DOI: 10.19279/TVZ.PD.2016-4-3-14

SPAJANJE DVIJU KOMPANIJA U VPN

CONNECTING TWO COMPANIES INTO VPN

Davor Ćulumović[1], Dubravko Žigman[2], Igor Mamuzić[3]

[1]Student TVZ-a
[2]Tehničko veleučilište u Zagrebu
[3]Instruktor na Tehničkom veleučilištu u Zagrebu, CCNA Security

Sažetak

Glavni cilj i svrha ovog rada jest prikazati kojim se sve sigurnosnim tehnologijama i protokolima može osigurati virtualna privatna mreža između dviju kompanija. Virtualna privatna mreža ili VPN je tehnologija koja je nezaobilazna pri međusobnom spajanju udaljenih lokacija neke kompanije, dviju različitih kompanija ili spajanju zaposlenika kompanije sa svoje osobne mreže na mrežu svoje kompanije. U radu će biti objašnjene tehnologije za prijenos podataka unutar VPN-a, razni protokoli za tuneliranje te dvije vrste VPN-a, Remote-access VPN i site-to-site VPN. Također, prikazana će biti i konfiguracija IPsec site-to-site VPN-a na Check Point 4000 vatrozidu te konfiguracija Remote-access VPN na Cisco ASA 5500 vatrozidu. Ta dva uređaja će predstavljati centralnu lokaciju ili kompaniju A, a Cisco usmjernik će predstavljati kompaniju B.

Ključne riječi: *VPN, IPsec, site-to-site, Remote-access, Check Point, Cisco ASA*

Abstract

The main objective and purpose of this paper is to show all security technologies and protocols that can provide a virtual private network between the two companies. Virtual Private Network or VPN is a technology that is indispensable for mutual connecting of remote locations of a company, two different companies or connecting company employees through their own personal network to their company's network.

In this paper describes technologies for data transfer within the VPN, various protocols for tunneling and also two types of VPNs, Remote-access VPN and site-to-site VPN. It also presents the configuration of IPsec site-to-site VPN on Check Point 4000 firewall and configuration of Remote-access VPN on the Cisco ASA 5500 firewall. The two devices represent a central location or company A, and Cisco router represents the company B.

Keywords: *VPN, IPsec, site-to-site, Remote-access, Check Point, Cisco ASA*

1. Uvod

1. *Introduction*

U ovom modernom svijetu, kompanije polako počinju dijeliti svoje informacije s drugim kompanijama i iz toga proizlazi potreba za virtualnim privatnim mrežama. Naime, potreba za umrežavanjem s udaljenim lokacijama iste kompanije i poslovnim partnerima postoji odavno, ali tek je od nedavno Internet postao dovoljno siguran za povezivanje putem VPN-a i polako istiskuje iz upotrebe VPN servise koje pružaju pružatelji Internet usluga (poput L2 i L3 VPN-ova), ako je potrebno samo bazično povezivanje bez velikih brzina ili naprednog upravljanja prometom. Ako je potrebno napredno upravljanje prometom ili velike brzine i dalje nema boljeg rješenja od MPLS-a i "dark fibera" za brzine 10 Gbps i više.

Cilj ovog rada jest prikazati što je sve potrebno od uređaja i konfiguriranja da bi se ostvarila povezanost između dvije kompanije unutar VPN-a te naučiti čitatelje što je to VPN i njezine vrste kako bi sami mogli uvesti VPN u svoje kompanije.

2. Virtualna privatna mreža

2. *Virtual private network*

Virtualna privatna mreža je tehnologija kojom se stvara enkriptirana konekcija preko manje sigurne mreže.[1]

Organizacije koriste VPN (slika 1) kako bi stvorile privatne mrežne konekcije ili tunele koristeći mrežu pružatelja Internet usluga. Ovim tunelom se eliminira negativnost koju stvara udaljenost između lokacija i omogućuje korisnicima na udaljenim lokacijama spajanje na te lokacije kako bi pristupili resursima tvrtke. Sam VPN tunel ne garantira da će informacije koje prolaze kroz njega ostati sigurne stoga se konfiguraciji VPN-a dodaju razne kriptografske metode koje omogućuju sigurne konekcije. Za konfiguriranje sigurnih VPN tunela koriste se IP Security ili IPsec radna okruženja koja preko Interneta omogućuju udaljenim lokacijama i poslovnim partnerima sigurno spajanje na centralnu lokaciju. Sa strane spajanje djelatnika na centralnu lokaciju sve više se koristi SSL VPN koji je gotovo potpuno istisnuo IPsec jer je sa SSL VPN-om puno lakše proći kroz vatrozide.

