Új generációs VPN technológia – Get VPN

Ács György

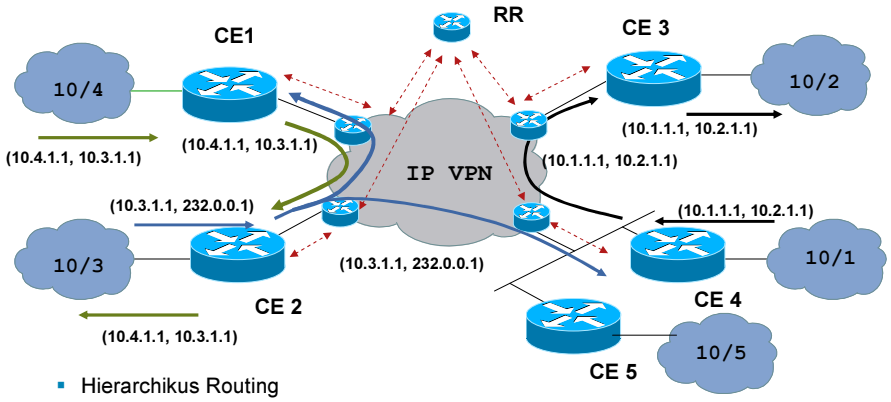
Cisco Systems, Közép-Európa

gacs (at) cisco.com

A paradoxon

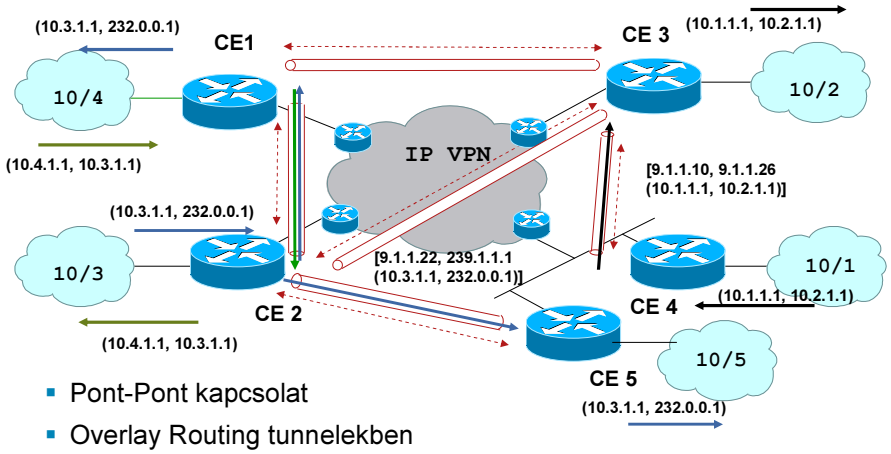
- IP VPN jellemzői …
  - Any to Any (bárki bárkivel) kapcsolat
  - Hierahikus és skálázható routing
  - Hatékony multicast szétosztás
  - Szegmentáció az Internettől
  - Egyszerűsített QoS modellek
- IPSec VPN jellemzői…
  - Titkosítás
  - Integritás
  - Autentikáció
- A két technológia szolgáltatásai eltérnek és konfliktusban vannak egymással

IP VPN jellemzői



- Hierarchikus Routing
- Any-to-Any kapcsolat
- Redundancia az IP VPN PE és P által
- IP VPN PE és P multicast replikáció

IPsec jellemzői



- Pont-Pont kapcsolat
- Overlay Routing tunnelekben
- Redundancia megvalósítása a CE-ben
- Multicast Replikáció megvalósítása CE-ben

