Pregled karakteristika ISA servera

Siniša Lale

Sadržaj – Aktuelni vremenski trenutak, koji karakteriše eksplozija Internet komunikacija, sa istovremenim porastom sigurnosnih rizika, nameće potrebu za korišćenjem bezbednosnog proizvoda koji bi bio postavljen na „ivicu“ mreže. Microsoft Internet Security and Acceleration Server 2006 je takav proizvod. Poseduje nekoliko ključnih bezbednosnih funkcija, upotrebljivost, jednostavnost korisničkog interfejsa i skalabilnost, posebno ako se koristi Enterprise edicija. Ovaj dokument istražuje ključna svojstva pomenutog proizvoda, neophodna za uspešan rad servera u realnim uslovima eksploatacije.

Ključne reči – bezbednost, ISA server, mrežna barijera, proksi.

I. UVOD

Naporedo sa aktuelnim porastom obima Internet komunikacija, web servisi postaju zahtevniji u pogledu utroška mrežnih resursa, sofisticiraniji u funkcionalnom i estetskom smislu ali istovremeno dolazi i do porasta sigurnosnih rizika prilikom svakodnevnog korišćenja ovih servisa. Za većinu preduzeća, sa adekvatnim budžetom, koja se u svakodnevnom poslovanju oslanjaju ili potpuno zavise od informacija transportovanih preko javne TCP/IP infrastrukture, obavezno je korišćenje bezbednosnog proizvoda koji se može postaviti na „ivicu“ lokalne mreže prema javnoj infrastrukturi. Microsoft Internet Security and Acceleration Server 2006, u daljem tekstu ISA server, je upravo takav, softverski proizvod. Postoji naravno i čitav niz konkurentskih, što hardverskih, što softverskih proizvoda kao što su [1]: Cisco PIX, Juniper Networks NetScreen, SonicWall, Watchguard, Symantec Enterprise Firewall, Blue Coat Systems ProxySG, kao i open source mrežne barijere IPchains, Juniper FWTK, IPCop.

Ovaj rad treba da prikaže osnovne karakteristike ISA servera kao i da sugeriše na njihovu upotrebnu vrednost u praktičnim situacijama. U poglavlju II, dati su najosnovniji preduslovi za razumevanje Microsoft-ovih mreža a ostala poglavlja predstavljaju izdvojivu i opisivu funkcionalnu celinu ISA servera.

S. Lale, CET - Computer Equipment and Trade, Knez Mihailova 6, 11000 Beograd (email: lalas@cet.co.rs)

II. KLASIFIKACIJA MREŽA

Prema klasifikaciji firme Majkrosoft, računarske mreže se dele na radne grupe i domene. Osnovni kriterijum ove podele je vrsta baze podataka koja, između ostalog, sadrži informacije o korisnicima mreže. Ove informacije se koriste za proveru identiteta korisnika a nakon ustanovljenja identiteta koriste se za autorizaciju pristupa resursima.

Radna grupa je logička grupa računara koju karakteriše jedino zajedničko ime. Ona nema nikakve bezbednosne karakteristike. Svaki računar koji pripada radnoj grupi oslanja se isključivo na lokalnu bazu podataka koja se naziva Security Accounts Manager, skraćeno SAM. Prema tome, korisnički nalozi, čije se informacije ovde nalaze, nazivamo lokalnim nalozima.

Domen je logička grupa mrežnih objekata koji dele zajedničku bezbednost. Odnosno, korisnici i računari se oslanjaju na zajedničku bazu podataka koja omogućava verifikaciju identiteta, a u kombinaciji sa drugim bezbednosnim tehnologijama i autorizaciju pristupa resursima. Promocijom proizvoljnog Windows servera u tzv. kontroler domena, obavlja se instalacija replike baze podataka na neki računar. Tehnologija baze podataka je Active Directory, u daljem tekstu Aktivni direktorij, a čine je u osnovi dva servisa: LDAP i Kerberos. Korisnički nalozi, smešteni u ovu bazu podataka, nazivaju se domenskim korisničkim nalozima.

Treba napomenuti da pripadnost računara domenu ne negira potencijalno korišćenje lokalne SAM baze podataka osim na kontrolerima domena.

