Cybersecurity

Subject: Windows IPsec

1. Network-layer VPN tunnels

1.1 IPsec protocol

Due to security deficiencies in the IPv4 protocol, an additional functionality called IPsec has been added (and is already incorporated in the IPv6 protocol). The primary purpose of IPsec is to ensure the integrity and confidentiality of the transmitted data. There are essentially two IPsec protocols: AH (*Authentication Header*) and ESP (*Encapsulation Security Payload*). AH is responsible for the integrity of the entire IP packet, while ESP ensures the protection of data confidentiality and integrity of the IP packet. Cryptographic hash functions, such as SHA-1, SHA-256, are used to ensure integrity, and block ciphers, such as 3DES or AES, to ensure confidentiality.

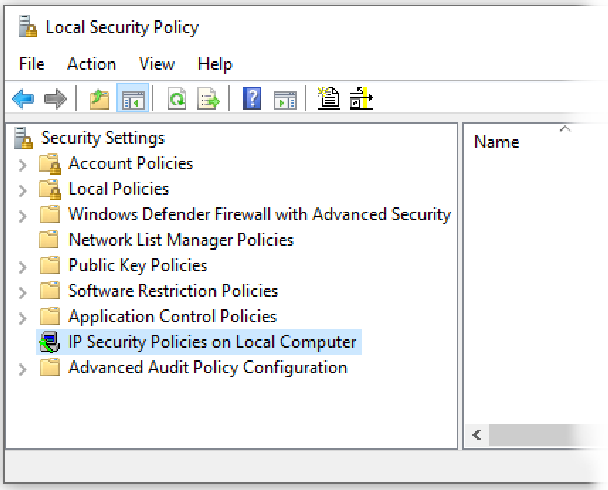
In order to establish IPsec secured communication, the parameters of the *Security Association* (SA) on both sides of the communication must be agreed. The SA associations are unidirectional. Parameter negotiation protocols, e.g. IKE (*Internet Key Exchange*), are used to automate the establishment of SA associations. An important function of these types of protocols is the authentication of the parties that establish an IPsec association. IKE consists of two components:

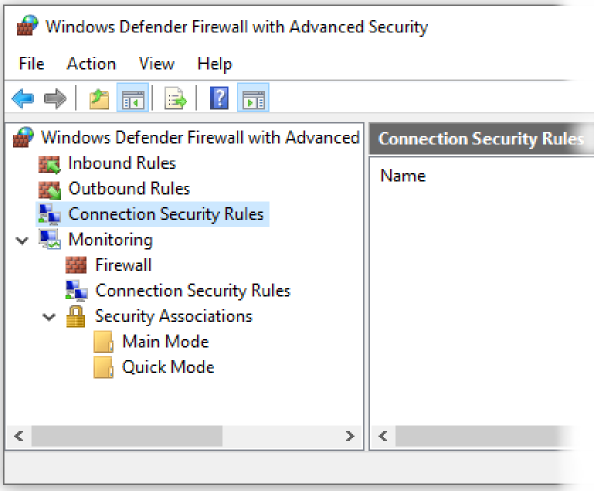
- ISAKMP (*Internet Security Association and Key Management Protocol*), which is the actual protocol for negotiating security association parameters
- *Oakley Key Determination Protocol*, which is a cryptographic Diffie-Hellman key exchange protocol.

IPsec together with IKE can be used to build VPN networks securing communication even in a very complex topology

1.2 IPsec in Windows

Implementation of the IPsec protocol is built into the Windows operating system as part of the Windows Filtering Platform component, integrated with the traffic filtering (firewall) and the address translation mechanism (NAT). IPsec settings can be accessed using the *Local Security Policy* administrative tool or the previously introduced *Windows Firewall Control Panel* applet:

