# security ipsec commands

## ONTAP commands

NetApp
February 03, 2026

This PDF was generated from https://docs.netapp.com/us-en/ontap-cli-98/security-ipsec-show-ikesa.html on February 03, 2026. Always check docs.netapp.com for the latest.

# Table of Contents


security ipsec commands . . . 1
- security ipsec show-ikesa . . . 1
  - Description . . . 1
  - Parameters . . . 1
  - Examples . . . 2
- security ipsec show-ipsecsa . . . 4
  - Description . . . 4
  - Parameters . . . 4
  - Examples . . . 6
- security ipsec config modify . . . 7
  - Description . . . 7
  - Parameters . . . 8
  - Examples . . . 8
- security ipsec config show . . . 8
  - Description . . . 8
  - Examples . . . 8
- security ipsec policy create . . . 9
  - Description . . . 9
  - Parameters . . . 9
  - Examples . . . 10
- security ipsec policy delete . . . 11
  - Description . . . 11
  - Parameters . . . 11
  - Examples . . . 11
- security ipsec policy modify . . . 12
  - Description . . . 12
  - Parameters . . . 12
  - Examples . . . 13
- security ipsec policy show . . . 14
  - Description . . . 14
  - Parameters . . . 14
  - Examples . . . 15

# security ipsec commands

## security ipsec show-ikesa

Show IKE SA Information

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `security ipsec show-ikesa` command displays information about IKE Security Associations (SA).

Running this command with the `-node` parameter displays information relevant to IKE SAs generated at the specified node.

Running this command with the `-vserver` parameter displays information relevant to IKE SAs associated with the specified vserver.

Running this command with the `-policy-name` parameter displays information relevant to IKE SAs created based on the specified security policy.

You can specify additional parameters to display only information matching those parameters. For example, to display IKE SAs associated with a specific local address, run the command with the `-local-address` parameter.

### Parameters

**{ [-fields <fieldname>,…]**

If you specify the `-fields <fieldname>,…` parameter, the command displays only the specified fields. Notice that key fields are always displayed.

**| [-instance ] }**

If you specify the `-instance` parameter, the command displays all fields of the IKE SAs.

**-node <nodename> - Node**

This required parameter specifies the node from which the IKE SA information will be collected and displayed.

**[-vserver <vserver name>] - Vserver Name**

Use this parameter to display the IKE SAs associated with the specified Vserver.

**[-policy-name <text>] - Policy Name**

Use this parameter to display the IKE SAs created based on the specified security policy.

**[-local-address <text>] - Local Address**

Use this parameter to display the IKE SAs with the specified local endpoint IP address.

**[-remote-address <text>] - Remote Address**

Use this parameter to display the IKE SAs with the specified remote endpoint IP address.

**[-initiator-spi <text>] - Initiator SPI**

Use this parameter to display the IKE SAs with the specified initiator Security Parameter Index (SPI).

**[-responder-spi <text>] - Responder SPI**

Use this parameter to display the IKE SAs with the specified responder SPI.

**[-is-initiator {true|false}] - Is Initiator**

Use this parameter to display the IKE SAs created when the given node matches the specified initiator role: true means initiator role and false means responder role in IKE negotiation.

**[-ike-version <integer>] - IKE Version**

Use this parameter to display the IKE SAs created using the specified IKE version.

**[-auth-method <IKE Authentication Method>] - Authentication Method**

Use this parameter to display the IKE SAs created using the specified authentication method.

**[-state <IKE SA State>] - IKE SA State**

Use this parameter to display only the IKE SAs that are in the specified state.

**[-cipher-suite <Cipher Suite Type>] - Cipher Suite**

Use this parameter to display the IKE SAs created using the specified cipher suite.

**[-lifetime <integer>] - Lifetime**

Use this parameter to display the IKE SAs with the specified remaining lifetime. Notice that lifetime keeps changing for the duration of the security association.

