

# **Network Security Controls, Protocols, and Devices**

## **Module 03**



# Network Security Controls, Protocols, and Devices

## Module 03

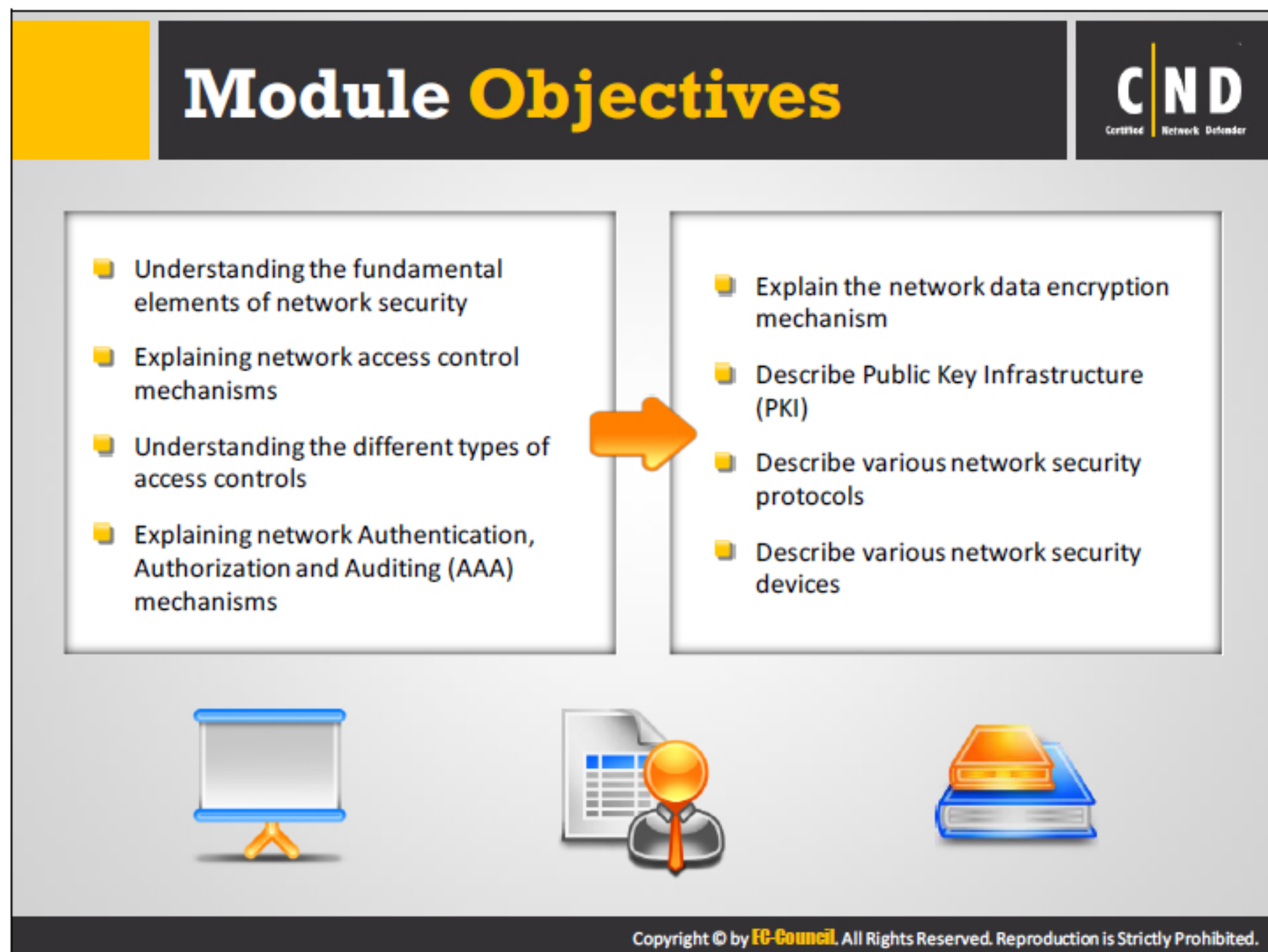


## Certified Network Defender

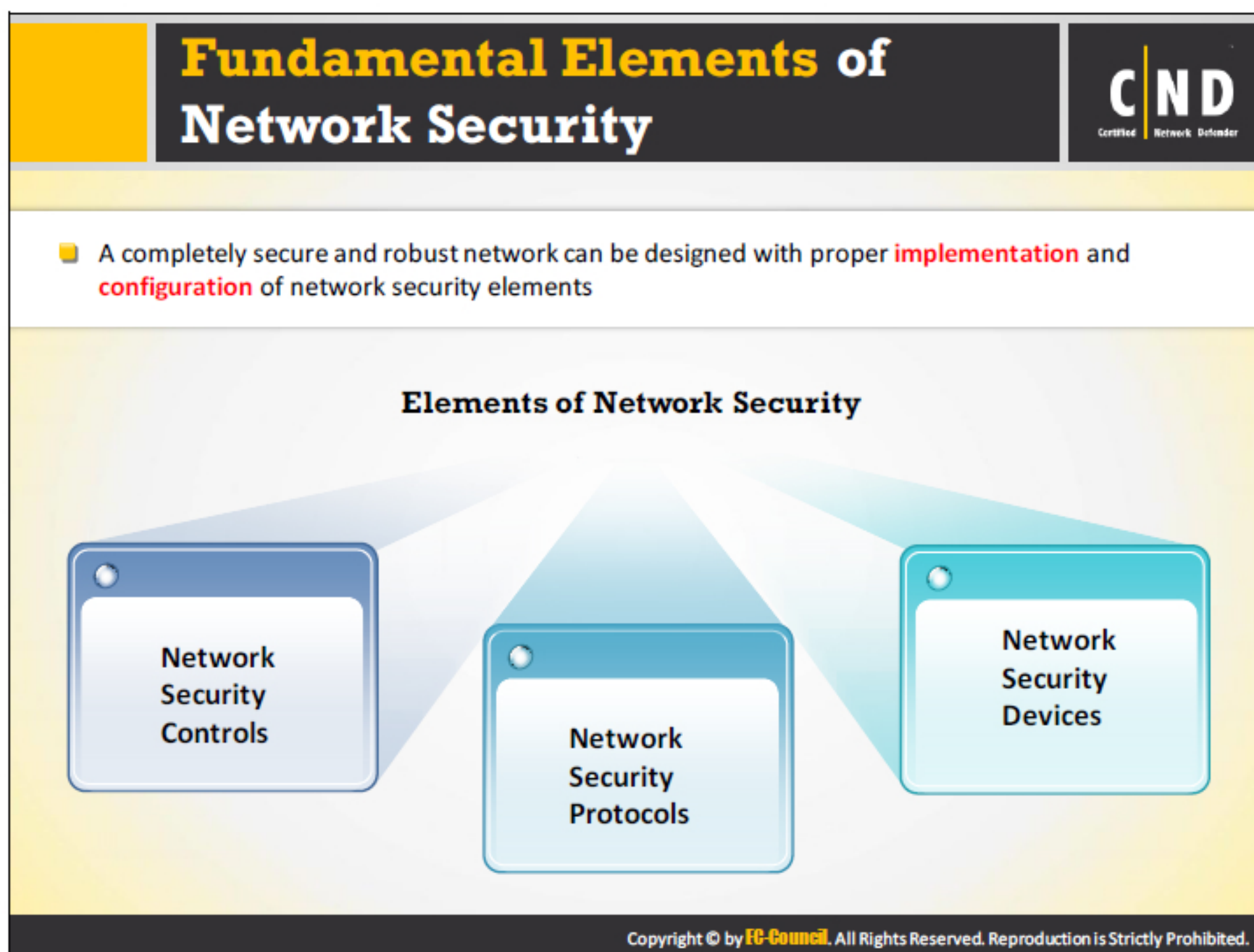
### Module 03: Network Security Controls, Protocols, and Devices

### Exam 312-38





This module discusses three important elements of network security, controls, protocols, and devices. The module will make teach you the various network security controls, including authentication, authorization, encryption and access controls. It also provides the necessary information on the different security protocols that should be implemented to secure the network. The module also discusses various security perimeter appliances commonly deployed in the network to defend against possible attacks.



Network security relies on three main security elements:

### Network Security Controls

Network security controls are the security features that should be appropriately configured and implemented to ensure network security. These are the cornerstones of any systematic discipline of security. These security controls work together to allow or restrict the access to organization's resources based on identity management.

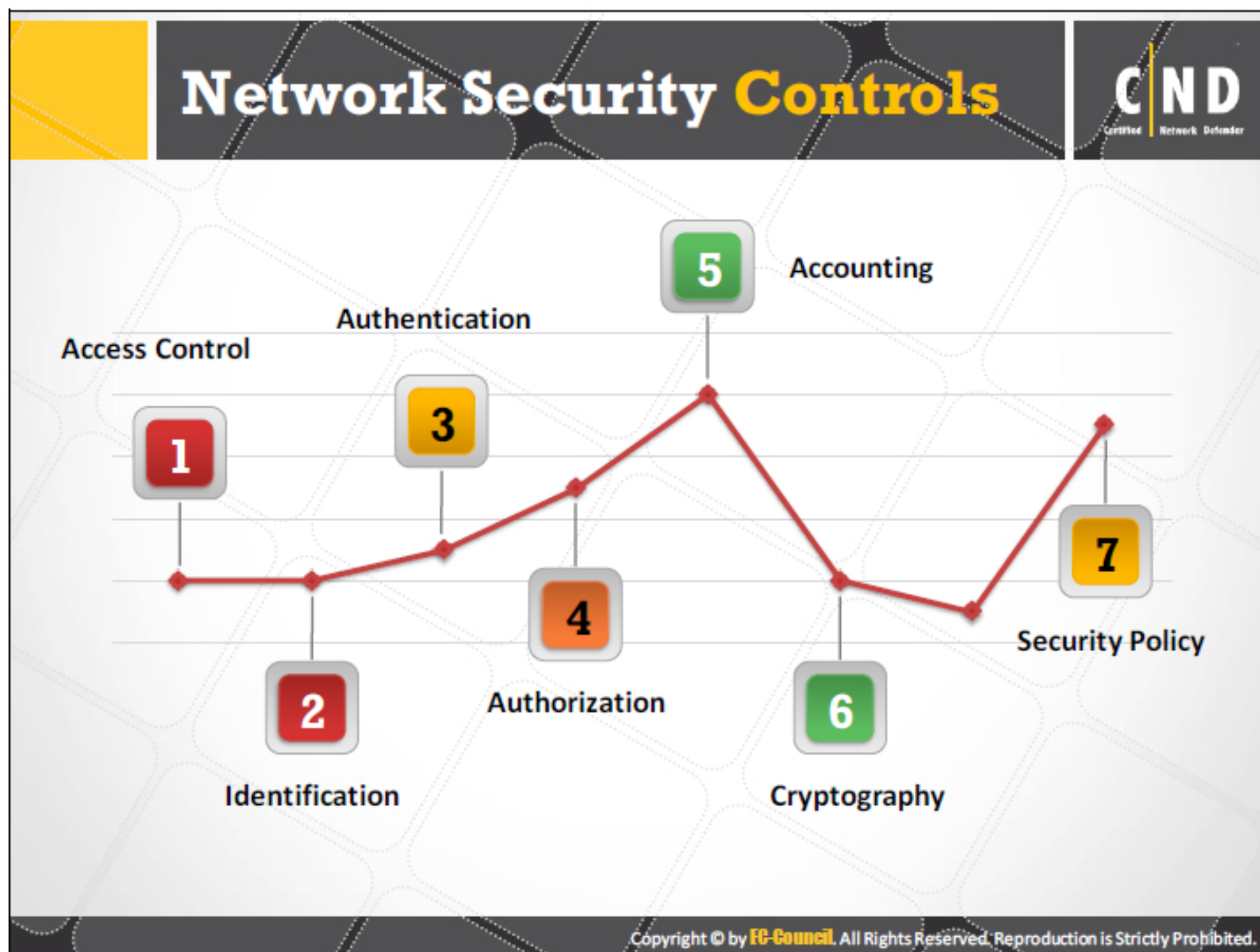
### Network Security Protocols

Network security protocols implement security related operations to ensure the security and integrity of data in transit. The network security protocols ensure the security of the data passing through the network. They implement methods that restrict unauthorized users from accessing the network. The security protocols use encryption and cryptographic techniques to maintain the security of messages passing through the network.

### Network Security Devices

Network security appliances are devices that are deployed to protect computer networks from unwanted traffic and threats. These devices can be categorized into active devices, passive devices, and preventative devices. It also consists of Unified Threat Management (UTM) which combines features of all the devices.





Network security controls are used to ensure the confidentiality, integrity, availability of the network services. These security controls are either technical or administrative safeguards implemented to minimize the security risk. To reduce the risk of a network being compromised, an adequate network security requires implementing a proper combination of network security controls.


These network security controls include:


- Authentication
- Authorization
- Accounting
- Access Control
- Identification
- Cryptography
- Security Policy

These controls help organizations with implementing strategies for addressing network security concerns. The multiple layers of network security controls along with the network should be used to minimize the risks of attack or compromise. The overlapping use of these controls ensures defense in depth network security.




# Access Control







Access control is the **selective restriction** of access to a place or other system/network resource



It **protects information assets** by determining who can and cannot access them



It **involves user identification**, authentication, authorization, and accountability



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Access control is a method for reducing the risk of data from getting affected and to save the enterprise's crucial data by providing limited access to users for accessing the computer resources. The crucial aspect of implementing access control is to maintain the integrity, confidentiality, and availability of the information. The mechanism of access control grants access to system resources to read, write, or execute to the user based on the access permissions and their associated roles.

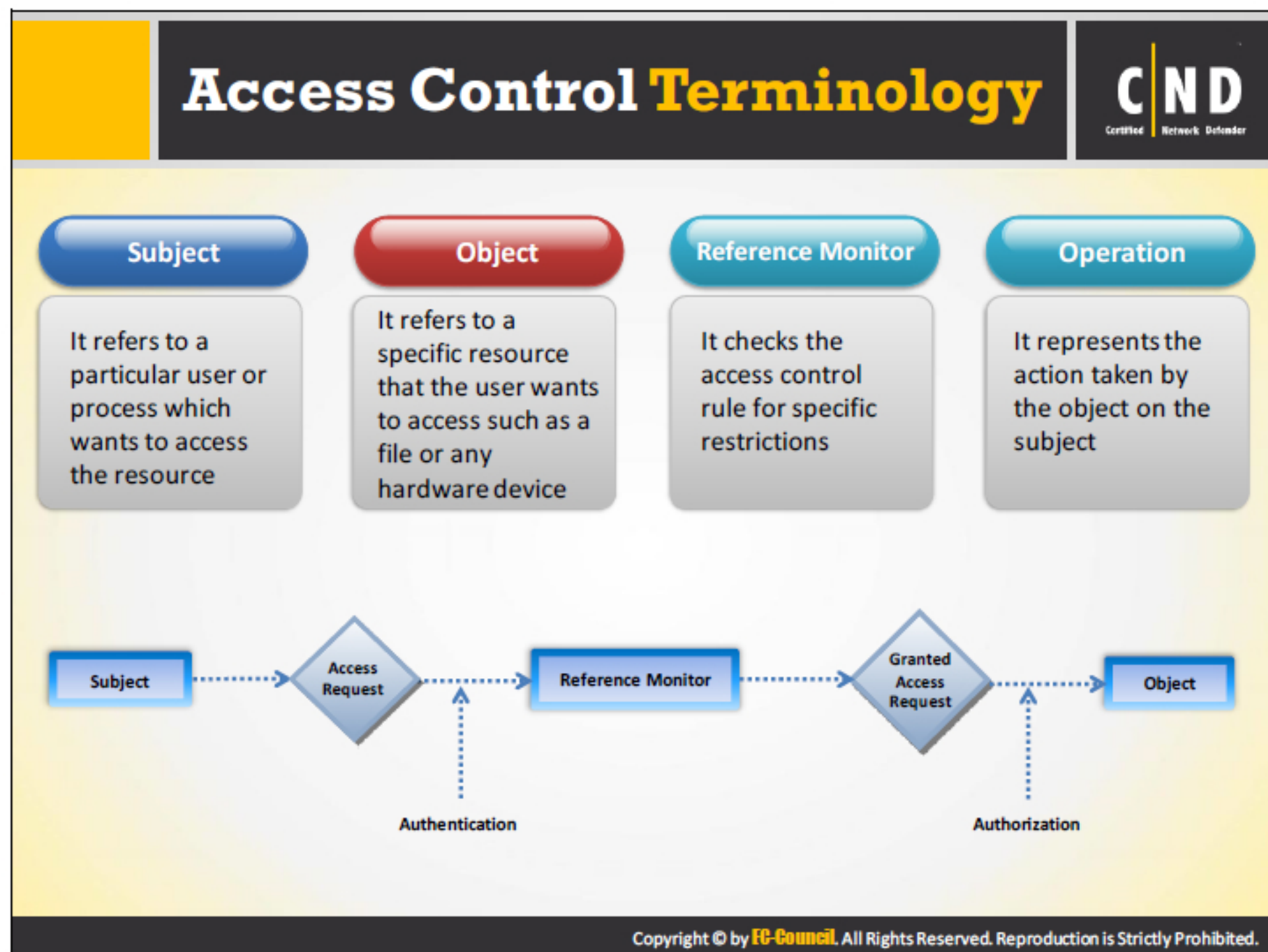
An access control system includes:

- File permissions, such as create, read, edit or delete.
- Program permissions, such as the right to execute a program.
- Data rights, such as the right to retrieve or update information in a database.

There are two types of access controls: physical and logical. The physical access controls the access to buildings, physical IT assets, etc. The logical access controls the access to networks and data.

In general, access control provides essential services like authorization, identification, authentication, access permissions and accountability. Authorization determines the action a user can perform whereas identification and authentication identify and permit only authorized users to access the systems. The access permissions determine approvals or permissions provided to a user to access a system and other resources. Accountability categorizes the actions performed by a user.





The following terminologies are used to define access control on specific resources:

### Subject

A subject may be defined as a user or a process, which attempts to access the objects. Further, subjects are those entities that perform certain actions on the system.

### Object

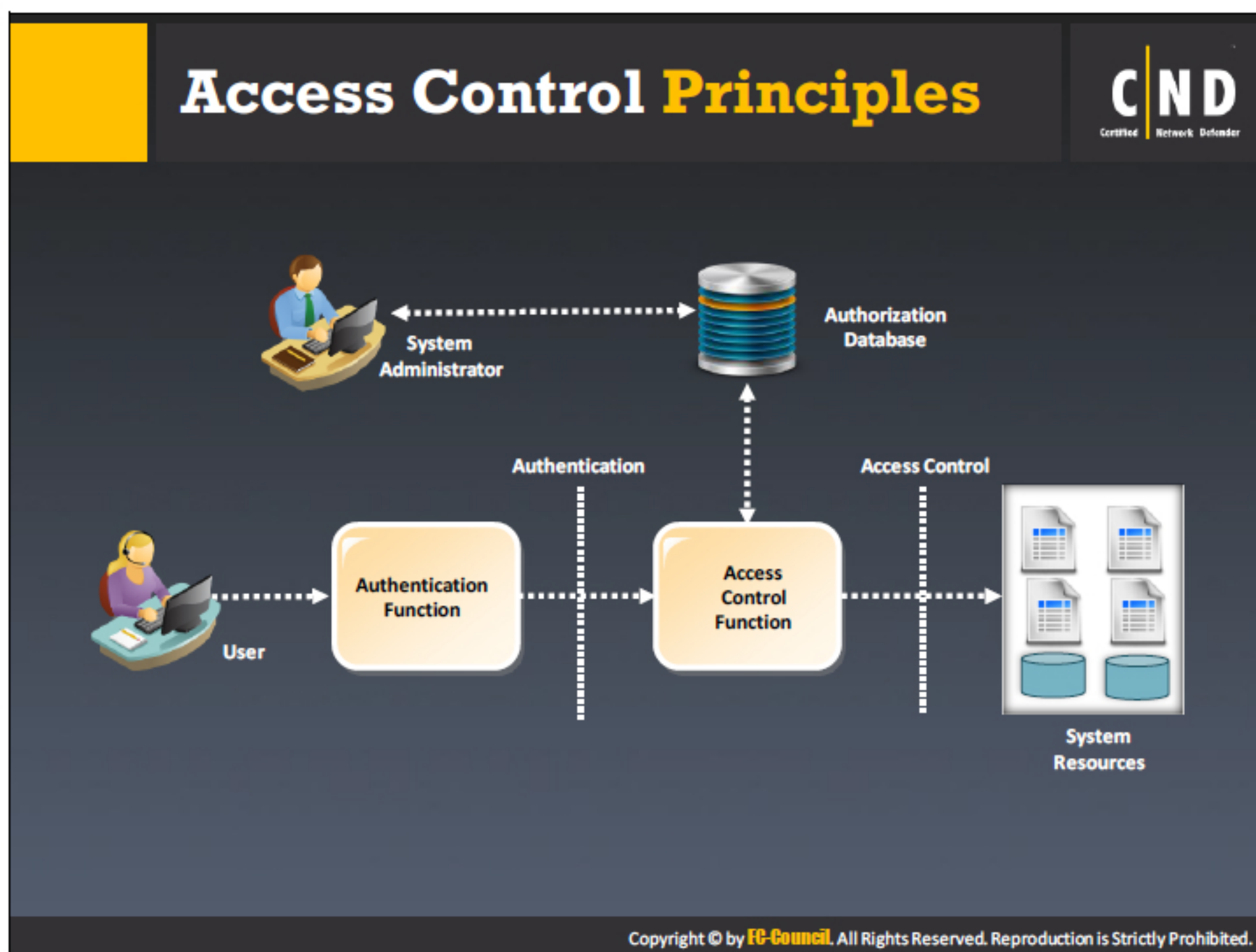
An object is an explicit resource on which access restriction is imposed. The access controls implemented on the objects further control the actions performed by the user. For example: Files or hardware devices.

### Reference Monitor

It monitors the restrictions imposed according to certain access control rules. Reference monitor implements a set of rules on the ability of the subject to perform certain actions on the object.

### Operation

An operation is an action performed by the subject on the object. A user trying to delete a file is an example of an operation. Here, the user is the subject, delete refers to the operation and file is the object.



Access control principles deal with restricting or allowing the access controls to users or processes. The principle includes the server receiving a request from the user and authenticating the user with the help of an Access Control Instruction (ACI). The server can either allow or deny the user to perform any actions like read, write, access files etc.

Access controls enable users to gain access to the entire directory, subtree of the directory and other specific set of entries and attribute values in the directory. It is possible to set permission values to a single user or a group of users. The directory and attribute values contain the access control instructions.

Access control function uses an authorization database, maintained by the security admin, to check the authorization details of the requesting user.

- General steps in Access Control:
  - **Step 1:** Users have to provide their credentials/identification while logging into the system.
  - **Step 2:** The system validates users with the provided credentials/identification such as password, fingerprint, etc. with the database.
  - **Step 3:** Once the identification of the user is successful, the system provides the user an access to use the system.
  - **Step 4:** The system then allows the user to perform only those operations or access only those resources for which the user is authorized.



- There are three main parts for an access control instruction:
  - **Target:** Permissions are set for certain attributes and entities. These attributes and entities are known as targets.
  - **Permission:** Permissions set for the target explains the actions allowed or denied for those targets.
  - **Bind Rule:** Specifies the subject to the access control instructions.



Administrative controls are management limitations, operational and accountability procedures, and other controls that ensure the security of an organization. The procedures prescribed in the administrative access control ensure the authorization and authentication of personnel at all levels. The components of an administrative access control are as follows:

### Security Policy and Procedures

Policies and procedures determine the method of implementing security practices in an organization. These specify the extent to which the company can accept a risk and specifies the level of actions allowed in the organization.

### Personnel Controls/Procedures

Personnel controls determine the methods by which the employees may handle the security principles. Personnel controls specify the steps taken in the case of any non-compliance issue. The change of security determines the steps taken right from the hiring of an employee until the employee leaves or shifts in any other department.

### Supervisory Structure

Supervisory structure consists of members that are responsible for the actions performed by the other employees in the organization in context of security.



## Security Awareness and Training

Trains the employees in an organization about the importance of access control. The training assists the employees to limit the attacks in the network and assists them in detecting and controlling the viruses and worms.

## Testing

Testing of the access controls brings out the weaknesses in the network, checks if all the access controls are working properly and evaluate the procedures and policies aligned for the proper functioning of the organization.

## Job Rotation

Job rotation improves error detection and fraud disclosures. Job rotation policy along with separation of duties is a good administrative access control. However, job rotation prevents employees to take up multiple roles at a time, which adds overhead to access control system. One needs to be aware of the impact of job rotation on access control system.

## Separation of Duties

Separation of duties comes into play when a single operation requires more than one person to complete it. When one individual is responsible for completing a task it gives them more power and the security risk is high. Whereas, if the same task is accomplished by a team of people, proper checks and balances are maintained and there is less chance for errors.

Example: Having one security administrator for doing actual planning and another team of security administrators implementing and testing will reduce the security risks and increase the chances of finding errors.

Separation of duties can be applied to a single person. For instance, if a user having limited access wants to perform a task requiring administrative privileges, User Account Control (UAC) can give access once the appropriate privileges are supplied.

## Information Classification

Implementing access control is impossible without Information classification. The information can be classified as: public, private, secret, proprietary, confidential, etc.

Process of Information Classification:

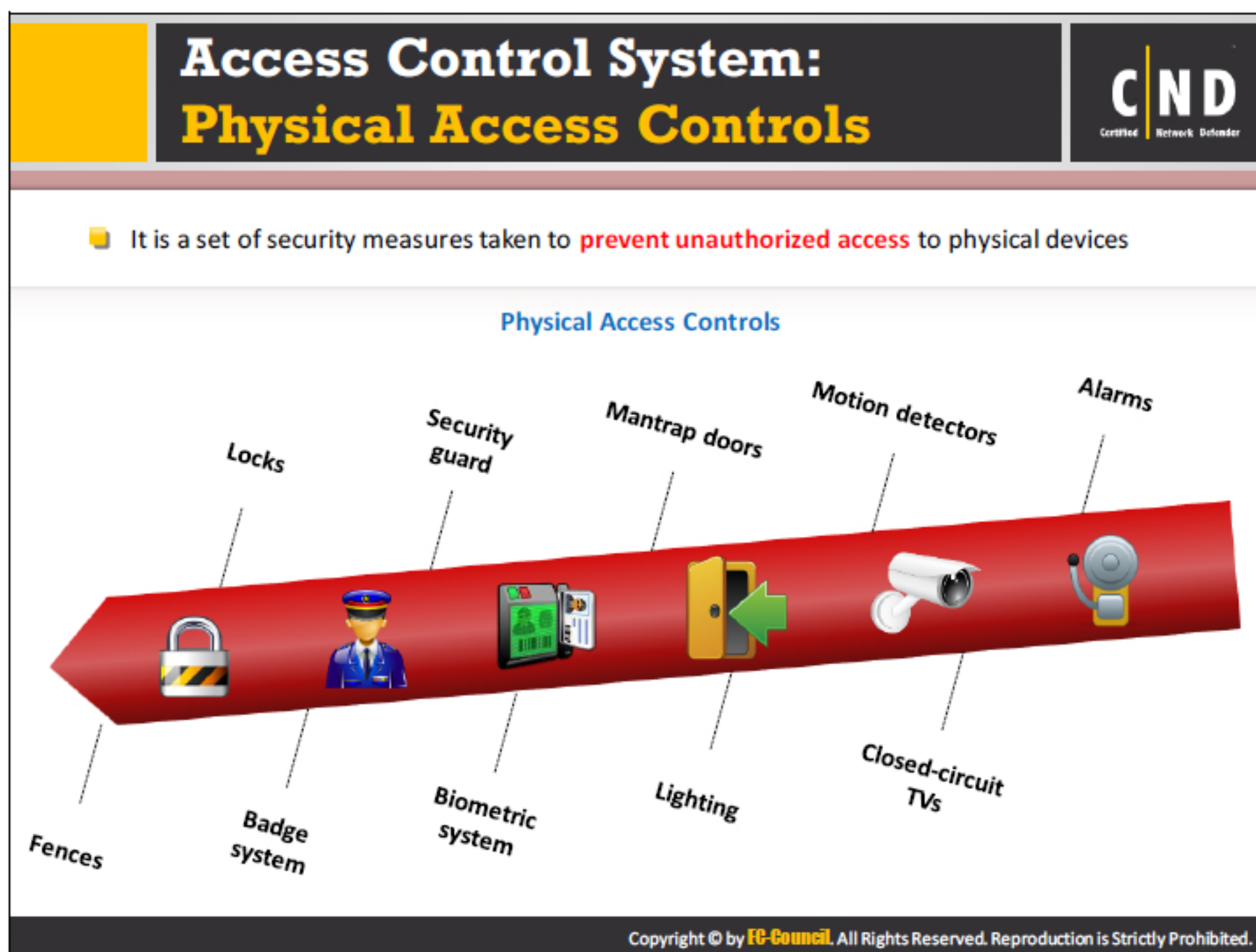
- Understand data classification project goals
- Build data classification policy
- Build data classification standards
- Build data classification process flow and procedures
- Create tools to support the process
- Determine application owners
- Determine data owners and data owner delegates

- Categorize information
- Define the audit process
- Save information in a repository
- Give user training
- Review and update Information classification at regular intervals

## Investigation

Investigate the logs for all doubtful activities and violations and make a report for further actions. Investigate unexpected information system related activities. Study the investigations periodically and make changes to access authorizations.





Appropriate physical access controls can reduce the chances of attacks and risks in an organization. Maintaining physical access controls provide physical protection of the information, buildings and all other physical assets of an organization.

The physical access controls are categorized into:

### Prevention Access Controls

They are used to prevent unwanted or unauthorized access to resources. It includes access controls such as fences, locks, biometrics, mantraps, etc.

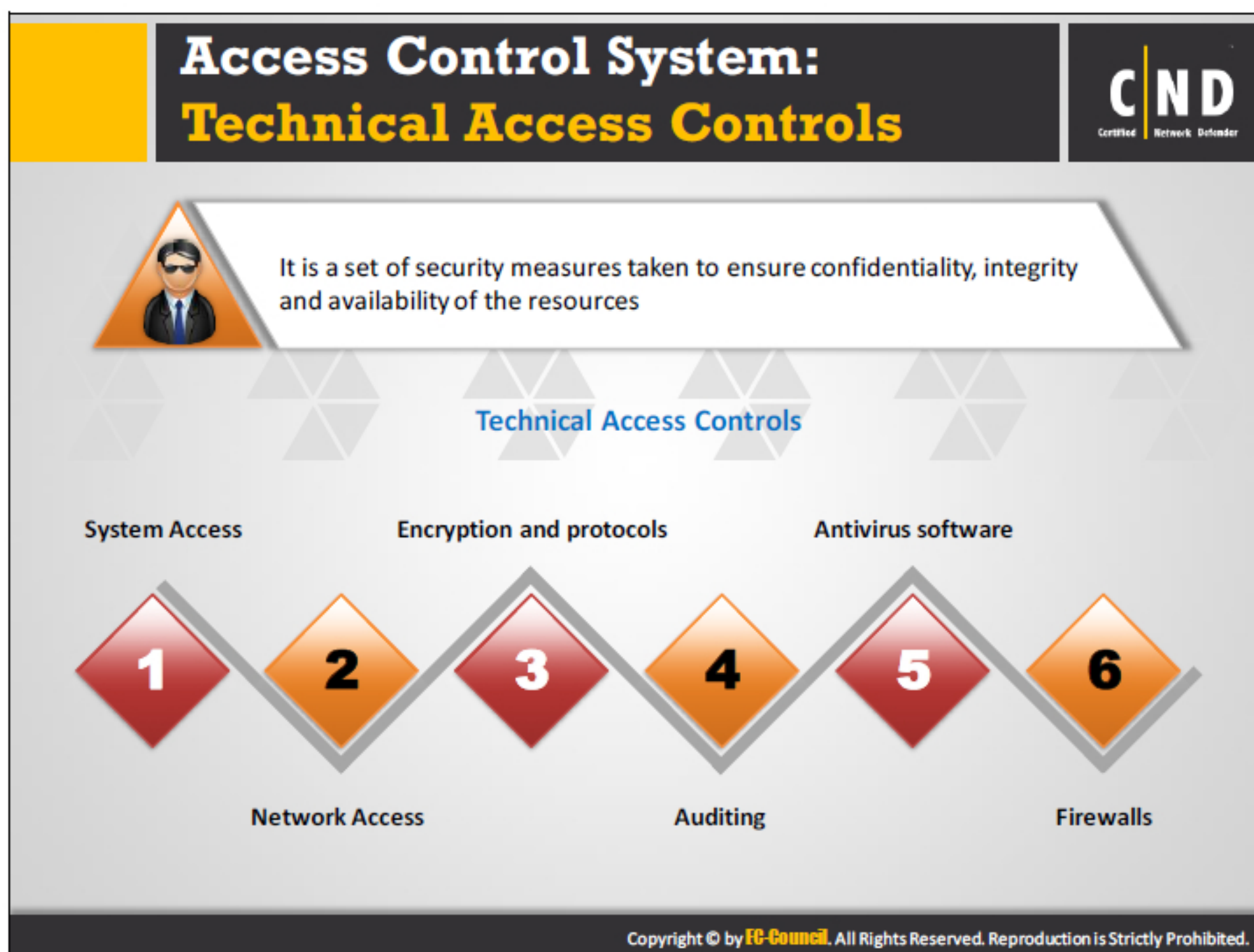
### Deterrence Controls

They are used to discourage the violation of security policies. It includes access controls such as security guards, warning signs, etc.

