



Cisco Expo 2009

conf t: Cisco IPSec
VPN rešenja u
mrežama poslovnih
korisnika

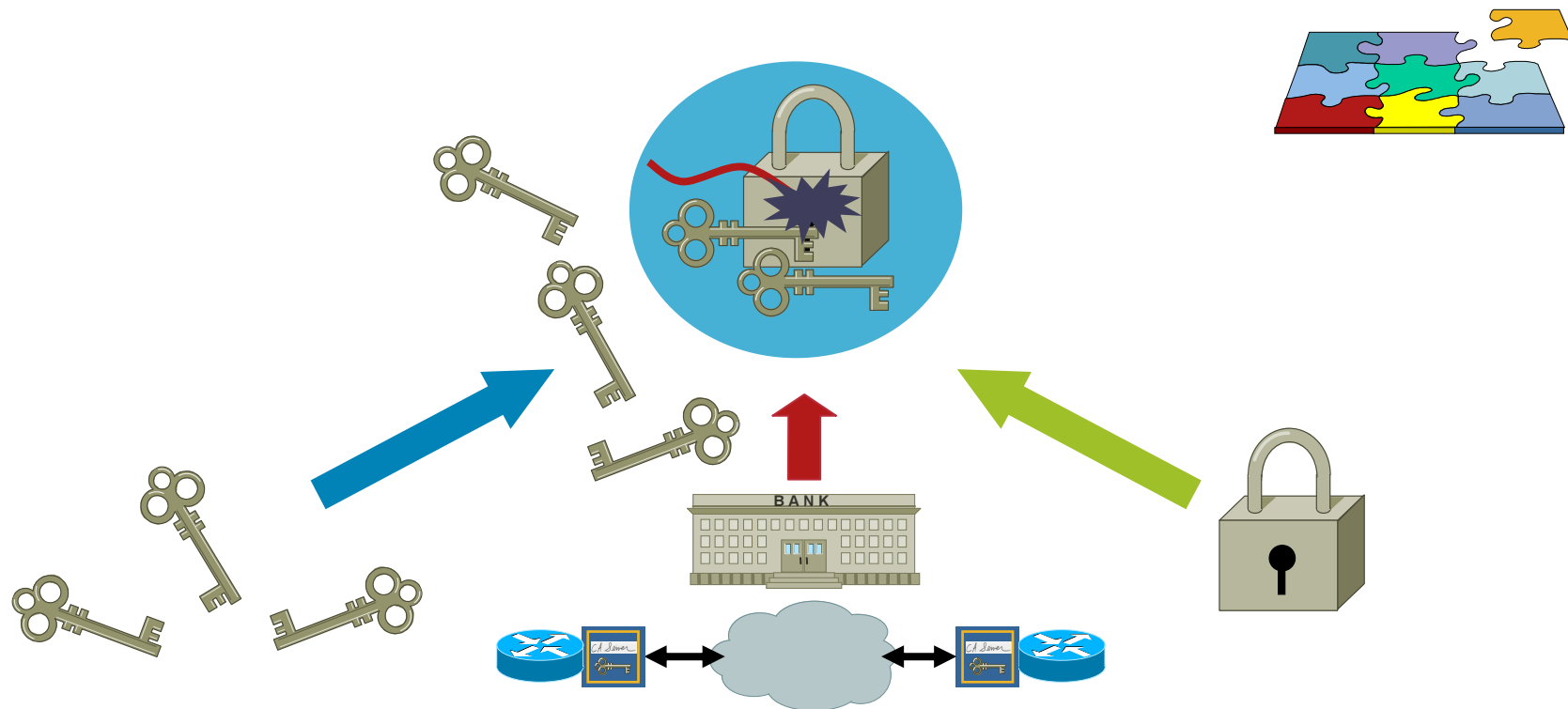


Dragan Novaković – Cisco Srbija
dnovakov@cisco.com

Agenda

1. Pregled VPN IPSec tehnologije
2. Konfiguracija ISAKMP/IKE Faza 1
3. Konfiguracija ISAKMP/IKE Faza 2
4. GRE
5. IPsec Profili
6. IPsec Virtual Tunnel Interfejsi
7. DMVPN
8. Group Encrypted Transport VPN

Pregled IPSec VPN



Tuneliranje

- IPSec
- GRE

Enkripcija

- DES
- 3DES
- AES

Autentikacija

- RSA digitalni sertifikati
- *Pre-shared* ključevi

Integritet

- HMAC-MD5
- HMAC-SHA-1

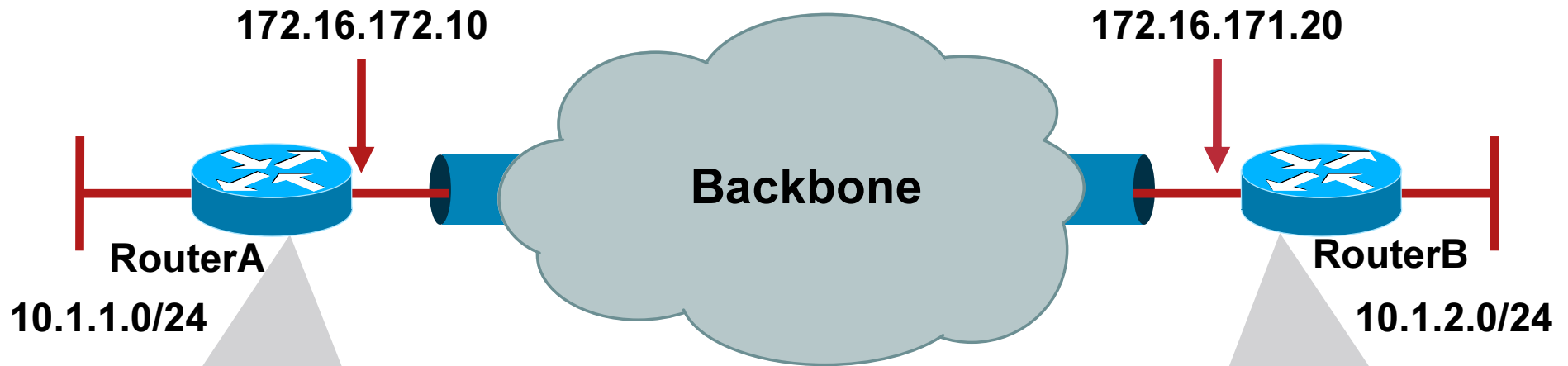
Agenda

1. Pregled VPN IPSec tehnologije
2. Konfiguracija ISAKMP/IKE Faza 1
3. Konfiguracija ISAKMP/IKE Faza 2
4. GRE
5. IPsec Profiles
6. IPsec Virtual Tunnel Interfaces
7. DMVPN
8. Group Encrypted Transport VPN

ISAKMP/IKE Faza 1

- Router(config)# [no] **crypto isakmp enable**
- Router(config)# **crypto isakmp policy** *priority*
- Router(config-isakmp)# **encryption** {*des* | *3des* | *aes*}
- Router(config-isakmp)# **hash** {*sha* | *md5*}
- Router(config-isakmp)# **authentication** {*rsa-sig* | *rsa-encr* | *pre-share*}
- Router(config-isakmp)# **group** {*1* | *2* | *5*}
- Router(config-isakmp)# **lifetime** *seconds*

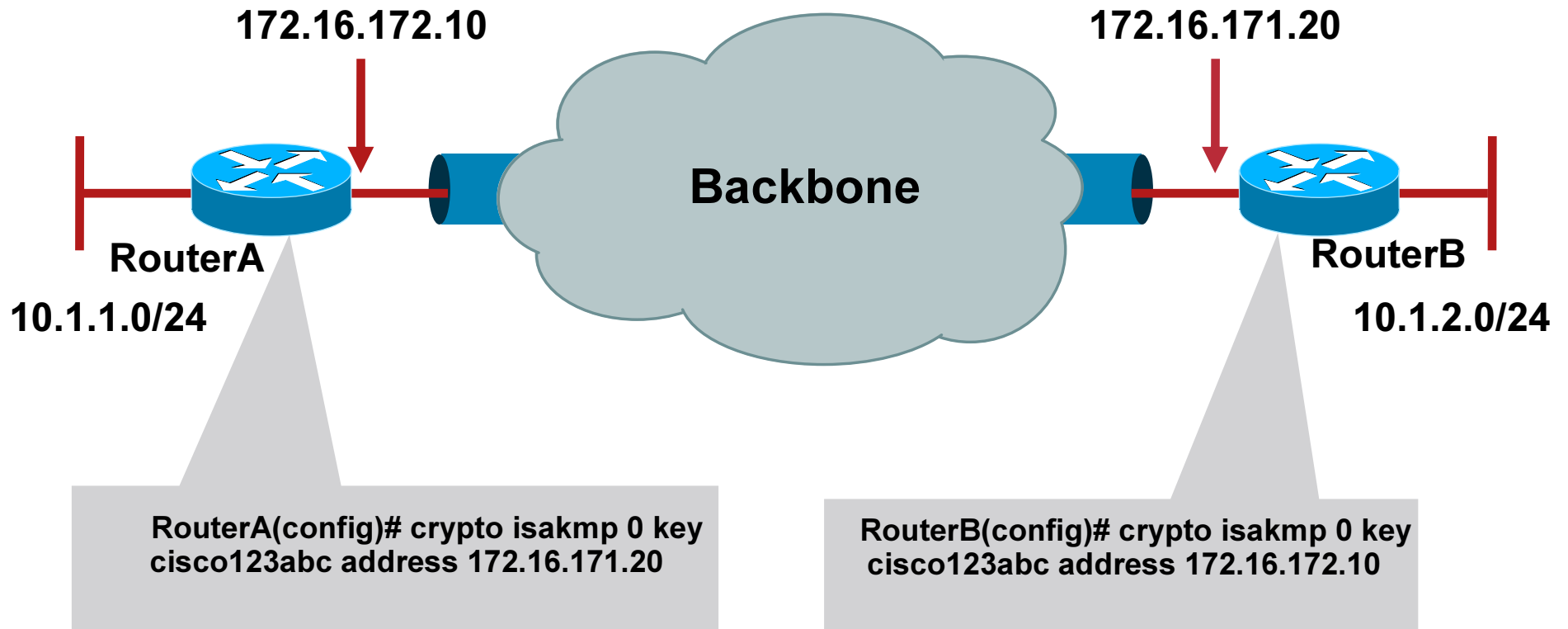
Konfiguracija ISAKMP/IKE Faza 1



```
RouterA(config)# crypto isakmp policy 1
RouterA(config-isakmp)# auth pre-share
RouterA(config-isakmp)# encryption 3des
RouterA(config-isakmp)# group 2
RouterA(config-isakmp)# lifetime 86400
RouterA(config)# crypto isakmp policy 2
RouterA(config-isakmp)# auth pre-share
RouterA(config-isakmp)# hash md5
```

```
RouterB(config)# crypto isakmp policy 1
RouterB(config-isakmp)# auth pre-share
RouterB(config-isakmp)# hash md5
RouterB(config)# crypto isakmp policy 2
RouterB(config-isakmp)# auth pre-share
RouterB(config-isakmp)# encryption 3des
RouterB(config-isakmp)# group 2
RouterB(config-isakmp)# lifetime 86400
```

Konfiguracija ISAKMP/IKE Faza 1



show crypto isakmp policy

```
Router# show crypto isakmp policy
```

```
Global IKE policy
```

```
Protection suite of priority 10
```

```
  encryption algorithm: AES - Advanced Encryption Standard  
                        (128 bit keys).
```

```
  hash algorithm:      Message Digest 5
```

```
  authentication method: Pre-Shared Key
```

```
  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
```

