Serviços de Rede 1 – **Lesson 12 - Practices**

2019-2020

Instituto Politécnico de Coimbra

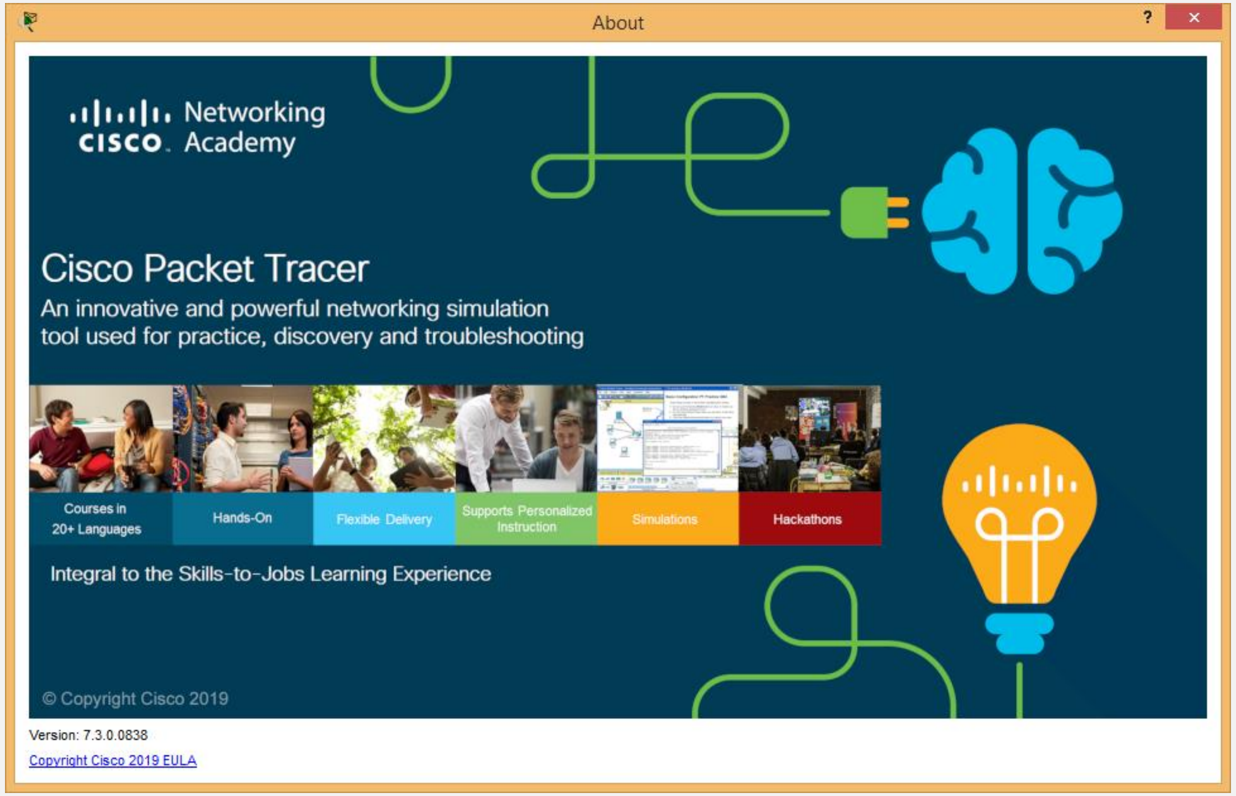
Departamento de Engenharia Informática

Imprtant Note

- On June 8 (16: 30-18: 30) the 3rd practical test will be held.
  - % - 3 points out of 20.
  - Feature:
    - NTP (class 9)
    - Proxy (class 10 and part of class 11)
    - VPN (part of lesson 11 and lesson 12)
  - Mandatory registration in Moodle.
- They must have installed Virtual Box 6.0.
- You must import images of Windows Server 2012 and Windows 8/10 “clean” in advance to VirtualBox.
- They must have Cisco Packet Tracer version 7.3.0 installed.

Pre - Requirements –Exercise 1

- Ter instalado o *Cisco Packet Tracer* versão 7.3.0



About
Networking Academy
Cisco Packet Tracer
An innovative and powerful networking simulation tool used for practice, discovery and troubleshooting
Courses in 20+ Languages
Hands-On
Flexible Delivery
Supports Personalized Instruction
Simulations
Hackathons
Integral to the Skills-to-Jobs Learning Experience
© Copyright Cisco 2019

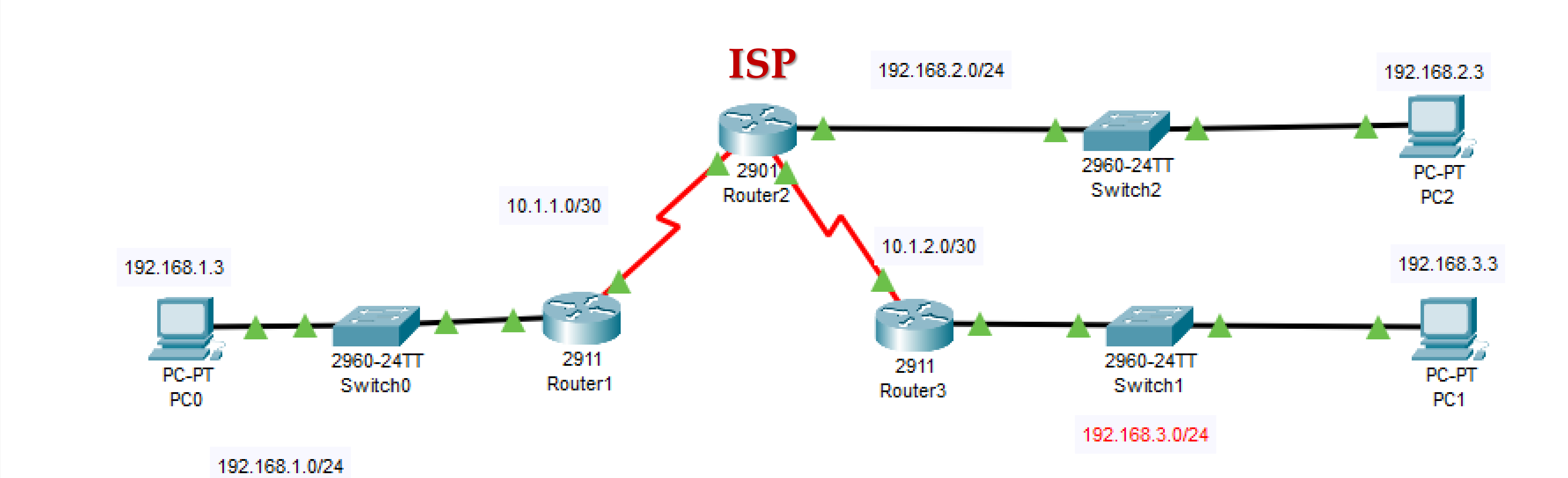
Version: 7.3.0.0838

Copyright Cisco 2019 EULA

Exercise 1 - IPSec VPN in Cisco environment

Exercise 1

- The company SR1.SA wants to connect the headquarters (192.168.1.0/24) to a delegation located in London (192.168.3.0/24). For this you want to use a secure tunnel.
- Decided to use IPSec.
- The topology is as follows:



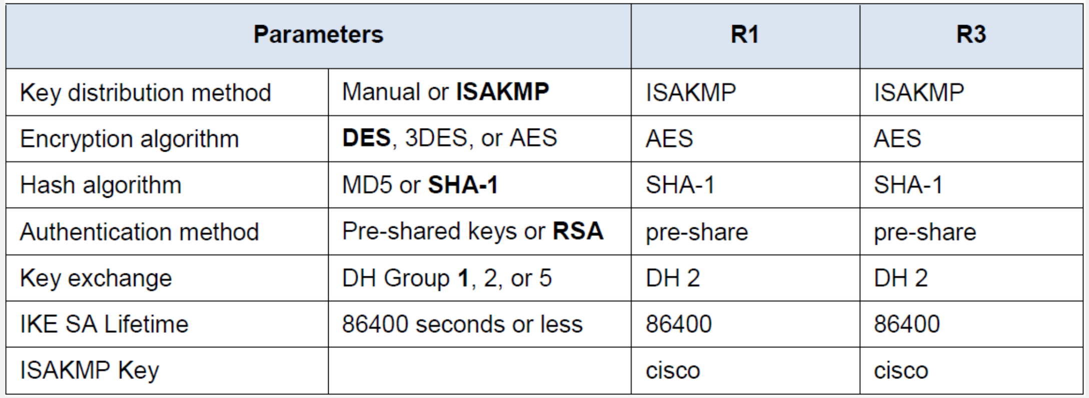
Exercise 1

- Save the simulation as VPN_IPSEC.
- Place the IP addresses of the different devices in a fixed way and according to the networks indicated in the image.
- Change the name of the routrs to:
  - R1 - R_Sede
  - R2 - R_ISP
  - R3 - R_Dele
- Disable the “IP Domain Name System hostname translation”
- Put only one default route on router 1 and router 2.
- Try to ping from PC0 to PC2.
- Try to ping from PC0 to PC1. You shouldn't be able to…

Exercise 1

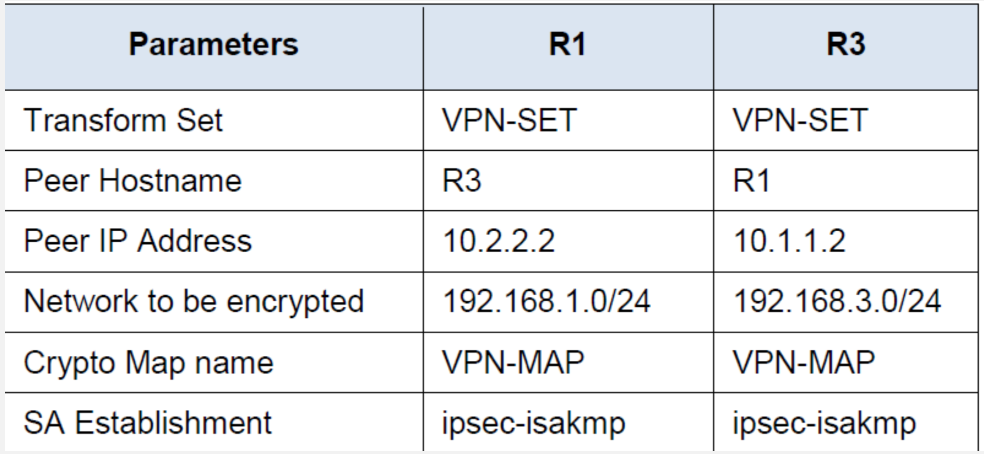
- Create a VPN between R1 and R3 with the following settings:

ISAKMP Phase 1



Parameters		R1	R3
Key distribution method	Manual or **ISAKMP**	ISAKMP	ISAKMP
Encryption algorithm	**DES**, 3DES, or AES	AES	AES
Hash algorithm	MD5 or **SHA-1**	SHA-1	SHA-1
Authentication method	Pre-shared keys or **RSA**	pre-share	pre-share
Key exchange	DH Group **1**, 2, or 5	DH 2	DH 2
IKE SA Lifetime	86400 seconds or less	86400	86400
ISAKMP Key		cisco	cisco

ISAKMP Phase2



Parameters	R1	R3
Transform Set	VPN-SET	VPN-SET
Peer Hostname	R3	R1
Peer IP Address	10.2.2.2	10.1.1.2
Network to be encrypted	192.168.1.0/24	192.168.3.0/24
Crypto Map name	VPN-MAP	VPN-MAP
SA Establishment	ipsec-isakmp	ipsec-isakmp

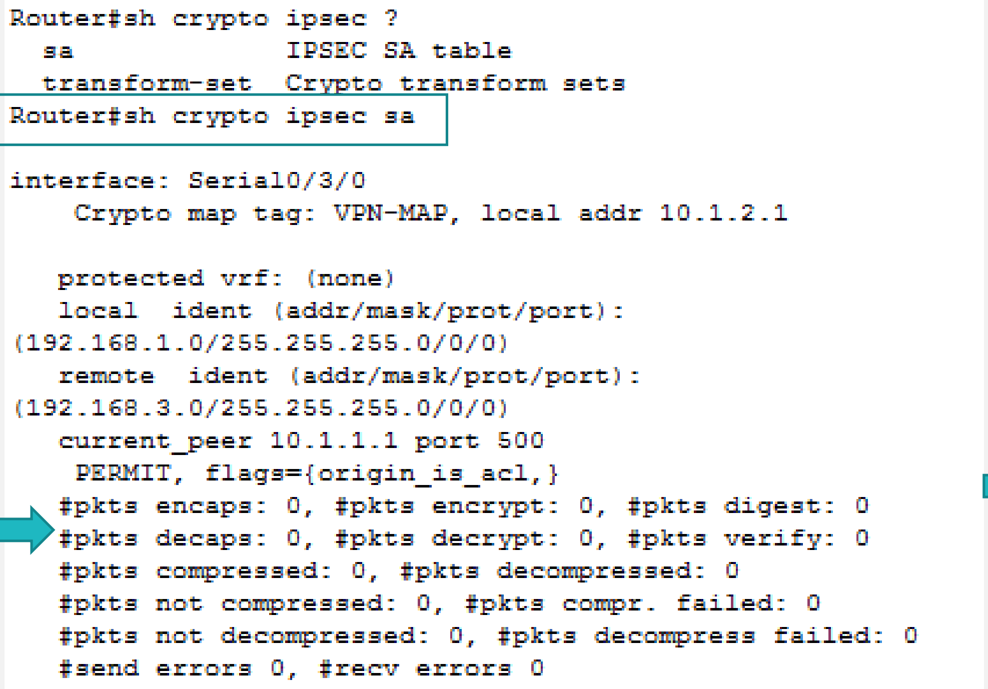
Note: Defaut parameters (are in bold) do not need to be written in the router configuration

