Netsh commands for Internet Protocol security

Updated: January 21, 2005

Netsh commands for Internet Protocol security (IPSec)

The Netsh commands for Internet Protocol security (IPSec) provide an equivalent alternative to the console-based management and diagnostic capabilities provided by the IP Security Policy Management and IP Security Monitor snap-ins available in the Microsoft Management Console (MMC). By using the Netsh commands for IPSec, you can configure and view static or dynamic IPSec main mode settings, quick mode settings, rules, and configuration parameters.

Administering IPSec from the command line is especially useful when you want to:

- Script IPSec configuration.
- Extend the security and manageability of IPSec by configuring the following features, which are not available in the IP Security Policy Management snap-in: IPSec diagnostics, default traffic exemptions, strong certificate revocation list (CRL) checking, IKE (Oakley) logging, logging intervals, computer startup security, and computer startup traffic exemptions.

You can run these commands from the Windows Server™ 2003 family command prompt or from the command prompt for the **netsh ipsec** context. For these commands to work at the Windows Server™ 2003 family command prompt, you must type **netsh ipsec** before typing commands and parameters as they appear in the syntax below.

Netsh ipsec static mode commands

You can use the **netsh ipsec static** commands to perform the same management and monitoring tasks that you can perform by using the IP Security Policy Management and IP Security Monitor consoles. By using these commands, you can create, modify, and assign IPSec policies without immediately affecting the configuration of the active IPSec policy.

Netsh ipsec dynamic mode commands

You can use the **netsh ipsec dynamic** commands to display the active state of IPSec and to immediately affect the configuration of the active IPsec policy. These commands directly configure the security policy database (SPD). Changes that you make to an IPSec policy while using these commands take effect only while the IPSec service is running. If the IPSec service is stopped, the dynamic policy settings are discarded. Although most of these commands take effect immediately, several configuration commands still require you to restart the IPSec service or restart the computer before they take effect. For more information about these commands, see the syntax descriptions for the **netsh ipsec dynamic set config** commands.

Caution

- Because the IPSec Policy Agent does not interpret the **netsh ipsec dynamic** commands, you must be knowledgeable in the application of IKE main mode and quick mode policies to use these commands effectively. Exercise caution when using these commands, because it is possible to create invalid IPSec policy configurations without warning.

Notes

- The Netsh commands for IPSec can only be used to configure IPSec policies on computers running members of the Windows Server™ 2003 family.

  To use the command line to configure IPSec policies on computers running Windows XP, use Ipseccmd.exe, which is provided on the Windows XPCD, in the \Support\Tools folder. To use the command line to configure IPSec policies on computers running Windows 2000, use Ipsecpol.exe, which is provided with the *Windows 2000 Server Resource Kit*.

- For more information about **netsh**, see Netsh overview [http://technet2.microsoft.com/WindowsServer/en/library/61427fbd-de1f-4c8a-b613-321f7a3cca6a1033.mspx] and Enter a netsh context [http://technet2.microsoft.com/WindowsServer/en/library/d9b4eed7-f79b-4daf-8c22-ffd9428ddea51033.mspx] .

- For more information about Netsh commands, see The Netsh Command-Line Utility [http://technet2.microsoft.com/WindowsServer/en/library/fd1e2fbe-15a6-413b-b712-28afb312c92f1033.mspx] .

Netsh ipsec

The following commands are available at the **ipsec**> prompt, which is rooted within the netsh environment.

Note

- Although the **dump** command is available at the **ipsec**> prompt, it is not functional.

To view the command syntax, click a command:

- static
- dynamic

static

Switches to the static context.

Syntax

static

Parameters

none

⇡ Top of page

dynamic

Switches to the dynamic context.

Syntax

dynamic

Parameters

none

⇡ Top of page

Netsh ipsec static

The following commands are available at the **ipsec static**> prompt, which is rooted within the netsh environment.

To view the command syntax, click a command:

- add filter
- add filteraction
- add filterlist
- add policy
- add rule
- delete all
- delete filter
- delete filteraction
-

add filter

Adds a filter to the specified filter list.

Syntax

add filter filterlist=srcaddr=dstaddr= [**description=**][**protocol=**][**mirrored=**] [**srcmask=**][**dstmask=**][**srcport=**][**dstport=**]

Parameters

filterlist=*String*

Required. Specifies the name of the filter list to which the filter is added. Each filter defines a set of inbound or outbound network traffic to be secured.

srcaddr={ Me| Any| *IPAddress*| *DNSName*| *ServerType*}

Required. Specifies the source IP address, DNS name, or server type for the IP traffic. You can use **WINS**, **DNS**, **DHCP**, or **gateway** for *ServerType*.

dstaddr={ Me| Any| *IPAddress*| *DNSName*| *ServerType*}

Required. Specifies the destination IP address, DNS name, or server type for the IP traffic. You can use **WINS**, **DNS**, **DHCP**, or **gateway** for *ServerType*.

[description=*String*]

Provides information about the IP filter.

[protocol={ ANY| ICMP| TCP| UDP| RAW| *Integer* }]

Specifies the IP protocol if, in addition to addressing information, you want to filter a specific IP protocol. The default value is **ANY**, meaning all protocols are used for the filter.

[mirrored={ yes| no}]

Specifies whether to create a mirrored filter. Use **yes** to create two filters based on the filter settings--one for traffic to the destination and one for traffic from the destination. The default value is **yes**.

[srcmask={ *Mask*| *Prefix*}]

Specifies the source address subnet mask or the prefix of the packets to be filtered. You can specify a prefix value in the range of 1 through 32. The default value is the mask of 255.255.255.255.

[dstmask={ *Mask*| *Prefix*}

Specifies the destination address subnet mask or the prefix value of the packets to be filtered. You can specify a prefix value in the range of 1 through 32. The default value is the mask of 255.255.255.255.

[srcport=*Port*]

Specifies the source port number of the packets to be filtered. This option only applies if you are filtering TCP or UDP packets. If 0 is specified, packets sent from any port are filtered. The default is any.

[dstport=*Port*]

Specifies the destination port number of the packets to be filtered. This option only applies if you are filtering TCP or UDP packets. If 0 is specified, packets sent to any port are filtered. The default is any.

Remarks

- If a filter list does not exist, it is created.
- Do not create a filter list with the name **all**. Doing this creates a conflict with the **netsh ipsec** option to select all IPSec filter lists (for example, **delete filterlist all**).
- To filter any packets sent from or to the computer, you can use **srcaddr=Me** or **dstaddr=Me**.
- To filter packets sent from or to any computer, you can use **srcaddr=Any** or **dstaddr=Any**.
- All string parameters are case-sensitive.

⇡ Top of page

add filteraction

Creates a filter action with the specified quick mode security methods.

Syntax

add filteractionname= [**description=**][**qmpfs=**][**inpass=**] [**soft=**][**action=**][**qmsecmethods=**]

Parameters

name=*String*

Required. Specifies the name of the filter action to be created.

[description=*String*]

Provides information about the filter action.

[qmpfs={ yes| no}]

Specifies whether to enable session key perfect forward secrecy (PFS). If **yes** is specified, new master key material is renegotiated each time a new session key is required. The default value is **no**.

[inpass={ yes| no}]

Specifies whether to allow an incoming packet that matches the configured filter list to be unsecured, but require IPSec-secured communication when replying. The default value is **no**.

[soft={ yes| no}]

Specifies whether to fall back to unsecured communication with other computers that do not support IPSec, or when IPSec negotiations with an IPSec-capable computer fail. The default value is **no**.

[action={ permit| block| negotiate}]

Specifies whether to permit traffic without negotiating IP security. If **permit** is specified, traffic is transmitted or received without negotiating or applying IP security. If **block** is specified, traffic is blocked. If **negotiate** is specified, IP security is used with the specified list of security methods. The default value is **negotiate**.

[qmsecmethods="*Neg1Neg2*"]

Specifies one or more security methods, separated by spaces and defined by the following format: {**ESP** [*ConfAlg*,*AuthAlg*]**:***k*/*s* | **AH** [*HashAlg*]**:***k*/*s* | **AH** [*HashAlg*+**ESP***ConfAlg*,*AuthAlg*]**:***k*/*s*}]Where:*ConfAlg*Specifies the encryption algorithm. *ConfigAlg* can be **DES** (Data Encryption Standard), **3DES**, or **none**. *AuthAlg*Specifies the integrity algorithm. *AuthAlg* can be **MD5** (Message Digest 5), **SHA1** (Secure Hash Algorithm 1), or **none**.*HashAlg*Specifies the hash function. *HashAlg* can be **MD5** (Message Digest 5) or **SHA1**.*k*Specifies the session key lifetime in kilobytes. After the specified number of kilobytes of data is transferred, a new session key for the quick mode SA is generated. The default value is 100000 kilobytes.*s*Specifies the session key lifetime in seconds. The default value is 3600 seconds.

Remarks

- Do not create a filter action with the name **all**. Doing this creates a conflict with the **netsh ipsec** option to select all

IPSec filter actions (for example, **delete filteraction all**).

- If **action=permit** or **action=block** are specified, and **qmsecmethods** parameters are specified, the **qmsecmethods** parameters are not used. In addition, if **qmpfs=yes**, **inpass=yes**, or **soft=yes** are specified, those parameters are also not used.
- Session key regeneration will start based on whichever interval, seconds or kilobytes, is reached first. If you do not configure new intervals, the default intervals are used.
- If you do not specify **qmsecmethods=** (quick mode security methods), the following default values are used:
  - ESP [3DES, SHA1]:100000k/3600s
  - ESP [3DES, MD5]:100000k/3600s
- The preference order of each quick mode security method is determined by the order in which it was specified in the command.
- All string parameters are case-sensitive.

⇡ Top of page

add filterlist

Creates an empty filter list with the specified name.

Syntax

add filterlistname= [**description=**]

Parameters

name=*String*

Required. Specifies the name of the filter list to be created.

[description=*String*]

Provides information about the filter list.

Remarks

- Do not create a filter list with the name **all**. Doing this creates a conflict with the **netsh ipsec** option to select all IPSec filter lists (for example, **delete filterlist all**).
- All string parameters are case-sensitive.

⇡ Top of page

add policy

Creates an IPSec policy with the specified name.

Syntax

add policyname= [**description=**][**mmpfs=**][**qmpermm=**] [**mmlifetime=**][**activatedefaultrule=**][**pollinginterval=**] [**assign=**][**mmsecmethods=**]

Parameters

name=*String*

Required. Specifies the name of the IPSec policy to be created.

[description=*String*]

Provides information about the IPSec policy.

[mmpfs={ yes| no}]

Specifies whether to enable master key perfect forward secrecy (PFS). If **yes** is specified, main mode security SAs are reauthenticated and new master key keying material is negotiated each time session key material for a quick mode SA is required. The default value is **no**.

[qmpermm=*Integer*]

Specifies the number of times that master keying material can be used to derive the session key. The default value is 0, meaning an unlimited number of quick mode SAs can be derived from the main mode SA.

[mmlifetime=*Integer*]

Specifies the number of minutes after which a new master key will be generated. The default value is 480 minutes.

[activatedefaultrule={ yes| no}]

Specifies whether to activate the default response rule for this IPSec policy. The default value is **yes**.

[pollinginterval=*Integer*]

Specifies how often IPSec polls for changes to this policy. The default value is 180 minutes.

[assign={ yes| no}]

Specifies whether to assign this IPSec policy (only one IPSec policy can be assigned) The default value is **no**.

[mmsecmethods="*SecMeth1SecMeth2*"]

Specifies one or more key exchange security methods, separated by spaces and defined by the following format: *ConfAlg-HashAlg-GroupNumb*, where:*ConfAlg*Specifies the encryption algorithm. *ConfAlg* can be **DES** (Data Encryption Standard) or **3DES**.*HashAlg*Specifies the hash function. *HashAlg* can be **MD5** (Message Digest 5) or **SHA1** (Secure Hash Algorithm 1).*GroupNum*Specifies the Diffie-Hellman group to be used for the base keying material. *GroupNumb* can be: **1** (low, protects with 768 bits of keying material), **2** (medium, protects with 1024 bits), and **3** (high, protects with 2048 bits).

