Serviços de Rede 1 –

Aula 12 - Práticas

2019-2020

Instituto Politécnico de Coimbra

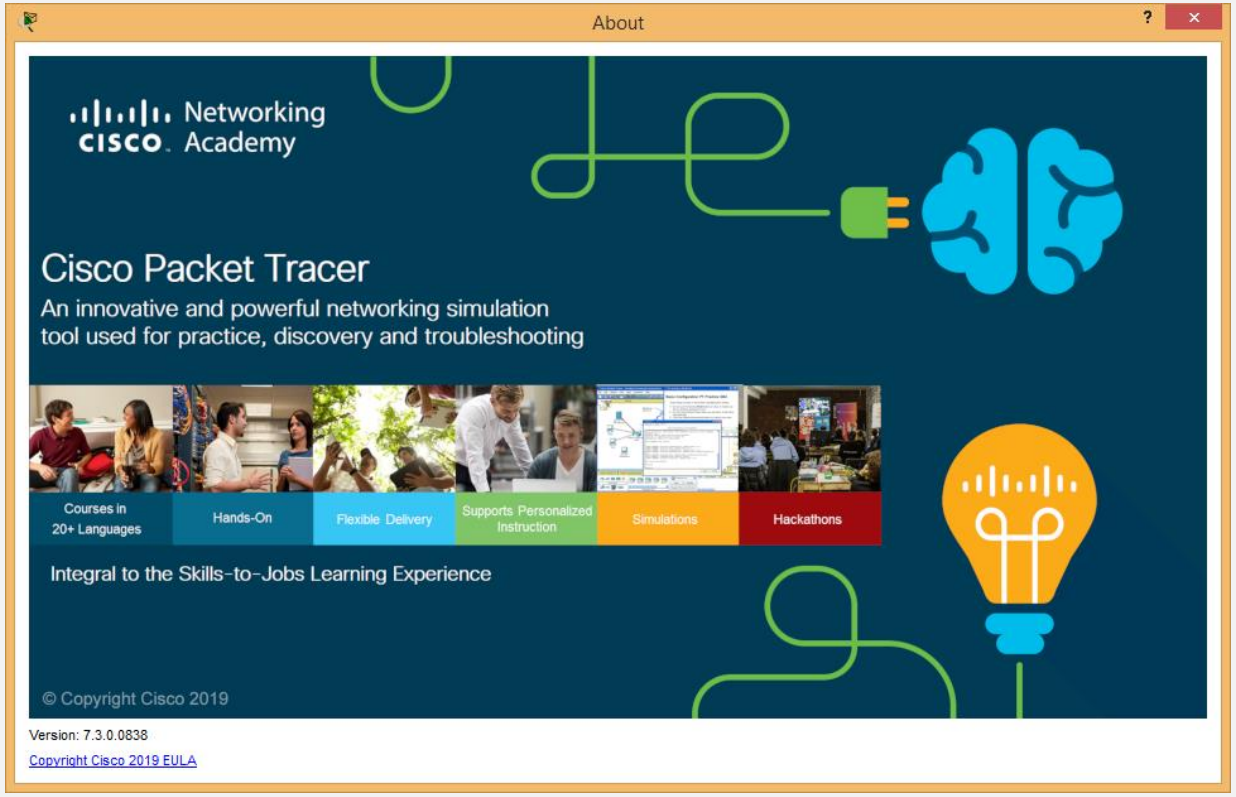
Departamento de Engenharia Informática

Nota Importante

- Dia 8 de junho (16:30-18:30) será realizado o 3º teste prático.
  - Peso – 3 valores em 20.
  - Matéria:
    - NTP (aula 9)
    - Proxy (aula 10 e parte da aula 11)
    - VPN (parte da aula 11 e aula 12)
  - Inscrição obrigatória no Moodle.
- Devem ter instalado o Virtual Box 6.0.
- Devem antecipadamente importar para o VirtualBox as imagens do Windows Server 2012 e do Windows 8/10 "limpas".
- Devem ter o *Cisco Packet Tracer* versão 7.3.0 instalado.

Pre – Requisitos -Exercício

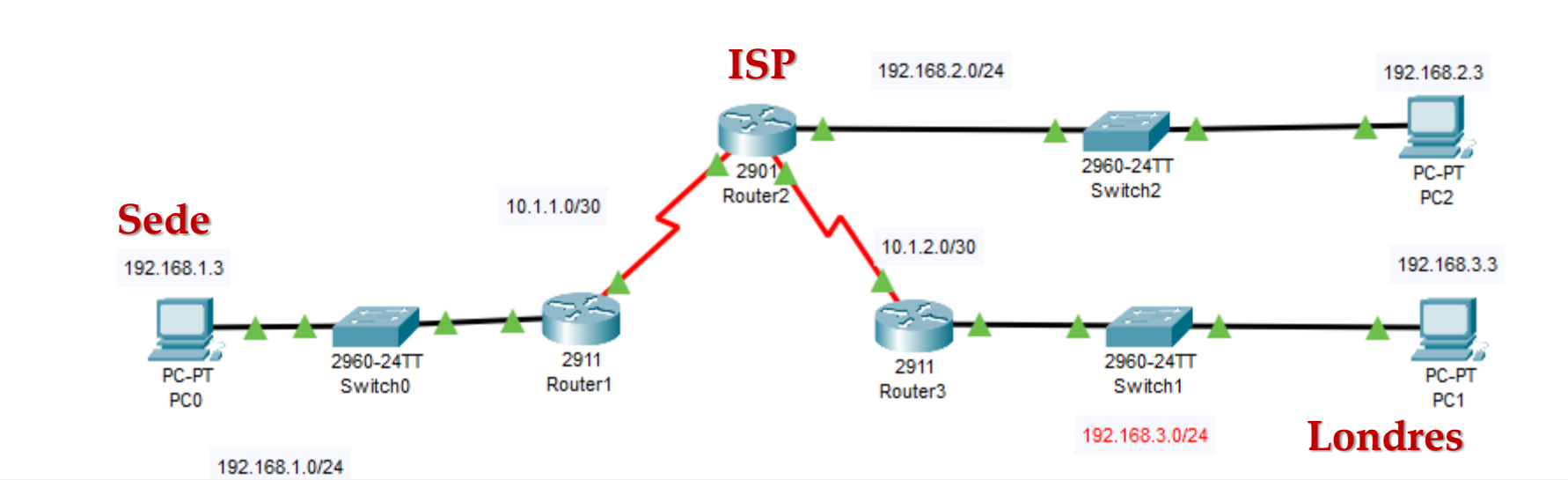
- Ter instalado o *Cisco Packet Tracer* versão 7.3.0



Exercício – VPN IPSec em ambiente Cisco

Exercício

- A empresa SR1.SA, deseja ligar a sede (192.168.1.0/24) a uma delegação localizada em Londres (192.168.3.0/24). Para tal deseja utilizar um túnel seguro. Decidiu utilizar o IPSec para fazer essa ligação entre a sede e a delagação.
- A topologia é a seguinte:



Exercício

- Grave a simulação como VPN_IPSEC.
- Coloque os endereços IP dos diferentes equipamentos de forma fixa e de acordo com as redes indicadas na imagem.
- Altere o nome dos routrs para:
  - R1 – R_Sede
  - R2 - R_ISP
  - R3 - R_Dele
- Desabilite o "*IP Domain Name System hostname translation*"
- Coloque apenas uma rota por defeito no router 1 e router 2.
- Tente pingar do PC0 para o PC2.
- Tente pingar do PC0 para o PC1. Não deve conseguir…

Exercício

- Crie uma VPN entre o R1 e R3 com as seguintes definições:

Parâmetros da 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

Parâmetros da 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

Nota: Os parâmetros por *defaut* (estão a negrito) não necessitam de ser escritos na configuração do router

Exercício

- Etapas
  - Defina as access-list nos router 1 e router 3.

    access-list 110 permit ***ip rede origem rede destino***
  - Configure the ISAKMP Phase 1.
  - Configure the ISAKMP Phase 2.
  - Ligue o crypto map à interface de saída.
  - Verifique o estado do seu túnel.
  - Gere trafego que vai ser encriptado (por exemplo do PC0 para o PC1).
  - Verifique o estado do seu túnel.