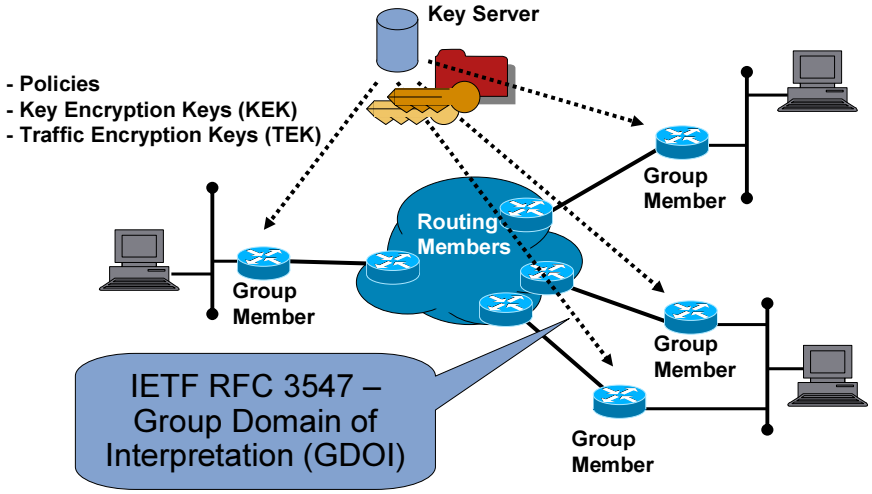
Hálózati paradigma kiértékelése

- IP VPN (e.g. MPLS VPN)
  - Any-to-any kapcsolat (CE-CE Tunnel szomszédság nélkül)
  - Egyszerű CE telepítés
  - Elosztott vagy hierarchikus routing (skálázható)
  - Optimális forgalom továbbítás
  - Biztonság
    - Titkosítás (csak szegmentálás)
    - Szegmentálás
    - Integritás
- IPsec
  - A Point-to-Point Tunnel szomszédok skálázhatósági korlátja
  - Új elem beillesztése
  - A Point-to-Point overlay routing vagy route inzertálás
  - Forgalom a tunneleknek megfelelően, nem biztos, hogy optimális
  - Biztonság
    - Szegmentáció
    - Titkosság
    - Integritás

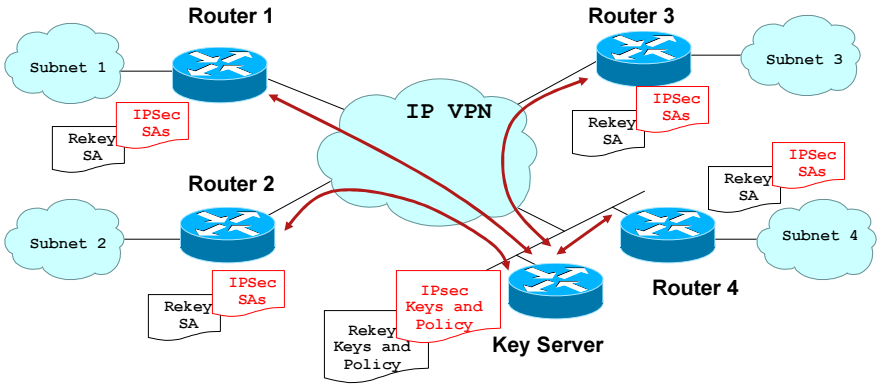
Csoport biztonsági elemek

- Key Server(s) (kulcs szerver, KS)
  - a Group Member-ek kiértékelése
  - A Group Security Policy-k menedzsere
  - A csoport kulcsok generálása
  - A csoport policy-k és kulcsok szétosztása
- Group Member-ek (csoport tagok, GM)
  - Titkosító eszközök
  - Routing a védett és a nem védett hálózati részek között
  - Multicast résztvevők
- Routing résztvevők
  - A GM-ek közötti titkosított forgalom továbbítása, replikálása
  - A titkosítatlan forgalom továbbítása a GM-ektől és GM-ek felé

Csoport biztonsági elemek



GDOI regisztráció



- **Minden egyes GM beregisztrál a KS-be. A KS autentikálja a routert, autorizációs ellenőrzést végez, letölti a titkosítási policy-t és a kulcsokat a GM routerbe**

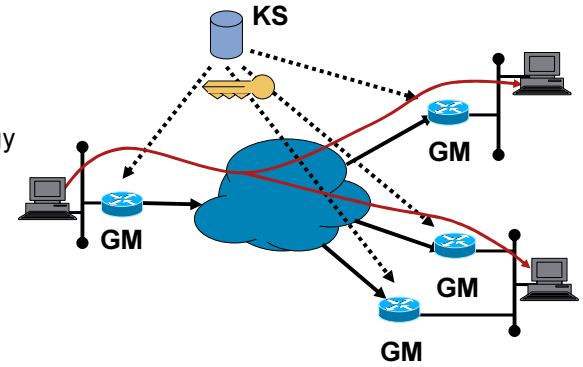
Csoport biztonsági kapcsolat

- A GM-eknek közös a biztonsági kapcsolatuk
  - A biztonsági kapcsolat nem egy adott GM-hez kötődik, hanem a GM-ek egy csoportjához
- A VPN gateway-ek (GM-ek) együttműködnek, hogy ugyanazt az adatot megvédjék
  - A GM-ek megbíznak egymásban
  - A forgalom bármely 2 GM között kialakulhat

