



## Crypto Access Check on Clear-Text Packets

---

The Crypto Access Check on Clear-Text Packets feature removes the checking of clear-text packets that go through the IP Security (IPSec) tunnel just prior to encryption or just after decryption. The clear-text packets were checked against the outside physical interface access control lists (ACLs). This checking was often referred to as a double ACL check. This feature enables easier configuration of ACLs and eliminates the security risks that are associated with a double check when using dynamic crypto maps.

### Feature History for Crypto Access Check on Clear-Text Packets

Release	Modification
12.3(8)T	This feature was introduced.

### Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for Crypto Access Check on Clear-Text Packets, page 2](#)
- [Restrictions for Crypto Access Check on Clear-Text Packets, page 2](#)
- [Information About Crypto Access Check on Clear-Text Packets, page 2](#)
- [How to Configure Crypto Map Access ACLs, page 6](#)
- [Configuration Examples for Crypto Access Check on Clear-Text Packets, page 8](#)
- [Additional References, page 14](#)
- [Command Reference, page 15](#)



---

**Corporate Headquarters:**  
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2004 Cisco Systems, Inc. All rights reserved.

## Prerequisites for Crypto Access Check on Clear-Text Packets

- You should be familiar with configuring IPsec.
- You should be familiar with ACLs.

## Restrictions for Crypto Access Check on Clear-Text Packets

- This feature does not apply to IPsec configurations on the Virtual Private Network (VPN) service module (card) on Cisco Catalyst 6500 series switches and Cisco 7600 series router platforms.
- This feature supports only extended ACLs.

## Information About Crypto Access Check on Clear-Text Packets

To use the crypto access check on clear-text packets, you should understand the following concepts:

- [Crypto Access Check on Clear-Text Packets Overview, page 2](#)
- [Configuration Changes That Are Required for This Feature, page 2](#)
- [How ACL Access Checking Worked Prior to This Feature, page 3](#)
- [ACL Checking Behavior After Upgrading to This Feature, page 4](#)
- [Backward Compatibility, page 6](#)

## Crypto Access Check on Clear-Text Packets Overview

The Crypto Access Check on Clear-Text Packets feature provides four changes for the interaction between IPsec and interface access lists. The changes are as follows:

- Removes the checking of inbound, just-decrypted clear-text packets against the outside interface inbound ACL.
- Removes the checking of outbound clear-text packets just prior to encryption against the outside interface outbound ACL.
- Adds the checking of outbound encrypted packets against the outside interface outbound ACL.
- Adds the capability to configure ACLs under the crypto map to check inbound clear-text packets after decryption or outbound clear-text packets prior to encryption.

This feature enables the easier and more consistent configuration of ACLs that control packet movement in and out of the outside interface as well as in and out of the IPsec encryption tunnel. This feature also eliminates security risks that are associated with the current double check when using dynamic crypto maps.

## Configuration Changes That Are Required for This Feature

This feature requires the following configuration changes to be performed. Some are required and some are optional.

## Prior to Upgrading

Prior to upgrading to this feature, you should do the following. This change is required.

Check all outside interfaces for outbound ACLs. If any outbound ACLs exist, check to ensure that they include access-list entries (ACEs) that permit outbound Encapsulating Security Payload (ESP) IP protocol 50 packets or Authentication Header (AH) IP protocol 51 packets. The ACL entries will be needed after the upgrade because the outbound encrypted packets will be checked against the outside interface outbound ACL. If the ESP or AH packets are not allowed by the outside interface outbound ACL, the IPsec VPN tunnels will not forward traffic.

## After Upgrading

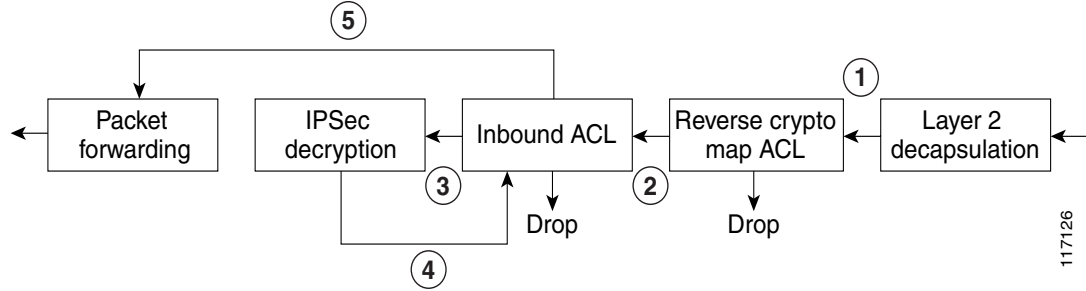
After upgrading to this feature, you should do the following. The first two procedures are required if you are using dynamic crypto maps. However, these procedures are recommended even if you are not using dynamic crypto maps. The third and fourth procedures are optional.

