ივანე ჯავახიშვილის სახელობის თბილისის
სახელმწიფო უნივერსიტეტი

იმედა ჯანგულაშვილი

კომპიუტერული ქსელების უსაფრთხოება

სამაგისტრო ნაშრომი შესრულებულია საინფორმაციო
ტექნოლოგიების მაგისტრის აკადემიური ხარისხის მოსაპოვებლად

ხელმძღვანელი: ლელა მირცხულავა

თბილისი

2013

ანოტაცია

სამაგისტრო ნაშრომში გადმოცემულია კორპორატიული ქსელის აგების და მისი დაცვის ზოგად პრინციპები, უსაფრთხოების პროტოკოლები და დაცულ არხები (VPN კავშირებს). ნაშრომში ასევე განხილულია ქსელური მოწყობილობების დაცვა და სხვადასხვა ქსელური მოწყობილობების კონფიგურაცია, რათა მათ შეძლონ გარედან და შიგნიდან წამოსული საფრთხეებთან გამკლავება. ნაშრომში განხილული საკითხები დაეხმარება ქსელის ადმინისტრატორებს, მოაწყონ მცირე და საშუალო ზომის ქსელები უსაფრთხოების ზომების მაქსიმალური დაცვით.

In this thesis, we consider the general principles of building the enterprise networks and their security, security protocols and secure channels (VPN connections). In this paper, network devices security and their different types of configuration are considered, in the purpose to avoid inside and outside threats. The topics, considered In this paper, will help network administrators to implement small- and medium-size enterprise networks with maximum security measure protection.

1. სარჩევი

2. შესავალი

21-ე საუკუნეში თანამედროვე ტექნოლოგიების განვითარებასთან ერთად უსაფრთხოების როლი უფრო და უფრო იმატებს. თანამედროვე ტექნოლოგიების საუკუნეში, როდესაც თითქმის ყველანაირი ოპერაცია კომპიუტერის და ქსელის საშუალებით ხდება, ინფორმაციის დაცვა ყველაზე მნიშვნელოვანი ფაქტორია. ინფორმაციის კონფიდენციალურობა განსაკუთრებით საჭიროა საბანკო სექტორში, სახელმწიფო დაწესებულებებში, ძალოვან სტრუქტურებში, სატელეფონო სისტემაში. უცხო პირის მიერ არასასურველი მონაცემების მოპოვებას შეიძლება სავალალო შედეგები მოყვეს როგორც კერძო პირისთვის (მაგ. საბანკო ანგარიშებზე შეღწევა, პირადი ინფორმაციის მოპოვება) ასევე მთლიანად ქვეყნისთვის (საიდუმლო და ქვეყნისთვის სტრატეგიულად მნიშვნელოვანი ინფორმაციაზე წვდომა).

ხშირ შემთხვევებში ინფორმაციის კონფიდენციალურობასა და დაცულობაზე IT გუნდში მუშაობენ ცალკე პიროვნებები და გუნდები (Security admins). მსოფლიოს მასშტაბით კი გავრცელებული პრაქტიკაა მთლიანად ორგანიზაციის მუშაობა აღნიშნულ საკთხზე. მაგალითისთვის შეგვიძლია მოვიყვანოთ:

NSI - National Security Institute http://www.nsi.org/index.html

NCSD - National Cyber Security Division http://www.dhs.gov/national-cyber-security-division

ჩვენს ქვეყანაში მსგავსი საქმიანობითაა დაკავებული საქარტველოს იუსტიციის სამინისტროს ს.ს.ი.პ. მონაცემთა გაცვლის სააგენტო, რომელიც უზრუნველყოფს სხვადასხვა სახელმწიფო დაწესებულებებს შორის მონაცემტა უსაფრთხო გადაცემას, საჯარო ორგანიზაციების ინფორმაციის დაცვას და ასე შემდეგ. მაგალითისთვის შეგვიძლია მოვიყვანოთ გასულ წელს მათ მიერ აღმოჩენილი ვირუსი, რომელიც ვრცელდებოდა საინფორმაციო საიტებიდან, გზავნიდა საჭირო ინფორმაციას დაინფიცირებული კომპიუტერიდან ვირუსის შემქმნელთან და ემატებოდა ახალ-ახალი ფუნქციები, ისე რომ ეს ყველაფერი შეუმჩნეველი იყო ანტივირუსული პროგრამებისთვის. მონაცემთა გაცვლის სააგენტოს ეფექტურმა მუსაობამ შესაძლებელი გახადა განეიტრალებულიყო ვირუსი და დაიცვა მნიშვნელოვანი სტრატეგიული ინფორმაცია გატეხვისგან. დაწვრილებითი ინფორმაცია: http://dea.gov.ge/uploads/CERT%20DOCS/CERT.GOV.GE.pdf

უსაფრთხოების კონცეფცია მოიცავს როგორც ქსელის და სერვერების უსაფრთხოებას, ასევე ლოკალური კომპიუტერების დაცვას მავნე და საშიში ვირუსებისგან. თითოეულ მათგანს სათითაოდ განვიხილავთ დაწვრილებით.

3. IP დამისამართება

3.1 ადრესაცია IP-ქსელებში

TCP/IP სტეკის მისამართების ტიპები

ქსელში ინფორმაციის დაცვისთვის აუცილებელია ვიცოდეთ, თუ როგორ გადაიცემა ეს ინფორმაცია არხში. იმისათვის, რომ ინფორმაცია ადრესატამდე მივიდეს, საჭიროა ქსელურმა მოწყობილობებმა იცოდნენ თუ სად მდებარეობს ადრესატის მისამართი, ანუ IP მისამართი. იპ მისამართი ერთ-ერთი მნიშვნელოვანი საკითხია არამარტო უსაფრთხოებაში, არამედ მთლიანად ქსელურ ტექნოლოგიებში. მოდით, დაწვრილებით განვიხილოთ IP მისამართების სტრუქტურა, შინაარსი და დანიშნულება

TCP/IP სტეკში გამოიყენება მისამართების სამი ტიპი: ლოკალური (ე.წ. აპარატურული) მისამართები, IP-მისამართები და სიმბოლური დომენური სახელები. TCP/IP ტერმინოლოგიაში ლოკალური მისამართის ქვეშ იგულისხმება მისამართის ტიპი, რომელიც გამოიყენება საბაზო ტექნოლოგიების საშუალებების მიერ ინფორმაციის გადასაცემად ქვექსელში, რომელიც წარმოადგენს შედგენილი ქვექსელის ელემენტს. სხვადასხვა ქვექსელებში გამოიყენება სხვადასხვა ქსელური ტექნოლოგიები, პროტოკოლების სხვადსხვა სტეკი, ამიტომაც TCP/IP სტეკის შექმნისას შემოღებულ იქნა ლოკალური მისამართების სხვადასხვა ტიპები. თუ ქვექსელი ლოკალური ქსელია მაშინ ლოკალურ მისამართს წარმოადგენს MAC-მისამართი. MAC-მისამართი განისაზღვრება ქსელური ადაპტერისა და

მარშრუტიზატორების ქსელური ინტერფეისების საშუალებით. MAC-მისამართები განისაზღვრება მოწყობილობის მწარმოებლის მიერ და არის უნიკალური, რადგანაც მათი მართვა ხდება ცენტრალიზებულად. ლოკალური ქსელის ყველა არსებული ტექნოლოგიებისათვის MAC-მისამართს გააჩნია 6 ბაიტიანი ფორმატი, მაგ. 11-A0-17-3D-BC-01. რადგან IP პროტოკოლს შეუძლია იმუშაოს უფრო მაღალი დონის პროტოკოლებთან, როგორიცაა IPX და X.25. ამ შემთხვევაში ლოკალური მისამართი IP პროტოკოლისათვის იქნება შესაბამისად IPX და X.25 მისამართები. უნდა გავითვალისწინოთ, რომ კომპიუტერს ლოკალური ქსელში შეიძლება ჰქონდეს რამოდენიმე ლოკალური მისამართი ერთი ქსელური ადაპტერის შემთხვევაშიც. ზოგიერთ ქსელური მოწყობილობას არ გააჩნია ლოკალური მისამართი. მაგ., ასეთ მოწყობილობებია მარშრუტიზატორების გლობალური პორტები, რომლებიც დანიშნულია შესაერთებლად “წერტილი-წერტილი”.

IP-მისამართი წარმოადგენს მისამართების ძირითად ტიპს, რომლის საფუძველზეც ქსელური დონე აგზავნის პაკეტებს ქსელებს შორის. ეს მისამართები შედგება 4 ბაიტისგან, მაგ. 109.26.17.100. IP-მისამართი განისაზღვრება ადმინისტრატორის მიერ კომპიუტერისა და მარშრუტიზატორების კონფიგურაციისას. IP-მისამართი შედგება ორი ნაწილისგან: ქსელის ნომრისა და კვანძის ნომრისაგან. ქსელის ნომერი შეირჩევა ადმინისტრატორის მიერ ნებისმიერი ან Internet-ის (Internet Network Information Center, InterNIC) სპეციალური ქვეგანყოფილების რეკომენდავიების მიხედვით, თუ ქსელმა უნდა იმუშაოს, როგორც Iნტერნეტ-ის შემადგენელმა ნაწილმა. Internet-ის სერვისების მიმწოდებლები ჩვეულებრივ მისამრთების დიაპაზონს იღებენ IInterNIC-გან და შემდგომ ანაწილებენ თავიანთ აბონენტებს შორის. მარშრუტიზატორი განსაზღვრების თანახმად შედის რამოდენიმე ქსელში და ამიტომაც მის ყოველ პორტს გააჩნია საკუთარი IP-მისამართი. საბოლოო კვანძი შეიძლება შედიოდეს რამოდენიმე IP-ქსელში. ამ შემთხვევაში კომპიუტერს უნდა გააჩნდეს რამოდენიმე IP-მისამართი ქსელური კავშირების რიცხვის მიხედვით. მაშასადამე, IP-მისამართით ხასიათდება არა ერთი ცალკეული კომპიუტერი ან მარშრუტიზატორი, არამედ ერთი ქსელური შეერთება.

სიმბოლური დომენური სახელები. სიმბოლურს სახელებს IP-ქსელებში ეწოდება დომენური და იგება იერარქიულად. სრული სიმბოლური სახელების შემადგენელები IP-ქსელებში იყოფა წერტილით და მათი ჩამოთვლა მიმდინარეობს შემდეგი თანმიმდევრობით: საბოლოო კვანძის მარტივი სახელი, შემდგომ კვანძების ჯგუფის სახელი (მაგ., ორგანიზაციის

სახელი, შემდგომ უფრო მსხვილი ჯგუფის (ქვედომენების) სახელი და ყველაზე მაღალი დონის დომნის სახელი (მაგ. ორგანიზაციების გამაერთიანებელი დომენი გეოგრაფიული თვალსაზრისით: RU-რუსეთი, UK-დიდი ბრიტანეთი, SU-აშშ). დეპმენურ სახელად შეიძლება გამოყენებულ იქნასbase2.sales.zil.ru. დომენურ სახელებსა და IP-მისამრთებს შორის არ არის არანაირი ალგორითმული შესაბამისობა, ამიტომაც აუცილებელია გამოყენებულ იქნას დამატებითი ცხრილები და სერვისები იმისათვის, რომ ქსელის კვანძი ერთმნიშვნელოვნად იქნას განსაზღვრული, როგორც დოემნური სახელების მიედ, ასევე IP-მისამრთის მიხედვითაც. TCP/IP ქსელებში გამოიყენება სპეციალური გამანაწილებებლი მომსახურება, რომელიც ადგენს ამ შესაბამისობას ქსელის ადმინისტრატორების მიერ შექმნილი შესაბამისობის ცხრილის საფუძველზე. ამიტომაც დომენურ სახელებს აგრეთვე უწოდებენ DNS-სახელებს.

