**ITT-430: IPsec & DNSSEC Implementation Instructions**

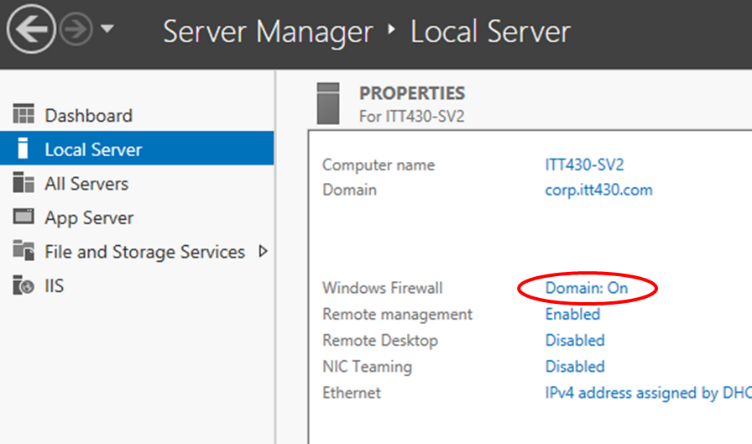
**IPsec: Internet Protocol Security**

On all Windows Servers, IPsec is embedded into the Windows Firewall. Become familiar with the Advanced Firewall settings, as it can also aid in troubleshooting connectivity issues. For example, right-click on 'Windows Firewall with Advanced Security on Local Computer' object and view the connection states in Domain, Private, and Public Profiles. These settings can affect PING functions between servers on the domain.

Connections are managed from the Windows Firewall.

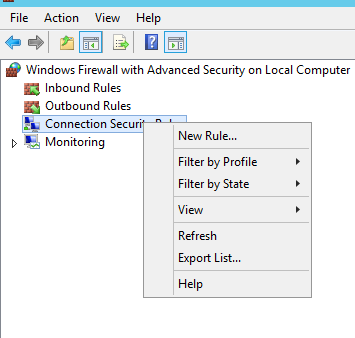
1. Domain Controller
2. From the Server Manager screen, select Local Server, and click Domain: On (Figure 1).
   * This opens the ***Windows Firewall with Advanced Security*** management console.

**Figure 1**

****

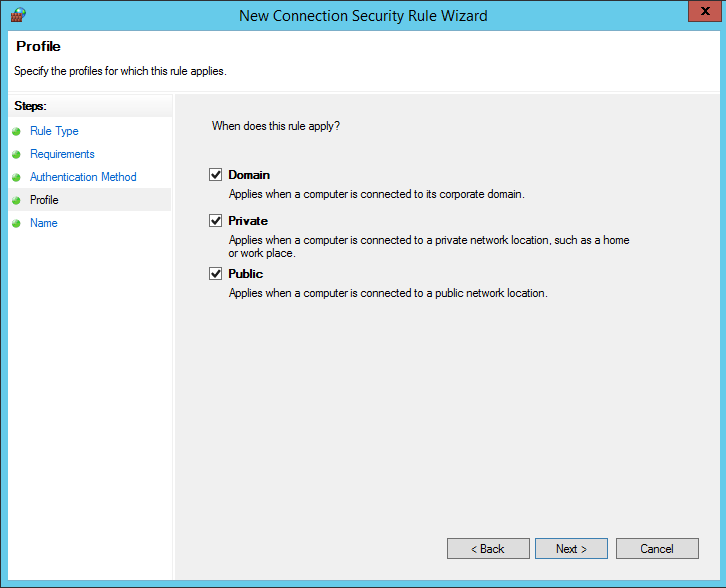
1. Click on ***Connection Security Rules*** then right-click and select **New Rule…** (Figure 2).

**Figure 2**

****

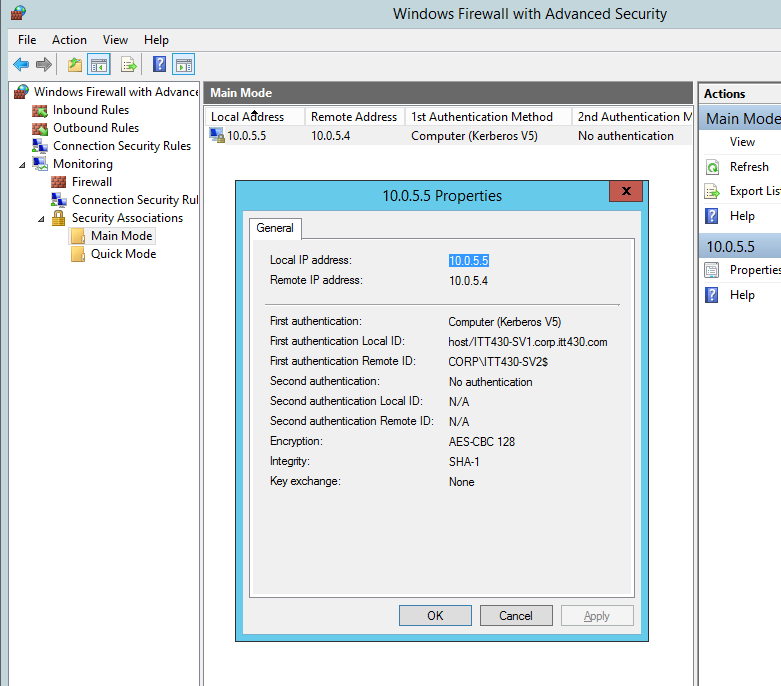
1. Select Isolation, then next
2. Select Request authentication for inbound and outbound connections, then next
3. Select Default, then next
4. Select all options for the firewall profiles that will use IPsec (Figure 3).