- Check all outside interfaces for inbound ACLs that contain ACEs that permit inbound, just-decrypted clear-text packets. These ACEs need to be removed if dynamic crypto maps are being used because when the IPsec tunnel is not “up,” the ACEs will allow the clear-text packets into the network. If dynamic crypto maps are not being used, the ACEs can still be removed to simplify the outside interface ACLs.
- Check all outside interfaces for outbound ACLs that contain ACEs that permit outbound clear-text packets that would be encrypted. These ACEs need to be removed if dynamic crypto maps are being used because when the IPsec tunnel is not up, these ACEs will allow the clear-text packets out of the network. If dynamic crypto maps are not being used, these ACEs can still be removed to simplify the outside interface ACLs.
- Add an outbound crypto map access ACL under the crypto map to deny to-be-encrypted, outbound clear-text packets that should be dropped. Be sure that you also permit all other packets in this ACL.
- Add an inbound crypto map access ACL under the crypto map to deny just-decrypted, inbound clear-text packets that should be dropped. Be sure to also permit all other packets in this ACL.

The last two configuration changes are needed only in the rare cases in which the crypto map ACL (that selects packets to be encrypted) is more general than the packet flows that you want to encrypt. Adding outbound or inbound crypto map ACLs is usually done to keep the crypto map ACL small and simple, which saves CPU utilization and memory. The **set ip access-group** command, which is used to cause the checking of clear-text packets after decryption and before encryption, can be used under the crypto map to accomplish this task independent of the outside interface ACLs.

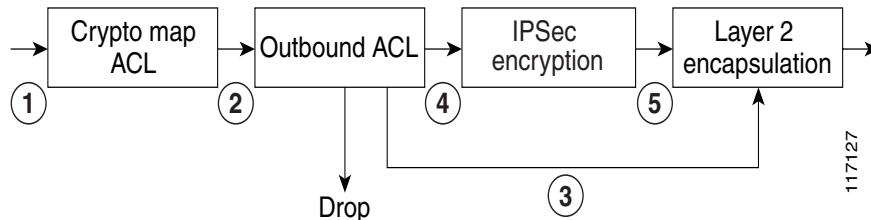
## How ACL Access Checking Worked Prior to This Feature

Prior to Cisco Release 12.3(8)T, there was a double ACL check on the inbound packets, once on the encrypted packet and then again on the just-decrypted clear-text packet. The process on the inbound path is shown in [Figure 1](#).

**Figure 1** Inbound Encrypted Packet Flow Prior to This Feature

1. Arriving IP packet is checked against the reverse crypto map ACL. If the packet is denied, it is dropped because the incoming packet was not encrypted. The IPSec configuration specifies that it should have been encrypted.
2. IP packet is checked against the interface inbound ACL. If denied, it is dropped.
3. If the IP packet is encrypted, it is then decrypted.
4. Just-decrypted IP packet is again checked against the interface inbound ACL. If denied, it is dropped.
5. Just-decrypted and not-encrypted IP packets that are permitted by the interface inbound ACL are forwarded.

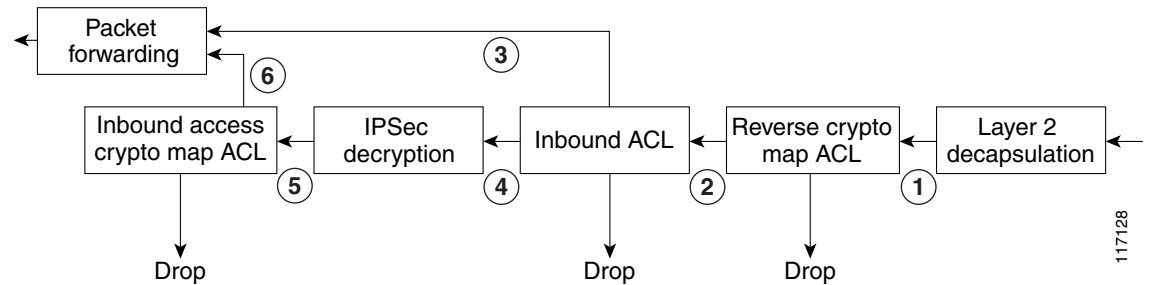
On the outbound path, crypto feature checking for encryption took place before the output feature check for the ACL. The output ACL was run on the clear-text packet before the packet was sent for encryption. After the packet was encrypted, it was not checked against the outside interface outbound ACL again. The process on the outbound path is shown in [Figure 2](#).