Remarks

- Do not create a policy with the name **all**. Doing this creates a conflict with the **netsh ipsec** option to select all IPSec policies (for example, **delete policy all**).
- Because only one IPSec policy can be assigned, if a policy is currently assigned and you assign a new policy, the currently assigned policy is automatically unassigned.
- If **set store=domain** is specified (when the IPSec policy is stored in Active Directory), **assign** has no effect. To assign a policy to a Group Policy object, you must first create a policy by using the **add policy** command, and then use the **set store** command.
- If **mmpfs=yes** is specified (master key PFS is enabled), by default **qmperm** is set to 1 and not configurable, because each new session will cause the master key keying material to be renegotiated.
- If you do not specify **mmsecmethods=** (key exchange security methods), the following default values are used:
  - 3DES-SHA1-2
  - 3DES-MD5-2
  - 3DES-SHA1-3
- IPSec peers must have at least one common key exchange security method (one that uses the same settings) or negotiations will fail.
- If the number of quick mode negotiations will exceed the value set for the number of quick mode negotiations per main mode negotiation during the main mode lifetime, a new main mode negotiation occurs.
- All string parameters are case-sensitive.

Top of page

add rule

Creates a rule that links the specified IPSec policy, filter list, and filter action with the specified authentication methods.

Syntax

add rulename=policy=filterlist=filteraction=[**tunnel=**][**conntype=**] [**activate=**][**description=**][**kerberos=**][**psk=**][**rootca=**]

Parameters

name=*String*

Required. Specifies the name of the IPSec rule to be created.

policy=*String*

Required. Specifies the name of the IPSec policy that contains this rule.

filterlist=*String*

Required. Specifies the name of the IP filter list for this rule.

filteraction=*String*

Required. Specifies the name of the filter action for this rule.

[tunnel={ *IPAddress*| *DNSName*}]

Specifies the IP address or DNS name of the tunnel endpoint for tunnel mode. By default, this option is not specified and transport mode is used.

[conntype={ lan| dialup| all}]

Specifies whether the rule applies only to remote access or dial-up connections or to local area network (LAN) connections, or to all connections. The default value is **all**.

[activate={ yes | no}]

Specifies whether to activate this rule for the specified IPSec policy. The default value is **yes**.

[description=*String*]

Provides information about the rule.

[kerberos={ yes | no}]

Specifies whether to use the Kerberos V5 protocol as an authentication method.

[psk=*String*]

Specifies the string of characters to use for the preshared key, if a preshared key is used as an authentication method.

[rootca="*String*certmap:{ yes| no} excludecaname:{ yes| no} "]

Specifies certificate authentication options, where: *String* Specifies the distinguished name of the certificate, if a certificate is used as an authentication method.**certmap:**{ **yes**| **no**} Specifies whether to enable certificate-to-account mapping. You can enable certificate-to-account mapping to verify that the certificate is being used by a trusted computer.**excludecaname:**{ **yes**| **no**} Specifies whether to exclude from the certificate request the list of trusted root CA names from which a certificate is accepted.

Remarks

- Do not create a rule with the name **all**. Doing this creates a conflict with the **netsh ipsec** option to select all IPSec rules (for example, **delete rule all**).
- You can only use Kerberos V5 authentication or certificate-to-account mapping for computers that are members of an Active Directory domain.
- Although you can use only one preshared key for authentication, you can use multiple certificates by specifying the **rootca** parameter once, for each certificate you want to use.
- All certificate authentication parameters must be contained within quotation marks. Embedded quotation marks must be replaced by a backslash followed by an apostrophe (\').
- All string parameters are case-sensitive.
- The preference order of each authentication method is determined by the order in which it was specified in the command.
- If no authentication methods are specified, dynamic defaults are used. By default, IPSec policies use Kerberos V5 authentication. If the computer has a computer certificate, any root CA to which the computer certificate chains is also used for authentication.
- If **excludecaname:yes** is specified, the list of trusted root CAs is not sent as part of the certificate request, which prevents the potential disclosure of sensitive information about the trust relationships of a computer. To enhance security for computers connected to the Internet, specify this option.
- The use of preshared key authentication is not recommended because it is a relatively weak authentication method. In addition, preshared keys are stored in plaintext.
- IPSec peers must have at least one common authentication method or communication will fail.

Top of page

delete all

Deletes all IPSec policies, filter lists, and filter actions.

Syntax

delete all

Parameters

None.

Top of page

delete filter

Deletes a filter from a filter list that matches the specified parameters.

Syntax

delete filter filterlist=srcaddr=dstaddr=[**protocol=**] [**srcmask=**][**dstmask=**][**srcport=**] [**dstport=**][**mirrored=**]

Parameters

filterlist=*String*

Required. Specifies the name of the filter list to which the filter was added.

srcaddr={ Me| Any| *IPAddress*| *DNSName*| *ServerType*}

Required. Specifies the source IP address, DNS name, or server type for the IP traffic being matched. You can use **WINS**, **DNS**, **DHCP**, or **gateway** for *ServerType*.

dstaddr={ Me| Any| *IPAddress*| *DNSName*| *ServerType*}

Required. Specifies the destination IP address, DNS name, or server type for the IP traffic being matched. You can use **WINS**, **DNS**, **DHCP**, or **gateway** for *ServerType*.

[protocol={ ANY| ICMP| TCP| UDP| RAW| *Integer* }]

Specifies the IP protocol if, in addition to addressing information, a specific IP protocol is filtered. A value of **ANY** matches filters with a protocol setting of **any**.

[srcmask={ *Mask*| *Prefix*}]

Specifies the source address subnet mask or the prefix of the packets being filtered. You can specify a prefix value in the range of 1 through 32. The default value is the mask of 255.255.255.255.

[dstmask={ *Mask*| *Prefix*}]

Specifies the destination address subnet mask or the prefix value of the packets being filtered. You can specify a prefix value in the range of 1 through 32. The default value is the mask of 255.255.255.255.

[srcport=*Port*]

Specifies the source port number of the packets being filtered. This option only applies if you are filtering TCP or UDP packets. A value of **0** matches filters with a source port setting of **any**.

[dstport=*Port*]

Specifies the destination port number of the packets being filtered. This option only applies if you are filtering TCP or UDP packets. A value of **0** matches filters with a destination port setting of **any**.

[mirrored={ yes| no}]

Specifies whether a mirrored filter was created.

Remarks

- This command only deletes a filter that matches the exact parameters specified.
- If no optional parameters are specified, all filters that match the specified (required) parameters are deleted.
- To delete a filter that filtered any packets sent from or to the computer, you can use **srcaddr=Me** or **dstaddr=Me**.
- To delete a filter that filtered packets sent from or to any computer, you can use **srcaddr=Any** or **dstaddr=Any**.
- All string parameters are case-sensitive.

Top of page

delete filteraction

Deletes the specified filter action, or all filter actions.

Syntax

delete filteractionname= | all

Parameters

name=*String*| all

Required. Specifies the name of the filter action to delete. Or, if **all** is specified, all filter actions are deleted.

Remarks

- All string parameters are case-sensitive.

⇡ Top of page

delete filterlist

Deletes the specified filter list, or all filter lists.

Syntax

delete filterlistname= | all

Parameters

name=*String*| all

Required. Specifies the name of the filter list to delete. Or, if **all** is specified, all filter lists are deleted.

Remarks

- All string parameters are case-sensitive.

⇡ Top of page

delete policy

Deletes the specified IPSec policy and all associated rules, or all IPSec policies.

Syntax

delete policyname= | all

Parameters

name=*String*| all

Required. Specifies the name of the IPSec policy to delete. Or, if **all** is specified, all IPSec policies are deleted.

Remarks

- All string parameters are case-sensitive.

⇡ Top of page

delete rule

Deletes a specified rule, or all rules from the specified IPSec policy.

Syntax

delete rulename= | ID= | allpolicy=

Parameters

name=*String*| ID=*Integer*| all

Required. Specifies the rule to delete. If either the rule name or the rule ID (the number identifying the position of the rule in the policy rule list) is specified, the corresponding rule is deleted. If **all** is specified, all rules are deleted.

policy=*String*

Required. Specifies the name of the policy from which one or more rules are deleted.

Remarks

- The default response rule cannot be deleted.
- After a rule is deleted, all IDs for the remaining rules change accordingly.
- All string parameters are case-sensitive.

⇡ Top of page

exportpolicy

Exports all IPSec policy information to the specified file.

Syntax

exportpolicyfile=

Parameters

file=*String*

Required. Specifies the name of the file into which the IPSec policy information is exported.

Remarks

- By default, when an IPSec policy is imported into a file, the .ipsec extension added to the file name.
- To enhance interoperablity in a mixed environment with computers running Windows 2000, limit the name of the file to which you want the policy information saved to 60 characters.
- All string parameters are case-sensitive.

⇡ Top of page

importpolicy

Imports all IPSec policy information from the specified IPSec file.

Syntax

importpolicyfile=

Parameters

file=*String*

Required. Specifies the name of the file from which the IPSec policy information is imported.

Remarks

- All string parameters are case-sensitive.

⇡ Top of page

restorepolicyexamples

Restores the default IPSec policies.

Syntax

restorepolicyexamplesrelease=

Parameters

release={ win2K| Win2003}

Required. Specifies the version of the default IPSec policies being restored. If **win2K** is specified, the default IPSec policies that were provided with Windows 2000 are restored. If **Win2003** is specified, the default IPSec policies that were provided with the Windows Server™ 2003 family are restored.

Remarks

- Restoring default IPSec policies will overwrite any changes to the original default policies, filter lists, and filter actions, even when the names of these configuration items have been changed. If you have modified these items and you do not want the modifications to be overwritten, do not restore the default policies.
- You can only restore default IPSec policies for computer-based IPSec policies. You cannot restore the default IPSec policies for IPSec policies in Active Directory.

Top of page

set defaultrule

Modifies the default response rule for the specified policy.

Syntax

set defaultrulepolicy=[**qmpfs=**][**activate=**] [**qmsecmethods=**][**kerberos=**][**psk=**][**rootca=**]

Parameters

policy=*String*

Required. Specifies the name of the IPSec policy for which the default response rule is to be modified.

[qmpfs={ yes| no}]

Specifies whether to enable session key perfect forward secrecy (PFS). If **yes** is specified, new master key material is renegotiated each time a new session key is required. The default value is **no**.

[activate={ yes | no}]

Specifies whether to activate this rule for the specified IPSec policy. The default value is **yes**.

[qmsecmethods="*Neg1Neg2*"]

Specifies one or more security methods, separated by spaces and defined by the following format: {**ESP** [*ConfAlg*,*AuthAlg*]**:***k***/***s* | **AH** [*HashAlg*]**:***k***/***s* | **AH** [*HashAlg*+**ESP***ConfAlg*,*AuthAlg*]**:***k***/***s*}]Where:*ConfAlg*Specifies the encryption algorithm. *ConfigAlg* can be **DES** (Data Encryption Standard), **3DES**, or **none**. *AuthAlg*Specifies the integrity algorithm. *AuthAlg* can be **MD5** (Message Digest 5), **SHA1** (Secure Hash Algorithm 1), or **none**.*HashAlg*Specifies the hash function. *HashAlg* can be **MD5** (Message Digest 5) or **SHA1**.*k*Specifies the session key lifetime in kilobytes. After the specified number of kilobytes of data is transferred, a new session key for the quick mode SA is generated. The default value is 100,000 kilobytes.*s*Specifies the session key lifetime in seconds. The default value is 3600 seconds.

[kerberos={ yes | no}]

Specifies whether to use the Kerberos V5 protocol as an authentication method.

[psk=*String*]

Specifies the string of characters to use for the preshared key, if a preshared key is used as an authentication method.

[rootca="*String*certmap:{ yes| no} excludecaname:{ yes| no} "]

Specifies certificate authentication options, where: *String* Specifies the distinguished name of the certificate, if a certificate is used as an authentication method. **certmap:**{ **yes**| **no**} Specifies whether to enable certificate-to-account mapping. You can enable certificate-to-account mapping to verify that the certificate is being used by a trusted computer.**excludecaname:**{ **yes**| **no**} Specifies whether to exclude from the certificate request the list of trusted root CA names from which a certificate is accepted.

