Static NAT is required to make internal hosts available for connection from external hosts.

It merely replaces port information on a one-to-one basis. This affords no protection to statistically translated hosts: hacking attacks will be just as efficiently translated as any other valid connection attempt.

NOTE FROM CLEMENT:
Hiding Nat or Overloaded Nat is when you have a group of users behind a unique public IP address. This will provide you with some security through obscurity where an attacker scanning your network would see the unique IP address on the outside of the gateway but could not tell if there is one user, ten users, or hundreds of users behind that IP.

NAT was NEVER built as a security mechanism.
In the case of Static NAT used for some of your servers for example, your web server private IP is map to a valid external public IP on a one on one basis, your SMTP server private IP is mapped to a static public IP, and so on.

If an attacker scan the IP address range on the external side of the gateway he would discover every single one of your servers or any other hosts using static natting. Ports that are open, services that are listening, and all of this info could be gathered just as if the server was in fact using a public IP. It does not provide this security through obscurity mentioned above.

All of the other answer are incorrect.

Reference used for this question:
STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 7: Network Address Translation.

QUESTION 842
Network cabling comes in three flavors, they are:

A. twisted pair, coaxial, and fiber optic.
B. tagged pair, coaxial, and fiber optic.
C. trusted pair, coaxial, and fiber optic.
D. twisted pair, control, and fiber optic.

Correct Answer: A
Explanation:
Network cabling comes in three flavors: twisted pair, coaxial, and fiber optic.

Twisted pair
Twisted pair cabling is a form of wiring in which two wires (the forward and return conductors of a single circuit) are twisted together for the purposes of canceling out electromagnetic interference (EMI) from external sources. This type of cable is used for home and corporate Ethernet networks. Twisted pair cables consist of two insulated copper wires. There are three types of twisted pair cables: Shielded, Unshielded and Foil Fiber Optic cable

An optical fiber cable consists of a center glass core surrounded by several layers of protective material. The outer insulating jacket is made of Teflon or PVC to prevent interference. It is expensive but has higher bandwidth and can transmit data over longer distances.

Coaxial cable
Coaxial lines confine the electromagnetic wave to area inside the cable, between the center

conductor and the shield. The transmission of energy in the line occurs totally through the dielectric inside the cable between the conductors. Coaxial lines can therefore be bent and twisted (subject to limits) without negative effects, and they can be strapped to conductive supports without inducing unwanted currents in them and though.

The most common use for coaxial cables is for television and other signals with bandwidth of multiple megahertz. Although in most homes coaxial cables have been installed for transmission of TV signals, new technologies (such as the ITU-T G.hn standard) open the possibility of using home coaxial cable for high-speed home networking applications (Ethernet over coax).

See the following page for more details: http://fcit.usf.edu/network/chap4/chap4.htm

Reference used for this question:

KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 101.
Wikipedia at http://en.wikipedia.org/wiki/Networking_cables

QUESTION 843
What type of attack involves IP spoofing, ICMP ECHO and a bounce site?

A. IP spoofing attack
B. Teardrop attack
C. SYN attack
D. Smurf attack

Correct Answer: D
Explanation:
A smurf attack occurs when an attacker sends a spoofed (IP spoofing) PING (ICMP ECHO) packet to the broadcast address of a large network (the bounce site). The modified packet containing the address of the target system, all devices on its local network respond with a ICMP REPLY to the target system, which is then saturated with those replies. An IP spoofing attack is used to convince a system that it is communication with a known entity that gives an intruder access. It involves modifying the source address of a packet for a trusted source's address. A teardrop attack consists of modifying the length and fragmentation offset fields in sequential IP packets so the target system becomes confused and crashes after it receives contradictory instructions on how the fragments are offset on these packets. A SYN attack is when an attacker floods a system with connection requests but does not respond when the target system replies to those requests.
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 76).

QUESTION 844
Which of the following does NOT use token-passing?

A. ARCnet
B. FDDI
C. Token-ring
D. IEEE 802.3

Correct Answer: D
Explanation:

IEEE 802.3 specifies the standard for Ethernet and uses CSMA/CD, not token-passing.
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 104).

QUESTION 845
Why is traffic across a packet switched network difficult to monitor?

A. Packets are link encrypted by the carrier
B. Government regulations forbids monitoring
C. Packets can take multiple paths when transmitted
D. The network factor is too high

Correct Answer: C
Explanation:
With a packet switched network, packets are difficult to monitor because they can be transmitted using different paths.

A packet-switched network is a digital communications network that groups all transmitted data, irrespective of content, type, or structure into suitably sized blocks, called packets. The network over which packets are transmitted is a shared network which routes each packet independently from all others and allocates transmission resources as needed.

The principal goals of packet switching are to optimize utilization of available link capacity, minimize response times and increase the robustness of communication. When traversing network adapters, switches and other network nodes, packets are buffered and queued, resulting in variable delay and throughput, depending on the traffic load in the network.

