Secure Firewall Configuration and Management

Module 07

Secure Firewall Configuration and Management

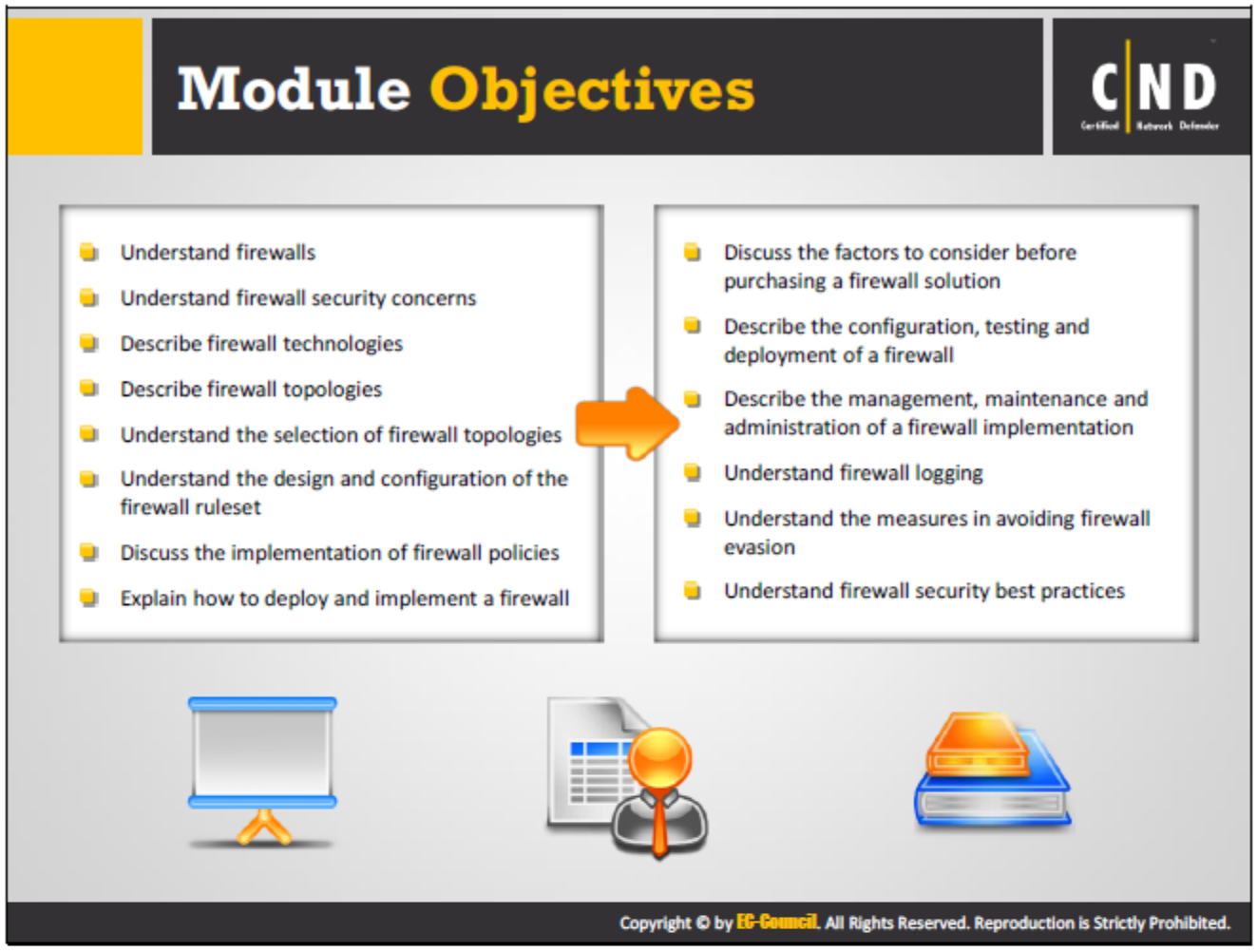
Module 07

C|N D
Certified Network Defender

Certified Network Defender

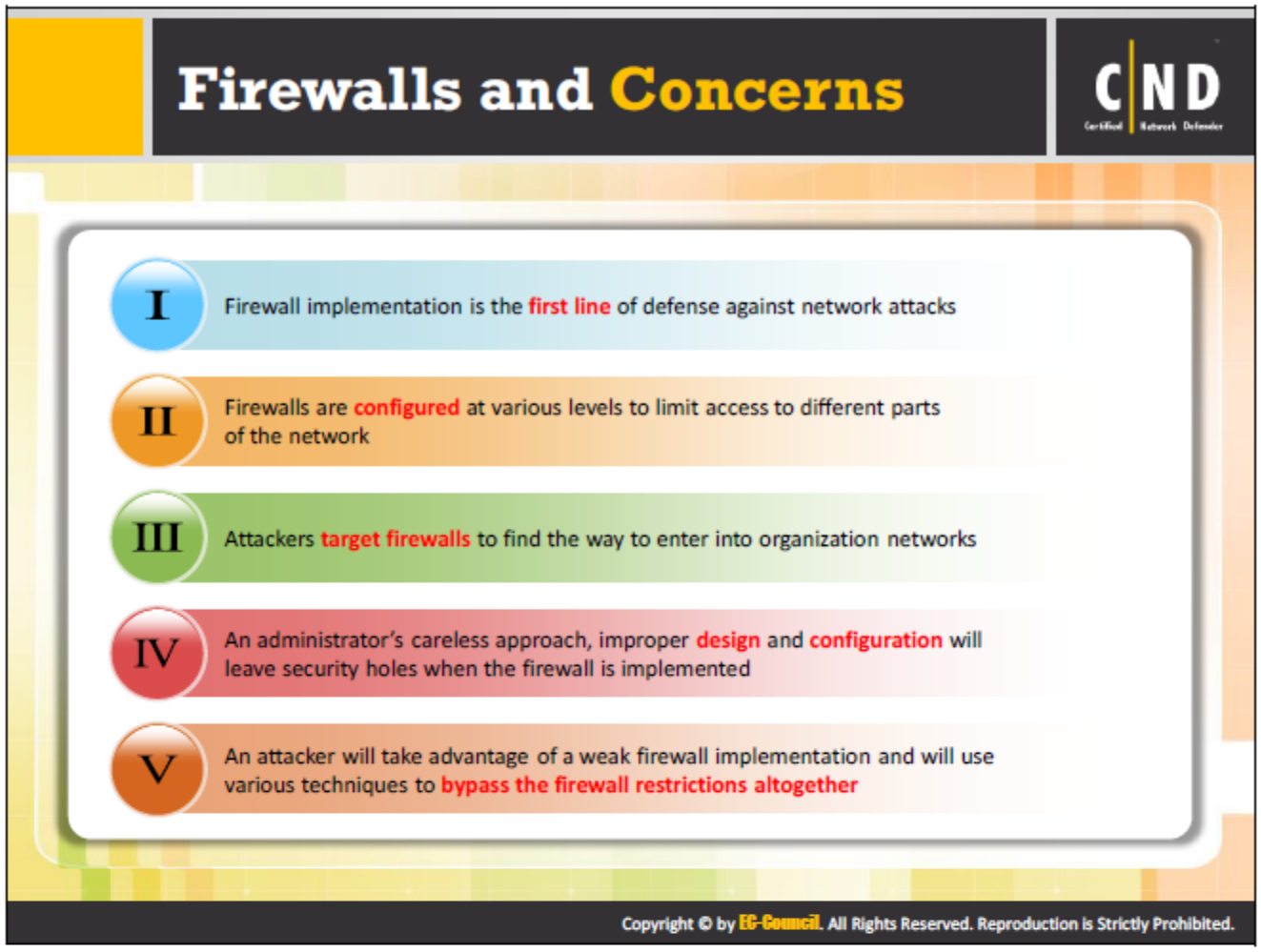
Module 07: Secure Firewall Configuration and Management

Exam 312-38



A firewall is the first line of defense for an organization's network. It plays a vital role in securing the link between their networks and the internet in today's connected world. It acts as a gateway or as a filtering device employing the network security policy and protects the network against external attacks. However, improper configuration and implementation of a firewall will diminish its ability to defend an organization's network.

This module focuses on firewall configuration and management, where you will learn the fundamental concepts of firewalls, the importance of implementing firewalls, different types of firewalls, firewall topologies, firewall implementation, firewall administration, firewall anti-evasion techniques and firewall best practices.

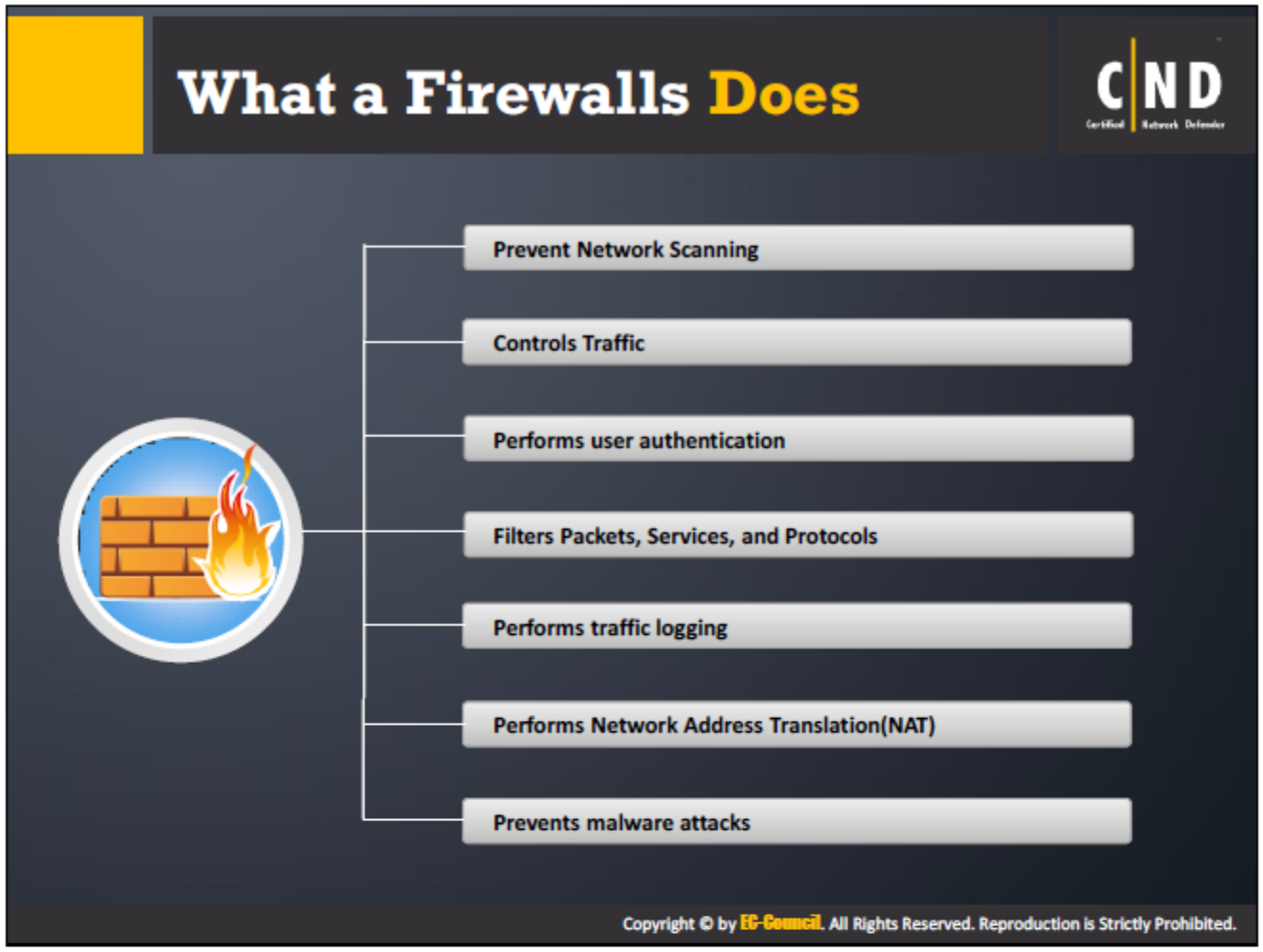


A firewall is a hardware device or a software program located at the network gateway server and used for secure communication between different networks according to a specified security policy. Networks have firewalls configured between the corporate and public network (internet). A firewall provides a line of defense, against attacks on an internal network from an external network. It helps prevent unauthorized access to or from private networks connected to the internet. A firewall application runs on a host that is connected to both trusted and untrusted networks.

A firewall helps organizations protect confidential information from unauthorized users. The most important feature of the firewall is that it can distinguish between good and bad traffic. A firewall placed between a corporate and a public network limits the access to various services on the internet. It also keeps track of what is going through the firewall. The firewall filters inbound traffic, known as ingress filtering and outbound traffic known as egress filtering.

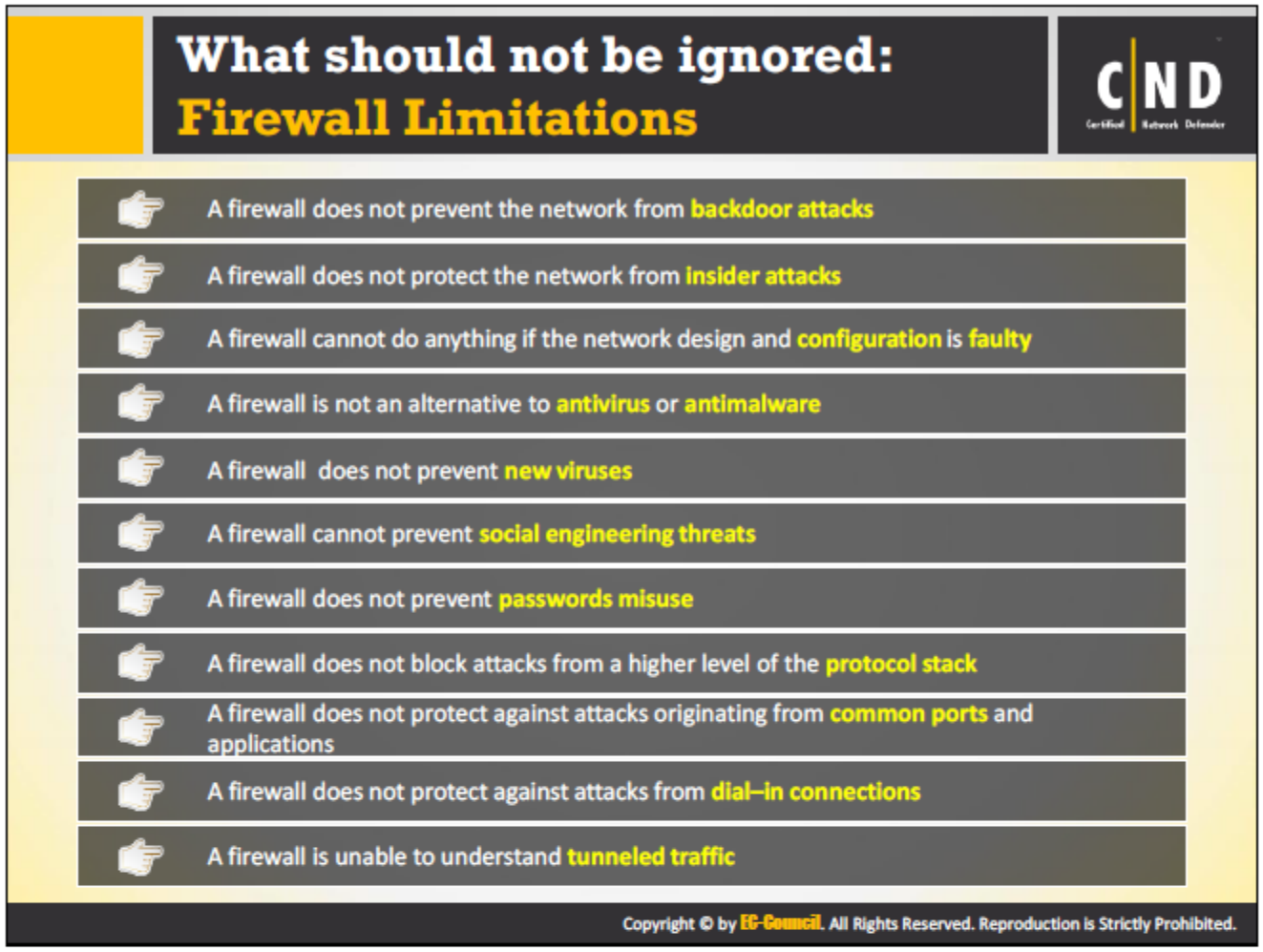
However, there are a few concerns with firewall functionality and they are:

- A firewall cannot block certain types of attacks. For example, social engineering, insider attacks, etc.
- Firewalls sometimes have less computing speed than their network interface. This can create a problem when a host with a network interface is faster than the firewalls internal processor.
- Firewalls can restrict certain services that the user wants. The services include: TELNET, FTP, X Windows, NFS, etc.
- Firewalls can restrict the communication between valid devices in the network thereby causing unwanted interruption in the flow of data.



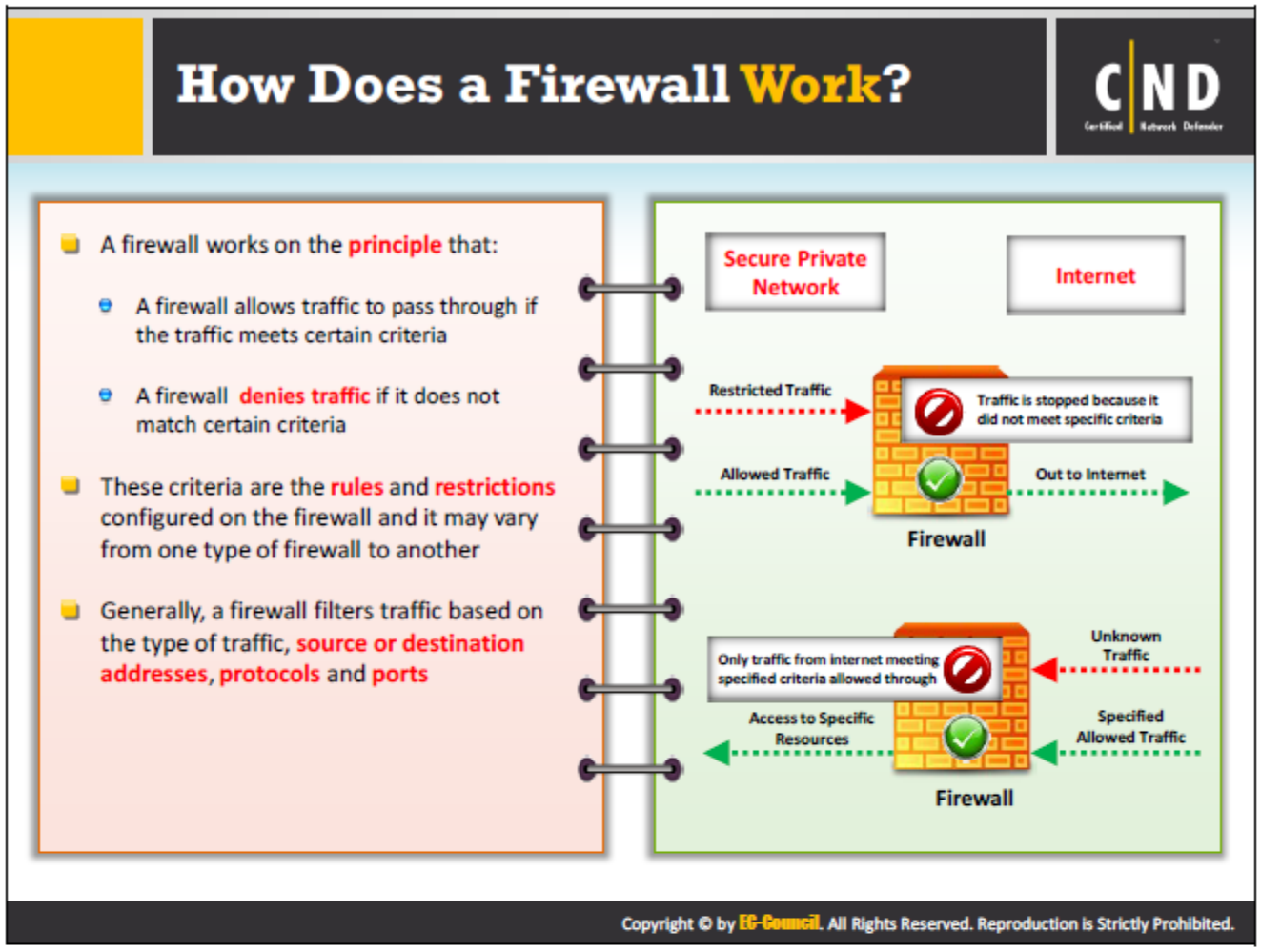
A firewall performs the following functions to protect the network from various types of threats.

- A firewall examines all the traffic flowing through it to see if it meets the firewall rule set criteria.
- It blocks identified packets between the networks that are matched to a deny rule.
- It filters both inbound and outbound traffic.
- It examines each packet passing through the network and decides whether to send the packet to the destination or not.
- It manages public access to private networked resources such as host applications.
- It logs all attempts to enter the private network and triggers alarms when hostile or unauthorized entry is attempted.
- Firewalls work as filters and help in preventing unsafe packet flow into the private network.
- The functions of the firewall include gateway defense, carrying out defined security policies, hiding and protecting internal network addresses, reporting threats and activity, and segregating activity between trusted networks.



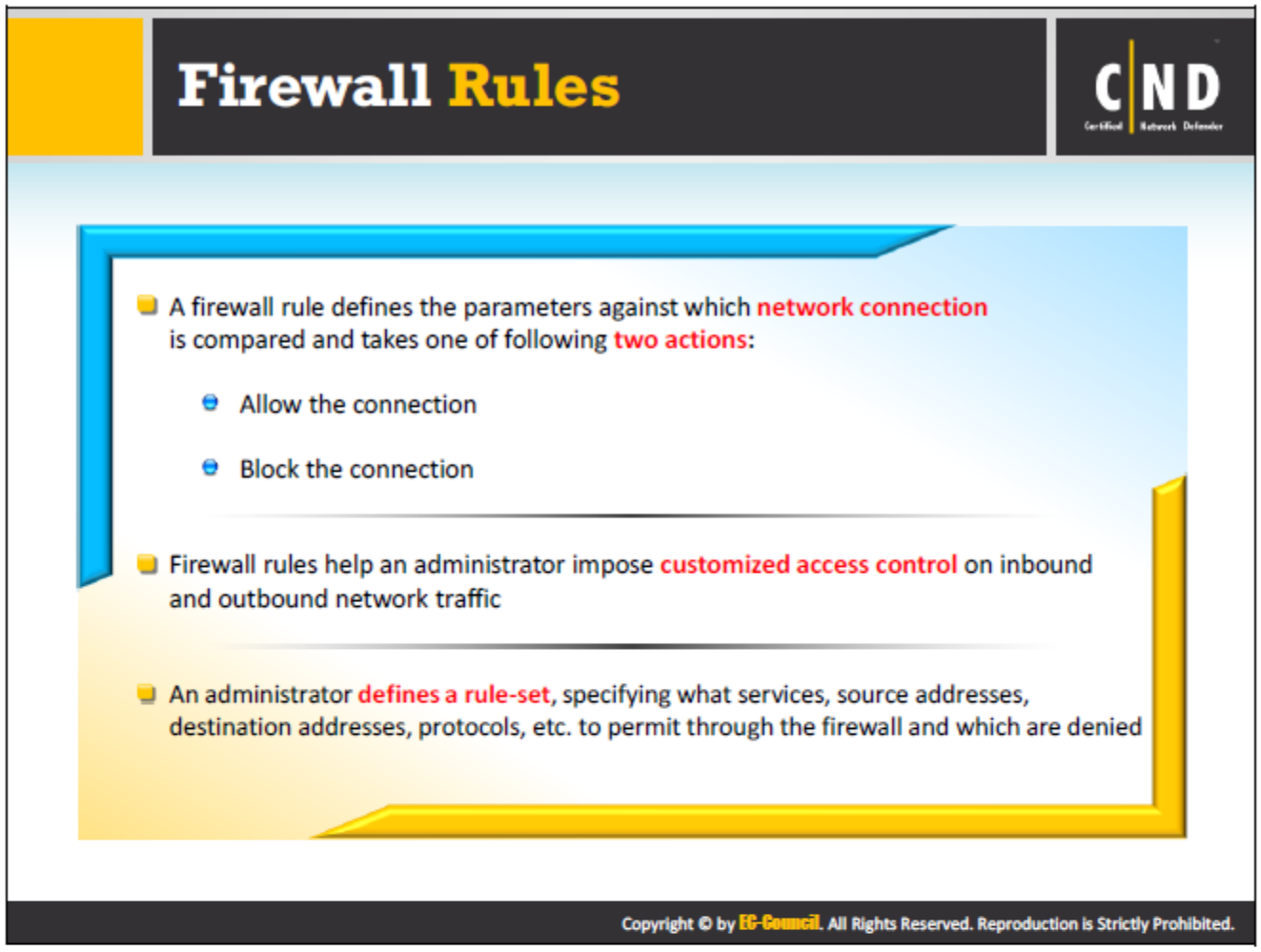
The need of a firewall in your security strategy is important, but firewalls have the following limitations:

- Firewalls can restrict users from accessing valuable services like FTP, Telnet, NIS, etc. and sometimes restricts Internet access as well.
- The firewall cannot protect you from internal attacks (backdoor) in a network. For example, a disgruntled employee who cooperates with the external attacker.
- The firewall concentrates its security at one single point which makes other systems within the network prone to security attacks.
- A bottleneck could occur if all the connections pass through the firewall.
- The firewall cannot protect the network from social engineering and data-driven attacks where the attacker sends malicious links and emails to employees inside the network.
- If external devices such as a laptop, mobile phone, portable hard drive, etc. are already infected and connected to the network, then a firewall cannot protect the network from these devices.
- The firewall is unable to fully protect the network from all types of zero day viruses that try to bypass it.



A firewall monitors the incoming and outgoing traffic of the network or a system and blocks the traffic that does not meet the specified security criteria. The security criteria of the network has a set of predefined rules. A firewall monitors all the traffic and allows good data generally known as permitted traffic and blocks suspect data also known as denied traffic. A firewall filters traffic using various methods such as packet filtering, proxy service, stateful inspection, etc.

- A firewall filters traffic that does not meet specific criteria.
- The type of criteria defined may differ in different firewalls.
- A firewall filters traffic based on the type of traffic, source and destination addresses, source and destination ports.
- Sometimes, even a complex rule base is set on the firewall to filter application traffic.



A firewall uses one or more sets of "rules" to inspect network packets as they come in or go out of the firewall and either allows the traffic through or blocks it.

A firewall rule defines the process to inspect one or more characteristics of network packets such as the protocol type, source or destination host address and source or destination port of the network connection. The firewall takes the required action based on the network policy of the organization.

Rules of the firewall should comply with the company's goals and security policies as well as offer convenience and cater to the organizational needs for averting all threats. You should frame the guidelines for sampling the work of a firewall and updating it at scheduled intervals.