Exercise 1

- Phases
  - Set the access-list on router 1 and router 3

    access-list 110 permit ***ip rede origem rede destino***
  - Configure the ISAKMP Phase 1
  - Configure the ISAKMP Phase 2
  - Connect the crypto map to the output interface
  - Check the status of your tunnel
  - Generate traffic that will be encrypted (for example from PC0 to PC1)
  - Check the status of your tunnel

Exercise 2

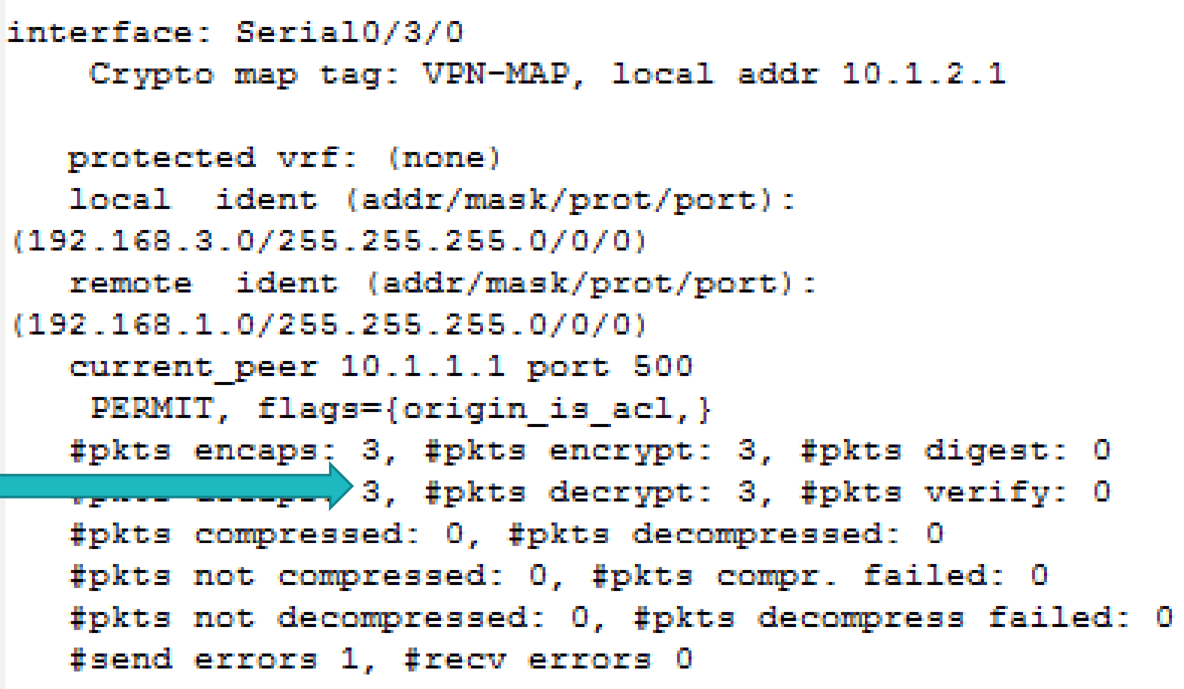


```
Router#sh crypto ipsec ?
  sa              IPSEC SA table
  transform-set   Crypto transform sets
Router#sh crypto ipsec sa

interface: Serial0/3/0
    Crypto map tag: VPN-MAP, local addr 10.1.2.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port):
(192.168.3.0/255.255.255.0/0/0)
   current_peer 10.1.1.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0
```

Before generating encrypted traffic



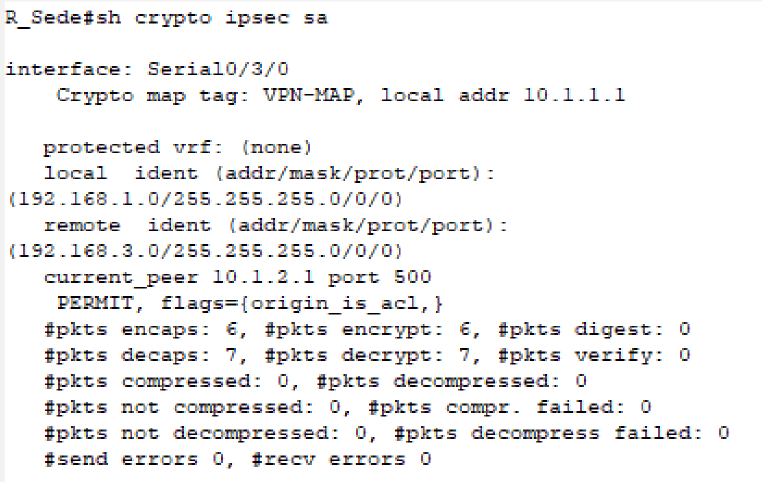
```
interface: Serial0/3/0
    Crypto map tag: VPN-MAP, local addr 10.1.2.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port):
(192.168.3.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0)
   current_peer 10.1.1.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 0
   #pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 1, #recv errors 0
```

After generating encrypted traffic

Exercise 2

- Test if PC2 can reach PC0.
- Look at what happened to the traffic passing through the IPSec tunnel. If all goes well, you should be able to "ping" the PC and not "add" encrypted traffic in the tunnel.
- Please drip from PC0 to PC1 again. What happened to the encrypted traffic in the tunnel?



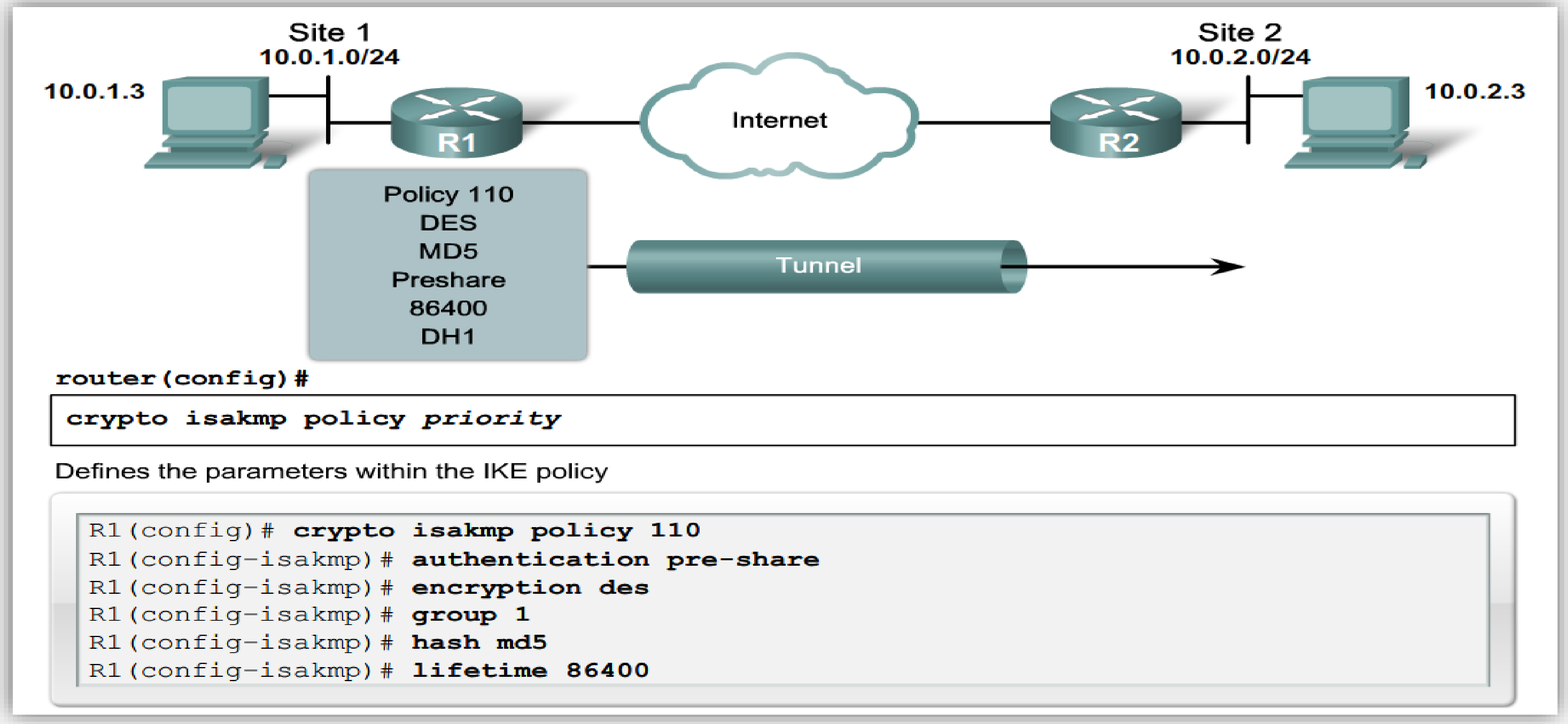
```
R_Sede#sh crypto ipsec sa

interface: Serial0/3/0
    Crypto map tag: VPN-MAP, local addr 10.1.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port):
(192.168.3.0/255.255.255.0/0/0)
   current_peer 10.1.2.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 6, #pkts encrypt: 6, #pkts digest: 0
   #pkts decaps: 7, #pkts decrypt: 7, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0
```

How To

Configuring IPSec Tunnels



```
router(config)#
```

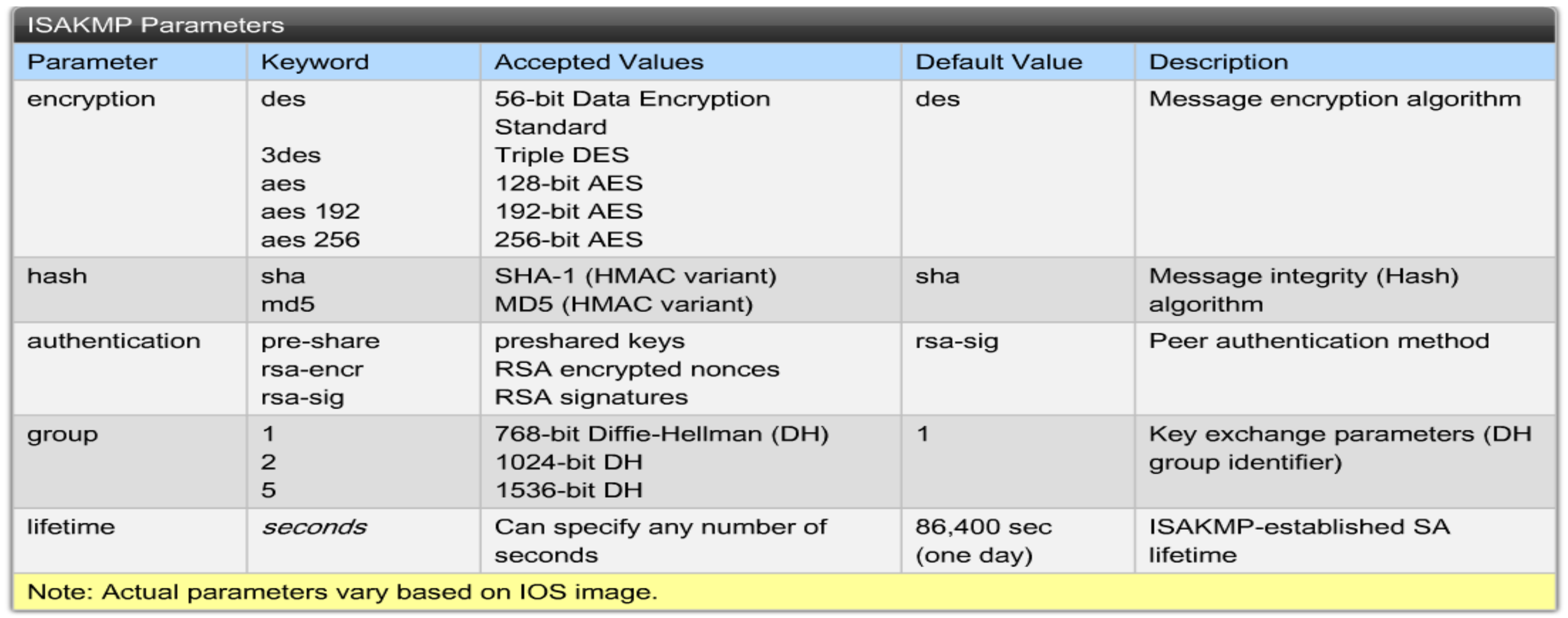
```
crypto isakmp policy priority
```

Defines the parameters within the IKE policy

```
R1(config)# crypto isakmp policy 110
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# encryption des
R1(config-isakmp)# group 1
R1(config-isakmp)# hash md5
R1(config-isakmp)# lifetime 86400
```

Configuring IPSec Tunnels

- The different options you can consider for setting the connection parameters are:



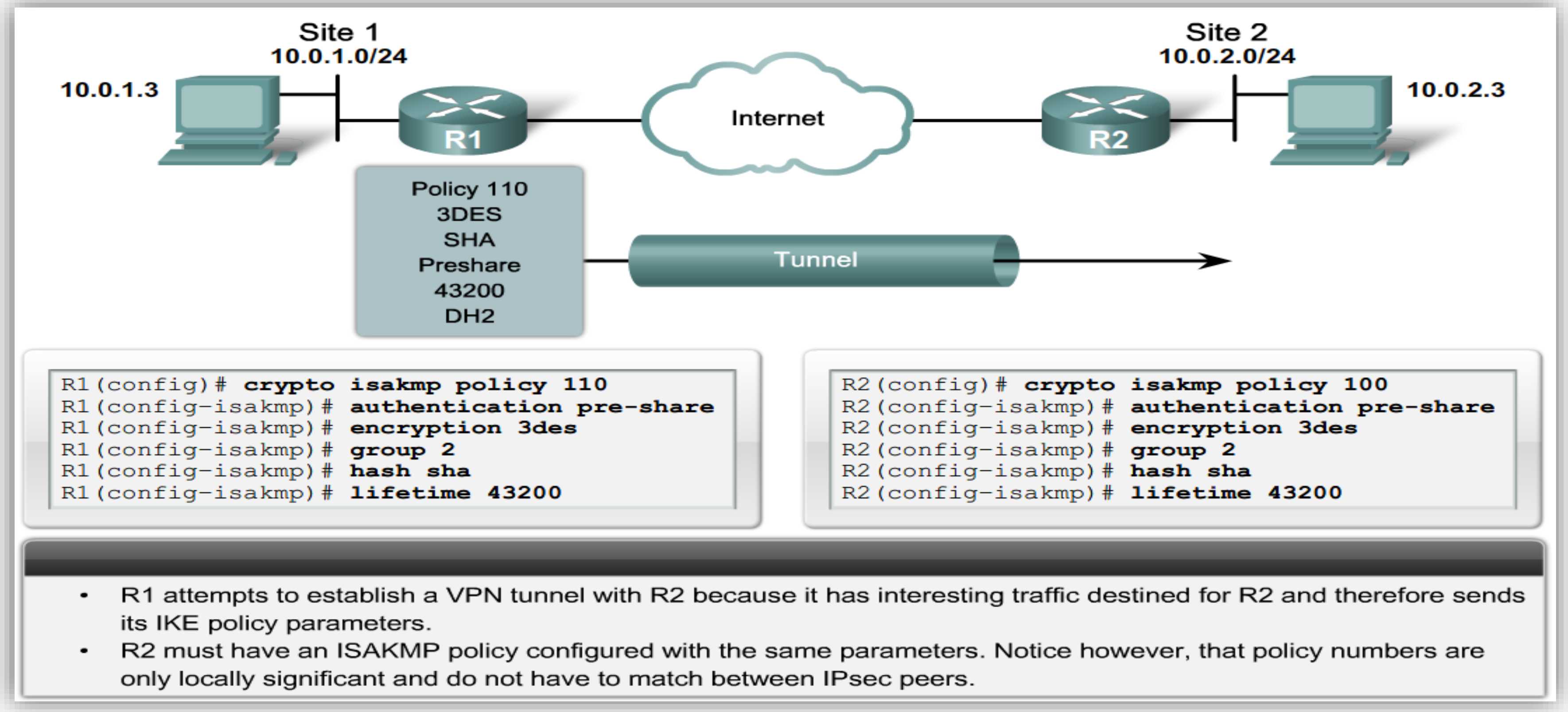
ISAKMP Parameters

Parameter	Keyword	Accepted Values	Default Value	Description
encryption	des 3des aes aes 192 aes 256	56-bit Data Encryption Standard Triple DES 128-bit AES 192-bit AES 256-bit AES	des	Message encryption algorithm
hash	sha md5	SHA-1 (HMAC variant) MD5 (HMAC variant)	sha	Message integrity (Hash) algorithm
authentication	pre-share rsa-encr rsa-sig	preshared keys RSA encrypted nonces RSA signatures	rsa-sig	Peer authentication method
group	1 2 5	768-bit Diffie-Hellman (DH) 1024-bit DH 1536-bit DH	1	Key exchange parameters (DH group identifier)
lifetime	*seconds*	Can specify any number of seconds	86,400 sec (one day)	ISAKMP-established SA lifetime

Note: Actual parameters vary based on IOS image.

Configuring IPSec Tunnels

- We have to ensure that in both extremes the IKE parameters are the same.



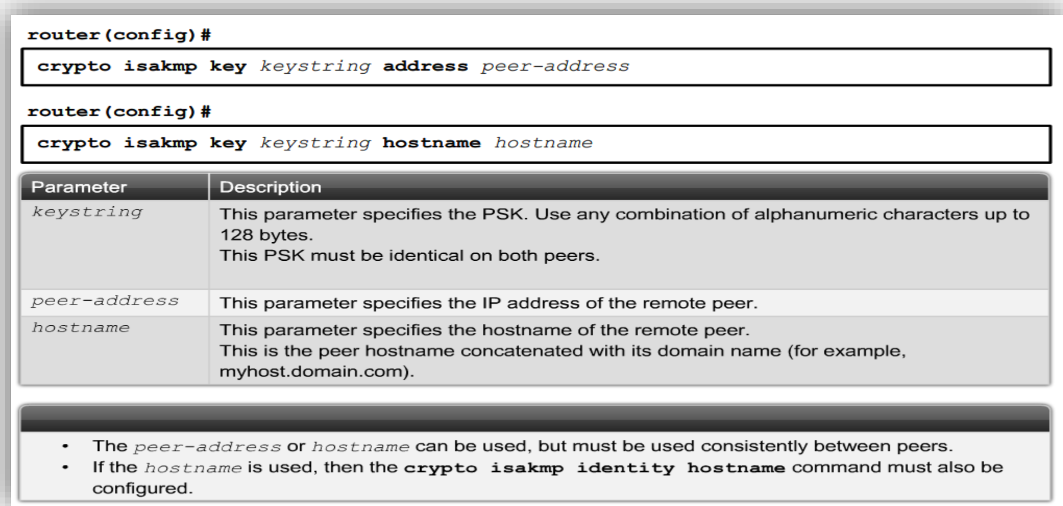
```
R1(config)# crypto isakmp policy 110
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# encryption 3des
R1(config-isakmp)# group 2
R1(config-isakmp)# hash sha
R1(config-isakmp)# lifetime 43200
```

```
R2(config)# crypto isakmp policy 100
R2(config-isakmp)# authentication pre-share
R2(config-isakmp)# encryption 3des
R2(config-isakmp)# group 2
R2(config-isakmp)# hash sha
R2(config-isakmp)# lifetime 43200
```

- R1 attempts to establish a VPN tunnel with R2 because it has interesting traffic destined for R2 and therefore sends its IKE policy parameters.
- R2 must have an ISAKMP policy configured with the same parameters. Notice however, that policy numbers are only locally significant and do not have to match between IPsec peers.

Configuring IPSec Tunnels

- The Pre-SharedKey (PSK) configuration still requires the definition on both routers of the common keyword to use for authentication.

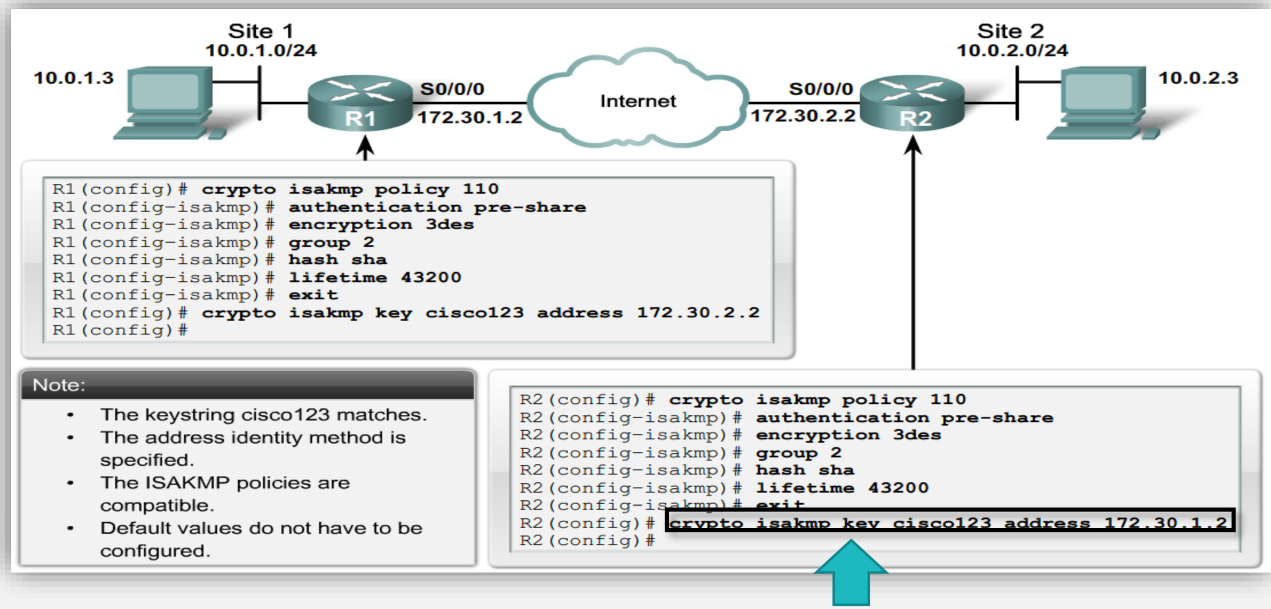


```
router(config)#
crypto isakmp key keystring address peer-address

router(config)#
crypto isakmp key keystring hostname hostname
```

Parameter	Description
keystring	This parameter specifies the PSK. Use any combination of alphanumeric characters up to 128 bytes. This PSK must be identical on both peers.
peer-address	This parameter specifies the IP address of the remote peer.
hostname	This parameter specifies the hostname of the remote peer. This is the peer hostname concatenated with its domain name (for example, myhost.domain.com).

- The *peer-address* or *hostname* can be used, but must be used consistently between peers.
- If the *hostname* is used, then the **crypto isakmp identity hostname** command must also be configured.



```
R1(config)# crypto isakmp policy 110
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# encryption 3des
R1(config-isakmp)# group 2
R1(config-isakmp)# hash sha
R1(config-isakmp)# lifetime 43200
R1(config-isakmp)# exit
R1(config)# crypto isakmp key cisco123 address 172.30.2.2
R1(config)#
```

Note:

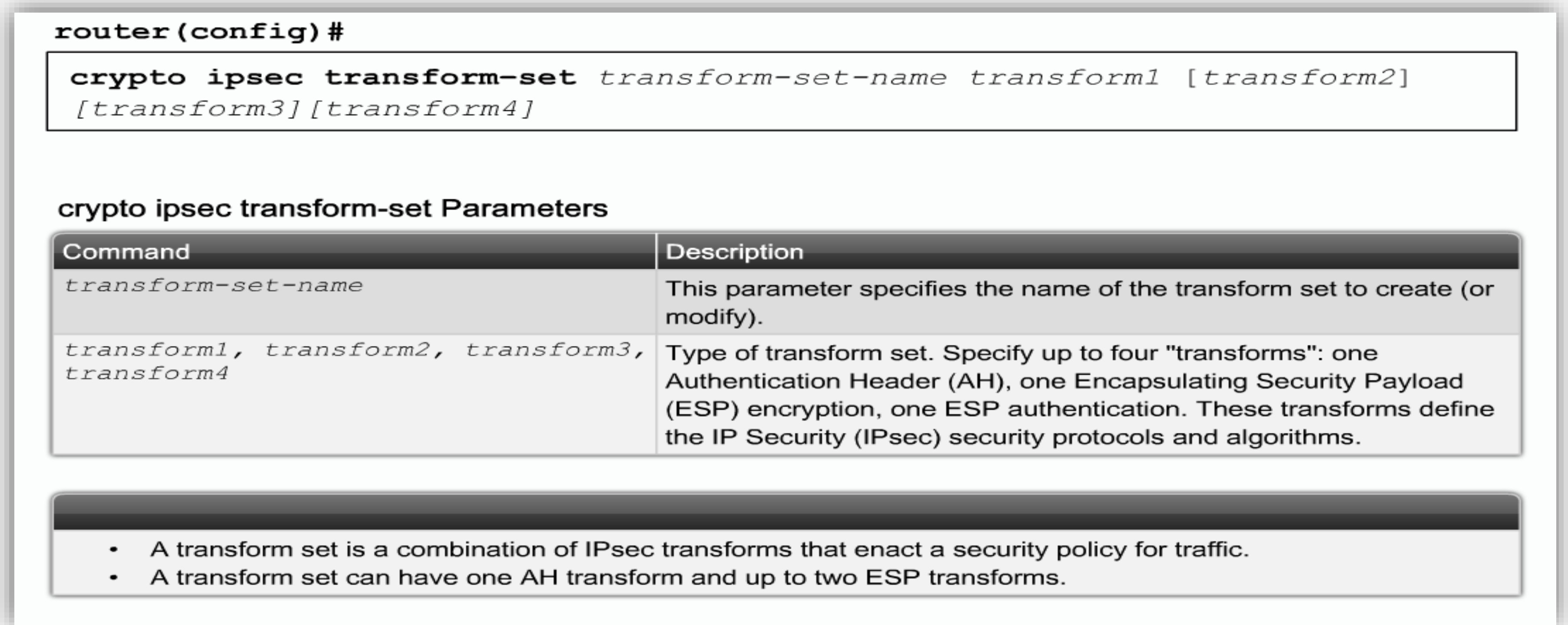
- The keystring cisco123 matches.
- The address identity method is specified.
- The ISAKMP policies are compatible.
- Default values do not have to be configured.

```
R2(config)# crypto isakmp policy 110
R2(config-isakmp)# authentication pre-share
R2(config-isakmp)# encryption 3des
R2(config-isakmp)# group 2
R2(config-isakmp)# hash sha
R2(config-isakmp)# lifetime 43200
R2(config-isakmp)# exit
R2(config)# crypto isakmp key cisco123 address 172.30.1.2
R2(config)#
```

Configuring IPSec Tunnels

- We have after defining the parameters of the second negotiation phase:
  - Configure "Transform Sets" - A combination of IPSec protocols and modes of operation.

