კლიენტ-სერვერული არქიტექტურით კომპიუტერული ვირტუალური კერძო ქსელის ორგანიზაციის ტექნოლოგია

ომარ გაბედავა, სიმონ პოჩოვიანი
საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

განხილულია კომპიუტერული ვირტუალური კერძო ქსელების (VPN) ორგანიზაციის ტექნოლოგია კლიენტ-სერვერული არქიტექტურის საფუძველზე. აღწერილია დანიშნულება, პროგრამული და ტექნიკური რეალიზაცია და კომპიუტერული VPN ორგანიზაციის მეთოდები, VPN-შეერთებათა ტიპები, კომპიუტერულ VPN-ში გადასაცემი ინფორმაციის დაცვისათვის საჭირო პროტოკოლები, აგრეთვე სერვერის ფუნქციონალური შესაძლებლობანი.

საკვანძო სიტყვები: კომპიუტერული ქსელი. VPN. ინტერნეტი. კომპიუტერული კორპორაცია. კლიენტ-სერვერი.

1. შესავალი

ქსელში მონაცემების ეფექტური და დაცული გადაცემისათვის ფირმები თავიანთ ფილიალებთანაა გაერთიანებული გამოყოფილი ხაზებით. მაგალითად, ერთი ოფისის გასაერთიანებლად დანარჩენ ოფისებთან გამოიყენება Frame Relay ან ATM ხაზები. ასეთი გადაწყვეტილება საკმაოდ ძვირია. ამიტომ, ასეთი მოთხოვნების დასაკმაყოფილებლად გამოიყენება კომპიუტერული ვირტუალური კერძო ქსელები (ვკქ; VPN-Virtual Private Network) [1].

კომპიუტერული VPN არის ტექნოლოგია, რომლის დროსაც ხდება დაშორებულ ლოკალურ კომპიუტერულ ქსელთან (ლკქ, Local Area Networks; LAN) ვირტუალური არხით, საერთო მოხმარების ქსელის გავლით, „წერტილი-წერტილი" კერძო მიერთების იმიტაცია. საერთო მოხმარების ქსელის ქვეშ იგულისხმება როგორც ინტერნეტის ქსელი, ასევე კორპორაციული კომპიუტერული ქსელი (კკქ), ინტრანეტი („Enterprise-Wide Networks").

2. ძირითადი ნაწილი

კომპიუტერული ვკქ (VPN) არის ორი კვანძის დაცული შეერთება გახსნილი ქსელის მეშვეობით. ასეთი შემთხვევისათვის ხდება ვირტუალური არხის ორგანიზება, რომელიც უზრუნველყოფს ინფორმაციის უსაფრთხო გადაცემას, ხოლო კვანძებს VPN შეერთებით შეუძლიათ იმუშაონ ისე, თითქოს შეერთებულნი არიან პირდაპირი კავშირით. პერსონალურ კომპიუტერს (პკ), რომელიც ახდენს VPN-შეერთების ინიცირებას, ეწოდება VPN-კლიენტი. პკ-ს რომელთანაც ხდება მიერთება, ეწოდება VPN-სერვერი. VPN-მაგისტრალი არის გახსნილი ქსელის კავშირის არხების მიმდევრობა, რომლის გავლითაც გადაიცემა ვკქ (VPN) პაკეტები. 1-ელ ნახაზზე მოცემულია ფირმის ორი ფილიალის ვირტუალური კერძო ქსელებით VPN კომპიუტერული კერძო ქსელის ორგანიზაციის ვარიანტი.

ნახ.1. ფირმის ორი ფილიალით კომპიუტერული კერძო ქსელის ორგანიზაცია

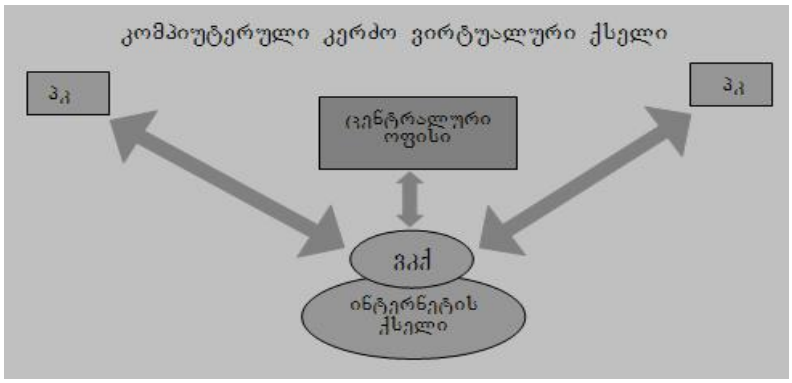
VPN საშუალებას იძლევა მოვახდინოთ დაცული შეერთება ორ კვანძს (ან ქსელებს შორის) და შევქმნათ გლობალური ქსელი (Wide Area Network; WAN) არსებული ლკქ-დან. განსხვავება

