БЕЗБЕДНОСТ КАЈ КОМПЈУТЕРСКИТЕ МРЕЖИ ОД АСПЕКТ НА КОНТРОЛА НА ПРИСТАП

Сашо Гелев[1]*, Јасминка Сукаровска Костадиновска[2]

[1]*Електротехнички факултет, Универзитет Гоце Делчев, П. Фах 201, 2000 Штип, saso.gelev@ugd.edu.mk*
** Сашо Гелев, е - адреса: saso.gelev@ugd.edu.mk*
[2] ул. Виенска бр. 4/10 Скопје, *jasme.sk@gmail.com*

Апстракт. Безбедноста на компјутерските мрежи е многу значаен процес, без кој во денешно време, незамисливо е функционирањето на една мрежа. Од особено значење се безбедносните услуги и механизми кои се користат за справување со различните видови на напади, како и стратегиите кои се преземаат за да се заштитат информационите системи. Контролата на пристап претставува еден механизам за определување на тоа кој има право на пристап кон определени ресурси. Таквата контрола кај компјутерските мрежи е имплементирана преку користење на повеќе методи: Access Control List – ите се темелат на дефинирани правила за пристапување, Firewall – ите чиј основен концепт на работа е на база на филтрирање на пакетите, proxy серверот кој има улога на посредник меѓу клиентот што бара услуги и другите сервери.
ISA Server – от е многу моќен Microsoft – ов производ, кој има способност да игра повеќе улоги во дадена средина. За прикажување на еден сегмент од огромниот сет на функции кои се обезбедени од ISA Server-от, практично е имплементиран ISA Server 2006 во виртуелна околина и се тестирани некои негови перформанси

Клучни зборови: ISA Server, правила на пристап, протокол, интернет сигурност

SECURITY IN COMPUTER NETWORKS FROM THE PERSPECTIVE OF ACCESS CONTROL

Saso Gelev[1]*, Jasminka Sukarovska Kostadinovska[2],
[1]*Electrotechnical Faculty, University Goce Delcev, saso.gelev@ugd.edu.mk*
*Saso Gelev, e - mail: saso.gelev@ugd.edu.mk
[2] str.Vienna no. 4/10 Skopje, jasme.sk@gmail.com

Abstract. Computer network security is a very important process, without which today we cannot imagine a fully functional network, especially without having security mechanisms and services used for handling different network attacks, and for creating strategies for securing informational systems. Access control is one of the mechanisms for granting and/or denying access to the specified resources. Such a control is implemented with using several different methods: Access Control Lists – based on defined access rules, Firewalls – for filtering incoming/outgoing packets, Proxy server – acts as a mediator between the clients and other servers.

ISA Server is a very powerful Microsoft product, capable of playing several roles in a specified deployment environment. To show a small segment of ISA Servers set of functions, ISA Server 2006 is implemented in a virtual environment and some of its performances are tested

Keywords: ISA Server, access rules, protocol, Internet security

1 Вовед

Во сите установи и компании се пропишува СИГУРНОСНА ПОЛИТИКА, односно ПОЛИТИКА НА КОРИСТЕЊЕ на Интернетот која мора да ја почитуваат сите кои се со компјутер приклучени на нејзините мрежни ресурси [3]. Сигурносните политики во деловниот свет се многу рестриктивни, се е забрането освен она што е изричито дозволено, а дозволено е само она што е неопходно за извршување на работата. Документот кој ја опишува оваа политика ќе содржи се што е потребно да се спречат инциденти: од начинот на кој, на пример, може да се влезе во управната зграда, регистрирање на влез и излез, постапка со доверливи информации и документи, па до начинот на физичка и програмска заштита на компјутерската опрема.

ISA Сервер (Internet Security and Acceleration Server) е Microsoft-ов производ, чија цел и задача се да овозможи заштита на ИТ средини од Интернет базирани закани, на начин на кој ќе им обезбеди на корисниците брз и сигурен далечински пристап до податоци и апликации [6]. ISA Серверот е наследник на Microsoft Proxy Server 2.0 и претставник на Microsoft за мрежна поддршка.

Она што е од особен интерес во врска со темата која е обработена во овој труд, секако е можноста која ISA серверот ја дава на администраторите, за креирање на политики за регулирање на користењето, зависно од корисник, група, дестинација, апликација, распоред и критериуми за типот на содржината.

ISA Серверот доаѓа во две изданија и тоа Standard Edition и Enterprise Edition.

