თბილისის სახელმწიფო უნივერსიტეტის ზუსტ და საბუნებისმეტყველო მეცნიერებათა ფაკულტეტი

შოთა ნოზაძე

VPN უსაფრთხოების ანალიზი

ინფორმაციული ტექნოლოგიების სამაგისტრო პროგრამა

ინფორმაციული ტექნოლოგიების მაგისტრი

სამაგისტრო ნაშრომის ხელმძღვანელი - ლელა მირცხულავა, დოქტორი, ასოცირებული პროფესორი

თბილისი

2021

სარჩევი

ანოტაცია

ქსელში გადაცემისას ინფორმაცია ხშირად ხდება პირდაპირი შეტევების საგანი, რომელიც გამოიხატება მისი მიტაცებისა თუ ცვლილების სახით. ყოველდღიურმა დაკვირვებებმა ცხადყო, რომ ღია ქსელში გადაცემული ინფორმაციის არასანქცირებულად მოპოვება ამ დარგში საშუალო ცოდნის მქონე ნებისმიერ პირს უპრობლემოდ შეუძლია.

ჩვენი მიზანია, განვიხილოთ ჩვენივე პირადი ინფორმაციის დაცვისთვის შემუშავებული ერთ-ერთი მეთოდი, რომელიც ღია ქსელების ბაზაზე დაფუძნებული ქვე-ქსელების ანუ ვირტუალური კერძო ქსელის სახელითაა ცნობილი.

განხილვის პროცესში ჩვენ შევქმნით, და დავაკონფიგურირეთ შესაბამისი ვირტუალური კექრძო ქსელი, რომელშიც გათვალისწინებული იქნება დაშიფვრის პროტოკოლები, რის შედეგადაც კონკრეტულ ქსელში გამავალი სენსიტიური ინფორმაცია იქნება მაქსიმალურად დაცული გარე ზემოქმედებისგან.

Annotation

The information exchanged through network communications often becomes the subject of a direct attack, which manifests itself in the form of its capture or change. Daily observations have shown that any person with average knowledge in this field can obtain information transmitted on the public network without any problems.

Our goal is to consider one of the methods developed for the protection of our own personal information, known as public network-based subnets, or virtual personal network(VPN).

During the review process, we will create, and configure the appropriate virtual network, which will include encryption protocols, so that sensitive information coming out of a particular network will be maximally protected from external influences.

შესავალი

ორგანიზაციები კომუნიკაციებისთვის ჰეტეროგენულ ქსელურ გარემოში იყენებენ TCP/IP პროტოკოლების ნაკრებს, რომელიც უზრუნველყოფს თავდებადობას სხვადასხვა ტიპის მოწყობილობებს შორის. ამ პროტოკოლების ნაკრებმა მოიპოვა პოპულარობა ინტერნეტის გლობალური ვირტუალური ქსელის თავსებადობისა და ხელმისაწვდომობის გამო და გახდა ინტერნეტის ეტალონური მოდელი შესაბამისი სტანდარტებით. ამასთან, TCP/IP პროტოკოლის სტეკის საყოველთაობამ გამოავლინა მისი სისუსტეებიც [1-5].

სწორედ ამიტომ ცალკეულ ქსელებზე შეტევის განხორციელება მარტივია, რადგან მათი კომპონენტები, როგორც წესი, იყენებენ მონაცემთა გადაცემის ღია არხებს, ხოლო შემკვეთს არა მხოლოდ პასიურად შეუძლია მოუსმინოს გადაცემულ ინფორმაციას, არამედ შეცვალოს გადაცემული ტრაფიკი.

დისტანციური შეტევის გამოვლენის სირთულე და მათი განხორციელების შედარებითი სიმარტივე (თანამედროვე სისტემების ზედმეტი ფუნქციონირების გამო) ხელს უწყობს ამ ტიპის უკანონო ქმედებებს და ყველაზე დიდ საშიშრობას წარმოადგენს, რაც აფერხებს ამ საფრთხეზე დროულ რეაგირებას, რის შედეგადაც თავდამსხმელისთვის შეტევის წარმატებით განხორციელების შანსები იზრდება.

საიტებსა და მომხმარებლებს შორის ქსელის ტრაფიკის უზრუნველსაყოფად, ორგანიზაციები იყენებენ ვირტუალურ კერძო ქსელებს (VPN), რათა შექმნან ქსელებს შორის კერძო ქსელური კავშირები. VPN ვირტუალურია იმით, რომ იგი ავრცელებს ინფორმაციას კერძო ქსელის შიგნით, მაგრამ ეს ინფორმაცია ტრანსპორტირდება საჯარო ქსელის საშუალებით. VPN კერძოა იმით, რომ ტრაფიკი დაშიფრულია იმისთვის, რომ მონაცემები კონფიდენციალური იყოს იმისდა მიუხედავად, რომ ისინი საზოგადოებრივ ქსელში მოძრაობს [6-13].

პირველი ტიპის VPN იყო მკაცრი IP გვირაბი, რომელიც არ შეიცავდა მონაცემების ავთენტიფიკაციას ან დაშიფვრას. მაგალითად, Generic Routing Encapsulation (GRE) არის გვირაბის პროტოკოლი, რომელიც შემუშავებულია Cisco-ს მიერ და არ შეიცავს დაშიფვრის სერვისებს. ის გამოიყენება IP გვირაბის შიგნით IPv4 და IPv6 ტრაფიკის კაფსულაციისთვის ვირტუალური Point-to-point კავშირების შესაქმნელად.

თავი. I. VPN და მისი უპირატესობები

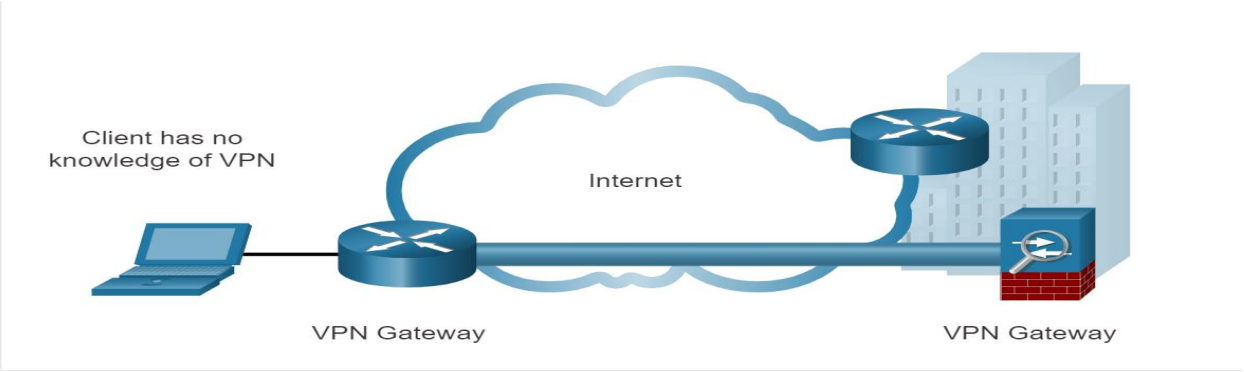
თანამედროვე VPN-ს აქვს დაშიფვრის მახასიათებლების მხარდაჭერა, როგორიცაა ინტერნეტის პროტოკოლის დაცვა (IPsec) და უსაფრთხო სოკეტების ფენის (SSL) VPN ქსელის ტრაფიკის უზრუნველსაყოფად. VPN–ს ძირითადი უპირატესობები მოცემულია ცხრილში 1.

ცხრილი 1

უპირატესობები	აღწერა
ნაკლები ღირებულება	ხარჯთეფექტური, მაღალი გამტარუნარიანობის ტექნოლოგიების გაჩენასთან ერთად, ორგანიზაციებს შეუძლიათ VPN–ების გამოყენება, მათი კავშირის ხარჯების შესამცირებლად, დისტანციური კავშირის გამტარობის გაზრდისას
დაცულობა	VPN უზრუნველყოფს უსაფრთხოების ყველაზე მაღალ დონეს, გაფართოებული დაშიფვრისა და ავთენტიფიკაციის პროტოკოლების გამოყენებით, რომლებიც მონაცემებს უნებართვო წვდომისგან იცავს
მაშტაბურობა	VPN საშუალებას აძლევს ორგანიზაციებს გამოიყენონ ინტერნეტი, რითაც მარტივდება ახალი მომხმარებლების დამატება მნიშვნელოვანი ინფრასტრუქტურის დამატების გარეშე
კომფორტულობა	VPN–ების განხორციელება WAN–ის ბმულების მრავალფეროვან ვარიანტშია შესაძლებელი, მათ შორის ყველა პოპულარული სამაუწყებლო ტექნოლოგია. დისტანციურ მუშაკებს შეუძლიათ ისარგებლონ ამ ჩქაროსნული კავშირით, რათა მიიღონ უსაფრთხო წვდომა თავიანთ კორპორაციულ ქსელებზე

1.1. Point-to-point და დისტანციური წვდომის VPN

წერილოვანი VPN იქმნება მაშინ, როდესაც VPN ეყრდნობა წერტილოვან მოწყობილობებს, რომლებსაც ასევე უწოდებენ VPN gataway-ს, წინასწარ განსაზღვული კონფიგურაციით უსაფრთხო გვირაბის დასადგენად. VPN ტრაფიკი დაშიფრულია მხოლოდ ამ მოწყობილობებს შორის. გარე ქსელს, ჰოსტს, არ აქვს ინფორმაცია, რომ VPN გამოიყენება.



სურ. 1.1. VPN gataway 1

დისტანციურად წვდომის VPN იქმნება დინამიურად, კლიენტისა და VPN მოწყობილობას შორის უსაფრთხო კავშირის უზრუნველსაყოფად. მაგალითად, დისტანციური წვდომის SSL VPN გამოიყენება მაშინ, როდესაც თქვენს საბანკო ინფორმაციას ინტერნეტით ამოწმებთ.

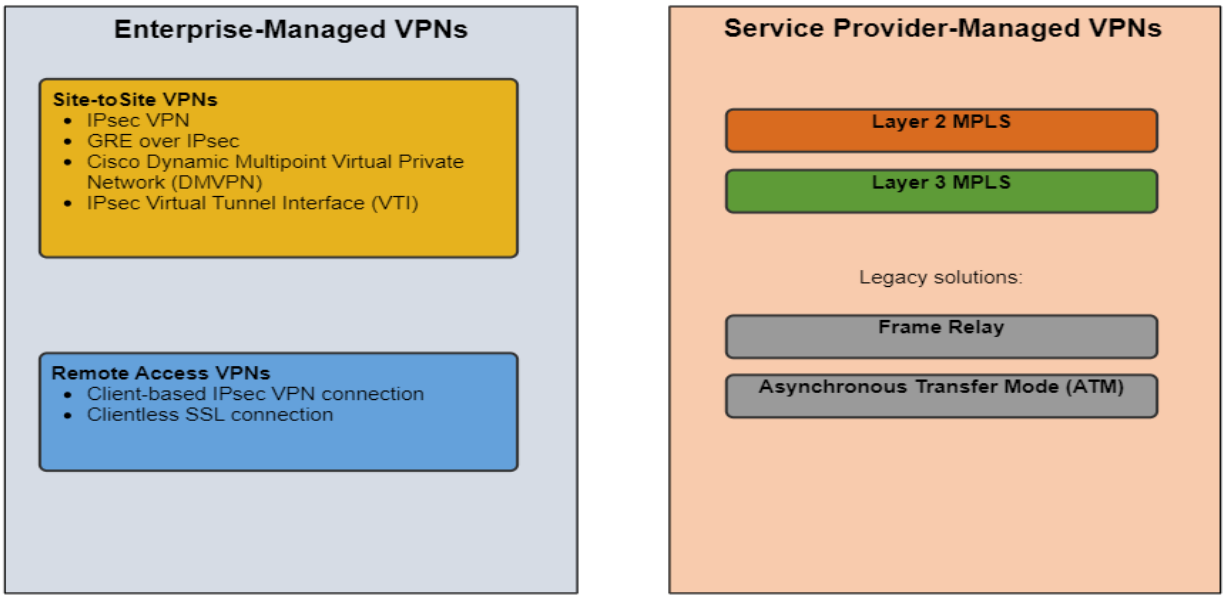
1.2. ორგანიზაციისა და მომსახურების მიმწოდებელი VPN

ორგანიზაციისთვის ტრაფიკის უზრუნველსაყოფად ბევრი განსხვავებული გზაა ხელმისაწვდომი. ეს გადაწყვეტილებები დამოკიდებულია იმაზე, თუ ვინ მართავს VPN-ს.