**Figure 2** Outbound Encrypted Packet Flow Prior to This Feature

1. Departing IP packet is checked against the crypto map ACL. If permitted, the packet is marked for encryption.
2. All IP packets are checked against the outbound interface ACL. If denied, they are dropped.
3. IP packets not marked for encryption are Layer 2 encapsulated.
4. IP packets marked for encryption are encrypted.
5. Encrypted IP packets are Layer 2 encapsulated.

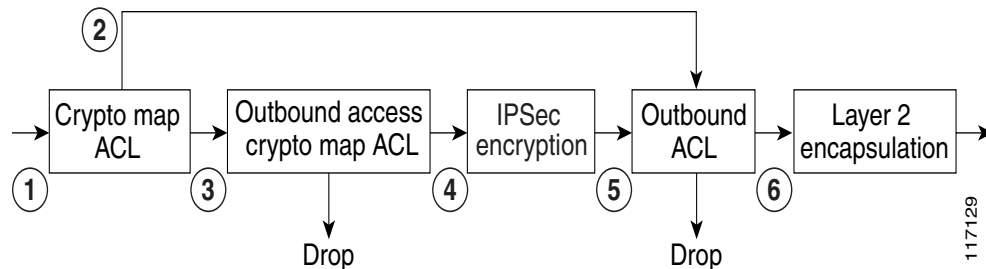
## ACL Checking Behavior After Upgrading to This Feature

[Figure 3](#) illustrates the ACL checking behavior on the inbound path using the Crypto Access Check on Clear-Text Packets feature.

**Figure 3** New Inbound Encrypted Packet Flow

1. Arriving IP packet is checked against the reverse crypto map ACL. If it is denied, it is dropped because the incoming packet was not encrypted. The IPSec configuration specifies that it should have been encrypted.
2. IP packet is checked against the interface inbound ACL. If denied, it is dropped.
3. If the IP packet is not encrypted, it is forwarded.
4. If the IP packet is encrypted, it is then decrypted.
5. Just-decrypted IP packet is checked against the inbound access crypto map ACL (optional). If the packet is denied, it is dropped.
6. Just-decrypted IP packet is forwarded.

Figure 4 illustrates the ACL checking behavior on the outbound path using the Crypto Access Check on Clear-Text Packets feature.

**Figure 4** New Outbound Encrypted Packet Flow

1. All departing IP packets are checked against the crypto map ACL. If the packets are permitted, they are marked for encryption.
2. IP packets not marked for encryption are checked against the outbound interface ACL. If the packets are denied, they are dropped.
3. IP packets marked for encryption are checked against the outbound access crypto map ACL (optional). If the packets are denied, they are dropped.
4. Permitted IP packets are encrypted.
5. Encrypted IP packets are checked against the outbound interface ACL. If the packets are denied, they are dropped.
6. Permitted IP packets are Layer 2 encapsulated.

## Backward Compatibility

If the Cisco IOS software is subsequently downgraded to a release that does not have the Crypto Access Check on Clear-Text Packets feature, the just-decrypted and to-be-encrypted clear-text packets will again be blocked by the outside interface ACLs. Therefore, if you have removed lines from the interface ACLs, you should undo the changes that were made to the ACLs if you are downgrading to an earlier version.

## How to Configure Crypto Map Access ACLs

This section contains the following procedures:

- [Adding or Removing ACLs, page 6](#) (optional)
- [Verifying the Configured ACLs, page 7](#) (optional)

## Adding or Removing ACLs

To add or remove crypto map access ACLs, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name seq-number*
4. **set ip access-group** {*access-list-number* | *access-list-name*} {**in** | **out**}

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	<b>crypto map</b> <i>map-name</i> <i>seq-number</i>  <b>Example:</b> Router(config)# <b>crypto map</b> vpn1 10	Selects the crypto map and the sequence map entry under the crypto map to which you want to add the crypto map access ACL; also enters crypto map configuration mode.
Step 4	<b>set ip access-group</b> [ <i>access-list-number</i>   <i>access-list-name</i> ]{ <b>in</b>   <b>out</b> }  <b>Example:</b> Router(config-crypto-map)# <b>set ip access-group</b> 151 in	Allows you to check the postdecrypted or preencrypted packet against an ACL without having to use the outside physical interface ACL.

