

Sponzor konferencije



Partner digitalnog oglašavanja



Partneri konferencije



Pokrovitelji konferencije



Tehnološki sponzori



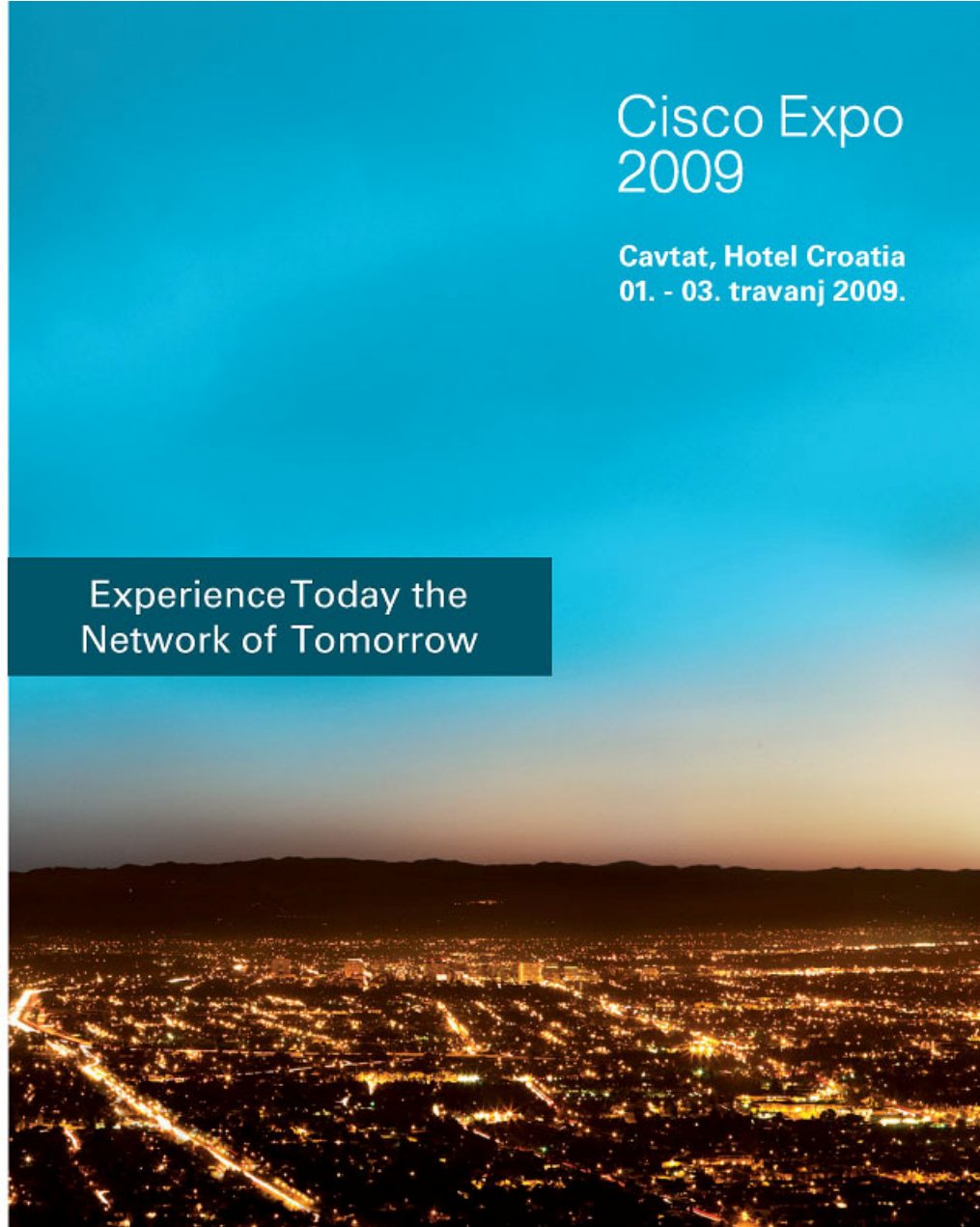
Medijski sponzori



Cisco Expo 2009

Cavtat, Hotel Croatia
01. - 03. travanj 2009.

Experience Today the
Network of Tomorrow

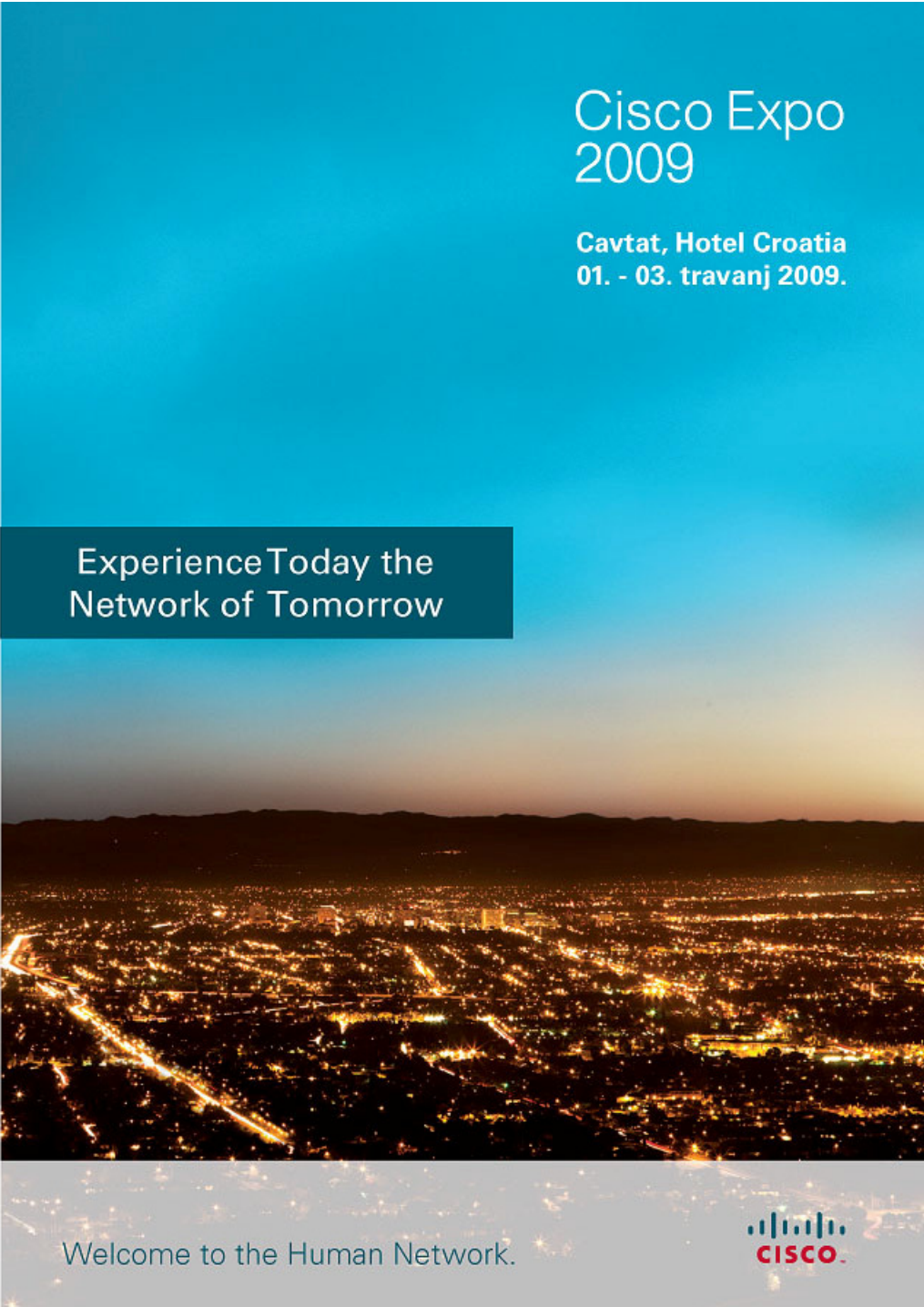


Welcome to the Human Network.