VPN– ების მართვა და განთავსება შესაძლებელია შემდეგნაირად:

- ორგანიზაციის VPN - ორგანიზაციის მიერ მართული VPN არის საერთო გადაწყვეტა ინტერნეტით ორგანიზაციას ტრაფიკის უზრუნველსაყოფად. წერტილოვან და დისტანციურ წვდომის VPN ქმნის და მართავს ორგანიზაცია, როგორც IPsec, ასევე SSL VPN.
- სერვისის პროვაიდერის VPN - მომსახურების მიმწოდებლის მიერ მართული VPN იქმნება და იმართება პროვაიდერის ქსელში. პროვაიდერი იყენებს Multiprotocol Label Switching (MPLS) Layer 2 ან Layer 3 დონეებზე, წერილებს შორის უსაფრთხო არხების შესაქმნელად. MPLS არის მარშრუტიზაციის ტექნოლოგია, რომელსაც პროვაიდერი იყენებს ვირტუალური ბილიკების შესაქმნელად. ეს ეფექტურად გამოყოფს ტრაფიკს სხვა მომხმარებელთა ტრაფიკისგან. სხვა მემკვიდრეობითი გადაწყვეტილებები მოიცავს Frame Relay-ს და Asynchronous Transfer Mode (ATM) VPN-ს.

სურათზე ჩამოთვლილია ორგანიზაციას მიერ მართული და მომსახურების მიმწოდებლის მიერ მართული VPN განლაგების სხვადასხვა ტიპები, რომელზეც უფრო დეტალურად ვისაუბრებთ ამ მოდულში.



სურ.1.2. VPN– ების ტიპები

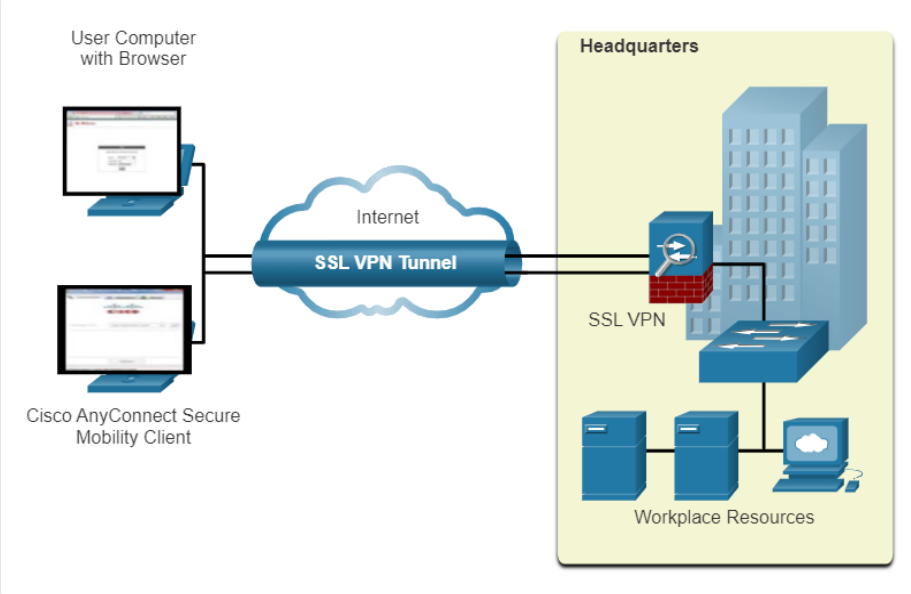
1.3. დისტანციური წვდომის VPN

წინა ნაწილში გავეცანით VPN– ის საფუძვლებს. აქ გავეცნობით VPN-ის ტიპებს.

VPN მრავალი მიზეზის გამო გახდა დისტანციური წვდომის კავშირის ლოგიკური გადაწყვეტა. როგორც სურათზეა ნაჩვენები, დისტანციური წვდომის VPN საშუალებას აძლევს დისტანციური და მობილური მომხმარებლები უსაფრთხოდ დაუკავშირდნენ ორგანიზაციას დაშიფრული გვირაბის შექმნით. დისტანციურ მომხმარებლებს შეუძლიათ უსაფრთხოდ გამოიყენონ თავიანთი ორგანიზაციის უსაფრთხო წვდომა, მათ შორის ელექტრონული ფოსტა და ქსელური პროგრამები. დისტანციური წვდომის VPN ასევე საშუალებას აძლევს კონტრაქტორებსა და პარტნიორებს შეზღუდული წვდომა ჰქონდეთ კონკრეტულ სერვერებზე, ვებგვერდებზე ან ფაილებზე, საჭიროებისამებრ. ეს ნიშნავს, რომ ამ მომხმარებლებს შეუძლიათ წვლილი შეიტანონ ბიზნესის პროდუქტიულობაში ქსელის უსაფრთხოების დარღვევის გარეშე.

დისტანციური წვდომის მქონე VPN– ები, როგორც წესი, მომხმარებელს დინამიურად აძლევს წვდომის საშუალებას საჭიროების შემთხვევაში. დისტანციური წვდომის VPN–ების შექმნა შესაძლებელია IPsec–ის ან SSL– ის გამოყენებით. როგორც ნაჩვენებია სურათზე, სწორედ დისტანციურმა მომხმარებელმა უნდა მოხდინოს დისტანციური წვდომის VPN კავშირის ინიციალიზაცია.

სურათი აჩვენებს დისტანციური მომხმარებელის წვდომის VPN კავშირის წამოწყების ორ ხერხს: კლიენტის გარეშე VPN და კლიენტზე დაფუძნებული VPN.



სურ.1.3. დისტანციური წვდომის VPN

- Clientless VPN კავშირი - კავშირი დაცულია ვებ ბრაუზერის SSL კავშირის გამოყენებით. SSL ძირითადად გამოიყენება HTTP ტრაფიკის (HTTPS) და ელ.ფოსტის პროტოკოლების დასაცავად, როგორიცაა IMAP და POP3. მაგალითად, HTTPS სინამდვილეში არის HTTP SSL გვირაბის გამოყენებით. თავდაპირველად მყარდება SSL კავშირი და შემდეგ მონაცემები იცვლება HTTP კავშირის საშუალებით.
- კლიენტზე დაფუძნებული VPN კავშირი - VPN კლიენტის პროგრამა, როგორიცაა Cisco AnyConnect Secure Mobility Client, უნდა იყოს დაინსტალირებული დისტანციური მომხმარებლის მოწყობილობაზე. მომხმარებლებმა უნდა წამოიწყონ კავშირი VPN კლიენტის გამოყენებით და შემდეგ ავთენტიფიკაცია დანიშნულების VPN gateway-ზე. დისტანციური მომხმარებლების ავტორიზაციის შემთხვევაში, მათ წვდომა აქვთ

კორპორაციულ ფაილებსა და პროგრამებზე. VPN კლიენტის პროგრამული უზრუნველყოფა შიფრავს ტრაფიკს IPsec ან SSL გამოყენებით და აგზავნის ინტერნეტით დანიშნულების VPN gateway-ზე .

1.4. SSL VPN

როდესაც კლიენტი წამოიწყებს SSL კავშირს VPN gateway-სთან, ის ფაქტობრივად უკავშირდება მას Transport Layer Security (TLS) გამოყენებით. TLS არის SSL-ის უფრო ახალი ვერსია და ზოგჯერ გამოიხატება როგორც SSL / TLS. ამასთან, ორივე ტერმინი ხშირად ერთმანეთის მაგიერ გამოიყენება.

SSL იყენებს საჯარო გასაღების ინფრასტრუქტურას და ციფრულ სერთიფიკატებს კავშირების ავთენტიფიკაციისთვის. როგორც IPsec, ისე SSL VPN ტექნოლოგიები გვთავაზობს პრაქტიკულად ნებისმიერ ქსელურ პროგრამასა თუ რესურსს. ამასთან, თუ უსაფრთხოების საკითხიც დგას, მაშინ IPsec არის საუკეთესო არჩევანი. თუ პირველადი საკითხებია მხარდაჭერა და განლაგების სიმარტივე, უპირატესობა ენიჭება SSL. განხორციელებული VPN მეთოდის ტიპი ემყარება მომხმარებელთა წვდომის მოთხოვნებს და ორგანიზაციის IT პროცესებს. ცხრილი ადარებს IPsec და SSL დისტანციური წვდომის განლაგებებს.

ცხრილი 2. IPsec-ის და SSL-ის შედარება

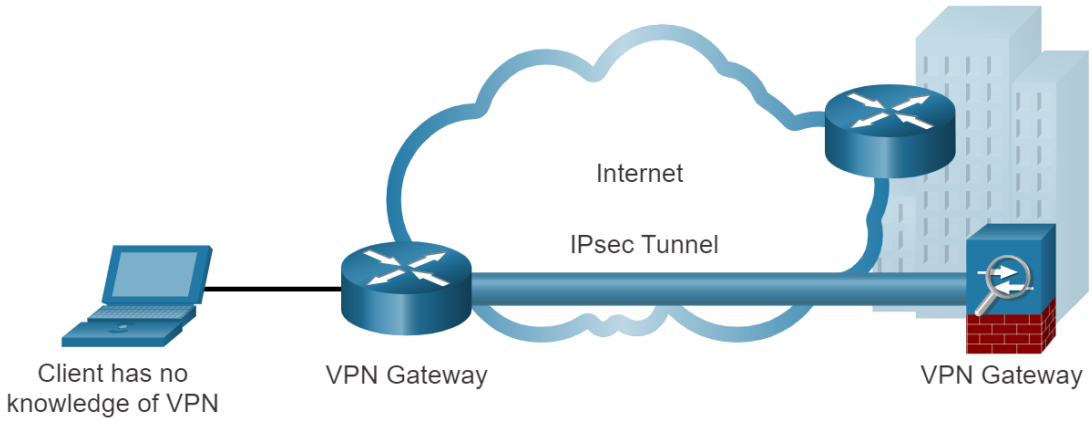
თვისება	IPsec	SSL
პროგრამების მხარდაჭერა	ვრცელი - მხარდაჭერა ყველა IP-ზე დაფუძვნებული აპლიკაცია	ლიმიტირებული - მხოლოდ Web-based აპლიკაციები და ფალიების გაცვლის მხარდაჭერა
ავთენტიფიკაციის სიძლიერე	ძლიერი - იყენებს ორმაგ ავთენტიკაციას გასაღებების გაზიარების ან ციფრული სერთიფიკატების სახით	ზომიერი - იყენებს ერთმაგ ან ორმაგ ავთენტიფიკაციას
დაშიფვრის სიძლიერე	ძლიერი - იყენებს გასაღებს სიგრძით 56 დან 256 ბიტამდე	ზომიერიდან ძლიერამდე - იყენებს გასაღებს სიგრძით 40 დან 256 ბიტამდე
კავშირის სირთულე	საშუალო - რადგან მოითხოვს კლიენტის ჩაწერას ჰოსტთან	დაბალი - მოითხოვს მხოლოდ ვებ ბრაუზერს ჰოსთისგან
კავშირის ვარიანტი	ლიმიტირებული - მხოლოდ სპეციფიური	ვრცელი - ნებისმიერი მოწყოვილობა შეუძლია

	მოწყობილობები და სპეციფიური კონფიგურაცია შეიძლება დაუკავშირდეს	დაუკავშირდეს რომელსაც ვებ ბრაუზერი აქვს

მნიშვნელოვანია გვესმოდეს, რომ IPsec და SSL VPN ერთმანეთს არ გამორიცხავს. ამის ნაცვლად, ისინი ერთმანეთს ავსებენ; ორივე ტექნოლოგია წყვეტს სხვადასხვა პრობლემას და ორგანიზაციამ შეიძლება გამოიყენოს IPsec, SSL ან ორივე, რაც დამოკიდებულია მისი ტელეკომუნიკაციების საჭიროებებზე.