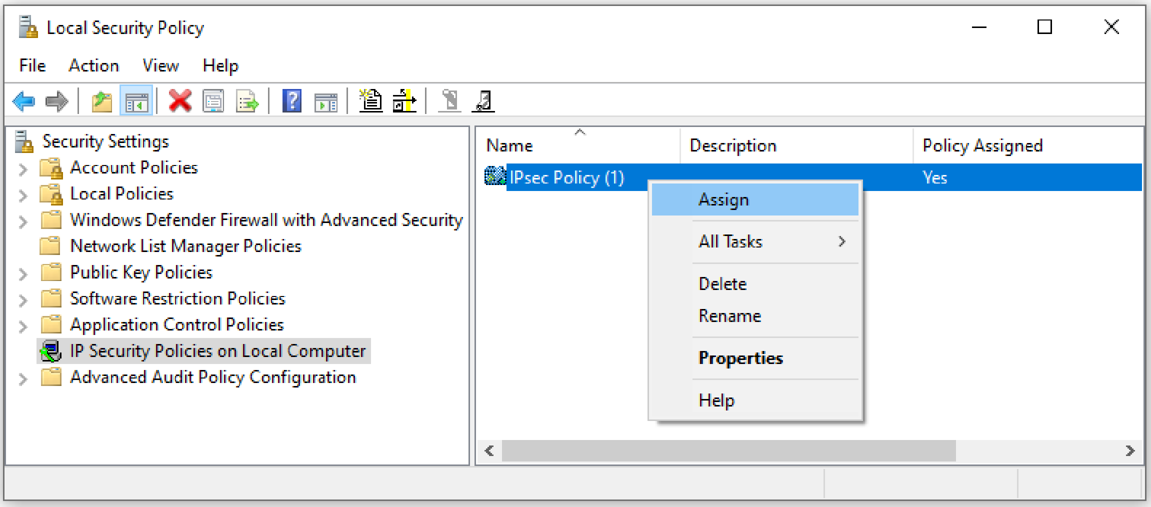

Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Windows Defender Firewall with Advanced Security
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration
Name


Windows Defender Firewall with Advanced Security
File
Action
View
Help
Windows Defender Firewall with Advanced
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Firewall
Connection Security Rules
Security Associations
Main Mode
Quick Mode
Connection Security Rules
Name

1.2.1 Windows IP security settings

IPsec policy is defined through the Local Security Policy. The policy contains traffic filtration rules. The specified traffic is going to be captured end forwarded throughout a VPN connection. In general, each filter allows to encapsulate the filtered traffic within ESP and AH, or completely block the traffic, or pass it through without any additional protection at all.

You can define many policies, but only one of them will be active (i.e. assigned):



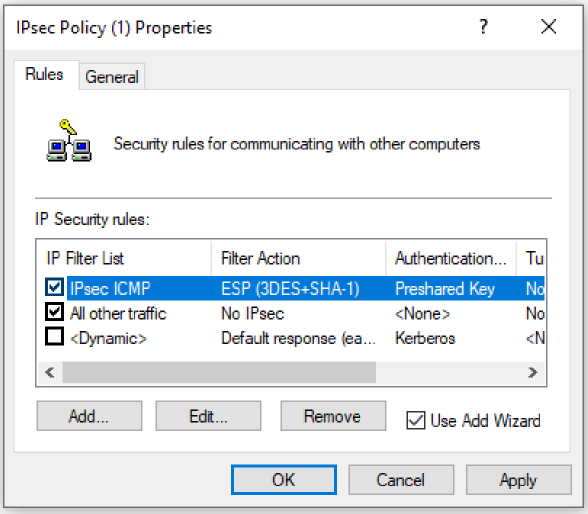
- Security Settings
  - Account Policies
  - Local Policies
  - Windows Defender Firewall with Advanced Security
  - Network List Manager Policies
  - Public Key Policies
  - Software Restriction Policies
  - Application Control Policies
  - IP Security Policies on Local Computer
  - Advanced Audit Policy Configuration

Name	Description	Policy Assigned
IPsec Policy (1)		Yes

Simple host-to-host VPN connection configuration example

For the purpose of this exercise, we will configure a VPN between two computers. In the example, we define a policy requiring security for ICMP traffic.

