Exam Report: 8.2.5 Practice Questions

Date: 10/16/2019 1:15:58 pm
Time Spent: 1:41

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 67%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

An all-in-one security appliance is best suited for which type of implementation?

- A credit card company that stores customer data.
- A remote office with no on-site technician.
- An office with a dedicated network closet.
- A company that transmits large amounts of time-sensitive data.

Explanation

All-in one security appliances are best suited for small offices with limited space or a remote office without a technician to manage the individual security components.

A company with a dedicated network closet would have the spaced necessary for multiple networking devices. A company that handles large amounts of data should use dedicated devices to maintain optimal performance. A credit card company should use dedicated security devices to secure sensitive data.

References

LabSim for Network Pro, Section 8.2.
[netpro18v5_all_questions_en.exm *NP15_SECURITY_APPLIANCES_01]

Question 2: Correct

Which of the following features are common functions of an all-in-one security appliance? (Select two.)

- [x] Spam filtering
- [ ] Quality of Service
- [ ] Password complexity
- [ ] Content caching
- [x] Bandwidth shaping

Explanation

All-in-one security appliances combine many security functions into a single device. Security functions in an all-in-one security appliance can include:

- Spam filter
- URL filter
- Web content filter

- Malware inspection
- Intrusion detection system

In addition to security functions, all-in-one security appliances can include:

- Network switch
- Router
- Firewall
- TX uplink (integrated CSU/DSU)
- Bandwidth shaping

References

LabSim for Network Pro, Section 8.2.
[netpro18v5_all_questions_en.exm *NP15_SECURITY_APPLIANCES_02]

Question 3: Incorrect

You recently installed a new all-in-one security appliance in a remote office. You are in the process of configuring the device. You need to:

- Increase the security of the device.
- Enable remote management from the main office.
- Allow users to be managed through Active Directory.

You want to configure the device so you can access it from the main office. You also want to make sure the device is as secure as possible.

Which of the following tasks should you carry out? (Select two.)

- [ ] Deny login from all external IP addresses.
- [x] Change the default username and password.
- [ ] Configure the device's authentication type to use Active Directory.
- [ ] Deny login from the device's WAN interface.
- [x] ~~Create an Active Directory user group and add all users to the group.~~

Explanation

When configuring a new all-in-one security appliance, the first thing you should do is change the default username and password. The device's default login credentials can be found on the internet and used to access the device. Most all-in-one security appliances can be integrated with a centralized authentication method, such as Active Directory. This is done in the domain configuration.

Denying login from the WAN interface or all external IP addresses would not allow you to remotely manage the device from your main office. Groups are used by the device only and are not used by an authentication server. Creating an Active Directory group would not allow centralized user management.

References

LabSim for Network Pro, Section 8.2.
[netpro18v5_all_questions_en.exm *NP15_SECURITY_APPLIANCES_03]