III. EDICIJE ISA SERVERA

ISA server se distribuira u dva odvojena pakovanja: Standard Edition i Enterprise Edition, u daljem tekstu Standardna i Enterprise edicija. Platforma za instalaciju je Windows Server 2003.

Standardna edicija je namenjena malim i srednjim preduzećima odnosno takvim okruženjima u kojima uslovi eksploatacije, mogućnosti ili ograničena materijalna sredstva ne opravdavaju ulaganja u Enterprise ediciju. Takođe se može koristiti i za udaljene lokacije velikih kompanija. Oslanja se na lokalnu registarsku bazu podataka za potrebe smeštaja konfiguracionih informacija.

Enterprise edicija je namenjena prevashodno velikim preduzećima odnosno lokacijama sa stotinama ili hiljadama korisnika. Idealna je za ona mrežna okruženja čiji su imperativi redundantnost servisa, jednostavno konfigurisanje farmi servera, neprimetno uklanjanje ili dodavanje pojedinačnih članova farme i skalabilnost, nasuprot ceni, koja je značajno veća u odnosu na standardnu ediciju, orijentaciono 3-4 puta.

Ova edicija se oslanja na specifičan LDAP servis, tzv. Active Directory Aplication Mode - ADAM, za potrebe centralizacije smeštaja i redundantnosti konfiguracionih podataka. To je posebna, limitirana verzija

tehnologije Aktivnog direktorijuma koja se, poput MySQL servera, može slobodno i besplatno koristiti za potrebe aplikacionog direktorijuma. Korišćenje ADAM tehnologije obezbeđuje nezavisnost implementacije Enterprise edicije u odnosu na domensko okruženje. Pojedinačnim ISA serverima se konfiguracija distribuira kao pripadnicima odgovarajuće farme servera iz centralne konfiguracione baze podataka. Na kraju, ova konfiguracija završava u registarskoj bazi lokalnog računara.

IV. FUNKCIJE ISA SERVERA

ISA server obezbeđuje sledeće osnovne funkcionalnosti bez obzira na ediciju[2]: mrežna barijera (Firewall), proksi server (Proxy), NAT server, VPN server. Pored pomenutih, Enterprise edicija obezbeđuje sledeće funkcionalnosti[2][3]: Active Directory Application Mode - ADAM, Cache Array Routing Protocol - CARP, Network Load Balancing - NLB.

Pored ovako nabrojanih glavnih funkcija, ISA server poseduje podršku za keširanje internet sadržaja preko HTTP i FTP protokola, vremenski programirano pokretanje dialup veza, minimalan Intrusion Detection System - IDS, a poseduje i podršku za praćenje rada i statistiku korišćenja itd. Treba naglasiti da su servisi mrežne barijere srce funkcionalnosti ISA servera.

V. MREŽNI OBJEKTI I MREŽNA PRAVILA

Mrežni objekti su suština objektno orijentisanog koncepta razumevanja strukture fizičke mreže od strane ISA servera. Između nekih vrsta mrežnih objekata se, prema tabeli 1, uspostavljaju mrežna pravila koja definišu relacije rutiranja ili translacije IP adresa. Postojanje mrežnog pravila između mrežnih objekata je preduslov komunikacije između računara u različitim fizičkim mrežama koje reprezentuju, kroz ISA server. Tačnije, u pitanju je potreban ali ne i dovoljan uslov za odvijanje komunikacije.

Njihove karakteristike i funkcionalnost su opisani u sledećoj tabeli.

Mrežni objekat	Reprezentuje	Rel
Computer	Jednu IP adresu.	Da
Address Range	Jedan opseg IP adresa.	Da
Subnet	Jedan IPv4 subnet.	Da
Computer Set	Skup objekata tipa Computer, Address Range ili Subnet.	Da
Nework	Više opsega IP adresa.	Da
Network Set	Skup objekata tipa Network.	Da
URL Set	Skup URL-ova.	Ne
Domain Name Set	Skup imena Internet domena.	Ne
Web Listener	IPv4 adresu osluškivanja dolaznog saobraćaja.	Ne

Tabela 1. Mrežni objekti na ISA serveru 2006 i njihove funkcije.

Takođe postoje predefinisani, odnosno podrazumevani, mrežni objekti. Dokumentovani su u narednoj tabeli.