## Verifying the Configured ACLs

The **show ip access-list** command can be used to verify the crypto input or output access-check ACLs that have been configured. Also, the packets that have been dropped in the context of the crypto input access-check ACL in the inbound path will be logged as receive (recv) errors, and packets dropped on the outbound path will be logged as send errors.

The **show crypto map** command can be used to verify crypto map configuration information.

### SUMMARY STEPS

1. **enable**
2. **show ip access-list** [*access-list-number* | *access-list-name* | **dynamic**]
3. **show crypto map** [**interface** *interface* | **tag** *map-name*]

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> <b>enable</b>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>show ip access-list</b> [ <i>access-list-number</i>   <i>access-list-name</i>   <b>dynamic</b> ]  <b>Example:</b> Router# <b>show ip access-list</b> Internetfilter	Displays a configured ACL.
Step 3	<b>show crypto map</b> [ <b>interface</b> <i>interface</i>   <b>tag</b> <i>map-name</i> ]  <b>Example:</b> Router# <b>show crypto map</b>	Displays the crypto maps that have been configured.

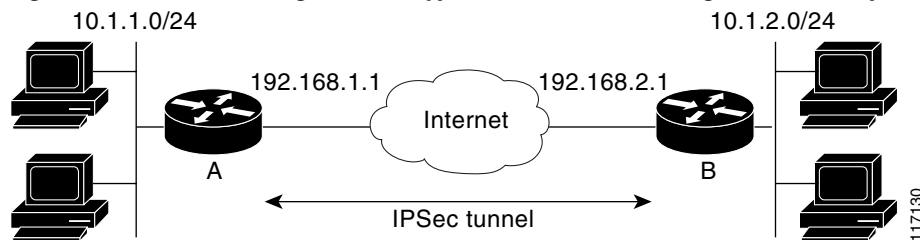
# Configuration Examples for Crypto Access Check on Clear-Text Packets

This section contains the output for the following stages of crypto access configuration:

- [Previous IPsec ACL Configuration: Example, page 8](#)
- [New IPsec ACL Configuration Without Crypto Access ACLs: Example, page 9](#)
- [New IPsec ACL Configuration with Crypto Access ACLs: Example, page 9](#)
- [Authentication Proxy, IPsec, and CBAC Configuration: Example](#)

The network diagram used for the following examples is shown in [Figure 5](#).

**Figure 5 Network Diagram for Crypto Access Check Configuration Examples**



The configuration examples assume these policy rules:

- Allow only encrypted host traffic between hosts on 10.1.1.0/24 and 10.1.2.0/24.
- No clear-text traffic from the Internet to any host.

## Previous IPsec ACL Configuration: Example

The following is a sample configuration using an earlier version of Cisco IOS software (before Release 12.3(8)T). The configuration shows outside interface ACLs with a double check on the inbound packets.

```
crypto map vpnmap 10 ipsec-isakmp
  set peer 192.168.2.1
  set transform-set trans1
  match address 101

interface Ethernet0/0
  ip address 10.1.1.1 255.255.255.0
interface Serial1/0
  ip address 192.168.1.1 255.255.255.0
  ip access-group 150 in
  ip access-group 160 out
  crypto map vpnmap

access-list 101 permit ip 10.1.1.0 0.0.0.255 10.1.2.0 0.0.0.255
access-list 150 permit udp host 192.168.2.1 eq 500 host 192.168.1.1 eq 500
access-list 150 permit esp host 192.168.2.1 host 192.168.1.1
access-list 150 permit ip 10.1.2.0 0.0.0.255 10.1.1.0 0.0.0.255

access-list 160 permit udp host 192.168.1.1 eq 500 host 192.168.2.1 eq 500
access-list 160 permit ip 10.1.1.0 0.0.0.255 10.1.2.0 0.0.0.255
```

