Kerio Control – უსაფრთხოების კედელი და ადმინისტრატორის კომპლექსური ინსტრუმენტი

კახაბერ რევაზიშვილი
საქართველოს საპატრიარქოს წმიდა ანდრია პირველწოდებულის
სახელობის ქართული უნივერსიტეტი

რეზიუმე

თანამედროვე კორპორატიული ქსელები თავისი სტრუქტურის და დატვირთვის საკმაოდ რთულ და დახვეწილ გადაწყვეტილებებს მოიცავს. არსებობს ისეთ პუნქტები, რომელთა უგულებელყოფა, უსაფრთხოების პრინციპიდან გამომდინარე, დაუშვებელია. საჭიროა მთელი რიგი მართვადი მოწყობილობები, რომელთა კონფიგურირების შემდეგ შეიძლება ჩაითვალოს, რომ კომპიუტერული ქსელი როგორც Lan ასევე WAN გამართულია. ჩვენ პირველ რიგში ვიხილავთ თუ რა სირთულის ქსელური სტრუქტურა შეიძლება შეგვხვდეს და შემდეგ იმ აპარატურულ თუ პროგრამულ უზრუნველყოფას, რომელიც დაგვჭირდებოდა მათ გასამართად.

საკვანძო სიტყვები: პროგრამული მარშრუტიზატორი. აპარატურული მარშრუტიზატორი. სტატიკური მარშრუტი. უსაფრთხოების კედელი. კორპორატიული ქსელი. ქსელის აპარატურულ პროგრამული უზრუნველყოფა.

1. შესავალი

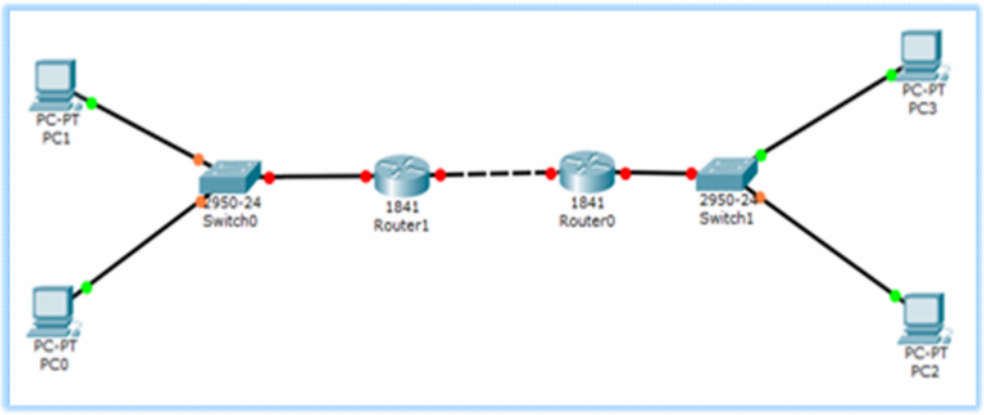
ორგანიზაციის ქსელური ინფრასტრუქტურის დაგეგმარება და მისი მოწყობა აპარატურულ-პროგრამულ დონეზე, თანამედროვე განვითარებული ტექნოლოგიების ფონზე უკვე პირველ-ხარისხოვანი ამოცანაა. პირველ რიგში გასათვალისწინებელია, რა ტიპის ორგანიზაციასთან გვაქვს საქმე, რა ამოცანა დგას ორგანიზაციის წინაშე, რამდენად მნიშვნელოვანია ამ ორგანიზაციის დოკუმენტური ბაზის დაცვა. თუ გადავხედავთ საჭირო მოწყობილობათა ფასებს მსოფლიო ბაზარზე, აღმოვაჩენთ, რომ არასწორი დაგეგმარების შემთხვევაში გაუმართლებელ ხარჯებამდე შეიძლება მივიდეს ორგანიზაცია [1].

