**1.** Enable ISAKMP.

**2.** Create ISAKMP policy.

**3.** Set the tunnel type.

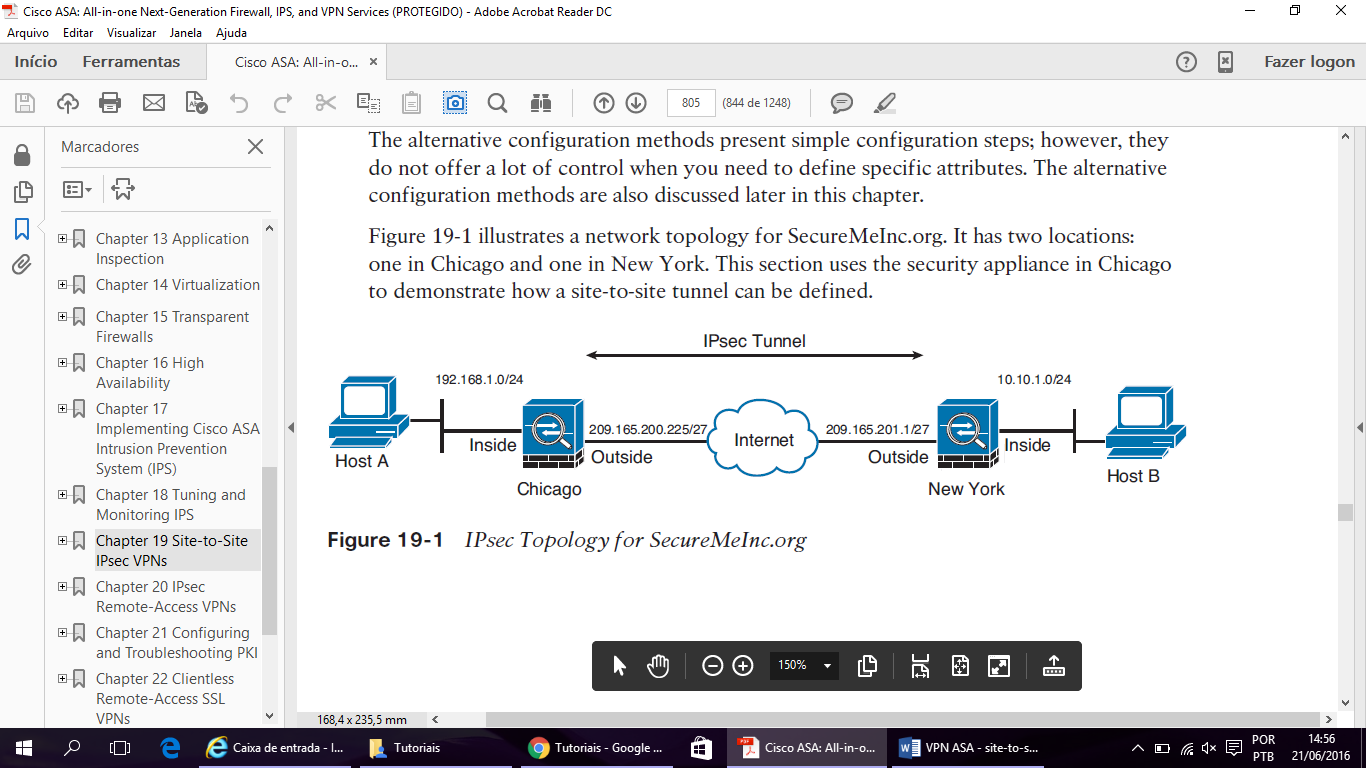
**4.** Define the IPsec policy.