Most modern Wide Area Network (WAN) protocols, including TCP/IP, X.25, and Frame Relay, are based on packet-switching technologies. In contrast, normal telephone service is based on a circuit-switching technology, in which a dedicated line is allocated for transmission between two parties. Circuit-switching is ideal when data must be transmitted quickly and must arrive in the same order in which it's sent. This is the case with most real- time data, such as live audio and video. Packet switching is more efficient and robust for data that can withstand some delays in transmission, such as e-mail messages and Web pages.

All of the other answer are wrong

Reference(s) used for this question:

TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.
https://en.wikipedia.org/wiki/Packet-switched_network
http://www.webopedia.com/TERM/P/packet_switching.html

QUESTION 846
Which one of the following is used to provide authentication and confidentiality for e-mail messages?

A. Digital signature
B. PGP
C. IPSEC AH
D. MD4

Correct Answer: B
Explanation:
Instead of using a Certificate Authority, PGP uses a "Web of Trust", where users can certify each other in a mesh model, which is best applied to smaller groups.

In cryptography, a web of trust is a concept used in PGP, GnuPG, and other OpenPGP compatible systems to establish the authenticity of the binding between a public key and its owner. Its decentralized trust model is an alternative to the centralized trust model of a public key infrastructure (PKI), which relies exclusively on a certificate authority (or a hierarchy of such). The web of trust concept was first put forth by PGP creator Phil Zimmermann in 1992 in the manual for PGP version 2.0.

Pretty Good Privacy (PGP) is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication. PGP is often used for signing, encrypting and decrypting texts, E-mails, files, directories and whole disk partitions to increase the security of e-mail communications. It was created by Phil Zimmermann in 1991.

As per Shon Harris's book:
Pretty Good Privacy (PGP) was designed by Phil Zimmerman as a freeware e-mail security program and was released in 1991. It was the first widespread public key encryption program. PGP is a complete cryptosystem that uses cryptographic protection to protect e- mail and files. It can use RSA public key encryption for key management and use IDEA symmetric cipher for bulk encryption of data, although the user has the option of picking different types of algorithms for these functions. PGP can provide confidentiality by using the IDEA encryption algorithm, integrity by using the MD5 hashing algorithm, authentication by using the public key certificates, and nonrepudiation by using cryptographically signed messages. PGP initially used its own type of digital certificates rather than what is used in PKI, but they both have similar purposes. Today PGP support X.509 V3 digital certificates.

Reference(s) used for this question:

KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 169).
Shon Harris, CISSP All in One book
https://en.wikipedia.org/wiki/Pretty_Good_Privacy
TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 847
What is the primary reason why some sites choose not to implement Trivial File Transfer Protocol (TFTP)?

A. It is too complex to manage user access restrictions under TFTP
B. Due to the inherent security risks
C. It does not offer high level encryption like FTP
D. It cannot support the Lightwight Directory Access Protocol (LDAP)

Correct Answer: B
Explanation:
Some sites choose not to implement Trivial File Transfer Protocol (TFTP) due to the inherent security risks. TFTP is a UDP-based file transfer program that provides no security. There is no user authentication.
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 88.

QUESTION 848
Which of the following devices enables more than one signal to be sent out simultaneously over one physical circuit?

A. Router
B. Multiplexer
C. Channel service unit/Data service unit (CSU/DSU)
D. Wan switch

Correct Answer: B
Explanation:
Multiplexers are devices that enable enables more than one signal to be sent out simultaneously over one physical circuit.
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 118).

QUESTION 849
Which of the following is NOT true about IPSec Tunnel mode?

A. Fundamentally an IP tunnel with encryption and authentication
B. Works at the Transport layer of the OSI model
C. Have two sets of IP headers
D. Established for gateway service

Correct Answer: B
Explanation:
IPSec can be run in either tunnel mode or transport mode. Each of these modes has its own particular uses and care should be taken to ensure that the correct one is selected for the solution:

Tunnel mode is most commonly used between gateways, or at an end-station to a gateway, the gateway acting as a proxy for the hosts behind it.

Transport mode is used between end-stations or between an end-station and a gateway, if the gateway is being treated as a host--for example, an encrypted Telnet session from a workstation to a router, in which the router is the actual destination.

As Figure 1 shows, basically transport mode should be used for end-to-end sessions and tunnel mode should be used for everything else. (Refer to the figure for the following discussion.)

Figure 1 Tunnel and transport modes in IPSec.

Figure 1 displays some examples of when to use tunnel versus transport mode:

Tunnel mode is most commonly used to encrypt traffic between secure IPSec gateways, such as between the Cisco router and PIX Firewall (as shown in example A in Figure 1). The IPSec gateways proxy IPSec for the devices behind them, such as Alice's PC and the HR servers in Figure 1. In example A, Alice connects to the HR servers securely through the IPSec tunnel set up between the gateways.

Tunnel mode is also used to connect an end-station running IPSec software, such as the Cisco Secure VPN Client, to an IPSec gateway, as shown in example B.