Agenda

1. Pregled VPN IPSec tehnologije
2. Konfiguracija ISAKMP/IKE Faza 1
3. Konfiguracija ISAKMP/IKE Faza 2
4. GRE
5. IPsec Profiles
6. IPsec Virtual Tunnel Interfaces
7. DMVPN
8. Group Encrypted Transport VPN

ISAKMP/IKE Faza 2

```
Router(config)# crypto map map_name seq_# ipsec-isakmp
```

```
Router(config-crypto-m)# match address ACL_name_or_#
```

```
Router(config-crypto-m)# set peer {hostname | IP_address}
```

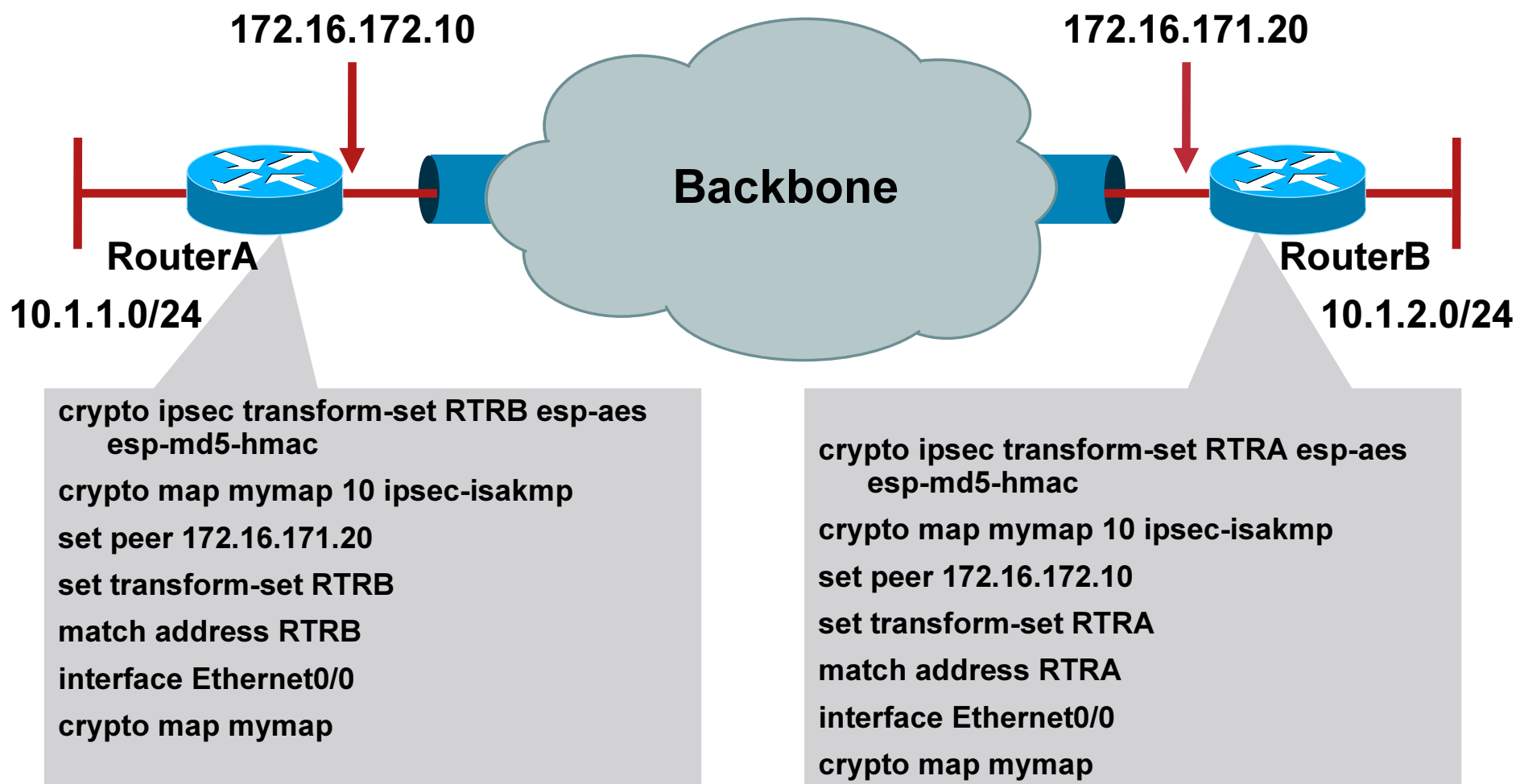
```
Router(config-crypto-m)# set transform-set transform_set_name1  
[transform-set-name2...transform-set-name6]
```

```
Router(config-crypto-m)# set pfs [group1 | group2 | group5]
```

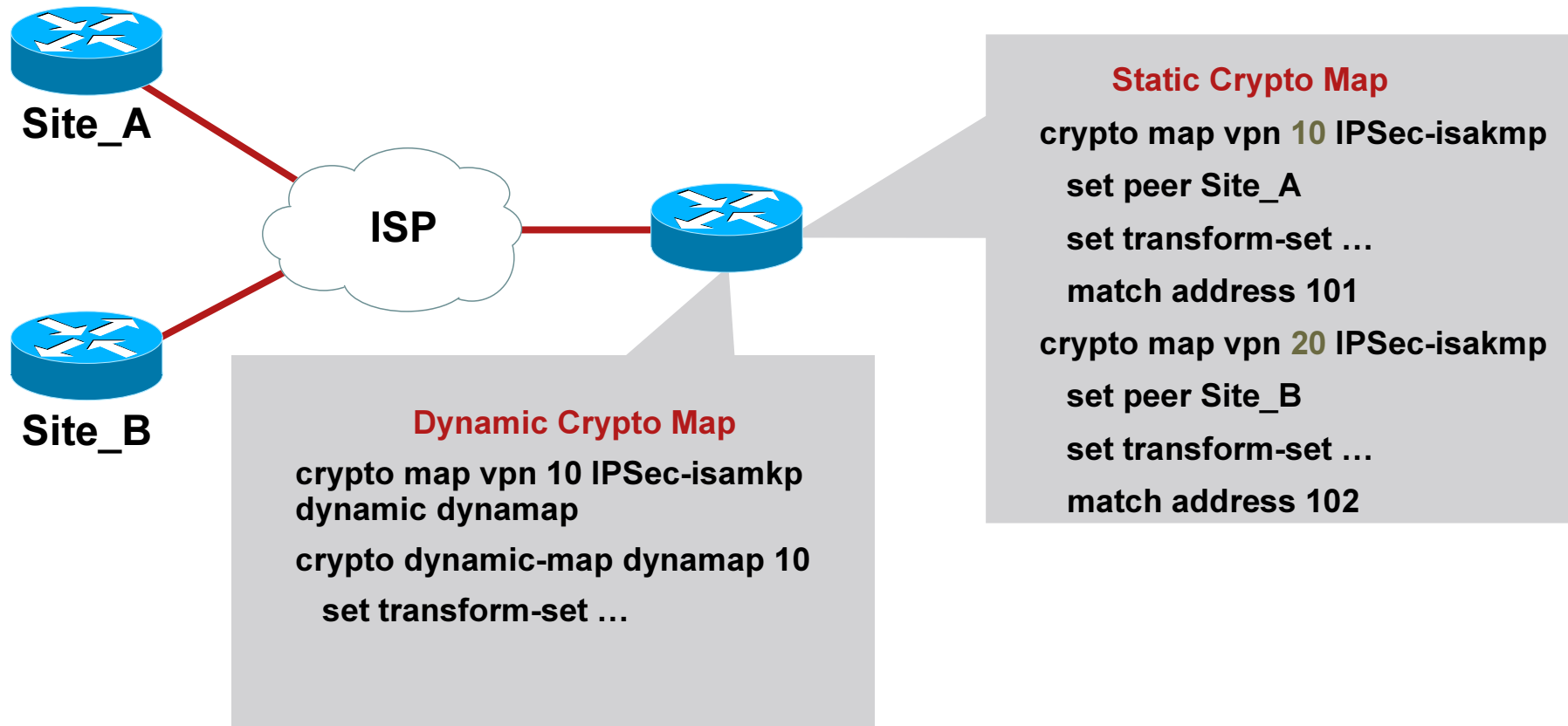
```
Router(config-crypto-m)# set security-association lifetime  
{seconds seconds | kilobytes kilobytes}
```

```
Router(config-crypto-m)# set security-association idle-time  
seconds
```