Configuring IPSec Tunnels



```
router(config)#
crypto ipsec transform-set transform-set-name transform1 [transform2]
 [transform3][transform4]
```

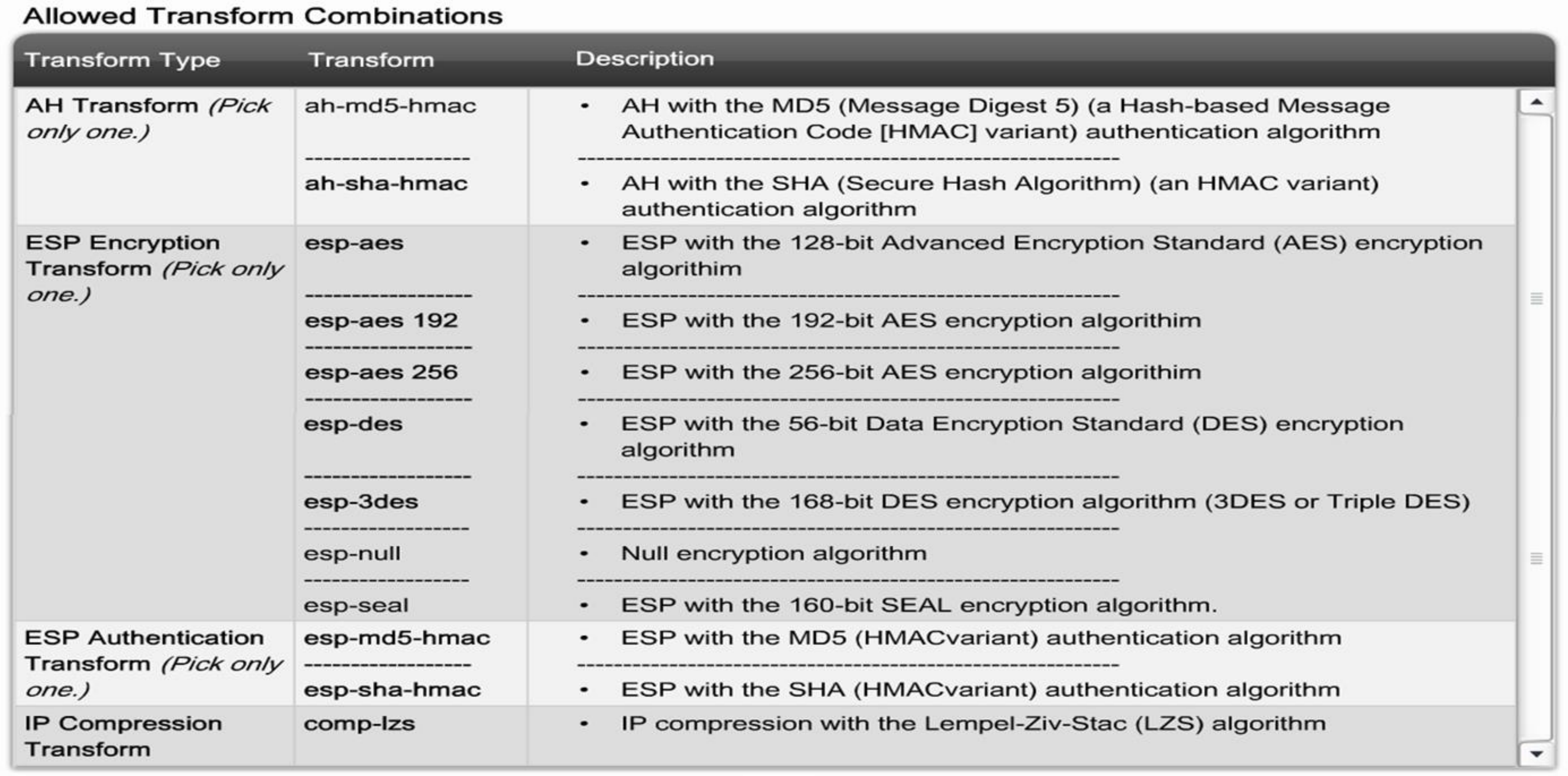
crypto ipsec transform-set Parameters

Command	Description
transform-set-name	This parameter specifies the name of the transform set to create (or modify).
transform1, transform2, transform3, transform4	Type of transform set. Specify up to four "transforms": one Authentication Header (AH), one Encapsulating Security Payload (ESP) encryption, one ESP authentication. These transforms define the IP Security (IPsec) security protocols and algorithms.

- A transform set is a combination of IPsec transforms that enact a security policy for traffic.
- A transform set can have one AH transform and up to two ESP transforms.

Configuring IPSec Tunnels

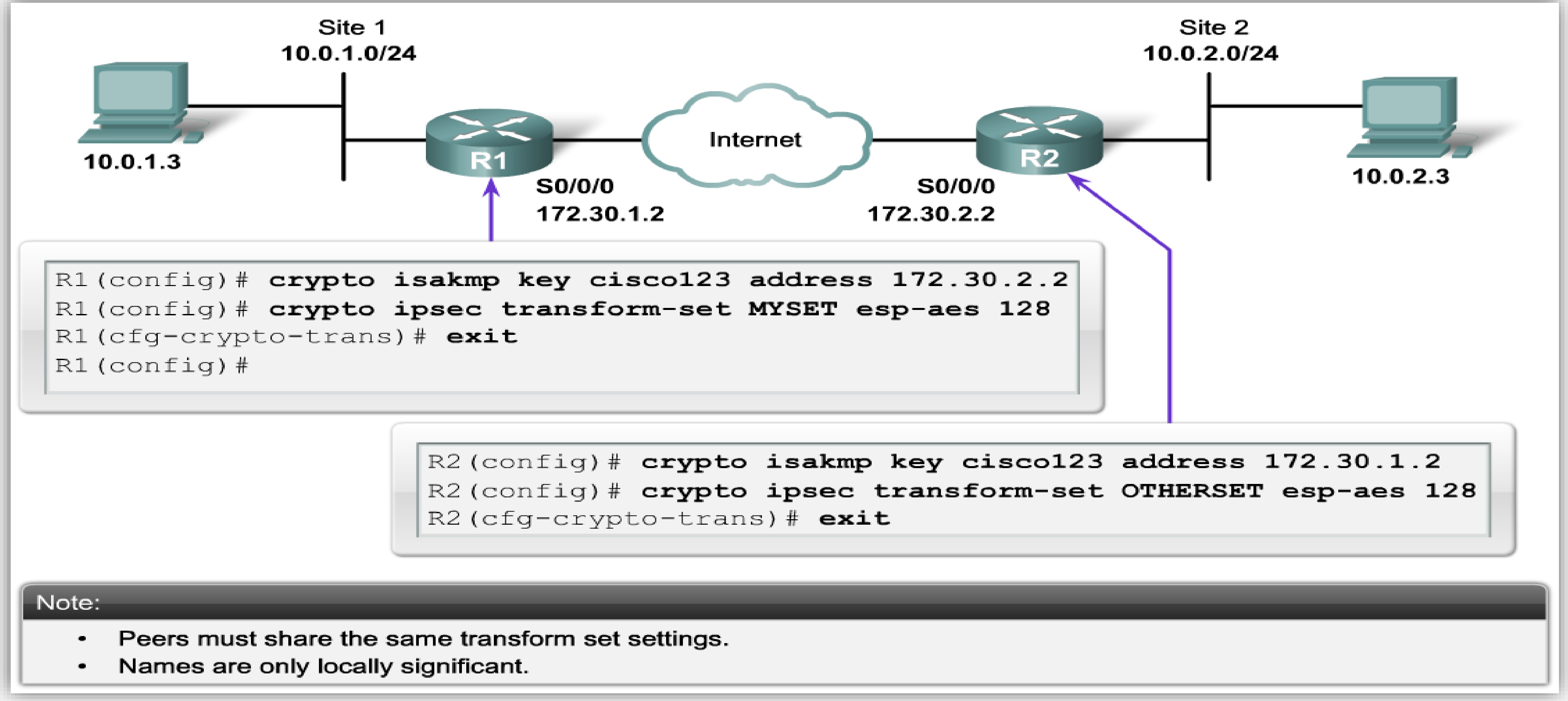
- The possible combinations are as follows:



Allowed Transform Combinations

Transform Type	Transform	Description
AH Transform *(Pick only one.)*	ah-md5-hmac	• AH with the MD5 (Message Digest 5) (a Hash-based Message Authentication Code [HMAC] variant) authentication algorithm
	ah-sha-hmac	• AH with the SHA (Secure Hash Algorithm) (an HMAC variant) authentication algorithm
ESP Encryption Transform *(Pick only one.)*	esp-aes	• ESP with the 128-bit Advanced Encryption Standard (AES) encryption algorithim
	esp-aes 192	• ESP with the 192-bit AES encryption algorithim
	esp-aes 256	• ESP with the 256-bit AES encryption algorithim
	esp-des	• ESP with the 56-bit Data Encryption Standard (DES) encryption algorithm
	esp-3des	• ESP with the 168-bit DES encryption algorithm (3DES or Triple DES)
	esp-null	• Null encryption algorithm
	esp-seal	• ESP with the 160-bit SEAL encryption algorithm.
ESP Authentication Transform *(Pick only one.)*	esp-md5-hmac	• ESP with the MD5 (HMACvariant) authentication algorithm
	esp-sha-hmac	• ESP with the SHA (HMACvariant) authentication algorithm
IP Compression Transform	comp-lzs	• IP compression with the Lempel-Ziv-Stac (LZS) algorithm

Configuring IPSec Tunnels



```
R1(config)# crypto isakmp key cisco123 address 172.30.2.2
R1(config)# crypto ipsec transform-set MYSET esp-aes 128
R1(cfg-crypto-trans)# exit
R1(config)#
```

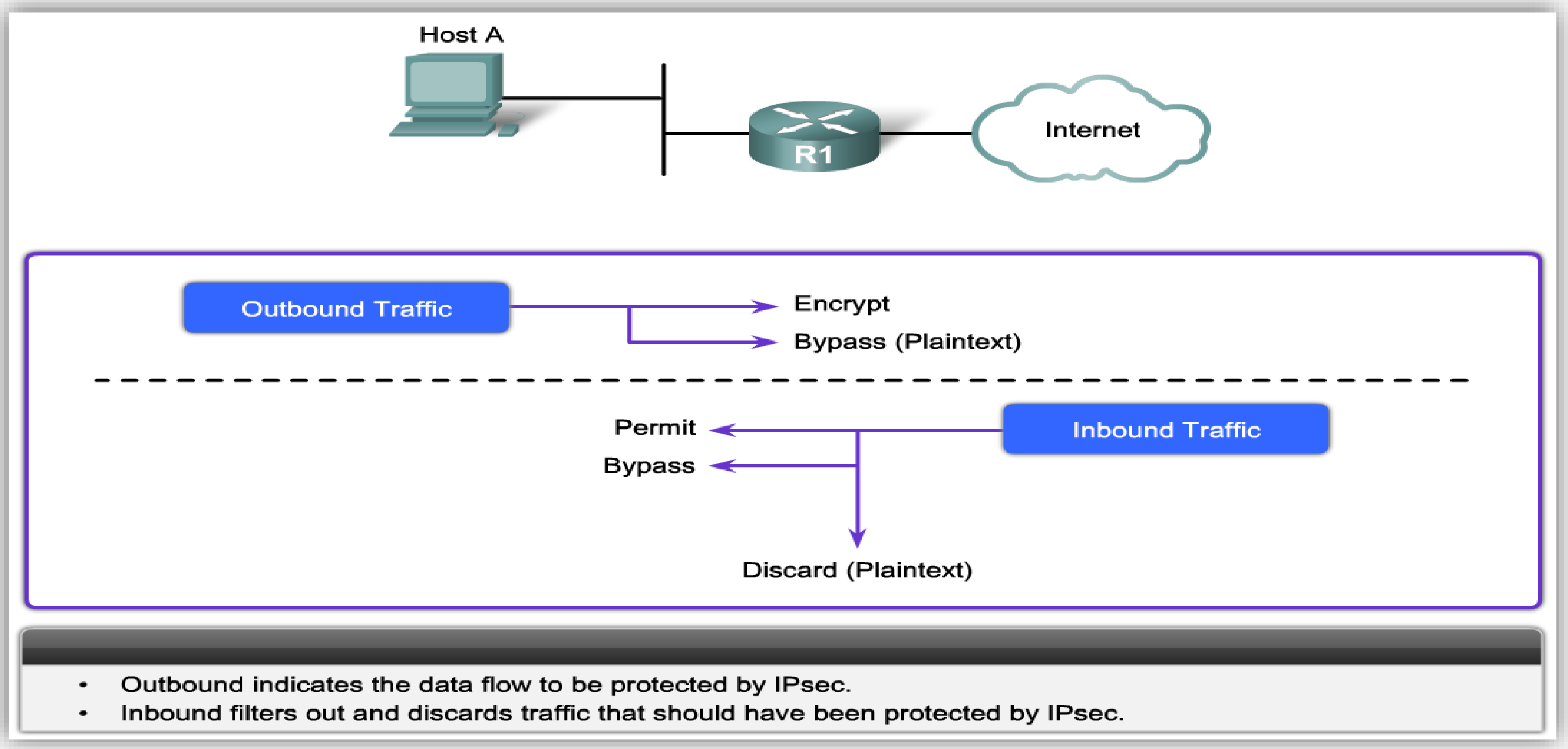
```
R2(config)# crypto isakmp key cisco123 address 172.30.1.2
R2(config)# crypto ipsec transform-set OTHERSET esp-aes 128
R2(cfg-crypto-trans)# exit
```

Note:

- Peers must share the same transform set settings.
- Names are only locally significant.

