УДК: 004.738.056.057.4

ISA SERVER - ПОЛИТИКИ ЗА РЕГУЛИРАЊЕ НА ИНТЕРНЕТ СООБРАЌАЈ ВО МРЕЖИ

Јасминка Сукаровска Костадиновска, Доц Др.Сашо Гелев
[1] Европски Универзитет – Скопје, Р. Македонија, sukarovska.jasminka@live.eurm.edu.mk
[2] Европски Универзитет – Скопје, Р. Македонија, saso.gelev@eurm.edu.mk

Апстракт *– ISA Server-от е моќен Microsoft-ов производ, кој има способност да игра повеќе улоги во дадена средина. Основната цел и задача е заштита на IT средини од Интернет базирани закани. Една од многуте функции на ISA Server-от е можноста што ја дава на администраторите за креирање на политики за регулирање на сообраќајот, зависно од корисник, група, дестинација, апликација, распоред и критериуми за типот на содржината. Во овој труд ќе биде опишан ISA Server-от со своите карактеристики и содржина, а посебен акцент ќе биде даден на Firewall полисите, особено правилата на пристап (access rules).*

Клучни зборови *– ISA Server, access rules, протокол, Интернет, сигурност*

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. 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. 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 е дизајниран за работа со Windows 2000 и со подоцнежните оперативни системи.
ISA Серверот доаѓа во две изданија и тоа Standard Edition и Enterprise Edition. Стандардното издание е самостоен сервер кој поддржува до 4 процесори. Enterprise изданието е за големи инсталации, за поддршка на низа од сервери, политика на мултиниво и компјутери со повеќе од 4 процесори. Лиценците се базирани на бројот на процесори.
Понатаму, подетално ќе биде опишан ISA Серверот со своите карактеристики, содржината и секако Firewall полисите, посебно правилата на пристап (access rules).

2. ПРЕГЛЕД НА ИСТОРИСКИОТ РАЗВОЈ НА MICROSOFT-ОВИТЕ БЕЗБЕДНОСНИ РЕШЕНИЈА

Со појавувањето на Интернетот, Microsoft започнува да развива производи кои ќе можат да одговорат на потребата за заштита при користењето на Интернет. Фокусот е ставен на потребата од обезбедување на непречен пристап на клиентите до Интернет. Директна последица на ова е развојот на продукт кој ќе обезбеди можности за веб прокси, за Microsoft-овите клиенти.
Во 1996 година, Microsoft ја реализира првата верзија (1.0) на Proxy Server, производ кој обезбедува веб прокси можности за клиентите. Можностите на оваа верзија се значително помали од конкурентските, во тоа време производите на Netscape. Следна и значително подобрена верзија на 1.0 е верзијата 2.0. Главната карактеристика на оваа верзија е можноста за креирање на група од сервери за поддршка на HTTP 1.1 и FTP, и можноста за “reverse proxy”, со што оваа верзија на продуктот е многу поуспешна
Во третата верзија на производот, Microsoft се фокусира повеќе на безбедносните аспекти, и го ребрендира производот во Internet Security and Acceleration (ISA) Server 2000. ISA Server 2000 се фокусира на потполно функционални безбедносни уреди. Тоа е првиот производ на пазарот, кој се декларира како firewall од интерната мрежа и кон интерната мрежа и е скептично прифатено од страна на IP безбедносната заедница
Додека ISA Server 2000 бавно се пробива на пазарот, тимот кој го развива овој производ, започнува со работа на нова верзија на ISA Server. Резултатот е ISA Server 2004. ISA Server 2004 нуди комплетно решение кога е во прашање давањето на пристап (Access Point) помеѓу