Exercício

```
R_Delega#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):
(192.168.3.0/255.255.255.0/0/0)
   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: 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

     local crypto endpt.: 10.1.2.1, remote crypto endpt.:10.1.1.1
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/3/0
     current outbound spi: 0x0(0)
```

Antes de gerar tráfego encriptado

```
R_Delega#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):
(192.168.3.0/255.255.255.0/0/0)
   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: 2, #pkts decrypt: 2, #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

     local crypto endpt.: 10.1.2.1, remote crypto endpt.:10.1.1.1
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/3/0
     current outbound spi: 0x06264741(103171905)
```

Depois de gerar tráfego encriptado

Exercício

- Teste se o PC2 consegue chegar ao PC0.
- Veja o que aconteceu com o trafego que não passa pelo túnel IPSec. Se tudo correr bem, deve conseguir "pingar" o PC e não "acrescentar" trafego encriptado no túnel.
- Volte a pingar do PC0 para o PC1. O que aconteceu ao tráfego encriptado no túnel?

```
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

- É possível que tenha de ativar *Security Technology Package license* em alguns routers. Para isso:
  - Faça **show version** em modo ***Enable***:

```
-----------------------------------------------------------------
Technology     Technology-package          Technology-package
               Current       Type          Next reboot
-----------------------------------------------------------------
ipbase         ipbasek9      Permanent     ipbasek9
security       None          None          None
uc             None          None          None
data           None          None          None
```

É necessário

```
---
Technology     Technology-package                    Technology-package
               Current                 Type          Next reboot
-----------------------------------------------------------------------
---
appxk9         None              None                None
uck9           None              None                None
securityk9     securityk9        Permanent           securityk9
ipbase         ipbasek9          Permanent           ipbasek9
security       securityk9        Permanent           securityk9
ipbase         ipbasek9          Permanent           ipbasek9

cisco ISR4331/K9 (1RU) processor with 1795999K/6147K bytes of memory.
Processor board ID FLM232010G0
```

Não é necessário

  - Pode não estar instalada a licença.
  - Entre em modo de configuração e faça:

license boot module cXXXX technology-package securityk9

- Grave a configuração.
- Faça ***reload***.
- Faça ***show version*** e já deve ter ativada *Security Technology Package license.*

```
Technology Package License Information for Module:'c2900'

-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      securityk9    Evaluation    securityk9
uc            None          None          None
data          None          None          None
```

Resumo

1. Configuração das politicas ISAKMP (Fase 1 do IKE – dados de gestão)

Comandos	Descrição
`Router# configure terminal`	Entrar no modo de configuração global
`Router(config)# crypto isakmp policy [prioridade]`	Definir a prioridade a atribuir a política. (Quanto menor o valor maior a prioridade)
`Router (config-isakmp)# authentication pre-shared`	Definir que a autenticação vai ser efectuada por uma chave partilhada pelos intervenientes.
`Router (config-isakmp)# encryption [des|3des|aes]`	Definir o algoritmo de encriptação que vai ser utilizado. No caso de escolher aes pode-se ainda definir o numero de bits de encriptação. [128|192|256].
`Router (config-isakmp)# group [1|2|5]`	Definir o grupo utilizado para as chaves Diffie-Hellman. 1 – 768 bit 2 – 1024 bit 5 – 1536 bit
`Router (config-isakmp)# hash [md5|sha]`	Definir o algoritmo de hash que vai ser utilizado.
`Router (config-isakmp)# lifetime [60|86400]`	Definir o tempo que esta política de ser utilizada antes de ser renegociada. O tempo está expresso em segundos.
`Router (config)# crypto isakmp key [0|6] segredo address endereço_publico_remoto no-xauth`	Definir a chave partilhada utilizada na autenticação. O 0 ou 6 define se a palavra deve ou não ser encriptada. O endereço de ser o endereço público do local remoto. Por fim no-xauth previne confusões na autenticação em interface que possuem servidores de acesso remotos, em que os utilizadores têm que efectuar autenticação estendida. (username/password)

Resumo

2. Configuração do IPSec Transform Set (Fase 2 do IKE – dados de transmissão)

Comandos	Descrição
`Router # configure terminal`	Entrar no modo de configuração global
`Router (config)# crypto ipsec transform-set` *`nome_atribuido`* `[opção de encriptação] [opção de hash]`	Definição o nome que se vai atribuir a este transform-set. Opções de encriptação: esp-des esp-3des esp-aes [128|192|256] Opções de hash: esp-md5-hmac esp-sha-hmac

Resumo

3. Configuração do tráfego interessante

Criar uma access-list que defina o tráfico que será considerado interessante para activar a VPN assim como o tráfico que vai ser encriptado e que vai ser enviado pela VPN.

Comandos
Router# configure terminal Router(config)# ip access-list extended *NOME_DA_LISTA* Router(config)# permit ip *ip_origem wild_card_origem ip_destino wild_card_destino*

Resumo

4. Configurar crypto map

Comandos	Descrição
`Router# configure terminal`	Entrar no modo de configuração global
`Router(config)# crypto map` *nome* `[numero de sequencia] ipsec-isakmp`	Definir a o nome que vai ser atribuído ao crypto map. Deve-se ter em conta que cada interface apenas pode ter um crypto map associado, deste forma o crytpo map pode conter configurações de várias conexões VPN. O número de sequência indica qual o ordem em que vai ser colocada a conexão que estamos a criar.
`Router (config-crypto-map)# set peer` *endereço_remote*	Definir o ponto remoto de ligação da VPN.
`Router (config-crypto-map)# match address` *acl-tráfico_interessante*	Definir a access-list que define o tráfego interessante para a ligação VPN.
`Router (config-crypto-map)# set transform-set` *nome_transform_set*	Definir o nome do transform-set que vai ficar agregado a esta ligação VPN no crypto-map

Resumo

5. Atribuir o crypto map com um interface

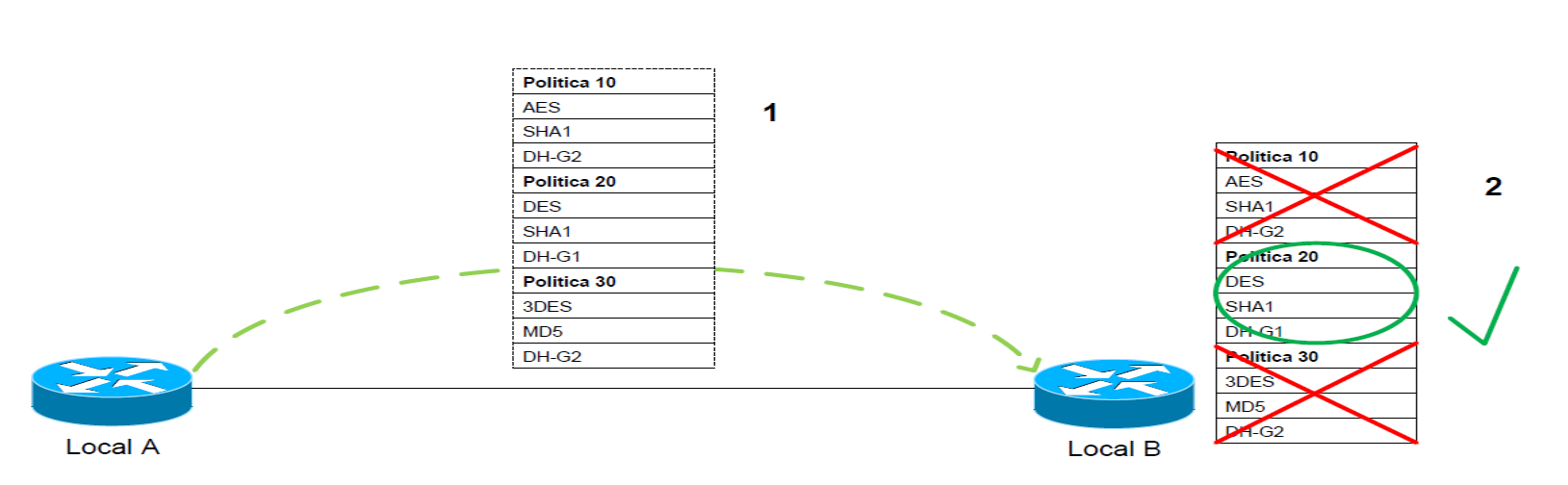
Comandos	Descrição
`Router# configure terminal`	Entrar no modo de configuração global
`Router(config)# interface` *`interface`*	Entrar no modo de configuração do interface de saída.
`Router (config-if)# crypto map` *`nome`*	Relacionar o crypto map definido anteriormente com o interface.

Configuração de túneis IPSec

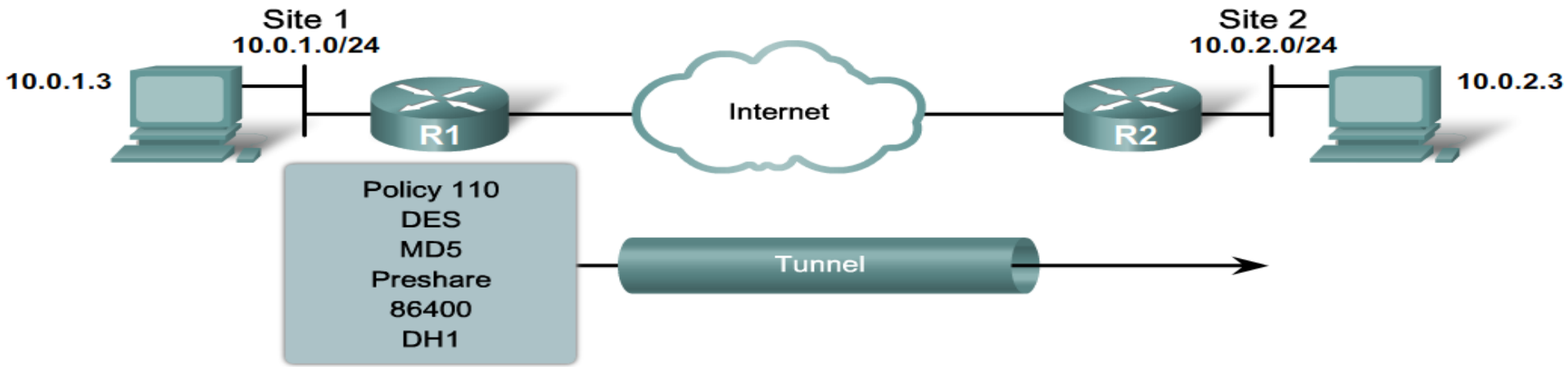
- Configurar as políticas a usar na fase de negociação.
- Isso é feito em duas fases:
  - **IKE fase 1:** Basicamente tem a função de negociar as políticas que serão utilizadas, autenticar os peers e fechar um túnel seguro, por onde serão configurados os demais parâmetros. Pode trabalhar em *Main Mode* ou *Agressive Mode*. Podemos dizer que é um "primeiro túnel", para proteger as mensagens de negociação para o túnel principal.
  - **IKE fase 2:** É a negociação do "segundo túnel". São definidos os parâmetros do IPSec e *transform sets*.

Configuração de túneis IPSec

- **Mensagem 1 (IKE 1- mainmode):** Troca e negociação de políticas de segurança O router que inicia a ligação VPN envia uma lista de políticas contendo vários grupos de possíveis alternativas. Dentro desta lista o recetor deve concordar com um conjunto para que seja possível criar a ligação.



Configuração de túneis IPSec