Biztonságos adat sík multicast forgalom

Adat védelem
Biztonságos Multicast

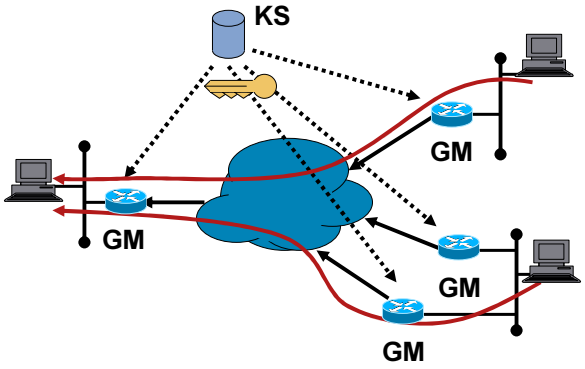
- Előfeltétel: A küldő nem ismeri a potenciális vevőket
- A küldő feltételezi, hogy a legitim csoporttagok megkapták az adott csoportra vonatkozó **Traffic Encryption Key**–ot a KS-től
- A multicast forgalmat úgy titkosítja, hogy az IP címet megőrzi
- Replikáció a core-ban az eredeti csomag alapján



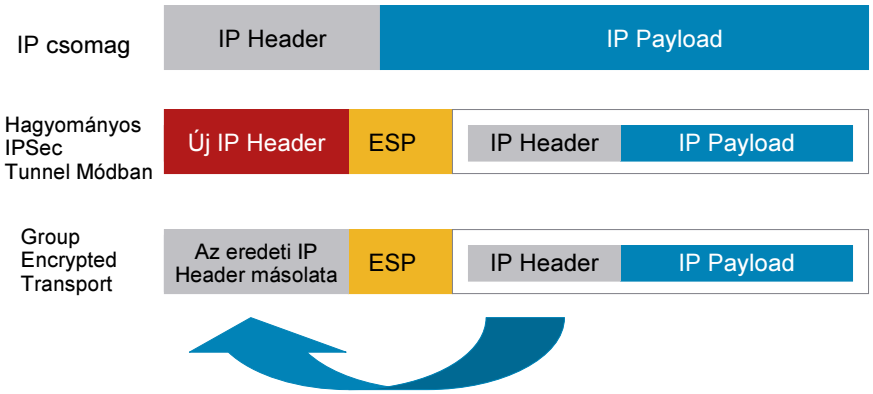
Biztonságos adat sík Unicast következmény

adat védelem
Biztonságos Unicast

- Előfeltétel: A vevő nem ismeri a potenciális küldőket
- A vevő feltételezi, hogy a legitim csoport tagok megkapták az adott csoportra vonatkozó **Traffic Encryption Key-t** a KS-től
- A vevő autentikálni tudja a csoport tagságot

