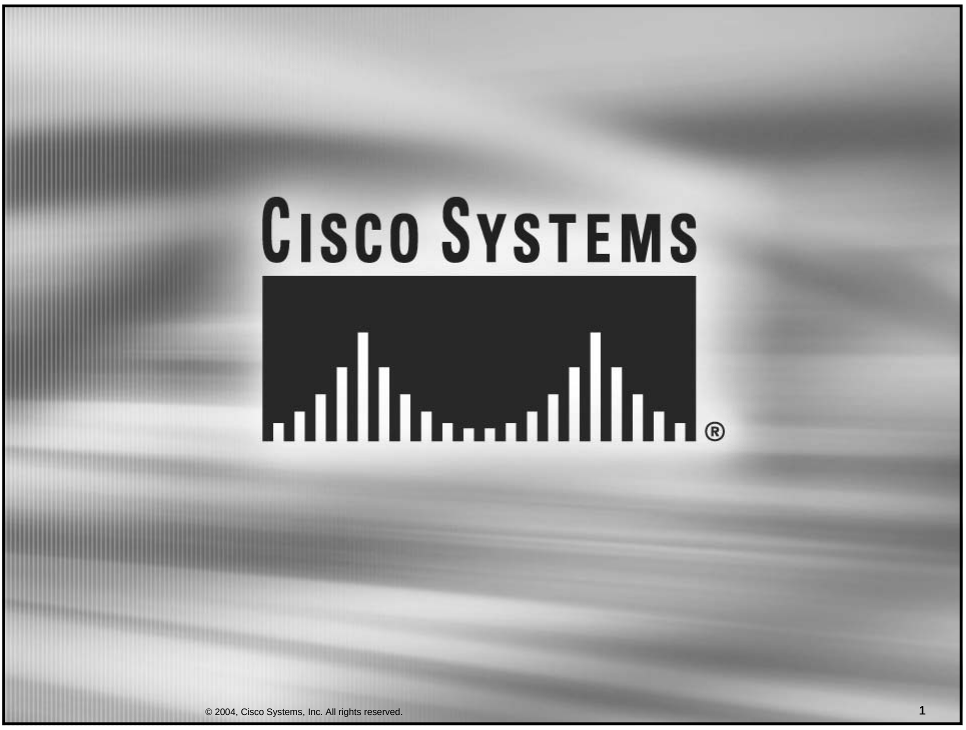
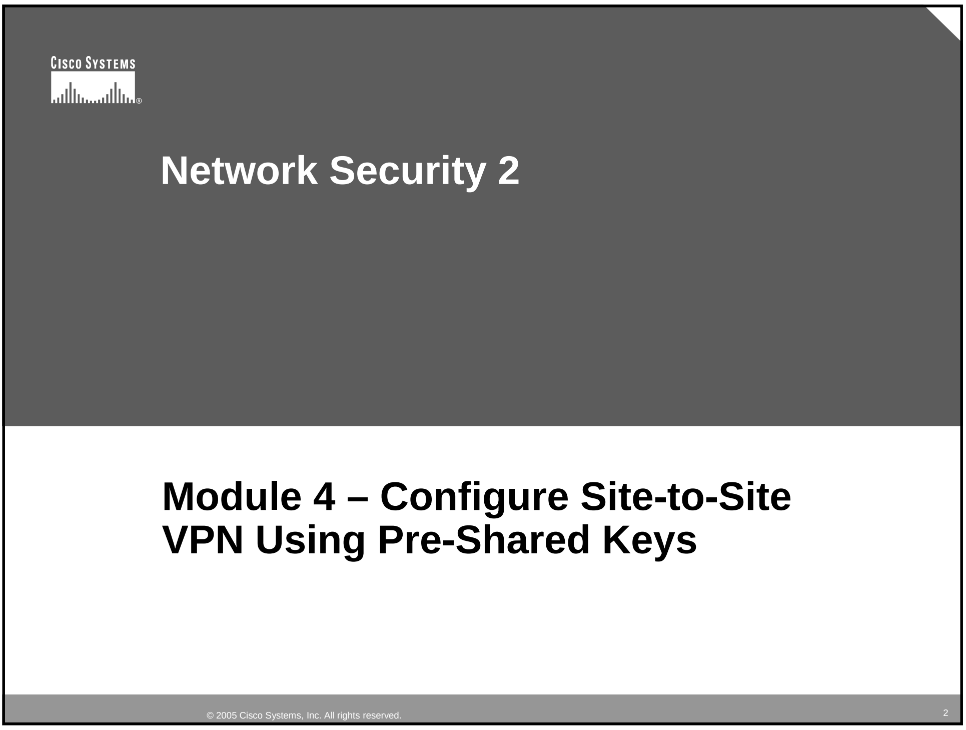


CISCO SYSTEMS

1

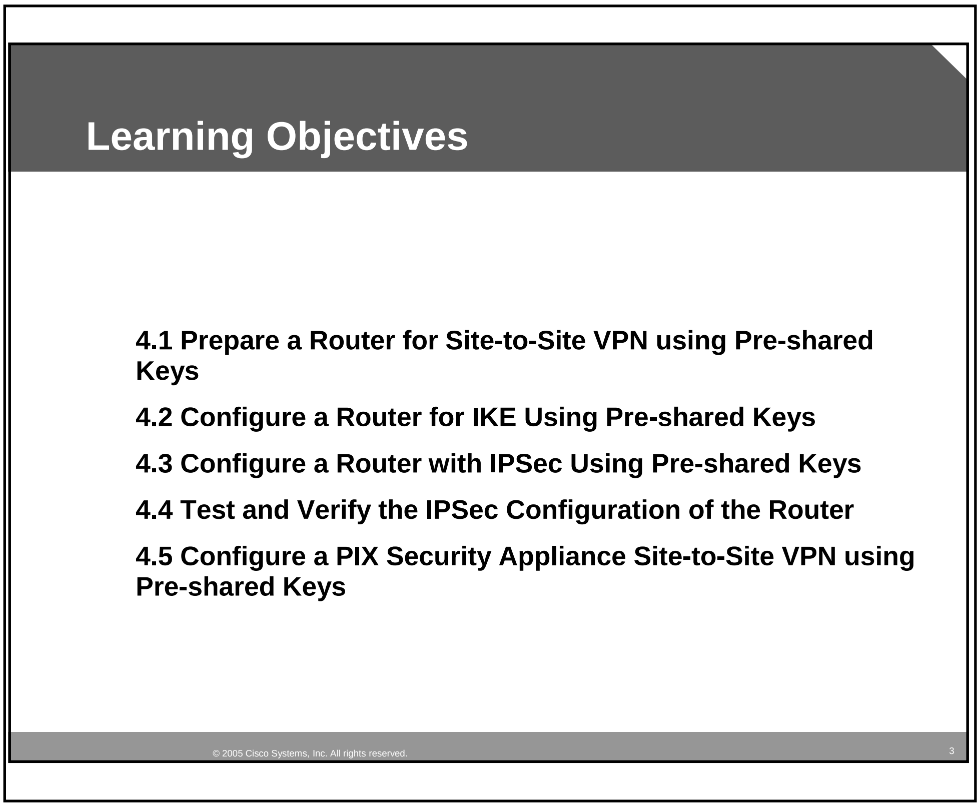


CISCO SYSTEMS

Network Security 2

Module 4 – Configure Site-to-Site VPN Using Pre-Shared Keys

2



Learning Objectives

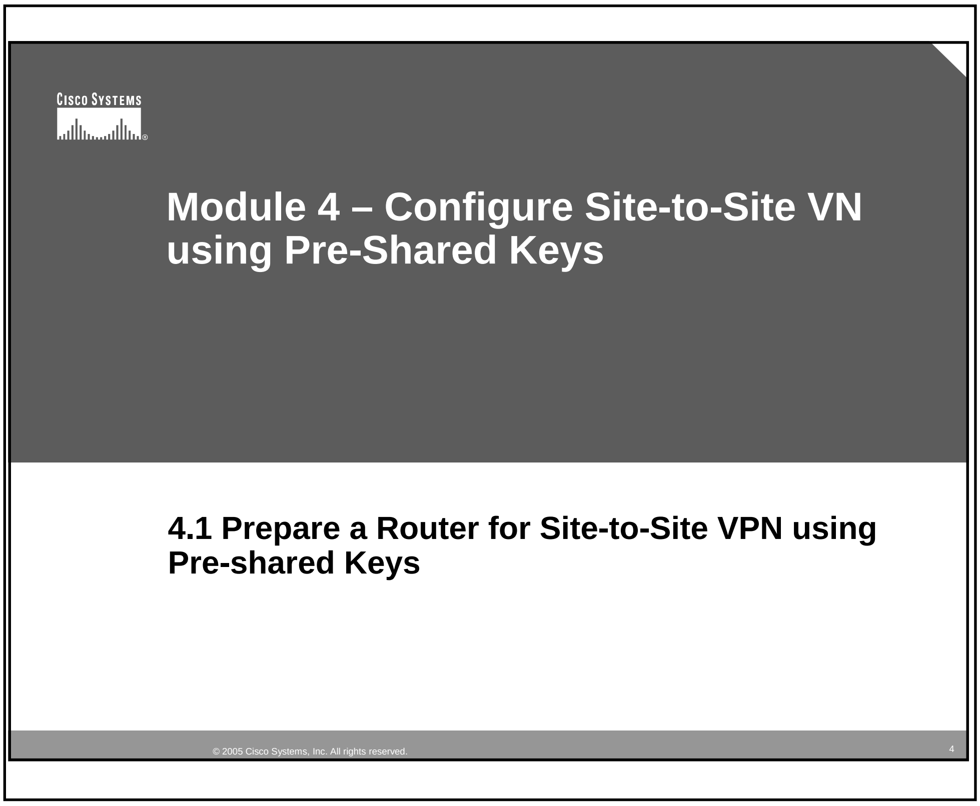
4.1 Prepare a Router for Site-to-Site VPN using Pre-shared Keys

4.2 Configure a Router for IKE Using Pre-shared Keys

4.3 Configure a Router with IPSec Using Pre-shared Keys

4.4 Test and Verify the IPSec Configuration of the Router

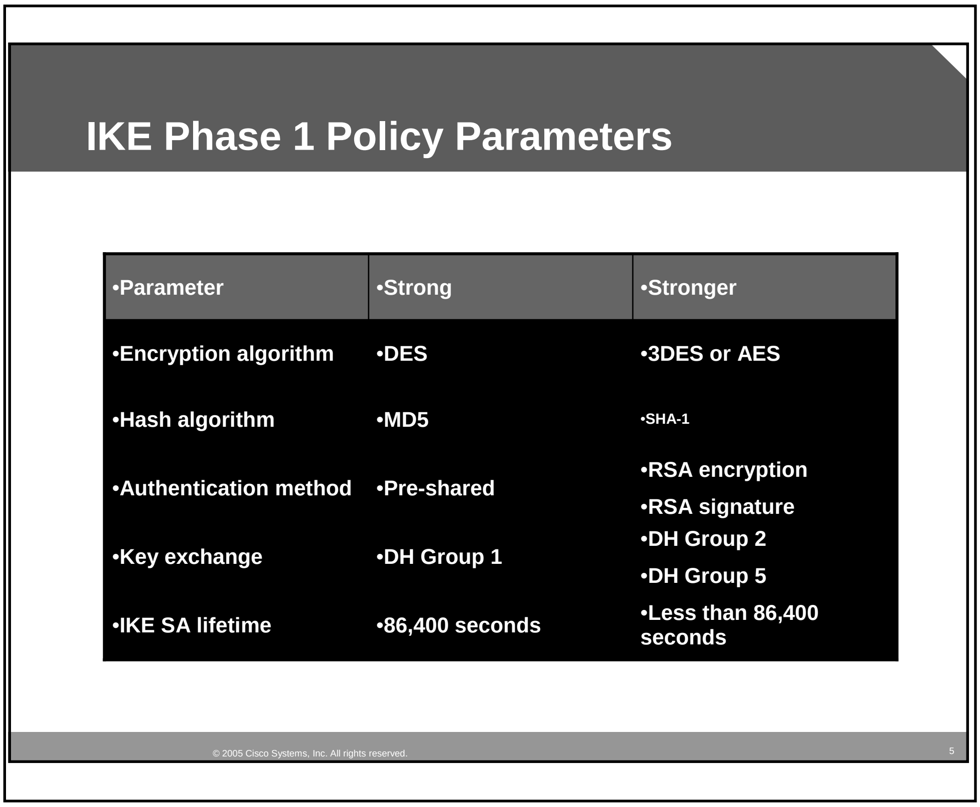
4.5 Configure a PIX Security Appliance Site-to-Site VPN using Pre-shared Keys



CISCO SYSTEMS

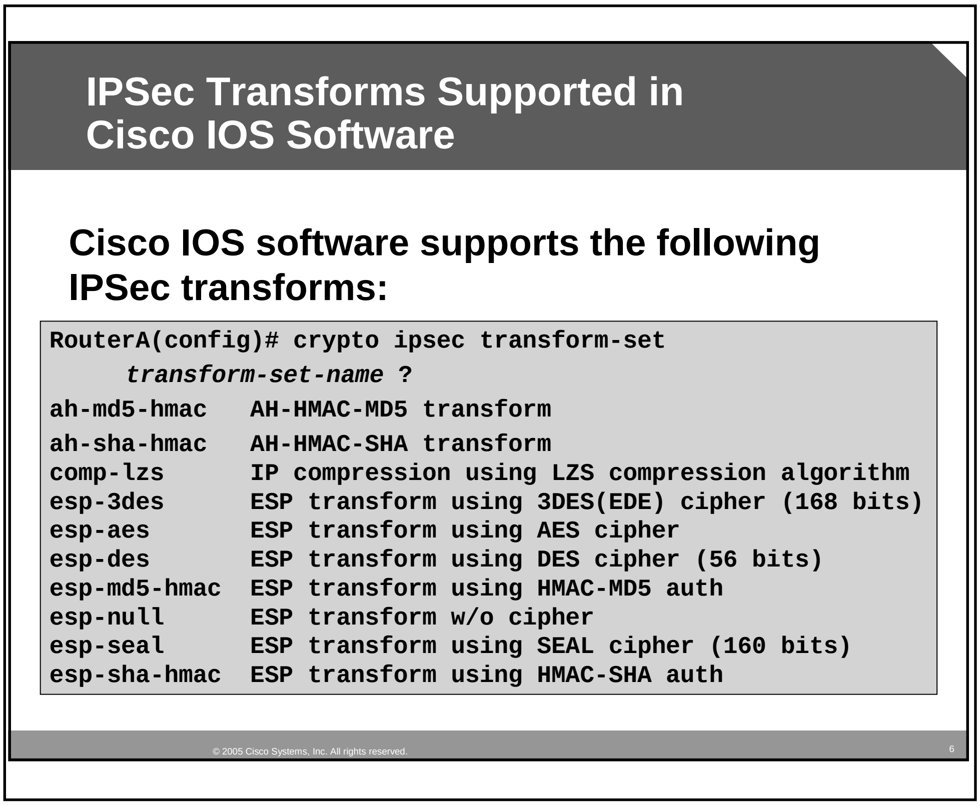
Module 4 – Configure Site-to-Site VN using Pre-Shared Keys

4.1 Prepare a Router for Site-to-Site VPN using Pre-shared Keys



IKE Phase 1 Policy Parameters

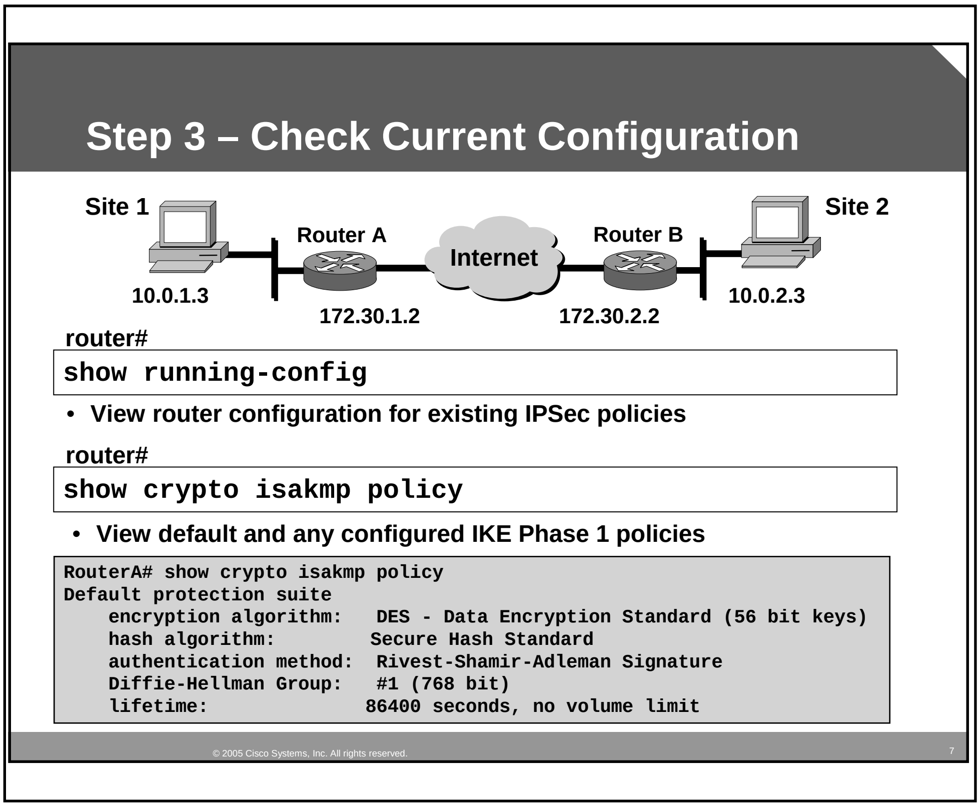
•Parameter	•Strong	•Stronger
•Encryption algorithm	•DES	•3DES or AES
•Hash algorithm	•MD5	•SHA-1
•Authentication method	•Pre-shared	•RSA encryption •RSA signature
•Key exchange	•DH Group 1	•DH Group 2 •DH Group 5
•IKE SA lifetime	•86,400 seconds	•Less than 86,400 seconds



IPSec Transforms Supported in Cisco IOS Software

Cisco IOS software supports the following IPSec transforms:

```
RouterA(config)# crypto ipsec transform-set
     transform-set-name ?
ah-md5-hmac   AH-HMAC-MD5 transform
ah-sha-hmac   AH-HMAC-SHA transform
comp-lzs      IP compression using LZS compression algorithm
esp-3des      ESP transform using 3DES(EDE) cipher (168 bits)
esp-aes       ESP transform using AES cipher
esp-des       ESP transform using DES cipher (56 bits)
esp-md5-hmac  ESP transform using HMAC-MD5 auth
esp-null      ESP transform w/o cipher
esp-seal      ESP transform using SEAL cipher (160 bits)
esp-sha-hmac  ESP transform using HMAC-SHA auth
```