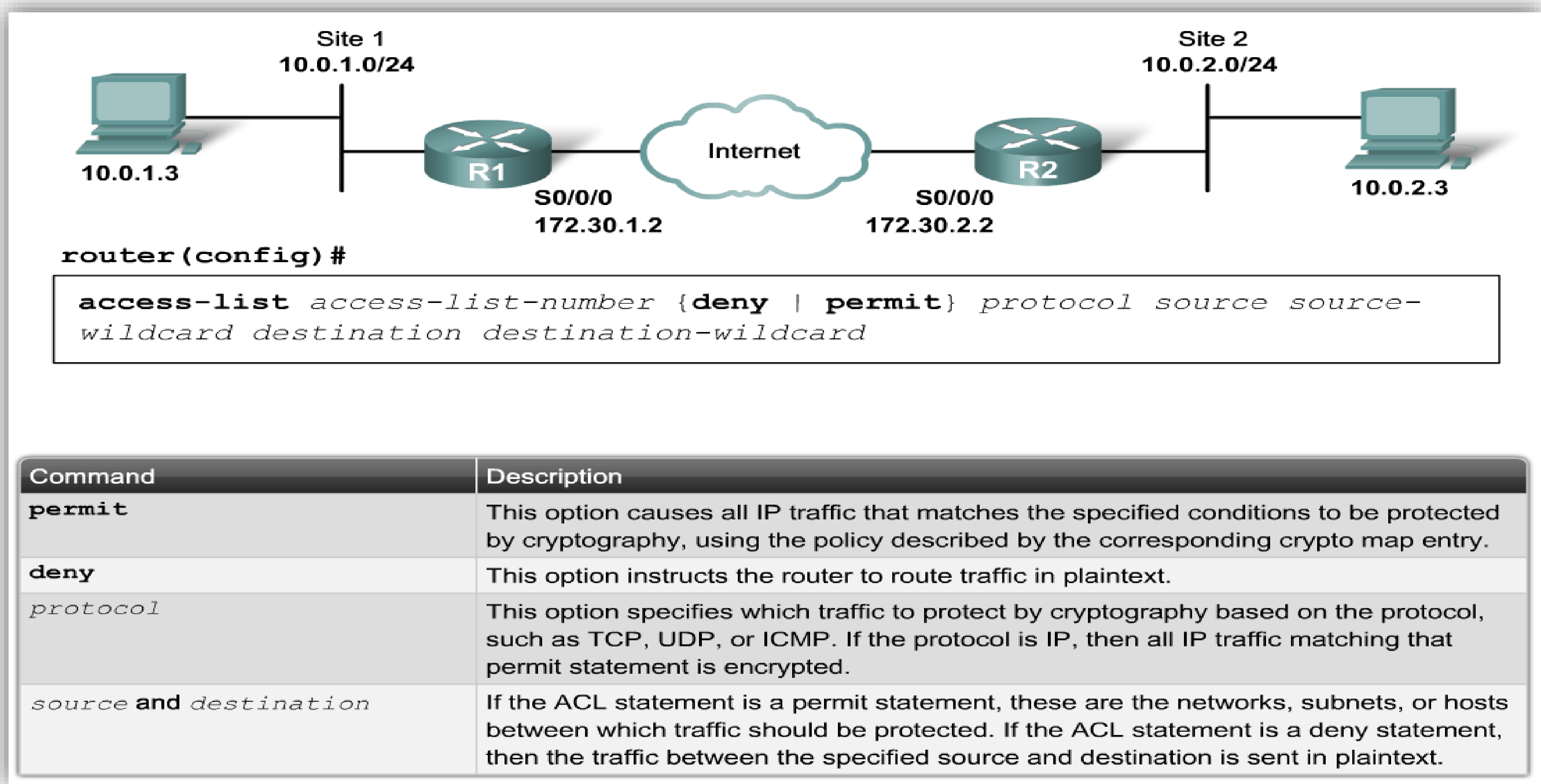
Configuring IPSec Tunnels

- Finally, we have to configure the "Crypto ACLs" to protect traffic:



- Outbound indicates the data flow to be protected by IPsec.
- Inbound filters out and discards traffic that should have been protected by IPsec.

Configuring IPSec Tunnels

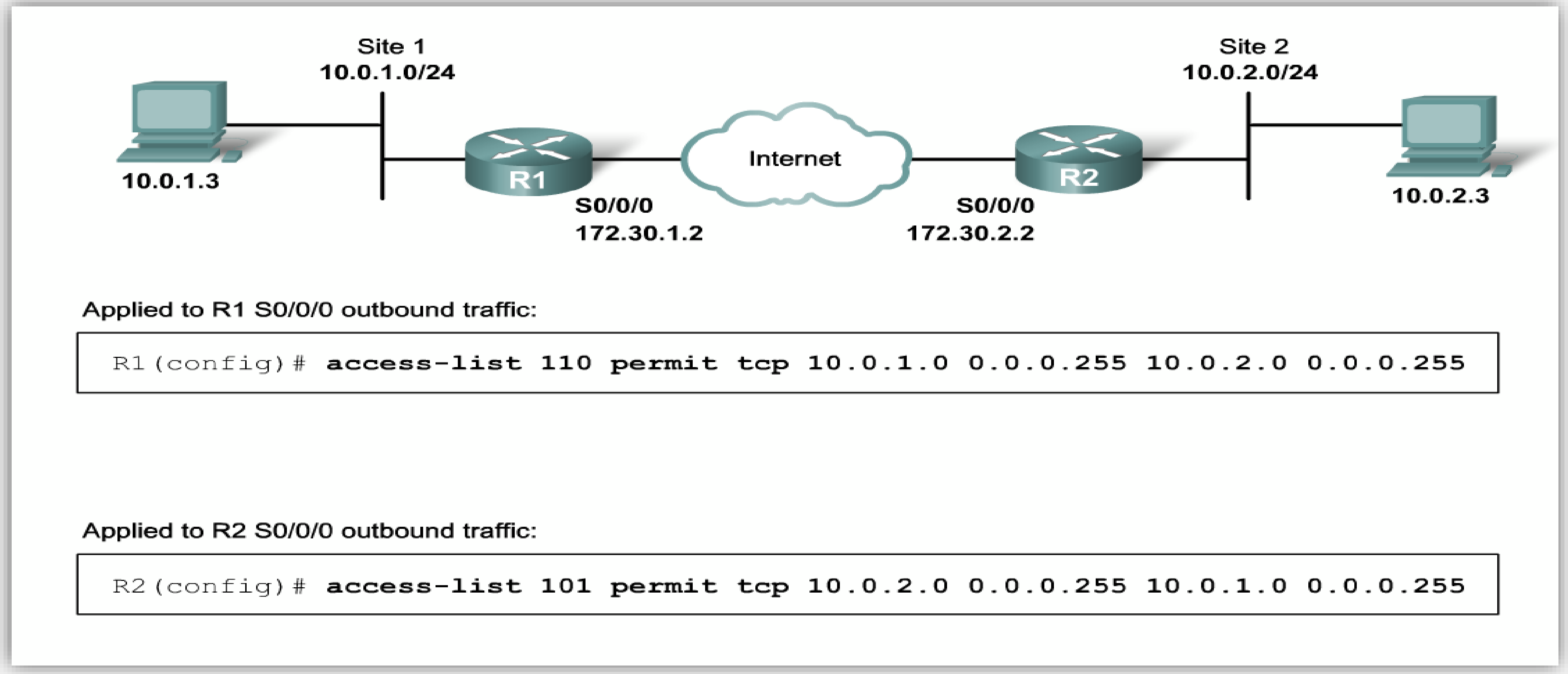


```
router(config)#
```

```
access-list access-list-number {deny | permit} protocol source source-
wildcard destination destination-wildcard
```

Command	Description
permit	This option causes all IP traffic that matches the specified conditions to be protected by cryptography, using the policy described by the corresponding crypto map entry.
deny	This option instructs the router to route traffic in plaintext.
protocol	This option specifies which traffic to protect by cryptography based on the protocol, such as TCP, UDP, or ICMP. If the protocol is IP, then all IP traffic matching that permit statement is encrypted.
source and *destination*	If the ACL statement is a permit statement, these are the networks, subnets, or hosts between which traffic should be protected. If the ACL statement is a deny statement, then the traffic between the specified source and destination is sent in plaintext.

Configuring IPSec Tunnels



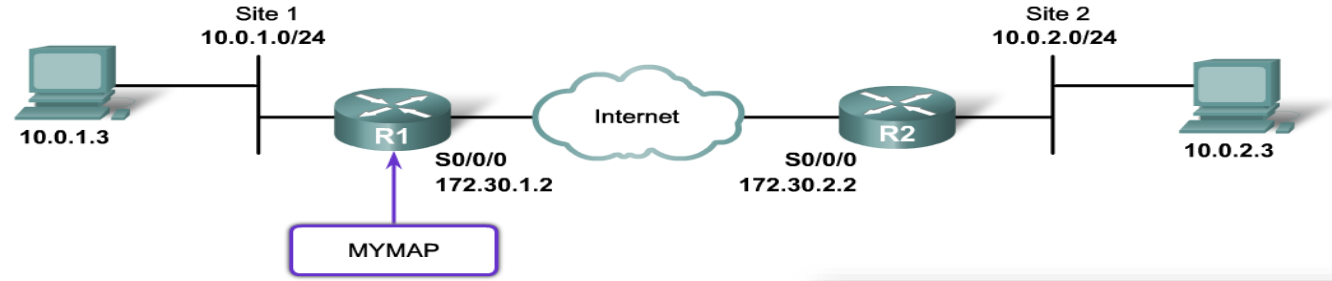
Applied to R1 S0/0/0 outbound traffic:

```
R1(config)# access-list 110 permit tcp 10.0.1.0 0.0.0.255 10.0.2.0 0.0.0.255
```

Applied to R2 S0/0/0 outbound traffic:

```
R2(config)# access-list 101 permit tcp 10.0.2.0 0.0.0.255 10.0.1.0 0.0.0.255
```

Configuring IPSec Tunnels

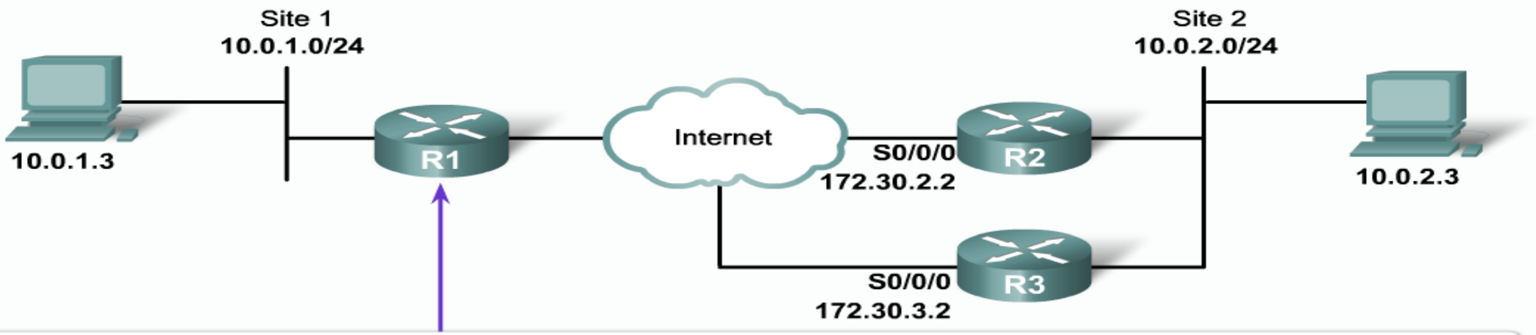


```
router(config-if)#
```

```
crypto map map-name
```

```
R1(config)# interface serial0/0/0
R1(config-if)# crypto map MYMAP
```

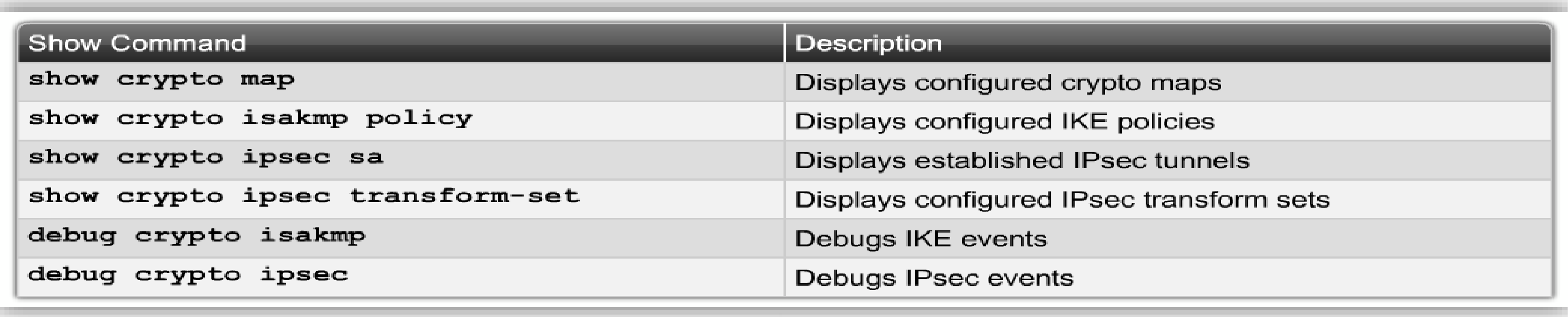
- Applies the crypto map to outgoing interface
- Activates the IPsec policy



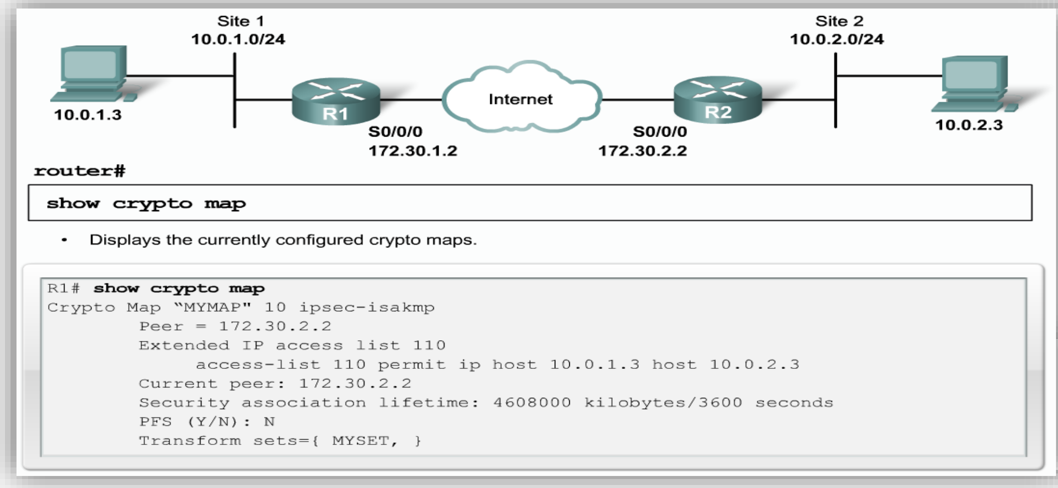
```
R1(config)# crypto map MYMAP 10 ipsec-isakmp
R1(config-crypto-map)# match address 110
R1(config-crypto-map)# set peer 172.30.2.2 default
R1(config-crypto-map)# set peer 172.30.3.2
R1(config-crypto-map)# set pfs group1
R1(config-crypto-map)# set transform-set mine
R1(config-crypto-map)# set security-association lifetime seconds 86400
```

- Multiple peers can be specified for redundancy.

