10: Lab 10 – Assisted - Using IPSec tunneling

Security+ (Exam SY0-701)

Congratulations, you passed!

Duration: 38 minutes

☑ **Configure IPSec policy is defined on PC10** *Score: 1*

Select the **Score** button to validate this task:
`IPSec policy 'Structureality IPSec Policy (attempt)' is defined.`

☑ **Configure IPSec policy is defined on PC20** *Score: 1*

Select the **Score** button to validate this task:
`IPSec policy 'Structureality IPSec Policy (required)' is defined.`

☑ Why is there no ICMP traffic captured for the ping from 10.1.24.102 (i.e., PC20) and 10.1.24.254? *Score: 1*

○ You did not ping the default gateway from PC20
○ PC20 is already encyrpting its communications
● Traffic from PC20 to all non-PC10 system is not sent to PC10 to be captured
○ The gateway sent any responses to the ping from PC20

Congratulations, you have answered the question correctly.

☑ What are the three main types of IPSec policies that can be configured? (Select 3) *Score: 1*

☑ Permit
☑ Block
☑ Negotiate
□ Request
□ Enable

Congratulations, you have answered the question correctly.

☑ What is the primary benefit of tunneling? *Score: 1*

● Encryption
○ Faster routing
○ Promiscuous sniffing
○ Availability
○ Non-repudiation

Congratulations, you have answered the question correctly.

☑ In the lab, why was PC10 unable to collect the packets from PC20 directed to the default gateway or the website? *Score: 1*

● The packets from PC20 were not sent to the PC10 interface
○ PC20 did not communicate with the default gateway or website
○ The IPSec policy was in effect even before it was assigned
○ PC10 has a filter to ignore all traffic from PC10

Congratulations, you have answered the question correctly.

☑ Which of the following are options for implementing encrypted tunnels for secure communications? (Select all that apply) *Score: 1*

☑ IPsec
☑ SSH
☑ TLS
□ DNS
□ HTTP
□ FTP
□ ICMP

Congratulations, you have answered the question correctly.

☑ Your company is implementing IPSec policies on all internal systems. However, the configuration change will be rolled out over a three-month period. What is the best choice for the IPSec policy during the initial implementation phase? *Score: 1*

○ Accept unsecured communication, but always respond using IPsec
● Allow fallback to unsecured communications if a secure connection can not be established
○ Require all communications use IPSec
○ Do not respond to IPSec initiation queries

Congratulations, you have answered the question correctly.