Exam Report: 13.12.5 Practice Questions

Date: 4/15/2020 5:39:29 pm
Time Spent: 1:08

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 78%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

While on a business trip, an employee accesses the company's internal network and transfer files using an encrypted connection.

Which of the following digital security methods is being used?

- Access control list
- DLP
- Firewall
- VPN

Explanation

A Virtual Private Network (VPN) is an encrypted tunnel between remote users and a private network.

Data Loss Prevention (DLP) programs or devices monitors operations such as file transfers and email for user activities that could compromise data security. An access control list contains users and groups of users that are granted access to files, folders, and other resources. Firewalls are placed between the company network and the internet to filter network traffic at the IP level. VPNs are usually allowed to tunnel through these firewalls. In some cases, both functions may be available on one device.

References

TestOut PC Pro - 13.12 VPN
[e_vpn_pp6.exam.xml Q_VPN_FCT_01]

Question 2: Correct

A VPN is used primarily for which purpose?

- Allow the use of network-attached printers.
- Support secured communications over an untrusted network.
- Support the distribution of public web documents.

Explanation

A VPN (Virtual Private Network) is used primarily to support secured communications over an untrusted network. A VPN can be used over a local area network, across a WAN connection, over the internet, and even between a client and a server over a dial-up connection through the internet.

All of the other items listed in this question are benefits or capabilities that are secondary to this primary purpose.

References

TestOut PC Pro - 13.12 VPN
[e_vpn_pp6.exam.xml Q_VPN_FCT_02]

Question 3: Incorrect

Which of the following networking devices or services is LEAST likely to be compatible with VPN connections?

- ~~Firewall~~
- Switch
- Router
- NAT

Explanation

When using a VPN through a NAT device, check your NAT solution to make sure that the router can support VPN connections. Not all VPN solutions are compatible with NAT.

References

TestOut PC Pro - 13.12 VPN
[e_vpn_pp6.exam.xml Q_VPN_FCT_03]

Question 4: Correct

Your organization employs a group of traveling salespeople who need to access the corporate home network through the internet while they are on the road. You want to funnel remote access to the internal network through a single server.

Which of the following solutions would be BEST to implement?

- Site-to-site VPN
- Host-to-host VPN
- VPN concentrator
- DMZ

Explanation

With a remote access VPN, a server on the edge of a network (called a VPN concentrator) is configured to accept VPN connections from individual hosts. Hosts that are allowed to connect using the VPN connection are granted access to resources on the VPN server or the private network.

References

TestOut PC Pro - 13.12 VPN
[e_vpn_pp6.exam.xml Q_VPN_FCT_04]

Question 5: Correct

A salesperson in your organization spends most of her time traveling between customer sites. After a customer visit, she must complete various managerial tasks, such as updating your organization's order database. Because she rarely comes back to your home office, she usually accesses the network from her notebook computer using Wi-Fi access provided by hotels, restaurants, and airports.

Many of these locations provide unencrypted public Wi-Fi access, and you are concerned that sensitive data could be exposed. To remedy this situation, you decide to configure her notebook to use a VPN when accessing the home network over an open wireless connection.

Which of the following key steps should you take when implementing this configuration? (Select TWO. Each option is part of the complete solution.)

- [ ] Configure the browser to send HTTPS requests directly to the Wi-Fi network without going through the VPN connection.
- [x] Configure the VPN connection to use IPsec.
- [ ] Configure the VPN connection to use MS-CHAPv2.
- [x] Configure the browser to send HTTPS requests through the VPN connection.
- [ ] Configure the VPN connection to use PPTP.

Explanation

It is generally considered acceptable to use a VPN connection to securely transfer data over an open Wi-Fi network. As long as strong tunneling ciphers and protocols are used, the VPN provides sufficient encryption to secure the connection even though the wireless network itself is not encrypted. It is recommended that you use IPsec or SSL to secure the VPN, as these protocols are relatively secure. You should also configure the browser's HTTPS requests to go through the VPN connection.

