PREGLEDNI RAD – REVIEW SCIENTIFIC ARTICLE 10.7251/ZRPIM2201449K

USPOSTAVA SIGURNE KOMUNKACIJE PUTEM SSL-VPN VEZE

Alen Kamiš

Visoka škola za uslužni biznis, Cara Lazara bb, 71350 Sokolac, Istočno Sarajevo, Bosna i Hercegovina, alen@vub.edu.ba

SAŽETAK

Naredni tekst predstavlja primjer iz prakse i kao takav ima veliku mogućnost primjene u radu i životu svakodnevnih korisnika. Uspostavom SSL-VPN veze korisnici pristupaju lokalnim resursima (LAN). SSL-VPN uspostavlja „sigurni tunel“ za konekaciju korisnika putem sigurne veze, a koji se nalaze van lokalne mreže, prema lokalnoj korisničkoj mreži. Primjena ovog rješenja ne mora izričito biti za poslovnu namjenu, već je primjenjiva i za svakodnevne potrebe i zadatke privatnih korisnika (na primjer: šahovski klub, gaming klub, i slično).

Ključne riječi: virtualna mreža, firewall, SSL-VPN konekcija.

UVOD

Trenutno u većini razvijenih zemalja vlada era značajne ekspanzije informatičke nauke i proizvoda. Veoma velika ulaganja su u sferi informatičke sigurnosti. Među najvećim ulaganjima su ulaganja u mrežnu sigurnost, pogotovo implementacije Firewall-a i sigurnih udaljenih veza (SSL-VPN).

Za implementaciju SSL-VPN virtualne veze potreban je Next-Generation Firewall (NGFW) uređaj. Firewall nove generacije (NGFW) je mrežni sigurnosni uređaj koji pruža mogućnosti izvan tradicionalnog firewall-a koji može da prati samo stanje sistema. Dok tradicionalni firewall obično pruža inspekciju stanja dolaznog i odlaznog mrežnog saobraćaja, firewall nove generacije uključuje dodatne funkcije kao što su svijest o aplikacijama i kontrola, integrirana prevencija upada i obavještavanje o prijetnjama koje se isporučuju iz oblaka (cloud) (Cisco, 2021).

NEXT-GENERATION FIREWALL I SSL-VPN VIRTUALNA MREŽA (SSL-VPN)

Next-Generation Firewall (NGFW) uređaj ima sve karakteristike osnovnog firewall-a plus neke ili sve dodatne karakteristike navedene u daljem tekstu.

Važno je napomenuti da svi dobavljači NGFW-a ne nude sve navedene funkcije, a ponekad se funkcije nazivaju i drugačijim imenima. Neki dobavljači zahtijevaju i skupe dodatne licence za neke od funkcija. A ponekad su funkcije isporučene pomoću usluge u oblaku, a ne unutar samog Next-Generation Firewall-a. Prilikom odabira veoma je bitno da dobavljač i kupac povedu računa o licenciranju i izboru NGFW rješenja.

Neke od najvažnijih uloga koje Next-Generation Firewall (NGFW) uređaj može da obavlja su:

Geolokacija - mogućnost povezivanja IP adresa sa fizičkim geolokacijama, odnosno državama. Umjesto da su podešeni određeni IP range-ovi koje korisnik želi da zabrani ili dopusti, uz pomoć navedene opcije moguće je odrediti zemlju (npr. zabraniti otvaranje stranica čija se IP adresa nalazi u Sjevernoj Koreji ili nekoj drugoj državi).

IDS/IPS - sistemi za detekciju ili prevenciju upada koji gledaju sadržaj paketa koji prolaze kroz firewall i pokušavaju uočiti stvari koje izgledaju kao napadi. U većini slučajeva, IDS/IPS uređaji koriste potpise (signature) za otkrivanje poznatih napada. Oni također traže generičke vrste napada, koji su manje zavisni od potpisa. Budući da se novi napadi stalno pojavljuju, IDS/IPS uređaji s vremenom postaju manje korisni osim ako su njihovi potpisi redovno ažurirani. Ovo obično zahtijeva uslugu pretplate kod proizvođača opreme.