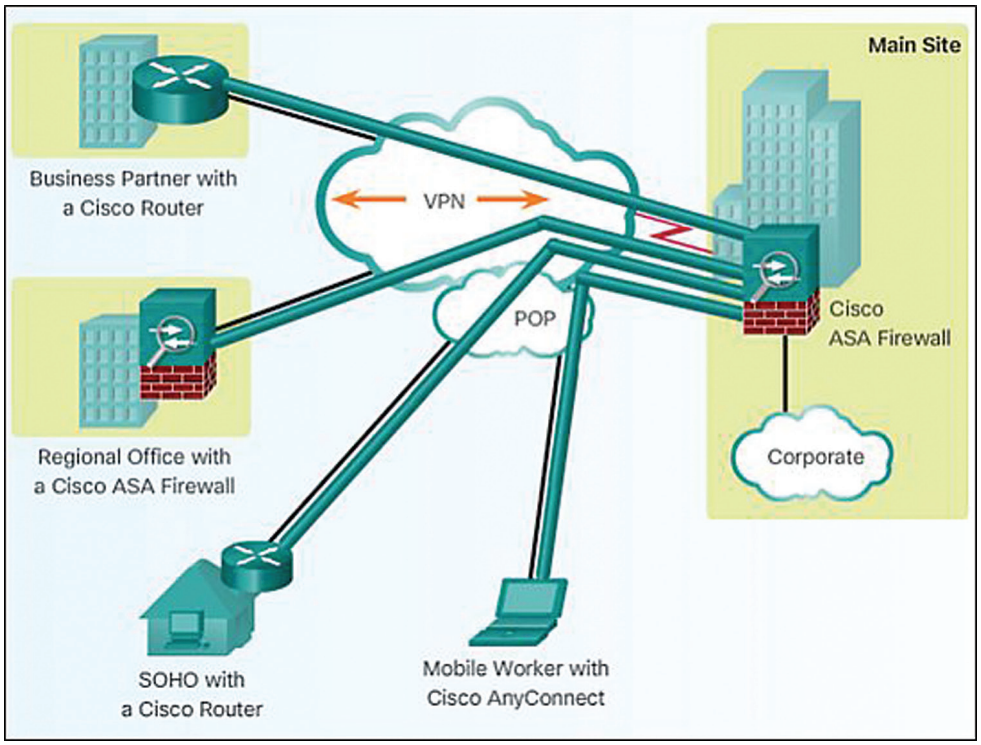
VPN koristi, umjesto fizičkih veza, virtualne konekcije rutirane kroz Internet od organizacije do udaljene lokacije. Riječ "virtualna" u virtualnim privatnim mrežama znači da informacija, podatak putuje unutar privatne mreže no zapravo je ta informacija transportirana preko javne mreže.[2]

2.1 Prednosti i mane VPN-a

2.1 *Advantages and disadvantages of VPN*

Glavna prednosti VPN-a je da svatko može s udaljenosti pristupiti lokalnoj mreži svoje kompanije koristeći javnu mrežu koju osigurava pružatelj Internet usluga što smanjuje troškove kompanija kod poslovanja.[3] Kompanije više ne trebaju koristiti skupe namjenske ili stalne WAN veze ili banke modema pružatelja Internet usluga jer dolaskom tehnologija visoke propusnosti kao što su DSL tehnologije. VPN je kompatibilan sa širokopojasnim tehnologijama što znači da djelatnici mogu iskoristiti svoju brzu Internet vezu iz svojeg doma kako bi lakše i brže pristupili svojim kompanijama. VPN osigurava najvišu razinu sigurnosti uz naprednu enkripciju i autentikaciju koristeći posebne protokole koji štite od neovlaštenog pristupa i hakiranja.[2]