3.2 IP-მისამართის დანიშნულება

IP-მისამართი (აი-პი მისამართი, შემოკლ. ინგლ. Internet Protocol Address-ინტერნეტ ოქმის მისამართი) – ლოკალურ ქსელში ან ინტერნეტში ჩართული მოწყობილობის (როგორწესი კომპიუტერის) უნიკალური იდენტიფიკატორია (მისამართია). IP-მისამართი წარმოადგენს 32-ბიტურ (IPv4 ვერსიით) ან 128-ბიტურ (IPv6 ვერსიით) ორნიშნა რიცხვს, რომელიც ჩაიწერება ოთხი ათობითი რიცხვის სახით (0-დან 255-მდე), დაყოფილს წერტილებით. მაგ., 192.168.0.1. (ან 128.10.2.30 – ათობითი ფორმაა, ხოლო ამავე მისამართის ორობითი ფორმაა – 10000000 00001010 00000010 00011110)

IP-მისამართი ენიჭება ჰოსტის ქსელის ინტერფეისს ანუ ქსელურ ინტერფეისულ კარტას (network interface card (NIC)) იგივე ქსელური ადაპტერი, რომელიც კომპიუტერის ერთ-ერთი შემადგენელი მოწყობილობაა. მაგალითად საბოლოო მომხმარებლის მოწყობილობები ქსელური ინტერფეისებით მოიცავს მუშა სადგურებს (workstation), სერვერებს, ქსელურ პრინტერებს, და IP-ტელეფონებს (IP phones). სერვერებს შეიძლება ჰქონდეთ ერთზე მეტი NIC და შესაბამისად ყოველ მათგანს ცალკეული IP-მისამართი. მარშრუტიზაციის ინტერფეისებსაც (Router interfaces), რომლებიც უზრუნველყოფენ კავშირს IP ქსელთან, შეიძლება გააჩნდეთ საკუტარი IP-მისამართი.ყოველი პაკეტი, რომელიც

გადაიცემა ინტერნეტში, შეიცავს მიმღებისა და გადამცემის IP-მისამართებს, რომლებიც საჭიროა იმისათვის, რომ მიაღწიოს ინფორმაციამ ადრესატამდე და უკან დაუბრუნდეს პასუხი.

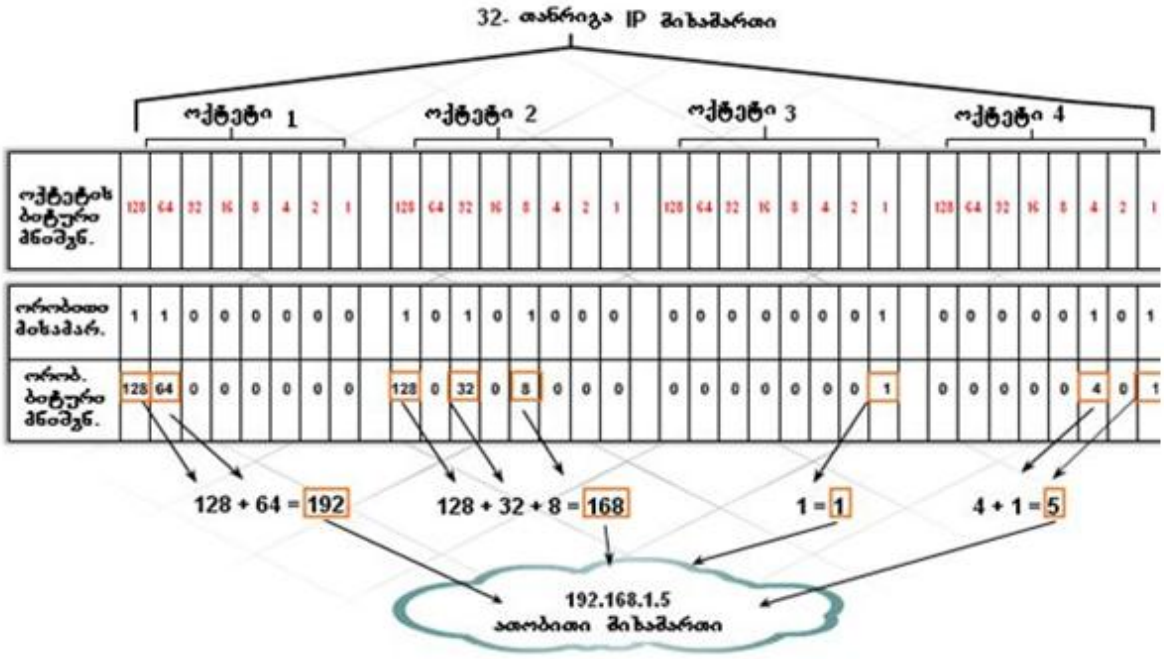
3.3 IP-მისამართის სტრუქტურა

IP-მისამართი – ეს არის 32 ბიტის (ნულებისა და ერთების) კომბინაცია (IPv4). ორობითი IP-მისამართის წაკითხვა ძალიან რთულია და ამიტომაც 32 ბიტი იყოფა 4 ბაიტად (8 ბიტად), რომლებსაც უწოდებენ ოქტეტებს. 32 ბიტისგან შემდგარი IP-მისამართის ფორმატი ძალიან რთულია წასაკითხად, ჩასაწერად და დასამახსოვრებლად და ამიტომ, რომ უფრო ადვილი გახდეს IP-მისამართის წაკითხვა ყოველი ოქტეტის წარმოდგენა ხდება მისი ათობითი მნიშვნელობით, რომლებიც ერთმანეთისგან გამოყოფილია ათობითი წერტილით.

ჰოსტის IP-მისამართით დაკონფიგურირებისას გამოიყენება IP-მისამართის ათობითი ფორმა, როგორიცაა 192.168.1.5. 32 ბიტიანი IP-მისამართი განისაზღვრება IP-ის მე-4 ვერსიით (IPv4), რომელიც ფართოდ გამოიყენება ინტერნეტში. 32-ბიტიანი დამისამრთების სქემა იყენებს სულ 4 მილიარდ IP-მისამართს. ჰოსტი ღებულობს IP-მისამართს 32-ვე ორობითი ბიტის სახით NIC-ის მიერ, რომელიც ძალიან რთულად გასაგებია მომხმარებლისთვის და ამიტომაც ის გარდაიქმნება მისი ექვივალენტურ ათობით ოთხ ოქტეტად. სადაც თითოეული ოქტეტი შედგება 8 ბიტისგან, ხოლო ყოველ ბიტს გააჩნია განსაზღვრული მნიშვნელობა. მარჯვნიდან პირველი ბიტის სიდიდე 1-ის ტოლია, ხოლო დანარჩენი ბიტების მნიშვნელობები მარჯვნიდან მარცხნივ ტოლია: 2, 4, 8, 16, 32, 64 და 128. განვსაზღვროთ ოქტეტის მნიშვნელობა: ამისათვის შევკრიბოთ ოქტეტის მხოლოდ ის მნიშვნელობები, რომლებიც გამოსახულია ორობითი ერთიანით.

- თუ პოზიციის მნიშვნელობა 0-ის ტოლია, მაშინ არ ვამატებთ ამ მნიშვნელობებს.
- თუ რვავე ბიტი 0-ის ტოლია მაშინ 00000000-ის მნიშვნელობა 0-ის ტოლია.
- თუ რვავე ბიტი 1-ის ტოლია მაშინ ოქტეტი 255-ის ტოლია (128+64+32+16+8+4+2+1=255).
- თუ ოქტეტი შეიცავს, როგორც ერთებს ასევე ნულებს, მაგ., 00100111, მაშინ ამ ოქტეტის მნიშვნელობა ტოლია 39-ის (32+4+2+1=39)

მაშასადამე, ყოველი ოქტეტის მნიშვნელობები იცვლება 0-დან 255-მდე დიაპაზონში.



IP-მისამართის გარდაქმნა ორობითიდან ათობითში

3.4 IP-მისამართის შემადგენელი ნაწილები

ლოგიკური IP-მისამართი იერარქიულია და შედგება ორი ნაწილისაგან.. პირველი განსაზღვრავს ქსელს, ხოლო მეორე ამავე ქსელის ჰოსტს.

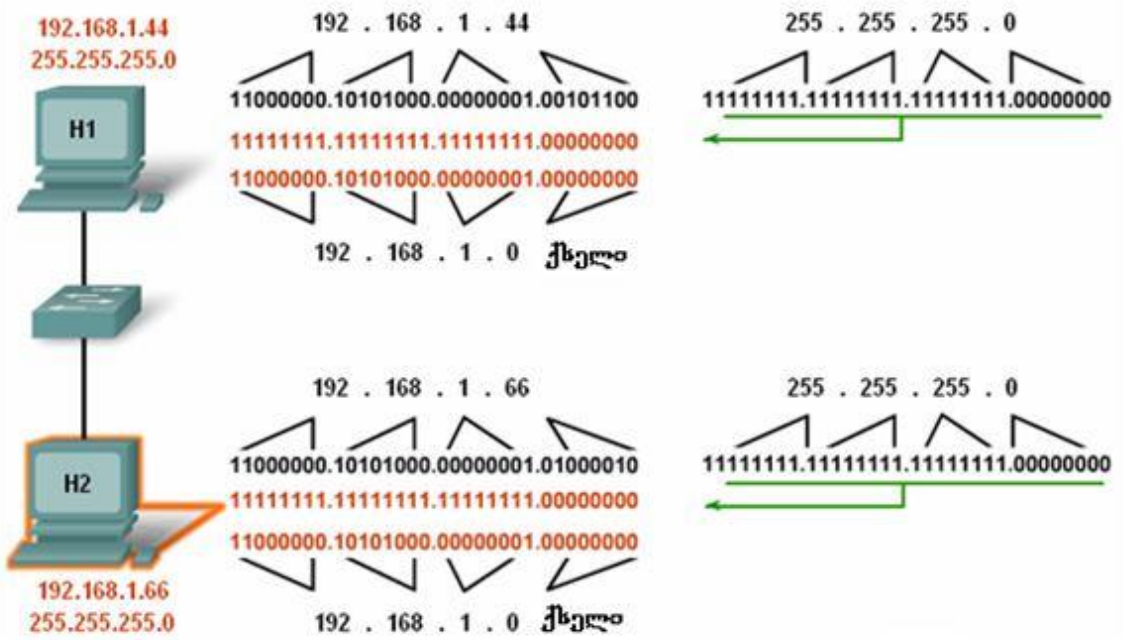
მაგ. თუ ჰოსტს აქვს 192.168.18.57 IP-მისამართი, მაშინ პირველი სამი ოქტეტი განსაზღვრავს ქსელს (192.168.18), ბოლო ოქტეტი (57) კი ჰოსტს. ასეთ დამისამართებას ეწოდება იერარქიული.

3.4.1 IP-მისამართებისა და Subnet მასკების ურთიერთკავშირი

როგორც აღინიშნა, IP-მისამართი შედგება ორი ნაწილისაგან: ქსელური და ჰოსტის ნაწილისაგან, მათი ერთმანეთისაგან გარჩევა კი ეკისრება სუბნეტ მასკებს.

IP-ჰოსტის დაკონფიგურებისას IP-მისამართთან ერთად მოიცემა სუბნეტ მასკაც, რომელიც

ასევე 32-ბიტიანია, როგორც IP-მისამართი. სუბნეტ მასკა განასხვავებს IP-მისამართში თუ რომელია ქსელის ნაწილი და რომელი ჰოსტის.



Subnet მასკისა და IP-მისამრთის შედარება

Subnet მასკისა და IP-მისამრთის შედარება ხდება მარცხნიდან მარჯვნივ თითოეული ბიტობით. ერთიანები Subnet მასკაში განსაზღვრავენ ქსელის ნაწილს, 0-ები კი ჰოსტის ნაწილს. როცა ჰოსტი აგზავნის პაკეტს, ის ადარებს Subnet მასკას თავის IP-მისამართთან და მიმღების IP-მისამართთან. თუ ქსელური ბიტები, როგორც გადამცემის ასევე მიმღების შეესაბამება ერთმანეთს მაშინ ორივე იმყოფება ერთ ქსელში და პაკეტი გადაეცემა ადრესატს ლოკალურად. თუ არ შეესაბამებიან, მაშინ გადამცემი ჰოსტი ამ პაკეტს გადაუგზავნის როუტერის ინტერფეისს სხვა ქსელში გადასაგზავნად.

