DMVPN

A biztonságos kapcsolat kialakítás érdekében VPN-t használunk a telephelyek közötti kapcsolathoz. A Cisco saját protokollját a DMVPN-t használjuk a könnyű kapcsolatkialakítás érdekében. Phase 3-as kapcsolatot építettünk ki, ami azt jelenti, hogy magát a full mesh topológiát kiépítik az eszközök egymás közt, így csak egy központi konfigurációt kell alkalmazni, és nem kell minden egyes eszközt (esetleges későbbi telephelyek kialakítása esetén sem), mindent egyes régi és új routeren felvenni a kapcsolatot az új eszközökkel. A VPN kapcsolatot IKEv2-s előre megosztott kulcsos megoldással van védve. Sha512-vel és aes256-tal van biztosítva az integritás és a titkosítás. A site-ok közötti, tehát a VPN alagúton belüli IP forgalomirányítást EIGRP-vel végezzük, amin keresztül átadjuk a site-ok /16-os tartományait.

A megoldás során a következő beállításokat használtuk:

BELERAKOM IDE A KONFIGOKAT, HA MÁSHOVA AKARJUK BELERAKNI AKKOR MAJD SZEDD KI

IR:

crypto ikev2 proposal IKE-PROP encryption aes-cbc-256 integrity sha256

group 16

crypto ikev2 policy IKE-POL

proposal IKE-PROP

crypto ikev2 keyring KKK-KEY

peer VPN

!

address 2.2.2.1

pre-shared-key KKKdmvpn

peer VPN2

!

address 3.3.3.1

pre-shared-key KKKdmvpn

crypto ikev2 profile IKE-PROF

match address local 1.1.1.1

match identity remote address 2.2.2.1 255.255.255.255

match identity remote address 3.3.3.1 255.255.255.255

authentication remote pre-share

authentication local pre-share

keyring local KKK-KEY

crypto ipsec transform-set VPN-TRANS esp-aes 256 esp-sha512-hmac

mode tunnel

crypto ipsec profile DMVPN

set transform-set VPN-TRANS

set ikev2-profile IKE-PROF

interface Tunnel1

ip address 10.255.255.1 255.255.255.0 no ip redirects

ip mtu 1400

no ip split-horizon eigrp 1

ip nhrp authentication KKKdmvpn

ip nhrp network-id 100000

delay 1000

tunnel source GigabitEthernet0/0

tunnel mode gre multipoint

tunnel key 100000

tunnel protection ipsec profile DMVPN

SZE/DEB:

crypto ikev2 proposal IKE-PROP

encryption aes-cbc-256

integrity sha256

group 16

crypto ikev2 policy IKE-POL

proposal IKE-PROP

crypto ikev2 keyring KKK-KEY

peer VPN

address 1.1.1.1

pre-shared-key KKKdmvpn

crypto ikev2 profile IKE-PROF

match address local 3.3.3.1

match address local 2.2.2.1

match identity remote fqdn IR.kkk.com

match identity remote address 1.1.1.1 255.255.255.255

authentication remote pre-share

authentication local pre-share

keyring local KKK-KEY

crypto ipsec transform-set KKK-TRANS esp-aes 256 esp-sha512-hmac

mode tunnel

crypto ipsec profile DMVPN

set transform-set KKK-TRANS

set ikev2-profile IKE-PROF

interface Tunnel1

ip address 10.255.255.2 255.255.255.0

no ip redirects

ip mtu 1400

no ip split-horizon eigrp 1

ip nhrp authentication KKKdmvpn

ip nhrp map 10.255.255.1 1.1.1.1

ip nhrp map multicast 1.1.1.1

ip nhrp network-id 100000

ip nhrp holdtime 300

ip nhrp nhs 10.255.255.1

delay 1000

tunnel source GigabitEthernet0/0

tunnel mode gre multipoint

tunnel key 100000

tunnel protection ipsec profile DMVPN

BELERAKOM IDE A KONFIGOKAT, HA MÁSHOVA AKARJUK BELERAKNI AKKOR MAJD SZEDD KI

A *x-y. képeken* a VPN-nel kibővített routing táblákat ás a DMVPN státuszokat láthatják.

|  |
| --- |
| *x. kép – KKK-IR ip routing tábla VPN beállítás után* |
| *y. kép – KKK-IR DMVPN állapota* |
| *x. kép – SZE-KKK-IR ip routing tábla VPN beállítás után* |
| *y. kép – SZE-KKK-IR DMVPN állapota* |
| *x. kép – DEB-KKK-IR ip routing tábla VPN beállítás után* |
| *y. kép – DEB-KKK-IR DMVPN állapota* |