 **GetVPN
Inovativno
Enkriptiranje WAN-a
na Korporativnoj Mreži**

Toni Kuzman
toni.kuzman@king-ict.hr


A promotional poster for Cisco Expo 2009. The top half has a blue gradient background with the event title and location. The bottom half shows a night view of a city with lights. A dark teal banner across the middle contains the slogan. The Cisco logo and slogan are at the bottom.

**Cisco Expo
2009**

Cavtat, Hotel Croatia
01. - 03. travanj 2009.

Experience Today the
Network of Tomorrow

Welcome to the Human Network.



Zašto GetVPN?

- GetVPN (Group encrypted transport VPN) je nastao kao odgovor na potrebu enkriptiranja prometa na WAN privatnim mrežama
- GetVPN kreira Group IPsec policy, te nema potrebe za kreiranje peer-to-peer tunela između enkripcijskih točaka, tunnel-less tehnologija
- GetVPN u fullmesh topologijama mreža kao IP/MPLS, omogućava nesmetan i kvalitetan protok kritičnih voice i video aplikacija, koristeći QOS, multicast i postojeći routing

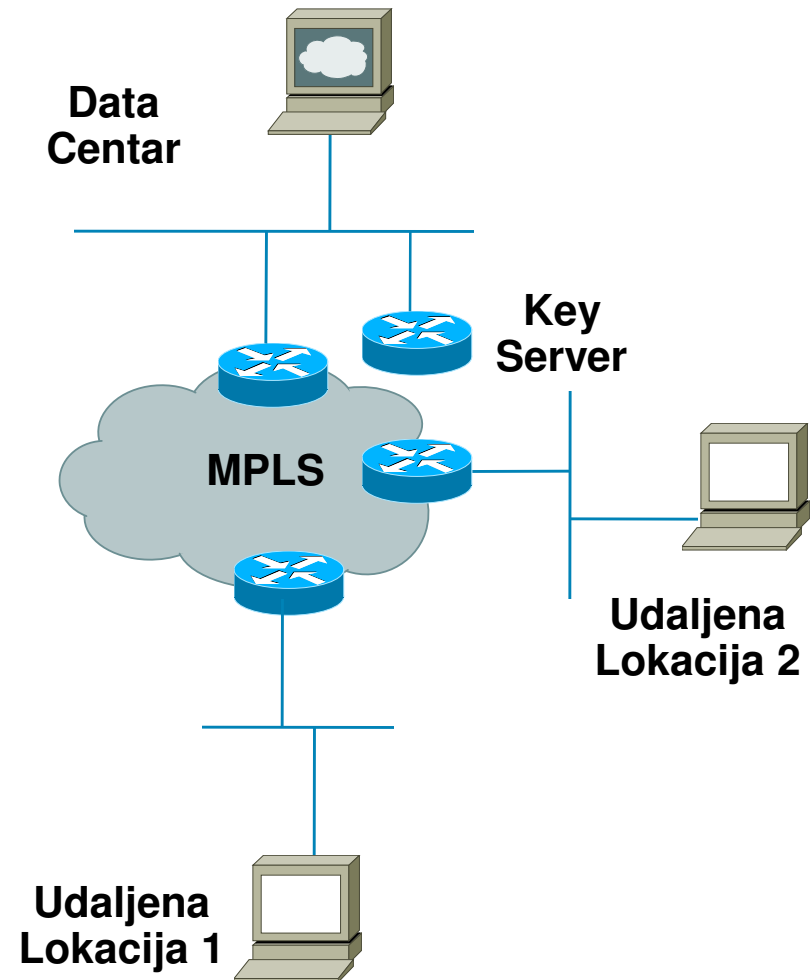
Osnovni Pojmovi GetVPN Tehnologije



Osnovni Pojmovi GetVPN Tehnologije

KS – Key Server

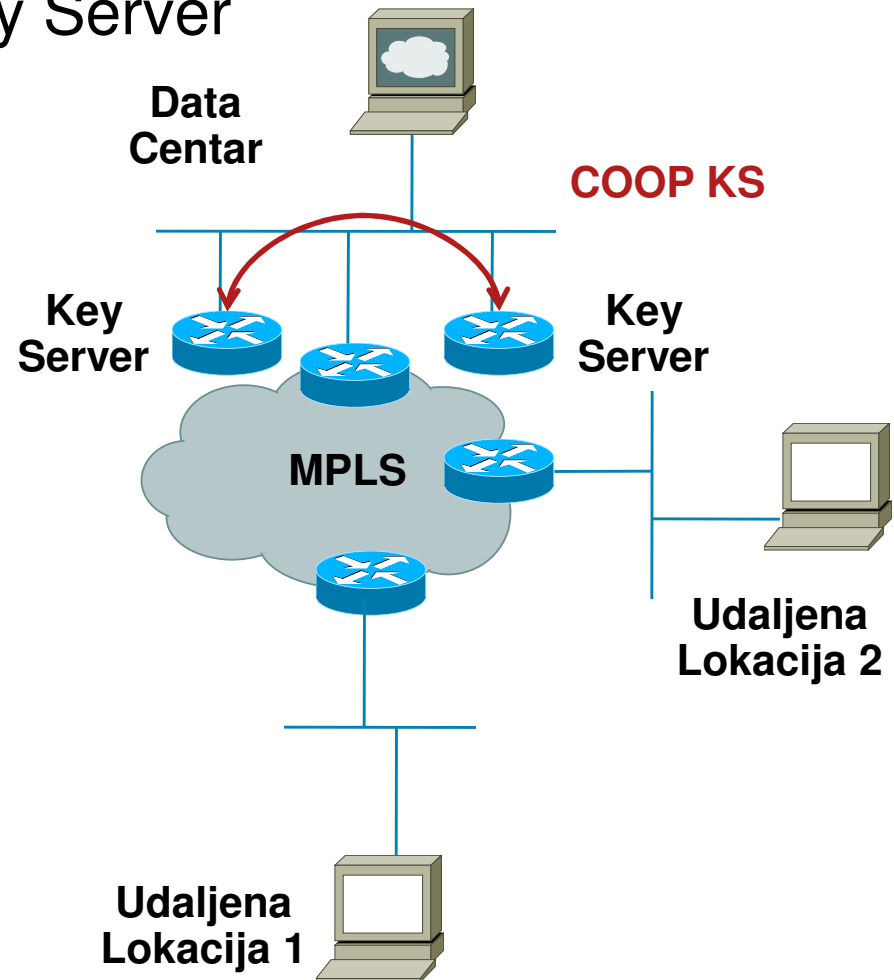
- KS je centralno mjesto za kreiranje i održavanje enkripcijske politike unutar GetVPN-a
- KS je usmjernik na kojem se kofiguriraju enkripcijski algoritmi, hash algoritmi, interesatni promet, rekey timers
- KS kreira i održava KEK (Key Encryption Key), TEK (Traffic Encryption Key) ključeve i pseudo-timer
- KS ne može biti Group Member