Step 3 – Check Current Configuration

router#

```
show running-config
```

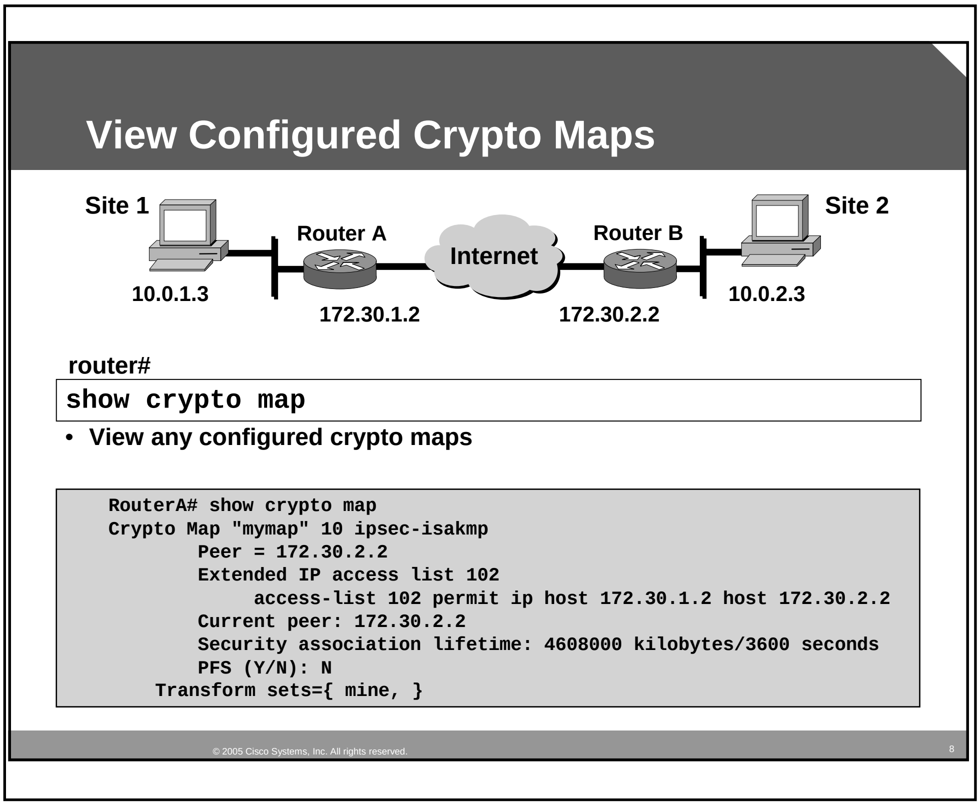
- View router configuration for existing IPSec policies

router#

```
show crypto isakmp policy
```

- View default and any configured IKE Phase 1 policies

```
RouterA# show crypto isakmp policy
Default protection suite
    encryption algorithm:   DES - Data Encryption Standard (56 bit keys)
    hash algorithm:        Secure Hash Standard
    authentication method:  Rivest-Shamir-Adleman Signature
    Diffie-Hellman Group:   #1 (768 bit)
    lifetime:             86400 seconds, no volume limit
```



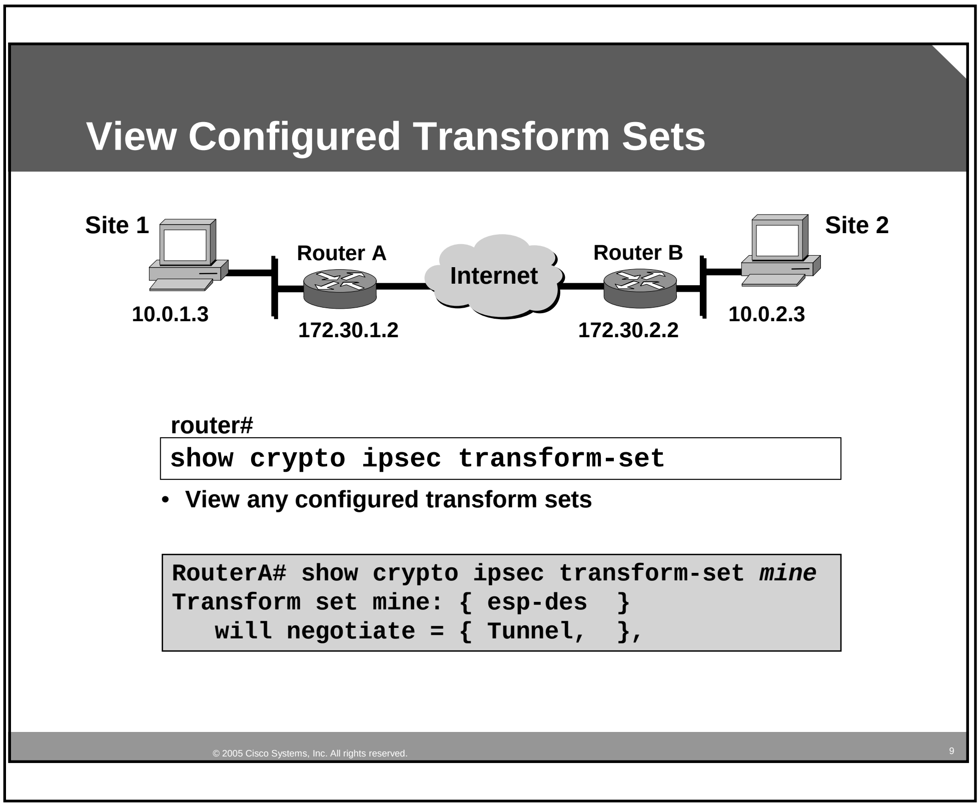
View Configured Crypto Maps

router#

```
show crypto map
```

- View any configured crypto maps

```
    RouterA# show crypto map
    Crypto Map "mymap" 10 ipsec-isakmp
            Peer = 172.30.2.2
            Extended IP access list 102
                 access-list 102 permit ip host 172.30.1.2 host 172.30.2.2
            Current peer: 172.30.2.2
            Security association lifetime: 4608000 kilobytes/3600 seconds
            PFS (Y/N): N
        Transform sets={ mine, }
```



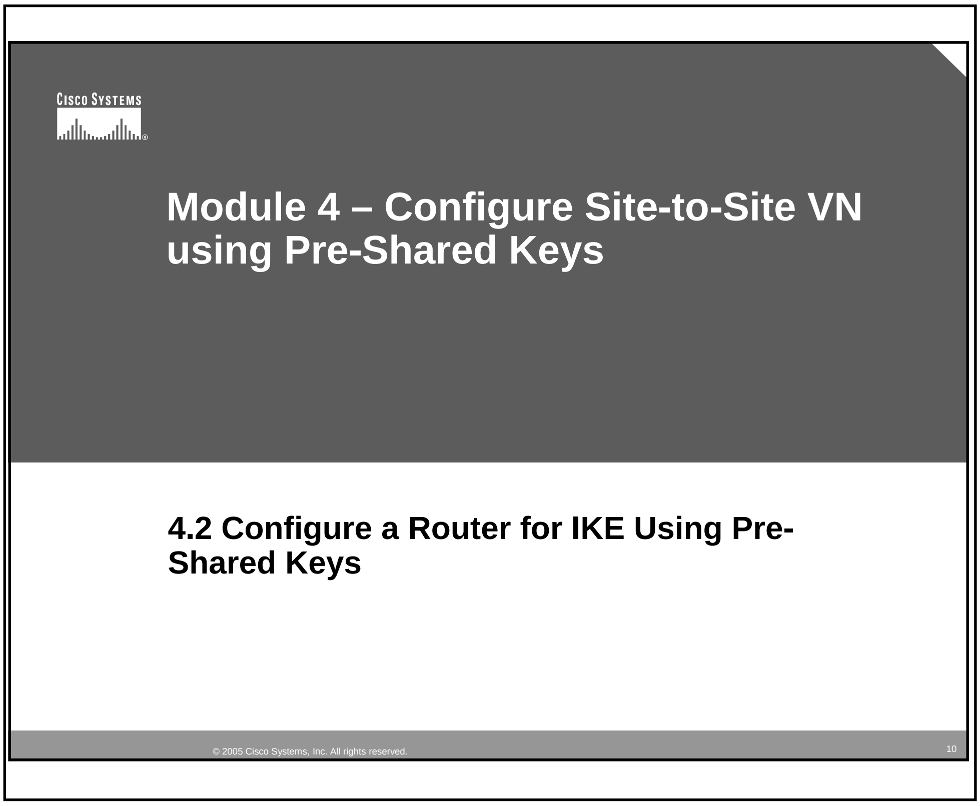
View Configured Transform Sets

router#

```
show crypto ipsec transform-set
```

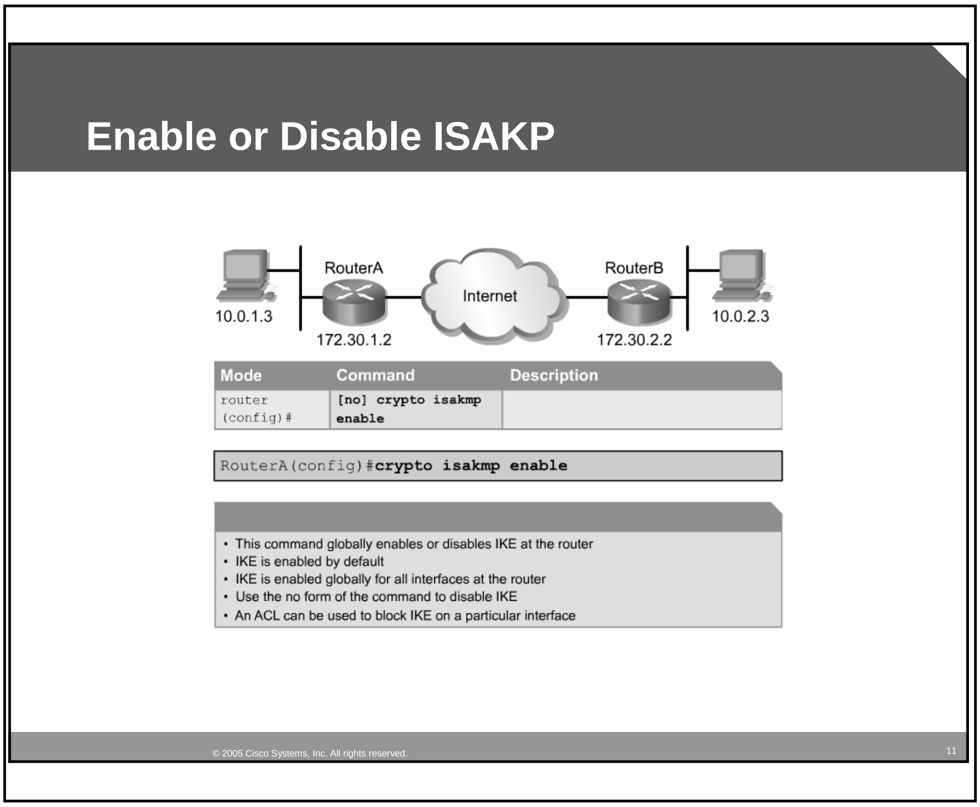
- View any configured transform sets

```
RouterA# show crypto ipsec transform-set mine
Transform set mine: { esp-des  }
   will negotiate = { Tunnel,  },
```



Module 4 – Configure Site-to-Site VN using Pre-Shared Keys

4.2 Configure a Router for IKE Using Pre-Shared Keys

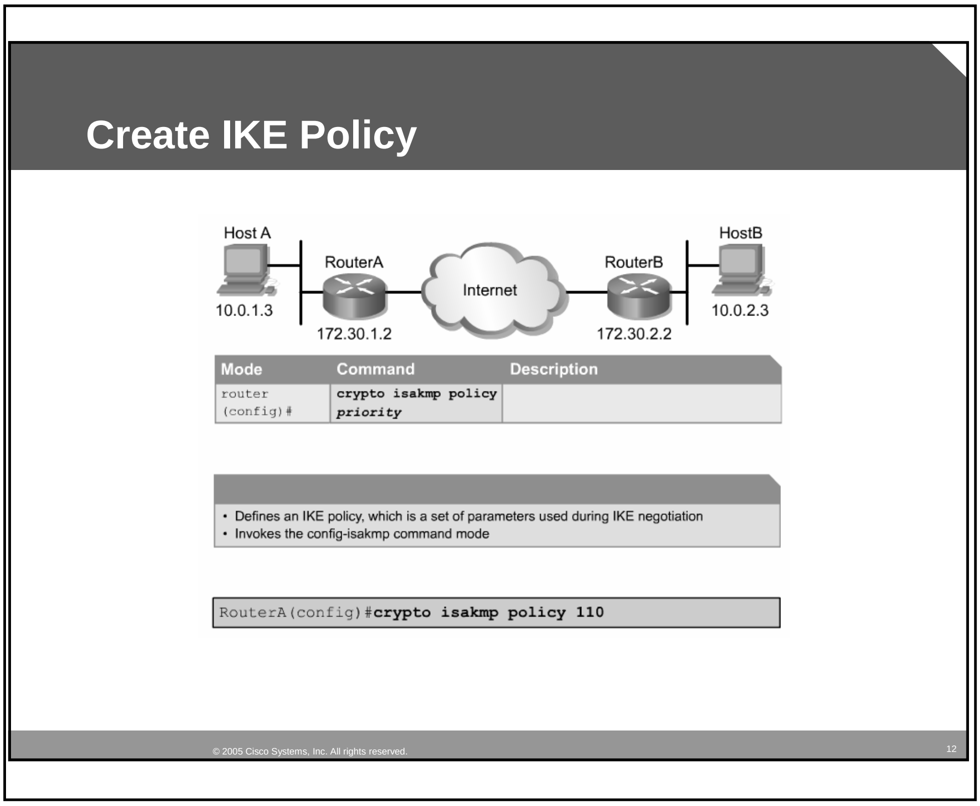

10.0.1.3
RouterA
172.30.1.2
Internet
RouterB
172.30.2.2
10.0.2.3

Enable or Disable ISAKP

Mode	Command	Description
router (config)#	**[no] crypto isakmp enable**	

```
RouterA(config)#crypto isakmp enable
```

- This command globally enables or disables IKE at the router
- IKE is enabled by default
- IKE is enabled globally for all interfaces at the router
- Use the no form of the command to disable IKE
- An ACL can be used to block IKE on a particular interface

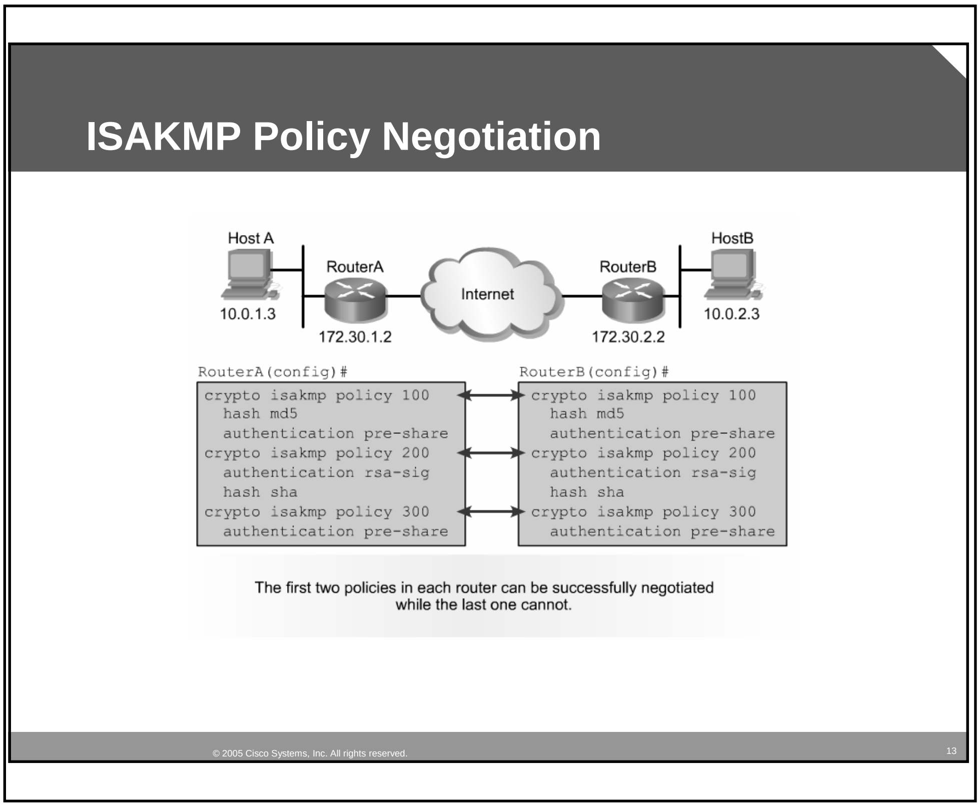

Host A
10.0.1.3
RouterA
172.30.1.2
Internet
RouterB
172.30.2.2
HostB
10.0.2.3

Create IKE Policy

Mode	Command	Description
router (config)#	**crypto isakmp policy *priority***	

- Defines an IKE policy, which is a set of parameters used during IKE negotiation
- Invokes the config-isakmp command mode

```
RouterA(config)#crypto isakmp policy 110
```

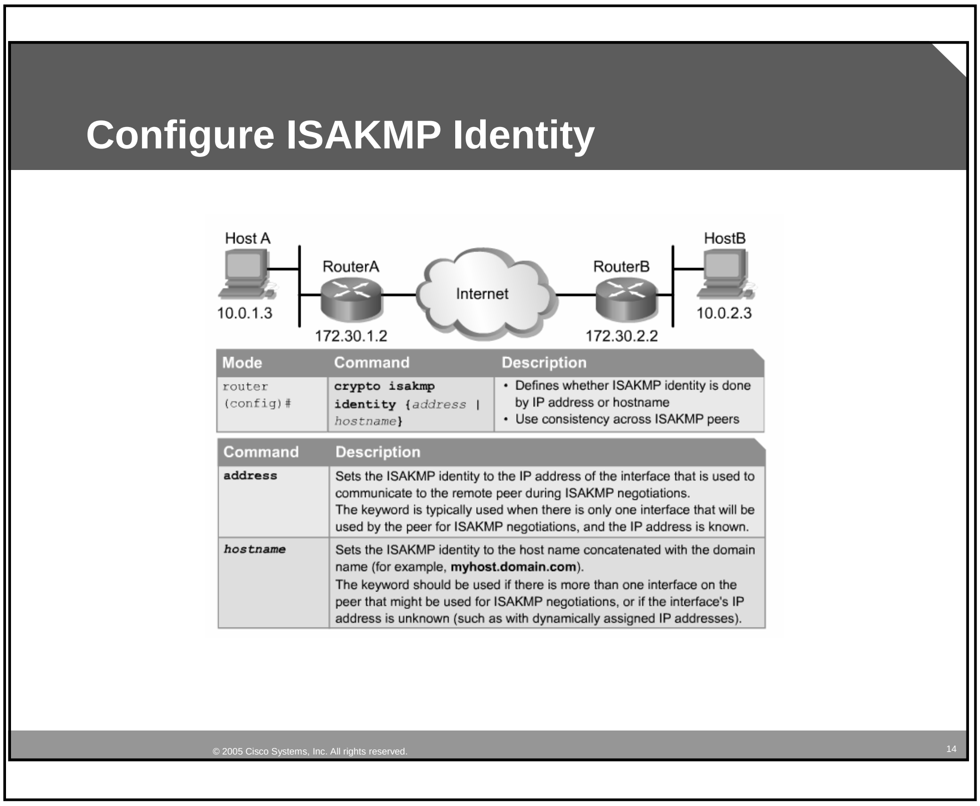


ISAKMP Policy Negotiation

```
RouterA(config)#
crypto isakmp policy 100
  hash md5
  authentication pre-share
crypto isakmp policy 200
  authentication rsa-sig
  hash sha
crypto isakmp policy 300
  authentication pre-share
```

```
RouterB(config)#
crypto isakmp policy 100
  hash md5
  authentication pre-share
crypto isakmp policy 200
  authentication rsa-sig
  hash sha
crypto isakmp policy 300
  authentication pre-share
```

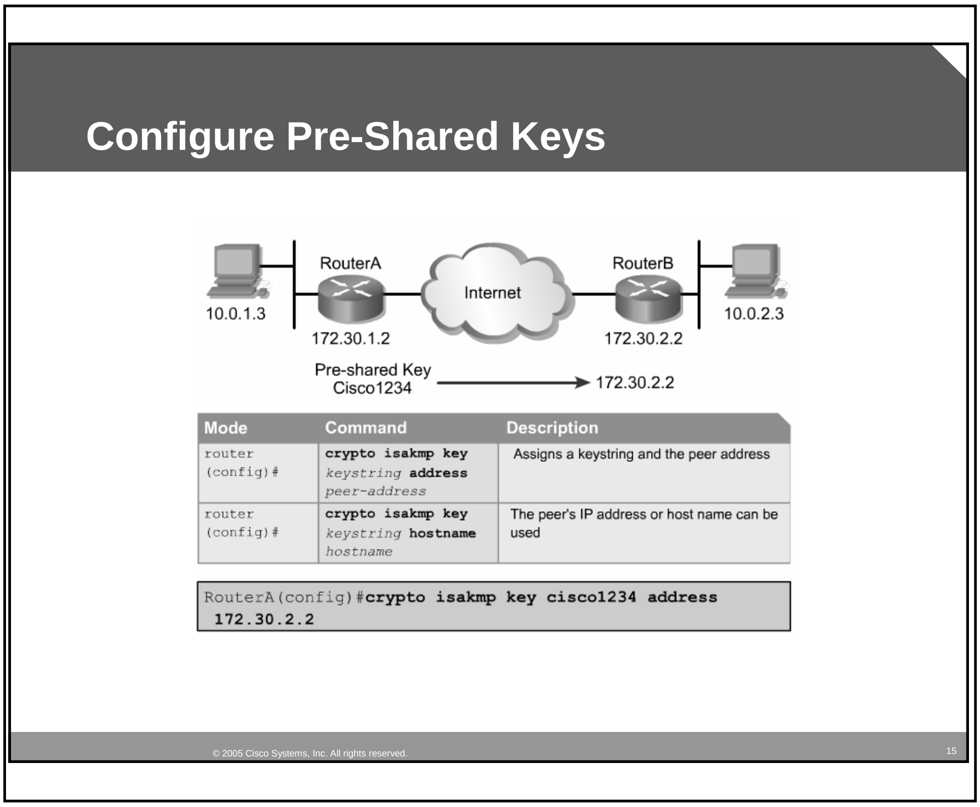
The first two policies in each router can be successfully negotiated while the last one cannot.