Statička kripto mapa



Static vs. Dynamic Crypto Map



Filtering/Access Control

IKE

UDP port 500

ESP, AH

IP protokol 50, 51

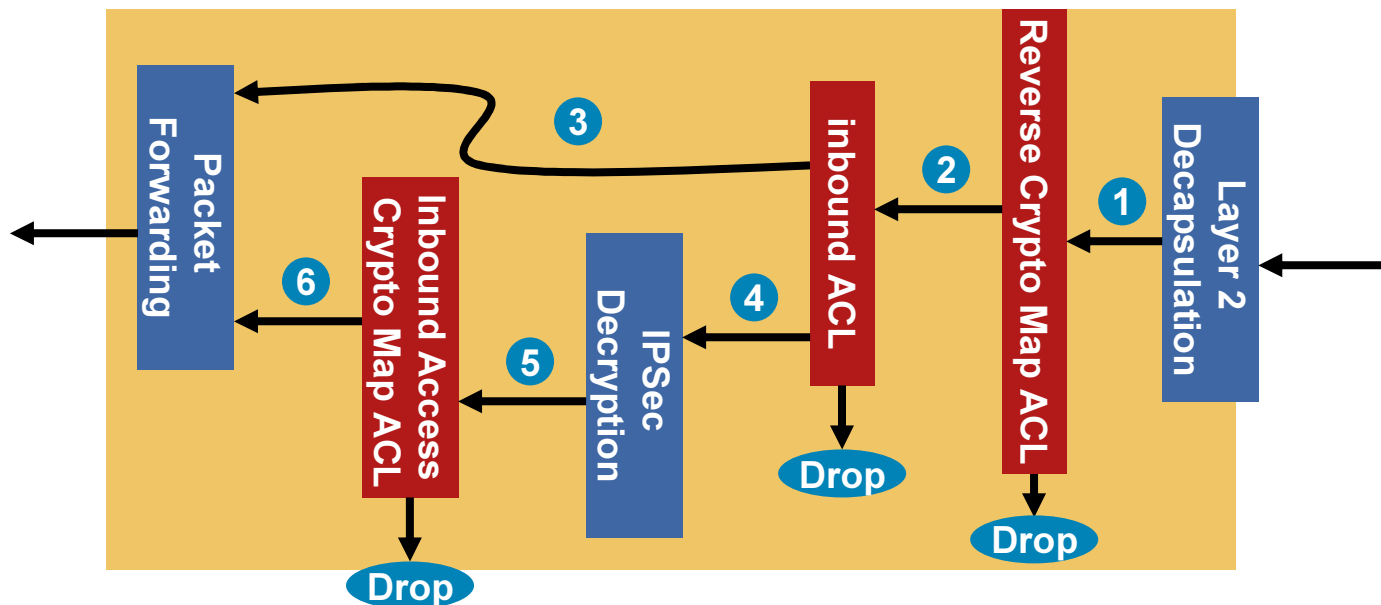
NAT-T

UDP port 4500

Filtriranje IPsec saobraćaja

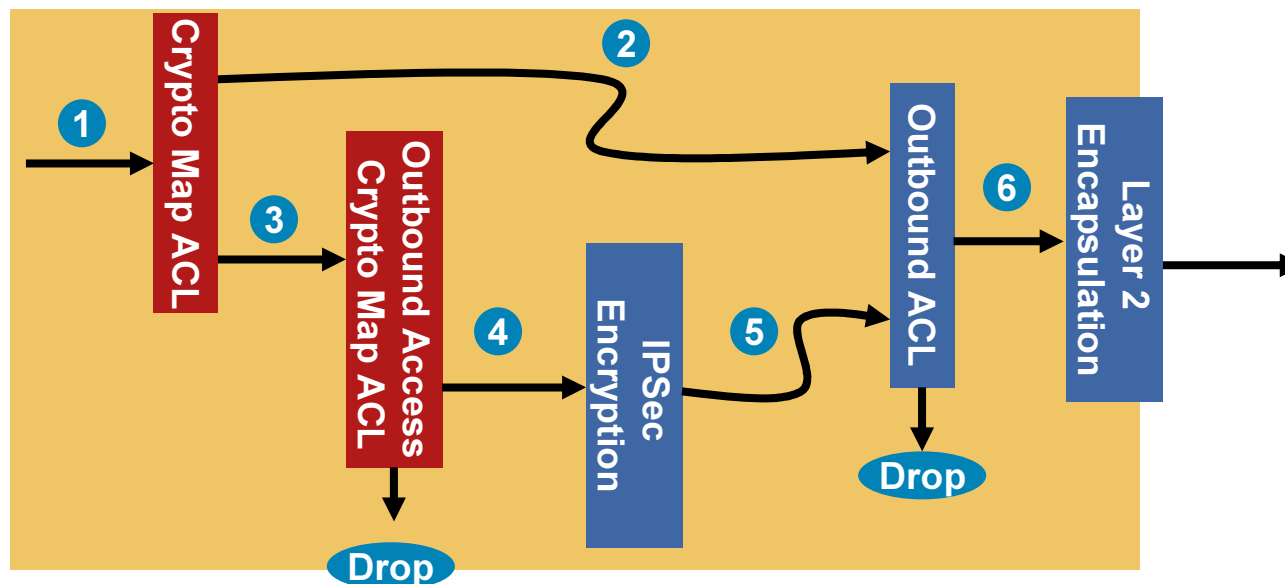
1. Router(config)# **crypto map** *map_name* *seq_#*
ipsec-isakmp
2. Router(config-crypto-map)# **set ip access-group**
{*ACL_#* | *ACL_name*} {**in** | **out**}

Tok ulaznog enkriptovanog paketa



1. IP paket se proverava u reverznoj crypto map ACL; ako paket treba da dođe enkriptovan, a nije, odbacuje se
2. IP paket se proverava u ulaznoj interfejs ACL;
3. Ako IP paket nije enkriptovan prosleđuje se dalje
4. Ako je IP paket enkriptovan deenkriptuje se
5. Deenkriptovan paket se proverava na opcionalnu ulaznu ACL u crypto mapi
6. Deenkriptovan IP paket se prosleđuje dalje

Tok izlaznog enkriptovanog paketa



1. Izlazni IP paketi se proveravaju u crypto map ACL, i markiraju za enkripciju
2. IP paketi koji nisu markirani za enkripciju se proveravaju u izlaznoj interfejs ACL
3. IP paketi koji su markirani za enkripciju se proveravaju u opcionalnoj crypto ACL
4. IP paket se enkriptuje
5. Enkriptovani IP paketi se proveravaju u izlaznoj interfejs ACL
6. IP paket se enkapsulira u Layer 2

Agenda

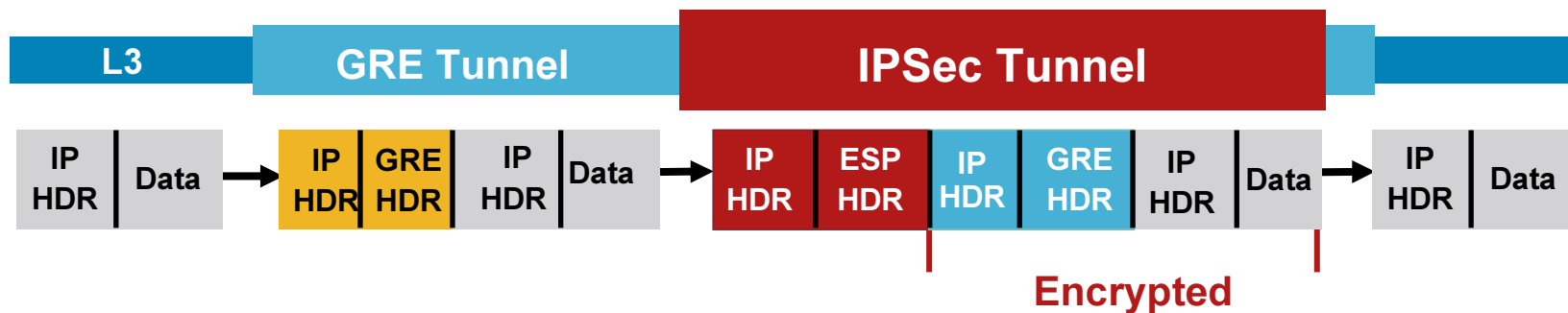
1. Pregled VPN IPSec tehnologije
2. Konfiguracija ISAKMP/IKE Faza 1
3. Konfiguracija ISAKMP/IKE Faza 2
4. **GRE**
5. IPsec Profiles
6. IPsec Virtual Tunnel Interfaces
7. DMVPN
8. Group Encrypted Transport VPN

Ne-Unicast saobraćaj

- Jedan od problema sa IPsec da on podržava samo unicast saobraćaj; multikast i broadcast paketi ne prolaze kroz data SA
- Inicijalno rešenje za ovakav problem je bila enkapsulacija multikast ili broadcast paketa u unicast paket, sa kojim IPsec može da radi.
- Generic Route Encapsulation (GRE) tuneliranje.

GRE tuneliranje

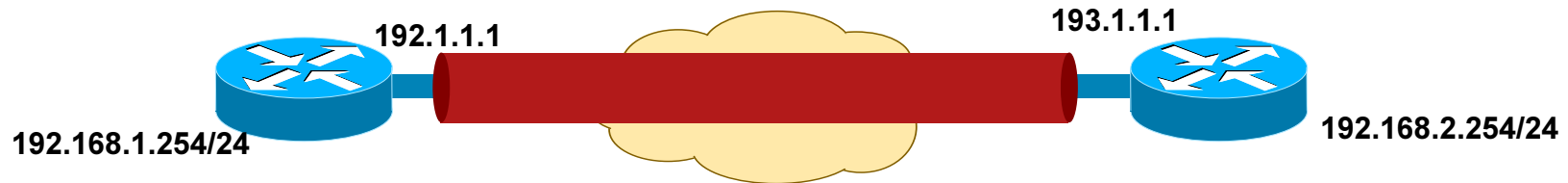
- GRE enkapsulira originalni paket u novi paket
- pravljenje tunel (virtual/logical) interfejsa.
- Tunel interfejs nije vezan ni za kakav fizički interfejs ili protokol već se samo koristi za potrebe enkapsulacije



GRE Tunnel konfiguracija

1. Router(config)# **interface tunnel** *port_#*
2. Router(config-if)# **tunnel source**
{*IP_address_on_router* | *interface_name_on_router*}
3. Router(config-if)# **tunnel destination**
{*IP_address_of_dst_router* | *name_of_dst_router*}
4. Router(config-if)# **keepalive** [*seconds* [*retries*]]
5. Router(config-if)# **tunnel mode** *mode*

Primer: GRE i OSPF



```
interface Tunnel0
ip address 192.168.3.1 255.255.255.0
tunnel source 192.1.1.1
tunnel destination 193.1.1.1
interface Ethernet0/1
ip address 192.168.1.254 255.255.255.0
interface Ethernet0/0
ip address 192.1.1.1 255.255.255.0
ip access-group perimeter in
router ospf 1
network 192.168.1.0 0.0.0.255 area 0
network 192.168.3.0 0.0.0.255 area 1
ip route 0.0.0.0 0.0.0.0 192.1.1.2
ip access-list extended perimeter
permit udp host 193.1.1.1 host 192.1.1.1 eq 500
permit esp host 193.1.1.1 host 192.1.1.1
permit gre host 193.1.1.1 host 192.1.1.1
deny ip any any
```

```
interface Tunnel0
ip address 192.168.3.2 255.255.255.0
tunnel source 193.1.1.1
tunnel destination 192.1.1.1
interface Ethernet0/1
ip address 192.168.2.254 255.255.255.0
interface Ethernet0/0
ip address 193.1.1.1 255.255.255.0
ip access-group perimeter in
router ospf 1
network 192.168.2.0 0.0.0.255 area 1
network 192.168.3.0 0.0.0.255 area 1
ip route 0.0.0.0 0.0.0.0 193.1.1.2
ip access-list extended perimeter
permit udp host 192.1.1.1 host 193.1.1.1 eq 500
permit esp host 192.1.1.1 host 193.1.1.1
permit gre host 192.1.1.1 host 193.1.1.1
deny ip any any
```

RTR B Routing Tabela

RTRB# show ip route

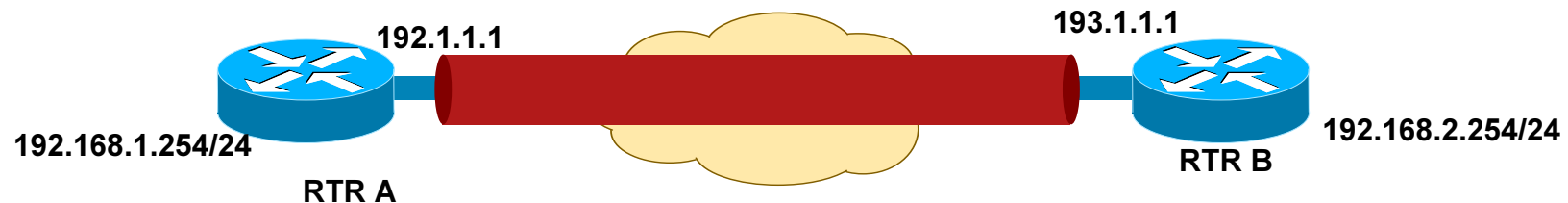
C 193.1.1.0/24 is directly connected, Ethernet0/0
192.168.1.0/32 is subnetted, 1 subnets

O IA 192.168.1.254 [110/11112] via 192.168.3.1,
00:04:53, Tunnel0

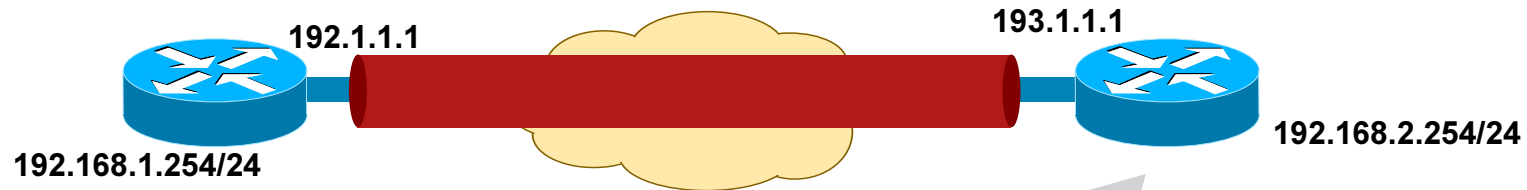
C 192.168.2.0/24 is directly connected, Ethernet0/1