A firewall follows three basic rules in order to secure an organization's systems:

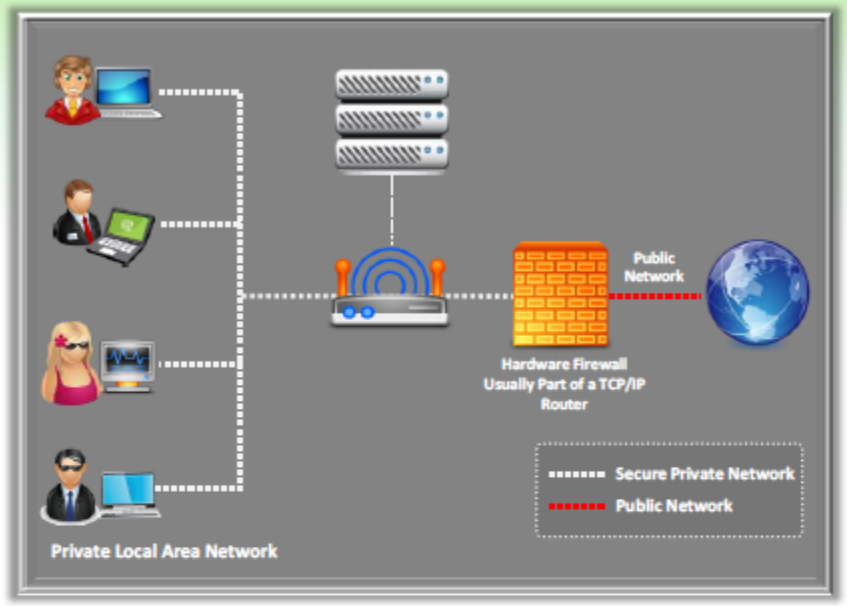
- **Allow:** A firewall allows "safe" traffic to flow that is defined by an administrator.
- **Block:** A firewall will block traffic that looks suspicious to your network.
- **Ask:** A firewall initially asks the administrator whether to allow incoming and outgoing traffic to access your organization's network resources. It also remembers your responses for future use.

With the help of firewall rules, firewalls decide which actions to be taken if the traffic coming from specific IP addresses and ports breaks the firewall rules. These firewall rules are set according to an organization's security policy.

Types of Firewalls

Hardware Firewall

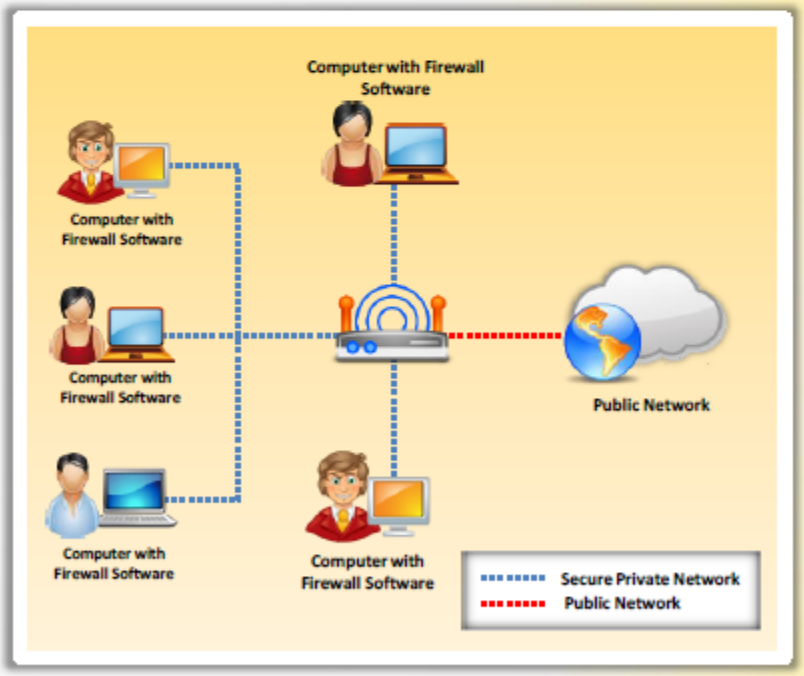
- A hardware firewall is either a dedicated stand-alone hardware device or it comes as part of a router
- Less effort is required to configure a hardware firewall
- The network traffic is filtered using the packet filtering technique
- It is used to filter out the network traffic for large business networks



Types of Firewalls (Cont'd)

Software Firewall

- A software firewall is a software program installed on a computer, just like normal software
- It provides more flexibility to customize filtering needs
- It is generally used to filter traffic for individual home users
- It only filters traffic for the computer on which it is installed, not for the network



Note: It is recommended to configure both a software and a hardware firewall for best protection

Hardware Firewall

A hardware firewall is a dedicated firewall device placed on the perimeter of the network. It is an important part of a network setup and is also built in to Broadband routers or as a stand-alone product. A hardware firewall helps protect systems on the local network and they are effective with little to no configuration. It employs a technique of packet filtering. It reads the header of a packet to find out the source and destination address and compares it with a set of predefined and/or user created rules that determine whether if it should forward or drop the packet. A hardware firewall functions on an individual system or an individual network connected using a single interface. Examples of a hardware firewall are Cisco ASA, Fortigate, etc. Hardware firewalls provide protection to the private local area network.

However, hardware firewalls are considered a more expensive option, difficult to implement and upgrade.

- **Advantages**
  - Security: An operating system with its own operating system is considered to reduce the security risks and has increased level of security controls.
  - Speed: Hardware firewalls initiate faster responses and enable more traffic.
  - Minimal Interference: Since a hardware firewall is a separate network component, it enables better management and allows the firewall to shutdown, move or be reconfigured with less interference on the network.
- **Disadvantages**
  - More expensive than a software firewall.
  - Hard to implement and configure.
  - Consumes more space and involves cabling.

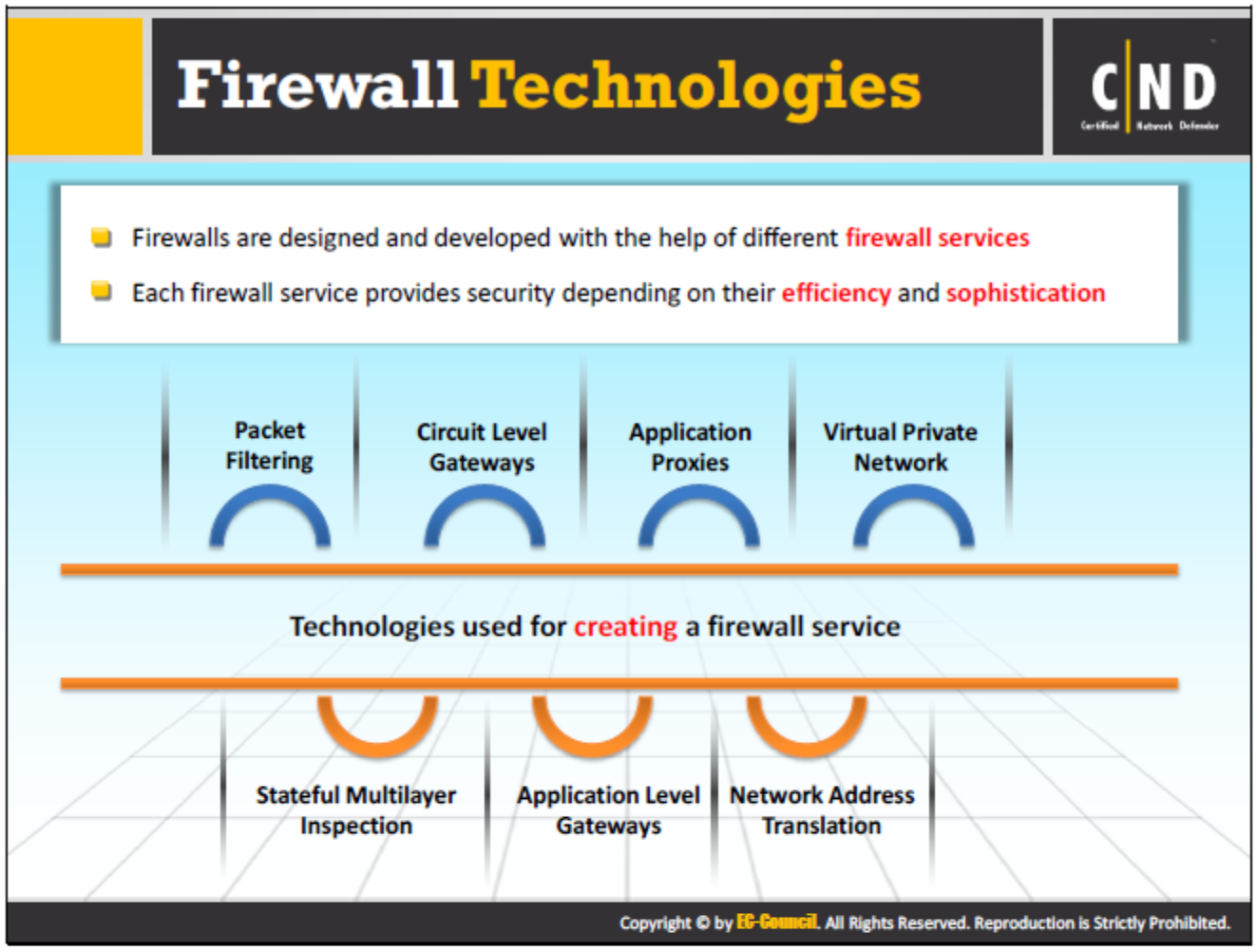
Software Firewall

A software firewall is similar to a filter. It sits between the normal application and the networking components of the operating system. It is more helpful for individual home users, is suitable for mobile users who need digital security working outside of corporate network and it is easy to install on an individual's PC, notebook, or workgroup server. It helps protect your system from outside attempts of unauthorized access and protects against common Trojans and email worms. It includes privacy controls and web filtering and more. A software firewall implants itself in the key area of the application/network path. It analyzes data flow against the rule set.

Configuration of a software firewall is simple compared to the hardware firewall. It intercepts all requests from a network to the computer to determine if they are valid and protects the computer from illicit attacks that try to access it. It incorporates user-defined controls, privacy controls, web filtering, content filtering, etc. to restrict unsafe applications from running on an individual system. Software firewalls utilize more resources and this reduces the speed of your

system. Examples of software firewalls are produced by Norton, McAfee and Kaspersky among others.

- **Advantages**
  - Less expensive than hardware firewalls.
  - Ideal for personal or home use.
  - Easier to configure and reconfigure.
- **Disadvantages**
  - Consumes system resources.
  - Difficult to un-install firewalls.
  - Not appropriate for environments requiring faster response times.



Several firewall technologies are available for organizations to implement their security through. Sometimes, firewall technologies are combined with other technologies to build another firewall technology. For example, NAT is a routing technology but when combined with a firewall, it is considered a firewall technology instead.

The various firewall technologies used are:

- Packet Filtering
- Stateful Multilayer Inspection
- Circuit Level Gateways
- Application Level Gateways
- Application Proxies
- Network Address Translation
- Virtual Private Network

The table below describes technologies working at each OSI layer:

OSI Layer	Firewall Technology
Application	Virtual private Network (VPN) Application Proxies
Presentation	VPN
Session	VPN Circuit-level gateway
Transport	VPN Packet Filtering
Network	VPN Network Address Translation (NAT) Packet Filtering Stateful Multilayer Inspection
Data Link	VPN Packet Filtering
Physical	Not Applicable

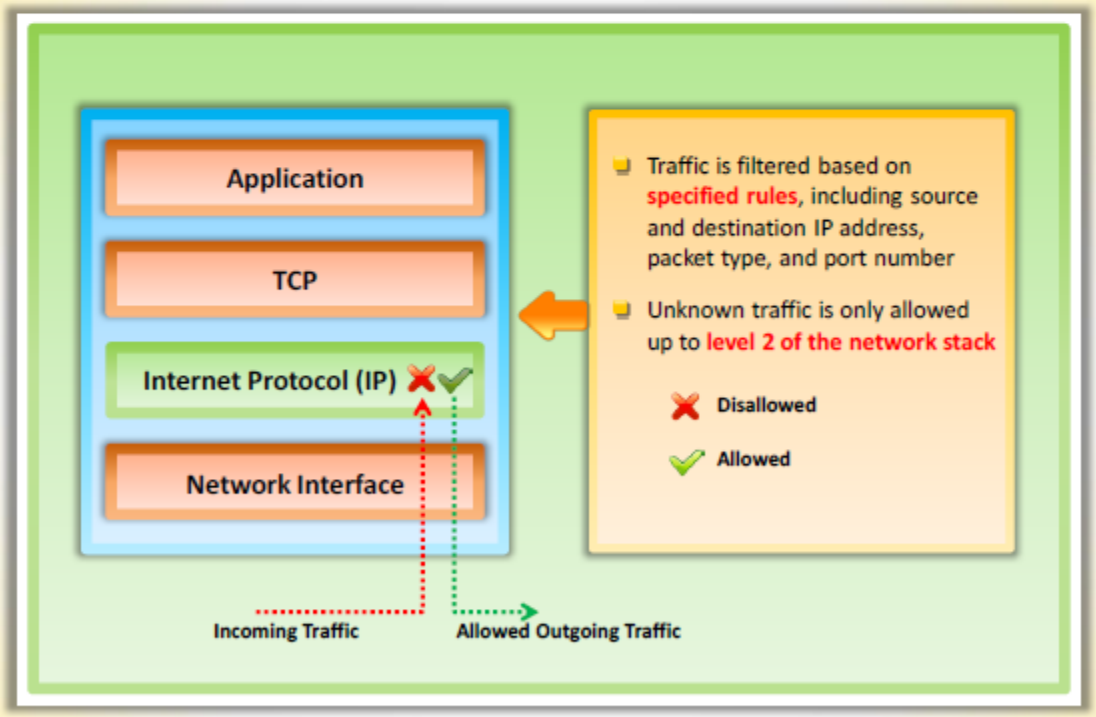
TABLE 7.1: Firewall technologies at OSI layer

The security level of these technologies varies according to the efficiency level of each technology. A comparison of these technologies can be concluded by allowing these technologies to pass through the OSI layer between the hosts. The data passes through the intermediate layers from a higher layer to a lower layer. Each layer adds additional information to the data packets. The lower layer now sends the obtained information through the physical network to the upper layers and thereafter to its destination.

Packet Filtering Firewall

- Packet filtering firewalls work at the network level of the OSI model (or the IP layer of TCP/IP)
- They are usually part of a router
- In a packet filtering firewall, each packet is compared to a set of criteria before it is forwarded
- Depending on the packet and the criteria, the firewall can:
  - Drop the packet
  - Forward it or send a message to the originator
- Rules include the source and destination IP addresses, source and destination port number and the protocol used
- The advantage of packet filtering firewalls is their low cost and low impact on network performance
- Most routers support packet filtering

Packet Filtering Firewall (Cont'd)



Packet filtering is the most basic core feature of all modern firewalls. They work at the network layer and are usually part of a router. A packet filtering firewall evaluates each packet on the basis of the packet header information including: source IP address, destination IP address, source port, destination port, protocol etc. If the criteria don't match, the firewall drops the packet or else forwards it. Rules can include source and destination IP address, source and destination port number, and protocol used. When a data packet passes through the network, a packet filter checks the packet header and compares it with the connection bypass table that keeps a log of the connections passing through the network.

There are three methods available for configuring packet filters after determining the set of filtering rules:

- **Rule 1**: This rule states that it accepts only those packets that are safe thereby dropping the rest.
- **Rule 2**: This rule states that the filter drops only those packets that are confirmed unsafe.
- **Rule 3**: This rule states that, if there are no specific instructions provided for any particular packet, then the user is given the chance to decide on what to do with the packet.

A network packet can pass through the network by entering the previously established connection. If a new packet enters the network, it verifies the packets and checks if the new packet follows/meets the rules. It then forwards the packet to the network and enters the new data packet entry of the connection in the bypass table. A packet filtering firewall does not cost very much and doesn't affect the network performance. Most routers support packet filtering. Packet filtering is a relatively low level security which can be bypassed by techniques such as packet spoofing, where the attacker crafts or replaces packet headers which are then unfiltered by the firewall.

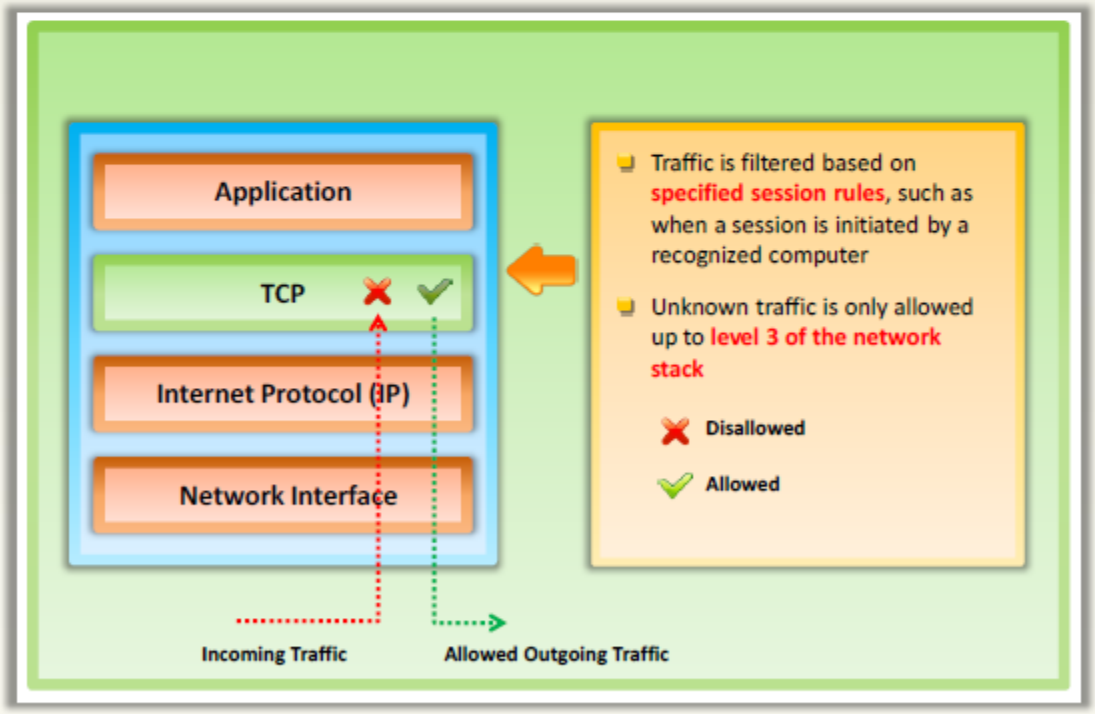
As you can tell from their name, packet filter-based firewalls concentrate on individual packets and analyze their header information as well as the directed path. Traditional packet filters make the decision based on the following information:

- **Source IP address:** This allows the user to check if the packet is coming from a valid source or not. IP header stores the information about the source of a packet and the address refers to the source system address.
- **Destination IP address:** It checks if the packet is heading towards the correct destination, while the IP header of the packet stores the destination address of the packet.
- **Source TCP/UDP port:** This allows checking the source port of the packet.
- **Destination TCP/UDP port:** The port checks and verifies the destination port to allow or deny the services.
- **TCP code bits:** Used to check whether the packet has a SYN, ACK, or other bits set for connecting.
- **Protocol in use:** Packets carry protocols, and this field checks the protocols and decides to allow or deny the related packets.
- **Direction:** Check whether the packet is coming from a packet filter firewall or leaving it.
- **Interface:** Used to check whether the packet is coming from an unreliable site.

Circuit Level Gateway

- Circuit level gateways work at the **session layer** of the OSI model, or the TCP layer of TCP/IP
- They monitor the TCP handshake between packets to determine whether a requested session is **legitimate or not**
- Information passed to a remote computer through a circuit level gateway appears to have originated from the **gateway**
- Circuit level gateways are relatively **inexpensive**
- They have the advantage of hiding information about the **private network** they protect
- Circuit level gateways do not filter **individual packets**

Circuit Level Gateway (Cont'd)



The circuit level gateway firewall uses the data present in the headers of the data packets to perform this action. It is not a stand-alone firewall, but it works in coordination with other firewalls like packet filter and application proxy to perform its functions. Information passed to a remote computer through a circuit level gateway appears to have originated from the gateway. They have the ability to hide the information of network they protect. Circuit level gateways are relatively inexpensive.

If one system wants to view information on the other system, then it sends a request to the second system and the Circuit level gateway firewall intercepts this request. The firewall forwards the packet to the recipient system with a different address. After the first system receives the reply, the firewall checks if the reply matches with the IP address of the initial system. If the reply matches, the firewall forwards the packet, otherwise it will drop the packet.

Advantages

- Private network data hiding.
- Exemption of filtering individual packets.
- Does not require a separate proxy server for each application.
- Easy to implement.

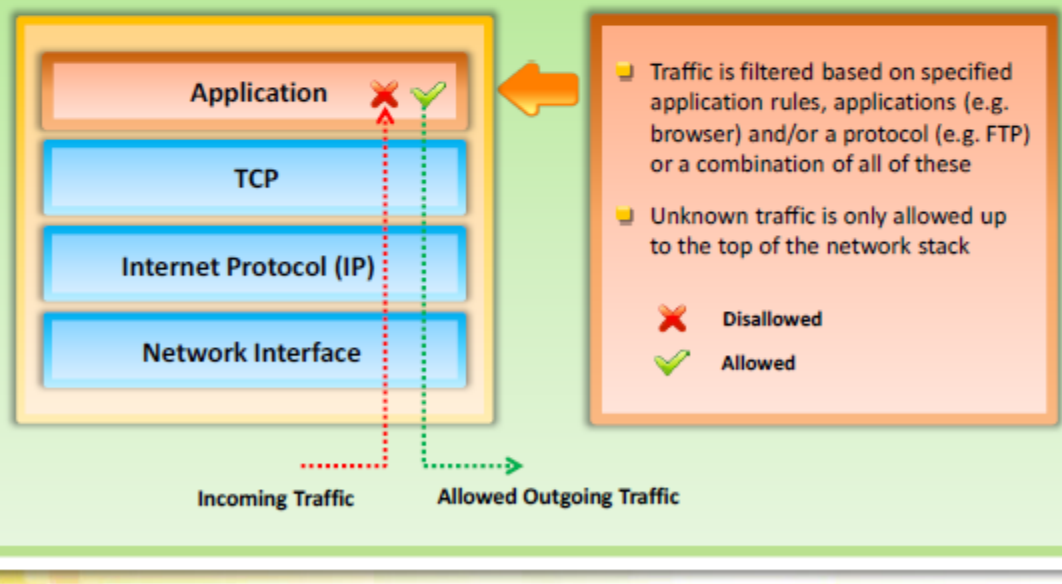
Disadvantages

- Inability to scan the active content.
- Able to handle only TCP connections.

Application Level Firewall

- Application level gateways are also called proxies
- They can filter packets at the application layer of the OSI model
- Incoming or outgoing packets cannot access services for which there is no proxy
- In plain terms, an application level gateway that is configured to be a web proxy will not allow any FTP, gopher, Telnet, or other traffic through
- Because they examine packets at the application layer, they can filter application-specific commands such as http:post and get

Application Level Firewall (Cont'd)



An application level firewall is a firewall that controls input, output, and/or access across an application or service. It monitors and possibly blocks the input, output, or system service calls, which do not meet the policy of the firewall. Before allowing the connection, it evaluates the network packets for valid data at the application layer of the firewall. The client and server communication does not happen directly, but happens only through a proxy server. This server acts as a gateway for two side communications and drops the data packets acting against the firewall's rules.

- Application level gateways, also called proxies, concentrate on the Application layer rather than just the packets.
- They perform packet filtering at the application layer and make decisions about whether or not to transmit the packets.
- A proxy-based firewall asks for authentication to pass the packets as it works at the Application layer.
- Incoming or outgoing packets cannot access services for which there is no proxy. In plain terms, design of an application level gateway helps it to act as a web proxy and drop packets such as FTP, gopher, Telnet, or any other traffic that should not be allowed to pass through.
- As packet filtering is performed at the application level, they are able to filter application-specific commands such as GET or POST requests.
- A content caching proxy optimizes performance by caching frequently accessed information instead of sending new requests for repetitive data transfers to the servers.

The application level firewall checks for those packets that do not comply with the filtration rules. The unauthorized packets are dropped and authorized packets are forwarded to the application layer of the destination.

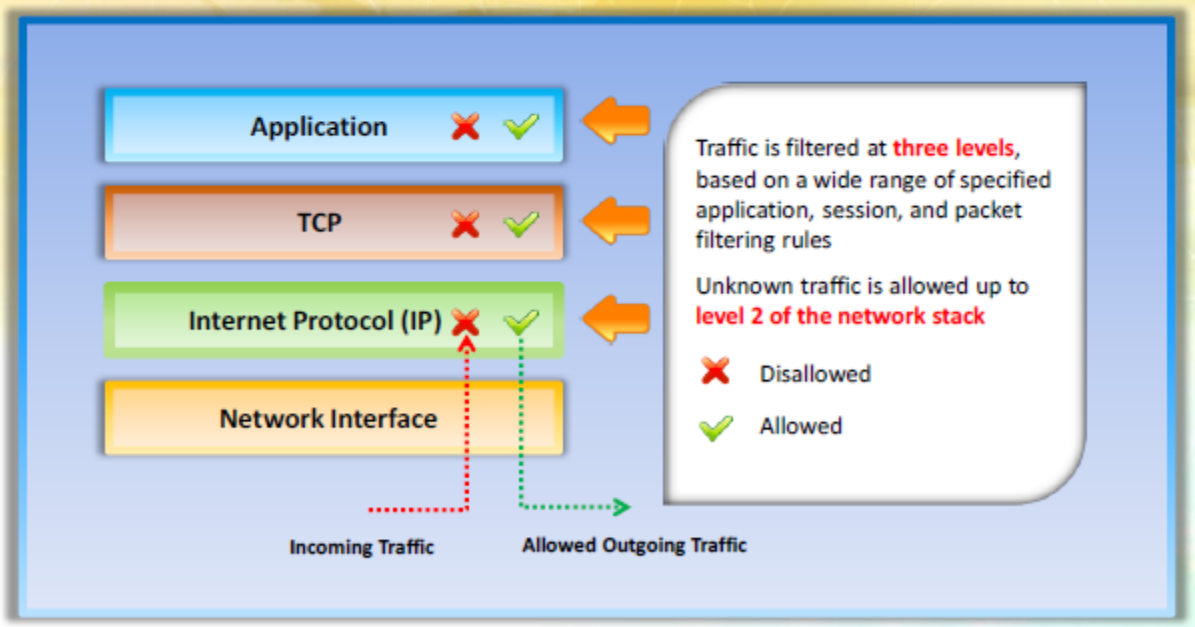
Stateful Multilayer Inspection Firewall

- A stateful multilayer inspection firewall **combines the aspects** of the other three types

- They filter packets at the network layer, determine whether **session packets** are **legitimate** and evaluate the contents of packets at the **application layer**

- They are **expensive** and require competent personnel to administer the device

Multilayer Inspection Firewall

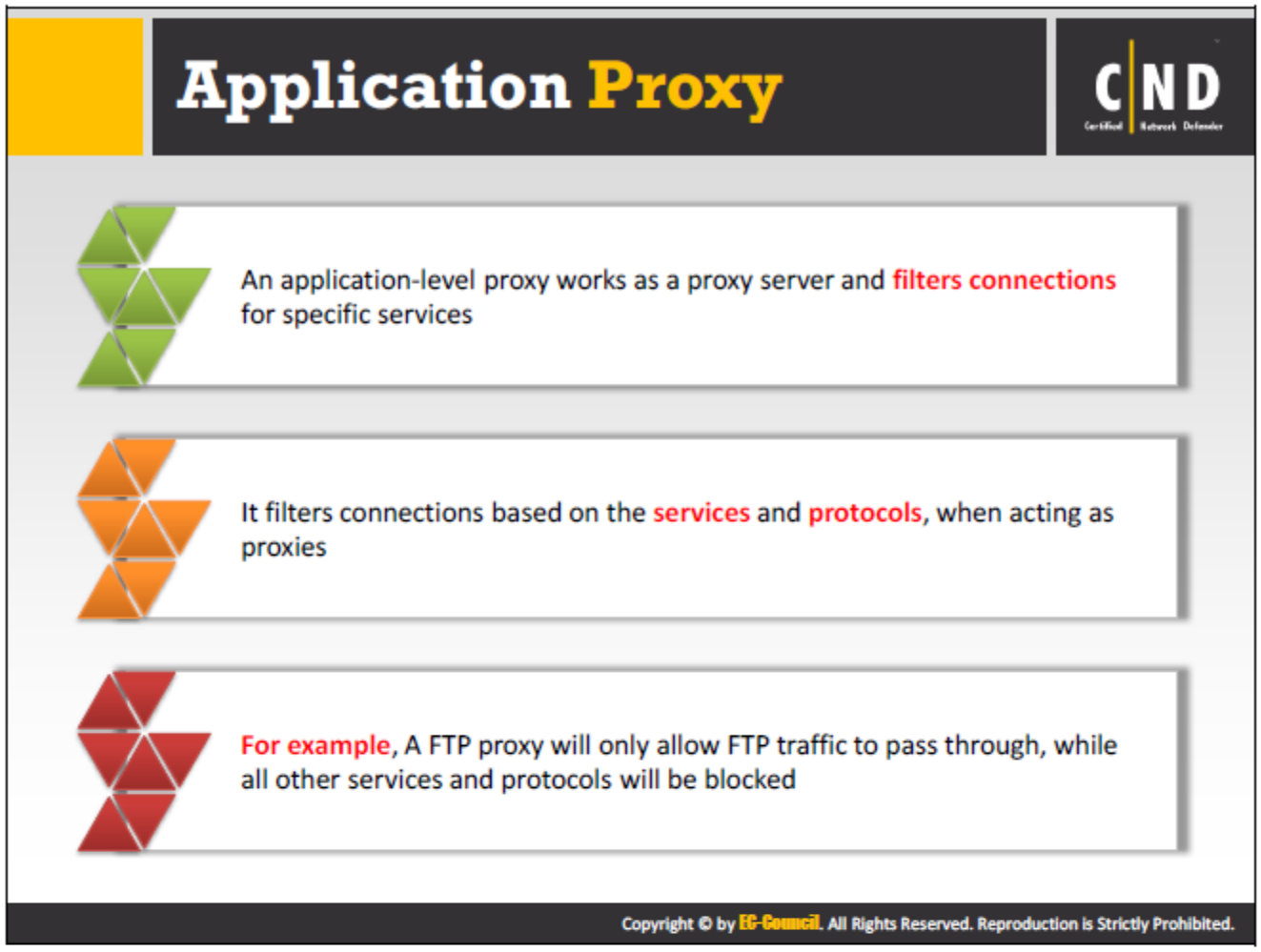


Stateful multilayer inspection firewalls combine the aspects of the other three types of firewalls. They filter packets at the network layer, determine whether session packets are legitimate, and evaluate contents of packets at the application layer. They are expensive and require competent personnel to administer the device. The packet filter firewall overcomes its inability to check the packet headers using stateful packet filtering.