Osnovni Pojmovi GetVPN Tehnologije

COOP KS – Cooperative Key Server

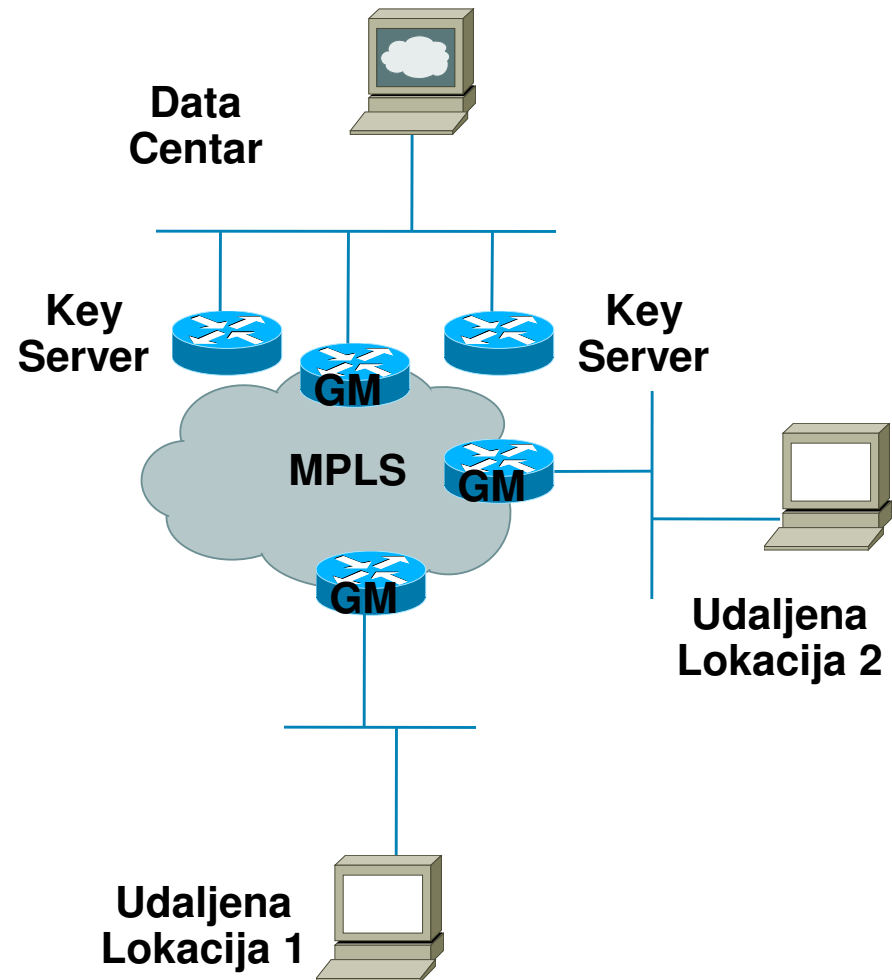
- KS kao centralno mjesto za kreiranje i održavanje enkripcijske politike ima najvažniju ulogu u GetVPN mreži
- COOP KS je protokol koji omogućava sinkronizaciju između više KS-a u grupi
- Samo je primarni KS zadužen za proces ažuriranja Group policy-a u mreži



Osnovni Pojmovi GetVPN Tehnologije

GM - Group Member

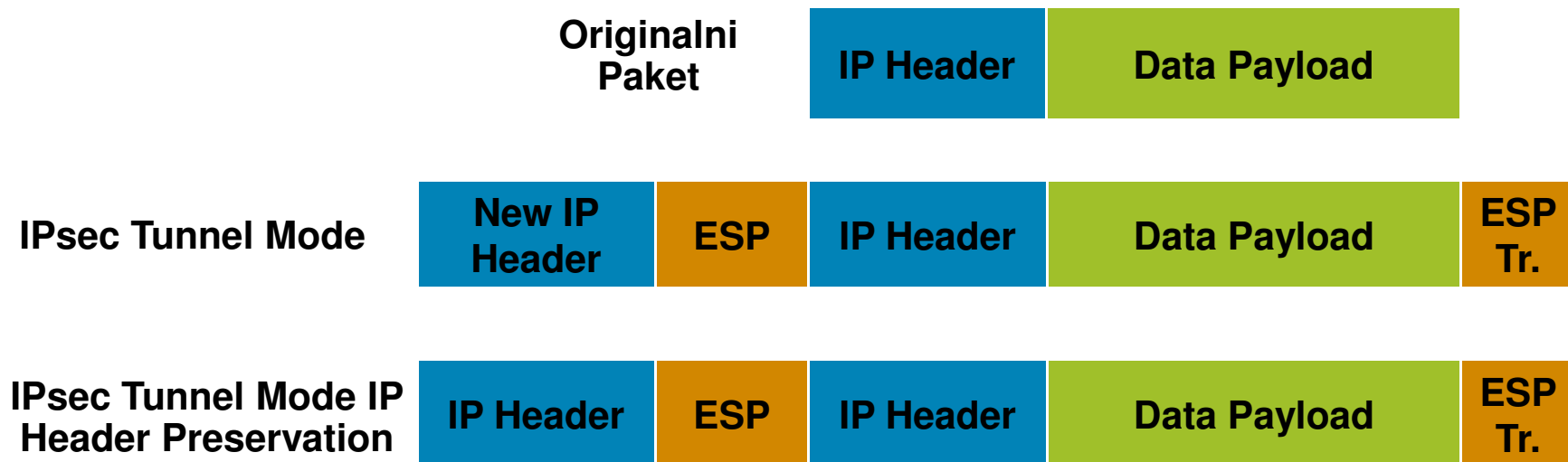
- GM je usmjernik u mreži zadužen za enkriptiranje/dekriptiranje IP prometa
- GM se konfigurira samo sa IKE postavkama i informacijama o KS/Group
- IPsec policy, informacije kako određeni IP promet tretirati GM dobiva od KS-a
- Na GM je moguće konfigurirati neophodne iznimke u odnosu na Global policy