Antivirus/anti-malware zaštita - kako se datoteke učitavaju ili preuzimaju, iste prolaze kroz firewall koji može obaviti osnovni pregled. U većini slučajeva, ovo će biti analiza zasnovana na potpisu, gledanje kontrolnih hash-ova i skeniranje bajtova koji su već viđeni u poznatom

zlonamjernom softveru u prošlosti. Ova funkcija zahtijeva da datoteke nisu šifrirane i da firewall ima redovno ažurirane definicije.

Sandbox - bolji oblik skeniranja zlonamjernog softvera. U pitanju je u suštini virtualna mašina (VM) koja pokreće zajednički targetirani operativni sistem kao što je Windows. Firewall presreće preuzimanje fajla i šalje ga u sandbox VM gdje se vrši provjera, što znači da VM pokušava da pokrene datoteku kao da je targetirani računar. Sandbox zatim traži uobičajene tipove zlonamjernog ponašanja kao što je povezivanje s komandnim i kontrolnim (C&C) mrežama. Nakon što je datoteka analizirana, VM je bezbjedno obrisana i kreirana je nova. U nekim slučajevima, sandbox je zaseban hardware-ski box koji se nalazi u izdvojenom djelu mreže (DMZ). U drugim slučajevima, to je usluga u oblaku.

Web proxy i provjera URL-a - još jedna korisna funkcija koja je često uključena u firewall nove generacije. Ista ili vrši provjeru URL-a, ili služi kao potpuna web proxy usluga. Web proxy se nalazi usred šifrirane HTTPS sesije. Za računar za pregledavanje web-a, on se pretvara da je web server. Za web server se pretvara da je pretraživač. Na ovaj način, proxy može dešifrovati HTTPS sesiju u oba smjera i vidjeti šta se tačno događa, sa očekivanjem da će otkriti bilo kakvu zlonamjernu aktivnost.

Obrnuti proxy (Reverse Proxy) – funkcija slična proxy-ju, s tim da umjesto da je radnja izvršena ispred web pretraživača štiteći ga od mnogih web stranica, ova funkcionalnost se nalazi ispred web servera štiteći ga od mnogih pretraživača. Obrnuti proxy sadrži SSL certifikate za web server i oslobađa ga SSL funkcionalnosti.

Web Application Firewall (WAF) - sofisticiranija verzija obrnutog proxy-ja. WAF sprovodi analizu HTTP i HTTPS ponašanja objavljenih servisa na Internetu. Obično je implementirano dešifrovanje HTTPS paketa i prosleđivanje istih na web server kao standardni HTTP saobraćaj. WAF sadrži SSL certifikate za web server. Na ovaj način, WAF je u mogućnosti da u potpunosti pregleda sadržaj svakog paketa.

Balansiranje saobraćaja - Next-Generation Firewall (NGFW) uređaji uključuju i funkciju balansiranja opterećenja. Opcija se veoma često koristi u data centrima, te za implementaciju udaljenih VPN lokacija. Jedna od najpopularnijih opcija balansiranja saobraćaja je SD-WAN.

Visoka dostupnost sistema - većina NGFW uređaja podržava opciju spajanja dva ili više uređaja u visoko dostupni sistem (cluster). Cluster može raditi u active/active ili active/pasive mode-u.

SSL-VPN je protokol koji šifrira podatke i osigurava nesmetan protok podataka s dodatnim slojem sigurnosti, čineći isti sigurnijim i neprobojnijim.

Jedna od najboljih prednosti SSL-VPN-a je ta što omogućava udaljeni pristup ograničenim informacijama, bez obzira na geografski položaj i web preglednik ili aplikaciju koja je korištena. To znači da SSL-VPN u suštini ne zahtijeva nikakvu instalaciju na korisnikovom sistemu (ako se koristi web portal). SSL-VPN omogućava siguran pristup i kritičnim administrativnim informacijama.

