DOI: 10.19279/TVZ.PD.2014-2-1-15

DINAMIČKE SKALABILNE VIRTUALNE PRIVATNE MREŽE

Ivan Filipaj, Danijela Pongrac, Dubravko Žigman

Tehničko veleučilište u Zagrebu

Sažetak

Virtualne privatne mreže (Virtual Private Network - VPN) danas su tehnologija koja se svakodnevno susreće unutar privatne i poslovne okoline. VPN se koristi u razmjeni podataka i komunikaciji između dvije ili više točaka koje imaju potrebu za pristup privatnim podacima. Tijekom takve komunikacije dolazi i potreba za zaštitom. Pod zaštitom se ne smatra samo zabrana pristupa neautoriziranim korisnicima nego i potvrda da preneseni podaci nisu mijenjani ili poslani sa neovlaštenog izvora. Svakodnevnim razvojem Interneta nemoguće je zamisliti poslovanje bez konstantnog pristupa Internetu, a sa tom mogućnošću razvilo se i poslovanje udaljenih lokacija koje ima potrebu funkcionirati kao jedna cjelina kako bi pristup svim potrebnim resursima bio nadohvat ruke i omogućen u svakom trenutku. Među raznim izvedbama i tehnologijama za realizaciju VPN mreže ovaj rad prikazuje prednosti korištenja DMVPN (Dynamic Multipoint Virtual Private Network) protokola.

Ključne riječi: *vpn, virtualne privatne mreže, dinamičke, dmvpn, ipsec*

Abstract

Virtual Private Networks (VPN) is a form of technology which is found within a private and business environment on a daily basis. A VPN is used in data exchange and in communication between two or more endpoints that have a need for access to private data. When such communication takes place, data protection is a necessity. Not only does this protection imply restricted access to unauthorized users, but also a confirmation that the data transferred have not been in any way altered or sent from an unauthorized source. With the internet in constant development, it is impossible to imagine doing business without uninterrupted internet access. With this capability comes a need for businesses to maintain a constant connection, with faraway locations acting as a whole, thus making immediate access to any and all necessary resources available at any moment. Among the different solutions and technologies used for creating a VPN, this paper displays the advantages of using the DMVPN (DynamicMultipointVirtual-PrivateNetwork) protocol.

Key words: *vpn, virtual private networks, dynamic, dmvpn, ipsec*

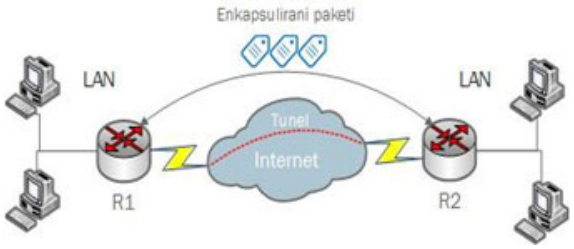
1. UVOD

Tehnička izvedba virtualnih privatnih mreža se prije sastojala od iznajmljivanja privatnih veza od Internetskog poslužitelja (ISP Internet Service Provider) ili putem nepouzdanog dial-up modemskog povezivanja. Razvojem ADSL-a (Asymmetric Digital Subscriber Line), a ponajviše razvojem MPLS (Multiprotocol Label Switching) tehnologije koja se koristi unutar ISP mreže, omogućila su se mnogo efektivnija rješenja koja osim jednostavnije upotrebe zahtijevaju i cjenovno puno manji izdatak.[1]

2. TEHNIČKA IZVEDBA VPN-A

Virtualne privatne mreže se tako mogu realizirati na više načina, ovisno o potrebi samog korisnika. Od jednostavnog točka-točka povezivanja dviju lokacija do kompleksnih rješenja gdje je broj povezanih lokacija gotovo neograničen. Unutar ovih rješenja razvijene su razne dodatne pogodnosti kao što su kombinacije fiksnih lokacija zajedno sa mobilnim spajanjem, spajanje putem više Internet konekcija i stvaranje backup konekcija u slučaju prekida glavnih veza.
Samo povezivanje se postiže tehnologijama tuneliranja, između dviju ili više lokacija, koje se svakodnevno razvijaju ispravljajući stare i dodajući nove mogućnosti. Tako povezane lokacije nisu sigurne od neovlaštenog pristupa i prisluškivanja pa ih je potrebno zaštititi nekom metodom enkripcije i digitalnim certifikatima. Zaštita podataka enkripcijom i certifikatima je glavni faktor za sigurnost prilikom komunikacije putem Interneta koji se u informatičkom svijetu gleda kao nesigurna javna mreža. Ne samo za komunikaciju unutar neke poslovne okoline nego i privatnog