Mrežni objekat	Tip	Reprezentuje
External	Network	Internet.
Internal	Network	Lokalnu mrežu.
Local Host	Network	ISA server.
VPN Clients	Network	VPN klijente.
Quarantined VPN Clients	Network	VPN klijente bez adekvatne bezbednosne konfiguracije (u karantinu).
All Networks	Network Set	Sve podrazumevane objekte tipa Network.
All Protected Networks	Network Set	Sve podrazumevane objekte tipa Network osim External.

Tabela 2. Podrazumevani mrežni objekti na ISA serveru 2006.

Adresni opseg objekta Internal se praktično definiše u toku instalacije ISA servera. Mreže „VPN Clients“ i „Quarantined VPN Clients“ su dinamičke, odnosno adrese se dodaju i uklanjaju kako VPN klijenti uspostavljaju i raskidaju veze.

Odnosi između mrežnih interfejsa i mrežnih objekata se mogu opisati na sledeći način:

- intefejs pripada jednom mrežnom objektu,
- interfejs ne može spadati u dva ili više mrežnih objekata,
- sve IP adrese „iza“ mrežnog interfejsa servera su deo iste mreže,
- sve IP adrese koje nisu definisane na ISA serveru se smatraju delom mreže External.

Sav mrežni saobraćaj koji se kreće između mreža reprezentovanih ovim objektima je predmet inspekcije saobraćaja. Podrazumevana konfiguracija ISA servera je takva da praktično nema komunikacije sve dok ne postoje:

- mrežna pravila koja određuju mreže između kojih je dopuštena komunikacija, odnosno relaciju rutiranja ili translacije adresa,
- pravila mrežne barijere koja određuju vrste saobraćaja kojima se dopušta komunikacija, odnosno koja dodatno preciziraju adrese između kojih je dopuštena komunikacija.

VI. PREDEFINISANI ŠABLONI

Šabloni na ISA serveru omogućavaju automatsko definisanje mrežnih pravila i mrežnih objekata prema scenariju korišćenja ISA Servera. Ovo ozbiljno skraćuje vreme neophodno za konfigurisanje servera. Scenariji korišćenja su dati u sledećoj tabeli.

Šablon	Opis
Edge Firewall	Prevashodna namena ISA servera u ovom scenariju je bezbedan pristup klijenata na Internet. Moguće je vršiti publikaciju servisa.
3-Leg Firewall	ISA server ima tri mreža adaptera. Jedan od adaptera je deo tampon zone. Publikovani servisi su smešteni u subnet tampon zonu.
Front Firewall	ISA server se koristi u scenariju sa dve mrežne barijere. Front firewall je izložen direktno Internetu i povezan na tampon zonu.
Back Firewall	ISA server se koristi u scenariju sa dve mrežne barijere. Back firewall je na granici tampon zone i mreže sa klijentima. Ovo je najrealnija uloga ISA servera u konfiguraciji sa dve mrežne barijere.
Single Network Adapter	Ovde ISA server ima samo jedan mrežni adapter i najčešće se koristi kao proksi/keš.

Tabela 3. Scenariji korišćenja ISA server – Šabloni

VII. PROKSI SERVISI

Proksi servisi se, prema definiciji, nalaze između klijenta i servera i posreduju u komunikaciji. Klijent i server ne vrše direktnu komunikaciju već preko proksi servera kao posrednika. ISA server obezbeđuje proksi servis za korisnike HTTP i SSL protokola, takozvani veb proksi. Dodatni sadržaji koji su podržani u vezi veb proksi servisa su: keširanje sadržaja, autentifikacija korisnika, filtriranje klijentskih zahteva, inspekcija tekućeg saobraćaja kao i snimanje rezultata inspekcije. Podržan je bilo koji HTTP 1.1 CERN kompatibilni klijentski program. U narednoj tabeli dat je pregled autentifkacionih metoda koje podržava ISA server u ulozi veb proksija.

Autentifikacioni metod	Opis
Basic	RFC 2617
Digest	RFC 2617
Integrated Windows	Koristi Kerberos ili NTLM protokol, podržava Internet Explorer 2.0 ili noviji
RADIUS	ISA server se oslanja na RADIUS server u procesu autentifikacije klijenta
Digital Certificate	Može da se koristi u autentifikaciji kod lančanja proksi servera

Tabela 4. Podržani autentifikacioni metodi veb proksi servisa.