Remarks

- You can only use Kerberos V5 authentication or certificate-to-account mapping for computers that are members of an Active Directory domain.
- Although you can use only one preshared key for authentication, you can use multiple certificates by specifying the **rootca** parameter once, for each certificate you want to use.
- All certificate authentication parameters must be contained within quotation marks. Embedded quotation marks must be replaced by a backslash followed by an apostrophe (\').
- All string parameters are case-sensitive.
- The preference order of each authentication method is determined by the order in which it was specified in the

command.

- If no authentication methods are specified, dynamic defaults are used. By default, IPSec policies use Kerberos V5 authentication. If the computer has a computer certificate, any root CA to which the computer certificate chains is also used for authentication.
- If **excludecaname:yes** is specified, the list of trusted root CAs is not sent as part of the certificate request, which prevents the potential disclosure of sensitive information about the trust relationships of a computer. To enhance security for computers connected to the Internet, specify this option.
- The use of preshared key authentication is not recommended because it is a relatively weak authentication method. In addition, preshared keys are stored in plaintext.
- IPSec peers must have at least one common authentication method or communication will fail.
- Modifying authentication methods will overwrite all previous authentication methods, even if the previous authentication methods were different. For example, if **kerberos=yes** and **psk=yes** were previously specified, and then you specify **kerberos=no**, the **psk=yes** parameter will also be overwritten, and preshared key authentication will no longer be used.
- *ConfAlg* and *AuthAlg* cannot both be set to **none**.

⇡ Top of page

set filteraction

Modifies a filter action.

Syntax

set filteractionname= | **guid=**[**newname=**] [**description=**][**qmpfs=**][**inpass=**] [**soft=**][**action=**][**qmsecmethods=**]

Parameters

name=*String*| guid= *guid*

Required. Specifies the name or global unique identifier (GUID) of the filter action to modify.

[newname=*String*]

Specifies the new name of the filter action.

[description=*String*]

Provides information about the filter action.

[qmpfs={ yes| no}]

Specifies whether to enable session key perfect forward secrecy (PFS). If **yes** is specified, new master key material is renegotiated each time a new session key is required.

[inpass={ yes| no}]

Specifies whether to allow an incoming packet that matches the configured filter list to be unsecured, but require IPSec-secured communication when replying.

[soft={ yes| no}]

Specifies whether to fall back to unsecured communications with other computers that do not support IPSec, or when IPSec negotiations with an IPSec-capable computer fail.

[action={ permit| block| negotiate}]

Specifies whether to permit traffic without negotiating IP security. If **permit** is specified, traffic is transmitted or received without negotiating or applying IP security. If **block** is specified, traffic is blocked. If **negotiate** is specified, IP security is used, with the specified list of security methods.

[qmsecmethods="*Neg1Neg2*"]

Specifies one or more security methods, separated by spaces and defined by the following format: {**ESP** [*ConfAlg*,*AuthAlg*]**:***k*/*s* | **AH** [*HashAlg*]**:***k*/*s* | **AH** [*HashAlg*+**ESP***ConfAlg*,*AuthAlg*]**:***k*/*s*}]Where:*ConfAlg*Specifies the encryption algorithm. *ConfigAlg* can be **DES** (Data Encryption Standard), **3DES**, or **none**. *AuthAlg*Specifies the integrity algorithm. *AuthAlg* can be **MD5** (Message Digest 5), **SHA1** (Secure Hash Algorithm 1), or **none**.*HashAlg*Specifies the hash function. *HashAlg* can be **MD5** (Message Digest 5) or **SHA1** (Secure Hash Algorithm 1).*k*Specifies the session key lifetime in kilobytes. After the specified number of kilobytes of data is transferred, a new session key for the quick mode SA is generated. The default value is 100000 kilobytes.*s*Specifies the session key lifetime in seconds. The default value is 3600 seconds.

Remarks

- If you specify a new name for the filter action, do not use the name **all**. Doing this creates a conflict with the **netsh ipsec** option to select all IPSec filter actions (for example, **delete filteraction all**).
- If **action=permit** or **action=block** are specified, do not set **qmpfs=yes**, **inpass=yes**, or **soft=yes**.
- Session key regeneration will start based on whichever interval, seconds or kilobytes, is reached first. If you do not configure new intervals, the default intervals are used.
- If **qmsecmethods=** (quick mode security methods) were not previously specified for this filter action, the following default values are used:
  - ESP [3DES, SHA1]:100000s/3600k
  - ESP [3DES, MD5]:100000s/3600k
- The preference order of each quick mode security method is determined by the order in which it was specified in the command.
- All string parameters are case-sensitive.

⇡ Top of page

set filterlist

Modifies a filter list.

Syntax

set filterlistname= [**newname=**] [**description=**]

Parameters

name=*String*

Required. Specifies the name of the filter list to modify.

[newname=*String*]

Specifies the new name of the filter list.

[description=*String*]

Provides information about the filter list.

Remarks

- If you specify a new name for the filter list, do not use the name **all**. Doing this creates a conflict with the **netsh ipsec** option to select all IPSec filter lists (for example, **delete filterlist all**).
- All string parameters are case-sensitive.

⇡ Top of page

set policy

Modifies an IPSec policy.

Syntax

set policyname=newname= [**description=**][**mmpfs=**][**qmpermm=**] [**mmlifetime=**][**activatedefaultrule=**] [**pollinginterval=**][**assign=**][**gponame=**][**mmsecmethods=**]

Parameters

name=*String*| guid=*guid*

Required. Specifies the name or GUID of the IPSec policy to modify.

newname=*String*

Required. Specifies the new name of the IPSec policy.

[description=*String*]

Provides information about the IPSec policy.

[mmpfs={ yes| no}]

Specifies whether to enable master key perfect forward secrecy (PFS). If **yes** is specified, main mode security SAs are reauthenticated and new master key keying material is negotiated each time session key material for a quick mode SA is required.

[qmpermm=*Integer*]

Specifies the number of times that master keying material can be used to derive the session key.

[mmlifetime=*Integer*]

Specifies the number of minutes after which a new master key will be generated.

[activatedefaultrule={ yes| no}]

Specifies whether to activate the default response rule for this IPSec policy.

[pollinginterval=*Integer*]

Specifies how often IPSec polls for changes to this policy. The default value is 180 minutes.

[assign={ yes| no}]

Specifies whether to assign this IPSec policy.

[gponame=*String*]

Specifies the name of the Group Policy object to which the IPSec policy is assigned. This parameter is only applicable if you are configuring policy for a computer that is an Active Directory domain member.

[mmsecmethods="*SecMeth1SecMeth2*"]

Specifies one or more key exchange security methods, separated by spaces and defined by the following format: *ConfAlg-HashAlg-GroupNumb*, where:*ConfAlg*Specifies the encryption algorithm. *ConfAlg* can be **DES** (Data Encryption Standard) or **3DES**. *HashAlg*Specifies the hash function. *HashAlg* can be **MD5** (Message Digest 5) or **SHA1** (Secure Hash Algorithm 1).*GroupNum*Specifies the Diffie-Hellman group to be used for the base keying material. *GroupNumb* can be: **1** (low, protects with 768 bits of keying material), **2** (medium, protects with 1024 bits), and **3** (high, protects with 2048 bits).

Remarks

- If you specify a new name for the policy, do not use the name **all**. Doing this creates a conflict with the **netsh ipsec** option to select all IPSec policies (for example, **delete policy all**).
- If **set store=domain** is specified (when the IPSec policy is stored in Active Directory), **assign** will have no effect.
- If **mmpfs=yes** is specified (master key PFS is enabled), by default **qmperm** is set to 1 and not configurable, because each new session will cause the master key keying material to be renegotiated.
- IPSec peers must have at least one common key exchange security method (one that uses the same settings) or negotiations will fail.
- You can only specify a Group Policy object name if **set store=domain**.
- All string parameters are case-sensitive.

Top of page

set rule

Modifies a rule in an IPSec policy.

Syntax

set rulename= | **ID=policy=** [**newname=**][**description=**][**filterlist=**] [**filteraction=**] [**tunnel=**][**conntype=**] [**activate=**][**kerberos=**][**psk=**][**rootca=**]

Parameters

name=*String*| ID=*Integer*

Required. Specifies the name or ID (the number identifying the position of the rule in the policy rule list) of the rule to modify.

policy=*String*

Required. Specifies the name of the IPSec policy that contains this rule.

[newname=*String*]

Specifies the new name of the rule.

[description=*String*]

Provides information about the rule.

[filterlist=*String*]

Specifies the name of the IP filter list for this rule.

[filteraction=*String*]

Specifies the name of the filter action for this rule.

[tunnel={ *IPAddress*| *DNSName*}]

Specifies the IP address or DNS name of the tunnel endpoint for tunnel mode.

[conntype={ lan| dialup| all}]

Specifies whether the rule applies only to remote access or dial-up connections or to local area network (LAN) connections, or to all connections.

[activate={ yes | no}]

Specifies whether to activate this rule for the specified IPSec policy.

[kerberos={ yes | no}]

Specifies whether to use the Kerberos V5 protocol as an authentication method.

[psk=*String*]

Specifies the string of characters to use for the preshared key, if a preshared key is used as an authentication method.

[rootca="*String*certmap:{ yes| no} excludecaname:{ yes| no} "]

Specifies certificate authentication options, where: *String* Specifies the distinguished name of the certificate, if a certificate is used as an authentication method.**certmap:**{ **yes**| **no**} Specifies whether to enable certificate-to-account mapping. You can enable certificate-to-account mapping to verify that the certificate is being used by a trusted computer.**excludecaname:**{ **yes**| **no**} Specifies whether to exclude from the certificate request the list of trusted root CA names from which a certificate is accepted.

Remarks

- You can only use Kerberos V5 authentication or certificate-to-account mapping for computers that are members of an Active Directory domain.
- Although you can use only one preshared key for authentication, you can use multiple certificates by specifying the **rootca** parameter once, for each certificate you want to use.
- All certificate authentication parameters must be contained within quotation marks. Embedded quotation marks must be replaced by a backslash followed by an apostrophe (\').
- All string parameters are case-sensitive.
- The preference order of each authentication method is determined by the order in which it was specified in the command.
- If no authentication methods are specified, dynamic defaults are used. By default, IPSec policies use Kerberos V5 authentication. If the computer has a computer certificate, any root CA to which the computer certificate chains is also used for authentication.
- If **excludecaname:yes** is specified, the list of trusted root CAs is not sent as part of the certificate request, which prevents the potential disclosure of sensitive information about the trust relationships of a computer. To enhance security for computers connected to the Internet, specify this option.
- The use of preshared key authentication is not recommended because it is a relatively weak authentication method. In addition, preshared keys are stored in plaintext.
- IPSec peers must have at least one common authentication method or communication will fail.
- Modifying authentication methods will overwrite all previous authentication methods, even if the previous authentication methods were different. For example, if **kerberos=yes** and **psk=yes** were previously specified, and then you specify **kerberos=no**, the **psk=yes** parameter will also be overwritten, and preshared key authentication will no longer be used.

Top of page

set store

Sets the current IPSec policy storage location.

Syntax

set storelocation= [**domain=**]

Parameters

location={ local| persistent| domain}

Required. Specifies the storage location for the IPSec policy.

[domain=]

Specifies the name of the domain where the IPSec policy is stored, if the policy is stored in Active Directory (when **location=domain** is specified).

Remarks

- The **set store** command only works from within the netsh environment, that is:
  - If you run this command from the command prompt for the **netsh ipsec** context).
  - If you run a batch file by using the **netsh.exe** command.
- The persistent store contains IPSec policies that can be assigned to secure this computer at start up, before the local policy or domain-based policy is applied. A persistent IPSec policy provides security in the event of a failure because it remains in effect whether the local policy or domain-based policy is applied or not (for example, an IPSec policy might not be applied if it is corrupted). For enhanced security, it is recommended that you create and assign a persistent policy.
- The local store contains IPSec policies that can be assigned to secure this computer. If a domain policy is available, the domain policy is applied instead of the local policy.
- The domain store contains IPSec policies that can be assigned to secure groups of computers in a domain.
- It is recommended that the persistent policy be the most restrictive of all policies. Domain policies and local policies should complement persistent policies.
- Use the **set machine** command to configure a remote computer.
- All string parameters are case-sensitive.

Top of page

show all

Displays configuration information for all IPSec policies, rules, filter lists, and filter actions.