1.5. Point-to-point IPsec VPN

Point-to-point VPN გამოიყენება ქსელების დასაკავშირებლად სხვა არასანდო ქსელში, მაგალითად საჯარო ინტერნეტში. წერტილოვან VPN-ში, ბოლო წერტილები აგზავნიან და იღებენ დაშიფრულ TCP / IP ტრაფიკს VPN-ში დაკავშირებული მოწყობილობის საშუალებით. VPN-ის დამხურავს, როგორც წესი, VPN gateway ეწოდება. VPN gateway მოწყობილობა შეიძლება იყოს როუტერი ან firewall, როგორც ეს ნაჩვენებია სურათზე. მაგალითად, Cisco Adaptive Security Appliance (ASA), რომელიც გამოსახულია ფიგურის მარჯვენა მხარეს, წარმოადგენს დამოუკიდებელ firewall მოწყობილობას, რომელიც აერთიანებს firewall– ს, VPN– ს კონცენტრატორს და შეჭრის პროფილაქტიკის ფუნქციებს ერთ პროგრამულ სურათში.



სურ.1.4. VPN gateway firewall-ის გამოყენებით

VPNgateway ათავსებს და შიფრავს გამავალ ტრაფიკს. ამის შემდეგ იგი აგზავნის ტრაფიკს VPN გვირაბის საშუალებით ინტერნეტით სამიზნე ადგილზე.მიღებისთანავე, მიმღები VPN gateway აძევებს სათაურებს, განშიფრავს შინაარსს დააგზავნის პაკეტს მის კერძო ქსელში სამიზნე ჰოსტისკენ.

Point-to-point VPN ჩვეულებრივ იქმნება და დაცულია ჩვეულებრივ IP უსაფრთხოების(IPsec) გამოყენებით.

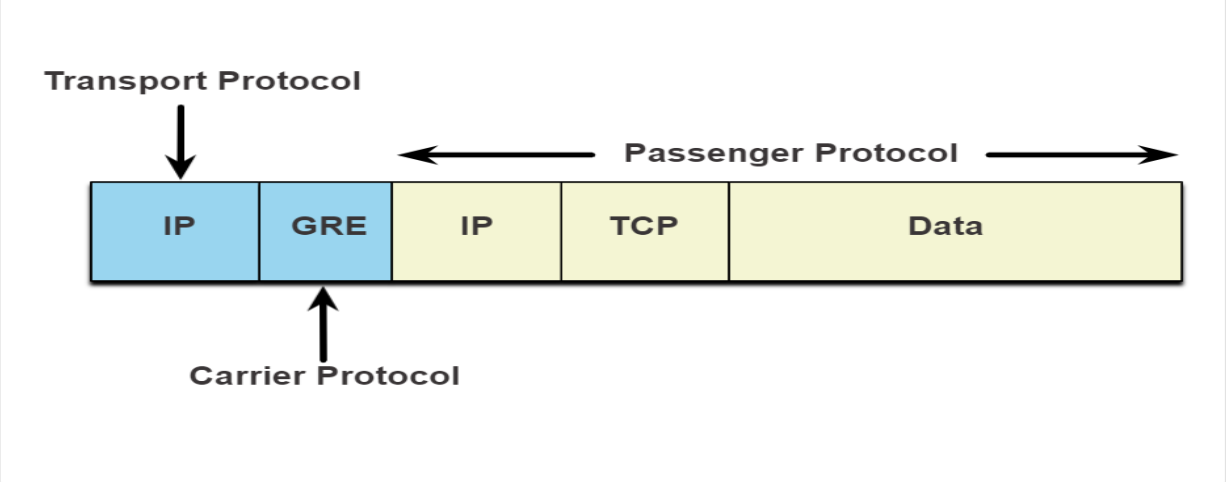
1.6. GRE-ს ჩაშენება IPsec-ში

Generic Routing Encapsulation (GRE) არის საიმედო VPN გვირაბის პროტოკოლი. მას შეუძლია სხვადასხვა ქსელის შრის პროტოკოლების აწყობა. იგი ასევე მხარს უჭერს მულტიკასტისა და სამაუწყებლო ტრაფიკს, რაც შეიძლება საჭირო გახდეს, თუ ორგანიზაცია მოითხოვს მარშრუტიზაციის ოქმებს VPN– ით მუშაობისთვის. ამასთან, GRE სტანდარტულად არ უზრუნველყოფს დაშიფვრის მხარდაჭერას; და შესაბამისად, ის არ უზრუნველყოფს უსაფრთხო VPN გვირაბს.

სტანდარტულ IPsec VPN (non-GRE) შეუძლია შექმნას მხოლოდ უსაფრთხო გვირაბები უნიკასტური ტრაფიკისთვის. ამიტომ, მარშრუტიზაციის პროტოკოლები არ გაცვლიან მარშრუტიზაციის ინფორმაციას IPsec VPN– ით.

ამ პრობლემის გადასაჭრელად, ჩვენ შეგვიძლია განვათავსოთ მარშრუტიზაციის პროტოკოლის მოძრაობა GRE პაკეტის გამოყენებით, შემდეგ კი GRE პაკეტი მოვათავსოთ IPsec პაკეტში, რათა უსაფრთხოდ გადავიტანოთ დანიშნულების VPN gatewayზე.

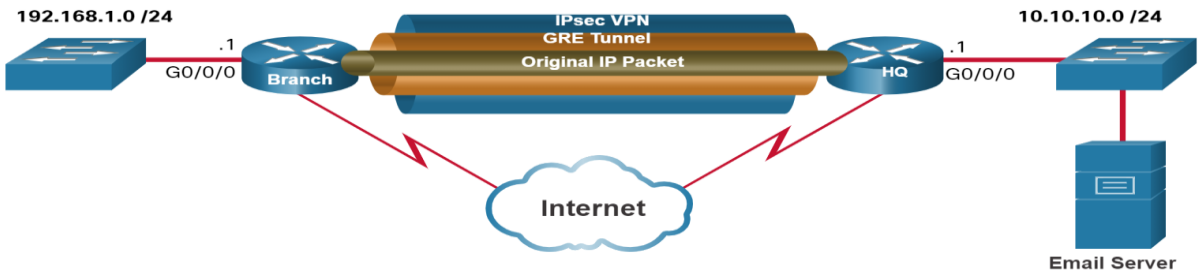
ტერმინები, რომლებიც გამოიყენება GRE–ის IPsec გვირაბზე ინკაფსულაციის აღსაწერად არის სამგზავრო პროტოკოლი, გადამზიდავი პროტოკოლი და ტრანსპორტირების პროტოკოლი, როგორც ეს ნაჩვენებია სურათზე.



სურ. 1.5. GRE პაკეტი

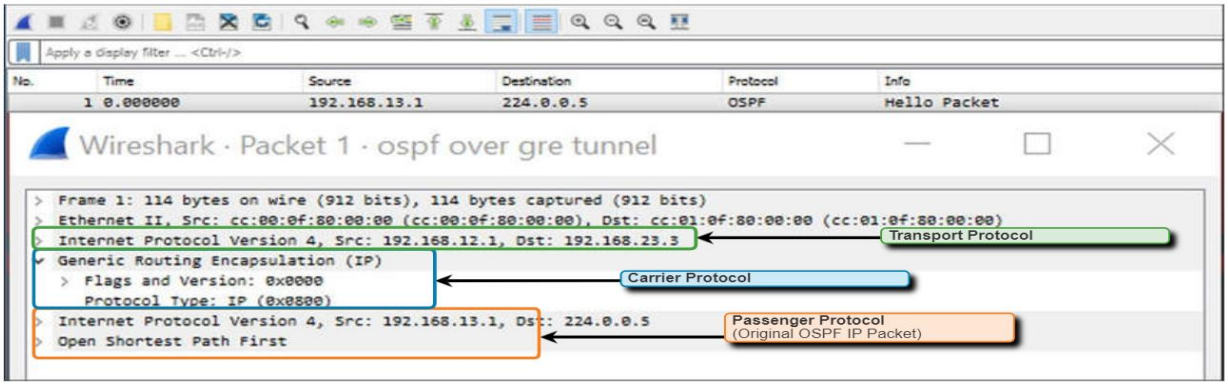
- სამგზავრო პროტოკოლი - ეს არის ორიგინალი პაკეტი, რომელიც უნდა დაიფაროს GRE– ს მიერ. ეს შეიძლება იყოს IPv4 ან IPv6 პაკეტი, მარშრუტიზაციის განახლება და სხვა.
- გადამზიდველის პროტოკოლი - GRE არის გადამზიდავი პროტოკოლი, რომელიც თავდაპირველ სამგზავრო პაკეტს ათავსებს.
- ტრანსპორტის პროტოკოლი - ეს არის პროტოკოლი, რომელიც რეალურად გამოყენებული იქნება პაკეტის გადასაგზავნად. ეს შეიძლება იყოს IPv4 ან IPv6.

მაგალითად, ტოპოლოგიის ამსახველ სურათზე ფილიალსა და შტაბს სურს გაცვალონ OSPF მარშრუტიზაციის ინფორმაცია IPsec VPN–ით. ამასთან, IPsec არ უჭერს მხარს მრავალრიცხოვან ტრაფიკს. ამიტომ, GRE ჩაშენებული Ipsec-ში გამოიყენება IPsec VPN–ით პროტოკოლის მარშრუტიზაციის მხარდასაჭერად. კერძოდ, OSPF პაკეტები (მაგ., სამგზავრო პროტოკოლი) უნდა იყოს დაინსტალირებული GRE-ს (მაგ., გადამზიდავი პროტოკოლი) მიერ და შემდგომში მოთავსებული IPsec VPN გვირაბში.



სურ.1.6. GRE Tunnel

Wireshark აჩვენებს OSPF პაკეტს, რომელიც გაიგზავნა GRE– ს გამოყენებით IPsec–ით. მაგალითში, თავდაპირველი OSPF მულტიკასტ პაკეტი (ე.ი. სამგზავრო პროტოკოლი) დაინსტალირებული იყო GRE სათაურით (მაგ., გადამზიდავი პროტოკოლით), რომელიც შემდგომში კაფსულირდება სხვა IP სათაურით (მაგ., ტრანსპორტის პროტოკოლით). შემდეგ ეს IP სათაური გადაგზავნილი იქნება IPsec გვირაბზე.