SSL VPN-ovi se oslanjaju na TLS protokol, koji je zamijenio stariji SSL protokol, kako bi osigurali daljinski pristup. SSL VPN-ovi omogućavaju autentikovanim korisnicima da uspostave sigurne veze na interne HTTP i HTTPS usluge putem standardnih web pretraživača ili klijentskih aplikacija koje omogućavaju direktan pristup mrežama.

Postoje dvije osnovne vrste SSL VPN-ova: VPN portal i VPN tunel. SSL portal VPN omogućava jednu po jednu SSL VPN vezu s udaljenim web lokacijama. Udaljeni korisnici pristupaju SSL VPN gateway-u sa svojim web pretraživačem nakon što su provjereni putem metode koju gateway podržava. Pristup je ostvaren putem web stranice koja služi kao portal za druge usluge.

SSL tunel VPN omogućava korisnicima siguran pristup višestrukim mrežnim uslugama putem standardnih web pretraživača, kao i drugih protokola i aplikacija koje nisu zasnovane na web-u. VPN tunel je veza uspostavljena između udaljenog korisnika i VPN servera; server istovremeno može biti povezani na jednu ili više udaljenih web stranica, mrežnih usluga ili resursa u ime klijenta. SSL tunelski VPN zahtijeva od web pretraživača da rukuje aktivnim sadržajem i pruži funkcionalnost koja inače nije dostupna putem VPN-a SSL portala.

Prednosti Next-Generation Firewall i SSL-VPN su velike a neke od njih su:

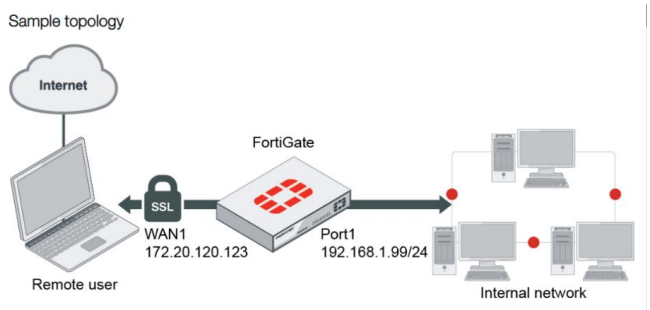
- Velika sigurnost veze i uređaja koje dobijene kroz zaštite ugrađene u firewall
- Korištenje standardnog HTTPS protokola TCP 443
- Nije potrebna instalacija klijenta pri korištenju web portala
- Jednostavna instalacija i konfiguracija iz koje proizilazi ušteda u vremenu
- Nije potrebna dnevna administracija, već po potrebi
- Veoma veliki forum korisnika i dijeljenje znanja i iskustva
- Dostupnost SSL-VPN klijenta za sve software-ske platforme (desktop i mobile)
- Otvoreno povezivanje sa ostalim sistemima, pomoću API-a ili RestFul API-a
- Automatski monitoring, reporting i alerting
- Nedostaci Next-Generation Firewall i SSL-VPN su uglavnom vezani za trošak, a to su:
- Cijena Next-Generation Firewall
- Cijena za update servise (IPS/IDS, web filtering, sandbox itd.).

Za implementaciju ovog zadatka, ili bolje reći rješenja, potreban na je Next-Generation Firewall. Uzimajući u obzir odnos kvalitete, pouzdanosti i podrške, izdvajaju se tri proizvođača opreme a to su: Palo Alto, FortiNet i Check Point. Isti proizvođači su prepoznati kao lideri u Gartner magičnom kvadrantu u polju Network Firewall.

U ovom tekstu korišten je FortiGate 60F uređaj, a slične ili identične komande koriste se i kod drugih proizvođača.

FortiNet je lider u Enterprise Security segmentu u mrežnim komunikacijama. FortiNet rješenja poboljšavaju performanse, povećavaju zaštitu i vidljivost, a istovremeno smanjuju troškove downtime (nedostupnosti sistema) i održavanja.