2 INTERNET SECURITY

Може да се нагласат некои случаи на примена како што се:

- *Одбрана од надворешни и внатрешни веб базирани закани.* Создаден е да дава посилна безбедност при управување и заштита на мрежите.
- *Безбедност при објавувањето на содржината за далечински пристап.* Го олеснува далечинскиот пристап до корпоративните податоци, ресурси и апликации.
- *Безбедно поврзување на експозитури.* Овозможува лесна и ефективна site-to-site конекција помеѓу експозитурите и заштеда на пропусен опсег, преку кеширање и компресија на податоци.

Поставување стратегии на ISA SERVER 2006

Она што ISA Серверот го прави производ кој може да се издвои од останатите производи, е неговата способност да игра повеќе улоги во дадената средина[2]. Некои од тие улоги се следните: ISA Server-от како целосно функционален firewall на апликациско ниво, можноста за веб кеширање, поддршката на VPN, reverse proxy како и комбинации на било кои од овие работи.

Употреба на ISA SERVER 2006 како дополнителна заштита на веќе заштитени средини

Кога дадена организација веќе користи некаков вид на безбедносна технологија, ISA Server-от може да биде додаден како дополнителен слој на сигурност. Ова е добродојдена можност за подобрување на безбедноста на многу од организациите[1].

Еден пример на одлична интеграција на ISA Server-от е во мрежа со веќе постоечки firewall, каде е дополнителен слој на безбедност, користејќи ги своите функции на reverse proxy или доделен VPN сервер. Исто така, ISA Server-от може да се интегрира и во околини кои користат Remote Authentication Dial-In User Service (RADIUS).

ACCESS RULES

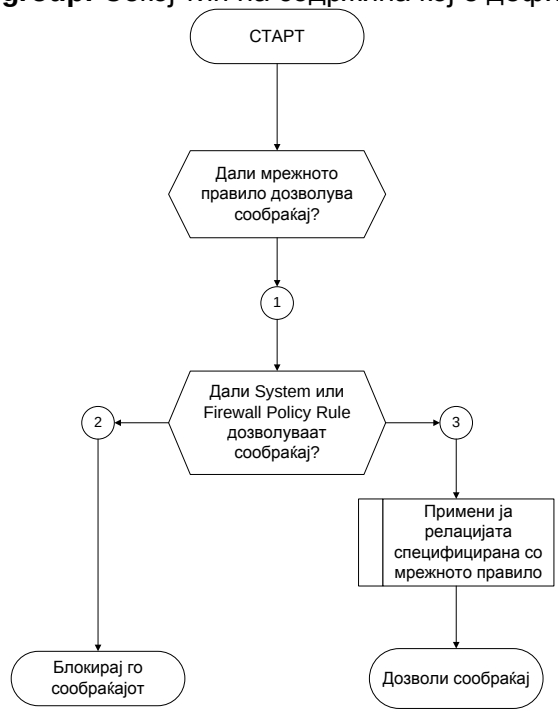
Кога станува збор за функционалноста на правилата за вмрежување кои се користат кај ISA серверите и опишувањето на дозволените комуникации помеѓу дефинираните мрежи, постојат три групи на листи на правила.

- **Мрежни правила:** Оваа листа ја опишува и дефинира топологијата на мрежата. Овие правила ја дефинираат врската помеѓу мрежните ентитети и типот на дефинираниот однос. Мора да бидат јасно и коректно дефинирани мрежните објекти и нивните меѓусебни релации, затоа што тоа е од исклучително значење за целокупната работа на ISA серверот.
- **System policy rules:** Оваа листа содржи 30 вградени правила за пристап и сите тие се применети на Local Host мрежата. Тие ги контролираат комуникациите од и до ISA серверот и се потребни за извршување на функции како што се автентикација, мрежна дијагностика, logging и далечинско управување.
- **Firewall policy rules:** Оваа листа содржи правила кои ги дефинира firewall администраторот. Ова е листа која содржи три можни видови на правила: access rule, web publishing rule и server publishing rule. Оваа листа вклучува и едно специјално предефинирано правило Last, кое го блокира целиот пристап до и од сите мрежи. Ова стандардно правило не може да биде изменето или избришано. Затоа, секое блокирање или овозможување на сообраќајот со ISA серверот е дефинирано со правила.

Со следниот дијаграм (слика 1) е дадено како ISA серверот ги применува правилата над трите листи при било кое излезно барање.