1.7. დინამიური მულტიპუნქტიანი VPN

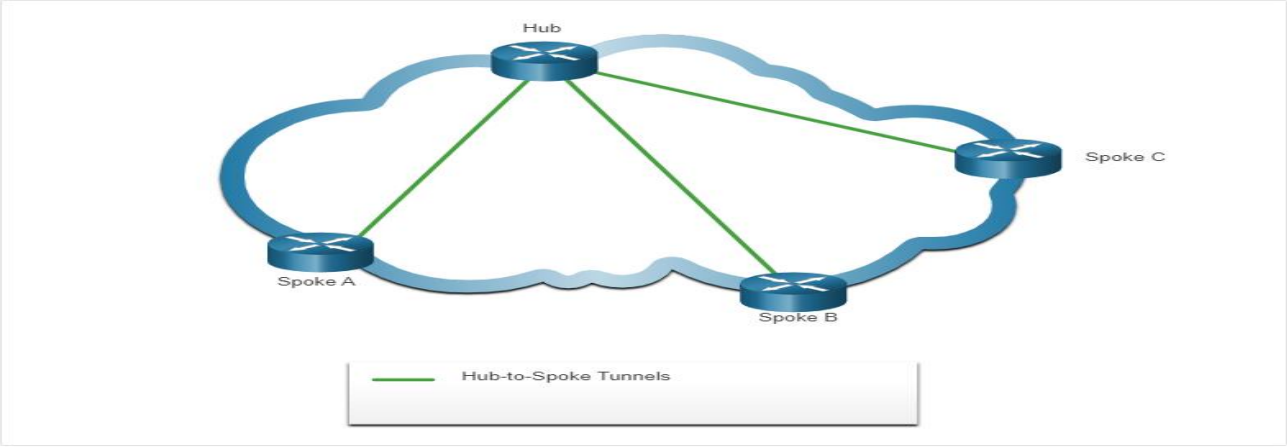
Point-to-point IPsec VPN და GRE ჩაშენებული IPsec ადეკვატურია, როდესაც მხოლოდ რამდენიმე წერტილია საიმედო ურთიერთდაკავშირების მიზნით. ამასთან, ისინი არ არიან საკმარისი, როდესაც ორგანიზაცია კიდევ ბევრ წერტილს ამატებს. ეს იმიტომ ხდება, რომ თითოეულ წერტილს დასჭირდება სტატიკური კონფიგურაცია ყველა სხვა წერტილისთის ან ცენტრალურისთვის.

Dynamic Multipoint VPN (DMVPN) არის Cisco პროგრამული უზრუნველყოფა, მრავალი VPN- ის მარტივი, დინამიური და მასშტაბური ფორმით შესაქმნელად. სხვა VPN ტიპის

მსგავსად, DMVPN ეყრდნობა IPsec-ს, რათა უზრუნველყოს უსაფრთხო ტრანსპორტი საზოგადოებრივი ქსელებით, მაგალითად ინტერნეტით.

DMVPN ამარტივებს VPN გვირაბის კონფიგურაციას და გთავაზობთ მოქნილ ვარიანტს ცენტრალური წერტილის პერიფერიულ წერტილებთან დასაკავშირებლად. იგი იყენებს ჰაბისა და Spoke-ს კონფიგურაციას სრული ბადის ტოპოლოგიის დასადგენად. Spoke წერტილები ქმნიან უსაფრთხო VPN გვირაბებს ჰაბის წერტილთან, როგორც ეს ნაჩვენებია სურათზე.

ფიგურაზე გამოსახულია დინამიური მრავალპუნქტიანი VPN ჰაბ – სპაიკის გვირაბები. Hub არის როუტერი, რომელსაც აქვს სამი კავშირი სხვა როუტერებთან, Spoke A, Spoke B და Spoke C.

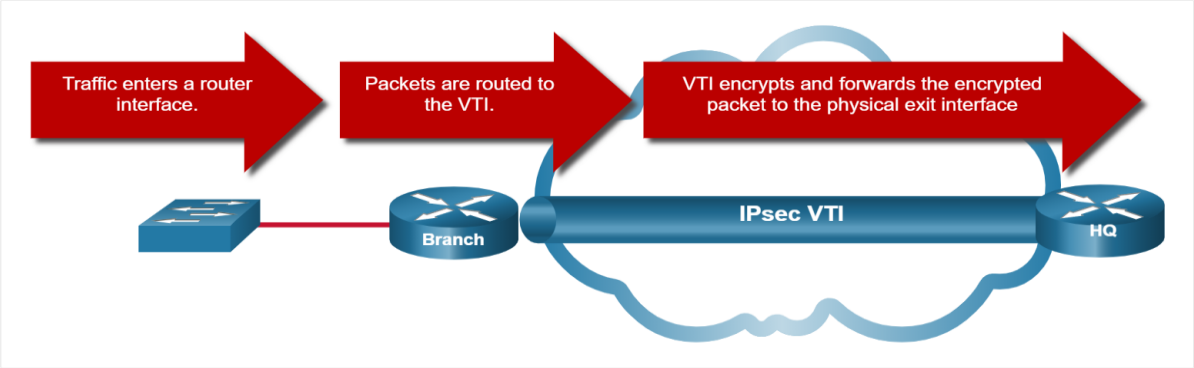


1.8. IPsec-ის ვირტუალური გვირაბის ინტერფეისი

როგორც DMVPN, IPsec ვირტუალური გვირაბის ინტერფეისი (VTI) ამარტივებს კონფიგურაციის პროცესს, რომელიც საჭიროა მრავალი წერტილის და დისტანციური წვდომის მხარდასაჭერად. IPsec VTI კონფიგურაციებს იყენებენ ვირტუალურ ინტერფეისზე, იმის მაგივრად, რომ IPsec სესიები სტატიკურად იყოს მიკუთვნებული ფიზიკურ ინტერფეისზე.

IPsec VTI- ს შეუძლია გააგზავნოს და მიიღოს როგორც IP უნიკასტი, ასევე მრავალკასტიანი დაშიფრული ტრაფიკი. ამიტომ, მარშრუტიზაციის პროტოკოლები ავტომატურად მხარს უჭერს GRE გვირაბებს კონფიგურაციის გარეშე.

IPsec VTI შეიძლება კონფიგურირებული იყოს წერტილებს შორის ან Hub-to-spoke-ს ცენტრში.



სურ. 1.9. IPsec VTI

1.9. მულტიპროტოკოლიანი სერვისის პროვაიდერი VPN (MPLS VPN)

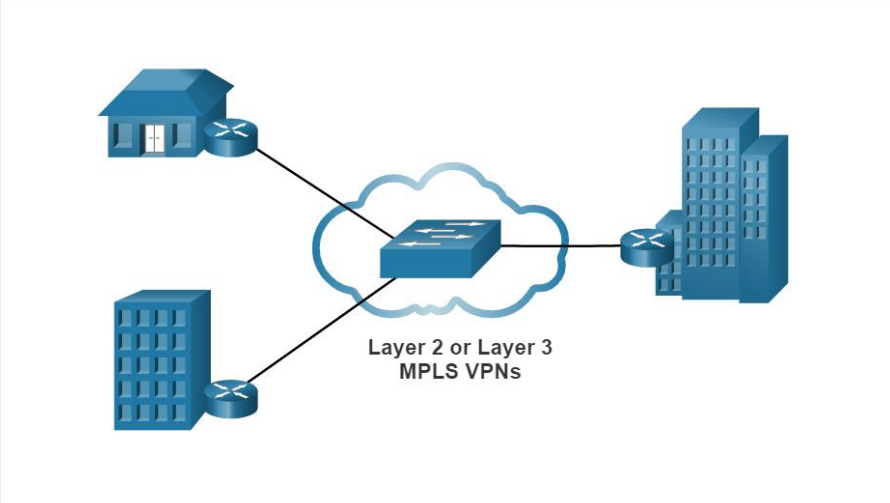
ტრადიციული მომსახურების მიმწოდებელი WAN გადაწყვეტილებები, როგორიცაა საიჯარო ხაზები, Frame Relay და ATM კავშირი, თავისებურად უსაფრთხო იყო მათი დიზაინის დროს. დღეს, მომსახურების მიმწოდებლები თავიანთ ძირითად ქსელში იყენებენ MPLS- ს. ტრეფიკი გადაეცემა MPLS ხერხემალის საშუალებით, ლეიბლების გამოყენებით, რომლებიც გადანაწილებულია ძირითად როუტერებში. მემკვიდრეობით მიღებული WAN კავშირების მსგავსად, ტრაფიკი უსაფრთხოა, რადგან მომსახურების მიმწოდებელი მომხმარებლები ვერ ხედავენ ერთმანეთის ტრაფიკს.

MPLS–ს შეუძლია კლიენტებს შესთავაზოს მართული VPN გადაწყვეტილებები; ამიტომ კლიენტის წერტილებს შორის ტრაფიკის დაცვა მომსახურების მიმწოდებელს ეკისრება. MPLS VPN გადაწყვეტილების ორი ტიპი არსებობს, რომელსაც მხარს უჭერენ მომსახურების მიმწოდებლები:

- Layer 3 MPLS VPN - მომსახურების მიმწოდებელი მონაწილეობს მომხმარებელთა მარშრუტიზაციაში კავშირის დამყარებით დამკვეთის მარშრუტიზატორებსა და პროვაიდერის მარშრუტიზატორებს შორის. მომხმარებელთა მარშრუტები, რომლებსაც იღებს მიმწოდებლის როუტერისგან, გადანაწილებულია MPLS ქსელის საშუალებით, მომხმარებლისთვის დისტანციურ ადგილებში

- Layer 2 MPLS VPN - მომსახურების მიმწოდებელი არ მონაწილეობს მომხმარებლის მარშრუტიზაციაში. სამაგიეროდ, პროვაიდერი აყენებს ვირტუალური კერძო ქსელის სერვისს (VPLS) MPLS ქსელში Ethernet მრავალმიმართულიანი LAN სეგმენტის იმიტაციისთვის. არ არის ჩართული მარშრუტიზაცია. მომხმარებლის მარშრუტიზატორები ეფექტურად ეკუთვნიან ერთსა და იმავე მრავალმიმართულ ქსელს.

სურათზე მოცემულია მომსახურების მიმწოდებელი, რომელიც გთავაზობთ Layer 2 და Layer 3 MPLS VPN-ს.



1.10. Layer 2 და Layer 3 MPLS VPN

თავი II. ვირტუალური კერძო ქსელის (VPN) თავდასხმების ძირითადი ტიპები

2.1. ვირტუალურ კერძო ქსელზე თავდასხმების კლასიფიკაცია (VPN)

ზემოქმედების ხასიათიდან გამომდინარე:

- პასიური
- აქტიური

ვირტუალური კერძო ქსელის (VPN) პასიური ზემოქმედება არის ერთგვარი გავლენა, რომელიც პირდაპირ არ მოქმედებს სისტემის მუშაობაზე, მაგრამ ამავდროულად შეიძლება დაარღვიოს მისი უსაფრთხოების პოლიტიკა. ვირტუალური კერძო ქსელის (VPN) მუშაობაზე პირდაპირი გავლენის არარსებობა იწვევს ზუსტად იმ ფაქტს, რომ პასიური დისტანციური ზემოქმედების ამოცნობა ძნელია. ვირტუალური კერძო ქსელის (VPN) ტიპიური პასიური დისტანციური ზემოქმედების შესაძლო მაგალითია ვირტუალურ ქსელში საკომუნიკაციო არხის მოსმენა.

ვირტუალური პერსონალური ქსელის (VPN) აქტიური გავლენა არის გავლენა, რომელსაც აქვს პირდაპირი გავლენა თავად სისტემის მუშაობაზე (გაუმართაობა, ვირტუალური პერსონალური ქსელის კონფიგურაციის შეცვლა (VPN) და ა.შ.), რაც არღვევს მასში მიღებულ უსაფრთხოების პოლიტიკას. დისტანციური შეტევების თითქმის ყველა ტიპი აქტიური გავლენაა.

ეს იმის გამო ხდება, რომ აქტიურობის პრინციპი შედის საზიანო ზემოქმედების ბუნებაში. აქტიური გავლენისა და პასიურის აშკარა განსხვავება მისი გამოვლენის ფუნდამენტური შესაძლებლობაა, ვინაიდან მისი განხორციელების შედეგად, სისტემაში ხდება გარკვეული ცვლილებები. პასიური ზემოქმედებით, არანაირი კვალი არ რჩება (იმის გამო, რომ თავდამსხმელი სისტემაში ხედავს სხვის შეტყობინებას, იმ მომენტში სინამდვილეში არაფერი იცვლება).