Na sljedećoj slici prikazan je primjer implementacije SSL VPN.



Slika 1. Prikaz primjera SSL VPN veze (Fortinet Document Library, 2022).
Figure 1. Display of an example of an SSL VPN connection (Fortinet Document Library, 2022).

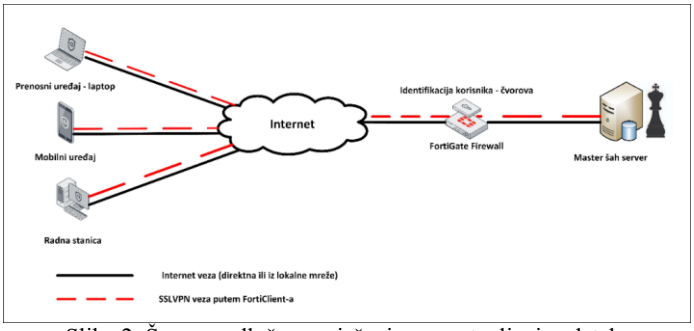
Za implementaciju SSL-VPN na FortiGate uređajima potreban je FortiClient VPN software, dostupan besplatno za sve poznate platforme: računare – desktope (Windows, Linux i MacOS) kao i mobilne uređaje i tablete (Android, Apple iPhone i iPad).

Uređaj posjeduje napredne servise kao što su: web filtering, IPS potpis, antivirusna zaštita itd. Sve navedeno znatno pomaže prilikom unapređenja sigurnosti. Firewall politikama može na veoma jednostavan način biti definisana tzv. ACL (Access Control List), odnosno do koje tačke krajnji korisnik, koji se povezuje putem SSL-VPN konekcije, može da pristupi u lokalnoj mreži. Firewall politikama može biti definisano i dozvoljeno vrijeme pristupanja korisnicima i naravno zabrana pristupanja u određenim terminima ili slučajevima.

Autorizacija SSL-VPN korisnika može biti izvršena lokalno na samom firewall uređaju (lokalni korisnici na firewall-u) ili na AD-u (Microsoft Active Directory), LDAP serveru ili NPS Serveru (Network Policy Server).

Kroz ovaj tekst obrađena je cjelokupna konfiguracija SSL-VPN FortiNet uređaja i pristupnih čvorova (primjeri za računar i mobitel). Uključeni su i primjeri kojima je prikazana mogućnost komunikacije i zabrana iste prema lokalnoj mreži (master šah server).

Na sljedećoj slici je prikaz kompletnog predloženog rješenja a u narednom tekstu nalazi se opis konfiguracija koje su neophodne za kreaciju istog.



Slika 2. Šema predloženog rješenja za postavljeni zadatak.
Figure 2. Scheme of the proposed solution for the task.

Konfiguracija uređaja

Cjelokupan konfiguracijski kod je objavljen na: https://github.com/alenkamis/NGFirewall (Kamiš, 2022) i kao takav je dostupan svim korisnicima kao primjer konfiguracije. U daljem tekstu objašnjen je postupak konfiguracije bez konfiguracijskog koda.

Kreiranje interface-a i statičke route

Konfiguracija započinje podešavanjem adresa na WAN (Internet) i LAN (lokalna mreža) interface-ima.

Konfiguracija WAN interface-a može biti definisana na više načina (statička IP adresa, DHCP ili PPPOE) u zavisnosti od usluge koji nudi ISP (Internet Service Provider). Konfiguracija LAN interface-a predstavlja vezu firewall-a sa lokalnom mrežom.

Da bi korisnicima (lokalnim korisnicima ili remote SSL-VPN korisnicima) bio omogućen pristup potrebno je konfigurisati statičke route za komunikaciju lokalnih korisnika prema default gateway-u ISP-a.