It eliminates the lack of transparency of application level gateways as it allows direct connection between client and host. These firewalls use algorithms to examine, filter and process the application layer data instead of using proxies. Stateful multilayer inspection firewalls have many advantages such as providing a high level of security, performance improvement and transparency to end users. They are quite expensive because of their complexity and are potentially less secure than simpler types of firewalls.

- This type of firewall can remember the packets that passed through it earlier and make decisions about future packets based on this memory.
- These firewalls provide the best of both packet filtering and application-based filtering.
- Cisco Adaptive Security Appliances contain stateful firewalls.
- These firewalls track and log slots or translations.

The firewall checks for those packets that do not comply with the filtration rules and are dropped at the network layer of the protocol stack. The other packets forwarded to the next layer undergo another layer of filtration validating whether the packets are in the proper session. Packets that are currently not a part of the session are dropped at the TCP layer. Next, packets are filtered at the application layer enabling the user to allow only authorized actions at the firewall.



An application level proxy works as a proxy server. It is a type of server that acts like an interface between the user workstation and the Internet. It correlates with the gateway server and separates the enterprise network from the Internet. It receives the request from a user to provide the internet service and responds to the original request only. A proxy service is an application or program that helps forward user requests (for example, FTP or Telnet) to the actual services. The proxies are also called an application level gateway, as they renew the connections and act as a gateway to the services. Proxies run on a firewall host that is either a dual-homed host or some other bastion host for security purposes. Some proxies, named caching proxies, run for the purpose of network efficiency. They keep copies of the requested data of the hosts they proxy. Such proxies can provide the data directly when multiple hosts request the same data. Caching proxies helps in reducing load on network connections whereas proxy servers provide both security and caching.

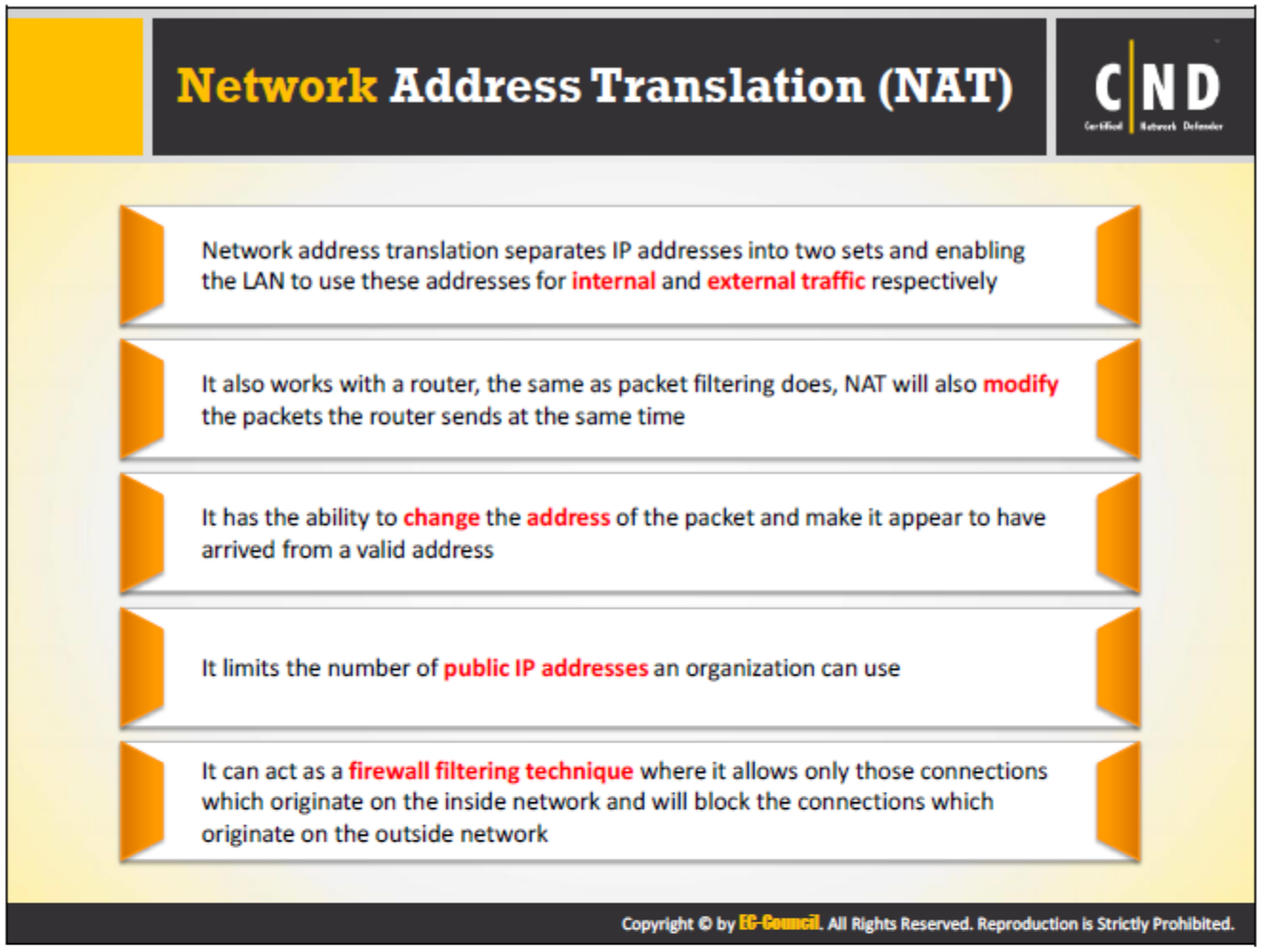
A proxy service is available between the user in the internal network, the service on the outside network (Internet) and is transparent. Instead of direct communication between each, they talk with the proxy and it handles all the communication between users and the internet services. Transparency is the advantage of proxy services. To the user, a proxy server presents the illusion that they are dealing directly with the real server whereas with the real server, the proxy server presents the illusion that it is dealing directly with the user.

Advantages

- Proxy services can be good at logging because they can understand application protocols and allow logging in an effective way.
- Proxy services reduce the load on network links as they are capable of caching copies of frequently requested data and allow it to be directly loaded from the system instead of the network.
- Proxy systems perform user-level authentication, as they are involved in the connection.
- Proxy systems automatically provide protection for weak or faulty IP implementations as it sits between the client and the internet and generates new IP packets for the client.

Disadvantages

- Proxy services lag behind non proxy services until suitable proxy software is available.
- Each service in a proxy may use different servers.
- Proxy services may require changes in the client, applications, and procedures.



The NAT helps hide an internal network layout and force connections to go through a choke point. The NAT works with the help of a router, helping to send packets and modifying them. When the internal machine sends the packet to the outside machine, NAT modifies the source address of the particular packet to make it appear as if it is coming from a valid address. When the outside machine sends the packet to the internal machine the NAT modifies the destination address to turn the visible address into the correct internal address. The NAT can also modify the source and destination port numbers. NAT systems use different schemes for translating between internal and external addresses:

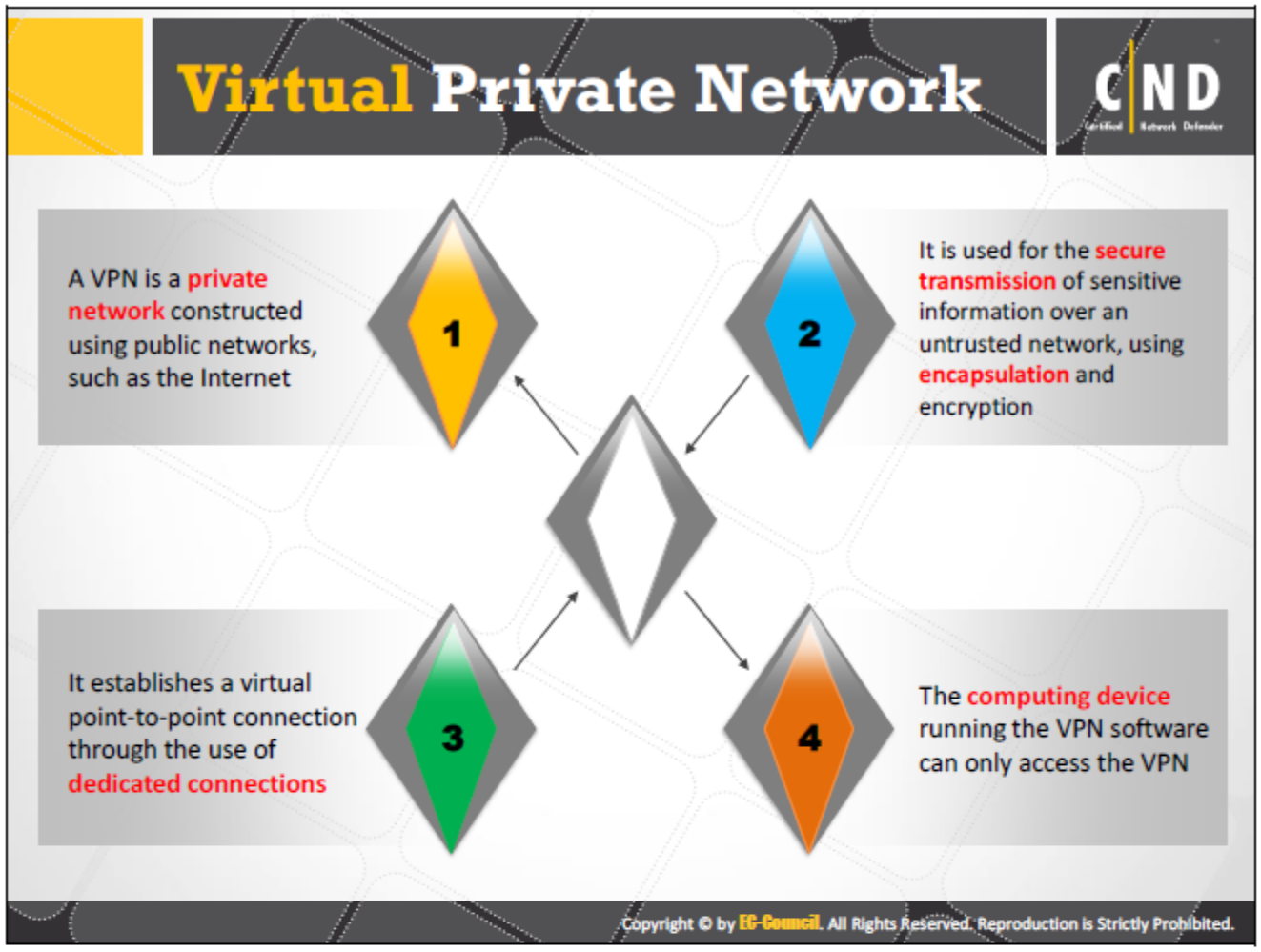
- Assigning one external host address for each internal address and always applying the same translation. This slows down connections and does not provide any savings in address space.
- Dynamically allocate an external host address without modifying the port numbers at the time when the internal host initiates a connection. This restricts the number of internal hosts that can simultaneously access the Internet to the number of available external addresses.
- Create a fixed mapping from internal addresses to externally visible addresses, but use port mapping so that multiple internal machines use the same external addresses.
- Dynamically allocate an external host address and port pair each time an internal host initiates a connection. This makes the most efficient possible use of the external host addresses.

Advantages

- Network address translation helps to enforce the firewall's control over outbound connections.
- It restricts incoming traffic and allows only packets that are part of a current interaction initiated from the inside.
- Helps hide the internal network's configuration and thereby reduces the success of attacks on the network or system.

Disadvantages

- The NAT system has to guess how long it should keep a particular translation, which is impossible to guess correctly every time.
- The NAT interferes with encryption and authentication systems to ensure security of the data.
- Dynamic allocation of ports may interfere with packet filtering.



A VPN is a network that provides secure access to the network through the internet. Used for connecting wide area networks (WAN). It allows computers of one network to connect to computers on another network. It employs encryption and integrity protection helping you to use a public network as a private network. A VPN performs encryption and the decryption outside the packet-filtering perimeter to allow the inspection of packets coming from other sites. A VPN encapsulates packets sent over the Internet. A VPN is an attempt to combine both the advantages of public and private networks. VPNs have no relation to firewall technology, but firewalls are convenient for adding VPN features as they help in providing secure remote services. All virtual private networks that run over the Internet employ these principles:

- Encrypts the traffic
- Checks for integrity protection
- Encapsulates into new packets, which are sent across the Internet to something that reverses the encapsulation
- Checks the integrity
- Then finally, decrypts the traffic

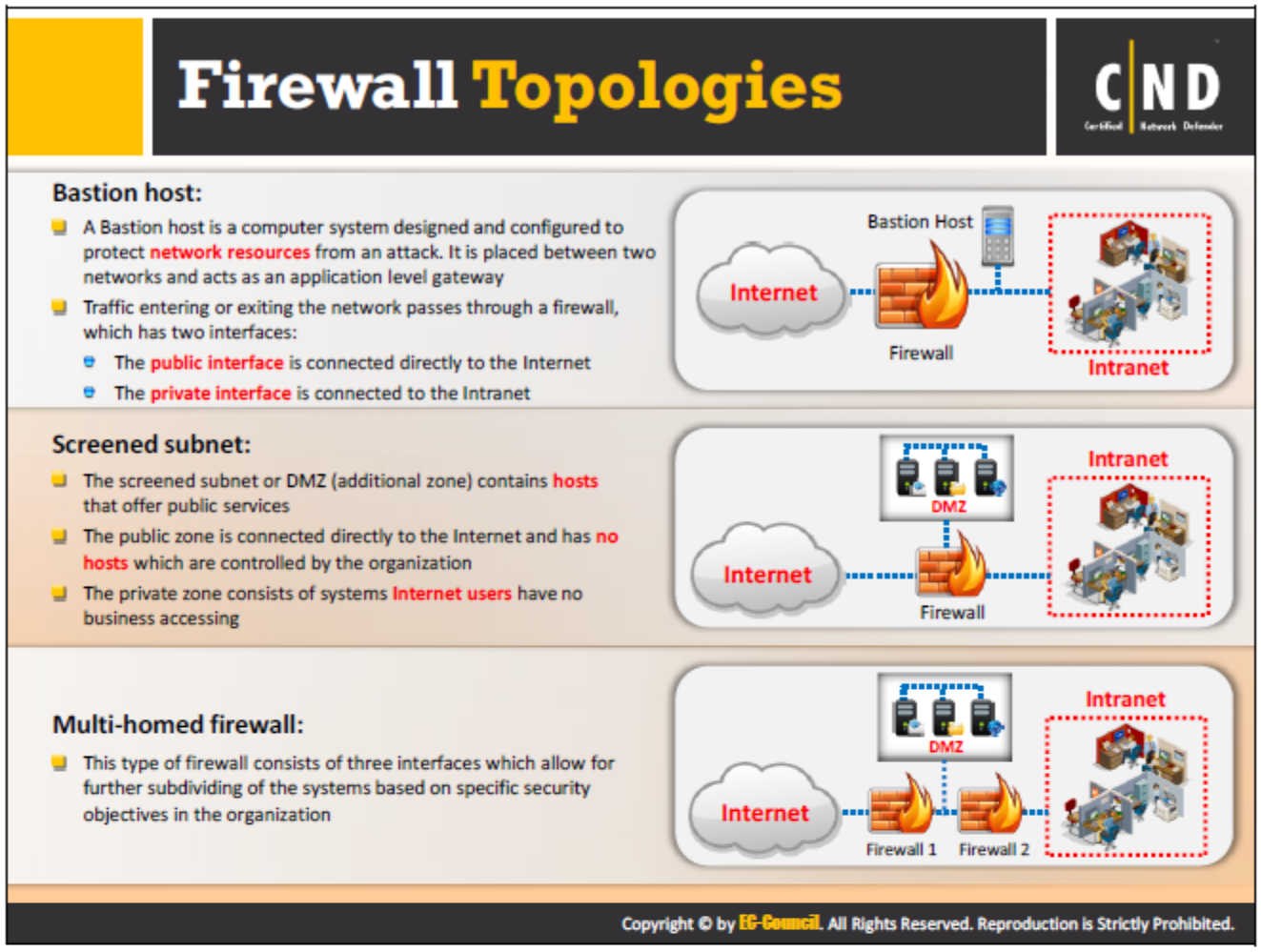
Advantages

VPNs provide some security advantages such as:

- A VPN hides all the traffic that flows over it, ensures encryption, and protects the data from snooping.
- It provides remote access for protocols without letting people attack from the Internet at large.

Disadvantages

- As the VPN runs on a public network, the user will be vulnerable to an attack on the destination network.



An organization will generally implement the firewall, which provides extremely effective network based security control on a single machine. It may be a router or a host. The three types of firewall architectures and their related use are explained below:

Bastion Host

A bastion host is a computer system designed and configured to protect network resources from attacks. It acts as a mediator between inside and outside networks. The firewall resides between the Internet and the protected private network. It filters all traffic that is incoming and outgoing from the network. The bastion host provides a platform for an application level or circuit level gateway. It requires additional authentication for the user to access the proxy services. A network administrator installs only the essential services or applications on the bastion host. Simple networks that do not offer any internet services use a bastion host topology. Suppose the system has two firewalls, then a bastion host is placed inside the two firewalls or on the public side of the DMZ. Examples of a bastion host include: mail, DNS and FTP servers.

Traffic entering or leaving the network passes through the firewall. It has two interfaces:

- **The Public Interface** is directly connected to the Internet.
- **The Private Interface** is connected to the Intranet.

Screened Subnet

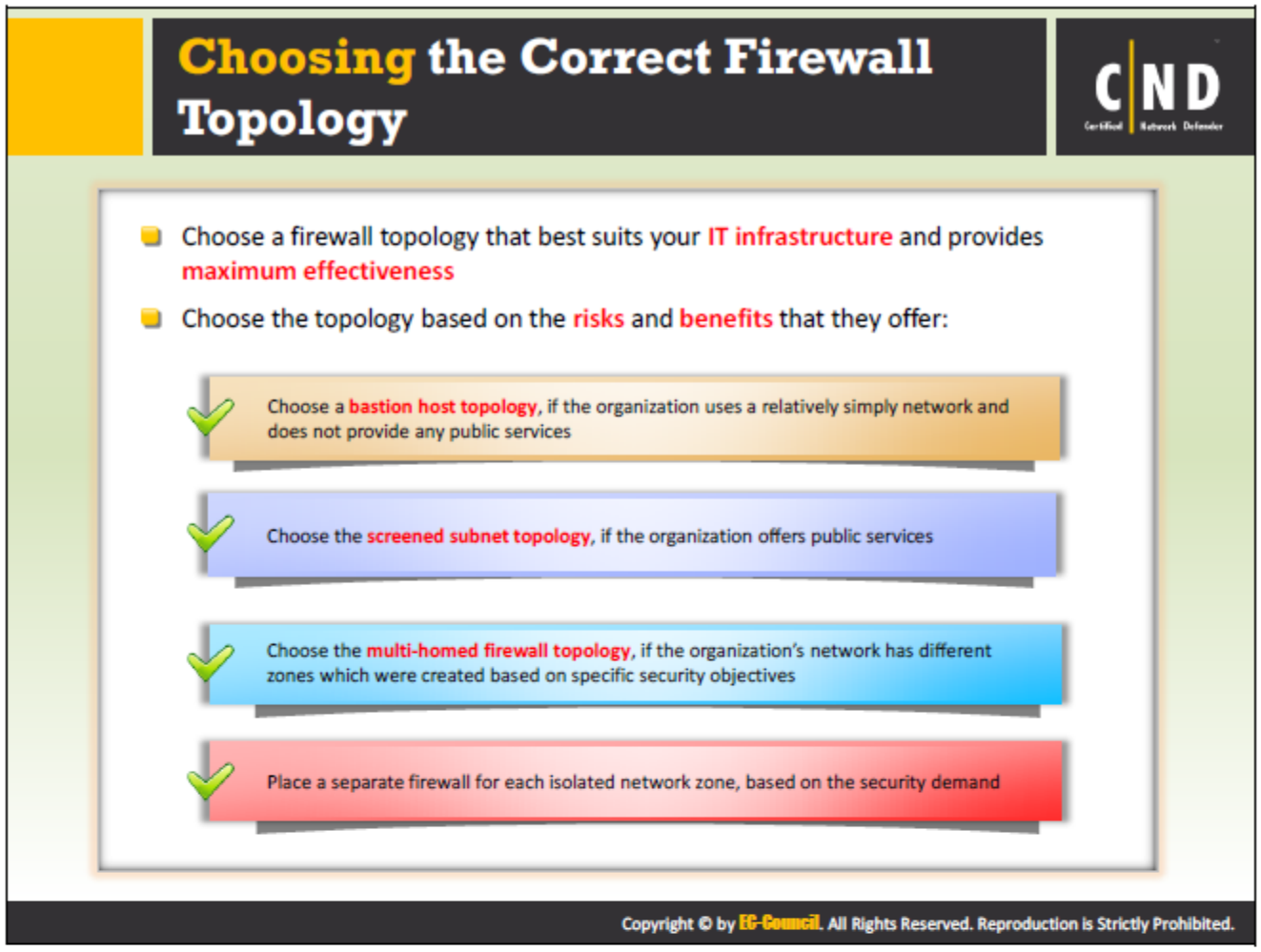
The screened subnet is also known as a "triple-homed firewall" and uses a single firewall with three network interfaces. The first interface connects the Internet, the second interface connects the DMZ, and the third interface connects the intranet. The screened subnet or DMZ (additional zone) contains hosts that offer public services. The public zone connects directly to the Internet and has no organization-controlled hosts. The main advantage with using the screened subnet is it separates the DMZ and Internet from the intranet. If the firewall is compromised, access to the intranet will not be possible.

The screened subnet architecture consists of two screening routers, one is placed between the perimeter net and the internal network, and the other is placed between the perimeter net and the external network. This architecture is more secure because to enter the internal network, the hacker/attacker has to pass both the routers.

Multi-homed Firewall

A multi-homed firewall refers to two or more networks. In this case, more than three interfaces are present allowing for further subdividing of the systems based on the specific security objectives of the organization. Each interface connects with the separate network segments logically and physically. A multi homed firewall allows administrators to assign a different security policy to each interface. Internet users access only presentation servers, which have access to middleware servers, which can access only data servers. A multi homed firewall increases the efficiency and reliability of an IP network. It duplicates all the functions of a firewall in a single box and replaces the IP router that does not forward packets at the IP layer. The multi-homed host processes the packets through the application layer, which provides complete control over handling the packets.

A dual-homed host is similar to the multi-homed host. It has two network interface cards (NIC's), one connected to an external network (untrusted) and the other to an internal network (trusted). The key point here is it does not allow traffic coming from the untrusted network to directly route on the trusted network. A firewall acts as an intermediary.



Before deploying a firewall on the network as part of their perimeter protection strategy, organizations should understand which firewall topology suits their business needs best.

Bastion Host

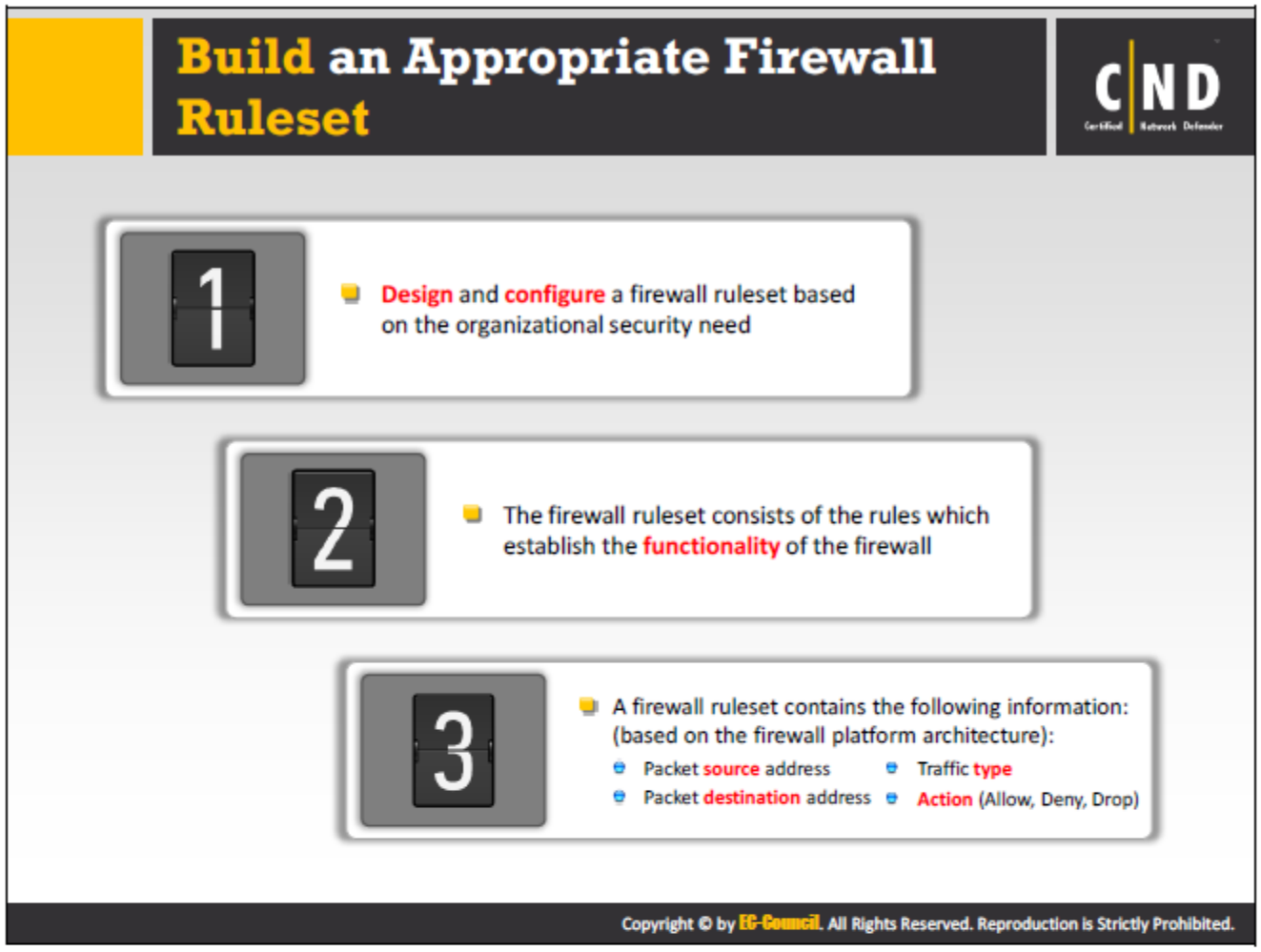
This type of topology is ideal for simple networks. It monitors the traffic between the private network and the outside world (Internet). This topology offers a single layer of protection. The network may be compromised if an attacker penetrates through this layer though. Restricting every user's Internet access through this firewall keeps the network relatively safe from threats. Organizations use this topology to protect a corporate network intended for surfing the Internet and other internal communications. It does not provide sufficient protection for web hosting or protecting an e-mail server.