ზემოქმედების მიზნის მიხედვით:

- სისტემის გაუმართაობა (სისტემაზე წვდომა)
- ინფორმაციული რესურსების მთლიანობის (IR) დარღვევა
- IR კონფიდენციალურობის დარღვევა

მთავარი მიზანი, რომელიც თითქმის ნებისმიერ შეტევაში ხორციელდება არის ინფორმაციის არასანქცირებული წვდომის მოპოვება. ინფორმაციის მიღების ორი ძირითადი ვარიანტი არსებობს: დამახინჯება და მიტაცება. ინფორმაციის მიტაცების ვარიანტი ნიშნავს მასზე წვდომას, მისი შეცვლის შესაძლებლობის გარეშე.

შესაბამისად, ინფორმაციის მიტაცება იწვევს მის კონფიდენციალურობის დარღვევას. ვირტუალურ ქსელში არხის მოსმენა ინფორმაციის მიტაცების მაგალითია. ამ შემთხვევაში არსებობს ინფორმაციაზე უკანონო წვდომა, მისი ჩანაცვლების შესაძლო ვარიანტების გარეშე. ასევე აშკარაა, რომ ინფორმაციის კონფიდენციალურობის დარღვევა მიეკუთვნება პასიურ გავლენას.

ინფორმაციის ჩანაცვლების შესაძლებლობა უნდა იქნას გაგებული, როგორც სისტემის ობიექტთა შორის ინფორმაციის ნაკადების სრული კონტროლი, ან სხვისი სახელით სხვადასხვა შეტყობინებების გადაცემის შესაძლებლობა. აქედან გამომდინარე, ცხადია, რომ ინფორმაციის ჩანაცვლება იწვევს მისი მთლიანობის დარღვევას. ასეთი ინფორმაციული დესტრუქციული გავლენა არის აქტიური გავლენის ტიპიური მაგალითი. დისტანციური შეტევის მაგალითი, რომელიც შექმნილია ინფორმაციის მთლიანობის დარღვევისთვის, შეიძლება ემსახურებოდეს დისტანციურ ქსელურ შეტევას (UA) "False object VIRTUAL PERSONAL NETWORK (VPN)".

შეტევით ობიექტთან კავშირის არსებობის მიხედვით:

- უკუკავშირით
- უკუკავშირის გარეშე (ქსელის ცალმხრივი შეტევა)
- თავდამსხმელი უგზავნის ზოგიერთ თხოვნას შეტეულ ობიექტს, რაზეც ის პასუხის მიღებას ელის.

შესაბამისად, თავდამსხმელსა და თავდასხმულს შორის გამოდის უკუკავშირი, რაც საშუალებას აძლევს პირველს ადეკვატურად მოახდინოს რეაგირება თავდასხმის ობიექტზე ყველა სახის ცვლილებებზე. ეს არის დისტანციური შეტევის არსი, რომელიც ხორციელდება შემტევი ობიექტის უკუკავშირის თანდასწრებით. ასეთი შეტევები ყველაზე დამახასიათებელია ვირტუალური კერძო ქსელისთვის (VPN).

უკუკავშირის გარეშე (ღია მარყუჟის) შეტევები ხასიათდება იმით, რომ მათ არ სჭირდებათ რეაგირება შეტეულ ობიექტზე განხორციელებულ ცვლილებებზე. ჩვეულებრივ, ასეთი შეტევები ხორციელდება დაზარალებულ ობიექტზე ერთი მოთხოვნის გაგზავნით.

თავდამსხმელს არ სჭირდება პასუხები ამ მოთხოვნებზე. ასეთ შეტევებს ასევე შეიძლება ეწოდოს ცალმხრივი შეტევები. ცალმხრივი შეტევების მაგალითია ტიპიური DoS- ქსელის შეტევა.

ზემოქმედების დაწყების პირობების მიხედვით:

დისტანციური ზემოქმედება ისევე როგორც ნებისმიერი სხვა, შეიძლება დაიწყოს მხოლოდ გარკვეულ პირობებში. ვირტუალურ კერძო ქსელში (VPN) ასეთი პირობების სამი ტიპი არსებობს:

- ქსელური შეტევა მოთხოვნილი ობიექტის მოთხოვნით
- ქსელური შეტევა მოსალოდნელი მოვლენის დადგომის შემდეგ შეტეულ ობიექტზე
- უპირობო ქსელის შეტევა

თავდამსხმელი დაიწყებს ზემოქმედებას იმ პირობით, რომ თავდასხმის პოტენციური სამიზნე გაგზავნის გარკვეული ტიპის თხოვნას. ასეთ შეტევას შეიძლება ეწოდოს შეტევა მოთხოვნით შეტეული ობიექტისგან. ამ ტიპის დისტანციური შეტევა ყველაზე დამახასიათებელია ვირტუალური კერძო ქსელისთვის (VPN). DNS და ARP მოთხოვნები წარმოადგენს ინტერნეტის ვირტუალურ ქსელში ასეთი მოთხოვნების მაგალითს და Novell NetWare- ში SAP მოთხოვნებს.

ქსელური შეტევა მოსალოდნელი მოვლენის დადგომის შემდეგ შეტეულ ობიექტზე. თავდამსხმელი განუწყვეტლივ აკონტროლებს შეტევის დისტანციური სამიზნის ოპერაციულ სისტემის მდგომარეობას და იწყებს გავლენას, როდესაც ამ სისტემაში ხდება კონკრეტული მოვლენა. თავდასხმის ობიექტი თავად არის თავდასხმის ინიციატორი. ასეთი მოვლენის მაგალითი იქნება მომხმარებლის სესიის სერვერთან შეწყვეტა Novell NetWare- ში LOGOUT ბრძანების გაცემის გარეშე.

უპირობო ქსელური შეტევა ხორციელდება დაუყოვნებლივ და მიუხედავად ოპერაციული სისტემის მდგომარეობისა და შეტეული ობიექტისა. შესაბამისად, თავდამსხმელი ამ შემთხვევაში თავდასხმის ინიციატორია.

შეტევის სუბიექტის ადგილმდებარეობის მიხედვით შეტეული ობიექტის მიხედვით:

- შიდა სეგმენტური
- შუალედური

2.2. განმარტებები

თავდასხმის წყარო (თავდასხმის საგანი) - არის პროგრამა (შესაძლოა ოპერატორი), რომელიც ახორციელებს შეტევას და ახორციელებს პირდაპირ მოქმედებას.

ჰოსტი - კომპიუტერი, რომელიც წარმოადგენს ვირტუალური ქსელის ელემენტს.

როუტერი არის მოწყობილობა, რომელიც უზრუნველყოფს ვირტუალური ქსელის პაკეტების მარშრუტიზაციას.

ქვე ქსელი არის მასპინძელთა ჯგუფი, რომელიც გლობალური ვირტუალური ქსელის ნაწილია, გამოირჩევა იმით, რომ როუტერმა გამოუყო იგივე ქვე ვირტუალური ქსელის ნომერი. თქვენ ასევე შეგიძლიათ თქვათ, რომ ქვე ქსელი არის ჰოსტების ლოგიკური ასოციაცია როუტერის საშუალებით. იმავე ვირტუალურ ქსელში მყოფ მასპინძლებს შეუძლიათ პირდაპირ დაუკავშირდნენ ერთმანეთს როუტერის გამოყენების გარეშე. ვირტუალური ქსელის სეგმენტი არის ჰოსტების დაჯგუფება ფიზიკურ დონეზე.

დისტანციური შეტევის თვალსაზრისით, სუბიექტისა და შეტევის ობიექტის ფარდობითი პოზიცია ძალზე მნიშვნელოვანია, ანუ, ისინი სხვადასხვა სეგმენტში იმყოფებიან, თუ ერთ სეგმენტში. შიდა სეგმენტის შეტევის დროს შეტევის საგანი და ობიექტი განლაგებულია იმავე სეგმენტში. ჯვარედინი სეგმენტის შეტევის შემთხვევაში, თავდასხმის საგანი და სამიზნე არის ქსელის სხვადასხვა სეგმენტებზე. კლასიფიკაციის ეს მახასიათებელი შესაძლებელს ხდის შევაფასოთ შეტევის ე.წ. "დაშორების ხარისხი".

ქვემოთ ნაჩვენები იქნება, რომ პრაქტიკულად შიდა სეგმენტის შეტევა უფრო ადვილია, ვიდრე ინტერსექციური. გაითვალისწინეთ ისიც, რომ ჯვარედინი სეგმენტის ქსელური შეტევა ბევრად უფრო საშიშია, ვიდრე შიდა სეგმენტური. ეს გამოწვეულია იმით, რომ შუალედური შეტევის შემთხვევაში, მისი ობიექტი და პირდაპირი თავდამსხმელი შეიძლება განლაგდეს ერთმანეთისგან ათასობით კილომეტრის მანძილზე, რაც მნიშვნელოვნად აფერხებს შეტევის მოგერიების ზომებს.

ISO / OSI მითითების მოდელის დონის მიხედვით, რომელზეც ხდება გავლენა:

- ფიზიკური
- არხული
- ქსელური
- სატრანსპორტო

- სასესიო
- პიროვნული
- გამოყენებითი

სტანდარტიზაციის საერთაშორისო ორგანიზაციამ (ISO) მიიღო ISO 7498 სტანდარტი, რომელიც აღწერს ღია სისტემების (OSI) თავსებადობას, რომელსაც ვირტუალური კერძო ქსელი (VPN) ეკუთვნის. ქსელის კომუნიკაციის ყველა პროტოკოლი, ისევე როგორც ქსელის ყველა პროგრამა, შეიძლება როგორმე დაპროექტდეს OSI 7 დონის მითითების მოდელზე. ამგვარი დონიანი პროექცია საშუალებას იძლევა OSI მოდელის მიხედვით აღვწეროთ ფუნქციები, რომლებიც გამოიყენება ქსელის პროტოკოლში ან პროგრამაში. დისტანციური შეტევა წარმოადგენს ქსელის პროგრამას და ლოგიკურია განვიხილოთ იგი პროექციის თვალსაზრისით ISO / OSI ეტალონურ მოდელზე [2].

2.2. ვირტუალური კერძო ქსელის (VPN) თავდასხმების ანალიზი

2.2.1. მონაცემთა ფრაგმენტაცია

ვირტუალური ქსელის მეშვეობით IP მონაცემთა პაკეტის გადაცემისას, ეს პაკეტი შეიძლება დაიყოს რამდენიმე ფრაგმენტად. შემდეგ, დანიშნულების ადგილზე მისვლისთანავე, პაკეტი ამოიღება ამ ფრაგმენტებიდან. თავდამსხმელს შეუძლია წამოიწყოს დიდი რაოდენობით ფრაგმენტების გაგზავნა, რაც იწვევს პროგრამული უზრუნველყოფის ბუფერების გადავსებას მიმღებ მხარეზე და, ზოგიერთ შემთხვევაში, სისტემის ავარიულ შეწყვეტას.

2.2.2. პინგით ქსელის გადატვირთვის შეტევა

ქსელის შეტევა მოითხოვს შემტევისგან ინტერნეტში სწრაფ არხებზე წვდომას. პინგ პროგრამა აგზავნის ICMP ECHO REQUEST პაკეტს დროსა და ID– ით. მიმღები მანქანის ბირთვი პასუხობს ასეთ მოთხოვნას ICMP ECHO REPLY პაკეტით. როდესაც ping იღებს მას, ის აძლევს პაკეტს სიჩქარეს.