VPN se, naravno, ne može koristiti ako osoba nema pristupa Internetu, to jest, ako ne radi lokacija od našeg pružatelja Internet usluga. Korištenjem VPN-a se smanjuje i naša brzina Interneta, na primjer, otvaranje Internet stranice je 10-15% sporije, a skidanje i učitavanje podataka je 20-25% sporije, no ako je sve pravilno konfigurirano korisnici ne bi mogli osjetiti nikakav "delay". Osim što spajanje u VPN može smanjiti brzinu našeg Interneta on može i usporiti rad usmjernika iz tog razloga usmjernici i vatrozidi svih većih proizvođača obavljaju enkripciju i dekripciju koristeći poseban procesor koji se zove crypto akcelerator.[4]



Slika 1
VPN tuneli preko Interneta [2]

Figure 1
VPN tunnels over Internet [2]

2.1 Vrste VPN-a

2.1 *Types of VPN*

Postoje dvije vrste VPN-a, to su: site-to-site VPN i Remote-access VPN. Site-to site VPN spaja dvije ili više mreža u jednu mrežu. Te mreže koriste sofisticirane načine kriptiranja kako bi zaštitile promet od hakera. Veza između nekog ureda odvojenog od glavne lokacije je jedan od primjera site-to-site VPN-a. Korisnici na tim lokacijama nisu svjesni njihovog pristupanja resursima na tim lokacijama.

Remote-access VPN dopušta korisniku s računalom spajanje na privatnu mrežu. Na primjer, korisnik ima službeno prijenosno računalo s kojim se spaja putem VPN softvera na mrežu svoje kompanije. Tada korisnik može pristupiti file serverima, e-mailovima ili spojiti se na svoje računalo.[5]

3. Protokoli za tuneliranje

3. *Tunneling protocols*

Tuneliranje omogućuje enkapsulaciju paketa jedne vrste protokola unutar jednog bloka podataka različitog protokola. Na primjer, VPN koristi PPTP protokol za enkapsulaciju IP paketa preko javne mreže kao što je Internet. Neki od protokola za tuneliranje su: PPTP, L2F, L2TP i GRE. Zbog niske razine sigurnosti često se koriste zajedno sa IPsec-om.[6]

4. Tehnologije za prijenos podataka unutar VPN

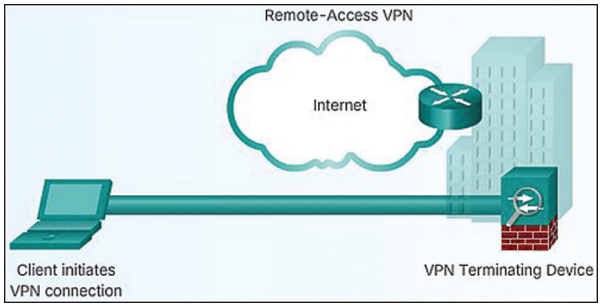
4. *Technologies for data transfer inside VPN*

Prijenos podataka između udaljenih lokacija neke kompanije u centralne lokacije iste kompanije se vrši između usmjernika pružatelja Internet usluga koji se nalaze na tim lokacijama. Usmjernici kompanije su spojeni na usmjernike pružatelja Internet usluga koji za prijenos podataka koriste tehnologije kao što su: ATM, Frame relay i MPLS. U prijenosu podataka im pomažu oznake virtualnih veza ili oznake ruta odredišta, što čini prijenos podataka bržim.[7]

5. Remote-access VPN

5. *Remote-access VPN*

Remote-access VPN (slika 2) podržava klijent-server arhitekturu gdje VPN klijent (udaljeni korisnik/računalo) traži sigurni pristup do mreže svoje kompanije preko VPN servera. U Remote-access VPN-u udaljeni korisnik je svjestan postojanja VPN-a i svaki puta kada se spaja na svoju kompaniju mora upisivati korisničko ime i lozinku u neki od VPN klijent programa. Primjeri Remote-access VPN-a su: Cisco IOS SSL VPN i Cisco Easy VPN.[2]



Slika 2 *Remote-access VPN* [2]

Figure 2 *Remote-access VPN* [2]

6. Site-to-site VPN

6. *Site-to-site VPN*

Site-to-site VPN dozvoljava uredima na više različitih lokacija da uspostave sigurnu konekciju između sebe preko javne mreže. Site-to-site VPN možemo podijeliti na:

- Intranet VPN – Ako kompanija ima više udaljenih lokacija koje se žele spojiti u jednu privatnu mrežu tada je moguće stvoriti Intranet VPN kako bi spojili više odvojenih LAN-ova u jedan WAN.
- Ekstranet VPN – Ako je kompanija u bliskom odnosu s drugom kompanijom (partner, dobavljač ili kupac) može stvoriti ekstranet VPN koji spaja LAN-ove tih kompanija.