**Figure 3**



1. Name the security rule ITT430 IPsec and click finish.
2. Next complete the same steps on the member servers.
3. After all servers are configured, try PINGing a server to refresh their connections.
4. Next… from the Domain Controller… navigate to Monitoring > Security Associations > Main Mode (you may need to refresh on the right column).
5. Locate the connection under Main Mode… double-click to open the properties (Figure 4).
   * This screenshot must be submitted with assignment to demonstrate connections between two or more systems on your network.
   * NOTE: This is only a simplified implementation. There are additional options within Group Policy that can control filtering and other rules for IPsec traffic.

**Figure 4**

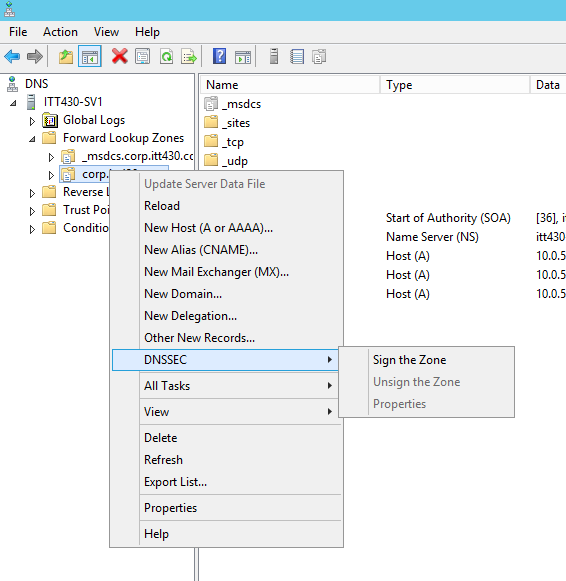


**DNSSEC: Domain Name System Security Extensions**

These steps will enable and test DNSSEC implementation throughout the domain, essentially Zone signing with digital keys (PKI):

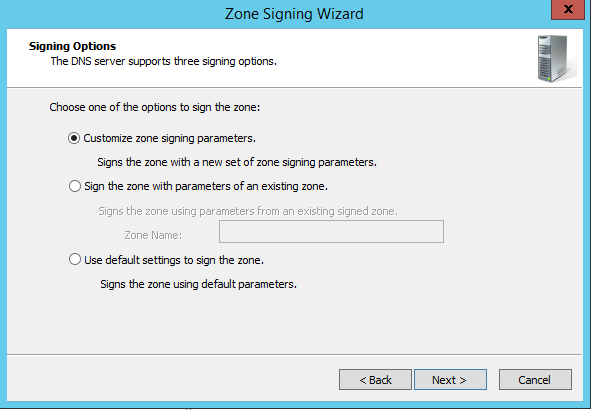
1. Begin on the Domain Controller.
2. Open DNS Manager > from Server Manager, Tools drop down and click DNS.
3. Navigate to your primary zone for your domain under Forward Lookup Zones, right-click the zone, select DNSSEC, then select Sign the Zone (Figure 5).

**Figure 5**



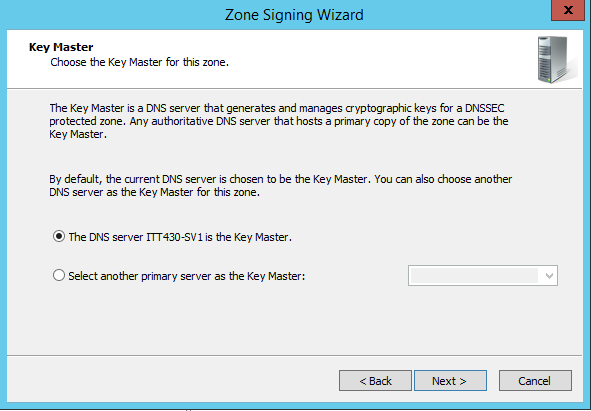
1. A wizard opens.
2. Select '**Customize zone signing parameters**' and click next (Figure 6).