Frame Relay ან ATM ქსელებისგან მდგომარეობს სატრანსპორტო გარემოში. VPN ტრაფიკი გადაეცემა IP მისამართით და გამოიყენება დატაგრამის სატრანსპორტო დონედ, რაც საშუალებას აძლევს მას გაიაროს ინტერნეტის ქსელით. VPN-ის პროგრამული რეალიზაცია ახდენს გახსნილი სტანდარტით დაშიფრვას, რათა მოხდეს გადასაცემი მონაცემების დამალვა. დაცვის გაძლიერების მიზნით ხდება VPN-ის როგორც აპარატული გადაწყვეტის დანერგვა, ასევე პროგრამული ან პროტოკოლური რეალიზაციის საფუძველზე. VPN-ის აპარატული და პროგრამული გადაწყვეტა მოქმედებს როგორც სპეციალიზებული მარშრუტიზატორები, რომლებიც განლაგებულია ოფისებს შორის IP-შეერთებათა ბოლოებზე. როდესაც კლიენტი გადასცემს პაკეტს, ის აგზავნის მას მარშრუტიზატორის ან რაბის გავლით, რომლებიც უმატებს სინამდვილეზე შემოწმების სათაურს (Authentication Header; AH), სინამდვილისა და მარშრუტიზაციის შესახებ ინფორმაციით. შემდეგ მონაცემები კოდირდება და დეკოდირების ინსტრუქციასთან ერთად ხდება ინკაპსულირებული დაცული სასარგებლო მონაცემები (Encapsulating Security Payload; ESP). მიღებული VPN მარშრუტიზატორი აუქმებს სათაურის ინფორმაციას, ახდენს მონაცემების გაშიფვრას და მიმართავს პაკეტს დანიშნულების მიხედვით (პკ ან ქსელი). თუ გამოიყენება ქსელებსშორისი დაშიფვრა, მაშინ კვანძი პაკეტს იღებს ლკქ-ში და შემდგომ ხდება მისი დამუშავება.

კოდირება/დეკოდირების პროცესი VPN-შეერთებისას გამჭვირვალეა ლოკალური კვანძისათვის. VPN-ში სინამდვილეზე შემოწმებისა და დაშიფრვის რამდენიმე დონე გამოიყენება, ამიტომაც VPN უსაფრთხო და ეფექტურია იმისათვის, რომ გავაერთიანოთ მრავალი დაშორებული კვანძები ერთიან კკქ-ში. ზემოთ აღნიშნულის გარდა შექმნილია უსადენო ვკქ თანამგზავრის გამოყენებით. კომუტატორები, წარმადობის ამაღლების გარდა საშუალებას იძლევა შევქმნათ VPN. მისი შექმნის ერთ-ერთ მეთოდად გამოიყენება ფართომაუწყებლიანი დომენის პორტების ლოგიკური შეერთებით საკომუნიკაციო მოწყობილობის ფიზიკური ინფრასტრუქტურის შიგნით (ეს შეიძლება იყოს როგორც ინტელექტუალური კონცენტრატორი, ასევე კომუტატორი-კადრების კომუტაცია).