2. მცირე ოფისის ტიპის ლოკალური ქსელი

ამ ტიპის ქსელის მოსაწყობად სრულიად საკმარისი იქნებოდა სტანდარტული მართვადი მარშრუტიზატორის დამონტაჟება, მისი შეერთება სტანდარტულ სვიჩზე. სტატიკური მარშრუტის გაწერის შემდეგ შეიძლება ჩაითვალოს, რომ ქსელი შეასრულებს თავის მოვალეობას და მომხმარებელს ექნება როგორც ლოკალურ, ასევე გლობალურ ქსელებთან წვდომა. აქვე აღვნიშნავთ, რომ დღეისთვის ფართოდ გავრცელებული „ღრუბლის" ტექნოლოგიებთან წვდომა, მცირე ოფისის მოწყობის შემთხვევაში, განსაკუთრებულ სირთულეებთანაა დაკავშირებული [2].

IP დამისამართება, სამივე ლოკალურ კლასზე 192.168.0.0/24, 172.16.0.0/16 და 10.0.0.0/8 შეიძლება დარჩეს სტანდარტულ „ქვექსელებზე", თუმცა მაინც რეკომენდებულია, რომ ქსელი გამოიყოს კონკრეტული საბნეტით, რომელშიც მოთავსდება საჭირო IP მისამართები და არა უმეტეს.

ჩვენი ამოცანიდან გამომდინარე განვიხილოთ Kerio Control, მისი კონფიგურირება და ყველა ის მოსახერხებელი ინსტრუმენტი, რომელსაც შემოგვთავაზებს აღნიშნული პროგრამული უზრუნველყოფა. აქ არ განვიხილავთ ამ სისტემის შესაძლებლობებს და მის უპირატესობას Cisco-ს ან ჯუნიპერის აპარატურასთან. იმისთვის, რომ ჩვენ თვითონ მივიღოთ გადაწყვეტილება, ვნახოთ როგორ კონფიგურირდება ლოკალური ქსელი და სტატიკური მარშრუტი Cisco-ს და Kerio-ს მაგალითებზე. 1-ელ ნახაზზე მოცემულია ზოგადი სტანდარტული სქემა.



ნახ.1. ქსელის სტანდარტული სქემა

მოცემულ სქემაზე განსაკუთრებული სირთულეები საერთოდ არ განიხილება. ვნახოთ როუტერის ჩართვის პრინციპი საბნეტი გამოყოფა და ა.შ. Cisco-ს ტერმინალში.

Router>enable

Router#configure terminal

Router(config)#hostname R1 (ამ ბრძანებით ჩვენ როუტერს მივანიჭეთ სახელი)

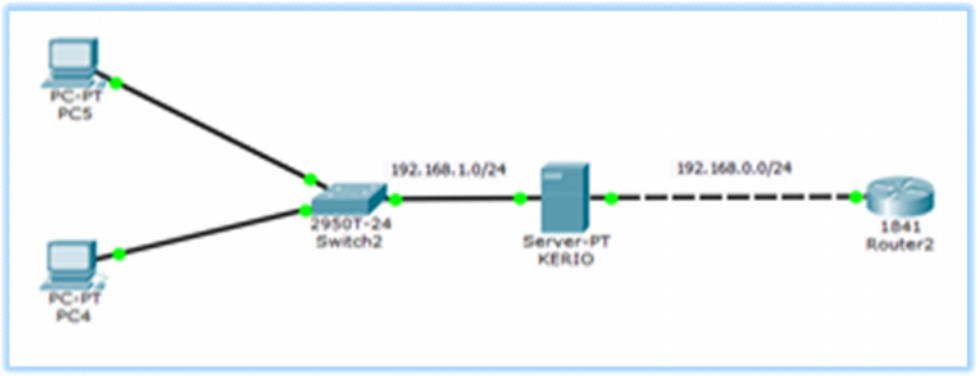
R1(config)# enable secret „პაროლი“ (ამ ბრძანების შესრულები შემდეგ როუტერის ტერმინალი დაიკეტება დაშიფრული პაროლით, რა თქმა უნდა არსებობს პაროლის მინიჭების მეორე გზაც enable password, მაგრამ ამ შემთხვევაში სიტყვა-გასაღები არ იშიფრება)

სტატიკური მარშრუტის გაწერის შემთხვევაში ტერმინალის ბრძანება სრულდება მარტივად:

R1(configure)#**ip route A.A.A.A** M.M.M.M F.F.F.F

სადაც A.A.A.A არის სასურველი ქსელი, რომელიც უნდა შევასწავლოთ ჩვენს როუტერს, M.M.M.M არის ამ ქსელის საბნეტი და F.F.F.F არის ინტერფეისის მისამართი ან მისი სახელი და ტიპი (მაგალითად fa0/0), რომლისკენაც მოიძებნება შემდგომში აღნიშნული ქსელი.