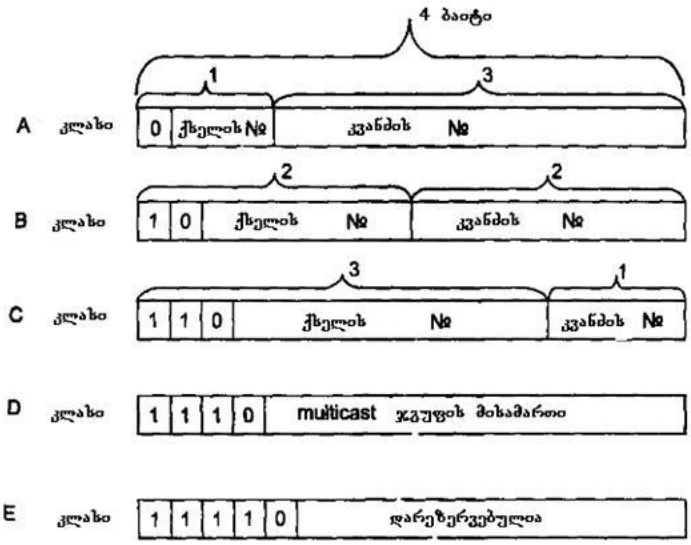
სუბნეტ მასკები მცირე და საშუალო ზომის ქსელებისათვის გამოიყურება შემდეგნაირად: 255.0.0.0 (8-ბიტი), 255.255.0.0 (16 ბიტი) და 255.255.255.0 (24 ბიტი). 255.255.255.0 (ათობითი) ანუ Subnet მასკა 11111111.11111111.1111111.00000000 (ორობითი) იყენებს 24 ბიტს ქსელის განსასაზღვრავად, ხოლო დანარჩენი 8 ბიტით განისაზღვრება ჰოსტი ამავე ქსელში. ჰოსტების რიცხვი გამოითვლება შემდეგნაირად: ჰოსტების ბიტების რიცხვი

უნდა ავიყვანოთ 2-ის ხარისხში ანუ (2(ხარისხად 8) = 256). Aამ რიცხვს უნდა გამოვაკლოთ 2 (256-2=254). 2-იანს იმიტომ ვაკლებთ, რომ ყველა 1-იანი IP-მისამრთის ჰოსტის ნაწილში არის ფართოამუწყებლობითი მისამართი (broadcast address) ქსელისათვის და შეუძლებელია მინიჭებული ჰქონდეს ჰოსტისთვის. ხოლო 0-იანები ჰოსტის ნაწილში მიეკუთვნება ქსელს და ასევე შეუძლებელია მიენიჭოს ჰოსტს.

მეორე მეთოდი ჰოსტების რიცხვის განსასაზღვრავად: შევკრიბოთ ჰოსტის ყველა შესაძლო ბიტი (128+64+32+16+8+4+2+1=255). ამ რიცხვს გამოვაკლოთ 1 (255-1=254), რადგანაც ჰოსტის ბიტები ყველა არ შეიძლება იყოს 1-ის ტოლი. Aაქ არ არის აუცილებელი გამოვაკლოთ 2, რადგანაც 0-ის მნიშვნელობა 0-ია და თავისთავად არ დაემატება. 16-ბიტიანი მასკის შემთხვევაში გვაქვს 16 ბიტი (ორი ოქტეტი) ჰოსტის მისამართისათვის და ამ შემთხვევაში ჰოსტის მისამართი შეიძლება შეიცავდეს ყველა 1-იანს (255) თითოეულ ოქტეტში. Mმაგრამ ამ შემთხვევაში შეიძლება გამოიყურებოდეს როგორც ფართომაუწყებლობითი, მაგრამ რადგან სხვა ოქტეტი არ შეიცავს 1-იანებს, ამ შემთხვევაში ის ნამდვილად ჰოსტის მისამართია.

3.5 IP-მისამართების კლასები

IP-მისამართის სიგრძე შეადგენს 4 ბაიტს და ჩვეულებრივ ჩაიწერება ოთხი რიცხვის სახით, სადაც ყოველი ბაიტი გამოისახება ათობითი რიცხვით, რომლებიც დაყოფილნი არიან წერტილებით. მაგ., 128.10.2.30 – ტრადიციული ათობითი ფორმა მისამართის წარმოსადგენად, 10000000 00001010 00000010 00011110 – ორობითი ფორმა ამავე მისამართისა. მისამართი შედგება ორი ლოგიკური ნაწილისგან – ქსელის ნომრისა და ქსელში კვანძის ნომრისგან. მისამართის თუ რომელი ნაწილი მიეკუთვნება ქსელის ნომერს და რომელი კვანძისას, განისაზღვრება მისამართის პირველი ბიტების მნიშვნელობებით. ამ ბიტების მნიშვნელობები კი განსაზღვრავენ თუ რომელ კლასს მიეკუთვნება ესა თუ ის IP-მისამართი. ნახაზზე ნაჩვენებია სხვადასხვა კლასების IP-მისამრთების სტრუქტურა.



IP-მისამართის სტრუქტურა

თუ მისამართი იწყება 0-ით, მაშინ ის მიეკუთვნება A კლასს და ამ შემთხვევაში ქსელის ნომერსი იკავებს 1 ბაიტს, ხოლოდ დანარჩენი ნომრები ინტერპრეტირდება, როგორც კვანძის ნომერი. A კლასის ქსელებს გააჩნიათ ნომრები 0-დან 126-მდე. (0 არ გამოიყენება, ხოლო 127 დარეზერვებულია სპეციალური მიზნებისათვის, რაზეც გამახვილებთ ყურადგებას მოგვიანებით). A კლასის ქსელები მცირეა, ხოლო მათში კვანძთა რიცხვმა შეიძლება მიაღწიოს 2(ხარისხად 24)-ს, ანუ 16777216-ს.

თუ მისამართის პირველი ორი ბიტი ტოლია 10-ის, მაშინ ის მიეკუთვნება B კლასს. B კლასის ქსელებში ქსელისა და კვანძის ნომრებისთის გამოყოფილია 16 16 ბიტი ანუ 2 ბაიტი. მაშასადამე B კლასის ქსელი მიეკუთვნება საშუალო სიდიდის ქსელს კვანძების მაქსიმალური რიცხვი რომელშიც ტოლია 2(ხარისხად 16)-ის, რომელიც შეადგენს 65 536 კვანძს.

თუ მისამრთი იწყება 110 მიმდევრობით, მაშინ ის მიეკუთვნება C კლასს. ამ შემთხვევაში ქსელის ნომრისთვის განკუთვნილია 24 ბიტი, ხოლო კვანძის ნომრისთვის – 8 ბიტი. ამ კლასის ქსელები უფრო ფართოდაა გავრცელებული. მათში კვანძების რიცხვი შეზღუდულია 2(ხარისხად 8)-მდე ანუ 256-მდე.თუ მისამართი იწყება 1110 თანმიმდევრობით, მაშინ ის მიეკუთვნება D კლასს და აღნიშნავს განსაკუტრებულ, ჯგუფურ მისამრთს – multicast. თუ პაკეტში დანიშნულების მისამართად მითითებულია D კლასის მისამართი, მაშინ ასეთი პაკეტი უნდა მიიღოს ყველა კვანძმა, რომლებსაც მინიჭებული აქვთ მოცემული მისამართი.

თუ მისამართი იწყება 11110 თანმიმდევრობით, მაშინ ის მიეკუთვნება E კლასს. ამ კლასის მისამრთები დარეზერვებულია მომავალში გამოსაყენებლად.

8.2 ცხრილში მოცემულია ქსელების ნომრები დიაპაზონი და კვანძების მაქსიმალური რიცხვი, რომლებიც შეესაბამება ქსელების ყოველ კლასს.

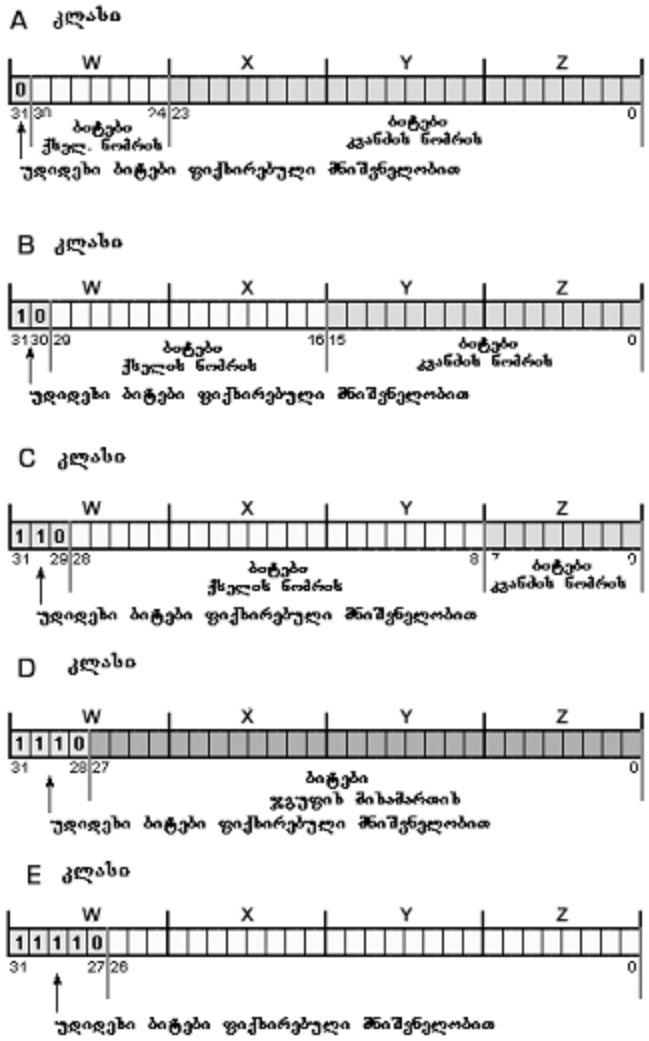
ხვადახვა კლახიხ მიხამართებიხ მახახიათებლები

კლახი	პირველი ბიტები	ქსელის უმცირესი ნომერი	ქსელის უდიდესი ნომერი	კვანძების მაქსიმალური რიცხვი ქსელში
A	0	1.0.0.0	126.0.0 0	2^{24}
B	10	128.0.0.0	191.255 0.0	2^{16}
C	110	192.0.1.0	223.255 255.0	2^{8}
D	1110	224.0.0.0	239.255.255.255	Multicast
E	11110	240.0.0.0	247.255.255.255	დარეზერვებულია

დიდი ქსელებს ენიჭებათ A კლასის მისამართები, საშუალო ზომის ქსელებს - B კლასის, ხოლო მცირე ზომის ქსელებს - C კლასის.

A, B, C, D და E კლახებიხ IP-მიხამართებიხ ორობითი ხქემები

IP-მისამართების კლასები	A	B	C	D	E
პირველი ოქტეტის დიაპაზონი	1-126	128-191	192-223	224-239	240-247



3.6 Unicast, Broadcast და Multicast მისამართები

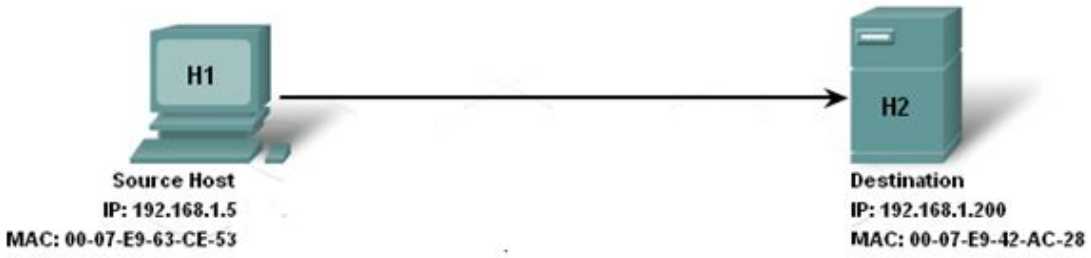
IP მისამართები იყოფა შემდეგ კატეგორიებად: Unicast, Broadcast დაMulticast მისამართები. ჰოსტი იყენებს Unicast IP მისამართს ერთი-ერთთან კომუნიკაციისას, Broadcast IP მისამართს ერთი-ბევრთან, ხოლო Multicast IP მისამართს ერთი-ყველასთან.