Configure ISAKMP Identity

Mode	Command	Description
router (config)#	**crypto isakmp identity** {*address* | *hostname*}	• Defines whether ISAKMP identity is done by IP address or hostname • Use consistency across ISAKMP peers

Command	Description
address	Sets the ISAKMP identity to the IP address of the interface that is used to communicate to the remote peer during ISAKMP negotiations. The keyword is typically used when there is only one interface that will be used by the peer for ISAKMP negotiations, and the IP address is known.
hostname	Sets the ISAKMP identity to the host name concatenated with the domain name (for example, **myhost.domain.com**). The keyword should be used if there is more than one interface on the peer that might be used for ISAKMP negotiations, or if the interface's IP address is unknown (such as with dynamically assigned IP addresses).

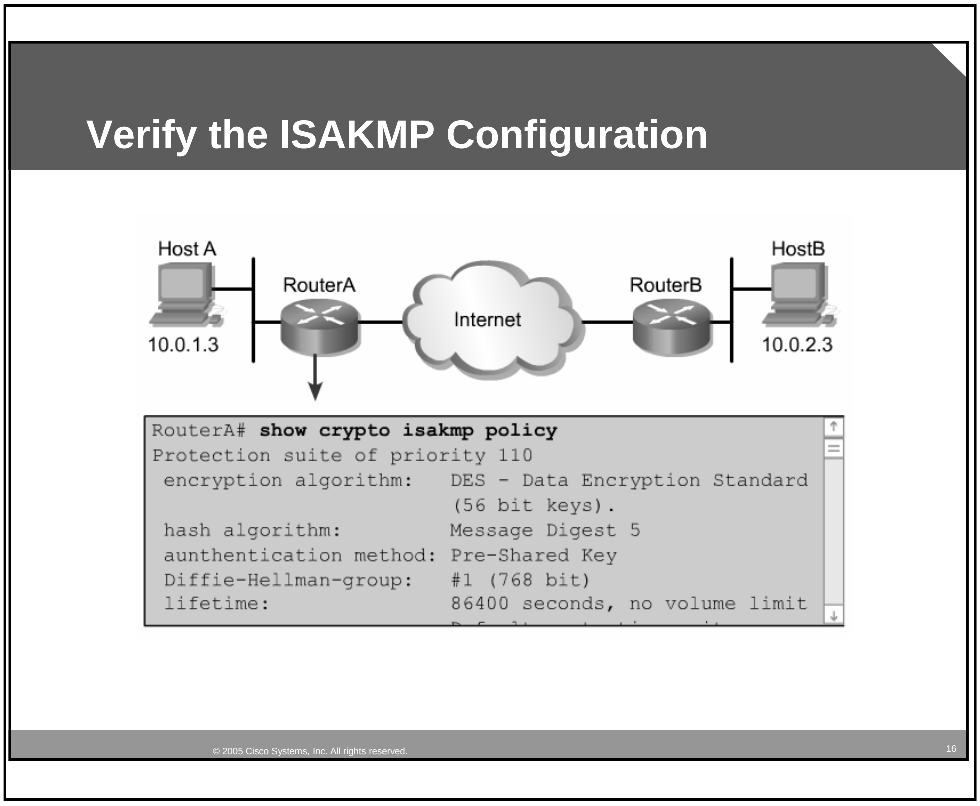


Configure Pre-Shared Keys

Mode	Command	Description
router (config)#	**crypto isakmp key** *keystring* **address** *peer-address*	Assigns a keystring and the peer address
router (config)#	**crypto isakmp key** *keystring* **hostname** *hostname*	The peer's IP address or host name can be used

```
RouterA(config)#crypto isakmp key cisco1234 address
 172.30.2.2
```

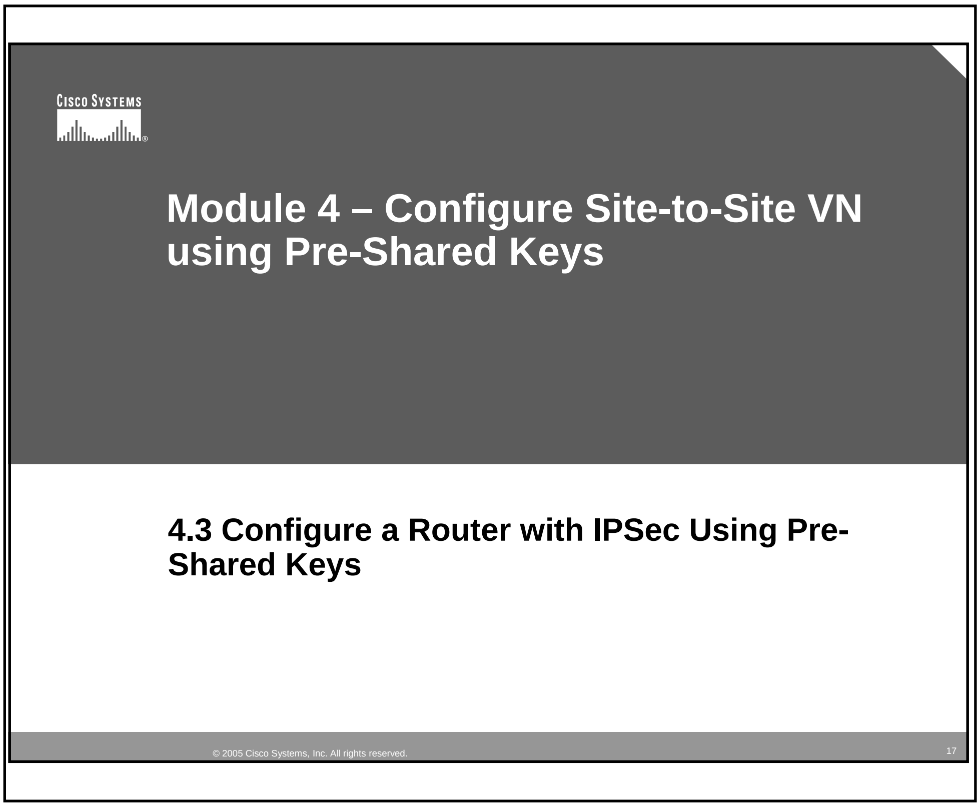
© 2005 Cisco Systems, Inc. All rights reserved. 15



Verify the ISAKMP Configuration

```
RouterA# show crypto isakmp policy
Protection suite of priority 110
 encryption algorithm:   DES - Data Encryption Standard
                         (56 bit keys).
 hash algorithm:         Message Digest 5
 aunthentication method: Pre-Shared Key
 Diffie-Hellman-group:   #1 (768 bit)
 lifetime:               86400 seconds, no volume limit
```

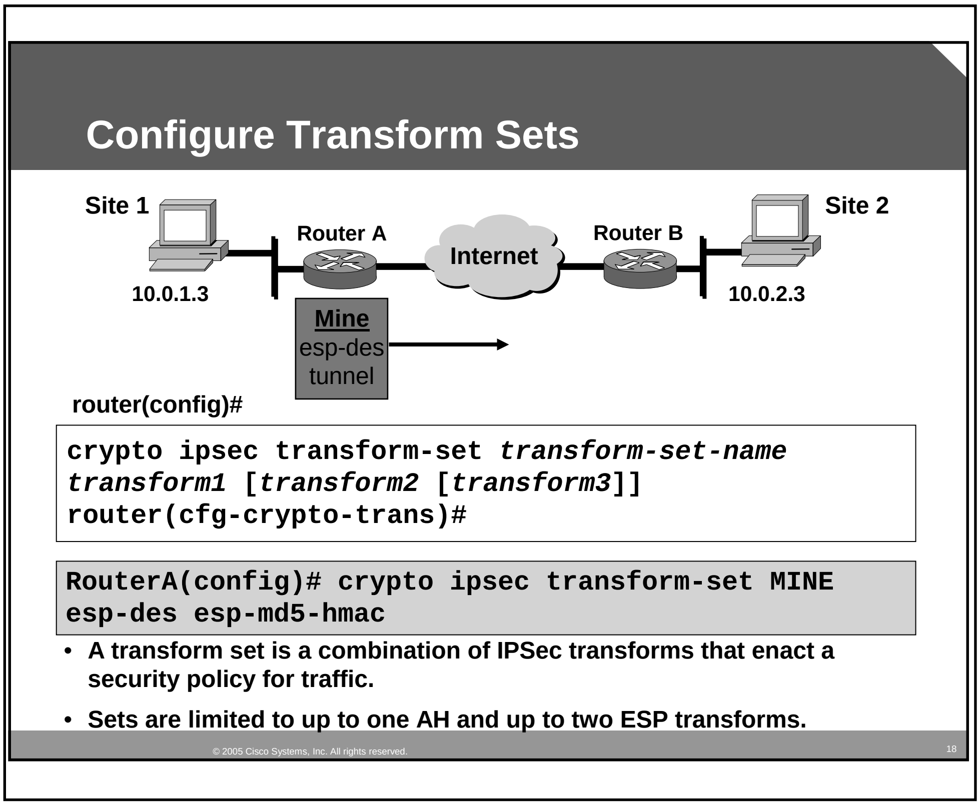
© 2005 Cisco Systems, Inc. All rights reserved. 16



CISCO SYSTEMS

Module 4 – Configure Site-to-Site VN using Pre-Shared Keys

4.3 Configure a Router with IPSec Using Pre-Shared Keys



Configure Transform Sets

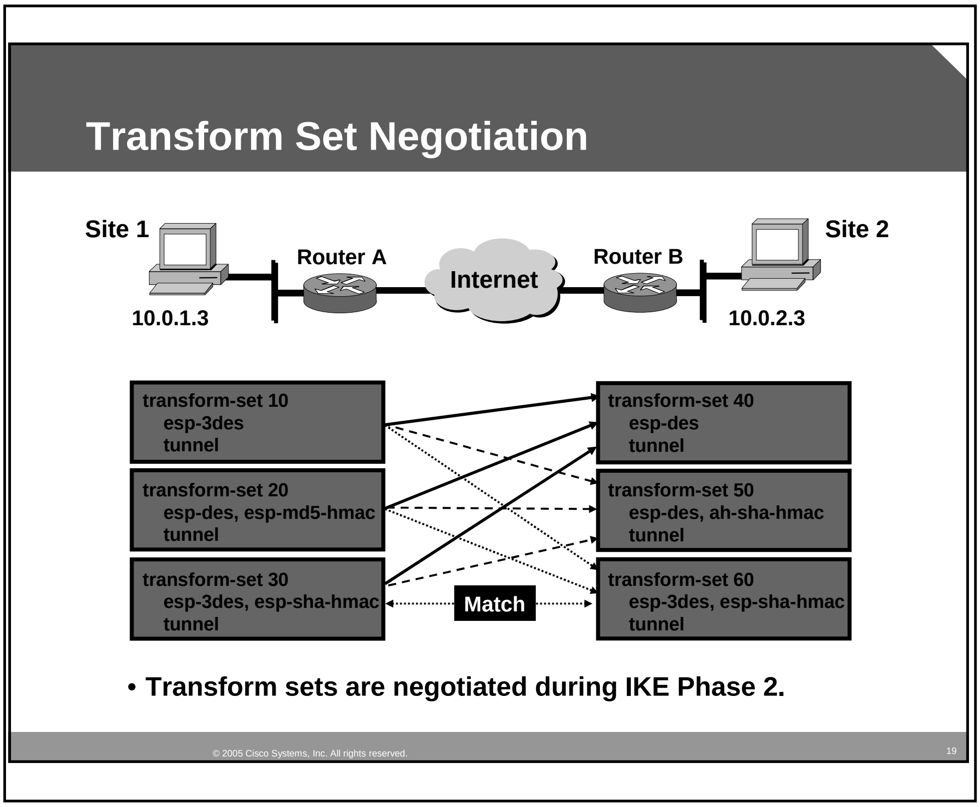
Site 1
Router A
Internet
Router B
Site 2
10.0.1.3
10.0.2.3
Mine
esp-des
tunnel

router(config)#

```
crypto ipsec transform-set transform-set-name
transform1 [transform2 [transform3]]
router(cfg-crypto-trans)#
```

```
RouterA(config)# crypto ipsec transform-set MINE
esp-des esp-md5-hmac
```

- A transform set is a combination of IPSec transforms that enact a security policy for traffic.
- Sets are limited to up to one AH and up to two ESP transforms.



Transform Set Negotiation

transform-set 10
esp-3des
tunnel

transform-set 20
esp-des, esp-md5-hmac
tunnel

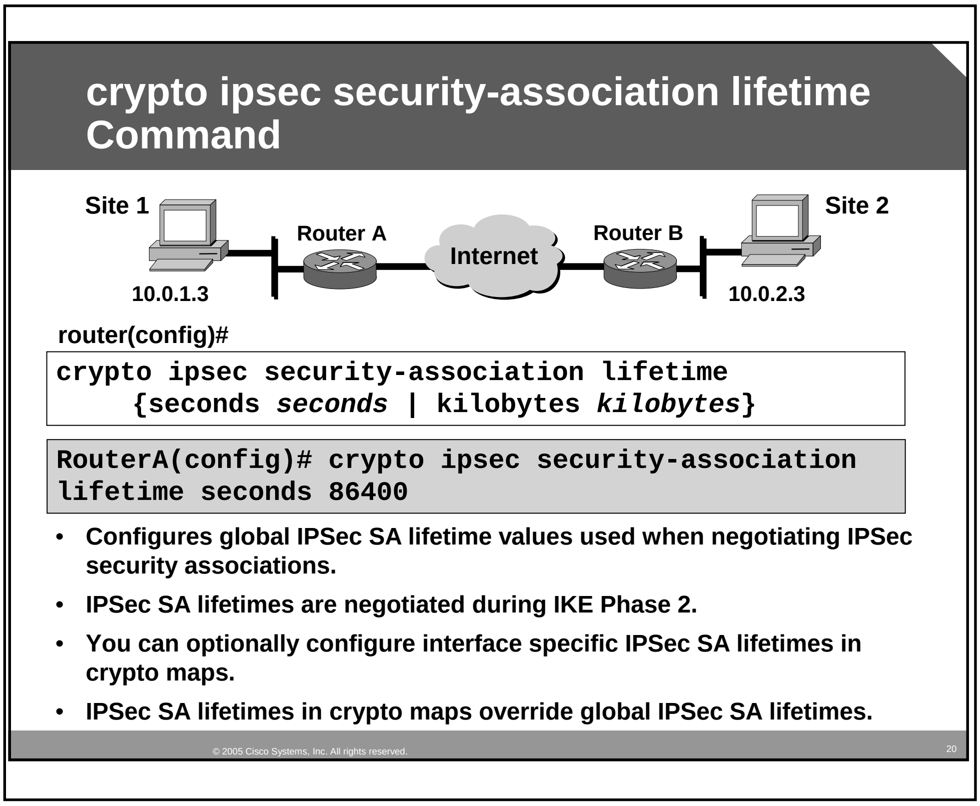
transform-set 30
esp-3des, esp-sha-hmac
tunnel

transform-set 40
esp-des
tunnel

transform-set 50
esp-des, ah-sha-hmac
tunnel

transform-set 60
esp-3des, esp-sha-hmac
tunnel

- Transform sets are negotiated during IKE Phase 2.



crypto ipsec security-association lifetime Command

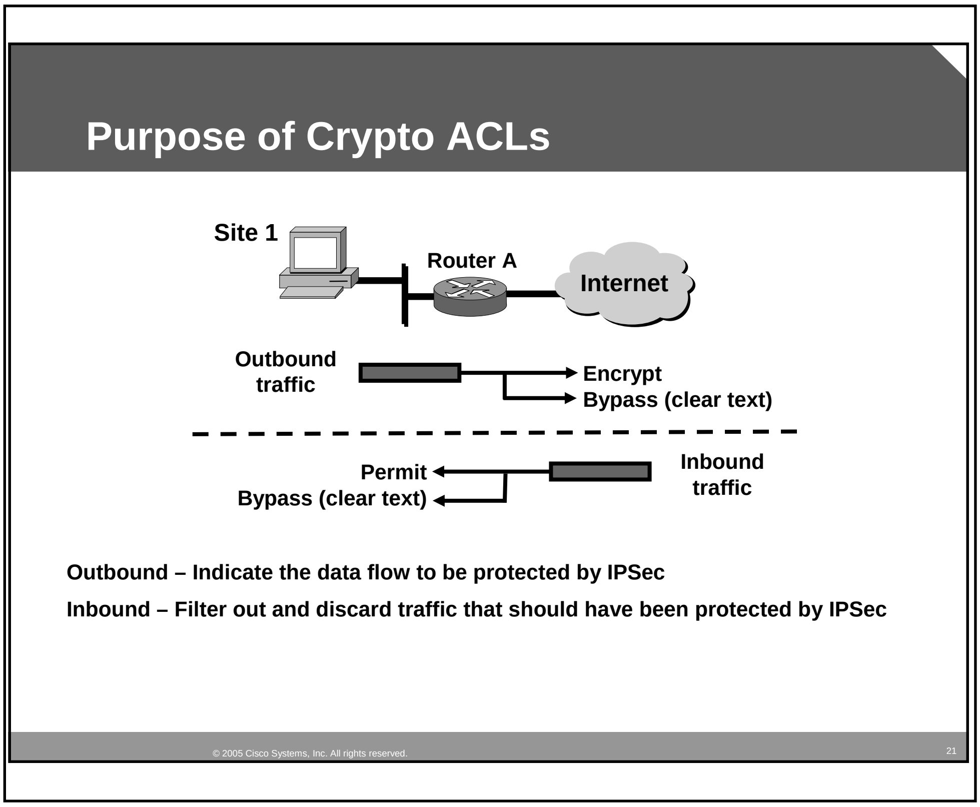
Site 1
Router A
Internet
Router B
Site 2
10.0.1.3
10.0.2.3

router(config)#

```
crypto ipsec security-association lifetime
    {seconds seconds | kilobytes kilobytes}
```

```
RouterA(config)# crypto ipsec security-association
lifetime seconds 86400
```

- Configures global IPSec SA lifetime values used when negotiating IPSec security associations.
- IPSec SA lifetimes are negotiated during IKE Phase 2.
- You can optionally configure interface specific IPSec SA lifetimes in crypto maps.
- IPSec SA lifetimes in crypto maps override global IPSec SA lifetimes.