Syntax

show all [**format=**] [**wide=**]

Parameters

[format={ list| table}]

Specifies whether to display IPSec configuration information in screen or tab-delimited format. The default value is **list**, meaning that output is displayed in screen format.

[wide={ yes | no}]

Specifies whether to allow the display of IPSec configuration information to exceed the screen width of 80 characters. The default value is **no**, meaning that the display of configuration information is limited to the screen width.

Remarks

- Because the **show all** command can result in lengthy, rapidly scrolling output, consider saving the output in a text file, unless you only need to view limited portions.

  To save output in a text file for the **show all** command, do either of the following:

  If you are in the netsh environment (netsh>)

  1. At the netsh prompt, type:

set file open *FileName*.txt

2. Then type:

   ipsec static show all

3. To stop sending output and close the file, type:

   set file close

If you are not in the netsh environment

- At the command prompt, type:

  netsh ipsec static show all >*FileName*.txt

- To stop the output of IPSec configuration information, you must exit **Netsh** by doing one of the following:
  - Close the **Netsh** window by clicking the **X** icon in the upper-right corner of the window.
  - Use Task Manager to end the **Netsh** program.

⇡ Top of page

show filteraction

Displays configuration information for one or more filter actions.

Syntax

show filteractionname= | **rule=** | **all** [**level=**][**format=**] [**wide=**]

Parameters

name=*String*| rule=*String*| all

Required. Specifies one or more filter actions for which configuration information is to be displayed. If **name** is specified, the filter action with the specified name is displayed. If **rule** is specified, all filter actions associated with the specified rule are displayed. If **all** is specified, all filter actions are displayed.

[level={ verbose| normal}]

Specifies the level of information to display. If **verbose** is specified, information about the security methods, policy storage location, and whether session key perfect forward secrecy (PFS) is enabled is displayed, in addition to basic filter action information. The default value is **normal**.

[format={ list| table}]

Specifies whether to display IPSec configuration information in screen or tab-delimited format. The default value is **list**, meaning that output is displayed in screen format.

[wide={ yes | no}]

Specifies whether to allow the display of IPSec configuration information to exceed the screen width of 80 characters. The default value is **no**, meaning that the display of configuration information is limited to the screen width.

Remarks

- All string parameters are case-sensitive.
- Because the **show filteraction** command can result in lengthy, rapidly scrolling output, consider saving the output in a text file, unless you only need to view limited portions.

  To save output in a text file for the **show filteraction** command, do either of the following:

  If you are in the netsh environment (netsh>)

  1. At the netsh prompt, type:

     set file open *FileName*.txt

  2. Then type:

     ipsec static show filteraction*Name* | *Rule* | **all** [**level=verbose** | **normal**]

  3. To stop sending output and close the file, type:

```
set file close
```

If you are not in the netsh environment

- At the command prompt, type:

  ```
  netsh ipsec static show filteractionName | Rule | all [level=verbose | normal] >FileName.txt
  ```

- To stop the output of IPSec configuration information, you must exit **Netsh** by doing one of the following:
  - Close the **Netsh** window by clicking the **X** icon in the upper-right corner of the window.
  - Use Task Manager to end the **Netsh** program.

⇡ Top of page

show filterlist

Displays configuration information for one or more filter lists.

Syntax

```
show filterlistname= | rule= | all [level=][format=][resolvedns=] [wide=]
```

Parameters

name=*String*| rule=*String*| all

Required. Specifies one or more filter lists to display. If **name** is specified, the filter list with the specified name is displayed. If **rule** is specified, all filter lists associated with the specified rule are displayed. If **all** is specified, all filter lists are displayed.

[level={ verbose| normal}]

Specifies the level of information to display. If **verbose** is specified, the source, destination, and type of IP traffic defined by each filter are displayed, in addition to basic filter list information. The default value is **normal**.

[format={ list| table}]

Specifies whether to display IPSec configuration information in screen or tab-delimited format. The default value is **list**, meaning that output is displayed in screen format.

[resolvedns={ yes | no}]

Specifies whether to resolve the Domain Name System (DNS) or NETBIOS computer name associated with an IP address when displaying sources or destinations. If **yes** is specified, **level** must also be set to **verbose**, or the DNS names are not displayed. The default value is **no**.

[wide={ yes | no}]

Specifies whether to allow the display of IPSec configuration information to exceed the screen width of 80 characters. The default value is **no**, meaning that the display of configuration information is limited to the screen width.

Remarks

- All string parameters are case-sensitive.
- Because the **show filterlist** command can result in lengthy, rapidly scrolling output, consider saving the output in a text file, unless you only need to view limited portions.

  To save output in a text file for the **show all** command, do either of the following:

  If you are in the netsh environment (netsh>)

  1. At the netsh prompt, type:

     ```
     set file open FileName.txt
     ```

  2. Then type:

     ```
     ipsec static show filterlistName | rule | all [level=verbose | normal][resolvedns=yes | no
     ```

  3. To stop sending output and close the file, type:

     ```
     set file close
     ```

  If you are not in the netsh environment

- At the command prompt, type:

  netsh ipsec static show filterlist*Name* | *rule* | **all** [**level=verbose** | **normal**][**resolvedns=yes** | **no** >*FileName*.txt

- To stop the output of IPSec configuration information, you must exit **Netsh** by doing one of the following:

  - Close the **Netsh** window by clicking the **X** icon in the upper-right corner of the window.

  - Use Task Manager to end the **Netsh** program.

⇡ Top of page

show gpoassignedpolicy

Displays configuration information for the active IPSec policy assigned to the specified Group Policy object.

Syntax

show gpoassignedpolicy [**name=**]

Parameters

[name=*String*]

Specifies the name of the Group Policy object to which the active IPSec policy is assigned. If no name is specified, the local IPSec policy is displayed.

Remarks

- You can only specify a Group Policy object name if **set store=domain**.

- All string parameters are case-sensitive.

  To save output in a text file for the **show gpossignedpolicy** command, do either of the following:

  If you are in the netsh environment (netsh>)

  1. At the netsh prompt, type:

     set file open *FileName*.txt

  2. Then type:

     ipsec static show gpoassignedpolicy [*Name*]

  3. To stop sending output and close the file, type:

     set file close

  If you are not in the netsh environment

  - At the command prompt, type:

    netsh ipsec static show gpoassignedpolicy [*Name*] >*FileName*.txt

⇡ Top of page

show policy

Displays configuration information for the specified IPSec policy, or for all IPSec policies.

Syntax

show policyname= | **all** [**level=**] [**format=**] [**wide=**]

Parameters

name=*String*| all

Required. Specifies the name of the IPSec policy to display or, if **all** is specified, that all IPSec policies are displayed.

[level={ verbose| normal}]

Specifies the level of information to display. If **verbose** is specified, the security methods and authentication method are displayed, in addition to information about filter actions and rules. The default value is **normal**.

[format={ list| table}]

Specifies whether to display IPSec configuration information in screen or tab-delimited format. The default value is **list**, meaning that output is displayed in screen format.

[wide={ yes | no}]

Specifies whether to allow the display of IPSec configuration information to exceed the screen width of 80 characters. The default value is **no**, meaning that the display of configuration information is limited to the screen width.

Remarks

- All string parameters are case-sensitive.
- Because the **show policy** command can result in lengthy, rapidly scrolling output, consider saving the output in a text file, unless you only need to view limited portions.

  To save output in a text file for the **show policy** command, do either of the following:

  If you are in the netsh environment (netsh>)

  1. At the netsh prompt, type:

     set file open *FileName*.txt

  2. Then type:

     ipsec static show policy*Name* | **all** >*FileName*.txt

  3. To stop sending output and close the file, type:

     set file close

  If you are not in the netsh environment

  - At the command prompt, type:

    netsh ipsec static show policy*Name* | **all** >*FileName***.txt**

- To stop the output of IPSec configuration information, you must exit **Netsh** by doing one of the following:
  - Close the **Netsh** window by clicking the **X** icon in the upper-right corner of the window.
  - Use Task Manager to end the **Netsh** program.

Top of page

show rule

Displays configuration information for a rule for a specified policy, or for all rules for a specified policy.

Syntax

show rulename= | **ID=** | **all** | **defaultpolicy=** [**type=**][**level=**][**format=**] [**wide=**]

Parameters

name={ *String*| ID=*Integer*| all| default}

Required. Specifies one or more rules to display. If either the rule name or the rule ID (the number identifying the position of the rule in the policy rule list) is specified, the corresponding rule is displayed. If **all** is specified, all rules for the specified policy are displayed. If **default** is specified, the default response rule is displayed.

policy=*String*

Required. Specifies the name of the policy for which the specified rule, or all rules, are displayed.

[type={ transport| tunnel}]

Specifies whether to display all transport rules or all tunnel rules. The default value is to display all rules.

[level={ verbose| normal}]

Specifies the level of information to display. If **verbose** is specified, information about associated filter actions is displayed, in addition to basic information about the rule. The default value is **normal**.

[format={ list| table}]

Specifies whether to display IPSec configuration information in screen or tab-delimited format. The default value is **list**, meaning that output is displayed in screen format.

[wide={ yes | no}]

Specifies whether to allow the display of IPSec configuration information to exceed the screen width of 80 characters. The default value is **no**, meaning that the display of configuration information is limited to the screen width.

Remarks

- If you use the **type** parameter, you must also use the **all** parameter (you must specify **show rule all**).
- All string parameters are case-sensitive.
- Because the **show rule** command can result in lengthy, rapidly scrolling output, consider saving the output in a text file, unless you only need to view limited portions.

  To save output in a text file for the **show rule** command, do either of the following:

  If you are in the netsh environment (netsh>)

  1. At the netsh prompt, type:

     set file open *FileName*.txt

  2. Then type:

     ipsec static show rule*Name* | *ID* | **all** | **default***Policy* [**level=verbose** | **normal**]

  3. To stop sending output and close the file, type:

     set file close

  If you are not in the netsh environment

  - At the command prompt, type:

    netsh ipsec static show rule*Name* | *ID* | **all** | **default***Policy* [**level=verbose** | **normal**] >*FileName*.txt

- To stop the output of IPSec configuration information, you must exit **Netsh** by doing one of the following:
  - Close the **Netsh** window by clicking the **X** icon in the upper-right corner of the window.
  - Use Task Manager to end the **Netsh** program.

⇡ Top of page

Netsh ipsec dynamic

The following commands are available at the **ipsec dynamic** > prompt, which is rooted within the netsh environment.

To view the command syntax, click a command:

- add mmpolicy
- add qmpolicy
- add rule
- delete all
- delete mmpolicy
- delete qmpolicy
- delete rule
- set config
- set mmpolicy
- set qmpolicy

- set rule
- show all
- show config
- show mmfilter
- show mmpolicy
- show mmsas
- show qmfilter
- show qmpolicy
- show qmsas
- show rule
- show stats

add mmpolicy

Creates an IPSec main mode policy with the specified name and adds it to the security policy database (SPD).

Syntax

add mmpolicyname= [**qmpermm=**] [**mmlifetime=**][**softsaexpirationtime=**][**mmsecmethods=**]

Parameters

name=*String*

Required. Specifies the name of the IPSec policy to be created.

[qmpermm=*Integer*]

Specifies the number of times that master keying material can be used to derive the session key. The default value is 0, The default value is 0, meaning an unlimited number of quick mode SAs can be derived from the main mode SA.

[mmlifetime=*Integer*]

Specifies the number of minutes after which a new master key is generated. The default value is 480 minutes.

[softsaexpirationtime=*Integer*]

Specifies the number of minutes after which an unprotected security association expires. The default value is 480 minutes.

[mmsecmethods="*SecMeth1SecMeth2*"]

Specifies one or more key exchange security methods, separated by spaces and defined by the following format: *ConfAlg-HashAlg-GroupNumb*, where:*ConfAlg*Specifies the encryption algorithm. *ConfAlg* can be **DES** or **3DES**. *HashAlg*Specifies the hash function. *HashAlg* can be **MD5** or **SHA1**.*GroupNum*Specifies the Diffie-Hellman group to be used for the base keying material. *GroupNumb* can be: **1** (low, protects with 768 bits of keying material), **2** (medium, protects with 1024 bits), and **3** (high, protects with 2048 bits).