Osnovni Pojmovi GetVPN Tehnologije

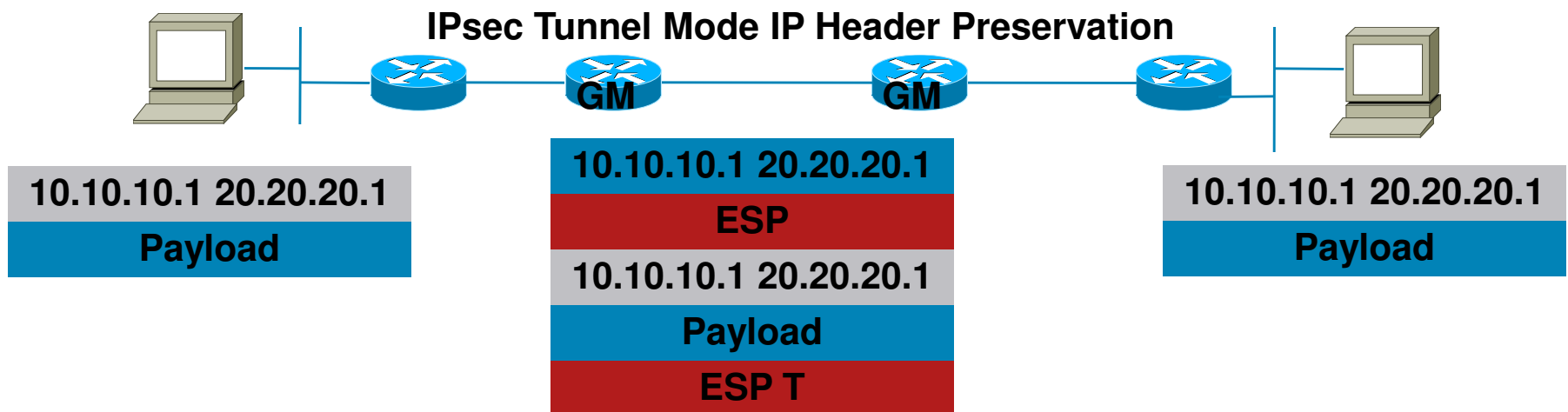
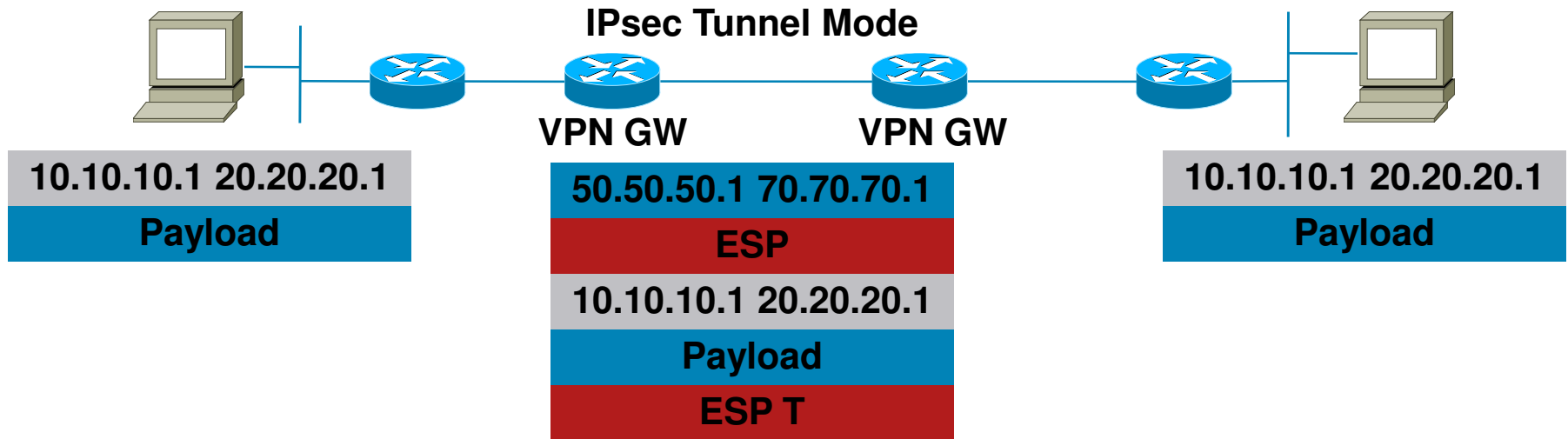
IP Header Preservation

- Za razliku od IPsec Tunnel ili Transport moda, GetVPN kopira originalni IP header i postavlja ga na početak enkriptiranog paketa
- IP header preservation omogućava korištenje postojećeg routinga u mreži, kao i QOS i multicast mehanizama



Osnovni Pojmovi GetVPN Tehnologije

IP Header Preservation



Osnovni Pojmovi GetVPN Tehnologije

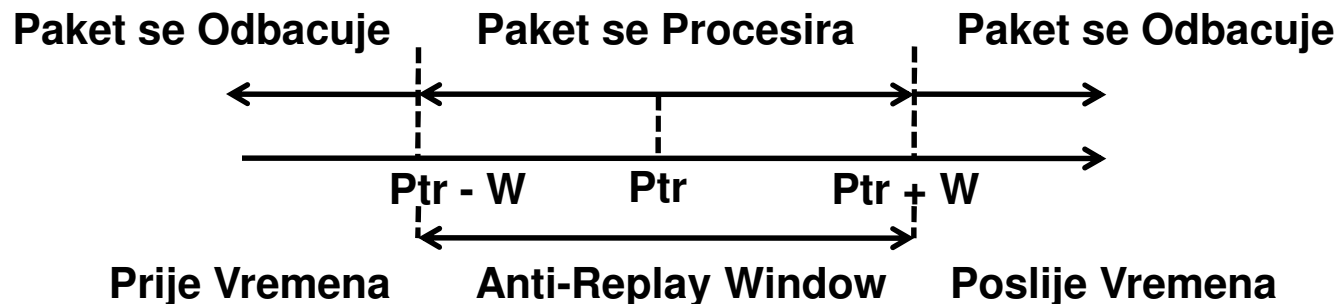
Group SA

- Svi registrirani GM imaju jednak Group policy i zajednički IPsec SA
- Nema potrebe za kreiranje peer-to-peer IPsec tunela
- Asimetričan protok IP prometa kroz mrežu

