ISSN 1512-1232

უსაფრთხო კავშირის არხის აგების ასპექტები ვირტუალური კერძო ქსელის (VPN) ბაზაზე

იოსებ ქართველიშვილი, თეა თოდუა
საქართველოს ტექნიკური უნივერსიტეტი, ქ. თბილისი, კოსტავას 77

ანოტაცია

ინფორმაციული ტექნოლოგიები გადამწყვეტ როლს თამაშობენ ნებისმიერი კომპანიის ეფექტურად ფუნქციონირებასა და მართვაში. საჭირო ინფორმაციის ოპერატიულად ხელმისაწვდომობის პირობებში შესაძლებელია სწორად შეფასდეს მიმდინარე სიტუაცია და მიღებული იქნას დროული გადაწყვეტილება. იმავდროულად, ინფორმაცია ხელმისაწვდომი უნდა იყოს მხოლოდ მათთვის, ვისთვისაც ის განკუთვნილია და დაფარული – სხვა უცხო პირთათვის. მას შემდეგ, რაც სხვადასხვა კომპანიებმა და ორგანიზაციებმა თავიანთ საქმიანობაში აქტიურად დაიწყეს კომპიუტერების გამოყენება, გაჩნდა მოთხოვნილება იმისა, რომ ეს კომპიუტერები, მონაცემთა სწრაფი გადაცემისთვის და ეფექტური ურთიერთქმედებისთვის, გაერთიანებული ყოფილიყვნენ ერთ საერთო ქსელში, ამასთან, ეს კავშირი აუცილებლად უნდა ყოფილიყო საიმედო და დაცული. ზემოთ აღნიშნულიდან გამომდინარე, ორგანიზაციები დაინტერესდნენ ინტერნეტ არხების გამოყენების შესაძლებლობებით. თუმცა, ინტერნეტის აგების პრინციპები ბოროტმოქმედებს შესაძლებლობას უქმნის, მოიპაროს და განზრახ დაამახინჯოს ინფორმაცია. კორპორაციული და საუწყებო ქსელები, რომლებიც დაფუძნებულია TCP/IP პროტოკოლების ბაზაზე და აგებულია სტანდარტულ ინტერნეტ-დანართებზე (E-mail, Web, FTP), უცხო პირთა შეჭრისგან გარანტირებული არ არის. სტატიაში განხილულია ვირტუალური კერძო ქსელების VPN (Virtual Private Network) აგების ტექნოლოგია, რომელიც უსაფრთხო კავშირის არხის შესაქმნელად დღეისათვის ერთ-ერთ ყველაზე ოპტიმალურ ვარიანტს წარმოადგენს.

საკვანძო სიტყვები: ვირტუალური კერძო ქსელი (VPN), უსაფრთხო კავშირის არხი

ბიზნესსა თუ საბანკო სფეროში ქსელური იერიშების წინააღმდეგ ეფექტურად საბრძოლველად და კომპიუტერული ქსელის აქტიური და უსაფრთხო გამოყენების შესაძლებლობის უზრუნველსაყოფად, XX საუკუნის 90–იანი წლების დასაწყისში შეიქმნა და აქტიურად ვითარდება ვირტუალური კერძო ქსელების აგების კონცეფცია – VPN (Virtual Private Network). სიტყვა „ვირტუალური“ VPN ტერმინში ჩართულია იმისათვის, რათა ხაზი გაესვას, რომ ორ კვანძს შორის შეერთება განხილული უნდა იყოს, როგორც დროებითი, რამდენადაც ის არ არის მუდმივი (მყარი) შეერთება და არსებობს მხოლოდ ღია ქსელში ინფორმაციული ნაკადების გადაცემის დროს. ვირტუალური კერძო გვირაბებისა და ქსელების ტექნიკური რეალიზაცია ისტორიულად მიმდინარეობდა ორი მიმართულებით:

ISSN 1512-1232

- ვირტუალური არხების ორგანიზაციის ჩაშენებული მექნიზმების გამოყენების გზით, ქსელის საერთო ინფრასტრუქტურის ორ წერტილს შორის შეერთების შერწყმის აგება (frame relay), რომელიც იზოლირებულია სხვა მომხმარებლებისგან.
- გვირაბის შექმნის ტექნოლოგიის გამოყენების გზით ქსელის ორ კვანძს შორის ვირტუალური IP-გვირაბის აგება, რომლის დროსაც ყოველი IP-პაკეტი იშიფრება და გადაინაცვლებს სპეციალური სახის ახალი პაკეტის მონაცემთა ველში.