## New IPsec ACL Configuration Without Crypto Access ACLs: Example

The following is a sample configuration using the current version of Cisco IOS software (Release 12.3(8)T). Before the crypto map access ACL is added, clear-text packets through the IPsec tunnel are not checked against an ACL (other packets are checked against the outside interface ACLs). Note the permitting of ESP packets in the outside interface outbound ACL.

```
crypto map vpnmap 10 ipsec-isakmp
  set peer 192.168.2.1
  set transform-set trans1
  match address 101

interface Ethernet0/0
  ip address 10.1.1.1 255.255.255.0
interface Serial1/0
  ip address 192.168.1.1 255.255.255.0
  ip access-group 150 in
  ip access-group 160 out
  crypto map vpnmap
access-list 101 permit ip 10.1.1.0 0.0.0.255 10.1.2.0 0.0.0.255

access-list 150 permit udp host 192.168.2.1 eq 500 host 192.168.1.1 eq 500
access-list 150 permit esp host 192.168.2.1 host 192.168.1.1

access-list 160 permit udp host 192.168.1.1 eq 500 host 192.168.2.1 eq 500
access-list 160 permit esp host 192.168.1.1 host 192.168.2.1
```

## New IPsec ACL Configuration with Crypto Access ACLs: Example

The following is a sample configuration using the current version of Cisco IOS software (Release 12.3(8)T). Before a crypto map access ACL is added, clear-text packets through the IPsec tunnel are checked against the crypto map access ACLs (other packets are checked against the outside interface ACLs).

**Note**

---

In the following example, all IP packets between the subnets 10.1.1.0/24 and 10.1.2.0/24 are to be encrypted, but the crypto map access ACLs allow only Telnet traffic through the IPsec tunnel.

---

```
crypto map vpnmap 10 ipsec-isakmp
  set peer 192.168.2.1
  set transform-set trans1
  set ip access-group 151 in
  set ip access-group 161 out
  match address 101

interface Ethernet0/0
  ip address 10.1.1.1 255.255.255.0
interface Serial1/0
  ip address 192.168.1.1 255.255.255.0
  ip access-group 150 in
  ip access-group 160 out
  crypto map vpnmap

access-list 101 permit ip 10.1.1.0 0.0.0.255 10.1.2.0 0.0.0.255

access-list 150 permit udp host 192.168.2.1 eq 500 host 192.168.1.1 eq 500
access-list 150 permit esp host 192.168.2.1 host 192.168.1.1
```

```

access-list 151 permit tcp 10.1.2.0 0.0.0.255 eq telnet 10.1.1.0 0.0.0.255
access-list 151 permit tcp 10.1.2.0 0.0.0.255 10.1.1.0 0.0.0.255 eq telnet

access-list 160 permit udp host 192.168.1.1 eq 500 host 192.168.2.1 eq 500
access-list 160 permit esp host 192.168.1.1 host 192.168.2.1

access-list 161 permit ip 10.1.1.0 0.0.0.255 10.1.2.0 0.0.0.255 eq telnet
access-list 161 permit ip 10.1.1.0 0.0.0.255 eq telnet 10.1.2.0 0.0.0.255

```

## Authentication Proxy, IPSec, and CBAC Configuration: Example

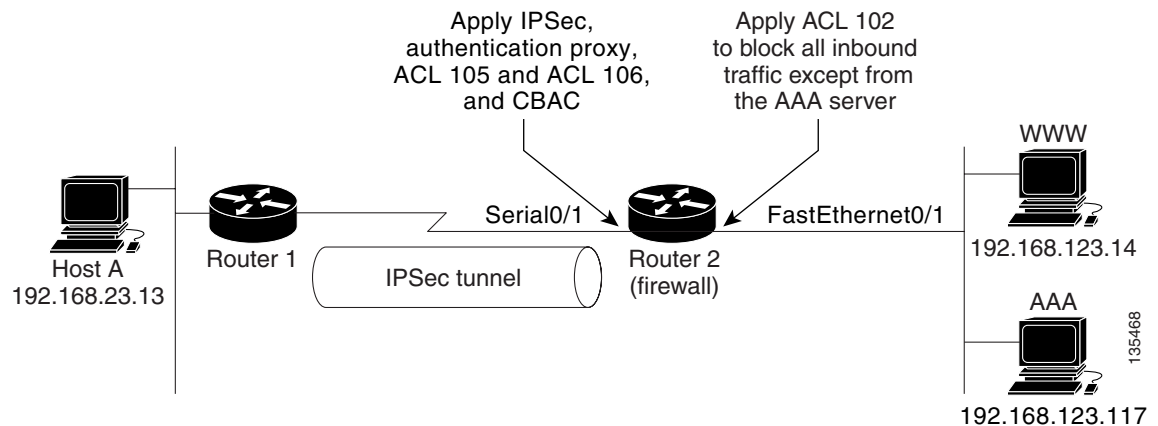
The following example shows a router configuration using the authentication proxy, IPSec, and CBAC features. [Figure 6](#) illustrates the configuration.