C 192.168.3.0/24 is directly connected, Tunnel0

S* 0.0.0.0/0 [1/0] via 193.1.1.2



GRE over IPsec konfiguracija



```
crypto isakmp policy 10
encryption aes 128
hash sha
authentication pre-share
group 2
crypto isakmp key cisco123 address 193.1.1.1 no-
xauth
ip access-list extended cryptoACL
permit gre host 192.1.1.1 host 193.1.1.1
crypto ipsec transform-set RTRtran esp-aes esp-
sha-hmac
mode transport
crypto map mymap 10 ipsec-isakmp
set peer 193.1.1.1
set transform-set RTRtran
match address cryptoACL
interface Ethernet0/0
crypto map mymap
ip access-list extended perimeter
! Ako je IOS 12.3(8)T i noviji
no permit gre host 193.1.1.1 host 192.1.1.1
```

```
crypto isakmp policy 10
encryption aes 128
hash sha
authentication pre-share
group 2
crypto isakmp key cisco123 address 192.1.1.1 no-
xauth
ip access-list extended cryptoACL
permit gre host 193.1.1.1 host 192.1.1.1
crypto ipsec transform-set RTRtran esp-aes esp-
sha-hmac
mode transport
crypto map mymap 10 ipsec-isakmp
set peer 192.1.1.1
set transform-set RTRtran
match address cryptoACL
interface Ethernet0/0
crypto map mymap
ip access-list extended perimeter
no permit gre host 192.1.1.1 host 193.1.1.1
```

GRE over IPSec Evolucija konfiguracije

- Pre 12.2(13)T, crypto mape su se primenjivale i na GRE tunel interfejs i na fizički interfejs
- Od 12.2(13)T
 - crypto map se primenjuje na fizičkom interfejsu ili
 - **tunnel protection IPSec profile** na tunel interfejsu

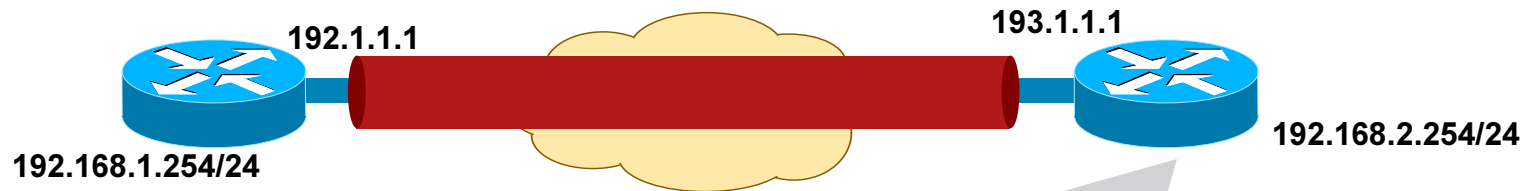
Agenda

1. Pregled VPN IPSec tehnologije
2. Konfiguracija ISAKMP/IKE Faza 1
3. Konfiguracija ISAKMP/IKE Faza 2
4. GRE
5. **IPsec Profili**
6. IPsec Virtual Tunnel Interfaces
7. DMVPN
8. Group Encrypted Transport VPN

IPsec Profili

- IPsec profili, predstavljeni sa IOS 12.2(13)T, apstrakuju informacije iz kripto mapa
- Profil se onda poziva u kripto mapi ili na tunel interfejsima
- Profil može da sadrži transform setove, PFS grupe, identity tipove i *lifetime SA*.
- U slučaju kada remote peer-ovi imaju slične parametre konekcija, profili čine konfiguraciju daleko jednostavnijom.

GRE over IPSec konfiguracija

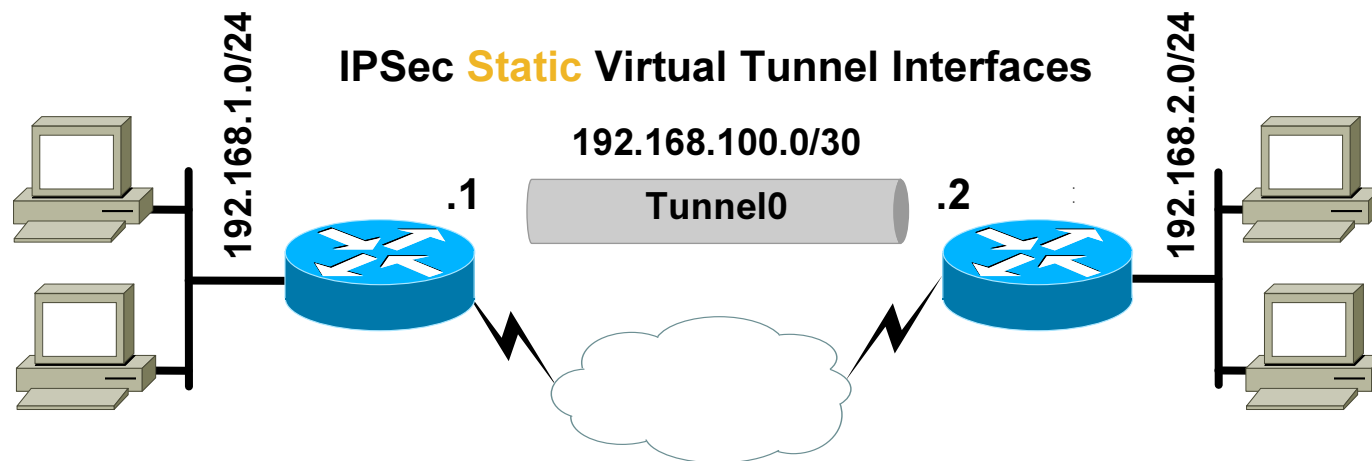


```
crypto isakmp policy 1
  authentication pre-share
crypto isakmp key cisco47 address 193.1.1.1
!
crypto ipsec transform-set trans2 esp-3des esp-md5-hmac
!
crypto map vpnmap2 local-address Ethernet1
crypto map vpnmap2 10 IPSec-isakmp
  set peer 193.1.1.1
  set transform-set trans2
  match address 110
interface Ethernet1
  ip address 192.1.1.1 255.255.255.0
  crypto map vpnmap2
interface Tunnel0
  ip address 192.168.3.1 255.255.255.0
  ip mtu 1400
  tunnel source Ethernet1
  tunnel destination 193.1.1.1
*****crypto map vpnmap2*****
ip route 0.0.0.0 0.0.0.0 172.16.175.1
!
access-list 110 permit gre host 192.1.1.1 host 193.1.1.1
```

12.2(13)T i noviji IOSi

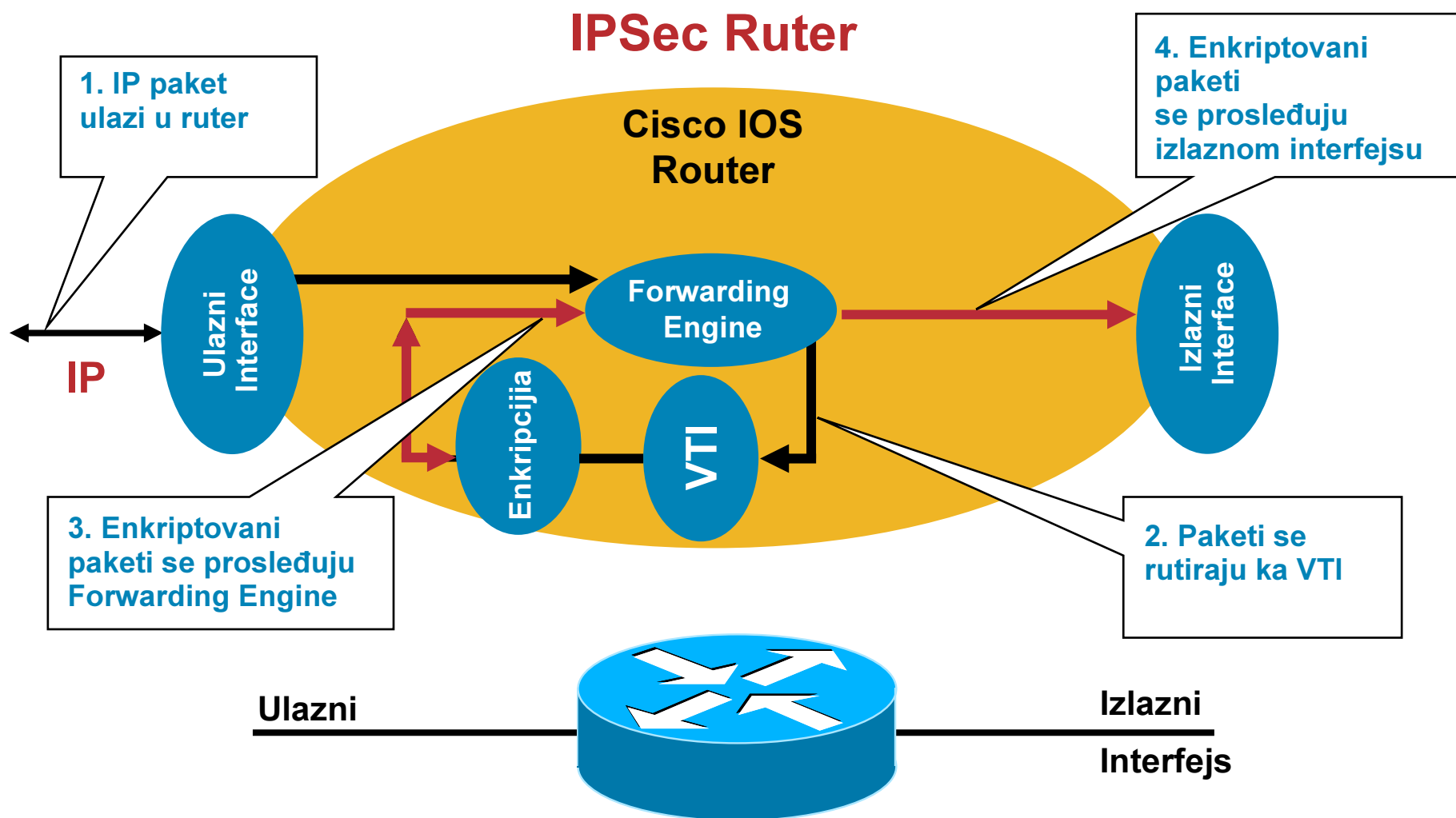
```
crypto isakmp policy 1
  authentication pre-share
crypto isakmp key cisco47 address 172.16.175.75
!
crypto ipsec transform-set trans2 esp-3des esp-md5-hmac
crypto ipsec profile vpnprof
  set transform-set trans2
!
interface Ethernet1
  ip address 193.1.1.1 255.255.255.0
interface Tunnel0
  ip address 192.168.3.2 255.255.255.0
  ip mtu 1400
  tunnel source Ethernet1
  tunnel destination 192.1.1.1
  tunnel protection ipsec profile vpnprof
ip route 0.0.0.0 0.0.0.0 193.1.1.2
```