To conserve VPN bandwidth and to improve latency, many VPN solutions automatically reroute web browsing traffic through the client's default network connection instead of through the VPN tunnel. This behavior would result in HTTP/HTTPS traffic being transmitted over the unsecure open wireless network instead of through the secure VPN tunnel. Avoid using PPTP with MS-CHAPv2 in a VPN over open wireless configuration, as these protocols are no longer considered secure.

References

TestOut PC Pro - 13.12 VPN
[e_vpn_pp6.exam.xml Q_VPN_FCT_05]

Question 6: Correct

You want to use a protocol that can encapsulate other LAN protocols and carry the data securely over an IP network. Which of the following protocols is suitable for this

- ○ PPP
- ➡ ◉ PPTP
- ○ SLIP
- ○ NetBEUI

Explanation

PPTP is used with VPNs, which allow you to send data securely over a public network.

References

TestOut PC Pro - 13.12 VPN
[e_vpn_pp6.exam.xml Q_VPN_FCT_06]

Question 7: Correct

Which of the following protocols can your portable computer use to connect to your company's network via a virtual tunnel through the internet? (Select TWO).

- ☐ Remote Desktop Protocol (RDP)
- ☐ PPPoE
- ➡ ☑ L2TP
- ☐ VNC
- ➡ ☑ PPTP

Explanation

PPTP (Point-to-Point Tunneling Protocol) and L2TP (Layer Two Tunneling Protocol) are two VPN (Virtual Private Networking) protocols that let you access your company's network through a public network, such as the internet.

PPPoE is used for connecting to the internet through an Ethernet connection to include authentication and accounting. VNC and RDP are remote desktop protocols used for remote administration or remote device access.

References

TestOut PC Pro - 13.12 VPN
[e_vpn_pp6.exam.xml Q_VPN_FCT_07]

Question 8: Incorrect

Which of the following protocols provides authentication and encryption services for VPN traffic?

- ○ SSL
- ➡ ○ IPsec
- ○ TCP

Explanation

IPsec is a security implementation that provides security for all other TCP/IP based protocols. IPsec provides authentication through a protocol called IPsec Authentication Header (AH) and encryption services through a protocol called IPsec Encapsulating Security Payloads (ESP).

The Transmission Control Protocol (TCP) is a transport layer connection-oriented protocol that provides data transmission services. It is not a secure protocol, and relies on other measures, such as IPsec, to provide security. The Secure Sockets Layer (SSL) is an application layer protocol that is designed to secure network traffic from certain other protocols, such as Hypertext Transfer Protocol (HTTP) and Post Office Protocol version 3 (POP3). It does not provide security for protocols lower in the TCP/IP protocol stack, such as TCP and UDP. The Layer 2 Tunneling Protocol (L2TP) is a protocol used to encapsulate Point-to-Point protocol (PPP) traffic.

References

TestOut PC Pro - 13.12 VPN
[e_vpn_pp6.exam.xml Q_VPN_FCT_08]

Question 9: Correct

Which of the following statements about an SSL VPN are true? (Select TWO).

- [x] Uses port 443.
- [x] Encrypts the entire communication session.
- [ ] Provides message integrity using HMAC.
- [ ] Uses pre-shared keys for authentication.
- [ ] Encapsulates packets by adding a GRE header.
- [ ] Uses UDP port 500.

Explanation

SSL VPN uses the SSL protocol to secure communications. SSL VPN:

- Authenticates the server to the client using public key cryptography and digital certificates.
- Encrypts the entire communication session.
- Uses port 443, which is already open on most firewalls.

IPsec uses pre-shared keys to provide authentication with other protocols. IPsec also uses HMAC to provide message integrity checks. GRE headers are used exclusively by the GRE tunneling protocol. UDP port 500 is used by the Layer Two Tunneling Protocol (L2TP).

References

TestOut PC Pro - 13.12 VPN
[e_vpn_pp6.exam.xml Q_VPN_FCT_09]