### Note

This configuration is effective for Cisco IOS Release 12.3(8)T software and later.

**Figure 6 Router Configuration Using Authentication Proxy, IPSec, and CBAC Features**



In this example, Host A initiates a HTTP connection with the web server (WWW). The HTTP traffic between Router 1 and Router 2 is encrypted using IPSec. The authentication proxy, IPSec, and CBAC are configured at interface Serial0/1 on Router 2, which is acting as the firewall. ACL 105 allows only IPSec traffic at interface Serial0/1. ACL 106 is crypto access check, which blocks all traffic. ACL 102 is applied at interface FastEthernet0/1 on Router 2 to block all traffic on that interface except traffic from the AAA server.

When Host A initiates a HTTP connection with the web server, the authentication proxy prompts the user at Host A for a username and password. These credentials are verified with the AAA server for authentication and authorization. If authentication is successful, the per-user ACLs are downloaded to the firewall to permit services.

The following examples provide both the Router 1 and Router 2 configurations for completeness:

- [Router 1 Configuration Example](#)
- [Router 2 Configuration Example](#)

**Router 1 Configuration Example**

```
version 12.3
service timestamps debug uptime
service timestamps log uptime
!
hostname Router1
!
boot-start-marker
boot-end-marker
!
ip subnet-zero
ip cef
!
!
no ip dhcp use vrf connected
!
!
no ip ips deny-action ips-interface
!
no ftp-server write-enable
!
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco1234 address 10.0.0.2
!
!
crypto ipsec transform-set rule_1 ah-sha-hmac esp-des esp-sha-hmac
!
crypto map testtag 10 ipsec-isakmp
 set peer 10.0.0.2
 set transform-set rule_1
 match address 155
!
!
interface FastEthernet0/0
 ip address 192.168.23.2 255.255.255.0
 speed auto
!
interface Serial1/1
 ip address 10.0.0.1 255.0.0.0
 encapsulation ppp
 clockrate 2000000
 crypto map testtag
!
ip classless
ip route 192.168.123.0 255.255.255.0 10.0.0.2
!
no ip http server
no ip http secure-server
!
access-list 155 permit ip 192.168.23.0 0.0.0.255 192.168.123.0 0.0.0.255
!
control-plane
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
!
end
```

**Router 2 Configuration Example**

```

version 12.3
service timestamps debug uptime
service timestamps log uptime
!
hostname Router2
!
boot-start-marker
boot-end-marker
!
!
resource policy
!
aaa new-model
!
!
aaa authentication login default group tacacs+
aaa authentication login console none
aaa authorization auth-proxy default group tacacs+
!
aaa session-id common
clock timezone MST -8
clock summer-time MDT recurring
no network-clock-participate slot 1
no network-clock-participate wic 0
ip subnet-zero
!
!
no ip dhcp use vrf connected
!
!
ip cef
ip inspect name rule22 tcp
ip inspect name rule22 ftp
ip inspect name rule22 smtp
ip auth-proxy name pxy http inactivity-time 60
no ip ips deny-action ips-interface
!
no ftp-server write-enable
!
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco1234 address 10.0.0.1
!
!
crypto ipsec transform-set rule_1 ah-sha-hmac esp-des esp-sha-hmac
!
crypto map testtag 10 ipsec-isakmp
 set peer 10.0.0.1
 ! Define crypto access check to filter traffic after IPSec decryption
 ! Authentication-proxy downloaded ACEs will be added to this ACL,
 ! not interface ACL.
 set ip access-group 106 in
 set transform-set rule_1
 match address 155
!
!
interface FastEthernet0/1
 ip address 192.168.123.2 255.255.255.0
 ip access-group 102 in
 duplex auto
 speed auto