korištenja servisa kao što su web mail, internet bankarstvo i kupovina putem web trgovina.[1] Kod implementacije virtualnih privatnih mreža postoje mnoga rješenja i razni elementi pomoću kojih se postižu zadani ciljevi za njihovu uspostavu. Jedan od osnovnih modela spajanja je povezivanje točka-točka lokacija gdje se povezuju udaljene LAN (Local Area Network) mreže putem Interneta u jednu privatnu mrežu. Na svakom izlaznom sučelju pojedinog LAN segmenta, nalazi se usmjernik koji povezuje lokalnu mrežu na Internet. Između tih usmjernika stvara se tunel koji omogućuje virtualnu lokalnu povezanost između dviju lokacija.



Slika 1. Prikaz tuneliranja paketa

Svi paketi namijenjeni za komunikaciju u virtualnoj privatnoj mreži enkapsuliraju se na izlazu iz usmjernika R1 i R2 i dekapsuliraju kada stignu na odredišni usmjernik. Ovim postupkom usmjernik zadržava privatne adrese unutar paketa te se tako promet ponaša kao da je u lokalnoj mreži LAN.

Kod VPN-a postoje dva osnovna koncepta spajanja:

Udaljeni pristup (Remote-access) – Koncept koji sporazumijeva spajanje jednog uređaja na krajnjoj točci u virtualnu privatnu mrežu. Najčešće se odnosi na mobilne uređaje (prijenosna računala) koja imaju potrebu pristupiti privatnoj mreži kada se nalaze izvan ureda.

Lokacija-na-lokaciju (Site-to-site) – Ovakvo spajanje predstavlja povezivanje dvije ili više kompletnih lokalnih mreža koje su geografski udaljene jedna od druge kako bi se stvorila virtualna privatna mreža.[2]

Tehnologije za tuneliranje
Najčešće korištene tehnologije za tuneliranje trenutno su L2TP (Layer 2 Tunneling Protocol) i GRE (Generic Routing Encapsulation) protokol koji stvaraju ranije spomenuti tunel između dvije lokacije.

3. ZAŠTITA TUNELA

L2TP i GRE protokoli za stvaranje tunela ne pružaju zaštitu informacija koje se razmjenjuju između udaljenih lokacija. Za funkcionalnost zaštite koristi se IPSec protokol (Internet Protocol Security koji danas predstavlja najbolji izbor za osiguranje komunikacije u VPN mrežama. IPSec je zapravo skup protokola za autentifikaciju i enkripciju koji pruža međusobnu kompatibilnost različitih protokola. Protokoli unutar IPSec skupa nisu krajnje definirani trenutnim popisom podržanih protokola, pa se tako ostavlja prostor za implementaciju budućih tehnologija u područjima koje pokriva, kao što su novi tipovi enkripcije, autentikacije itd.

4. ZNAČAJKE IPSEC PROTOKOLA

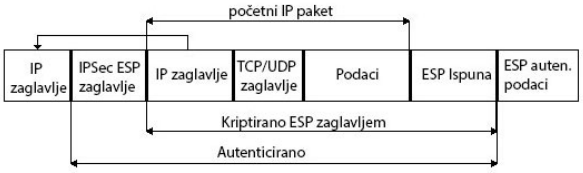
IPSec pruža elemente sigurnosnog modela koji određuje virtualne privatne mreže.
Povjerljivost – osigurava da samo ovlašteni korisnici mogu pristupiti zaštićenim podacima koristeći enkripciju i ograničavanje pristupa.
Integritet – osigurava da se podaci nisu promijenili tijekom prijenosa od strane neovlaštenih korisnika.
Dobavljivost – osigurava da su podaci uvijek dostupni zaštitom od napada koji onemogućavaju pristup resursima kao što su Denial-of-Service (DoS) napadi.[2]
Neki od podržanih protokola unutar pojedinih elemenata IPSec protokola su:
Pregovaranje:
- AH Authentication Header
- ESP Encapsulating Security Payload
- ESP+AH kombinacija oba protokola

