Exam Report: 5.6.5 Practice Questions

Date: 1/20/2020 8:37:02 pm
Time Spent: 15:10

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 50%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Incorrect

You have a small network at home that is connected to the internet. On your home network, you have a server with the IP address of 192.168.55.199/16. You have a single public address that is shared by all hosts on your private network.

You want to configure the server as a web server and allow internet hosts to contact the server to browse a personal website.

What should you use to allow access?

- Static NAT
- ~~Dynamic NAT~~
- DNS A record
- Multicast
- DNS CNAME record

Explanation

Static NAT maps an internal IP address to a static port assignment. Static NAT is typically used to take a server on the private network (such as a web server) and make it available on the internet. External hosts contact the internal server using the public IP address and the static port. Using a static mapping allows external hosts to contact internal hosts.

Dynamic NAT automatically maps internal IP addresses with a dynamic port assignment. On the NAT device, the internal device is identified by the public IP address and the dynamic port number. Dynamic NAT allows internal (private) hosts to contact external (public) hosts, but not vice versa. External hosts cannot initiate communications with internal hosts.

DNS records associate a host name with an IP address. With multicast, a single data stream can be forwarded to all computers that are members of the same multicast group.

References

LabSim for Security Pro, Section 5.6.
[All Questions SecPro2017_v6.exm NAT_01]

Question 2: Incorrect

You are the network administrator for a small company that implements NAT to access the internet. However, you recently acquired five servers that must be accessible from outside your network. Your ISP has provided you with five additional registered IP addresses to support these new servers, but you don't want the public to access these servers directly. You want to place these servers behind your firewall on the inside network, yet still allow them to be accessible to the public from the outside.

Which method of NAT translation should you implement for these servers?

- Static

- Overloading
- ~~Dynamic~~
- Restricted

Explanation

Static translation consistently maps an unregistered IP address to the same registered IP address on a one-to-one basis. Static NAT is particularly useful when a device needs to be assigned the same address so it can be accessed from outside the network, such as web servers and other similar devices.

Dynamic translation would not work for these servers because it maps an unregistered host IP address to any available IP address configured in a pool of one or more registered IP addresses. Accessing a server assigned one of these addresses would be nearly impossible because the addresses are still shared by multiple hosts.

References

LabSim for Security Pro, Section 5.6.
[All Questions SecPro2017_v6.exm NAT_02]

Question 3: Incorrect

You want to connect your small company network to the internet. Your ISP provides you with a single IP address that is to be shared between all hosts on your private network. You do not want external hosts to be able to initiate connection to internal hosts. What type of network address translation (NAT) should you implement?

- ~~Restricted~~
- Shared
- Static
- Dynamic

Explanation

Use dynamic NAT to share public addresses with multiple private hosts. Dynamic NAT allows private hosts to access the internet, but does not allow internet hosts to initiate contact with private hosts.

References

LabSim for Security Pro, Section 5.6.
[All Questions SecPro2017_v6.exm NAT_03]

Question 4: Correct

Which of the following is *not* one of the IP address ranges defined in RFC 1918 that are commonly used behind a NAT server?

- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 169.254.0.0 - 169.254.255.255
- 192.168.0.0 - 192.168.255.255

Explanation

169.254.0.1 - 169.254.255.254 is the range of IP addresses assigned to Windows DHCP clients if a DHCP server does not assign the client an IP address. This range is known as the Automatic Private IP Addressing (APIPA) range.

The other three ranges listed in this question are defined as the private IP addresses from RFC 1918, which are commonly used behind a NAT server.

References

LabSim for Security Pro, Section 5.6.
[All Questions SecPro2017_v6.exm NAT_04]

Question 5: Correct

Which of the following networking devices or services prevents the use of IPSec in most cases?

- NAT
- Router
- Firewall
- Switch

Explanation

Typically, IPSec cannot be used when static IP addresses are not used by both communication partners. NAT proxy performs network address translation on all communications. For this reason, the IP address seen for a system outside of the proxied network is not that system's real IP address. This prevents the use of IPSec.

IPSec can be deployed without problems with the presence of firewalls, routers, and switches. However, in the case of firewalls, you will need to configure special access ports to allow IPSec traffic to pass.

References

LabSim for Security Pro, Section 5.6.
[All Questions SecPro2017_v6.exm NAT_05]

Question 6: Correct

Which of the following is *not* a benefit of NAT?

- Improving the throughput rate of traffic
- Preventing traffic initiations from outside the private network
- Using fewer public IP addresses
- Hiding the network infrastructure from external entities

Explanation

NAT does not provide improved throughput for traffic. A proxy server may provide improved performance when accessing previously-used resources from a temporary cache.

NAT provides the benefits of hiding your network infrastructure (IP address ranges and assignments) from external entities. It allows you to employ fewer public IP addresses for a larger number of internal clients who need internet access, and it prevents traffic that was not initiated by an internal client from entering into the private network.

References

LabSim for Security Pro, Section 5.6.
[All Questions SecPro2017_v6.exm NAT_06]