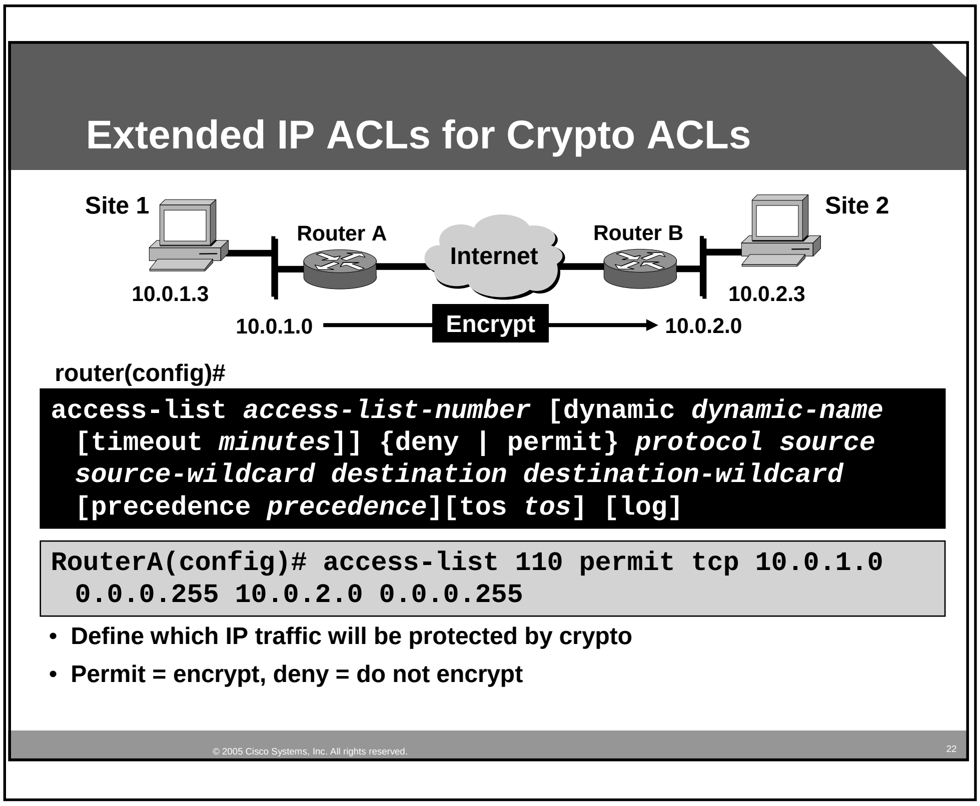


Purpose of Crypto ACLs

Outbound – Indicate the data flow to be protected by IPSec

Inbound – Filter out and discard traffic that should have been protected by IPSec

21



Extended IP ACLs for Crypto ACLs

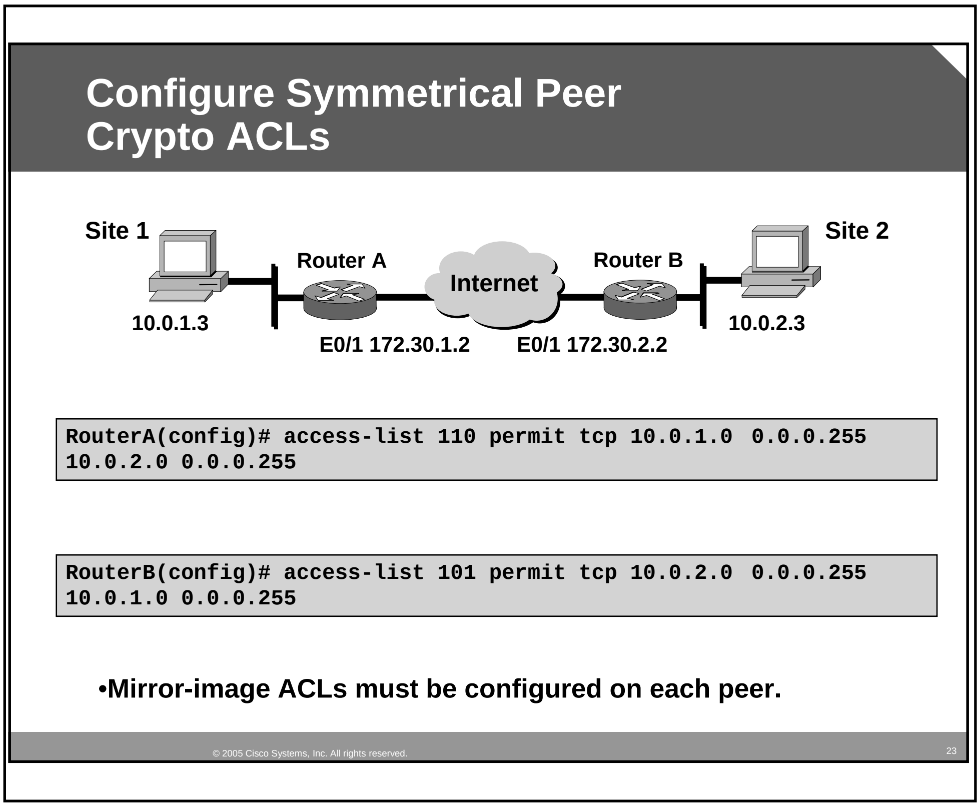
router(config)#

```
access-list access-list-number [dynamic dynamic-name
  [timeout minutes]] {deny | permit} protocol source
  source-wildcard destination destination-wildcard
  [precedence precedence][tos tos] [log]
```

```
RouterA(config)# access-list 110 permit tcp 10.0.1.0
  0.0.0.255 10.0.2.0 0.0.0.255
```

- Define which IP traffic will be protected by crypto
- Permit = encrypt, deny = do not encrypt

22



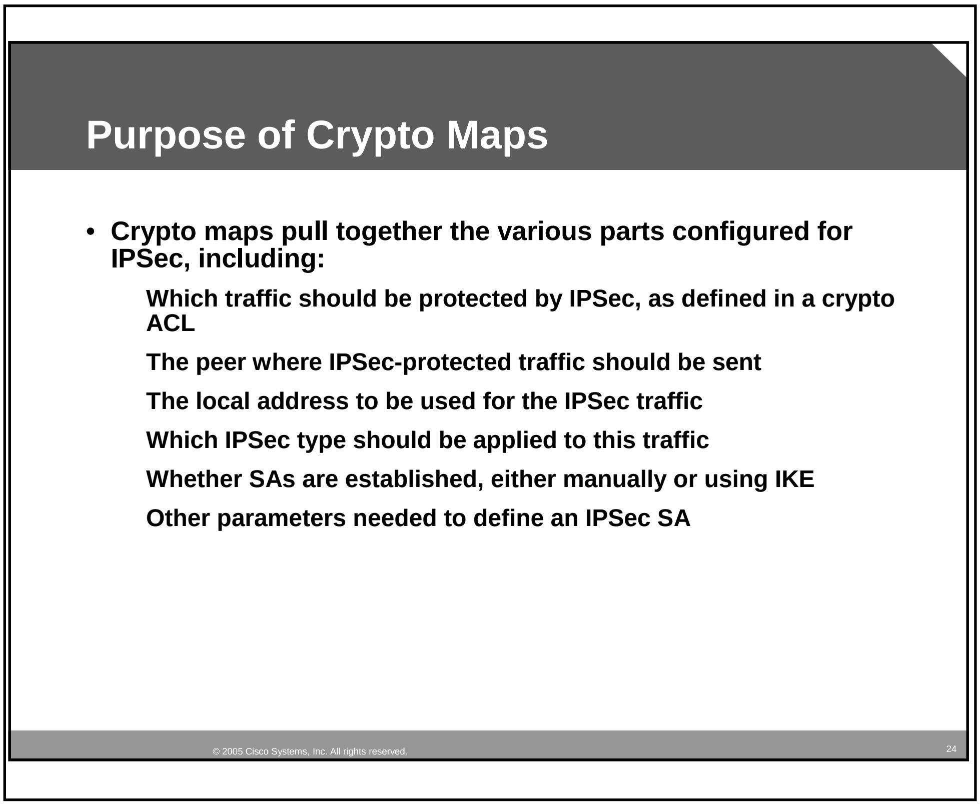
Configure Symmetrical Peer Crypto ACLs

```
RouterA(config)# access-list 110 permit tcp 10.0.1.0  0.0.0.255
10.0.2.0 0.0.0.255
```

```
RouterB(config)# access-list 101 permit tcp 10.0.2.0  0.0.0.255
10.0.1.0 0.0.0.255
```

•Mirror-image ACLs must be configured on each peer.

23



Purpose of Crypto Maps

- Crypto maps pull together the various parts configured for IPSec, including:

  Which traffic should be protected by IPSec, as defined in a crypto ACL

  The peer where IPSec-protected traffic should be sent

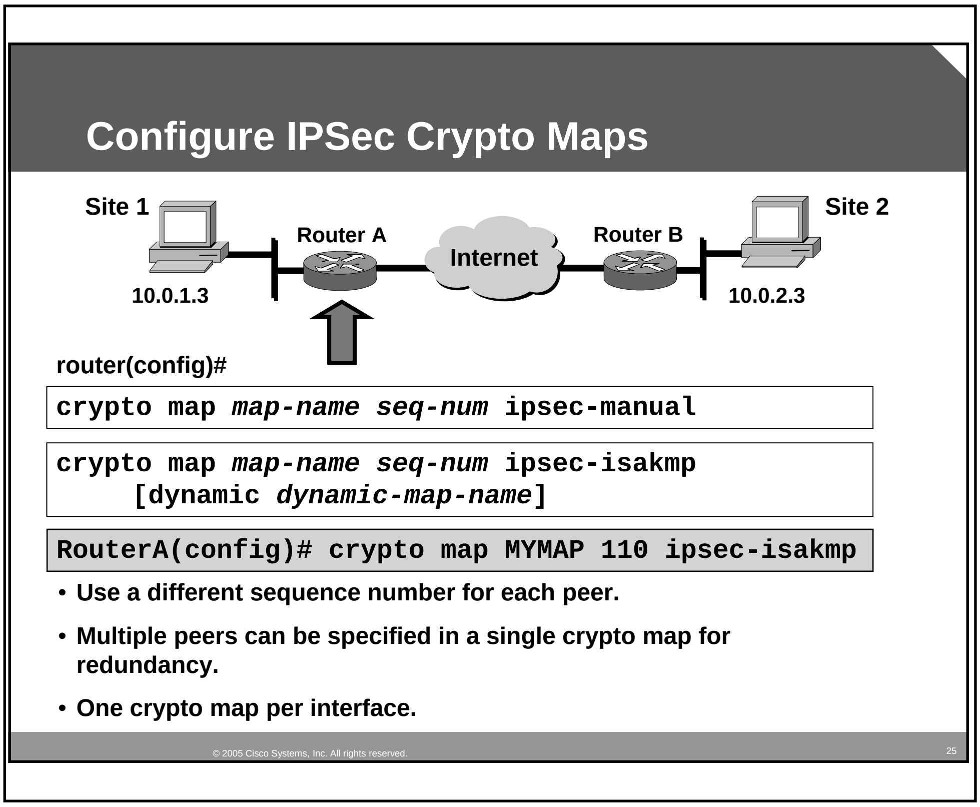
  The local address to be used for the IPSec traffic

  Which IPSec type should be applied to this traffic

  Whether SAs are established, either manually or using IKE

  Other parameters needed to define an IPSec SA

24



Configure IPSec Crypto Maps

Site 1

10.0.1.3

Router A

Internet

Router B

Site 2

10.0.2.3

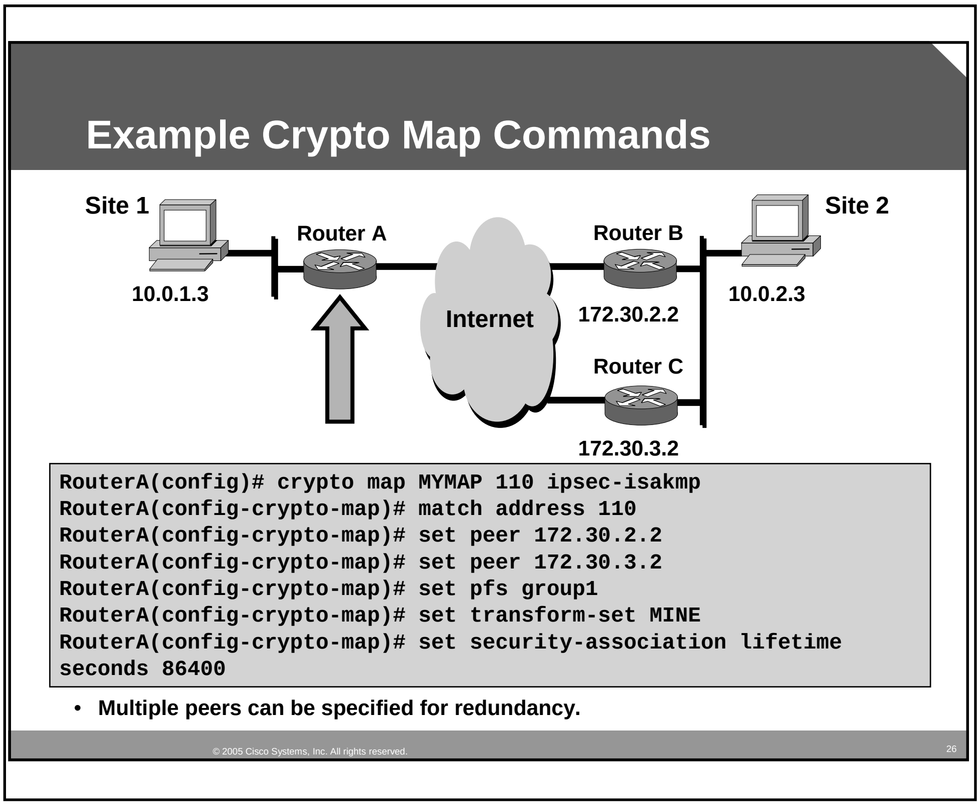
router(config)#

```
crypto map map-name seq-num ipsec-manual
```

```
crypto map map-name seq-num ipsec-isakmp
     [dynamic dynamic-map-name]
```

```
RouterA(config)# crypto map MYMAP 110 ipsec-isakmp
```

- Use a different sequence number for each peer.
- Multiple peers can be specified in a single crypto map for redundancy.
- One crypto map per interface.



Example Crypto Map Commands

Site 1

10.0.1.3

Router A

Internet

Router B

172.30.2.2

Router C

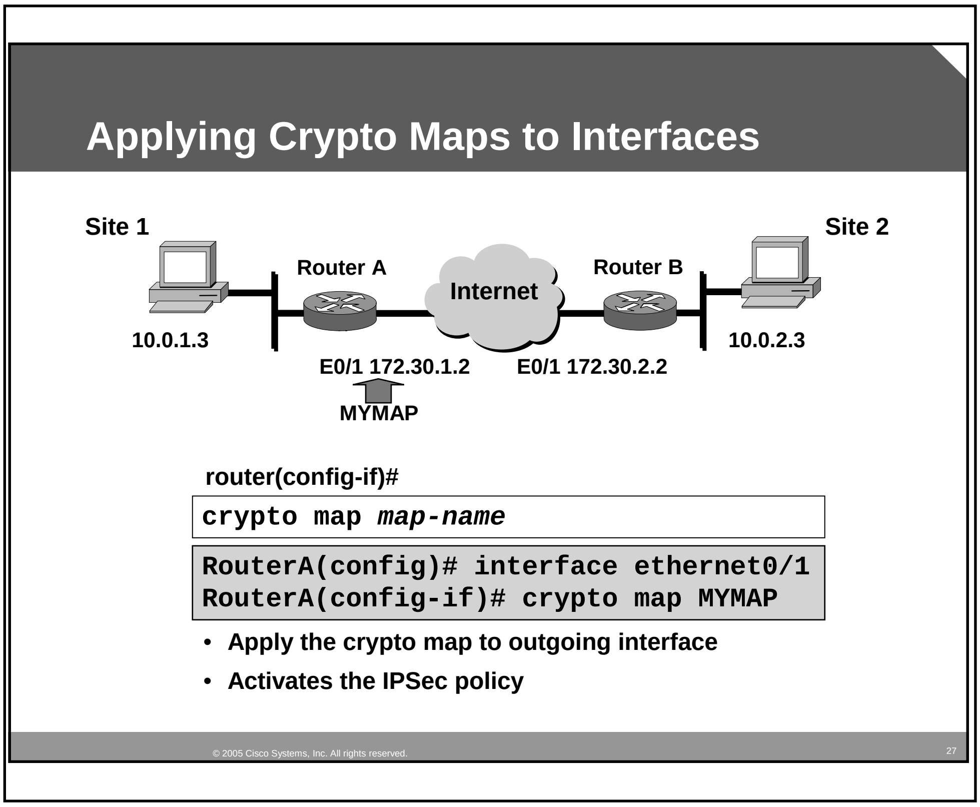
172.30.3.2

Site 2

10.0.2.3

```
RouterA(config)# crypto map MYMAP 110 ipsec-isakmp
RouterA(config-crypto-map)# match address 110
RouterA(config-crypto-map)# set peer 172.30.2.2
RouterA(config-crypto-map)# set peer 172.30.3.2
RouterA(config-crypto-map)# set pfs group1
RouterA(config-crypto-map)# set transform-set MINE
RouterA(config-crypto-map)# set security-association lifetime
seconds 86400
```

- Multiple peers can be specified for redundancy.