Screened Subnet

This type of topology is ideal for an organization hosting a website or an e-mail server. A screened subnet topology provides secure services to internet users. In this type of topology, the servers that provide public services are set up in separate zone called a demilitarized zone (DMZ), keeping the trusted network secure from the internet. Users inside the trusted network will have access to the Internet through the DMZ. Even though a malicious user compromises the firewall, they cannot access the network inside the DMZ.

Multi-homed Firewall

A multi-homed firewall offers the advantage of protecting your trusted network even if the demilitarized zone (DMZ) is compromised. This topology operates on two or more network interfaces. One interface connects to the untrusted network (Internet) and other interface connects to the trusted network. A DMZ can add a multi-homed firewall by adding a third interface. The rules for accessing the DMZ are less than those protecting the private network. This topology is ideal for organizations maintaining two or more network zones.



You should build rulesets that support and implement the organization's firewall policy while offering better performance. These should be specific and dependent on the network traffic they interact with and include information such as traffic types required and protocols used for management purposes. The type of firewall and specific products affect the ruleset's development process.

The firewall rule allows a computer to send or receive packets from a program, services, computers and/or users. Firewall rules allow three actions:

- Allow the connection.
- Allow the connection only if secured through IPsec.
- Block the connection.

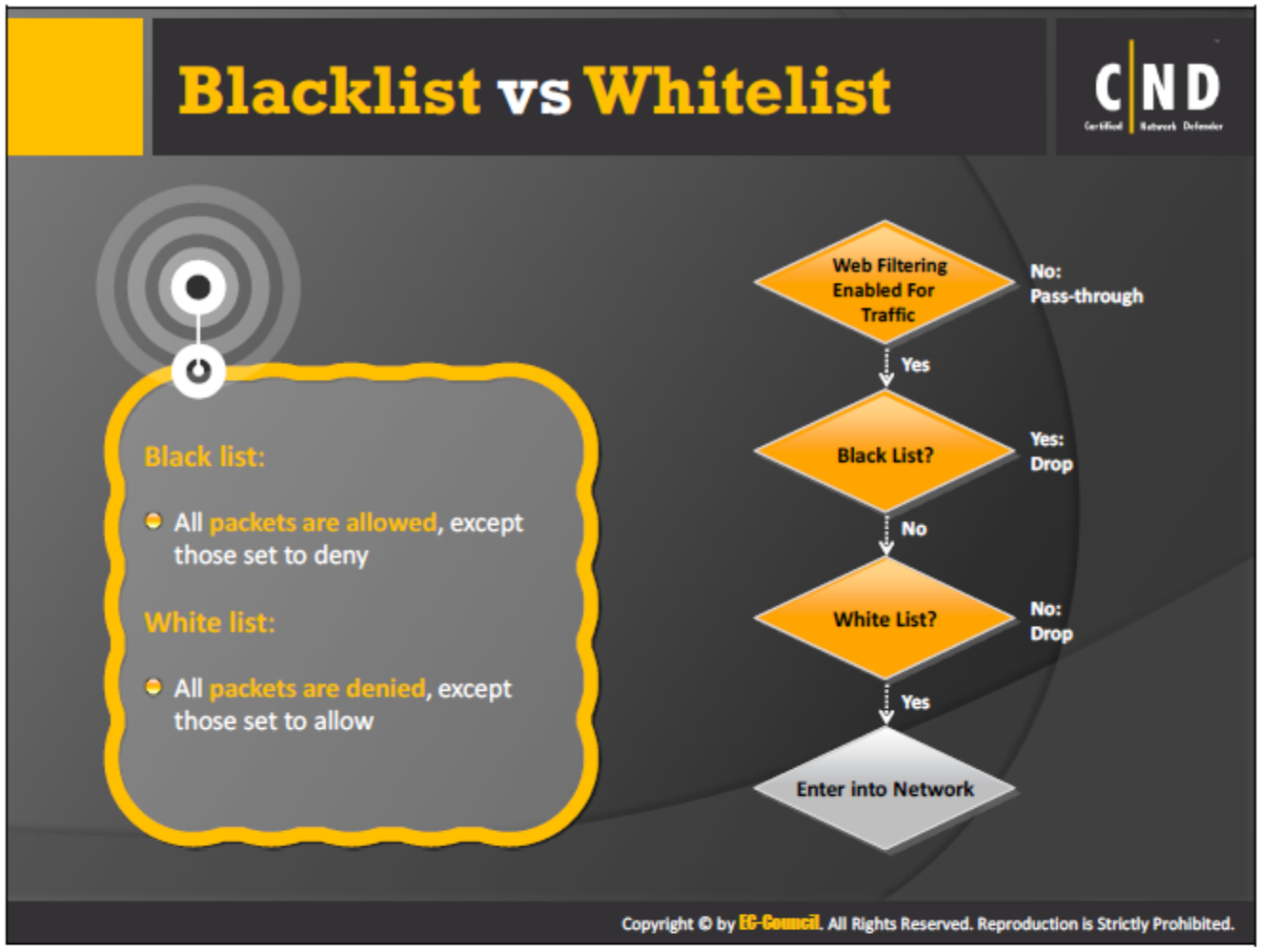
These rules are applicable for both inbound and outbound traffic. Rules can be applied to a variety of network adapters including LAN, Wireless and remote access.

Most firewall platforms use rulesets as their common system for implementing security controls. The contents of the firewall ruleset will establish the functionality of the firewall. Based on the firewall's platform architecture, firewall rulesets contain the following information:

- Packet source address.
- Packet destination address.

- Traffic type.

The ruleset should ensure that port filtering is performed both at the outer edge of the network, and inside the network. The ruleset should also be capable of raising an alert if a user logs on or changes any of the rules.



There are two ways to define firewall rules based on the appropriate approach selected when creating protocols, reducing vulnerabilities on a network and the desired functionality offered. The two approaches are:

Black list

- In this approach, the network administrator estimates and defines all the properties of malicious traffic and the firewall will prevent such traffic from entering the internal network.
- With this type of configuration, it is easier to protect the internal network when using a firewall.
- The firewall allows all packets, except the ones set to deny.

White list

- In this approach, the firewall contains the properties of acceptable traffic.
- All packets are denied by the firewall, except those, that are set to allow.

Example: The Packet Filter Firewall Ruleset

- The following tables illustrate a sample packet filter firewall ruleset, helping you to configure the packet filtering rules in software as well as hardware firewalls

S.No	Source Address	Source Port	Dest Address	Dest Port	Action
1	Any	Any	10.1.1.0	>1023	Allow
2	10.1.1.1	Any	Any	Any	Deny
3	Any	Any	10.1.1.1	Any	Deny
4	10.1.1.1	Any	Any	Any	Allow
5	Any	Any	10.1.1.2	HTTP	Allow
6	Any	Any	10.1.1.3	SMTP	Allow
7	Any	Any	Any	Any	Deny

The following table shows how to build the ruleset for packet filtering firewalls.

The 1st rule in the table is described as:

This row states that if traffic originates from any IP address and port source and for a specified destination IP address (10.1.1.0 in this case) and the port source is greater than 1023, this type of traffic will be allowed to pass through the firewall.

S.No	Source Address	Source Port	Dest Address	Dest Port	Action
1	Any	Any	10.1.1.0	>1023	Allow
2	10.1.1.1	Any	Any	Any	Deny
3	Any	Any	10.1.1.1	Any	Deny
4	10.1.1.1	Any	Any	Any	Allow
5	Any	Any	10.1.1.2	HTTP	Allow
6	Any	Any	10.1.1.3	SMTP	Allow
7	Any	Any	Any	Any	Deny

TABLE 7.2: Packet filtering firewall ruleset

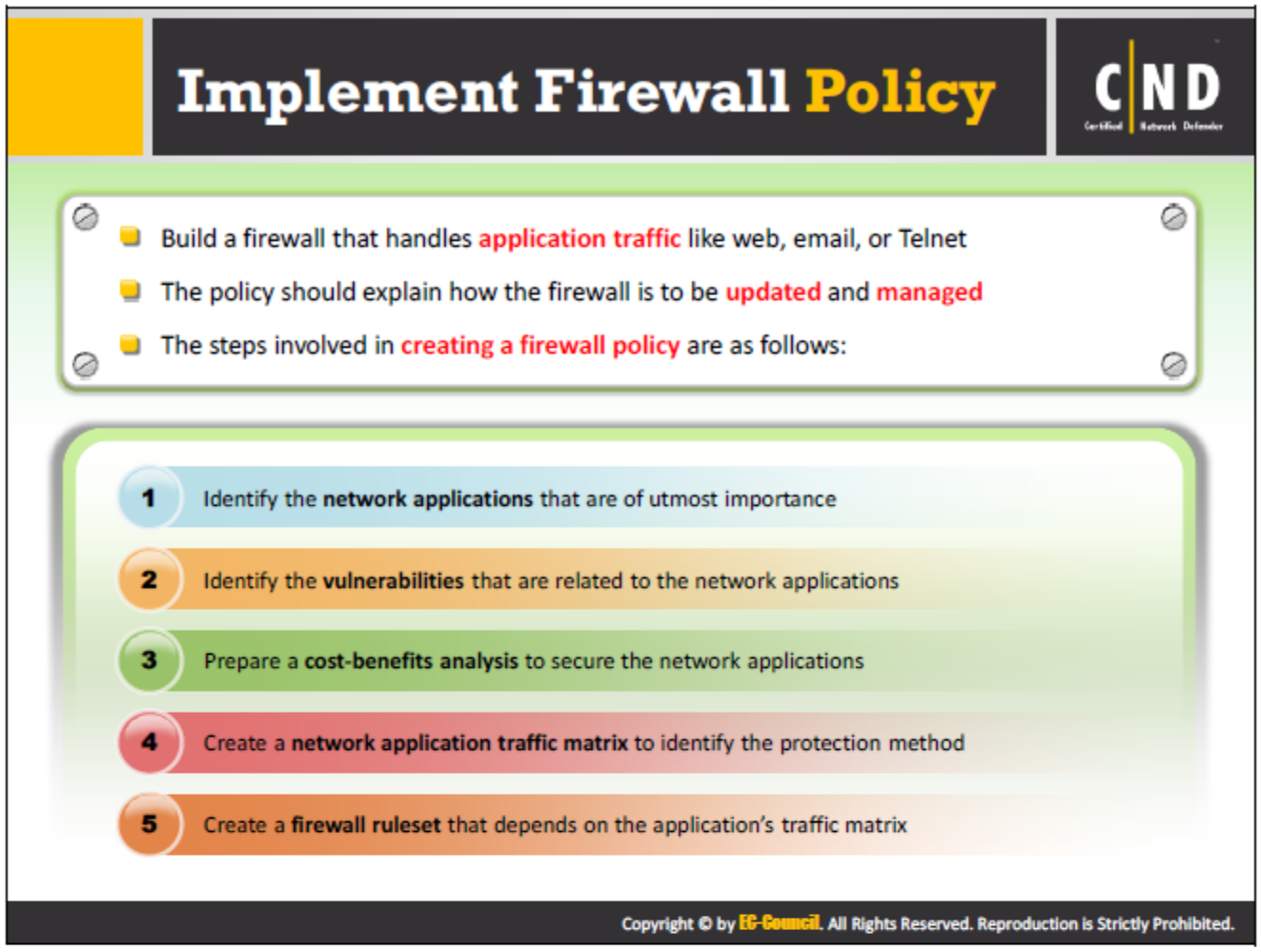
If you want to allow all IP traffic between a trusted external host and your internal hosts, the firewall rule will be as shown in following table

				ACK	
Rule	**Direction**	**Source Address**	**Destination Address**	**Set**	**Action**
A	Inbound	Trusted external host	Internal	Any	Permit
B	Outbound	Internal	Trusted external host	Any	Permit
C	Either	Any	Any	Any	Deny

TABLE 7.3: IP traffic between a trusted external host and internal hosts

You should use the following tricks to build packet filtering firewall rulesets more effectively and securely.

- Edit your filtering rules offline.
- Reload rule sets from scratch each time.
- Always use IP addresses, never hostnames.



Firewall policy implementation should be performed following the organization's system security plan with regards to network traffic, types of traffic protocols, source addresses and destination addresses, required by applications of the organization.

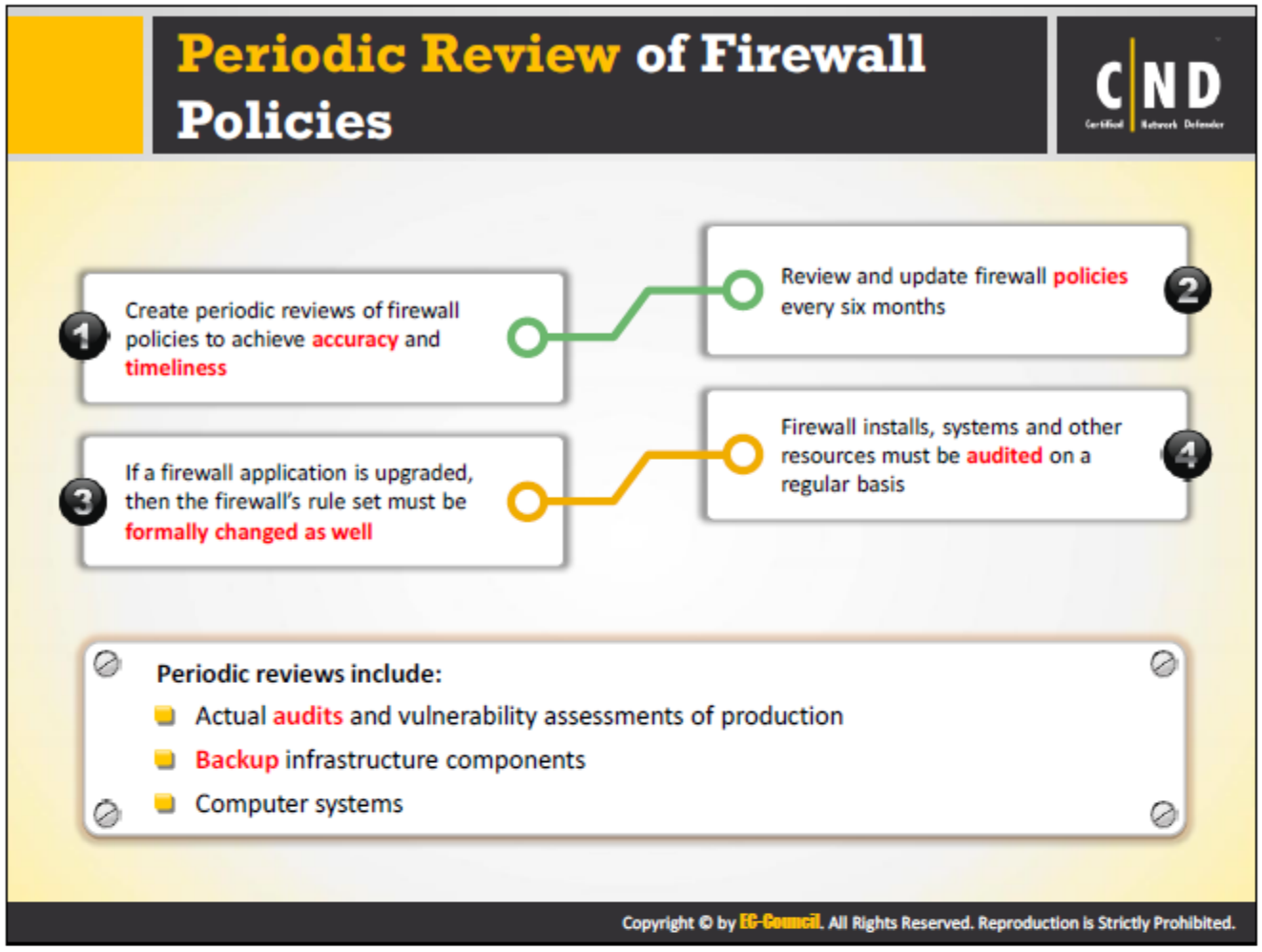
Define a firewall policy, which explains how the firewall is setup, operated, updated and maintained. The policy includes the scope of the firewall, services offered and types of communications supported.

The steps involved in creating a firewall policy are:

- **Step 1:** Identify the network applications that are of utmost importance, the traffic they generate, bandwidth required and type of connection they use
- **Step 2:** Identify the vulnerabilities that are related to the network applications and their impact over the network as well as the systems
- **Step 3:** Prepare a cost-benefit analysis to secure the network applications
- **Step 4:** Create a network application traffic matrix to identify the protection method
- **Step 5:** Create a firewall rule set that depends on the application's traffic matrix

Checklist: Implementing a basic firewall policy

- Always confirm that the policies implemented meet the needs of the organization.
- Always create one or more firewall rules for inbound traffic to allow voluntary inbound network traffic.



According to recent studies, almost 80% of the firewalls installed were misconfigured. Any small error in the firewall increases risk for an organization. Security, regulatory compliance, network availability and performance get altered if there are any issues in the firewall.

Firewall policies should align with day-to-day advancements in threat levels in order to deploy a protected network. You have to verify the policy defining the processes regularly to check if they are able to combat any new risks and attacks.

The steps to review the policies are:

- Create periodic reviews for firewall policies to achieve accuracy and timeliness.
- Review and update firewall policies every six months.
- If a firewall's application is upgraded, then the firewall's ruleset must be formally changed.
- Firewall installs, systems and other resources must be audited on a regular basis.

The scheduled periodic firewall policy reviews include:

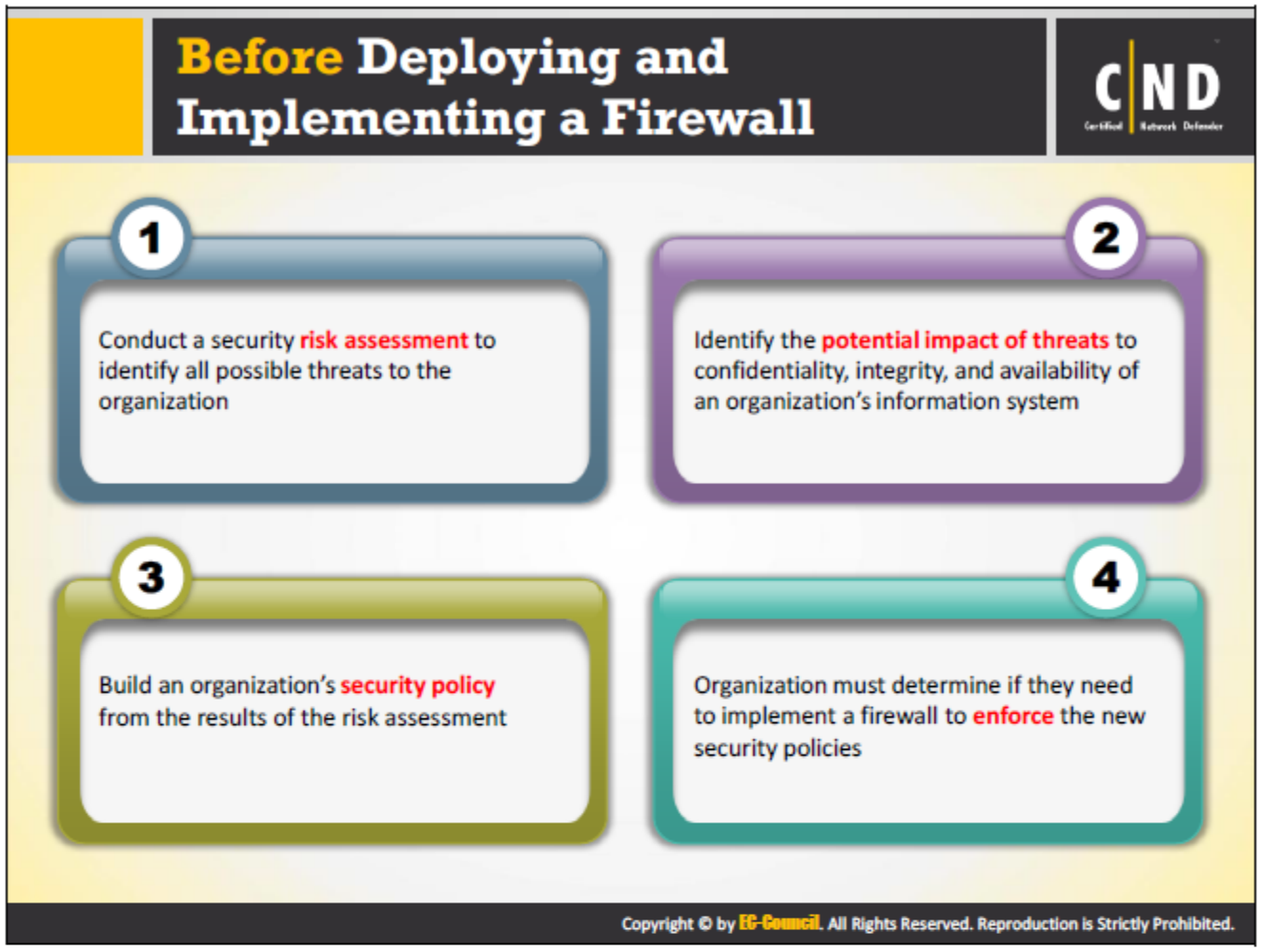
- Actual audits and vulnerability assessments of production that give a good idea on what systems are being used, internal communications patterns deployed and the type of attacks they are prone to.
- Backup infrastructure components help create a backup in case an attack is performed leading to data loss.

- Computer systems, shared drives, email servers, web servers and secured networks placed at various locations must also be reviewed in order to keep the system updated which offers the utmost speed and efficiency .

Scheduled reviews examine the following:

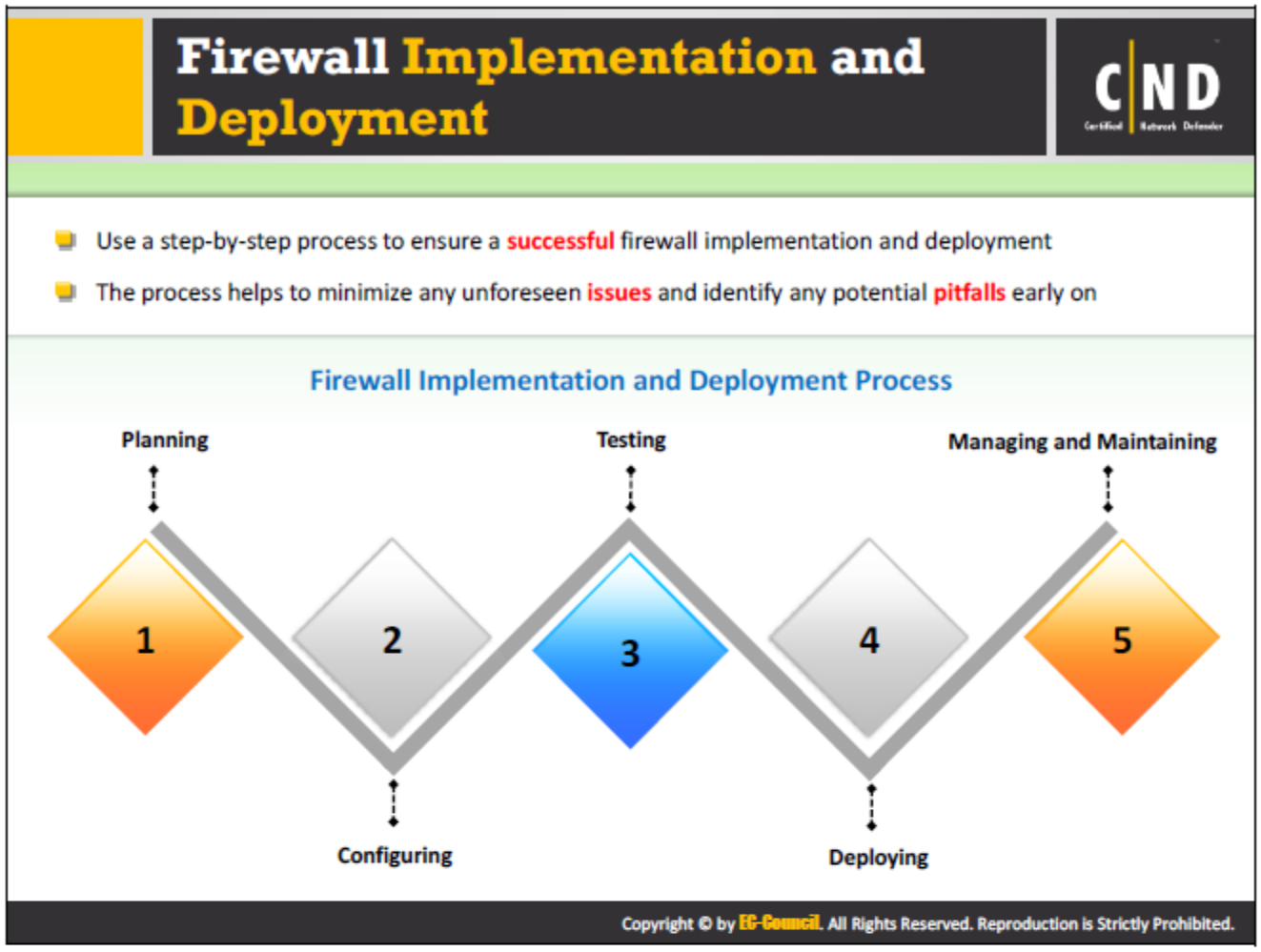
- Whether proper firewall policies are implemented for each firewall.
- The firewall rules that are not used often and whether they can be eliminated.
- Any changes in network security gives rise to additional or new security exposures.

Periodic firewall reviews help increase security, availability and performance of the organization's network.