Enkripcija:
- DES Data Encryption Standard
- 3DES Triple DES
- AES Advanced Encryption Standard
- Autentičnost (cryptographic hash function):
- MD5
- SHA-1

Sigurnost:
- DH1 Diffie–Hellman key exchange
- DH2

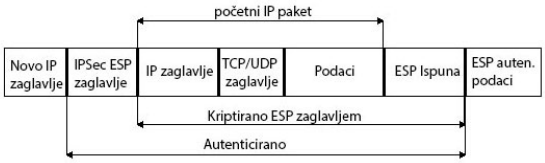
IPSec ima dva načina rada za realizaciju zaštite između lokacija. Transportni način (engl. Transport mode) i tunel način (engl. Tunnel mode). Razlika između ova dva načina je u dijelovima paketa koji su zaštićeni. U transportnom načinu osigurava se sve od prijenosnog sloja OSI (Open

Systems Interconnection model) modela. Stoga interne IP adrese koje djeluju u području nižeg, mrežnog sloja, nisu zaštićene enkripcijom.



Slika 2. Prikaz paketa enkapsuliranog u transport načinu

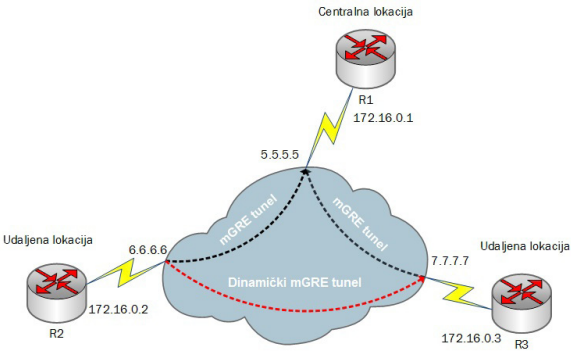
U tunel načinu osigurava se sve od mrežnog sloja OSI modela pa tako i zaglavlja koja sadrže informacije o privatnim IP adesama.



Slika 3. Prikaz paketa enkapsuliranog u tunel načinu

5. DINAMIČKE SKALABILNE VIRTUALNE PRIVATNE MREŽE (DMVPN)

Virtualne privatne mreže se najčešće izvode putem stvaranja točka-točka principa spajanja gdje je potrebno na svakoj strani nekog tunela konfigurirati virtualna sučelja koja predstavljaju krajnju točku nekog tunela. Dinamičke skalabilne virtualne privatne mreže DMVPN (Dynamic Multipoint Virtual Private Network) je rješenje nastalo iz potrebe za pojednostavnjenjem izvedbe VPN mreže. Ovo se najviše odnosi na jednostavnost implementacije i održavanje uređaja unutar VPN-a. Kod konfiguracije DMVPN mreže centralnu lokaciju je potrebno samo jednom konfigurirati te se tako svaka nova udaljena lokacija dinamički povezuje i stvara tunele potrebne za privatnu komunikaciju krajnjih točaka.[3]
Najbitniji elementi koji čine DMVPN protokol su:
Multipoint GRE (mGRE) – predstavlja tehniku kojom se omogućuje stvaranje više GRE tunela putem jednog sučelja. Konfiguracijom jednog tunel sučelja na centralnom usmjerniku definiraju se svi budući tuneli koji će se stvarati putem ovog sučelja.[4]
Rezolucijski protokol slijedeće točke (NHRP) - Next-Hop Resolution Protocol je protokol drugog mrežnog sloja koji stvara bazu povezanih tunela kreiranih preko stvarne mreže. NHRP automatski povezuje vanjske javne adrese sa internim adresama koje predstavljaju neki tunel, te sa tom bazom pruža informaciju svim usmjernicima o traženim destinacijama preko kojih se želi uspostaviti tunel. Ova dinamičnost omogućuje povezivanje javnih adresa koje nisu stalne ukoliko se koriste dinamičke adrese zbog puno manje cijene usluge. [5]