## Examples

This example displays all IKE SAs for node *cluster1-node1* :

```
cluster-1::> security ipsec show-ikesa -node cluster1-node1
             Policy Local           Remote
Vserver      Name   Address         Address         Initator-SPI     State
------------ ------ --------------- --------------- ----------------
------------
vs1          Policy1
                    192.186.10.1    192.186.10.2    e658e5bc7ece199e
ESTABLISHED
vs2          Policy2
                    192.168.20.1    192.168.20.2    8eac392028ab4f12
ESTABLISHED
2 entries were displayed.
```

This example displays selected fields of all IKE SAs for node *cluster1-node1* :

```
cluster-1::> security ipsec show-ikesa -node cluster1-node1 -fields is-
initiator,initiator-spi,responder-spi,auth-method,cipher-suite,lifetime

node           vserver policy-name local-address remote-address initiator-
spi    responder-spi    is-initiator auth-method cipher-suite  lifetime
-------------- ------- ----------- ------------- --------------
---------------- ---------------- ------------ ----------- -------------
--------
cluster1-node1 vs1     Policy1     192.186.10.1  192.186.10.2
e658e5bc7ece199e 9b61befff71e8ca2 false        PSK         SUITEB_GCM256
6300
cluster1-node1 vs2     Policy2     192.186.20.1  192.186.20.2
4d43aaba8ca01cd8 00bdd5aac569e08a true         PSK         SUITEB_GCM256
6720
2 entries were displayed.
```

This example displays all IKE SAs for vserver *vs1* :

```
cluster-1::> security ipsec show-ikesa -node cluster1-node1
            Policy Local           Remote
Vserver     Name   Address         Address         Initator-SPI     State
----------- ------ --------------- --------------- ----------------
-----------
vs1         Policy1
                   192.186.10.1    192.186.10.2    e658e5bc7ece199e
ESTABLISHED
```

This example displays instance view (all fields) for all IKE SAs associated with node *cluster1-node1* , vserver *vs1* and created using policy *Policy1* :

```
cluster-1::> security ipsec show-ikesa -node cluster1-node1 -vserver vs1
-policy-name Policy1 -instance
Node: cluster1-node1
         Vserver Name: vs1
          Policy Name: Policy1
        Local Address: 192.168.10.1
       Remote Address: 192.168.10.2
        Initiator SPI: e658e5bc7ece199e
        Responder SPI: 9b61befff71e8ca2
         Is Initiator: false
          IKE Version: 2
Authentication Method: PSK
         IKE SA State: ESTABLISHED
         Cipher Suite: SUITEB_GCM256
             Lifetime: 6000
```

# security ipsec show-ipsecsa

Show IPsec SA Information

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `security ipsec show-ipsecsa` command displays information about IPsec Security Associations (SA).

Running the command with the `-node` parameter displays information relevant to IPsec SAs at the specified node.

Running this command with the `-vserver` parameter displays information relevant to IPsec SAs associated with the specified vserver.

Running this command with the `-policy-name` parameter displays information relevant to IPsec SAs created using the specified security policy.

You can specify additional parameters to display only information matching those parameters. For example, to display IPsec SAs only about a certain local address, run the command with the `-local-address` parameter.

## Parameters

**{ [-fields <fieldname>,…]**

If you specify the `-fields <fieldname>,…` parameter, the command displays only the specified fields. Notice that key fields are always displayed.

**| [-instance ] }**

If you specify the `-instance` parameter, the command displays all fields of matching IPsec SAs.

**-node <nodename> - Node**

This required parameter specifies from which node the IPsec SA information will be collected and displayed.

**[-vserver <vserver name>] - Vserver Name**

Use this parameter to display the IPsec SAs associated with the specified Vserver.

**[-policy-name <text>] - Policy Name**

Use this parameter to display the IPsec SAs created based on the specified security policy.

**[-local-address <text>] - Local Address**

Use this parameter to display the IPsec SAs with the specified local endpoint IP address.

**[-remote-address <text>] - Remote Address**

Use this parameter to display the IPsec SAs with the specified remote endpoint IP address.

**[-inbound-spi <text>] - Inbound SPI**

Use this parameter to display the IPsec SA having the specified inbound Security Parameter Index (SPI).

**[-outbound-spi <text>] - Outbound SPI**

Use this parameter to display the IPsec SA having the specified outbound SPI.

**[-action <IPsec Action Type>] - IPsec Action**

Use this parameter to display IPsec SAs with the specified security action type, such as ESP_TRA for ESP transport mode protection or BYPASS to bypass IPsec, or DISCARD.

**[-state <text>] - IPsec SA State**

Use the parameter to display only the IPsec SAs that are in the specified state.