```
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
```

Configuração de túneis IPSec

- As diferentes opções que pode considerar para o definição dos parâmetros da ligação são:

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

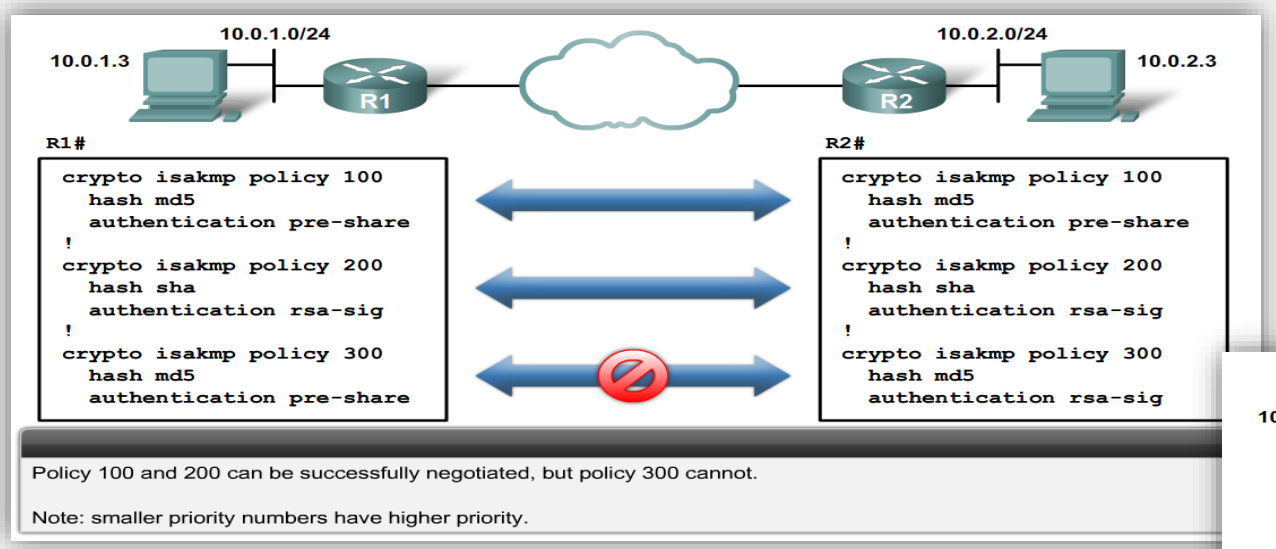
Note: Actual parameters vary based on IOS image.

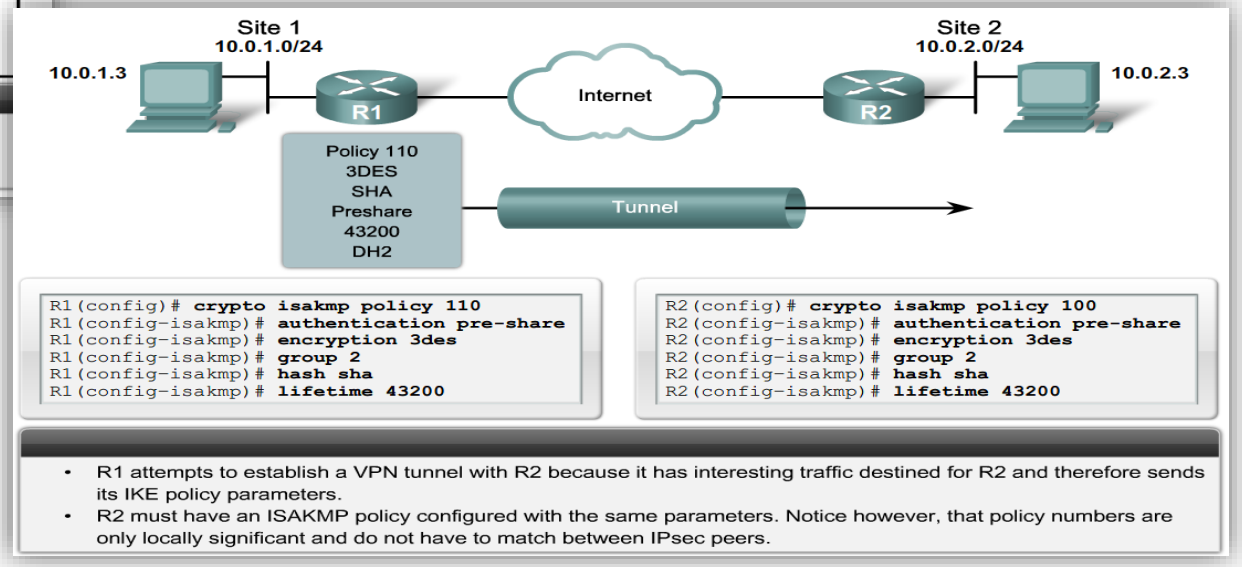
Configuração de túneis IPSec

- **Mensagem 2 (IKE 1):** Troca de chaves públicas possibilitando uma ligação segura entre os pontos
- **Mensagem 2 (IKE 2):** Verificação de identidade. Uma vez garantida a segurança pode ser trocada a identificação dos intervenientes sem o risco de esta ser capturada por terceiros.

Configuração de túneis IPSec

- Temos de garantir que em ambos os extremos os parâmetros IKE são iguais.





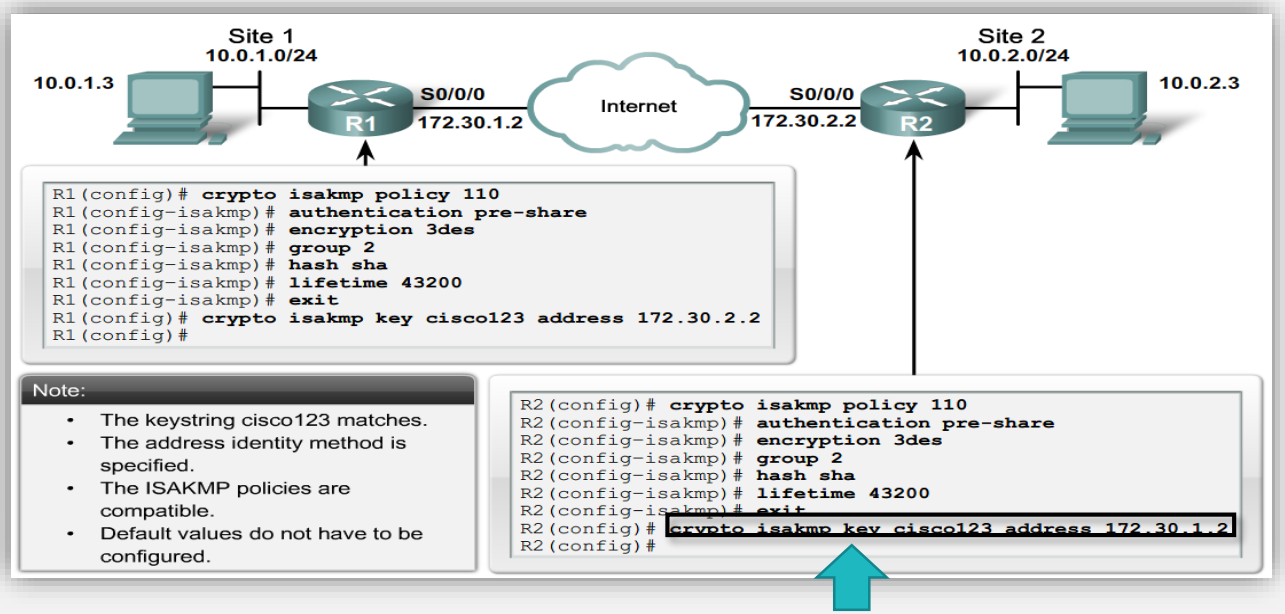
Configuração de túneis IPSec

- A configuração da *Pre-SharedKey* (PSK) necessita ainda da definição em ambos os routers da palavra chave comum a utilizar na autenticação.

```
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.



Configuração de túneis IPSec

- Temos depois de definir os parâmetros da segunda fase de negociação:
  - Configurar os "*Transform Sets*" - Combinação de protocolos e modos de funcionamento do IPSec.