3.6.1 Unicast

Unicast მისამართი ყველაზე ზოგადი ტიპია IP ქსელისა. პაკეტი Unicast მისამართით დანიშნულია სპეციალური ჰოსტისთვის. მაგალითად შეიძლება მოვიყვანოთ ჰოსტი

192.168.1.5 IP მისამართით (გადამცემი), რომელმაც გააგზავნა მოთხოვნა WEB გვერდზე სერვერისგან IP მისამართისგან 192.168.1.200 (მიმღები).

Unicast პაკეტის გადაცემის და მიღების მომენტში მიმღების IP მისამართს შეიცავს IP პაკეტის თავსართი. შესაბამისი მიმღების MAC მისამართი გამოისახება Ethernet frame-ის თავსართი. IP მისამართი და MAC მისამართი კომბინირდება მონაცემების გადასაცემად სპეციალრული ჰოსტისთვის.



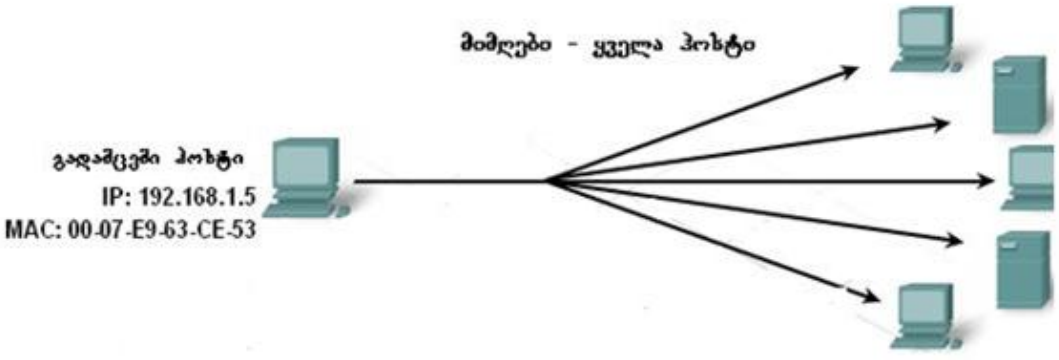
3.6.2 Broadcast

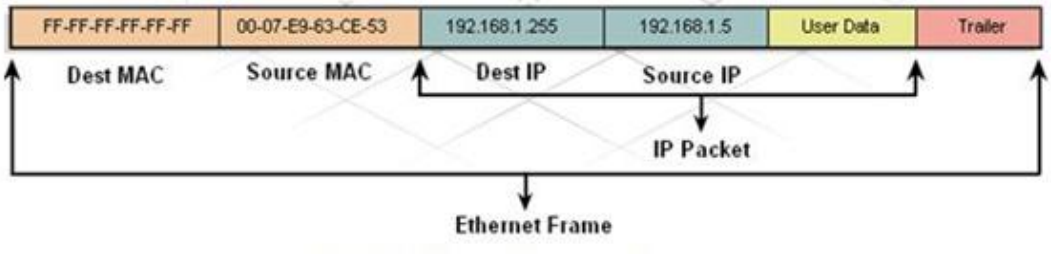
Broadcast მისამართის შემთხვევაში პაკეტი შეიცავს მიმღების IP მისამართს, რომელიც შეიცავს მხოლოდ ერთიანებს ჰოსტის ნაწილში. ეს ნიშნავს, რომ ყველა ჰოსტს ლოკალურ ქსელში შეუძლია მიიღოს და ნახოს პეკეტები. ქსელური პროტოკოლების უმრავლესობა, როგორიცაა: ARP და DHCP იყენებენ Broadcast –ს.

C კლასის ქსელს 192.168.1.0 შესაბამისი სუბნეტ მასკით 255.255.255.0 აქვს Broadcast მისამართი 192.168.1.255. ჰოსტის ნაწილი არის, როგორც ათობითი 255 ასევე ორობითი 11111111 (ყველა ერთიანია).

B კლასის ქსელს 172.16.0.0 შესაბამისი Subnet მასკით 255.255.0.0 აქვს Broadcast მისამართი 172.16.255.255.

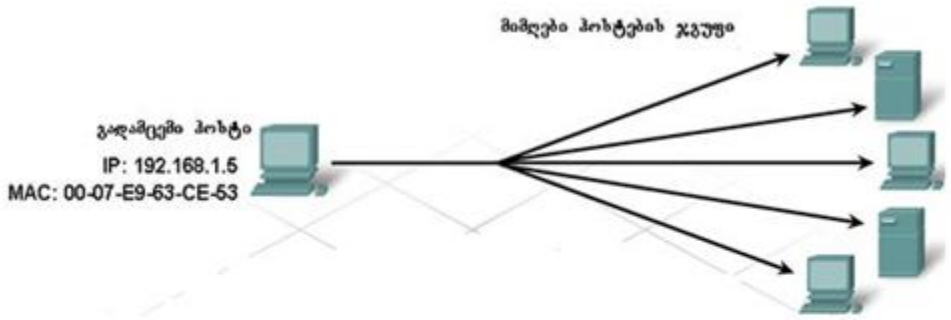
A კლასის ქსელს 10.0.0.0 შესაბამისი Subnet მასკით 255.0.0.0 აქვს Broadcast მისამართი 10.255.255.255.Broadcast მისამართს ქსელური ნაწილისთვის სჭირდება შესაბამისი Broadcast MAC მისამართი Ethernet frame-ში. Ethernet ქსელში Broadcast MAC მისამართი გამოისახება 48 ერთიანით თექვსმეტობითი ფორმით FF-FF-FF-FF-FF

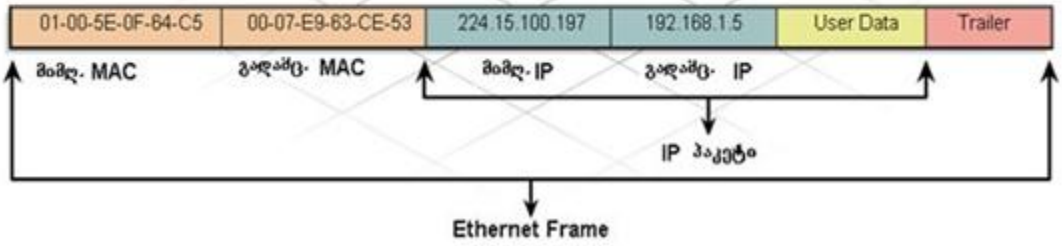




3.6.3 Multicast

Multicast მისამართის მეშვეობით გადამცემი პაკეტს გადასცემს მოწყობილობათა ჯგუფს. მოწყობილობებს, რომელიც მიეკუთვნება Multicast ჯგუფს მიენიჭება Multicast ჯგუფის IP მისამრთი. Multicast მისამრთის დიაპაზონი შეადგენს 224.0.0.0-დან 239.255.255.255-მდე. ე.ი. მულტიქასთ მისამართები გამოსახავენ მისამართების ჯგუფს (ზოგჯერ უწოდებენ ჰოსტის ჯგუფებს), რომლებიც გამოიყენება პაკეტის მიმღებად. გადამცემს კი ყოველთვის Multicast მისამრთი გააჩნია. Multicast მისამრთების მაგალითად შეიძლება გამოყენებულ იქნას რემოტე თამაშები, როცა მოთამაშეები თამაშობენ დაშორებულ მანძილზე ერთ და იგვე თამაშს. მეორე მაგალითი შეიძლება იყოს დისტანციური სწავლება ვიდეო კონფერენციით, სადაც ბევრი სტუდენტი შეერთებულია ერთი და იგივე კლასთან. როგორც unicast ან broadcast, ასევე Multicast IP მისამრთები საჭიროებენ შესაბამის MAC მისამართებს ლოკალურ ქსელში ფრეიმების გადასაგზავნად. Multicast MAC მისამრთი სპეციალური სიდიდეა, რომელიც იწყება 01-00-5E (თექვსმეტობითში).





4. უსაფრთხოების პოლიტიკა

უსაფრთხოების პოლიტიკა არის IT გუნდის მიერ შედგენილი წესების და პოლისების ნაკრები, რომელიც უზრუნველყოფს მონაცემთა დაცულობას და უცხო პირთა შეუღწევადობას ქსელში. უსაფრთხოების პოლიტიკის შემუშავებაში იგულისხმება ქსელურ და სერვერულ აპარატურაში არასანქცირებული შეღწევისგან თავის დაცვა, კომპიუტერებში მოთავსებული მონაცემების ხელშეუხებლობა, მეილსერვერის და ვებ გვერდის გატეხვისგან დაცვა, პირადი ინფორმაციის არაკანონიერი გზით მოპოვების აღკვეთა (ისეთი ინფორმაციის, როგორიცაა პაროლები, სხვადასხვა საბანკო და ასე შემდეგ).

განვიხილოთ security police-ები ქსელურ მოწყობილობაზე. ძირითადი პრინციპები შემდეგში მდგომარეობს:

Password Security. ნებისმიერ მოწყობილობაზე პაროლი უნდა იყოს რთული, უნიკალური და უნდა შედგებოდეს დიდი და პატარა ასოებისგან, ციფრებისა და სიმბოლოებისგან. პაროლი უნდა შეიცვალოს ხშირ-ხშირად (მაქსიმუმ 3 თვეში მაინც).

აპარატურის დაცვა რთული პაროლით აპარატურაში აუტენტიკაცია AAA\Radius სერვერის საშუალებით. ამ მეთოდში იგულისხმება მოწყობილობაზე აუტენტიკაცია მოშორებული სერვერის საშუალებით, სადაც ინახება მომხმარებლების და მათი პაროლების შესახებ ინფორმაცია.

ტრაფიკის ფილტრაცია. გარე ქსელიდან შიდა ქსელში დაშვებული უნდა იყოს მხოლოდ ისეთი ტრაფიკი, რომელიც წარმოშობილია შიდა ქსელის კომპიუტერებიდან. აკრძალული უნდა იყოს ქსელის გარედან სერვისები: telnet, ssh, snmp, RDP და ასე შემდეგ. უნდა ვიმოქმედოთ შემდეგი პრინციპის მიხედვით: „აკრძალულია ყველაფერი, დაშვებულია მხოლოდ საჭირო სერვისები (ვებ სერვისები, მეილი ფტპ და სხვა ცნობილი სერვისები).

შიდა ქსელში ჩართული უნდა იყოს მხოლოდ ორგანიზაციის კომპიუტერები და არ უნდა მოხდეს უცხო კომპიუტერის ჩართვა. ამ საფრთხისგან თავის დასაცავად არსებობს საკმაოდ კარგი მეთოდი 802.1x authentication. ამ აუტენტიკაციის საშუალებით კომპიუტერი ქსელის პარამეტრებს იღებს მხოლოდ მას შემდეგ, რაც აქტივ დირექტორიის ექაუნთით გაივლის ავტორიზაციას ქსელურ მოწყობილობაზე. (ამ მეთოდზე დაწვრილებით მოგვიანებით ვისაუბრებთ).

კომპიუტერის უსაფრთხოება. კომპიუტერზე აუცილებლად უნდა დაყენდეს ანტივირუსული პროგრამა, უნდა იჯდეს აქტივ დირექტორიაში და მომხმარებელს უნდა ჰქონდეს საკუთარი უნიკალური პაროლი (password security) კომპიუტერზე დაბლოკილი უნდა იყოს გასართობი პროგრამების გაშვება, მომხმარებელს შეზღუდული უნდა ჰქონდეს წვდომა ისეთ საიტებზე, რომლებიც საფრთხის შემცველია.

ჩამოვაყალიბეთ უსაფრთხოების პოლიტიკის ძირითადი პრინციპები, თუმცა ეს არ არის სრული სია. თითოეული ორგანიზაციისთვის ინდივიდუალურად უნდა შედგეს

მოთხოვნები, გაიწეროს რისკები და კომპანიის მუშაობის მიზნები და მას შემდეგ შედგეს მასზე მორგებული უსაფრთხოების პოლიტიკის დოკუმენტაცია.

4.1 უსაფრთხოების პროტოკოლები, ალგორითმები.

ინფორმაციის დაცულობაზე ადამიანებთან ერთად სხვადასხვა პროტოკოლები და ალგორითმებიც მუშაობენ.