**[-cipher-suite <Cipher Suite Type>] - Cipher Suite**

Use this parameter to display the IPsec SAs that use the specified cipher-suite.

**[-ib-bytes <integer>] - Inbound Bytes Processed**

Use this parameter to display the IPsec SAs matching the processed inbound bytes. Notice that ib-bytes keeps changing as inbound packets are processed.

**[-ib-pkts <integer>] - Inbound Pkts Processed**

Use this parameter to display the IPsec SAs matching the processed inbound packets. Notice that ib-pkts keeps changing as inbound packets are processed.

**[-ob-bytes <integer>] - Outbound Bytes Processed**

Use this parameter to display the IPsec SAs matching the processed outbound bytes. Notice that ob-bytes keeps changing as outbound packets are processed.

**[-ob-pkts <integer>] - Outbound Pkts Processed**

Use this parameter to display the IPsec SAs matching the processed outbound packets. Notice that ob-pkts keeps changing as outbound packets are processed.

**[-lifetime <integer>] - IPsec SA Lifetime Seconds**

Use this parameter to display the IPsec SAs matching the remaining lifetime. Notice that lifetime keeps changing for the duration of the security association.

## Examples

The this example displays all IPsec SAs for node *cluster1-node1* :

```
cluster-1::> security ipsec show-ipsecsa -node cluster1-node1
             Policy  Local           Remote          Inbound  Outbound
Vserver      Name    Address         Address         SPI      SPI
State
------------ ------- --------------- --------------- -------- --------
---------
vs1          Policy1
                     192.186.10.1    192.186.10.2    c68de9db c84f913b
INSTALLED
vs2          Policy2
                     192.186.20.1    192.186.20.2    cbc01493 c6ee7424
INSTALLED
2 entries were displayed.
```

This example displays selected fields of all IPsec SAs for node *cluster1-node1* :

```
cluster-1::> security ipsec show-ipsecsa -node cluster1-node1 -fields
local-address,remote-address,inbound-spi,outbound-spi
node           vserver policy-name local-address  remote-address inbound-
spi outbound-spi
-------------- ------- ----------- -------------- --------------
----------- ------------
cluster1-node1 vs1     Policy1     192.186.10.1   192.186.10.2   c68de9db
c84f913b
cluster1-node1 vs2     Policy2     192.186.20.1   192.186.20.2   cbc01493
c6ee7424
2 entries were displayed.
```

```
This example displays selected fields of all IPsec SAs associated with
node ``_cluster1-node1_``:
cluster-1::> security ipsec show-ipsecsa -node cluster1-node1 -fields ib-
bytes,ib-pkts,ob-bytes,ob-pkts
node           vserver policy-name local-address  remote-address inbound-
spi ib-bytes ib-pkts ob-bytes ob-pkts
-------------- ------- ----------- -------------- --------------
----------- -------- ------- -------- -------
cluster1-node1 vs1     Policy1     192.186.10.1   192.186.10.2   c68de9db
4704     56      6720     56
cluster1-node1 vs2     Policy2     192.186.20.1   192.186.20.2   cbc01493
20434    115     23082    120
2 entries were displayed.
```

This example displays instance view (all fields) for all IPsec SAs associated with node *cluster1-node1* , vserver *vs1* and created using policy *Policy1* :

```
cluster-1::> security ipsec show-ipsecsa -node cluster1-node1 -vserver vs1
-policy-name Policy1 -instance
Node: cluster1-node1
             Vserver Name: vs1
              Policy Name: Policy1
              Inbound SPI: c68de9db
             Outbound SPI: c84f913b
            Local Address: 192.168.10.1
           Remote Address: 192.168.10.2
             IPsec Action: ESP_TRA
           IPsec SA State: INSTALLED
             Cipher Suite: SUITEB_GCM256
  Inbound Bytes Processed: 4704
   Inbound Pkts Processed: 56
 Outbound Bytes Processed: 6720
  Outbound Pkts Processed: 56
IPsec SA Lifetime Seconds: 1800
```

# security ipsec config modify

## Modify IPsec config

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

### Description

This command modifies IPsec configuration parameters.

### Parameters

**[-is-enabled {true|false}] - Is IPsec Enabled**

This parameter enables and disables IPsec on the storage system.

**[-log-level <IPsec Log Level>] - IPsec Logging Level**

This parameter sets the IPsec logging level, where logging level 0 means no logging, and logging level 5 is most verbose. Default value is 2.