Virtual Tunnel Interface

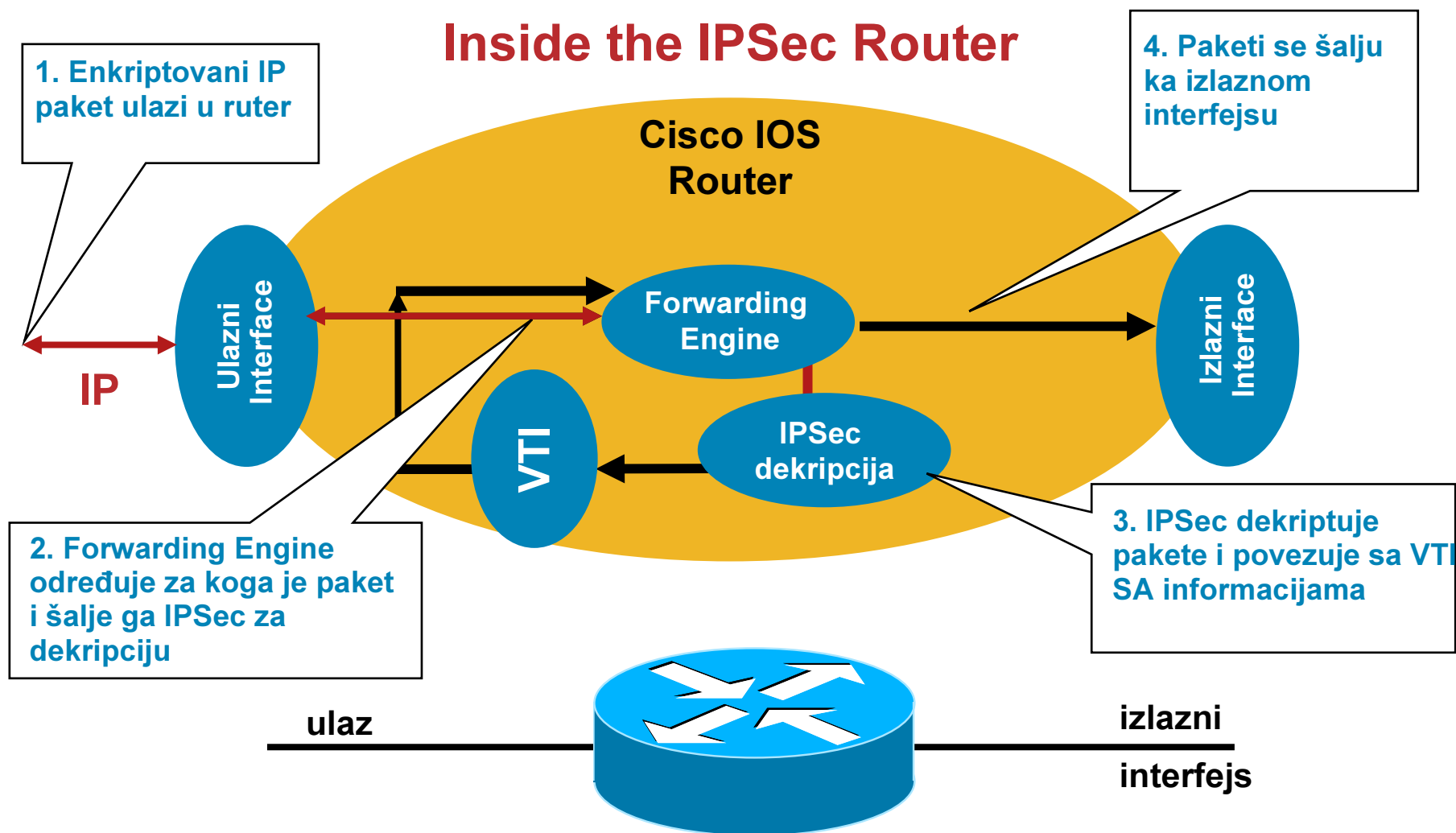


1. Koncept predstavljen u IOS 12.3(14)T – pojednostavljuje VPN konfiguraciju eliminišući crypto mape, access control liste, i GRE
2. Jednostavniji VPN dizajn:
1:1 odnos između tunela i sajtova
3. Skalabilniji od GRE
4. VTI podržava Quality of Service (QoS), multicast, i druge ruting f-je
5. Poboljšana VPN interoperabilnost