სტანდარტულ ოპერაციულ/სამუშაო რეჟიმში პაკეტები იგზავნება ინტერვალებით, პრაქტიკულად ქსელის დატვირთვის გარეშე. მაგრამ "აგრესიულ" რეჟიმში, ICMP ექოს მოთხოვნის / პასუხის პაკეტების ნაკადმა შეიძლება გადავსება გამოიწვიოს მცირე ხაზზე, რაც მას ჩამოართმევს სასარგებლო ინფორმაციის გადაცემის შესაძლებლობას.

IP- კაფსულირებული არასტანდარტული პროტოკოლები

IP პაკეტი შეიცავს ველს, რომელიც განსაზღვრავს ჩანართული პაკეტის (TCP, UDP, ICMP) ოქმს. თავდამსხმელებს შეუძლიათ გამოიყენონ ამ ველის არასტანდარტული მნიშვნელობა მონაცემთა გადასაცემად, რომელიც არ იქნება აღებული ინფორმაციის ნაკადის კონტროლის სტანდარტული საშუალებით.

2.2.3. Smurf ქსელური შეტევა

Smurf ქსელის შეტევა მოიცავს ICMP მაუწყებლობის გაგზავნას ქსელში დაზარალებული კომპიუტერის სახელით. შედეგად, კომპიუტერებმა, რომლებმაც მიიღეს ასეთი ფართო სამაუწყებლო პაკეტები, რეაგირებენ დაზარალებულ კომპიუტერზე, რაც იწვევს საკომუნიკაციო არხის გამტარობის მნიშვნელოვან შემცირებას და, ზოგიერთ შემთხვევაში, შეტეული ვირტუალური ქსელის სრულ იზოლაციას. Smurf ქსელის შეტევა ძალზე ეფექტური და ფართოდ გავრცელებულია.

საწინააღმდეგო ზომები: ამ შეტევის ამოცნობისთვის საჭიროა არხის დატვირთვის ანალიზი და გამტარუნარიანობის შემცირების მიზეზების დადგენა.

2.2.4. ქსელური შეტევა ყალბი DNS-ით

ამ შეტევის შედეგია დაყენებული კორესპონდენციის შემოღება IP მისამართსა და დომენის სახელს შორის DNS სერვერის ქეშში. ასეთი წარმატებული შეტევის შედეგად, DNS სერვერის ყველა მომხმარებელი მიიღებს არასწორ ინფორმაციას დომენური სახელების და IP მისამართების შესახებ. ამ ქსელურ შეტევას ახასიათებს დიდი რაოდენობით DNS პაკეტები იგივე დომენის სახელით. ეს გამოწვეულია DNS გაცვლის ზოგიერთი პარამეტრის არჩევის აუცილებლობით.

საწინააღმდეგო ზომები: ასეთი შეტევის დასადგენად საჭიროა DNS ტრაფიკის შინაარსის ანალიზი.

2.2.5. ქსელის თავდასხმა ყალბი IP-თ

ვირტუალურ ინტერნეტ ქსელზე თავდასხმების დიდი რაოდენობა ასოცირდება თავდაპირველი IP მისამართის გაყალბებასთან. ეს ქსელური შეტევები მოიცავს syslog spoofing-ს, რაც გულისხმობს მსხვერპლის კომპიუტერში შეტყობინების გაგზავნას შიდა ვირტუალურ ქსელში სხვა კომპიუტერის სახელით. მას შემდეგ, რაც syslog პროტოკოლი გამოიყენება სისტემის ჟურნალების შესანარჩუნებლად, შესაძლებელია ინფორმაციის შეფუთვა ან არასანქცირებული წვდომის კვალის დაფარვა დაზარალებულ კომპიუტერში ყალბი შეტყობინებების გაგზავნით.

საწინააღმდეგო ზომები: IP მისამართების გაყალბებასთან დაკავშირებული შეტევების გამოვლენა შესაძლებელია პაკეტის ერთ-ერთ ინტერფეისზე მიმღების მონიტორინგით იმავე ინტერფეისის წყაროს მისამართით ან შიდა ვირტუალური ქსელის IP მისამართებით პაკეტების მიღების მონიტორინგით გარე ინტერფეისზე.

2.2.6. პაკეტების შეფუთვა

თავდამსხმელი აგზავნის პაკეტებს ქსელში ყალბი საპასუხო მისამართით. ამ შეტევით თავდამსხმელს შეუძლია გადმორთოს თავის კომპიუტერზე სხვა კომპიუტერებს შორის დამყარებული კავშირები. ამ შემთხვევაში თავდამსხმელის წვდომის უფლებები უდრის იმ მომხმარებლის უფლებებს, რომელთა კავშირი სერვერთან იყო თავდამსხმელის კომპიუტერზე.

არხის მოსმენა

შესაძლებელია მხოლოდ ადგილობრივი/ლოკალური ვირტუალური ქსელის სეგმენტში. თითქმის ყველა ქსელური ბარათი მხარს უჭერს ადგილობრივი ვირტუალური ქსელის საერთო არხზე გადაცემული პაკეტების მიტაცების შესაძლებლობას. ამ შემთხვევაში, სამუშაო სადგურს შეუძლია მიიღოს პაკეტები, რომლებიც მიმართულია ვირტუალური ქსელის იმავე სეგმენტის სხვა კომპიუტერებზე. ამრიგად, ვირტუალური ქსელის სეგმენტში ინფორმაციის გაცვლა თავდამსხმელისთვის ხელმისაწვდომი ხდება. იმისათვის, რომ ეს შეტევა წარმატებული იყოს, თავდამსხმელის კომპიუტერი უნდა განთავსდეს იმავე LAN სეგმენტზე, რომელზეც „შესატევად შერჩეული“ კომპიუტერი იმყოფება..

2.2.7. პაკეტების წართმევა როუტერზე

როუტერის ქსელურ პროგრამულ უზრუნველყოფას აქვს წვდომა ამ როუტერის საშუალებით გადაცემულ ყველა ქსელურ პაკეტზე, რაც პაკეტის აღების/მიტაცების საშუალებას იძლევა. ამ შეტევის ჩასატარებლად, თავდამსხმელს უნდა ჰქონდეს პრივილეგირებული წვდომა მინიმუმ ერთ ვირტუალურ ქსელურ როუტერზე. მას შემდეგ, რაც ბევრი პაკეტი ჩვეულებრივ გადადის/გადაეცემა როუტერის საშუალებით, მათი მთლიანი/ტოტალური მიტაცება თითქმის შეუძლებელია. ამასთან, ინდივიდუალური პაკეტები შეიძლება მიიტაცოს და შეინახოს თავდამსხმელმა მოგვიანებითი ანალიზისთვის. მომხმარებლის პაროლების, აგრეთვე ელ.ფოსტის შემცველი FTP პაკეტების მიტაცება ყველაზე ეფექტურია.

2.2.8. ICMP- ის გამოყენებით ჰოსტისთვის ყალბი მარშრუტის დაწესება

ვირტუალურ ინტერნეტ ქსელში არის სპეციალური პროტოკოლი ICMP (Internet Control Message Protocol), (ინტერნეტ კონტროლის შეტყობინებების პროტოკოლი), რომლის ერთ-ერთი ფუნქციაა მასპინძლების ინფორმირება მიმდინარე როუტერის შეცვლის შესახებ. ამ საკონტროლო შეტყობინებას redirect გადამისამართება ეწოდება. შესაძლებელია როუტერის სახელით გააგზავნოთ ყალბი გადამისამართების შეტყობინება ვირტუალურ ქსელურ სეგმენტში ნებისმიერი ჰოსტისგან შესატევ მასპინძელზე. შედეგად, შეიცვლება სამიზნის ამჟამინდელი მარშრუტიზაციის ცხრილი და, მომავალში, მისი მთელი ქსელის ტრაფიკი გაივლის, მაგალითად, ჰოსტის მეშვეობით, რომელმაც გაგზავნა ცრუ გადამისამართების შეტყობინება. ამრიგად, შესაძლებელია ვირტუალური ინტერნეტ ქსელის ერთ სეგმენტში ყალბი მარშრუტის აქტიურად დაწესება.

2.2.9. WinNuke

TCP კავშირით გაგზავნილ ჩვეულებრივ მონაცემებთან ერთად, სტანდარტი ასევე ითვალისწინებს გადაუდებელი (Out Band) მონაცემების გადაცემას. TCP პაკეტის ფორმატის დონეზე, ეს გამოიხატება, როგორც ნულოვანი გადაუდებელი მაჩვენებელი. Windows- ზე მომუშავე კომპიუტერების უმეტესობას აქვს NetBIOS ქსელის პროტოკოლი, რომელიც იყენებს

სამ IP პორტს საჭიროებისთვის: 137, 138, 139. თუ თქვენ დაუკავშირდებით Windows აპარატს 139 პორტზე და გააგზავნით რამდენიმე ბაიტ OutOfBand მონაცემებს, მაშინ NetBIOS არ ეცოდინება რა უნდა გააკეთოს ამ მონაცემთან, ის უბრალოდ გაითიშება ან გადატვირთავს მანქანას.

Windows 95-ისთვის ეს ჩვეულებრივ ჰგავს ლურჯი ტექსტური ეკრანის შეტყობინებას TCP / IP დრაივერის შეცდომისა და ქსელთან მუშაობის შეუძლებლობისა ოპერაციული სისტემის გადატვირთვამდე NT 4.0 მომსახურების პაკეტების გადატვირთვის გარეშე, NT 4.0 ServicePack 2 პაკეტით ცისფერ ეკრანზე გადადის. ვირტუალური ქსელის ინფორმაციით ვიმსჯელებთ, Windows NT 3.51 და Windows 3.11 სამუშაო ჯგუფებისათვის მგრძნობიარეა ასეთი შეტევისთვის. მონაცემების გაგზავნა 139 პორტზე იწვევს NT 4.0- ის გადატვირთვას, ან "სიკვდილის ლურჯი ეკრანის" ჩვენებას Service Pack 2-ით. მონაცემების 135 და ზოგიერთ სხვა პორტებზე გაგზავნას იწვევს RPCSS.EXE პროცესის მნიშვნელოვან დატვირთვას. Windows NT WorkStation– ზე ეს მნიშვნელოვან შენელებას იწვევს, Windows NT სერვერი პრაქტიკულად იყინება.

2.2.10. სანდო ჰოსტის გაყალბება

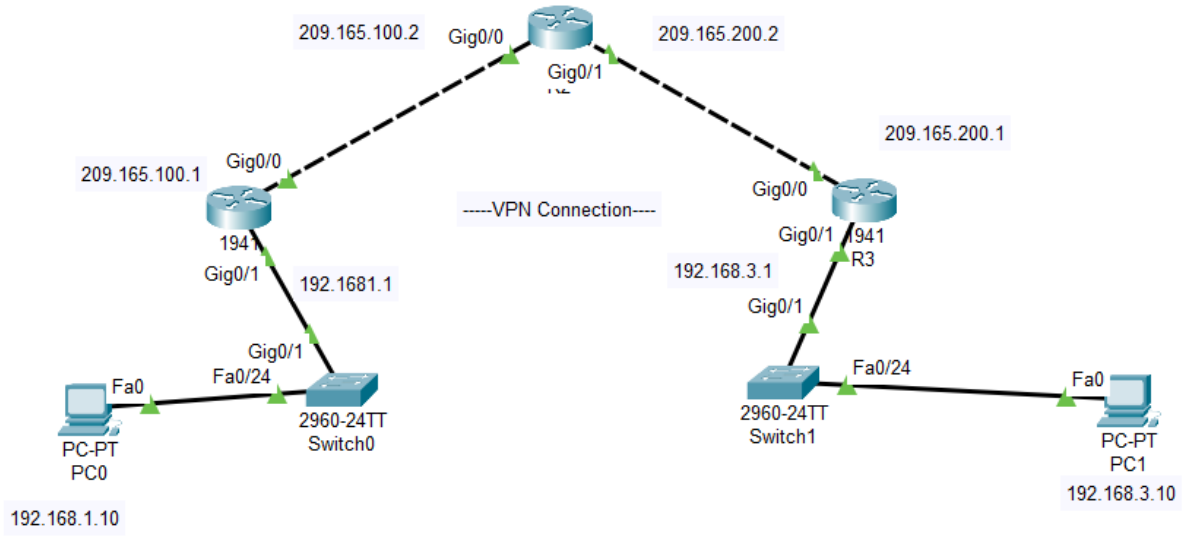
ამ ტიპის წარმატებული დისტანციური შეტევები თავდამსხმელს საშუალებას მისცემს შევიდეს სერვერზე სანდო ჰოსტის სახელით. (სანდო ჰოსტი არის სადგური, რომელიც ლეგალურად არის დაკავშირებული სერვერთან). ამ ტიპის შეტევის განხორციელება ჩვეულებრივ მოიცავს გაცვლითი პაკეტების გაგზავნას თავდამსხმელის სადგურიდან მისი კონტროლის ქვეშ მყოფი სანდო სადგურის სახელით.