1. IPsec security policy rules definition



Security rules for communicating with other computers

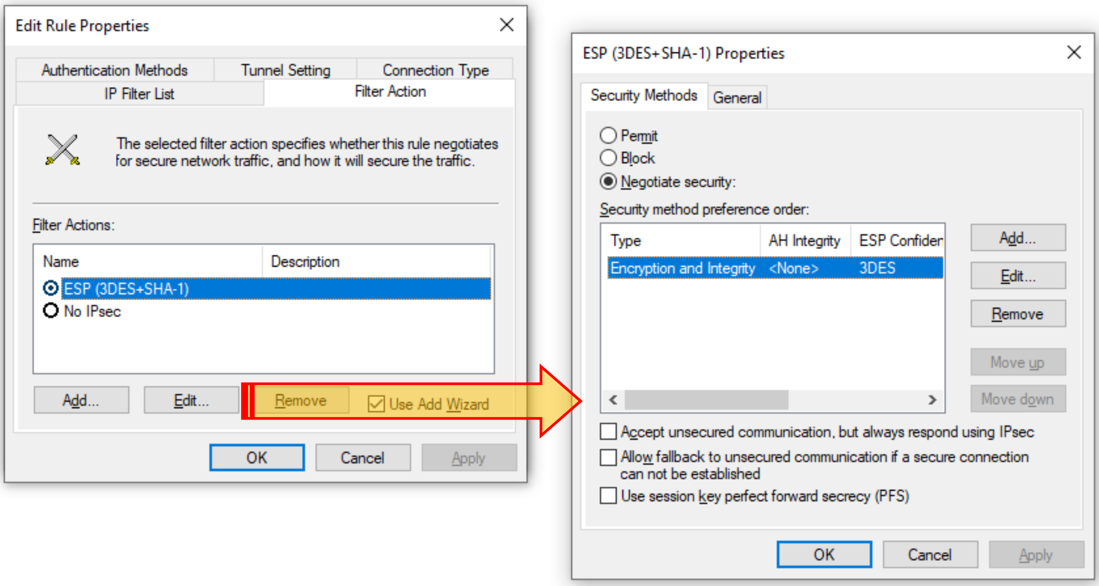
IP Security rules:

IP Filter List	Filter Action	Authentication...	Tu
☑ IPsec ICMP	ESP (3DES+SHA-1)	Preshared Key	No
☑ All other traffic	No IPsec	<None>	No
□ <Dynamic>	Default response (ea...	Kerberos	<N

☑ Use Add Wizard

For each rule, an IP filter (similar to a firewall filter), an action (that is IPsec protection, blocking or pass-through), endpoint authentication method, and possible further net-to-net tunnel endpoints (unnecessary in our case) has to be defined. The rule action defines the required IPsec SA parameters and allows you to specify whether the SA is mandatory or optional (in the latter case SA can be established even if the other endpoint does not support IPsec or the actual negotiation of SA parameters fails, and IP packets are sent unsecured).

2. Basic Security Association parameters specification



The selected filter action specifies whether this rule negotiates for secure network traffic, and how it will secure the traffic.

Filter Actions:

Name	Description
● ESP (3DES+SHA-1)	
○ No IPsec	

☑ Use Add Wizard

○ Permit
○ Block
● Negotiate security:

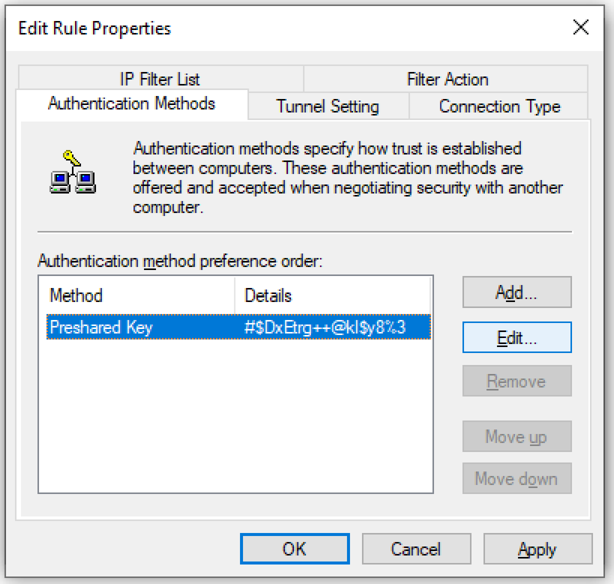
Security method preference order:

Type	AH Integrity	ESP Confider
Encryption and Integrity	<None>	3DES

☐ Accept unsecured communication, but always respond using IPsec
☐ Allow fallback to unsecured communication if a secure connection can not be established
☐ Use session key perfect forward secrecy (PFS)

3. Authentication specification

In our first example, we will choose the simplest (*preshared key*) method:



Authentication methods specify how trust is established between computers. These authentication methods are offered and accepted when negotiating security with another computer.

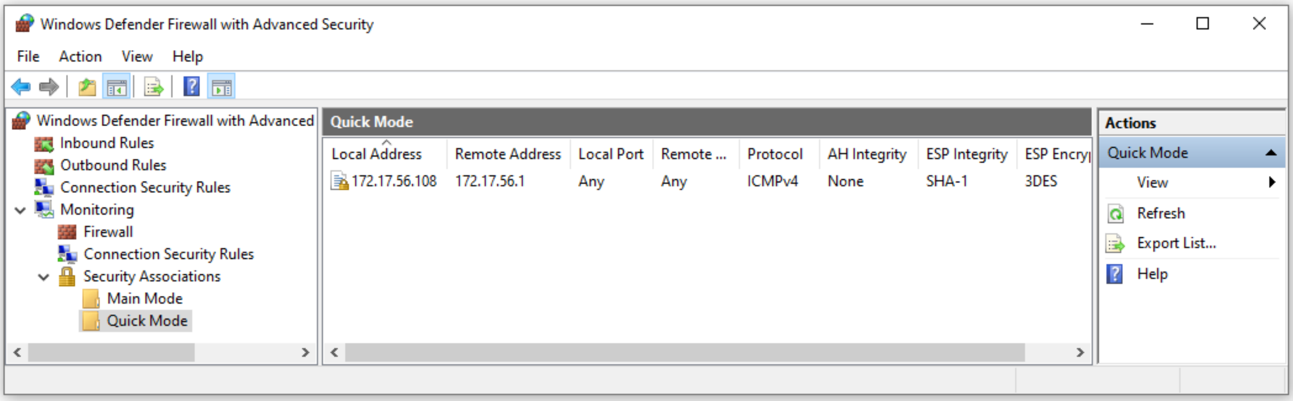
Authentication method preference order:

Method	Details
Preshared Key	#$DxEtrg++@kl$y8%3

1.2.2 Monitoring IPsec association state

SA Database (SAD) and parameters of their compilation (e.g. ISAKMP SA) monitoring is possible thanks to the Windows firewall management applet.

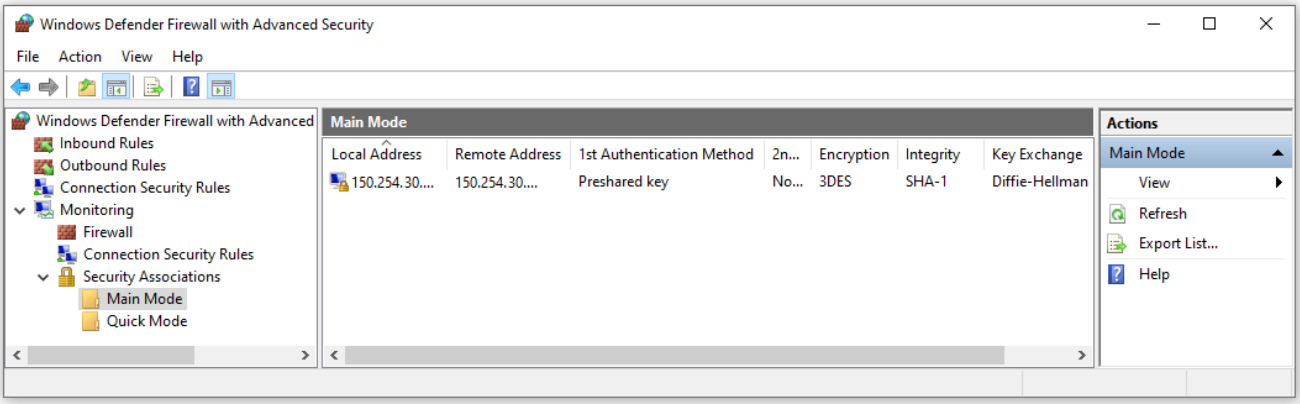
Established IPsec SA associations can be viewed in Quick Mode IKE associations mode:



Quick Mode

Local Address	Remote Address	Local Port	Remote ...	Protocol	AH Integrity	ESP Integrity	ESP Encry
172.17.56.108	172.17.56.1	Any	Any	ICMPv4	None	SHA-1	3DES

and ISAKMP SA associations (used to protect the authentication process and parameter negotiation) are visible in IKE Main Mode:

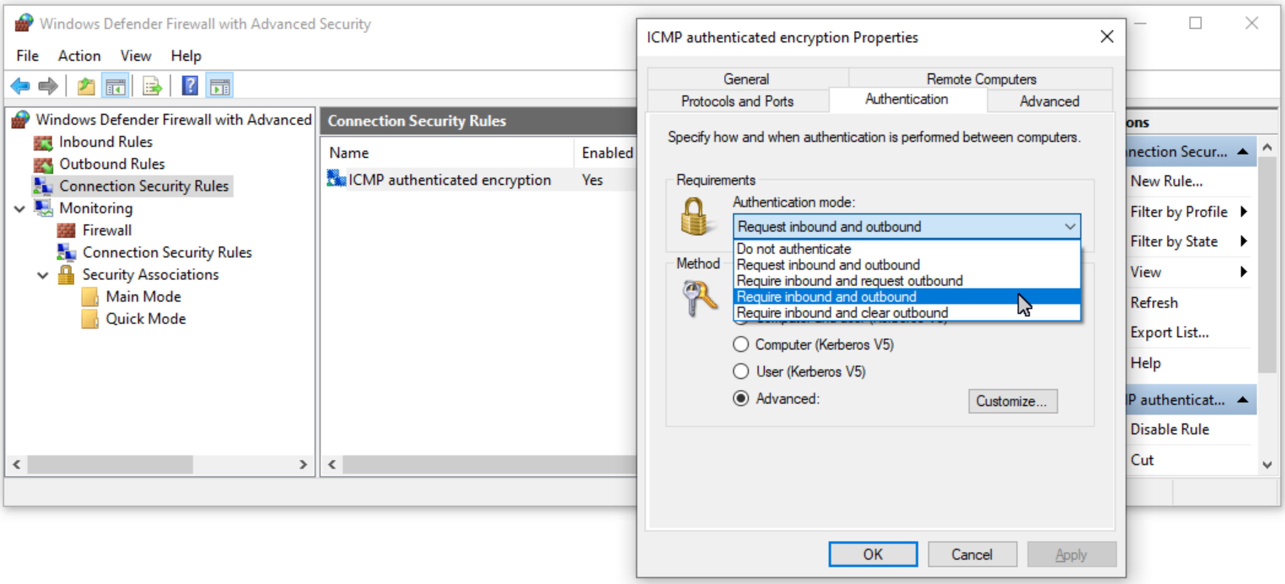


Main Mode

Local Address	Remote Address	1st Authentication Method	2n...	Encryption	Integrity	Key Exchange
150.254.30....	150.254.30....	Preshared key	No...	3DES	SHA-1	Diffie-Hellman

1.2.3 Connection security rules of Windows Firewall

A new firewall mechanism called connection security was introduced with Windows 7. It implies the use of IPsec, with a predefined configuration by default including communication authentication via IKEv2 and packet integrity protection via ESP (SHA-1). Moreover, if the other side of the association requires ESP encryption, the encryption algorithm is automatically negotiated (by default AES, starting from Windows 7 version of the operating system, or 3DES in former versions).