Configuração de túneis IPSec

```
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.

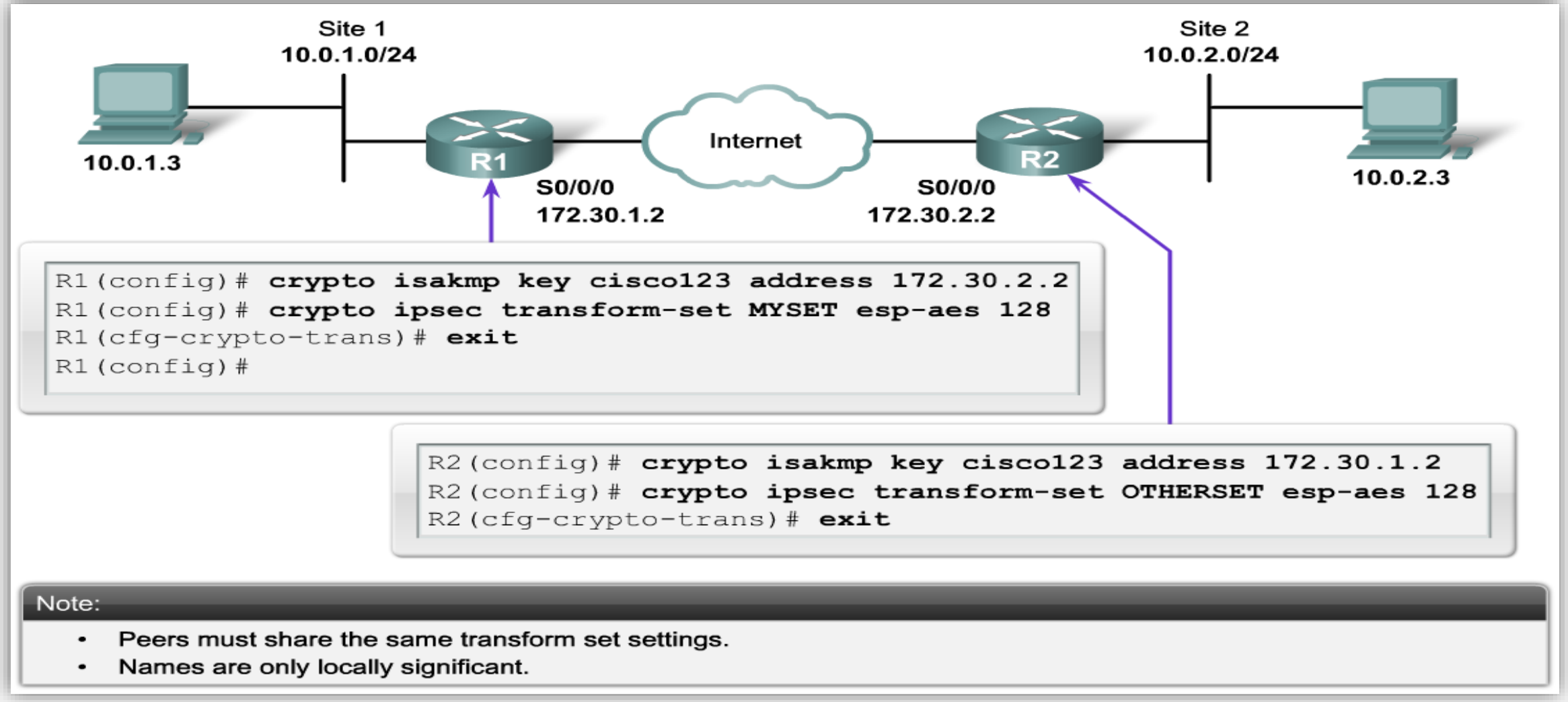
Configuração de túneis IPSec

- As combinações possíveis são as seguintes:

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

Configuração de túneis IPSec

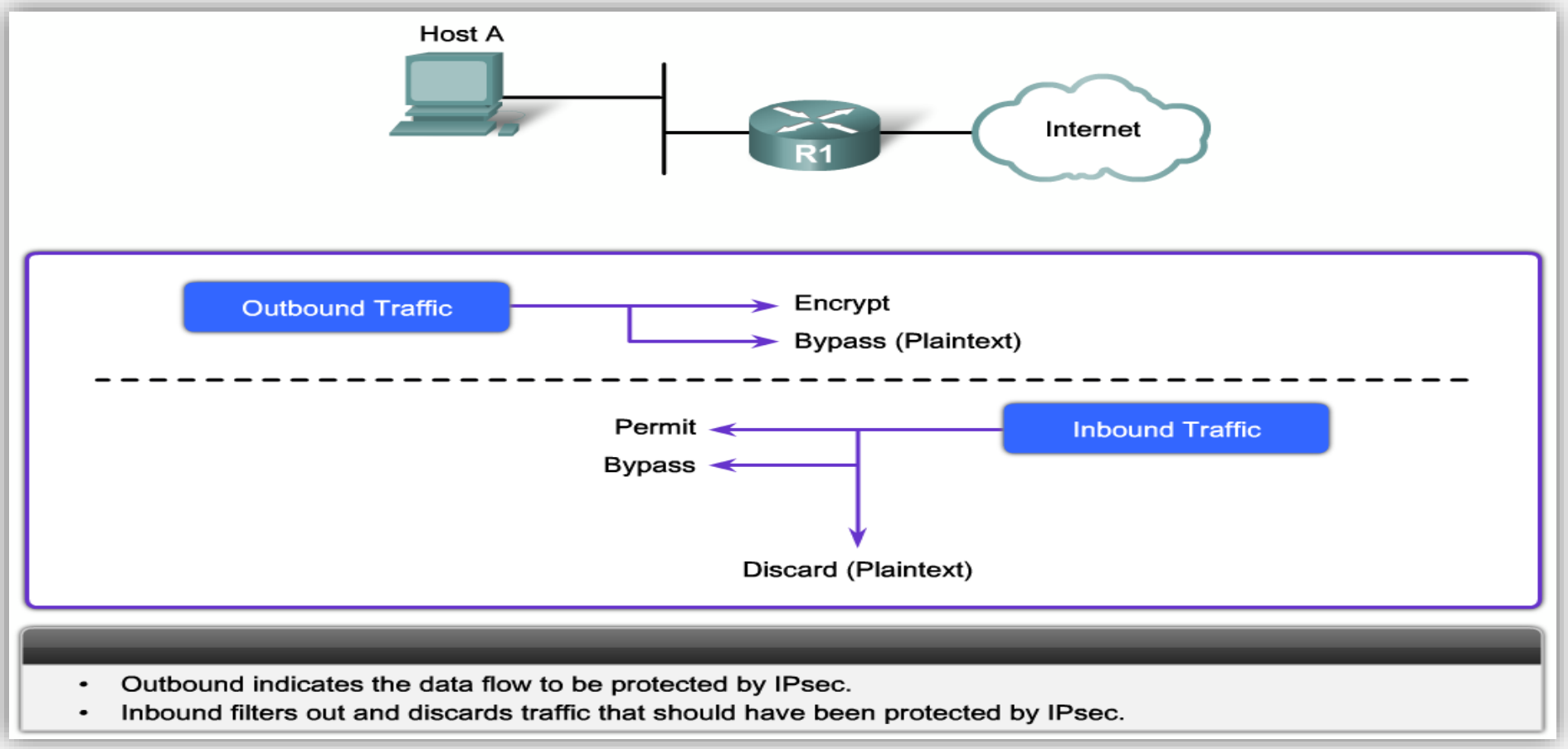


Note:

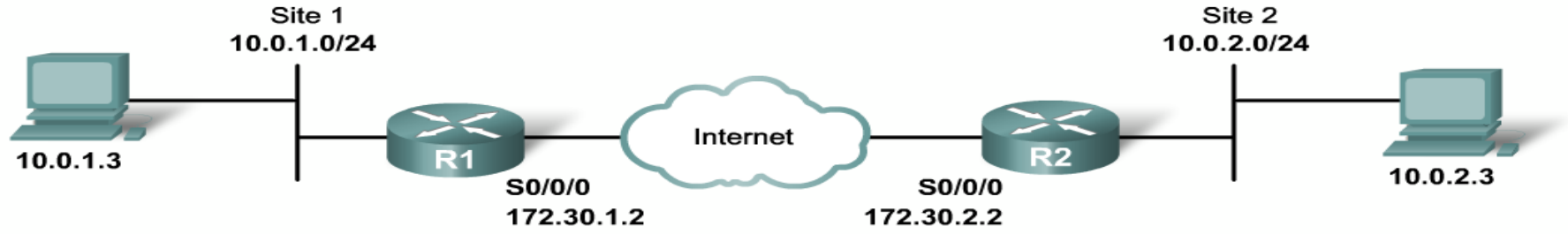
- Peers must share the same transform set settings.
- Names are only locally significant.

Configuração de túneis IPSec

- Por fim, temos de proceder à configuração do "*Crypto ACLs*" que permita proteger o tráfego



Configuração de túneis IPSec

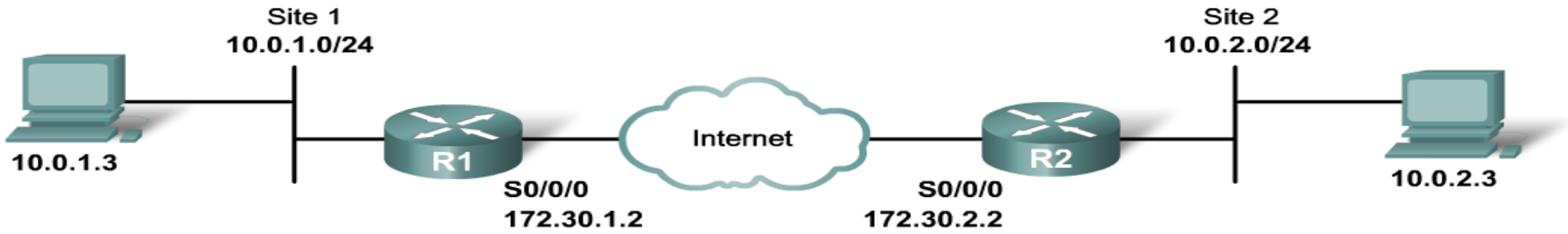



```
router(config)#
```

```
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.