### Detection Controls

They are used to detect unauthorized access attempts. It includes access controls such as CCTV, alarms, etc.

An access control point can be a physical barrier such as a door or parking gate, where electronic access control is placed; users must enter their credentials before they get access. Using a PIN for authentication, checks the identity of a user. For example, in an office, the employee must place an access card to the card reader to be able to access the premises.



Technical access controls the subject's access to an object. It involves implementing technical access controls for restricting access to devices in an organization to protect the integrity of sensitive data.

The components of technical access control include:

### System Access

System access deals with restriction of access to data according to sensitivity of data, clearance level of users, user rights, and permissions.

### Network Access

Network access control offers different access control mechanisms for network devices like routers, switches, etc.

### Encryption and Protocols

Encryption and protocols protect the information passing through the network and preserves the privacy and reliability of the data.

### Auditing

Deals with tracking the activities of the network devices in a network. This mechanism helps in identifying the weaknesses in the network.

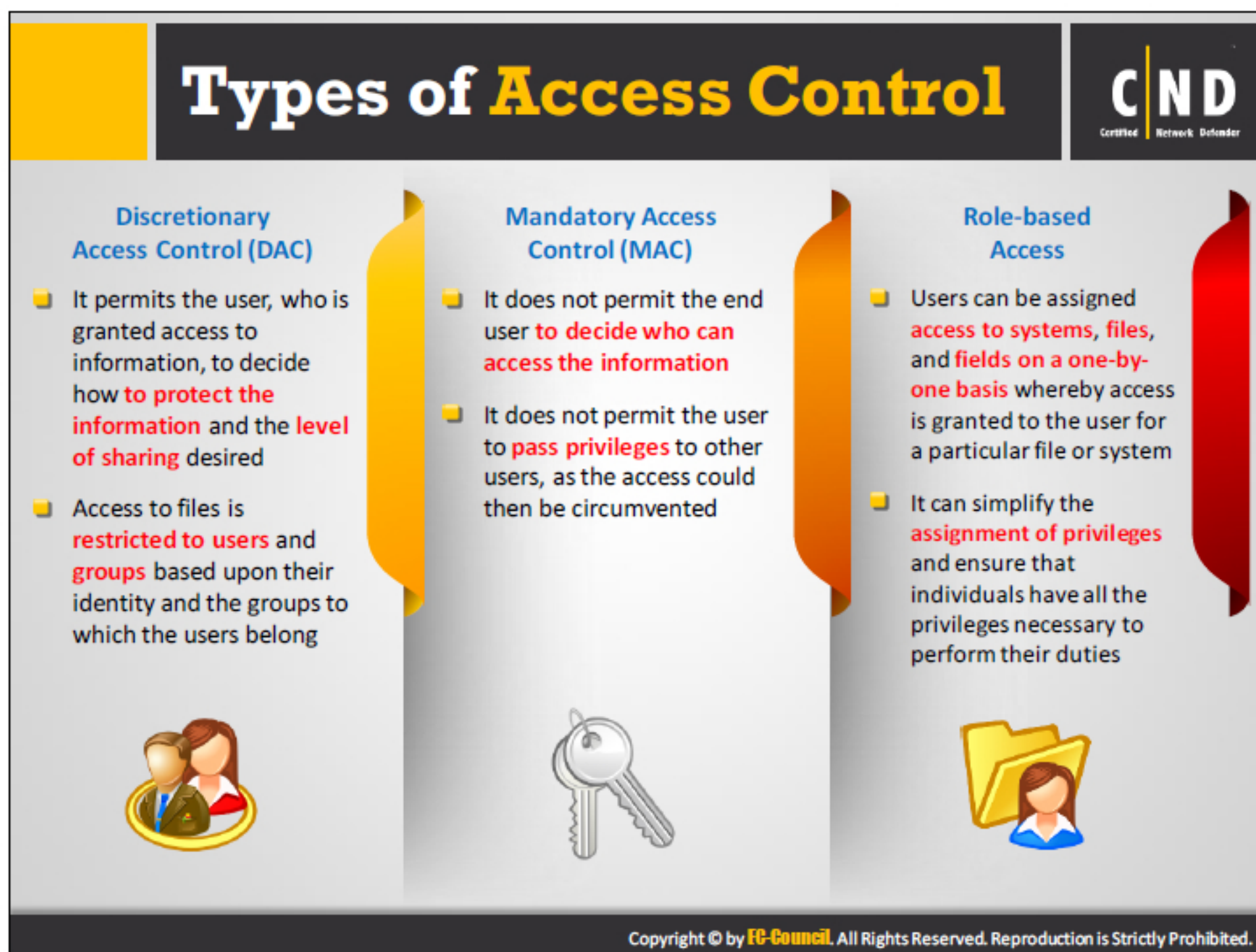
### Firewalls

Firewalls are implemented to filter unwanted traffic and prevent attacks on the network.



## Antivirus Software

Antivirus software is installed to prevent the system from malware infections.



Types of access control determine how a subject can access an object. The policies for determining the mechanism, uses access control technologies and security.

The types of access control include:

### Discretionary Access Control (DAC)

Discretionary access controls determine the access controls taken by any possessor of an object in order to decide the access controls of the subjects on those objects. The other name for DAC is a **need-to-know** access model. The decision taken by the owner depends on the following measures:

- **File and data ownership:** Determines the access policies of the user.
- **Access rights and permissions:** Setting access privileges to other subjects by the possessor.

The owner can provide or deny access either to any particular user or a group of users. The attributes of a DAC include:

- The owner of an object can transfer the ownership to another user.
- Access control prevents multiple unauthorized attempts to access an object.
- Prevents unauthorized users to view details like file size, file name, directory path etc.
- The DAC uses access control lists in order to identify and authorize users.



- **Disadvantages:**

- It requires to maintain the access control list and access permissions for the users.
- Examples of DAC include UNIX, Linux, and Windows access control.

## Mandatory Access Control (MAC)

The mandatory access controls determine the usage and access policies of the users. Users can access a resource only if that particular user has the access rights to that resource. MAC finds its application in the data marked as highly confidential. The network administrators impose MAC, depending on the operating system and security kernel.

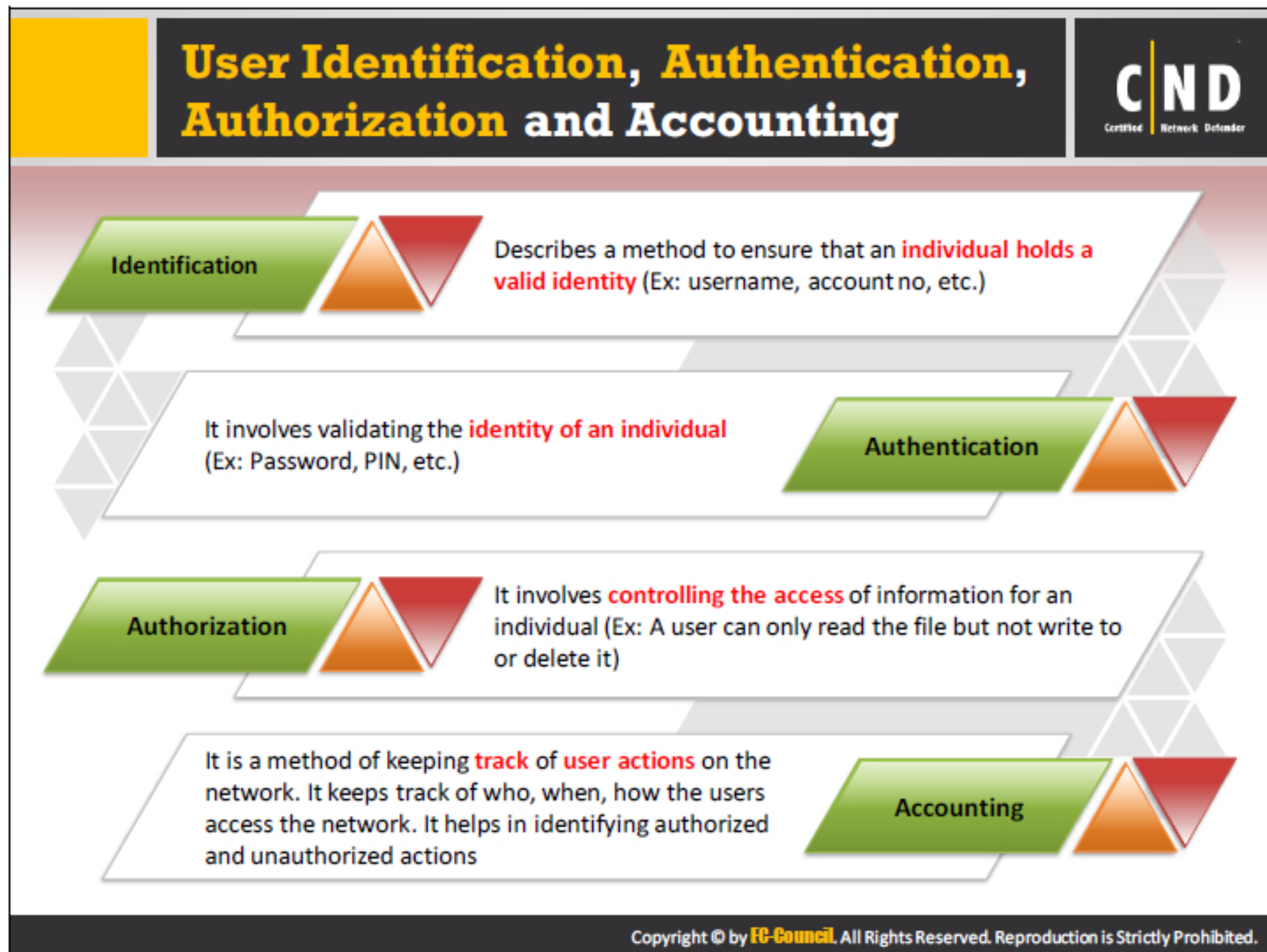
- There are two techniques to implement MAC:
  - **Rule based access control:** Rule based MAC specifies whether to allow or deny access to an object depending upon the levels of trust between the subject and the object.
  - **Lattice-based access control:** The lattice based access control defines the complex controls required for multiple subjects and objects.
- The advantages and disadvantages of MAC include:
  - MAC provides a high level of security as the network administrators determine the access controls.
  - The MAC policies minimize the chances of errors.
  - The operating system, depending on the MAC, mark and label the incoming data, thereby creating an external application control policy.
- Examples of MAC include SE Linux, trusted Solaris.

## Role Based Access Control (RBAC)

In role based access control, the access permissions are available based on the access policies determined by the system. The access permissions are out of user control which means that users cannot amend the access policies created by the system. The rules for determining the role based access controls are:

- **Role Assignment:** Assigning a certain role to a user that enables them to perform a transaction.
- **Role Authorization:** User needs to perform a role authorization in order to achieve that role.
- **Transaction Authorization:** Transaction authorization allows users to execute only those transactions for which they are authorized.





## Identification

Identification deals with confirming the identity of a user, process, or device accessing the network. User identification is the most common technique used in authenticating the users in the network and applications. Users have a unique user ID which helps in identifying them.

The authentication process includes verifying a user ID and a password. Users need to provide both the credentials in order to gain access to the network. The network administrators provide access controls and permissions to various other services depending on the user ID's.

Example: Username, Account Number, etc.

## Authentication

Authentication refers to verifying the credentials provided by the user while attempting to connect to a network. Both wired and wireless networks perform authentication of users before allowing them to access the resources in the network. A typical user authentication consists of a user ID and a password. The other forms of authentication are authenticating a web site using a digital certificate, comparing the product and the label associated with it. The factors associated with the process of authentication are:

- **Knowledge factors:** The knowledge factors refer to the mandatory entities that a user should know while trying to log into a system or network. For example, usernames and passwords.



- **Possession factors:** The possession factors refer to the entities that a user should hold while performing logging. For example: One-time password token, Employee ID cards, etc.
- **Inherence factors:** The inherence factors, mostly apply to the biometric factors that the users use for authentication. For example: retina scan, fingerprint scan, etc.

Common authentication methods include:

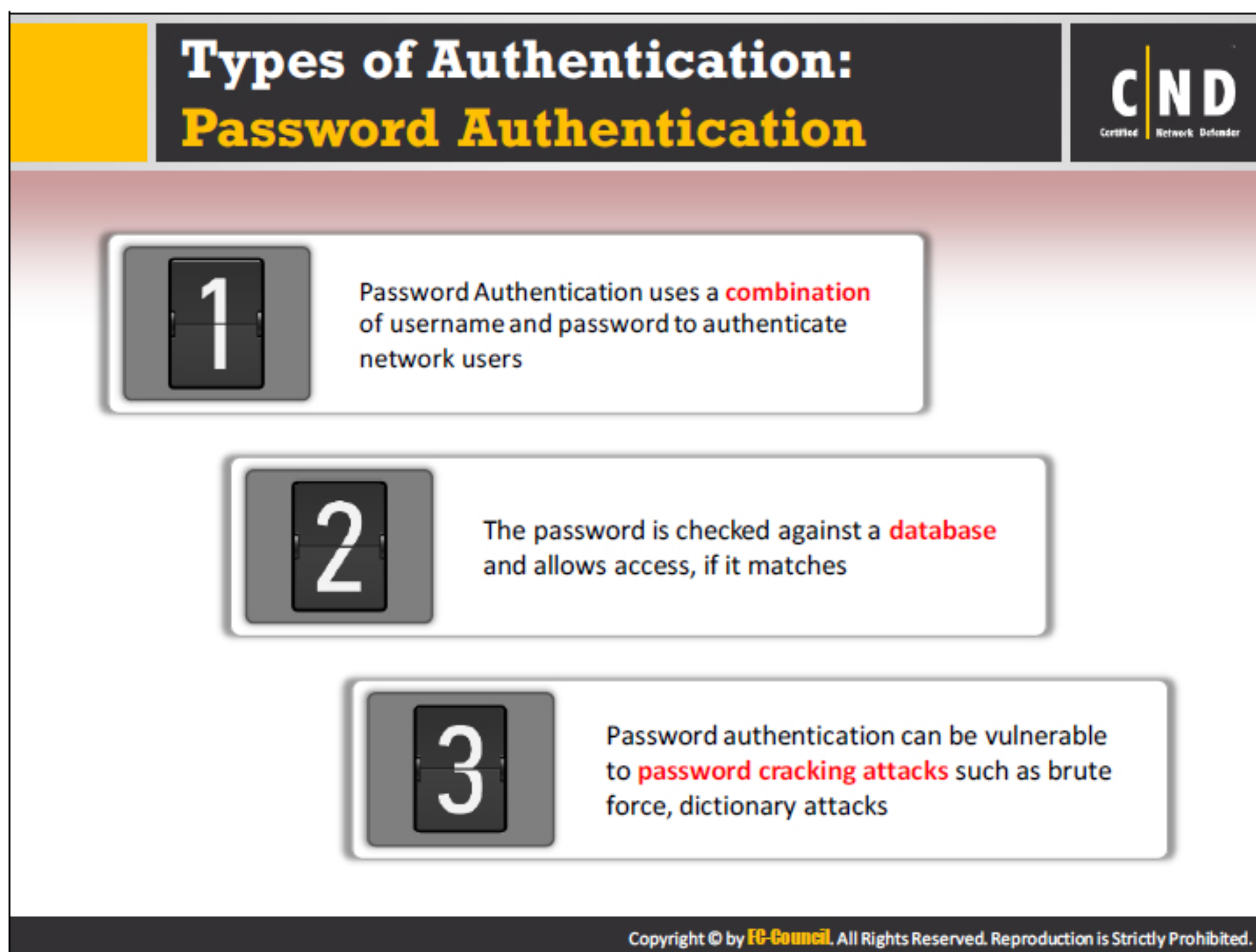
- Passwords
- Biometrics
- Token management
- Authorization

## Authorization

Authorization refers to the process of providing permission to access the resources or perform an action on the network. Network administrators can decide the access permissions of users on a multi-user system. They even decide the user privileges. The mechanism of authorization can allow the network administrator to create access permissions for users as well as verify the access permissions created for each user. In logical terms, authorization succeeds authentication. But, the type of authentication required for authorization varies. However, there are cases that do not require any authorization of the users requesting for a service. For example, no user authorization is needed when a user tries to access a web page from the Internet.

## Accounting

User accounting refers to tracking the actions performed by the user on a network. This includes verifying the files accessed by the user, functions like alteration or modification of the files or data.

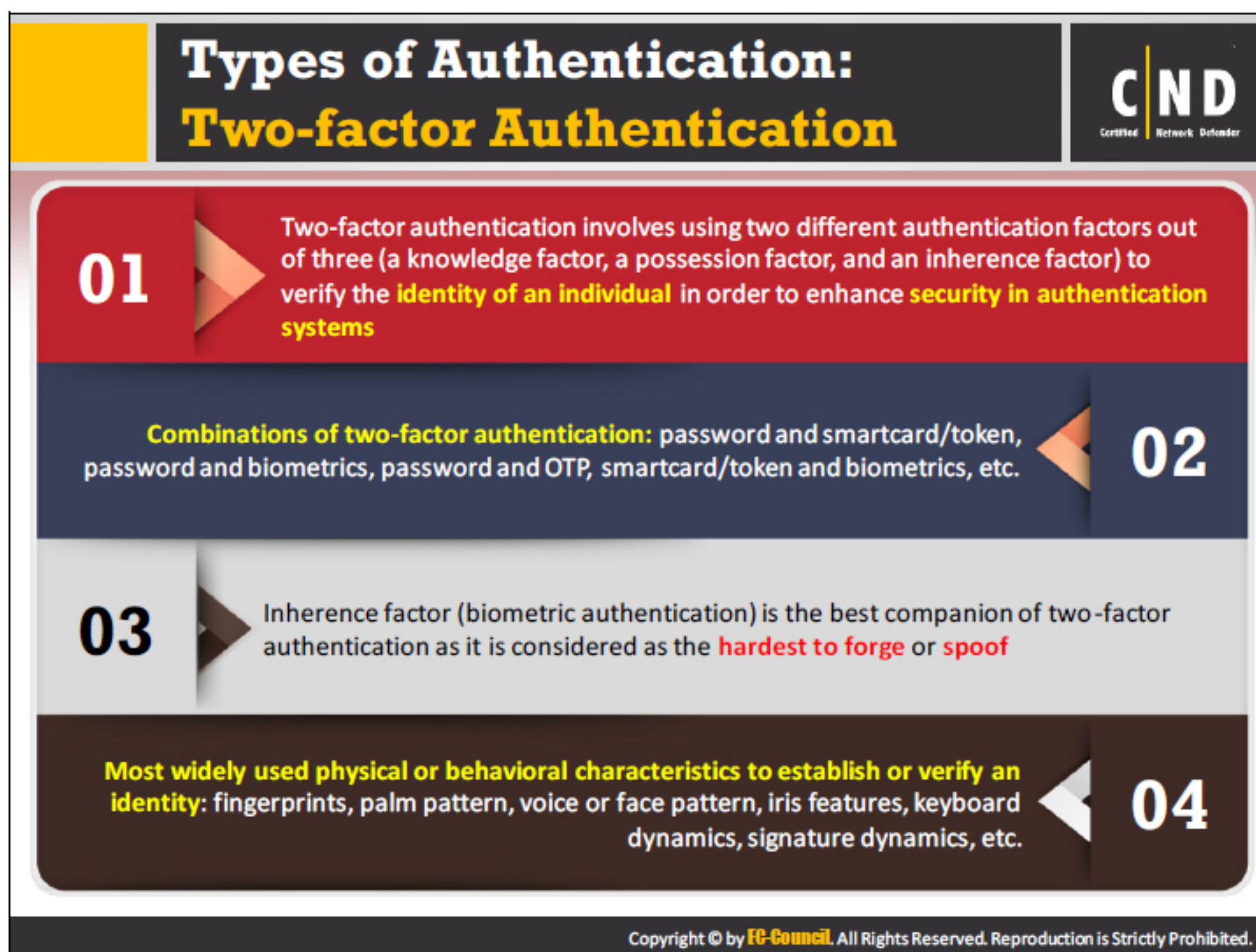


In password authentication, users need to provide usernames and the passwords to prove their identity to a system, application or network. The username and password are then matched against the list of authorized users in the database/windows active directory. Once matched, users can access the system.

The user password should follow standard password creation practices, including a mixture of alphabet letters, numbers and special characters, having a length greater than 8 characters (small passwords are easily guessed).

Password authentication is vulnerable to brute force attacks (A person trying possible combinations of characters to guess the password or capture packets using a protocol “sniffer” while sending across the network as plain text).





The two-factor authentication is a process where a system confirms the user identification in two steps. The users may use a physical entity like a security token as one of the credentials and the other credential can include security codes.

Two-factor authentication depends on two factors:

- Something you have
- Something you know

Example: A bank card – A user requires swiping the bank card and entering the PIN while accessing the bank card. Here, bank card is the physical entity and the PIN is the security code.

Advantage of two factor authentication includes decreasing the chances of identity theft and phishing. However, there are certain drawbacks for this two-step process. There are situations where the user will have to wait for the organization to issue the physical token to the user. The delay in getting the token results in users waiting for a long time to access their private data.

Identity evaluation depends on Knowledge, Possession, and Inherent Factors. Out of these, inherent factors are difficult to change as they depend on the characteristics of a human being.

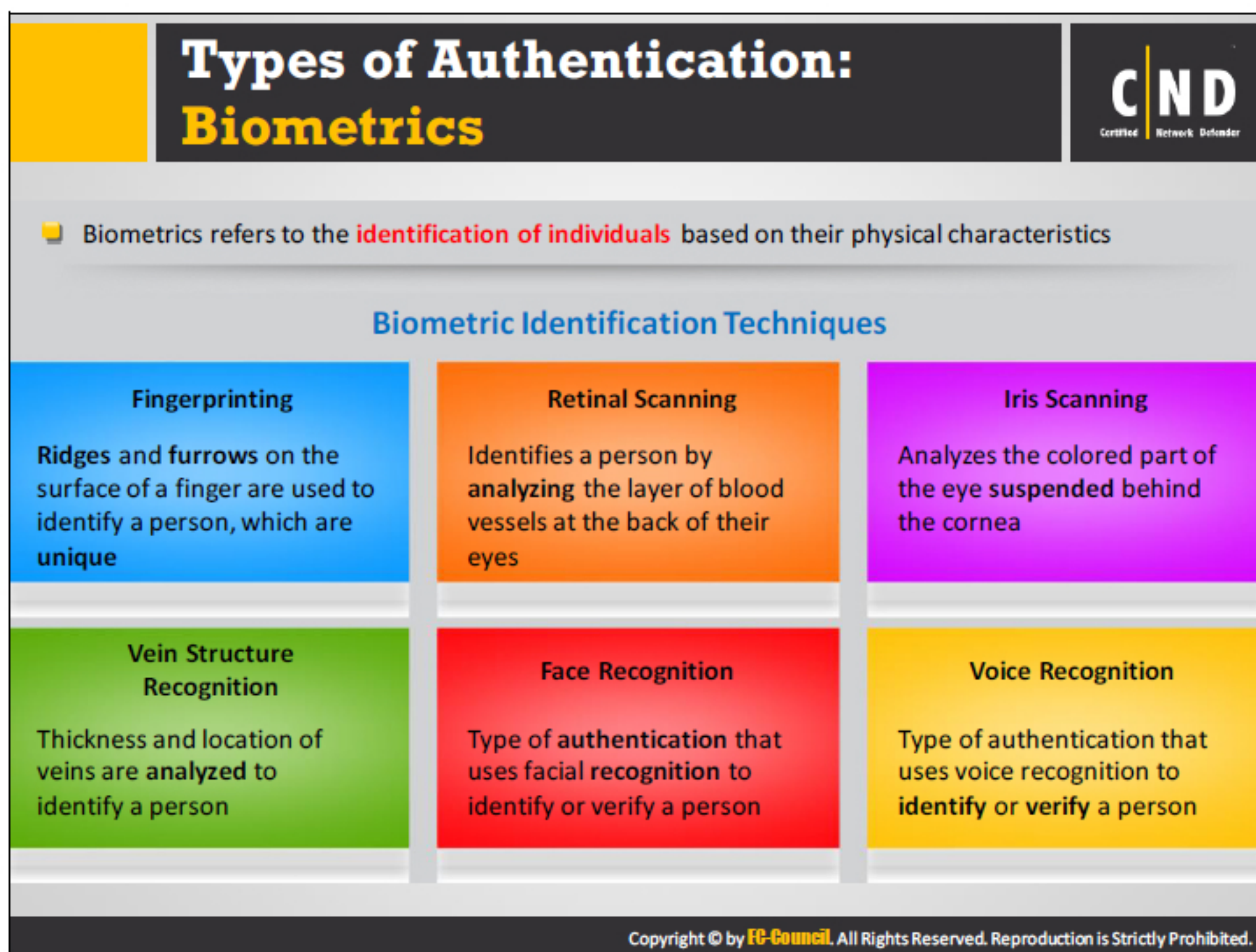
There are many combinations available in the two-factor authentication. Commonly found are:

- Password and Smart card
- Password and Biometrics
- Password and OTP

- Smart card and Biometrics

Two-factor authentications performed without the use of tokens are called Tokenless authentication. They can be implemented quickly across the network.





Biometric is a technology which identifies human characteristics for authorizing people. The most common used biometrics are fingerprint scanner, retina scanner, facial recognition, DNA, and voice recognition.

Biometric authentication involves following steps:

- The reader scans biometric data
- A software converts the scanned information into a digital form and compares against the stored data


Biometric takes the current biometric data and compares it with the biometric data stored in the database. If both data matches, then it confirms the authenticity of the user and allows permission.


- Types of identification techniques used in biometrics are:
  - **Fingerprint Scanning:** Compares two fingerprints for verification and identification using the patterns on the finger. The patterns depend on ridges and minutia points that differentiate each user's finger prints.
  - **Retinal Scanning:** Compares and identifies a user using the distinctive patterns of retina blood vessels.
  - **Iris Scanning:** Compares and identifies the images of the iris of one or both eyes of a user. The iris pattern differs from one person to another.

- **Vein structure Recognition:** Compares and identifies the patterns produced by user's veins. Each person has different patterns according to the flow of blood.
- **Face Recognition:** Compares and identifies a person depending on the facial patterns from an image or a video source.
- **Voice Recognition:** Compares and identifies a person according to the voice patterns or speech patterns.
- **Advantages of Biometrics:**
  - It is difficult to tamper the biometric details like a password or username. They cannot be shared or stolen using social engineering techniques. The biometric authentication requires the presence of the user which reduces the chances unauthorized access.




## Types of Authentication: Smart Card Authentication






- Smartcard is a small **computer chip device** that holds a users' personal information required to authenticate them



- Users have to insert their Smartcards into readers and their **Personal Identification Number (PIN)** to authenticate themselves



- Smartcard Authentication is a **cryptography-based authentication** and provides stronger security than password authentication

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Organizations use smart card technology to ensure strong authentication. The smart technology can store password files, authentication tokens, one-time password files, biometric templates, etc. Smart card technology finds its usage with another authentication token providing a multi-factor authentication. This enables a better logical access security. Smart card technology finds its application in VPN authentication, email and data encryption, electronic signatures, secure wireless logon, biometric authentication.

Smart card consists of a small computer chip and stores personal information of the user for identification. Smart cards are inserted into the machine for authentication along with providing the Personal Identification Number (PIN). Smart cards also help in storing the public and the private keys.

The main advantage of using a smart card is that it eliminates the risk of credentials being stolen from a computer as they are stored in the card's chip itself. However, it only enables a limited amount of information to be stored in the card's microchip.


- **Advantages of Smart Card:**

- Uses highly secure technology: The smart card technology uses better encryption and authentication methods, increasing the security of the card.
- Easy to carry: Smart cards are easy to carry and a user just needs to know the PIN of the card.

- Reduces the chances of deception by users: The smart card enables users to store information like fingerprint, other biometric details, thereby allowing organizations to recognize their employees.
- **Disadvantages of Smart cards:**
  - Can be easily lost: Since the smart cards are small in size, the chances of losing it are very high.
  - Security issues: Losing a smartcard puts its owner's information and identity at great risk.
  - High cost for production of smart cards: As smart cards have microchips and other encryption technologies; its production cost is high.




## Types of Authentication: Single Sign-on (SSO)



It allows a user to authenticate themselves to **multiple servers** on a network with **single password** without re-entering it every time

**Advantages:**

- Don't need to remember passwords of multiple applications or systems
- Reduces the time for entering a username and password
- Reduces the network traffic to the **centralized server**
- Users need to enter credentials only once for multiple applications



Single Sign-on (SSO) Authentication

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

As the name suggests, it allows users to access multiple applications using a single user name and password. The SSO stores the credentials of a user in an SSO policy server. An example for SSO is Google applications. Users can access all Google applications using a single user name and password combination. Consider Google as a central service. The central service creates a cookie for all users logging in for the first time in any of the applications present in the central service. When a user attempts to access other applications of the central service, it eliminates the need for the user to enter the credentials again due to the cookie which is already created. The system checks the credentials using the cookie created.

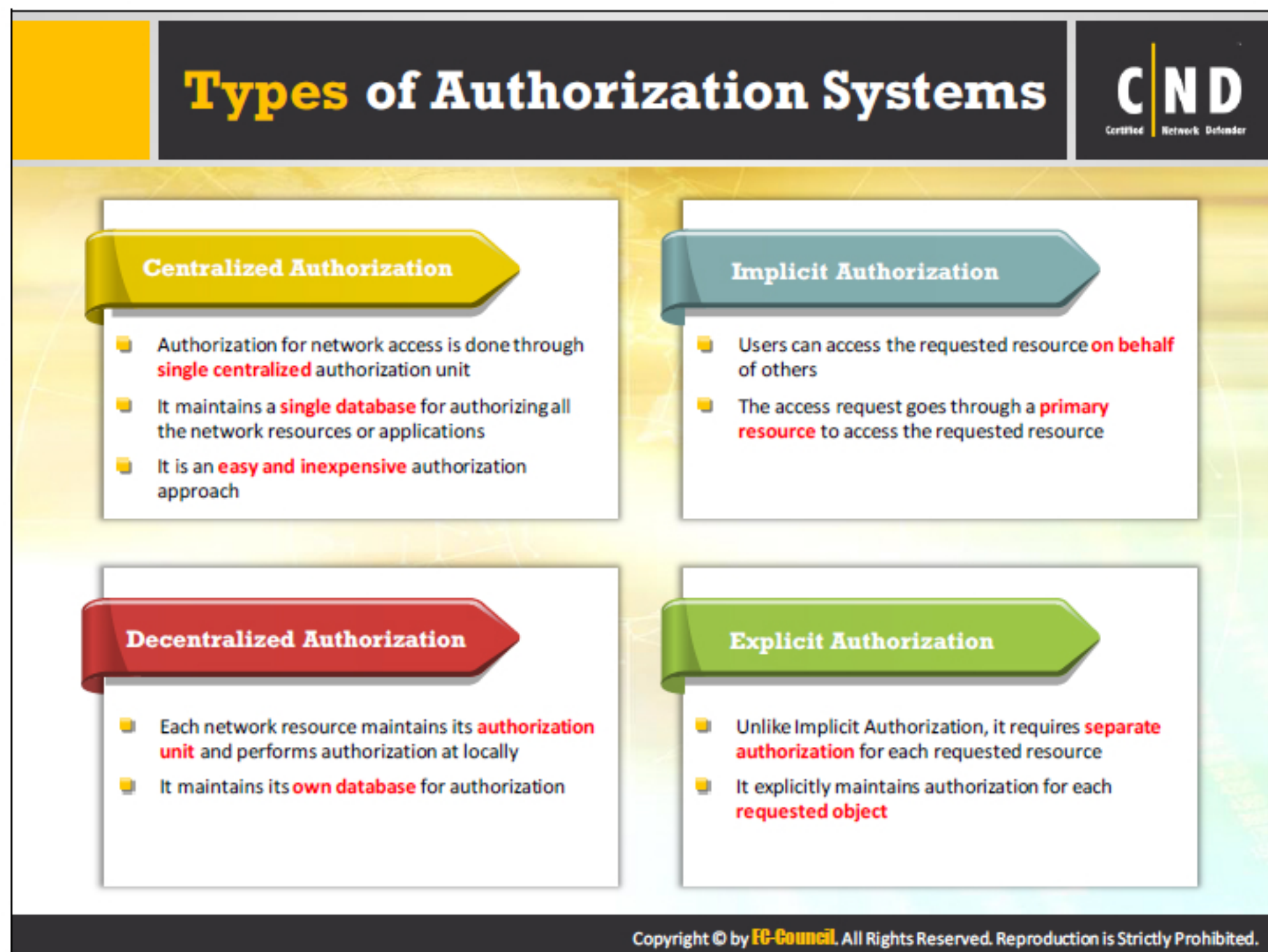
▪ **Advantages of SSO:**

- Reduces the chances of re-authentication thereby increasing the productivity.
- Removes the chances of Phishing.
- Provides a better management of applications due to a centralized database.