Configuration check



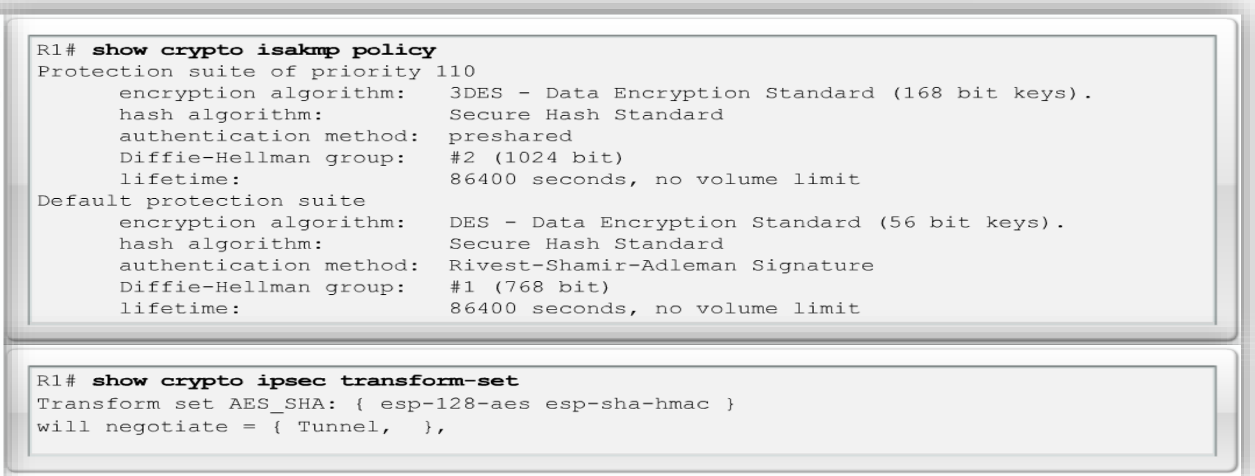
Show Command	Description
`show crypto map`	Displays configured crypto maps
`show crypto isakmp policy`	Displays configured IKE policies
`show crypto ipsec sa`	Displays established IPsec tunnels
`show crypto ipsec transform-set`	Displays configured IPsec transform sets
`debug crypto isakmp`	Debugs IKE events
`debug crypto ipsec`	Debugs IPsec events



```
router#
show crypto map
```

- Displays the currently configured crypto maps.

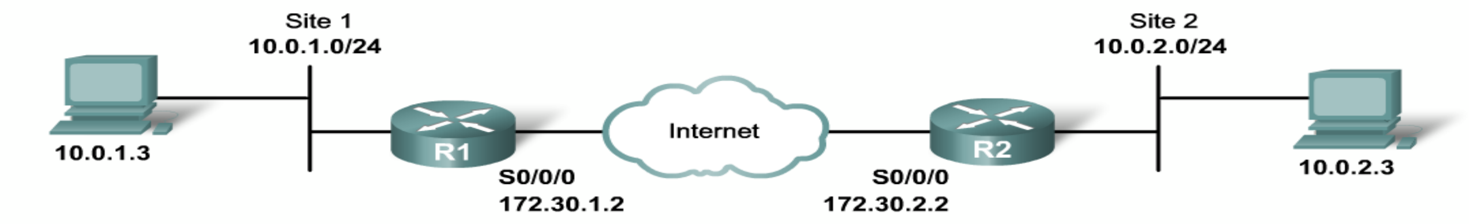
```
R1# show crypto map
Crypto Map "MYMAP" 10 ipsec-isakmp
        Peer = 172.30.2.2
        Extended IP access list 110
             access-list 110 permit ip host 10.0.1.3 host 10.0.2.3
        Current peer: 172.30.2.2
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={ MYSET, }
```

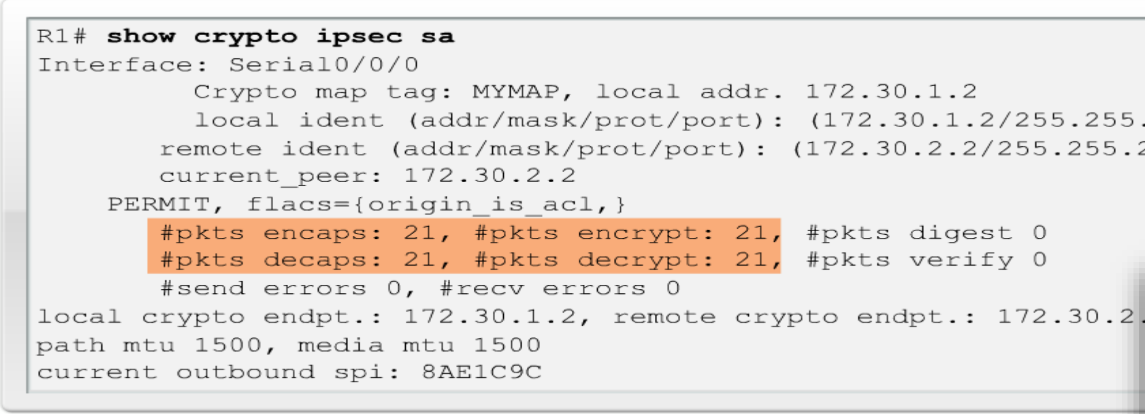


```
R1# show crypto isakmp policy
Protection suite of priority 110
        encryption algorithm:   3DES - Data Encryption Standard (168 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  preshared
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               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
```

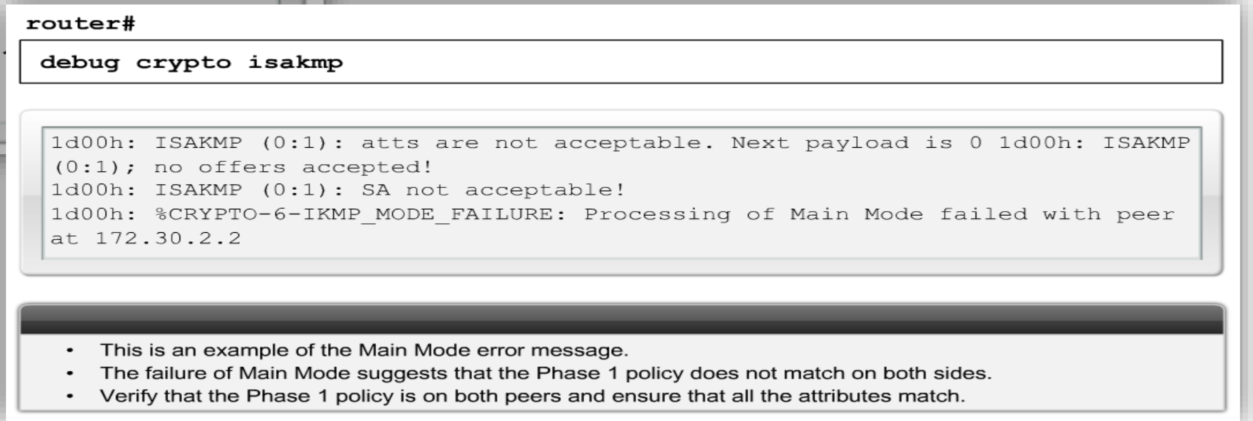
```
R1# show crypto ipsec transform-set
Transform set AES_SHA: { esp-128-aes esp-sha-hmac }
will negotiate = { Tunnel,  },
```

Configuration check





```
R1# show crypto ipsec sa
Interface: Serial0/0/0
          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, flacs={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.
path mtu 1500, media mtu 1500
current outbound spi: 8AE1C9C
```



```
router#
debug crypto isakmp
```

```
1d00h: ISAKMP (0:1): atts are not acceptable. Next payload is 0 1d00h: ISAKMP
(0:1); no offers accepted!
1d00h: ISAKMP (0:1): SA not acceptable!
1d00h: %CRYPTO-6-IKMP_MODE_FAILURE: Processing of Main Mode failed with peer
at 172.30.2.2
```

- This is an example of the Main Mode error message.
- The failure of Main Mode suggests that the Phase 1 policy does not match on both sides.
- Verify that the Phase 1 policy is on both peers and ensure that all the attributes match.

Pre-Requisites -Exercise 2

- Use the server and client for the second test.
- On the Windows server 2012 server disable NAT.

Exercise 2 - VPN in windows environment

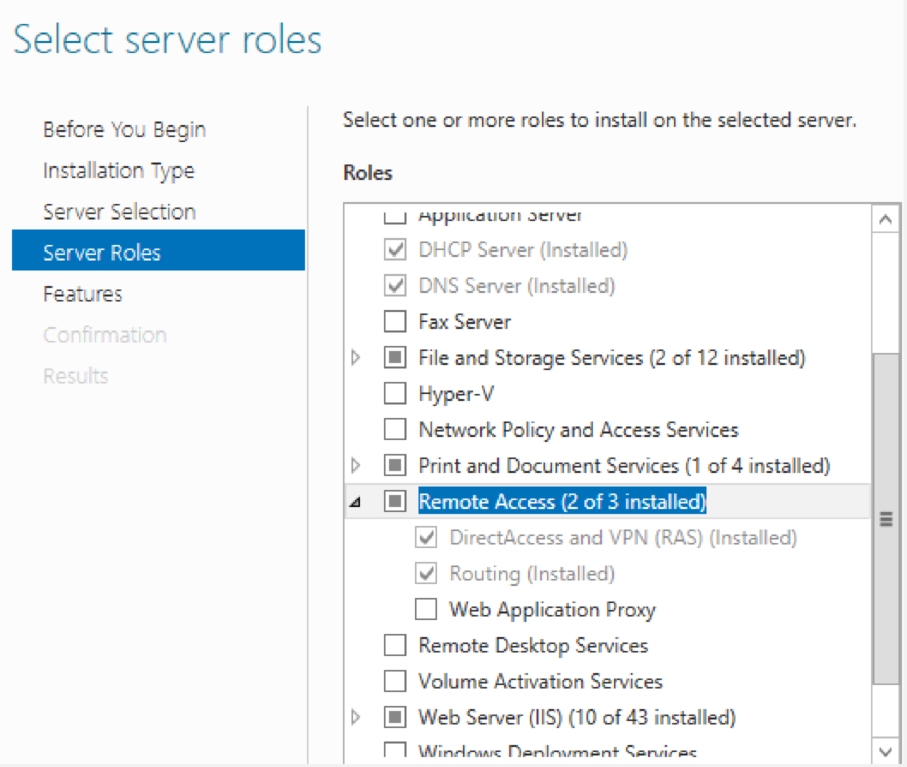
Exercise 2

- The company SR1.SA wants to implement a VPN remote access solution for its vendors.
- As you do not have a big budget and want to test how this solution works, it was decided to make this VPN on Windows 2012 R2 using your SMTP server.
- Install the service
- Configure the remote service on the server:
- Enter 3 addresses from your network to be made available for remote connections.
- Choose L2TP as VPN protocol
- Configure the connection on the client
- **Try to access the created VPN on the client.**

How To

Service installation

- Access of remote computers to the server is done through the remote access service



Select server roles

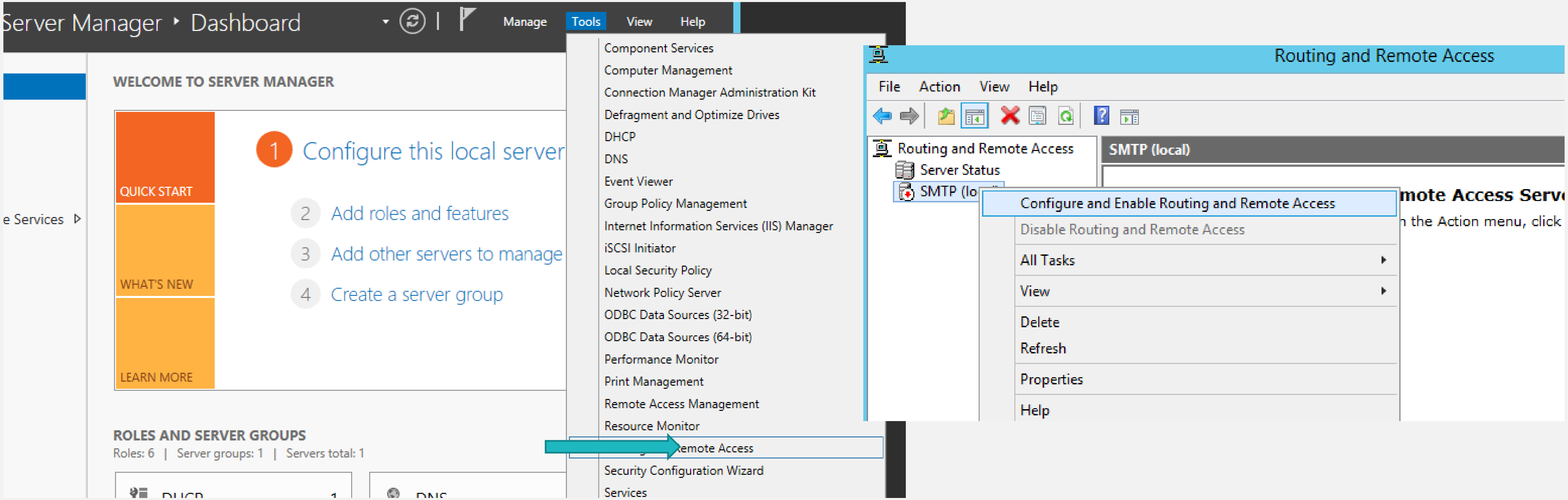
- Before You Begin
- Installation Type
- Server Selection
- **Server Roles**
- Features
- Confirmation
- Results

Select one or more roles to install on the selected server.