ალგორითმებია: DES, AES, 3DES, RSA, ჰეშირების ფუნქცია.

დაცული პროტოკოლები: HTTPS, SSH, SFTP, SSL, TSL, IKE, IPSEC და სხვები...

რამდენიმე მათგანს დაწვრილებით განვიხილავთ.

DES (ინგ. **Data Encryption Standard**) - მონაცემთა დაშიფრვის სიმეტრიული ალგორითმი, რომელშიც ერთი და იგივე გასაღები გამოიყენება როგორც მონაცემთა დასაშიფრად, აგრთვე მის გასაშიფრად.

DES-ი მუშაობს მონაცემთა 64-ბიტიან ბლოკებზე, დაშიფრვისთვის იყენებს 56-ბიტიან გასაღებს, აქვს ფეისტელის ქსელის 16-ციკლიანი სტრუქტურა.

ალგორითმი იყენებს წრფივ (E, P, IP, FP გადანაცვლებები) და არაწრფივ (S-box) კომბინირებულ გარდაქმნებს. DES-ისთვის რეკომენდირებულია რამდენიმე რეჟიმი, მაგ., Electronic Code Book (ECB)და Cipher Block Chaining (CBC). აგრეთვე ცნობილია, როგორც მონაცემთა დაშიფრვის ალგორითმი DEA (ინგ. Data Encryption Algorithm). დღესდღეობით მისი გამოყენება აღარ არის რეკომენდირებული, მისი შესრულების სინელისა და მოკლე გასაღების გამო, რის გამოც იგი მუდმივი თავდასხმის საშიშროების ქვეშ დგას. DES-მეთოდი

ძირითადად გამოიყენებოდა Unix-პაროლების დასაშიფრად. მისი ყველაზე გავრცელებული ნაირსახეობა იყო Triple DES.

AES - Advanced Encryption Standard არის DES-ის გაუმჯობესებული ალგორითმი, რომელიც პირველად გამოქვეყნდა 1998 წელს. AES-ში გამოიყენება სამნაირი, 128, 192 და 256 ბიტის სიგრის გასაღები. ის მუშაობს 128 ბიტიან ბლოკზე.

RSA-წარმოადგენს ალგორითმს, რომელიც ღია გასაღების საშუალებით შიფრავს ინფორმაციას. ალგორითმი პირველად გამოქვეყნდა 1977 წელს. მისი მუშაობის პრინციპი შემდეგია: პერსონა A უგზავნის პერსონა B-ს საკუთარ ღია გასაღებს (n, e) და თავისთვის იტოვებს დახურულ გასაღებს. B-ს უნდა რომ გაუგზავნოს M ინფორმაცია A-ს. B ირჩევს ისეთ m რიცხვს, რომელიც 0 ≤ m < n, შიფრავს ინფორმაციას და გადასცემს c დაშიფრულს A-ს.

$$c \equiv m^e \pmod{n}.$$

A-ს შეუძლია აღადგინოს m საკუთარი დახურული d გასაღების საშუალებით, ხოლო m-ით დააბრუნებს ინფორმაციის ორიგინალს - M.

$$m \equiv c^d \pmod{n}.$$

ამ და სხვა ალგორითმების დახმარებით შესაძლებელი იქნა შექმნილოყო არხში უსაფრთხოდ გადამცემი პროტოკოლები.

HTTPS – HTTP პროტოკოლის დაცული ვერსია. გამოიყენება ვებ გვერდებზე შესვლისას. როგორც წესი http პროტოკოლი არხში გადის ღია, დაუშიფრავ ტექსტად და მისი წაკითხვა ნებისმიერ packet analyzer პროგრამას შეუძლია. https პროტოკოლი საშუალებას გვაძლევს დავშიფროთ კონტენტი და ისე გადავცეთ მიმღებს. ეს პროტოკოლი ძირითადად გამოიყენება ინტერნეტსაიტებიდან საბანკო ოპერაციების ჩატარებისას, სისტემაში აუტორიზაციის დროს, ელექტრონული ფოსტის შემოწმებისას და ასე შემდეგ... მსოფლიოში ნომერ პირველ search engine – Google-ს საკუთარი საძიებო სისტემა https პროტოკოლზე აქვს გამართული. ასევე https-ზე მუშაობის შესაძლებლობა აქვს სოციალურ ქსელ - ფეისბუქს და სკაიპს.

SSH – Secure Shell პროტოკოლი არის Telnet -ის დაცული ვერსია. ის გამოიყენება სხვადასხვა ქსელურ და სერვერულ აპარატურაზე კავშირის დასამყარებლად და კონფიგურაციის გასამართად. telnet http-ს მსგავსად დაუშიფრავ ინფორმაციას გზავნის

ქსელში და როდესაც საქმე ეხება ქსელურ მოწყობილობებს და მათ გამართულად მუშაობას, რათქმაუნდა არ შეიძლება რომ კონფიგურაციის ფაილი ან თუნდაც უზერი და პაროლი packet sniffing-ის საშუალებით უცხო ადამიანის ხელშ მოხვდეს. ასეთ სიტუაციაში აუცილებელია SSH-ის გამოყენება.

SFTP – Secure File Transfer Protocol ეს პროტოკოლიც არის FTP-ს დაცული ვერსია. მისი საშუალებითაც ანალოგიურად ხდება ინფორმაციის დაშიფვრა და სერვერზე ატვირთვა.

IPSEC - Internet Protocol Security ამ პროტოკოლის საშუალებით დგება VPN ტუნელი ორ დაშორებულ ოფისს შორის და მონაცემების გადაცემა ხდება დაშიფრულად. IPsec გულისხმობს IP პროტოკოლის ენკაფსულაციას და პაკეტის დაშიფვრას ახალ, ჰედერშეცვლილ პაკეტად. IPsec პროტოკოლი იყენებს აუტენტიკაციის, ენკაპსულაციის და ჰეშირების ალგორითმებსა და პროტოკოლებს, კრავს ტუნელს ინტერნეტში და იცავს მონაცემებს უცხო ადამიანებისგან. სხვა პროტოკოლებისგან განსხვავებით იგი მუშაობს OSI მოდელის ქვედა დონეზე (Network layer) და შიფრავს მთლიანად პაკეტს.

4.2 გარედან წარმოქმნილი საფრთხეები

ქსელის ტოპოლოგიის დაგეგმვისას აუცილებლად უნდა იყოს გათვალისწინებული უსაფრთხოების პოლიტიკის მოთხოვნები, security კრიტერიუმები და ამ ყველაფრისთვის გამოყოფილი ბიუჯეტი. ყველაზე კარგი და უსაფრთხო გადაწყვეტილებაა ლოკალური ქსელის დაცვა ფაირვოლის საშუალებით. ფაირვოლი არსებობს ორნაირი სახის:

Hardware Firewall

Software Firewall

Hardware Firewall არის ფიზიკური მოწყობილობა, რომელიც აპარატურულ დონეზე ფილტრავს ტრაფიკს. Hardware Firewall-ის ყველაზე ცნობილი და გავრცელებული მწარმოებლებია Cisco და Barracuda, რომლებიც აწარმოებენ PIX/ASA და NG Firewall-ებს.

Hardware Firewall -ის ძირითადი მახასიათებლებია ტრაფიკის გამტარუნარიანობა დაკვირვების რეჟიმში, მაქსიმალური კავშირების დამყარება (max connections established), დაკრიპტული ვპნ ტრაფიკის გამტარუნარიანობა, სხვადასხვასიჩქარიანი პორტების რაოდენობა და ასე შემდეგ. დაწვრილებით განვიხილოთ ეს პარამეტრები ზემოთ აღნიშნულ მწარმოებლების ფაირვოლებზე. დღესდღეობით Cisco PIX Firewall აღარ არის წარმოებაში, ის ჩაანაცვლა Cisco ASA-მ რომელიც გაცილებით მძლავრი და მეტი შესაძლებლობებისაა მის წინამორბედთან შედარებით. მოცემული ცხრილის და ჩვენი მოთხოვნების საშუალებით შევძლებთ ზუსტად შევარჩიოთ სასურველი აპარატურა.

დეტალური ინფორმაცია შეგვიძლია მოვიძიოთ საიტზე:
http://www.cisco.com/en/US/products/ps6120/prod_models_comparison.html

მაგალითად თუ გვინდა ფაირვოლი სახლისთვის ან მცირე ოფისისთვის (10-30 კომპიუტერი) შეგვიძლია შევარჩიოთ 5505 სერიის ASA. იგი არ გამოირჩევა სწრაფი გამტარუნარიანობითა (150 Mbps) და ბევრი კავშირების რაოდენობით (4000. ერთი კომპიუტერი ინტერნეტში გასვლისას შეიძლება რამდენიმე ასეულ კავშირს ამყარებდეს სხვადასხვა სერვერზე და სხვადასხვა პორტზე), თუმცა საკმაოდ მცირე ფასი აქვს სხვა მოდელებთან შედარებით და მისი შეძენა 300$-ის ფარგლებშია შესაძლებელი. ასევე შეგვიძლია არჩევანი შევაჩეროთ საკმაოდ მძლავრ ASA 5550 მოდელზე, რომელსაც 1200mbps-მდე ტრაფიკის გატარება და 33000 ახალი კავშირის დამყარების შესაძლებლობა აქვს. მისი ფასი 4500$-ის ფარგლებშია.

დიდი კომპანიის შემთხვევაში არჩევანი შეიძლება გაკეთდეს ASA 5580 და ASA 5585 სერიებზე, რომელთა ფაირვოლის რეჟიმში გამტარუნარიანობა რამდენიმე ათეულ გიგაბიტს აღწევს ერთ წამში. მათ ასევე რამდენიმე ასეულ-ათასი კავშირის დამყარება შეუძლიათ ერთდროულად, თუმცა მათი ფასი ძალიან ძალიან დიდია.

თითქმის იგივე პარამეტრების საშუალებით შეიძლება შეირჩეს ფაირვოლი ბარაკუდას NG მოდელის სერიებიდან. მაგალითისთვის რომ განვიხილოთ F9 სერიის ფაირვოლი. მას

შეუძლია წამში 21GB ჩვეულებრივი, ხოლო 3.8GB - დაკრიპტული ტრაფიკის გატარება. მისი საორიენტაციო ფასი 38000$-ია.

Software Firewall-ებში მეტად გავრცელებული პროდუქტებია ლინუქსის ოპერაციულ სისტემაზე აწყობილი Squid, ბარაკუდას პროგრამული ფაირვოლები, Kerio, Windows ISA server და ასე შემდეგ... მათი მუშაობის პრონციპი იგივეა, უბრალოდ ისინი ტრაფიკის ფილტრაციას პროგრამულ დონეზე ახდენენ. მათი გამართვა შესაძლებელია სერვერზე დაყენებულ სხვადასხვა ოპერაციულ სისტემებზე.

ფაირვოლები თავდაპირველად მუშაობდნენ Packet filtering რეჯიმში, რაც ნიშნავს რომ ისინი არ უყურებდნენ მთლიან ნაკადს და ფილტრავდნენ სათითაოდ ყველა პაკეტს. ასეთი მიდგომით ფაირვოლები ხარჯავდნენ უაზროდ ბევრ რესურსს და არ ჰქონდათ შესაძლებლობა, შეესრულებინათ სხვა მრავალი ფუნქცია.