Kod Site-to-site VPN-a korisnik nije svjestan svoje povezanosti sa VPN-om što znači da ne treba upisivati svoje korisničko ime i lozinku da se spoji u VPN. Neki primjeri site-to-site VPN-a su: IPsec site-to-site VPN, Dynamic Multipoint VPN i GET VPN.[8]

Primjer konfiguriranja IPsec site-to-site VPN-a
Example of IPsec site-to-site VPN configuration

Za konfiguraciju IPsec site-to-site VPN-a ćemo koristiti Check Point 4000 vatrozid i program SmartDashboard R77.30. Prvi korak je konfiguracija samog vatrozida, znači, konfiguriraju se sučelja, instaliraju se certifikati i dodaju se značajke Firewall, IPsec VPN i IPS pod Network Security opcije (slika 3).

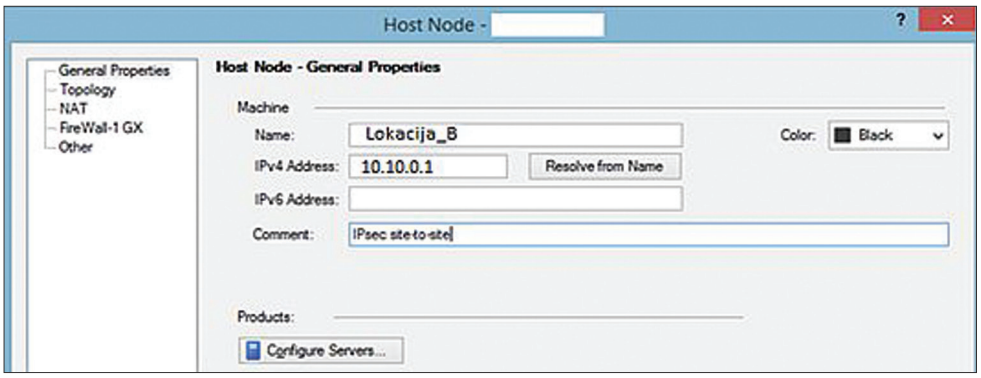
Zatim se konfigurira VPN oblak ili zajednica gdje možemo dodati objekte koji se nalaze u VPN-u, odrediti način enkripcije, hashiranja i razmjene ključeva i podataka te koju zajedničku lozinku koriste objekti unutar VPN-a. Poslije VPN oblaka se mogu konfigurirati objekti (Node) koji predstavljaju svaki mrežni objekt koji nema instaliran Check Point softver. Objektima se dodaje IP adresa i njihovo ime (slika 4).

Sljedeći korak je izrada pravila kojima govorimo koje lokacije komuniciraju jedna s drugom i na koji način (slika 5).

Na sličan način kao i sučelja vatrozida se konfiguriraju mreže koje komuniciraju kroz vatrozid i sateliti koji predstavljaju usmjernike ili vatrozide lokacija koje komuniciraju s centralnim vatrozidom, u ovom slučaju Check Point vatrozidom. Kod konfiguriranja mreže upisuje se njezino ime, IP adresa mreže i njezina maska,