Lančanje proksi servera je posebno zanimljivo svojstvo veb proksi servisa. Namenjeno je situaciji u kojoj preduzeće ima više proksi servera na udaljenim lokacijama pri čemu se svi zahtevi usmeravaju preko jedne veze, smeštene na centralnoj lokaciji. Važna prednost ovakve konfiguracije je korišćenje kumulativnog keša na serverima koji su deo lanca.

ISA server se može koristiti i kao SOCKS V4 proksi, mada ovo, razumljivo, iz perspektive Microsoft-a, nije podrazumevana konfiguracija.

VIII. PRAVILA MREŽNE BARIJERE

ISA server razlikuje nekoliko tipova pravila komunikacije. Podrazumevana konfiguracija je takva da se blokira sva komunikacija između računara na različitim mrežama kroz ISA server. U stvari, postoji podrazumevano pravilo koje se naziva „Default Rule" koje blokira komunikaciju koja potiče sa mreže „All Networks" na mrežu „All Networks".

U narednoj tabeli je dat opis i namena pravila mrežne barijere.

Vrsta pravila	Opis
Access Rules (pristupna pravila)	Vrsta pravila komunikacije koja omogućava tok saobraćaja između dve mreže definisane mrežnim objektima kroz ISA server kao posrednika. Primarno su namenjena publikaciji Internet resursa lokalnim korisnicima ili međusobnoj komunikaciji između zaštićenih mreža.
System Policy (sistemske politike)	Pravila komunikacije za različite administrativne funkcije ISA servera. Na primer, pravilo „Microsoft Management Console“ omogućava komunikaciju administrativne MMC aplikacije sa ISA serverom. Manuelno definisanje ovakvih pravila bi znatno usporilo proces konfigurisanja ISA servera.
Publishing Rules (pravila publikacije)	Vrsta pravila komunikacije koja su namenjena primarno publikovanju lokalnih resursa spoljnim korisnicima. U odnosu na pristupna pravila, mogu publikovati samo jedan server. Takođe neke vrste aplikacionog filtriranja su dizajnirane samo za ovu vrstu pravila a ne i za pristupna pravila npr. SMTP filter.

Tabela 5. Vrste pravila mrežne barijere.

Osnovni elementi konfiguracije pristupnih pravila su dati u narednoj tabeli.

Element konfiguracije	Opis
Action	Allow/Deny, dopušta ili zabranjuje vrstu saobraćaja.
Protocols	Omogućava selekciju objekta koji reprezentuje protokol koji se propušta ili zabranjuje pravilom zajedno sa parametrima broja izvornog i odredišnog porta.
From	Mreža sa koje potiče saobraćaj.
To	Mreža kojoj je namenjen saobraćaj.
Users	Omogućava selekciju objekta koji reprezentuje grupu korisnika. Grupe mogu biti predefinisane ili se kreirati po potrebi. Omogućavaju korišćenje autententifikacije korisnika prilikom korišćenja pravila.
Schedule	Definiše vremenski interval dostupnosti pravila.
Content types	Tipovi sadržaja koji se mogu transportovati preko HTTP protokola.

Tabela 6. Elementi konfiguracije pristupnih pravila.

Pravila publikacije se bitno razlikuju prema tome kakva vrsta servera se publikuje, na primer „Mail Server Publishing Rule“ ili „Web Site Publishing Rule“. Nazivi su samoopisni. Redosled pravila se može konfigurisati. Sva pravila se, bez obzira na vrstu, procesiraju sekvencijalno od strane ISA servera u momentu primanja zahteva, od pravila sa rednim brojem 1 do eventualno poslednjeg. Osnovni kriterij primene pravila je IP adresa izvora i odredišta. Odnosno, server procesira pravila sve dok ne naiđe na pravilo čiji se parametri izvorišta i odredišta poklapaju sa klijentovim zahtevom. Navedeno pravilo se primenjuje na klijenta, sa svim ostalim parametrima. U tom slučaju ostala pravila se ne uzimaju u obzir.

Pravila mrežne barijere, očigledno imaju primarnu funkciju definisanja paketnog filtera i eventualno aplikacionog filtera.