კერიო შემთხვევაში, მოცემული ამოცანის გადაწყვეტა სხვაგვარადაა. მოვიყვანოთ კერიოს საშუალებით ქსელის მოწყობის სქემა (ნახ.2).



ნახ.2. ქსელის სტრუქტურა Kerio-ს ბაზაზე

როგორც შევამჩნიეთ, კერიოს მოსაწყობად საჭიროა სერვერული სისტემა (პლატფორმა შეზღუდული არაა, იგი ინსტალირდება Windows, Linux, MacOS x პლატფორმებზე), თუმცა, აუცილებელი არაა, რომ სერვერული ოპერაციული სისტემა დავაინსტალიროთ. ჩვენთვის მთავარია

აღნიშნულ სერვერზე ჩავდგათ საჭირო რაოდენობის ინტერფეისები (ჩვენ შემთხვევაში სერვერში მოთავსებულია ორი ინტერფეისი: 192.168.0.0/24 და 192.168.1.0/24 ქსელების აღწერისთვის).

შეიძლება ჩაითვალოს, რომ ამოცანა უკვე გადაწყვეტილია და ჩვენ ქსელს აქვს როგორც ლოკალური ასევე გლობალური წვდომა, რადგან კერიო თავისთავად წარმოადგენს პირველ რიგში მარშრუტიზატორს. მისი ინსტალირების და გაშვების პირველივე მომენტიდან სისტემა თვითონ გვთავაზობს მარშრუტების აღწერას. აღწერაში იგულისხმება ინტერფეისების მითითება. მოხმარებლის მხარე მოწყობილობებისთვის Default Gateway იქნება კერიოს ლოკალური ქსელისკენ მომართული ინტერფეისი (როუტერის შემთხვევაში Default Gateway იქნებოდა როუტერის ლოკალური ინტერფეისი).

შეიძლება დაისვას შეკითხვა, მხოლოდ ამით შემოიფარგლება კერიოს ფუნქციები? დავრწმუნდებით, რომ ასე არაა. განვიხილოთ რამდენიმე ფუნქცია რომელსაც უზრუნველყოფს კერიო და ვისაუბროთ მის დადებით თუ უარყოფითი მხარეებზე.

კერიოს უარყოფითი მხარე, რომელიც ხშირ შემთხვევაში ქმნის დისკომფორტს, ისაა, რომ იგი ძალიან ცუდად ან სულაც არ იმუშავებს ვირტუალურ ინტერფეისებზე და დამატებით მისამართებზე. და კიდევ, რა თქმა უნდა, პროგრამული უზრუნველყოფა აპარატურულ უზრუნველყოფასთან შედარებით ნელია და კარგად უნდა მოვიფიქროთ, რა სიმძლავრის სერვერი დაგვჭირდება ამოცანის გადასაწყვეტად. ეს, რა თქმა უნდა, ჩვენი ქსელის სირთულეზეა დამოკიდებული. განვიხილოთ კერიოს ფუნქციები უკვე საშუალო და დიდი კორპორატიული ქსელის მაგალითზე.

3. საშუალო და დიდი კორპორატიული ქსელი Kerio-ს გამოყენებით

ამ ტიპი ქსელზე უკვე გაცილებით მეტი მოთხოვნა და სირთულეები მოდის, როგორც აპარატურულ-პროგრამულ, ასევე პროტოკოლების გამოყენების მიმართულებით. კერიოში ინტერფეისები განიხილება როგორც კონკრეტული ფუნქციის მატარებელი. მაგალითად, Trusted/Local და Internet ინტერფეისები. ამ ჯგუფებში ჩვენი სურვილისამებს შეგვიძლია განვათავსოთ ინტერფეისები (ნახ.3).