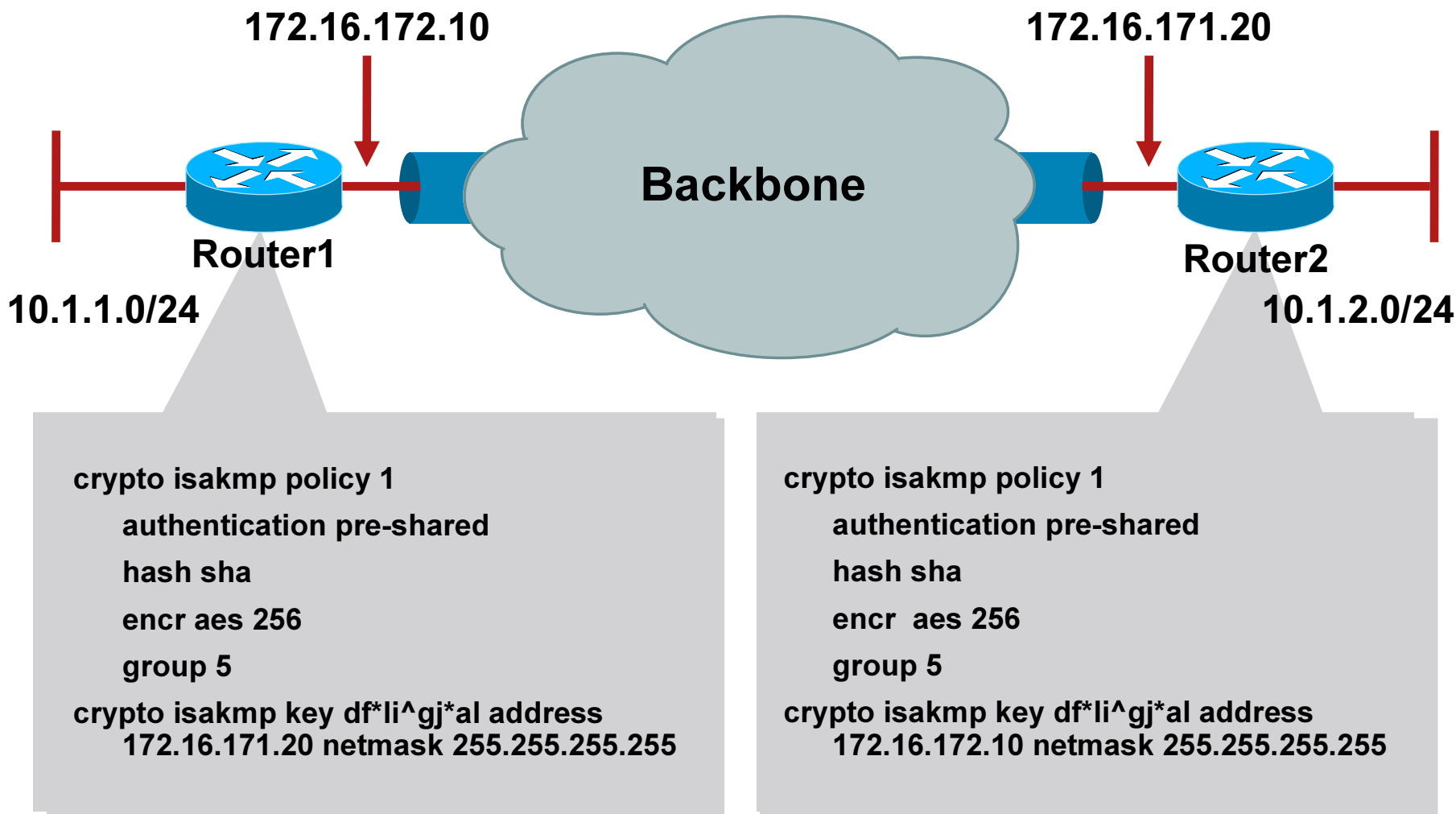
Tok izlaznog paketa



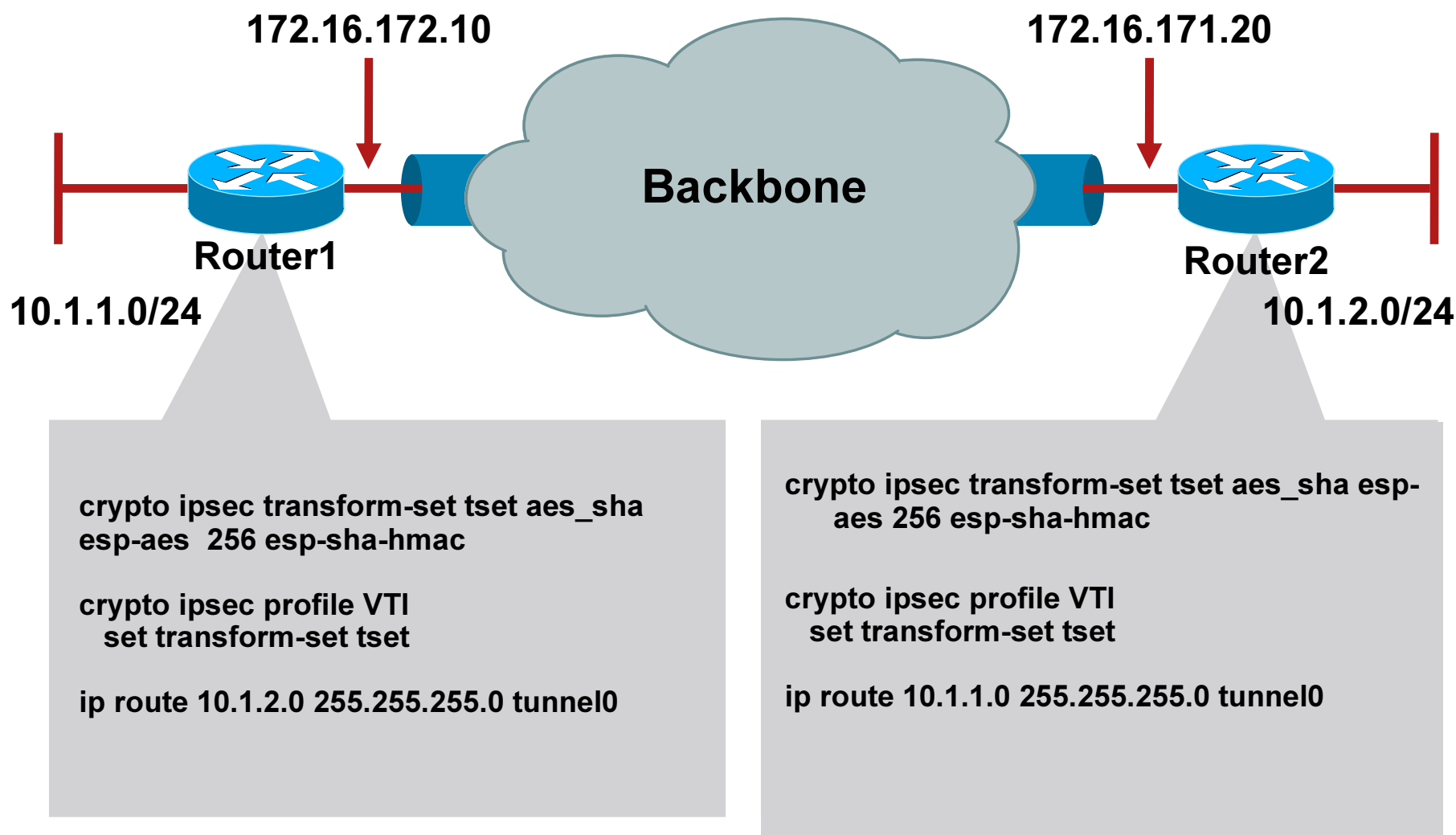
Tok ulaznog paketa



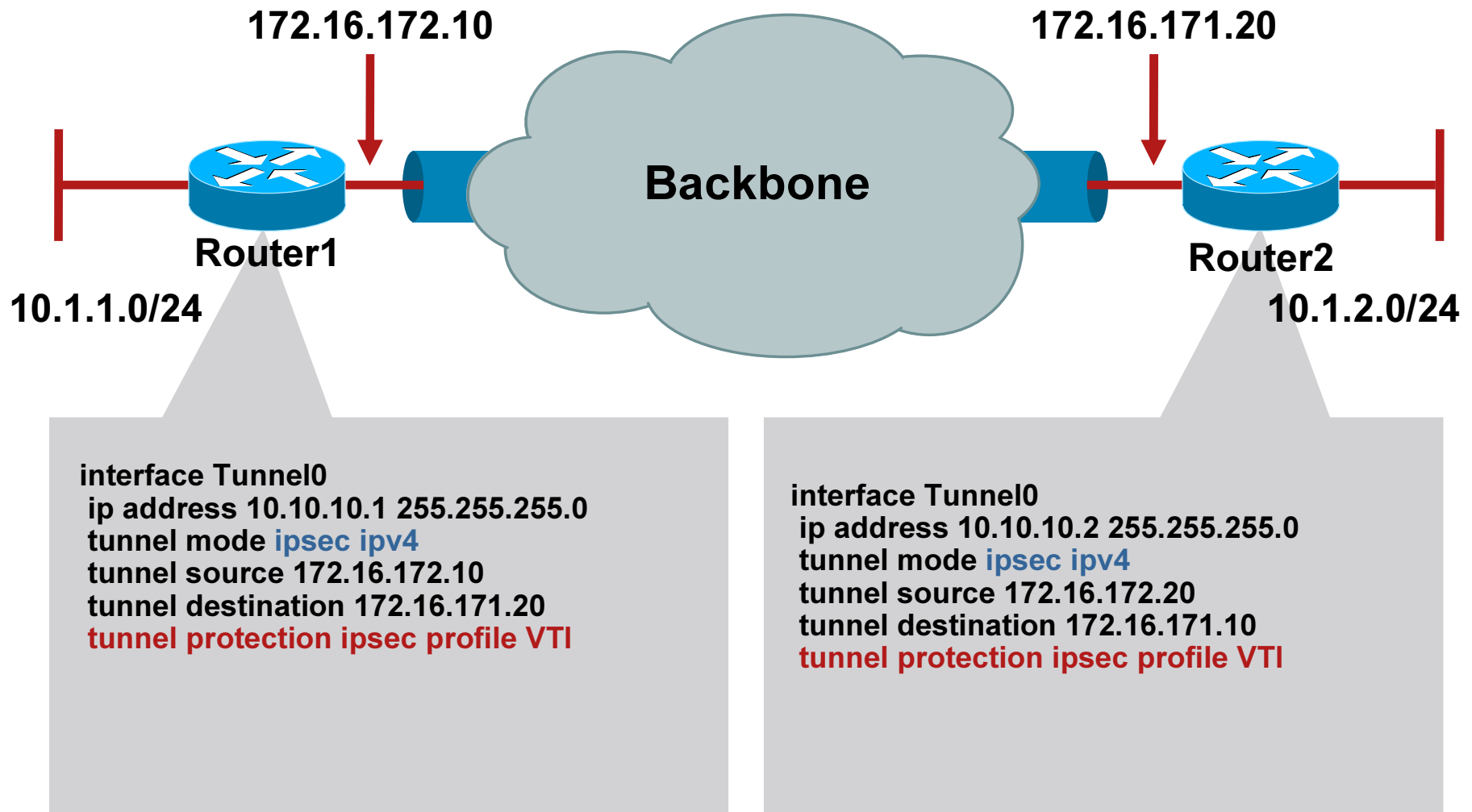
VTI konfiguracija: IKE (Faza 1)



IPSec (Faza 2)



Apply VPN Configuration



Agenda

1. Pregled VPN IPSec tehnologije
2. Konfiguracija ISAKMP/IKE Faza 1
3. Konfiguracija ISAKMP/IKE Faza 2
4. GRE
5. IPsec Profiles
6. IPsec Virtual Tunnel Interfaces
7. **DMVPN**
8. Group Encrypted Transport VPN

Šta je Dynamic Multipoint VPN ?

1. DMVPN je Cisco IOS software rešenje za pravljenje IPsec+GRE VPNova na jednostavan, dinamički i skalabilan način

2. Oslanja se na dve tehnologije

Next Hop Resolution Protocol (NHRP)

Pravi distribuiranu bazu koja mapira VPN
(tunnel interface) u realnu (public interface) adresu

Multipoint GRE Tunnel Interface

GRE interface koji podržava multiple
GRE/IPsec tunele i krajnje uređaje

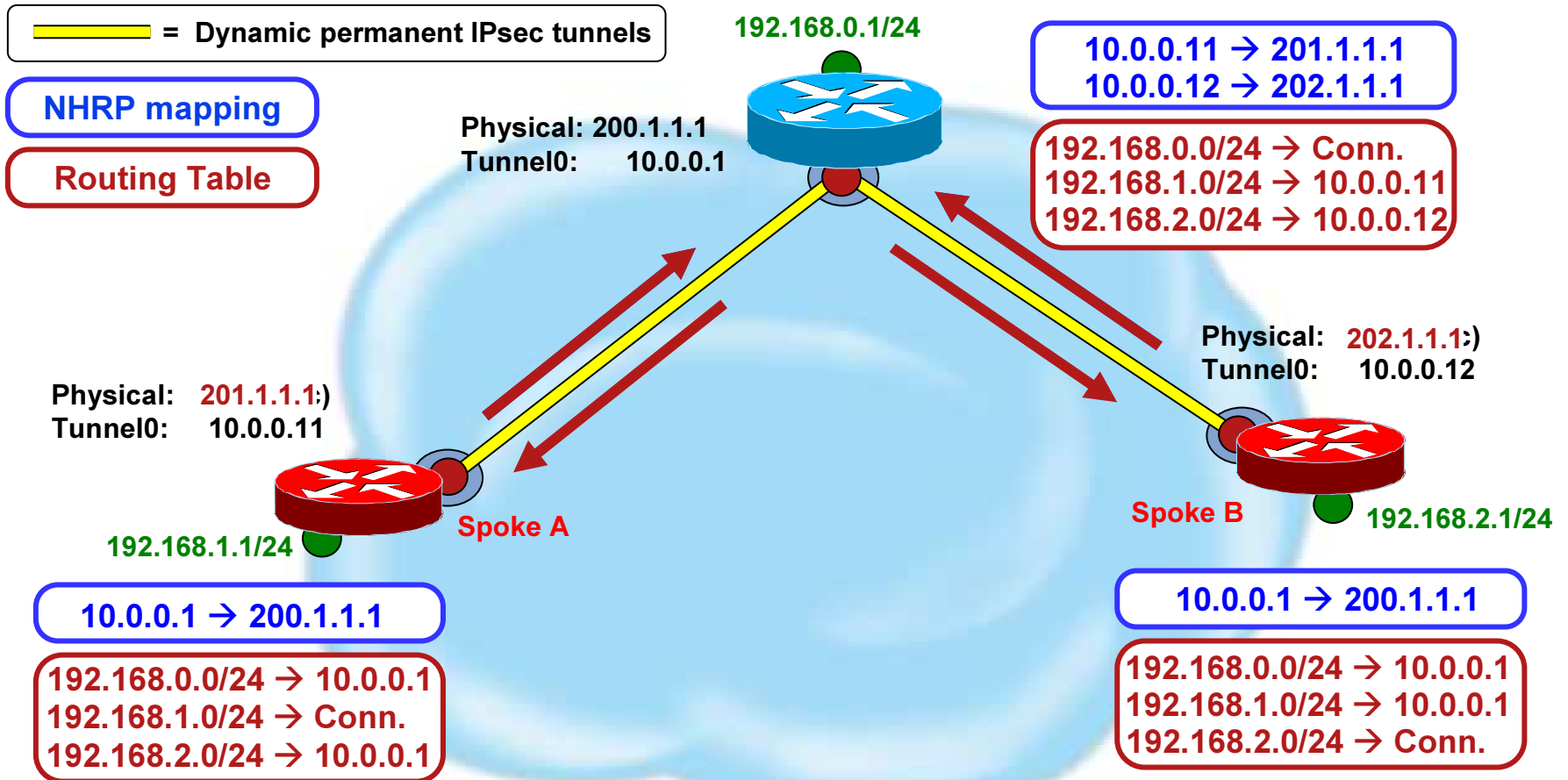
Smanjuje veličinu i kompleksnost konfiguracije

Podržava dinamičko kreiranje tunela

DMVPN – način rada

- Spoke ruter pravi dinamički permanentni GRE/IPsec tunel ka hubu, ali ne i ka drugim spoke ruterima. Oni se registruju kao klijenti na NHRP serveru (hub).
- Kad spoke želi da pošalje paket ka mreži iza nekog drugog spoke rutera , on traži preko NHRP pravu (outside) adresu destinacionog uređaja
- Sada spoke može da inicira dinamički GRE/IPsec tunel ka odredišnom spoke ruteru.
- Dinamički spoke-to-spoke tunel se prave preko mGRE interfejsa.
- Po razmeni saobraćaja spoke-to-spoke tunel se briše

Primer:NHRP Registracija



Konfiguracija HUB rutera pre DMVPN

```
hub(config)# crypto isakmp policy 1
hub(config-isakmp)# authentication pre-share
hub(config-isakmp)# encryption aes
hub(config-isakmp)# exit
hub(config)# crypto isakmp key cisco123 address
    0.0.0.0 0.0.0.0
        no-xauth
hub(config)# access-list 101 permit gre host 200.1.1.1
        host 201.1.1.1
hub(config)# access-list <x+100> permit gre host
    200.1.1.1
        host <200+x>.1.1.1
hub(config)# crypto ipsec transform-set trans2 esp-aes
    esp-sha-hmac
hub(cfg-crypto-trans)# mode transport
hub(config)# crypto map mymap local-address
    Ethernet0
hub(config)# crypto map mymap 10 ipsec-isakmp
hub(config-crypto-map)# set peer 201.1.1.1
hub(config-crypto-map)# set transform-set trans2
hub(config-crypto-map)# match address 101
hub(config)# crypto map mymap <x*10> ipsec-isakmp
hub(config-crypto-map)# set peer <200+x>.1.1.1
hub(config-crypto-map)# set transform-set trans2
hub(config-crypto-map)# match address <x+100>
```

```
hub(config)# interface Tunnel1
hub(config-if)# description Connection to Spoke1
hub(config-if)# bandwidth 1000
hub(config-if)# ip address 10.0.0.1 255.255.255.252
hub(config-if)# ip mtu 1440
hub(config-if)# delay 1000
hub(config-if)# tunnel source Ethernet0
hub(config-if)# tunnel destination 201.1.1.1
hub(config)# interface Tunnel<x>
hub(config-if)# description Connection to SpokeX
hub(config-if)# bandwidth 1000
hub(config-if)# ip address 10.0.0.<4*x-1> 255.255.255.252
hub(config-if)# ip mtu 1440
hub(config-if)# delay 1000
hub(config-if)# tunnel source Ethernet0
hub(config-if)# tunnel destination <200+x>.1.1.1
hub(config)# interface Ethernet0
hub(config-if)# description Internet Connection
hub(config-if)# ip address 200.1.1.1 255.255.255.0
hub(config-if)# crypto map mymap
hub(config)# interface Ethernet1
hub(config-if)# description Local LAN
hub(config-if)# ip address 192.168.0.1 255.255.255.0
hub(config)# router ospf 1
hub(config-router)# network 10.0.0.0 0.0.0.255 area 1
hub(config-router)# network 192.168.0.0 0.0.0.255 area 0
```