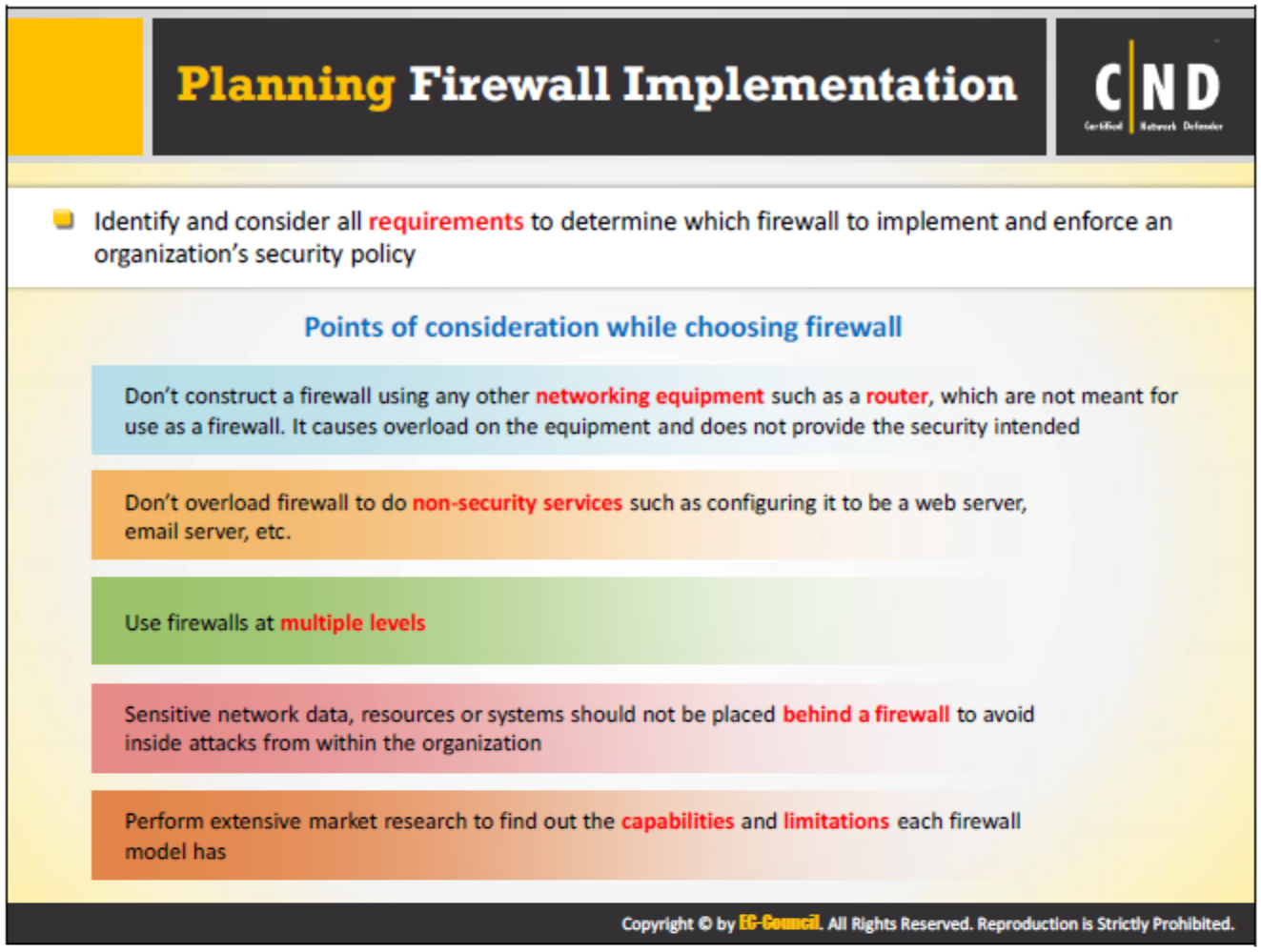
There are some factors to consider before implementing a firewall solution on the network. It is the responsibility of a network administrator to specify network security issues and address them during firewall implementation.

When implementing a firewall for the network, organizations must plan the positioning of firewalls in advance. They should also consider conducting a security risk assessment to know where a threat to the network would most likely originate and the reasons behind it. Depending on the potential origin of threats, administrators attempt to build a layout for firewall implementation. If an organization is considering implementing a firewall, remember to outline a consistent security policy in advance based on the risk assessment. The security policy must determine how basic communication will take place at the firewall, where the firewall must sit and how to configure it.



Administrators consider a phased approach to implement and deploy a firewall ensuring network security. The use of a five-phased approach for implementation and deployment minimizes unforeseen issues and identifies potential pitfalls. The phases involved in implementing and deploying a firewall include planning, configuring, testing, deploying and managing.

- While planning a firewall implementation, consider all the requirements to determine which firewall to implement while enforcing network security policies.
- After planning, administrators focus on configuring the firewall hardware and software components and setting up rules for the system to work effectively.
- Administrators test the firewall prototype and its environment after successfully configuring the firewall. They need to assess the functionality, performance, scalability, and security of the firewall for possible vulnerabilities and issues in the components.
- After resolving all issues encountered during the testing phase, administrators need to deploy the firewall into the network.
- After successfully deploying the firewall, administrators monitor it for component maintenance and resolving operational issues throughout its lifecycle. They consider incorporating enhancements or significant changes when needed.



A proper risk assessment is conducted before planning a firewall implementation

The planning includes:

- Detecting possible threats and vulnerabilities in the network.
- Evaluating possible impacts of a threat.
- Identifying appropriate security controls.

Points to consider while choosing a firewall:

- Do not configure a firewall on a device not meant for firewall purposes. For example, configuring a firewall to function on a router can put additional burdens on the router's functionality.
- Do not enable additional non-security services such as a web server or email server on the firewall. This will overload the device and reduce its efficiency to provide network security.
- Administrators should consider deploying firewalls at different locations at the perimeter, departments and an individual host level.
- Consider implementing a firewall as an obligation especially as a part of the overall security program.
- Concentrating on external threats leaves the network vulnerable to internal threats or inside attacks. Consider keeping all sensitive and critical systems behind internal firewalls.

- The administrator needs to be careful while deploying a specific type of firewall. It should be done based on their techniques and limitations. Organizational security policies have great impact on the type of firewall used.

Factors to Consider before Purchasing any Firewall Solution

Management

- Will it provide **Remote** and **Centralized** management capabilities?

Performance

- What will be its **throughput**, maximum simultaneous connections, connections per second, and latency time?

Integration

- Will it be **easy to integrate** into the existing network infrastructure or require specific hardware?

Security Capabilities

- What do you need to **secure**?
- Which types of **firewall technologies** should it support?
- What kind of **additional security** features does it have?

Factors to Consider before Purchasing any Firewall Solution (Cont'd)

Physical Requirements

- Will it require any additional physical requirements such as **additional power**, backup power, cooling system, or **network connections**?

Personnel

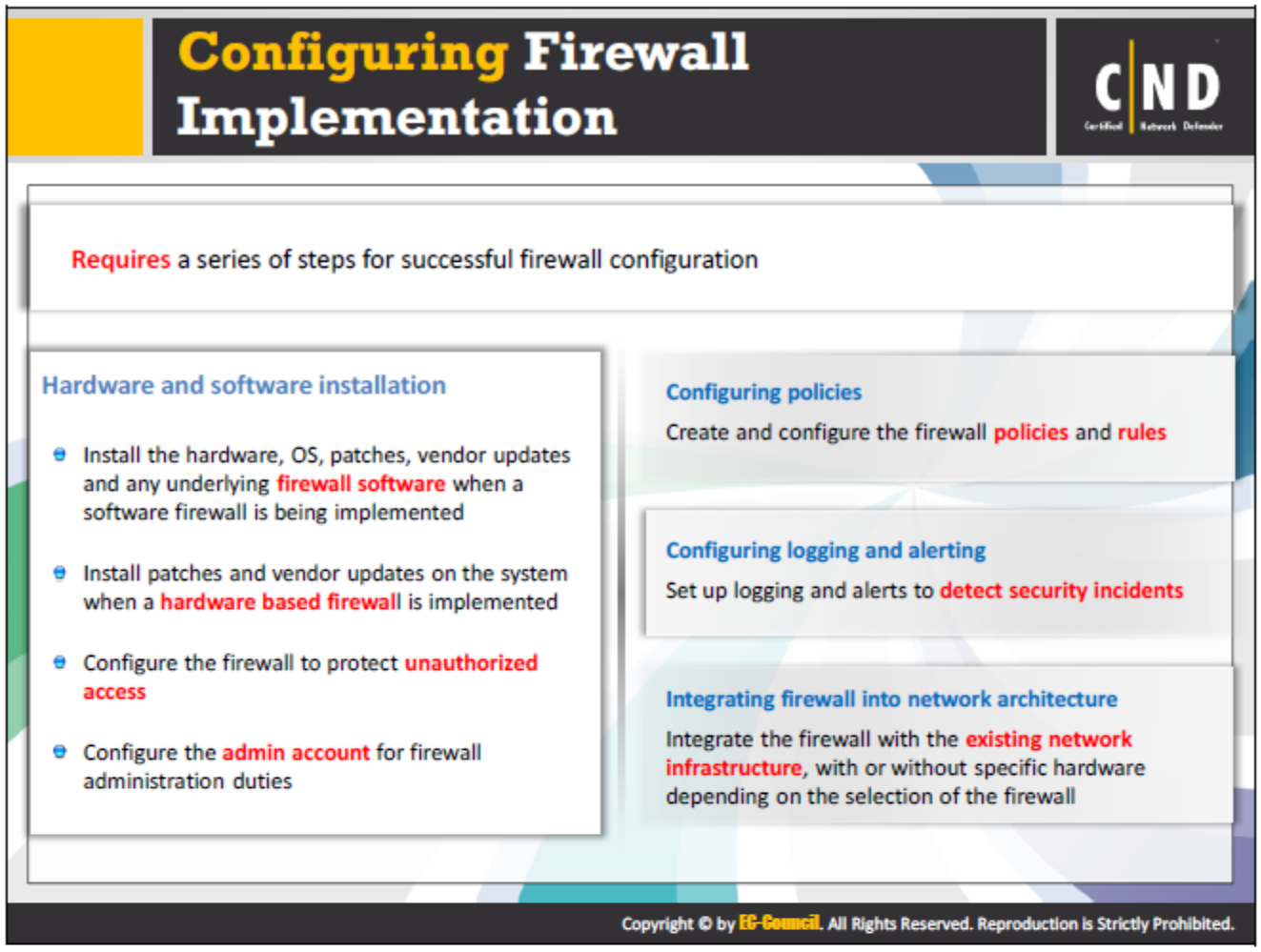
- Will the administrator require any **training** to implement, deploy, administer and manage the firewall?

Future Needs

- Will it **meet** the future needs of the organization?

The organization should consider the following factors before purchasing and implementing any firewall solution for their network.

- **Management:** The firewall should support encrypted protocols such as HTTPS, SSH, and access over a serial cable for remote management. Check whether any of these remote management protocols are acceptable for use with the organization's policies. Administrators need to ensure that it is possible to restrict remote management to certain firewall interfaces and source IP addresses. In firewalls, look for centralized management from the same vendor. If it is available, check whether it is a vendor-specific application which performs this operation or any other application which controls it.
- **Performance**: Consider the performance of the firewall based on throughput, number of connections, time required for each connection and its latency time. Check its resistance against bottleneck problems. Evaluate its failover and load balancing functionality.
- **Integration:** Consider the hardware requirement for firewall implementation. The implemented firewalls need to be compatible with all other security devices. Check the compatibility of the firewall log system with the existing log management system.
- **Security Capabilities:** Consider all the possible areas of the organization that require security. Choose the type of firewall technology including packet filtering, stateful inspection, application firewall, application-proxy gateway that will best address the kinds of traffic you want to monitor. The administrators should also consider other network security capabilities like an intrusion detection system, VPN and content filtering while choosing a firewall.
- **Physical Requirements:** Consider the physical space and protection required for a firewall. For example, extra shelf or rack space, adequate power backup facilities and air conditioning facilities at the location of the placement of the firewall.
- **Personnel:** Management should choose network operators or the personnel responsible for managing the firewall. The organization must train network administrators on managing and maintaining the firewall before deploying it.
- **Future Needs:** Choose a firewall that meets the future needs of the organization such as plans to move to IPv6, anticipated bandwidth requirements, and compliance with regulations expected to be implemented.



Configuring a firewall involves configuring various components and features such as hardware, software, policy configuration, implementing logging and alerting mechanisms.

Hardware and Software installation

After selecting a certain type of firewall for implementation, the administrator proceeds with the installation and configuration of the hardware and operating system. If a software based firewall is being implemented, administrators will consider installing the necessary software. It is important to perform a timely installation of patches and vendor updates both types of firewalls. Install the remote management capability software to remotely access the firewall console and manage it to prevent any unauthorized access. Access to the firewall should be restricted to the network administrator responsible for managing the firewall. Also, disable management services for the firewall, such as SNMP. Configure new admin accounts, if the firewall supports having a separate administrator account to perform firewall administration duties.

Configuring Policies

Administrators have to focus on creating the firewall's policies after installing the hardware and software of a firewall. A ruleset's design depends on the type of traffic flowing through the network, including the protocols of the firewall such as DNS, SNMP, and NTP. If multiple firewalls need to have the same rules, synchronize all the rules across all the firewalls.

The mandatory ruleset for every firewall should include:

- Enable port filtering at the outer edge and inside the network.
- Create rules to perform content filtering close to the content receiver.

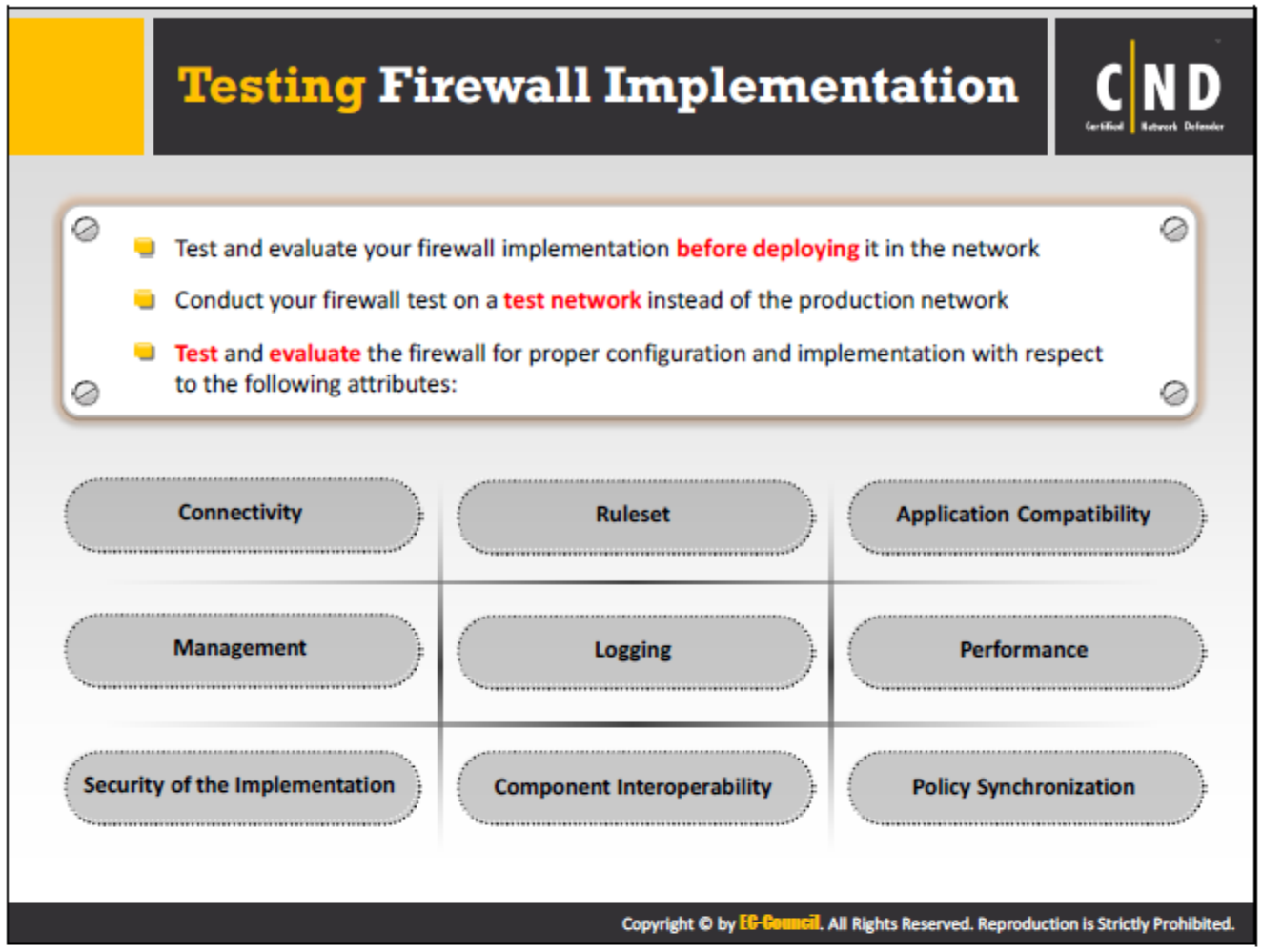
Configure Logging and Alerting

The firewalls should have the capability to store the logs and send and synchronize them in a centralized log management system. Logging should be done on a case-by-case basis to determine what to log and how long to keep logs. Administrators create user accounts with read-access enabled to perform read-only tasks such as auditing and evaluation of the logs. The administrators should enable alarm systems that notify them in the event of any attack on the firewall. The sign of attacks can be:

- Any attempt of manipulation for any of the firewall rules.
- Events like system reboots or disk shortages.
- Any system status changes.

Integrating a firewall into the Network Architecture

There are requirements for integrating a firewall with existing network devices which will interact with the firewall as well as the network's routing structure. Configuring the network router at the boundary of the network enables it to handle firewall addressing.



Testing a firewall involves examining the firewall for any bugs. The firewall implementation test mainly focuses on whether the firewall rules are set according to the actions performed by the firewall. Firewall testing increases the reliability of the products using the firewall.

Before deploying a firewall, the administrator runs a test on a test network, replicating the original network. Different aspects of the firewall are evaluated in this phase:

- **Connectivity:** It involves testing whether users can establish a connection through the implemented firewall.
- **Ruleset:** Checks whether the firewall permits and blocks the traffic as per security policies. The analysis of the firewall rule set includes manual testing to verify if the rules work according to the outlined security rules.
- **Application compatibility:** Check whether the implemented firewall solution is compatible between the existing application or communications.
- **Management:** Test whether an administrator can manage the firewall in an effective manner.
- **Logging:** Test whether logging and data management functions adhere to an organization's policies and strategies.
- **Performance:** Test the performance of a firewall on a live network using simulated traffic generators. The testing process needs to include applications that can affect the network throughput and latency.

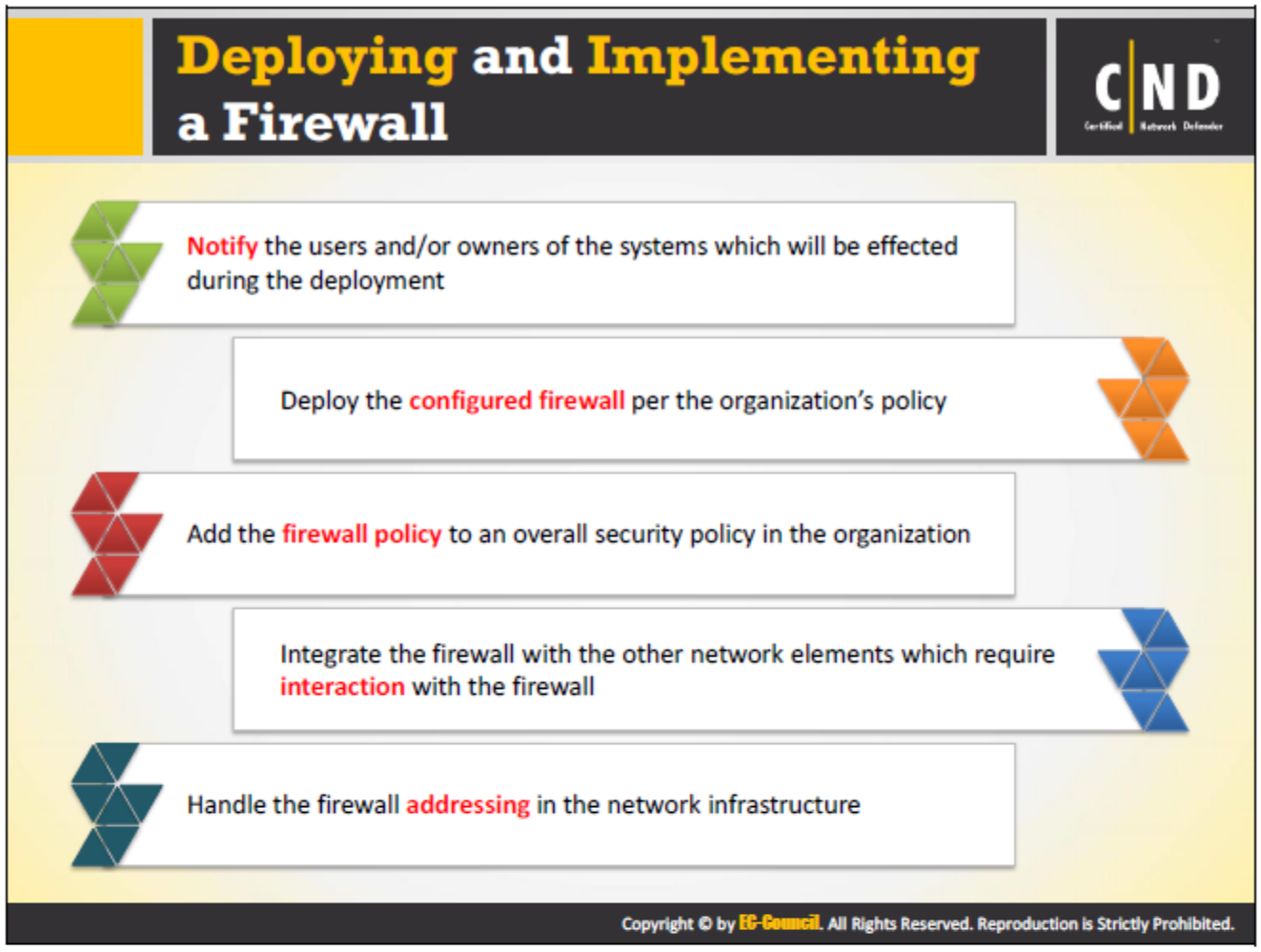
- **Security of the implementation:** Conduct a vulnerability assessment to identify any vulnerabilities and weaknesses in the firewall implementation.
- **Component interoperability:** Evaluate the functioning of different components of the firewall. Using different firewall components from different vendors can create performance issues.
- **Policy synchronization:** Test how synchronized policies work or rulesets when multiple firewalls are used in multiple scenarios.

Testing a firewall includes the following steps

- Developing an appropriate test case
- Derive the test packets from the test case
- Send test packets to the firewall
- Examine the performance of the firewall

If the firewalls do not perform as proposed? Then, the following reasons could be the reason for their failure:

- Development of incorrect test cases and which causes the wrong prediction for firewall performance.
- Incorrect implementation of security policies when designing the firewall rules.
- Errors in the implementation of the firewall.
- Losing packets in the network.
- The test environment has bugs.
- Corrupted hardware components.

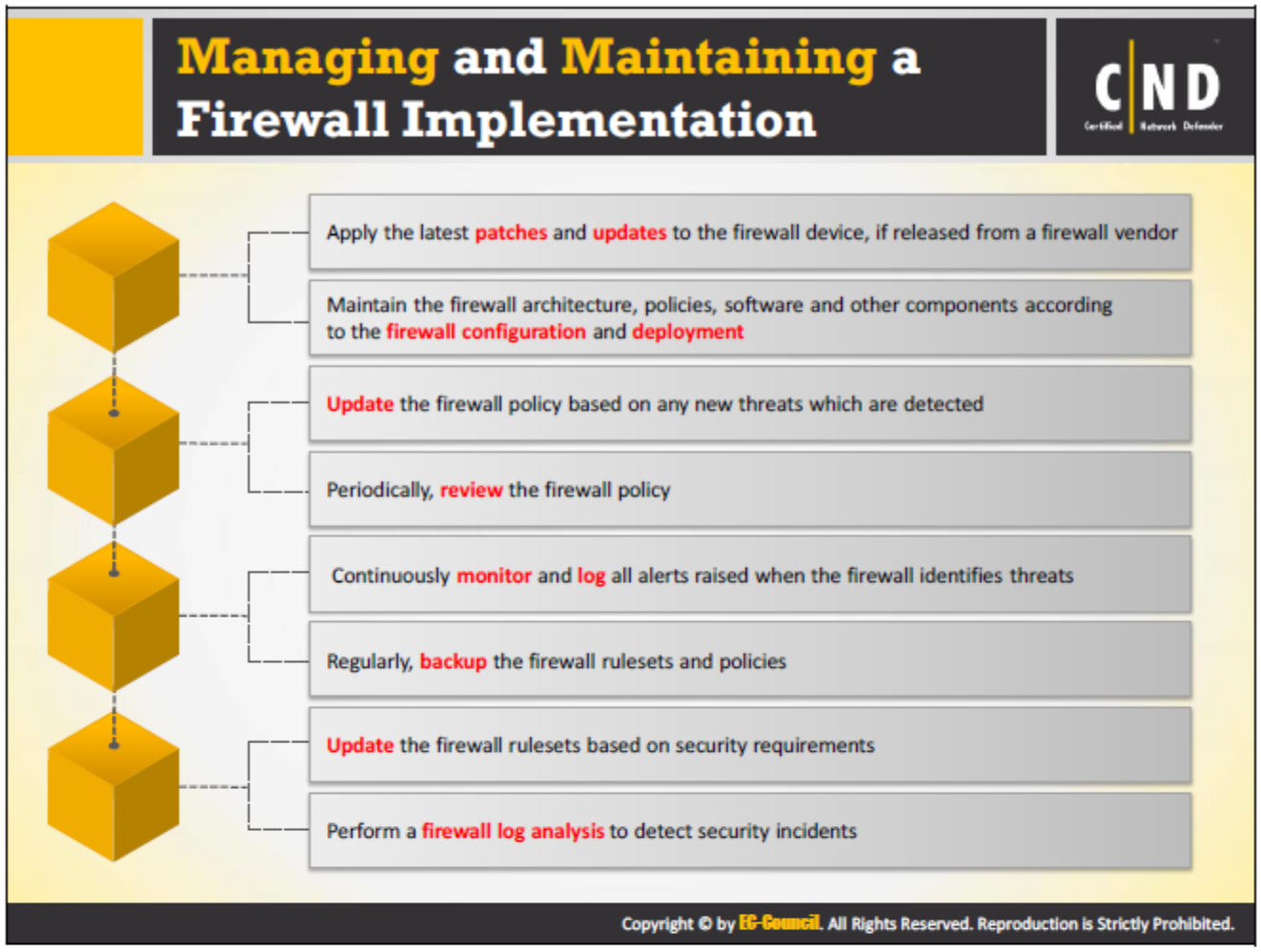


Administrators need to ensure they deploy the firewall according to the security policies of the organization. Administrators should also alert the users of the deployment of the firewall. Add the security policy of the firewall to the network's overall policy and any configuration changes which happened during implementation should also be included. Employing a phased approach to deploy multiple firewalls on a network helps detect and resolve issues regarding conflicting policies.

Reconfigure the network device on the outside of the network to handle addressing of the firewall. Proper deployment of a firewall facilitates the sending and receiving of traffic from the newly configured firewall system.

Deploying a firewall and implementing it is done using

- Update all hosts for the new firewall deployment.
- Alert all the users regarding the deployment of a new firewall into their operational environment.
- Allow private traffic through the newly deployed firewall.



Managing a firewall includes maintaining the firewall architecture, policies, software, and other components deployed on the network. Administrators should update the policy rules when they identify new threats and if requirements change. The network administrator needs to ensure the security of the firewall by constantly monitoring and addressing the issues in the network. They monitor the firewall logs continuously in order to detect new threats and attacks in the network.

Perform regular backups of the firewall policies and rulesets depending on the rule format used by the firewall. Use restrictions offered by firewalls on who can change a ruleset and from which addresses. Review the firewall policy regularly to uncover:

- Rules that are not required.
- Adding new rules to the firewall.

Managing and maintenance of a firewall includes

- Extending its life.
- Make sure it is operating properly.
- Confirm it provides a protective layer to the operational environment.
- Improve the performance.
- Check for required updates.
- Confirm the components are working properly.