Кога правилата на пристап се поклопуваат со параметрите на барањето, тоа значи дека се применува тоа правило и ISA серверот не одговара на барањето на други правила. Овде се појавува прашањето, кога правилото на пристап се поклопува со бараните параметри. ISA серверот го применува правилото, после извршената проверка на некои критериуми, кои се одвиваат по следниот редослед:

1. **Протокол:** Еден или повеќе дефинирани протоколи со излезна насока за примарна конекција.
2. **Од (извор):** Еден или повеќе мрежни објекти кои можат да вклучат Network, Network Sets, Computers, Computer Sets, Address Ranges и Subnets.
3. **Распоред:** било кој дефиниран распоред.
4. **До (дестинација):** еден или повеќе мрежни објекти кои вклучуваат Network, Network Sets, Computers, Computer Sets, Address Ranges, Subnets, Domain Name Sets и URL Sets.
5. **Content group:** Секој тип на содржина кој е дефиниран во сетот.



Слика 1 Дијаграм за примена на правилата од страна на ISA Server 2006

3 ЕКСПЕРИМЕНТАЛЕН ДЕЛ

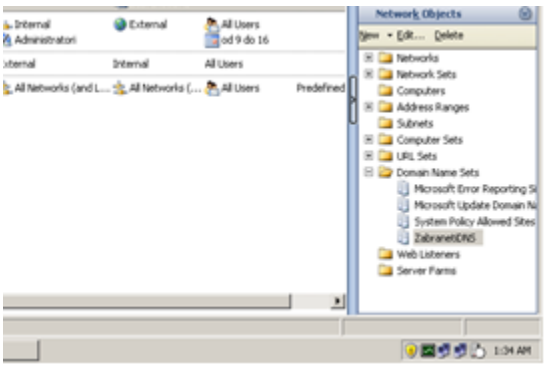
Идејата за експериментот е добиена од креирањето на правила за пристап, на ISA Server, а за таа цел инсталиран е ISA Server 2006 на виртуелен PC. Исто така инсталиран е и Microsoft Windows Server 2003 R2 со Routing and Remote Access Service и VPN и со две мрежни карти, едната LAN, а другата WAN. Алатка која е користена за креирање на тест процедурата е Microsoft Visual Studio 2008, Professional Edition.

Сценарио

Една од многуте опции кои ги нуди ISA Server-от кога е во прашање контролата на пристап е забрана и дозвола на определени сајтови и домени. Кога е потребно да се направи забрана за неколку сајтови или домени, тоа може мануелно да се конфигурира. Се поставува

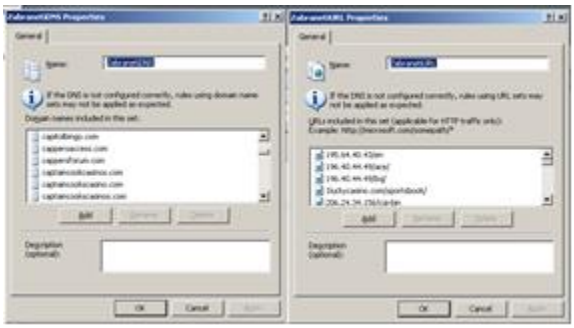
прашањето што ќе се случи ако е потребно да се забранат голем број (илјадници), како на пример цели листи на блокирани сајтови. Би било премногу неблагодарно ако тие се внесуваат мануелно како што е претходниот случај. ISA Server-от има решение за ваквиот проблем и сето тоа би се направило со само неколку минути работа. Се користат VB скрипти кои што читаат од текстуална датотека исполнета со имиња на домени кои сакаме да ги блокираме и истите ги додава во *Domain Name Set*–от или *URL Set*-от, претходно дефинирани на ISA Server-от. Скриптите кои се користени, се од сајтот http://technet.microsoft.com/hiin/library/cc302454%28en-us%29.aspx. [4] Користени се два типа на VB скрипти, една за додавање на *Domain Name*, а друга за додавање на *URL*. Синтаксата за користење на скриптите е следна:

AddListToDomainNameSet.vbs domains.txt ZabranetiDNS
AddUrlsToUrlSet.vbs urls.txt ZabranetiURL



Слика 2 Скрипти Забранети URL и Забранети DNS

Со користење на претходните скрипти се врши полнење на ZabranetiDNS и ZabranetiURL, што може да се види на следната слика



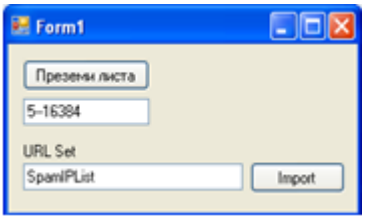
Слика 3 Полнење на листитеЗабранети URL и Забранети DNS

Од практични причини, целиот овој процес на полнење згодно би било да се автоматизира. Еден начин е со користење на Windows Service кој ќе ги „собира“ веб локациите или IP адресите и автоматски ќе ги импортира. За тоа, може да се искористи креираната програма

изработена во C#, која од некој извор, превзема листа од IP адреси. Во случајов користена е листа на IP адреси контролирани од спамери, која преку програмата, автоматски се импортира во URL Set –от.