ვირტუალური კერძო ქსელის შექმნისთვის პირველი თანამედროვე ქსელური ტექნოლოგია გახდა კადრების რეტრანსლაციის სამსახური (frame relay). აღნიშნული ქსელი ამარტივებს შეერთებების შექმნას, რადგან, იმისთვის, რომ იმუშაოს, საჭიროა მხოლოდ კვანძის მიერთება პროვაიდერთან. მარშრუტიზატორები კი მონაცემებს თვითონ მიმართავენ საჭირო მისამართისკენ, ამასთან, მისი გამოყენება გაცილებით იაფია. თუმცა, frame relay ქსელი არ პასუხობდა მობილური მომხმარებლების მოთხოვნებს და ორგანიზაციები იძულებული ხდებოდნენ გამოეყენებინათ მოდემური კავშირი, რაც მობილური ჩართვების მოთხოვნილებების გაზრდის შესაძლებლობას არ იძლევა. აქედან გამომდინარე, საჭირო გახდა საერთო გადაწყვეტილების მიღება, რომელიც უზრუნველყოფდა არა მარტო კორპორაციული ტრაფიკის უსაფრთხოებას, არამედ მოქნილობას ჩართვისა და გამართვის დროს.

მას შემდეგ, რაც გაჩნდა ქსელური სერვისები, დაცალკევებული ქსელების კვანძების შეერთებისთვის, შესაძლებელი გახდა ვირტუალური კერძო (დაცული) ქსელის, VPN-ის აქტიურად გამოყენება, რომელიც დაფუძნებულია ინტერნეტის ბაზაზე. ასეთი გადაწყვეტა გაცილებით იაფი აღმოჩნდა, წინა მიდგომებთან შედარებით. ყოველივე ამან, შესაძლო გახადა აქტიურად ყოფილიყო გამოყენებული ინტერნეტის ერთ-ერთი ძირითადი ღირსება – იოლი ხელმისაწვდომობა. აქედან გამომდინარე, ნებისმიერ ადამიანს ინტერნეტ კავშირის დახმარებით ადვილად შეეძლო ბანკთან ან სხვადასხვა კომპანიასთან დაკავშირება დედამიწის ნებისმიერი წერტილიდან. თუმცა, ინტერნეტ მონაცემების გახსნილობიდან გამომდინარე, ამ ქსელით გადაცემული მონაცემები ყველასთვის ხელმისაწვდომია მისი წაკითხვისა თუ ცვლილების მიზნით. ამიტომ ინტერნეტზე დაფუძნებულ VPN ქსელებს გააჩნიათ VPN კვანძებს შორის გადაცემული ინფორმაციების დაცვის საშუალებები. ამის გამო, მოცემულ ქსელებს ჩვეულებრივ უწოდებენ ვირტუალურ დაცულ ქსელებს VPN (Virtual Private Networks), ტერმინი Private ამ კონტექსტში ნიშნავს „კერძოს“, „დაცულს“.

ინტერნეტის ბაზაზე აგებული VPN ქსელის საფუძველს წარმოადგენს ორი ძირითადი ტექნოლოგია. პირველი – ეს არის გვირაბის წარმოქმნა (ტუნელირება), რომელიც საშუალებას იძლევა შეიქმნას ვირტუალური არხები, მეორე არის გადაცემული ინფორმაციების კონფიდენციალობისა და უვნებლობის უზრუნველყოფის, ასევე მომხმარებლის აუტენტიფიკაციისა და ავტორიზაციის სხვადასხვა მეთოდი. აუტენტიფიკაცია (Authentication) არის უტყუარობის მტკიცება, სუბიექტისა და მისი შესაბამისობის შემოწმების პროცედურა, უნიკალური ინფორმაციის, უმარტივეს შემთხვევაში – სახელისა და პაროლის დახმარებით. ავტორიზაცია (Authorization) აუცილებელი პარამეტრების შემოწმების პროცესია, ასევე პროცესის შედეგი და პირზე ან პირთა ჯგუფზე განსაზღვრული უფლებამოსილების გადაცემა (ხელმისაწვდომობის უფლება), შეზღუდული ხელმისაწვდომობის სხვადასხვა