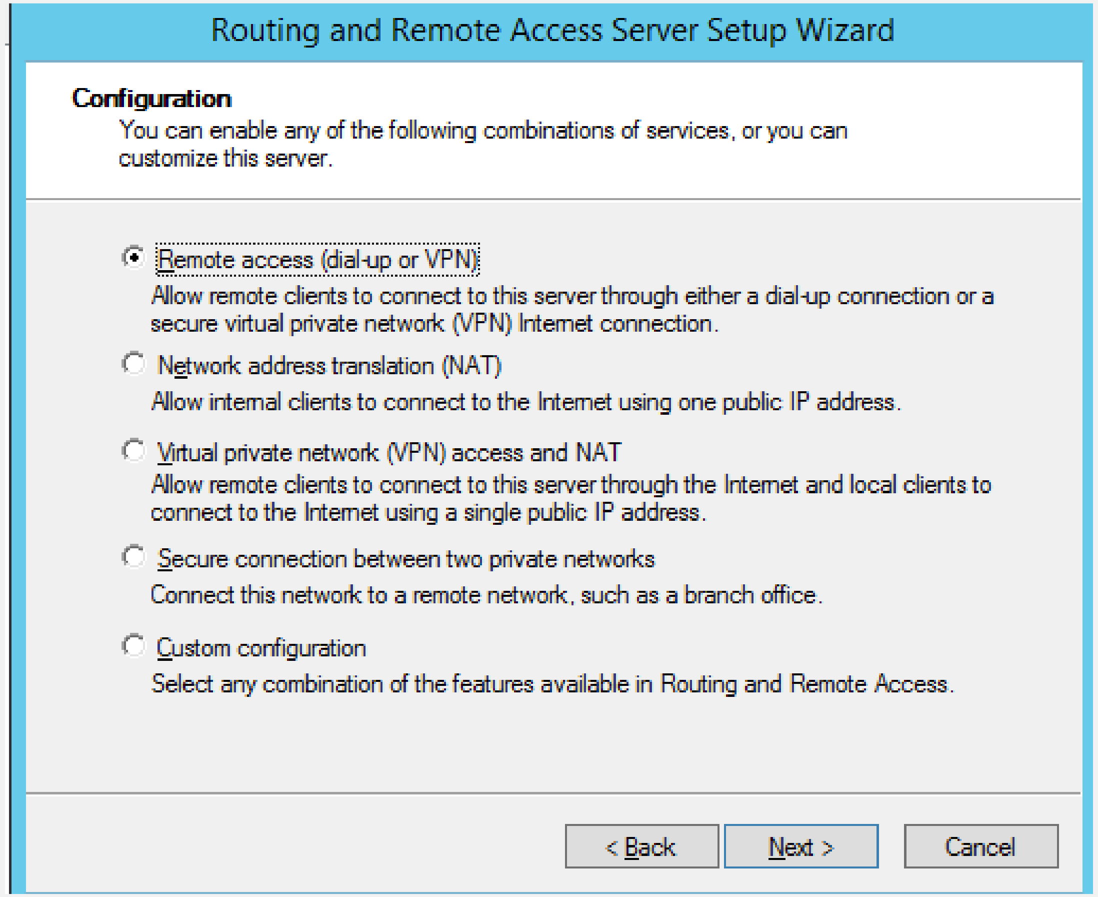
Roles

☐ Application Server
☑ DHCP Server (Installed)
☑ DNS Server (Installed)
☐ Fax Server
▷ ▣ File and Storage Services (2 of 12 installed)
☐ Hyper-V
☐ Network Policy and Access Services
▷ ▣ Print and Document Services (1 of 4 installed)
◢ ▣ Remote Access (2 of 3 installed)
    ☑ DirectAccess and VPN (RAS) (Installed)
    ☑ Routing (Installed)
    ☐ Web Application Proxy
☐ Remote Desktop Services
☐ Volume Activation Services
▷ ▣ Web Server (IIS) (10 of 43 installed)
☐ Windows Deployment Services

Service configuration



Service configuration



Routing and Remote Access Server Setup Wizard

Configuration

You can enable any of the following combinations of services, or you can customize this server.

● Remote access (dial-up or VPN)

Allow remote clients to connect to this server through either a dial-up connection or a secure virtual private network (VPN) Internet connection.

○ Network address translation (NAT)

Allow internal clients to connect to the Internet using one public IP address.

○ Virtual private network (VPN) access and NAT

Allow remote clients to connect to this server through the Internet and local clients to connect to the Internet using a single public IP address.

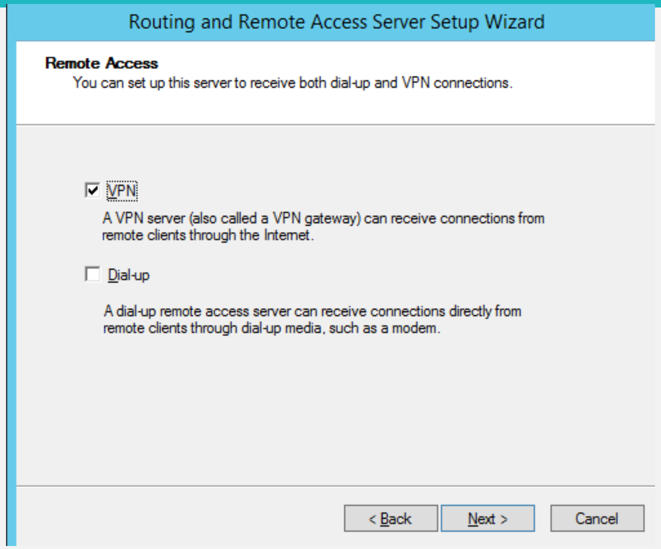
○ Secure connection between two private networks

Connect this network to a remote network, such as a branch office.

○ Custom configuration

Select any combination of the features available in Routing and Remote Access.

Service configuration



Routing and Remote Access Server Setup Wizard

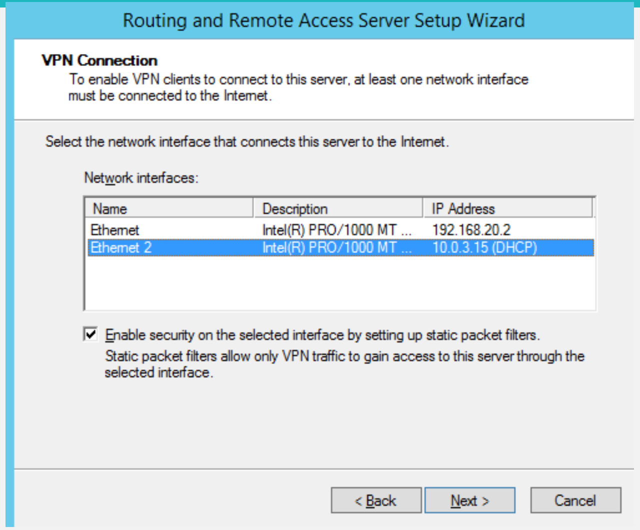
Remote Access
You can set up this server to receive both dial-up and VPN connections.

☑ VPN

A VPN server (also called a VPN gateway) can receive connections from remote clients through the Internet.

□ Dial-up

A dial-up remote access server can receive connections directly from remote clients through dial-up media, such as a modem.



Routing and Remote Access Server Setup Wizard

VPN Connection
To enable VPN clients to connect to this server, at least one network interface must be connected to the Internet.

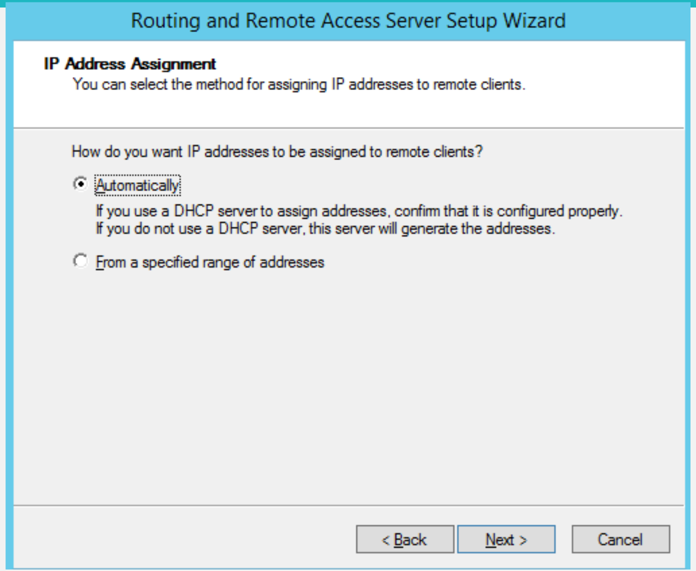
Select the network interface that connects this server to the Internet.

Network interfaces:

Name	Description	IP Address
Ethernet	Intel(R) PRO/1000 MT ...	192.168.20.2
Ethernet 2	Intel(R) PRO/1000 MT ...	10.0.3.15 (DHCP)

☑ Enable security on the selected interface by setting up static packet filters.

Static packet filters allow only VPN traffic to gain access to this server through the selected interface.



Routing and Remote Access Server Setup Wizard

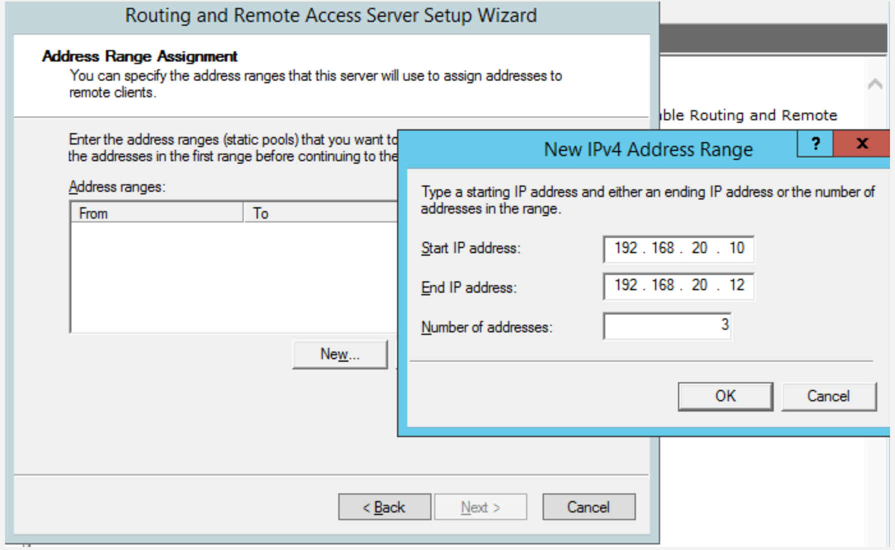
IP Address Assignment
You can select the method for assigning IP addresses to remote clients.

How do you want IP addresses to be assigned to remote clients?

● Automatically

If you use a DHCP server to assign addresses, confirm that it is configured properly.
If you do not use a DHCP server, this server will generate the addresses.

○ From a specified range of addresses



Routing and Remote Access Server Setup Wizard

Address Range Assignment
You can specify the address ranges that this server will use to assign addresses to remote clients.

Enter the address ranges (static pools) that you want to
the addresses in the first range before continuing to the

Address ranges:

From	To

ble Routing and Remote

New IPv4 Address Range

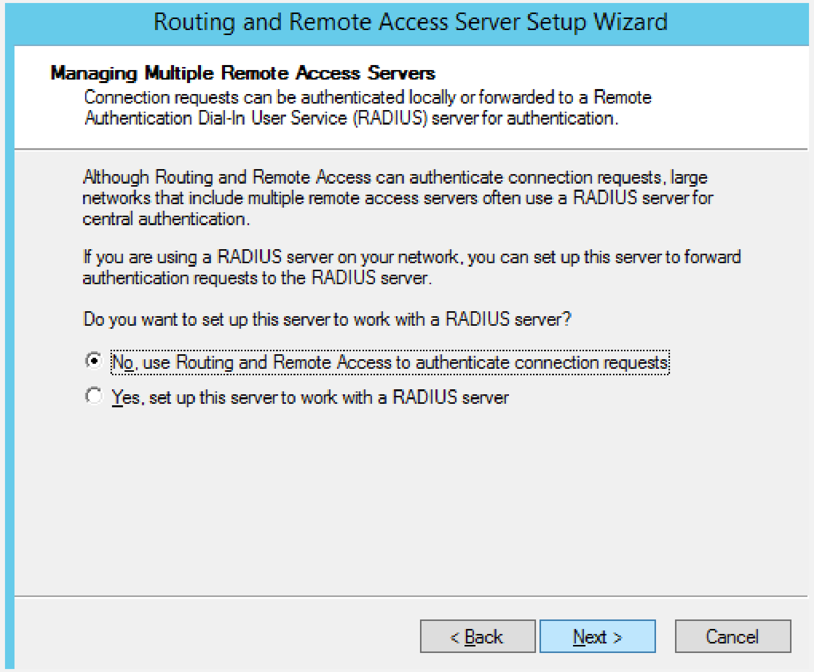
Type a starting IP address and either an ending IP address or the number of addresses in the range.

Start IP address: 192 . 168 . 20 . 10

End IP address: 192 . 168 . 20 . 12

Number of addresses: 3

Service configuration



Routing and Remote Access Server Setup Wizard

Managing Multiple Remote Access Servers

Connection requests can be authenticated locally or forwarded to a Remote Authentication Dial-In User Service (RADIUS) server for authentication.