Remarks

- Do not create a main mode policy with the name **all**. Doing this creates a conflict with the **netsh ipsec** option to select all IPSec main mode policies (for example, **delete mmpolicy all**).
- If the number of quick mode negotiations will exceed the value set for the number of quick mode negotiations per main mode negotiation during the main mode lifetime, a new main mode negotiation occurs.
- If you do not specify **mmsecmethods=** (key exchange security methods), the following default values are used:
  - 3DES-SHA1-2
  - 3DES-MD5-2
  - 3DES-SHA1-3
- IPSec peers must have at least one common key exchange security method (one that uses the same settings) or negotiations will fail.
- All string parameters are case-sensitive.

Top of page

add qmpolicy

Creates an IPSec quick mode policy with the specified name and adds it to the SPD.

Syntax

add qmpolicyname= [**soft=**][**pfsgroup=**][**qmsecmethods=**]

Parameters

name=*String*

Required. Specifies the name of the IPSec quick mode policy to be created.

[soft={ yes| no}]

Specifies whether to fall back to unsecured communications with other computers that do not support IPSec, or when IPSec negotiations with an IPSec-capable computer fail. The default value is **no**.

[pfsgroup={ grp1| grp2| grp3| grpmm| nopfs}]

Specifies the Diffie-Hellman group to use for session key PFS. If **grp1** is specified, Group 1 (low) is used. If **grp2** is specified, Group 2 (medium) is used. If **grp3** is specified, Group 2048 (high) is used. If **grpmm** is specified, the group value is taken from the current main mode settings. The default value is **nopfs**, meaning session key PFS is disabled.

[qmsecmethods="*Neg1Neg2*"]

Specifies one or more security methods, separated by spaces and defined by the following format: {**ESP** [*ConfAlg*,*AuthAlg*]**:***k*/*s* | **AH** [*HashAlg*]**:***k/s* | **AH** [*HashAlg*+**ESP***ConfAlg*,*AuthAlg*]**:***k*/*s*}]Where:*ConfAlg*Specifies the encryption algorithm. *ConfigAlg* can be **DES** (Data Encryption Standard), **3DES**, or **none**. *AuthAlg*Specifies the integrity algorithm. *AuthAlg* can be **MD5** (Message Digest 5), **SHA1** (Secure Hash Algorithm 1), or **none**.*HashAlg*Specifies the hash function. *HashAlg* can be **MD5** (Message Digest 5) or **SHA1** (Secure Hash Algorithm 1).*k*Specifies the session key lifetime in kilobytes. After the specified number of kilobytes of data is transferred, a new session key for the quick mode SA is generated. The default value is 100000 kilobytes.*s*Specifies the session key lifetime in seconds. The default value is 3600 seconds.

Remarks

- Do not create a quick mode policy with the name **all**. Doing this creates a conflict with the **netsh ipsec** option to select all IPSec quick mode policies (for example, **delete qmpolicy all**).
- If you do not specify **qmsecmethods=** (quick mode security methods), the following default values are used:
  - ESP [3DES, SHA1]100000k/3600s
  - ESP [3DES, MD5]100000k/3600s
- *ConfAlg* and *AuthAlg* cannot both be set to **none**.
- IPSec peers must have the same **pfsgroup** enabled (that is, both peers must use the same Diffie-Hellman group for session key PFS), or communication will fail.
- For enhanced security, do not use Diffie-Hellman Group 1. For maximum security, use Group 2048 whenever possible. Use Group 2 when required for interoperability with Windows 2000 and Windows XP.
- All string parameters are case-sensitive.

⇡ Top of page

add rule

Creates an IPSec rule with the specified main mode policy and quick mode policy and adds it to the SPD.

Syntax

add rulesrcaddr=dstaddr=mmpolicy=[**qmpolicy=**][**protocol=**][**srcport=**][**dstport=**][**mirrored=**][**conntype=**][**actioninbound=**][**actionoutbound=**][**srcmask=**][**dstmask=**][**tunneldstaddress=**][**kerberos=**][**psk=**][**rootca=**]

Parameters

srcaddr={ Me| Any| *IPAddress*| *DNSName*| *ServerType*}

Required. Specifies the source IP address, DNS name, or server type for the IP traffic. You can use **WINS**, **DNS**, **DHCP**, or **gateway** for *ServerType*.

dstaddr={ Me| Any| *IPAddress*| *DNSName*| *ServerType*}

Required. Specifies the destination IP address, DNS name, or server type for the IP traffic. You can use **WINS**, **DNS**,

DHCP, or **gateway** for *ServerType*.

mmpolicy=*String*

Required. Specifies the name of the main mode policy.

[qmpolicy=] *String*

Specifies the name of the quick mode policy. Required if **actioninbound=negotiate** or **actionoutbound=negotiate** are specified.

[protocol={ ANY| ICMP| TCP| UDP| RAW| *Integer* }]

Specifies the IP protocol if, in addition to address information, you want to filter a specific IP protocol. The default value is **ANY**, meaning all protocols are used for the filter.

[srcport=*Port*]

Specifies the source port number of the packets to be filtered. This option only applies if you are filtering TCP or UDP packets. If 0 is specified, packets sent from any port are filtered. The default is any.

[dstport=*Port*]

Specifies the destination port number of the packets to be filtered. This option only applies if you are filtering TCP or UDP packets. If 0 is specified, packets sent to any port are filtered. The default is any.

[mirrored={ yes| no}]

Specifies whether to create a mirrored filter. Use **yes** to create two filters based on the filter settings, one for traffic to the destination and one for traffic from the destination. The default value is **yes**.

[conntype={ lan| dialup| all}]

Specifies whether the rule applies only to remote access or dial-up connections or to local area network (LAN) connections, or to all connections. The default value is **all**.

[actioninbound={ permit| block| negotiate}]

Specifies the action that IPSec is required to take for inbound traffic. If **permit** is specified, traffic is received without negotiating or applying IP security. If **block** is specified, traffic is blocked. If **negotiate** is specified, IP security is used, with the list of security methods specified in the main mode and quick mode policies. The default value is **negotiate**.

[actionoutbound={ permit| block| negotiate}]

Specifies the action that IPSec is required to take for outbound traffic. If **permit** is specified, traffic is sent without negotiating or applying IP security. If **block** is specified, traffic is blocked. If **negotiate** is specified, IP security is used, with the list of security methods specified in the main mode and quick mode policies. The default value is **negotiate**.

[srcmask={ *Mask*| *Prefix*}]

Specifies the source address subnet mask or the prefix of the packets to be filtered. You can specify a prefix value in the range of 1 through 32. The default value is the mask of 255.255.255.255.

[dstmask={ *Mask*| *Prefix*}]

Specifies the destination address subnet mask or the prefix value of the packets to be filtered. You can specify a prefix value in the range of 1 through 32. The default value is the mask of 255.255.255.255.

[tunneldstaddress={ *IPAddress*| *DNSName*}]

Specifies whether the traffic is tunneled and, if it is, the IP address or DNS name of the tunnel destination (the computer or gateway on the other side of the tunnel).

[kerberos={ yes | no}]

Specifies whether to use the Kerberos V5 protocol as an authentication method.

[psk=*String*]

Specifies the string of characters to use for the preshared key, if a preshared key is used as an authentication method.

[rootca="*String*certmap:{ yes| no} excludecaname:{ yes| no} "]

Specifies certificate authentication options, where: *String* Specifies the distinguished name of the certificate, if a certificate is used as an authentication method. **certmap:**{ **yes**| **no**} Specifies whether to enable certificate-to-account mapping. You can enable certificate-to-account mapping to verify that the certificate is being used by a trusted computer.**excludecaname:**{ **yes**| **no**} Specifies whether to exclude from the certificate request the list of trusted root CA names from which a certificate is accepted.

Remarks

- Do not create a rule with the name **all**. Doing this creates a conflict with the **netsh ipsec** option to select all IPSec rules (for example, **delete rule all**).
- If the filter action for both inbound and outbound traffic (**actioninbound** and **actionoutbound**) are set to **Permit** or **Block**, a quick mode filter is not required.
- If a tunnel rule is specified, **mirror** should be set to **no** (by default, **mirror** is set to **yes**). For IPSec tunnels, you must

create two rules--one rule describes the traffic to be sent through the tunnel (outbound traffic) and the other describes the traffic to be received through the tunnel (inbound). Next, create two rules that use the inbound and outbound filter lists in your policy.

- To filter any packets sent from or to the computer, you can use **srcaddr=Me** or **dstaddr=Me**.
- To filter packets sent from or to any computer, you can use **srcaddr=Any** or **dstaddr=Any**.
- You can only use Kerberos V5 authentication or certificate-to-account mapping for computers that are members of an Active Directory domain.
- Although you can use only one preshared key for authentication, you can use multiple certificates by specifying the **rootca** parameter once, for each certificate you want to use.
- All certificate authentication parameters must be contained within quotation marks. Embedded quotation marks must be replaced by a backslash followed by an apostrophe (\').
- All string parameters are case-sensitive.
- The preference order of each authentication method is determined by the order in which it was specified in the command.
- If no authentication methods are specified, dynamic defaults are used. By default, IPSec policies use Kerberos V5 authentication. If the computer has a computer certificate, any root CA to which the computer certificate chains is also used for authentication.
- If **excludecaname:yes** is specified, the list of trusted root CAs is not sent as part of the certificate request, which prevents the potential disclosure of sensitive information about the trust relationships of a computer. To enhance security for computers connected to the Internet, specify this option.
- The use of preshared key authentication is not recommended because it is a relatively weak authentication method. In addition, preshared keys are stored in plaintext.
- IPSec peers must have at least one common authentication method or communication will fail.

⇡ Top of page

delete all

Deletes all IPSec policies, filters, and authentication methods, if possible, from the SPD.

Syntax

delete all

Parameters

None.

⇡ Top of page

delete mmpolicy

Deletes the specified IPSec main mode policy, or all IPSec main mode policies, from the SPD.

Syntax

delete mmpolicyname= | **all**

Parameters

name=*String*| all

Required. Specifies the name of the IPSec main mode policy to delete. Or, if **all** is specified, all IPSec main mode policies are deleted.

Remarks

- If a rule is associated with the main mode policy, you must delete the rule before you can delete the policy.
- All string parameters are case-sensitive.

⇡ Top of page

delete qmpolicy

Deletes the specified IPSec quick mode policy, or all IPSec quick mode policies, from the SPD.

Syntax

delete qmpolicy [**name=**] | [**all**]

Parameters

name=*String*| all

Required. Specifies the name of the IPSec quick mode policy to delete. Or, if **all** is specified, all IPSec quick mode policies are deleted.

Remarks

- If a rule is associated with the quick mode policy, you must delete the rule before you can delete the policy.
- All string parameters are case-sensitive.

⇡ Top of page

delete rule

Deletes an IPSec rule from the SPD.

Syntax

delete rulesrcaddr=dstaddr=protocol=srcport=dstport=mirrored=conntype=[**srcmask=**][**dstmask=**][**tunneldstaddress=**]

Parameters

srcaddr={ Me| Any| *IPAddress*| *DNSName*| *ServerType*}

Required. Specifies the source IP address, DNS name, or server type for the IP traffic. You can use **WINS**, **DNS**, **DHCP**, or **gateway** for *ServerType*.

dstaddr={ Me| Any| *IPAddress*| *DNSName*| *ServerType*}

Required. Specifies the destination IP address, DNS name, or server type for the IP traffic. You can use **WINS**, **DNS**, **DHCP**, or **gateway** for *ServerType*.

protocol={ ANY| ICMP| TCP| UDP| RAW| *Integer* }

Required. Specifies the IP protocol used for the filter.

srcport=*Port*

Required. Specifies the source port number of the packets being filtered. This option only applies if you are filtering TCP or UDP packets. A value of **0** matches filters set to a source port of **0** or **any**.

dstport=*Port*

Required. Specifies the destination port number of the packets being filtered. This option only applies if you are filtering TCP or UDP packets. A value of **0** matches filters set to a destination port of **0** or **any**.

mirrored={ yes| no}

Required. Specifies whether the rule was created with mirrored filters.

conntype={ lan| dialup| all}

Required. Specifies whether the rule to be deleted applies only to remote access or dial-up connections or to local area network (LAN) connections, or to all connections.