▪ **Disadvantages of SSO:**

- Losing credentials have a higher impact as all the applications of the central service become unavailable.
- There are many vulnerability issues related with the authentication to all the applications.
- It is an issue in multi-user computers and requires certain security policies implemented to ensure security.





Network authorization can take different forms based on the organization's need.

## Centralized Authorization

The need for centralized authentication came into existence when it became difficult to implement the authorization process individually for each resource. It uses a central authorization database that allows or denies access to users. The decision depends on the policies created by the centralized units. This enables easy authorization for users accessing different platforms. The centralized authorization units are easy to handle and have low costs. A single database provides access to all applications, thereby enabling better security. The centralized database also provides an easy method of adding, modifying, and deleting the applications from the centralized unit.

## Decentralized Authorization

The decentralized authorization maintains a separate database for each resource. The database contains the details of all users permitted to access that resource. The decentralized authorization process enables users to provide access to other users as well. This increases the flexibility level of the users in using the decentralized method. However, certain issues related to the decentralized authorization are cascading and cyclic authorizations.

## Implicit Authorization

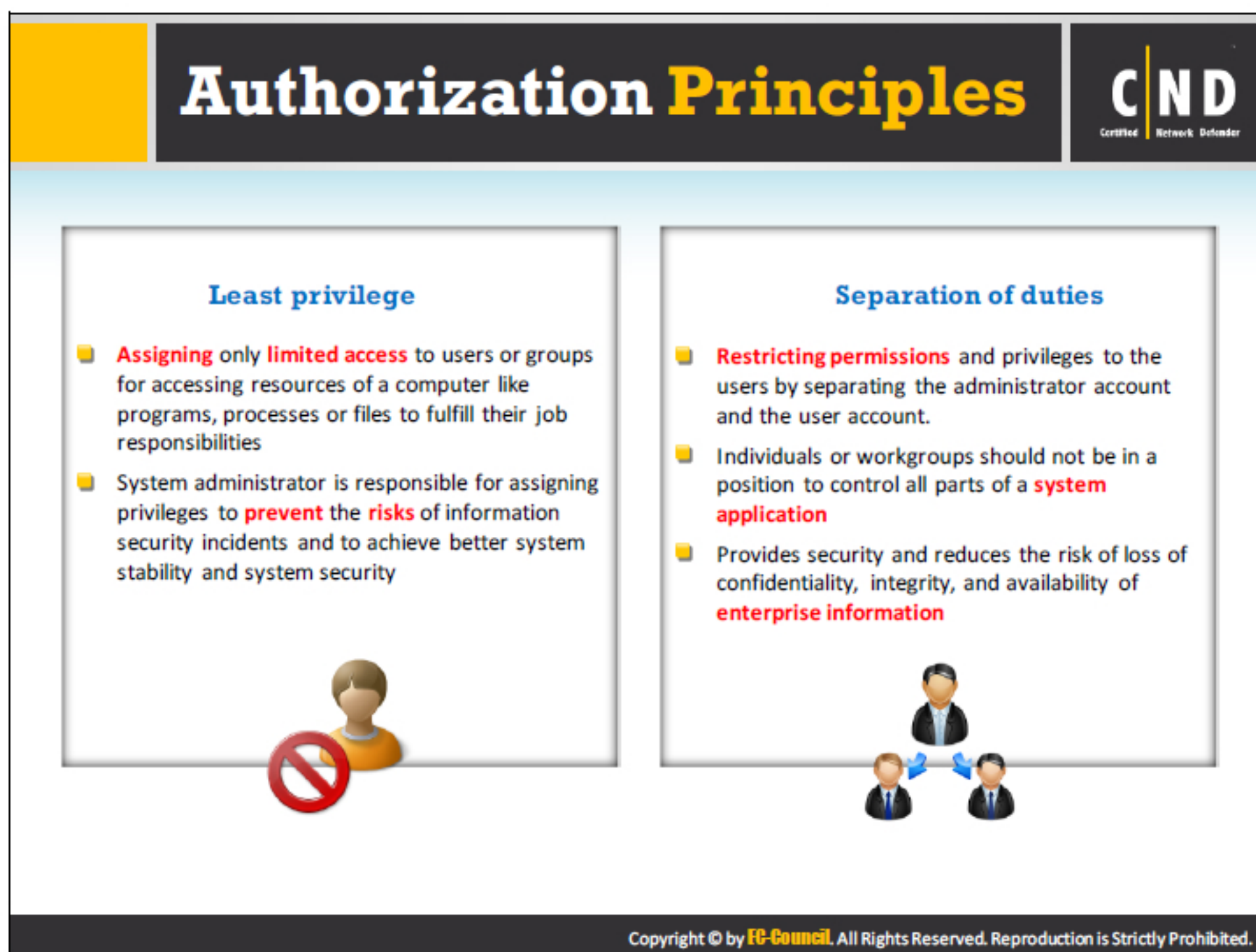
Implicit authorization provides the access to resources indirectly. The task is possible after the user gets authorization for a primary resource through which the access to the requested



resource is possible. For example, the user requesting a web page has permission to access the main page as well as all pages linked to the main page. Hence, the user is gaining an indirect access to the other links and documents attached to the main page. The implicit authorization provides a level of better granularity.

### **Explicit Authorization**

The explicit authorization maintains separate authorization details for each resource request. The explicit authorization technique is simpler than implicit technique; however, this technique makes use of more storage space due to storage of all authorization details.



Authorization principle describes in detail the access permission levels of users. Enabling authorization process ensures the security of the processes and resources. The process of authorization should be based on the following principles:

### Least Privilege


Least privilege provides access permissions to only those users who really need the access and resources. The permission granted depends on the roles and responsibilities of the user requesting the access. There are two underlying principles involved in the least privilege method: Less right and Less risk. According to these principles, users need to complete the task using the limited amount of resources in a limited amount of time provided to the users. This approach reduces the unauthorized access to the system resources.

### Separation of Duties

It involves the breaking authorization process into various steps. Different privileges are assigned to each step for individual subjects requesting for a resource. It ensures that no one individual has authorization rights to perform all functions and at the same time does not allow access to all the objects to one individual. This division makes sure that one person is not responsible for a larger process. For example, granting web server administrator rights to only configure a web server without granting administrative rights to other servers.




# Encryption



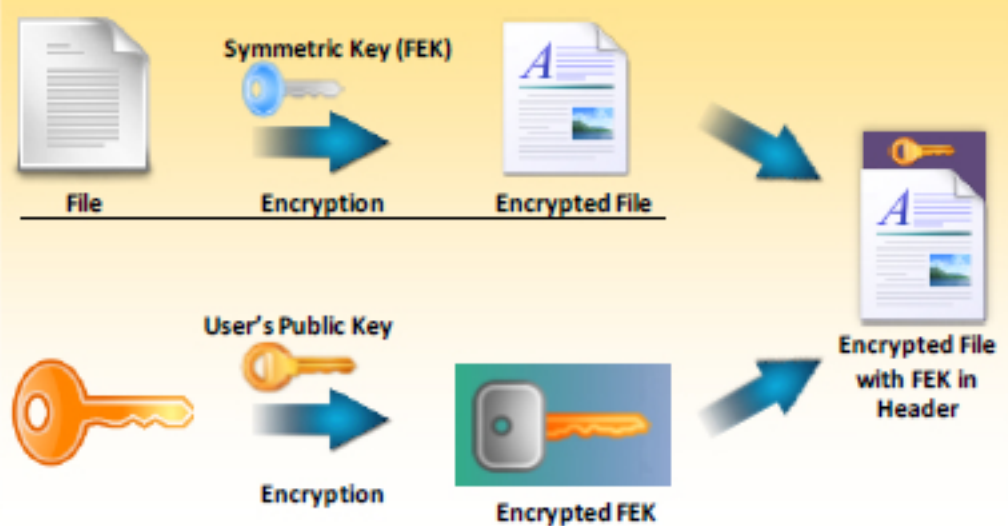
- Encryption is a way of **protecting information** by transforming it in such a way that the resulting transformed form is unreadable to an unauthorized party
- To encrypt data, an encryption algorithm uses a **key** to perform a transformation on the data

## Types of Encryption

- Symmetric Encryption
- Asymmetric Encryption



## ENCRYPTION



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.


Encryption is the practice of concealing information by converting plain text (readable format) into cipher text (unreadable format) using a key or encryption scheme. Encryption guarantees confidentiality and integrity of organizational data, at rest or in transit.

The encryption algorithm encrypts the plain text with the help of an encryption key. The encryption process creates a cipher text that needs decrypting with the help of a key. The process of decryption involves the same steps except for the usage of keys in the reverse order.

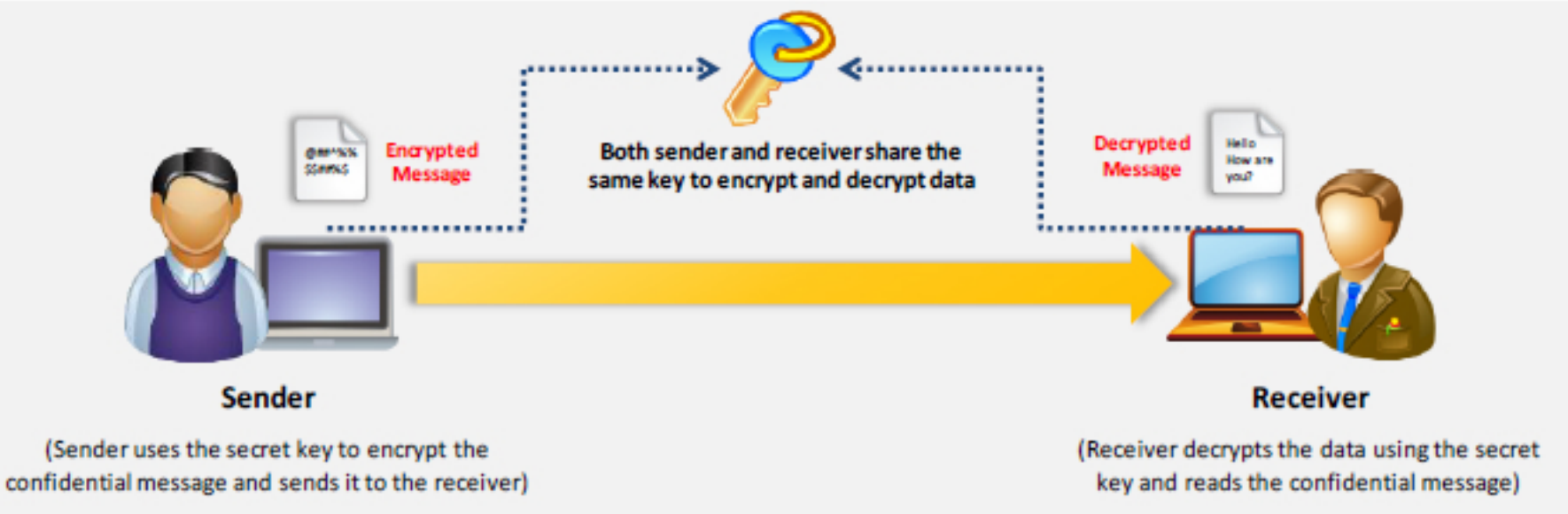
Common encryption algorithms used to encrypt data include RSA, MD5, SHA, DES, AES, etc.

The encryption process finds its application while transmitting data through a network, mobile phones, and wireless transmission and Bluetooth devices.

# Symmetric Encryption



- Symmetric encryption is the oldest cryptographic technique used to **encrypt digital data** in order to **ensure data confidentiality**
- It is called symmetric encryption as a **single key** is used for encrypting and decrypting the data
- It is used to encrypt **large amounts of data**



The diagram illustrates the symmetric encryption process. On the left, a **Sender** (person with a laptop) is shown. A document icon labeled "SECRET MESSAGE" is being processed into an **Encrypted Message** (document icon with a lock). A large yellow arrow points from the sender to the **Receiver** (person with a laptop) on the right. Above the arrow, a key icon is shown with a dashed line connecting it to both the sender and receiver, with the text "Both sender and receiver share the same key to encrypt and decrypt data". The receiver is shown with a document icon labeled "Decrypted Message" (document icon with a lock) and the text "Hello How are you?". Below the sender, it says "(Sender uses the secret key to encrypt the confidential message and sends it to the receiver)". Below the receiver, it says "(Receiver decrypts the data using the secret key and reads the confidential message)".

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Symmetric encryption requires that both the sender and the receiver of the message possess the same encryption key. The sender uses a key to encrypt the plaintext and sends the resulting cipher text to the recipient, who uses the same key to decrypt the cipher text into plain text. Symmetric encryption is also known as secret key cryptography as it uses only one secret key to encrypt and decrypt the data. This kind of cryptography works well when you are communicating with only a few people.

Because the sender and receiver must share the key prior to sending any messages, this technique is of limited use for the Internet, where individuals who have not had prior contact frequently require a secure means of communication. The solution to this problem is public-key cryptography.

The symmetric key encryption can use stream ciphers or block ciphers. Stream ciphers encrypt the bits of a message, one at a time whereas block ciphers encrypt blocks of bits.

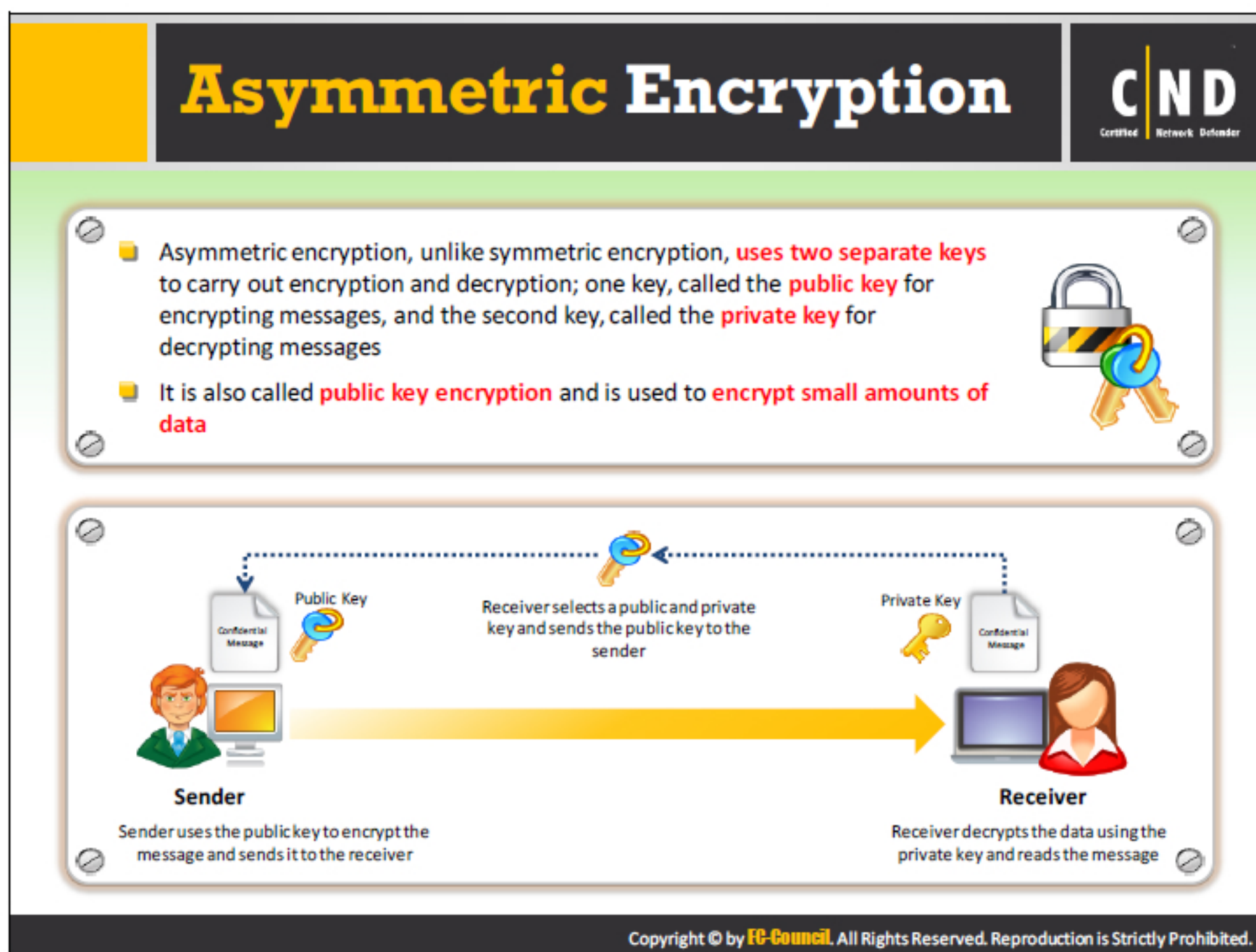
■ **Advantages:**

- Easy to encrypt and decrypt the message.
- Faster than asymmetric encryption.

■ **Disadvantages:**

- The communicating parties need to share the key used for transmission of data.
- Unauthorized access to the symmetric key compromises data at both ends.





The introduction of asymmetric encryption (also known as public-key cryptography) was to solve key-management problems. Asymmetric encryption involves a public key and a private key. The public key is publicly available, but the sender keeps the private key a secret.

Asymmetric encryption uses the following sequence to send a message:

1. An individual finds the public key of the person they want to contact in a directory.
2. This public key is used to encrypt a message that is then sent to the intended recipient.
3. The receiver uses the private key to decrypt the message and read it.

No one but the holder of the private key can decrypt a message composed with the corresponding public key. This increases the security of the information because all communications involve only public keys; the message sender never transmits or shares the private keys. The sender must link the public keys with the usernames in a secured method to ensure that unauthorized individuals claiming to be the intended recipient do not intercept information. To meet the need for authentication, one can use digital signatures.

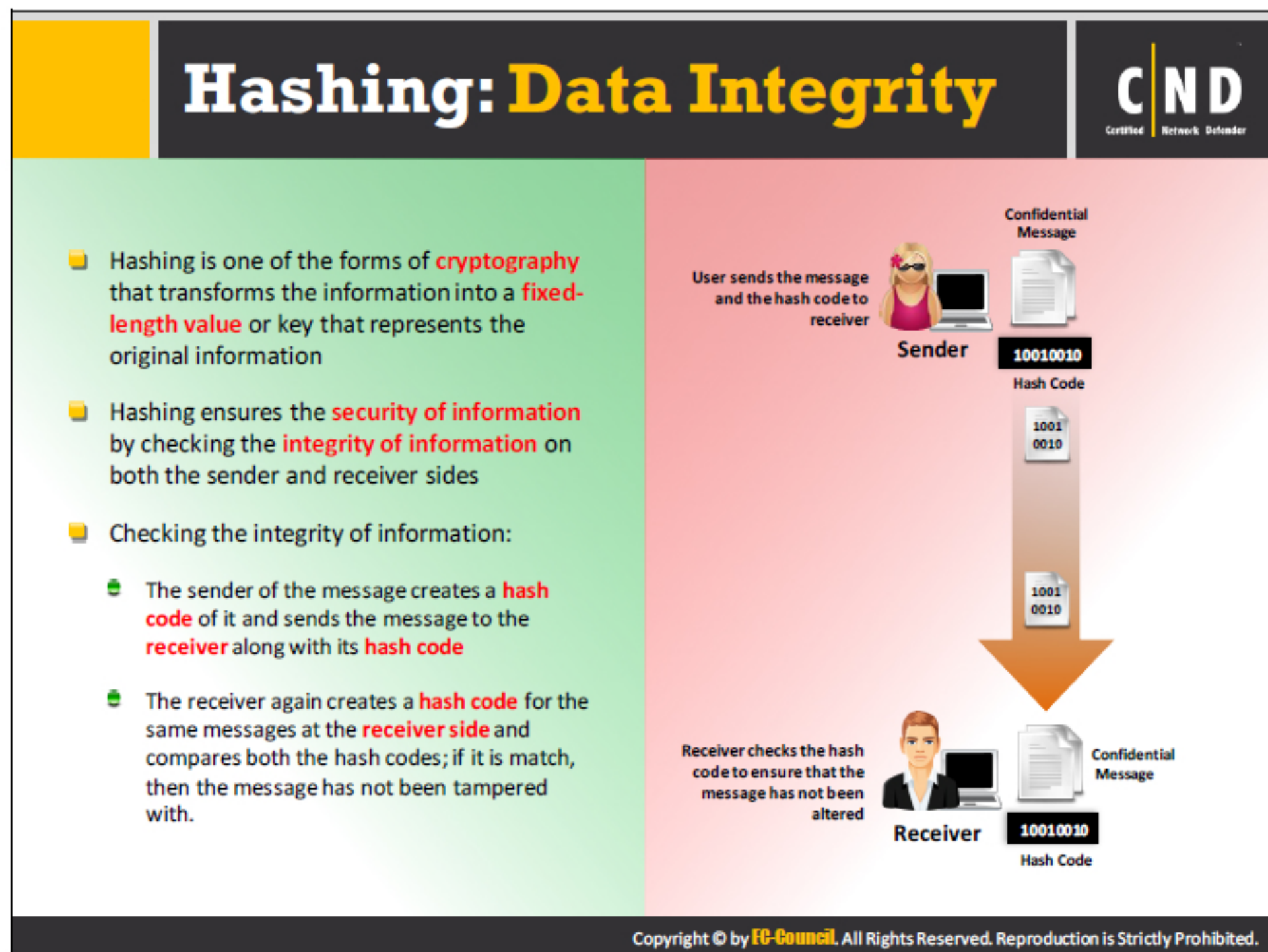
▪ **Advantages:**

- More secure than symmetric encryption.
- No need to distribute the keys.

▪ **Disadvantages:**

- It takes a longer time than symmetric encryption as it involves various combinations of the secret keys and the public keys.
- Various complex algorithms involved in the process of asymmetric encryption also increase the time taken to implement it.





Hashing is a method to generate a fixed length string of random characters for a message using an algorithm. It involves the conversion of the original message into a short-fixed length value or a key that carries the original information.

▪ **Hashing finds its application in:**

- **Secure storage of Passwords:** Passwords are hashed before storing in the database. Every time the user enters the password to login, it is first hashed and the generated hash is matched with the hash stored in the database. If both the hashes match, the user is granted access. Hashing secures passwords from attackers who gain access to the database. The stored hash is useless until the attacker is able to generate the password using a reverse algorithm.
- **Monitoring File Integrity:** Hashing helps identify if a downloaded file is tampered with. A hash of the downloaded file is generated and matched with the one provided by the website. If both hashes match, it is assumed that the file is in its original form.
- **Monitoring Message Integrity:** Hashing ensures that the transmitted messages are not tampered with. An encrypted hash is sent along with the message to the receiver who decrypts the message and hash, and generates a hash from the decrypted hash. If the sent hash and the generated hash are same the message is assumed to have been transmitted safely.

▪ **COMMON HASHING FUNCTIONS:**

- **MD5 (Message Digest 5):** Generates hashes of 128 bits in length, expressed as 32 hexadecimal characters.
- **SHA (Secure Hashing Algorithm):** Considered a more secure hashing algorithm. SHA-1 (generates hashes of 160 bits in length, expressed as 40 hexadecimal characters).
- **SHA-256** (generates hashes of 256 bits in length, expressed as 64 hexadecimal characters).

▪ **LIMITATIONS OF HASHING:**

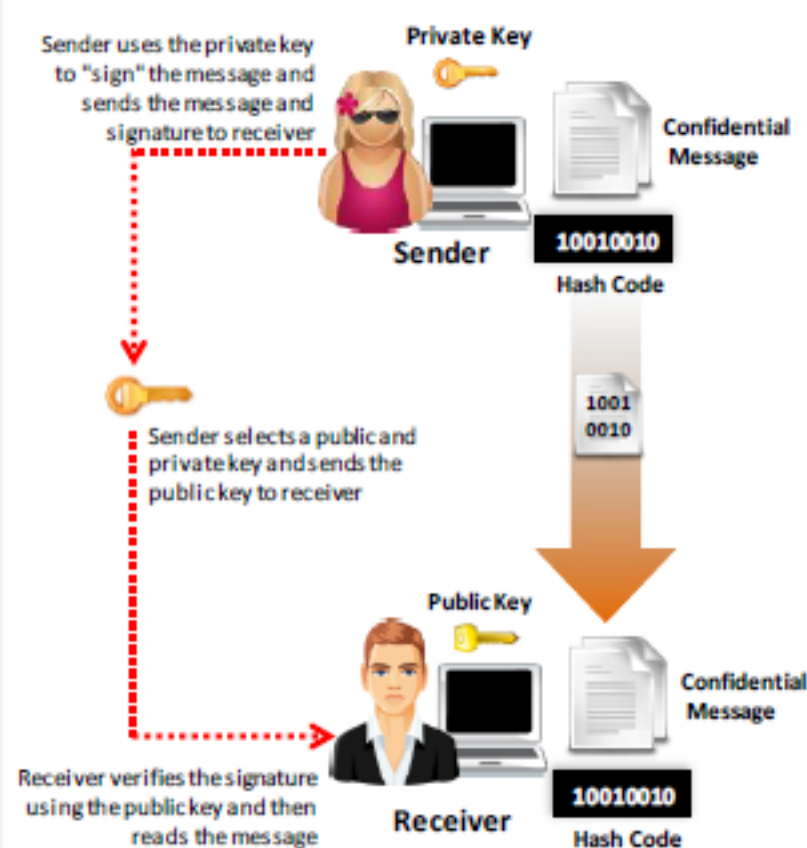
- As Hash is a fixed length string it may result in collision (generating same hash for different data). Hash of smaller length is more prone to collision.



# Digital Signatures



- Digital signatures use the **asymmetric key algorithms** to provide **data integrity**
- A specific signature function is added to the asymmetric algorithm at the sender's side to **digitally sign the message** and a specific **verification function** is added to verify the signature to ensure message integrity at the recipient side
- The asymmetric algorithms that support these two functions are called **digital signature algorithms**
- Digitally signing messages **slows performance**; the hash value of the message is used instead of the message itself for better performance
- A **digital signature** is created using the hash code of the message, the **private key** of the sender, and the signature function
- It is then verified using the hash code of message, the **public key** of sender, and the verification function

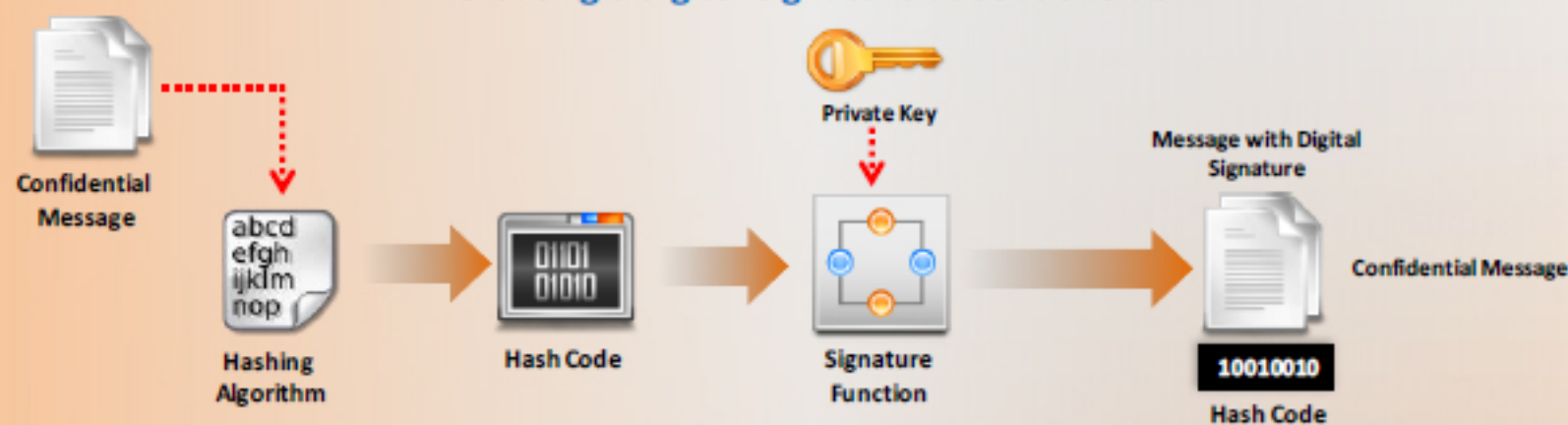


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Digital Signatures (Cont'd)



### Creating a digital signature at sender side



### Verifying a digital signature at recipient side



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

A digital signature is a cryptographic means of authentication. Public-key cryptography uses asymmetric encryption and helps the user to create a digital signature.

A hash function is an algorithm that helps users to create and verify digital signatures. This algorithm creates a digital representation, also known as the message fingerprint. This fingerprint has a hash value that is much smaller than the message, but one that is unique. If the attacker changes the message, the hash function will automatically produce a different hash value.

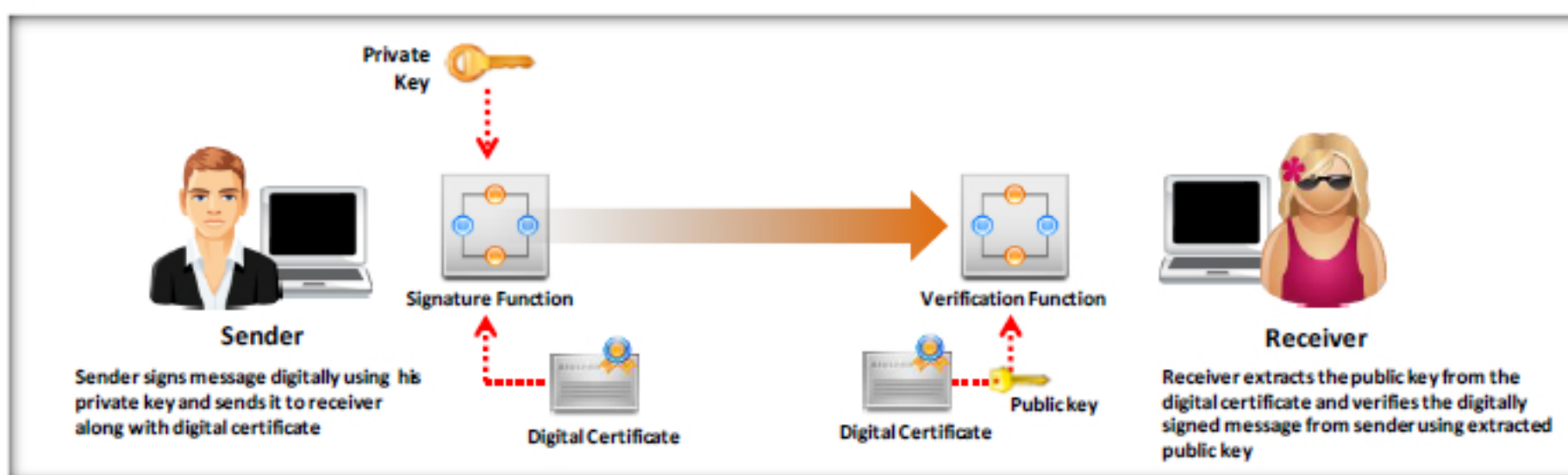
To verify the digital signature, one needs the hash value of the original message and the hash function used to create the digital signature. With the help of the public key and the new result, the verifier checks to see if the digital signature was created with the related private key, and whether the new hash value is the same as the original.



# Digital Certificates



- The public key in a digital signature can be transmitted securely by sending it over a **secured channel** like SSL, but if the sender wants to send his public key to **more users**, a number of these secured channels need to be created for each user communication; this process will become quite tedious and unmanageable
- The digital certificates are used to deal with security concerns about **transmitting public keys securely** to the receiver in the digital signature
- The **trusted intermediary solution** is used to secure public keys, where the public key is bound with the name of its owner
- Owners of the public key need to get their public keys certified from the intermediary; the intermediary then issues certificates called **digital certificates** to the owners which they can use to send the public key to a number of users



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Digital Certificates (Cont'd)



## Digital Certificate Attributes

**Serial number:** Represents the unique certificate identity

**Subject:** Represents the owner of the certificate which may be a person or an organization

**Signature algorithm:** States name of algorithm used for creating the signature

**Key-usage:** Specifies the purpose of the public key, whether it should be used for encryption, signature verification, or both

**Public key:** Used for encrypting the message or verifying the signature of the owner

**Issuer:** Provides the identity of the intermediary that issued the certificate

**Valid from:** Denotes the date from which the certificate is valid

**Valid to:** Denotes the date till which the certificate is valid

**Thumbprint algorithm:** Specifies the hashing algorithm used for digital signatures

**Thumbprint:** Specifies the hash value for the certificate, which is used for verifying the certificate's integrity

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Digital certificates allow the secure interchange of information between a sender and a receiver. This enables the use of a public key by the sender to the receiver. The sender applies for a digital certificate from the Certificate Authority (CA). The CA along with the encrypted message and the public key provides other identity validating information. The receiver accepts the encrypted message and uses the CA's public key to decode the digital certificate. This allows the receiver to identify the digital signature and then obtain the sender's public key and other identification details.

The digital certificate can hold information like the name of the sender who applied for the certificate, expiration date, and copy of the sender's public key digital signature of the CA. The receivers receiving the digital certificate can check the validity of the certificate using the signature attached from the approved authorities using the private key of the authority. Each operating system and web browser carry authorized certificates from the CA which enables easy validation. The main aim in implementing a digital certificate is to ensure nonrepudiation.

Most of the SSL/TLS protocols use certificates in order to prevent attackers from changing or modifying the data. The certificates find application in e-mail servers and code signing.