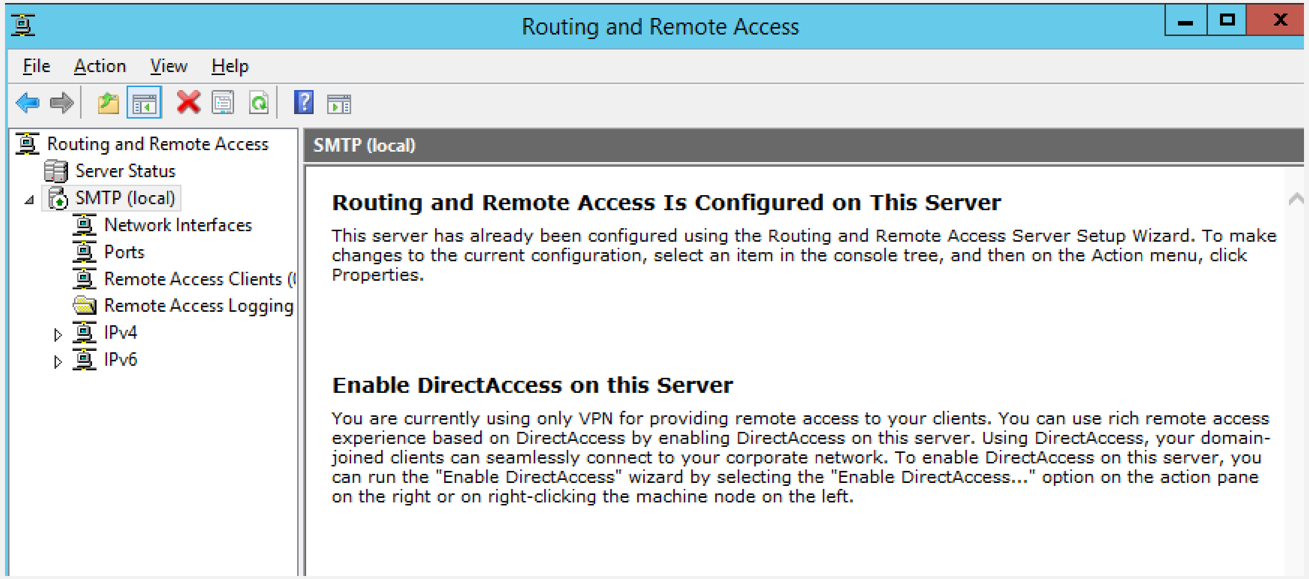
Although Routing and Remote Access can authenticate connection requests, large networks that include multiple remote access servers often use a RADIUS server for central authentication.

If you are using a RADIUS server on your network, you can set up this server to forward authentication requests to the RADIUS server.

Do you want to set up this server to work with a RADIUS server?

● No, use Routing and Remote Access to authenticate connection requests

○ Yes, set up this server to work with a RADIUS server



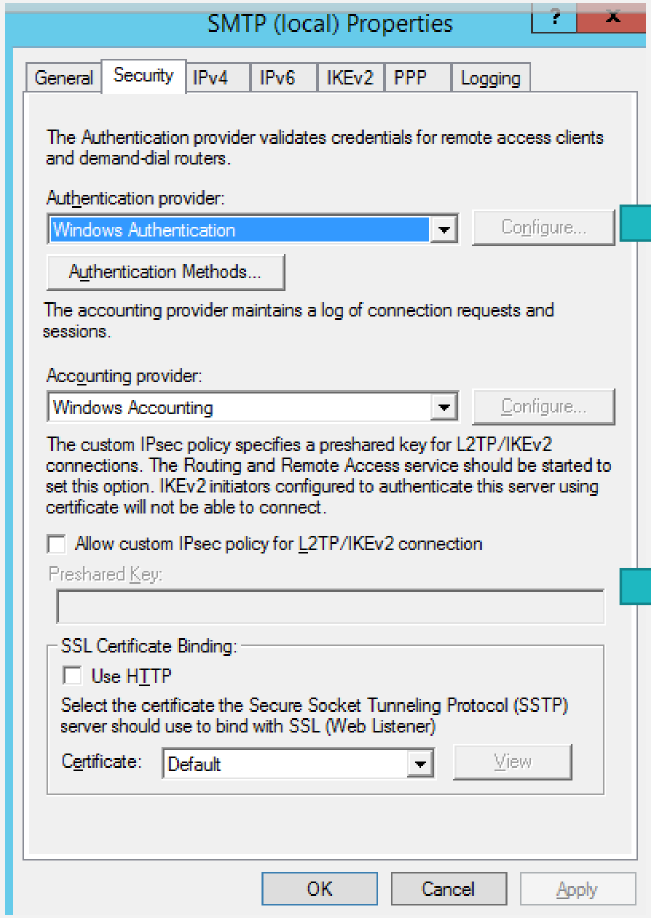
Routing and Remote Access Is Configured on This Server

This server has already been configured using the Routing and Remote Access Server Setup Wizard. To make changes to the current configuration, select an item in the console tree, and then on the Action menu, click Properties.

Enable DirectAccess on this Server

You are currently using only VPN for providing remote access to your clients. You can use rich remote access experience based on DirectAccess by enabling DirectAccess on this server. Using DirectAccess, your domain-joined clients can seamlessly connect to your corporate network. To enable DirectAccess on this server, you can run the "Enable DirectAccess" wizard by selecting the "Enable DirectAccess..." option on the action pane on the right or on right-clicking the machine node on the left.

Service configuration



The Authentication provider validates credentials for remote access clients and demand-dial routers.

Authentication provider: Windows Authentication

The accounting provider maintains a log of connection requests and sessions.

Accounting provider: Windows Accounting

The custom IPsec policy specifies a preshared key for L2TP/IKEv2 connections. The Routing and Remote Access service should be started to set this option. IKEv2 initiators configured to authenticate this server using certificate will not be able to connect.

☐ Allow custom IPsec policy for L2TP/IKEv2 connection

Preshared Key:

SSL Certificate Binding:

☐ Use HTTP

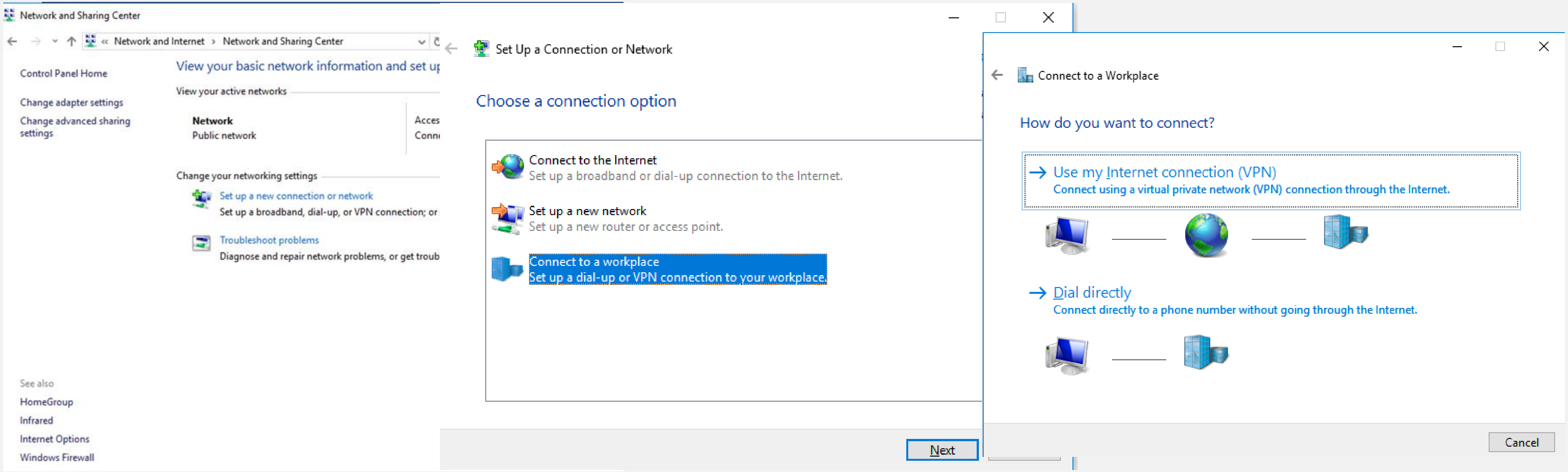
Select the certificate the Secure Socket Tunneling Protocol (SSTP) server should use to bind with SSL (Web Listener)

Certificate: Default

Client Authentication Type

Tunnel management type and data encapsulation

Client Configuration



Network and Sharing Center
Network and Internet › Network and Sharing Center
Control Panel Home
Change adapter settings
Change advanced sharing settings
See also
HomeGroup
Infrared
Internet Options
Windows Firewall
Set Up a Connection or Network
Next
Connect to a Workplace
Cancel

View your basic network information and set u

View your active networks

Network
Public network

Acces
Conn

Change your networking settings

Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or

Troubleshoot problems
Diagnose and repair network problems, or get troub

Choose a connection option

Connect to the Internet
Set up a broadband or dial-up connection to the Internet.

Set up a new network
Set up a new router or access point.

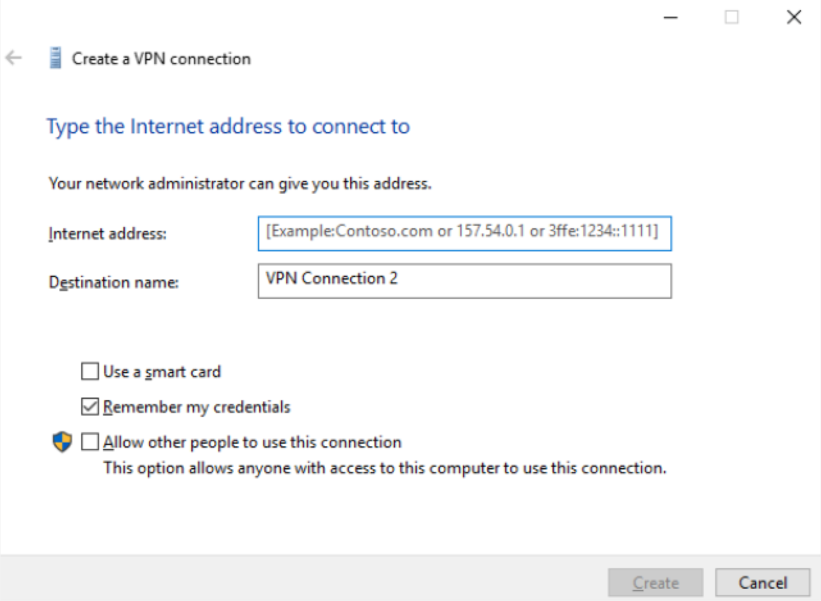
Connect to a workplace
Set up a dial-up or VPN connection to your workplace.

How do you want to connect?

→ Use my Internet connection (VPN)
Connect using a virtual private network (VPN) connection through the Internet.

→ Dial directly
Connect directly to a phone number without going through the Internet.

Client Configuration



Create a VPN connection

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: [Example:Contoso.com or 157.54.0.1 or 3ffe:1234::1111]

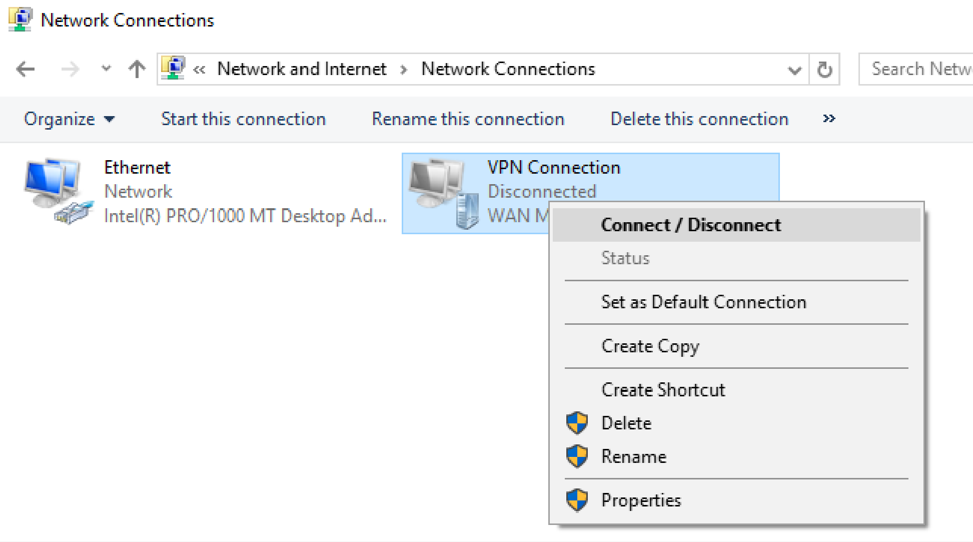
Destination name: VPN Connection 2

☐ Use a smart card

☑ Remember my credentials

☐ Allow other people to use this connection

This option allows anyone with access to this computer to use this connection.



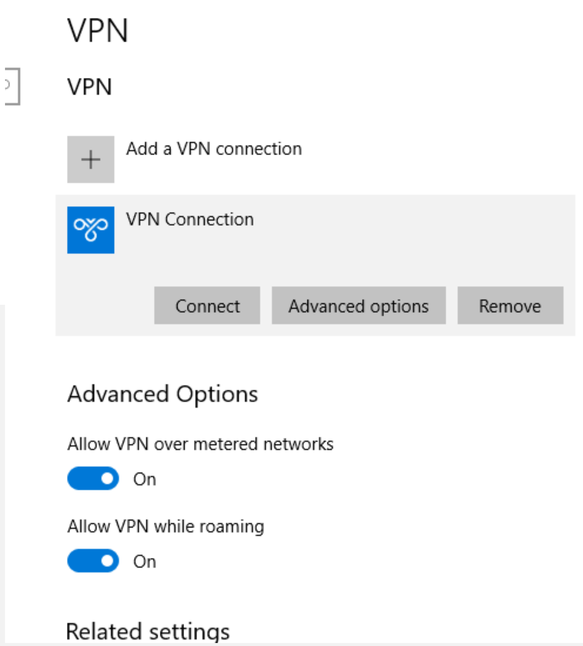
Network Connections

« Network and Internet › Network Connections

Search Network Connecti

Ethernet
Network
Intel(R) PRO/1000 MT Desktop Ad...

VPN Connection
Disconnected
WAN M



VPN

VPN

VPN Connection

Advanced Options

Allow VPN over metered networks

● On

Allow VPN while roaming

● On

Related settings

Doubts

References

- Cisco Networking Academy – Packet Tracer – Configuring VPNs