ISSN 1512-1232

სისტემაში ზოგიერთი მოქმედების შესასრულებლად. VPN ტექნოლოგიის განვითარებამ გამოიწვია მისი დაკავშირება ინფორმაციის დაცვის კრიპტოგრაფიულ მეთოდებთან.

ვირტუალურად დაცული ქსელების აგების კონცეფციას საფუძვლად უდევს საკმაოდ მარტივი იდეა: თუ გლობალურ ქსელში არის ორი კვანძი, რომელთაც უნდათ ინფორმაციის გაცვლა, მაშინ ამ ორ კვანძს შორის აუცილებელია აიგოს ვირტუალურად დაცული გვირაბი, ღია ქსელით გადაცემული ინფორმაციის კონფიდენციალობისა და დაუზიანებლობის უზრუნველსაყოფად. ამ გვირაბთან ხელმისაწვდომობა უნდა იყოს ძალიან გართულებული, ყველა შესაძლო აქტიური და პასიური გარე დამკვირვებლისათვის. მაგალითად, ასეთი ვირტუალური გვირაბების შექმნით ბანკებს შეუძლიათ მიიღონ ფინანსური საშუალებების მნიშვნელოვანი ეკონომია. ბანკს შეუძლია უარი თქვას საკუთარი Internet/extranet--ქსელების შექმნისთვის ძვირადღირებული განცალკევებული არხების აგებაზე ან იჯარაზე და გამოიყენოს ამისთვის იაფი ინტერნეტ-არხები, რომლის გადაცემის სიჩქარე და საიმედობა არ ჩამორჩება განცალკევებულ ხაზებს. თუმცა, კორპორაციული ლოკალური ქსელის ღია ქსელთან ჩართვისას ჩნდება ორი ძირითადი ტიპის თავდასხმის საფრთხე:

– კორპორაციული ლოკალური ქსელების შიგა რესურსებთან არასანქცირებული წვდომა, რომელსაც ბოროტმოქმედი იღებს ამ ქსელში არაავტორიზებული შესვლის შედეგად;

– კორპორაციულ მონაცემებთან არასანქცირებული წვდომა, ღია ქსელში მათი გადაცემის პროცესში.

ლოკალური ქსელებისა და ცალკეული კომპიუტერების ღია ქსელით, კერძოდ ინტერნეტ ქსელით საინფორმაციო ურთიერთქმედების უსაფრთხოების უზრუნველყოფა შესაძლებელია შემდეგი ამოცანების ეფექტურად გადაჭრის გზით:

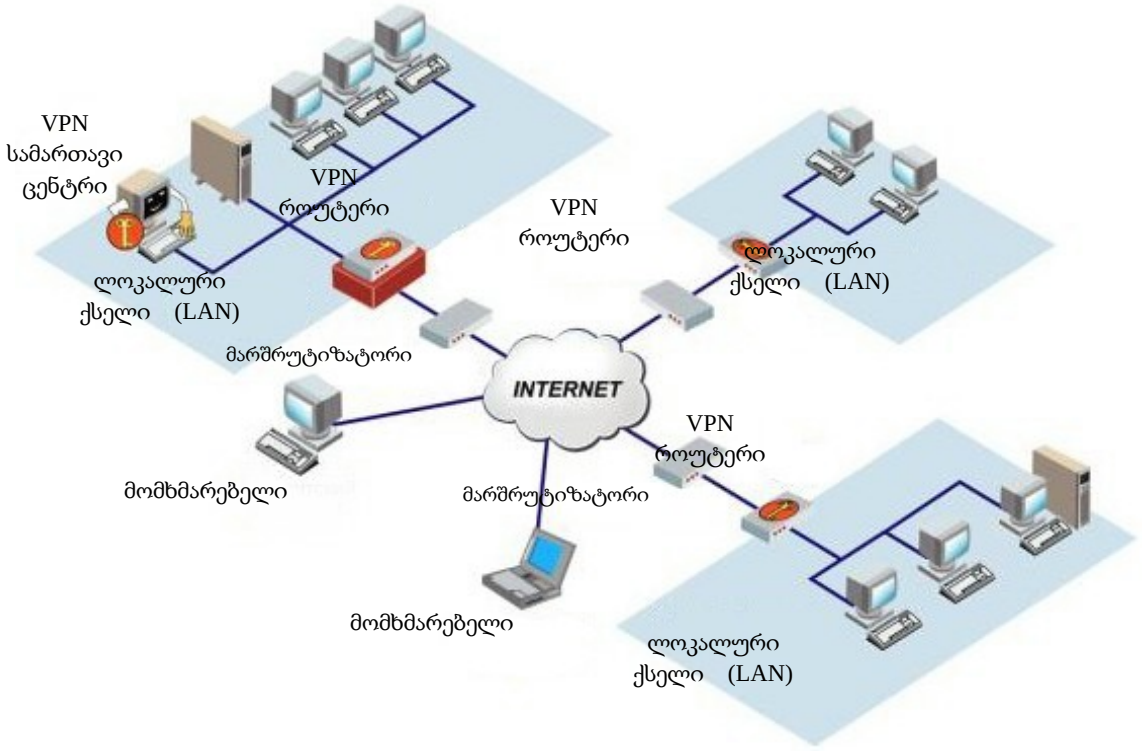
– ღია არხებთან ჩართული ლოკალური ქსელებისა და მოქმედი კომპიუტერების კავშირების დაცვა გარედან არაავტორიზებული მოქმედებისგან;

– ინფორმაციის დაცვა, მისი კავშირის ღია არხებით გადაცემის პროცესში.

ლოკალური ქსელებისა და ცალკეული კომპიუტერების გარემოდან არასანქცირებული მოქმედებისგან დასაცავად, ჩვეულებრივ იყენებენ ქსელთაშორის ეკრანებს (Firewalls). მას ათავსებენ ლოკალურ და ღია ქსელებს შორის. ცალკეული დაშორებული კომპიუტერის დაცვისთვის, რომელიც შეერთებულია ღია ქსელში, ამ კომპიუტერზე აინსტალირებენ ქსელური ეკრანის პროგრამულ უზრუნველყოფას და ასეთ ქსელურ ეკრანს უწოდებენ პერსონალურს.

ინფორმაციის დაცვა ღია არხებით მისი გადაცემის პროცესში დაფუძნებულია ვირტუალური დაცული VPN ქსელების გამოყენებაზე. ვირტუალურად დაცულ VPN ქსელებს უწოდებენ ლოკალური ქსელებისა და ცალკეული კომპიუტერების გაერთიანებას ერთიან ვირტუალურ კორპორაციულ ქსელში, რომელიც უზრუნველყოფს ცირკულირებად მონაცემთა უსაფრთხოებას. ვირტუალური დაცული VPN ქსელები ფორმირდება ვირტუალური დაცული კავშირის არხების აგების გზით. ამ ვირტუალურ დაცულ კავშირის ხაზებს უწოდებენ VPN გვირაბებს. VPN ქსელი საშუალებას იძლევა VPN გვირაბების დახმარებით ერთმანეთთან დააკავშიროს ცენტრალური ოფისი, ფილიალების ოფისები, ბიზნეს-პარტნიორების ოფისები, მომხმარებლები, იმისათვის რომ ინტერნეტის საშუალებით უსაფრთხოდ მოხდეს ინფორმაციის მიმოცვლა (ნახ. 1).

ISSN 1512-1232



ნახ.1. VPN ქსელი

VPN გვირაბი წარმოადგენს ღია ქსელში დამყარებულ კავშირს, რომლითაც გადაეცემა ვირტუალური ქსელის შეტყობინებების კრიპტოგრაფიულად დაცული ინფორმაციული პაკეტები. ინფორმაციის დაცვა, მისი VPN გვირაბით გადაცემის პროცესში დაფუძნებულია შემდეგი ფუნქციების შესრულებასთან:

- ურთიერთმოქმედი მხარეების აუტენტიფიკაცია;
- გადასაცემი მონაცემების კრიპტოგრაფიული დაშიფვრა;
- გადაცემული ინფორმაციის უტყუარობისა და უვნებლობის შემოწმება.