Name	Enabled
ICMP authenticated encryption	Yes

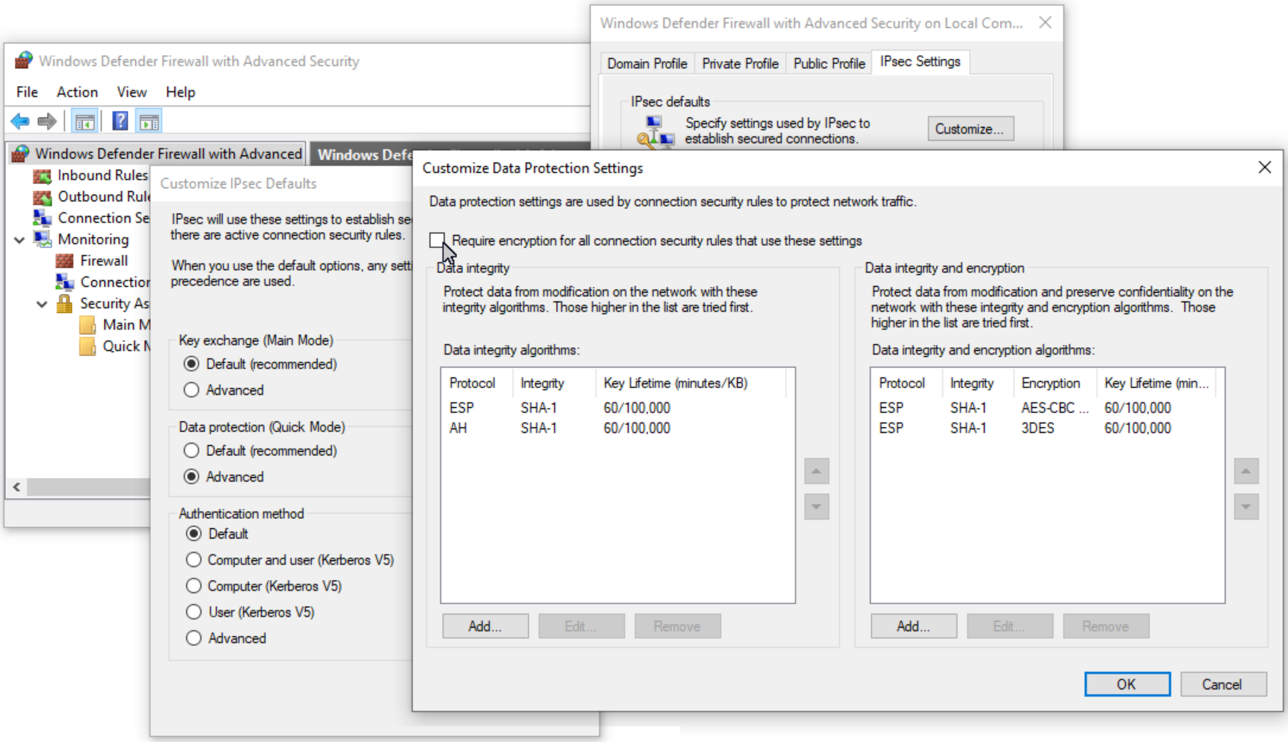
Specify how and when authentication is performed between computers.

Authentication mode: Request inbound and outbound

Do not authenticate
Request inbound and outbound
Require inbound and request outbound
Require inbound and outbound
Require inbound and clear outbound

○ Computer (Kerberos V5)
○ User (Kerberos V5)
● Advanced:

ESP encryption can be forced in the security policy default settings:



Specify settings used by IPsec to establish secured connections.

IPsec will use these settings to establish se there are active connection security rules.

When you use the default options, any setti precedence are used.

Key exchange (Main Mode)
● Default (recommended)
○ Advanced

Data protection (Quick Mode)
○ Default (recommended)
● Advanced

Authentication method
● Default
○ Computer and user (Kerberos V5)
○ Computer (Kerberos V5)
○ User (Kerberos V5)
○ Advanced

Data protection settings are used by connection security rules to protect network traffic.

□ Require encryption for all connection security rules that use these settings

Data integrity

Protect data from modification on the network with these integrity algorithms. Those higher in the list are tried first.