Firewall Administration

Accessing Firewall Platform

- Threats to firewalls arise from exploiting **remote management resources** such as the graphical management interface
- **Control access** to the firewall management using encryption, strong authentication and limiting access through the IP address

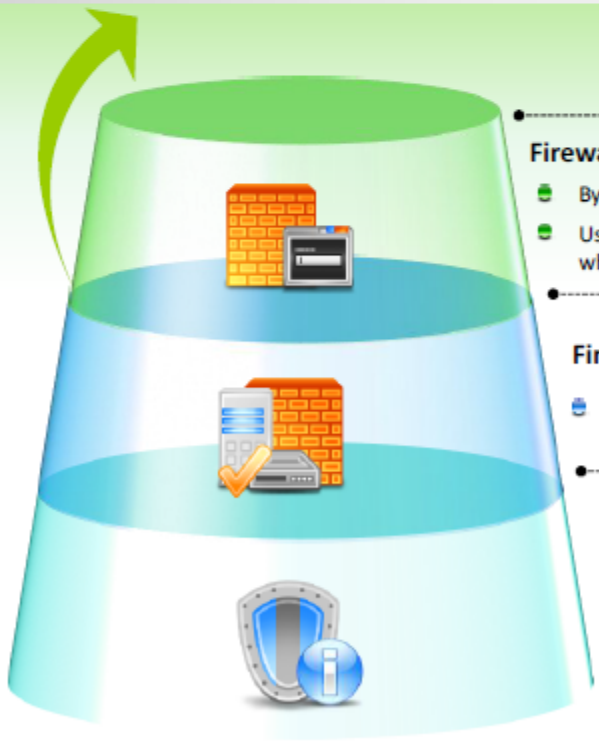
Build Operating System Platform for Firewall

- Implement the firewalls on systems tailored to specifically **strong security applications** e.g. Bastion host
- Patch and remove any unnecessary **features** and **services** before implementing the firewall on the platform

Firewall Failover Strategies

- Use failover services like **network switches** and **heartbeat-based** services in case of primary firewall service failure
- Network switches are devices responsible for **failover** and provides load balancing capabilities
- A heartbeat mechanism initiates the backup systems when a failover event **triggers**. It includes the back-end/customized network interfaces

Firewall Administration (Cont'd)



Firewall Logging Functionality:

- By default, all firewalls have a method for **logging capabilities**
- Use a **centralized logging service** such as a Unix syslog application which also provides log examination and parsing

Firewall Backups:

- Use **full backups** instead of incremental backups

Security Incidents:

- Firewalls play a critical role in **security incidents**. They correlate all the events which have passed through it, especially where network attacks are concerned
- Synchronize the firewall with **network time protocol** (NTP) to effectively correlate the incident events

Firewall administration is the process of maintaining security by managing firewall devices and/or software. It includes access to the firewall platform, operating system builds, firewall failover strategies, firewall logging functionality, security incidents, firewall backups etc.

Firewall administration includes the modification of security policies, assessment of vulnerabilities, identification, detection of new threats and development of counter measures to combat them. Firewall administrators monitor firewall activities regularly to ensure proper functionality to prevent the network from attacks.

Methods of firewall administration are:

- **Access to the Firewall Platform/Accessing Firewall Platform:** Threats to firewalls arise from exploiting remote management resources such as the graphical management interface or an operating system console. To prevent unauthorized access to these resources, a firewall administrator should manage the firewall using encryption and strong user authentication techniques. The graphic management interface uses Secure Socket Layer (SSL) which relies on the Hypertext Transfer Protocol (HTTP) to secure communication over the network.

  Under an internal individual authentication process, the user should have a unique user ID and password to gain access to the interface. Some firewalls also support Token based authentication to grant access to centralized servers using Remote Authentication Dial-In User Service (RADIUS).

- **Build an Operating System Platform for A firewall:** Platform consistency plays a vital role in the successful implementation of a firewall such as Operating systems (OS) with hardened security features for the applications. Do not install a firewall on systems that offer all possible installation options especially after removing unnecessary OS features. Firewall installations should not affect the functioning of the OS. Install all security patches on the OS before installing the firewall. Unused network services, network protocols, applications and user accounts must be disabled.

- **Firewall Failover Strategies:** Failover strategies are required to balance the security of the network when a firewall failure occurs. Specially designed Network switches work on a customized 'heartbeat' mechanism to balance the firewall failover by shifting all the inbound and outbound traffic to the backup firewall. They reduce the chances of a network failure. Both primary and backup firewalls are behind a single Media Access Control (MAC) address to provide seamless functionality.

- **Firewall Logging Functionality:** Every firewall is equipped with a logging function. Firewalls use an UNIX syslog application to manage, examine and parse logs. Various operating systems such as Windows, UNIX and Linux variants support logging of firewalls. The firewall preserves these logs on the centralized server for maximum security and uses only few software packages to examine them.

  A firewall that does not support a syslog interface will have their own internal logging functionality. Third party firewalls provide log maintenance and parsing tools such as firewall analyser and Sawmill.

- **Security Incidents**: A security incident is a situation when an unauthorized individual tries to access the computer or network resources. The administrator has various responsibilities in this situation such as temporarily disabling remote access to the resources and revoking user authentication until the situation comes under control.

  In a minor security incident, the attacker can use basic network probes. Due to its lower severity, many companies don't treat these incidents as threats. In medium security incidents, the attacker tries to get unauthorized access to the resources or the system.

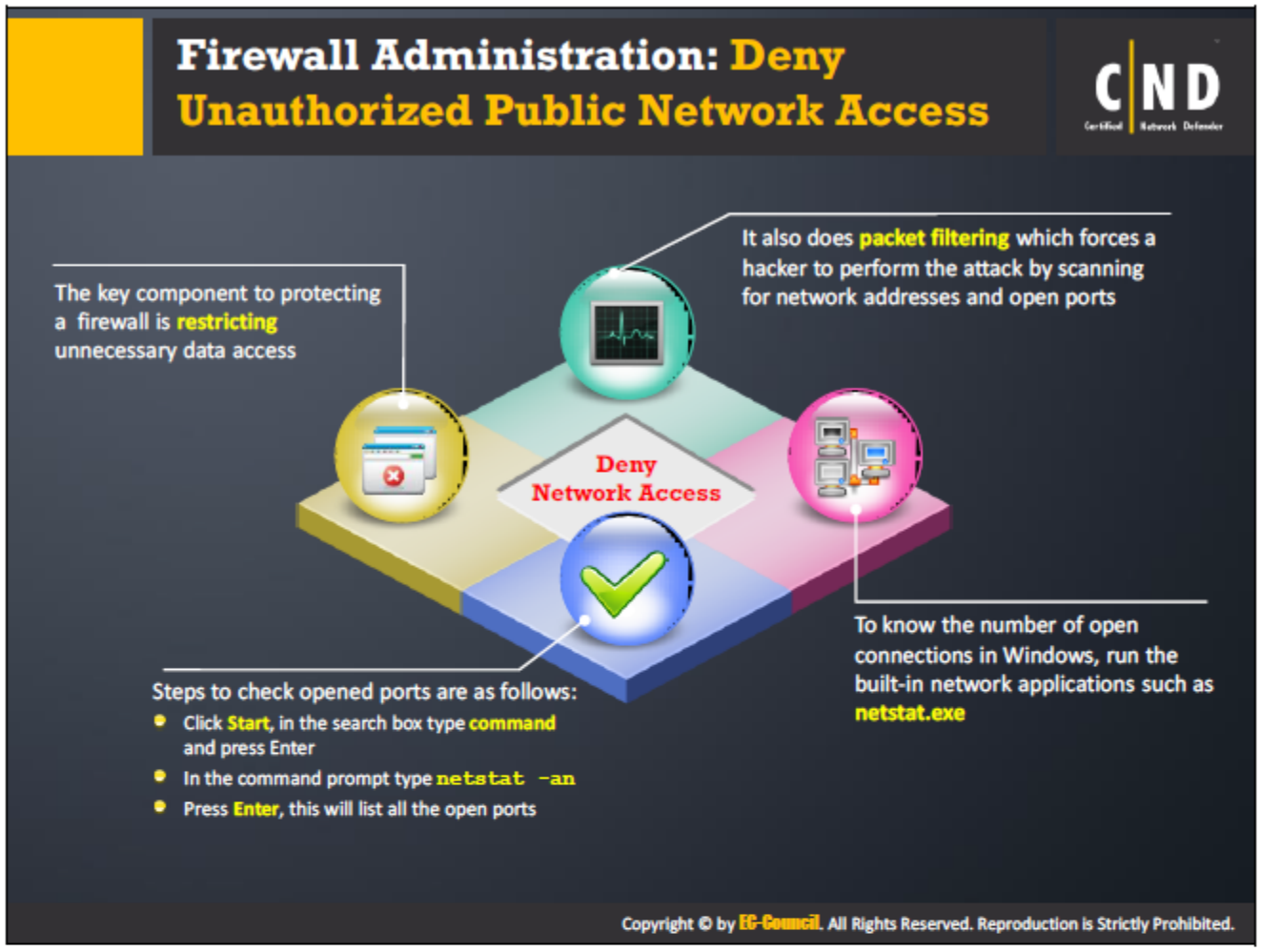
  A high-end incident describes a situation, where an attacker is successful in obtaining access to the system. These incidents restrict resource availability, and are treated as a serious situation.

  A firewall uses an event-correlation technique, which works based on the time synchronization rolling back the state of the firewall to a unique state in order to reconstruct the phases of the incident.

- **Firewall Backups**: All firewall backups should be Day Zero or full backups instead of incremental backups immediately before the production release. Because firewall access control does not permit a centralized backup scheme, firewalls have in-built backup facilities.

  It is desirable to have all critical file systems backed up to external devices in Windows operating systems. In UNIX the /var file system directory and sub directories require write access and contain all the system logs and spool directories.

- **System Administration**: Proper system administration also contributes to firewall administration:
  - Standardizing operating systems making it ready for updates and fixtures.
  - Centralized system administration contributes to better firewall security.
  - Examine the communication path between the firewall and the system in order to uncover any errors or faults in the configuration.
  - Decide on the type of firewall that is best suited for a particular company.



Weak network access controls increase the chances of unauthorized public network access. This leads to the manipulation of data, services and denial of service attacks. Proper controls such as user access restrictions and security controls for granting permissions can limit unauthorized public network access.

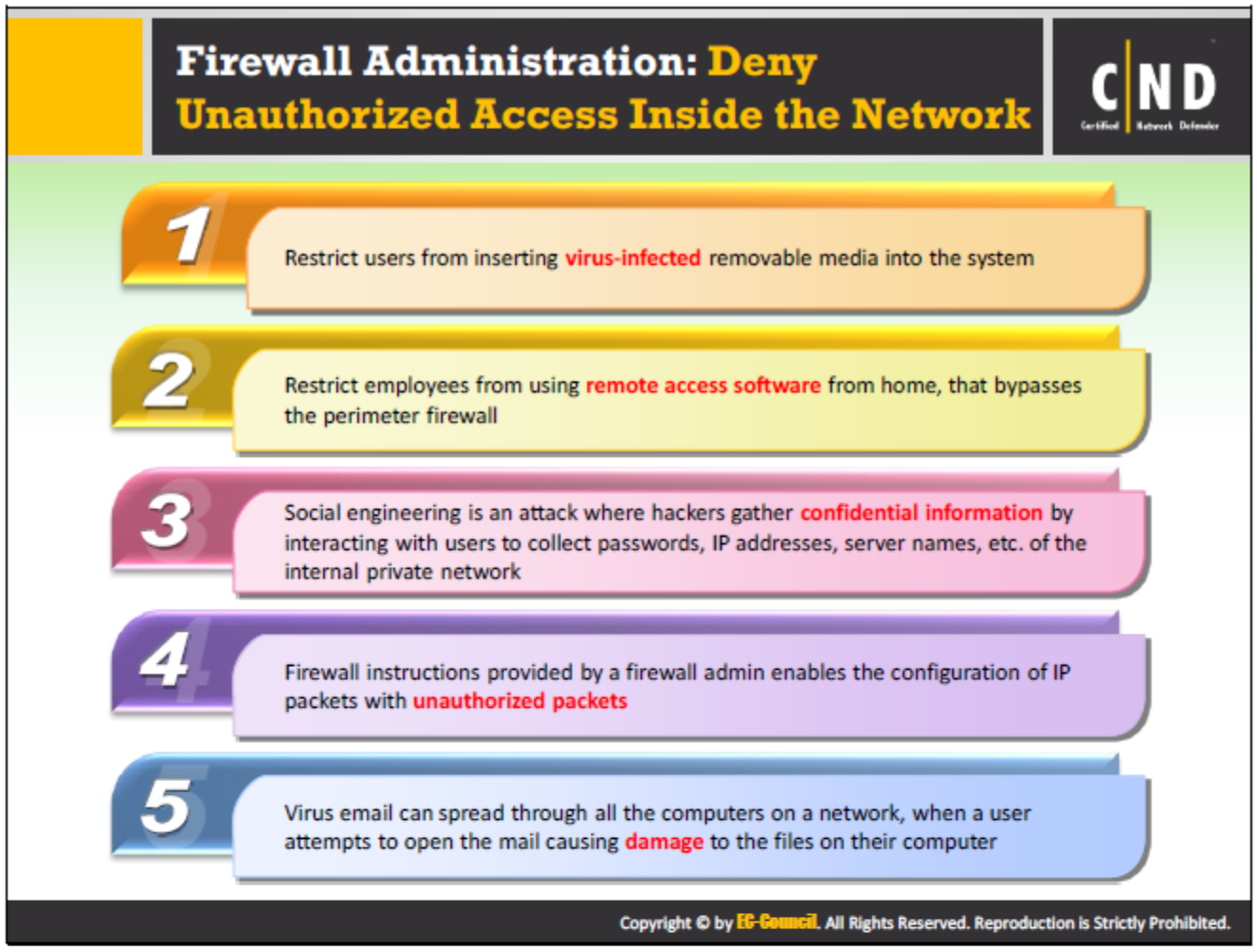
Firewalls are equipped with a real time packet filtering mechanism that checks all the packets for their malicious content and drops the packets if they are suspicious. Organizations should use SSL and HTTPS protocol services while accessing corporate resources using public networks, this will ensure the consistency of a firewall policy as these protocols pass only encrypted information.

To prevent unauthorized public network access, you should scan the network regularly for open ports and disable them to ensure proper utilization of any remotely accessible resources.

Netstat.exe is the built-in Windows network application, providing a list of open connections.

Steps to check for an open port are

- **Step 1**: Click **Start**, in the search box type **command** and press **Enter**
- **Step 2**: In command prompt, type **`netstat -an`**
- **Step 3**: Press **Enter**, this will list all of the open ports

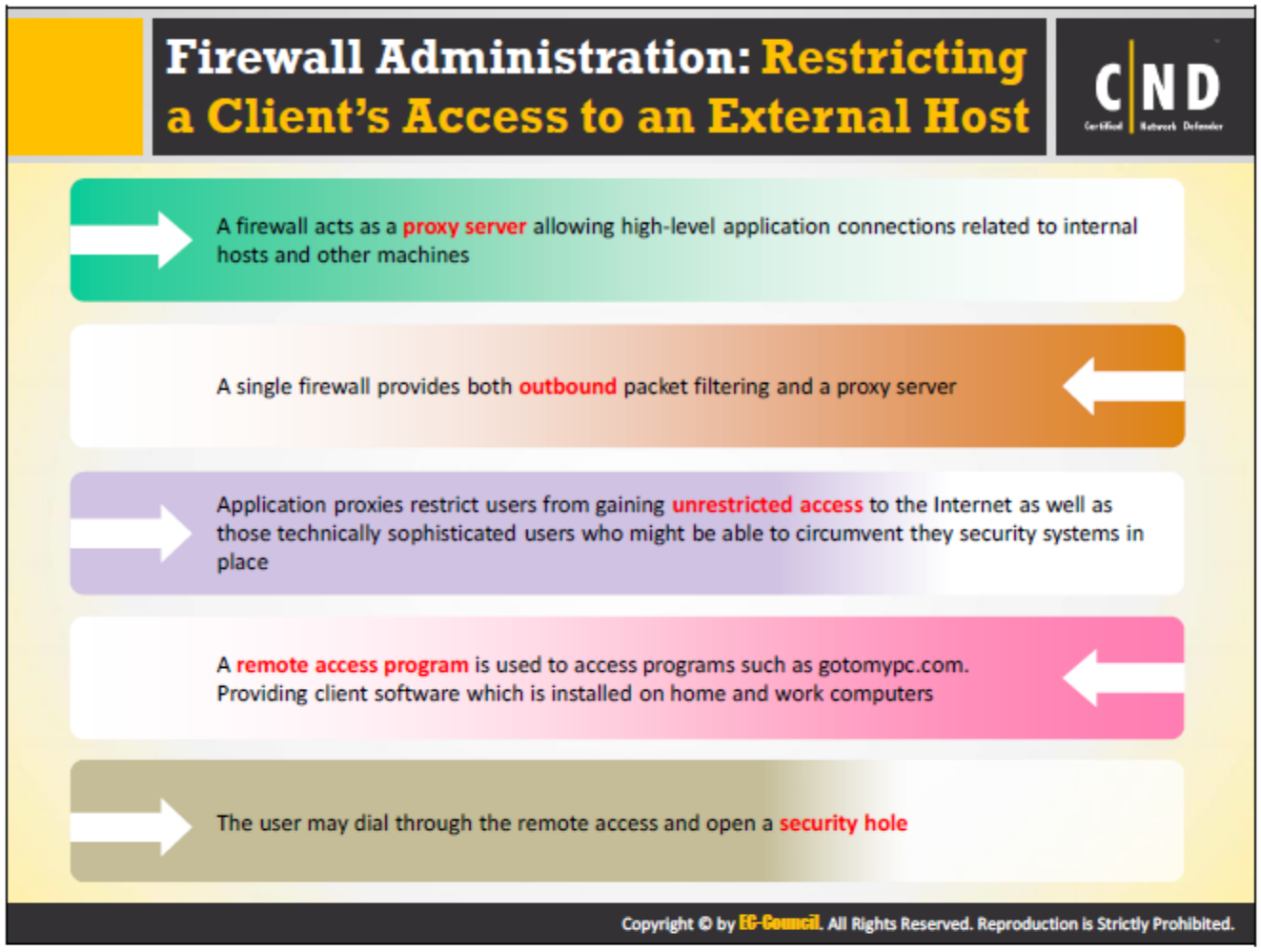


Restriction of unauthorized access from inside the network prevents the user from running malicious programs, installation of suspected software, etc.

Necessary security measures to prevent unauthorized access inside the network are

- Prohibit users from installing plug-and-play devices such as flash drives which may be virus-infected and when executed can corrupt the data present in the host system or network.
- Restrict employees from using remotely available corporate resources from public networks such as an internet café or free public Wi-Fi (e.g. hotels), which bypasses the perimeter of the firewall.
- Educate employees on the topic of social engineering. Which is an attack involving hackers who build confidence with the unsuspecting user to trick them into collecting personal information such as user credentials, server information, IP addresses etc. which is then used to perform network attacks against an organization.
- Firewall instructions are provided by well-trained firewall administrators enabling users to configure their firewall to filter IP packets for detection of unauthorized packets.
- Emails containing viruses can spread through all the computers on a network, when the user attempts to open the mail. Using an updated internet security solution can prevent such email attacks.

- Providing access only to required documents and files. This controls access to those people working inside an organization that do not have access to all the sensitive information.
- Account rights should be carefully structured in order to facilitate proper data access.
- Proper training to users can prevent unauthorized access inside an internal network. There are limits to this strategy but educating users has many threat prevention benefits.



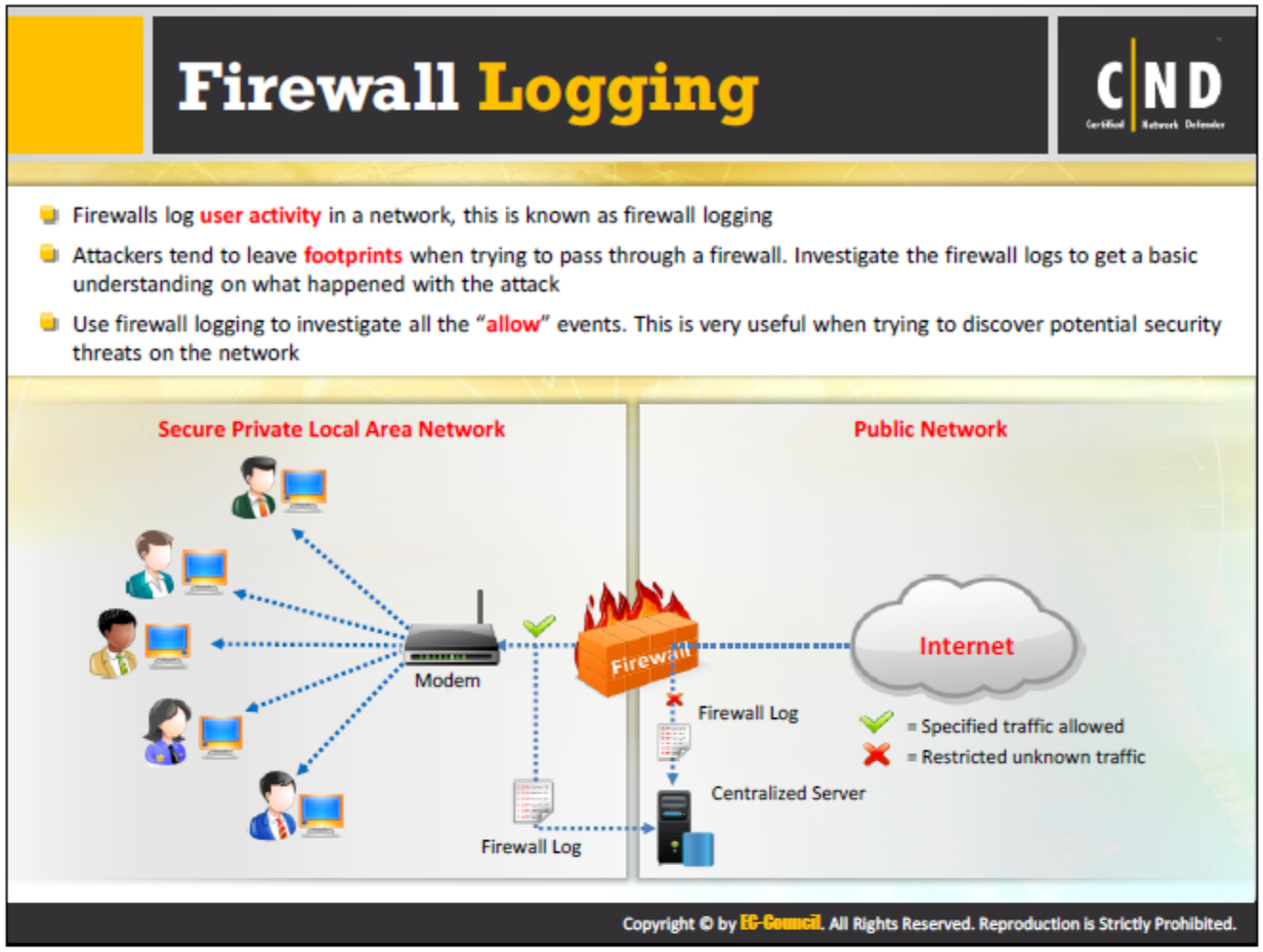
A client should not have direct access to an external host which could make it vulnerable to threats. As a result, the client should access the host through the firewall. The firewall would act as a proxy server allowing high-level application connections related to internal hosts and other machines. A single firewall acts as both packet filtering at the application level and a proxy server at the domain level. Application proxies restrict users from gaining unrestricted access to the Internet. Technically sophisticated users might be able to circumvent the security systems altogether.

Vulnerable external hosts gather sensitive information from clients such as IP addresses, types of security, level of security, server locations and remote access credentials. Remote access to programs can be useful such as gotomypc.com providing remote access to work systems, the concern is the risks associated with these, such as password sniffing, packet stealing and IP Spoofing.

The user might dial through the remote access to connect with an illicit server and application, which opens a security hole.

It is possible to restrict authorized access to areas by employing the following policies:

- Allow only internal IP addresses to pass through the firewall.
- Block traffic containing private addresses.
- Block all outbound traffic from VLAN workgroups.
- Block broadcast traffic and all traffic from servers that require no connectivity with any of the external networks.



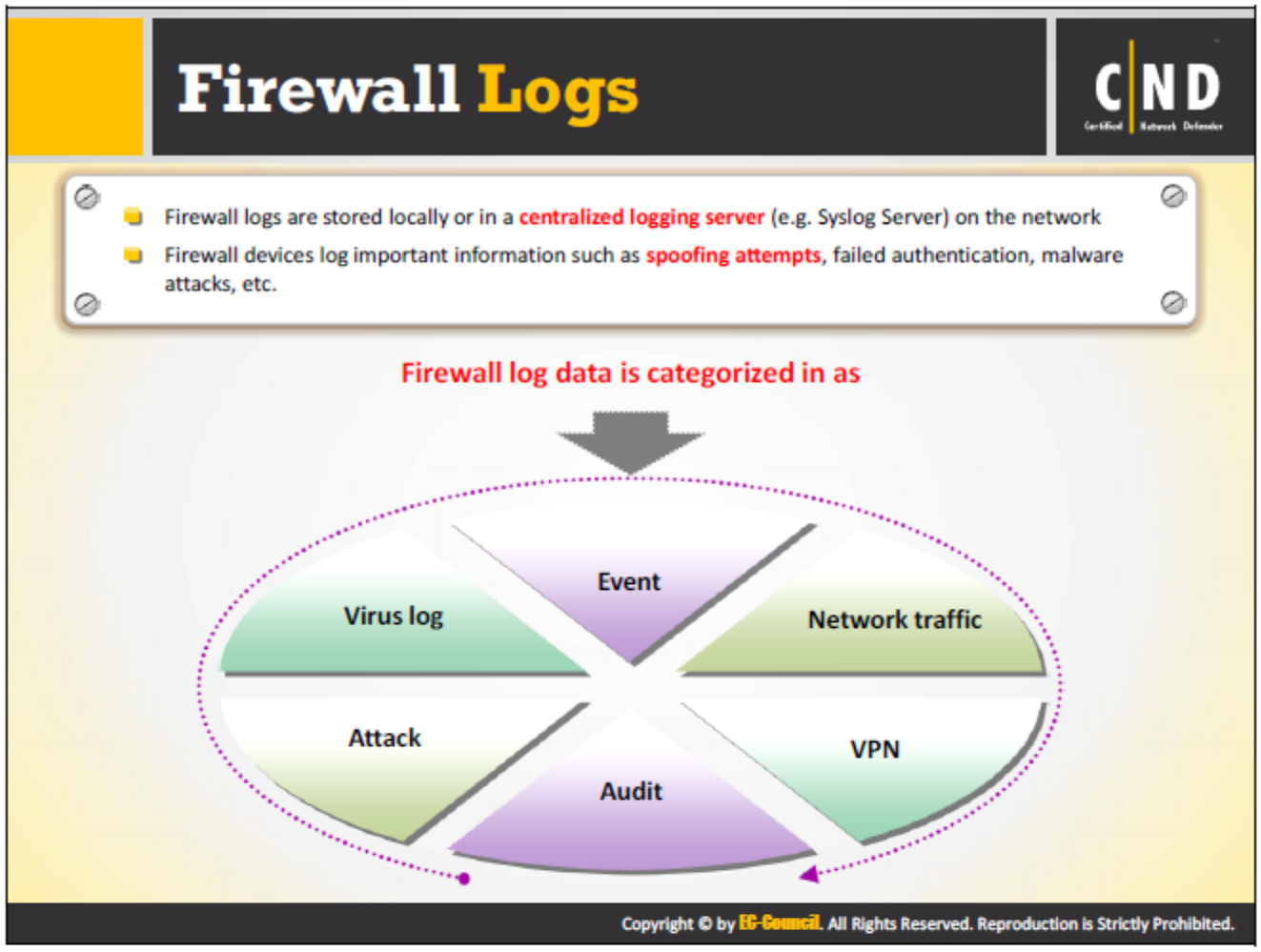
Firewall logging is the ability of a firewall to record or log the details of user's activities on a network. Log file maintenance is crucial to overcoming security breaches, as the attackers unknowingly leave their footprints when trying to pass through a firewall. Firewall logs can help you investigate such incidents.

Firewall logs contain information about activities such as port scans, unauthorized connection attempts, activities from compromised systems and security threat attempts at the boundary of the network. It helps you trace the source of the network attacks.

An administrator can disable the firewall logs temporarily, while troubleshooting or monitoring its behavior. A centralized secure server should contain the firewall logs in order to protect it from the attackers. Otherwise, an attacker could delete the logs which contain their footprints.