**5.** Configure the crypto map.

**6.** Configure traffic filtering (optional).

**7.** Bypass NAT (optional).

**8.** Enable Perfect Forward Secrecy (optional).



**Step 1: Enable ISAKMP**

Chicago(config)# **crypto ikev2 enable outside**

Chicago(config)#

**Step 2: Create the ISAKMP Policy**

Chicago(config)# **crypto ikev2 policy 1**

Chicago(config-isakmp-policy)# **encryption aes-256**

Chicago(config-isakmp-policy)# **integrity sha**

Chicago(config-isakmp-policy)# **group 5**

Chicago(config-isakmp-policy)# **prf sha**

Chicago(config-isakmp-policy)# **lifetime seconds 86400**

**Step 3: Set Up the Tunnel Groups**

Chicago(config)# **tunnel-group 209.165.201.1 type ipsec-l2l**

Chicago(config)# **tunnel-group 209.165.201.1 ipsec-attributes**

Chicago(config-tunnel-ipsec)# **ikev2 remote-authentication pre-shared-key C!$c0K3y**

Chicago(config-tunnel-ipsec)# **ikev2 local-authentication pre-shared-key C!$c0K3y**

**Step 4: Define the IPsec Policy**

Chicago(config)# **crypto ipsec ikev2 ipsec-proposal NY-AES256SHA512**

Chicago(config-ipsec-proposal)# **protocol esp encryption aes-256**

Chicago(config-ipsec-proposal)# **protocol esp integrity sha-512**

**Step 5: Create a Crypto Map**

Chicago# **configure terminal**

Chicago(config)# **access-list outside\_cryptomap line 1 remark ACL to encrypt traffic**

**from Chicago to NY**

Chicago(config)# **access-list outside\_cryptomap line 2 extended permit ip 192.168.10.0**

**255.255.255.0 10.10.10.0 255.255.255.0**

Chicago(config)# **crypto map outside\_map 1 match address outside\_cryptomap**

Chicago(config)# **crypto map outside\_map 1 set peer 209.165.201.1**

Chicago(config)# **crypto map outside\_map 1 set ikev2 ipsec-proposal NY-AES256SHA512**

Chicago(config)# **crypto map outside\_map interface outside**

**Step 6: Configure Traffic Filtering (Optional)**

Chicago(config)# **access-list outside\_acl extended permit tcp host 10.10.10.10 host**