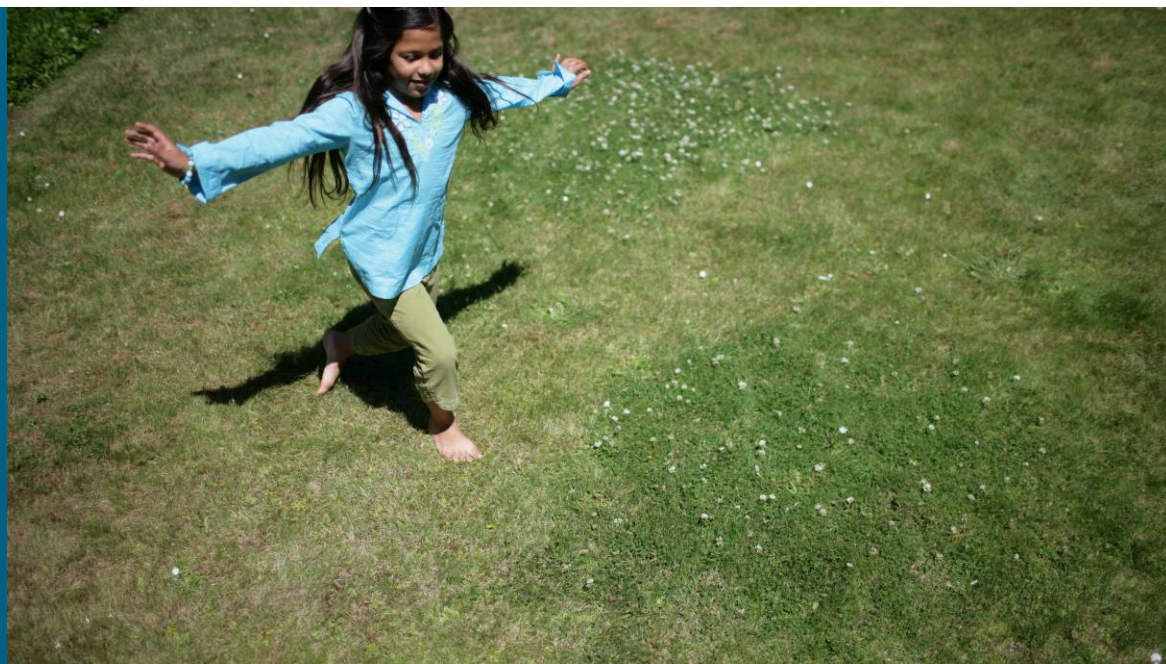
Osnovni Pojmovi GetVPN Tehnologije

TBAR - Time Based Anti-Replay

- U GetVPN grupi, GM ne zna a priori svoj IPsec peer
- Korištenje Anti-Replay mehanizma baziranog na counter windowu nema smisla
- TBAR mehanizam, baziran na pseudo-timeru, kreira, distribuira i održava primarni KS u mreži
- Pseudo-timer je relativan sat za cijelu grupu i neovisan je o NTP ili GPS-u



GetVPN Data Plane



Data Plan

Multicast

- Sender Multicast prometa ne zna ko je receiver poruke
- GM sender pretpostavlja da svi GM u GetVPN mreži imaju validne TEK ključeve
- Enkripcija Multicast prometa sa IP Header preservation
- Multicast replikacija u Core mreži

Unicast

- GM receiver ne zna ko je sender a priori
- GM receiver pretpostavlja da svi GM u GetVPN mreži imaju validne TEK ključeve
- Enkripcija Unicast prometa sa IP Header preservation

GetVPN Kontrolni Promet



GM Kontrolni Promet

- GM se odmah nakon reboota pokušava registrirati na KS
- Ako se ispravno autentificira, uspostavlja se IKE SA tunel, kroz koji GM dobiva security policy zajedno sa enkripcijskim ključevima, KEK, TEK i Public RSA Key.
- KEK ključ se koristiti za enkripciju kontrolnog prometa
- TEK ključ se koristi za enkripciju IP prometa
- RSA key GM koristi kako bi provjerio vjerodostojnost poruke koju je primio putem GDOI protokola
- Kako bi GM bio funkcionalan u GetVPN mreži, mora redovno održavati i primjenjivati nove sigurnosne politike, KEK i TEK ključeve, i vremensku sinkronizaciju

GM Kontrolni Promet

- GM prije nego postane član GetVPN grupe šalje i prima clear tekst data, Fail-open mod
- Nakon registracije u GetVPN grupi, GM prelazi u Fail-closed mode rada
- U slučaju vremenskog isteka IPsec policy i nemogućnosti re-registracije, GM ostaje u Fail-close modu i odbacuje sav promet koji bi prema security policy trebao biti enkriptiran/dekriptiran

ISAKMP Policy

```
crypto isakmp policy 10  
  encr aes  
  authentication pre-share  
  group 2
```

KS Poslužitelji i Autentikacijski Ključevi

```
crypto isakmp key tektek address 10.0.0.4  
crypto isakmp key tektek address 10.0.0.3
```

GDOI Grupa

```
crypto gdoi group GetVPN  
  identity number 5555  
  server address ipv4 10.0.0.3  
  server address ipv4 10.0.0.4
```

Crypto Mapa

```
crypto map getvpn-map 10 gdoi  
  set group GetVPN
```

Fail-Open vs Fail-Close

- Koji će se model koristiti ovisi da li promet kroz WAN mrežu smije biti clear tekst ili ne
- Fail-close mode se može osigurati sa access-listom na izlaznom sučelju GM, koja osigurava samo propuštanje ESP i kontrolnog prometa, sav drugi promet biva odbačen
- Sa IOS 12.4 (22) T, paradigmu Fail-close, je moguće konfigurirati kako bi bila prijavljena na GM i prije nego se GM registira na KS

GDOI Grupa

```
crypto gdoi group GetVPN  
identity number 5555  
server address ipv4 10.0.0.3  
server address ipv4 10.0.0.4
```

Fail-Close Crypto Map

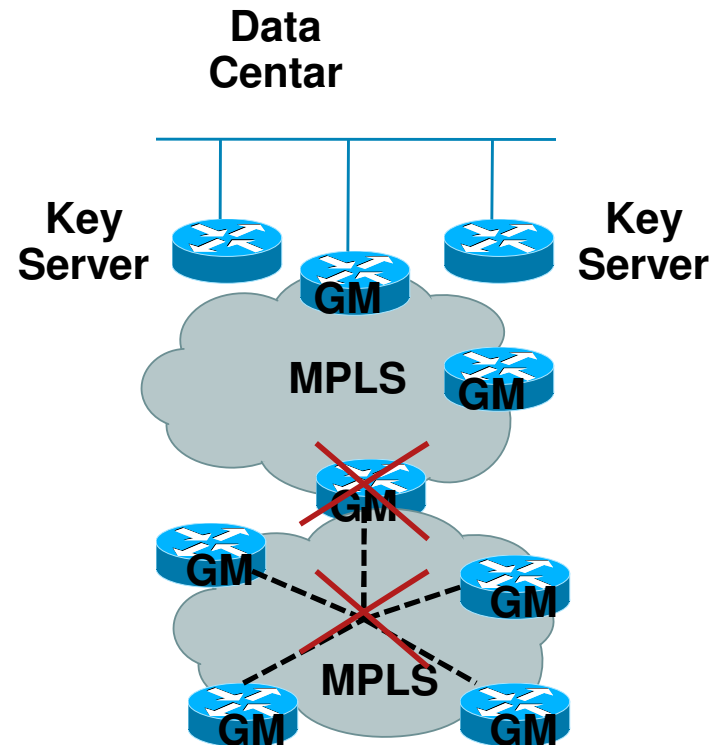
```
crypto map sec gdoi fail-close  
match address Get_Eny  
activate
```

ACL za Fail-Close Mapu

```
access-list extended Get_Eny  
deny tcp any any eq 22  
deny tcp any eq 22 any  
deny tcp any any eq telnet  
deny tcp any eq telnet any  
deny ospf any any
```

Regija Odsječena od KS-a?

- Nije moguća re-registracija GM
- GM u Fail-close modu
- Prekinuta komunikacija unutar regije
- Fail-open je moguće postići sa *čišćenjem* IPsec policy sa GM
- Komanda: *clear crypto gdoi*



Regija Odsječena od KS-a?