Configuração de túneis IPSec



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
```

Configuração de túneis IPSec

- Aplicação do "*Crypto Map*"
  - ACL a usar
  - Equipamentos remotos com os quais se vai estabelecer a VPN
  - *Transform Set* a ser usada
  - Método de gestão de chaves
  - Tempo de vida das *Security Associations*
- Podem ser criados vários *Crypto Maps*

```
router(config)#
crypto map map-name seq-num ipsec-manual
crypto map map-name seq-num ipsec-isakmp [dynamic dynamic-map-name]
```

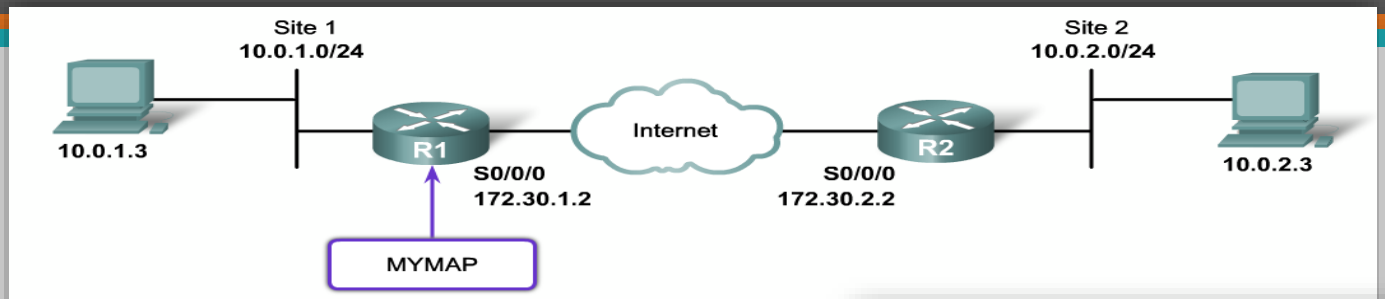
`crypto map` Parameters

Command Parameters	Description
map-name	Defines the name assigned to the crypto map set or indicates the name of the crypto map to edit.
seq-num	The number assigned to the crypto map entry.
ipsec-manual	Indicates that ISAKMP will not be used to establish the IPsec SAs.
ipsec-isakmp	Indicates that ISAKMP will be used to establish the IPsec SAs.
cisco	(Default value) Indicates that CET will be used instead of IPsec for protecting the traffic.
dynamic	(Optional) Specifies that this crypto map entry references a preexisting static crypto map. If this keyword is used, none of the crypto map configuration commands are available.
dynamic-map-name	(Optional) Specifies the name of the dynamic crypto map set that should be used as the policy template.

`crypto map` Configuration Mode Commands

Command	Description
set	Used with the **peer**, **pfs**, **transform-set**, and **security-association** commands.
peer [*hostname* | *ip-address*]	Specifies the allowed IPsec peer by IP address or hostname.
pfs [**group1** | **group2**]	Specifies DH Group 1 or Group 2.
transform-set [*set_name(s)*]	Specify list of transform sets in priority order. When the **ipsec-manual** parameter is used with the **crypto map** command, then only one transform set can be defined. When the **ipsec-isakmp** parameter or the **dynamic** parameter is used with the **crypto map** command, up to six transform sets can be specified.
security-association lifetime	Sets SA lifetime parameters in seconds or kilobytes.
match address [*access-list-id* | *name*]	Identifies the extended ACL by its name or number. The value should match the access-list-number or name argument of a previously defined IP-extended ACL being matched.
no	Used to delete commands entered with the **set** command.
exit	Exits crypto map configuration mode.

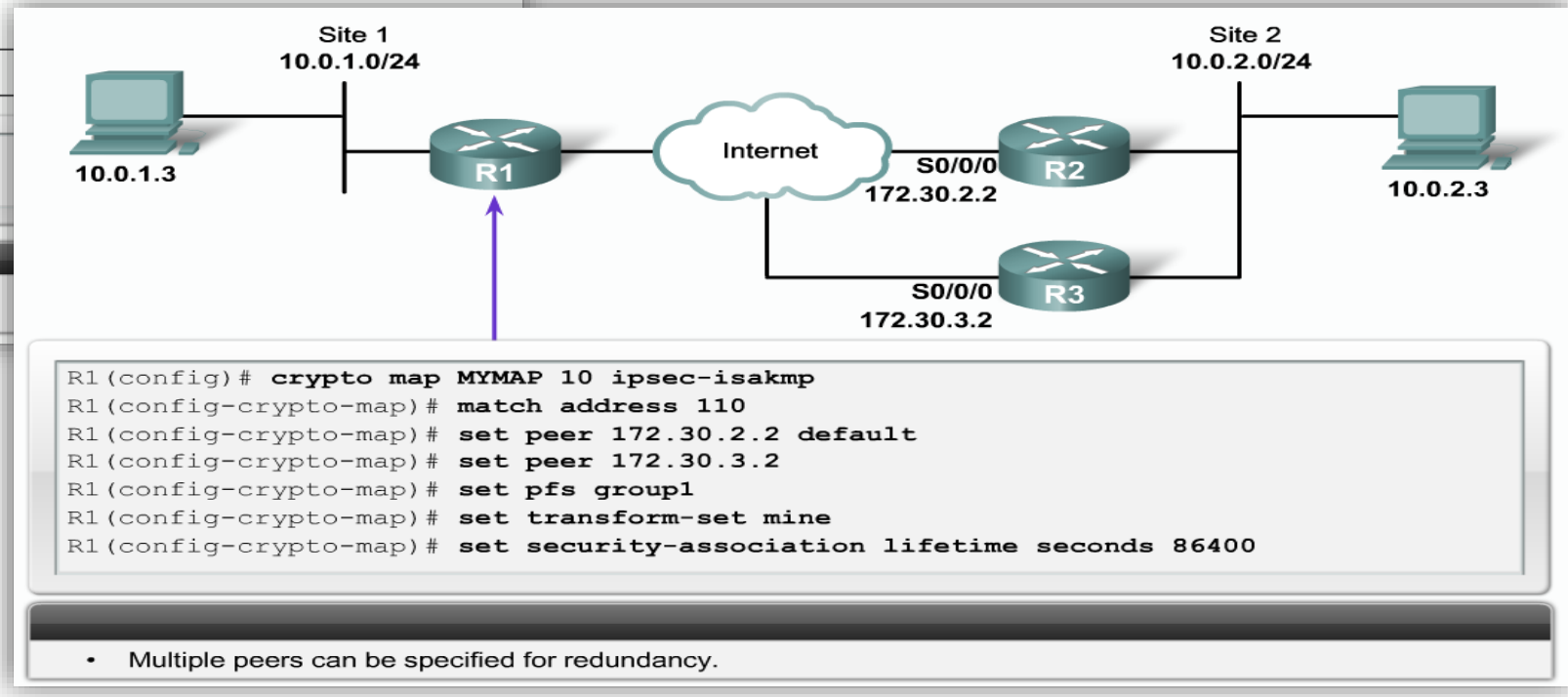
Configuração de túneis IPSec




```
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

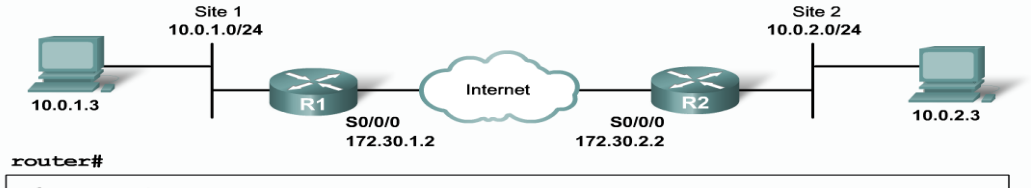



```
R1(config)# crypto map MYMAP 10 ipsec-isakmp
R1(config-crypto-map)# match address 110
R1(config-crypto-map)# set peer 172.30.2.2 default
R1(config-crypto-map)# set peer 172.30.3.2
R1(config-crypto-map)# set pfs group1
R1(config-crypto-map)# set transform-set mine
R1(config-crypto-map)# set security-association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

- Multiple peers can be specified for redundancy.

Verificação da configuração

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
```