## Public Key Infrastructure (PKI)



- Public Key Infrastructure (PKI) is a set of hardware, software, people, policies, and procedures required to create, manage, distribute, use, store, and revoke **digital certificates**

### Components of PKI

A certificate authority (**CA**) that issues and verifies digital certificates



A registration authority (**RA**) that acts as the verifier for the certificate authority



A certificate management system for generation, distribution, storage, and **verification** of certificates

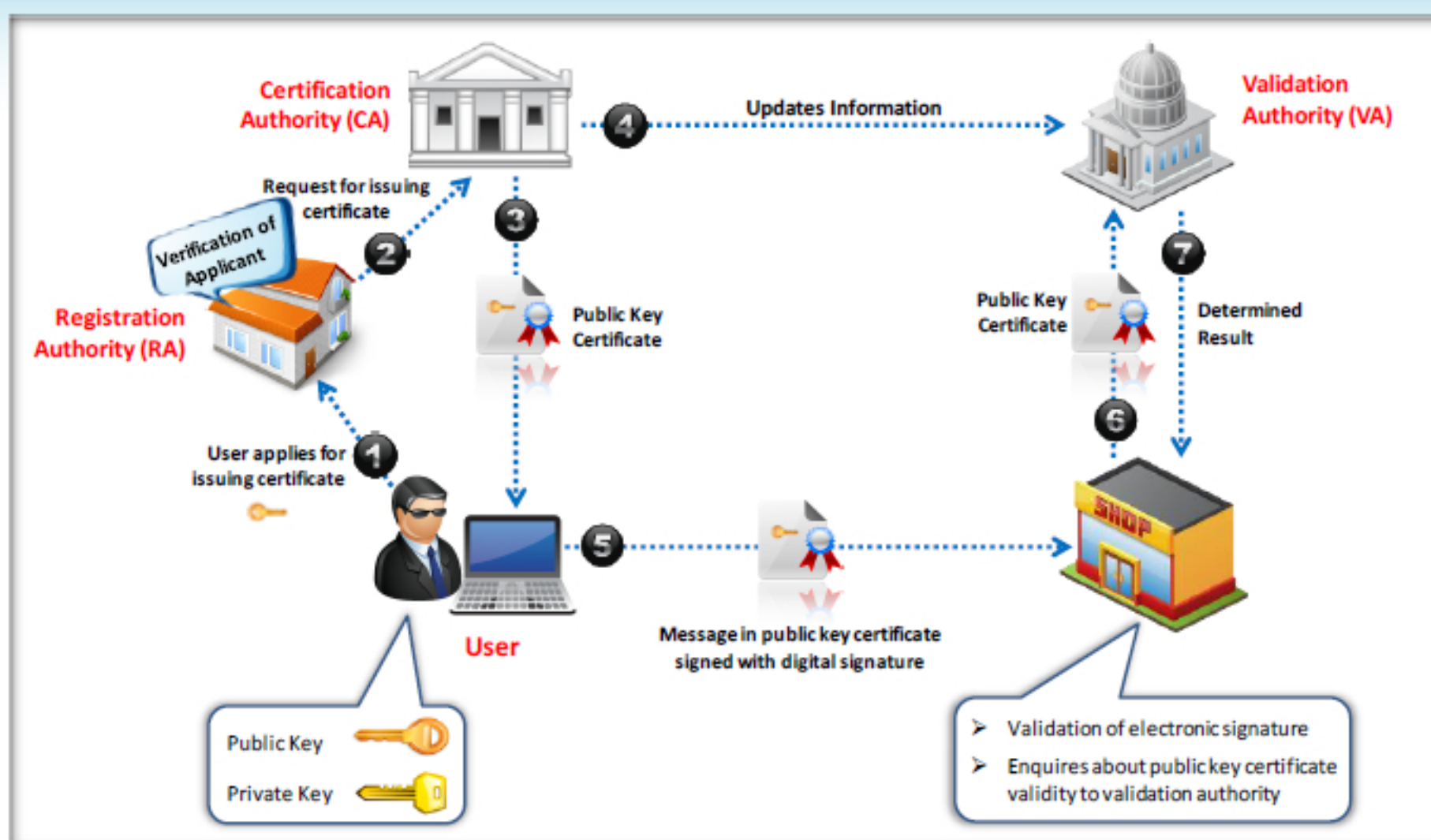


One or more directories where the **certificates** (with their public keys) are stored



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Public Key Infrastructure (PKI) (Cont'd)



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Public Key Infrastructure (PKI) is a security architecture developed to increase the confidentiality of information exchanged over the Internet. It includes hardware, software, people, policies, and procedures required to create, manage, distribute, use, store, and revoke digital certificates. In cryptography, the PKI helps to bind public keys with corresponding user identities by means of a Certificate Authority (CA).

PKI is a comprehensive system that allows the use of public-key encryption and digital signature services across a wide variety of applications. PKI authentication depends on digital certificates (also known as public-key certificates) that CAs sign and provide. The digital certificate is a digitally signed statement with a public key and the subject (user, company, or system) name on it.

Public-key infrastructure is widely recognized as a best practice for ensuring digital verification for electronic transactions. These are the most effective method for providing verification while enabling electronic transactions. The digital signatures supported by PKI include the following:

- With whom you are dealing (identification)
- Who is authorized to access what information (entitlements)
- A verifiable record of the transaction (verification)

## Uses of PKI

PKI does not serve as a business function only; it provides the foundation for other security services. The primary use of PKI is to allow the distribution and use of public keys and certificates with security. The security mechanisms that are based on PKI include email, chip card application, value exchange with e-commerce, home banking, and electronic postal systems. PKI enables basic security services for varied systems that are as follows:


- Uses SSL, IPsec, and HTTPS protocols for communication security.
- Uses S/MIME and PGP protocols for email security.
- Uses SET protocol for value exchange.


The following are the key benefits of PKI:

- Reduces the transactional processing expenses.
- Reduces risk.
- Improve efficiency and performance of systems and networks.
- Reduces the difficulty of security systems with binary symmetrical methods.




# Network Security Policy






- Network Security policy defines the rules for access of **network resources** of an organization



- It helps in **restricting unauthorized access** to network resources from outside malicious users as well as from users within the organization




- It is **updated** continuously depending upon technology and employee requirements

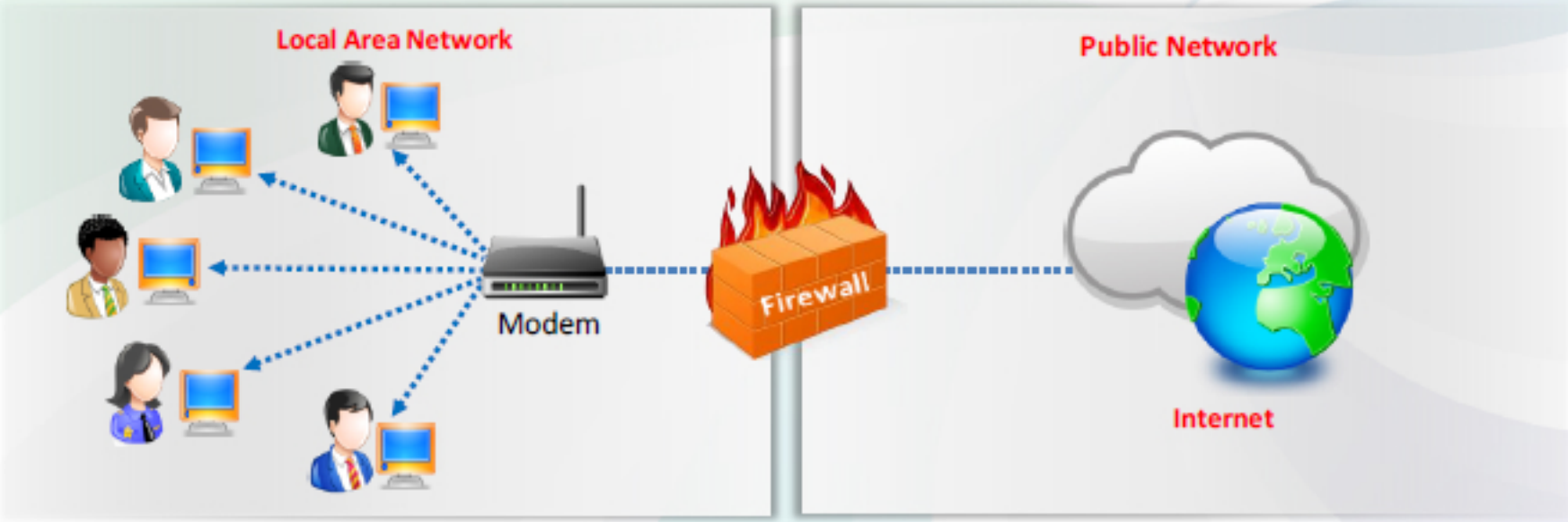
Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Network security policy is a document describing the various policies used to build the network security architecture of the organization. The security policies generally examine the data access, web browsing methods, and encryption processes. It also helps in restricting unauthorized users and malicious users from the organization. A security policy should include the type of services that are available and the probability of damage to these services. The security policies decide the access permissions of users and security of the network. Security policies enable permissions to only minimal level of resources that is enough in completing the task by the user. Organizations need to monitor the policies and confirm they meet their security needs.

## Network Security Devices: Firewalls



- Firewall is a software or hardware, or combination of both, **which is generally used to separate a protected network from an unprotected public network**
- It monitors and filters the incoming and outgoing **traffic** of the network and prevents unauthorized access to private networks
- It works at the network layer of the OSI model, or the IP layer of TCP/IP.



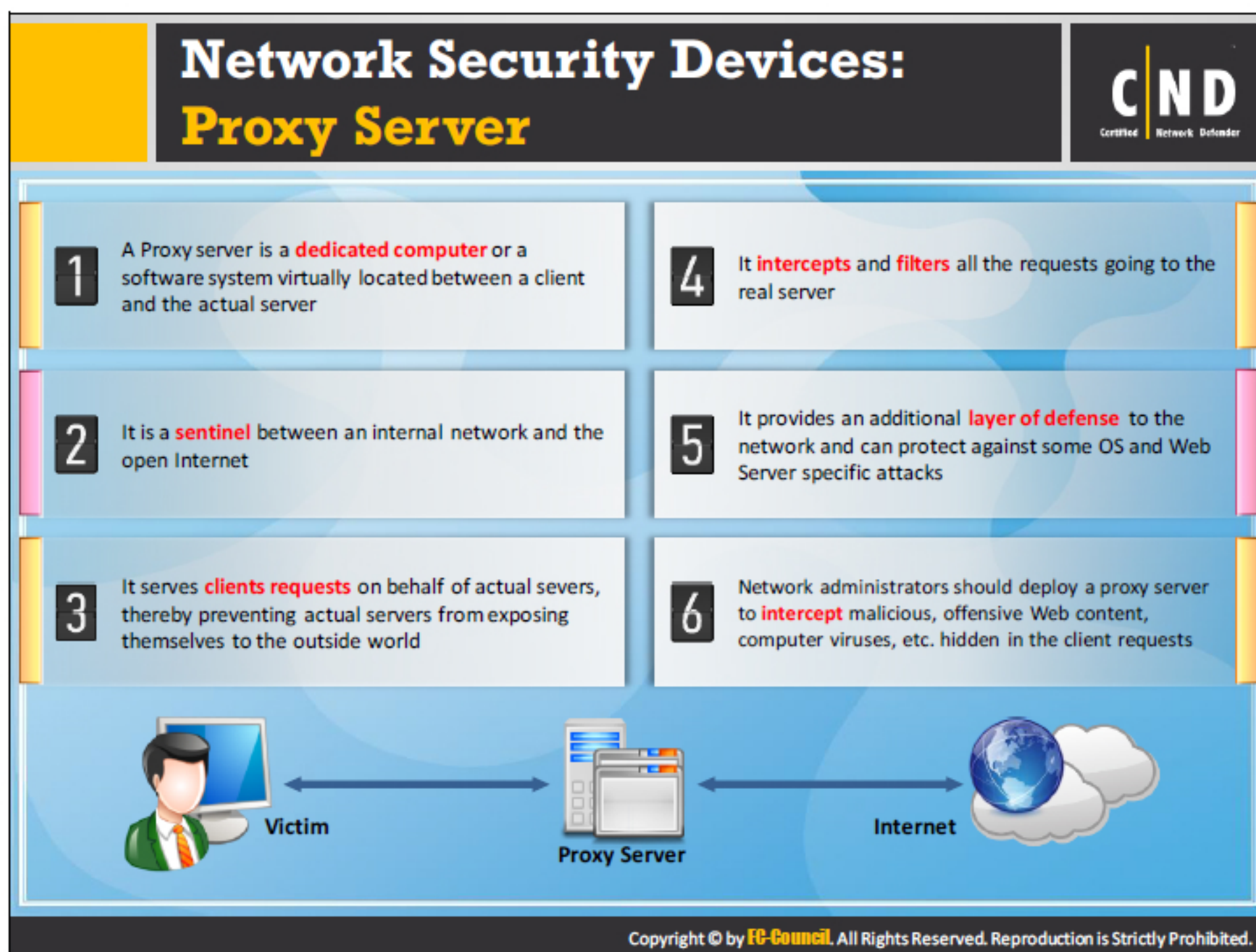
Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

A firewall is a secure, reliable, and trusted device placed between private and public networks. It helps in protecting a private network from the users of a different network. It has a set of rules to trace the incoming and outgoing network traffic and is also responsible for allowing, denying the traffic to pass through.

### Typical use of firewalls:

- Protect the private network applications, services on the internal network from the unauthorized traffic, and the public network.
- Restrict the access of the hosts on the private network and the services of the public network.
- Support network address translation, which helps in using the private IP addresses and to share a single Internet connection.





A proxy server is an application that can serve as an intermediary when connecting with other computers.

### A proxy server is used:

- As a firewall, and to protect the local network from outside attacks.
- As an IP address multiplexer, allowing a number of computers to connect to the Internet when you have only one IP address (NAT/PAT).
- To anonymously surf the web (to some extent).
- To filter out unwanted content, such as ads or “unsuitable” material (using specialized proxy servers).
- To provide some protection against hacking attacks.
- To save bandwidth.

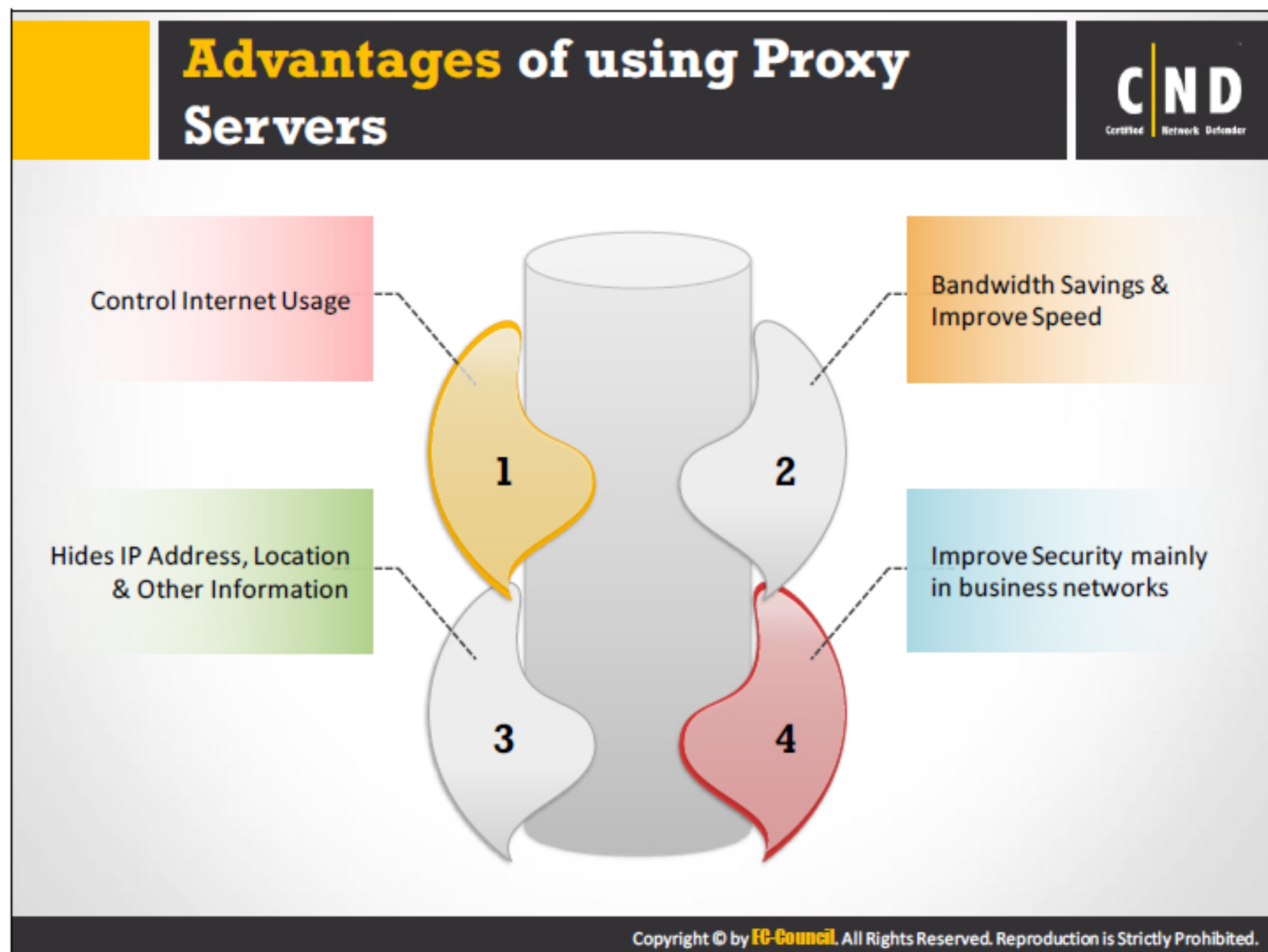
### How proxy servers work?

Initially, when you use a proxy to request a particular web page on an actual server, the proxy server receives it. The proxy server then sends your request to the actual server on behalf of your request—it mediates between you and the actual server to send and respond to the request.

A proxy server improves security, administrative control, and caching services. It is also used for evaluating network traffic and maintaining user confidentiality.

Proxy servers in an organization help in maintaining security and administrative controls. However, attackers use proxy servers to hide their presence on the internet.






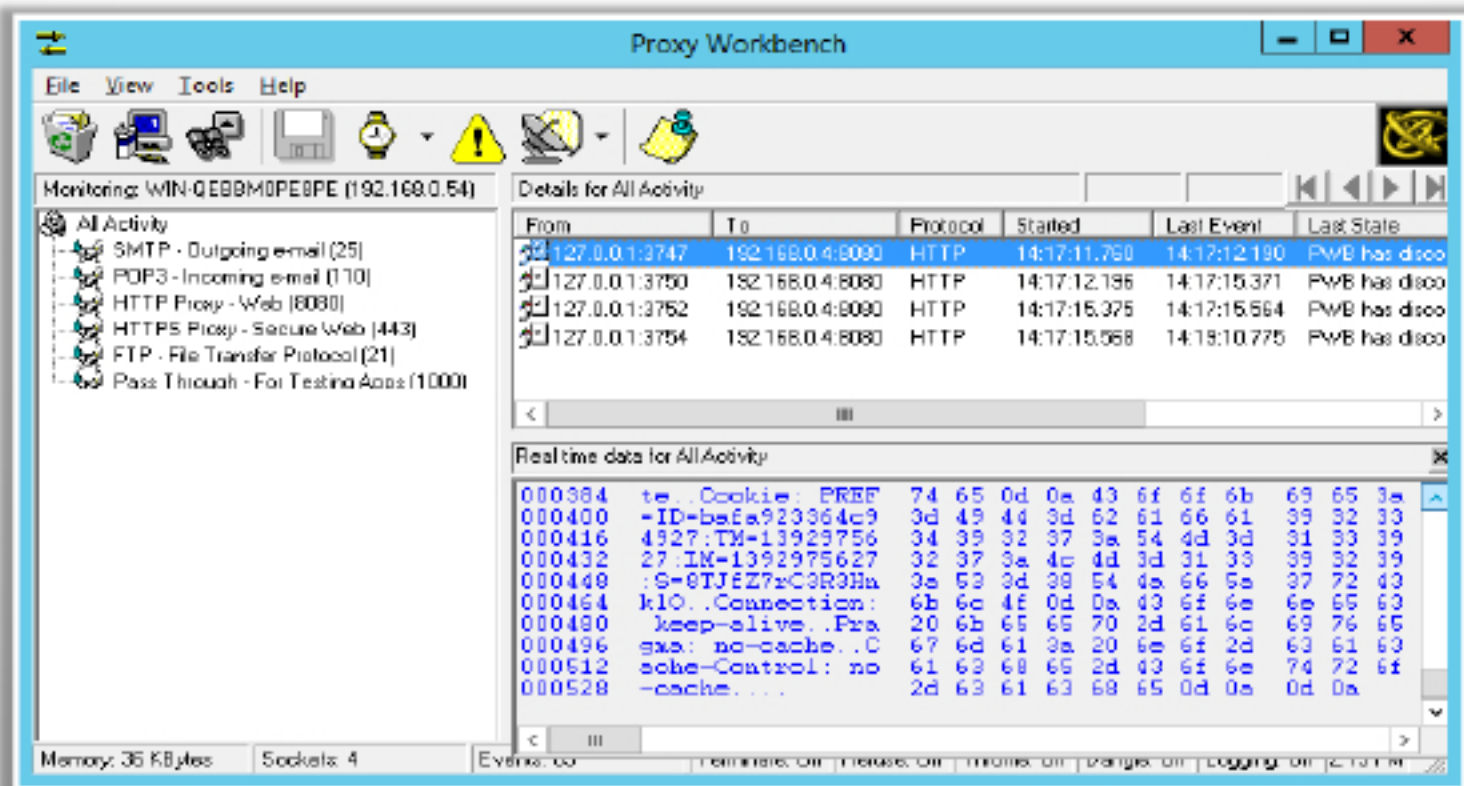
The following are some more benefits of using a proxy server in the network

- Acts as security protector between user devices and server.
- Enhances the security and privacy of client devices.
- Improves browsing speed.
- Provides advanced logging capabilities for user activities.
- Used to control access to specific types of restricted services.
- Helps the organization to hide its internal IP address.
- Reduces the chances of the modifying cookies in the browser configuration and protects from any kind of malware.
- Filters requests from external sites.
- Improves delivery of the requested web pages to the users.
- Enables authentication for the proxy servers before it handles the user requests and services.

# Proxy Tool: Proxy Workbench



- Proxy Workbench is a proxy server that **displays data passing through it in real time**
- It allows you to drill into specific TCP/IP connections, view their history, save the data to a file, and view the socket connection diagram



<http://www.proxyworkbench.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Proxy Workbench is a proxy server utility that displays the passage of data in real time. It allows getting details like saving data, viewing history and viewing socket diagram of a socket connection for a particular TCP/IP connection. Socket connection diagram displays the graphical history of all the previous events that took place in that socket connection.

- **Advantages:**
  - Displays an animated view of the socket connection.
  - Handles POP3 and HTTPS (Secure sockets).
  - Displays real time logging of data.
- **Proxy workbench is mainly used by:**
  - People interested in Web browsing, sending and receiving e-mails etc.
  - Programmers
  - IT training industry
  - Internet security practitioners

Source: <http://proxyworkbench.com>





## Socks Chain

Source: <http://ufasoft.com>

Socks Chain is a program that allows working with any Internet service through a chain of SOCKS or HTTP proxies to hide the real IP-address. Socks Chain functions as a usual SOCKS-server that transmits queries through a chain of proxies. It allows using with client programs that do not support the SOCKS protocol, but work with one TCP-connection, such as TELNET, HTTP, IRC, etc.

## Burp Proxy

Source: <http://www.portswigger.net>

Burp Suite Burp Proxy is an intercepting proxy server that operates as a man-in-the-middle between your browser and the target application, allowing you to intercept and modify all HTTP/S traffic passing in both directions.

## Proxifier

Source: <https://www.proxifier.com>

Proxifier allows network applications that do not support working through proxy servers to operate through a SOCKS or HTTPS proxy and chains.

## WinGate

Source: <http://www.wingate.com>

WinGate Proxy Server is an integrated Internet gateway and communications server which meets the control, security, and communications needs of today's businesses. It provides the flexibility to match the company's budget, irrespective of the size of the organization.

## Charles

Source: <http://www.charlesproxy.com>

Charles is an HTTP proxy / HTTP monitor / Reverse Proxy that enables developers to view all HTTP and SSL / HTTPS traffic between their machine and the Internet. This includes requests, responses and the HTTP headers (which contain the cookies and caching information).

## Fiddler

Source: <http://www.telerik.com>

Fiddler is a proxy server that is compatible with any browser, system or platform.

Key features of Fiddler include:

- Web Debugging
- Performance Testing
- Security Testing
- Web session manipulation
- HTTP/HTTPS traffic recording
- Customizing Fiddler

## AnalogX Proxy

Source: <http://www.analogx.com>

AnalogX Proxy is a server that allows any other machine on the local network to route its requests through a central machine. The protocols supported by proxy are HTTP (web), HTTPS (secure web), POP3 (receive mail), SMTP (send mail), NNTP (newsgroups), FTP (file transfer), and Socks4/4a and partial Socks5.

## Protoport Proxy chain

Source: <http://www.protoport.com>

Protoport Proxy Chain software enables users to build a chain of proxy servers from different countries. The proxy server tool enables them to surf the internet anonymously.

## ProxyCap

Source: <http://www.proxycap.com>

ProxyCap redirects computer's network connections through proxy servers. ProxyCap determines the applications that can connect to the Internet through a proxy. ProxyCap supports the SSH protocol, allowing the user to specify an SSH server as the proxy server.





## CCProxy

Source: <http://www.youngzsoft.net>


CCProxy is a windows proxy server that assists users to build their own proxy server and to share the Internet connection within the LAN. CCProxy can support broadband, DSL, dial-up, optical fiber, satellite, ISDN, and DDN connections. CC Proxy Server can act as an HTTP, mail, FTP, SOCKS, news, Telnet, and HTTPS proxy server. The functions provided by the CCProxy are: Internet access control, bandwidth control, Internet web filtering, content filtering and time control, web caching, online access monitoring, access logging and bandwidth usage statistics functions.

## Network Security Devices: Honeypot






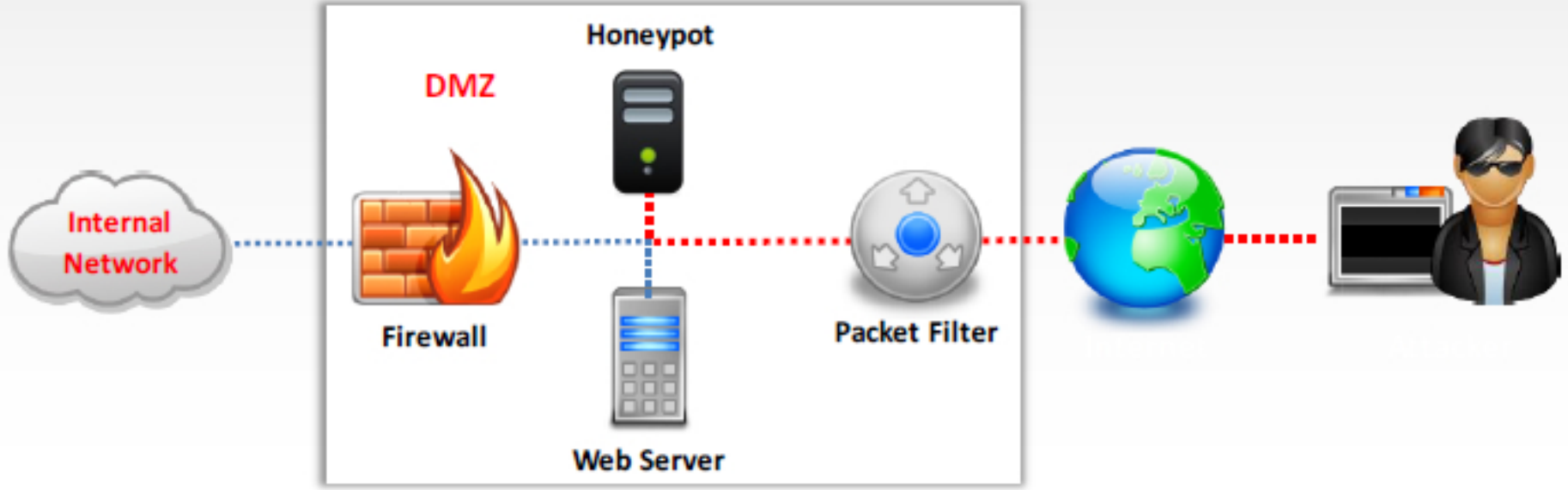
A honeypot is an information system resource that is explicitly **set up to attract and trap people** who attempt to penetrate an organization's network



It has no authorized activity, does not have any production value, and any traffic to it is **likely a probe or an attack**



A honeypot can **log port access attempts, or monitor an attacker's keystrokes**. These could be early warnings of a more concerted attack



The diagram illustrates a network architecture. On the left, a cloud labeled 'Internal Network' is connected to a 'Firewall' (represented by a brick wall with a flame). The Firewall is part of a 'DMZ' (Demilitarized Zone). Inside the DMZ, there is a 'Honeypot' (represented by a server icon) and a 'Web Server' (represented by a server rack icon). A 'Packet Filter' (represented by a circular icon with arrows) is positioned between the DMZ and the Internet. The Internet is represented by a globe, and an attacker (represented by a person with a laptop and sunglasses) is shown on the right, connected to the Internet. A red dashed line indicates the path of traffic from the Internal Network, through the Firewall, into the DMZ, and then through the Packet Filter to the Internet.

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

A honeypot is a computer system on the Internet intended to attract and trap people who try unauthorized or illicit utilization of the host system. It is a fake proxy run in an attempt to frame attackers by logging traffic through it, and then sending complaints to victim ISPs. Whenever there is any interaction with a honeypot, it is most likely to be a malicious activity. Honeypots are unique; they do not solve a specific problem. Instead, they are a highly flexible tool with many different security applications. Some honeypots help in preventing attacks, others can be used to detect attacks, while others can be used for information gathering and research. It requires a considerable amount of attention to maintain a honeypot.

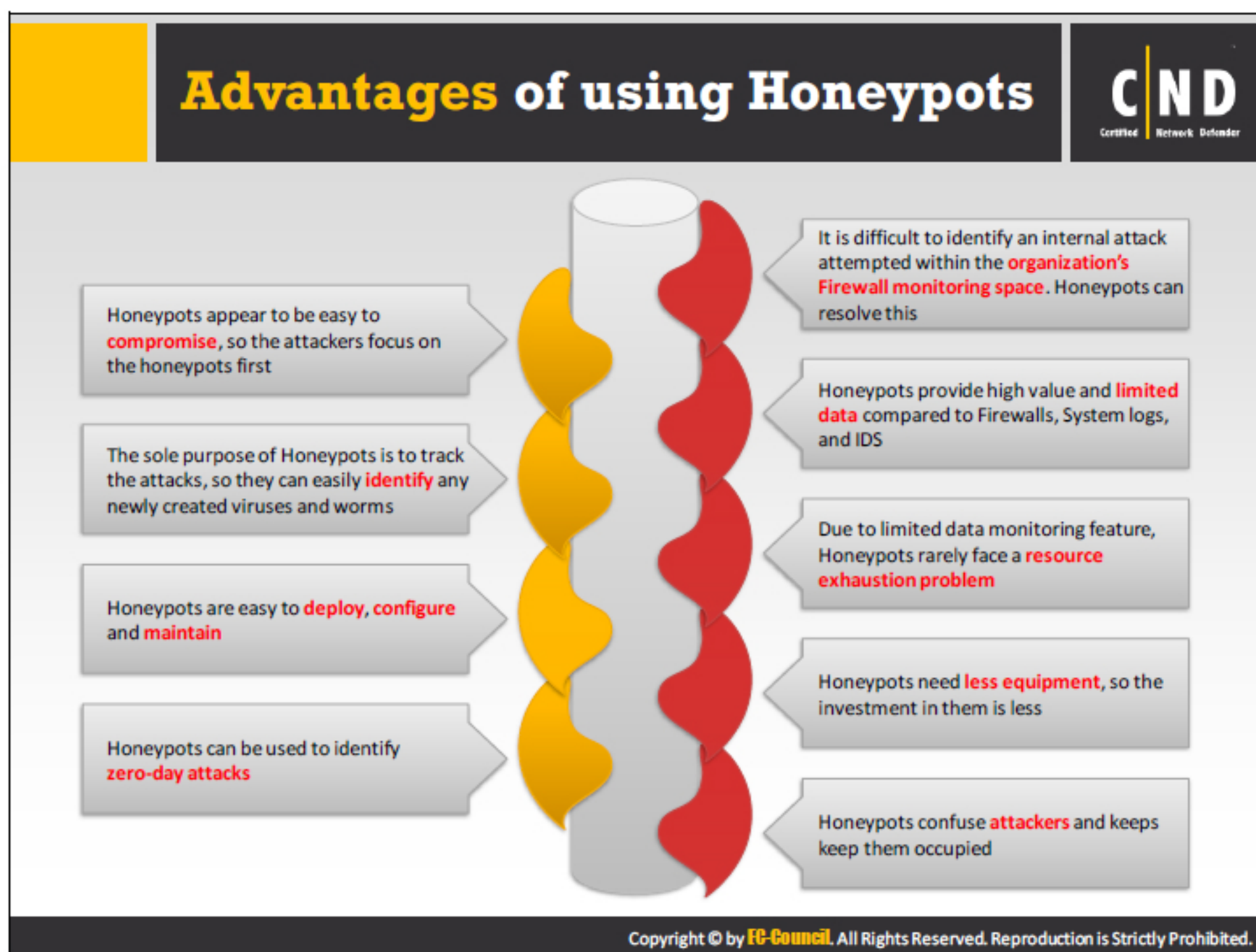
- To **set up** a honey pot:
  - Install a system on the network with no particular purpose other than to log all attempted access.
  - Install an older, unpatched operating system on a network. For example, the default installation of WinNT 4 with IIS 4 can be hacked using several different techniques. A standard intrusion detection system can then be used to log hacks directed against the system and further track what the intruder attempts to do with the system once it is compromised. Install special software designed for this purpose, which will have the advantage of making it appear that the intruder is successful without really allowing them access to the network.
  - Ensure that the attacker cannot easily delete system data intended to be in the honeypot.