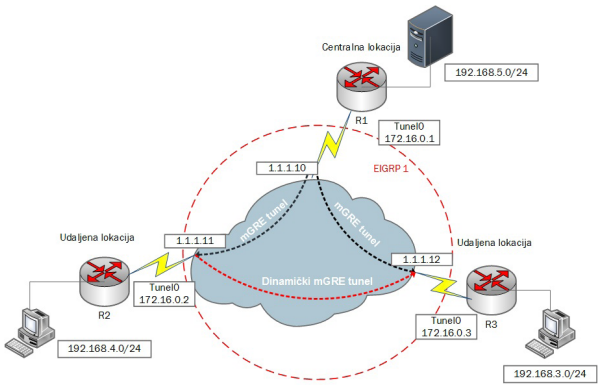
Slika 4. Prikaz DMVPN tunela

Jedna od bitnih prednosti DMVPN protokola je mogućnost dinamičkog stvaranja direktnih kanala između udaljenih točaka. Kada usmjernik na udaljenoj lokaciji R2 zatraži pristup drugoj udaljenoj lokaciji R3, usmjernik na centralnoj lokaciji R1 javlja informaciju R2 o odredišnoj IP adresi udaljene lokacije R3. Nakon ovoga ostvaruje se direktna komunikacija između R2 i R3 usmjernika. Ovime se postiže kraća ruta kojom paketi putuju te se izbjegava promet preko centralnog usmjernika koji u tom slučaju troši dodatnu propusnost u odlaznom smjeru (upload). Druga prednost je mogućnost korištenja dinamičkih usmjerničkih protokola kao što su često korišteni EIGRP i OSPF za usmjeravanje prometa udaljenih mreža. Ovo omogućuje GRE protokol koji ima mogućnost slanja broadcast i multicast poruka koje su nužne za rad navedenih usmjerničkih protokola.[4]
Nedostatak DMVPN protokola je nemogućnost korištenja na uređajima koji nisu marke Cisco budući da je DMVPN razvijen i u vlasništvu ove tvrtke.

6. PRIMJER KONFIGURACIJE DMVPN RJEŠENJA

Virtualna privatna mreža stvorena korištenjem DMVPN rješenja sastoji se od dvije cjeline. Prvi korak je konfiguracija tunel sučelja putem GRE protokola kojima se stvara virtualno povezivanje. Drugi korak je opcionalno ali uvijek poželjno osiguranje prijenosa podataka putem IPSec pro-

tokola. U primjeru je prikazano rješenje sa jednim centralnim usmjernikom i dvije udaljene lokacije.



Slika 5. Prikaz konfiguracije DMVPN rješenja

Javna sučelja u ovom primjeru na svakoj lokaciji imaju postavljenu statičku IP adresu radi jednostavnijeg prikaza funkcionalnosti DMVPN protokola. U realnom scenariju koristi se dinamička javna adresa na udaljenim lokacijama i statička na centralnoj lokaciji. Za funkcionalnost DMVPN-a putem takvih dinamičkih adresa nije potrebna dodatna konfiguracija jer NHRP protokol automatski povezuje trenutnu javnu IP adresu sa tunel sučeljem i pohranjuje poveznicu unutar tablice.

Tablica 1. Popis sučelja i adresa

Uređaj	Sučelje	IP adresa /24
R1	FastEthernet0/0	192.168.5.1
	FastEthernet0/1	1.1.1.10
	Tunnel 0	172.16.0.1
R2	FastEthernet0/0	192.168.4.1
	FastEthernet0/1	1.1.1.11
	Tunnel 0	172.16.0.2
R3	FastEthernet0/0	192.168.3.1
	FastEthernet0/1	1.1.1.12
	Tunnel 0	172.16.0.3

R1 Tunnel

```
interface Tunnel0
 description R1 DMVPN Tunnel

 ip address 172.16.0.1 255.255.255.0(1)
 no ip redirects
 ip nhrp authentication kljuc          (2)
 ip nhrp map multicast dynamic         (3)
 ip nhrp network-id 1                  (4)
 tunnel source 1.1.1.10                (5)
 tunnel mode gre multipoint            (6)
```

Ovdje je prikazana konfiguracija tunela na centralnom usmjerniku R1. Vidljiva je postavljena privatna adresa tunel sučelja (1), postavljanje lozinke za pristup NHRP bazi (2), omogućavanje multicast prometa (3), označavanje ID-a privatne mreže (4) i odabir izlazne točke tunela (5) koja na centralnom usmjerniku mora biti statička adresa kako bi udaljene lokacije imale fiksno odredište prema kojem će se stvarati tunel. U zadnjoj naredbi (6) tunel sučelje se označava kao višestruko sučelje bez fiksno određenog odredišta. U točka-točka konfiguraciji tunela koristila bi se naredba tunnel destination.