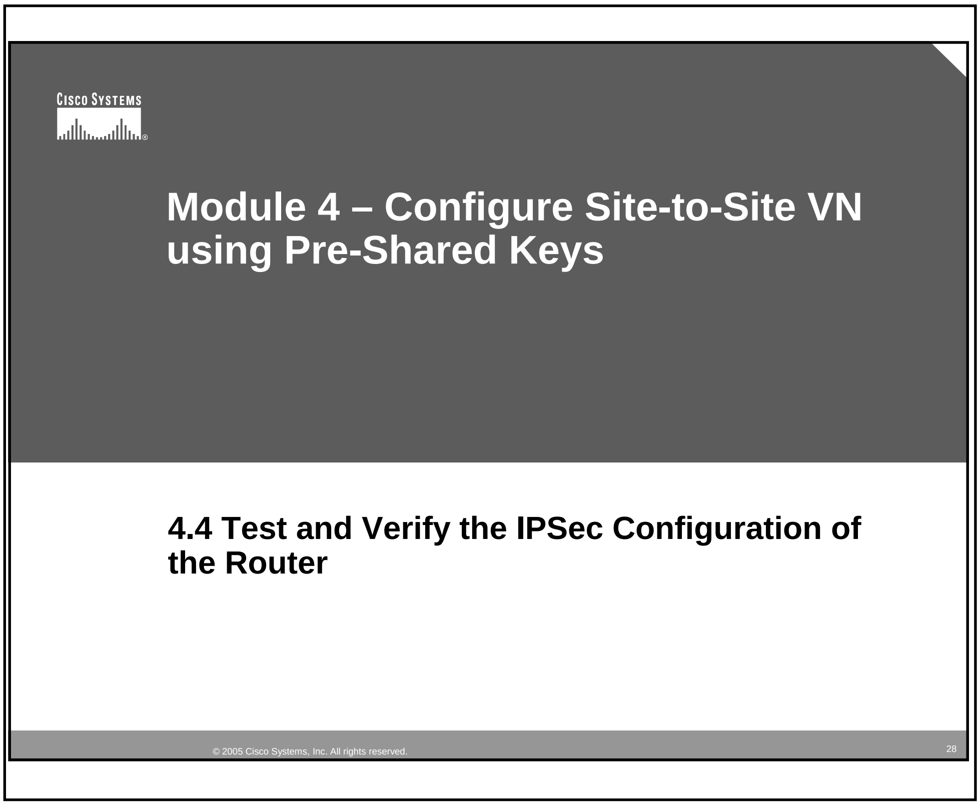
Applying Crypto Maps to Interfaces

router(config-if)#

```
crypto map map-name
```

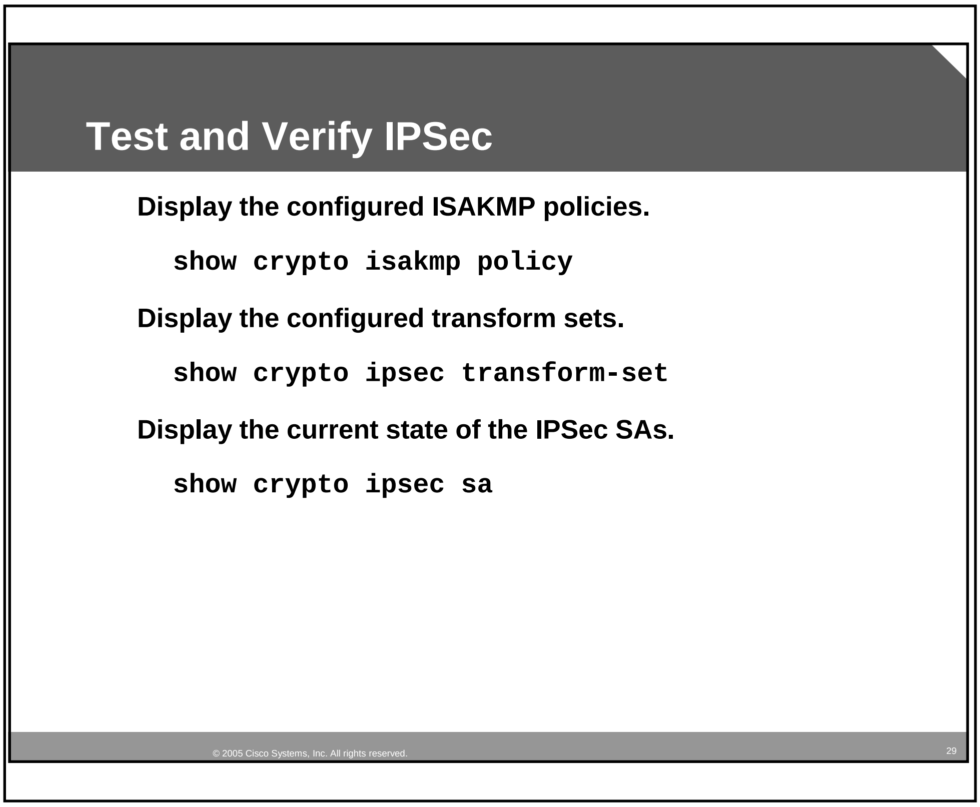
```
RouterA(config)# interface ethernet0/1
RouterA(config-if)# crypto map MYMAP
```

- Apply the crypto map to outgoing interface
- Activates the IPSec policy



Module 4 – Configure Site-to-Site VN using Pre-Shared Keys

4.4 Test and Verify the IPSec Configuration of the Router



Test and Verify IPSec

Display the configured ISAKMP policies.

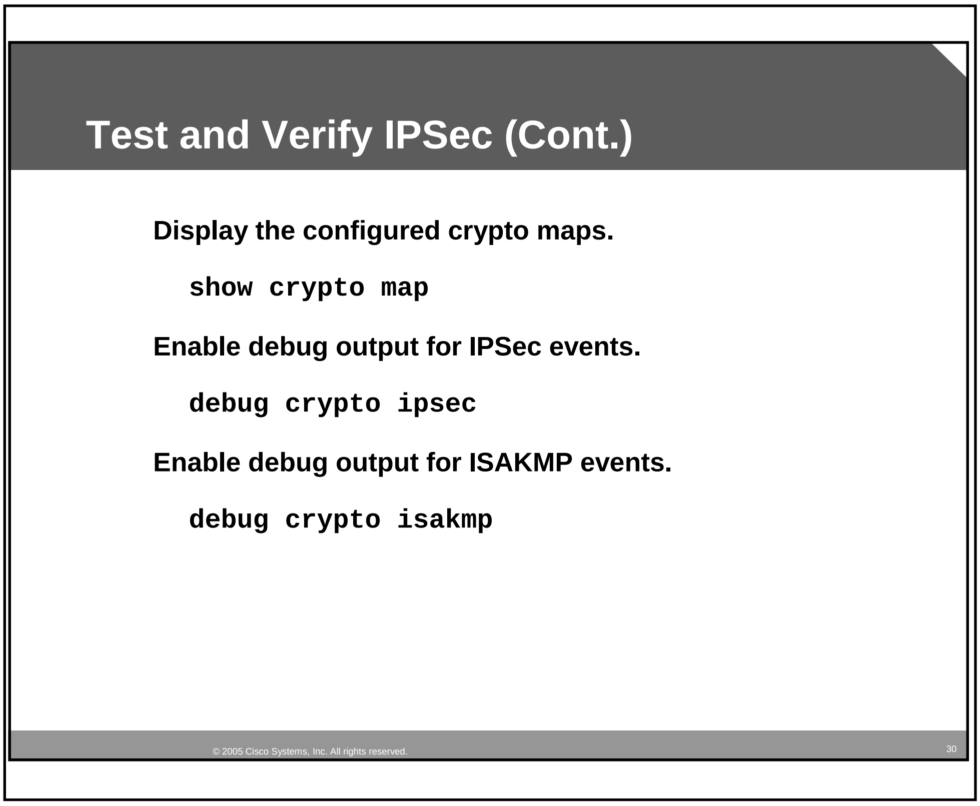
```
show crypto isakmp policy
```

Display the configured transform sets.

```
show crypto ipsec transform-set
```

Display the current state of the IPSec SAs.

```
show crypto ipsec sa
```



Test and Verify IPSec (Cont.)

Display the configured crypto maps.

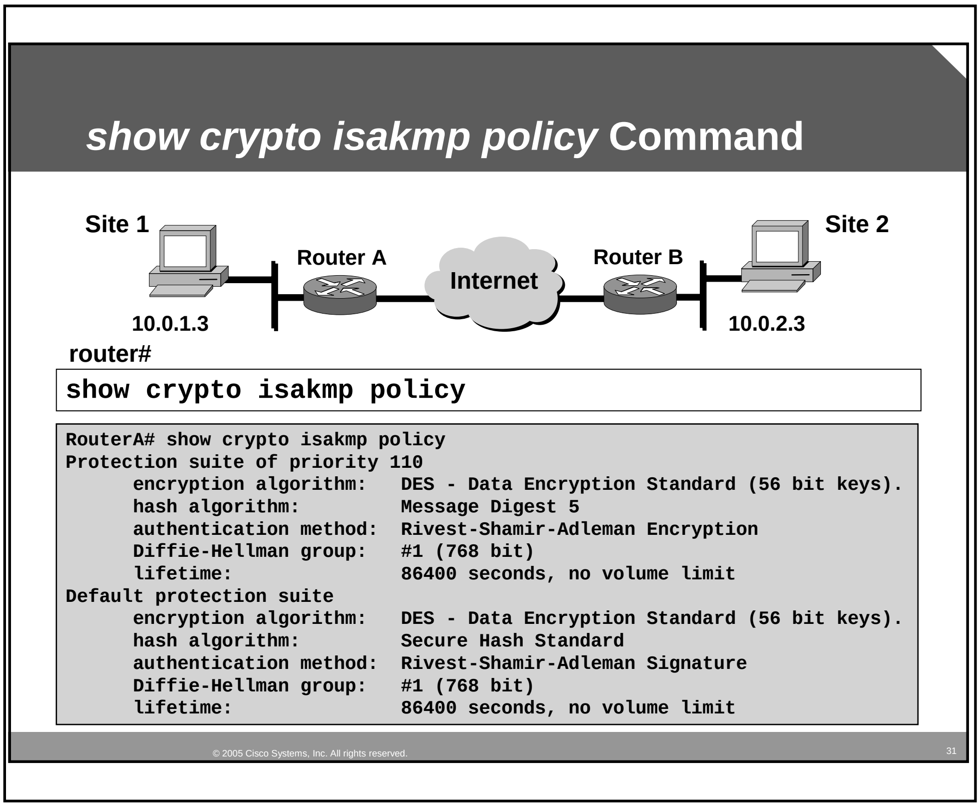
```
show crypto map
```

Enable debug output for IPSec events.

```
debug crypto ipsec
```

Enable debug output for ISAKMP events.

```
debug crypto isakmp
```



show crypto isakmp policy Command

Site 1 Site 2

Router A Internet Router B

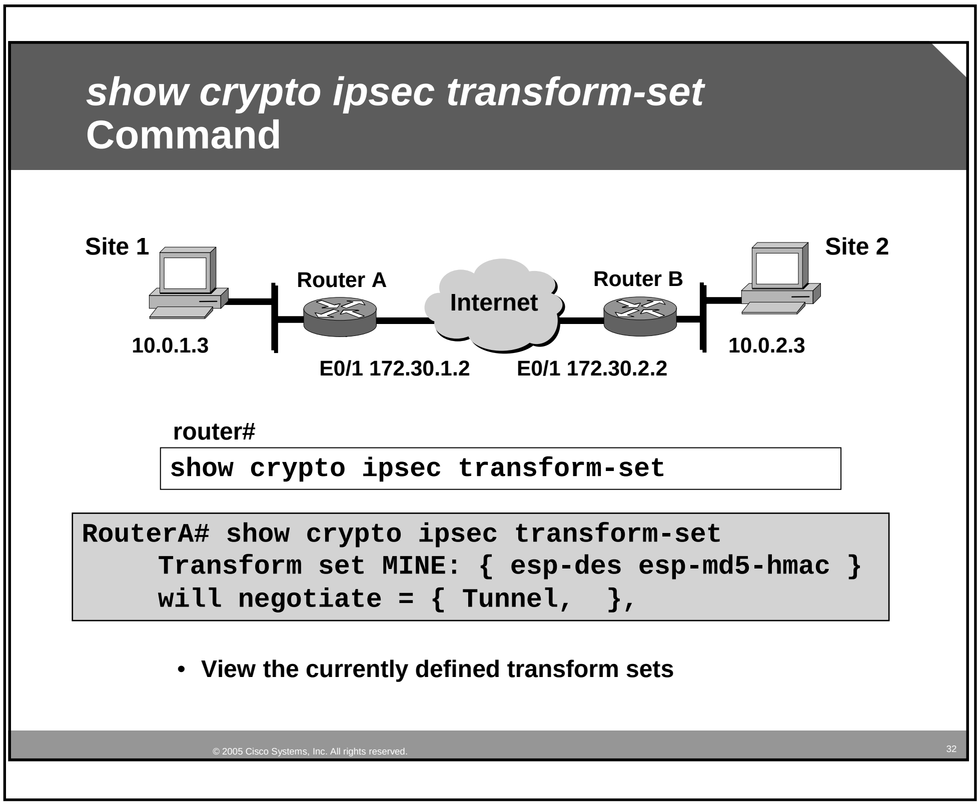
10.0.1.3 10.0.2.3

router#

```
show crypto isakmp policy
```

```
RouterA# show crypto isakmp policy
Protection suite of priority 110
      encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
      hash algorithm:         Message Digest 5
      authentication method:  Rivest-Shamir-Adleman Encryption
      Diffie-Hellman group:   #1 (768 bit)
      lifetime:               86400 seconds, no volume limit
Default protection suite
      encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
      hash algorithm:         Secure Hash Standard
      authentication method:  Rivest-Shamir-Adleman Signature
      Diffie-Hellman group:   #1 (768 bit)
      lifetime:               86400 seconds, no volume limit
```

© 2005 Cisco Systems, Inc. All rights reserved. 31



show crypto ipsec transform-set Command

Site 1 Site 2

Router A Internet Router B

10.0.1.3 10.0.2.3

E0/1 172.30.1.2 E0/1 172.30.2.2

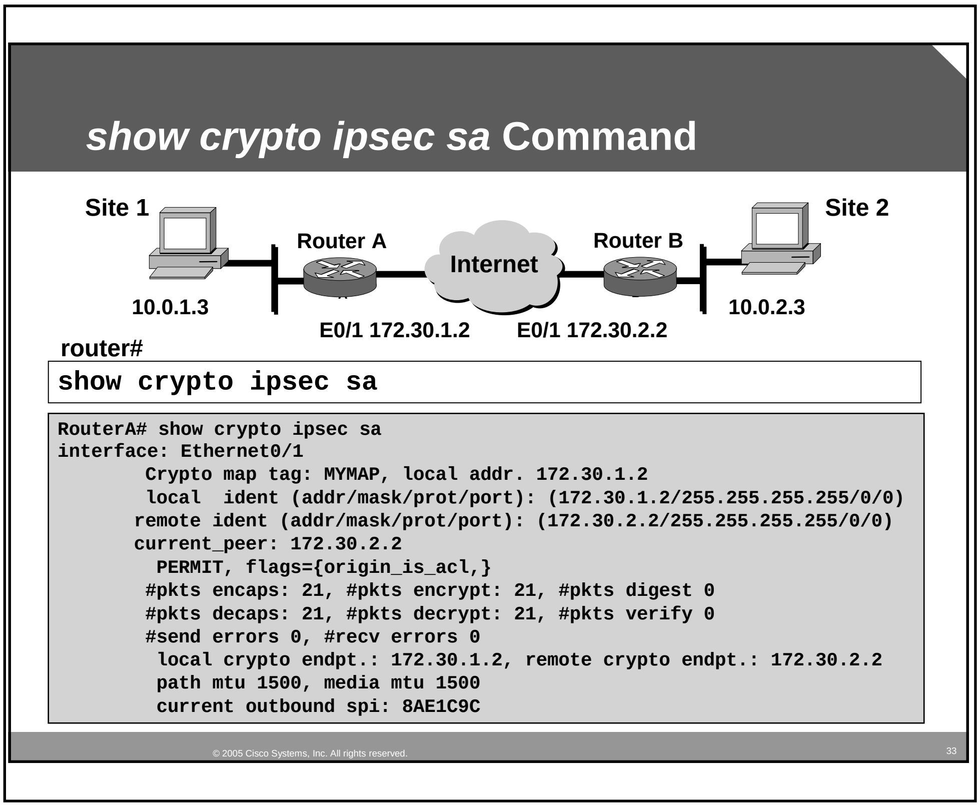
router#

```
show crypto ipsec transform-set
```

```
RouterA# show crypto ipsec transform-set
     Transform set MINE: { esp-des esp-md5-hmac }
     will negotiate = { Tunnel,  },
```

- View the currently defined transform sets

© 2005 Cisco Systems, Inc. All rights reserved. 32



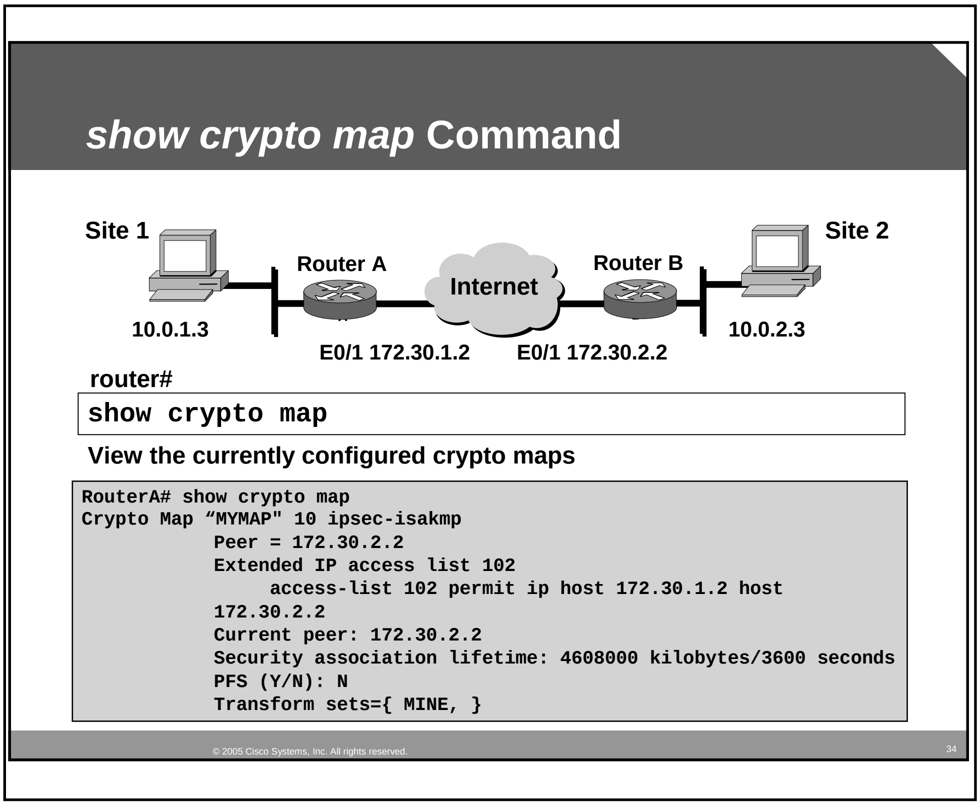
show crypto ipsec sa Command

Site 1
Router A
Internet
Router B
Site 2
10.0.1.3
E0/1 172.30.1.2
E0/1 172.30.2.2
10.0.2.3

router#

```
show crypto ipsec sa
```

```
RouterA# show crypto ipsec sa
interface: Ethernet0/1
        Crypto map tag: MYMAP, local addr. 172.30.1.2
        local  ident (addr/mask/prot/port): (172.30.1.2/255.255.255.255/0/0)
       remote ident (addr/mask/prot/port): (172.30.2.2/255.255.255.255/0/0)
       current_peer: 172.30.2.2
         PERMIT, flags={origin_is_acl,}
        #pkts encaps: 21, #pkts encrypt: 21, #pkts digest 0
        #pkts decaps: 21, #pkts decrypt: 21, #pkts verify 0
        #send errors 0, #recv errors 0
         local crypto endpt.: 172.30.1.2, remote crypto endpt.: 172.30.2.2
         path mtu 1500, media mtu 1500
         current outbound spi: 8AE1C9C
```