ასეთი დაცვის ეფექტურობა უზრუნველყოფილია სიმეტრიული და ასიმეტრიული კრიპტოგრაფიული სისტემების ერთობლივი გამოყენების ხარჯზე. VPN მოწყობილობებით ფორმირებულ VPN გვირაბს გააჩნია დაცული გამოყოფილი ხაზის თვისებები. ამასთან, ეს დაცული გამოყოფილი ხაზი იშლება საერთო კავშირის მქონე ქსელის ჩარჩოებში, მაგალითად, ინტერნეტ VPN მოწყობილობებს ვირტუალურ კერძო ქსელებში შეუძლიათ ითამაშონ VPN-კლიენტის ან VPN-სერვერის როლი. VPN-კლიენტი წარმოადგენს პროგრამულ ან პროგრამულ-აპარატულ კომპლექსს, რომელიც ჩვეულებრივ სრულდება პერსონალური კომპიუტერის ბაზაზე. მისი ქსელური პროგრამული უზრუნველყოფა მოდიფიცირდება ინფორმაციული ნაკადის დაშიფვრისა და აუტენტიფიკაციის შესასრულებლად, რომლითაც ეს მოწყობილობა ურთიერთგაცვლის ოპერაციებს ატარებს სხვა VPN-კლიენტებთან ან VPN-სერვერებთან. VPN-სერვერი წარმოადგენს პროგრამულ ან პროგრამულ-აპარატულ კომპლექსს, რომელიც დაყენებულია კომპიუტერზე და ასრულებს სერვერის ფუნქციებს. VPN-სერვერი უზრუნველყოფს სერვერების დაცვას გარემოდან არასანქცირებული წვდომისგან, ასევე ცალკეულ კომპიუტერებთან და შესაბამისი VPN-პროდუქტებით დაცული ლოკალური ქსელის სეგმენტის კომპიუტერებთან დაცული შეერთების

ISSN 1512-1232

ორგანიზაციას. VPN-სერვერი წარმოადგენს VPN-კლიენტის ფუნქციონალურ ანალოგს, სერვერული პლატფორმისთვის. ის, უპირველეს ყოვლისა, გამოირჩევა გაფართოებული რესურსებით, VPN-კლიენტებთან მრავალრიცხოვანი შეერთებების მხარდასაჭერად. VPN-სერვერს აგრეთვე შეუძლია მხარი დაუჭიროს მობილურ მომხმარებელთან დაცულ შეერთებასაც.

ვირტუალურად დაცული კერძო VPN ქსელების აგების ტექნოლოგიები სულ უფრო და უფრო მეტ ყურადღებას იქცევს მსხვილი კომპანიების მხრიდან (ბანკები, უწყებები, მსხვილი სახელმწიფო სტრუქტურები და სხვ.). მსგავსი ინტერესის მიზეზი იმაში მდგომარეობს, რომ VPN ტექნოლოგიები ასეთ კომპანიებს საშუალებას აძლევს, არა მარტო მნიშვნელოვნად შეამციროს თავიანთი ხარჯები დაშორებულ ქვეგანყოფილებებთან (ფილიალებთან) დასაკავშირებლად გამოყოფილი არხების გასამართავად, არამედ აამაღლოს ინფორმაციის გაცვლის კონფიდენციალობა. VPN–ის გამოყენება უზრუნველყოფს დაცული გვირაბების ორგანიზებას, როგორც კომპანიის ოფისებს შორის, ისე ცალკეულ მუშა სადგურებსა და სერვერებთან. ამასთან, მნიშვნელობა არ აქვს, ინტერნეტის რომელი პროვაიდერით ჩაერთვება კონკრეტული მუშა სადგური საწარმოს დაცულ რესურსებთან. ყველაფერს, რასაც უცხო დამკვირვებელი დაინახავს, არის ჩვეულებრივი IP-პაკეტების ნაკადი, ამოუცნობი შიგთავსით. მოდემების ან გამოყოფილი ხაზების საშუალებით ინტერნეტ მომხმარებლებს შორის დაკავშირების ტრადიციული მეთოდის ნაცვლად შემოდის ვირტუალური კერძო ქსელები – VPN , რომლებიც მომხმარებლებს საშუალებას აძლევს თავისუფლად დაუკავშირდნენ ერთმანეთს ინტერნეტის საშუალებით.