**[-replay-window <IPsec Replay Window Size>] - IPsec Replay Window Size**

This parameter sets the IPsec replay window size. The possible values are 0, 64, 128, 256, 512 and 1024. Default value is 0.

### Examples

The following example enables IPsec:

```
cluster-1::> security ipsec config modify -is-enabled true
```

The following example sets the IPsec logging level to 4:

```
cluster-1::> security ipsec config modify -log-level 4
```

The following example sets the IPsec replay window size to 64:

```
cluster-1::> security ipsec config modify -replay-window 64
```

# security ipsec config show

Display IPsec config

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command shows the current IPsec configuration parameters.

### Examples

The following example shows the state of IPsec (enabled/disabled) and the IPsec logging level:

```
cluster-1::> security ipsec config show
Is IPsec Enabled: true
 IPsec Log Level: 4
```

# security ipsec policy create

Create an IPsec policy

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

This command creates a new IPsec policy. The traffic to be protected is specified by the traffic selectors (local-ip-subnets, remote-ip-subnets, local-ports, remote-ports, protocols).

## Parameters

**`-vserver <vserver name>` - Vserver**

Specifies the Vserver to which the policy will belong. If there is only a single Vserver capable of supporting IPsec, the Vserver parameter is implied.

**`-name <text>` - Policy Name**

This required parameter specifies the name of the policy which may be a text string (1-64 bytes), a hexadecimal string (begining with '0x') or a base64 encoded binary string (beginning with '0s').

**`-local-ip-subnets <IP Address/Mask>,…` - Local IP Subnets**

This required parameter specifies the IPv4 or IPv6 subnet (address and mask, can be subnet or individual address) representing the local address (range) to be protected by this policy.

**`-remote-ip-subnets <IP Address/Mask>,…` - Remote IP Subnets**

This required parameter specifies the IPv4 or IPv6 subnet (address and mask, can be subnet or individual address) representing the remote address (range) to be protected by this policy.

**`[-local-ports {<Number>|<StartingNumber>-<EndingNumber>}]` - Local Ports**

This optional parameter specifies logical port associated with the local address to be protected by this policy. The port defaults to any port ('0-0' or '0') but a single port may be specified ('port number' or 'port number-port number').

**`[-remote-ports {<Number>|<StartingNumber>-<EndingNumber>}]` - Remote Ports**

This optional parameter specifies logical port associated with the remote address to be protected by this policy. The port defaults to any port ('0-0' or '0') but a single port may be specified ('port number' or 'port number-port number').

**`[-protocols {<Protocol Number>|<Protocol Name>}]` - Protocols**

This optional parameter specifies the protocol to be protected by by this policy. The protocol defaults to any protocol ('any' or '0') but a single protocol may be specified ('tcp', 'udp' or protocol number).

**`[-action <IPsec Action Type>]` - Action**

This optional parameter specifies the action to be performed when a packet meets the traffic selectors described by this policy. The possible values are 'ESP_TRA' (IPsec protect traffic), 'DISCARD' (discard matching traffic), or 'BYPASS' (send matching traffic in cleartext (not protected by IPsec)). NOTE: if the action is 'ESP_TRA', then 'shared-key' becomes a required parameter. If the action is 'BYPASS' or 'DISCARD' and a shared-key is provided, then the shared-key value will be ignored and discarded. The default value is 'ESP_TRA'.

**[-cipher-suite <Cipher Suite Type>] - Cipher Suite**

This optional parameter specifies the suite of algorithms that will be used to protect the traffic. The possible values are 'SUITEB_GCM256', 'SUTIEB_GMAC256' and 'SUITE_AESCBC' The default value is 'SUITEB_GCM256'.

**[-ike-lifetime <integer>] - IKE Security Association Lifetime**

This optional parameter specifies the lifetime of an IKE Security Association (in seconds). Shortly before the expiration of the IKE-lifetime, a new IKE security association will be created and the existing IKE security association (and child IPsec security associations) will be destroyed. The default value is 86400 seconds.

**[-ipsec-lifetime <integer>] - IPsec Security Association Lifetime**

This optional parameter specifies the lifetime of an IPsec Security Association (in seconds). Shortly before the expiration of the ipsec-lifetime, a new IPsec security association will be created and the existing IPsec security association will be destroyed. The default value is 28800 seconds.