Name	IP Address	Mask	Status	Internet	Details
Internet interfaces					
Ethernet 3	[redacted]	255.255.255.252	Up		Realtek RTL8139/810x Family Fast Ethernet NIC
Trusted/Local interfaces					
Ethernet	192.168.10.1	255.255.255.0	Up		Realtek PCI GBE Family Controller
Ethernet 2	10.0.0.1	255.255.255.128	Up		Marvell Yukon Ethernet Controller
Ethernet 4	172.16.0.1	255.255.0.0	Up		Realtek RTL8139/810x Family Fast Ethernet NIC
VPN interfaces					
VPN Server	[redacted]		Down		VPN driver is not loaded.
Other interfaces					
Dial-In			Down		

ნახ.3.

ამასთან ერთად აღსანიშნავია, რომ Kerio არ თხოულობს ერთი ტიპის ინტერფეისების ჩაყენებას. ეს კარგად ჩანს სქემაზე.

ახლა განვიხილოთ კერიოს ფუნქციები [3]:

1. Traffic Rules – ტრაფიკის სცენარი. აღნიშნული სცენარი ჩვენ თვითონ შეგვიძლია დავაკონფიგურიროთ. გავხსნათ ან დავკეტოთ კონკრეტული მიმართულება. დავბლოკოთ ან შევზღუდოთ მომხმარებლის წვდომა ამა თუ იმ სერვისზე. აგრეთვე ვაწარმოოთ ლოგების ჟურნალი. უნდა აღვნიშნოთ, რომ ლოგების ჟურნალის გამოყენებისას სერვერი მოითხოვს საკმაოდ სწრაფ და დიდი მოცულობის მყარ დისკებს [4];

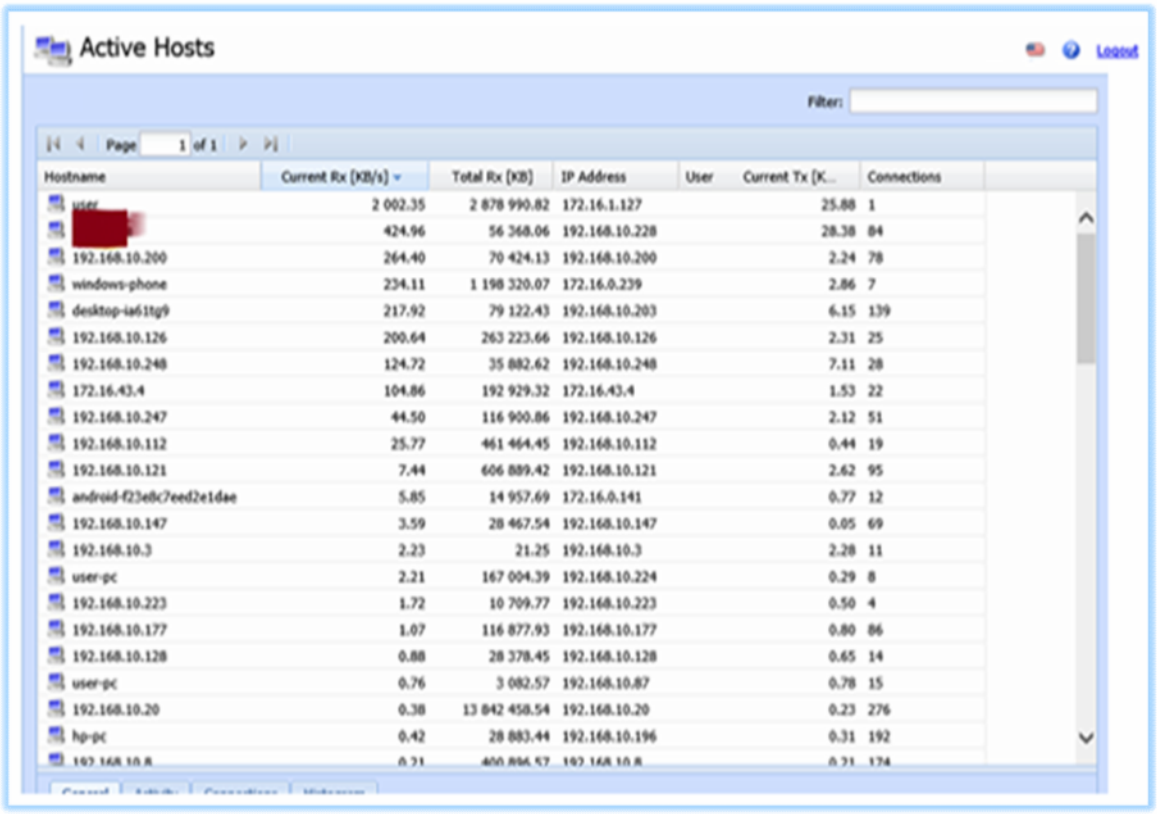
2. Infusion prevention – ამ ინსტრუმენტის საშიალებით შეგვიძლია აღვწეროთ და დავბლოკოთ ის ბაზები და რესურები, რომელთა წვდომაც ჩვენს სივრცეში არასასურველი იქნებოდა;