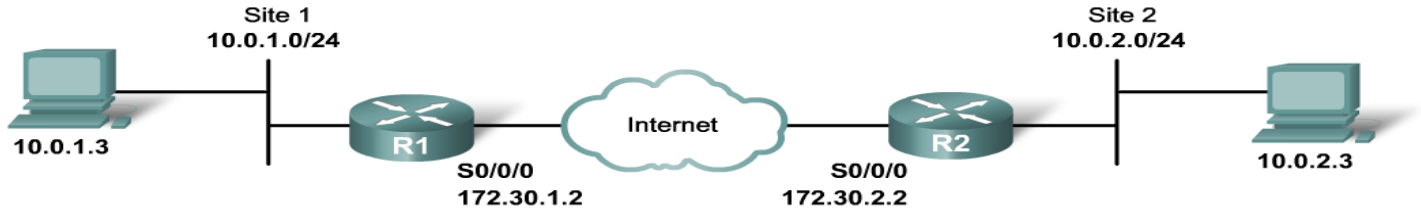
- Displays the currently configured crypto maps.

```
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,  },
```

Verificação da configuração




```
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 – Requisitos -Exercício 2

- Utilize o servidor e o cliente do segundo teste ou da aula prática nº. 10.
- No servidor Windows server 2012 desabilite o NAT.

Exercício 2 – VPN em ambiente *windows*

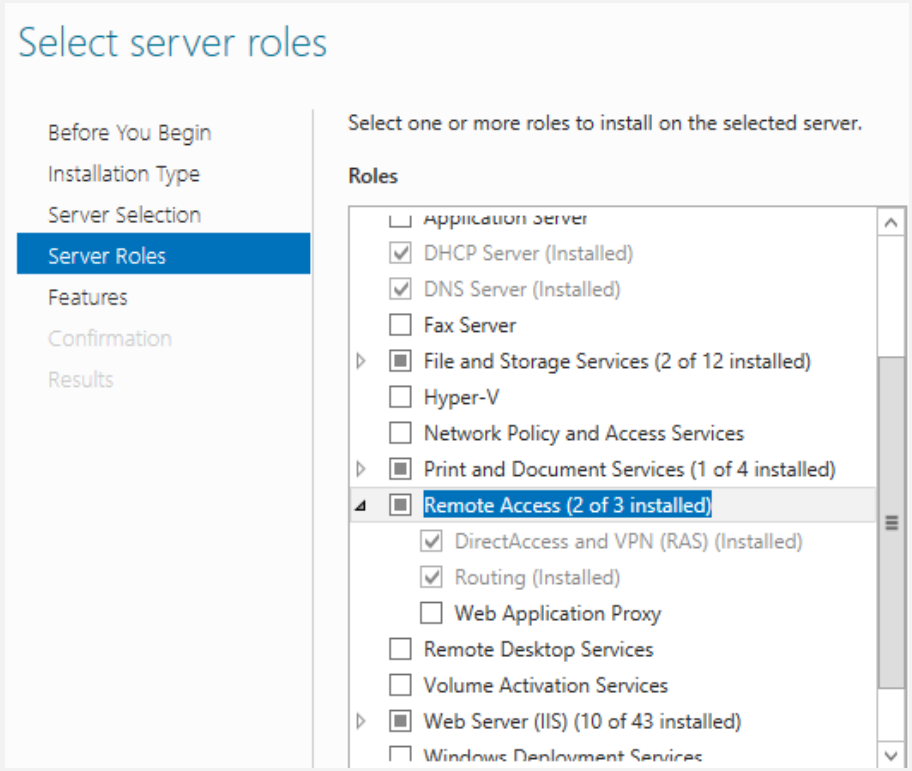
Exercício

- A empresa SR1.SA deseja implementar uma solução de acesso remoto por VPN para os seus vendedores.
- Como não tem um grande orçamento e deseja testar como funciona esta solução, foi decidido fazer esta VPN sobre Windows 2012 R2 utilizando o seu servidor de DNS.
- Instale o serviço