DMVPN Hub Konfiguracija

```
hub(config)# crypto ipsec profile profile_name
```

```
hub(ipsec-profile)# set transform-set  
transform_set_name
```

```
hub(config)# interface tunnel tunnel_#
```

```
hub(config-if)# tunnel mode gre multipoint
```

```
hub(config-if)# tunnel key key_#
```

```
hub(config-if)# tunnel protection ipsec profile  
profile_name
```

```
hub(config-if)# ip nhrp network-id network_identifier
```

```
hub(config-if)# ip nhrp authentication string
```

```
hub(config-if)# ip nhrp map multicast dynamic
```

```
hub(config-if)# ip nhrp holdtime seconds
```

DMVPN Spoke Konfiguracija

```
spoke(config)# crypto ipsec profile profile_name
spoke(ipsec-profile)# set transform-set transform_set_name
spoke(config)# interface tunnel tunnel_#
spoke(config-if)# tunnel mode gre multipoint
spoke(config-if)# tunnel key key_#
spoke(config-if)# tunnel protection ipsec profile profile_name
spoke(config-if)# ip nhrp network-id network_identifier
spoke(config-if)# ip nhrp authentication string
spoke(config-if)# ip nhrp map hub_GRE_IP_address
                        hub_external_interface_IP_address
spoke(config-if)# ip nhrp map multicast
                        hub_external_interface_IP_address
spoke(config-if)# ip nhrp nhs hub_GRE_IP_address
spoke(config-if)# ip nhrp holdtime seconds
```

DMVPN Routing Konfiguracija

- EIGRP:
 - hub(config)# interface tunnel tunnel_#
 - hub(config-if)# no ip split-horizon eigrp AS_#
 - hub(config-if)# no ip next-hop-self eigrp AS_#
- OSPF:
 - hub(config) interface tunnel tunnel_#
 - hub(config-if)# ip ospf network broadcast
 - hub(config-if)# ip ospf priority #_>_1

DMVPN Hub Konfiguracija

```
hub(config)# crypto isakmp policy 1
hub(config-isakmp)# authentication pre-share
hub(config-isakmp)# encryption aes
hub(config)# crypto isakmp key cisco123 address
0.0.0.0 0.0.0.0 no-xauth
hub(config)# crypto isakmp keepalive 20 3
hub(config)# crypto ipsec transform-set trans2 esp-
aes esp-sha-hmac
hub(cfg-crypto-trans)# mode transport
hub(cfg-crypto-trans)# exit
hub(config)# crypto ipsec profile dmvpnprofile
hub(ipsec-profile)# set transform-set trans2
hub(config)# interface tunnel0
hub(config-if)# description Connection to Spokes
hub(config-if)# bandwidth 1000
hub(config-if)# ip address 10.0.0.1 255.255.255.0
hub(config-if)# ip mtu 1436
hub(config-if)# delay 1000
```

```
hub(config-if)# ip ospf network broadcast
hub(config-if)# ip ospf priority 2
hub(config-if)# ip nhrp authentication cisco123
hub(config-if)# ip nhrp map multicast dynamic
hub(config-if)# ip nhrp network-id 100000
hub(config-if)# ip nhrp holdtime 600
hub(config-if)# tunnel source Ethernet0
hub(config-if)# tunnel mode gre multipoint
hub(config-if)# tunnel key 100000
hub(config-if)# tunnel protection ipsec profile dmvpnprofile
hub(config)# interface Ethernet0
hub(config-if)# description Internet Connection
hub(config-if)# ip address 200.1.1.1 255.255.255.0
hub(config)# interface Ethernet1
hub(config-if)# description Local LAN
hub(config-if)# ip address 192.168.0.1 255.255.255.0
hub(config)# router ospf 1
hub(config-router)# network 10.0.0.0 0.0.0.255 area 1
hub(config-router)# network 192.168.0.0 0.0.0.255 area 0
```

DMVPN Spoke Konfiguracija

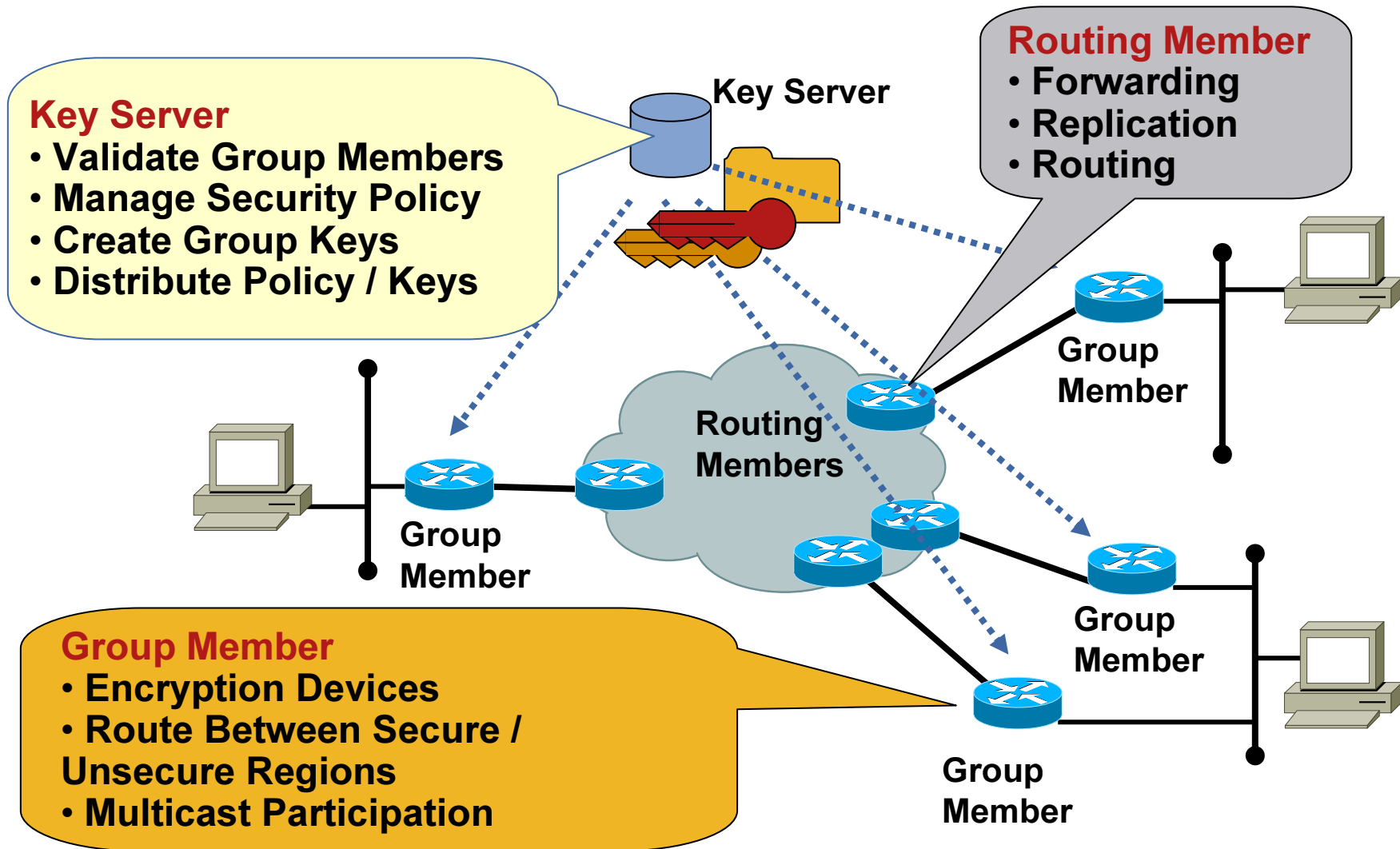
```
spokeX(config)# crypto isakmp policy 1
spokeX(config-isakmp)# authentication pre-share
spokeX(config-isakmp)# encryption aes
spokeX(config)# crypto isakmp key cisco123
address
    0.0.0.0 0.0.0.0 no-xauth
spokeX(config)# crypto isakmp keepalive 20 3
spokeX(config)# crypto ipsec transform-set trans2
esp-aes
    esp-sha-hmac
spokeX(cfg-crypto-trans)# mode transport
spokeX(cfg-crypto-trans)# exit
spokeX(config)# crypto ipsec profile dmvpnprofile
spokeX(ipsec-profile)# set transform-set trans2
spokeX(config)# interface tunnel0
spokeX(config-if)# description Connection to hub
spokeX(config-if)# bandwidth 1000
spokeX(config-if)# ip address 10.0.0.<x+1>
    255.255.255.0
spokeX(config-if)# ip mtu 1436
spokeX(config-if)# delay 1000
```

```
spokeX(config-if)# ip ospf network broadcast
spokeX(config-if)# ip ospf priority 0
spokeX(config-if)# ip nhrp authentication cisco123
spokeX(config-if)# ip nhrp map multicast 200.1.1.1
spokeX(config-if)# ip nhrp map 10.0.0.1 200.1.1.1
spokeX(config-if)# ip nhrp nhs 10.0.0.1
spokeX(config-if)# ip nhrp network-id 100000
spokeX(config-if)# ip nhrp holdtime 300
spokeX(config-if)# tunnel source Ethernet0
spokeX(config-if)# tunnel mode gre multipoint
spokeX(config-if)# tunnel key 100000
spokeX(config-if)# tunnel protection ipsec profile dmvpnprofile
spokeX(config)# interface Ethernet0
spokeX(config-if)# description Connection to Internet
spokeX(config-if)# ip address dhcp hostname Spoke<x>
spokeX(config)# interface Ethernet1
spokeX(config-if)# description Local LAN
spokeX(config-if)# ip address 192.168.<x>.1 255.255.255.0
spokeX(config)# router ospf 1
spokeX(config-router)# network 10.0.0.0 0.0.0.255 area 1
spokeX(config-router)# network 192.168.<n>.0 0.0.0.255 area 1
```