**192.168.10.10 eq 23**

Chicago(config)# **access-group outside\_acl in interface outside**

Chicago(config)# **no sysopt connection permit-vpn**

**Step 7: Bypass NAT (Optional)**

Chicago(config)# **object network 192.168-Net**

Chicago(config-network-object)# **subnet 192.168.10.0 255.255.255.0**

Chicago(config-network-object)# **object network 10.10-Net**

Chicago(config-network-object)# **subnet 10.10.10.0 255.255.255.0**

Chicago(config-network-object)# **exit**

Chicago(config)# **nat (inside,outside) source static 192.168-Net**

**10.10-Net destination static 192.168-Net 10.10-Net**

**Step 8: Enable Perfect Forward Secrecy (Optional)**

Chicago(config)# **crypto map outside\_map 10 set pfs group5**

**Optional Attributes and Features**

**OSPF Updates over IPsec**

Chicago(config)# **interface GigabitEthernet0/0**

Chicago(config-if)# **nameif outside**

Chicago(config-if)# **security-level 0**

Chicago(config-if)# **ip address 209.165.200.225 255.255.255.224**

Chicago(config-if)# **ospf network point-to-point non-broadcast**

Chicago(config)# **router ospf 10**

Chicago(config-router)# **network 209.165.200.225 255.255.255.255 area 0**

Chicago(config-router)# **neighbor 209.165.201.1 interface outside**

**Reverse Route Injection**

Chicago(config)# **crypto map outside\_cryptomap\_10 10 set reverse-route**

Chicago# **show route**

S 0.0.0.0 0.0.0.0 [1/0] via 209.165.200.226, outside

C 192.168.10.0 255.255.255.0 is directly connected, inside

C 209.165.200.224.0 255.255.255.224 is directly connected, outside

S 10.10.10.0 255.255.255.0 [1/0] via 209.165.200.226, outside

Chicago(config)# **router ospf 10**

Chicago(config-router)# **redistribute static subnets**

Router1# **show ip route**

C 192.168.10.0/24 is directly connected, GigabitEthernet0

C 192.168.20.0/24 is directly connected, FastEthernet0

O E2 10.10.10.0/24 [110/20] via 192.168.10.1, 00:00:03, GigabitEthernet0

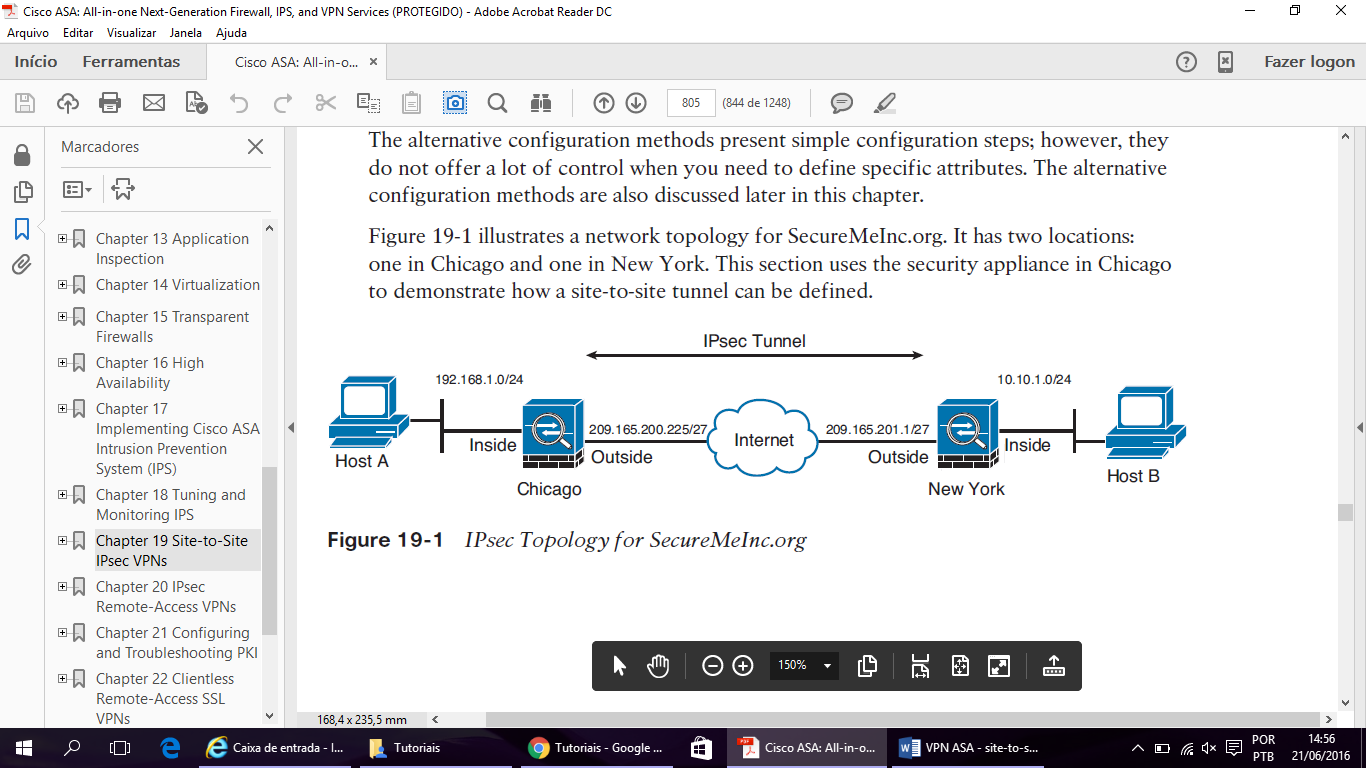
**Tunnel Default Gateway**

Chicago(config)# **route inside 0.0.0.0 0.0.0.0 192.168.10.2 tunneled**

**Management Access**

Chicago(config)# **management-access inside**

**RESUMO**



ASA 1 (Chicago)