IX. VRSTE FILTRIRANJA SAOBRAĆAJA

ISA server podržava sledeće vrste filtriranja saobraćaja: paketno filtriranje, aplikaciono filtriranje i filtriranje sa uspostavom stanja[4]. Paketno filtriranje je opisano u delu „Pravila mrežne barijere”. Aplikaciono filtriranje je podrazumevano ograničeno na određen skup podržanih protokola kao što su HTTP, SMTP, DNS. Postoje čak i mnogi specifični aplikacioni filteri čija uloga je prosto obezbeđivanje funkcionalnosti. Filter za FTP saobraćaj, na primer, automatski obezbeđuje sve funkcije za komunikaciju sa FTP serverom bez obzira na režim rada, pasivni ili aktivni. Prilikom definisanja pristupnog pravila ili pravila publikacije za FTP servis, potrebno je odrediti samo port 21 kao odredišni port. Ostatak posla, na primer publikaciju porta 20 u smeru ka klijentu kod aktivnih veza, obezbeđuje aplikacioni filter automatski.

Filtriranje sa uspostavom stanja se odnosi na analizu TCP veza i obezbeđuje da je sav saobraćaj koji teče kroz ISA server deo postojeće TCP sesije. ISA takođe sprečava napade na tzv. „Three way handshake“ proces.

X. VPN SERVISI

Kada su u pitanju VPN servisi, ISA server se može koristiti u dva scenarija: kod direktnog pristupa korisnika na mrežu – „VPN clients“ scenario i kod povezivanja lokacija – „Site-to-Site“ scenario. Podržani VPN protokoli su PPTP i L2TP a u scenariju povezivanja lokacija podržan je i IPSec u tunelskom režimu rada.

U procesu autentifikacije VPN veza, ISA server podržava PAP, SPAP, CHAP, MSCHAPv1, MSCHAPv2 i EAP protokole. Umesto lokalne SAM baze podataka ili Aktivnog direktorijuma može da se oslanja i na RADIUS servis kao posrednika u procesu autentifikacije.

Kriterijum autentifikacije korisnika je pripadnost Windows grupi pri čemu grupa može biti lokalna ili domenska a alternativa je korišćenje RADIUS servisa.

VPN servisi podržavaju specifičnu funkcionalnost koja se naziva "Quarantine Control". Originalni opis izraza, koji definiše epidemiološku meru suzbijanja širenja zaraznih bolesti putem izolacije obolelih, prilično je deskriptivan. Preciznije, u procesu uspostavljanja VPN veze, odnosno nakon što se veza uspešno uspostavi, na klijentskoj strani se izvršava skripta pisana tipično u VBScript, JScript ili nekom drugom podržanom interpreterskom jeziku. Skripta proverava sigurnosnu konfiguraciju klijenta. Podrazumevana skripta je trivijalna i proverava samo status lokalne mrežne barijere. Kompleksnije provere zahtevaju pažljiv razvoj skripte. Uspešan rezultat provere se prosleđuju klijentskom procesu rqc.exe.

U međuvremenu, na serverskoj strani klijent se tretira kao deo mrežnog objekta Quarantined VPN clients, sve dok ne istekne predefinisani tajmaut ili ne stigne potvrda o neinficiranosti klijenta. Klijentu se, prema tome, omogućava ograničena komunkacija, definisana najčešće pristupnim pravilima, čiji je jedan krajnji komunikacioni čvor objekat Quarantined VPN clients, u potencijano ograničenom vremenskom intervalu.

Zatim, proces rqc.exe kontaktira serverski proces rqs.exe na ISA serveru nakon čega se klijent prihvata i prebacuje iz objekta Quarantined VPN clients u objekat VPN clients sa sopstvenim skupom komunikacionih pravila, najčešće manje restriktivnih u odnosu na pravila definisana za objekat Quarantined VPN clients.

S obzirom na kompleksan niz komponenti koje treba instalirati na klijentskoj strani preporučuje se predefinisanje VPN veze putem softvera Connection Manager Administration Kit – CMAK.