R2 Tunnel

```
interface Tunnel0
 description R2 DMVPN Tunnel

 ip address 172.16.0.2 255.255.255.0   (1)
 no ip redirects
 ip nhrp authentication kljuc
 ip nhrp map multicast dynamic
 ip nhrp map 172.16.0.1 1.1.1.10       (2)
 ip nhrp map multicast 1.1.1.10
 ip nhrp network-id 1
 ip nhrp nhs 172.16.0.1                (3)
 tunnel source FastEthernet0/1         (4)
 tunnel mode gre multipoint
```

Prikaz konfiguracije tunel sučelja na jednom od udaljenih usmjernika, R2. Konfiguracija na svim ostalim udaljenim usmjernicima je jednaka osim što se mijenjaju adrese pojedinog tunel sučelja (1). Naredbom u (2) i (3) podešava se putanja prema centralnom usmjerniku R1 kako bi se stvorio sam tunel i povezane adrese spremile unutar NHRP tablice. Označavanjem izvora tunela (3) kao naziv sučelja ne određuje se statična izvorišna adresa nego se automatski povezuje sa onom trenutnom koja se nalazi na tom sučelju. Ovo omogućava konfiguraciju ukoliko se javna IP adresa dodjeljuje dinamički.

```
R1#
crypto isakmp policy 1                 (1)
 encr 3des
 hash md5
 authentication pre-share
 group 2
 lifetime 86400

crypto ipsec transform-set TRANSSET esp-3des
```

```
esp-md5-hmac                    (2)
crypto ipsec profile IPSECPROFIL
set transform-set TRANSSET

interface tunnel 0
tunnel protection ipsec profile IPSECPROFIL (3)
```

Kako bi se konfigurirani tuneli zaštitili potrebno je primijeniti IPSec protokol. Nakon konfiguracije IPSec skupa sigurnosnih parametara poznatih kao faza 1 (ISAKMP) (1) gdje se definiraju algoritmi za enkripciju i autentifikaciju i faze 2 (2) u kojoj se konfigurira transformacijski skup i IPSec profil, potrebno je profil primijeniti na tunel sučelje (3).

```
R1#ping 192.168.4.1 source 192.168.5.1 (1)
2103  2843.735155000   1.1.1.10      1.1.1.11
ESP   180    ESP (SPI=0x33dce96c)
2104  2843.785158000   1.1.1.11      1.1.1.10
ESP   180    ESP (SPI=0x5de15f47)
```

Naredbom ping (1) između R1 i R2 usmjernika vidljiv je zaštićen promet enkapsuliran i zaštićen GRE/IPSEC protokolima.
Kod spajanja dodatnih lokacija dokazuje se prednost DMVPN protokola jer je potrebno konfigurirati samo udaljeni usmjernik prema parametrima podešenim na centralnom usmjerniku. Ukoliko se želi ostali internet promet odvojiti od VPN mreže potrebno je konfigurirati pristupne liste koje će odrediti promet namijenjen virtualnoj privatnoj mreži, a sav ostali proslijediti kao običan internet promet na odgovarajuće sučelje. Dodatne opcije ovakve mreže su konfiguracija više Internet konekcija za backup ili load-balancing i konfiguracija centralnog usmjernika za mogućnost stvaranja tunela putem udaljenog mobilnog pristupa.