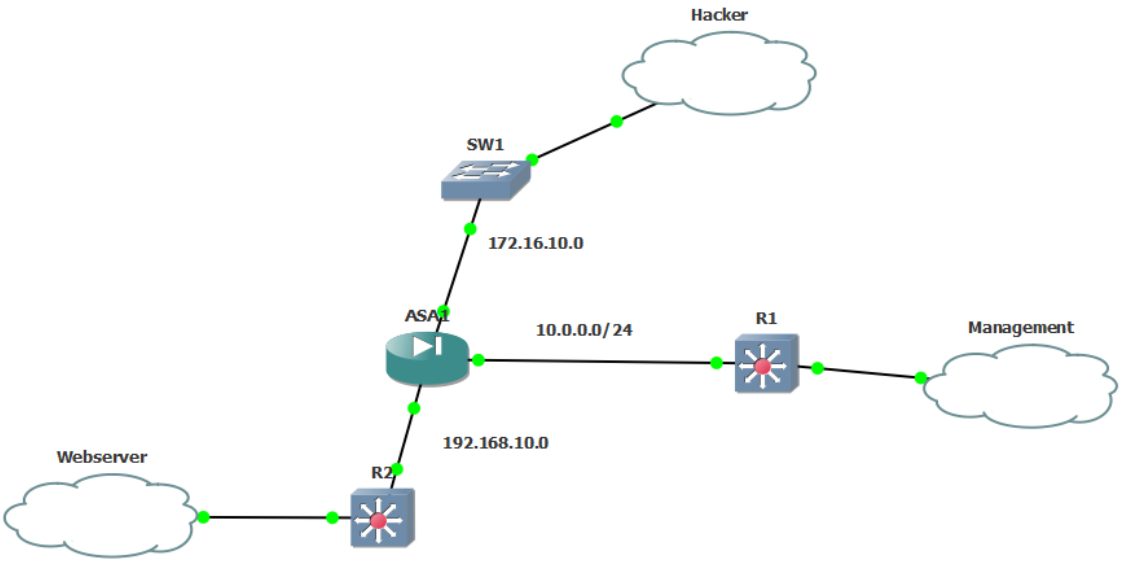
მეორე თაობის ფაირვოლებს უკვე უწოდეს "Stateful" filters მათ შეეძლოთ OSI მოდელის 4-ე დონეზე ედევნებინათ თვალი კავშირისთვის და გამოერკვიათ ესა თუ ის პაკეტი ახალი კავშირის დასაწყისი იყო თუ უკვე არსებულის გაგრძელება.

მესამე თაობის ფაირვოლები უკვე Application layer-ზე მოქმედებენ. მათ შეუძლიათ 7-ე დონის პროტოკოლების შიგთავსში ჩახედვა და გამორკვევა ესა თუ ის პაკეტი დაიშვება თუ არა ქსელის შიგნით. ასეთი ტიპის ფილტრაცია გაცილებით ეფექტურად მუშაობს ვიდრე მხოლოდ პორტების და იპ მისამართების მიხედვით ფილტრაცია.

ჩემს სამაგისტრო ნაშრომში გამოყენებული მაქვს Cisco ASA 5520 სერიის ფაირვოლი. მისი მუშაობის მთავარი პრინციპია, დაკვირვება მოახდინოს ყველა იმ პაკეტზე და კავშირზე რომელიც მისი გავლით ინტერნეტში ხვდება ან ინტერნეტიდან შიდა ქსელში ცდილობს შეღწევას, წინასწარ განსაზღვრული წესების მიხედვით გაფილტროს ისინი და გაატაროს მხოლოდ სანდო ინფორმაცია. ტრაფიკის ფილტრაციის მთავარი წესი შემდგომში მდგომარეობს: თავდაპირველად დაიბლოკოს ყველანაირი ტრაფიკი, ხოლო შემდეგ გაიხსნას წვდომა მხოლოდ საჭირო პროტოკოლებსა და იპ მისამართებზე. მაგალთად, არ არსებობს ქსელი სადაც არ იყენებდნენ HTTP ტრაფიკს, ამიტომ ის აუცილებლად დაშვებული უნდა იყოს. ასევე უნდა გაიხსნას DNS პროტოკოლიც, რათა უპრობლემოდ შეიძლებოდეს ინტერნეტ

საიტებზე შესვლა. მოთხოვნის შესაბამისად შეიძლება გაიხსნას FTP, Telnet E-mail და სხვადასხვა Remote desktop პროგრამების პორტები. ყველანაირი ტრაფიკი, ინიცირებული უცხო იპ მისამართიდან არაცნობად პორტზე უნდა იყოს დაბლოკილი ფაირვოლის გარე ინტერფეისზევე.

ჩვენს შემთხვევაში შიდა ქსელში გვაქვს ერთი ვირტუალური ვებ, სერვერი, რომელზეც ატვირთულია უბრალო საიტი, გაშვებულია FTP, Telnet და DNS სერვისები. გარე ქსელიდან წვდომა გახსნილია HTTP, DNS და FTP(მხოლოდ გადმოწერა) სერვისებზე, დანარჩენი სერვისები დაბლოკილია.



ფაირვოლი იმათება ფიზიკური კომპიუტერიდან(Management), აქვს შიდა ქსელი იპ დამისამართებით: 192.168.10.0/24 რომელშიც მდებარეობს ვებსერვერი და აქვს გარე ქსელი(პირობითად: ინტერნეტის მხარე) სადაც ზის ჰაკერი. ჰაკერის მთავარი ფუნქციაა რომ შეაღწიოს შიდა ქსელში, გატეხოს სერვერი ან თუ ვერ შეძლებს ამას, განახორციელოს DOS (Denial On Service) შეტევა და მიუწვდომელი გახადოს ვებსერვერი სხვა მომხმარებლებისთვის.

განვიხილეთ ქსელის დაცვის მეთოდები ფაირვოლის საშუალებით, მაგრამ არის შემთხვევები, როდესაც ორგანიზაციას არ შეუძლია, დამატებითი რესურსები გაიღოს აპარატურის ყიდვაზე. ასეთ შემთხვევაში უსაფრთხოებას უზრუნველყოფს როუტერში ჩაშენებული ფაირვოლი. როუტერებზე შეგვიძლია გავააქტიუროთ აქსეს ლისტები და დავბლოკოთ ტრაფიკი პორტების, იპ მისამართების, სერვისების და დროის მიხედვით. შედარებით ახალ როუტერებს (2900, 3900 სერიის) აქვთ Statefull firewall და Application Firewall-ების შესაძლებლობაც, რაც საშუალებას გვაძლევს განვახორციელოთ ზემოთ ჩამოთვლილი უსაფრთხოების მოთხოვნები მინიმალური რესურსებით.

აქსეს ლისტის მაგალითი:

Extended IP access list TestACL

10 permit tcp 192.168.1.0 0.0.0.255 any eq www

20 deny udp host 192.168.1.1 host 8.8.8.8 eq domain

30 deny tcp 192.168.2.0 0.0.0.255 host 192.168.1.1 eq telnet time-range TimeACL (active)

40 permit ip any any

აქსეს ლისტს სახელი ჰქვია Test ACL, პირველი ჩანაწერი გვეუბნება, რომ 192.168.1.0/24 ქსელიდან ნებადართულია ვებ პაკეტები ნებისმიერი მიმართულებით. მეორე ჩანაწერი გვეუბნება, რომ 192.168.1.1 ჰოსტს აკრძალული აქვს გაუგზავნოს 8.8.8.8-ს დნს პაკეტები. მესამე ჩანაწერი გვეუბნება რომ ტელნეტი 192.168.2.0/24 ქსელიდან 192.168.1.1 ჰოსტზე აკრძალულია წინასწარ განსაზღვრულ TimeACL დროის მონაკვეთში. სტანდარტულად ყველა აქსეს ლისტს ბოლოში ეწერება ყველაფრის აკრძალვა, ამიტომ თუ გვინდა რომ არ დაიბლოკოს ყველაფერი, უნდა გავუწეროთ permit ip any any ბრძანება.

4.3 უსაფრთხოება ქსელის შიგნით

გარე საფრთხეებისგან თავის დაცვასთან ერთად საჭიროა, ვიზრუნოთ ქსელის შიგნიდან დაცვაზეც, რადგან ჰაკერი შესაძლოა რომელიმე თანამშრომლის კომპიუტერზე მოხვდეს და შიდა ქსელიდან მოინდომოს ინფორმაციის მოპოვება. ამ მხრივ საჭიროა:

გამოვყოთ ცალკე DMZ (Demilitarized Zone) სადაც განთავსებული იქნება ორგანიზაციის სერვისები (ვებ გვერდი, ელ-ფოსტის სერვერი, ვებ სერვისები, მონაცემთა ბაზა და ასე შემდეგ.

აუცილებელია, ქსელურ მოწყობილობაზე მართვა დაშვებული იყოს მხოლოდ ერთი, დაცული და საიმედო კომპიუტერიდან, რათა ჰაკერმა ქსელის შიგნიდან ვერ შეძლოს აპარატურაზე შესვლა.

სვიჩზე უნდა გავთიშოთ ყველა ის პორტი რომელიც არ გამოიყენება მომხმარებლების მიერ.

შიდა ქსელი უნდა დავყოთ სხვადასხვა VLAN-ებად და სხვადასხვა სერვისებზე წვდომა (პრინტ სერვერებზე, პროგრამულ უზრუნველყოფაზე და ასე შემდეგ) უნდა გავწეროთ მხოლოდ შესაბამის ვილანებზე და მომხმარებლებზე,

სასურველია შიდა ქსელში გაშვებული იყოს 802.1X აუტენტიკაციის პროტოკოლი. ეს პროტოკოლი მომხმარებლის სახელს და პაროლს იღებს კომპიუტერიდან, ადარებს ორგანიზაციის აქტივ დირექტორიის სიაში ჩანაწერებს და თუ ამ მომხმარებელს აქვს უფლება რომ გაიაროს აუტენტიკაცია და ჩაერთოს შიდა ქსელში, მხოლოდ ამის შემდეგ ანიჭებს IP მისამართს. აღნიშნული მეთოდის საშუალებით უცხო პირი ვეღარ ჩაერთვება საკუთარი კომპიუტერით შიდა ქსელში და ვერ შეძლებს ვერანაირი ოპერაციის განხორციელებას.

სვიჩებზე Native Vlan არ უნდა იყოს Vlan1. Native Vlan-ის საშუალებით სვიჩები უგზავნიან ერთმანეთს ტრაფიკს, ხოლო რადგანაც Vlan1-ში ტეგირების გარეშე იგზავნება ფრეიმები, უსაფრთხოების მიზნით სასურველია რომ მათ ინფორმაცია სხვა ვილანში, ტეგირებული ფრეიმების საშუალებით გაცვალონ.

DHCP snooping - მეთოდი, რომელიც უზრუნველყოფს DHCP სერვისის გამართულად მუშაობას. მაგალითისთვის:ჰაკერმა ააწყო საკუთარი dhcp სერვერი შიდა ქსელში და მომხმარებლებს დაურიგა სულ სხვა იპ მისამართები. ამით ის გამოიწვევს ქსელის

პარალიზებს მანამ, სანამ ქსელის ადმინისტრატორი არ აღმოაჩენს ამას. ასევე შეიძლება უცხო პირმა საკუთარ კომპიუტერზე გაუწეროს გეითვეის მისამართი IP მისამართად და თანამშრომლების ტრაფიკი თავისკენ გადაამისამართოს. DHCP snooping უზრუნველყოფს, რომ ქსელში იმუშაონ მხოლოდ ავტორიზებულმა DHCP სერვერებმა და მხოლოდ ისეთ ჰოსტებს ჰქონდეთ ქსელი, რომლებსაც IP მისამართი სწორედ ავტორიზებულმა DHCP სერვერებმა მიანიჭეს.

Spanning Tree Protocol - ამ პროტოკოლს ქსელის ოპტიმიზაციასთან ერთად მისი უსაფრთხოების უზრუნველყოფის ფუნქციაც აქვს. კერძოდ - უცხო ადამიანმა რომ შეაერთოს ერთმანეთზე 2 სვიჩი 2-ზე მეტი კაბელით და გამოიწვიოს ე.წ. Swithing loop, დაეკიდებს ეს ორივე სვიჩი და ქსელის ეს სეგმენტი მთლიანად. Spanning Tree Protocol უზრუნველყოფს მსგავსი შემთხვევების აღმოჩენას და ზედმეტი პორტების მყისიერ გათიშვას. მისი მუშაობის პრინციპი ასეთია. ყველა სვიჩს გაეწერება პრიორიტეტი და ყველაზე მაღალი პრიორიტეტის მქონე მოწყობილობა გახდება Root Bridge. ხოლო დანარჩენი მოწყობილობები გამოითვლიან მანძილს მთავარ სვიჩამდე და მასთან მისასვლელ მხოლოდ ერთ გზას დაიტოვებენ, ხოლო დანარჩენ პორტებს გათიშავენ. აღნიშნული ალგორითმის შემდეგ უკვე აღარ არსებობს შანსი, რომ შიდა ქსელში Switching Loop მოხდეს.