Data integrity algorithms:

Protocol	Integrity	Key Lifetime (minutes/KB)
ESP	SHA-1	60/100,000
AH	SHA-1	60/100,000

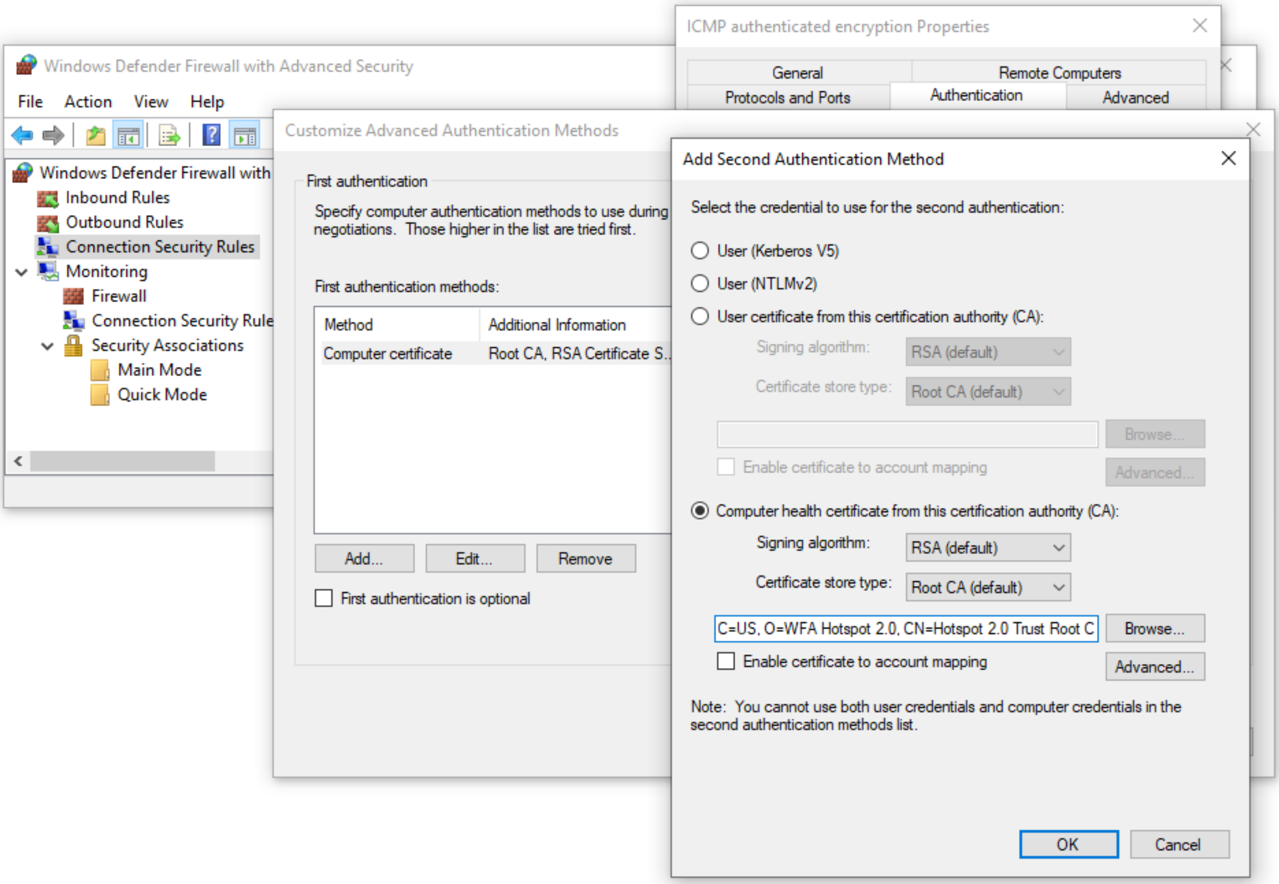
Data integrity and encryption

Protect data from modification and preserve confidentiality on the network with these integrity and encryption algorithms. Those higher in the list are tried first.