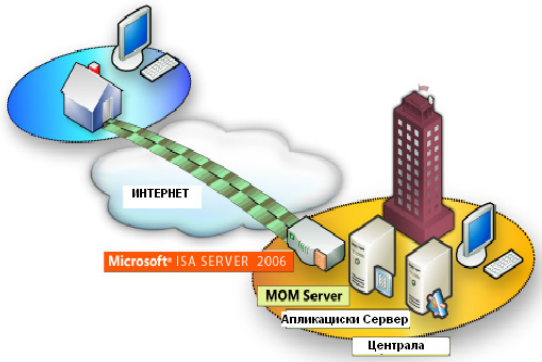
Интернет и корпорациската интерна мрежа (LAN). Може да работи како firewall, да го ограничува пристапот кон интерните мрежи на организацијата и од интерните мрежи на организацијата. Исто така има можност за конфигурирање на Proxy & Cashing сервер и овозможува пристап на ресурси на Интернет за интерни мрежни клиенти. Како додаток може да се конфигурира и VPN сервер и рутер кои ќе овозможуваат пристап кон интерни мрежни ресурси.

По успешното реализирање на ISA Server 2004, Microsoft се фокусира на новиот ISA Server 2006, кој е во многу нешта сличен на претходниот, со специфични подобрувања направени во неколку клучни области. Оваа верзија е широко и без скептицизам прифатена од страна на Интернет сигурносната заедница. ISA Server 2006 со полно право може да се каже дека е Интернет firewall, со можности за VPN и веб кеширање. Значи, без разлика на политиките и дебатите меѓу Microsoft привржаниците и анти Microsoft силите, ISA Server 2006 претставува еден импресивен производ.

2.1. Примена на ISA Server 2006

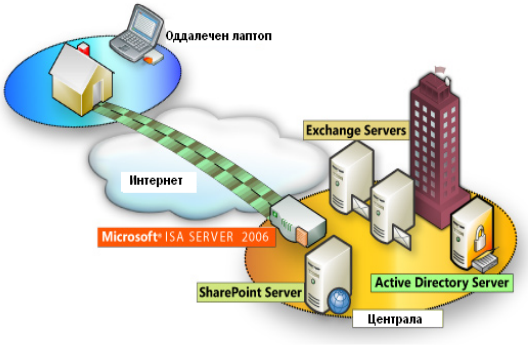
Може да се нагласат некои случаи на примена како што се:

Одбрана од надворешни и внатрешни веб базирани закани. Создаден е да дава посилна безбедност при управување и заштита на мрежите. Потребен е во бизнис организациите, за отстранување на штетните ефекти на малициозниот софтвер и напаѓачите, преку сет од алатки за скенирање, блокирање на штетни содржини, датотеки и веб сајтови. ISA Server 2006 има хибридна proxy-firewall архитектура, извршува детално филтрирање на содржината, поддржува грануларни политики, врши сеопфатно известување и следење на можностите, со што се обезбедува полесно управување и заштита на мрежата.



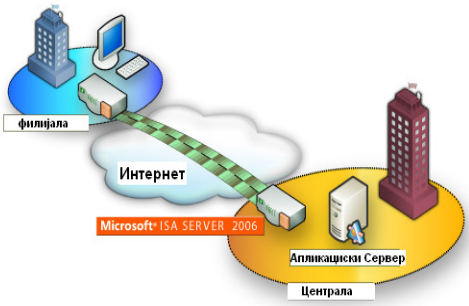
Сл.1 Одбрана од внатрешни и надворешни веб базирани закани

Безбедност при објавувањето на содржината за далечински пристап. Го олеснува далечинскиот пристап до корпоративните податоци, ресурси и апликации. Бизнис организациите потребно е да обезбедат сигурен далечински пристап до документи и податоци од било кој компјутер или уред. ISA Server 2006 им овозможува на организациите да прават безбедна размена, споделување на информации и други веб апликациски сервери на начин сигурен и за далечинските корисници кои се надвор од корпоративната мрежа. Значи, лесно обезбедува сигурност за корпоративни апликации, достапни преку Интернет.



Сл.2 Безбедност при објавувањето на содржината за далечински пристап

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. Потребата од поврзување на оддалечените експозитури со нивните корпоративни централи, бара зголемена безбедност при Интернет пристапот од подружниците и поефикасно користење на пропусниот опсег. Користењето на ISA Server 2006 го овозможува ова, на тој начин што обезбедува HTTP компресија, кеширање на содржина (како и софтверски update), и секако можност за користење site-to-site VPN-и интегрирани со филтрирање на апликациско ниво.