- Postoje dva načina za aktiviranje komande *clear crypto gdoi*:
 - Ručno, nije moguće ako nemamo administrativni backup ulaz, vremenski zatjevno u ovisnosti od broja GM u regiji
 - Automatski sa EEM
- Bez obzira u kojem se modu radi, GM konstatno pokušava sa re-registracijom na KS u pravilnim vremenskim razmacima

KS Kontrolni Promet

- Uloga KS može biti primarna ili sekundarna u GetVPN mreži
- Prilikom izbora u COOP KS procesu, svi KS startaju kao sekundarni
- Primarni KS postaje onaj sa najvećim konfiguriranim priority-em ili sa najvećom IP adresom
- Primarni KS je zadužen za kreiranje, distribuiranje, i održavanje Group policy-a u GetVPN mreži
- Primarni KS ažurira sve sekundarne KS sa Group policy-em
- Sekundarni KS ne sudjeluje u procesu ažuriranja prema GM

KS Kontrolni Promet

- Prvi korak u konfiguriranju KS je generiranje RSA ključeva koji se exportiraju na sve KS u GetVPN mreži
- KS u COOP KS grupi moraju imati iste RSA ključeve
- Primarni KS ne distribuira GetVPN postavke na ostale KS u grupi
- Svaki KS se mora zasebno konfigurirati, kao i sve naknadne promjene u GetVPN postavkama

KS Kontrolni Promet

```
crypto ipsec profile GetTEST
set security-association lifetime seconds 7200
set transform-set GET
```

```
crypto gdoi group GetVPN
identity number 5555
server local
```

```
rekey lifetime seconds 21600
rekey retransmit 40 number 3
rekey authentication mypubkey rsa KEY_KS2
rekey transport unicast
authorization address ipv4 55
registration interface FastEthernet0/1
```

```
sa ipsec 50
profile GetTEST
match address ipv4 Get
replay time window-size 5
address ipv4 10.0.0.4
```

```
redundancy
local priority 100
peer address ipv4 10.0.0.3
```

IPsec Profil

GetVPN Grupa
Identifikacijski Broj Grupe
Konfiguriranje KS poslužitelja

KEK Lifetime
Vrijeme i Broj Rekey Retransmisija
RSA Ključ za Potpis Rekey Poruke
Transportni Mehanizam
Autorizacijski ACL
Sučelje za Registraciju

IPsec za Kreiranje TEK
IPsec Profil
Enkripcijski ACL
Anti-Replay Window
IP Adresa za Rekey Proces

Kreiranje COOP KS
Lokalni Priority
Peer IP Adresa

KS Kontrolni Promet

ip access-list extended Get

deny esp any any

deny udp any eq isakmp any eq isakmp

deny udp any eq 848 any eq 848

deny tcp any any eq 22

deny tcp any eq 22 any

deny ospf any any

permit ip any any

ACL – ACL za IPsec Policy

Nekriptirati ESP

Nekriptirati ISAKMP

Nekriptirati GDOI

Nekriptirati SSH Destination

Nekriptirati SSH Source

Nekriptirati OSPF

Kriptirati Sav Ostali Promet

- Svaki permit zapis u ACL-u kreira jedan IPsec SA na GM u odlaznom i dolaznom smjeru
- Dozvoljeno je 100 ACL linija deny/permit
- Nije moguće definirati range portova
- Preopuka je držati ACL listu što jednostavnijom
- Nastojati obuhvatit promet koji treba enkriptirati sa što manje permit linija

Proces Ažuriranja IPsec SAs



Proces Ažuriranja IPsec SAs

- Rekey je proces ažuriranja IPsec SA, KEK & TEK ključevi, pseudo-timer
- Rekey je vremenski kraći proces re-registracije GM od full re-registracije
- KS je zadužen za Rekey proces
- Rekey može koristiti Multicast ili Unicast transportnu tehnologiju

Proces Ažuriranja IPsec SAs

Multicast

- Multicast ažuriranje je efikasnije i procesorski manje zahtjevno
- Preduvjet je da su GM članovi multicast grupe
- KS ne zna dali je GM primio novi ključ ili ne
- KS ne održava listu GM-a
- Multicast je default mode Rekey procesa
- Izračun Multicast refresh time, $TEK=7200\text{sec}$

Offset Time = $7200 * 10\% = 720\text{s}$

Retransmisija $2 * 40\text{sec} = 80\text{s}$

Rekey T = $7200 - 720 - 80 = 6400\text{s}$

Proces Ažuriranja IPsec SAs

Unicast

- Za svaku poslanu Unicast Rekey poruku, KS očekuje ACK od GM
- Ako GM propusti Rekey poruku, neće poslati ACK, te KS starta sa retransmisijom
- KS održava listu aktivnih GM, i samo njima šalje Rekey poruku
- Ako i nakon ponovljenih Rekey poruka GM ne pošalje ACK, biva izbrisan sa liste aktivnih GM
- Izračun za GetVPN grupu od 100GM, vrijeme za Rekey proces 10sec, TEK=7200sec

TEK = 7200 – 10 = 7190sec

Offset Time = 7200 * 10% = 720s

Retransmisija 2 * 40sec = 80sec

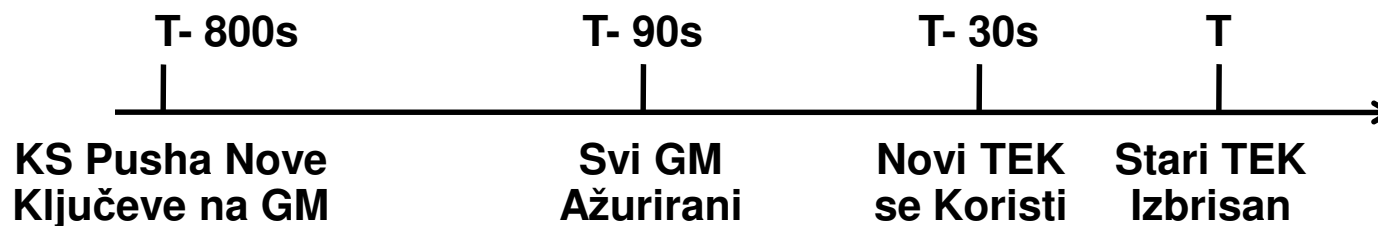
Refresh T = 7190 – 720 – 80 = 6390s

rekey lifetime seconds rekey 21600
rekey retransmit 40 number 3
rekey authentication mypubkey rsa *KEY*
rekey transport unicast

Proces Ažuriranja IPsec SAs

Rekey Proces

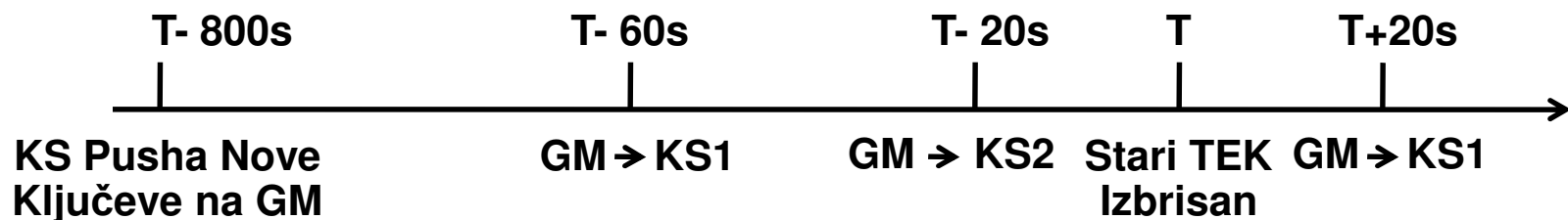
- KS generira i *pusha* TEK ključ prije isteka starog TEK ključa na GM
- GM počinje koristiti novi TEK ključ 30 sec prije isteka starog TEK ključa
- Time je osigurano da se poruke koje su enkriptirane sa starim TEK ključem i dalje mogu dekriptirati