- Configure o serviço remoto no servidor:
  - Coloque 3 endereços da sua rede para serem disponibilizados para as ligações remotas.
  - Escolha o L2TP como protocolo VPN
- Configure a ligação no cliente.
- Tente aceder no cliente à VPN criada.

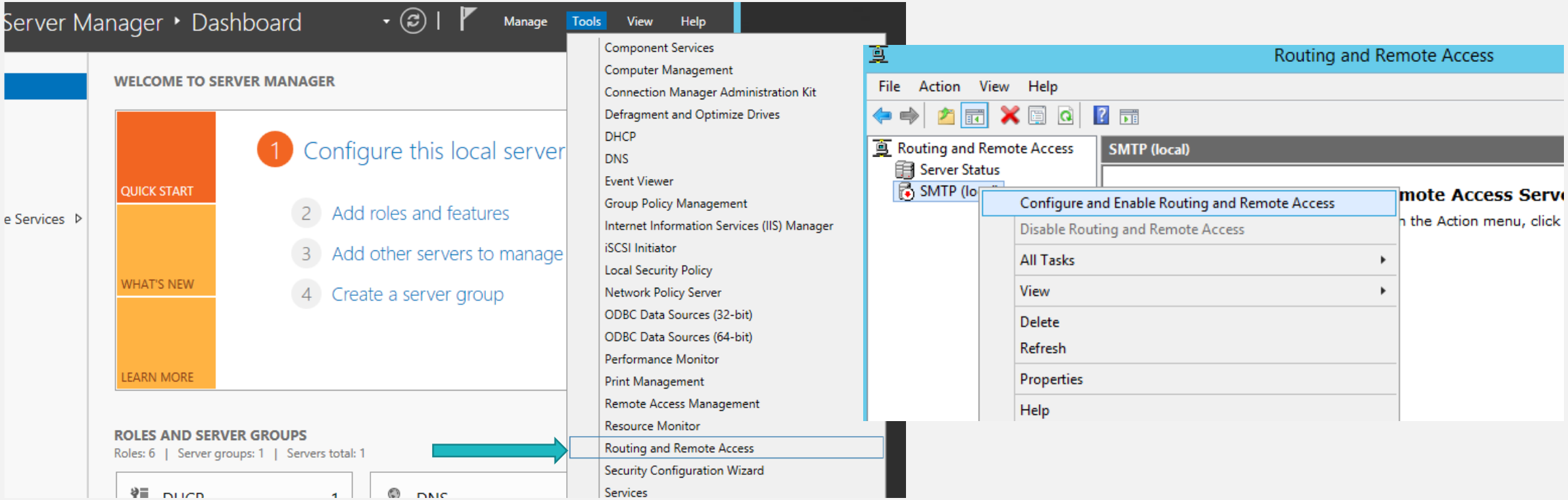
How To

Instalação do serviço

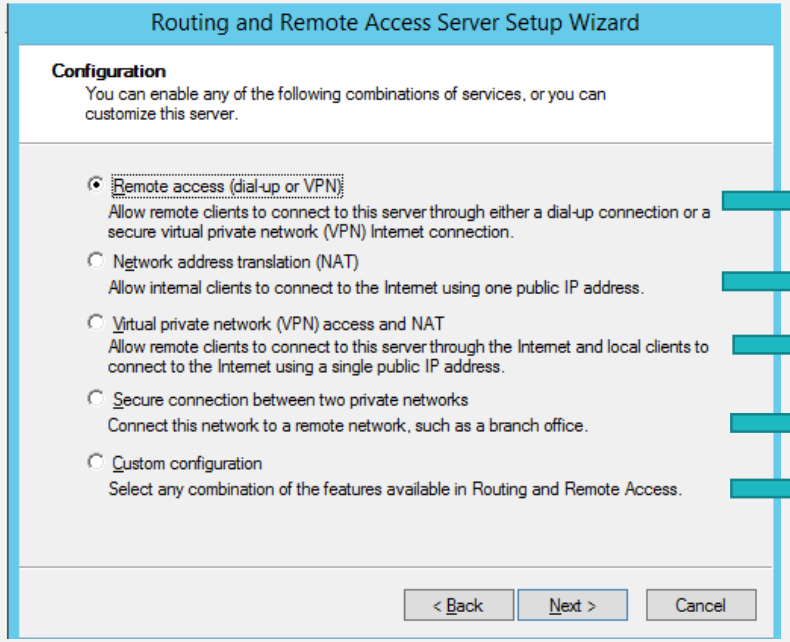
- O acesso remoto de computadores a um servidor Windows é feito através do serviço de acesso remoto (*Remote Access*)- **Veja a aula prática nº 7.**



Configuração do serviço



Configuração do serviço



Acesso remoto ao servidor utilizando a linha telefónica ou a ligação à Internet

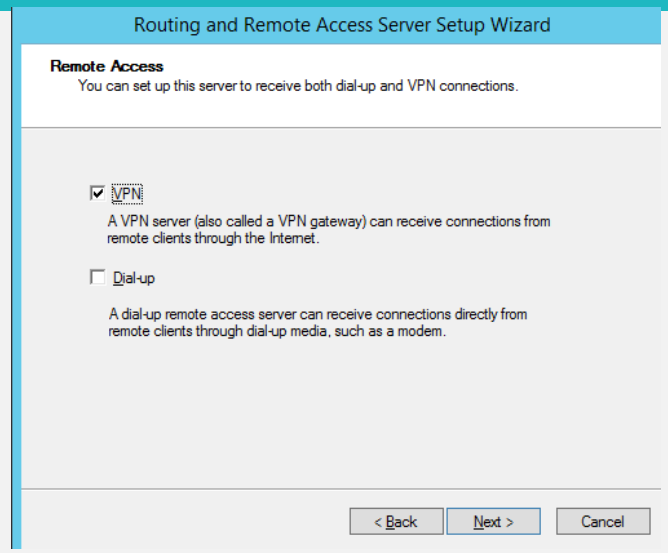
Acesso a clientes internos ao acesso à Internet com IP publico – já vimos em aulas anteriores