Konfiguracija DHCP-a

Da bi korisnici automatski dobili IP adrese u lokalnoj mreži, potrebno je izvršiti konfiguraciju DHCP (Dynamic Host Configuration Protocol). DHCP server lokalnim korisnicima automatski dodjeljuje IP adrese u rasponu od 192.168.1.110 do 192.168.1.210. Pored IP adrese automatski je dodijeljen default gateway 192.168.1.99 i DNS serveri 8.8.8.8 i 8.8.4.4 (Google javni DNS serveri),

Kreiranje Adresa i VIP adresa

Kako bi firewall security policy bilo lakše konfigurisati, potrebno je za IP i VIP adrese uvesti aliase u obliku imena. VIP adresa koristi kod public-ovanja servisa (na primjer web servera prema Internetu).

Konfiguracija dinamičkog DNS

Da bi virtualna mreža lakše bila uspostavljena, i da ne bi javna IP adresa morala biti upamćena, uveden je DNS (Domain Name System) servis, odnosno uvodimo FQDN (Fully Qualified Domain Name) ili uvodimo jedinstveno ime po kojem je ovaj firewall čvor jedinstven. Većina WAN IP adresa korisnika u svijetu nije statička i mijenja se unutar par sati iz razloga velikog nedostatka IP adresa. Tada nije idealno koristiti DNS servis jer je isti statičan, već se koristi Dinamički DNS servis koji automatski osvježava zapise trenutne WAN IP adrese. Za potrebe ovog rada kreiran je dinamički DNS zapis alfatest.fortiddns.com koji će biti korišten prilikom konfiguracije virtualne mreže.

Konfiguracija certifikata

Nakon što je implementiran dinamički DNS, potrebno je izvršiti konfiguraciju certifikata za dinamičko DNS ime: alfatest.fortiddns.com. Izdavanjem letsencrypt certifikata za ime alfatest.fortiddns.com i primjenom istog na firewall uređaj, sam uređaj neće više prijavljivati greške da certifikat nije validan ili da njegovo ime nije tačno.

Kreiranje SSL-VPN korisnika

Da bi korisnici mogli uspješno ostvariti vezu sa virtualnom VPN mrežom, potrebno je da imaju univerzalne identifikatore u vidu korisničkog imena i šifre (password-a). Svakom korisniku (ukupno pet) dodijeljen je username i password koji je unikatan za svakog od njih. Pored toga kreiran je i korisnik koji ima puna prava na cijeloj mreži.

Kreiranje Grupa

Radi lakšeg administriranja, upravljanja, te da ne treba dodavati pojedinačno korisnike, kreirane su grupe za VPN i to „VPN korisnici“ - korisnici koji mogu samo komunicirati samo sa samim sobom i serverom, kao i „Full-Access“ grupa koja ima puni pristup računarskoj mreži.

Kreiranje SSL-VPN portala

Kreiranjem SSLVPN portala postiže se mogućnost spajanja udaljenih korisnika na lokalnu mrežu. Za ove potrebe kreirana su tri SSL-VPN portala.

„Full-access“ ima mogućnost spajanja putem sljedeća dva mode-a:

Web - pristup gdje je konfigurisan samo Web mode, a ugašen Tunnel mode.

Tunnel - pristup gdje je konfigurisan samo Tunnel mode, a Web mode ugašen.

Web mode je SSL-VPN gdje krajnji korisnik dobije pristup Web portalu te može otvarati druge aplikacije i Web stranice koje se nalaze unutar lokalne mreže. Web portal nije baš najpopularnije rješenje zbog ograničenja lokalne aplikacije (aplikacije koju otvara), na primjer otvaranje Java ili Flash.

Tunnel mode je puno bolja opcija i kroz nju se definišu osnovni parametri za SSL-VPN, kako će korisnik koristiti Internet, lokalne aplikacije, da li može pohraniti password i još dosta drugih opcija.

Konfiguracija SSL-VPN postavki

U sljedećem tekstu prikazan je cjelokupni kod konfiguracije SSL-VPN postavki. Kroz kod se jasno vide ranije definisani objekti, dinamička DNS adresa, VPN adresni pool, ssl-VPN portal, itd.

