ST2612 Tutorial 5 (Week 14)

Recap of Practical 5, Lecture 6 (Part 1)

Self-evaluation Check list

- List the two WSUS synchronization methods.
  - Manual method - Synchronize Now.
  - Schedule method - can set the synchronization schedule.
- Briefly describe one advantage of defining computer groups in WSUS management console.
  - Using computer groups to categorize computer by their OSs or Services. This helps to batch approval of updates to the same type of computers.
  - Using computer groups to setup selected computers for pilot test.

  [Any one of the above or accepted answers]
- Would you briefly describe the 'relationship/difference' between the following lists of paired items?

  -IKE authentication and AH authentication

  IKE Authentication authenticates whether the other end of the communicating party is a trusted host. AH authentication authenticates the integrity of each incoming packet. (Difference)

  -IPsec filter and IPsec rule

  Each IPsec rule consists a filter. The filter defines a specific type of IP traffic by source/destination addresses, protocol, ports. The respected rule will be activated only when the inflow or outflow traffic matches the filter. [Relationship]

  -IPsec Policies and Group Policies

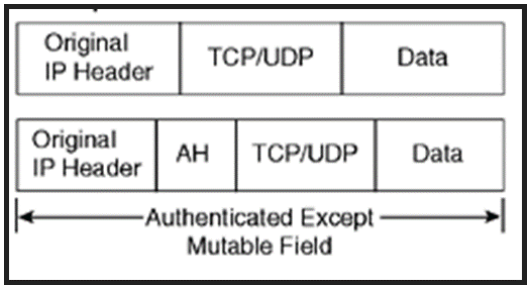
  IPsec Policies defines IPsec rule(s) , Group Policies define computer or user settings for the target systems. [Difference]

  Or

  IPsec Policies can be deployed to the target systems via the Group Policies distribution channel. By setting an IPsec policy to be assigned in a GPO, this IPsec policy will be deployed to the systems that receiving the GPO. [Relationship]
- Would you describe and explain one possible but not recommended usage of IPsec?
  - Enable all intranet traffic to be protected by IPsec. The overhead for the CPUs , bandwidth and connection time will slow down the entire network.
- Would you identify and explain a couple of scenarios that the IPsec implementation can be helpful in terms of tighten the network security?
  - Deploy IPsec for clients to a server, in which, the server is a legacy system which does not have any security option to decrypt/encrypt its inflow/outflow traffic.

- Deploy IPsec to protect a specific point to point communication that requires the highest level of secrecy.

- Would you explain the following IPsec packet transformation?



For the AH transformation, it does not encrypt any part of the original packet. It adds in a AH (Authentication Header) to the packet. It contains the hash value that bases on the data of the entire new transformed packet. There are some data in the mutable field in the IP Header not included for the computation of the hash value. This hash value enables the detection of any data integrity issues.

~ That's All ~