Тест процедура

На ISA Server-от се креира URL Set со име SpamIPList.
Програмата за тестирање превзема листа од адресата: http://www.spamhaus.org/drop/drop.lasso. [7]. Листата се состои од цели IP адреса/ранг. Од листата се издвојуваат 5 линии и се запишуваат во текстуална датотека IPList.txt. Потоа се наведува името на URL сетот каде што сакаме да ја импортираме листата.



Слика 4 Форма дефинирање на URL сетот каде ќе се импортира листата

Понатаму, автоматски се извршува .vbs скриптата со параметри: креираната датотека IPList.txt и зададеното име на URL сетот. На ISA Server-от се проверува дали се импортирани IP адресите.

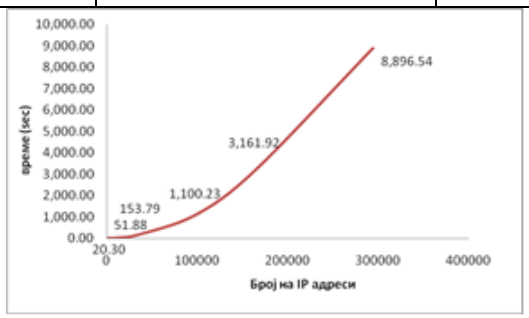
Резултати

Со повеќекратно извршување на тест процедурата за различен број на линии од листата, соодветно се добиваат резултати за бројот на IP адреси и времетраењето на импортирањето на истите во URL Set-от на ISA Server-от. Целта на тестирањето е да се покаже дека оваа постапка успешно ги импортира IP адресите, но проблем се појавува при времетраењето на импортот за голем број на адреси. Овие резултати се добиени на машина со послаби хардверски карактеристики, но реално серверите имаат подобри карактеристики.
По извршеното тестирање, добиени се следните резултати:

Табела 1 бројот на IP адреси и времетраењето на импортирањето на истите во URL Set-от на ISA Server-от.

Број на линии	Број на адреси	Време за импорт
1	1024	00:00:20.31
2	2048	00:00:21.82
3	6144	00:00:23.47
4	14336	00:00:51.88
5	16384	00:00:54.02
6	32768	00:02:33.79
7	98304	00:18:20.23

8	163840	00:52:41.92
10	294912	02:28:16.54



Слика 5 Графички приказ на резултатите

4 ЗАКЛУЧОК

Предноста со ваквото ажурирање на листите е автоматизмот. Изворниот код од програмата може да се искористи за креирање на Windows Service, со што би се придонело за постојано ажурирање. Потребно е да се истакне дека, постојат провајдери кои нудат сервиси за автоматско превземање на листите, така што со претходна регистрација и претплата, може да се дојде до истите.

Од друга страна, како што може да се види од резултатите, стапката на раст на временската сложеност при пресметувањето е многу висока кога се извршува импортирање на голем број на IP адреси во URL Set – от на ISA Server-от. Тоа е негативност на ваквиот пристап. Уште една негативна страна е тоа што не е овозможено едитирање на постоечка листа, со што би се намалило времето и потрошувачката на ресурси при импортирање на истата. Веројатно, поправилен пристап за администрирање и менаџирање на ISA Server-от е користењето на неговиот SDK (Software Development Kit) со што би се забрзала постапката и би се овозможило поедноставно ажурирање.

На крај, сакам да нагласам дека во овој експеримент е земена листа на IP адреси контролирани од спамери, но може да се земе тоа да биде листа на домени или URL листи.

ЛИТЕРАТУРА

[1] Michael Noel, *Microsoft ISA Server 2006 Unleashed*, 2008 by Sams Publishing

[2] Dr.Thomas W. Shinder, Debra Littlejohn Shinder, *How to Cheat at Configuring ISA Server 2004*, Syngress Publishing Inc. 2006

[3] Сашо Гелев, Интернет Технологии, ЕУРМ 2010

[4] http://technet.microsoft.com/enus/library/cc302621.aspx

[5] http://www.portcullissystems.com/index.php?option=com_content&view=article&id=73:isa&catid=14:test1&Itemid=125

[6] http://www.microsoft.com

[7] http://www.spamhaus.org/drop/drop.lasso