Data integrity and encryption algorithms:

Protocol	Integrity	Encryption	Key Lifetime (min...
ESP	SHA-1	AES-CBC ...	60/100,000
ESP	SHA-1	3DES	60/100,000

For association authentication, a proprietary IKEv2-compatible AuthIP mechanism is used. It enables several authentication methods at both system and user level.



Customize Advanced Authentication Methods

First authentication

Specify computer authentication methods to use during negotiations. Those higher in the list are tried first.

First authentication methods:

Method	Additional Information
Computer certificate	Root CA, RSA Certificate S...

Add... Edit... Remove

□ First authentication is optional

Add Second Authentication Method

Select the credential to use for the second authentication:

○ User (Kerberos V5)

○ User (NTLMv2)

○ User certificate from this certification authority (CA):

Signing algorithm: RSA (default)

Certificate store type: Root CA (default)

Browse...

□ Enable certificate to account mapping Advanced...

● Computer health certificate from this certification authority (CA):

Signing algorithm: RSA (default)

Certificate store type: Root CA (default)

C=US, O=WFA Hotspot 2.0, CN=Hotspot 2.0 Trust Root C Browse...

□ Enable certificate to account mapping Advanced...

Note: You cannot use both user credentials and computer credentials in the second authentication methods list.

OK Cancel

If there exist filters in both the firewall connection security rules and in the IPsec policy (defined using the method described in section 1.2.1) that match the same IP datagram, the policy takes priority.

🕮 Additional reading:

Microsoft technical support:

https://technet.microsoft.com/pl-pl/library/dd125380%28v=ws.10%29.aspx
(netsh ipsec) https://technet.microsoft.com/en-us/library/cc725926.aspx
(netsh advfirewall consec) https://technet.microsoft.com/en-us/library/dd736198.aspx

Problems to discuss:

- The IPsec protocol inherits from the IP protocol connectionless semantics of communication, but it uses some mechanisms known typical for connection-oriented protocols, such as sequence numbers, for instance. Does the IPsec association use any kind of sliding window mechanism (as in TCP)?

💻 Exercises:

1. Please configure network connection between two computers: A and B, according to the example provided above. Define simple network shares from selected filesystem directories (on both endpoints) and setup access permissions to them, so the parties can read the shared directories contents. Observe the unsecured communication using a network traffic analyzer.
2. Then setup appropriate IPsec policy settings for the A endpoint only (not allowing for rollback to unsecured communication).

   Define your own IPsec filter for ICMP traffic between A and B. As we use direct IPsec mode (host-to-host model), so the filter rules will not actually apply to what Windows calls "tunnel" (which corresponds to net-to-net or host-to-net model). Make sure that the filter refers to both directions. Choose the authentication method on both sides using pre-shared key. Leave all the remaining traffic unsecured.

   Verify that both sides of the tunnel can access the network shares. Observe the communication using your network analyzer.

   WARNING: To be sure that the SAD rules get refreshed, all changes to the policy properties (e.g. filters) it is best to modify the policy being unassigned (inactive). If you happen to change an active policy, then it should be unassigned afterwards (which will disable all active associations in SAD) and then reassigned back again.

3. In the next step, change the IPsec policy settings for A as to negotiate SA, but accepting also unsecured communication (allowing a fallback to unsecured communication). Double-check if it is now possible to access the network shares.
4. Now, make the appropriate IPsec security settings for side B as well. Make sure that the network shares can still be accessed from both sides.
5. Analyze the communication using your network analyzer.
6. Check the effect of various settings of filter action (AH/ESP algorithms) on the IPsec tunnel. Examine the IPsec monitoring available through the firewall console.
7. Now, disable the previously defined IPsec policy on both computers. On the A side, define a connection security rule (in the firewall console) to *request* authentication for inbound and outbound communication. Verify the impact of this configuration on mutual communication between A and B.
8. Then, still on the A side, change the rule to *require* authentication for inbound and outbound communication. Verify the result.
9. Adjust the configuration on B’s firewall to allow communication between A and B. Verify the result.
10. On the B side (only) disable the connection security rule and restore the last IPsec policy. Verify the result.