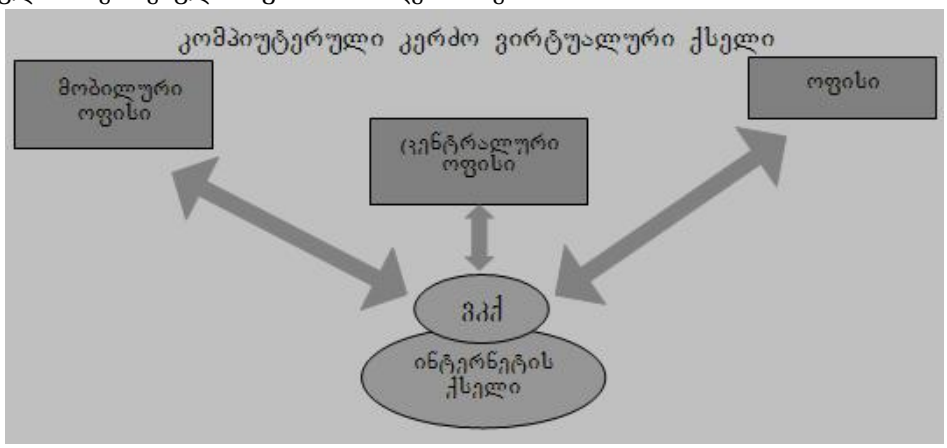
კომუტატორები დაპროგრამებულია ტრაფიკის გადადგილებაზე ლოგიკური სეგმენტების შესაბამისად და არა ფიზიკური შეერთებებით. VPN ხდება სეგმენტაციის მეთოდის უპირატეს პუნქტად, განსაკუთრებით გლობალურ ქსელებში. VPN სეგმენტირების ყველა ფუნქცია სრულდება კომუტატორების შიგნით პროგრამული უზრუნველყოფით. ვკქ-ის კონფიგურაცია, კონტროლი და მართვა ხორციელდება პროგრამულად, მოწყობილობების ფიზიკური ადგილმდებარეობის მიუხედავად. გამოყოფენ ვკქ (VPN) ორგანიზაციის სამ ძირითად მეთოდს:

1) კორპორაციის (ფირმის) თანამშრომელთა დაშორებული დაშვება კკქ-თან მოდემის ან საერთო დაშვების ქსელით (ნახ.2). ასეთი მოდელის ორგანიზაცია ითვალისწინებს VPN-სერვერის არსებობას ცენტრალურ ოფისში, რომელთანაც მიერთებული იქნება დაშორებული კლიენტები. მათ შეუძლიათ მუშაობა სახლში, ან გადასატანი კომპიუტერით ხელმისაწვდომი ინტერნეტის ქსელის პირობებში.



ნახ. 2. ვირტუალური კერძო ქსელების ორგანიზაციის პირველი მეთოდი

2) კორპორაციის (ფირმის) ტერიტორიულად განაწილებული ფილიალების ერთ საერთო ქსელში კავშირი (ნახ.3). ვკქ (VPN) ორგანიზაციის ამ მეთოდს ეწოდება ინტრანეტი Intranet VPN. ასეთი სქემით ჩართვის ორგანიზაციისათვის საჭიროა VPN სერვერი, რომელთა რაოდენობაც დამოკიდებულია მიერთებული ოფისთა რაოდენობაზე.

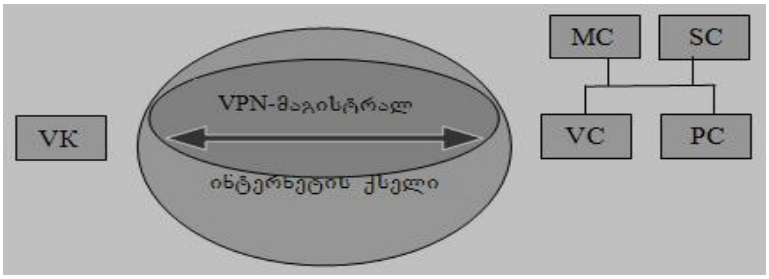


ნახ.3. ვირტუალური კერძო ქსელების ორგანიზაციის მეორე მეთოდი

3) Extranet VPN, როდესაც უსაფრთხო არხები დასაშვებია, მაშინ დაშვების ნებართვა მიეცემათ ფირმის კლიენტებსაც. ვკქ (VPN) ორგანიზაციის ასეთმა მეთოდმა მიიღო ფართო გავრცელება ელექტრონული კომერციის პოპულარობის გამო. ამ მეთოდის გამოყენებისას დაშორებულ კლიენტებს არ აქვთ შესაძლებლობა გამოიყენონ კკქ, ფირმის იმ რესურსების დაშვებაზე შეზღუდულნი არიან, რომლებიც აუცილებელია თავიანთი კლიენტებისათვის (მაგალითად, კომერციული წინადადებების საიტებთან დაშვება). ვკქ (VPN) გამოიყენება კონფიდენციალური მონაცემების გადაცემის დროს. ინფორმაციის დაცვის საშუალებას წარმოადგენს დაშიფრვის პროტოკოლები.

VPN-შეერთება შესაძლებელია არა მარტო ინტერნეტის ქსელის მეშვეობით, არამედ ლკქ-თაც. არსებობს VPN-შეერთების ორი ტიპი:

1. დაშორებულ მომხმარებლებთან შეერთება (Remote Access VPN Connection). დაშორებულ მომხმარებლებთან შეერთება მოხდება იმ შემთხვევაში, თუ ფირმის ერთეული კლიენტი მიუერთდება ლკქ-თან VPN-ის გავლით (ნახ.4.). სხვა პკ-ები, რომლებიც მიერთებულია VPN-კლიენტთან, ვერ მიიღებენ ლკქ-ის რესურსებთან დაშვებას.