თავი III. ვირტუალური უსაფრთხო ქსელების განვითარება და აგება ვირტუალური კერძო ქსელის (VPN) სერტიფიცირებული პროდუქტის საფუძველზე ViPNet (c) CUSTOM

3.1. ვირტუალური უსაფრთხო არხების აგება

ინფორმაციის გაცვლის უსაფრთხოება უზრუნველყოფილი უნდა იყოს როგორც ადგილობრივი ქსელების ურთიერთდაკავშირების შემთხვევაში, ასევე დისტანციური ან მობილური მომხმარებლების ლოკალურ ქსელებზე წვდომის შემთხვევაში. ვირტუალური კერძო ქსელის (VPN) შემუშავებისას, ჩვეულებრივ, განიხილება ორი ძირითადი სქემა:

- ვირტუალური დაცული არხი ადგილობრივ ქსელებს შორის (LAN-LAN არხი);
- ვირტუალური დაცული არხი მასპინძელსა და ადგილობრივ ქსელს შორის (კლიენტი-LAN არხი)



სურ. 3.1. - ვირტუალური დაცული არხები LAN-LAN და client-LAN ტიპის

კავშირი სქემა 1 საშუალებას გაძლევთ შეცვალოთ მძირადღირებული საიჯარო ხაზები ცალკეულ ოფისებს შორის და შექმნათ მათ შორის მუდმივად ხელმისაწვდომი უსაფრთხო არხები. ამ შემთხვევაში, უსაფრთხოების gateway წარმოადგენს გვირაბსა და LAN- ს შორის ინტერფეისს, LAN მომხმარებლები გვირაბს იყენებენ ერთმანეთთან კომუნიკაციისთვის.

მრავალი კომპანია იყენებს ამ ტიპის ვირტუალურ კერძო ქსელს (VPN) როგორც არსებული WAN გლობალური კავშირების ჩანაცვლებას ან დამატებას, მაგალითად ჩარჩოს რელე.

ვირტუალური კერძო ქსელის (VPN) უსაფრთხო არხის სქემა 2 შექმნილია დისტანციურ ან მობილურ მომხმარებლებთან კავშირების დასადგენად. კლიენტი (დისტანციური მომხმარებელი) იწყებს გვირაბის შექმნას. დისტანციური ქსელის დაცულ gatewayსთან კომუნიკაციისთვის, იგი უშვებს სპეციალურ კლიენტურ პროგრამულ უზრუნველყოფას თავის კომპიუტერში.

ამგვარი ვირტუალური პერსონალური ქსელი (VPN) ცვლის აკრიფილ/კომუტირებულ კავშირებს და მისი გამოყენება შესაძლებელია დისტანციური წვდომის ტრადიციულ მეთოდებთან ერთად. ვირტუალური დაცული არხების სქემების ვარიანტები არსებობს. პრინციპში, ვირტუალური კორპორატიული ქსელის ნებისმიერი ორი კვანძიდან, რომელთა შორის იქმნება ვირტუალური დაცული არხი, შეიძლება მიეკუთვნებოდეს დაცული შეტყობინების ნაკადის ბოლოს ან შუალედურ წერტილს.

ინფორმაციის უსაფრთხოების თვალსაზრისით, საუკეთესო ვარიანტი განიხილება, როდესაც დაცული გვირაბის საბოლოო წერტილები მსგავსია დაცული შეტყობინების ნაკადის საბოლოო წერტილებისა. შემდეგ არხის უსაფრთხოება შენარჩუნებულია შეტყობინებების პაკეტების მთელი მარშრუტის გასწვრივ. მაგრამ ეს ვარიანტი იწვევს მენეჯმენტის დეცენტრალიზაციას და რესურსების ხარჯების გადაჭარბებას. ამისათვის თქვენ უნდა დააინსტალიროთ ვირტუალური პერსონალური ქსელის (VPN) შექმნის ინსტრუმენტები ადგილობრივი ვირტუალური ქსელის ნებისმიერ კლიენტ კომპიუტერზე.

ეს ართულებს კომპიუტერულ რესურსებზე წვდომის ცენტრალიზებულ კონტროლს და ყოველთვის არ არის ეკონომიკურად შესაძლებელი. ნებისმიერი კლიენტის პერსონალური კომპიუტერის ცალკე ადმინისტრირება, რომელიც მიზნად ისახავს მასში თავდაცვის საშუალებების კონფიგურაციას, საკმაოდ დიდ ვირტუალურ ქსელში საკმაოდ შრომატევად ოპერაციად ითვლება.

თუ ვირტუალური ქსელში ჩართული ადგილობრივი ვირტუალური ქსელის შიგნით საჭირო არ არის ტრაფიკის დაცვა, მაშინ უკვე დაცული გვირაბის საბოლოო წერტილის სახით, შესაძლებელია ამ ადგილობრივი ვირტუალური ქსელის სასაზღვრო როუტერის აღება. და რადგან ადგილობრივი ვირტუალური ქსელის შიგნით სიახლეების ნაკადები დაცული უნდა იყოს, ამიტომ ამ გვირაბის საბოლოო წერტილის სახით უკვე ამ ვირტუალურ ქსელში უნდა

მოქმედებდეს კომპიუტერი, რომელიც მონაწილეობს დაცულ ურთიერთქმედებებში. დისტანციური მომხმარებლის ლოკალურ ქსელში შესვლისას, მისი კომპიუტერი უნდა იყოს ვირტუალური დაცული არხის ბოლო წერტილი.

საკმაოდ გავრცელებული ვარიანტია, როდესაც უსაფრთხო გვირაბი იდება მხოლოდ ღია ვირტუალური პაკეტით გადართული ქსელის შიგნით, მაგალითად, ინტერნეტის შიგნით. ეს ვარიანტი არის მარტივად გამოსაყენებელი, მაგრამ აქვს შედარებით დაბალი უსაფრთხოება. ასეთი გვირაბის საბოლოო წერტილები, როგორც წესი, არიან ინტერნეტ პროვაიდერები ან ადგილობრივი ვირტუალური ქსელის სასაზღვრო როუტერი (ეკრანები).

ადგილობრივი ქსელების შეერთებისას გვირაბი იქმნება მხოლოდ საზღვრისპირა ინტერნეტ პროვაიდერებს ან ადგილობრივი ვირტუალური ქსელის მარშრუტიზატორებს (ეკრანები) შორის. ლოკალურ ვირტუალურ ქსელზე დისტანციური წვდომის შემთხვევაში იქმნება გვირაბი ინტერნეტ – პროვაიდერის დისტანციური წვდომის სერვერსა და ასევე ადგილობრივი ვირტუალური ქსელის სასაზღვრო ინტერნეტ – პროვაიდერს ან როუტერს (firewall) შორის.

ვირტუალურ კორპორატიულ ქსელებს, რომლებიც ამ ვარიანტის მიხედვით აიგება, აქვს კარგი მასშტაბურობა და მართვადობა. ჩამოყალიბებული უსაფრთხო გვირაბები სრულიად გამჭვირვალეა კლიენტური კომპიუტერებისთვის და ადგილობრივი ვირტუალური ქსელის სერვერებისთვის, რომლებიც ასეთ ვირტუალურ ქსელში შედის. ამ კვანძების პროგრამული უზრუნველყოფა უცვლელი რჩება. ამასთან, ამ ვარიანტს ახასიათებს ინფორმაციის ურთიერთქმედების შედარებით დაბალი უსაფრთხოება, ვინაიდან ტრეფიკი ნაწილობრივ გადის დაუცველი სახით ღია საკომუნიკაციო არხებით.

თუ ISP პროვაიდერი თავის თავზე აიღებს ამგვარი ვირტუალური პერსონალური ქსელის (VPN) შექმნას და ფუნქციონირებას, მაშინ მთელი ვირტუალური კერძო ქსელი შეიძლება აიგოს მის gatewayებზე გამჭვირვალედ ადგილობრივი ქსელების და ორგანიზაციას დისტანციური მომხმარებლებისთვის. ამ შემთხვევაში, არსებობს მიმწოდებლისადმი ნდობის პრობლემები და მისი მომსახურებების მუდმივი გადახდისაც. უსაფრთხო გვირაბს ქმნის ვირტუალური ქსელის კომპონენტები, რომლებიც მუშაობენ კვანძებზე, რომელთა შორისაც გვირაბი იქმნება. ამ კომპონენტებს ჩვეულებრივ უწოდებენ გვირაბის ინიციატორს და გვირაბის დამამთავრებელს.

გვირაბის ინიციატორი თავდაპირველ პაკეტს ათავსებს ახალ პაკეტში, რომელიც შეიცავს ახალ სათაურს, ინფორმაციას გამგზავნისა და მიმღების შესახებ. კაფსულირებული პაკეტები შეიძლება იყოს ნებისმიერი ტიპის პროტოკოლი, მათ შორის, არა – რუტირებადი პროტოკოლის პაკეტები, როგორიცაა NetBEUI. გვირაბის საშუალებით გადაცემული ყველა პაკეტი არის IP პაკეტი. მარშრუტი გვირაბის ინიციატორსა და ტერმინატორს შორის განსაზღვრავს ჩვეულებრივ მარშრუტიზებულ IP ქსელს, რომელიც შეიძლება იყოს სხვა ქსელი, გარდა ინტერნეტისა.

სხვადასხვა ქსელურ მოწყობილობასა და პროგრამულ უზრუნველყოფას შეუძლია გვირაბის წამოწყება/ინიცირება და გატეხვა. მაგალითად, გვირაბის წამოწყება შეიძლება მობილური მომხმარებლის ლეპტოპის მიერ, რომელიც აღჭურვილია მოდემით და შესაბამისი პროგრამული უზრუნველყოფით, dial-up კავშირების დასადგენად. ინიციატორი ასევე შეიძლება იყოს ადგილობრივი ვირტუალური ქსელის როუტერი, რომელსაც გააჩნია შესაბამისი ფუნქციონირება. გვირაბი ჩვეულებრივ მთავრდება ვირტუალური ქსელის გადართვით ან სერვისის პროვაიდერის კარიბჭით.

გვირაბის ტერმინატორი ასრულებს ინკაფსულაციის პროცესის საპირისპიროს. ტერმინატორი ხსნის/აცილებს ახალ სათაურებს და თითოეულ ორიგინალ/საწყის პაკეტს აგზავნის დანიშნულების ადგილზე ადგილობრივ ვირტუალურ ქსელში.
კაფსულირებული პაკეტების კონფიდენციალურობას უზრუნველყოფს მათი დაშიფვრა, ხოლო მათი მთლიანობა და ნამდვილობა უზრუნველყოფილია ელექტრონული ციფრული ხელმოწერის ფორმირებით.