3. Security Settings – აქ განიხილება წვდომის შეზღუდვა MAC მისამართების აღწერით.

ძალზე მნიშვნელოვანია, რომ Kerio kontrol სისტემას გააჩნია თავისი DHCP სერვისი და საკმაოდ მოსახერხებელიცაა, იმ მიმართულებით, რომ აღნიშნული სერვისის გამოყენება და ჩართვა შესაძლებელია მარტივი ვიზარდის საშუალებით და სპეციალური ცოდნა DHCP-ს სფეროში არ მოითხოვება. აქ მარტივად შეიძლება ინტერფეისის ამორჩევა და მასზე პულის და ლიზის დაყენება. აგრეთვე შეგვიძლია ვაკონტროლოთ (ვიზუალურად) კლიენტები, რომლებიც არიან ჩართული ამ სერვისზე.

Kerio Control-ს აქვს მომხმარებელთა შექმნის და მათზე უფლებათა გაწერის საშუალებაც. აგრეთვე IP მისამართების ჯგუფების შექმნა, VPN სერვისის მოწყობა. მომხმარებელთა სტატისტიკის ჩართვა და ასე შემდეგ.

ყველაზე მეტად, რაც ხიბლავს Kerio Control-ის ადმინისტრატორებს, ესაა ქსელური რესურსების და მათი გამოყენების ვიზუალური კონტროლის შესაძლებლობა (ნახ.4).



ნახ.4.

ამ სქემაზე კარგად ჩანს, რომ ჩვენი ქსელი, მისი გამოყენების მიხედვით, საკმაოდ კარგადაა აღწერილი ადმინისტრატორისთვის და მას აქვე შეუძლია იმ მომხმარებელს, რომელმაც გადააჭარბა ლიმიტებს, შეუზღუდოს წვდომა. თუმცა მას წინასწარვე შეუძლია დააყენოს რესურსის გამოყენების კვოტები. ზემოთ მოცემულ სურათზე კარგად ჩანს, რომ Kerio თვილის კავშირების რაოდენობას, რომელსაც ამყარებს მომხმარებლის მოწყობილობა ქსელში. ეს ძალიან მნიშვნელოვანია, რადგან ხშირად გადაჭარბებული კავშირების არსებობა მიუთითებს კომპიუტერზე ვირუსული სისტემის არსებობას და არა კომპიუტერის რეალურ დატვირთვას ქსელში. ეს საშუალებას იძლევა უკვე ყურადღება გავამახვილოთ კომპიუტერის გაწმენდაზე მავნე პროგრამული ჩანართებისგან.

საინტერესოა აგრეთვე ლოგირების სისტემა, რომელიც იმდენად მარტივადაა მოწყობილი, რომ რაიმეს კონფიგურირებას არ საჭიროებს. უსაფრთხოების პრინციპიდან გამომდინარე, ჩავთვალოთ, რომ ლოგების შენახვა და მათი გადახედვა საჭიროების შემთხვევაში, ალბათ ბევრ უსიამოვნებას აგვარიდებს.