Сл.3 Безбедно поврзување на експозитури

3. ОПИС НА ПОСТАВЕНИТЕ 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. Во делот кој следува, ќе биде опишан развојот на 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.

3.1. ISA Server 2006 како напреден firewall со филтрирање на апликациско ниво

ISA серверот е дизајниран да обезбеди целосна firewall заштита, на начин кој би се очекувал од било кој firewall уред. Во основа ISA северот овозможува блокирање на Интернет сообраќајот преку користење на специфични порти, како што се RPC или FTP порти, за пристап до внатрешни ресурси. Ваков вид на филтрирање користат традиционалните firewall-и, при што се врши филтрирање на IP сообраќајот на мрежно ниво. Разликата помеѓу ISA и повеќето страндардни firewall-и е во можноста за филтрирање на IP сообраќајот на апликациско ниво. Оваа функционалност на ISA овозможува ISA firewall-от интелигентно да утврди, на пример, дали содржината која се реализира преку IP сообраќај е опасна.

3.2. Reverse-Proxy можности на ISA Server 2006

Иако ISA Server 2006 на пазарот се декларира како firewall, се почесто во средните и големите организации се развиваат неговите reverse-proxy способности. Оваа функционалност на ISA, овозможува заштита на интерните веб и други апликациски ресурси од надворешни закани. За хостовите на Интернет, ISA изгледа и функционира како вообичаен веб или апликациски сервер. Барањата направени од страна на клиентот потоа се враќаат назад кон актуелната машина која ја врши услугата, но не пред да бидат проверени дали се некаква опасност или закана. Исто така, може да бидат конфигурирани да го автентицираат корисникот, пред да дозволат барањата да бидат пренесени назад, што е дополнителен фактор во обезбедувањето на инфраструктурата.

3.3. Забрзување на Интернет пристапот со Web-Cashing компонентата на ISA Server 2006

Оригиналната функција на ISA Server-от кога тој се уште бил познат како Proxy Server, била да дејствува како веб прокси. Концептот на веб и FTP кеширањето на ISA Server 2006 е прилично јасен. Сите клиенти преферираат да го користат ISA за кеширање, при испраќање на барања за веб страни преку ISA серверот. Ако прв пат се бара да се отвори определена веб страна, тогаш ISA серверот од Интернет ја спушта бараната содржина и ја доставува до клиентот, додека во исто време локално зачувува копија од текстот, сликите и другата HTTP или FTP содржина. Ако друг клиент од мрежата ја побара истата страна, механизмот за кеширање ќе ја достави локалната копија на страната до корисникот, без притоа да оди на Интернет. Ова значително ја зголемува брзината на пристап кон веб страните.

3.4. Контрола и управување на пристапот на клиент кон ресурси во компанија преку VPN

Некои од поголемите подобрувања на ISA Server 2006, се во областа на VPN. VPN функционалноста е значително подобрена, а и флексибилноста на VPN-ите кај правилата за пристап е зголемена.

Употребата на VPN кај ISA Server 2006, типично вклучува безбеден, енкриптиран тунел, поставен помеѓу клиенти на Интернет и ISA firewall-от од страната на Интернет. По автентикацијата на клиентот, клиентот има пристап до специфични интерни ресурси, дефинирани од страна на ISA администраторот. Ресурсите до кои може да се пристапи се специфицирани преку правила на пристап, така да контролата може да биде многу детална. Преку оваа контрола, ISA Server-от може да ги изолира оние корисници кои немаат инсталирано антивирусни програми. Различни правила на пристап може да се конфигурираат за изолираните VPN корисници на мрежата, на пример уште поголемо ограничување на нивниот пристап.

Конечно, ISA серверот исто така вклучува можност да воспостави site-to-site VPN конекции до далечински сајтови преку Интернет. Ова им овозможува на мрежите да се приклучат преку VPN врски. Дополнителна предност е тоа што Internet Key Exchange (IKE) протоколот, кој се користи за воспоставување на конекција, исто така може да се искористи за да постави site-to-site VPN помеѓу ISA Server и трета страна на VPN продуктот. Оваа функционалност е значително подобрена во верзијата од 2004 година.