ნახ. 4. დაშორებულ მომხმარებლებთან VPN-შეერთება (სადაც: VK – VPN-კლიენტი; VC – VPN-სერვერი; PC – სამუშაო სადგური; MC – Mail-სერვერი; SC – SGL-სერვერი)

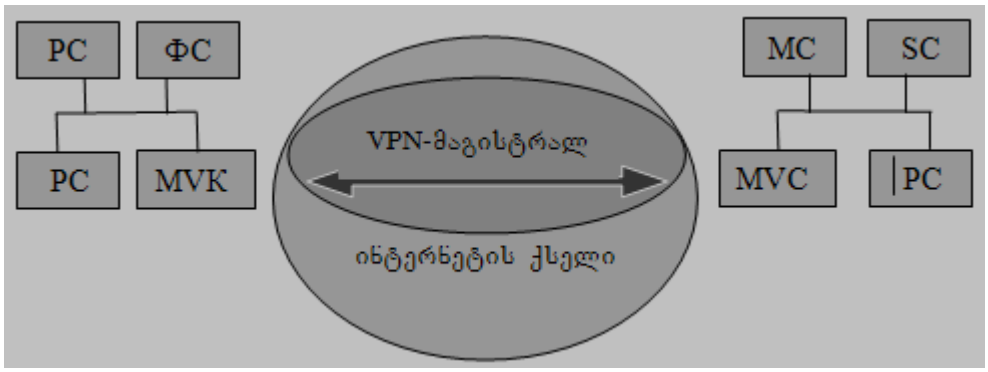
2. მარშრუტიზატორების შეერთება (Router-to-Router VPN Connection). მარშრუტიზატორების შეერთება ხდება ორ ლკქ შორის, თუ ორივე ქსელის კვანძი საჭიროებს ერთმანეთის რესურსებთან

დაშვებას (ნახ.5). ამ შემთხვევაში ერთ-ერთი მარშრუტიზატორი გამოდის VPN-სერვერის როლში, მეორე კი კლიენტის როლში.

ვკქ (VPN) გადასაცემი ინფორმაციის დასაცავად, რომელიც გადაეცემა საერთო დაშვების ქსელით გამოიყენება მრავალი პროტოკოლი, რომლებიც იყოფიან ორ ტიპად და მუშაობს წყვილად:

– პროტოკოლები ინკაპსულირებული მონაცემებით, რომლებიც აფორმირებს VPN შეერთებებს;

– პროტოკოლები, რომლებიც ახდენს მონაცემების გაშიფრვას გვირაბის შიგნით.



ნახ. 5. მარშრუტიზატორებს შორის VPN-შეერთება (სადაც: MVK – მარშრუტიზატორი (VPN-კლიენტი); MVC – მარშრუტიზატორი (VPN-სერვერი); PC – სამუშაო სადგური; ФС – ფაილური სერვერი; MC – Mail-სერვერი; SC – SGL-სერვერი)

პროტოკოლების პირველი ტიპი ახდენს გვირაბულ შეერთებებს, მეორე ტიპი ახდენს მონაცემების გაშიფრვას. სტანდარტული ანაკრების სახით წარმოდგენილია ორი პროტოკოლიდან არჩევანი:

1) PPTP (Point-to-Point Tunneling Protocol) – „წერტილი-წერტილი" გვირაბული პროტოკოლია და გამოიყენება როგორც გამფართოებელი PPP (Point-to-Point Protocol). გამოიყენება ინფორმაციის შეკუმშვისა და გაშიფრვისათვის. პროტოკოლის სტანდარტული ამორჩევისას შესაძლებელია გამოვიყენოთ გაშიფრვის მეთოდი MPPE (Microsoft Point-to-Point Encryption). შესაძლებელია მონაცემების გადაცემა გაშიფრვის გარეშე, გახსნილი სახით. მოცემული პროტოკოლით ინკაპსულაცია ხდება სათაურის დამატებით GRE (Gtntric Routing En-capsulation) და IP-ს სათაური, რომელიც მუშავდება PPP პროტოკოლით.