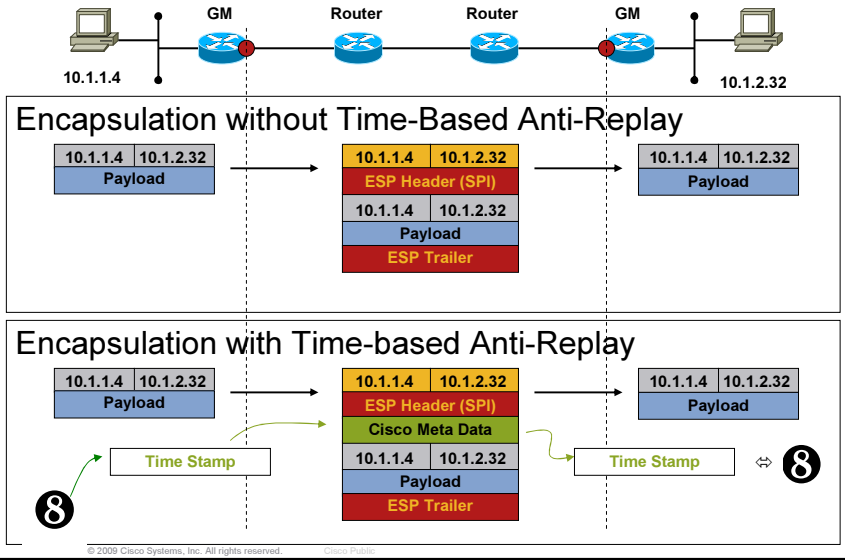


IPSec Tunnel mód IP cím megőrzéssel

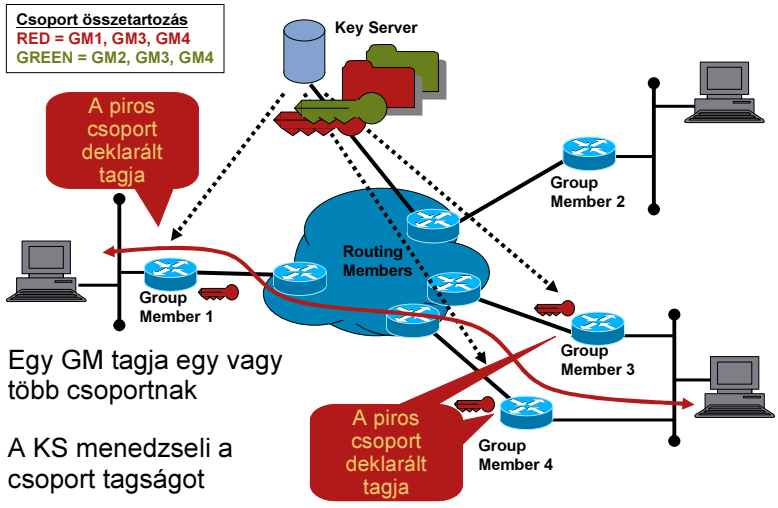


Következmény : QoS és multicast is megmarad, nincs szükség overlay routing-ra

Group Encrypted Transport (adat sík)

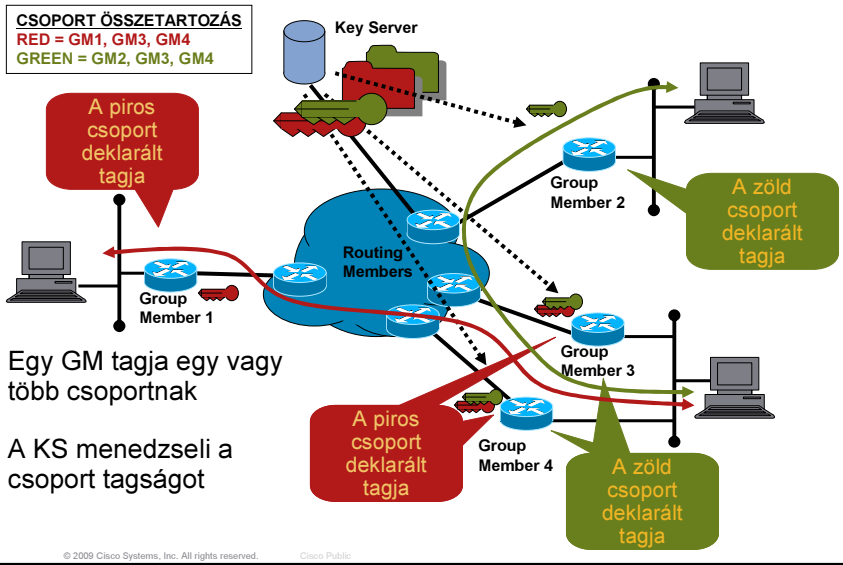


Csoport összetartozás (piros csoport)



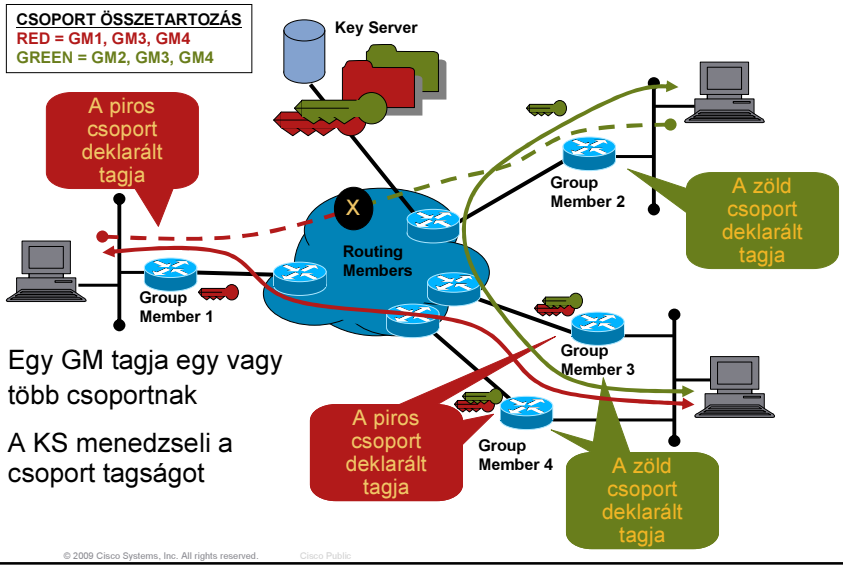
- Egy GM tagja egy vagy több csoportnak
- A KS menedzseli a csoport tagságot