3.5. Користење на Firewall Client за контрола на индивидуален кориснички пристап

Освен стандардните можности за поддршка на сообраќајот од било кој Интернет клиент (SecureNAT Client), ISA вклучува можност и за рестрикција, контрола и запис на кориснички акции преку инсталирање и конфигурирање на ISA Firewall Client. Со користењето на ISA Firewall Client, може да се креираат сценарија кои се побезбедни, а исто така му се овозможува на администраторот, да ја контролира firewall политиката, базирана на индивидуалните корисници или групите на корисници.

Гледано од административно ниво, за било кој систем администратор, во било која компанија, полесно е да се администрира една листа на правила која ќе важи за сите компјутери во мрежата, отколку на секој компјутер поединечно да се креираат и администрираат правилата. Оваа можност заштедува многу време, затоа што во спротивно, истата задача би се повторувала многу пати, во зависност од бројот на компјутерите во компанијата.

4. 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.

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). Бидејќи RADIUS технологиите не поддржуваат автентикација и логирање, тоа е задача која е дополнета од страна на ISA серверот.

5. АДМИНИСТРИРАЊЕ И ОДРЖУВАЊЕ НА ISA SERVER 2006 ОКОЛИНА

По инсталацијата и поставувањето на ISA Server-от, започнуваат важните задачи на администрирање и одржување на околината. За среќа ISA Server-от е моќен, а сепак лесен за употреба поради соодветните алатки и посебно поради функционалностите кои тие алатки ги нудат за да им помогнат на администраторите.

ISA Management Tools: Користењето на ISA Server Management Console значително олеснува во решавањето на комплексните задачи и му овозможува на администраторот да ги има сите функционалности на едно место. Конфигурирањето, известувањето, запишувањето, мониторингот и обезбедувањето може да бидат следени од една централна конзола и тоа на тој начин што ќе обезбедат поедноствно управување и при евентуални грешки во конфигурирањето, да не резултираат со нарушување на безбедноста.
ISA конзолата исто така вклучува и некои вградени визарди и темплејти кои му овозможуваат на администраторот да извршува некои заеднички функции и процедури, како што се креирање на access rules, дефинирање на мрежи и сл.
Back up и restore на ISA Server околина: Back up-от и restore-от може да бидат многу комплексен и тежок процес, кога станува збор за Windows средина, но за среќа тоа не е таков случај со ISA Server 2006. Зачувувањето (backing up) на конфигурацијата на firewall-от се изведува во XML датотека, која може да се реимпортира на друг ISA Server за да може да се направи restore на конфигурацијата. Индивидуалните ISA елементи, како што се firewall правилата, може да се зачуваат во индивидуални датотеки, со можност да се рестартираат еден по еден. Оваа флексибилност придонесува да се намали бројот на restore-и и да се олесни повратокот на серверите или на одделните елементи.
Одржување на ISA Server околина: Иако ISA Server околината не е премногу захтевна за одржување, сепак одржувањето опфаќа голем број на процедури и вклучува типови на задачи на дневно, неделно, месечно и квартално ниво, кои треба да се извршуваат за да се зачува топ формата на ISA.
Monitoring и логирање на кориснички акции: ISA користи механизам за чување на логовите на корисничките акции, на тој начин што ги чува во база на податоци.Со помош на овие логови, администраторот може да изврши детална анализа на типот на сообраќајот кој проаѓа низ ISA серверите.

6. УПОТРЕБА НА ISA SERVER 2006 ЗА БЕЗБЕДНОСТ НА АПЛИКАЦИИТЕ

Една од основните и најпопуларни карактеристики на ISA Server-от е да ги обезбеди и заштити од напади, Интернет ориентираните апликации.
Безбедност на Exchange Outlook Web Access со ISA Server 2006: Една од задачите на ISA Server 2006 е да обезбеди reverse proxy за Exchange Outlook Web Access (OWA) серверите. Развојниот тим на ISA, работејќи заедно со развојниот тим на Exchange, развиваат специфични OWA филтри, со што ја приближуваат интеграцијата помеѓу овие две технологии. Покрај основните бенефити кои ги обезбедува reverse-proxy, ISA ги има и следните клучни точки за безбедност на OWA:

- Нуди end-to-end Secure Sockets Layer (SSL) поддршка од клиентот до ISA серверот и назад до Exchange OWA серверот.
- Forms-based authentication (FBA) на ISA – претставена е од Exchange Server 2003 и им овозможува на корисниците да се автентицираат, спротивно од OWA серверот, со пополнување на информациски образец. Предноста на ова секако е и во спречување на неавтентициран пристап до Exchange серверот.
- Во прилог на филтрирањето и заштитата на OWA сообраќајот, ISA исто така вклучува и сопствени филтри за скенирање и заштита на mail сообраќај, како што е Simple Mail Transport Protocol –от и Exchange MAPI (Outlook-style) пристап.

Заклучување за веб апликативен софтвер: HTTP филтрирањето кое го изведува ISA серверот, може да идентификува и да искоренува HTTP закани, пред да пристапат кон некои традиционални веб сервери и веб апликации. Исто така HTTP филтрирањето може да се модифицира и проширува мануелно, или дури и да се користат други софтверски продукти кои ќе лимитираат специфични HTTP повици, ќе лимитираат пристап до специфични веб сајтови или ќе

блокираат некои извршни превземања (executable downloads).

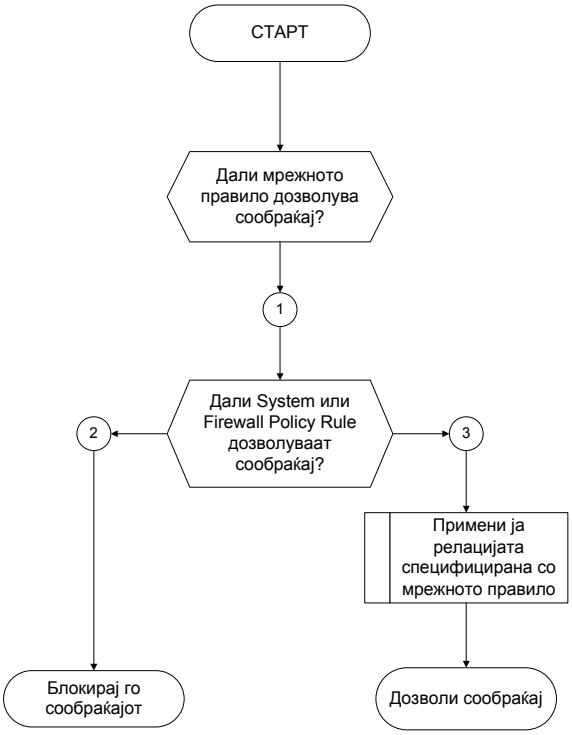
Безбедност на Remote Procedure Call (RPC) сообраќај: Една од најголемите закани за Windows инфраструктурата во последните години е подемот на вирусите, што резултира со крајно штетни последици по инфраструктурата на компаниите и дури до комплетно нарушување на меѓумрежните поврзувања. ISA серверот е од непроценливо значење токму за овие видови на RPC експлоатирања, поради можноста да го скенира RPC сообраќајот и на интелигентен начин да ги отвори само оние портови кои се потребни за функционирањето на специфичните RPC услуги.

7. 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. Ова се правила кои може само да се овозможат или оневозможат и на нив може да се применат само некои мали измени на определени својства.
- **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 е дадено како ISA серверот ги применува правилата над трите листи при било кое излезно барање:



Сл.4 Дијаграм за примена на правилата од страна на ISA Server 2006

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.

8. ЕКСПЕРИМЕНТАЛЕН ДЕЛ

Во овој дел ќе биде прикажан и презентиран извршениот експеримент и ќе биде дискутиран добиениот резултат. Најпрво ќе биде објаснето имплементираното сценарио, користените алатки и тест процедурата.