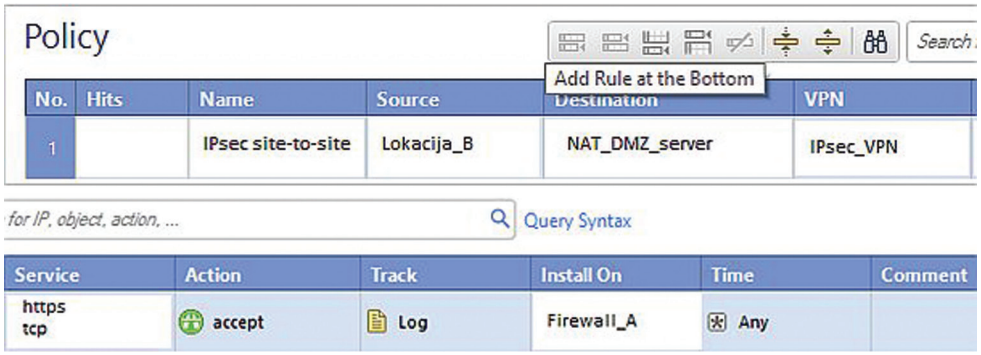
Slika 3
Network Security opcije

Figure 3
Network Security options



Slika 4
Konfiguracija objekta

Figure 4
Node configuration



Slika 5
Izrada pravila

Figure 5
Making of policy

No.	Original Packet			Translated Packet			Install On
	Source	Destination	Service	Source	Destination	Service	
1	Any	NAT_DMZ	Any	Original	DMZ	Original	Firewall_A
2	DMZ	NAT_LAN_B	Any	NAT_DMZ	Original	Original	Firewall_A

Slika 6 *NAT*

Figure 6 *NAT*

a kod satelita se, osim imena i IP adrese, dodaje kojoj mreži i kojem VPN oblaku pripada satelit. Rutiranje se radi na web sučelju ili komandnoj liniji Check Point vatrozida.

Na kraju se radi natiranje (slika 6) to jest stvaranje pravila natiranje u kojima definiramo sa koje IP adrese će doći upit i sa koje IP adrese će doći odgovor na upit.

8. Primjer konfiguriranja Remote-access VPN-a

8. *Example of Remote-access VPN configuration*

Za konfiguraciju Remote-access VPN-a će se koristiti vatrozid Cisco ASA 5500. Za početak se konfiguriraju sučelja, ime domene i rute. Potrebno je iskonfigurirati pool IP adresa koje dobivaju korisnici prilikom spajanja u VPN i pristupnu listu koja dopušta svima iz pool-a da se spoje na vatrozid.

- *ip local pool EASYVPN_POOL 10.10.0.1-10.10.0.253 mask 255.255.255.0*
- *access-list EASYVPN_ACL extended permit tcp 10.10.0.0 255.255.0.0 192.168.13.0 255.255.255.0 eq https*

Sljedeći korak jest konfiguriranje skupine ili objekta koji će predstavljati skupinu korisnika (slika 7) i stvaranje profila tunela (slika 8).

```
group-policy EASYVPN_GROUP internal
group-policy EASYVPN_GROUP attributes
 address-pools value EASYVPN_POOL
 default-domain value vpn.hr
 dns-server value 8.8.8.8
 pfs enable
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value EASYVPN_ACL
 vpn-idle-timeout 3600
 vpn-tunnel-protocol IPSec svc
```

Slika 7 *Group-policy*

Figure 7 *Group-policy*

Na vatrozidu omogućimo korisnicima da preuzmu program Cisco AnyConnect, natiramo uređaj do kojeg korisnici žele doći i specificiramo certifikate koji predstavljaju SSL certifikate na izlaznom sučelju.

```
tunnel-group EASYVPN_GROUP general-attributes
 default-group-policy EASYVPN_GROUP
tunnel-group EASYVPN_GROUP ipsec-attributes
 isakmp ikev1-user-authentication none
 trust-point CA_VPN
tunnel-group EASYVPN_GROUP webvpn-attributes
 authentication certificate
 group-alias vpn enable
 group-url https://firewall_A.vpn.hr/vpn enable
```

Slika 8 *Tunnel-group*

Figure 8 *Tunnel-group*

Prije instaliranja certifikata na vatrozid moramo generirati RSA ključeve za vatrozid i definirati certificate authority za vatrozid (slika 9).

- *crypto key generate rsa general-keys Label FIREWALL_A modulus 1024*

```
crypto ca trustpoint CA_VPN
 revocation-check crl none
 enrollment url http://caserver.vpn.hr
 fqdn firewall_A.vpn.hr
 subject-name CN=firewall_A,OU=vpn,O=vpn,C=hr
 no client-types
 crl configure
```

Slika 9 *Definiranje certifikata za vatrozid*

Figure 9 *Defining certificate for firewall*

Zatim dohvaćamo korijenski certifikat od CA (certificate authority) i dohvaćamo certifikat za vatrozid.