Csoport összetartozás (zöld csoport)



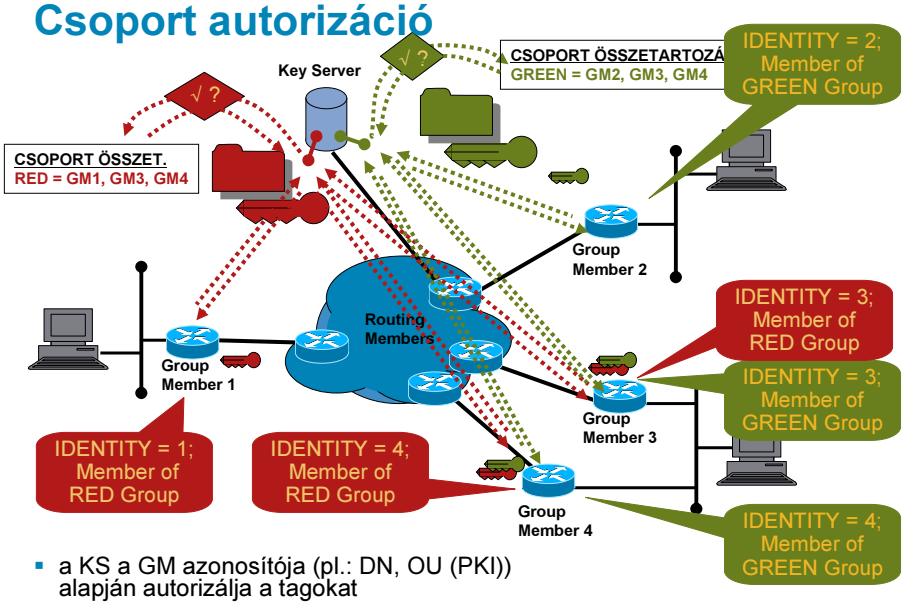
- Egy GM tagja egy vagy több csoportnak
- A KS menedzseli a csoport tagságot

Csoport összetartozás (kölcsönösen kizáró)



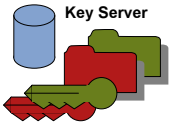
- Egy GM tagja egy vagy több csoportnak
- A KS menedzseli a csoport tagságot

Csoport autorizáció



- a KS a GM azonosítója (pl.: DN, OU (PKI)) alapján autorizálja a tagokat

Titkosító eljárások



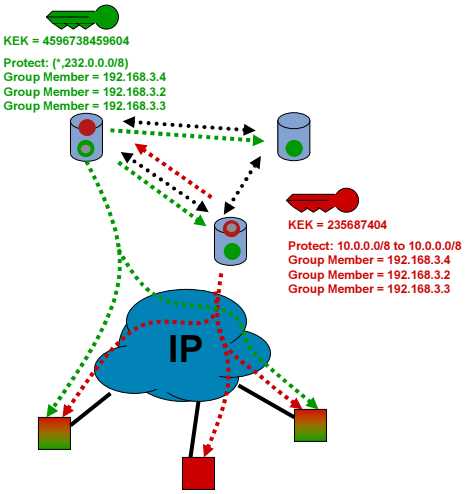
- A KS csoportonként kezeli a policy-t és a titkosítási jellemzőket

- IPsec Attributes
  - IPsec Tunnel Mode w/Header Preservation
  - Receive-Only
  - 3DES
- Policy
  'permit ip 10/8 10/8'

- IPsec Attributes
  - IPsec Tunnel Mode w/Header Preservation
  - Anti-Replay
  - AES
- Policy
  - 'permit ip 10/8 232/8'

