns users a matrix of authorizations for particular areas of access, incorporating the information assets of subjects such as users and objects.

3.
The selective method by which systems specify who may use a particular resource and how they may use it.

6.
An example of a nondiscretionary control where privileges are tied to the role a user performs in an organization, and are inherited when a user is assigned to that role. Roles are considered more persistent than tasks. RBAC is an example of an LDAC.

5.
In a lattice-based access control, the row of attributes associated with a particular subject (such as a user).

8.
An access control approach whereby the organization specifies the use of objects based on some attribute of the user or system.

7.
A characteristic of a subject (user or system) that can be used to restrict access to an object. Also known as a *subject attribute*.

10.
A required, structured data classification scheme that rates each collection of information as well as each user. These ratings are often referred to as sensitivity or classification levels.

9.
An example of a nondiscretionary control where privileges are tied to a task a user performs in an organization and are inherited when a user is assigned to that task. Tasks are considered more temporary than roles. TBAC is an example of an LDAC.

11.
Identification

12.
Authentication

13.
subject attributes

14.
authentication factors

15.
passphrase

16.
password

17.
synchronous tokens

18.
virtual password

19.
smart card

20.
dumb cards

12.
The access control mechanism that requires the validation and verification of an unauthenticated entity's purported identity.

11.
The access control mechanism whereby unverified or unauthenticated entities who seek access to a resource provide a label by which they are known to the system.

14.
Three mechanisms that provide authentication based on something an unauthenticated entity knows, something an unauthenticated entity has, and something an unauthenticated entity is.

13.
See *attribute*.

16.
A secret word or combination of characters that only the user should know; a password is used to authenticate the user.

15.
A plain-language phrase, typically longer than a password, from which a virtual password is derived.

18.
The derivative of a passphrase. See *passphrase*.

17.
An authentication component in the form of a token—a card or key fob that contains a computer chip and a liquid crystal display and shows a computer-generated number used to support remote login authentication. This token must be calibrated with the corresponding software on the central authentication server.

20.
An authentication card that contains digital user data, such as a personal identification number (PIN), against which user input is compared.

19.
An authentication component similar to a dumb card that contains a computer chip to verify and validate several pieces of information instead of just a PIN.

21.
Asynchronous tokens

22.
strong authentication

23.
Authorization

24.
auditability

25.
Accountability

26.
access control matrix

27.
Biometric access control

28.
false reject rate

29.
false accept rate

30.
minutiae

22.
In access control, the use of at least two different authentication mechanisms drawn from two different factors of authentication.

21.
An authentication component in the form of a token—a card or key fob that contains a computer chip and a liquid crystal display and shows a computer-generated number used to support remote login authentication. This token does not require calibration of the central authentication server; instead, it uses a challenge/response system.

24.
See *accountability*.

23.
The access control mechanism that represents the matching of an authenticated entity to a list of information assets and corresponding access levels.

26.
An integration of access control lists (focusing on assets) and capabilities tables (focusing on users) that results in a matrix with organizational assets listed in the column headings and users listed in the row headings. The matrix contains ACLs in columns for a particular device or asset and capabilities tables in rows for a particular user.

25.
The access control mechanism that ensures all actions on a system—authorized or unauthorized—can be attributed to an authenticated identity. Also known as *auditability*.

28.
The rate at which authentic users are denied or prevented access to authorized areas as a result of a failure in the biometric device. This failure is also known as a Type I error or a false negative.

27.
The use of physiological characteristics to provide authentication for a provided identification. Biometric means “life measurement” in Greek. Sometimes referred to as *biometrics*.

30.
In biometric access controls, unique points of reference that are digitized and stored in an encrypted format when the user’s system access credentials are created.

29.
The rate at which fraudulent users or nonusers are allowed access to systems or areas as a result of a failure in the biometric device. This failure is also known as a Type II error or a false positive.

31.
crossover error rate (CER)

32.
reference monitor

33.
covert channels

34.
trusted computing base (TCB)

35.
Storage channels

36.
firewall

37.
Timing channels

38.
untrusted network

39.
static packet filtering

40.
trusted network

32.
Within TCB, a conceptual piece of the system that manages access controls—in other words, it mediates all access to objects by subjects.

31.
Also called the equal error rate, the point at which the rate of false rejections equals the rate of false acceptances.

34.
Under the Trusted Computer System Evaluation Criteria (TCSEC), the combination of all hardware, firmware, and software responsible for enforcing the security policy.

33.
Unauthorized or unintended methods of communications hidden inside a computer system.

36.
In information security, a combination of hardware and software that filters or prevents specific information from moving between the outside network and the inside network.

35.
TCSEC-defined covert channels that communicate by modifying a stored object, such as in steganography.

38.
The system of networks outside the organization over which the organization has no control. The Internet is an example of an untrusted network.

37.
TCSEC-defined covert channels that communicate by managing the relative timing of events.

40.
The system of networks inside the organization that contains its information assets and is under the organization’s control.