XI. ENTERPRISE EDICIJA

Primarno, Enterprise ediciju karakteriše ADAM – Active Directory Application Mode, dodatni softver čije su karakteristike ranije definisane. ISA server na koji je instaliran ADAM se preciznije naziva CSS - Configuration Storage Server. Mora postojati najmanje jedan CSS u organizaciji, koja se onda iz perspektive ISA servera, formalnije naziva „enterprise". Preporučuje se kreiranje takve infrastrukture koja bi obezbeđivala redundantan CSS. To znači da CSS treba da bude instaliran na najmanje dva odvojena računara. Pored ove komponente na server se mogu instalirati i ISA servisi. ISA servisi mogu egzistirati odvojeno ili istovremeno na istom računaru na kome je pokrenut CSS, što je pitanje odabira adekvatne instalacione opcije.

Sekundarno, Enterprise ediciju karakteriše ugrađena podrška za NBL - Network Load Balancing, tehnologiju softverskog balansiranja opterećenja ISA servera. Algoritam balansiranja je statističko mapiranje dolaznih veza na pojedinačne članove klastera uz rebalansiranje u slučaju dodavanja ili uklanjanja servera. Osnovna konfiguraciona jedinica NBL-a se zove klaster. Klasteri se mogu sastojati iz maksimalno 32 ISA servera, pri čemu može biti više klastera.

Konfiguracija pravila na Enterprise ediciji je takva da postoje dva nivoa za definisanje pravila:

- enterprajz nivo, vredi za sve klastere i
- nivo NLB klastera.

Tercijarno, Enterprise ediciju karakteriše oslanjanje na CARP – Cache Array Routing Protocol. Prednosti CARP-a su sledeće:

- eliminacija dupliciranja sadržaja keša na više ISA servera,
- određivanje servera koji će keširati određeni sadržaj,
- automatsko prilagođavanje situaciji uklanjanja ili dodavanje servera,
- ravnopravna raspodela opterećenja ili prema faktoru opterećenja za svaki server pojedinačno.

Kada postoji podrška za CARP na klijentskoj strani, web browser učitava array.dll?Get.Routing.Script sa nekog ISA servera u klasteru. URL se prosleđuje skripti koja onda kalkuliše server na kome će sadržaj biti keširan. Skripta uključuje podršku za CARP algoritam. Postoji i podrška za klijente bez CARP protokola, odnosno za procesiranje skripte na serverskoj strani.

XII. ZAKLJUČAK

U ovom radu su predstavljena ključna svojstva ISA servera. Jednostavnost interfejsa, adekvatan skup svojstava za mrežnu barijeru, podešavanje uloge servera putem šablona i visoka skalabilnost su njegovi najveći aduti. Sve zajedno, omogućava efikasan rad administrativnog osoblja. Slaba strana su IPS/IDS svojstva. Najnovija generacija ovog softvera[5], koja nasleđuje mnoge pomenute osobine ISA servera, poznata je pod imenom Microsoft Forefront Threat Management Gateway 2010. Budući rad iz ove kategorije bi se svakako odnosio na najnoviju verziju softvera.

ZAHVALNICA

Zahvaljujem se profesoru Đorđu Babiću, uz čiju je pomoć ovaj dokument ugledao svetlost dana.

LITERATURA

[1] T. W. Schinder i D. L. Schinder, Dr. Tom Shinder's Configuring ISA Server 2004, Syngress Publishing, 2005.
[2] Microsoft Corporation Official Course, Implementing Microsoft Internet Security and Acceleration Server 2004, Microsoft Corporation, 2005.
[3] M. Noel, Microsoft ISA Server 2006 Unleashed, SAMS Publishing, 2007.
[4] D. Pleskonjić, N. Maček, B. Đorđević i M, Carić, Sigurnost računarskih mreža, Viša elektrotehnička škola u Beogradu, 2006.
[5] http://en.wikipedia.org/wiki/Microsoft_Forefront_Threat_Management_Gateway

ABSTRACT

Current moment in time, characterized by the explosion of Internet communications, with simultaneous increase of security risks, imposes the need to place a security product on the network edge. Microsoft Internet Security and Acceleration Server 2006 is such product.

It features several key security functionalities, usability, interface simplicity and scalability, especially if Enterprise flavor is used. This document investigates key features of aforementioned product, which are necessary for the successful deployment in real world situations.

Analysis of ISA server characteristics

Siniša Lale