```

```

!
interface Serial0/1
 ip address 10.0.0.2 255.0.0.0
 ip access-group 105 in
 ip inspect rule22 in
 ip auth-proxy pxy
 encapsulation ppp
 crypto map testtag
!
no ip classless
ip route 192.168.23.0 255.255.255.0 10.0.0.1
!
!
ip http server
ip http access-class 15
ip http authentication aaa
no ip http secure-server
!
access-list 15 deny any
access-list 102 permit tcp host 192.168.123.20 117 eq tacacs host 192.168.123.2
! ACL 155 is interface ACL which allows only IPSec traffic
access-list 105 permit ahp any any
access-list 105 permit esp any any
access-list 105 permit udp any any eq isakmp
! ACL 106 is crypto access check ACL
access-list 106 deny ip any any
access-list 155 permit ip 192.168.123.0 0.0.0.255 192.168.23.0 0.0.0.255
!
!
tacacs-server host 192.168.123.117
tacacs-server directed-request
tacacs-server key cisco
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 login authentication console
line aux 0
 transport input all
 speed 38400
 flowcontrol hardware
line vty 0 4
 login authentication console
!
End

```

### TACAC+ User Profile Example

```

user = http_1 {
  default service = permit
  login = cleartext mypassword
  service = auth-proxy
  {
    priv-lvl=15
    proxyacl#1="permit tcp any any eq 23"
    proxyacl#2="permit tcp any any eq 21"
    proxyacl#3="permit tcp any any eq 25"
    proxyacl#4="permit tcp any any eq 80"
    proxyacl#5="permit udp any any eq 53"
  }
}

```

**ACL 106, Before Auth-Proxy Authentication**

```
Router2# show access-list 106

Extended IP access list 106
  10 deny ip any any (4 matches)
```

**ACL 106, After Auth-Proxy Authentication**

```
Router2# show access-list 106

Extended IP access list 106
  permit tcp host 192.168.23.116 any eq telnet
  permit tcp host 192.168.23.116 any eq ftp
  permit tcp host 192.168.23.116 any eq smtp
  permit tcp host 192.168.23.116 any eq www (6 matches)
  permit udp host 192.168.23.116 any eq domain
  10 deny ip any any (4 matches)
```

## Additional References

The following sections provide references related to the Crypto Access Check on Clear-Text Packets feature.

## Related Documents

Related Topic	Document Title
Configuring IPsec	“ <a href="#">Implementing IPsec and IKE</a> ” section of the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4
Configuring ACLs	“ <a href="#">Traffic Filtering, Firewalls, and Virus Detection</a> ” section of the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4
IPsec Commands	<i>Cisco IOS Security Command Reference</i> , Release 12.4

## Standards

Standards	Title
There are no new or modified standards associated with this feature.	—

## MIBs

MIBs	MIBs Link
There are no new or modified MIBs associated with this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFCs	Title
There are no new or modified RFCs associated with this feature.	—

## Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	<a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a>

## Command Reference

This section documents only the following new and modified commands.

### New Command

- [set ip access-group](#)

### Modified Command

- [show crypto map \(IPSec\)](#)

## set ip access-group

To check a preencrypted or postdecrypted packet against an access control list (ACL) without having to use the outside physical interface ACL, use the **set ip access-group** command in crypto map configuration mode. To disable the check, use the **no** form of this command.

**set ip access-group** {*access-list-number* | *access-list-name*} {**in** | **out**}

**no set ip access-group** {*access-list-number* | *access-list-name*} {**in** | **out**}

### Syntax Description

<i>access-list-number</i>	Number of an access list. Values 100 through 199 are used for IP access lists (extended). The values 2000 through 2699 are used for expanded access lists (extended).
<i>access-list-name</i>	Name of an access list.
<b>in</b>	Sets access control for inbound clear-text packets (after decryption).
<b>out</b>	Sets access control for outbound clear-text packets (prior to encryption).

### Defaults

No crypto map access ACLs are defined to filter clear-text packets going through the IPsec tunnel.

### Command Modes

Crypto map configuration

### Command History

Release	Modification
12.3(8)T	This command was introduced.

### Usage Guidelines

The **set ip access-group** command is used after the crypto map has been configured.

### Examples

The following example shows that a crypto map access ACL has been configured:

```
Router (config)# crypto map map vpn1 10
Router (config-crypto-map)# set ip access-group 151 in
```

### Related Commands

Command	Description
<b>crypto map</b>	Assigns a previously defined crypto map set to an interface so that the interface can provide IPsec services.