Proces Ažuriranja IPsec SAs

Rekey Proces

- Što ako GM nije dobio novi TEK ključ?
- 60 sec prije isteka aktivnog TEK ključa, GM pokušava sa re-registracijom na KS
- GM radi retransmisiju 4 puta u razmacima od po 10sec
- GM se pokušava registrirati na drugi KS, ako je konfiguriran
- Ako je i drugi KS nedostupan, GM pokušava registraciju opet na prvi KS
- Back-off Time 30sec, 1min, 2min, 4min, 8min

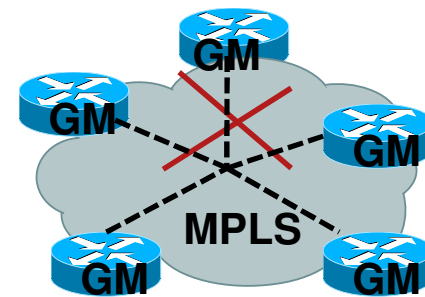


Tranzicija sa Clear na Crypto GetVPN Mrežu



Tranzicija sa Clear na Crypto GetVPN Mrežu

- Izazov je implementirati enkripciju na mreži, bez prekida prometa
- Prilikom registracije prvog GM, započinje enkriptiranje IP prometa
- Receive-only način rada, omogućava implementaciju GetVPN na siguran način, bez prekida
- Receive-only se konfigurira na KS-u



Tranzicija sa Clear na Crypto GetVPN Mrežu

Faze Implementacije

- Konfigurirati receive-only na KS-u
- Provjeriti da li svi GM imaju validan Group policy
- Testirati GetVPN funkcionalnosti sa passive modom rada na GM
- Rekonfiguriranje receive-only na KS-u

```
crypto gdoi group GetVPN  
identity number 5555  
server local  
sa receive-only
```

```
show crypto gdoi
```

```
crypto gdoi gm ipsec  
direction inbound optional
```

```
crypto gdoi group GetVPN  
identity number 5555  
server local  
no sa receive-only
```

Tranzicija sa Clear na Crypto GetVPN Mrežu

Proces Nakon No Receive-Only

- KS generira novi Group policy i pusha na članove grupe
- GM iz receive-only načina rada prelaze u passive
- Iz passive načina rada GM prelaze u conformant
- Group policy se prijavljuje na oba smjera prometa
- Od IOS 12.4 (22) T uvedena je mogućnost trajnog passive načina rada u svrhu testiranja

```
R1#sh cry gdoi
GROUP INFORMATION

Group Name           : GetVPN
Group Identity       : 5555
Rekeys received      : 3679
IPSec SA Direction   : Inbound Only
```

```
R1#sh cry gdoi
GROUP INFORMATION

Group Name           : GetVPN
Group Identity       : 5555
Rekeys received      : 3680
IPSec SA Direction   : Inbound Optional
```

```
R1#sh cry gdoi
GROUP INFORMATION

Group Name           : GetVPN
Group Identity       : 5555
Rekeys received      : 3681
IPSec SA Direction   : Both
```

GetVPN Design



GetVPN Design

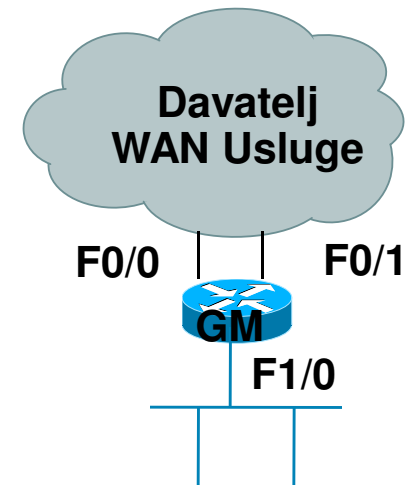
- GetVPN je podržan na Cisco usmjernicima od verzije IOS 12.4 (11) T Advanced Security
- Podržani hardware

	Crypto	GM	KS
87x	On-Board	Da	Da (Avoid)
1800	AIM-VPN	Da	Da
2800	AIM-VPN	Da	Da
3800	AIM-VPN	Da	Da
7200 NPE GE1/2	VAM2+	Da	Da
7200 NPG2	VSA	Da	Da
ASR	ESP	Da	Ne
6500	VPN-SPA	Da	Ne

GetVPN Design

GM Design

- Osigurati visoki stupanje dostupnosti i pouzdanosti
- Crypto Map se može prijaviti na više WAN sučelja
- Kao Source IP adresa za registraciju GM koristiti Loopback adresu



```
crypto map getvpn-map local-address Loopback0
```

```
interface FastEthernet0/0  
description MPLS  
ip address 10.5.5.1 255.255.255.0  
crypto map getvpn-map
```

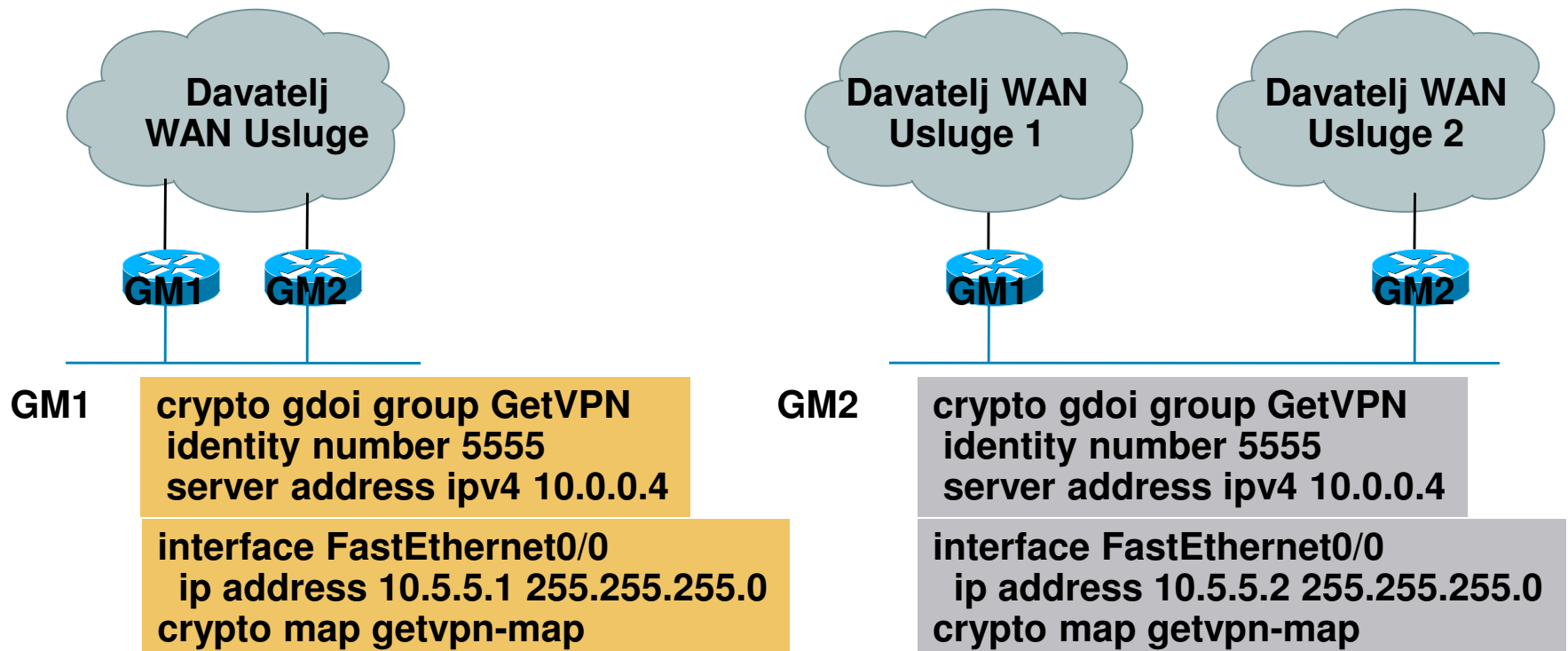
```
interface FastEthernet0/1  
description MPLS  
ip address 10.5.5.1 255.255.255.0  
crypto map getvpn-map
```

```
KS2#sh cry gdoi ks members  
Group Member Information :  
Number of rekeys sent for group GetVPN : 4099  
Group Member ID : 10.0.0.1  
Group Member ID : 10.0.0.10  
Group Member ID : 10.0.0.11
```