- The main intention of implementing a honeypot is to:
  - Track the activities performed by the attackers, thereby allowing the network administrators to build countermeasures for those attacks.
  - Collect forensic information that can be used for the further investigation of the attack.
- There are two types of honeypots classified based on their deployment:
  - **Production Honeypot:** Normally placed inside a production network along with the other production servers, thereby giving a notion to the attackers that it contains real and valuable data. The organization evaluating the traffic through the honeypot can now understand the activities performed by an attacker. Honeypots also allow the organization to identify the attackers and bring them behind bars.
  - **Research Honeypot:** The research honeypots enable an organization to closely evaluate each step taken by the attackers while attacking the network. Enabling the organization to understand each step carefully and thereby developing the measures required for each attack. The use of honeypot also enables the organization to easily track the data stolen by the attackers.
- The further classification of honeypots available based on their design:
  - **Pure Honeypots:** The presence of pure honeypots makes it possible to track the activities of an attacker in a complete manner. It places a small tap in between the honeypot's link to the network.
  - **Low-interaction Honeypots:** As the name suggests, low-interaction honeypots generally fake those services frequently asked by the attacker. They are essentially a single machine with multiple virtual machines.
  - **High-Interaction Honeypots:** The high-interaction honeypots stage a lot of services and activities performed by the real production systems, tricking the attackers into believing that they are accessing a real production system. Multiple honeypots on a single machine is possible by implementing a virtual machine. The high-interaction honeypots are highly secure and examine each activity of the attacker. But, the disadvantage with the honeypot is that they are very costly to maintain and implement.

Honeypots implemented need to look as genuine as any other original production system. It should contain information that can attract the attackers and persuade them to perform activities.



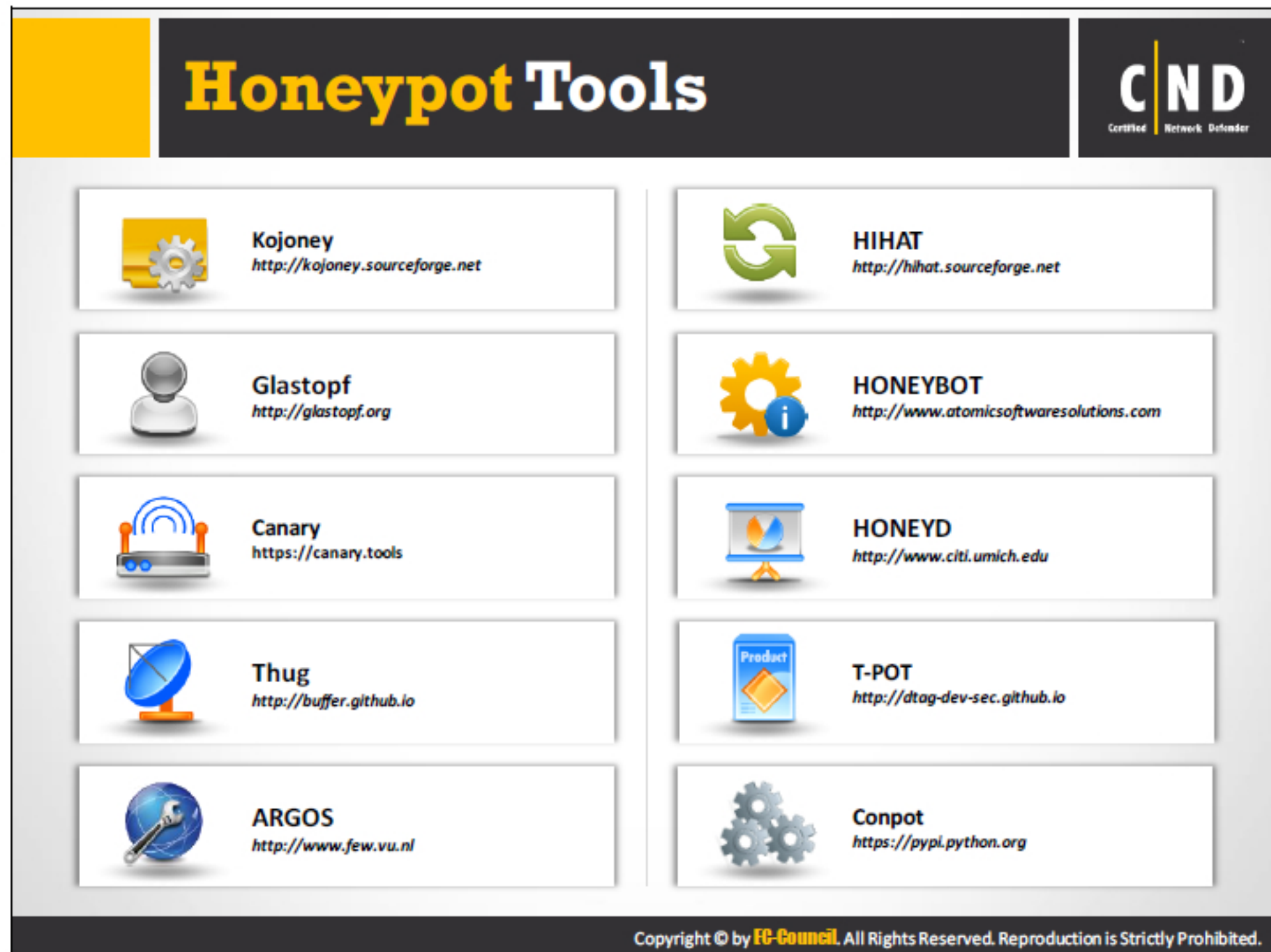


The following are some security benefits of implementing Honeypots in the network:

- **Simplicity:** Honeypots are simple to implement as they do not contain complex algorithms.
- **Detect Inside attacks:** Honeypots help detect insiders (Employees) misusing the system.
- **Reduce False Positive:** Any connection to a honeypot is considered a hostile attack. Any information sent from the honeypot represents an intrusion.
- **Identify False Negatives:** Since any activity with the honeypot is considered abnormal, they help capture new attacks or activity against them easily.
- **Data Collection:** Honeypots collect little high value data. This little information is the exact information presented in an easy to understand format.
- **Resources:** As honeypots capture less activity, they do not come across a resource exhaustion issue.
- **Encryption:** Honeypots capture the activity even if they are encrypted.
- **IPv6:** Honeypots are capable to detect, capture, and log all IP activity.
- **Incident response:** Allows the organization to detect and prevent attacks by taking the necessary steps
- **Warning system:** Provides alerts regarding threats in the network.



- **Ability to mislead:** Easy to mislead attackers.
- **Stores information:** Information collected by honeypots is considered highly beneficial.



## Kojoney

Source: <http://kojoney.sourceforge.net>

Kojoney is a low level interaction honeypot that emulates an SSH server. The prerequisites required for Kojoney are:

- OpenSSL
- Python
- Sh or Bash (Bourne Again SHell)
- Zope-Interfaces (included in the package)
- Twisted (included in the package)
- Twisted Conch (included in the package)

## Glastopf

Source: <http://glastopf.org>

Glastopf is a honeypot, which emulates thousands of vulnerabilities to gather data from attacks targeting web applications. Glastopf follows a very simple principle: Send the correct response to the attacker exploiting the web application.



## Canary

Source: <https://canary.tools>

Canary honeypot mimics a production system when deployed. It helps an organization in the early detection of network breaches.

## Thug

Source: <http://buffer.github.io>

Thug is a low interaction honeyclient. The main aim behind Thug is to mimic the behavior of a web browser in order to detect and emulate malicious contents. A honeyclient is a tool designed to mimic the behavior of a user-driven network client application, such as a web browser, and be exploited by an attacker's content.

## Argos

Source: <http://www.few.vu.nl>

Argos's honeypot uses dynamic taint analysis to detect and analyze control flow attacks.

## HIHAT

Source: <http://hihat.sourceforge.net>

The High Interaction Honeypot Analysis Toolkit (HIHAT) transforms arbitrary PHP applications into web-based high-interaction honeypots. It provides a graphical user interface which performs the process of monitoring the Honeypot and analyzing the acquired data.

## HoneyBot

Source: <http://www.atomicsoftwaresolutions.com>

HoneyBot is a medium interaction honeypot for windows. A honeypot creates a safe environment to capture and interact with unsolicited traffic on a network. HoneyBOT is an ideal tool for network security research or as part of an early warning IDS.

## HoneyD

Source: <http://www.citi.umich.edu>

HoneyD creates virtual hosts on a network. The hosts can be configured to run arbitrary services, and their personality can be adapted so that they appear to be running certain operating systems. HoneyD enables a single host to claim multiple addresses.

## T-POT

Source: <http://dtaq-dev-sec.github.io>

The main aim of implementing a T-POT is to create a system, whose entire TCP network range as well as some important UDP services act as a honeypot, and to forward all incoming attack traffic to the best-suited honeypot daemons in order to respond and process it.


## Conpot

Source: <https://pypi.python.org>

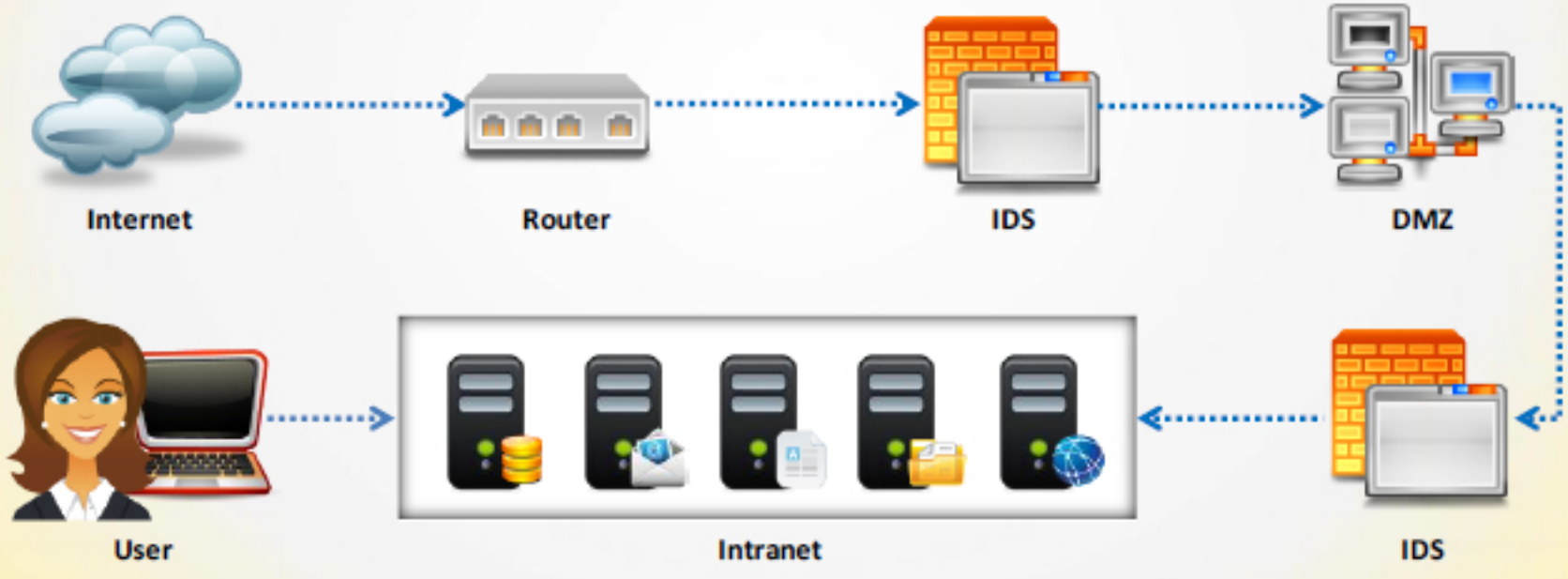
Conpot is an ICS honeypot that collect intelligence about the motives and methods of adversaries targeting industrial control systems.



## Network Security Devices: Intrusion Detection System (IDS)



- An intrusion detection system (IDS) is a network security appliance that **inspects all inbound and outbound network traffic** for suspicious patterns that may indicate a network or system security breach
- If found, the IDS will alert the network administrator about the **suspicious activities**
- IDS checks traffic for **signatures** that match known intrusion patterns, and triggers an alarm when a match is found



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Intrusion Detection System (IDS) performs an evaluation of the network traffic for illegal activities and policy violations. Intrusion detection uses vulnerability assessment for ensuring the security of the network. Features of Intrusion Detection include:

- Evaluating system and network activities.
- Analyzing vulnerabilities in the network.
- Measuring the system and file reliability.
- Skill to identify the possibilities of attacks.
- Monitoring irregular activities in the network and system.
- Evaluating the policy violations.

Organizations can identify the presence of attacks or intrusions from outside the network as well as the intrusions or misuse within the network. Mostly the intrusion detection systems use vulnerability assessment or scanning in order to identify the vulnerabilities in the network and to monitor the security of the network.


Firewalls prevent intrusions within the network, but do not actually alert regarding the intrusion or attack. IDS systems can monitor and identify the intrusions within the network as well as signal an alarm to the network administrator.




## Advantages and disadvantages of IDS:


- The IDS allows continuous monitoring and tracking of all intrusions and attacks in the network.
- The IDS provides an extra layer of security to the network.
- The IDS can also provide a log or data regarding the attack or intrusion that can be later used for investigation of the incident.
- The IDS requires more maintenance when compared to the firewalls.
- It is not always possible for the IDS to detect the intrusions.
- IDS requires properly trained and experienced users to maintain it.
- IDS can raise false alarms to the network administrator.

## Network Security Devices: Intrusion Prevention System (IPS)






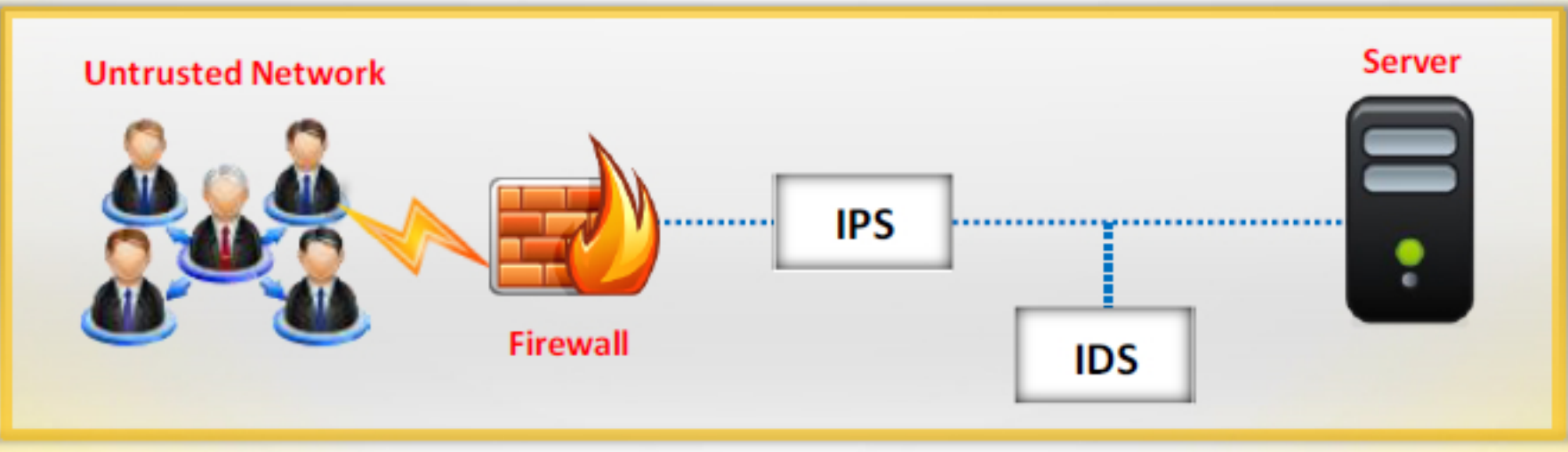
IPS is a **network security appliance** that combines functions of both a firewall and an IDS



It is an extension of an IDS used to monitor network traffic for **malicious activities**



Unlike IDS, an IPS is able to **actively** prevent/block detected intrusions on the network



The diagram illustrates the flow of network traffic. On the left, an 'Untrusted Network' is represented by a group of five people icons. A yellow lightning bolt arrow points from this network to a 'Firewall' icon (a brick wall with a flame). From the Firewall, a dashed blue line leads to an 'IPS' (Intrusion Prevention System) box. Below the IPS box, a dashed blue line leads to an 'IDS' (Intrusion Detection System) box. Finally, a dashed blue line leads from the IDS box to a 'Server' icon (a black server tower) on the right.

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

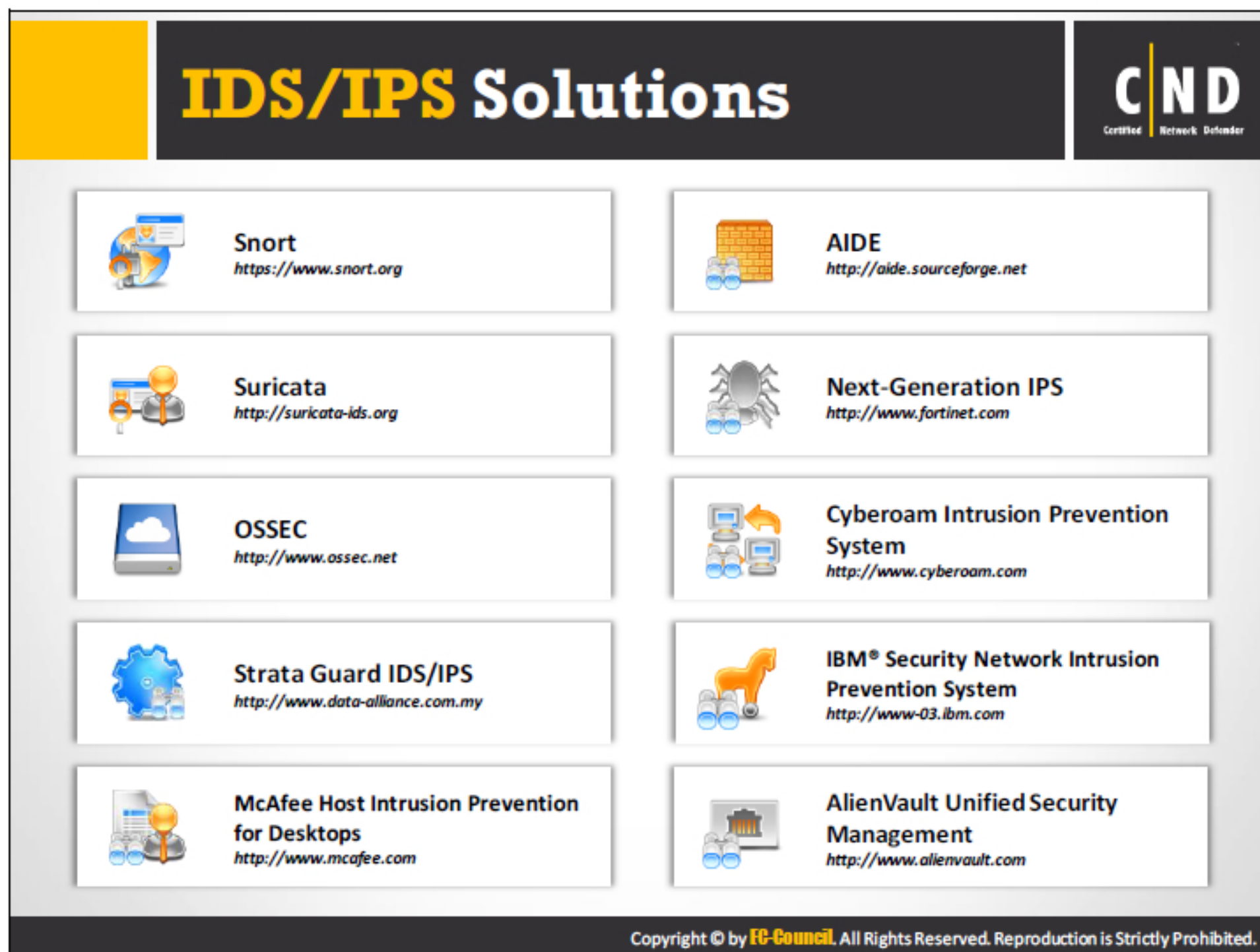
Intrusion Prevention Systems (IPS) work similar to an IDS. Like an IDS, an IPS monitors the network traffic for any intrusion or attack. IPS systems have the capability to carry out quick action against any kind of intrusion. An IPS takes actions based on certain rules and policies configured into it. In other words, the IPS system can identify, log, and prevent the occurrence of any intrusions or attacks in the network.

- The **features** of an IPS include:
  - Identify illegal activities.
  - Recording information about any illegal activity.
  - Restricting the attack across the network.
  - Reporting the attack to network administrator.

IPS may include firewalls or anti-virus software in order to deny access to intruders in the network.

- **Advantages of IPS over IDS:**
  - Unlike an IDS, the IPS systems can block as well as drop illegal packets in the network.
  - An IPS can be used to monitor activities occurring in a single organization.
  - An IPS prevents the occurrence of direct attacks in the network by controlling the amount of network traffic.





The graphic is titled "IDS/IPS Solutions" in large, bold, yellow and white text on a dark background. To the right of the title is the "CND Certified Network Defender" logo. Below the title, there is a grid of ten white boxes, each containing an icon, the name of a security solution, and its website URL. The solutions are arranged in two columns of five. The first column includes Snort, Suricata, OSSEC, Strata Guard IDS/IPS, and McAfee Host Intrusion Prevention for Desktops. The second column includes AIDE, Next-Generation IPS, Cyberoam Intrusion Prevention System, IBM® Security Network Intrusion Prevention System, and AlienVault Unified Security Management. At the bottom of the graphic, a black bar contains the copyright notice: "Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited."

Solution	Website
Snort	<a href="https://www.snort.org">https://www.snort.org</a>
AIDE	<a href="http://aide.sourceforge.net">http://aide.sourceforge.net</a>
Suricata	<a href="http://suricata-ids.org">http://suricata-ids.org</a>
Next-Generation IPS	<a href="http://www.fortinet.com">http://www.fortinet.com</a>
OSSEC	<a href="http://www.ossec.net">http://www.ossec.net</a>
Cyberoam Intrusion Prevention System	<a href="http://www.cyberoam.com">http://www.cyberoam.com</a>
Strata Guard IDS/IPS	<a href="http://www.data-alliance.com.my">http://www.data-alliance.com.my</a>
IBM® Security Network Intrusion Prevention System	<a href="http://www-03.ibm.com">http://www-03.ibm.com</a>
McAfee Host Intrusion Prevention for Desktops	<a href="http://www.mcafee.com">http://www.mcafee.com</a>
AlienVault Unified Security Management	<a href="http://www.alienvault.com">http://www.alienvault.com</a>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Snort

Source: <https://www.snort.org>

Snort is an open source network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis and content searching/matching, and is used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, and OS fingerprinting attempts.

Uses of Snort:

- Straight packet sniffer like tcpdump.
- Packet logger (useful for network traffic debugging, etc.).
- Network intrusion prevention system.

## Suricata

Source: <http://suricata-ids.org>

Suricata is a Network IDS, IPS and Network Security Monitoring engine. The Suricata tool is highly scalable that allows to run one instance which balances the load of processing across every processor on which it is configured. The tool enables identifying thousands of files passing through the network.



## OSSEC

Source: <http://www.ossec.net>

OSSEC actively monitors all aspects of UNIX system activity with file integrity monitoring, log monitoring, root check, and process monitoring. During the course of an attack, OSSEC alerts through alert logs and emails and also exports alerts to any SIEM system via SYSLOG.

## Strata Guard IDS/IPS

Source: <http://www.data-alliance.com.my>

Strata Guard enforces network audit, usage policies and can block peer-to-peer file sharing, instant messaging, chat, prohibited browsing activity, and worm propagation. It can detect anomalous activity such as spoofed attack source addresses, TCP state verification and rogue services running on the network.

## McAfee Host Intrusion Prevention for Desktops

Source: <http://www.mcafee.com>

McAfee Host Intrusion for Desktop safeguards your business against complex security threats that may be unintentionally introduced or allowed by desktops and laptops.

## AIDE

Source: <http://aide.sourceforge.net>

AIDE stands for Advanced Intrusion Detection Environment. It is a file and directory integrity checker. It creates a database from the regular expression rules that it finds from the config file(s). Once this database is initialized, it can be used to verify the integrity of the files. It has several message digest algorithms that are used to check the integrity of the file. All of the usual file attributes can also be checked for inconsistencies. It can read databases from older or newer versions.

## Next – Generation IPS

Source: <http://www.fortinet.com>

It is used for advanced threat protection by integrating:

- Real-time contextual awareness.
- Intelligent security automation.
- Superior performance with industry-leading network intrusion prevention.

## Cyberoam Intrusion Prevention System

Source: <http://www.cyberoam.com>

Cyberoam Intrusion Prevention System protects against network and application-level attacks, securing organizations against intrusion attempts, malware, Trojans, DoS and DDoS attacks, malicious code transmission, backdoor activity and blended threats. It can carry thousands of automatically updated signatures, enabling protection against the latest vulnerabilities.



## **IBM® Security Network Intrusion Prevention System**

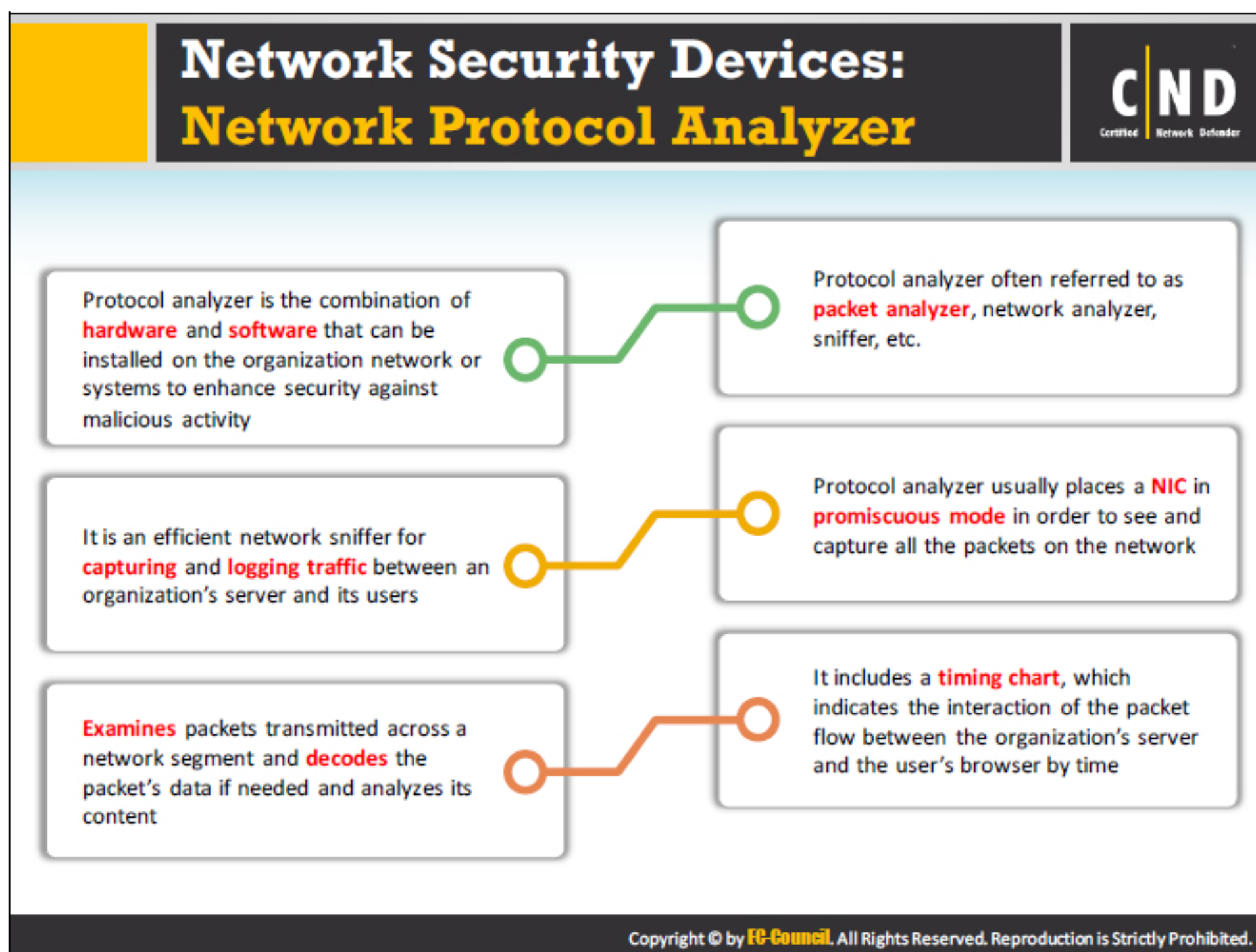
Source: <http://www-03.ibm.com>

IBM® Security Network Intrusion Prevention System stops constantly evolving threats before they impact your business. It provides both high levels of protection and performance, while lowering the complexity associated with deploying and managing a large number of point solutions.

## **AlienVault Unified Security Management**

Source: <http://www.alienvault.com>

AlienVault Unified Security Management analyzes system behavior and configuration status to track user access and activity. It detects potential security exposures such as system compromise, modification of critical configuration files (e.g. registry settings, /etc/passwd), common rootkits, and rogue processes. It identifies the latest attacks, malware infections, system compromise techniques, policy violations, and other threats.



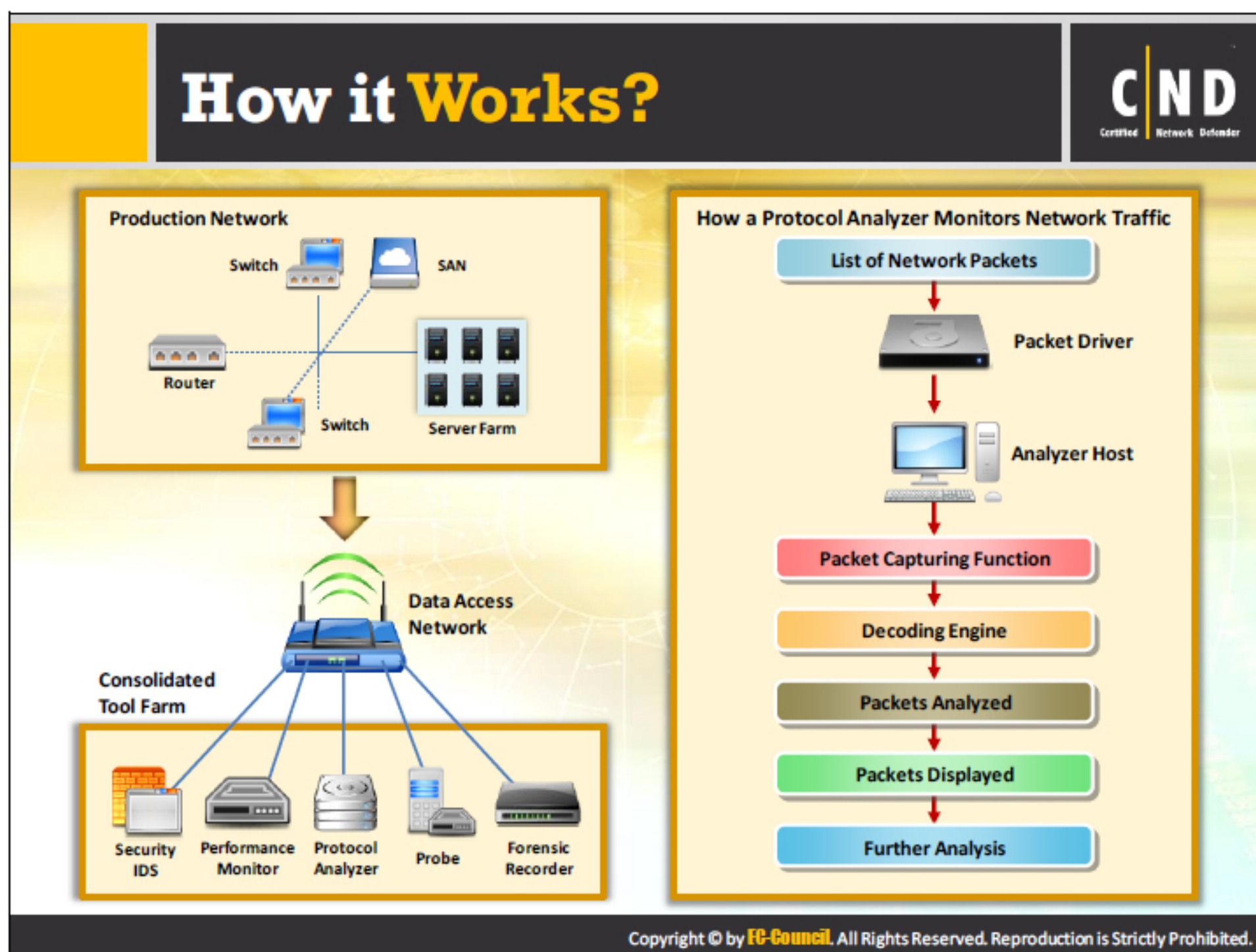
A network protocol analyzer is a computer hardware device or software that monitors and analyzes data passing through a network. A network protocol analyzer can complement a firewall, an anti-virus, and a spyware in a network. It analyzes the raw data in each packet and identifies the content in each packet passing through the network. It reduces the probability of occurrence of an attack in a network and also provides immediate response to an attack on the network.