show crypto map Command

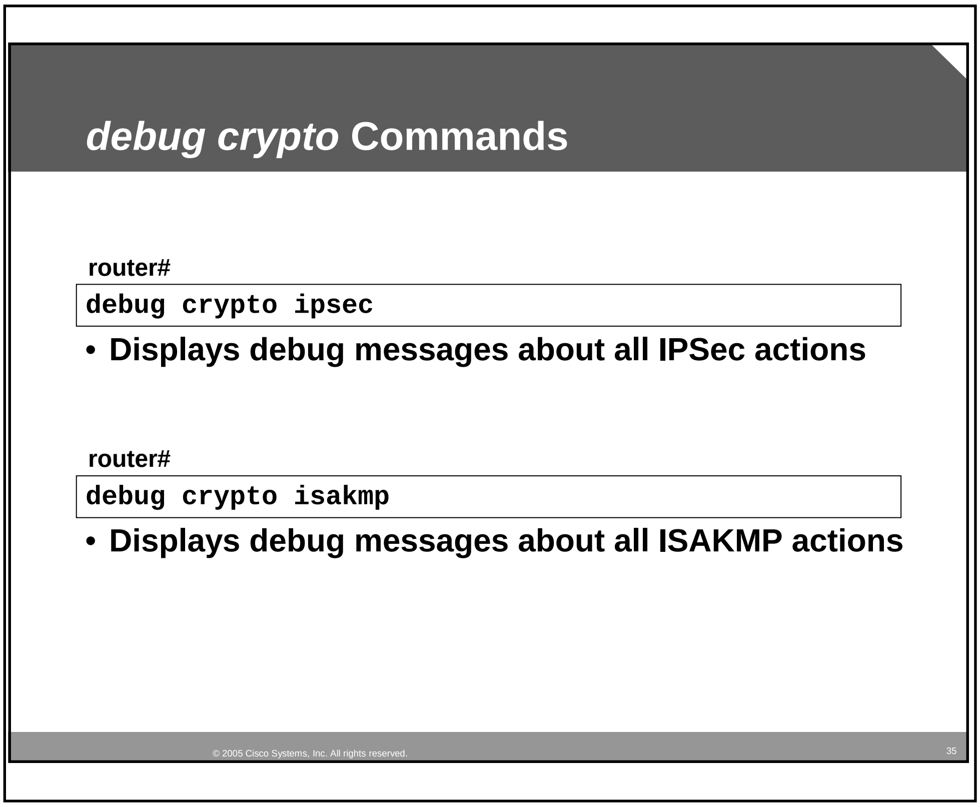
Site 1
Router A
Internet
Router B
Site 2
10.0.1.3
E0/1 172.30.1.2
E0/1 172.30.2.2
10.0.2.3

router#

```
show crypto map
```

View the currently configured crypto maps

```
RouterA# show crypto map
Crypto Map “MYMAP" 10 ipsec-isakmp
            Peer = 172.30.2.2
            Extended IP access list 102
                 access-list 102 permit ip host 172.30.1.2 host
            172.30.2.2
            Current peer: 172.30.2.2
            Security association lifetime: 4608000 kilobytes/3600 seconds
            PFS (Y/N): N
            Transform sets={ MINE, }
```



debug crypto Commands

router#

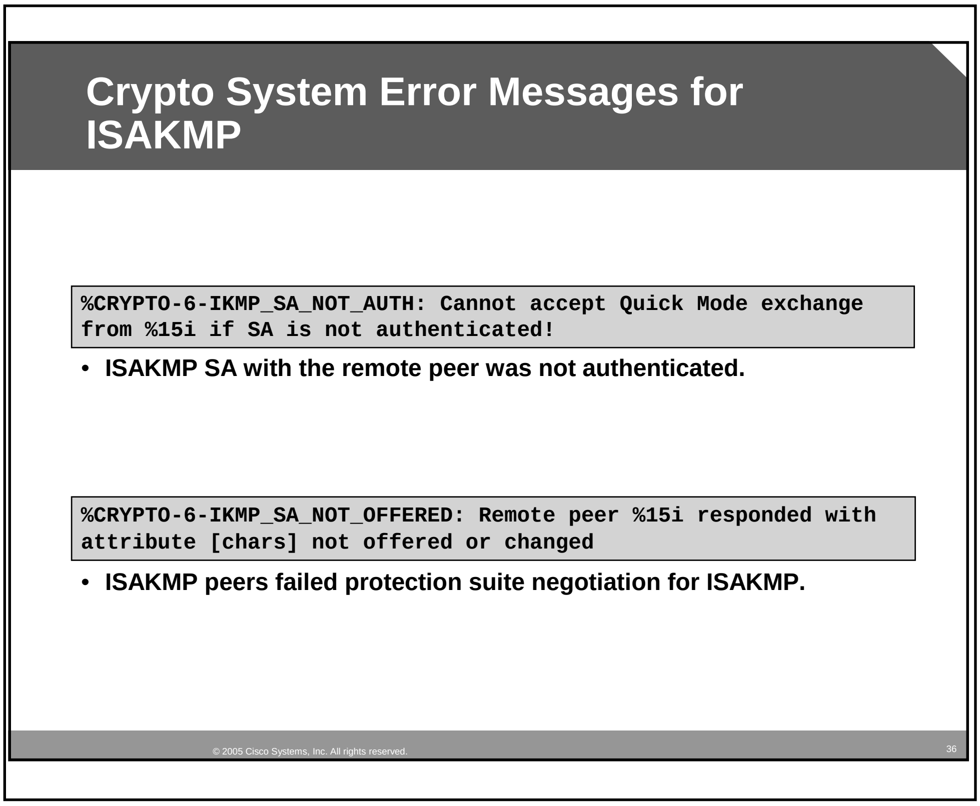
```
debug crypto ipsec
```

- Displays debug messages about all IPSec actions

router#

```
debug crypto isakmp
```

- Displays debug messages about all ISAKMP actions



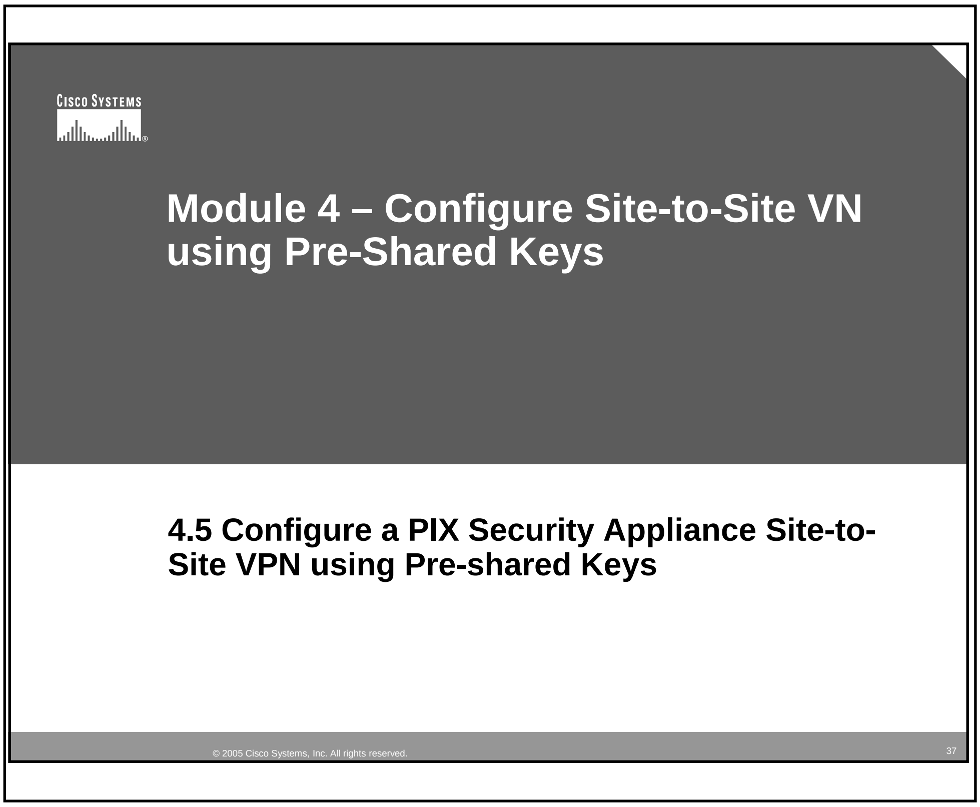
Crypto System Error Messages for ISAKMP

```
%CRYPTO-6-IKMP_SA_NOT_AUTH: Cannot accept Quick Mode exchange
from %15i if SA is not authenticated!
```

- ISAKMP SA with the remote peer was not authenticated.

```
%CRYPTO-6-IKMP_SA_NOT_OFFERED: Remote peer %15i responded with
attribute [chars] not offered or changed
```

- ISAKMP peers failed protection suite negotiation for ISAKMP.

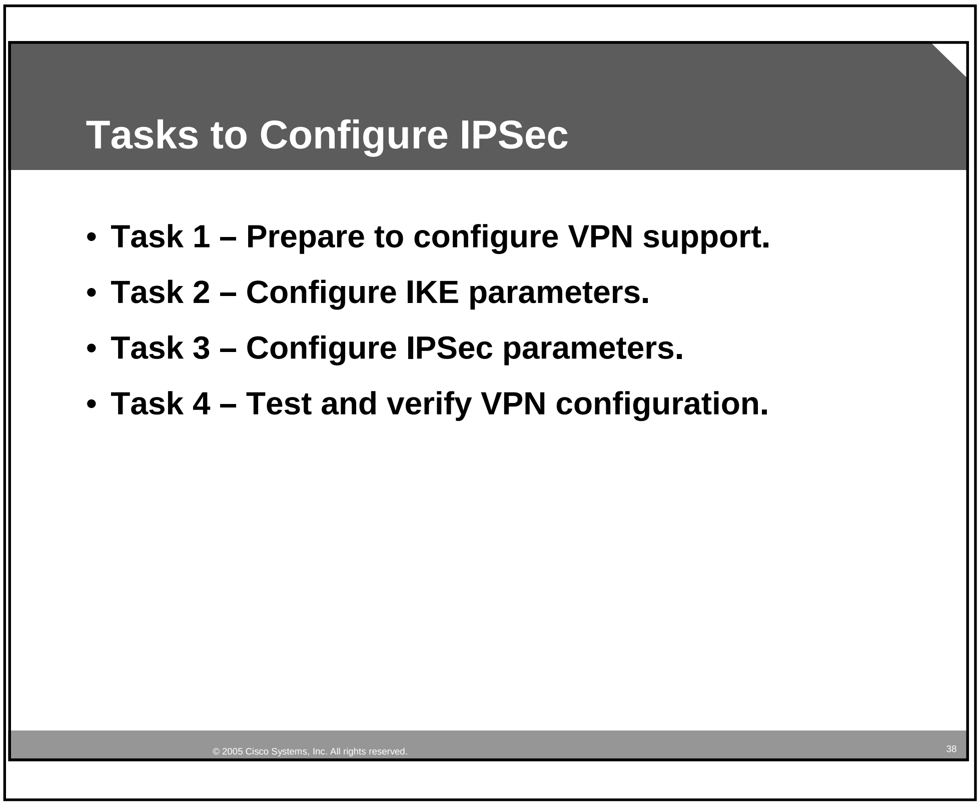


CISCO SYSTEMS

Module 4 – Configure Site-to-Site VN using Pre-Shared Keys

4.5 Configure a PIX Security Appliance Site-to-Site VPN using Pre-shared Keys

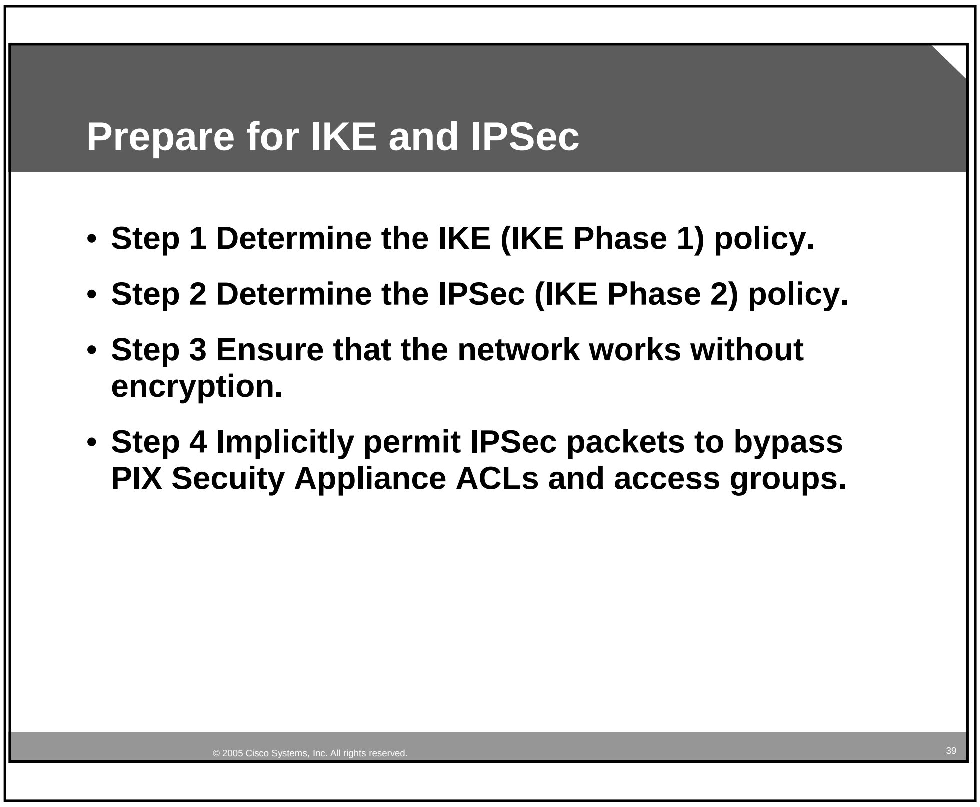
© 2005 Cisco Systems, Inc. All rights reserved. 37



Tasks to Configure IPSec

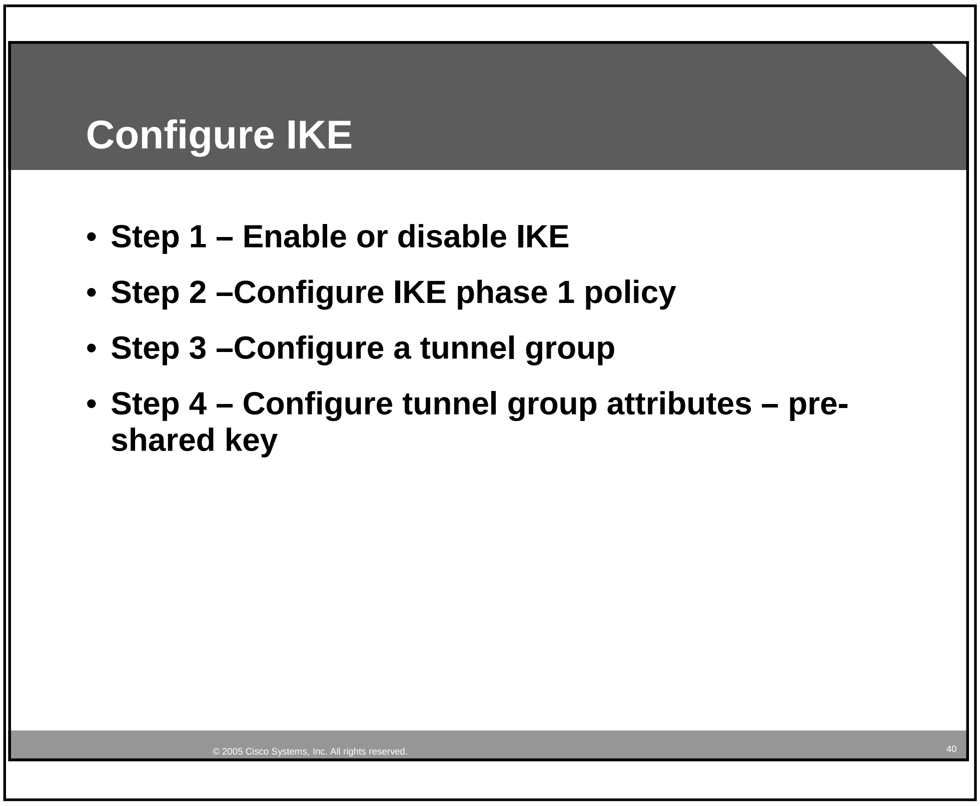
- Task 1 – Prepare to configure VPN support.
- Task 2 – Configure IKE parameters.
- Task 3 – Configure IPSec parameters.
- Task 4 – Test and verify VPN configuration.

© 2005 Cisco Systems, Inc. All rights reserved. 38



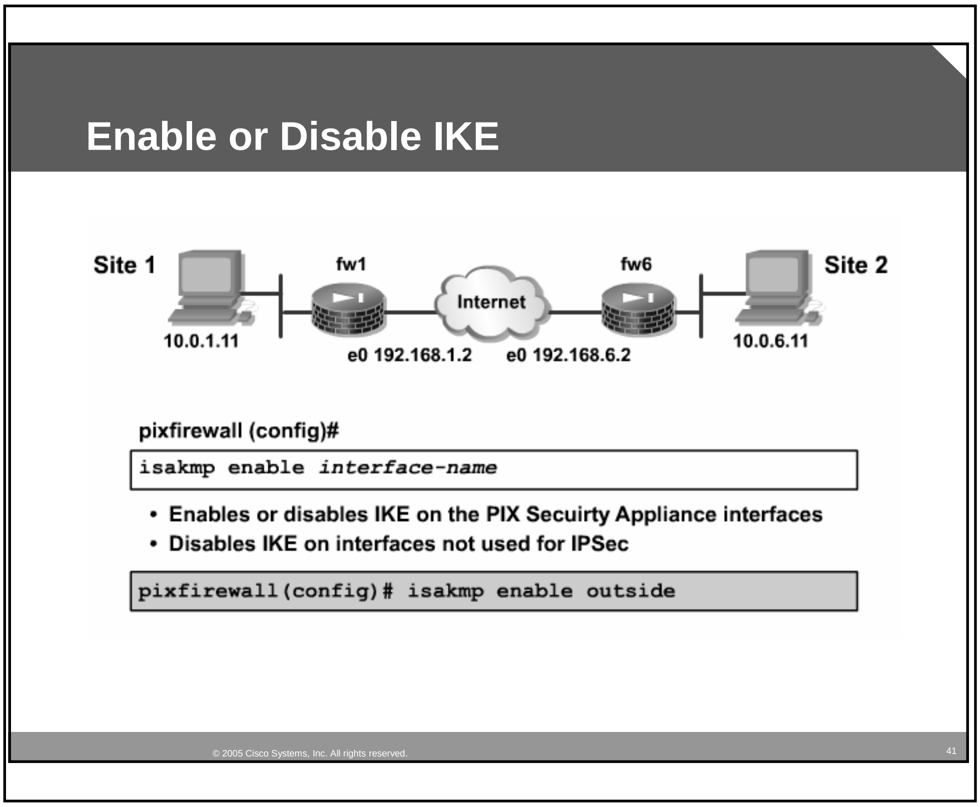
Prepare for IKE and IPSec

- Step 1 Determine the IKE (IKE Phase 1) policy.
- Step 2 Determine the IPSec (IKE Phase 2) policy.
- Step 3 Ensure that the network works without encryption.
- Step 4 Implicitly permit IPSec packets to bypass PIX Secuity Appliance ACLs and access groups.