**[-ipsec-lifetime-bytes <integer>] - IPsec Security Association Lifetime (bytes)**

This optional parameter specifies the byte lifetime of an IPsec Security Association. Shortly before the expiration of the ipsec-lifetime-bytes (ipsec-lifetime-bytes have been processed by the IPsec security association), a new IPsec security association will be created and the existing IPsec security association will be destroyed. The default value is 0, i.e infinity bytes.

**[-is-enabled {true|false}] - Is Policy Enabled**

This optional parameter specifies whether the IPsec policy is enabled or not. Any policy that is created is stored in a replicated database. The 'is-enabled' parameter determines if the policy will be included in those evaluated when determining the best-matched policy to match the traffic selectors of the packet. The default value is 'true'.

**[-local-identity <text>] - Local Identity**

This optional parameter specifies the local IKE endpoint’s identity for authentication purpose. If this field is not explicitly specified, local-ip-subnet will assume the role for identity.

**[-remote-identity <text>] - Remote Identity**

This optional parameter specifies the remote IKE endpoint’s identity for authentication purpose. If this field is not explicitly specified, remote-ip-subnet will assume the role for identity.

## Examples

This is an example of the creation of an IPsec policy that IPsec protects matching traffic, with all parameters specified. The preshared key can be string of length 18-128 bytes, a sequence hexadecimal digits beginning with 0x or a sequence of Base64 encoded binary data with 0s.

```
cluster-1::> security ipsec policy create -vserver vs_data1 -name Policy1
-local-ip-subnets 192.168.10.1/32 -remote-ip-subnets 192.168.20.1/32
-local-ports 4000 -remote-ports 5001 -protocols tcp -action ESP_TRA
-shared-key This_is_a_shared_key_for_ipsec_policy -ike-version 2 -cipher
-suite SUITEB_GCM256 -ike-lifetime 4000 -ipsec-lifetime 1800 -ipsec
-lifetime-bytes 104880 -is-enabled true

Enter the preshared key for IPsec Policy "Policy1" on Vserver "vs_data1":
Re-enter the preshared key:
```

This is an example of the creation of an IPsec policy that discards matching traffic:

```
cluster-1::> security ipsec policy create -vserver vs_data1 -name
DiscardTraffic -local-ip-subnets 192.168.10.1/32 -remote-ip-subnets
192.168.20.1/32 -action DISCARD
```

# security ipsec policy delete

Delete an IPsec policy

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

This command deletes an existing IPsec policy.

## Parameters

**`-vserver <vserver name>` - Vserver**

Specifies the Vserver to which the policy belongs. If there is only a single Vserver capable of supporting IPsec, the Vserver parameter is implied.

**`-name <text>` - Policy Name**

This required parameter specifies the name of the policy to be deleted. The name may be a text string (1-64 bytes), a hexadecimal string (begining with '0x') or a base64 encoded binary string (beginning with '0s').

## Examples

This is an example of IPsec policy deletion where two or more Vservers are capable of supporting IPsec:

```
cluster-1::> security ipsec policy delete -vserver vs_data1 -name
DiscardTraffic
```

This is an example of IPsec policy deletion where only a single Vserver is capable of supporting IPsec:

```
cluster-1::> security ipsec policy delete -name policy1
```

This is an example of an attempt to delete a non-existent IPsec policy:

```
cluster-1::> security ipsec policy delete -vserver vs_data1 -name Discard

Error: There are no entries matching your query.
```

# security ipsec policy modify

Modify an IPsec policy

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

This command modifies an existing IPsec policy. You cannot modify the name or vserver of a policy. Moving a policy from one Vserver to another or renaming a policy requires that the existing policy be deleted and then a new policy created in the desired Vserver with the desired name.

It is highly recommended that the user set the field `-is-enabled` to `false` prior to making any other modifications to the policy. This will disable the policy and allow all existing IPsec and IKE Security Associations associated with policy to get flushed. Then, the user can modify the policy with the desired changes, along with setting the `-is-enabled` field to `true` to re-enable the policy.

## Parameters

**`-vserver <vserver name>` - Vserver**

Specifies the Vserver to which the policy belongs. If there is only a single Vserver capable of supporting IPsec, the Vserver parameter is implied.