კრიპტოგრაფიული მონაცემების დაცვის მრავალი მეთოდი და ალგორითმი არსებობს, ამიტომ აუცილებელია გვირაბის ინიციატორი და ტერმინატორი დროულად შეთანხმდნენ ერთმანეთთან და გამოიყენონ დაცვის ერთი და იგივე მეთოდები და ალგორითმები. იმისათვის, რომ მონაცემების გაშიფვრა და ციფრული ხელმოწერის გადამოწმება შეძლოთ, გვირაბის ინიციატორმა და ტერმინატორმა ასევე უნდა უზრუნველყონ გასაღების გაცვლის უსაფრთხო ფუნქციები.

გარდა ამისა, კომუნიკაციების ბოლო მხარეები უნდა დადასტურდეს, რომ ვირტუალური კერძო ქსელის (VPN) გვირაბები შეიქმნას მხოლოდ ავტორიზებულ მომხმარებლებს შორის.

კორპორაციის არსებული ქსელის ინფრასტრუქტურა შესაძლებელია ვირტუალური კერძო ქსელის (VPN)თვის უზრუნველყოფისთვის, როგორც პროგრამული უზრუნველყოფის, ასევე აპარატურის გამოყენებით.

თავი IV. პრაქტიკული დავალების კონფიგურაცია

პრაქტიკული დავალება შედგება კონფიგურაციათა მიმდევრობის რამდენიმე ეტაპისგან, ესენია :

- საბაზისო კონფიგურაციის აწყობა როუტერებზე.
- Access-List მისამართების გაწერა როუტერებზე.
- ISAKMP პროტოკოლის კონფიგურაცია.
- ISAKMP პროტოკოლის გასაღების მინიჭება.
- პროტოკოლის მიმართულების აგება.(Transform-set)
- კრიპტაციის რუკის აგება.(Crypto-map)
- კრიპტაციის მინიჭება.(Set-Crypto)

საბაზისო კონფიგურაციისთვის ჩვენ დაგვჭრდება 3 ერთნაირი როუტერი(1941), 2 სვიჩი(2940), და ორიც მომხმარებელი(PC).

როუტერების კონფიგურაცია შეგვიძლია შემდეგი თანმიმდევრობით R1, R2, R3.

R1: en

conf t

hostname R1

interface g0/1

ip address 192.168.1.1 255.255.255.0

no shut

interface g0/0

ip address 209.165.100.1 255.255.255.0

no shut

exit

ip route 0.0.0.0 0.0.0.0 209.165.100.2

R2: en

conf t

hostname R2

interface g0/1

ip address 209.165.200.2 255.255.255.0

no shut

interface g0/0

ip address 209.165.100.2 255.255.255.0

no shut

exit

ip route 0.0.0.0 0.0.0.0 209.165.200.1

ip route 0.0.0.0 0.0.0.0 209.165.100.1

R3: en

conf t

hostname R3

interface g0/1

ip address 192.168.3.1 255.255.255.0

no shut

interface g0/0

ip address 209.165.200.1 255.255.255.0

no shut

exit

ip route 0.0.0.0 0.0.0.0 209.165.200.2

საბაზისო კონფიგურაციის დასრულების შემდეგი ბიჯი, არის პირველ და მესამე როუტერებზე Security Policy-ს ჩართვა შემდეგი ბრძანებით:

conf t

license boot module c1900 technology-package securityk9

reload

ამ ბიჯის შემდეგ უკვე შეგვიძლია გადავიდეთ პრაქტიკული ნაწილის მეორე ეტაპზე და როუტერებზე გავწეროთ შესაბამისი Access-list მონაცემები, რომლის შემდეგაც პირველი როუტერის შესაბამის ქსელს ეცოდინება მესამე როუტერის შესაბის ქსელი. ამ სიას კი პირობითად დავარქვათ ნომერი 100.

R1: en

conf t

access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255

R3: en

conf t

access-list 100 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255

სიის შედგენის შემდეგ გადავდივართ ISAKMP პროტოკოლის აგებაზე. პროტოკოლის ნომერი ავიღოთ პირობითად 10, კრიპტაციის ტიპი aes 256, აუთენტიკაციის ტიპი კი წინასწარი მიმოცვლის. საბოლოოდ კი გავაერთიანოთ ისინი ერთ ჯგუფში ნომრად 5. შესაბამისად როუტერებზე გასაშვები სკრიპტი მიიღებს შესაბამის სახეებს.

R1: conf t

crypto isakmp policy 10

encryption aes 256

authentication pre-share

group 5

R3: conf t

crypto isakmp policy 10

encryption aes 256

authentication pre-share

group 5

პროტოკოლის შედგენის შემდეგ კი დროა რომ თითოეულმა წერტილმა „გაიგოს“ მეორე წერტილის გასაღები. ეს გასაღები ჩვენს შემთხვევაში არის სიტყვა „secretkey”. ამის შესრულება ერთი ბრძანებით არის შესაძლებელი:

R1: crypto isakmp key secretkey address 209.165.200.1

R3: crypto isakmp key secretkey address 209.165.100.1

ავაგოთ პროტოკოლის მიმართულება სახელებით R1->R3 და R3->R1 იმის შესაბამისად თუ რომელი როუტერიდან რომელი როუტერისკენ იგება ის. პროტოკოლს აუცილებლად უნდა მივაწოდოთ კრიტპატიის უკვე დადგენილი ტიპი, რომელიც არის aes 256. შესაბამისად ბრძანებები მიიღებენ შემდეგ სახეს:

R1: crypto ipsec transform-set R1-R3 esp-aes 256 esp-sha-hmac

R3: crypto ipsec transform-set R3-R1 esp-aes 256 esp-sha-hmac

კონფიგურაციის ბოლო ნაბიჯი, რის შემდეგაც უკვე შეგვიძლია ჩავრთოთ ვირტუალური ქსელი, არის კრიპტაციის რუკის დადგენა. ამ რუკას ასევე უნდა მიეცეს სახელი, რომელიც ჩვენს შემთხვევაში იქნება IPSEC-MAP, საიდენტიფიკაციო ნომრად მივანიჭოთ 10, და ბოლოს მივუთითოთ ის მეთოდები რომელსაც კრიპტაციისთვის გამოვიყენებთ. ამ ინფორმაციით შეგვიძლია შევხედოთ სკრიპტებს:

R1: crypto map IPSEC-MAP 10 ipsec-isakmp

set peer 209.165.200.1

set pfs group5 (ISAKMP group 5)

set security-association lifetime seconds 86400

set transform-set R1-R3

match address 100 (Access list 100)

R3: crypto map IPSEC-MAP 10 ipsec-isakmp

set peer 209.165.100.1

set pfs group5 (ISAKMP group 5)

set security-association lifetime seconds 86400

set transform-set R3-R1

match address 100 (Access list 100)

ამ უკანასკნელი ბრძანების წარმატებად შესრულების შემდეგ, კი ჩავრთოთ კრიპტაცია როგორც R1 ასევე R3 როუტერების G0/0 სოკეტებზე და გავუშვათ პინგი საბოლოო წერტილებიდან, რათა დავრწმუნდეთ რომ ქსელი აგებულია.

R1/R3: conf t

interface GigabitEthernet0/0

crypto map IPSEC-MAP.

დასკვნა

თანამედროვე სამყაროში დისტანციური კავშირის უსწრაფეს მეთოდად ინტერნეტ კომუნიკაციები მიიჩნევა, მისი დახმარებით ერთმანეთში მიმოიცვლება როგორც საჯარო, ისე პერსონალური ინფორმაცია. შესაბამისად ამ სასიცოცხლო ინფორმაციის დაცულობა და კონფიდენციალურობა უსაზღვროდ მნიშვნელოვანია.

ინტერნეტ ქსელში ერთმანეთთან კავშირი დაგენერირებული პაკეტების საშუალებით წარმოიქმნება, რომელთან მოპარვა, მოსმენა და შეცვლა საჯარო ქსელის გამოყენებისას დღევანდელი ტექნოლიგიების საშუალებით ძალიან მარტივია. სწორედ ამიტომ მიზანშეწონილია და აუცილებელიც კია ამ ინფორმაციის ისეთი კრიპტაცია, რომ მისი გაჟონვის შემთხვევაში თავს მაინც დაცულად ვგრძნობდეთ.

ამ საკითხის უზრუნველსაყოფად შეიქმნა და დამუშავდა ეგრეთ წოდებული ვირტუალური პირადი ქსელები, რომელიც სტანდარტულად TCP/IP ტექნოლოგიას იყენებს და მოძრაობს სასჯარო ქსელის საფუძველზე, თუმცა მასში გამავალი თითოეული პაკეტი იშიფრება ისეთი ენით, რომლის „გაგება“ მხოლოდ კონკრეტულად დაფიქსირებულ ორ წერტილს შეეძლოს.

რა თქმა უნდა, ამ სფეროში დახელოვნებულ პირებს, კვლავ შეეძლებათ შეტევები განახორციელონ ვირტუალურ ქსელებზეც, რომლისგან თავის დაცვაც საკმაოდ რთულია. თავის დაცვის ზოგიერთ წარმატებულ ხერხზე ჩვენ ზემოთ ვისაუბრეთ.

ქსელური შეტევების პერიოდული ანალიზი და მას შემდეგი ცვლილებების შეტანა საუკეთსო გამოსავალია ვირტუალური კერძო ქსელების დაცულობის კოეფიციენტის გასაზრდელად, რაც უზრუნველყოფს ინფორმაციის სწორ მიმოცვლას და მის იზოლირებას არასასურველი პერსონებისგან, რომლებიც ცდილობენ მის მიტაცებას.

გამოყენებული ლიტერატურა:

1. Cisco Systems, Inc. (2004). Internetworking Technologies Handbook. Networking Technology Series (4 ed.). Cisco Press. p. 233.
2. Lela Mirtskhulava, Nugzar Meshveliani, Nana Gulua and Larysa Globa. Cryptanalysis of Internet of Things (IoT) Wireless Technology. IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics – UkrMicO 2019. Odessa, Ukraine**.** The best paper award.
3. Lela Mirtskhulava, Nana Gulua, Nugzar Meshveliani. NTRU Cryptosystem Analysis f or Securing IoT. Reviewed Electronic Scientific journal. GESJ: Computer Science and Telecommunications 2019|No.1(56)
4. Lela Mirtskhulava, Nana Gulua, Nugzar Meshveliani, Iot Security Analysis using Neural Key Exchange Protocol. GESJ: Computer Science and Telecommunications|. Reviewed Electronic Scientific journal. 2019|No. 2(57).
5. Lela Mirtskhulva, Larysa Globa, Nana Gulua and Nugzar Meshveliani. Complex Approach in Cryptanalysis of Internet of Things (IoT) Using Blockchain Technology and Lattice-Based Cryptosystem. Advances in Information and Communication Technology and Systems. Springer. P. 55-66. 2021.
6. IETF (1999), RFC 2661, Layer Two Tunneling Protocol "L2TP"
7. "Virtual Private Networking: An Overview". 18 November 2019.
8. Yang, Yanyan (2006). "IPsec/VPN security policy correctness and assurance". Journal of High Speed Networks. 15: 275–289. CiteSeerX 10.1.1.94.8561
9. "Overview of Provider Provisioned Virtual Private Networks (PPVPN)". Secure Thoughts. Retrieved 29 August 2016.
10. Mason, Andrew G. (2002). Cisco Secure Virtual Private Network. Cisco Press. p. 7.
11. RFC 2917, A Core MPLS IP VPN Architecture
12. Yang, Yanyan (2006). "IPsec/VPN security policy correctness and assurance". Journal of HighSpeed Networks. 15: 275–289. CiteSeerX 10.1.1.94.8561
13. http://wikipedia.org.