2) L2TP (Layer Two Tunneling Protocol) – რომელიც შექმნილია PPTP (Microsoft) და L2F (Cisco) პროტოკოლების გაერთიანებით, წარმოადგენს უფრო დაცულ შეერთებას. გაშიფრვა ხდება IP Sec (IP-security) პროტოკოლით. L2TP წარმოადგენს დაშორებული დაშვების კლიენტისათვის ჩაშენებულს Windows-ში, კლიენტი დასაწყისში ცდილობს მიუერთდეს სერვერს ამ პროტოკოლით, როგორც უფრო უსაფრთხო. მონაცემების ინკაპსულაცია ხდება სათაურის დამატებით L2TP და IPSec მონაცემებთან რომელიც დამუშავებულია PPP პროტოკოლით. მონაცემთა გაშიფვრა ხდება ალგორითმით DES (Data En-cryption Standard) ან 3DES, რის შედეგადაც მიიღწევა გადაცემული მონაცემების უსაფრთხოება.

კომპიუტერული VPN მხარდასაჭერად გამოიყენება სერვერი ISA (Internet Security and Acceleration) Server.

სერვერი რეალიზაციას უკეთებს სამდონიან ქსელთაშორის ეკრანის ფუნქციონალურ შესაძლებლობებს. სერვერი საშუალებას იძლევა:

1. VPN-კლიენტებს მიეცეს დაშვების შესაძლებლობა ქსელის რესურსებთან და სერვისებთან, თუ იგი ასრულებს VPN-სერვერის როლს;

2.ინტერნეტის ქსელთან დაშვების სიჩქარის გაზრდა Web-გვერდების კეშირების ხარჯზე;

3. გავაერთიანოთ ლკქ VPN-შეერთებებით, შემთხვევისათვის როდესაც VPN ასრულება რაბის როლს;

4. გავაფართოოთ VPN-შეერთების მონიტორინგი და ფუნქციები, რომელიც შესაძლებლობას გვაძლევს თვალყური მივადევნოთ და შევინახოთ ტრაფიკი ცალკეული დანართების დონეზე.

3. დასკვნა

ინფორმაციული ტექნოლოგიების განვითარების თანამედროვე პირობებში კომპიუტერული ვირტუალური კერძო ქსელების (ვკქ; VPN) შექმნის აუცილებლობა კონკურენტგარეშეა. კომპიუტერული VPN ძირითად უპირატესობას წარმოადგენს:

– სისტემის მასშტაბურობა. ახალი ფილიალის გახსნისას ან ფირმის ახალი თანამშრომლისთვის, რომელსაც უფლება აქვს ისარგებლოს დაშორებულ დაშვებასთან, არ სჭირდება დამატებითი ხარჯები კომუნიკაციისათვის;

– სისტემის მოქნილობა. კომპიუტერულ VPN-თვის მნიშვნელობა არ აქვს ფირმის თანამშრომელი საიდან ახორციელებს დაშვებას. გამოიყენება მობილური ოფისები, სადაც არ არის საჭირო განსაზღვრული ადგილის შერჩევა; სამუშაო ადგილის ორგანიზაციისათვის თანამშრომელი გეოგრაფიულად არ არის შემოსაზღვრული კერძო ქსელის გამოყენებაზე.

ლიტერატურა:

1. Габедава О.В., Почовян С.М. Серверные технологии. ГТУ. Тб., 2010

2. გაბედავა ო., პოჩოვიანი ს. სერვერული ტექნოლოგიები. სტუ. თბ., 2012.

THE TECHNOLOGY OF ORGANIZACION OF COMPUTER VIRTUAL PRIVATE NETWORKS ON THE BASIC OF CLIENT-SERVAR ARCHITECTURE

Gabedava Omar, Pochovyan Simon
Georgian Technology University

Summary

In the article there is considered the technology of the computer virtual private networks (VPN) organization on the basis of client-server architecture. There are described a purpose, technical realization and methods of organization of computers (VPN), the types of VPN-protocols for the protection of transferred information in the computer (VPN), and the functional possibility of server.

ТЕХНОЛОГИЯ ОРГАНИЗАЦИИ КОМПЬЮТЕРНЫХ ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЕЙ НА ОСНОВЕ КЛИЕНТ-СЕРВЕРНОЙ АРХИТЕКТУРЫ

Габедава О.В., Почовян С.М.
Грузинский Технический Университет

Резюме

Рассмотрена технология организации компьютерных виртуальных частных сетей (ВЧС, VPN) на основе клиент-серверной архитектуры. Описаны назначение, программная и техническая реализация и способы организации компьютерных ВЧС (VPN), типы VPN-

соединений, протоколы для защиты передаваемой информации в компьютерных ВЧС (VPN), а также функциональные возможности сервера.