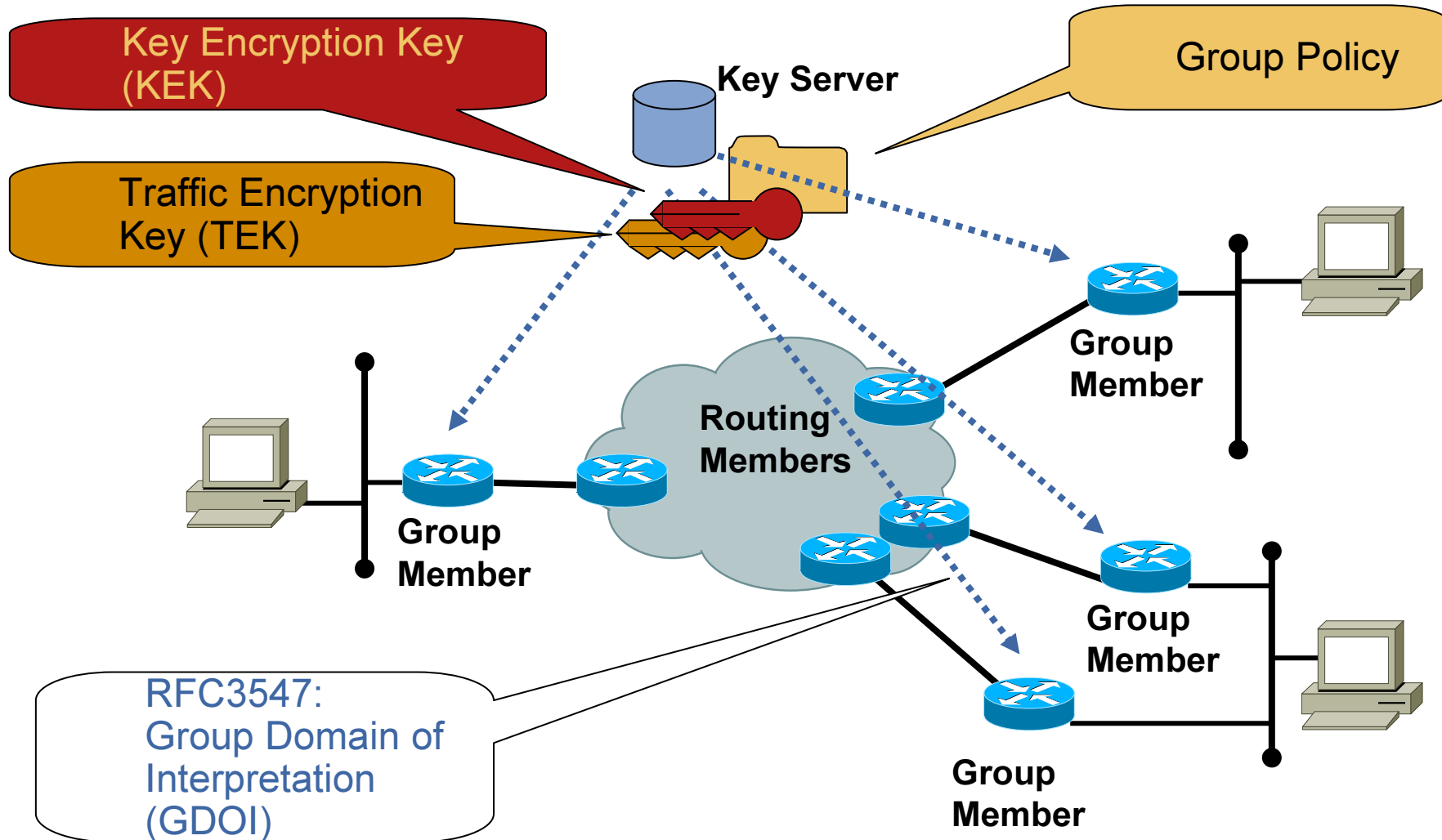
Agenda

1. Pregled VPN IPSec tehnologije
2. Konfiguracija ISAKMP/IKE Faza 1
3. Konfiguracija ISAKMP/IKE Faza 2
4. GRE
5. IPsec Profiles
6. IPsec Virtual Tunnel Interfaces
7. DMVPN
8. **Group Encrypted Transport VPN**

Group Security Functions



Group Security Elements

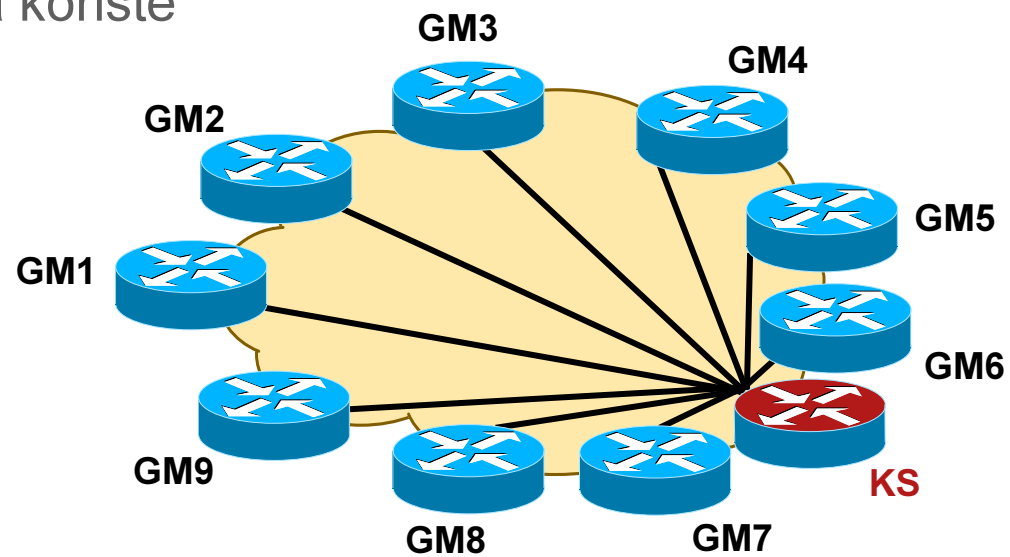


Group Security Association

- Članovi grupe dele zajednički SA
 - SA nije specifičan za pojedine članove već
 - SA važi za sve članove grupe
- VPN gw rade zajedno na zaštiti saobraćaja
 - VPN gw imaju isti status
 - Saobraćaj se razmenjuje između bilo kog VPN gw

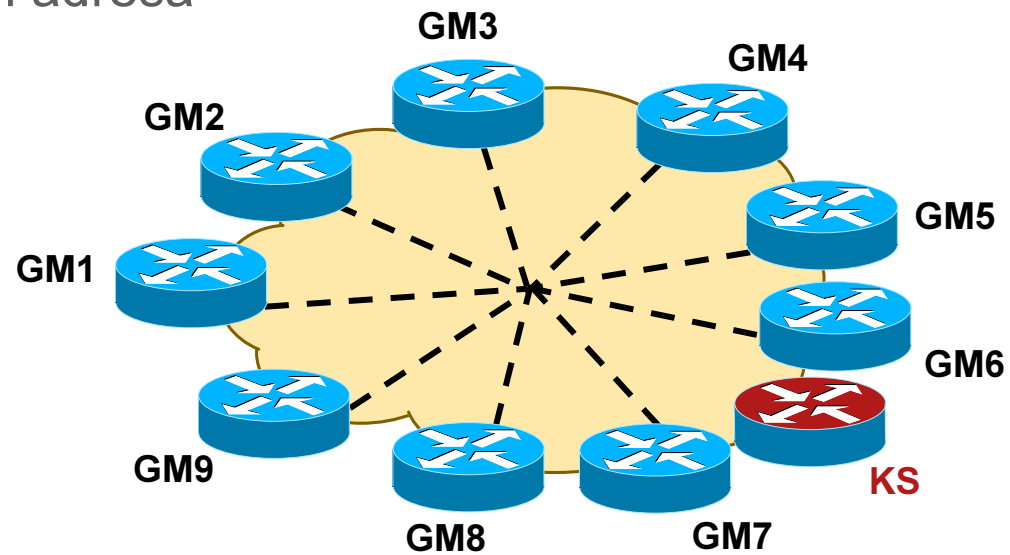
Osnovna GET VPN arhitektura

- korak 1: članovi grupe (GM) se “registruju” putem GDOI na Key Serveru (KS)
 - KS autentikuje & autorizuje GM
 - KS vraća skup IPsec SA koje GM treba da koriste



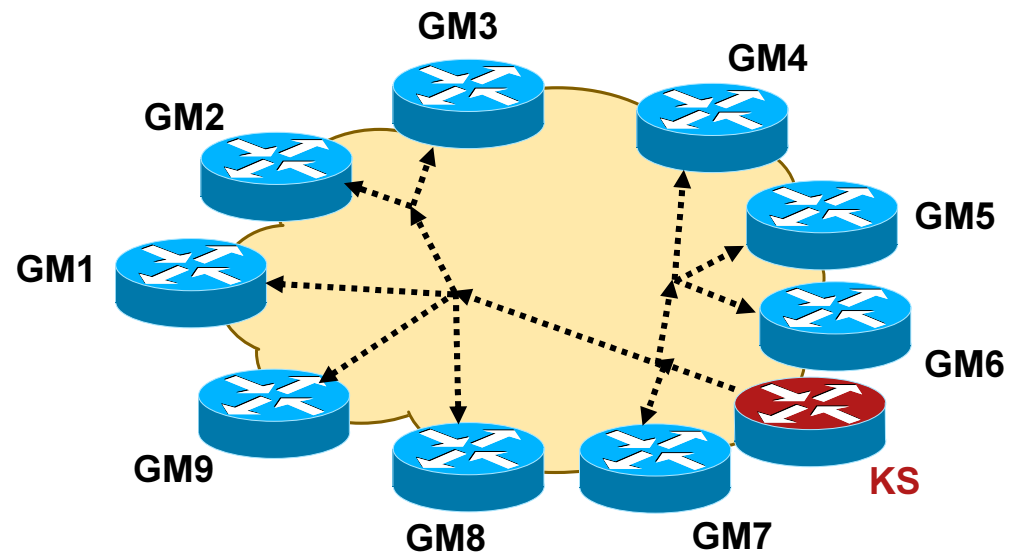
Osnovna GET VPN arhitektura

- korak 2: Data Plane enkripcija
 - GM razmenjuju enkriptovan saobraćaj koristeći grupne ključeve
 - Koristi se IPSec Tunnel Mode sa “prezervacijom adresa”



Osnovna GET VPN arhitektura

- korak 3: Periodični Rekey proces
 - KS šalje novi IPsec ključ pre no što važeći IPsec ključ istekne.



Key Server

Key Server konfiguracija

```
crypto gdoi group secure-wan
  identity number 3333          <- GROUPED
  server local                  <- KEY SERVER
  rekey address ipv4 102        <- REKEY ADDRESSES REKEY
  rekey retransmit 40 number 3  <- REKEY RETRANSMITS
  authorization address ipv4 member-list <- GROUP MEMBER AUTHORIZATION
  sa ipsec 1                    <- SECURITY ASSOCIATION
  profile gdoi-p                <- CRYPTO ATTRIBUTES SELECTION
  match address ipv4 lans-only  <- ENCRYPTION POLICY LAN-to-LAN
  no replay                     <- NO ANTI-REPLAY
  address ipv4 <ks_address>     <- KS ADDRESS
```

Rekey Profile (needed multicast rekey only)

```
access-list 102 permit any host 239.192.1.1
                                                    <- REKEY SOURCE / DESTINATION
```

Group Member Authorization List (optional)

```
ip access-list extended member-list          <- GM AUTH LIST
  permit <ks_peer_address>                   <- PEER KS
  permit <gm_address>                         <- GROUP MEMBER
```

Encryption IPsec Proxy (mandatory)

```
ip access-list extended lans-only           <- ENCRYPTION POLICY
  deny udp any eq 848 any eq 848           <- GDOI IN CLEAR
  permit ip 10.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255 <- UNICAST
  permit ip 10.0.0.0 0.255.255.255 232.0.0.0 0.255.255.255 <- MULTICAST
```

Group Member

Secured Group Member Interface

```
interface Serial0/0
  ip address 192.168.1.14 255.255.255.252
  crypto map svn                                <- WAN ENCRYPTION
```

Crypto Map Association to Group Security

```
crypto map svn 10 gdoi                          <- GROUP CRYPTO MAP ENTRY
  set group secure-wan                          <- GROUPMEMBERSHIP
```

Group Member Association

```
crypto gdoi group secure-wan                    <- GROUPENCRYPTION
  identity number 3333                          <- GROUPIDENTITY FOR MEMBER
  server address ipv4 <ks_address>              <- KS ADDRESS TO REGISTER
```

Cisco Networkers

25-28. Januar 2010. Barcelona
28-31. Mart 2010. Bahrein



Registrujte se