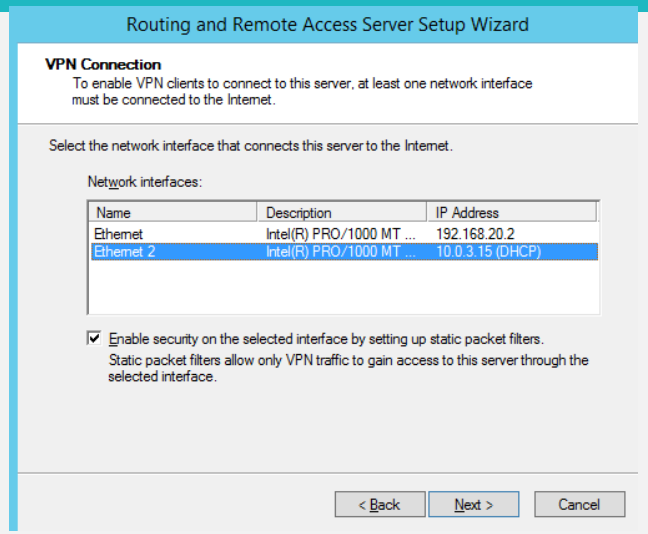
Um misto das situações anteriores

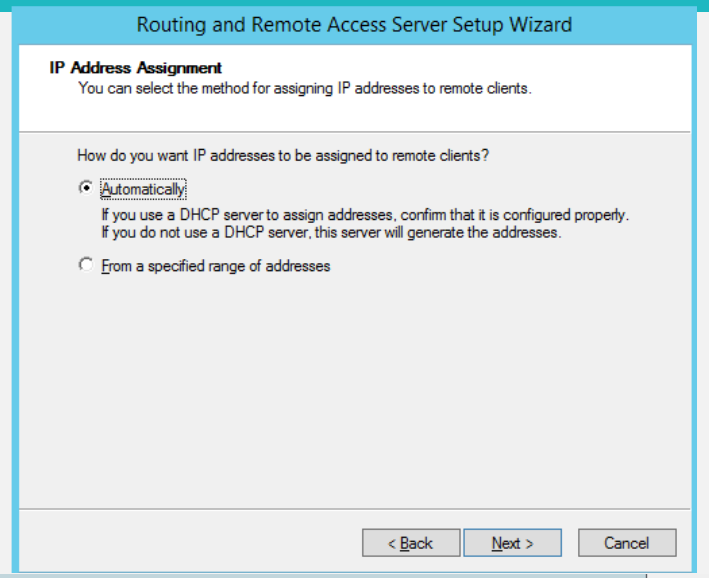
Acesso remoto entre dois servidores

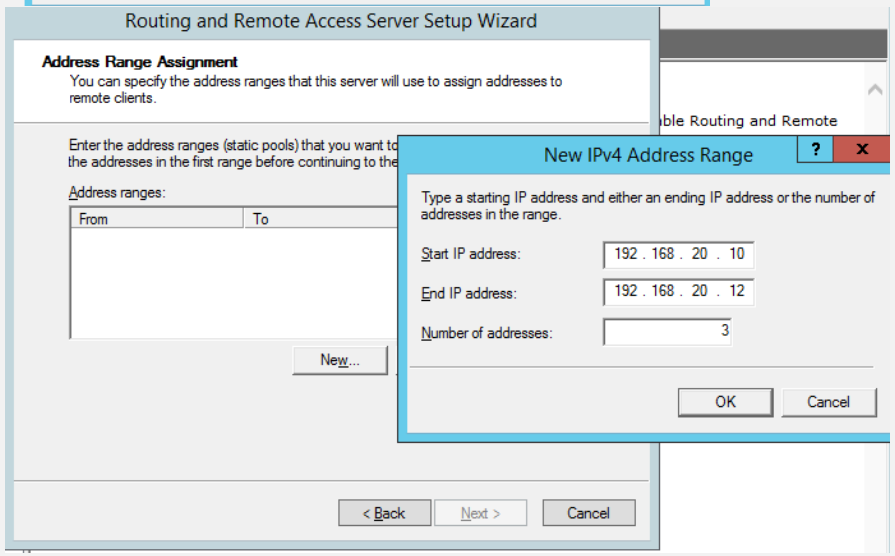
Pode criar um serviço à sua escolha

Configuração do serviço

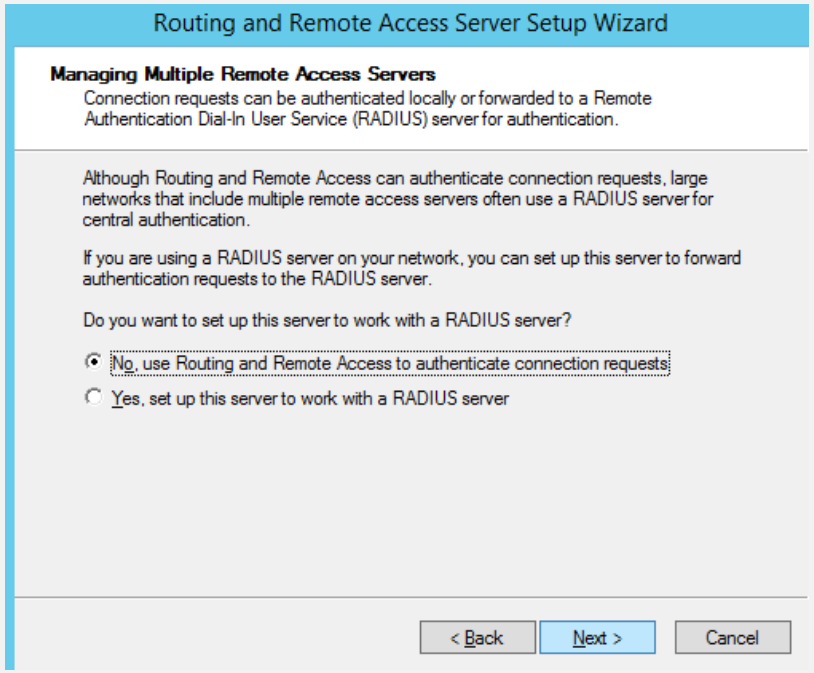


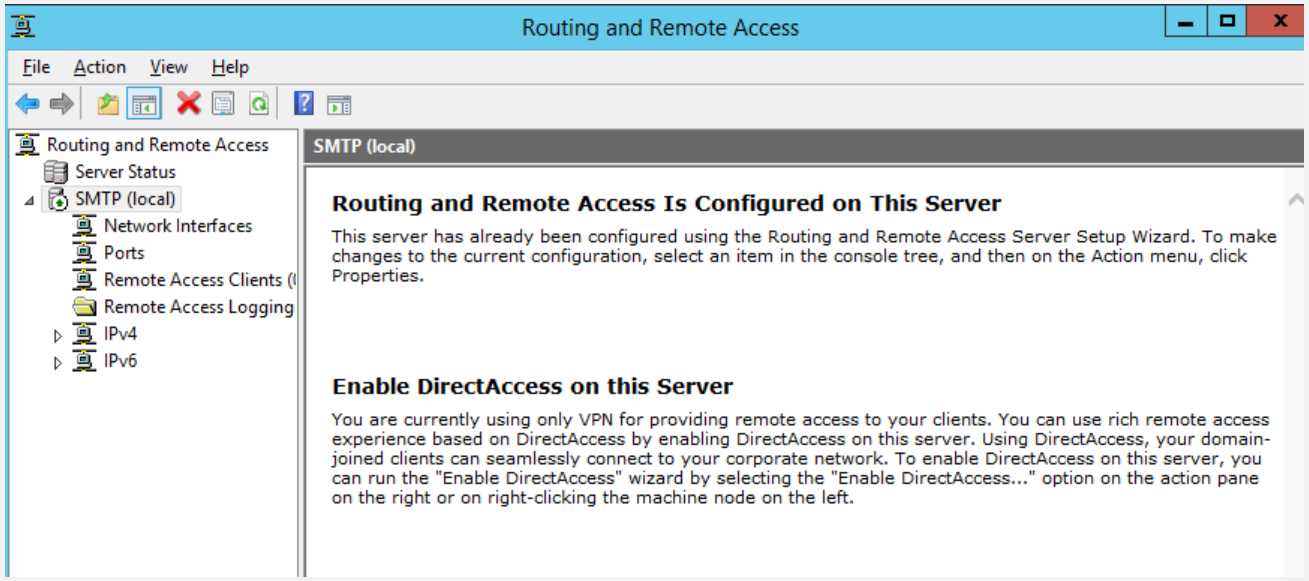


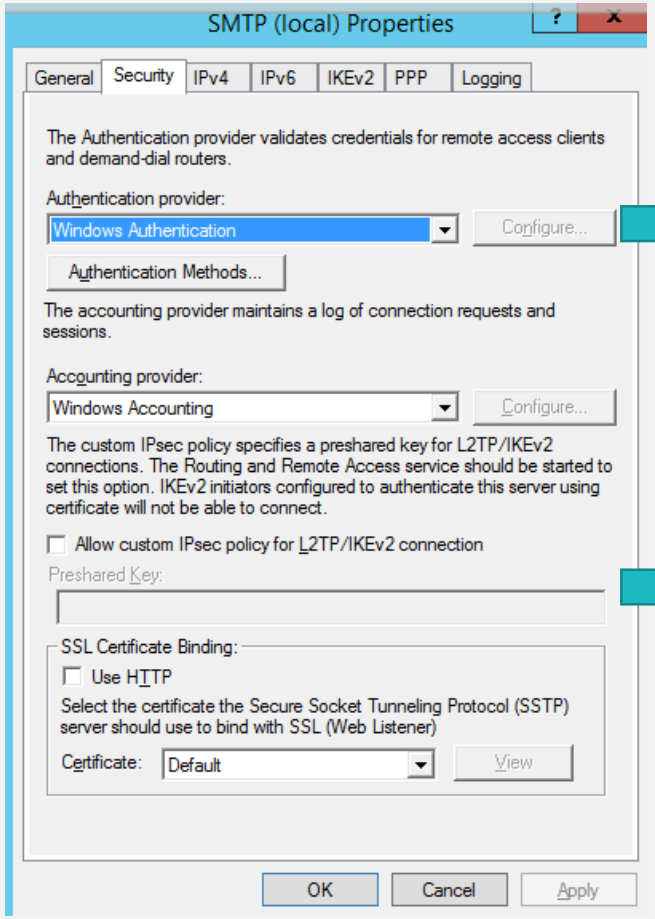




Configuração do serviço



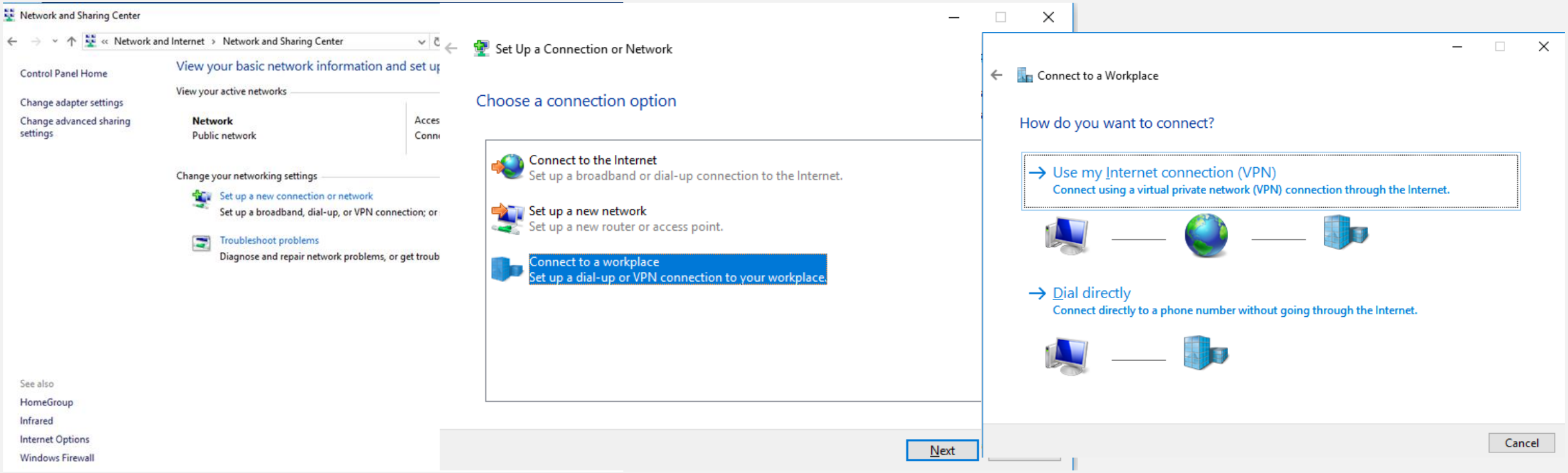




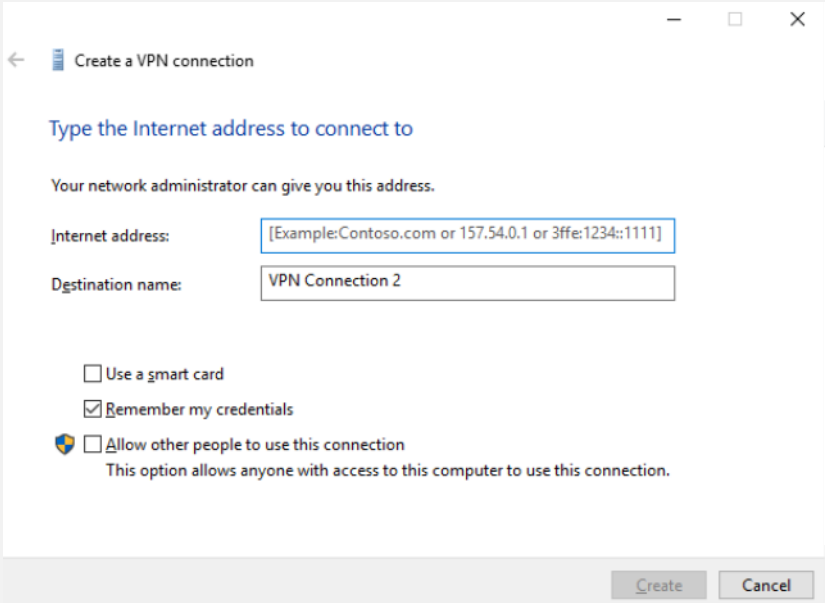
Tipo de autenticação do cliente

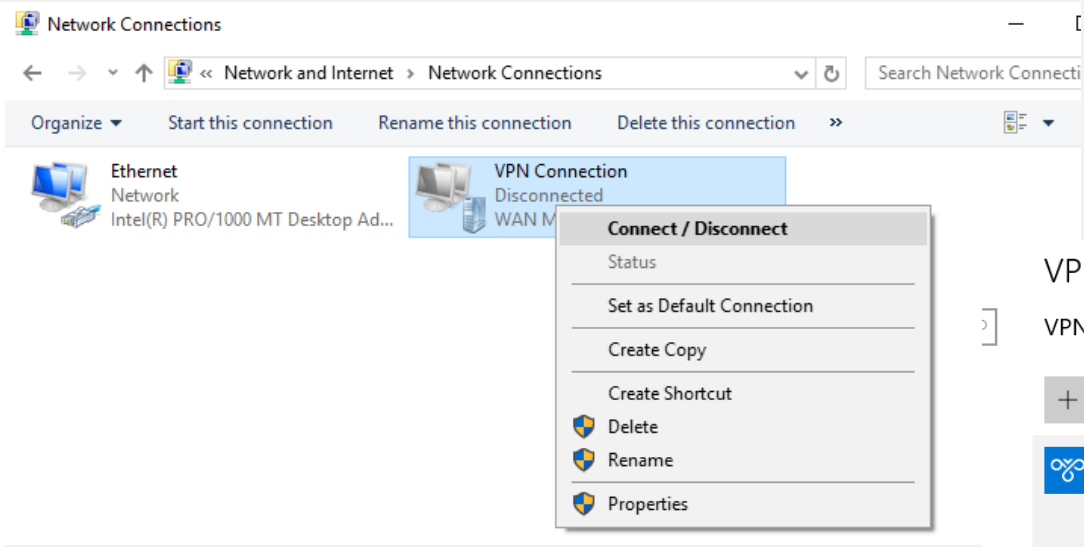
Tipo de gestão do túnel e encapsulamento dos dados

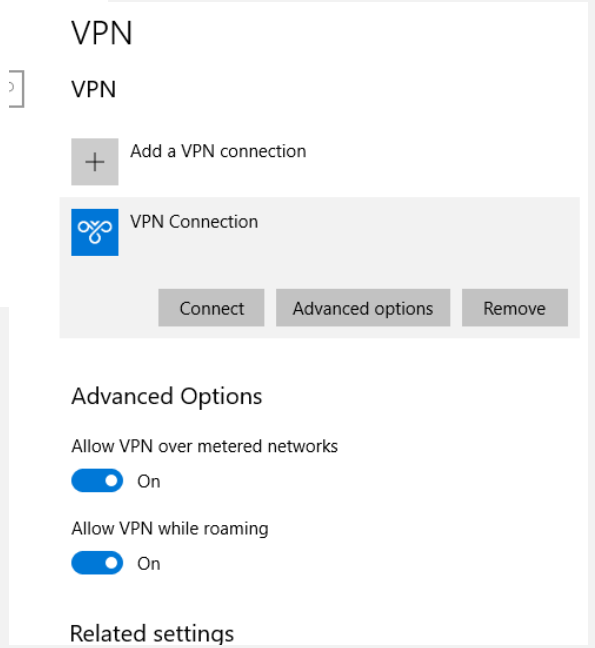
Configuração do Cliente



Configuração do Cliente







Dúvidas

Referências

- Cisco Networking Academy – Packet Tracer – Configuring VPNs