7. ZAKLJUČAK

DMVPN predstavlja skalabilno rješenje za implementaciju virtualnih privatnih mreža koje će naći primjenu unutar gotovo svake organizacije. Jednostavnost konfiguracije i dodavanje novih udaljenih lokacija smanjuje troškove i potrebno vrijeme za implementaciju i održavanje. Zadržava sve prednosti klasičnih VPN izvedbi, te ih proširuje dodatnim opcijama. Jedini nedostatak DMVPN protokola je ovisnost o jednom proizvođaču opreme dok alternativna rješenja ne nude funkcionalnost direktnog povezivanja udaljenih lokacija. Obilaženje ovog nedostatka kod ostalih izvedbi je moguće riješiti kvalitetnim vezama prema centralnoj lokaciji koja mora imati dovoljnu propusnost i hardversku snagu za veći broj povezanih lokacija što povećava trošak i komplicira samu izvedbu stvaranja virtualne privatne mreže.

8. LITERATURA

[1.] Catherine Paquet: „Implementing Cisco IOS Network Security (IINS) Foundation Learning Guide“, Cisco Press, Indianapolis, 2013

[2.] Vijay Bollapragada; Mohamed Khalid; Scott Wainner: „IPSec VPN Design (Networking Technology)“, Cisco Press, Indianapolis, 2005

[3.] Cisco Systems: „Cisco IOS DMVPN Overview“, s interneta: http://www.cisco.com/c/dam/en/us/products/collateral/security/dynamic-multipoint-vpn-dmvpn/DMVPN_Overview.pdf , veljača, 2008.

[4.] Petr Lapukhov: „DMVPN Explained“, s interneta: http://blog.ine.com/2008/08/02/dmvpn-explained/, 02.Kolovoz,2008

[5.] Cisco Systems, „Configuring NHRP“ s Interneta: http://www.cisco.com/c/en/us/td/docs/ios/12_4/ip_addr/configuration/guide/hadnhrp.pdf, 03.travanj, 2007.

AUTORI

Ivan Filipaj rođen je 09.05.1986. godine u Zagrebu, završava osnovnu školu u Sesvetskom Kraljevcu i srednju elektrotehničku školu u Sesvetama, smjer tehničar za elektroniku. Nakon srednje škole upisuje stručni studij na Tehničkom Veleučilištu Zagreb smjer informatika koji završava 2010. godine. Upisuje specijalistički studij informatike na TVZ-u, smjer: Projektiranje i implementacija računalnih mreža kojeg završava 2014. godine. Tijekom specijalističkog studija zapošljava se u tvrtci Optima Telekom d.d. na poziciji: Specijalist u odjelu za operativne poslove,

na kojem radi od 2011. pa do danas. Nositelj je certifikata CCNA i CCNA Security.

Danijela Pongrac rođena je 1969. godine u Zagrebu. Diplomirala je 1998. godine pri Filozofskom Fakultetu Sveučilišta u Zagrebu među najboljim studentima odsjeka pedagogije. Od 1998. do 2006. radi kao Voditelj informatičkog učilišta firme SYS, u organizaciji stručnih tečajeva za sistem i mrežne inženjere iz područja Microsoft, Novell i Citrix tehnologija. Od 2006. godine radi na Tehničkom veleučilištu Zagreb, kao voditelj Cisco edukacije i ispitnog centra. Voditelj projekta organizacije i doprinosa edukacije mrežnih tehnologija NetAkademije, nagrađeno s tri priznanja koje dodjeljuje Cisco. Upisala je 2010. na Filozofskom Fakultetu poslijediplomski doktorski studij Informatologije i komunikologije. Od 2011. godine u statusu je predavača.

Mr. sc. Dubravko Žigman rođen je 1970. godine u Zagrebu, gdje završava osnovnu školu i srednju matematičku školu. Studij završava 1996. godine na smjeru Elektroenergetika, usmjerenju Opća energetika. 2002. godine stiče stručni naziv magistra znanosti iz polja Elektrotehnike, smjer Elektroenergetika. Od 2006. radi na TVZ-u kao viši predavač. Dobitnik je slijedećih nagrada: 2013 nagrada u kategoriji CCNP Curricula Excellence, 2008 dobitnik tri od četiri priznanja koje dodjeljuje Cisco: Education Recognition, Extraordinary Contributions i Pioneer Recognition. 2005 NetAkademija proglašena za najbolju lokalnu Cisco akademiju u EMEA regiji. Nositelj je nekoliko priznatih industrijskih certifikata: CompTIA A+, MCP, CCNA, CCAI, CCNP, NLP-Practitioner IANLP.