If any suspicious activity is detected in a firewall log, it should be handled immediately and all necessary actions taken to avoid any security incidents.

Firewall analyzer, is an application for firewall log analysis providing many features to gather, analyze, and report any logs found.



Firewall log data contains information such as failed authentication attempts, abnormal protocols, virus attacks, etc. Firewall logs are huge datasets to look into. Especially for big enterprises with more than one or two firewalls. These, record many log files with a very large number of log file entries every day. Firewall logs are stored locally or in a centralized logging server (Syslog Server) on the network. The collection of firewall log data helps administrators to analyze the transactions between the source IP address and the destination IP address. A firewall creates a huge log volume (approximately 10000 or even more events /sec), it is necessary to use specialized software to collect and analyze them.

Firewall log data includes activities such as:

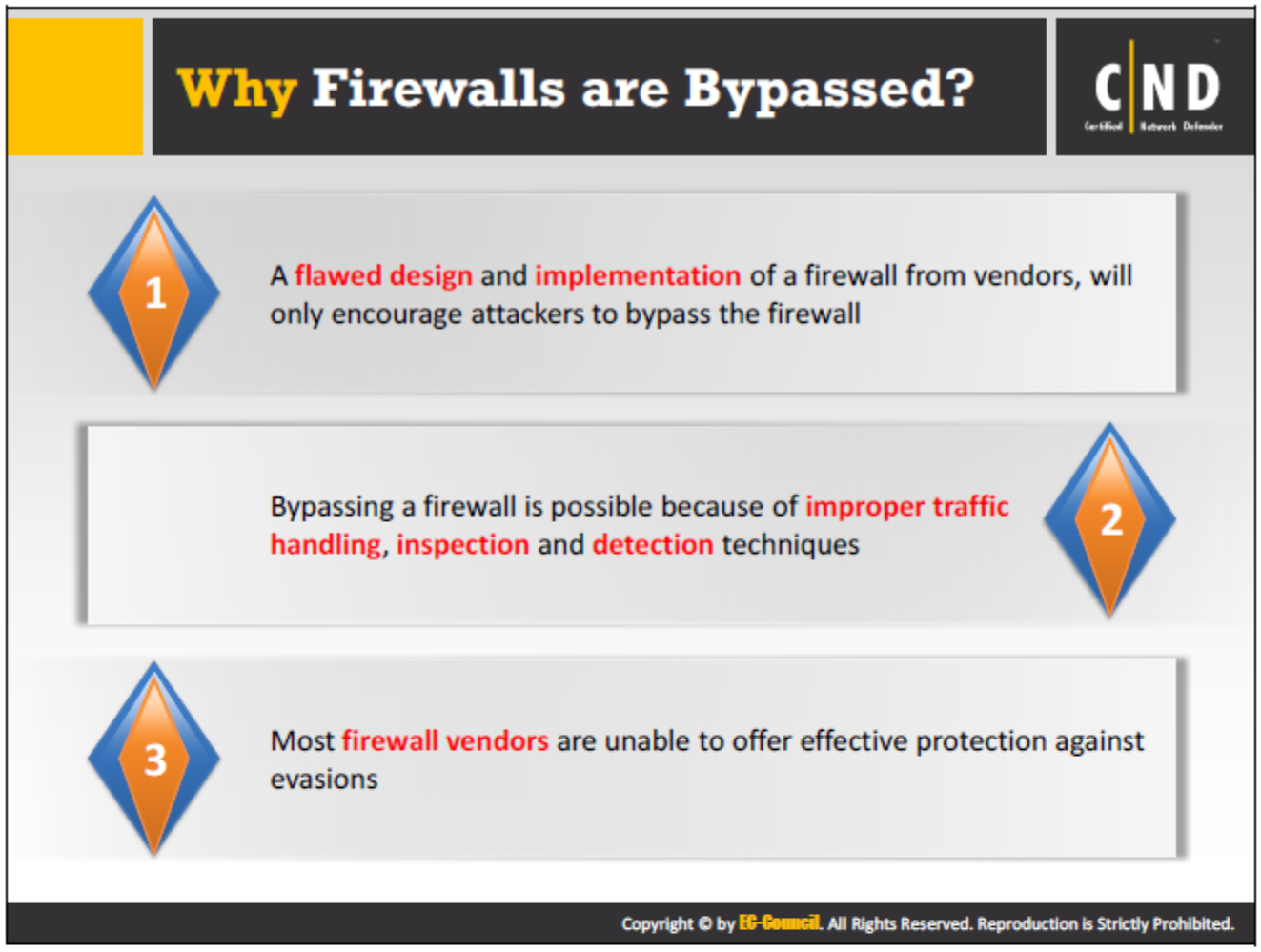
- Virus logs.
- Network and device attacks.
- Audit trail.
- Event logs.
- Network traffic.
- VPN connection establishment.

Importance of firewall logs:

- The firewall logs provide details regarding the status of the firewall.

Benefits of firewall logs include:

- Enhances network administration, troubleshooting and debugging.
- Creates baseline information for comparison.
- Provides a clearer outlook of the system.
- Provides solutions for better forensic analysis.



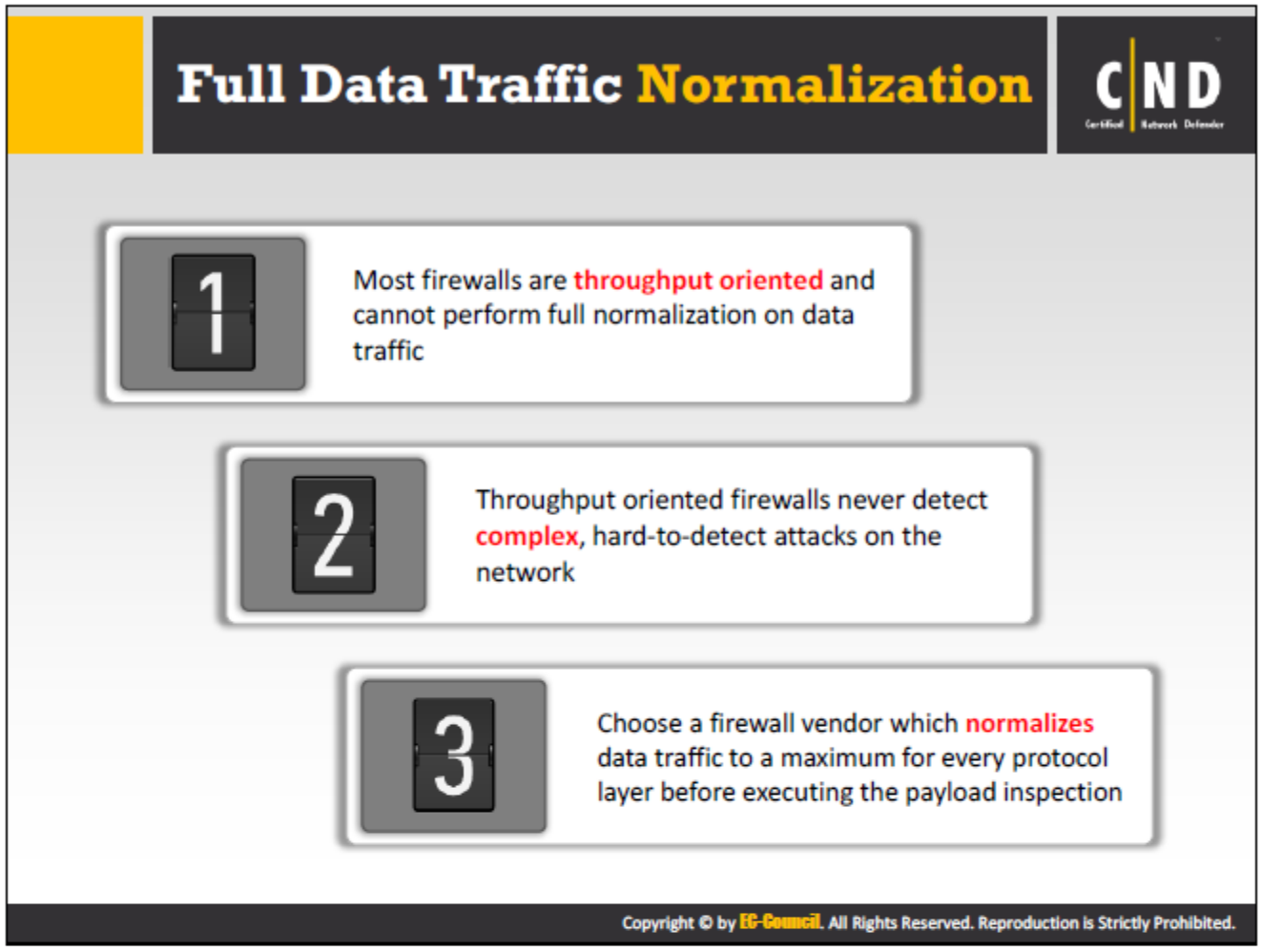
The flawed design and/or implementation of firewalls encourage attackers to bypass them. An attacker takes advantage of improper traffic handling, inspection, and detection techniques of a firewall to bypass it. Most of the firewall vendors are unable to offer effective protection against evasions.

An administrator should be aware of the following items to limit firewall evasion:

- Accept the fact that evasion can and probably will happen.
- Determine the level of protection offered by a firewall against evasion.
- Measure the level of risk if such an attack happens.
- Enhance security monitoring procedures continuously.
- Perform advanced penetration testing and assess intrusion detection systems.

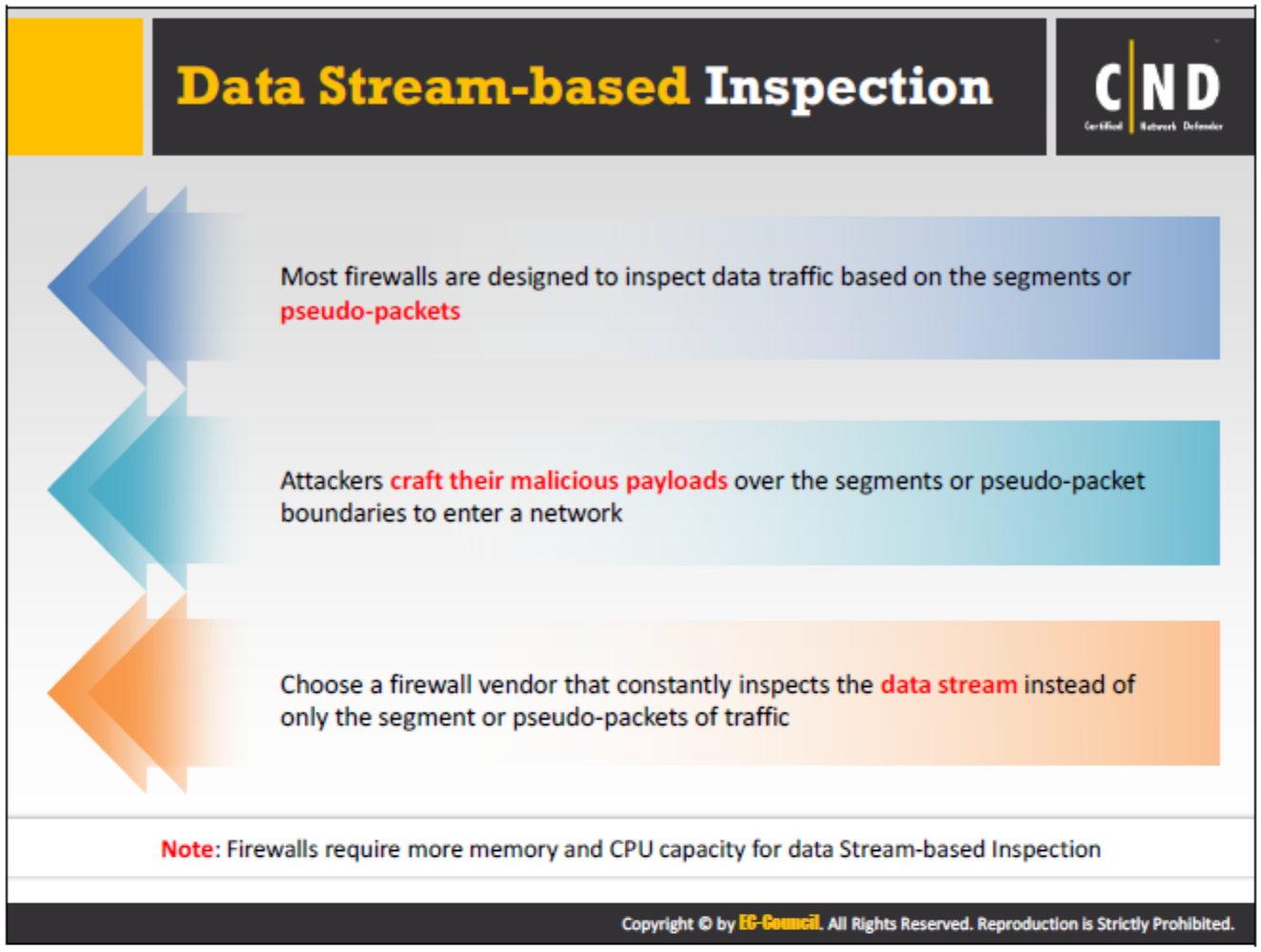
To prevent users from bypassing the firewall:

- Block access from their computers to port 80 anywhere on the Internet.
- All common proxy ports should be blocked to prevent users from using an open proxy server on the Internet.
- TCP ports including 20, 21, 80, 443, 3128, 8000, 8080 should be blocked.
- A default-deny approach will restrict access by default and every access needed (port, protocol, service, network) must be explicitly enabled.

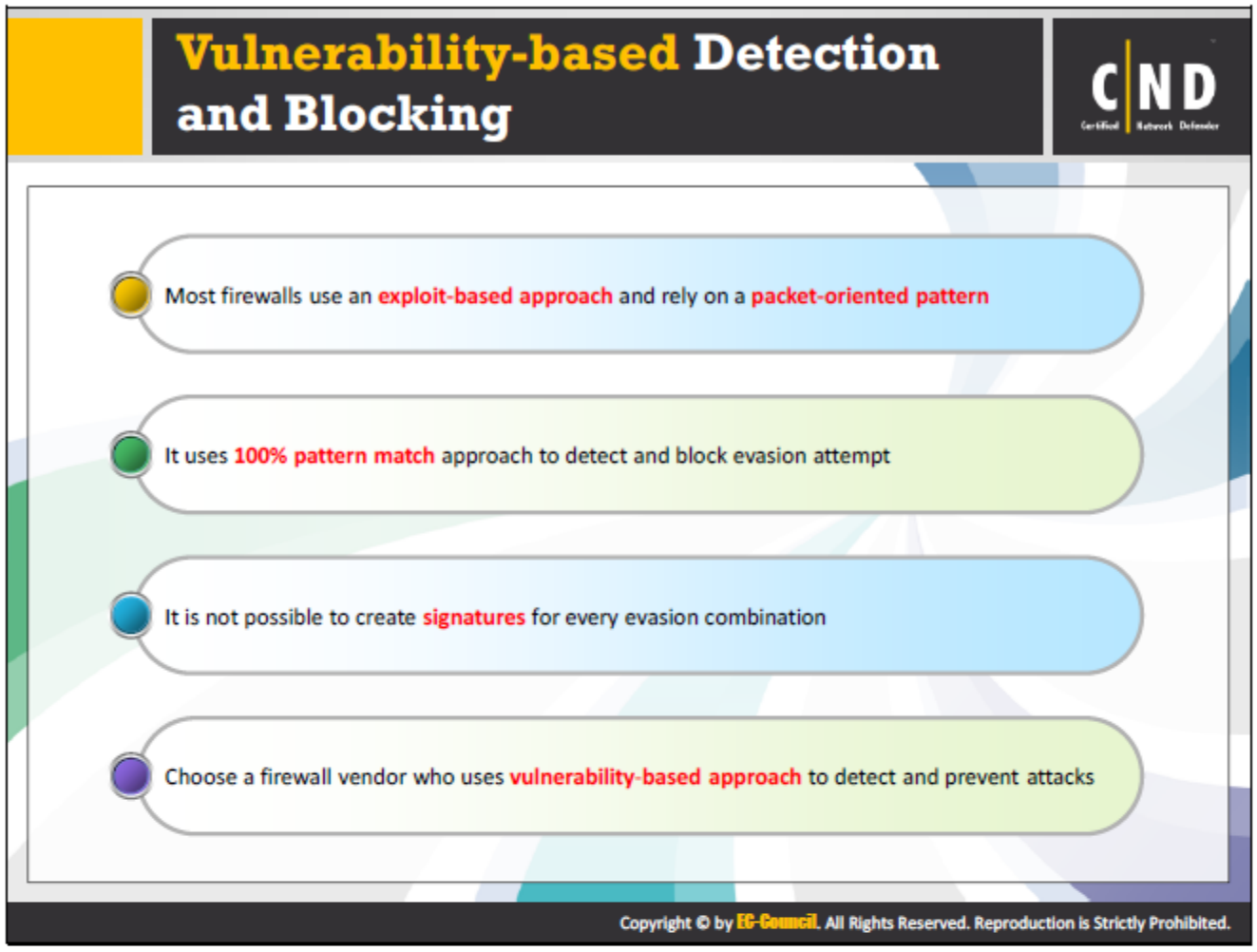


Normalization is one of the techniques to prevent firewall evasion. Full data traffic normalization can prevent firewall evasion by keeping you away from known attacks or by restricting access to internal machines from an external host. Especially when a firewall detects a probe or an attack.

Firewall design must incorporate and optimize the inline throughput performance in a network to prevent attacks. Firewall vendors use shortcuts and execute only partial normalization and inspection. For instance, TCP segmentation handling is very limited and done only for selected protocols or ports (if not disabled by default). Evasions exploit these shortcuts and weaknesses in normalization and inspection processes. Administrators should choose the firewall vendor that normalizes data traffic to a maximum on every protocol layer before executing the payload inspection.



A firewall should be able to examine a constant data stream instead of fragments or pseudo-packets. This vital design issue is extremely difficult to change. Especially in the case of hardware-based products, the redesign of security devices would require significant R&D. Data stream based inspection requires more memory and CPU capacity to perform efficiently. For many vendors, this is impossible and the inspection scope is sacrificed. The attacker can take advantage of this by spreading attacks over segments or pseudo-packet boundaries. The administrator should choose the firewall vendor who implements a constant data stream inspection instead of segments or pseudo-packets of traffic.



Some firewall vendors implement an exploit-based approach to detect and block exploit attempts. An exploit-based approach works on the principle of a packet-oriented pattern (signature). It uses a 100% pattern match approach to detect and block evasion attempts. However, it is not possible to create signatures for every evasion combination, new attack patterns and signatures are invented daily. Firewalls with exploit-based approaches cannot detect and block all firewall evasion attempts. Relying on these types of firewalls can pose a risk to the organization's network.

Use a firewall with a vulnerability approach instead. These are implemented and used in the organization's network. Vulnerability-based protections block exploitation attempts on both the network and the application layers.

Secure Firewall Implementation: Best Practices

- Filter unused and common **vulnerable** ports
- If possible, create a **unique user ID** to run the firewall services. Rather than running the services using the administrator or root IDs
- Set the firewall ruleset to deny all traffic and enable only the services required
- Change all the **default passwords** and create a strong password which is not found in any dictionary. A strong password to ensure brute force attacks also fail.
- To enhance the **performance** of the firewall, limit the applications which are running
- Configure a **remote syslog server** and apply strict measures to protect it from malicious users
- Monitor **firewall logs** at regular intervals. Include them in your data retention policy
- Immediately investigate all **suspicious log** entries found
- Backup the firewall logs on a set **schedule**. Store these backups on a secondary storage device for future reference or for any legal issues arising from an incident
- Perform **audits** at least once a year on the firewalls. This is done to evaluate the standards implemented in securing an organization's IT resources

Secure Firewall Implementation: Best Practices (Cont'd)

- Clearly define a firewall **change management** plan
- By default, **disable** all FTP connections to or from the network
- Catalog and review all **inbound** and **outbound traffic** allowed through the firewall
- Keep firewall rules as **granular** as possible
- Prioritize the rules in a proper **logical order**
- Ensure the implementation passes business and technology-based **risk assessments**
- Allow **secure Email access** through the firewall
- Set a default "**deny**" rule for inbound traffic with explicit "**allow**" rules
- Ensure all rules and objects follow standard **naming conventions**
- For easy management, always **group** similar rules together

Secure Firewall Implementation: Best Practices (Cont'd)

- ✗ Don't complicate firewall management by unnecessarily nesting rule objects
- ✓ Try to use the same ruleset for similar firewall policies within the same group object
- ✓ Add expiration dates to temporary rules and review them later for clean-up
- ✓ Run regular risk queries to identify vulnerable firewall rules
- ✓ Test the impact of a firewall policy change
- ✓ Clean and optimize the firewall rule base
- ✓ Schedule regular firewall security audits
- ✓ Monitor user access to firewalls and control who can modify the firewall configuration
- ✓ Update the firewall software on a regular basis
- ✓ Centralize firewall management for multi-vendor firewalls

Secure Firewall Implementation: Best Practices (Cont'd)

- Run the firewall as a unique user ID, instead of using an Admin or root ID ✓
- Specify the source and destination IP addresses as well as the ports ✓
- Change the default administrator password before connecting to public networks ✓
- Keep the firewall configuration simple ✓
- Eliminate redundant rules to ensure secure firewall configuration ✗
- Set specific policy configurations with a minimum level of privilege ✓
- Only run the required services ✓

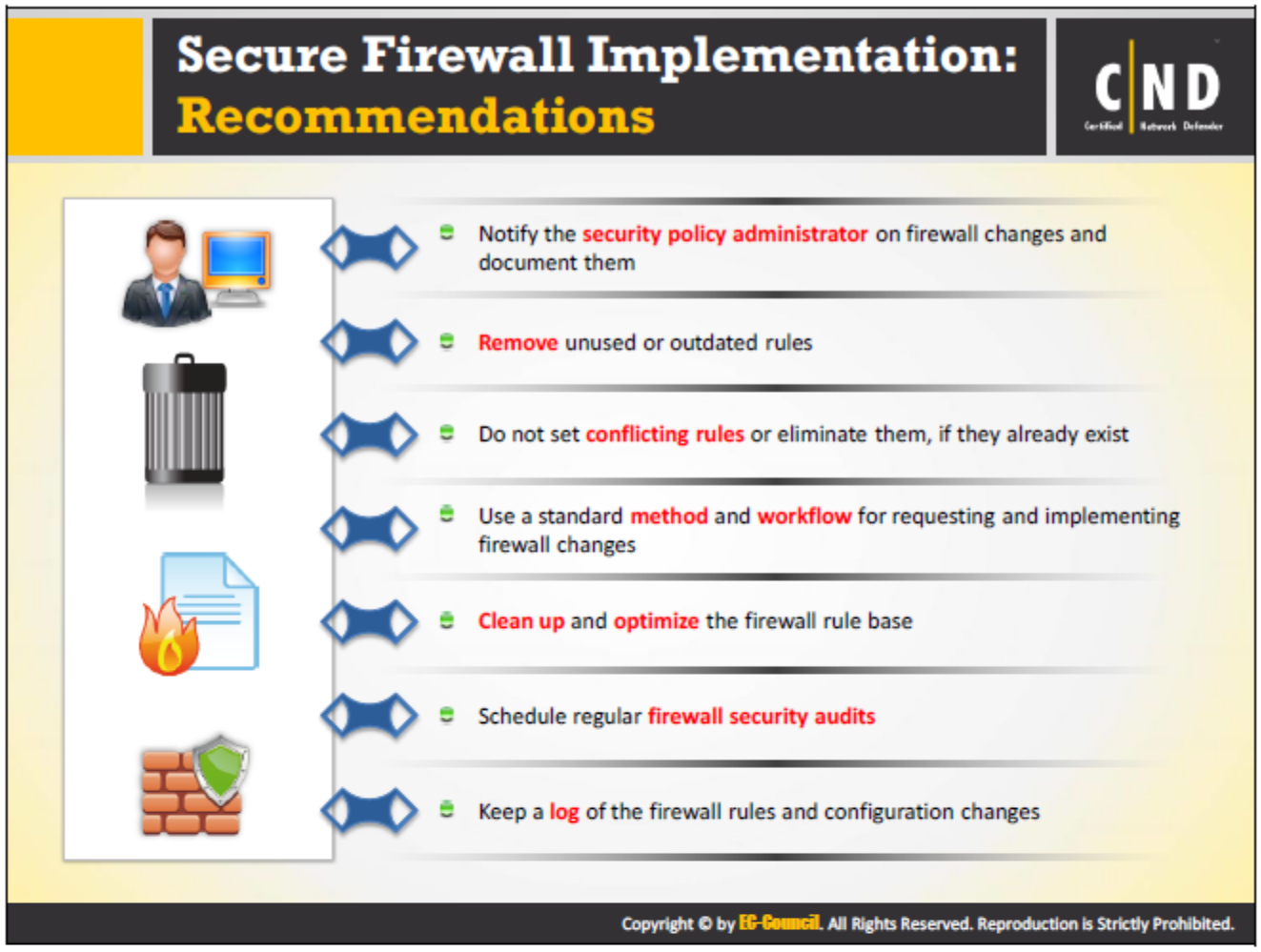
The following best practices will help you harden the security in your firewall.