[srcmask={ *Mask*| *Prefix*}]

Specifies the source address subnet mask or the prefix of the packets being filtered. You can specify a prefix value in the range of 1 through 32. The default value is the mask of 255.255.255.255.

[dstmask={ *Mask*| *Prefix*}]

Specifies the destination address subnet mask or the prefix value of the packets being filtered. You can specify a prefix value in the range of 1 through 32. The default value is the mask of 255.255.255.255.

[tunneldstaddress={ *IPAddress*| *DNSName*}]

Specifies whether the traffic is tunneled and, if it is, the IP address or DNS name of the tunnel destination (the computer or gateway on the other side of the tunnel).

Remarks

- To filter any packets sent from or to the computer, you can use **srcaddr=Me** or **dstaddr=Me**.
- To filter packets sent from or to any computer, you can use **srcaddr=Any** or **dstaddr=Any**.

⇡ Top of page

set config

Creates or modifies the following IPSec settings: IPSec diagnostics, default traffic exemptions, strong certificate revocation list (CRL) checking, IKE (Oakley) logging, logging intervals, computer startup security, and computer startup traffic exemptions.

Syntax

set config [**property=**] [**value=**]

Parameters

[property=]{ ipsecdiagnostics value=| ipsecexempt value=| ipsecloginterval value=| ikelogging value=| strongcrlcheck value=| bootmode value=| bootexemptions value=}

Required. Specifies the name of the IPSec setting to be created or modified and a value for the setting, where:**ipsecdiagnostics value=**{ **0**| **1**| **2**| **3**| **4**| **5**| **6**| **7**} Specifies whether to enable IPSec diagnostic logging and, if so, which level of logging to provide. The default value is **0**, meaning that logging is disabled. If you change the value for this setting, you must restart the computer for the new value to take effect. You can specify other values as follows, to enable different levels of logging:When **1** is specified, bad SPI packets (the total number of packets for which the Security Parameters Index or SPI was incorrect), IKE negotiation failures, IPSec processing failures, packets received with invalid packet syntax, and other errors are recorded in the System log. Unauthenticated hashes (with the exception of the "Clear text received when should have been secured" event) are logged as well. When **2** is specified, inbound per-packet drop events are recorded in the System log. When **3** is specified, level 1 and level 2 logging are performed. In addition, unexpected clear text events (packets that are sent or received in plaintext) are also recorded. When **4** is specified, outbound per-packet drop events are recorded in the System log. When **5** is specified, level 1 and level 4 logging are performed.When **6** is specified, level 2 and level 4 logging are performed.When **7** specified, all levels of logging are performed.**ipsecexempt value=**{ **0**| **1**| **2**| **3**} Specifies whether to modify the default IPSec traffic exemption (traffic that is not matched against IPSec filters but is still permitted). The default value is **3**, meaning that only IKE traffic is exempted from IPSec filtering. If you change the value for this setting, you must restart the computer for the new value to take effect. You can specify other values as follows:If **0** is specified, multicast, broadcast, RSVP, Kerberos, and IKE traffic is exempted from IPSec filtering. If **1** is specified, Kerberos and RSVP traffic is not exempted from IPSec filtering (multicast, broadcast, and IKE traffic is exempted).If **2** is specified, multicast and broadcast traffic is not exempted from IPSec filtering (RSVP, Kerberos, and IKE traffic is exempted).**ipsecloginterval value=**{ *Integer*} Specifies the interval, in seconds, after which IPSec event logs are sent to the System log. For *Integer*, valid values range from **60** through **86400**. The default value is **3600**. If you change the value for this setting, you must restart the computer for the new value to take effect.**ikelogging value=**{ **0**| **1**} Specifies whether to enable IKE (Oakley) logging, to generate details about the SA establishment process. The default value is **0**, meaning that IKE logging is disabled.**strongcrlcheck value=**{ **0**| **1**| **2**} Specifies the level of CRL checking to use. If **0** is specified, CRL checking is disabled. If **1** is specified, standard CRL checking is used, and certificate validation fails only if the certificate is determined to be revoked. If **2** is specified, strong CRL checking is used, and certificate validation fails if any CRL check error occurs. The default value is **1**.**bootmode value=**{ **stateful**| **block**| **permit**} Specifies the action that IPSec is required to take when the computer starts. If **stateful** is specified, only the following traffic is permitted during computer startup: outbound traffic initiated by the computer during startup, inbound traffic that is sent in response to the outbound traffic, and DHCP traffic. If **block** is specified, all inbound and outbound traffic is blocked until a local IPSec policy or a domain-based IPSec policy is applied. If **permit** is specified, all traffic is transmitted and received. The default value is **stateful**. If you use either stateful filtering or if you specify that traffic be blocked during computer startup, you can also use the **bootexemptions** parameter to specify traffic types that you want to exempt from IPSec filtering during computer startup. If you change the value for this setting, you must restart the computer for the new value to take effect.**bootexemptions value=***Exemption1Exemption2*Specifies one or more IPSec traffic exemptions from startup security, separated by spaces and defined by the following format for TCP and UDP traffic: *protocol*:*srcport*:*dstport*:*direction* and the following format for non-TCP/UDP traffic: *protocol*:*direction*, where:*protocol*={ **ICMP**| **TCP**| **UDP**| **RAW**| *Integer* } Specifies the IP protocol type to exempt from IPSec filtering during computer startup. *srcport*=*Port*Specifies the source port number of the packets to exempt from IPSec filtering during computer startup. A value of 0 means that any source port is exempted. *dstport*=*Port*Specifies the destination port number of the packets to exempt from IPSec filtering during computer startup. A value of 0 means that any destination port is exempted.*direction*={ **inbound** | **outbound**} Specifies the direction of the traffic to exempt from IPSec filtering during computer startup.

Remarks

- Use strong CRL checking (set **property=strongcrlcheck value=2**) if the CRL distribution point must be reachable on the network and certificates can only be validated if no CRL check error occurs.
- IPSec can only negotiate security associations for Kerberos traffic if your IPSec policy does not use Kerberos as the authentication method. If Kerberos is required for authentication, you must exempt Kerberos traffic by using the **ipsecexempt** parameter.
- In Windows 2000 and Windows XP, by default, all broadcast, multicast, Internet Key Exchange (IKE), Kerberos, and Resource Reservation Protocol (RSVP) traffic was exempted from IPSec filtering. In the Windows Server™ 2003 family, only IKE traffic is exempted from IPSec filtering by default. All other traffic types are now matched against IPSec filters, and you can configure block or permit filter actions specifically for multicast and broadcast traffic (IPSec does not negotiate security associations for multicast and broadcast traffic).

  As a result of this change in default behavior for IPSec, you should verify the behavior of IPSec policies designed for Windows 2000 or Windows XPand determine whether to configure explicit permit filters to permit specific traffic types. To restore the default behavior of Windows 2000 and Windows XPfor IPSec policies, edit the following registry key: **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\IPSec**. Add a new DWORD value named **NoDefaultExempt** and assign to it a value of **0**. For more information about adding values to registry keys, see Add a value to a registry key entry [http://technet2.microsoft.com/WindowsServer/en/library/c3cfc102-9341-4828-a7f8-14b0d4c192341033.mspx] .

Caution

- Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on the computer.
- Modifying IPSec traffic exemptions from startup security (that is, modifying the **bootexemptions=** parameter) will overwrite all previous exemptions from startup security.

⇡ Top of page

set mmpolicy

Modifies an IPSec main mode policy and writes the changes to the SPD.

Syntax

set mmpolicyname= [**qmperm=**][**mmlifetime=**][**softsaexpirationtime=**][**mmsecmethods=**]

Parameters

name=*String*

Required. Specifies the name of the IPSec main mode policy to modify.

[qmpermm=*Integer*]

Specifies the number of times that master keying material is used to derive the session key. A value of 0 means that an unlimited number of quick mode SAs can be derived from the main mode SA.

[mmlifetime=*Integer*]

Specifies the number of minutes after which a new master key is generated.

[softsaexpirationtime=*Integer*]

Specifies the number of minutes after which an unprotected security association expires.

[mmsecmethods="*SecMeth1SecMeth2*"]

Specifies one or more key exchange security methods, separated by spaces and defined by the format *ConfAlg-HashAlg-GroupNumb*, where:*ConfAlg*Specifies the encryption algorithm. *ConfAlg* can be **DES** or **3DES**.*HashAlg*Specifies the hash function. *HashAlg* can be **MD5** or **SHA1**.*GroupNum*Specifies the Diffie-Hellman group to be used for the base keying material. *GroupNumb* can be: **1** (low, protects with 768 bits of keying material), **2** (medium, protects with 1024 bits), and **3** (high, protects with 2048 bits).

Remarks

- IPSec peers must have at least one common key exchange security method (one that uses the same settings) or negotiations will fail.
- If the number of quick mode negotiations will exceed the value set for the number of quick mode negotiations per main mode negotiation during the main mode lifetime, a new main mode negotiation occurs.
-

- All string parameters are case-sensitive.

⇡ Top of page

set qmpolicy

Modifies an IPSec quick mode policy and writes the changes to the SPD.

Syntax

set qmpolicyname= [**soft=**][**pfsgroup=**][**qmsecmethods=**]

Parameters

name=*String*

Required. Specifies the name of the IPSec quick mode policy to modify.

[soft={ yes| no}]

Specifies whether to fall back to unsecured communications with other computers that do not support IPSec, or when IPSec negotiations with an IPSec-capable computer fail.

[pfsgroup={ grp1| grp2| grp3| grpmm| nopfs}]

Specifies the Diffie-Hellman group to use for session key PFS. If **grp1** is specified, Group 1 (low) is used. If **grp2** is specified, Group 2 (medium) is used. If **grp3** is specified, Group 2048 (high) is used. If **grpmm** is specified, the group value is taken from the current main mode settings. A value of **nopfs** means that session key PFS is disabled.

[qmsecmethods="*Neg1Neg2*"]

Specifies one or more security methods, separated by spaces and defined by the following format:{**ESP** [*ConfAlg*,*AuthAlg*]**:***k*/*s* | **AH** [*HashAlg*]**:***k*/*s* | **AH** [*HashAlg*+**ESP***ConfAlg*,*AuthAlg*]**:***k*/*s*}] Where:*ConfAlg*Specifies the encryption algorithm. *ConfigAlg* can be **DES** (Data Encryption Standard), **3DES**, or **none**. *AuthAlg*Specifies the integrity algorithm. *AuthAlg* can be **MD5** (Message Digest 5), **SHA1** (Secure Hash Algorithm 1), or **none**.*HashAlg*Specifies the hash function. *HashAlg* can be **MD5** or **SHA1**.*k*Specifies the session key lifetime in kilobytes. After the specified number of kilobytes of data is transferred, a new session key for the quick mode SA is generated. The default value is 100000 kilobytes.*s*Specifies the session key lifetime in seconds. The default value is 3600 seconds.

Remarks

- The preference order of each quick mode security method is determined by the order in which it was specified in the command.
- IPSec peers must have the same **pfsgroup** enabled (that is, both peers must use the same Diffie-Hellman group for session key PFS), or communication will fail.
- For enhanced security, do not use Diffie-Hellman Group 1. For maximum security, use Group 2048 whenever possible. Use Group 2 when required for interoperability with Windows 2000 and Windows XP.
- All string parameters are case-sensitive.

⇡ Top of page

set rule

Modifies an IPSec rule that defines a set of filters and writes the changes to the SPD.

Syntax

set rulesrcaddr=dstaddr=protocol=srcport=dstport=mirrored=conntype= [**srcmask=**][**dstmask=**][**tunneldstaddress=**][**mmpolicy=**][**qmpolicy=**][**actioninbound=**][**actionoutbound=**][**kerberos=**][**psk=**][**rootca=**]

Parameters

srcaddr={ Me| Any| *IPAddress*| *DNSName*| *ServerType*}

Required. Specifies the source IP address, DNS name, or server type for the IP traffic. You can use **WINS**, **DNS**, **DHCP**, or **gateway** for *ServerType*.

dstaddr={ Me| Any| *IPAddress*| *DNSName*| *ServerType*}

Required. Specifies the destination IP address, DNS name, or server type for the IP traffic. You can use **WINS**, **DNS**, **DHCP**, or **gateway** for *ServerType*.

protocol={ ANY| ICMP| TCP| UDP| RAW| *Integer* }

Required. Specifies the IP protocol used for the filter.

srcport=*Port*

Required. Specifies the source port number of the packets being filtered. This option only applies if you are filtering TCP or UDP packets. A value of **0** matches filters set to a source port of **0** or **any**.

dstport=*Port*

Required. Specifies the destination port number of the packets being filtered. This option only applies if you are filtering TCP or UDP packets. A value of **0** matches filters set to a destination port of **0** or **any**.

mirrored={ yes| no}

Required. Specifies whether the rule was created with mirrored filters.

conntype={ lan| dialup| all}

Required. Specifies whether the rule applies only to remote access or dial-up connections or to local area network (LAN) connections, or to all connections.