# show crypto map (IPSec)

To display the crypto map configuration, use the **show crypto map** command in privileged EXEC or user EXEC mode.

```
show crypto map [interface interface | tag map-name]
```

Syntax Description	
<b>interface</b> <i>interface</i>	(Optional) Displays only the crypto map set that is applied to the specified interface.
<b>tag</b> <i>map-name</i>	(Optional) Displays only the crypto map set with the specified <i>map-name</i> .

**Defaults** No crypto maps are shown.

**Command Modes** Privileged EXEC  
User EXEC

Command History	Release	Modification
	11.2	This command was introduced.
	12.3(8)T	Output has been modified to display the crypto input and output access control lists (ACLs) that have been configured.

**Usage Guidelines** The **show crypto map** command provides output that is IP specific, and it allows you to specify a particular crypto map.

**Examples** The following example shows that crypto input and output ACLs have been configured:

```
Router# show crypto map

Crypto Map "test" 10 ipsec-isakmp
Peer
Extended IP access list ipsec_acl
  access-list ipsec_acl permit ip 192.168.2.0 0.0.0.255 192.168.102.0 0.0.0.255
Extended IP access check IN list 110
  access-list 110 permit ip host 192.168.102.47 192.168.2.0 0.0.0.15
  access-list 110 permit ip host 192.168.102.47 192.168.2.32 0.0.0.15
  access-list 110 permit ip host 192.168.102.47 192.168.2.64 0.0.0.15
  access-list 110 permit ip host 192.168.102.57 192.168.2.0 0.0.0.15
  access-list 110 permit ip host 192.168.102.57 192.168.2.32 0.0.0.15
  access-list 110 permit ip host 192.168.102.57 192.168.2.64 0.0.0.15
Extended IP access check OUT list 120
  access-list 120 permit ip 192.168.2.0 0.0.0.15 host 192.168.102.47
  access-list 120 permit ip 192.168.2.32 0.0.0.15 host 192.168.102.47
  access-list 120 permit ip 192.168.2.64 0.0.0.15 host 192.168.102.47
  access-list 120 permit ip 192.168.2.0 0.0.0.15 host 192.168.102.57
  access-list 120 permit ip 192.168.2.32 0.0.0.15 host 192.168.102.57
  access-list 120 permit ip 192.168.2.64 0.0.0.15 host 192.168.102.57
```

■ **show crypto map (IPSec)**

```

Current peer: 10.0.0.2
Security association lifetime: 4608000 kilobytes/3600 seconds
PFS (Y/N): N
Transform sets=test
Interfaces using crypto map test:
  Serial0/1

```

Table 1 describes the output in the display.

**Table 1** *show crypto map Field Descriptions*

<b>Field</b>	<b>Description</b>
Peer	Possible peers that are configured for this crypto map entry.
Extended IP access list	Access list that is used to define which data packets are to be encrypted. Packets that are denied by this access list are forwarded but not encrypted. The “reverse” of this access list is used to check the inbound return packets, which are also encrypted. Packets that are denied by the “reverse” access list are dropped because they should have been encrypted but were not.
Extended IP access list check	Access lists that are used to more finely control which data packets are allowed into or out of the IPSec tunnel. Packets that are allowed by the “Extended IP access list” ACL but denied by the “Extended IP access list check” ACL are dropped.
Current peer	Current peer that is being used for this crypto map entry.
Security association lifetime	Number of bytes that are allowed to be encrypted or decrypted or the age of the security association before new encryption keys must be negotiated.
PFS	(Perfect Forward Secrecy) If “Yes,” the Internet Security Association (ISAKMP) SKEYID-d key is also renegotiated each time IPSec security association (SA) encryption keys are renegotiated (requires another Diffie-Hillman calculation). Otherwise, the same ISAKMP SKEYID-d key is used when renegotiating IPSec SA encryption keys. ISAKMP keys are renegotiated on a separate schedule, with a default time of 24 hours.
Transform sets	List of transform sets (encryption, authentication, and compression algorithms) that can be used with this crypto map.
Interfaces using crypto map test	Interfaces to which this crypto map is applied. Packets that are leaving from this interface are subject to the rules of this crypto map for encryption. Encrypted packets may enter the router on any interface, and they will be decrypted. Nonencrypted packets that are entering the router through this interface are subject to the “reverse” crypto access list check.

---

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

---

Copyright © 2004 Cisco Systems, Inc. All rights reserved.

■ show crypto map (IPSec)