- *crypto ca authenticate CA_VPN*
- *crypto ca enroll CA_VPN*

Konfiguriraju se ISAKMP pravila sa naglaskom na autentikaciju putem digitalnog potpisa. Kad se pravila iskonfiguriraju trebaju se omogućiti na izlaznom sučelju (slika 10).

```
crypto isakmp policy 10
 authentication rsa-sig
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
```

Slika 10 *ISAKMP policy*

Figure 10 *ISAKMP policy*

Za kraj se postavljaju set transformacija i dinamična i statična kripto mapa koja se postavlja na izlazno sučelje (slika 11).

```
crypto ipsec transform-set EASYTS esp-aes-256 esp-sha-hmac
crypto ipsec security-association lifetime seconds 86400
crypto ipsec security-association lifetime kilobytes 460800
!
crypto dynamic-map EASYVPN_MAP 10 set transform-set EASYTS
!
crypto map EASYVPN_MAP2 ipsec-isakmp EASYVPN_MAP
crypto map EASYVPN_MAP2 interface outside
```

Slika 11 *Konfiguracija seta transformacija i dinamične i statične kripto mape*

Figure 11 *Configuration of transform-set and dynamic and static crypto map*

9. Zaključak

9. *Conclusion*

VPN je tehnologija za povezivanje dviju mreža koristeći enkripcijske protokole preko manje sigurne javne mreže. U početku, VPN je imao nekoliko mana, moralo se paziti koji se enkripcijski protokoli mogu koristiti na kojem operativnom sustavu i moralo se paziti na opterećenje koje konfiguriranje VPN-a stvara na vatrozide i usmjernike. Danas su te mane eliminirane korištenjem poznatih SSL i TLS enkripcijskih metoda i pojačanim procesorima vatrozida i usmjernika.

VPN možemo podijeliti na site-to-site VPN i Remote-access VPN. Glavna razlika između ta dva VPN-a jest da u site-to-site VPN-u korisnik nije svjestan postojanja VPN-a, a kod Remote-access VPN-a je svjestan jer mora upisati svoje korisničko ime i lozinku da bi povezao s drugom mrežom.

Primjerima site-to-site i Remote-access VPN-a je ukratko prikazano što se mora konfigurirati na vatrozidu da bi VPN uspješno funkcionirao. U budućnosti možemo očekivati samo još veća poboljšanja u korištenju VPN-a i njegovoj sigurnosti jer kako se stalno izmišljaju novi načini napada na sustave kompanija tako se smišljaju novi načini obrane protiv takvih napada. Najvrjednija stvar koju neka kompanija može posjedovati jest informacija koju je potrebno zaštititi, stoga VPN nikada neće izumrijeti.

10. Reference

10. *References*

[1] http://searchenterprisewan.techtarget.com/definition/virtual-private-network, 21.02.2016., Rouse Margaret

[2] https://static-course-assets.s3.amazonaws.com/CCNAS/index.html#8, https://www.netacad.com/, 22.02.2016.

[3] https://www.cactusvpn.com/beginners-guide-to-vpn/vpn-history/, 29.02.2016., Cactus VPN

[4] http://pcchip.hr/posao-i-financije/vpn-i-tehnologija-iza-njega/, 27.02.2016., Kubat Nenad

[5] http://study.com/academy/lesson/what-is-a-virtual-private-network-vpn-definition-types-quiz.html, 26.03.2016., Blackman Raymond

[6] https://technet.microsoft.com/en-us/library/cc771298(v=ws.10).aspx, 07.05.2016., Microsoft

[7] https://www.youtube.com/watch?v=vABIIJJftao, 06.03.2016., Vambar

[8] http://computer.howstuffworks.com/vpn4.htm, 02.04.2016., Tyson Jeff

AUTORI · *AUTHORS*

Dubravko Žigman – nepromjenjena biografija nalazi se u časopisu Polytechnic & Design Vol. 1, No. 1, 2013.

Korespodencija
dzigman@tvz.hr