39.
A firewall type that requires the configuration rules to be manually created, sequenced, and modified within the firewall.

41.
dynamic packet filtering

42.
packet-filtering firewall

43.
stateful packet inspection (SPI)

44.
state table

45.
address restrictions

46.
application firewall

47.
application layer proxy firewall

48.
proxy server

49.
demilitarized zone (DMZ)

50.
media access control layer firewalls

42.
A networking device that examines the header information of data packets that come into a network and determines whether to drop them (deny) or forward them to the next network connection (allow), based on its configuration rules.

41.
A firewall type that can react to network traffic and create or modify configuration rules to adapt.

44.
A tabular record of the state and context of each packet in a conversation between an internal and external user or system. A state table is used to expedite traffic filtering.

43.
A firewall type that keeps track of each network connection between internal and external systems using a state table and that expedites the filtering of those communications. Also known as a stateful inspection firewall.

46.
See *application layer proxy firewall*.

45.
Firewall rules designed to prohibit packets with certain addresses or partial addresses from passing through the device.

48.
A server that exists to intercept requests for information from external users and provide the requested information by retrieving it from an internal server, thus protecting and minimizing the demand on internal servers. Some proxy servers are also cache servers.

47.
A device capable of functioning both as a firewall and an application layer proxy server.

50.
A firewall designed to operate at the media access control sublayer of the network's data link layer (Layer 2).

49.
An intermediate area between two networks designed to provide servers and firewall filtering between a trusted internal network and the outside, untrusted network. Traffic on the outside network carries a higher level of risk.

51.
reverse proxy

52.
Unified Threat Management (UTM)

53.
Next Generation Firewall (NextGen or NGFW)

54.
single bastion host

55.
bastion host

56.
Network Address Translation (NAT)

57.
sacrificial host

58.
Port Address Translation (PAT)

59.
content filter

60.
screened subnet architecture

52.
Networking devices categorized by their ability to perform the work of multiple devices, such as stateful packet inspection firewalls, network intrusion detection and prevention systems, content filters, spam filters, and malware scanners and filters.

51.
A proxy server that most commonly retrieves information from inside an organization and provides it to a requesting user or system outside the organization.

54.
See *bastion host*.

53.
A security appliance that delivers unified threat management capabilities in a single appliance.

56.
A technology in which multiple real, routable external IP addresses are converted to special ranges of internal IP addresses, usually on a one-to-one basis; that is, one external valid address directly maps to one assigned internal address.

55.
A device placed between an external, untrusted network and an internal, trusted network. Also known as a *sacrificial host*, a bastion host serves as the sole target for attack and should therefore be thoroughly secured.

58.
A technology in which multiple real, routable external IP addresses are converted to special ranges of internal IP addresses, usually on a one-to-many basis; that is, one external valid address is mapped dynamically to a range of internal addresses by adding a unique port number to the address when traffic leaves the private network and is placed on the

57.
See *bastion host*.

60.
A firewall architectural model that consists of one or more internal bastion hosts located behind a packet filtering router on a dedicated network segment, with each host performing a role in protecting the trusted network.

59.
A software program or hardware/software appliance that allows administrators to restrict content that comes into or leaves a network—for example, restricting user access to Web sites from material that is not related to business, such as pornography or entertainment.

61.
extranet

62.
screened host architecture

63.
war dialer

64.
reverse firewalls

65.
data loss prevention

66.
Virtual private networks (VPNs)

67.
Kerberos

68.
Remote Authentication Dial-In User Service (RADIUS)

69.
hybrid VPN

70.
Secure VPNs

62.
A firewall architectural model that combines the packet filtering router with a second, dedicated device such as a proxy server or proxy firewall.

61.
A segment of the DMZ where additional authentication and authorization controls are put into place to provide services that are not available to the general public.

64.
See *content filter*.

63.
An automatic phone-dialing program that dials every number in a configured range (for example, 555–1000 to 555–2000) and checks whether a person, answering machine, or modem picks up.

66.
A private, secure network operated over a public and insecure network. A VPN keeps the contents of the network messages hidden from observers who may have access to public traffic.

65.
A strategy to gain assurance that the users of a network do not send high-value information or other critical information outside the network.

68.
A computer connection system that centralizes the management of user authentication by placing the responsibility for authenticating each user on a central authentication server.

67.
An authentication system that uses symmetric key encryption to validate an individual user's access to various network resources by keeping a database containing the private keys of clients and servers that are in the authentication domain it supervises.

70.
A VPN implementation that uses security protocols to encrypt traffic transmitted across unsecured public networks.

69.
A combination of trusted and secure VPN implementations.

71.
trusted VPN

71.

Also known as a legacy VPN, a VPN implementation that uses leased circuits from a service provider who gives contractual assurance that no one else is allowed to use these circuits and that they are properly maintained and protected.