Features of a network protocol analyzer include:

- Detailed description of activities in a network.
- Network traffic analysis.
- Packet data analysis.
- Alarms for threats in the network.
- Bandwidth analysis.


Network protocol analyzer enables the network administrator to gain a snapshot of the traffic in the network.










The analyzer works on the host machine. After starting the analyzer in the promiscuous mode, the NIC on the host captures all traffic passing through it. The analyzer then forwards the captured traffic into the packet-decoder engine of the analyzer. Here, the decoder engine monitors the behavior of the traffic and splits the packets into their respective layers. The analyzer software will now verify these packets and later display the packet information on the host screen of the analyzer. The analyzer also enables filtering of the packet depending on the product capability.

## Advantages of using a Network Protocol Analyzer



Detects <b>network misuse</b> by internal and external users	
Analyzes <b>network problems</b>	
Detects network <b>intrusion attempts</b>	
Monitors <b>network usage</b> and WAN bandwidth utilization	
Gathers and reports <b>network statistics</b>	
<b>Debugs</b> network protocol implementations	
<b>Troubleshoots</b> hard-to-solve problems	
<b>Gathers information</b> , such as baseline traffic patterns and network utilization metrics	
Identifies <b>unused protocols</b> so that you can remove them from the network	
<b>Generates traffic</b> for penetration testing	
Eavesdrops on traffic and <b>filters suspected traffic</b> from network	

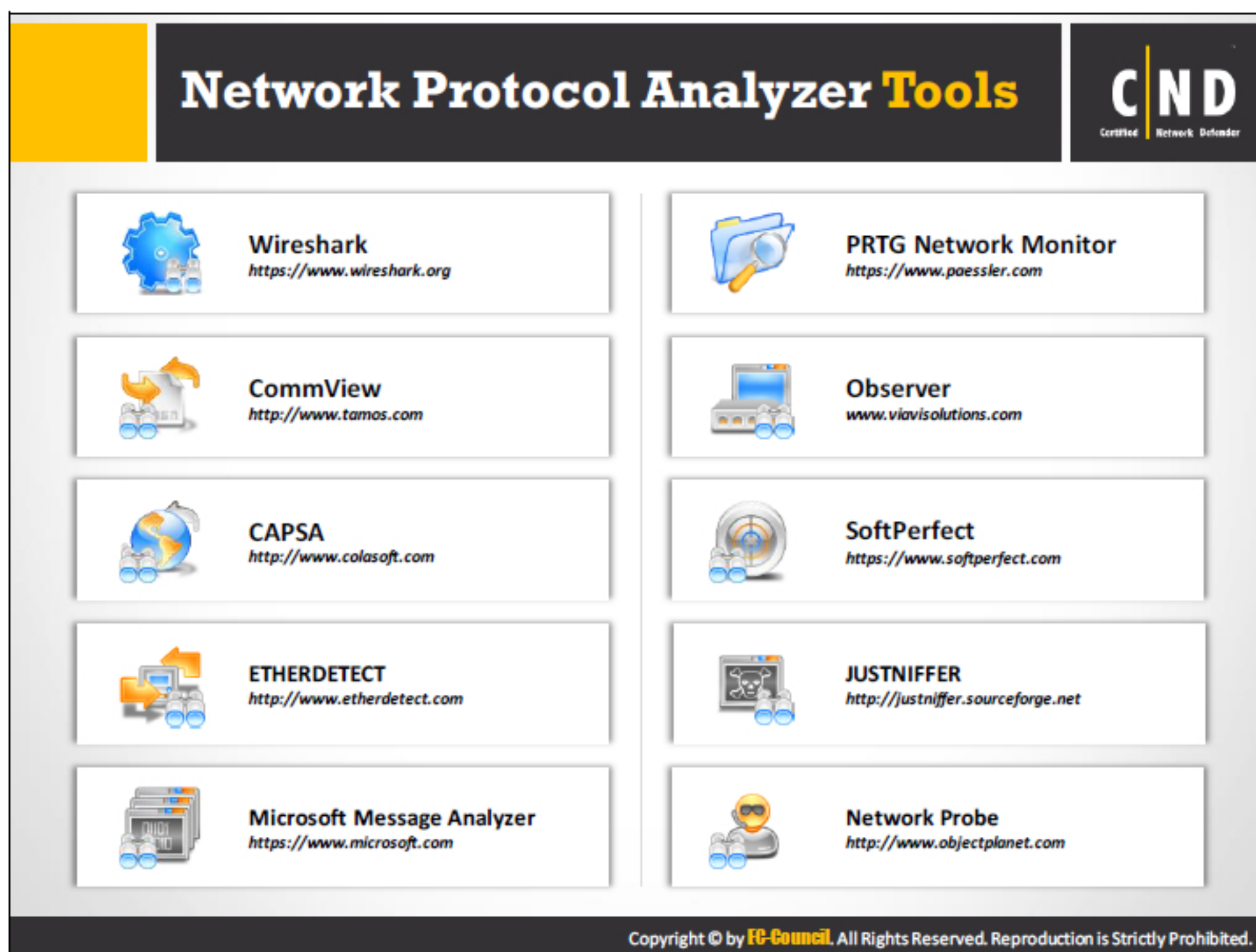
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

The following are some benefits of using a Network Protocol Analyzer in the network:

- It can be used as a network troubleshooting and debugging tool. It helps in figuring out the reason for performance issues, identifying protocol errors, reason for DHCP to stop working, reason for virtual network not routing traffic correctly, and various other related problems.
- It is used to identify implementation and configuration errors while implementing a new service or altering an existing one.
- It helps in improving the performance of security products like firewalls and intrusion-detection systems. By analyzing the packets using the protocol analyzer reasons for access issues like passing of malicious traffic and the restriction of authorized packets can be identified.
- It is used to analyze attacks like a Denial of Service (DoS) attack.
- It generates application statistics such as average HTTP traffic transaction time, DNS query and SQL Server response time, retransmission rates, and top talkers and listeners on the network.
- It provides all the current and latest updates of the activities occurring in the network.
- It verifies the occurrences for any irregularity in the network traffic and checks if there is any variation in the features of a data packet.



- It records details that later assist in the forensic investigation of any incident. This minimizes the risk of users gaining information related to any previous incident.
- It can inquire about any particular data string in a given packet.
- It can disable any unwanted protocols.
- Gets details about the untrusted contents in a packet.
- Monitors other network users.
- Helps in reinstating client-server communications.
- Helps in debugging network protocol applications.
- Blocks all unwanted traffic in the network or in other words, blocking all traffic that is not required for analyzing.



## Wireshark

Source: <https://www.wireshark.org>

Wireshark captures network packets and tries to display that packet data as detailed as possible. It examines what's going on inside a network cable.

## CommView

Source: <http://www.tamos.com>

CommView is a network monitor and analyzer designed for LAN administrators, security professionals, network programmers, home user. It captures every packet on the wire to display important information such as a list of packets and network connections, vital statistics, protocol distribution charts, and so on. It allows examining, saving, filtering, import and export captured packets, view protocol decodes down to the lowest layer with full analysis of over 100 supported protocols.

## CAPSA

Source: <http://www.colasoft.com>

Capsa is a portable network analyzer application for both LANs and WLANs, which performs real-time packet capturing capability, 24x7 network monitoring, advanced protocol analysis, in-depth packet decoding, and automatic expert diagnosis. It gives quick insight to network administrators or network engineers allowing them to rapidly pinpoint and resolve application problems.



## **ETHERDETECT**

Source: <http://www.etherdetect.com>

EtherDetect provides a connection-oriented view for analyzing packets more effectively.

Few of the features of EtherDetect include:

- Captures full packets, organized by TCP connections or UDP threads.
- Passively monitors your network, with no need to install the program on target PCs.
- Packet viewing in Hex format and syntax highlighting viewer.

## **Microsoft Message Analyzer**

Source: <https://www.microsoft.com>

The Microsoft Message Analyzer supports the latest protocol parsers for capturing, displaying, and analyzing protocol messaging traffic, events, and other system or application messages in troubleshooting and diagnostic scenarios.

## **PRTG Network Monitor**

Source: <https://www.paessler.com>

PRTG protocol analyzer allows you to use an unlimited number of NetFlow / flow sensors. Using its built-in protocol analyzer, PRTG can monitor and classify network traffic by IP address, protocol or user-defined, custom parameters.

## **Observer**

Source: <http://www.viavisolutions.com>

Observer Analyzer delivers individual packet views and decodes over 740 primary protocols and countless sub-protocols.

## **SoftPerfect**

Source: <https://www.softperfect.com>

Softperfect performs analyzing, debugging, maintaining and monitoring local networks and Internet connections. It captures the data passing through the dial-up connection or Ethernet network card, analyses this data and then represents it in a readable form. This is a useful tool for network administrators, security specialists, network application developers and anyone who needs a comprehensive picture of the traffic passing through their network connection or a segment of a local area network.

## **JUSTNIFFER**

Source: <http://justniffer.sourceforge.net>

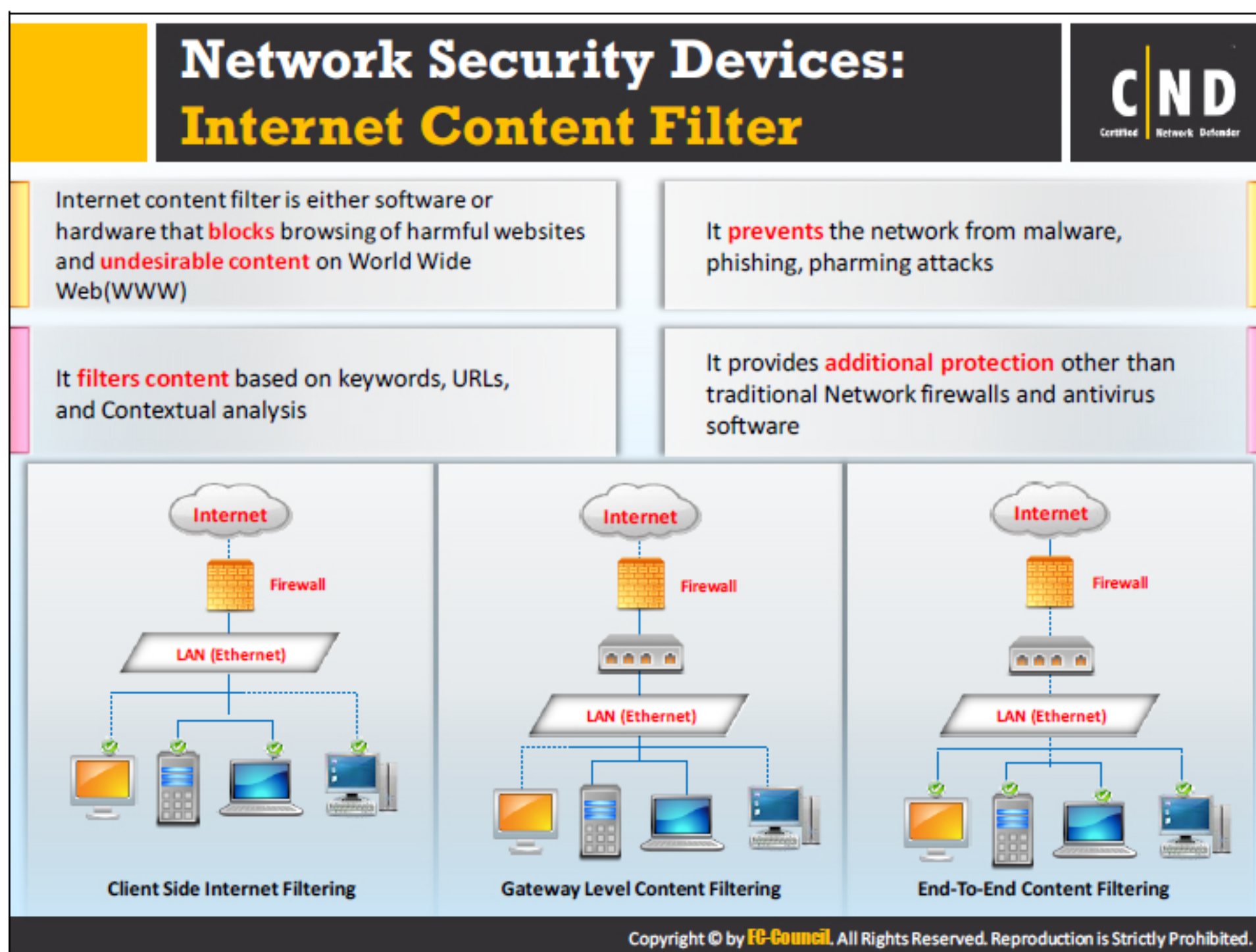
Justniffer is a network protocol analyzer that captures network traffic and produces logs in a customized way. It can also emulate Apache web server log files, track response times and extract all "intercepted" files from the HTTP traffic.

## Network Probe

Source: <http://www.objectplanet.com>

Network Probe is a network monitor and protocol analyzer to monitor network traffic in real-time, and will help you find the sources of any network slowdowns.

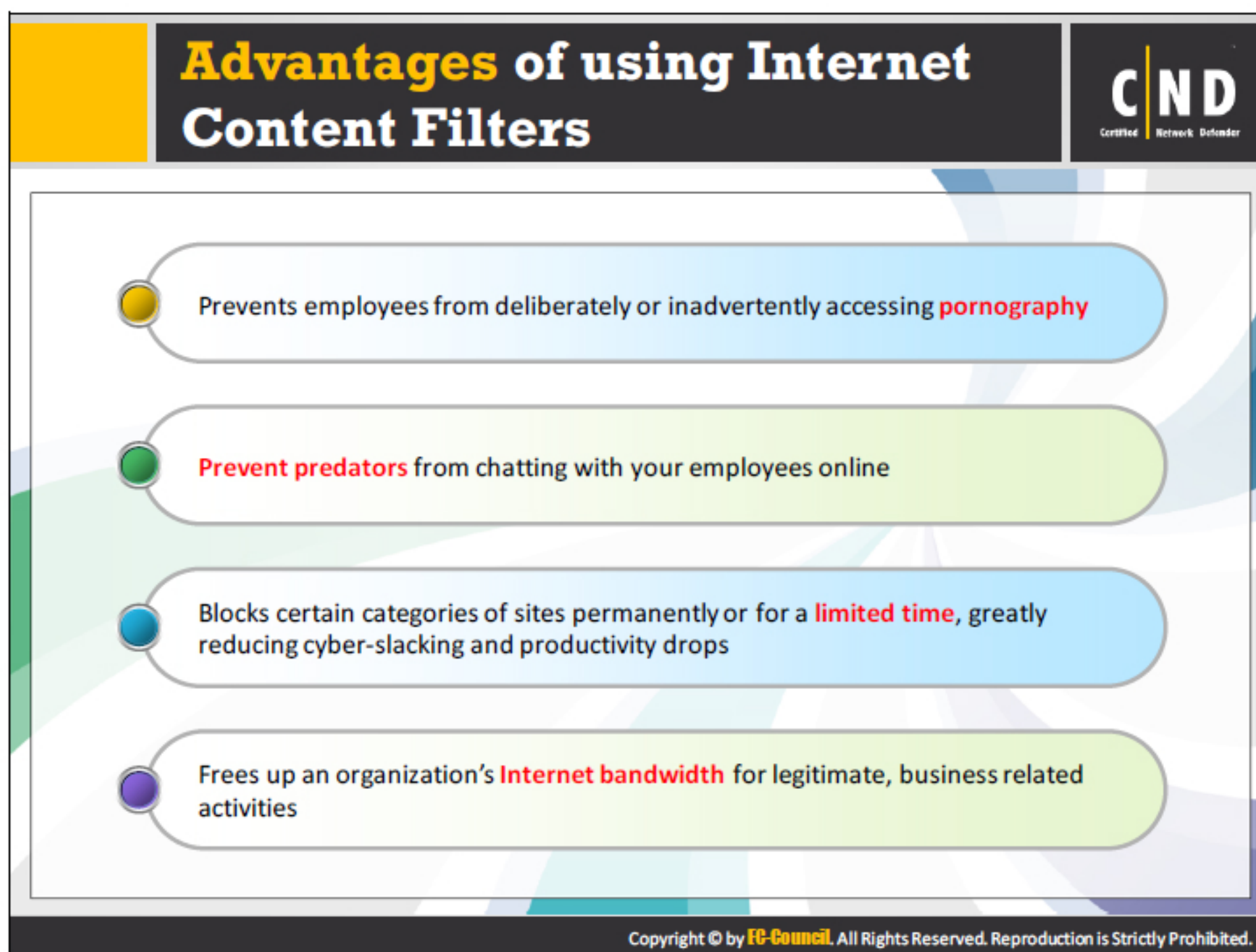




Content filters block deceptive web pages or emails. It protects the network from malware and other systems that are unreceptive and interfering. A content filter allows the organization to block certain web sites. Organizations can implement different types of Internet filtering:

- Browser-based filters
- E-mail filters
- Client-side filters
- Content-limited filters
- Network-based filtering
- Search engine filters

In the process of content filtering, it compares each character string in the web site in order to screen it. Most of the organizations filter pornographic or violence related websites. Content filtering can protect a network from all kinds of malware codes or other attacks that can make massive changes in the system and network.



## Controls the productivity

It is often difficult to manage employee activities in a large organization. The Internet content filter can assist the organization from restricting the employees from using any social networking sites or any illegitimate sites. Network administrators can block sites not related to work and thereby increase the efficiency and productivity of the organization.

## High-level of protection

Internet content filters normally provide protection from malware programs and software.

## Restricts all kinds of liability issues

Content filtering software can prevent users from sharing files and other documents outside the organization.

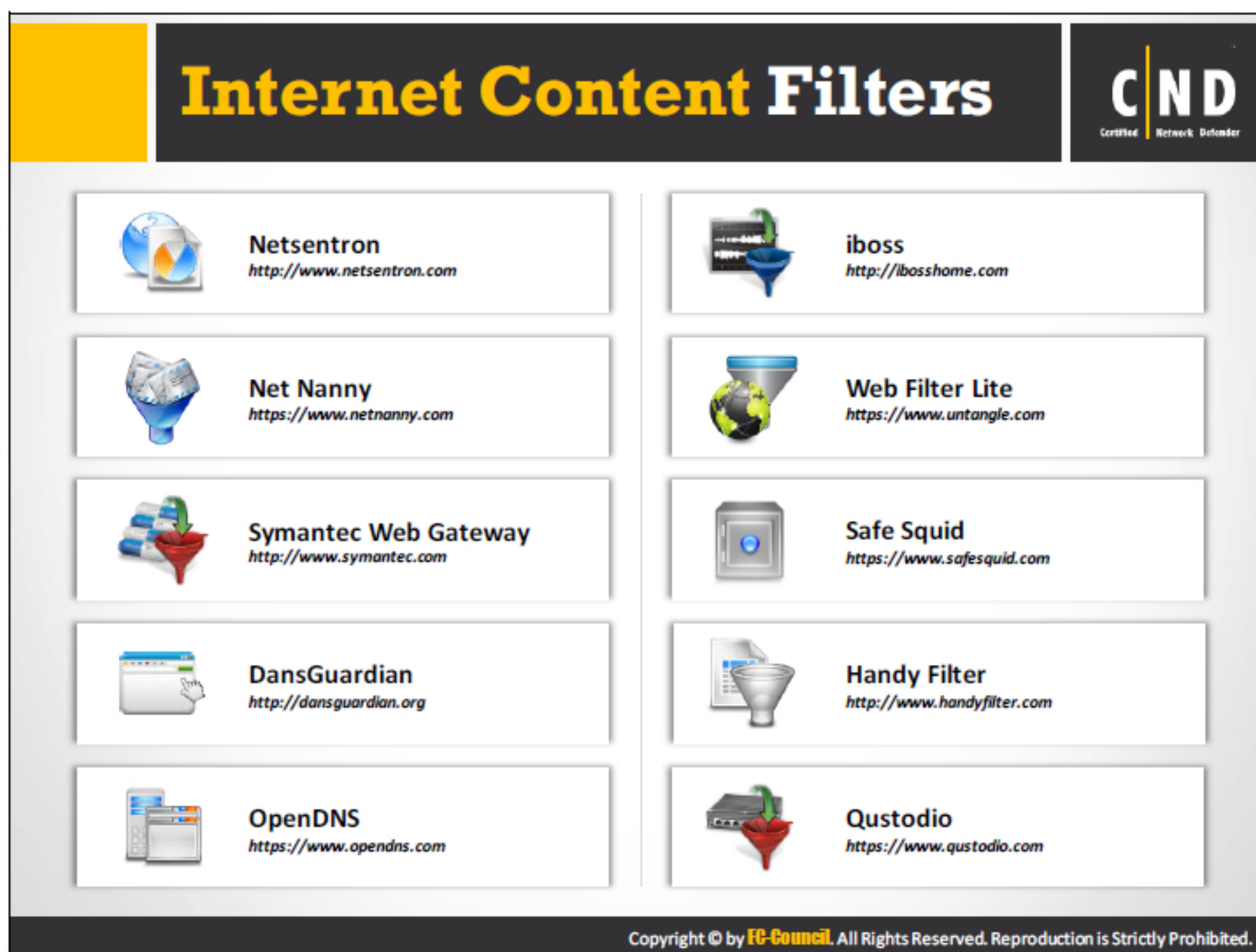
## Highly flexible

It enables the organization to decide on the sites that need to be blocked. It also provides the organization the ability to change the site blocking setting at any time.

## Increased speed

Using Internet content filtering allows the organization to control the bandwidth of the Internet connection by blocking sites. This in turn increases the speed of the Internet.





### Netsentron

Source: <http://www.netsentron.com>

Netsentron content filter is primarily used in schools and businesses. It stops all unauthorized access to a network and also blocks pornographic, offensive, and unapproved websites. It also provides the flexibility to work on files remotely.

### Net Nanny

Source: <https://www.netnanny.com>

Net Nanny helps parents filter out the harmful content and other dangers of the Internet.

Various features of Net Nanny include:

- Compatible with Windows, Mac, Android, iPhone, iPod Touch, and iPad.
- Blocks pornography.
- Masks profanity before it appears on the screen.
- Controls access to set time limits on Internet usage.
- Sends alerts and reports to console or email.
- Creates user profiles to tailor protection to the individual family member's needs.

### **Symantec Web Gateway**

Source: <http://www.symantec.com>

Symantec Web Gateway protects organizations against multiple types of malware and gives organizations the flexibility of deploying it as either as a virtual appliance or on physical hardware.

### **DansGuardian**

Source: <http://dansguardian.org>

DansGuardian filters the actual content of pages based on many methods, including phrase matching, PICS filtering and URL filtering.

### **OpenDNS**

Source: <https://www.opendns.com>

OpenDNS Web filtering lets you manage the Internet experience on and off your network with the acceptable use or compliance policies, putting you in control.

### **Iboss**

Source: <http://ibosshome.com>

The iboss Home allows you to take control of the Internet in your home by restricting the websites and online content.

### **Web Filter Lite**

Source: <https://www.untangle.com>

Web Filter Lite enables administrators to enforce network usage policies and monitor user behavior. Zero client installation and category block lists make it easy to protect the network from malware, block potential time wasting sites, and conserve bandwidth by blocking video downloads.

### **Safe Squid**

Source: <https://www.safesquid.com>

SafeSquid detects and blocks malware at the web-gateway before it can reach the users. Also, it protects users from fraudulent websites, web-applications, and security breaches.

### **Handy Filter**

Source: <http://www.handyfilter.com>

Handy Filter is a Web Content Filtering Software which enables you to track the user visited websites. Block web access at specific hours you choose.


### **Qustodio**

Source: <https://www.qustodio.com>

Qustodio internet filter blocks inappropriate content, even in private browsing mode. It also tracks and monitors the time spent on specific sites.



## Network Security Devices: Unified Threat Management (UTM)




- UTM is a network security management solution which allows administrator to **monitor and manage** the organization's network security through a centralized management console
- It provides firewall, intrusion detection, antimalware, spam filter, load balancing, content filtering, data loss prevention, and VPN capabilities using a **single UTM appliance**

### Advantages

- Reduced complexity
- Simplicity
- Easy Management

### Disadvantages

- Single point of failure
- Single point of compromise



The diagram illustrates the components of UTM Solutions. A central yellow circle labeled "UTM Solutions" is surrounded by six colored circles, each connected to a specific security function by a line: Load Balancer (blue), Content Filter (purple), VPN (yellow), Network Firewall (pink), Anti-Virus and Anti-Spam (light blue), and IDS/IPS (orange).

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Unified Threat Management or UTM is a security management method that enables the administrator to evaluate and examine security related applications and other components through a single console. UTM helps in minimizing the complexity of the network by protecting users from blended threats.

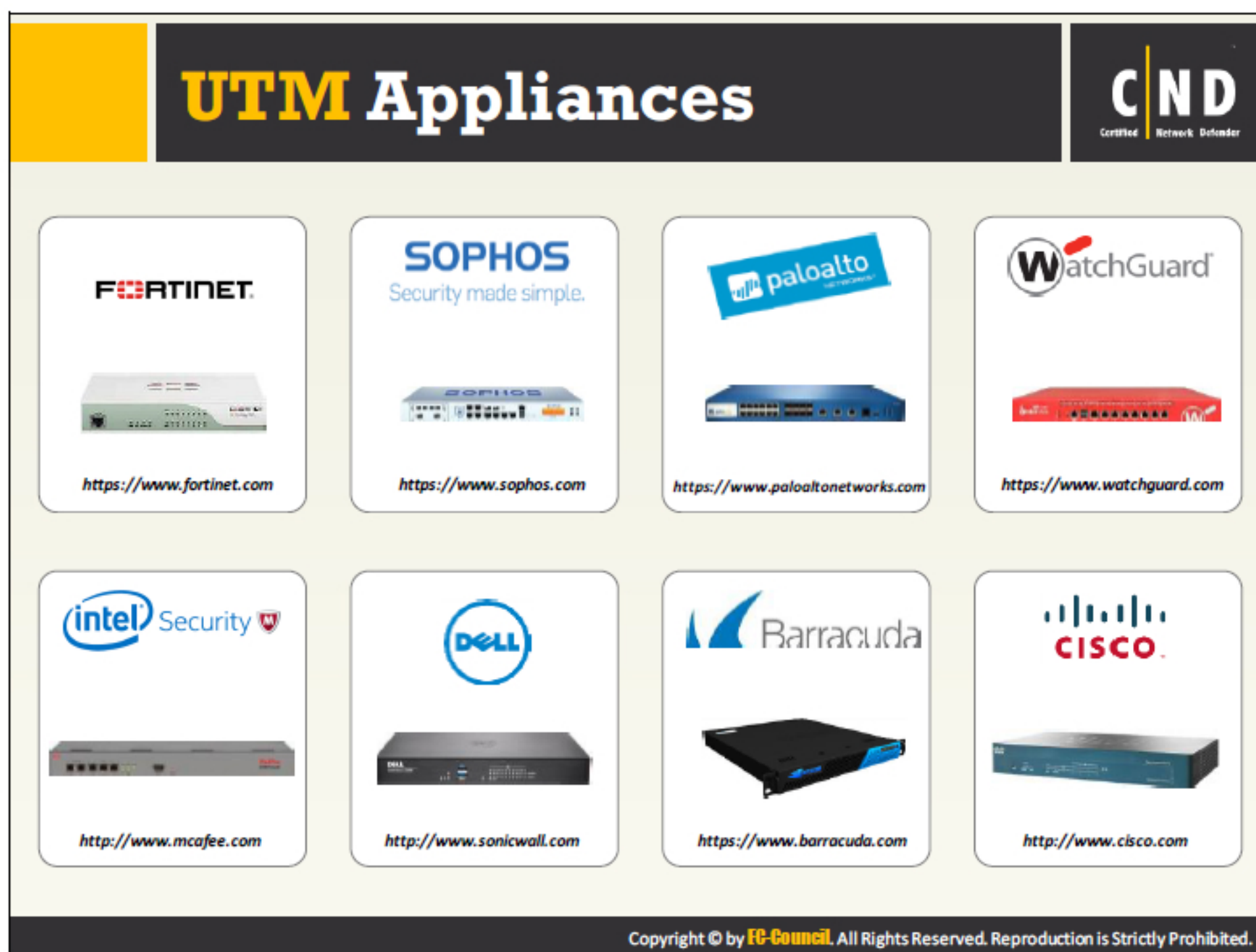
### Advantages of UTM:

- **Less cost:** Reduces the cost of buying multiple devices. UTM needs only a single console that can manage the whole network.
- **Low maintenance cost:** As only a single console is used, it needs little maintenance.
- **Easy installation and management:** UTM involves the use of only a single console that requires minimum wiring and other installation requirements.
- **Fully integrated:** UTM is a complete console that incorporates every feature required for protecting a network.

## Disadvantages of UTM:

- Less specialization: As UTM is a single console managing the whole security of the network, there are chances of it missing out certain features required to maintain the security. The case can be avoided by using dedicated devices for each feature.
- Single point-of-failure: UTM involves the use of a single console with all features included in it. Failure of one feature can affect the performance of the other features and the working of the UTM as such.
- Possible performance constraints: The single console in UTM performs various tasks at the same time. There are chances that all the tasks or features do not get the CPU time adequately. This situation may lead to many attacks on the system.





## Fortinet

Source: <https://www.fortinet.com>

Fortinet helps in protecting the entire network from the endpoint to the cloud, delivering industry-leading, end-to-end simplified security.

## SOPHOS

Source: <https://www.sophos.com>

With SOPHOS UTM, it is easy to configure firewall rules that cover multiple destinations, sources, and services. It also provides country blocking and intrusion prevention (IPS). It allows control of web applications proactively or in real-time using the popular flow-monitor.

## Watch Guard

Source: <http://www.watchguard.com>

Watch guard provides an all-in-one network security platform. It provides monitoring and isolation of threats present in the console.

## **Dell**

Source: <https://www.sonicwall.com>

UTM technology delivers comprehensive protection and simplifies security management, all without affecting the speed of the network. It decontaminates VPN and wireless traffic and ensures the integrity of all traffic passing through.

## **Barracuda**

Source: <https://www.barracuda.com>

Barracuda Firewall provides comprehensive network security and optimization. It uses the power of the cloud in innovative ways to deliver next-generation firewall and content-security features without bogging down the network.

## **Palo Alto Networks**

Source: <https://www.paloaltonetworks.com>

Palo Alto Networks is a network security appliance built around the next-generation firewall. It easily integrates with every other security element. It is used for networking, security, content inspection, and management.

## **McAfee**

Source: <http://www.mcafee.com>

McAfee's network security solutions detect advanced targeted attacks and get actionable threat information. It optimizes threat detection and response by closing the gap from malware encounter to containment.


## **Cisco**

Source: <http://www.cisco.com>

Cisco's security appliances provide zone-based firewall, IPS, Web threat protection and URL filtering. It also involves application control, spam filter, gateway anti-virus, site-to-site VPN, remote user VPN with Cisco.



## Network Security Devices: Network Access Control (NAC)



- Network Access Control, also known as Network Admission Control (NAC) are appliances or solutions that attempt to protect the network by **restricting the connection** of an end user to the network based upon a security policy
- The **pre-installed software agent** may inspect several items before admitting the device and may restrict where the device may be connected

### What NAC does?

**Authentication** of users connected to network resources

**Identification** of devices, platforms, and operating systems

**Defining** a connection point of network devices

**Development** and application of security policies

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Network Access Control (also known as Network Administration Control) deals with restricting the availability of a network to the end user depending on the security policy. It mainly restricts systems without antivirus, intrusion prevention software from accessing the network. NAC allows you to create policies for each user or systems and define policies for networks in terms of IP addresses.

- NAC **implements** detection programs using the following points:
  - Searching for an antivirus program and examining whether it is updated or not.
  - Checking if the end system has a configured firewall or Intrusion Prevention Software.
  - Looking for any viruses on the network, and checking if the operating system is updated.
- NAC **performs** the following actions:
  - Evaluate unauthorized users, devices, or behaviors in the network. It provides access to authorized users and other entities.
  - NAC helps in identifying users and devices on a network. Also determines whether these users and devices are secure or not.
  - Examines the system integration with the network according to the security policies of the organization.