[srcmask={ *Mask*| *Prefix*}]

Specifies the source address subnet mask or the prefix of the packets being filtered. You can specify a prefix value in the range of 1 through 32. The default value is the mask of 255.255.255.255.

[dstmask={ *Mask*| *Prefix*}]

Specifies the destination address subnet mask or the prefix value of the packets being filtered. You can specify a prefix value in the range of 1 through 32. The default value is the mask of 255.255.255.255.

[tunneldstaddress={ *IPAddress*| *DNSName*}]

Specifies whether the traffic is tunneled and, if it is, the IP address or DNS name of the tunnel destination (the computer or gateway on the other side of the tunnel).

[mmpolicy=*String*]

Specifies the name of the main mode policy.

[qmpolicy=*String*]

Specifies the name of the quick mode policy.

[actioninbound={ permit| block| negotiate}]

Specifies the action that IPSec is required to take for inbound traffic. If **permit** is specified, traffic is received without negotiating or applying IP security. If **block** is specified, traffic is blocked. If **negotiate** is specified, IP security is used, with the list of security methods specified in the main mode and quick mode policies.

[actionoutbound={ permit| block| negotiate}]

Specifies the action that IPSec is required to take for outbound traffic. If **permit** is specified, traffic is sent without negotiating or applying IP security. If **block** is specified, traffic is blocked. If **negotiate** is specified, IP security is used, with the list of security methods specified in the main mode and quick mode policies.

[kerberos={ yes | no}]

Specifies whether to use the Kerberos V5 protocol as an authentication method.

[psk=*String*]

Specifies the string of characters to use for the preshared key, if a preshared key is used as an authentication method.

[rootca="*String*certmap:{ yes| no} excludecaname:{ yes| no} "]

Specifies certificate authentication options, where: *String* Specifies the distinguished name of the certificate, if a certificate is used as an authentication method.**certmap:**{ **yes**| **no**} Specifies whether to enable certificate-to-account mapping. You can enable certificate-to-account mapping to verify that the certificate is being used by a trusted computer.**excludecaname:**{ **yes**| **no**} Specifies whether to exclude from the certificate request the list of trusted root CA names from which a certificate is accepted.

Remarks

- You can modify the following parameters: **mmpolicy=**, **qmpolicy=**, **actioninbound=**, and **actionoutbound=**. All other parameters are used to identify the rule that you want to modify, and therefore they cannot be modified.
- If the filter action for both inbound and outbound traffic (**actioninbound** and **actionoutbound**) are set to **Permit** or **Block**, a quick mode filter is not required.
- If a tunnel rule is specified, **mirror** should be set to **no** (by default, **mirror** is set to **yes**). For IPSec tunnels, you must create two rules: one rule describes the traffic to be sent through the tunnel (outbound traffic) and the other describes the traffic to be received through the tunnel (inbound). Next, create two rules that use the inbound and outbound filter lists in your policy.

- To filter any packets sent from or to the computer, you can use **srcaddr=Me** or **dstaddr=Me**.
- To filter packets sent from or to any computer, you can use **srcaddr=Any** or **dstaddr=Any**.
- You can only use Kerberos V5 authentication or certificate-to-account mapping for computers that are members of an Active Directory domain.
- Although you can use only one preshared key for authentication, you can use multiple certificates by specifying the **rootca** parameter once, for each certificate you want to use.
- All certificate authentication parameters must be contained within quotation marks. Embedded quotation marks must be replaced by a backslash followed by an apostrophe (\').
- All string parameters are case-sensitive.
- The preference order of each authentication method is determined by the order in which it was specified in the command.
- If no authentication methods are specified, dynamic defaults are used. By default, IPSec policies use Kerberos V5 authentication. If the computer has a computer certificate, any root CA to which the computer certificate chains is also used for authentication.
- If **excludecaname:yes** is specified, the list of trusted root CAs is not sent as part of the certificate request, which prevents the potential disclosure of sensitive information about the trust relationships of a computer. To enhance security for computers connected to the Internet, specify this option.
- The use of preshared key authentication is not recommended because it is a relatively weak authentication method. In addition, preshared keys are stored in plaintext.
- IPSec peers must have at least one common authentication method or communication will fail.
- Modifying authentication methods will overwrite all previous authentication methods, even if the previous authentication methods were different. For example, if **kerberos=yes** and **psk=yes** were previously specified, and then you specify **kerberos=no**, the **psk=yes** parameter will also be overwritten, and preshared key authentication will no longer be used.

⇡ Top of page

show all

Displays configuration information for all IPSec policies, filters, statistics, and security associations in the SPD.

Syntax

show all [**resolvedns=**]

Parameters

[resolvedns={ yes | no}]

Specifies whether to resolve the Domain Name System (DNS) or NETBIOS computer name associated with an IP address when displaying sources or destinations.

Remarks

- Because the **show all** command can result in lengthy, rapidly scrolling output, consider saving the output in a text file, unless you only need to view limited portions.

  To save output in a text file for the **show all** command, do either of the following:

  If you are in the netsh environment (netsh>)

  1. At the netsh prompt, type:

     set file open *FileName*.txt

  2. Then type:

     ipsec dynamic show all

  3. To stop sending output and close the file, type:

     set file close

If you are not in the netsh environment

- At the command prompt, type:

  netsh ipsec dynamic show all >*FileName*.txt

- To stop the output of IPSec configuration information, you must exit **Netsh** by doing one of the following:
  - Close the **Netsh** window by clicking the **X** icon in the upper-right corner of the window.
  - Use Task Manager to end the **Netsh** program.

⇡ Top of page

show config

Displays values for the following IPSec settings: IPSec diagnostics, default traffic exemptions, strong certificate revocation list (CRL) checking, IKE (Oakley) logging, logging intervals, computer startup security, and computer startup traffic exemptions.

Syntax

show config

Parameters

None.

Remarks

- To save output in a text file for the **show config** command, do either of the following:

  If you are in the netsh environment (netsh>)

  1. At the netsh prompt, type:

     set file open *FileName*.txt

  2. Then type:

     ipsec dynamic show config

  3. To stop sending output and close the file, type:

     set file close

  If you are not in the netsh environment

  - At the command prompt, type:

    netsh ipsec dynamic show config >*FileName*.txt

⇡ Top of page

show mmfilter

Displays configuration information for the specified IPSec main mode filter, or for all IPSec main mode filters, in the SPD.

Syntax

show mmfiltername= | **all** [**type=**] **srcaddr=dstadd=** [**srcmask=**][**dstmask=**] [**resolvedns=**]

Parameters

name=*String*| all

Required. Specifies the name of the IPSec main mode filter to display. Or, if **all** is specified, all IPSec main mode filters are displayed.

type={ generic| specific}

Specifies whether to display generic or specific main mode filters. The default value is **generic**.

[srcaddr={ Me| Any| *IPAddress*| *DNSName*| *ServerType* }]

Specifies the source IP address, DNS name, or server type for the IP traffic being filtered. You can use **WINS**, **DNS**, **DHCP**, or **gateway** for *ServerType*.

[dstaddr={ Me| Any| *IPAddress*| *DNSName*| *ServerType* }]

Specifies the destination IP address, DNS name, or server type for the IP traffic being filtered. You can use **WINS**, **DNS**, **DHCP**, or **gateway** for *ServerType*.

[srcmask={ *Mask*| *Prefix* }]

Specifies the source address subnet mask or the prefix of the packets being filtered. You can specify a prefix value in the range of 1 through 32. The default value is the mask of 255.255.255.255.

[dstmask={ *Mask*| *Prefix* }]

Specifies the destination address subnet mask or the prefix value of the packets being filtered. You can specify a prefix value in the range of 1 through 32. The default value is the mask of 255.255.255.255.

[resolvedns={ yes | no }]

Specifies whether to resolve the Domain Name System (DNS) or NETBIOS computer name associated with an IP address when displaying sources or destinations. The default value is **no**.

Remarks

- All string parameters are case-sensitive.
- Because the **show mmfilter** command can result in lengthy, rapidly scrolling output, consider saving the output in a text file, unless you only need to view limited portions.

  To save output in a text file for the **show mmfilter** command, do either of the following:

  If you are in the netsh environment (netsh>)

  1. At the netsh prompt, type:

     set file open *FileName*.txt

  2. Then type:

     ipsec dynamic show mmfilter*Name* | **all**

  3. To stop sending output and close the file, type:

     set file close

  If you are not in the netsh environment

  - At the command prompt, type:

    ipsec dynamic show mmfilter*Name* | **all >=***FileName*.txt

- To stop the output of IPSec configuration information, you must exit **Netsh** by doing one of the following:
  - Close the **Netsh** window by clicking the **X** icon in the upper-right corner of the window.
  - Use Task Manager to end the **Netsh** program.

Top of page

show mmpolicy

Displays configuration information for the specified IPSec main mode policy, or for all IPSec main mode policies, in the SPD.

Syntax

show mmpolicyname= | **all**

Parameters

name=*String*| all

Required. Specifies the name of the IPSec main mode policy to display. Or, if **all** is specified, all IPSec main mode policies are displayed.

Remarks

- All string parameters are case-sensitive.
- Because the **show mmpolicy** command can result in lengthy, rapidly scrolling output, consider saving the output in a text file, unless you only need to view limited portions.

  To save output in a text file for the **show mmpolicy** command, do either of the following:

  If you are in the netsh environment (netsh>)

  1. At the netsh prompt, type:

     set file open *FileName*.txt
  2. Then type:

     ipsec dynamic show mmpolicy*Name* | **all**
  3. To stop sending output and close the file, type:

     set file close

  If you are not in the netsh environment

  - At the command prompt, type:

    ipsec dynamic show mmpolicy*Name* | **all >***FileName*.txt
- To stop the output of IPSec configuration information, you must exit **Netsh** by doing one of the following:
  - Close the **Netsh** window by clicking the **X** icon in the upper-right corner of the window.
  - Use Task Manager to end the **Netsh** program.

Top of page

show mmsas

Displays the IPSec main mode security associations for the specified source and destination addresses, or all IPSec main mode security associations, in the SPD.

Syntax

show mmsas [**all**] [**srcaddr=**][**dstaddr=**][**format=**] [**resolvedns=**]

Parameters

[all]

Specifies that all main mode security associations are displayed.

[srcaddr={ Me| Any| *IPAddress*| *DNSName*| *ServerType*}]

Specifies the source IP address, DNS name, or server type for the IP traffic being filtered. You can use **WINS**, **DNS**, **DHCP**, or **gateway** for *ServerType*.

[dstaddr={ Me| Any| *IPAddress*| *DNSName*| *ServerType*}]

Specifies the destination IP address, DNS name, or server type for the IP traffic being filtered. You can use **WINS**, **DNS**, **DHCP**, or **gateway** for *ServerType*.

[format={ list| table}]

Specifies whether to display IPSec configuration information in screen or tab-delimited format. The default value is **list**, meaning that output is displayed in screen format.

[resolvedns={ yes | no}]

Specifies whether to resolve the Domain Name System (DNS) or NETBIOS computer name associated with an IP address when displaying sources or destinations. The default value is **no**.

Remarks

- If no parameters are specified, all main mode security associations are displayed.
- All string parameters are case-sensitive.
- Because the **show mmsas** command can result in lengthy, rapidly scrolling output, consider saving the output in a

text file, unless you only need to view limited portions.