**`-name <text>` - Policy Name**

This required parameter specifies the name of the policy which may be a text string (1-64 bytes), a hexadecimal string (begining with '0x') or a base64 encoded binary string (beginning with '0s').

**`[-local-ip-subnets <IP Address/Mask>,…]` - Local IP Subnets**

This parameter specifies the IPv4 or IPv6 subnet (address and mask, can be subnet or individual address) representing the local address (range) to be protected by this policy.

**`[-remote-ip-subnets <IP Address/Mask>,…]` - Remote IP Subnets**

This parameter specifies the IPv4 or IPv6 subnet (address and mask, can be subnet or individual address) representing the remote address (range) to be protected by this policy.

**`[-local-ports {<Number>|<StartingNumber>-<EndingNumber>}]` - Local Ports**

This parameter specifies the logical port associated with the local address to be protected by this policy. The value may be specified by 'port number' or 'port number-port number'.

**[-remote-ports {<Number>|<StartingNumber>-<EndingNumber>}] - Remote Ports**

This parameter specifies the logical port associated with the remote address to be protected by this policy. The value may be specified by 'port number' or 'port number-port number'.

**[-protocols {<Protocol Number>|<Protocol Name>}] - Protocols**

This parameter specifies the protocol to be protected by this policy. The protocol may be specified as 'tcp', 'udp' or protocol number.

**[-cipher-suite <Cipher Suite Type>] - Cipher Suite**

This parameter specifies the suite of algorithms that will be used to protect the traffic. The possible values are '256-bit AES-CBC', '256-bit AES-GCM' and '256-bit AES-GMAC'.

**[-ike-lifetime <integer>] - IKE Security Association Lifetime**

This parameter specifies the lifetime of an IKE Security Association (in seconds). Shortly before the expiration of the IKE-lifetime, a new IKE security association will be created and the existing IKE security association (and child IPsec security associations) will be destroyed.

**[-ipsec-lifetime <integer>] - IPsec Security Association Lifetime**

This parameter specifies the lifetime of an IPsec Security Association (in seconds). Shortly before the expiration of the ipsec-lifetime, a new IPsec security association will be created and the existing IPsec security association will be destroyed.

**[-ipsec-lifetime-bytes <integer>] - IPsec Security Association Lifetime (bytes)**

This parameter specifies the byte lifetime of an IPsec Security Association. Shortly before the expiration of the ipsec-lifetime-bytes (ipsec-lifetime-bytes have been processed by the IPsec security association), a new IPsec security association will be created and the existing IPsec security association will be destroyed.

**[-is-enabled {true|false}] - Is Policy Enabled**

This parameter specifies the whether the IPsec policy is enabled or not. Any policy which is created is stored in a replicated database. The 'is-enabled' parameter determines if the policy will be included in those evaluated when determining the best-matched policy to match the traffic selectors of the packet. The default value is 'true'.

**[-local-identity <text>] - Local Identity**

This optional parameter specifies the local IKE endpoint’s identity for authentication purpose. If this field is not explicitly specified, local-ip-subnet will assume the role for identity.

**[-remote-identity <text>] - Remote Identity**

This optional parameter specifies the remote IKE endpoint’s identity for authentication purpose. If this field is not explicitly specified, remote-ip-subnet will assume the role for identity.

## Examples

The following example modifies the local-ip-subnets value of an IPsec policy:

```
cluster-1::> security ipsec policy modify -vserver vs_data1 -name Policy1
-local-ip-subnets 192.168.30.2/32
```

# security ipsec policy show

Display IPsec policies

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `security ipsec policy show` command displays information about configured IPsec policies. All parameters are optional. This command is supported only when IPsec is enabled.

Running the command with the `-vserver` parameter displays all policies associated with the specified vserver.

You can specify additional parameters to display only information that matches those parameters. For example, to display policies associated with a certain local ip subnet, run the command with the `-local-ip-subnets` parameter.

## Parameters

**{ [-fields <fieldname>,…]**

If you specify the `-fields <fieldname>,…` parameter, the command displays only the specified fields. Notice that key fields are always displayed.

**| [-instance ] }**

If you specify the `-instance` parameter, the command displays all fields of the policies.

**[-vserver <vserver name>] - Vserver**

If you specify this parameter, only policies associated with this Vserver will be displayed.