inter gig 0

ip add 200.0.0.1 255.255.255.0

security-level 0

nameif outside

no shut

inter gig 1

ip add 192.168.1.1 255.255.255.0

security-level 100

nameif inside

no shut

exit

dhcpd address 192.168.1.10-192.168.1.20 inside

dhcpd enable inside

crypto ikev2 enable outside

crypto ikev2 policy 1

encryption aes-256

integrity sha

group 5

prf sha

lifetime seconds 86400

exit

tunnel-group 200.0.0.2 type ipsec-l2l

tunnel-group 200.0.0.2 ipsec-attributes

ikev2 remote-authentication pre-shared-key cisco

ikev2 local-authentication pre-shared-key cisco

exit

crypto ipsec ikev2 ipsec-proposal NY-AES256SHA512

protocol esp encryption aes-256

protocol esp integrity sha-1

exit

access-list outside\_cryptomap line 1 remark ACL to encrypt traffic from Chicago to NY

access-list outside\_cryptomap line 2 extended permit ip 192.168.1.0 255.255.255.0 10.10.1.0 255.255.255.0

crypto map outside\_map 1 match address outside\_cryptomap

crypto map outside\_map 1 set peer 200.0.0.2

crypto map outside\_map 1 set ikev2 ipsec-proposal NY-AES256SHA512

crypto map outside\_map interface outside

route outside 10.10.1.0 255.255.255.0 200.0.0.2

**access-list outside\_acl extended permit icmp any any**

**access-group outside\_acl in interface outside**

**no sysopt connection permit-vpn**

ASA 2 (New York)

inter gig 0

ip add 200.0.0.2 255.255.255.0

security-level 0

nameif outside

no shut

inter gig 1

ip add 10.10.1.1 255.255.255.0

security-level 100

nameif inside

no shut

exit

dhcpd address 10.10.1.10-10.10.1.20 inside

dhcpd enable inside

crypto ikev2 enable outside

crypto ikev2 policy 1

encryption aes-256

integrity sha

group 5

prf sha

lifetime seconds 86400

exit

tunnel-group 200.0.0.1 type ipsec-l2l

tunnel-group 200.0.0.1 ipsec-attributes

ikev2 remote-authentication pre-shared-key cisco

ikev2 local-authentication pre-shared-key cisco

exit

crypto ipsec ikev2 ipsec-proposal NY-AES256SHA512

protocol esp encryption aes-256

protocol esp integrity sha-1

exit

access-list outside\_cryptomap line 1 remark ACL to encrypt traffic from Chicago to NY

access-list outside\_cryptomap line 2 extended permit ip 10.10.1.0 255.255.255.0 192.168.1.0 255.255.255.0

crypto map outside\_map 1 match address outside\_cryptomap

crypto map outside\_map 1 set peer 200.0.0.1

crypto map outside\_map 1 set ikev2 ipsec-proposal NY-AES256SHA512

crypto map outside\_map interface outside

route outside 192.168.1.0 255.255.255.0 200.0.0.1

Testar o Tunnel

**show isakmp sa**

**CONFIGURAÇÃO ROTEADOR(New York)**

inter fas 0/0

ip add 200.0.0.2 255.255.255.0

no shut

inter fas 1/0

ip add 10.10.1.1 255.255.255.0

no shut

exit

ip dhcp pool REDE10

network 10.10.1.0 255.255.255.0

default-router 10.10.1.1

ip dhcp excluded 10.10.1.1 10.10.1.9

crypto ikev2 enable outside

crypto ikev2 policy 1

encryption aes-256

integrity sha

group 5

prf sha

lifetime seconds 86400

exit

tunnel-group 200.0.0.1 type ipsec-l2l

tunnel-group 200.0.0.1 ipsec-attributes

ikev2 remote-authentication pre-shared-key cisco

ikev2 local-authentication pre-shared-key cisco

exit

crypto ipsec ikev2 ipsec-proposal NY-AES256SHA512

protocol esp encryption aes-256

protocol esp integrity sha-1

exit

access-list outside\_cryptomap line 1 remark ACL to encrypt traffic from Chicago to NY

access-list outside\_cryptomap line 2 extended permit ip 10.10.1.0 255.255.255.0 192.168.1.0 255.255.255.0

crypto map outside\_map 1 match address outside\_cryptomap

crypto map outside\_map 1 set peer 200.0.0.1

crypto map outside\_map 1 set ikev2 ipsec-proposal NY-AES256SHA512

crypto map outside\_map interface outside

ip route 192.168.1.0 255.255.255.0 200.0.0.1