Free Questions for SSCP

Shared by Hoffman on 04-10-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

Upon which of the following ISO/OSI layers does network address translation operate?

Options:

A- Transport layer

B- Session layer

C- Data link layer

D- Network layer

Answer:

D

Explanation:

Network address translation (NAT) is concerned with IP address translation between two networks and operates at the network layer (layer 3).

Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, Chapter 3: Telecommunications and Network Security (page 440).

Question 2

Question Type: MultipleChoice

Which of the following is the simplest type of firewall ?

Options:

A- Stateful packet filtering firewall

B- Packet filtering firewall

C- Dual-homed host firewall

D- Application gateway

Answer:

B

Explanation:

A static packet filtering firewall is the simplest and least expensive type of firewalls, offering minimum security provisions to a low-risk computing environment.

A static packet filter firewall examines both the source and destination addresses of the incoming data packet and applies ACL's to them. They operates at either the Network or Transport layer. They are known as the First generation of firewall.

Older firewalls that were only packet filters were essentially routing devices that provided access control functionality for host addresses and communication sessions. These devices, also known as stateless inspection firewalls, do not keep track of the state of each flow of traffic that passes though the firewall; this means, for example, that they cannot associate multiple requests within a single session to each other. Packet filtering is at the core of most modern firewalls, but there are few firewalls sold today that only do stateless packet filtering. Unlike more advanced filters, packet filters are not concerned about the content of packets. Their access control functionality is governed by a set of directives referred to as a ruleset. Packet filtering capabilities are built into most operating systems and devices capable of routing; the most common example of a pure packet filtering device is a network router that employs access control lists.

There are many types of Firewall:

Application Level Firewalls -- Often called a Proxy Server. It works by transferring a copy of each accepted data packet from one network to another. They are known as the Second generation of firewalls.

An application-proxy gateway is a feature of advanced firewalls that combines lower-layer access control with upper-layer functionality. These firewalls contain a proxy agent that acts as an intermediary between two hosts that wish to communicate with each other, and never allows a direct connection between them. Each successful connection attempt actually results in the creation of two separate connections---one between the client and the proxy server, and another between the proxy server and the true destination. The proxy is meant to be transparent to the two hosts---from their perspectives there is a direct connection. Because external hosts only communicate with the proxy agent, internal IP addresses are not visible to the outside world. The proxy agent interfaces directly with the firewall ruleset to determine whether a given instance of network traffic should be allowed to transit the firewall.

Stateful Inspection Firewall - Packets are captured by the inspection engine operating at the network layer and then analyzed at all layers. They are known as the Third generation of firewalls.

Stateful inspection improves on the functions of packet filters by tracking the state of connections and blocking packets that deviate from the expected state. This is accomplished by incorporating greater awareness of the transport layer. As with packet filtering, stateful inspection intercepts packets at the network layer and inspects them to see if they are permitted by an existing firewall rule, but unlike packet filtering, stateful inspection keeps track of each connection in a state table. While the details of state table entries vary by firewall product, they typically include source IP address, destination IP address, port numbers, and connection state information.

Web Application Firewalls - The HTTP protocol used in web servers has been exploited by attackers in many ways, such as to place malicious software on the computer of someone browsing the web, or to fool a person into revealing private information that they might not have otherwise. Many of these exploits can be detected by specialized application firewalls called web application firewalls that reside in front of the web server.

Web application firewalls are a relatively new technology, as compared to other firewall technologies, and the type of threats that they mitigate are still changing frequently. Because they are put in front of web servers to prevent attacks on the server, they are often considered to be very different than traditional firewalls.

Host-Based Firewalls and Personal Firewalls - Host-based firewalls for servers and personal firewalls for desktop and laptop personal computers (PC) provide an additional layer of security against network-based attacks. These firewalls are software-based, residing on the hosts they are protecting---each monitors and controls the incoming and outgoing network traffic for a single host. They can provide more granular protection than network firewalls to meet the needs of specific hosts.

Host-based firewalls are available as part of server operating systems such as Linux, Windows, Solaris, BSD, and Mac OS X Server, and they can also be installed as third-party add-ons. Configuring a host-based firewall to allow only necessary traffic to the server provides protection against malicious activity from all hosts, including those on the same subnet or on other internal subnets not separated by a network firewall. Limiting outgoing traffic from a server may also be helpful in preventing certain malware that infects a host from spreading to other hosts.11 Host-based firewalls usually perform logging, and can often be configured to perform address-based and application-based access controls

Dynamic Packet Filtering -- Makes informed decisions on the ACL's to apply. They are known as the Fourth generation of firewalls.

Kernel Proxy - Very specialized architecture that provides modular kernel-based, multi-layer evaluation and runs in the NT executive space. They are known as the Fifth generation of firewalls.

The following were incorrect answers:

All of the other types of firewalls listed are more complex than the Packet Filtering Firewall.

Reference(s) used for this question:

HARRIS,

Shon, All-In-One CISSP Certification Exam Guide, 6th Edition, Telecommunications and Network Security, Page 630.

and

NIST Guidelines on Firewalls and Firewalls policies, Special Publication 800-4 Revision 1

Question 3

Question Type: MultipleChoice

Which of the following is the biggest concern with firewall security?

Options:

A- Internal hackers

B- Complex configuration rules leading to misconfiguration

C- Buffer overflows

D- Distributed denial of service (DDOS) attacks

Answer:

B

Explanation:

Firewalls tend to give a false sense of security. They can be very hard to bypass but they need to be properly configured. The complexity of configuration rules can introduce a vulnerability when the person responsible for its configuration does not fully understand all possible options and switches. Denial of service attacks mainly concerns availability.

Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, Chapter 3: Telecommunications and Network Security (page 412).

Question 4

Question Type: MultipleChoice

What is the framing specification used for transmitting digital signals at 1.544 Mbps on a T1 facility?

Options:

A- DS-0

B- DS-1

C- DS-2

D- DS-3

Answer:

B

Explanation:

Digital Signal level 1 (DS-1) is the framing specification used for transmitting digital signals at 1.544 Mbps on a T1 facility. DS-0 is the framing specification used in transmitting digital signals over a single 64 Kbps channel over a T1 facility. DS-3 is the framing specification used for transmitting digital signals at 44.736 Mbps on a T3 facility. DS-2 is not a defined framing specification.

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 114).

Question 5

Question Type: MultipleChoice

Which xDSL flavour can deliver up to 52 Mbps downstream over a single copper twisted pair?

Options:

A- VDSL

B- SDSL

C- HDSL

D- ADSL

Answer:

A

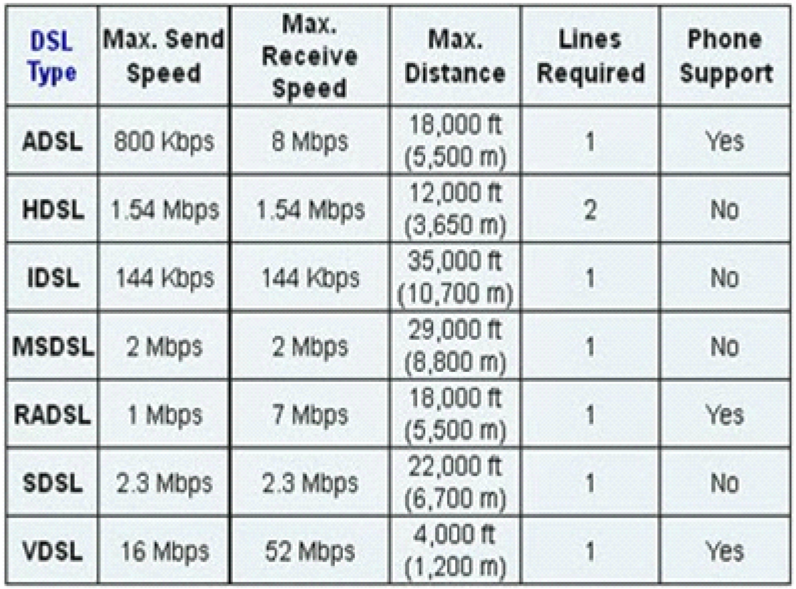
Explanation:

Very-high data-rate Digital Subscriber Line (VDSL) can deliver up to 52 Mbps downstream over a single copper twisted pair over a relatively short distance (1000 to 4500 feet).

DSL (Digital Subscriber Line) is a modem technology for broadband data access over ordinary copper telephone lines (POTS) from homes and businesses. xDSL refers collectively to all types of DSL, such as ADSL (and G.Lite), HDSL, SDSL, IDSL and VDSL etc. They are sometimes referred to as last-mile (or first mile) technologies because they are used only for connections from a telephone switching station to a home or office, not between switching stations.

xDSL is similar to ISDN in as much as both operate over existing copper telephone lines (POTS) using sophisticated modulation schemes and both require the short runs to a central telephone office

Graphic below from: http://computer.howstuffworks.com/vdsl3.htm



DSL Type	Max. Send Speed	Max. Receive Speed	Max. Distance	Lines Required	Phone Support
ADSL	800 Kbps	8 Mbps	18,000 ft (5,500 m)	1	Yes
HDSL	1.54 Mbps	1.54 Mbps	12,000 ft (3,650 m)	2	No
IDSL	144 Kbps	144 Kbps	35,000 ft (10,700 m)	1	No
MSDSL	2 Mbps	2 Mbps	29,000 ft (8,800 m)	1	No
RADSL	1 Mbps	7 Mbps	18,000 ft (5,500 m)	1	Yes
SDSL	2.3 Mbps	2.3 Mbps	22,000 ft (6,700 m)	1	No
VDSL	16 Mbps	52 Mbps	4,000 ft (1,200 m)	1	Yes

DSL speed chart

The following are incorrect answers:

Single-line Digital Subscriber Line (SDSL) deliver 2.3 Mbps of bandwidth each way.

High-rate Digital Subscriber Line (HDSL) deliver 1.544 Mbps of bandwidth each way.

ADSL delivers a maximum of 8 Mbps downstream for a total combined speed of almost 9 Mbps up and down.

Reference used for this

Question;

http ://computer.howstuffworks.com/vdsl3.htm

http ://computer.howstuffworks.com/vdsl3.htm

and

http://www.javvin.com/protocolxDSL.html

and

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 115).

Question 6

Question Type: **MultipleChoice**

Which xDSL flavour delivers both downstream and upstream speeds of 1.544 Mbps over two copper twisted pairs?

Options:

A- HDSL

B- SDSL

C- ADSL

D- VDSL

Answer:

A

Explanation:

High-rate Digital Subscriber Line (HDSL) delivers 1.544 Mbps of bandwidth each way over two copper twisted pairs. SDSL also delivers 1.544 Mbps but over a single copper twisted pair. ADSL and VDSL offer a higher bandwidth downstream than upstream.

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 115).