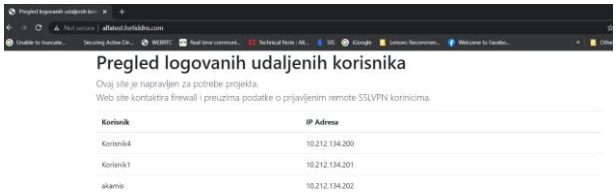
Konfiguracija firewall policy

Da bi SSL-VPN veza bila uspostavljena, te ostvario pristup tačno definisanim lokalnim resursima (na primjer server), potrebno je napraviti policy za SSL-VPN korisnike. Na Firewall policy definisana su i ostala pravila pristupa lokalnoj mreži, serverima i Internetu.

Kreiranje Web site-a za evidenciju SSL-VPN korisnika

U svrhu evidencije udaljenih korisnika (SSL-VPN) kreirana je Web stranica koja preuzima podatke sa firewall-a i svakih 20 sekundi objavljuje iste. Navedena Web stranica može biti potpuno integrisana u bilo koji Web site ili Web aplikaciju različite namjene.

Na sljedećoj slici je prikazan izgled Web stranice sa trenutno konektovanim SSL-VPN korisnicima.



Slika 3. Prikaz povezanih SSL-VPN korisnika na Web stranice.
Figure 3. Display of connected SSL-VPN users on Web pages.

ZAKLJUČCI

Ovaj rad predstavlja samo jedan primjer koji se može koristiti za razne namjene. Implementacija SSL-VPN rješenja napravljena je na FortiNet uređaju, trenutno lideru u oblasti mrežne sigurnosti (Next- Generation Firewall). U tekstu je postavljen link gdje su dostupne sve potrebne komande kako bi SSL-VPN bio uspješno implementiran. Veoma slične komande i logika bile bi korištene i na ostalim Next- Generation Firewall uređajima od drugih proizvođača. Na taj način predočen je dobar šablon za početnike kako bi sami mogli izvršiti konfiguraciju SSL-VPN-a.

Pored implementacije SSL-VPN-a, napravljena je i Web stranica koja u svakom momentu prikazuje koji udaljeni korisnici su spojeni na Next-Generation Firewall putem SSL-VPN klijenta.

Rješenje, zasnovano na Next-Generation Firewall-u i SSL-VPN virtualnoj mreži, primjenjivo je, i prvenstveno namijenjeno, za enterprise korisnike kojima je potrebna sigurnost, ali isto tako može biti primjenjivo i za manje korisnike, budući da izvedbe uređaja dolaze u više modela, odnosno od entry-level pa sve do high-end nivoa.

LITERATURA

Fortinet Document Library. (n.d.). SSL VPN split tunnel for remote user | Administration Guide. Preuzeto 29. 10. 2021. sa https://docs.fortinet.com/document/fortigate/7.0.4/administration-guide/307303/ssl-vpn-split-tunnel-for-remote-user

Cisco. (2021). What Is a Next-Generation Firewall. Preuzeto 29. 10. 2021. sa https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-next-generation-firewall.html

Kamis, A. (2022). Konfiguracijski kod - Prilog.pdf. GitHub - Alen Kamis. Preuzeto 03. 03. 2022. sa https://github.com/alenkamis/NGFirewall/blob/main/Prilog.pdf

ESTABLISHING SECURE COMMUNICATION USING SSL VPN

Alen Kamiš

The College of Service Business, Cara Lazara bb, 71350 Sokolac, East Sarajevo, Bosnia and Herzegovina, alen@vub.edu.ba

ABSTRACT

A following text represents a real life sample and as such it has a large possibility for use and everyday life. By setting up SSL-VPN connection, users can have access to local resources (LAN). SSL-VPN uses safe connections and creates a “safe tunnel” for clients to communicate from outside of local network to the local user network. Application of this solution does not necessarily have to be for a business needs, it is also applicable to the everyday needs of private users (for example: chess club, gaming club, etc.).

Keywords: virtual network, firewall, SSL-VPN connection.