NAC helps in maintaining security policies for increased control of the network. An organization must look into the threats to its network while considering the cost of implementing NAC. Organizations need to have plans to rectify the faults in the policies while implementing a NAC. Organizations may consider the following points:






- Do the NAC policies authenticate users?
- How well is the NAC implemented?
- Is NAC properly integrated with the device?
- Does the NAC tool check if the end user is blocked?

Organizations need to consider the following resources while implementing a NAC:

- **Network Infrastructure:** Incorporate network access control policies within the network infrastructure.
- **Security:** Managing the infrastructure.
- **Human Resources:** Reporting the network policies to the employees in an organization.
- **Operations:** Management of response, procedures and actions.
- **Management:** Decides the priority of the policies, effect of policies on the organization and managing the budget issues.





 <b>ForeScout CounterACT™</b> <a href="https://www.forescout.com">https://www.forescout.com</a>	 <b>Bradford Networks' Network Sentry/NAC</b> <a href="https://www.bradfordnetworks.com">https://www.bradfordnetworks.com</a>
 <b>Extreme Networks NAC</b> <a href="http://www.extremenetworks.com">http://www.extremenetworks.com</a>	 <b>PacketFence NAC</b> <a href="http://packetfence.org">http://packetfence.org</a>
 <b>Trustwave Network Access Control</b> <a href="https://www.trustwave.com">https://www.trustwave.com</a>	 <b>Arubanetworks ClearPass Policy Manager</b> <a href="http://www.arubanetworks.com">http://www.arubanetworks.com</a>
 <b>Cisco NAC Appliance</b> <a href="http://www1.cisco.com">http://www1.cisco.com</a>	 <b>Portnox Network Access Control</b> <a href="http://www.portnox.com">http://www.portnox.com</a>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### ForeScout CounterACT™

Source: <https://www.forescout.com>

ForeScout CounterACT provides real-time visibility of users, devices, operating systems and applications connected to the network. CounterACT provides comprehensive network access control capabilities to enforce network access and compliance policies, after discovering and classifying devices.

### Extreme Networks NAC

Source: [www.extremenetworks.com](http://www.extremenetworks.com)

Extreme Networks NAC provides an unparalleled range of choices for fine grained network access control.

### Trustwave Network Access Control

Source: <https://www.trustwave.com>

Trustwave NAC enables granular control over network access and continuous monitoring of corporate-sanctioned and bring-your-own-device (BYOD) endpoints. This helps prevent the spread of malware and other threats that can harm infrastructure and make the business vulnerable to attack and data loss.

## **Cisco NAC Appliance**

Source: <http://www1.cisco.com>

The Cisco Network Admission Control System, composed of the Cisco NAC Manager and Server, is a policy component of the Cisco TrustSec solution. Cisco NAC Appliance extends NAC to all network access methods, including access through LANs, remote-access gateways, and wireless access points. It also supports posture assessment for guest users.

## **Bradford Networks' Network Sentry/NAC**

Source: <https://www.bradfordnetworks.com>

It dynamically leverages the continuously growing library of security commands and controls built into today's switches, routers, wireless controllers and wireless access points to perform pre-connect risk assessments on every device attempting to connect to the network.

## **PacketFence NAC**

Source: <http://packetfence.org>

PacketFence effectively secures networks from small to very large heterogeneous networks. PacketFence's operation is completely out-of-band which allows the solution to scale geographically and to be more resilient to failures.

## **Arubanetworks ClearPass Policy Manager**

Source: <http://www.arubanetworks.com>

ClearPass solves today's digital workplace security challenges across any multivendor network by replacing outdated legacy AAA with context-aware policies. It delivers visibility, policy control and workflow automation in one cohesive solution.


## **Portnox Network Access Control**

Source: <http://www.portnox.com>

It evaluates all networking layers – Ethernet, wireless, virtual, VPN and even the cloud to illuminate, visualize, analyze and control all connected users and devices. It communicates with user-driven devices such as laptops, desktops, VoIP phones, tablets, etc. to identify the user currently using the device. Every decision Portnox NAC makes factors in the Device, Network and Identity (DNI).

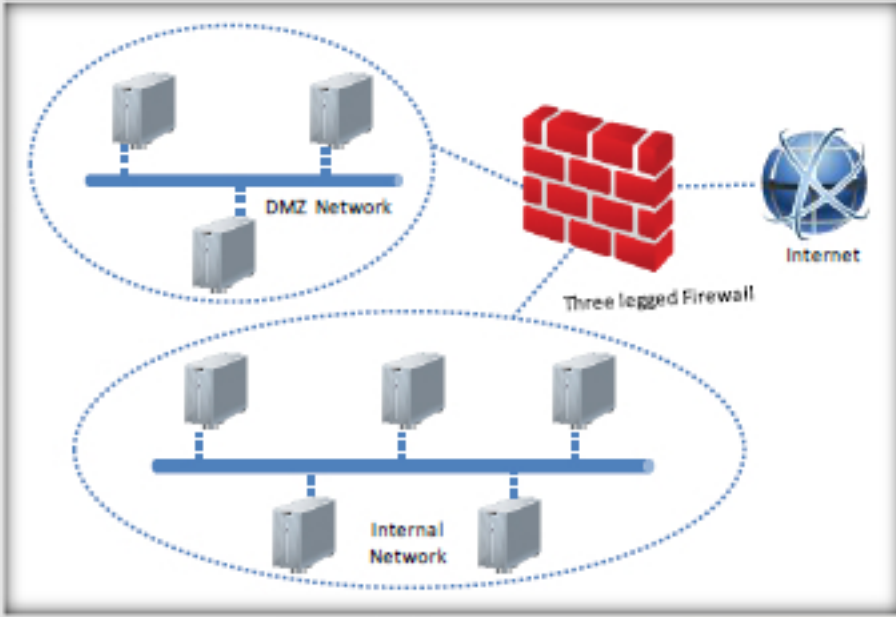


# Demilitarized Zone (DMZ)



Computer sub network is placed between the organization's private network, such as **LAN**, and an outside public network, such as the **Internet**, and acts as an additional security layer

- Contains the servers which need to be accessed from an outside network
  - Web servers
  - Email servers
  - DNS servers
- DMZ configurations
  - Both **internal** and **external** networks can connect to DMZ
  - Hosts** in the DMZ can connect to external networks
  - But hosts in the DMZ can not connect to internal networks



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

A DMZ is a small network which is placed between the organization's private network and an outside public network. It prevents the outsider from getting direct access to the organization's server. For example, if an attacker uses the public network to access the DMZ host and penetrates it, then only the information on that host will be compromised. In this way, a DMZ acts as an additional security layer for networks and lowers the threat of intrusion in the internal network. A DMZ contains the following servers, which need to be accessible from outside the network:

- Web servers
- Email servers
- DNS servers

Two basic methods of designing a network with a DMZ are using a single firewall (three legged model) and using dual firewalls. It is also possible to extend these configurations according to the network requirements.

- **Single Firewall:** In this model, the network architecture containing the DMZ consists of three network interfaces. The first network interface connects the ISP to the firewall forming the external network, whereas the second interface forms the internal network. The third interface forms the DMZ. The firewall acts as the single point of failure and should be able to manage all the traffic to the DMZ.

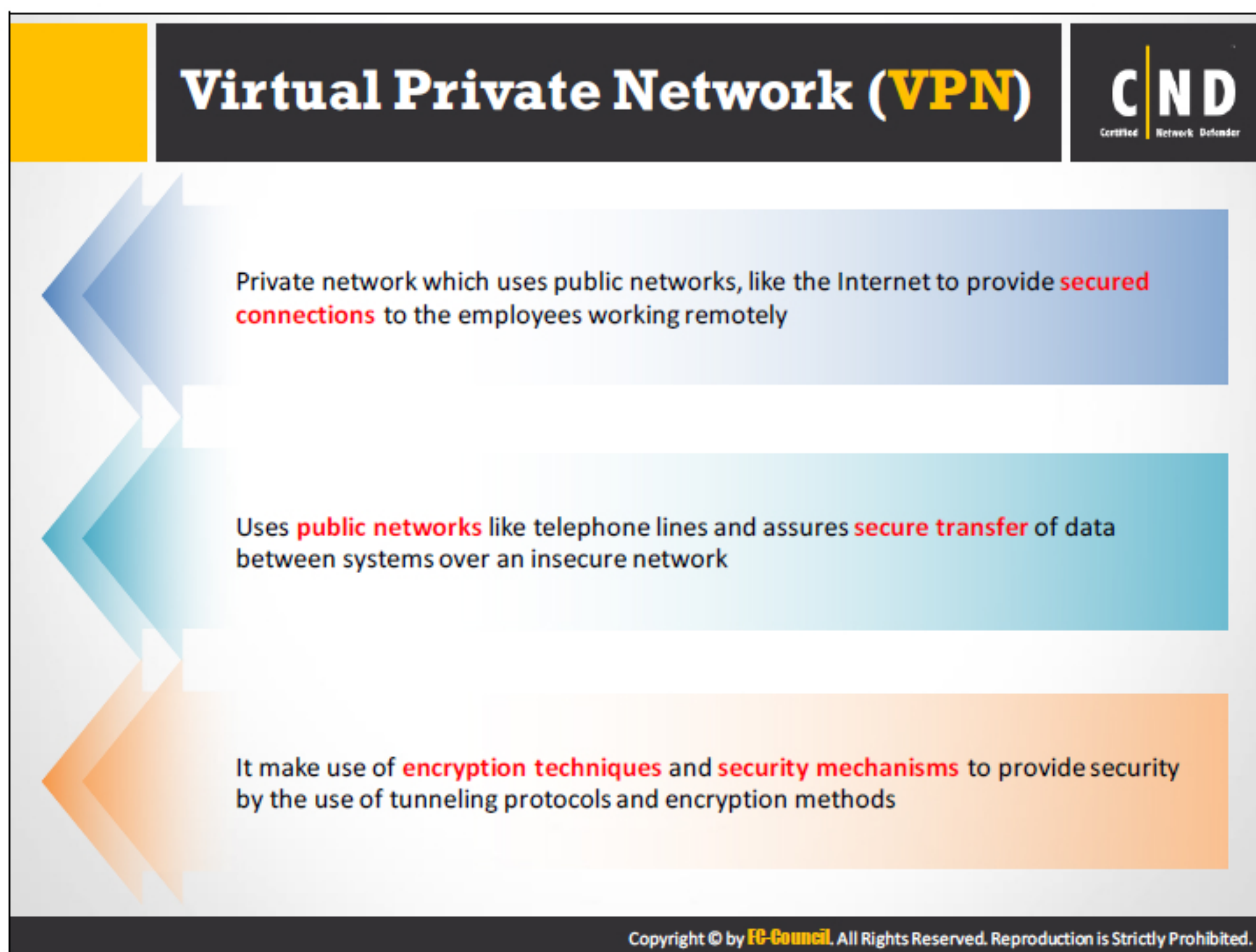
- **Dual Firewall:** The dual firewall approach uses two firewalls to create a DMZ. The first firewall allows only sanitized traffic to enter the DMZ and the second firewall double checks it. The dual approach is the most secure approach in implementing a DMZ.

Any server that needs exposure to the public network can be placed in the demilitarized zone. It is possible for the network administrator to place servers like web server, DNS server, e-mail server, FTP server, in the DMZ and enable access for internal and external clients.

### **Advantages of DMZ:**

- Separation of DMZ from LAN enables the high level protection of LAN.
- Provide an increased control of resources.
- It uses multiple software and hardware based products of different platforms in order to provide an additional layer of protection.
- Provides a high level of flexibility for Internet-based applications like email, web services, etc.

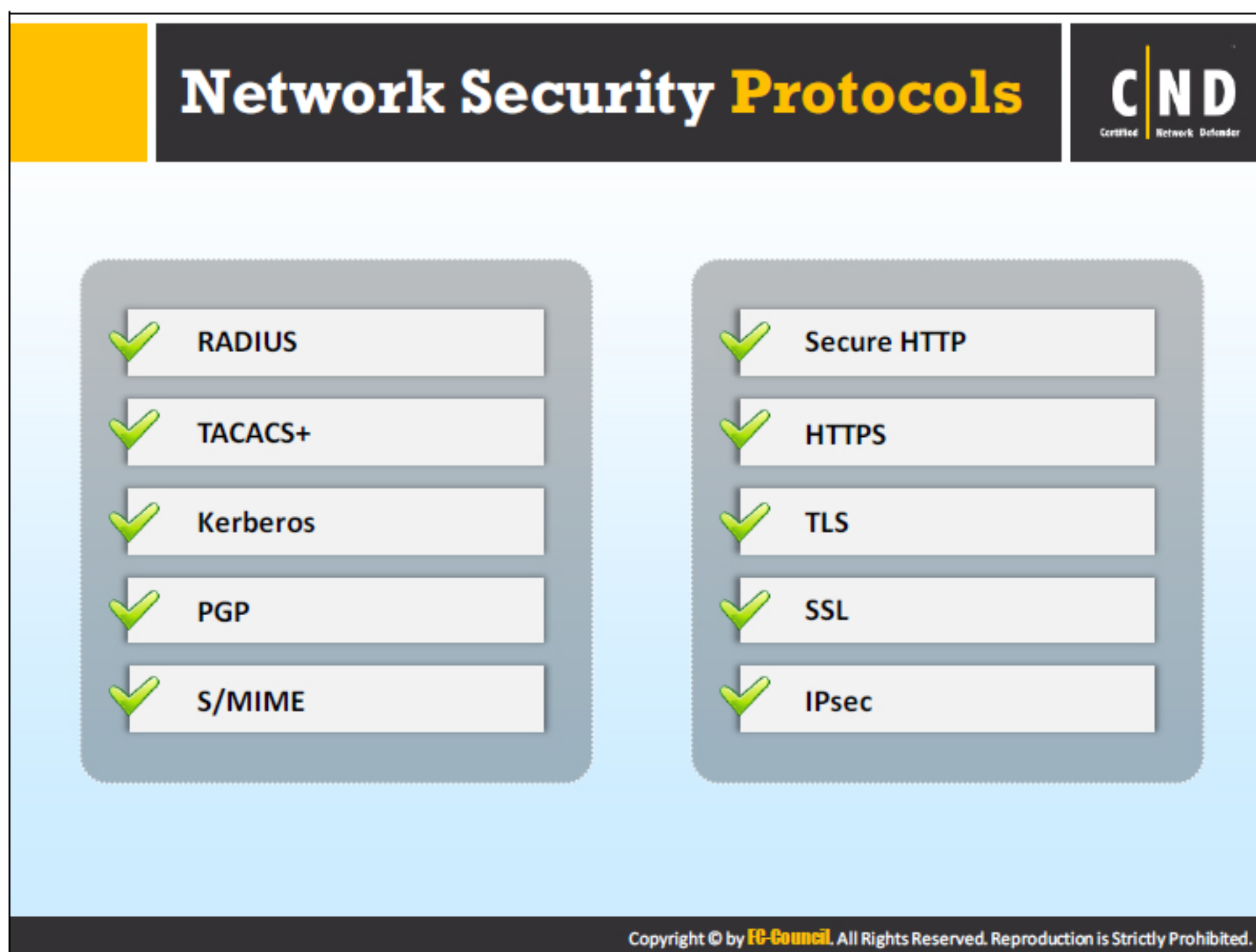




A VPN uses public networks, such as the Internet, and assures secure transfer of data between systems over them. Certain tunneling protocols employed by the VPN help to achieve encryption, data integrity, and authentication. A VPN ensures scalability in organizing to support new clients, organizations, and applications. It ensures solutions to business problems with its embedded technology.

A VPN enables a virtual connection between users and the public network. A packet that is transmitted is encapsulated inside a new packet along with a new header. The header facilitates packet traversal in the network. The path through which the encapsulated packet traverses is known as a tunnel. The encapsulated packet, after reaching the end point of the tunnel is de-encapsulated so that the original packet is forwarded to the final destination.

The tunnel needs to carry the same tunneling protocols that operate at layer 2 - data link layer or layer 3 - network layer of the OSI layer. Commonly used tunneling protocols are: IPsec, PPTP, L2TP and SSL.



There are various security protocols that work at network, transport and application layers. These protocols help organizations in enhancing the security of their data and communication against different types of attacks.

- The security protocols that work at the **transport layer** are as follows:
  - **Transport Layer Security (TLS):** The TLS protocol provides security and dependability of data between two communicating parties
  - **Secure Sockets Layer (SSL):** The SSL protocol provides security to the communication between a client and a server.
- The security protocols that work at the **network layer** are as follows:
  - **Internet Protocol Security (IPsec):** The IPsec protocol authenticates the packets during the transmission of data.
- The security protocols that work at the **application layer** are as follows:
  - **Pretty Good Service (PGP) protocol:** The PGP protocol provides security to the data through the method of encryption and decryption.
  - **S/MIME Protocol:** Commonly known as Secure/Multi-Purpose Internet mail Extensions, provides security to the e-mails.
  - **Secure HTTP:** Secure HTTP provides security to the data traversing through the world wide web



- **Hyper Text Transfer Protocol Secure (HTTPS):** The HTTPS protocol ensures the security of data in the network
- **KERBEROS:** The Kerberos protocol provides security using a client-server model
- **RADIUS:** The RADIUS protocol provides security to the remote access servers to communicate with a central server.
- **TACACS+:** The TACACS+ provides security using a client-server model

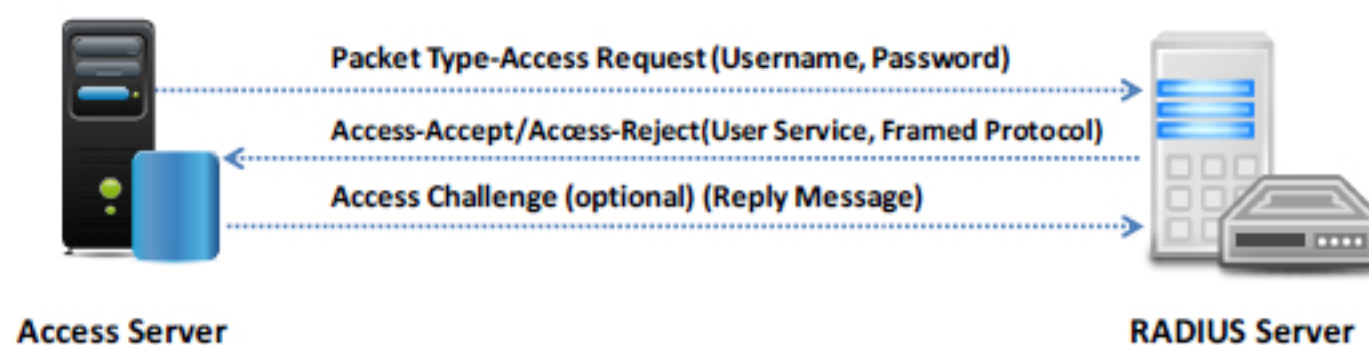
# RADIUS



- Remote Authentication Dial-In User Service (RADIUS) is an **authentication protocol** which provides centralized authentication, authorization, and accounting(AAA) for the remote access servers to communicate with the central server.

## RADIUS Authentication Steps:

1. The client initiates the connection by sending **Access-Request packet** to the server
2. The server receives the access request from the client and compares the credentials with the ones stored in the database. If the provided information matches, then it sends the **Accept-Accept message** along with the **Access-Challenge** to the client for additional authentication else it sends back Accept Reject message
3. Client sends the **Accounting-Request** to the server to specify accounting information for a connection that was accepted



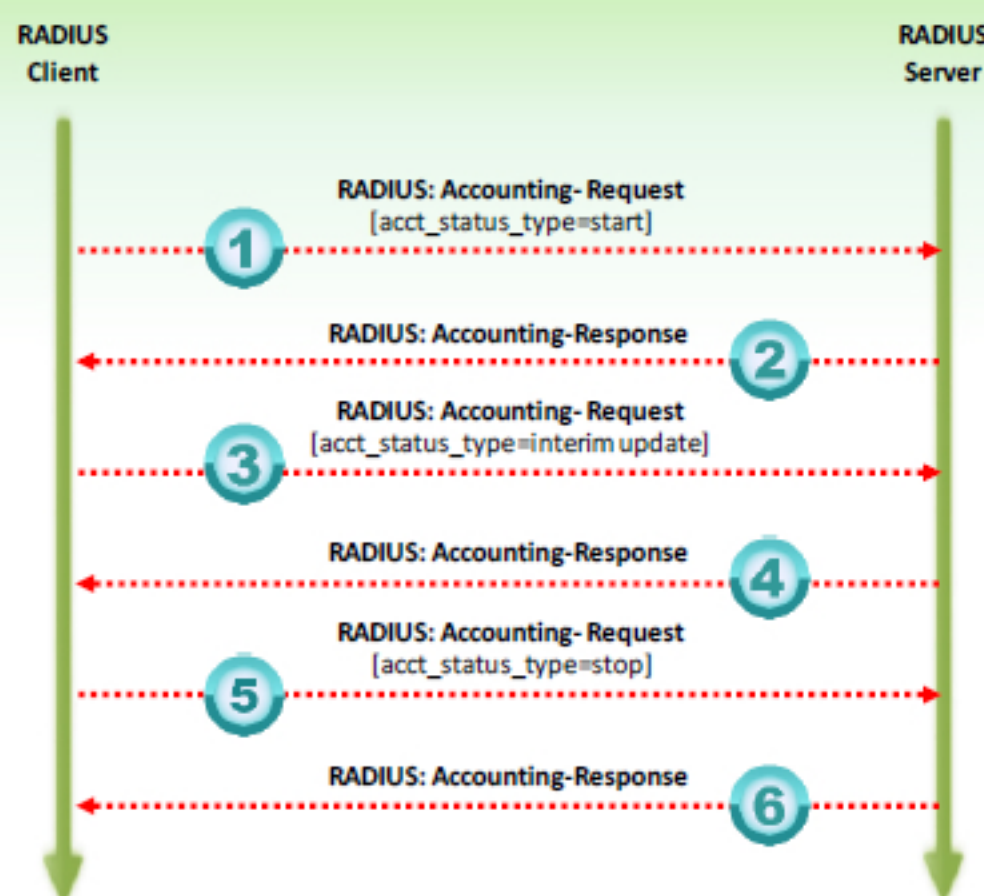
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# RADIUS (Cont'd)



## RADIUS Accounting Steps:

- Client sends the **Accounting-Request** to the server to specify accounting information for a connection that was accepted.
- The server receives the Accounting-Request message and sends back the **Accounting-Response message** which states the successful establishment of network



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

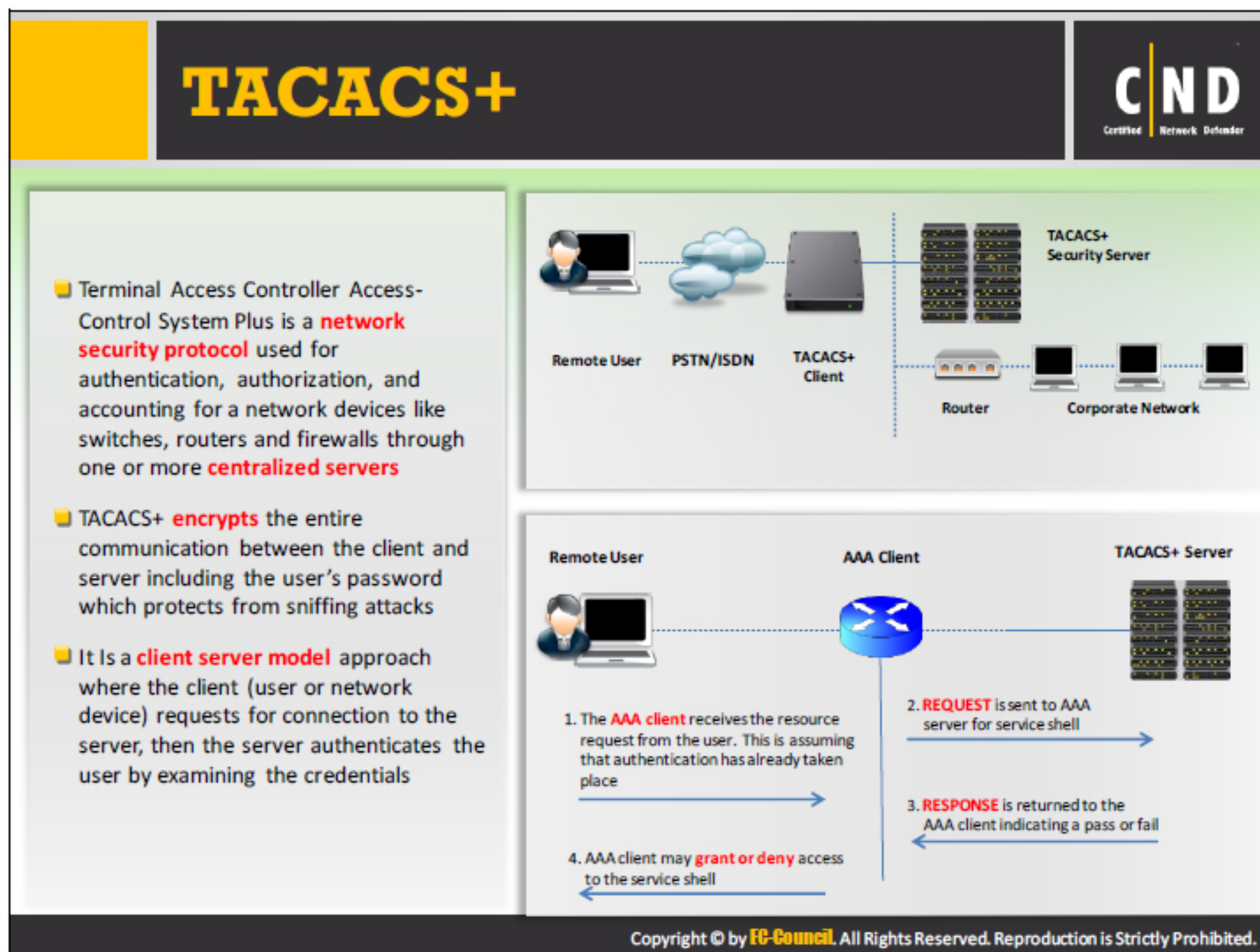


RADIUS stands for Remote Authentication Dial-In User Service. It was developed by Livingston Enterprises as a networking protocol, which provides centralized authentication, authorization, and accounting for remote access servers to communicate with a central server. RADIUS has a client server model, which works on the application layer of the OSI model by using UDP or TCP as a transport protocol. The RADIUS protocol is the de facto standard for remote user authentication and it is documented in RFC 2865 and RFC 2866.

The RADIUS protocol is an AAA protocol that works on both, mobile and local networks. It uses PAP, CHAP, or EAP in order to authenticate the users communicating with servers. The components of a RADIUS AAA protocol are as follows:

- Access clients
- Access servers
- RADIUS proxies
- RADIUS servers
- User account databases

RADIUS messages are sent as UDP messages and allow only one RADIUS message in the UDP payload section of the RADIUS packet. RADIUS messages consist of a RADIUS header and other RADIUS attributes.



Terminal Access Controller Access-Control System Plus (TACACS+) is a protocol developed by Cisco. It is derived from the TACACS protocol. It performs authentication, authorization, and accounting separately unlike RADIUS. It is primarily used for device administration.

### Authentication of TACACS+

Consider the following example of authentication where a laptop user is connecting to a NAS (router). The TACACS+ authentication involves following steps:

- **Step 1:** User initiates the connection for authentication.
- **Step 2:** Router and user exchange authentication parameters.
- **Step 3:** Now, the router sends the parameters to the server for authentication purpose.
- **Step 4:** Server responds with the REPLY message based on the provided information.



## Difference between RADIUS and TACACS+

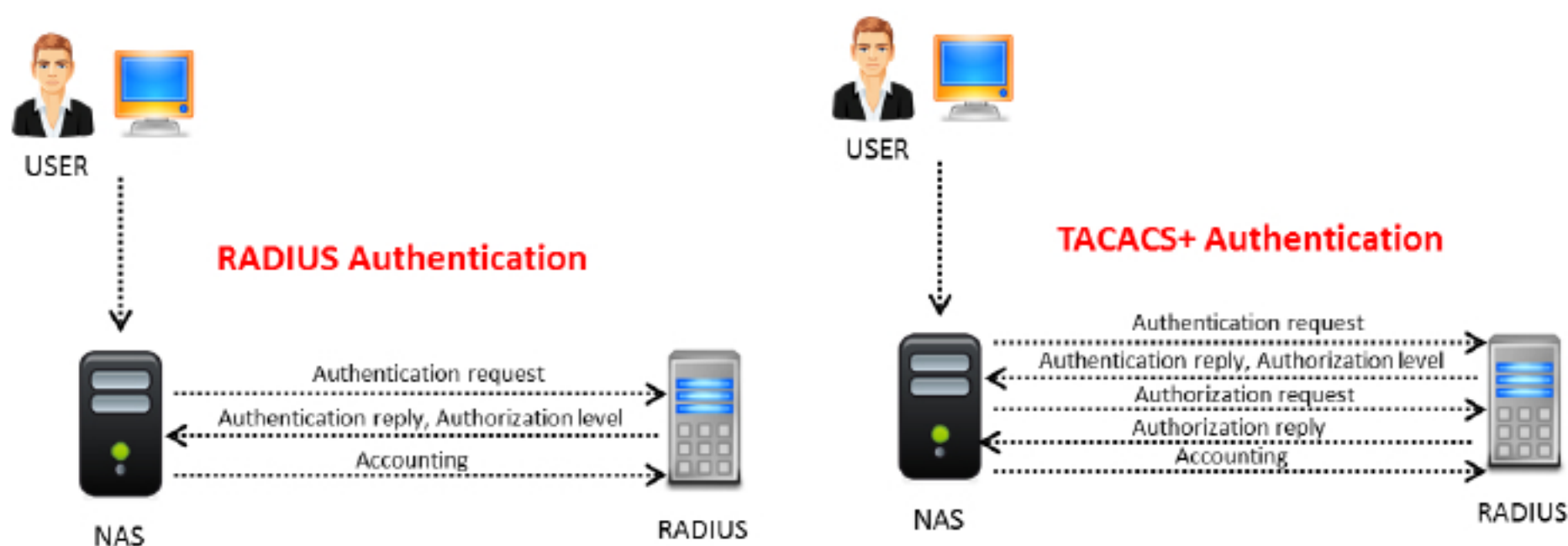
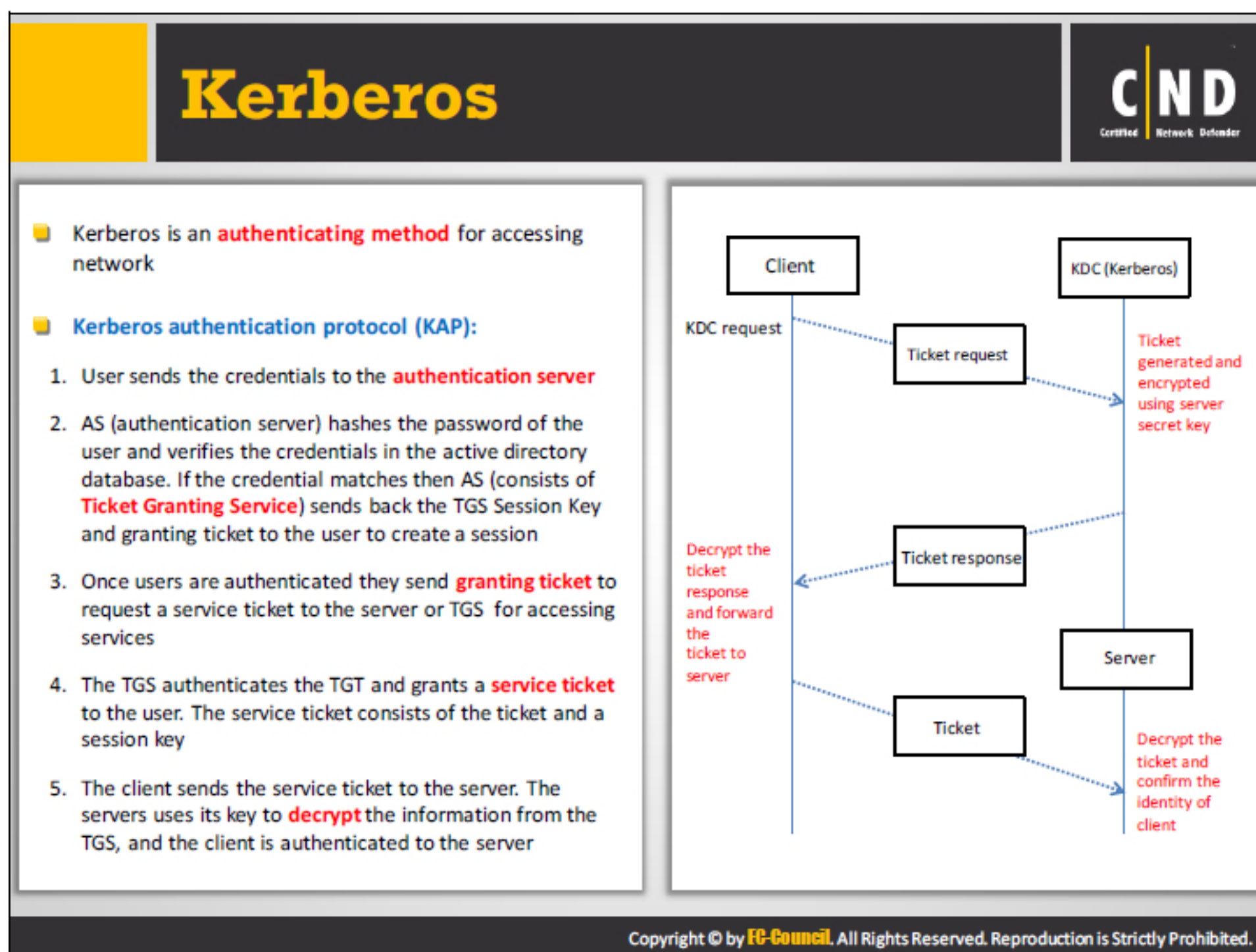


FIGURE 3.1: RADIUS vs TACACS+

RADIUS	TACACS+
Combines authentication & authorization.	Separates all 3 elements of the AAA, making it more flexible.
Encrypts only the password.	Encrypts the username and password.
Requires each network device to contain authorization configuration.	Central management for authorization configuration.
UDP- Connectionless UDP ports 1645/1646, 1812/1813	TCP- Connection oriented TCP port 49

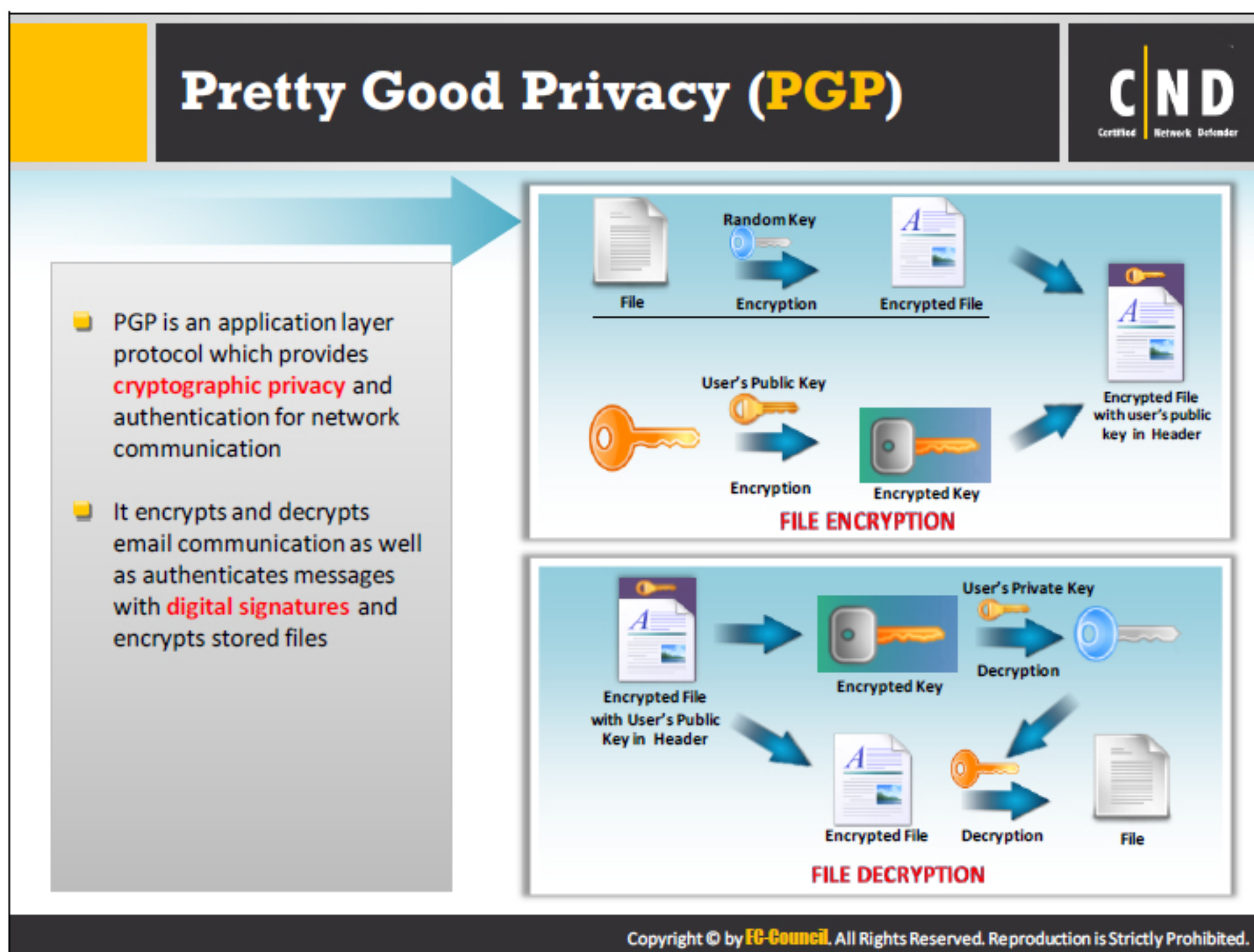
TABLE 3.1: Difference between RADIUS and TACACS+



Kerberos is a network authentication protocol for authenticating requests in computer networks. It is based on client server model, which uses an encryption technology and a “Ticket” mechanism to prove the identity of a user on a non-secure network. Kerberos protocol messages protect the network from replay attacks and eavesdropping. It commonly uses public-key cryptography while authenticating users attempting to access the server.