GetVPN Design

GM Design

- Povećanje stupnja dostupnosti se može izvesti sa redundantnim hardware-om na lokaciji
- Odabir više davatelja WAN usluge



GetVPN Design

GM Skalabilnost

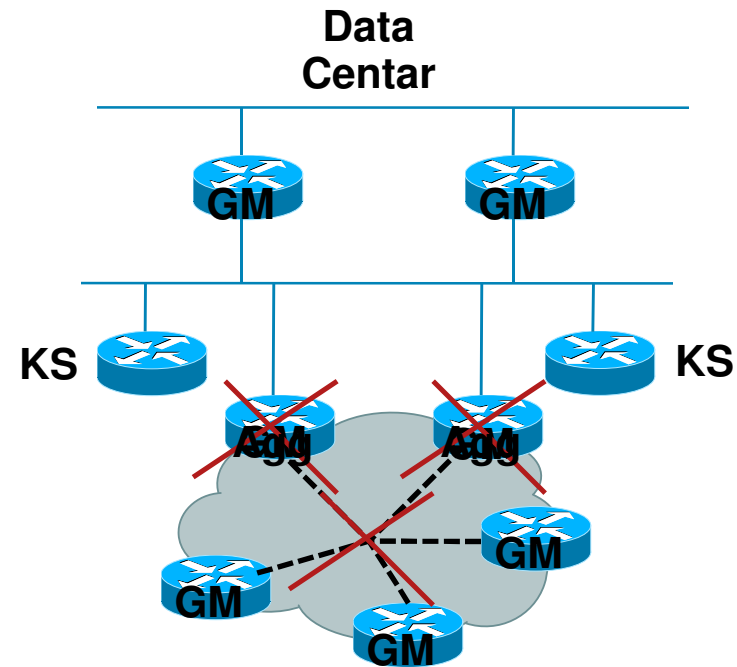
- Propusnost usmjernika u Mbit/s
- IMIX, uzorak 7 *
64, 4*568,
1*1400 Bytes

	Crypto	74 Bytes	IMIX	1400 Bytes
7200 NPE G2	VSA	230	230	940
3845	AIM-VPN	31	140	200
2851	AIM-VPN	16	86	190
2821	AIM-VPN	15	70	190
1841	AIM-VPN	4	22	83
871	On-Board	1	9	28

GetVPN Design

KS Design

- Preporuka je redundatni KS hardware na centralnoj lokaciji
- Razdvojiti Agg i GM funkcionalnosti
- Dodatna redundancija KS u pojedinim regijama
- Osigurati dovoljno resursa za registracijski proces i Rekey proces
- Backup veza između KS u KS COOP grupi
- Maximalno 2000 GM po KS-u, preporuka 1000 GM

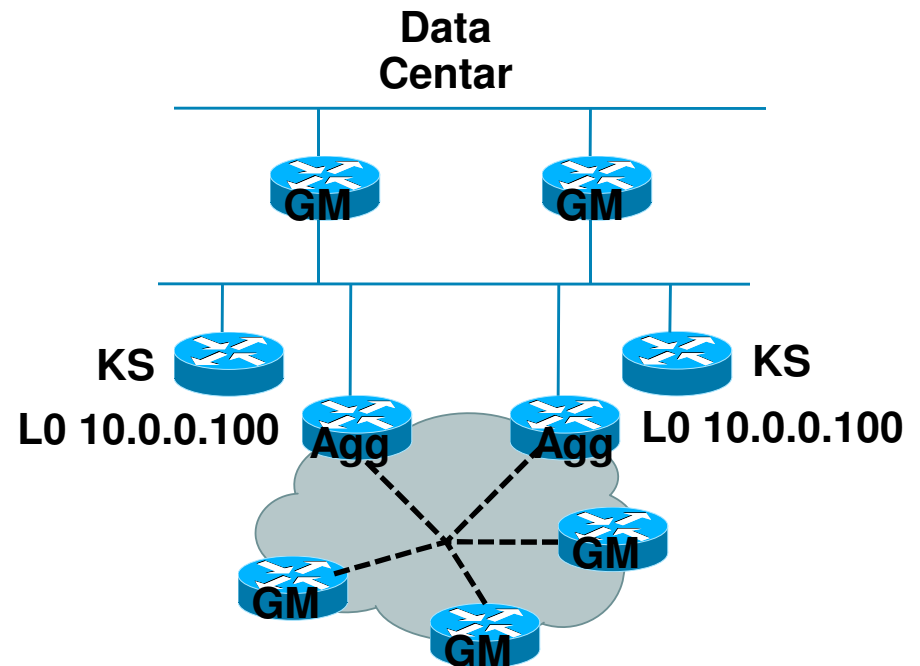


GetVPN Design

KS Design

- Load-balancing prilikom registracije GM na KS se može postići na tri načina:
- Jedna Loopback adresa na svim KS
- GM po regijama imaju definirano u hijerarhiji različite KS
- SLB – Server Load Balancing

```
crypto gdoi group GetVPN  
identity number 5555  
server local  
registration interface Loopback0
```



```
crypto gdoi group GetVPN  
identity number 5555  
server address ipv4 10.0.0.4  
server address ipv4 10.0.0.3
```

```
crypto gdoi group GetVPN  
identity number 5555  
server address ipv4 10.0.0.3  
server address ipv4 10.0.0.4
```

GetVPN Design

KS Skalabilnost

- Broj podržanih GM u odnosu na Rekey transport i KS hardware

Usmjernik	Unicast Rekey	Multicast Rekey
<ul style="list-style-type: none">• 7200• 3845• 3825• 2851• 2821• 1841	<ul style="list-style-type: none">• 1000• 500• 250• 100• 50• 25	<ul style="list-style-type: none">• 2000• 1000• 500• 200• 100• 50

Q and A





CISCO