**Figure 6**



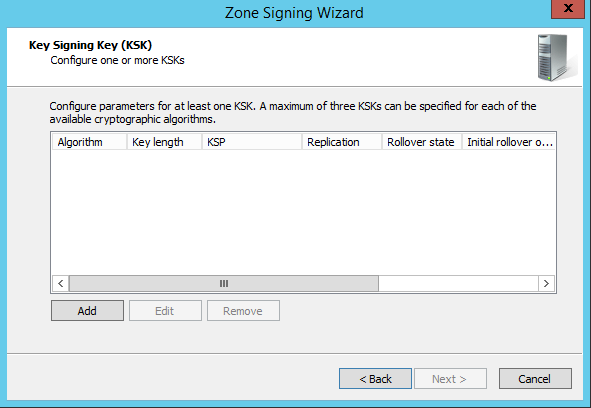
1. Keep the default local server for the Key Master (Figure 7).

**Figure 7**



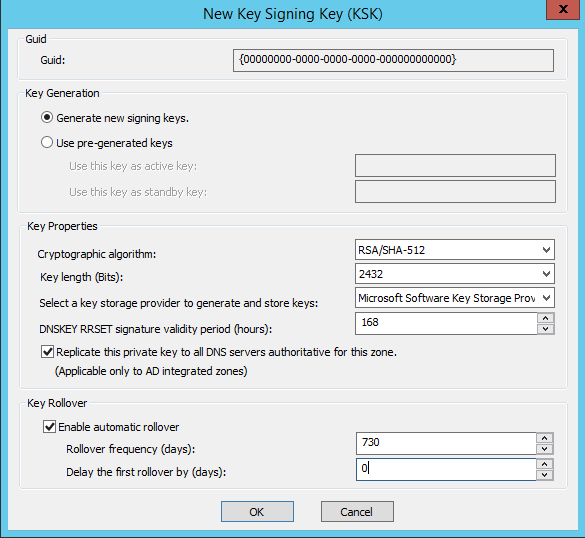
1. Click next to move to the Key Signing Key (KSK) screen and click Add (Figure 8).

**Figure 8**



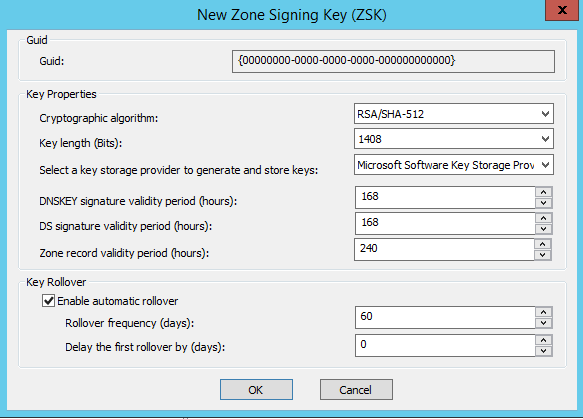
1. In the **New Key Signing Key (KSK)** window configure the following options (Figure 9):
   * Generate new signing keys
   * Cryptographic algorithm: RSA/SHA-512
   * Key length (Bits): 2432
   * Select a key storage provider to generate and store keys: Microsoft Software Key Storage Provider
   * DNSKEY RRSET signature: 168
   * CHECK: Replicate this private key to all DNS servers…
   * CHECK: Enable automatic rollover
   * Rollover frequency: 730
   * Delay the first rollover by: 0

**Figure 9**



1. Click next until Zone Signing Key, then click add.
2. In the New Zone Signing Key (ZSK) window configure the following options (Figure 10):
   * Cryptographic algorithm: RSA/SHA-512
   * Key length (Bits): 1408
   * Select a key storage provider to generate and store keys: Microsoft Software Key Storage Provider
   * DNSKEY signature validity period: 168
   * DS signature validity period: 168
   * Zone record validity period: 240
   * CHECK: Enable automatic rollover
   * Rollover frequency: 60
   * Delay the first rollover by: 0

**Figure 10**



1. Click next to the Trust Anchors.
   * CHECK: Enable the distribution of trust anchors for this zone.
   * CHECK: Enable automatic update of trust anchors on key rollover.
2. Click next and keep remaining defaults and FINISH.
3. Within the DNS Manager console, navigate to Trust Points, and expand all folders.
4. Click on last folder to view the newly created trust points.
5. Take a screenshot of the two points, displaying Algorithm and Valid From dates (Figure 11).
   * This screenshot must be submitted with assignment to demonstrate DNSSEC is configure appropriately.

**Figure 11**