Együttműködő KS-ek

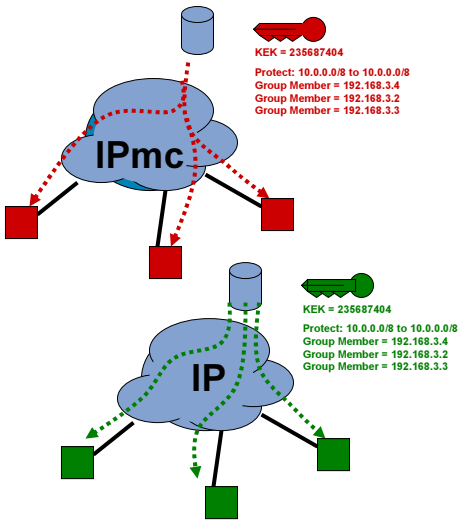
- Csoportonként van egy kijelölt elsődleges KS
  1. Prioritás alapján megbeszélt
  2. Legnagyobb IP cím alapján megbeszélt
- Csoportonként több másodlagos KS lehet
  - Elsődlegessé válik, ha a kijelölt elsődleges kiesik
- A policy adatbázis szinkronizációja – állapotkövető átkapcsolás
  - Csoport Policy, aktív GM-ek, KEK, TEK: mindent szinkronizál



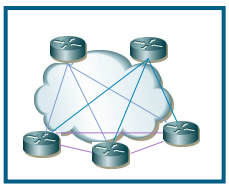
Jelenleg max. 8 KS/GetVPN

Multicast / Unicast kulcs szétosztás

- Multicast kulcs szétosztás multicast képes hálózaton
  - Multicast formában küldött csomag és hálózati replikáció
  - Visszatérés a GM GDOI Unicast regisztrációra hiba esetén
- Unicast kulcs szétosztás multicast-ra nem képes hálózaton
  - Unicast formában GM-enként külön
  - Visszatérés a GM GDOI Unicast regisztrációra hiba esetén

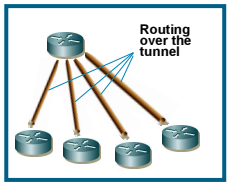


Tervezési szempontok



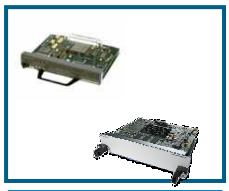
Policy?

Megengedő vagy kizáró



Skálázhatóság?

Kulcsfrissítési eljárás, KS architektúra



Titkosítási teljesítmény?

VAM2+, VSA, SPA

Finomhangolás

Policy menedzsment

1. lépés : Milyen forgalmat kell titkosítani?

2. lépés: A szükséges KS kiválasztása, a KS architektúra megtervezése

3. lépés : A szükséges GM platform és titkosító kártya kiválasztása

4. lépés: A policy finomhangolása, az időzítők optimalizálása

Általános javaslatok

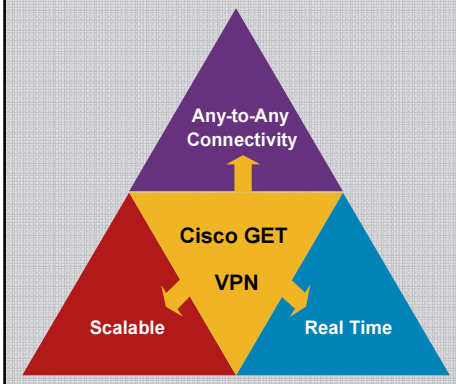
- Titkosítás
  - AES
  - PKI a GM / KS autentikációra
  - TEK lifetime min. 1 hour
  - KEK lifetime min. 24 hours
  - Multicast Rekey a KEK / TEK kulcs szétosztásra
- Architektúra
  - – Osszuk meg a GM-ket, más legyen a preferált KS-ük, ahová először megpróbálnak beregisztrálni
  - – Egyszerűsítsük a konfigurációt szimmetrikus IPsec proxy policy-kel
  - (pl.: ‘permit ip any any’ vagy ‘permit ip 10/8 10/8’)
  - – A KS állomások fizikai szeparációja; közöttük megbízható, redundáns út

Kérdések?

Összefoglalás

Cisco Group Encrypted Transport (GET) VPN –
Megoldás tunnel nélküli VPN-ekre

Cisco GET VPN forradalmi megoldás a tunnel nélküli, any-to-any biztonságos, titkosított kommunikációra



- **Skálázható**
- **Natív routing tunnel nélkül**
- **Optimális QoS és multicast támogatás – javítja az alkalmazás teljesítményét**
- **Sokféle transzport réteg – privát LAN/WAN, FR/ATM, IP, MPLS**
- **Rugalmas vezérlésmegosztás az előfizetők és szolgáltatók között**
- **Támogatják: Cisco ISR routerek, Cisco 7200 és Cisco 7301, ASR**

További információk:

GetVPN:
http://www.cisco.com/go/getvpn