Spanning Tree გაშვებულია სვიჩის ყველა პორტზე, თუმცა ისეთ პორტებზე, სადაც დანამდვილებით ვიცით რომ მომხმარებლები არიან დაერთებული, შეგვიძლია გავუწეროთ ბრძანება Switch(config-if)# spanning-tree portfast და ეს პორტი აღარ მიიღებს STP-ს ალგორითმში მონაწილეობას. ეს მეთოდი ეხმარება მომხმარებლებს, სვიჩის ჩართვისთანავე ჰქონდეთ შიდა ქსელი და არ იყოს დაყოვნება, რომელიც დაახლოებით 1 წუთამდეა. თუმცა portfast ბრძანების გაწერა საკმაოდ სარისკო გადაწყვეტილებაა, რადგანაც შეიძლება ბოროტმა ადამიანმა კომპიუტერის მაგივრად ქსელური მოწყობილობა დააერთოს ასეთ პორტზე, განახორციელოს Frame Broadcasting და პარალიზება მოახდინოს სვიჩის. ასეთი შემთხვევების თავიდან ასაცილებლად გამოიყენება BPDU Guard.

```
Switch(config)#
spanning-tree portfast bpduguard
```

პორტზე BPDU Guard ბრძანების გაწერის შემდეგ ის ისე მუშაობს, როგორც უზერის პორტი (Portfast ჩართულია), მაგრამ საკმარისია ამ პორტზე მივიდეს 1 BPDU პაკეტი მაინც,

რომ სვიჩი Switching Loop-ის თავიდან აცილების მიზნით გათიშავს ამ პორტს და მისი ჩართვა მხოლოდ ქსელის ადმინისტრატორის მიერ იქნება შესაძლებელი.

5. VPN კავშირები

VPN არის კერძო ქსელი, რომელიც იგება ინტერნეტში ტუნელის შექმნით. VPN ორი დაშორებული ოფისის დასაკავშირებლად იყენებს ვირტუალურ კავშირებს. თავდაპირველად ვპნ-ები იყო მხოლოდ ტუნელები ინტერნეტში, შიფრაციისა და დაცვის გარეშე. ამის ერთ-ერთი ნათელი მაგალითია GRE ტუნელი. GRE ტუნელი შექმნილია Cisco-ს მიერ და ის სვავს პაკეტებს ახალ, ჰედერშეცვლილ IP პაკეტებში. ასეთი მეთოდით იქმნება ვირტუალური point-to-point ლინკი ორ დაშორებულ მოწყობილობას შორის.

VPN არის სატელეკომუნიკაციო გარემო, სადაც მკაცრად კონტროლდება სათითაო კავშირი და განისაზღვრება მომხმარებლების უფლებები და შესაძლებლობები. ინფორმაციის კონფიდენციალურობა მიიღწევა მონაცემების დაშიფვრით და დღესდღეობით თანამედროვე VPN ტექნოლოგიები მომხმარებლებს მაქსიმალურ უსაფრთხოებას სთავაზობენ.

VPN კავშირებს აქვს ბევრი დადებითი მხარე:

- ხარჯების შემცირება - ვიპიენი საშუალებას აძლევს ორგანიზაციებს, გამოიყენონ იაფფასიანი ინტერნეტის კავშირი თავიანთი მოშორებული ოფისების სათაო ფილიალთან დასაკავშირებლად. ნაცვლად გამოყოფილი არხისა, ინფორმაცია მოძრაობს ინტერნეტის გავლით, რაც მნიშვნელოვნად ამცირებს კომპანიის დანახარჯებს.
- უსაფრთხოება - სხვადასხვა კომპლექსური პროტოკოლებისა და ალგორითმების მეშვეობით ვიპიენები უზრუნველყოფენ მაღალი დონის უსაფრთხოებას ინფორმაციის გადაცემისას.
- თავსებადობა - ვიპიენ ტექნოლოგია საშუალებას აძლევს ქსელის ადმინისტრატორს კომბინირებულად ამუშაოს დაშიფრული არხი სხვადასხვა მწარმოებლის მოწყობილობებზე.

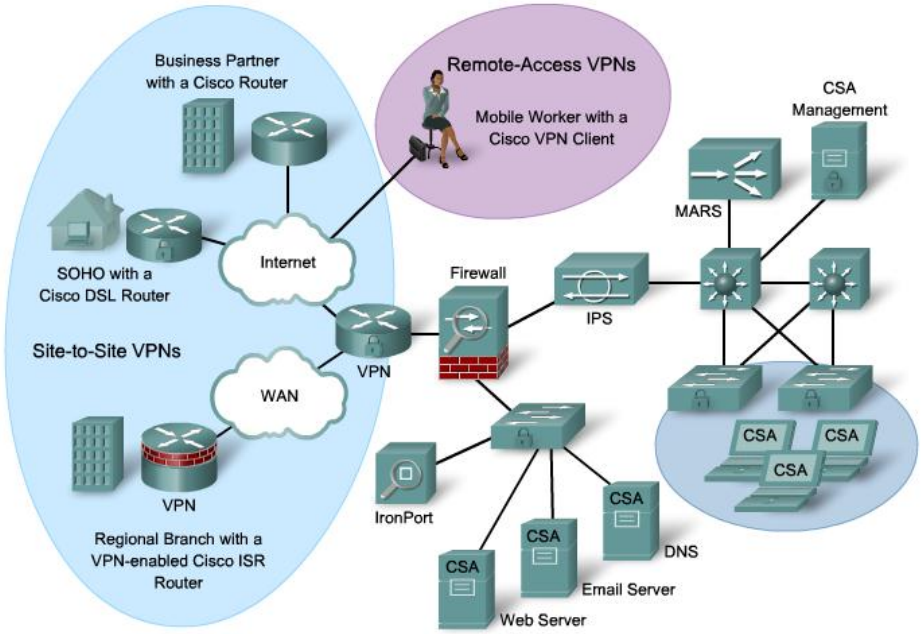
- გაზრდის სიმარტივე - იქიდან გამომდინარე, რომ ვიპიენ კავსირები დამოკიდებულია ინტერნეტზე, კომპანიის გაზრდის შემთხვევაში ადვილადაა შესაძლებელი კავშირების გაზრდა და გაფართოვება. ამისთვის არ იქნება დამატებითი ხარჯები საჭირო.

VPN კავშირების ორი ტიპი არსებობს:

- Site-to-Site VPN
- Remote Access VPN

Site-to-Site VPN მაშინ როცა, ტუნელის ორივე მხარეს ქსელური მოწყობილობებია. VPN ხდება სტატიკური და მომხმარებლები საერთოდ ვერ ხვდებიან, რომ ტუნელი არსებობს. Frame Relay, ATM, GRE და MPLS VPN ტექნოლოგიები ნათელი მაგალითია Site-to-Site VPN-ის.

Remote Access VPN იქმნება მაშინ, როდესაც ტუნელის პარამეტრები წინასწარ არ არის გაწერილი. სტატუსი შეიძლება დინამიურად შეიცვალოს. მაგალითისთვის ავიღოთ თანამშრომელი, რომელიც მივლინებით არის წასული საზღვარგარეთ. მას სჭირდება ინტერნეტის საშუალებით კავშირი თავისი კომპანიის ქსელსა და სერვისებზე. თანამშრომელს არ აქვს მუდმივად ჩართული კომპიუტერი და არ არის მუდმივი კავშირი მასსა და კომპანიის ქსელს შორის. კომპიუტერი უკავშირდება ქსელს Cisco VPN Client-ის და ამ პოგრამაში წინასწარ გაწერილი კონფოგურაციის საშუალებით. ტუნელის ერთი მხარის პარამეტრები (თანამშრომლის მხარე) მუდმივად იცვლება, იმის მიხედვით თუ სად არის ეს ადამიანი და რა IP მისამართი აქვს.



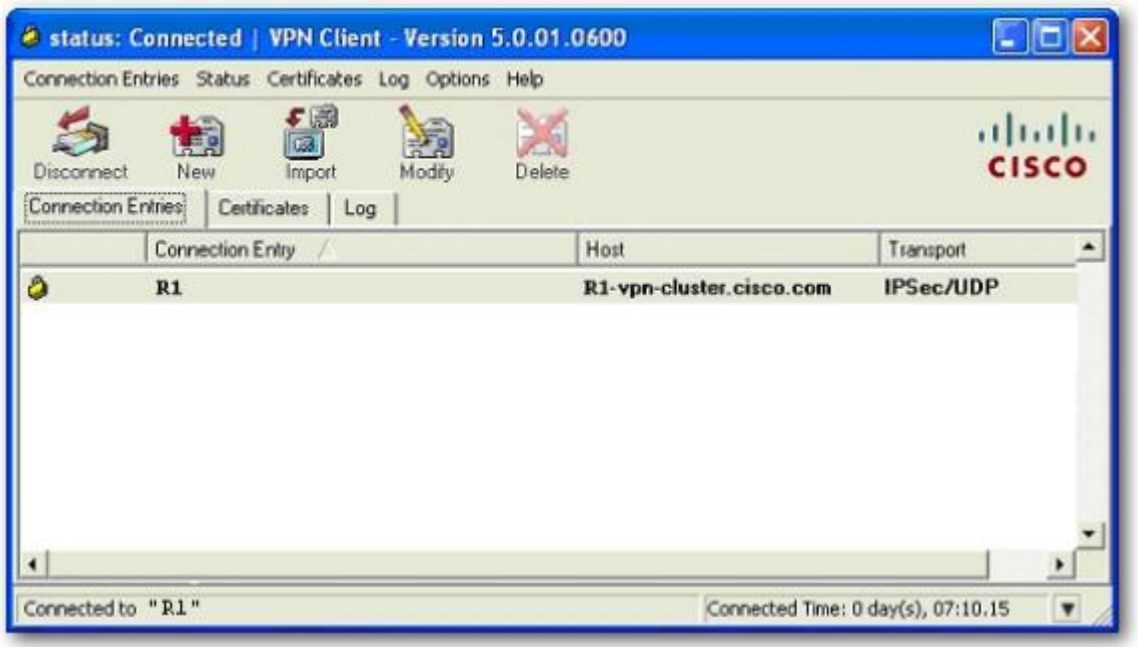
5.1 Site-to-Site VPN

Site-to-Site VPN არის WAN ქსელის ერთ-ერთი გავრცელებული მოდელი. ამგვარი ვპნ კავშირი აკავშირებს ორ ქსელს ერთმანეთთან. მაგალითად, მას შეუძლია დაუკავშიროს ფილიალი სათაო ოფისს. ადრე მსგავსი კავშირებისთვის სპეციალურად ამ საქმისთვის გამოყოფილი ხაზები გამოიყენებოდა (Leased Lines ან Frame Relay), მაგრამ, რადგანაც დღესდღეობით თითქმის ყველა კორპორატიულ ქსელს აქვს ინტერნეტთან კავშირი, ზემოთაღნიშნული კავშირები თავისუფლად შეიძლება შეიცვალოს VPN-ებით.

Site-to-Site VPN-ში უზერები აგზავნიან სტანდარტულ TCP/IP ტრაფიკს, ხოლო შემდეგ VPN მოწყობილობა (VPN Concentrator, Cisco ASA ან Cisco Router) ახდენს ამ ტრაფიკის დაშიფვრას, ინკაფსულაციას და გადაცემას დაცულ არხში ტუნელის მეორე მოწყობილობამდე. მეორე მოწყობილობა გაშიფრავს ამ პაკეტებს, მოაცლის დამატებულ ჰედერებს და გადაუგზავნის პაკეტს შიდა ქსელის უზერებს.