To save output in a text file for the **show mmsas** command, do either of the following:

If you are in the netsh environment (netsh>)

1. At the netsh prompt, type:

   set file open *FileName*.txt

2. Then type:

   ipsec dynamic show mmsas

3. To stop sending output and close the file, type:

   set file close

If you are not in the netsh environment

- At the command prompt, type:

  netsh ipsec dynamic show mmsas >*FileName*.txt

- To stop the output of IPSec configuration information, you must exit **Netsh** by doing one of the following:
  - Close the **Netsh** window by clicking the **X** icon in the upper-right corner of the window.
  - Use Task Manager to end the **Netsh** program.

⇡ Top of page

show qmfilter

Displays configuration information for the specified quick mode filter, or for all quick mode filters, in the SPD.

Syntax

show qmfiltername= | **all** [**type=**] [**srcaddr=**][**dstaddr=**][**srcmask=**][**dstmask=**][**protocol=**][**srcport=**][**dstport=**][**actioninbound=**][**actionoutbound=**][**resolvedns=**]

Parameters

name=*String*| all

Required. Specifies the name of the IPSec quick mode filter to display, or, if **all** is specified, that all IPSec quick mode filters are displayed.

[type={ generic| specific}]

Specifies whether to display generic or specific quick mode filters. The default value is **generic**.

[srcaddr={ Me| Any| *IPAddress*| *DNSName*| *ServerType*}]

Specifies the source IP address, DNS name, or server type for the IP traffic being filtered. You can use **WINS**, **DNS**, **DHCP**, or **gateway** for *ServerType*.

[dstaddr={ Me| Any| *IPAddress*| *DNSName*| *ServerType*}]

Specifies the destination IP address, DNS name, or server type for the IP traffic being filtered. You can use **WINS**, **DNS**, **DHCP**, or **gateway** for *ServerType*.

[srcmask={ *Mask*| *Prefix*}]

Specifies the source address subnet mask or the prefix of the packets being filtered. You can specify a prefix value in the range of 1 through 32. The default value is the mask of 255.255.255.255.

[dstmask={ *Mask*| *Prefix*}]

Specifies the destination address subnet mask or the prefix value of the packets being filtered. You can specify a prefix value in the range of 1 through 32. The default value is the mask of 255.255.255.255.

[protocol={ ANY| ICMP| TCP| UDP| RAW| *Integer* }]

Specifies the IP protocol if, in addition to addressing information, a specific IP protocol is filtered. The default value is **ANY**, meaning all protocols are used for the filter.

[srcport=*Port*]

Specifies the source port number of the packets being filtered. This option only applies if you are filtering TCP or UDP packets. If 0 is specified, packets sent from any port are filtered. The default is any.

[dstport=*Port*]

Specifies the destination port number of the packets being filtered. This option only applies if you are filtering TCP or UDP packets. If 0 is specified, packets sent to any port are filtered. The default is any.

[actioninbound={ permit| block| negotiate}]

Specifies the action that IPSec is required to take for inbound traffic. The default value is **negotiate**.

[actionoutbound={ permit| block| negotiate}]

Specifies the action that IPSec is required to take for outbound traffic. The default value is **negotiate**

[resolvedns={ yes | no}]

Specifies whether to resolve the Domain Name System (DNS) or NETBIOS computer name associated with an IP address when displaying sources or destinations. The default value is **no**.

Remarks

- All string parameters are case-sensitive.
- Because the **show qmfilter** command can result in lengthy, rapidly scrolling output, consider saving the output in a text file, unless you only need to view limited portions.

  To save output in a text file for the **show qmfilter** command, do either of the following:

  If you are in the netsh environment (netsh>)

  1. At the netsh prompt, type:

     set file open *FileName*.txt

  2. Then type:

     ipsec dynamic show qmfilter *Name* | **all**

  3. To stop sending output and close the file, type:

     set file close

  If you are not in the netsh environment

  - At the command prompt, type:

    netsh ipsec dynamic show qmfilter *Name* | **all** >*FileName*.txt

- To stop the output of IPSec configuration information, you must exit **Netsh** by doing one of the following:
  - Close the **Netsh** window by clicking the **X** icon in the upper-right corner of the window.
  - Use Task Manager to end the **Netsh** program.

Top of page

show qmpolicy

Displays configuration information for the specified IPSec quick mode policy, or for all IPSec quick mode policies, in the SPD.

Syntax

show qmpolicyname= | **all**

Parameters

name=*String*| all

Required. Specifies the name of the IPSec quick mode policy to display. Or, if **all** is specified, all IPSec quick mode policies are displayed.

Remarks

- All string parameters are case-sensitive.
- Because the **show qmpolicy** command can result in lengthy, rapidly scrolling output, consider saving the output in a

text file, unless you only need to view limited portions.

To save output in a text file for the **show qmpolicy** command, do either of the following:

If you are in the netsh environment (netsh>)

1. At the netsh prompt, type:

   set file open *FileName*.txt

2. Then type:

   ipsec dynamic show qmpolicy*Name* | **all**

3. To stop sending output and close the file, type:

   set file close

If you are not in the netsh environment

- At the command prompt, type:

  netsh ipsec dynamic show qmpolicy*Name* | **all** >*FileName*.txt

- To stop the output of IPSec configuration information, you must exit **Netsh** by doing one of the following:
  - Close the **Netsh** window by clicking the **X** icon in the upper-right corner of the window.
  - Use Task Manager to end the **Netsh** program.

⇡ Top of page

show qmsas

Displays the IPSec quick mode security associations for the specified source and destination addresses, or all IPSec quick mode security associations, in the SPD.

Syntax

show qmsas [**all**][**srcaddr=**][**dstaddr=**][**protocol=**][**format=**][**resolvedns=**]

Parameters

[all]

Specifies that all IPSec quick mode security associations are displayed.

[srcaddr={ Me| Any| *IPAddress*| *DNSName*| *ServerType* }]

Specifies the source IP address, DNS name, or server type for the IP traffic being filtered. You can use **WINS**, **DNS**, **DHCP**, or **gateway** for *ServerType*.

[dstaddr={ Me| Any| *IPAddress*| *DNSName*| *ServerType*]

Specifies the destination IP address, DNS name, or server type for the IP traffic being filtered. You can use **WINS**, **DNS**, **DHCP**, or **gateway** for *ServerType*.

[protocol={ ANY| ICMP| TCP| UDP| RAW| *Integer* }]

Specifies the IP protocol if, in addition to addressing information, a specific IP protocol is being used for the security association. The default value is **ANY**, meaning all protocols are used for the security association.

[format={ list| table}]

Specifies whether to display IPSec configuration information in screen or tab-delimited format. The default value is **list**, meaning that output is displayed in screen format.

[resolvedns={ yes | no}]

Specifies whether to resolve the Domain Name System (DNS) or NETBIOS computer name associated with an IP address when displaying sources or destinations. The default value is **no**.

Remarks

- Because the **show qmsas** command can result in lengthy, rapidly scrolling output, consider saving the output in a text file, unless you only need to view limited portions.

  To save output in a text file for the **show qmsas** command, do either of the following:

If you are in the netsh environment (netsh>)

1. At the netsh prompt, type:

   set file open *FileName*.txt

2. Then type:

   ipsec dynamic show qmsas all

3. To stop sending output and close the file, type:

   set file close

If you are not in the netsh environment

- At the command prompt, type:

  netsh ipsec dynamic show qmsas all >*FileName*.txt

- To stop the output of IPSec configuration information, you must exit **Netsh** by doing one of the following:
  - Close the **Netsh** window by clicking the **X** icon in the upper-right corner of the window.
  - Use Task Manager to end the **Netsh** program.

⇡ Top of page

show rule

Displays configuration information for one or more IPSec rules in the SPD.

Syntax

show rule [**type=**][**srcaddr=**] [**dstaddr=**][**srcmask=**][**dstmask=**] [**protocol=**][**srcport=**][**dstport=**] [**actioninbound=**][**actionoutbound=**][**resolvedns=**]

Parameters

[type={ transport| tunnel}]

Specifies whether to display a transport rule or a tunnel rule. The default value is to display all rules.

[srcaddr={ Me| Any| *IPAddress*| *DNSName*| *ServerType*}]

Specifies the source IP address, DNS name, or server type for the IP traffic being filtered. You can use **WINS**, **DNS**, **DHCP**, or **gateway** for *ServerType*.

[dstaddr={ Me| Any| *IPAddress*| *DNSName*| *ServerType*}]

Specifies the destination IP address, DNS name, or server type for the IP traffic being filtered. You can use **WINS**, **DNS**, **DHCP**, or **gateway** for *ServerType*.

[srcmask={ *Mask*| *Prefix*}]

Specifies the source address subnet mask or the prefix of the packets being filtered. You can specify a prefix value in the range of 1 through 32. The default value is the mask of 255.255.255.255.

[dstmask={ *Mask*| *Prefix*}]

Specifies the destination address subnet mask or the prefix value of the packets being filtered. You can specify a prefix value in the range of 1 through 32. The default value is the mask of 255.255.255.255.

[protocol={ ANY| ICMP| TCP| UDP| RAW| *Integer* }]

Specifies the IP protocol if, in addition to addressing information, a specific IP protocol is used for the rule. The default value is **ANY**, meaning all protocols are used for the rule.

[srcport=*Port*]

Specifies the source port number of the packets being filtered. This option only applies if you are filtering TCP or UDP packets. If 0 is specified, packets sent from any port are filtered. The default is any.

[dstport=*Port*]

Specifies the destination port number of the packets being filtered. This option only applies if you are filtering TCP or UDP packets. If 0 is specified, packets sent to any port are filtered. The default is any.

[actioninbound={ permit| block| negotiate}]

Specifies the action that IPSec is required to take for inbound traffic. The default value is **negotiate**.

[actionoutbound={ permit| block| negotiate}]

Specifies the action that IPSec is required to take for outbound traffic. The default value is **negotiate**.

[resolvedns={ yes | no}]

Specifies whether to resolve the Domain Name System (DNS) or NETBIOS computer name associated with an IP address when displaying sources or destinations. The default value is **no**.

Remarks

- All string parameters are case-sensitive.
- Because the **show rule** command can result in lengthy, rapidly scrolling output, consider saving the output in a text file, unless you only need to view limited portions.

  To save output in a text file for the **show rule** command, do either of the following:

  If you are in the netsh environment (netsh>)

  1. At the netsh prompt, type:

     set file open *FileName*.txt

  2. Then type:

     ipsec dynamic show rule

  3. To stop sending output and close the file, type:

     set file close

  If you are not in the netsh environment

  - At the command prompt, type:

    netsh ipsec dynamic show rule >*FileName*.txt

- To stop the output of IPSec configuration information, you must exit **Netsh** by doing one of the following:
  - Close the **Netsh** window by clicking the **X** icon in the upper-right corner of the window.
  - Use Task Manager to end the **Netsh** program.

⇡ Top of page

show stats

Displays main mode and quick mode statistics for IPSec.

Syntax

show stats [**type=**]

Parameters

[type=all| ike| ipsec]

Specifies the IPSec statistics to display. If **all** is specified, IPSec main mode and quick mode statistics are displayed. If **ike** is specified, only IPSec main mode statistics are displayed. If **ipsec** is specified, only IPSec quick mode statistics are displayed.

Remarks

- Because the **show stats** command can result in lengthy, rapidly scrolling output, consider saving the output in a text file, unless you only need to view limited portions.

  To save output in a text file for the **show stats** command, do either of the following:

  If you are in the netsh environment (netsh>)

  1. At the netsh prompt, type:

     set file open *FileName*.txt

2. Then type:

   ipsec dynamic show stats

3. To stop sending output and close the file, type:

   set file close

If you are not in the netsh environment

- At the command prompt, type:

  netsh ipsec dynamic show stats >*FileName*.txt

- To stop the output of IPSec configuration information, you must exit **Netsh** by doing one of the following:
  - Close the **Netsh** window by clicking the **X** icon in the upper-right corner of the window.
  - Use Task Manager to end the **Netsh** program.

⇡ Top of page

Formatting legend

Format	**Meaning**
Italic	Information that the user must supply
Bold	Elements that the user must type exactly as shown
Ellipsis (...)	Parameter that can be repeated several times in a command line
Between brackets ([])	Optional items
Between braces ({}); choices separated by pipe (|). Example: {even|odd}	Set of choices from which the user must choose only one
`Courier font`	Code or program output