არსებობს VPN კლასიფიკაციის სხვადასხვა ვარიანტი. ტექნიკური გადაწყვეტილების არქიტექტურის მიხედვით გამოიყოფა ვირტუალური კერძო ქსელების სამი ძირითადი სახე:

- შიდაკორპორაციული VPN;
- VPN დაშორებული წვდომით;
- კორპორაციათაშორისი VPN.

შიდაკორპორაციული ქსელები VPN (Intranet VPN) განკუთვნილია საწარმოს შიგნით ქვეგანყოფილებების ან საწარმოთა ჯგუფებს შორის დაცული ურთიერთქმედების უზრუნველსაყოფად, რომლებიც გაერთიანებული არიან კავშირის კორპორაციული ქსელებით, გამოყოფილი ხაზების ჩათვლით.

ვირტუალური კერძო ქსელები VPN დაშორებული წვდომით (Remote Access VPN) განკუთვნილია დაშორებულ კორპორაციულ ინფორმაციულ რესურსებს შორის უსაფრთხო წვდომის უზრუნველსაყოფად.

კორპორაციათაშორისი VPN (Extranet VPN) გათვალისწინებულია სტრატეგიულ პარტნიორებს შორის ინფორმაციის უსაფრთხო გაცვლის უზრუნველსაყოფად. აგრეთვე უზრუნველყოფს პირდაპირ წვდომას ერთი კომპანიის ქსელიდან მეორე კომპანიის ქსელთან და ამით ხელს უწყობს კავშირის საიმედოობას.

ზემოთაღნიშნულიდან გამომდინარე შეგვიძლია დავასკვნათ, რომ მოშორებულ კომპიუტერებს შორის, რომლებიც იყენებენ გლობალური ქსელის – ინტერნეტის ინფრასტრუქტურას, უსაფრთხო კავშირის არხის შექმნისთვის, ვირტუალური კერძო ქსელების VPN (Virtual Private Network) აგების ტექნოლოგია დღეისათვის წარმოადგენს ერთ-ერთ ყველაზე ოპტიმალურ ვარიანტს. წამოჭრილი საკითხი უაღრესად აქტუალურია, ვინაიდან საიმედო კავშირი, რომლის საშუალებითაც შესაძ-

ISSN 1512-1232

ლებელია გადაიცეს კონფიდენციალური ინფორმაცია, აუცილებელია ადამიანის მოღვაწეობის უამრავ სფეროში, მაგალითად, საბანკო საქმეში, ელექტრონულ კომერციაში და სხვა. ვირტუალური კერძო ქსელები ძალზედ მოსახერხებელია აღნიშნული ამოცანის გადასაჭრელად და ადამიანების უმრავლესობა გლობალურ ქსელში სხვადასხვა ტიპის კავშირების დასამყარებლად VPN ტექნოლოგიას მიიჩნევს ერთ-ერთ ყველაზე მძლავრ და მოსახერხებელ საშუალებად.

ლიტერატურა:

1. ი. ქართველიშვილი, ო. შონია, ზ. ბერიძე, ი. შონია. ვირტუალურ კერძო ქსელებში (VPN) სიმბოლოების დაშიფრვის კომბინირებული მეთოდი. საქართველოს ტექნიკური უნივერსიტეტი, მართვის ავტომატიზებული სისტემები N1(12), თბილისი, 2012წ.
2. Б.Ф.Шаньгин. Комплексная защита информации в корпоративных системах. М., ИД ,,ФОРУМ-инфра-м,” 2010;
3. Markus Feilner. OpenVPN - Building and Integrating Virtual Private Networks. 2007.

Article received 2014-09-24