4. დასკვნა

განსაკუთრებით უნდა აღინიშნოს, რომ სპეციალური უსაფრთხოების პოლიტიკის არსებობა ორგანიზაციაში აუცილებელია. სამწუხაროდ ბევრ ორგანიზაციაში, რომელთა პროგრამული და ქსელური სისუფთავე კრიტიკულად მნიშვნელოვანია, საერთოდ არ განიხილება და კომპიუტერული ტექნიკის გამოყენება დაყვანილია ელემენტარულ ქსელურ გადაწყვეტილებამდე: როუტერი (პროვაიდერის მიერ დაკონფიგურირებული), უმართავი სვიჩი და IP დამისამართება, რომელიც საერთოდ არ მოიცავს არანაირ IP ჯგუფებს და გამოიყენებენ სრულ საბნეტებს. ასეთ შემთხვევაში, Kerio-ს გამოყენება ყოვლად დაუშვებელია. დაუშვებელია თუნდაც იმიტომ, რომ მოხმარებელი უნდა გაეცნოს იმ უსაფრთხოების პოლისებს, რომელიც მოქმედებს კერიოს გამოყენების დროს. უნდა განვუმარტოთ, რომ კერიოს სისტემური გამართვის შემდეგ ადმინისტრატორს ხელისგულზე აქვს ყველა ის რესურსი რაზედაც მოხმარებელს ჰქონდა წვდომა. ჩანს ყველა ლინკი და ფაილი, რომელსაც მოეჭიდა ქსელში. უნდა ავუხსნათ, რომ კერიოს ჩართვის შემთხვევაში, IT თანამშრომელს არ მიუწვდება ხელი მის პირად ინფორმაციაზე (საბანკო ანგარიშები, პირადი ელფოსტა, სოციალური ქსელი და ა.შ.).

ჩვენი აზრით, ქსელის მოწყობა, უსაფრთხოების დაყენება და ა.შ., იწყება მარტივი, თუმცა აუცილებელი, ქსელის დაგეგმარებით და ამოცანების დასმით, რაც IT მენეჯერის პირველადი და ყველაზე მნიშვნელოვანი ამოცანაა. კომპიუტერული ქსელის გარეშე თითქმი აღარ განიხილება ორგანიზაციის ნაყოფიერი ფუნქციონირება, მითუმეტეს, თუ გადავხედავთ ტექნოლოგიებს, ვნახავთ, რომ უფრო და უფრო მეტი ორგანიზაცია ერთვება ღრუბლის ტექნოლოგიებში.

ლიტერატურა:

1. Брашинский П.А. (2001). Локальная сеть. Самое необходимое. БХВ-Петербур.

2. Kerio Control - Administrators guide. (2011). Kerio Technologies s.r.o. Description on configuration and administration of Kerio Control, version 7.1.2. All additional modifications and updates reserved. documents addressing the product, see http://www.kerio.com/firewall/manual

3. Kerio Control – Step-by-step. (2012). Kerio Technologies s.r.o. All Rights Reserved. http://www.kerio.com/control/manuals.

4. Masich G.F. (2011). IP маршрутизации.

KERIO CONTROL – NETWORK FIREWALL AND ADMINISTRATOR'S COMPLEX TOOLS

Revazishvili Kakhaber

St. Andrew the First-Called Georgian University of Patriarchate of Georgia

Summary

The structure of modern corporative network is more loaded and complicated system. Need a number of manageable devices, which can moderate our LAN and WAN. In First, we need to manage our network, need to get software and hardware what we need in our topology. One of Solution to manage out LAN is Kerio Control. It is new name of Kerio WinRoute Firewall. This software provides lot of network tasks. The main task of Kerio control is to replace expensive network hardware, such as routers, firewalls and etc.

KERIO CONTROL – МЕЖСЕТЕВОЙ ЭКРАН И УДОБНЫЙ ИНСТРУМЕНТ ДЛЯ АДМИНИСТРАТОРА

Ревазишвили К.

Грузинский университет им. Андрея Первозванного Патриашества Грузии

Резюме

Структура сети в современном офисе, по своей структуре, уже являеться сложной структурой. Для решений всех задач требуеться множество устройств и протоколов. Одним из решении является Керио Контроль. Главная задача этого програмного обеспечения, организовать сетевые протоколы организации. Также это алтернативное решение, которое заменит множество дорогих устройств.