Configure IKE

- Step 1 – Enable or disable IKE
- Step 2 –Configure IKE phase 1 policy
- Step 3 –Configure a tunnel group
- Step 4 – Configure tunnel group attributes – pre-shared key



Enable or Disable IKE

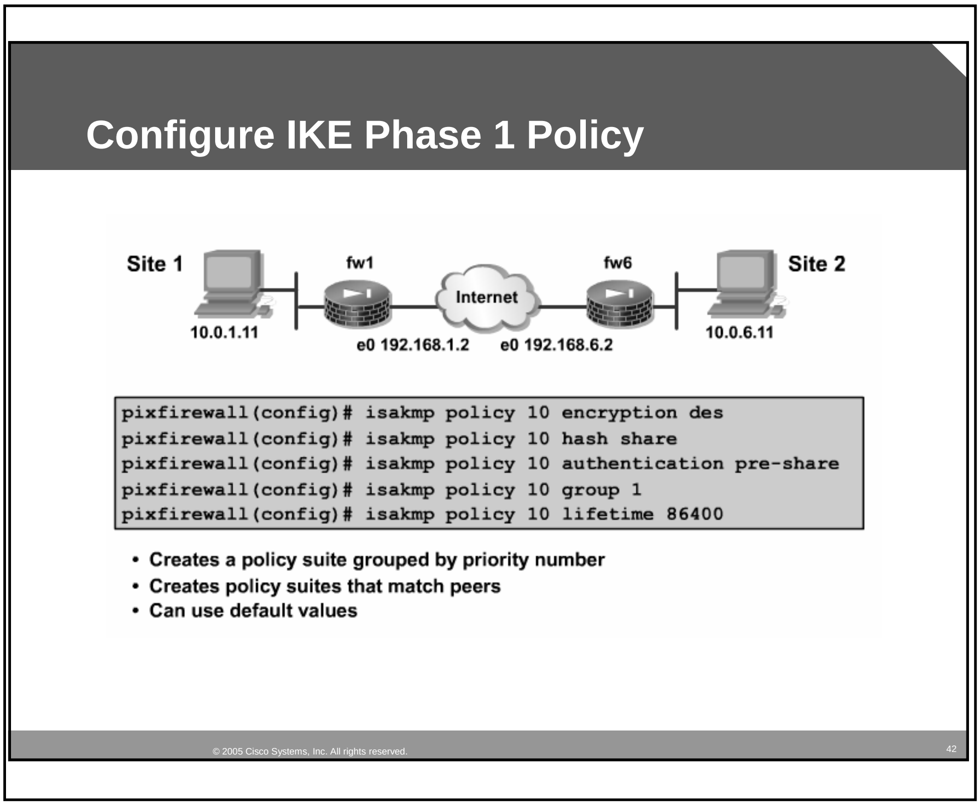
Site 1
10.0.1.11
fw1
e0 192.168.1.2
Internet
fw6
e0 192.168.6.2
Site 2
10.0.6.11

pixfirewall (config)#

```
isakmp enable interface-name
```

- Enables or disables IKE on the PIX Secuirty Appliance interfaces
- Disables IKE on interfaces not used for IPSec

```
pixfirewall(config)# isakmp enable outside
```

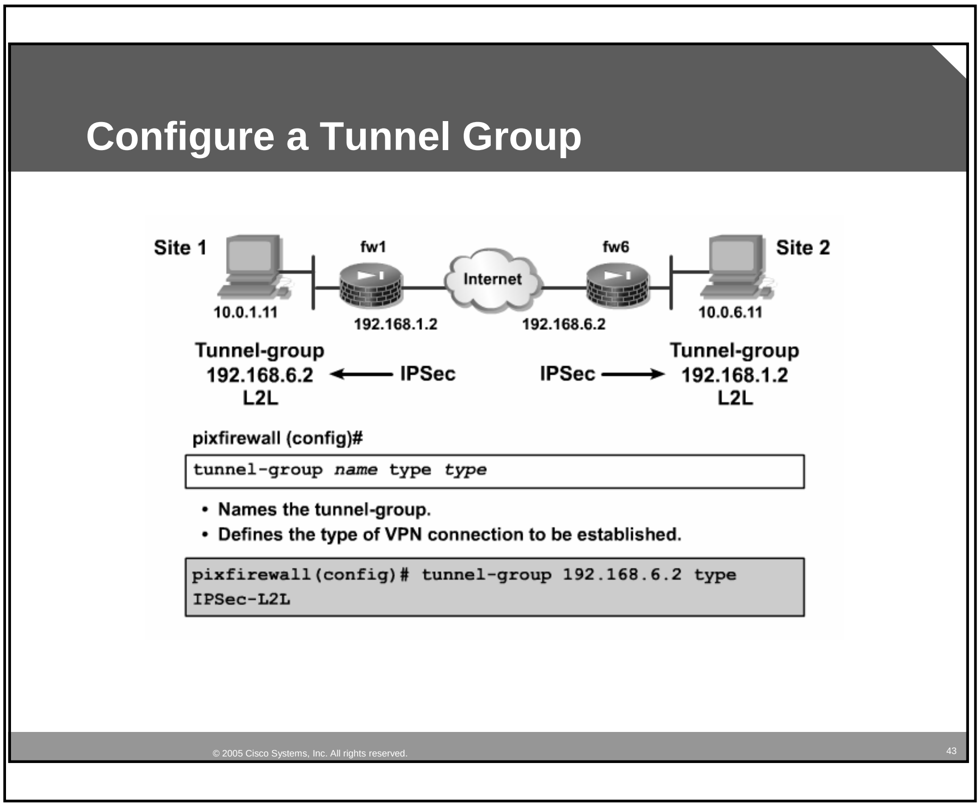


Configure IKE Phase 1 Policy

Site 1
10.0.1.11
fw1
e0 192.168.1.2
Internet
fw6
e0 192.168.6.2
Site 2
10.0.6.11

```
pixfirewall(config)# isakmp policy 10 encryption des
pixfirewall(config)# isakmp policy 10 hash share
pixfirewall(config)# isakmp policy 10 authentication pre-share
pixfirewall(config)# isakmp policy 10 group 1
pixfirewall(config)# isakmp policy 10 lifetime 86400
```

- Creates a policy suite grouped by priority number
- Creates policy suites that match peers
- Can use default values



Configure a Tunnel Group

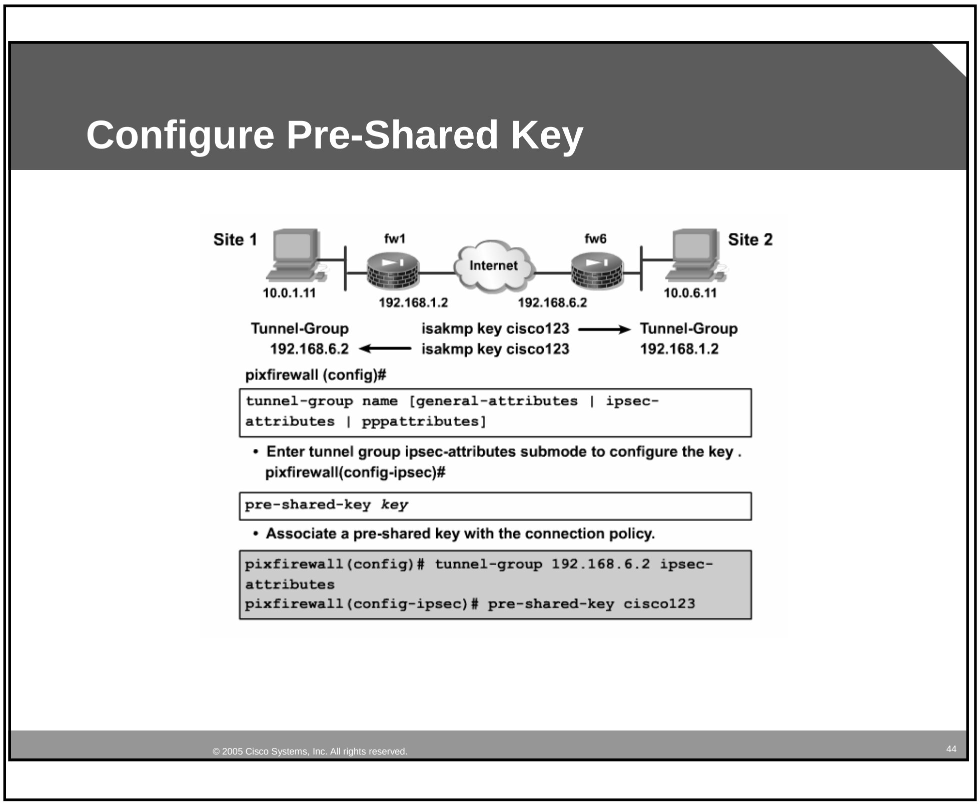
pixfirewall (config)#

```
tunnel-group name type type
```

- Names the tunnel-group.
- Defines the type of VPN connection to be established.

```
pixfirewall(config)# tunnel-group 192.168.6.2 type
IPSec-L2L
```

43



Configure Pre-Shared Key

pixfirewall (config)#

```
tunnel-group name [general-attributes | ipsec-
attributes | pppattributes]
```

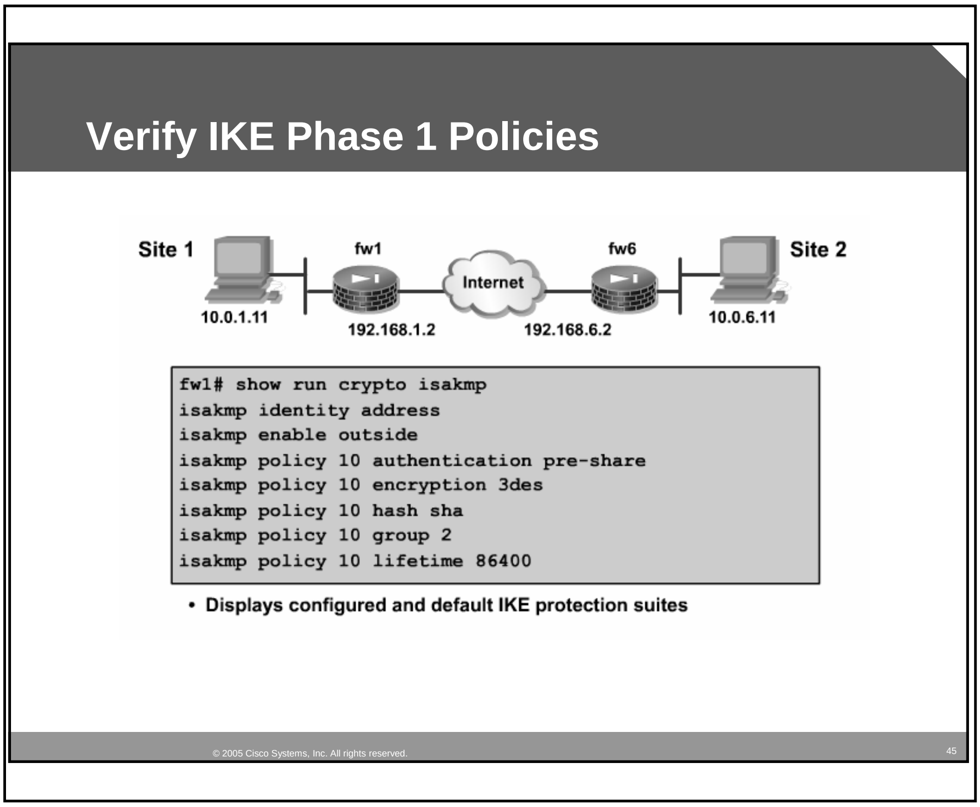
- Enter tunnel group ipsec-attributes submode to configure the key .
  pixfirewall(config-ipsec)#

```
pre-shared-key key
```

- Associate a pre-shared key with the connection policy.

```
pixfirewall(config)# tunnel-group 192.168.6.2 ipsec-
attributes
pixfirewall(config-ipsec)# pre-shared-key cisco123
```

44

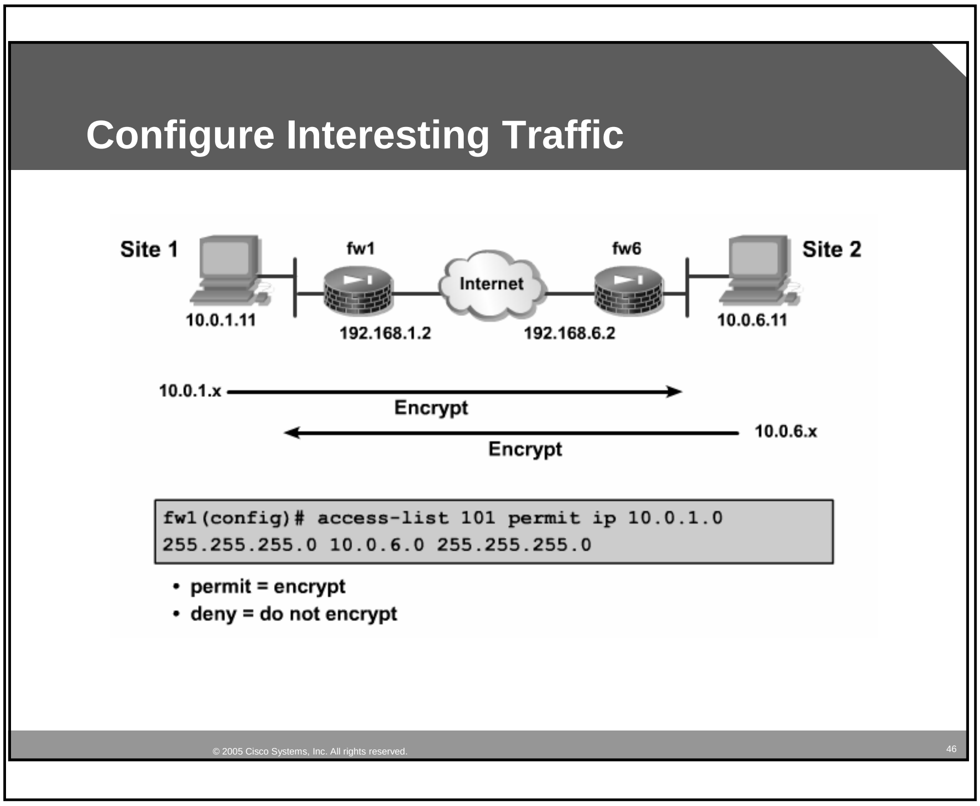


Verify IKE Phase 1 Policies

```
fw1# show run crypto isakmp
isakmp identity address
isakmp enable outside
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash sha
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
```

- Displays configured and default IKE protection suites

45

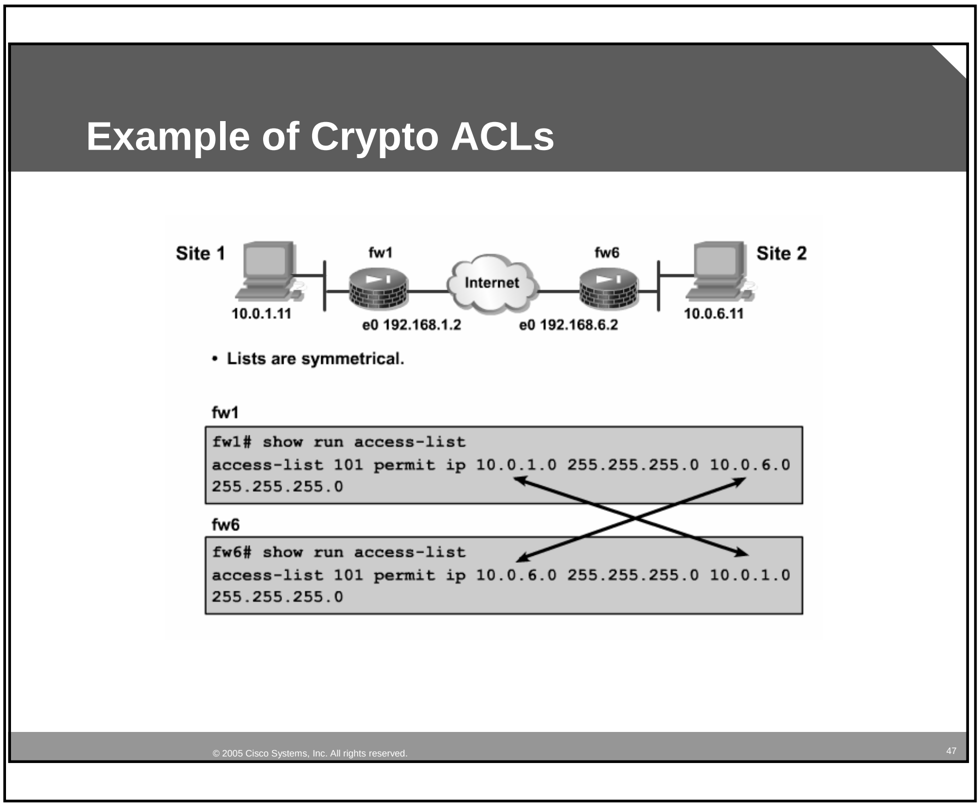


Configure Interesting Traffic

```
fw1(config)# access-list 101 permit ip 10.0.1.0
255.255.255.0 10.0.6.0 255.255.255.0
```

- permit = encrypt
- deny = do not encrypt

46



Example of Crypto ACLs

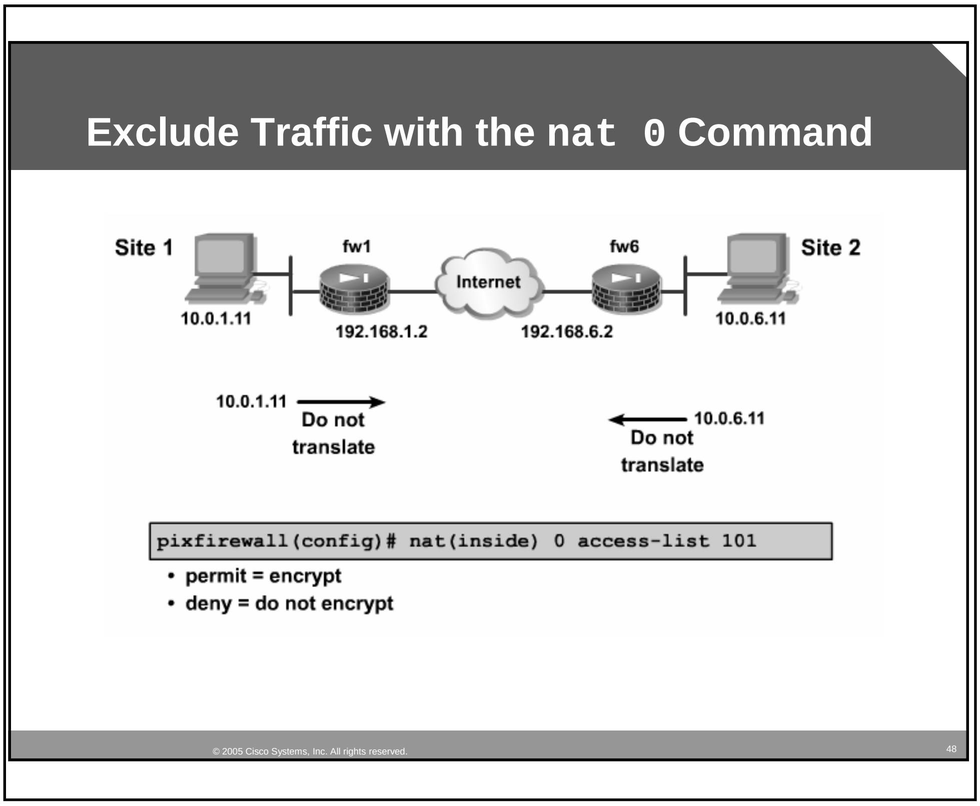
- Lists are symmetrical.

