ST2612 Tutorial 6 (Week 16)

Recap of Practical 6, Practical 7, Lecture 6 (Part 2), Lecture 7

Learning objective of

Practical 6:

- Understand the basic procedures of IPsec Configuration
  - Via IPsec Policy and Windows Firewall Advanced Security (WFAS).
- Define IPsec Policy Rule to filter ICMP packets between hosts.
- Deploy IPsec Policy with GPO and other ways (LPO, netsh)
- Understand the relationship between, Rule, Filter List, Filter Action, and Authentication Methods in IPsec operation.
- Apply netsh and GPRESULT commands to monitor GPO deployment status.

Practical 7:

- Certificate Service at a Member Server that runs on Windows Server 2016 to provide Enterprise Root CA services
- Download and Install Root CA Chain to local computer via Web interface
- Request Certificate from Root CA via Web interface with ActiveX capable browser
- Create and Configure Certificate Template for Enterprise Root CA
- Apply PKI to deploy IPsec Authentication using Certificates
- Configure a Web Server to only allow https access with proper SSL certificate issued by in-house Enterprise RootCA.
- Configure a Web server that utilizes mutual certificate authentication to enhance the security measure.

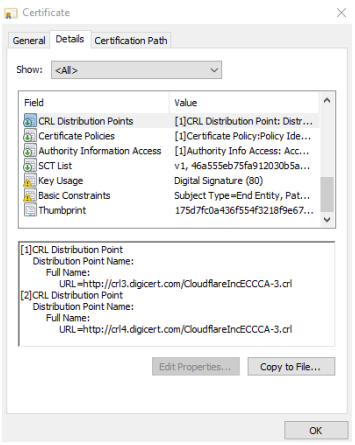
Lecture 6 (Part 2):

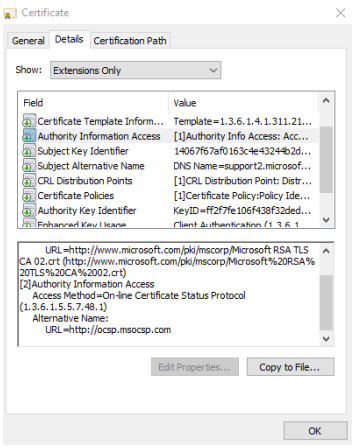
- Transport mode vs Tunnel mode
  - Applications.
  - IPsec Protocol and Packet Transformations.
- IPsec Policy
  - Configuration & Deployment
    - Via Local Security Policy (Standalone and Local).
    - Via Group Policies (Domain based)

Lecture 7

- Define certificate requirements
  - Apply Public Key Infrastructure (PKI) to distribute authenticated Public Keys via trusted digital certificates.
- Plan, build, and manage certification authority hierarchies
  - Generic Models

    - Rooted Trusted Model
    - Cross Certification Model
    - Hybrid Model (Mixture of the above two)
- Select a certificate enrolment and renewal method
    - Certificate Enrolment
        - Submit Request -> Aprrove/Reject -> Retrieval of the issued certificate.
    - Renewal Method
        - Auto-renewal upon expiry
        - Manual renewal before expiry
- Configure and deploy certificate authorities (CA)
    - Windows based RootCA implemation - Active Directory Certificate Services (ADCS)
        - Enterprise RootCA - Close bind with the Active Directory to server mainly the targeted Active Directory.
        - Standalone RootCA - Support any internal / external certificate enrolment.
- Considerations of secured Web Content access
    - HTTPS with mutual certificate authentication.
        - Host and client are required to hold a valid and trusted certificate.
- Deploy and manage SSL certificates
    - Essential fields of a SSL certificate.
    - Configure a Web server for SSL certificates
    - Configure a client for SSL certificates
- Certificate revocation checking
    - Certificates may be revoked by the issuers due to various situation
    - Certificate Revocation List (CRL)
        - Base on a set of CRL published by the issuer.
    - Online Certificate Status Protocol (OCSP)
    - Good, Revoked, unknown, or no response from the OCSP responder
    - Each certificate should contain a URL to the issuer's CRL and/or OCSP responder.

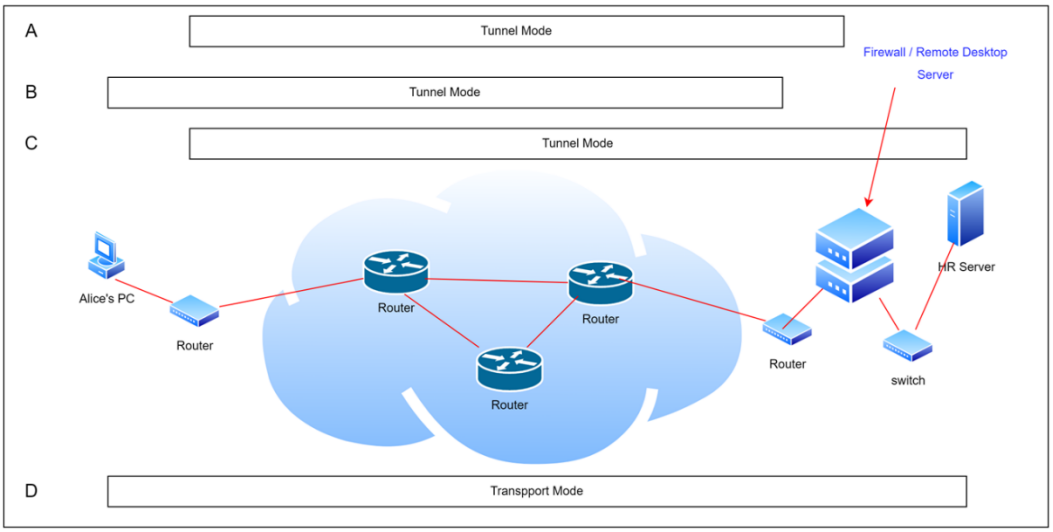




- Determine certificate renewal
    - Key renewal vs Certificate renewal.

Self-evaluation Check list

- What is your view of Lecture 6 slides 24? The question on whether the IPsec applied in that scenario is redundant.



(Assume that Alice PC established a VPN connection to the Company Firewall.)

- The following few items should always be found in a valid digital certificate. Would you briefly explain what will be the impact/issues if they are missing from the design of a digital certificate?

  -Serial number

  -Subject

  -Public key

  -Digital Signature

  -Expiry Date

- What will be the impact(s) to an https enabled website when its corresponding certificate authority server (The SSL cert issuer) is having an outage?
- PKI framework is very much depending on the 'Trust'. From the end users' point of view, what should be the main factor for them to decide which certificates to be trusted?
- Can you figure out why our windows browser(s) are accepting the certificates issued by letsencrypt.org.
- In page 21 of the lecture slide, what is the purpose or the effect of installing the downloaded certificate chain to the Trusted Root Certificate Authority Repository?
- In slide 41. It mentioned self-signed certificate and self-issued certificate. Both of them are only used for in-house applications and they are not accepted by general public, but what is their difference?

Nano Test Questions (Will be given by your tutor).

(For each attempted question: Correct answer earns 1 mark. Incorrect answer subtract 0.5 marks)

(Maximum scores: 2 marks)

Q1.

Q2.

Q3.

Q4

Submit your answers to the Nano Test Journal before the end of the class.

~ That's All ~