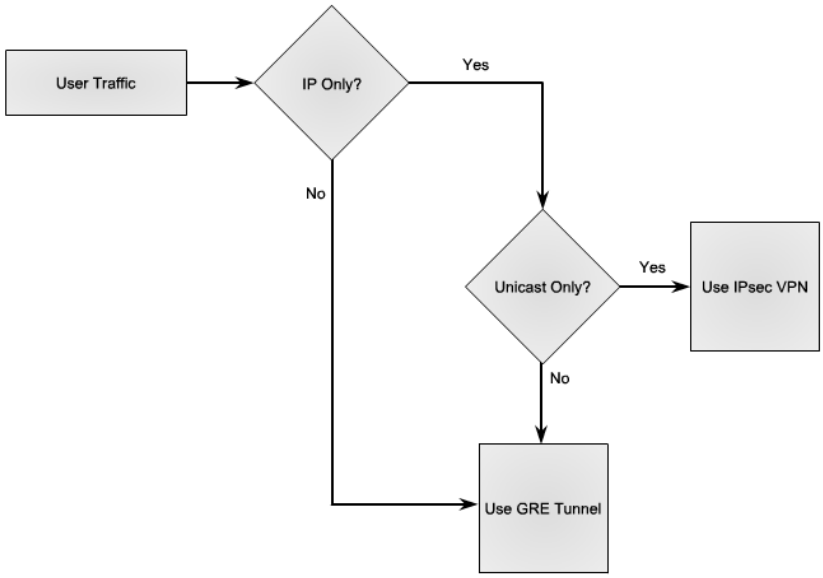
5.2 Remote Access VPN

Remote Access VPN-ები არის circuit-switching ქსელების ევოლუცია. ასეთი ტიპის კავშირები იგება კლიენტ/სერვერული არქიტექტურით, სადაც VPN კლიენტი ამყარებს დაცულ კავშირს კორპორატიულ ქსელთან. ადრე ასეთი ტიპის მოთხოვნებისთვის იყო ISDN ან POTS გადაწყვეტილებები. Remote Access VPN-ებისთვის საჭიროა მხოლოდ ღია ინტერნეტი (გზა VPN სერვერამდე). ჰოსტებს დაინსტალირებული აქვთ პროგრამული უზრუნველყოფა (Cisco VPN client) მასში გაწერილი პარამეტრებით (სერვერის IP მისამართი, ჯგუფის სახელი და პაროლი, მომხმარებლის სახელი და პაროლი). როდესაც კლიენტი აგზავნის ინფორმაციას დაცულ ქსელში, პროგრამა ახდენს ამ ტრაფიკის დაშიფვრას, ინკაფსულაციას და გადაცემას დაცულ არხში ტუნელის მეორე მოწყობილობამდე. მეორე მოწყობილობა გაშიფრავს ამ პაკეტებს იმავე პრინციპით, როგორც Site-to-Site VPN-ის დროს.

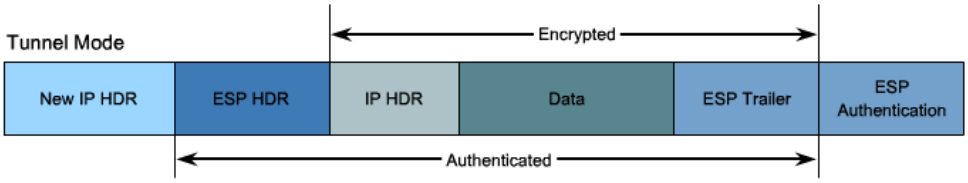


5.3 VPN ტუნელის გამართვა

ვიპიენ ტუნელის აგება ხდება ძირითადად ორი პროტოკოლის საშუალებით: Generic routing encapsulation (GRE) და Internet Protocol Security (IPsec). GRE ტუნელის აგება საჭიროა, მაშინ როდესაც ტუნელში IP--ის გარდა სხვა პროტოკოლის ტრაფიკმაც უნდა იმოძრაოს. სხვა შემთხვევაში გამართლებულია IPSec პროტოკოლის გამოყენება, რადგანაც GRE-ს არ გააჩნია ინფორმაციის დაცვის მექანიზმები(შიფრაცია, კონფიდენციალობა, ჰეშირება და ასე შემდეგ).



IPSec ტუნელი საკმაოდ კომპლექსურია, ის არის ნაკრები აუტენტიკაციის პროტოკოლების, შიფრაციის, უსაფრთხოების ალგორითმებისა და სხვა გაცვლის მექანიზმებისა. ეს პროტოკოლი მუშაობს ქსელურ დონეზე, იცავს იპ პაკეტს და ინკაფსულაციას უკეთებს ახალ, დაცულ პაკეტში რომლის გახსნა და დეშიფრაცია მხოლოდ ტუნელის მეორე მხარეს მყოფ მოწყობილობას შეუძლია.



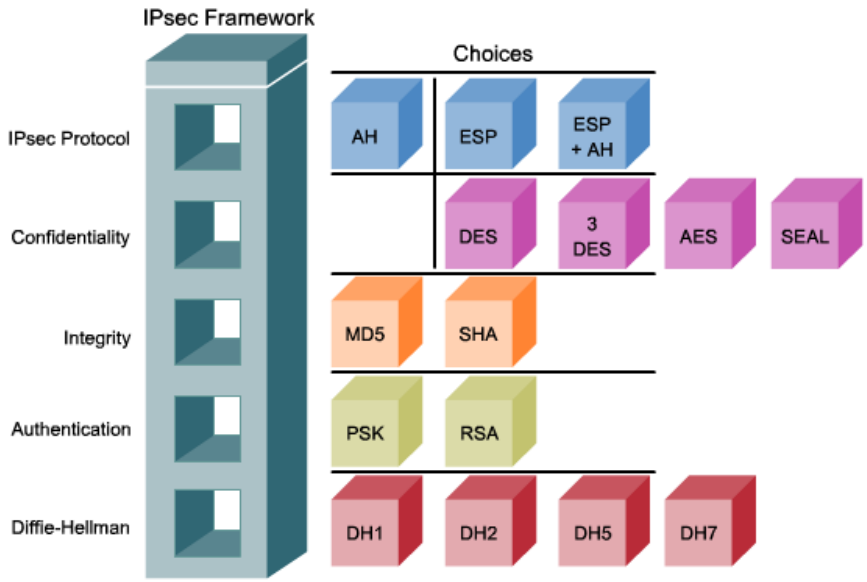
IPSec-ის აგება 5 ნაწილისგან შედგება

- პირველ ნაწილში ვირჩევთ IPSec-ის ტიპს, ESP ან AH ჰედერი.
- მეორე ნაწილში ვირჩევთ შიფრაციის ალგორითმს (DES, 3DES, AES, ან SEAL).
- მესამე ნაწილი წარმოადგენს ინფორმაციის ერთიანობას, მთლიანობას. (MD5 ად SHA)

- ვირჩევთ მეთოდს, თუ როგორი უნდა იყოს გასაღები, როგორ უნდა გადაიცეს. აქ არჩევანი გვაქვს pre-shared key-სა და RSA-ს შორის.
- ბოლო მეთოდი არის დიფერ-ჰელმანის ალგორითმის ჯგუფი. შეგვიძლია ავირჩიოთ 1-დან 7-მდე ჯგუფი.

IPSec სტრუქტურა შედგება სხვადასხვა ალგორითმებისა და წესებისგან და მხოლოდ ქსელის ადმინისტრატორი ირჩევს მისთვის უკეთეს პროტოკოლებს. IPSec-ს აქვს შესაძლებლობა, განახორციელოს შემდეგი უსაფრთხოების მეთოდები.

- კონფიდენციალურობა - ტრაფიკის დაშიფვრა და დარწმუნება იმაში, რო სხვა ვერ გახსნის.
- ინფორმაციის მთლოანობა - შემოწმება იმისა, იყო თუ არა ეს ინფორმაცია წაკითხული უცხო პირის მიერ.
- აუტენტიკაცია - ავტორიზირებული მომხმარებლების აუტენტიკაცია სხვადასხვა მეთოდებით, უზერნეიმი და პაროლით, სერთიფიკატით, ID ბარათებით და ასე შემდეგ.



6. კომპიუტერის უსაფრთხოება

გარდა ქსელის უსაფრთხოებისა, IT გუნდმა უნდა იზრუნოს თითოეული კომპიუტერის უსაფრთხოებასა და მასში ჩაწერილი ინფორმაციის კონფიდენციალურობაზე. კომპიუტერის უსაფრთხოებისათვის აუცილებელია მასზე ეყენოს მუდმივად განახლებადი ანტივირუსული პროგრამა, ხშირად ხდებოდეს კომპიუტერის სკანირება და ვირუსების აღმოჩენა, პროგრამების და ოპერაციული სისტემის განახლება. ასევე სასურველია ჩართული იყოს ოპერაციული სისტემის პროგრამული ფაირვოლი, რომელიც ფილტრავს კომპიუტერში გაშვებულ პროგრამებს, მათ კავშირს ქსელთან და ბლოკავს არასაჭირო Connection-ებს.

ანტივირუსული პროგრამებიდან გამოარჩევენ:

Kaspersky Antivirus

Microsoft Security Esentials

Norton Internet Security

Avast

Nod32

Avida

AVG და სხვებს...

არსებობს თითოეული მათგანის უფასო და ფასიანი ვერსიები, რომლებიც უზრუნველყოფენ კომპიუტერის სხვადასხვა ხარისხის დაცვას ვირუსებისა და არასაჭირო პროგრამებისგან.

კომპიუტერის მომხმარებელს აუცილებლად უნდა ედოს რთული პაროლი Password Security პოლისის გათვალისწინებით. ასევე რთული და უზერის პაროლისგან განსხვავებული უნდა ედოს ადმინისტრატორის ექაუნთს. მომხმარებელს არ უნდა ჰქონდეს ადმინისტრატორის უფლებები და სხვადასხვა პროგრამების დაყენების შესაძლებლობა.

პროგრამულ უზრუნველყოფასთან ერთად აუცილებელია უზერმა იცოდეს ყველაზე ხშირად გავრცელებული malware საფრთხეების შესახებ. არ გახსნას უცხო და საეჭვო ფაილები, არ დააწვეს ინტერნეტში უცბად ამოვარდნილ რეკლამებს და არ გადავიდეს უცხო და არასანდო საიტებზე. არ გახსნას ასევე მეილზე მოსული სპამი წერილები. არ დააყენოს უცხო და გატეხილი პროგრამები და ასე შემდეგ...

7. დასკვნა

როგორც ვნახეთ ინფორმაციის დაცვა საკმაოდ კომპლექსური თემაა და მთლიანად ვერცერთ ნაშრომში ვერ ჩაეტევა, თუმცა შევეცადე შევხებოდი რაც შეიძლება მეტ საკითხს და უფრო დეტალურად განმეხილა მათ შორის აუცილებელი თემები.

ქსელში ინფორმაციის დაცვისთვის საჭიროა, ყურადღება გავამახვილოთ ყველა დეტალზე, დავიცვათ ქსელი როგორც გარე საფრთხეებისგან, ასევე შიდა და გაუთვალისწინებელი შემთხვევებისგან. სამუშაოების დაწყებამდე უნდა განისაზღვროს:

- კომპანიის მოთხოვნები, თუ რამდენად დაცული უნდა იყოს ინფორმაცია.
- ფინანსური შესაძლებლობები, თუ რამდენად უღირს ესა თუ ის სერვისი.
- გუნდის შესაძლებლობები, შეუძლია თუ არა IT გუნდს თავი გაართვას უსაფრთხოების ამოცანებს.
- სხვა ხელის შემშლელი და ხელის შემწყობი ფაქტორები (მაგ. ქსელის ტოპოლოგია, ქსელის ხელმისაწვდომობა, აპარატურის ფიზიკური დაცულობა და ასე შემდეგ..)

ამის შემდეგ უნდა დაიწეროს კომპანიაზე მორგებული უსაფრთხოების პოლიტიკა და ზედმიწევნით შესრულდეს ეს წესები, ხოლო მომავალში ქსელი უნდა იყოს მუდმივად განახლებადი და სისუსტეების გამოსწორებაზე ორიენტირებული.

ყოველივე ზემოთ ჩამოთვლილი რეკომენდაცია, მეთოდი თუ აპარატურა ზრუნავს დღევანდელი თანამედროვე ტექნოლოგიების და ინფორმაციის დაცვასა და კონფიდენციალურობაზე. ვფიქრობ ნაშრომში მოყვანილი რჩევები და რეკომენდაციები გამოადგებათ ახალბედა ქსელის ადმინისტრატორებს, გახადონ საკუთარი ქსელი უფრო დაცული, სანდო და ეფექტური.