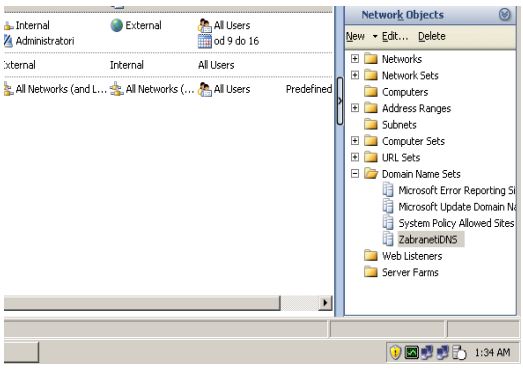
8.1. Тест околина и користена алатка

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.

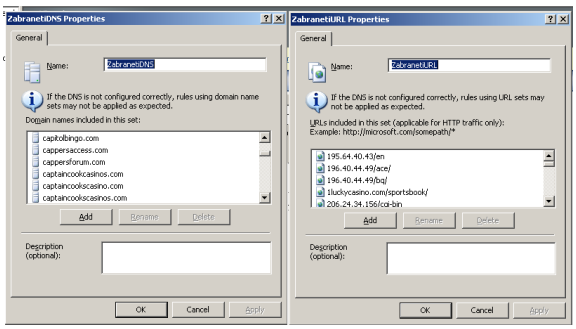
8.2. Сценарио

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 исконфигурира. 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. 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



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

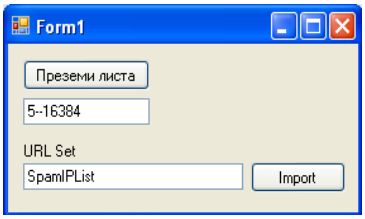


Од практични причини, целиот овој процес на полнење згодно би било да се автоматизира. Еден начин е со користење на Windows Service кој ќе ги „собира“ веб локациите или IP адресите и автоматски ќе ги импортира. За тоа, може да се искористи креираната програма изработена во C#, која од некој извор, превзема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

8.3. 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. 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.



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.

8.4. Резултати

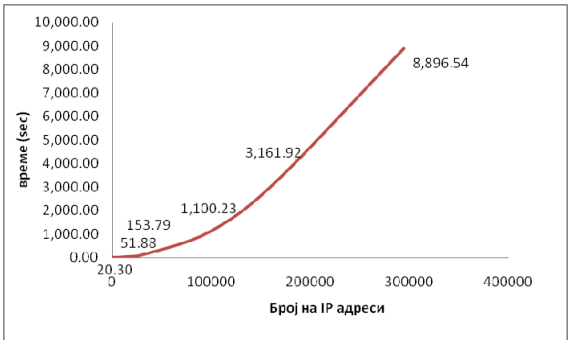
Со повеќекратно извршување на тест процедурата за различен број на линии од листата, соодветно се добиваат резултати за бројот на IP адреси и времетраењето на импортирањето на истите во URL Set-от на ISA Server-от. Целта на тестирањето е да се покаже дека оваа постапка успешно ги импортира IP адресите, но проблем се појавува при времетраењето на импортот за голем број на адреси.

По извршеното тестирање, добиени се следните резултати:

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

Табела 1. Табеларно претставени резултати



Графички приказ на резултатите

Овие резултати се добиени на машина со послаби хардверски карактеристики отколку, реално, појаките карактеристики на серверите.

9. 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). На тој начин сигурно 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.

БЛАГОДАРНОСТ

Посебна благодарност до асистентот Александар Соколовски за помоштa при инсталирањето на ISA Server 2006 и до Милорад Костадиновски за поддршката, трпението и критиките при изработката на трудот.

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

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

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

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

ISA SERVER – INTERNET SECURITY POLICIES

Jasminka Sukarovska Kostadinovska, Doc. Dr.Saso Gelev

[1] European University – Skopje, R. Macedonia, sukarovska.jasminka@live.eurm.edu.mk

[2] European University – Skopje, R. Macedonia, saso.gelev@eurm.edu.mk

Abstract *– ISA Server is a very powerful Microsoft product, capable of playing several roles in a specified deployment environment. The basic tasks and goals are to protect IP network from Internet based threats. One of many functions of ISA Server is administration of traffic policies defined on users, groups, applications, content type, different type of schedules, etc. In this paper I will describe characteristics and content of the ISA Server, specially firewall policies and access rules.*

Keywords *– ISA Server, access rules, protocol, Internet, security*