fw1

```
fw1# show run access-list
access-list 101 permit ip 10.0.1.0 255.255.255.0 10.0.6.0
255.255.255.0
```

fw6

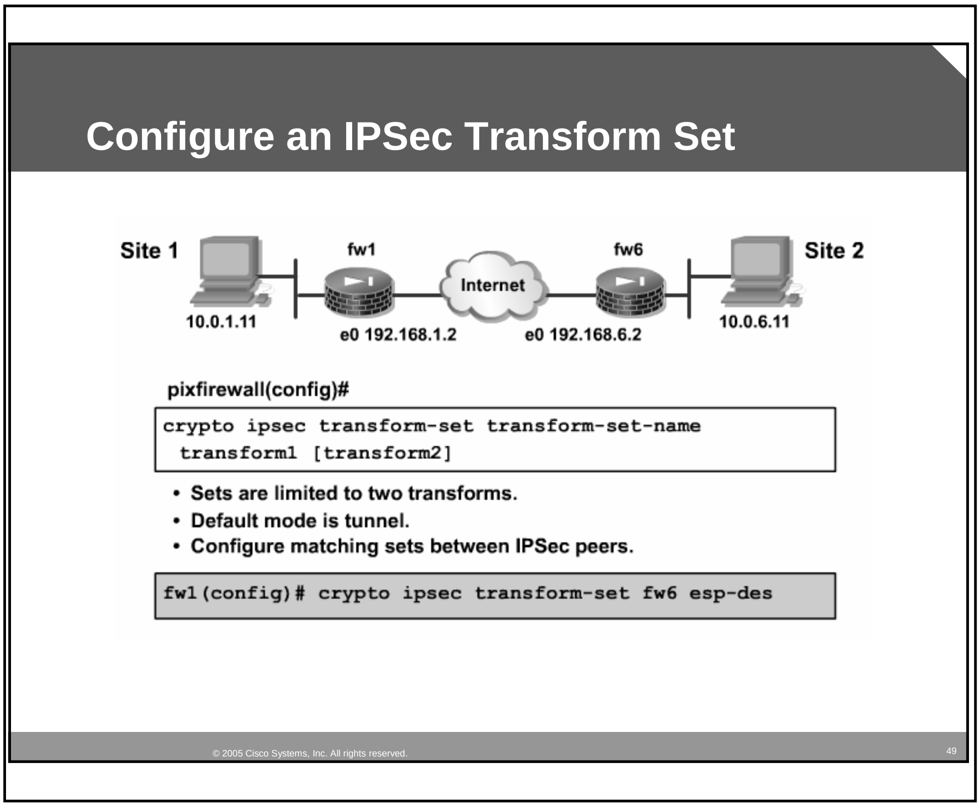
```
fw6# show run access-list
access-list 101 permit ip 10.0.6.0 255.255.255.0 10.0.1.0
255.255.255.0
```



Exclude Traffic with the `nat 0` Command

```
pixfirewall(config)# nat(inside) 0 access-list 101
```

- permit = encrypt
- deny = do not encrypt



Configure an IPSec Transform Set

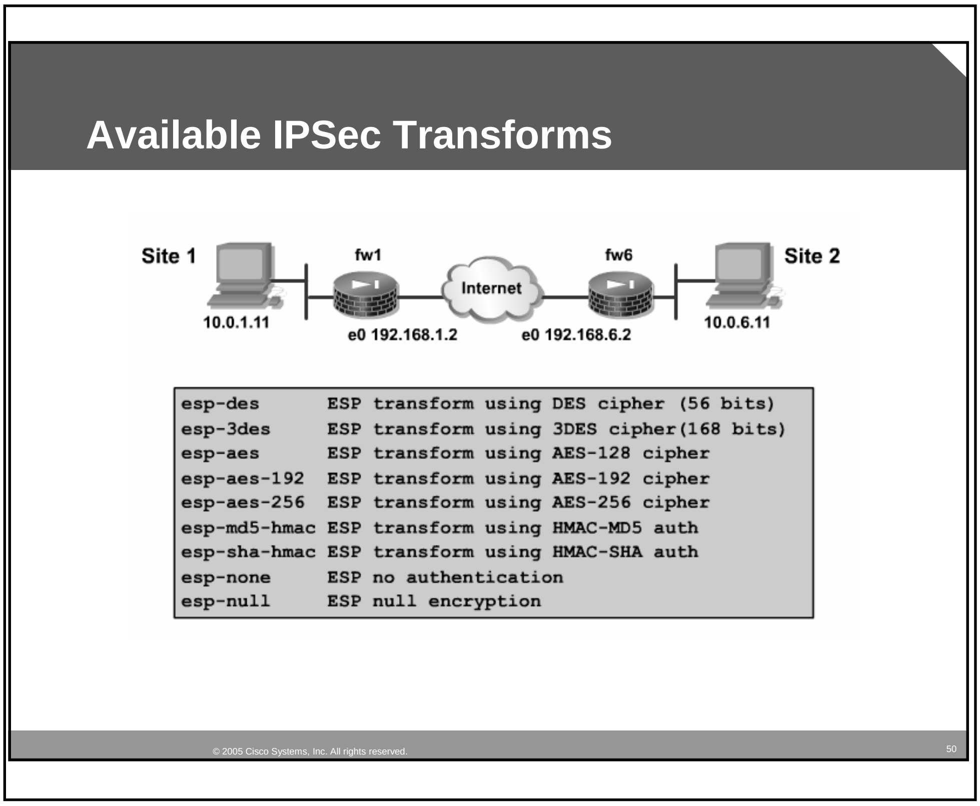
pixfirewall(config)#

```
crypto ipsec transform-set transform-set-name
 transform1 [transform2]
```

- Sets are limited to two transforms.
- Default mode is tunnel.
- Configure matching sets between IPSec peers.

```
fw1(config)# crypto ipsec transform-set fw6 esp-des
```

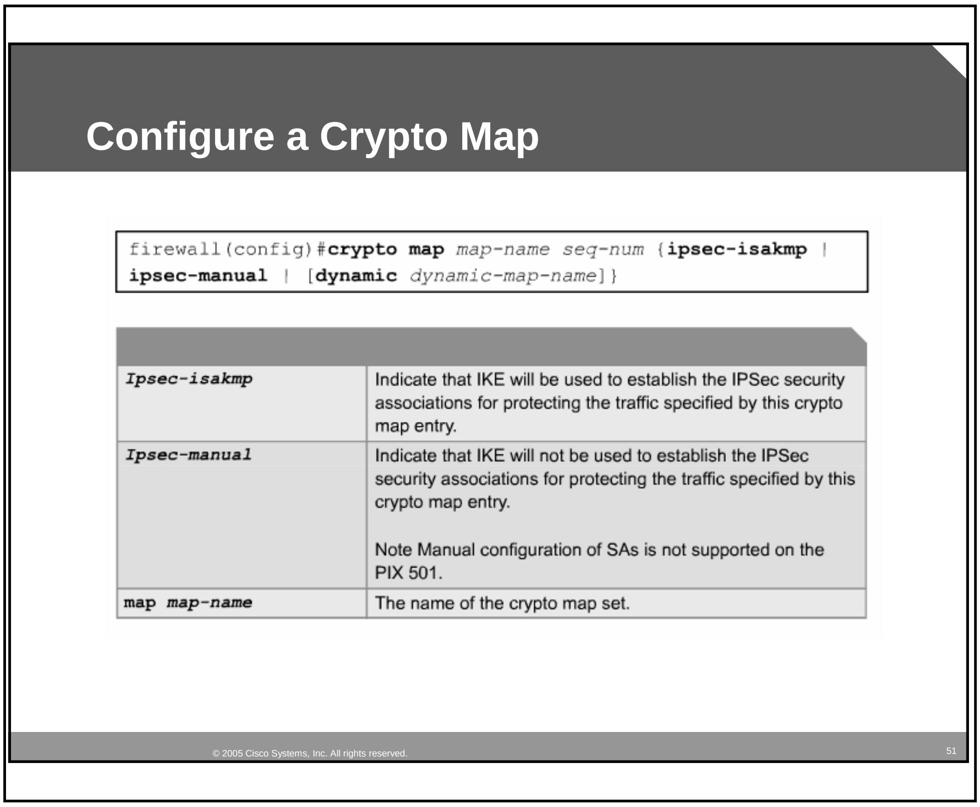
© 2005 Cisco Systems, Inc. All rights reserved. 49



Available IPSec Transforms

```
esp-des      ESP transform using DES cipher (56 bits)
esp-3des     ESP transform using 3DES cipher(168 bits)
esp-aes      ESP transform using AES-128 cipher
esp-aes-192  ESP transform using AES-192 cipher
esp-aes-256  ESP transform using AES-256 cipher
esp-md5-hmac ESP transform using HMAC-MD5 auth
esp-sha-hmac ESP transform using HMAC-SHA auth
esp-none     ESP no authentication
esp-null     ESP null encryption
```

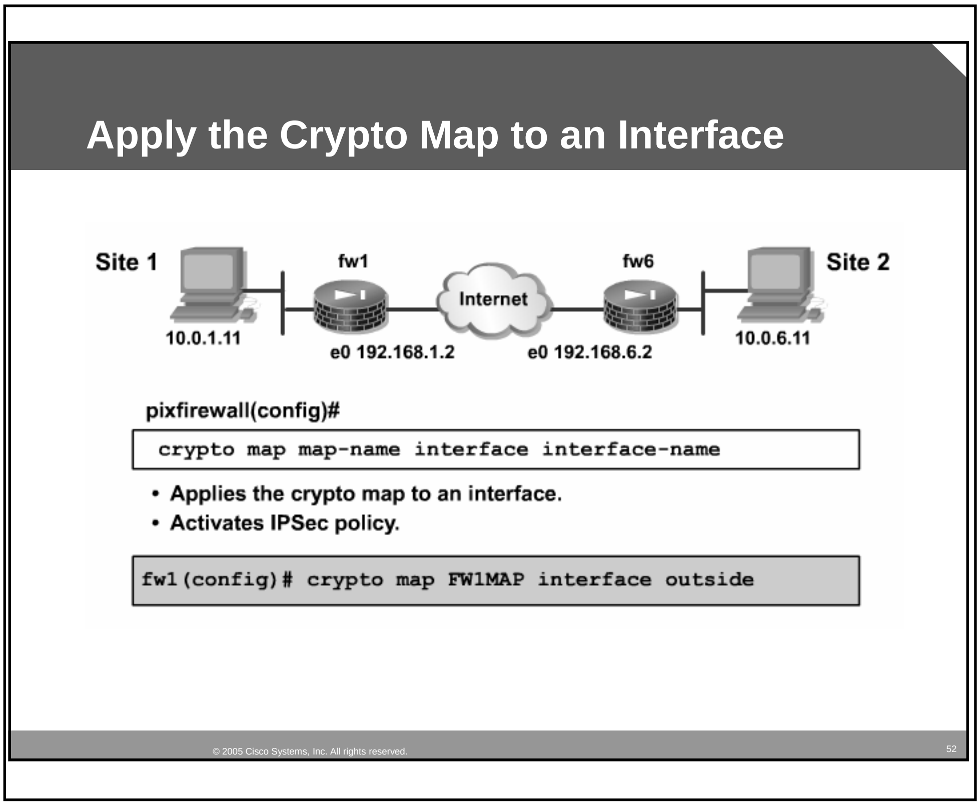
© 2005 Cisco Systems, Inc. All rights reserved. 50



Configure a Crypto Map

```
firewall(config)#crypto map map-name seq-num {ipsec-isakmp |
ipsec-manual | [dynamic dynamic-map-name]}
```

Ipsec-isakmp	Indicate that IKE will be used to establish the IPSec security associations for protecting the traffic specified by this crypto map entry.
Ipsec-manual	Indicate that IKE will not be used to establish the IPSec security associations for protecting the traffic specified by this crypto map entry. Note Manual configuration of SAs is not supported on the PIX 501.
map *map-name*	The name of the crypto map set.



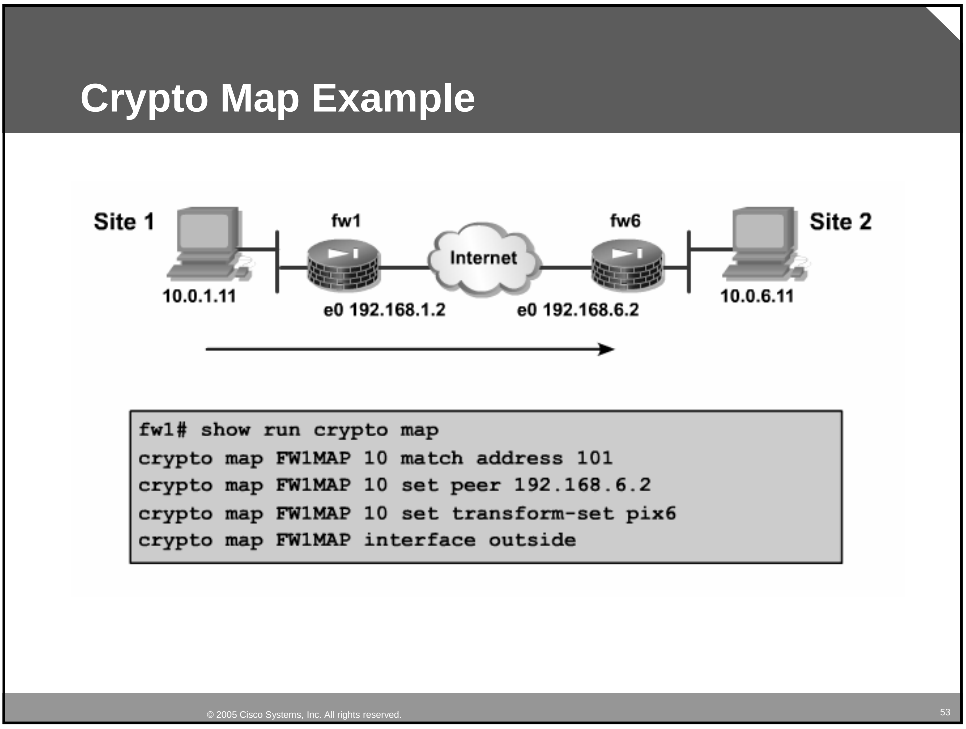
Apply the Crypto Map to an Interface

pixfirewall(config)#

```
crypto map map-name interface interface-name
```

- Applies the crypto map to an interface.
- Activates IPSec policy.

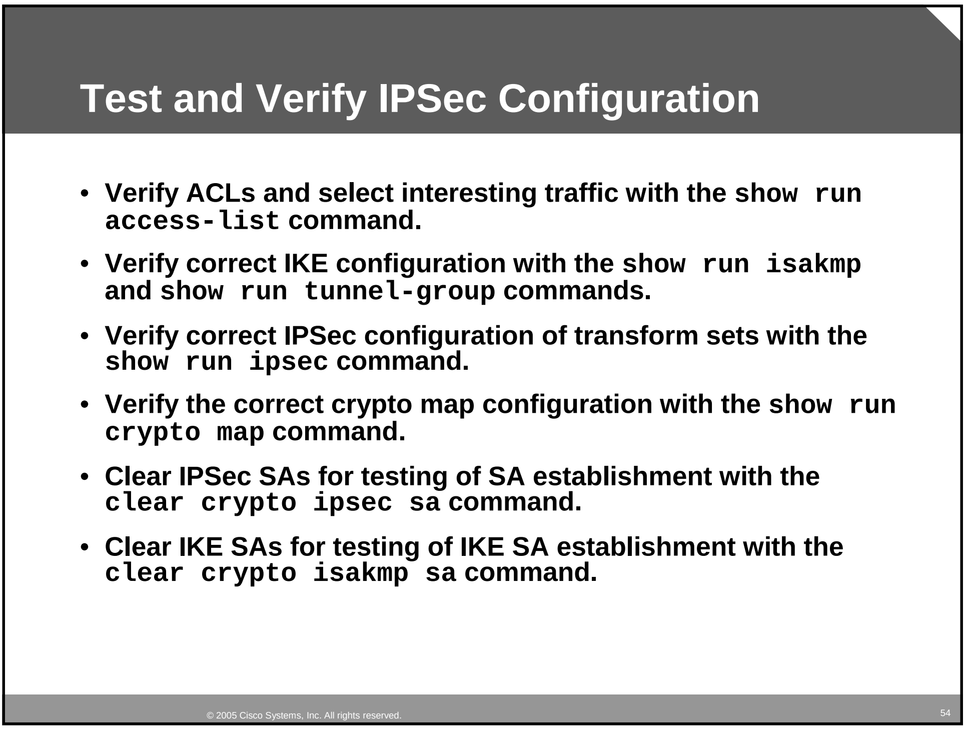
```
fw1(config)# crypto map FW1MAP interface outside
```



Crypto Map Example

```
fw1# show run crypto map
crypto map FW1MAP 10 match address 101
crypto map FW1MAP 10 set peer 192.168.6.2
crypto map FW1MAP 10 set transform-set pix6
crypto map FW1MAP interface outside
```

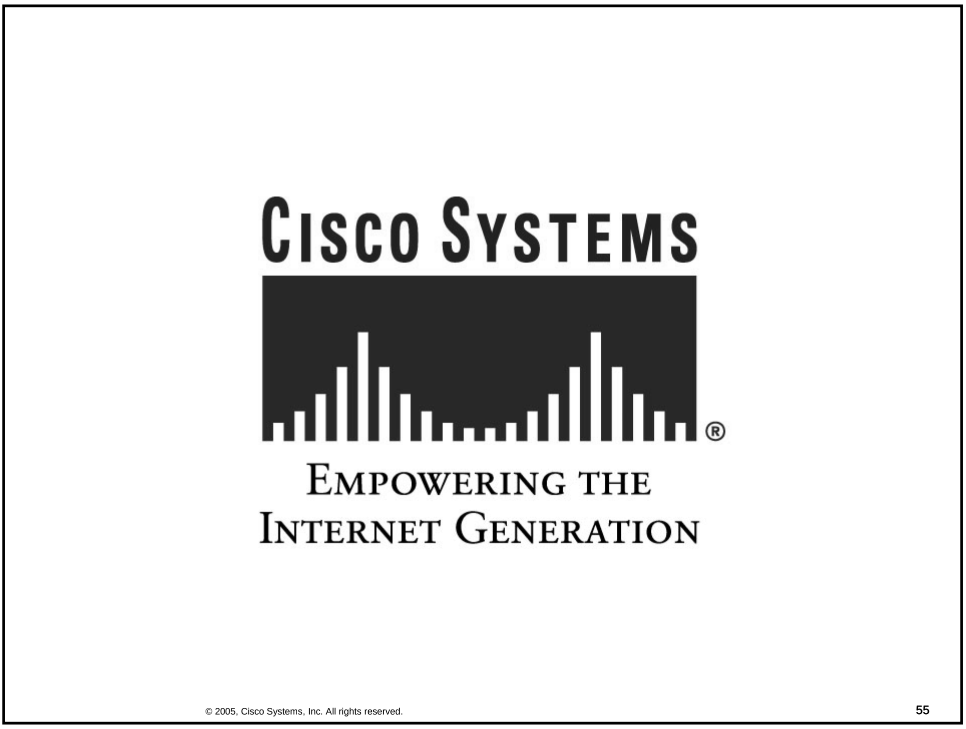
53



Test and Verify IPSec Configuration

- Verify ACLs and select interesting traffic with the `show run access-list` command.
- Verify correct IKE configuration with the `show run isakmp` and `show run tunnel-group` commands.
- Verify correct IPSec configuration of transform sets with the `show run ipsec` command.
- Verify the correct crypto map configuration with the `show run crypto map` command.
- Clear IPSec SAs for testing of SA establishment with the `clear crypto ipsec sa` command.
- Clear IKE SAs for testing of IKE SA establishment with the `clear crypto isakmp sa` command.

54



Cisco Systems

Empowering the Internet Generation