**[-name <text>] - Policy Name**

This parameter specifies the policy to be displayed.

**[-local-ip-subnets <IP Address/Mask>,…] - Local IP Subnets**

If you specify this parameter, information about local-ip-subnets will be displayed.

**[-remote-ip-subnets <IP Address/Mask>,…] - Remote IP Subnets**

If you specify this parameter, information about remote-ip-subnets will be displayed.

**[-local-ports {<Number>|<StartingNumber>-<EndingNumber>}] - Local Ports**

If you specify this parameter, information about local-ports will be displayed.

**[-remote-ports {<Number>|<StartingNumber>-<EndingNumber>}] - Remote Ports**

If you specify this parameter, information about remote-ports will be displayed.

**[-protocols {<Protocol Number>|<Protocol Name>}] - Protocols**

If you specify this parameter, information about protocols will be displayed.

**[-action <IPsec Action Type>] - Action**

If you specify this parameter, information about action will be displayed.

**[-cipher-suite <Cipher Suite Type>] - Cipher Suite**

If you specify this parameter, information about cipher-suite will be displayed.

**[-ike-lifetime <integer>] - IKE Security Association Lifetime**

If you specify this parameter, information about ike-lifetime will be displayed.

**[-ipsec-lifetime <integer>] - IPsec Security Association Lifetime**

If you specify this parameter, information about ipsec-lifetime will be displayed.

**[-ipsec-lifetime-bytes <integer>] - IPsec Security Association Lifetime (bytes)**

If you specify this parameter, information about ipsec-lifetime-bytes will be displayed.

**[-is-enabled {true|false}] - Is Policy Enabled**

If you specify this parameter, information about is-enabled will be displayed.

**[-local-identity <text>] - Local Identity**

If you specify this parameter, information about local IKE endpoint's identity, if configured, will be displayed.

**[-remote-identity <text>] - Remote Identity**

If you specify this parameter, information about remote IKE endpoint's identity, if configured, will be displayed.

## Examples

The this example displays all policies in all Vservers:

```
cluster-1::> security ipsec policy show
        Policy                                          Cipher
Vserver Name       Local IP Subnet    Remote IP Subnet   Suite
Action
------- ---------- ------------------ ------------------ --------------
-------
vs_data1
        Policy1    192.168.10.1/32    192.168.20.1/32    SUITEB_GCM256
ESP_TRA
        Policy3    192.158.10.10/32   192.158.10.20/32   SUITEB_GCM256
DISCARD
vs_data2
        Policy2    10.10.10.10/32     20.20.20.20/32     SUITE_AESCBC
ESP_TRA
3 entries were displayed.
```

This example displays all of the IPsec policies from a single Vserver:

```
cluster-1::> security ipsec policy show -vserver vs_data1
        Policy                                          Cipher
Vserver Name       Local IP Subnet    Remote IP Subnet   Suite
Action
------- ---------- ------------------ ------------------ --------------
-------
vs_data1
        Policy1    192.168.10.1/32    192.168.20.1/32    SUITEB_GCM256
ESP_TRA
        Policy3    192.158.10.10/32   192.158.10.20/32   SUITEB_GCM256
DISCARD
2 entries were displayed.
```

This example displays a specific policy:

```
cluster-1::> security ipsec policy show -vserver vs_data1 -name Policy1
Vserver Name: vs_data1
                               Policy Name: Policy1
                          Local IP Subnets: 192.168.10.1/32
                         Remote IP Subnets: 192.168.20.1/32
                               Local Ports: 0-0
                              Remote Ports: 0-0
                                 Protocols: any
                                    Action: ESP_TRA
                              Cipher Suite: SUITEB_GCM256
          IKE Security Association Lifetime: 10800
        IPsec Security Association Lifetime: 3600
IPsec Security Association Lifetime (bytes): 0
                           Is Policy Enabled: true
                              Local Identity:
                             Remote Identity:
```

This example displays a specific field from all policies:

```
cluster-1::> security ipsec policy show -fields local-ip-subnets
vserver  name    local-ip-subnets
-------- ------- ----------------
vs_data1 Policy1 192.168.10.1/32
vs_data1 Policy3 192.158.10.10/32
vs_data2
         Policy2 10.10.10.10/32
3 entries were displayed.
```

## Copyright information

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

## Trademark information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.