- Filtering unused and vulnerable ports on a firewall is an effective and efficient method of blocking malicious packets and payloads. There are different types of filters in firewalls ranging from simple packet filters to complex application filters. A defense in depth approach using layered filters is a very effective way to block attacks.
- Configuring administrator accounts to run a firewall depends on the security requirements of the organization and different administrative roles the organization requires. A role defines the type of access the associated administrator has to the firewall system. If possible, create a unique ID to run the firewall services rather than running it as administrator or root.
- While creating a firewall ruleset, organizations should first determine what types of traffic is needed to run the approved applications. Administrators need to set firewall rules to deny all the traffic and allow only those services the organization needs.
- Firewalls use a complex rule base to analyze applications and determine if the traffic should be allowed through or not. Setting up firewall rules to grant access to important applications and block the rest will improve the performance of the firewall.
- Administrators should ensure the date, time, and time zone on the remote syslog server matches the network configuration, in order for the server to send syslog messages. Syslog data is not useful for troubleshooting if it shows the wrong date and time. Also, configuring all network devices to use NTP ensures a correct and synchronized system clock on all network devices.
- Network administrators should monitor the firewall logs at regular intervals even if the company's management policy allows for some private use of its equipment. Monitoring what websites employees are visiting, what files employees are sending and receiving, and even the content in their e-mails will assist administrators in maintaining the network securely.
- Logging firewalls ‘allow’ actions offer greater insight into malicious traffic and tracking firewall ‘deny’ actions help administrators identify threats.
- Take regular backups of the firewall logs, at least on a monthly basis and store these backups on secondary storage devices for future reference or for legal issues in case there is an incident. The best way to achieve this is to use a scheduling function in the firewall. Backup the firewall before and after making a change in its rules and ensure that the backup configuration file is usable.
- Administrators should perform audits at least once a year on firewalls to evaluate the standards implemented to secure the organization's IT resources. This will offer a record of all the files employees open and even failed attempts to access files. Ensuring every change is accounted for will greatly simplify audits and help the daily troubleshooting.
- Firewalls cannot secure the network from internal attacks. Organizations are required to implement different strategies such as policies that will restrict employee usage of

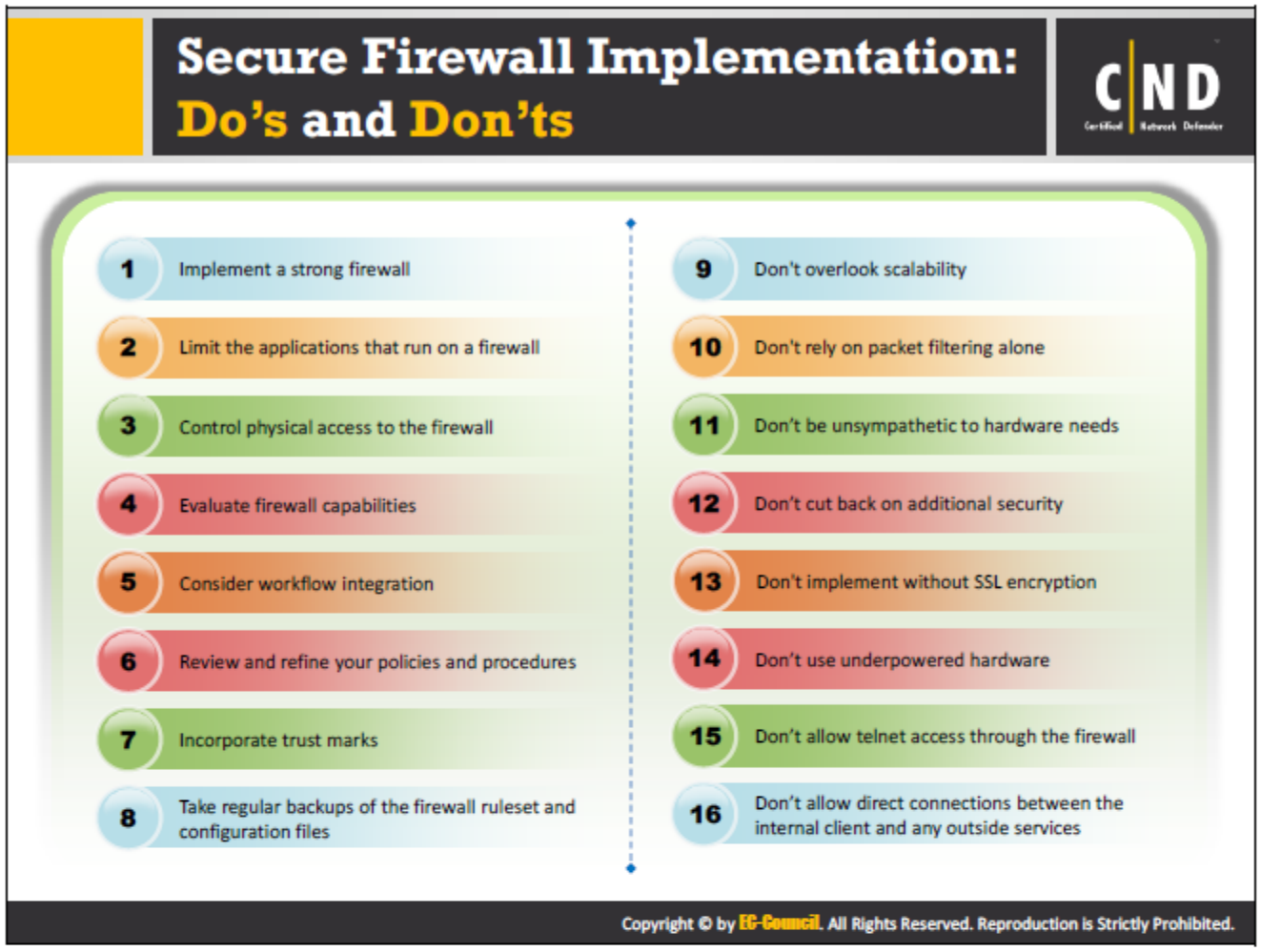
external devices in the internal network. For preventing any internal network attacks, administrators should install monitoring software that will help detect any suspicious internal activity.

- Clearly defining a centralized firewall management plan and a documented process can help prevent unwanted changes to the current configuration of the network. It can limit the chance of a change, opening vulnerabilities in network security.
- The effectiveness of any firewall solution depends on the rules with which it is configured. In general, a firewall is configured to monitor inbound and outbound traffic and to protect a network in which it is configured. It also monitors the source and type of traffic traversing the network.
- Most organizations use it for protecting the network environment from threats and in tracking the source of a threat. Augmenting a firewall ruleset with an effective logging mechanism makes it an effective security mechanism to protect the network.
- Administrators should set a default 'deny' rule for inbound traffic with explicit 'allow' rules. Deny policies at the end of a ruleset ensures you catch traffic that is trying to go to the wrong zone. It is significant to cover every combination.
- A firewall rule should be properly prioritized based on the security requirement of the organization.
- Organizations should consider monitoring employee's e-mail messages through the firewall. They should create a separate email network zone that is firewalled from both the DMZ and the internal network. Then place both the email and the webmail servers in that zone. This enables the organization to allow secure email access through the firewall.
- Manage the lifecycle of a firewall rule policy by enforcing an expiration date. This will help administrators clean up newly created temporary rules for new services. When an expiration date is set for a rule, the administrator can delete the rule after its lifetime or can extend its duration if needed.
- Always perform testing of the firewall policies before implementing them in the network. Testing a firewall can discover unexpected errors in the implementation by assessing firewall performance, network traffic and other devices. These details provide the network administrator with a view on how the proposed changes in the firewall configuration will affect the environment.
- Auditing firewall security policies ensures the firewall rules implemented are according to the security regulations of an organization. It is the responsibility of the network administrator to perform firewall security audits to identify policy violation activities.
- The organization needs to ensure they upgrade their firewall to the latest patches and updates released by the firewall's vendor. Any delay in upgrading to the latest version can impact the security of the network. Upgrading to the latest firewall version minimizes the chances of a vulnerability in the network. It is also possible to conduct vulnerability assessments on the firewall, enabling an administrator to easily assess the flaws and weaknesses.

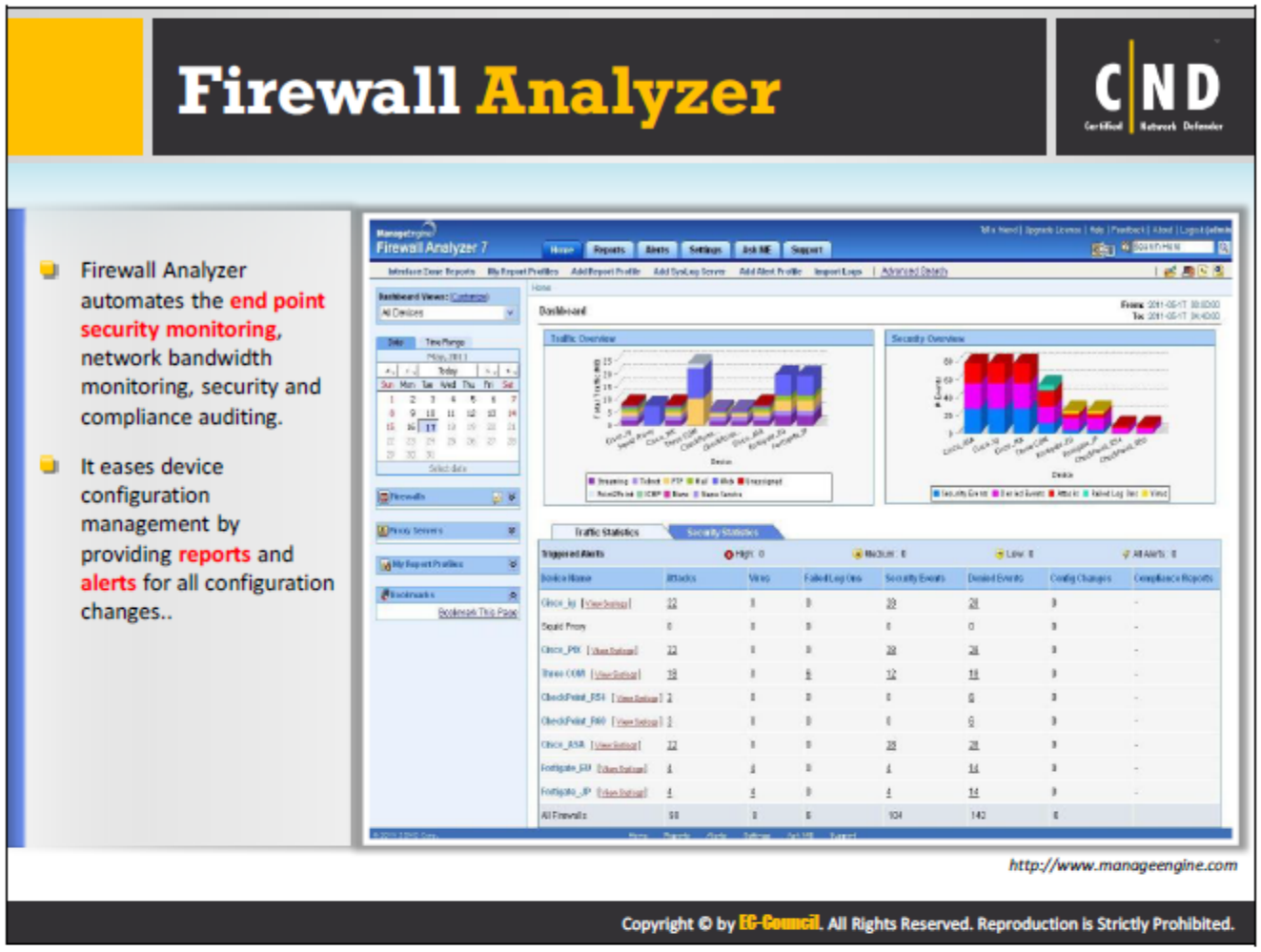
- The firewall administrator needs to ensure they remove the firewall rule base regularly as it improves firewall security, firewall performance and efficiency. Cleaning the firewall rule base prevents security and management issues.
- Restrict unauthorized access to prevent any modification in the firewall configuration. Organizations can implement access permissions which will only permit authorized users to make changes to the firewall configuration.
- Most organizations implement firewalls from different vendors and the firewall configuration architecture differs from one organization to another. The organization needs to ensure that only skilled personnel are looking after the firewall administration and maintenance.
- Always filter packets for the correct source and destination address in order to prevent attackers from accessing the network.
- Always make sure to change the passwords regularly, at least every six months.
- The configuration of the firewall is kept simple and should meet company requirements. Periodic review of the firewall configuration helps maintain the firewall security.
- Always provide minimal access to the firewall in order to avoid any incidents.



- Administrators should document any changes they make to the firewall. With firewalls, it is especially critical to document the rules they add or change so that other administrators know the purpose of each rule and who to contact about them. Good documentation can make troubleshooting easier and reduces the risk of service disruptions which are caused when an administrator deletes or changes a rule they do not understand.
- Organizations can generate analysis reports to evaluate firewall access rules. This assists them in identifying rules that overlap or conflict with other rules in the access rule policy. Delete, move or edit conflicting rules using the data from the report. Organizations can develop an easier to use and more efficient access rules policy if they eliminate unnecessary rules.
- Implement a consistent workflow solution to manage and streamline the firewall change process. Identify potential risks and fix configuration errors before making changes to the firewall. Reduce the time required to evaluate and implement the changes to support the network.



- A firewall should include intrusion prevention and detection capabilities to guard against denial of service attacks (DDoS). The consequences of not having these measures in place will get worst in the future, if a DDoS incident occurs.
- While implementing a firewall do not overlook scalability. Most firewall vendors claim they can scale up to thousands of devices. Determine what that actually means in terms of management and the ability to perform under stress.
- After choosing a firewall that meets the business requirements of an organization, test the firewall on a live production environment. The organization determines the network requirements and evaluates the product capabilities accordingly. The test should determine whether the chosen solution actually performs as expected.
- Installation of proxy servers assures security as it provides access only to selective users.
- When implementing a firewall solution, organizations need to focus on the hardware required for the implementation. Refrain from buying more technology. First, make sure it works for you and improves your security.
- The idea behind a workflow in firewall management is a natural extension from the change management functionality. Manage the change process to ensure only the correct rules are created. Most vendors offer complimentary workflow products to integrate their core capabilities with change-management workflow tools. This may not be important if your organization has a well-defined process and supporting tools already in place.



A firewall analyzer is a program that collects, correlates, and analyzes security device information from enterprise-wide heterogeneous firewalls, proxy servers from Cisco, Fortinet, CheckPoint, WatchGuard, NetScreen, and more. It is browser-based firewall/VPN/proxy server reporting solution.

It generates scheduled reports on firewall traffic, security breaches, and more that help network administrators secure networks before security threats arise, avoid network abuses, manage bandwidth requirements, monitor web site visits, and ensure appropriate usage of a network by employees.

A firewall analyzer, analyzes the firewall and proxy server logs and provides support with answering issues such as:

- Who are the top web surfers and the websites they visit?
- Which of the servers receives the maximum number of hits?
- Are there hacking attempts?
- Where do these attempts originate?
- How much network activity is originating from each side of the firewall?

Source: *http://www.manageengine.com*

Firewalk is an active reconnaissance network security tool for enumerating firewalls. It attempts to determine what layer 4 protocols a firewall will allow to pass through to internal hosts.

Firewalk sends out TCP or UDP packets with a TTL one greater than the targeted gateway/firewall. If the gateway/firewall allows the traffic, it will forward the packets to the next hop where they will expire and elicit an ICMP_TIME_EXCEEDED message. If the gateway host does not allow the traffic, it will likely drop the packets and there will be no response.

To get the correct IP TTL that will result in expired packets you need to ramp up the hop-counts.

Example Usage

- `nmap --script=firewall --traceroute <host>`
- `nmap --script=firewall --traceroute --script-args=firewall.max-retries=1 <host>`
- `nmap --script=firewall --traceroute --script-args=firewall.probe-timeout=400ms <host>`
- `nmap --script=firewall --traceroute --script-args=firewall.max-probed-ports=7 <host>`

FIGURE 7.1: Firewalk example

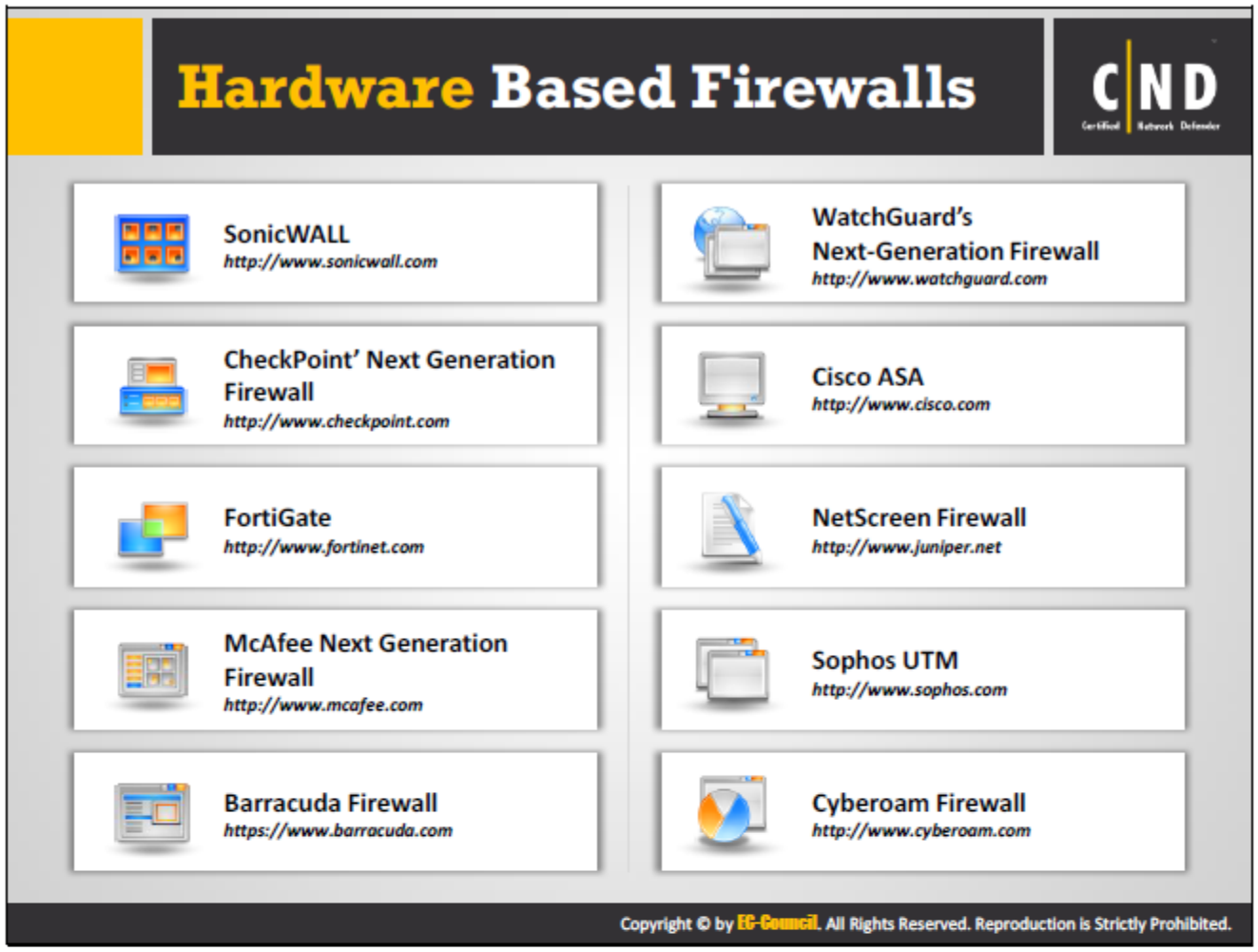
Source: *https://nmap.org*

WinGate Proxy Server is an integrated Internet gateway and communications server designed to meet the control, security and communication needs. WinGate Proxy Server's license options offer the flexibility to satisfy requirements to manage an enterprise, small business, or home network.

Features of Wingate include:

- Secure and manage Internet access for your entire network via a single or multiple shared internet connections.
- Enforce advanced, flexible access-control and acceptable use policies.
- Monitor usage in real time, maintain per-user and per-service audit logs.
- Stop viruses, spam and inappropriate content from entering your network.
- Provide comprehensive internet and intranet email services.
- Protect your servers from internal and/or external threats.
- Improve network performance and responsiveness with web and DNS caching.
- Ease administration burdens on your internal networks.

Source: *http://www.wingate.com*



Sonic WALL

Source: http://www.sonicwall.com

The Sonic Wall firewall is a tool that supports network security, secured remote access, and data protection. It applies Unified Threat Management (UTM) against an array of attacks, combining intrusion prevention, anti-virus and antispyware with application-level control of SonicWALL Application Firewall. It provides services for network firewalls, UTMs (Unified network management), VPNs (Virtual Private Network), backup and recovery, and anti-spam for email.

Check Point's Next Generation Firewall

Source: http://www.checkpoint.com

Checkpoint firewall products are used in education, energy, financial services, healthcare, Internet and media, manufacturing, public sector, and telecommunications sectors where this firewall is preferred.

FortiGate

Source: http://www.fortinet.com

Fortinet Firewall is a Network Security Solution that helps protect the network, users and data from continually evolving threats. It helps to secure and manage network security. It also offers a Data Center Firewall (DCFW), Unified Threat Management (UTM), and Next Generation

Firewall (NGFW) technologies. It is preferred for creating a secure connection between a protected private network and the Internet. It provides protection against today's wide range of advanced threats targeting applications, data, and users.

McAfee Next Generation Firewall

Source: http://www.mcafee.com

McAfee Next Generation Firewall delivers complete, centrally managed network security with availability, multi tenancy, evasion protection, application control, and flexible deployment options, including software, physical and virtual firewall appliances. This firewall uses application control, an intrusion prevention system (IPS), and evasion prevention into a single solution. It is the next-generation firewall solution to unite anti-evasion security with enterprise-scale availability. It defends critical assets, such as regulated data sources (customer, financial, and healthcare data), email and web servers, extranets, and data centers.

Barracuda Firewall

Source: https://www.barracuda.com

The Barracuda Spam Firewall is a hardware and software solution designed to protect email servers from spam, viruses, spoofing, phishing and spyware attacks. It controls 12 defense layers to provide industry-leading defense capabilities for any email server within a large corporation or a small business.

WatchGuard's Next-Generation Firewall

Source: http://www.watchguard.com

The Watch guard's next generation firewall provides security inspection that blocks attacks and unwanted traffic without stopping Internet usage. It provides users with a platform for network traffic inspection and enforces a network security policy, with state-of-the-art security and compatibility. It has secure throughput and with real-time visibility tools.

Cisco ASA

Source: http://www.cisco.com

The Cisco ASA firewall enables businesses to segment campus networks and secure data center environments by integrating firewall security directly into the network infrastructure. .

NetScreen Firewall

Source: http://www.juniper.net

The NetScreen firewall provides a broad range of options from all-in-one security and networking devices to chassis-based data center security solutions that can secure any size enterprise data center or service provider with performance, functionality, and security options. Support for fast, secure, data center and enterprise operations, with performance and scalability, session volumes, and large-scale connectivity.

Sophos UTM

Source: http://www.sophos.com

Sophos gives complete security, from the network firewall to web and application control, in a single modular appliance. The Web Application Firewall intercepts traffic to servers using a reverse proxy with dual scanning engines and attack pattern recognition. It uses layered protection to prevent APTs, command and control traffic and targeted attacks.

Cyberoam Firewall

Source: http://www.cyberoam.com

The Cyberoam Firewall offers stateful and deep packet inspection for network, application and user identity-based security. It protects organizations from DOS, DDoS and IP Spoofing attacks. It helps with policy creation for multiple security features through a single interface.

Comodo Internet Security Pro 7

Source: http://www.comodo.com

Comodo Internet Security Pro 7 offers protection against viruses and malware, focusing on detection and prevention. Comodo Internet Security Pro 7 offers protection against Viruses, Trojans, Adware, Spyware and other Malware threats. It contains Auto Sandbox Technology, which provides protection from unknown threats.

Kaspersky Internet Security

Source: http://www.kaspersky.com

Kaspersky internet security provides protection from internet threats such as viruses, spyware, phishing, spam, rootkit, banners and online transactions for online banking and shopping. Additional features include dangerous website alerts, advanced parental control and safe social networking.

Total Defense Internet Security Suite

Source: http://www.totaldefense.com

Total Defense Internet Security Suite software provides protection for up to 3 devices against viruses, malware, spyware, spam, inappropriate content, lost files, and data corruption. Without all the hassle and includes Mobile Security in its protection circle. It provides features such as industry grade solutions, parental controls and mobile security.

Bitdefender Internet Security

Source: http://www.bitdefender.com

Bitdefender prevents unauthorized access to your private data. Internet security includes two-way firewall, provides parental control and many more. Other products of Bitdefender are Anti-Virus and mobile security.

Private Firewall

Source: http://www.privacyware.com

The Private firewall monitors the web traffic in accordance with native firewall. It prevents viruses, spyware and other online threats. It protects the system using application monitoring, registry monitors, process monitors and Email anomalies.

Outpost Firewall Pro

Source: http://www.agnitum.com

Outpost Firewall Pro provides standard firewall protection by scanning web traffic and preventing it from entering into the host systems. It keeps the ports closed when they are not in use to prevent attacks. It offers services such as malware blocking, information privacy and security, blocks incoming targeted attacks, makes PCs invisible and works without much utilization of computer resources to boost the system performance.

ZoneAlarm Pro Firewall

Source: http://www.zonealarm.com

ZoneAlarm firewall offers services such as a firewall, two-way firewall, private browsing, identity protection, Do Not Track methodology, Facebook Privacy scan, Online backup and a security privacy toolbar.

Norton Internet Security

Source: http://in.norton.com

Norton Internet security provides protection for almost all types of online threats such as viruses, worms and spyware. It provides safe online banking and shopping. It warns the user about social media scams, suspicious content and blocks harmful files from downloading. It also improves system performance by boosting system startup time.

Windows 8 Firewall Control

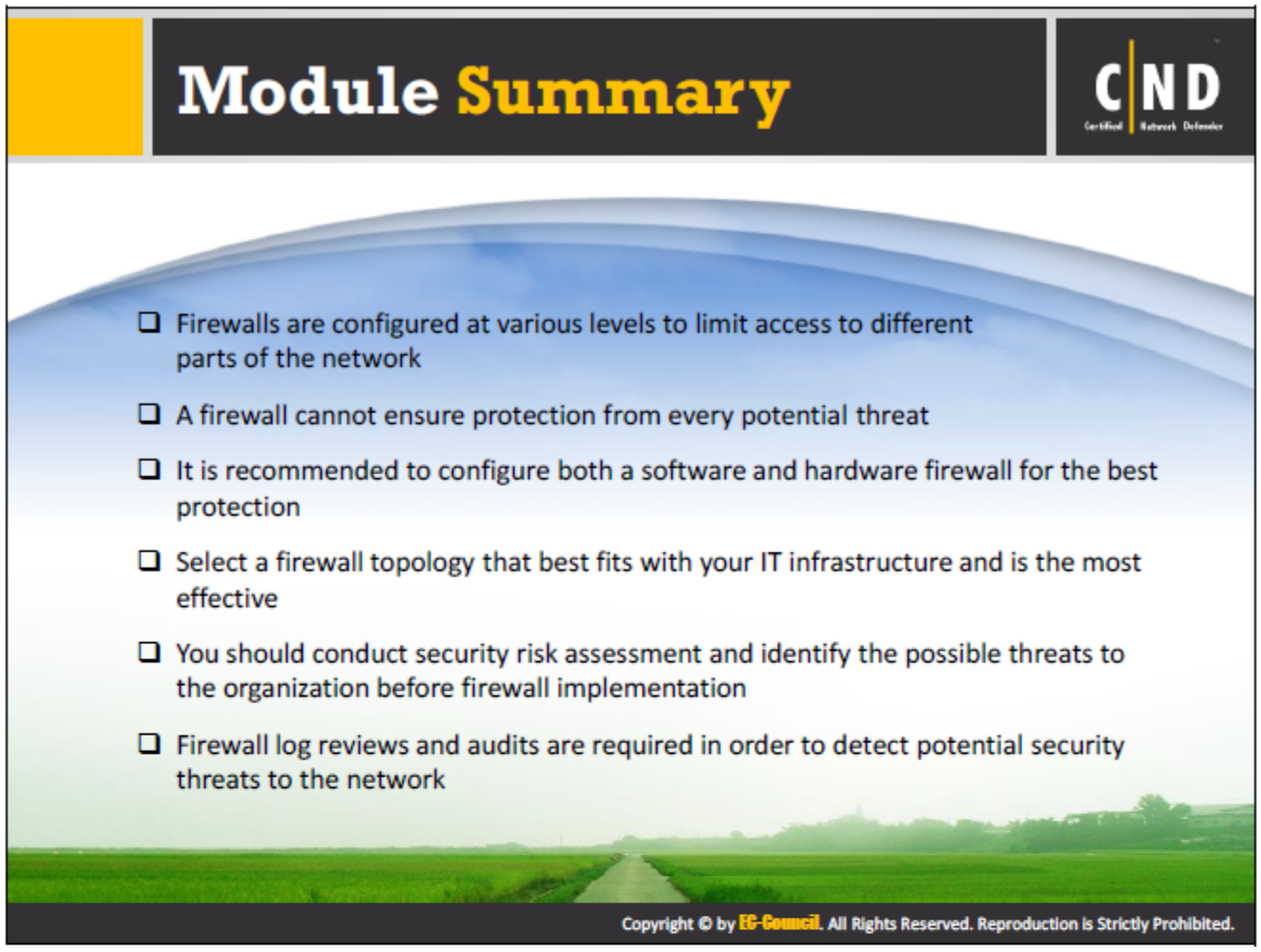
Source: http://www.sphinx-soft.com

Windows 8 Firewall Control protects both local and remote running applications from undesirable incoming and outgoing network activity in Windows operating systems. It provides services such as per-application security settings, instant notification of blocked activity and zone based network permissions. The program manages external connectivity by automatically synchronizing hardware firewalls.

McAfee Internet Security

Source: http://home.mcafee.com

McAfee internet security provides online security from threats and other internet attacks, which include viruses, worms, phishing websites and spywares. It offers protection to Windows and Mac operating systems, smartphones and tablets. It protects you from social networking by preserving the identity. It provides a cloud backup facility to backup and restore important files and information in case of a system breach.



In this module, you learned the various security measures, techniques, tricks, and recommendations on firewall design and implementation. The module showed you how to decide on the right topology, technology and solutions to be used for your network, based on the organization's need. It guided you on firewall administration activities to perform during firewall management. You also learned how to harden a firewall.