- **Step 1:** User sends the credentials to the authentication server.
- **Step 2:** AS (authentication server) hashes the password of the user and verifies the credentials in the active directory database. If the credential matches, then AS (consists of the Ticket Granting Service) sends back the TGS Session Key and ticket granting the ticket to the user to create a session
- **Step 3:** Once the user authenticates, they send the ticket granting the ticket to request a service ticket to the server or TGS for accessing services.
- **Step 4:** The TGS authenticates the TGT and grants a service ticket to the user. The service ticket consists of a ticket and a session key.
- **Step 5:** The client sends the service ticket to the server. The servers use its key to decrypt the information from the TGS, and the client is authenticated to the server





PGP (Pretty good privacy) is an encryption and decryption computer program that is used to provide confidentiality and validation while communication. PGP enhances the security of emails.

### How Does PGP work?

Every user has a public encryption key and a private key. Messages are sent to another user after encrypting using the public key. The receiver decrypts the message using their private key. PGP compresses the message which increases the security of the message in the network. PGP creates a session key which is used only once. PGP encrypts the message using the session key along with the encryption algorithm. The session key encrypted by the recipient's public key. The public key encrypted session key is sent to the recipient along with the encrypted message. Recipient uses their private key to decrypt the session key and to decrypt the entire message.

There are two versions of PGP:

- Rivest- Shamir-Adleman Algorithm
- Diffie-Hellman Algorithm

PGP creates a hash code from the user's name and signature to encrypt the sender's private key. The receiver uses the sender's public key to decrypt the hash code.

## S/MIME



S/MIME (Secure/Multipurpose Internet Mail Extensions) is an application layer protocol which is used to send **digitally signed** and **encrypted email messages**



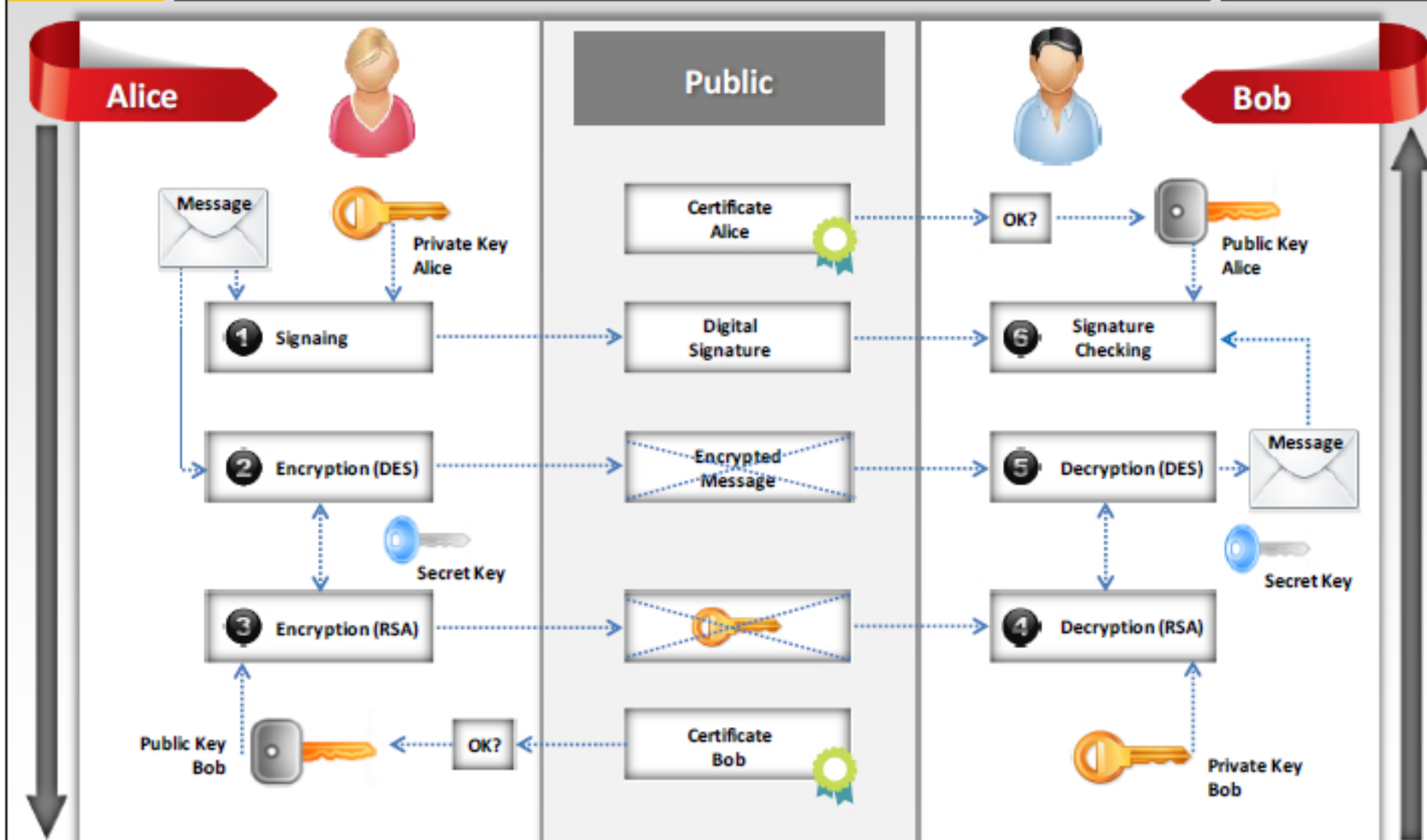
It uses the Rivest-Shamir-Adleman encryption (**RSA**) system for email encryption



Administrators need to **enable** S/MIME-based security for mailboxes in their organizations

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## How it Works



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Difference between PGP and S/MIME		
Mandatory Features	S/MIME v3	OpenPGP
Message Format	Binary, Based on CMS	Application/Pkcs 7-mime
Certificate Format	Binary, Based on X.509v3	Binary, Based on previous PGP
Symmetric Encryption Algorithm	Triple DES (DES, EDE3, CBC)	Triple DES (DES, EDE3, Eccentric CFB)
Signature Algorithm	Diffie-Hellman (X9.42) with DSS or RSA	ElGamal with DSS
Hash Algorithm	SHA- 1	SHA- 1
MIME Encapsulation of Signed Data	Choice of Multipart/signed or CMS Format	Multipart/signed ASCII armor
MIME Encapsulation of Encrypted Data	Application/Pkcs 7-mime	Multipart/Encrypted

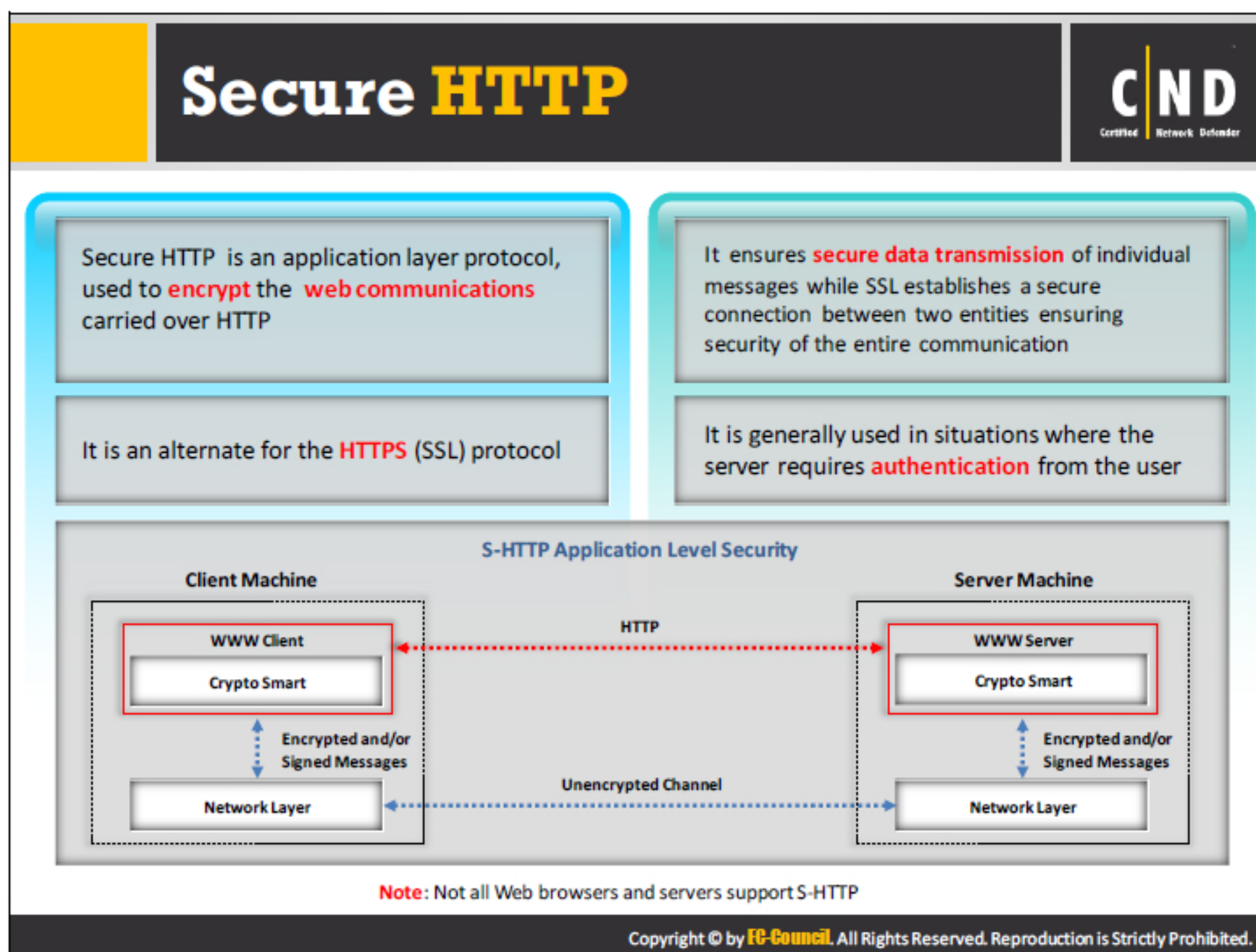
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

S/MIME is used to send digitally signed and encrypted messages. It allows you to encrypt the email messages and then digitally sign them to ensure confidentiality, integrity and non-repudiation for messages. It provides cryptographic security services such as:

- Authentication
- Message Integrity
- Non-Repudiation
- Privacy
- Data Security

S/MIME ensures e-mail security and has been included in the latest versions of browsers. It uses a RSA encryption method and provides details regarding including encryption and digital signatures in the message.


S/MIME protocol needs to ensure that it gains a certificate from the CA or from a public CA. The protocol uses different private keys for signature and for encryption.



Secure HTTP ensures a secured interchange of data on the World Wide Web. It implements application level security that offers encryption and digital signatures on the message. S-HTTP verifies the user by using a certificate. S-HTTP provides many cryptographic algorithms and modes of operations. The S-HTTP protocol uses client-server protocol to determine the security conditions for a client-server communication. It allows the client to send a certificate in order to authenticate a user. There are many web servers that support the S-HTTP protocol that allows them to communicate without the need for any encryption.

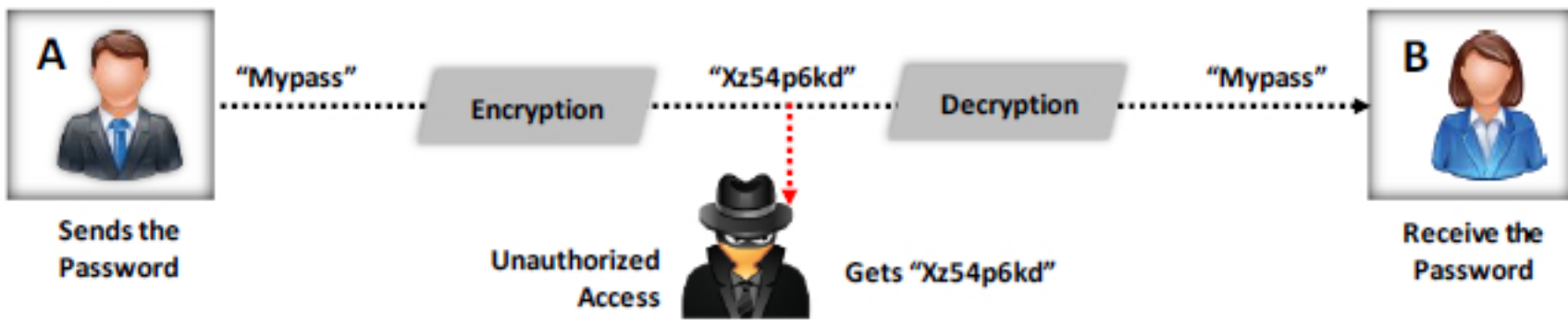


# Hyper Text Transfer Protocol Secure (HTTPS)



- HTTPS ensures **secure communication** between two computers over HTTP
- The connection is **encrypted** using Transport Layer Security (TLS) or Secure Sockets Layer(SSL) protocol
- It is often used in **confidential online transactions**
- It protects against **man-in-the-middle attacks** as data is transmitted over encrypted channel

### How it works



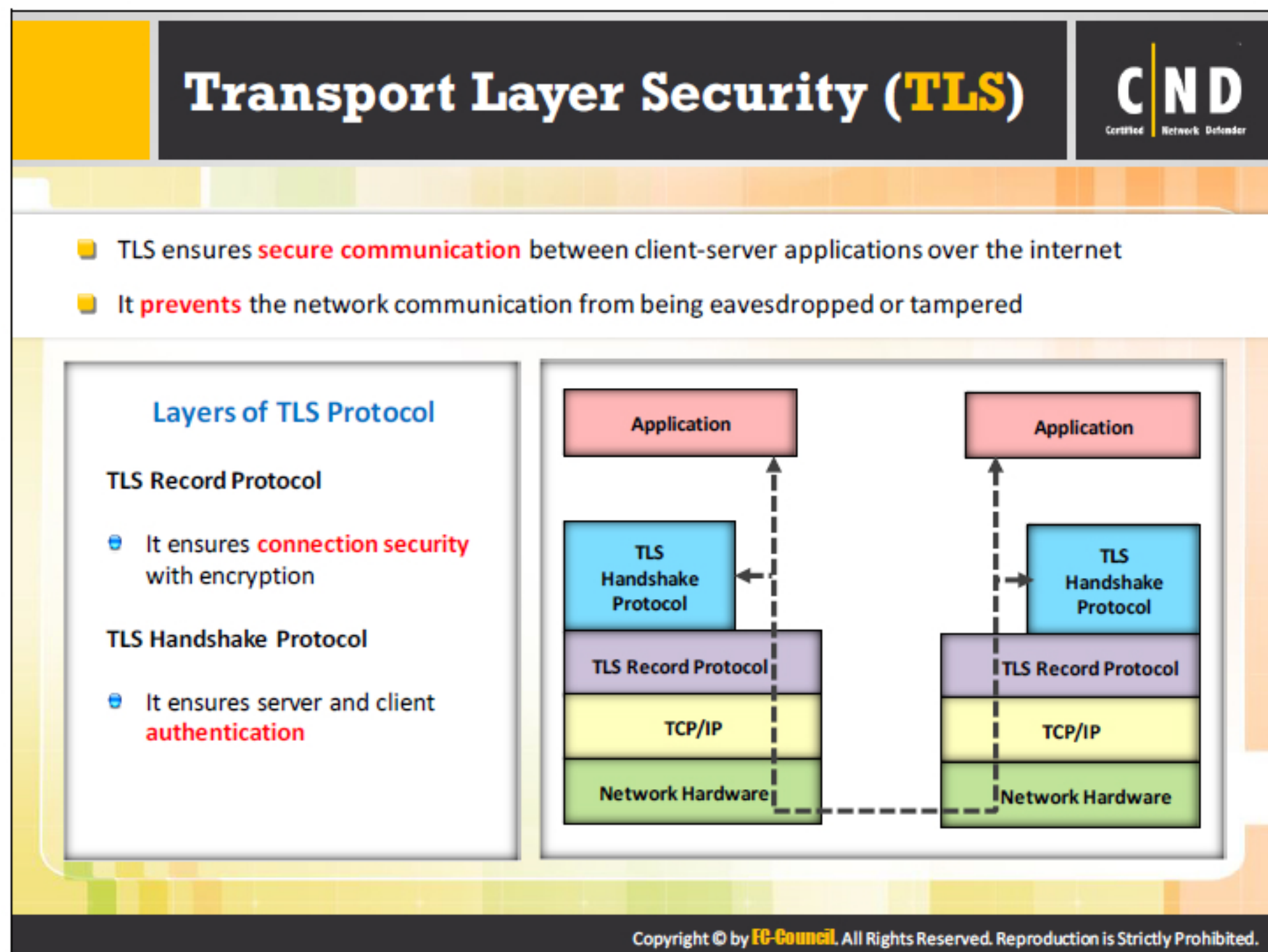
The diagram illustrates the HTTPS process. On the left, a person labeled 'A' sends the password 'Mypass' to an 'Encryption' box. The output of the encryption box is 'Xz54p6kd'. An 'Unauthorized Access' character (a man in a hat) is shown intercepting this encrypted data. The 'Xz54p6kd' then passes through a 'Decryption' box, which outputs 'Mypass' to a person labeled 'B' on the right. Person B is labeled 'Receive the Password'.

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

It is a protocol used to ensure secure communication in the network. It uses protocols such as TLS (Transport layer security) and Secure Sockets Layer (SSL) to ensure secure transmission of data. HTTPS confirms the verification of the websites and preserves the confidentiality and reliability of the messages passed over the Internet.

HTTPS mainly uses SSL in order to protect the website making it easier for users to access the website. SSL has the following advantages:

- Encrypts confidential information during exchange of data.
- Maintains a record of the details regarding the certificate owner.
- A certificate authority checks the owner of the certificate while issuing it.

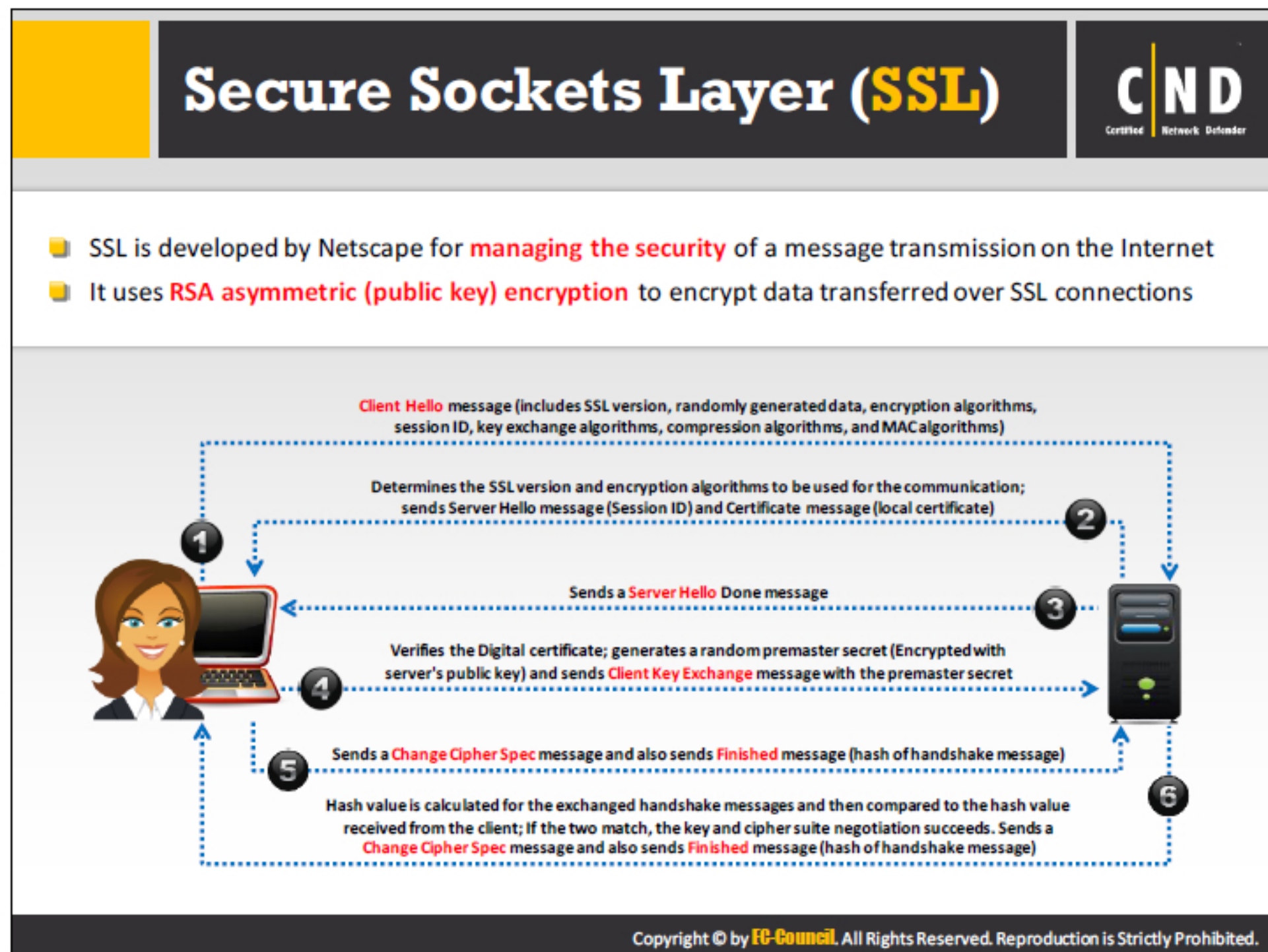


TLS provides secure communication of data in addition to confidentiality and reliability between the communicating parties.

A secure TLS connection includes the following properties:

- Ensured confidentiality and reliability of data during communication between client and server using symmetric cryptography.
- Authenticate communication applications using public key cryptography.
- Authentication codes can maintain the reliability of the data.
- TLS consists of two protocols:
  - **TLS Record Protocol:** Provides security using encryption method.
  - **TLS Handshake Protocol:** Provides security using authentication of client and server before communication.





The Secure Sockets Layer (SSL) is a protocol used to provide a secure authentication mechanism between two communicating applications, such as a client and a server. The SSL requires a reliable transport protocol, such as TCP, for data transmission and reception.

Any application-layer protocol that is higher than SSL, such as HTTP, FTP, and telnet, can form a transparent layer over the SSL. SSL acts as an arbitrator between the encryption algorithm and session key; it also verifies the destination server prior to the transmission and reception of data. The SSL encrypts the complete data of the application protocol to ensure security.


The SSL protocol also offers “**channel security**” with three basic properties:

- **Private channel:** All the messages are encrypted after a simple handshake is used to define a secret key.
- **Authenticated channel:** The server endpoint of the conversation is always encrypted, whereas the client endpoint is optionally authenticated.
- **Reliable channel:** message transfer has an integrity check.

SSL uses both asymmetric and symmetric authentication mechanisms. Public-key encryption verifies the identities of the server, the client, or both. Once authentication has taken place, the client and server can create symmetric keys allowing them to communicate and transfer data rapidly. An SSL session is responsible for carrying out the SSL handshake protocol to organize the states of the server and clients, thus ensuring the consistency of the protocol.

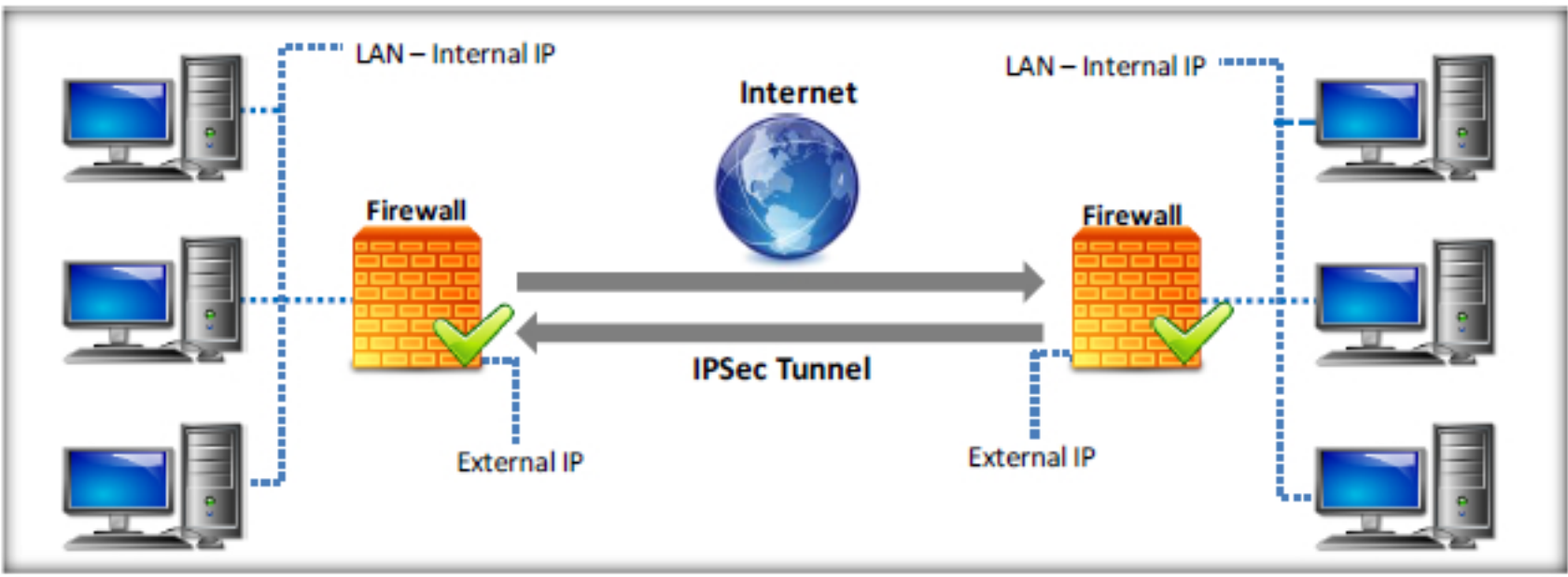


## Internet Protocol Security (IPsec)



- IPsec is a network layer protocol that ensures **secure Internet Protocol (IP)** level communication
- It provides **end-to-end security** at the Internet Layer of the Internet Protocol Suite

- It **encrypts** and **authenticates** each IP packet in the communication
- It **supports** network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection



The diagram illustrates an IPsec Tunnel setup between two networks. On the left, a LAN with three desktop computers is connected to a Firewall. The LAN is labeled 'LAN - Internal IP' and the Firewall is labeled 'External IP'. On the right, another LAN with three desktop computers is connected to another Firewall, also labeled 'LAN - Internal IP' and 'External IP'. A double-headed arrow labeled 'IPSec Tunnel' connects the two Firewalls. Above the tunnel, a globe icon represents the 'Internet'. Green checkmarks are placed on the Firewall icons, indicating successful authentication or encryption.

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.


IPsec ensures secure communications over the Internet Protocol (IP) network. It works at the application layer of the communications model. It makes use of cryptographic security services to ensure secure communication. It allows authenticating the IP packets during communication of data. IPsec finds its applications in Virtual Private Networks and remote user access. IPsec is used between a pair of hosts, a pair of security gateways, or between a security gateway and a host. The IPsec consists of two security services: Authentication Header (AH) and Encapsulating Security payload (ESP). The AH allows authentication of the sender, whereas the ESP allows authentication of the sender as well as encryption of the data.

It provides secure communication for network-level peer authentication, data origin authentication and ensures data integrity, data confidentiality (encryption), and replay protection


IPsec consists of two encryption modes, namely Transport and Tunnel:


- In Transport mode, data portion or the payload is encrypted.
- In Tunnel mode, the entire IP is encrypted.





# Module Summary





- ☐ A completely secure and robust network can be designed with the proper implementation and configuration of network security elements
- ☐ Network Access Control protects the network by restricting the connection of an end user to the network based upon a security policy
- ☐ Administrators are responsible for assigning privileges to prevent the risks of information security incidents and to achieve better system stability and system security in enterprises
- ☐ Network security policies define the rules of behaviors for access and the use of network resources of the an organization
- ☐ Network security devices and protocols help minimize security risks on the network

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

In this module, you were introduced to various security features such as network controls, protocols, and devices used to ensure the security of the network. The combined use of these elements helps organizations to attain confidentiality, integrity, and availability of their network. An administrator should consider designing and configuring an organization's security policies, firewall, IDS, VPN, and other security features to attain defense in depth security in the network. The design and implementation of these security features are discussed in the next modules individually.