|  |
| --- |
| **A ტიპის მარშუტიზატორი - ოთხი ცალი** |
| **მარშრუტიზატორს უნდა გააჩნდეს შემდეგი ტექნიკური მახასიათებლები:** |
| 1. **მარშრუტიზატორი უნდა იყოს მულტისერვისული, მომავალში პროგრამული და აპარატურული კომპონენტების დამატებით, საკუთრივ მარშრუტიზატორს უნდა გააჩნდეს:** |
| 1.1 ხმოვანი მარშრუტიზატორის მხარდაჭერა:  1.1.1 უნდა შეეძლოს ხმოვანი სიგნალიზაციის (SIP და H323) ოქმებით განხორციელებული ზარების მარშრუტიზაცია;  1.1.2 უნდა შეეძლოს ხმოვანი სიგნალიზაციის (SIP და H323) ოქმების უსაფრთხოების უზრუნველყოფა;  1.1.3 საჭიროების შემთხვევაში უნდა გააჩნდეს სპეციალური აპარატურული მოდულების მხარდაჭერა, რათა აღნიშნული მოდულების დონეზე განხორციელდეს სატელეფონო ზარების დამუშავება. მათ შორის ხმოვანი კოდეკების ტრანსლირება, DTMF -ის კონვერტირება, ციფრული PSTN ქსელიდან TDM ტექნოლოგიით მიღებული ზარის კონვერტაცია IP ქსელში; |
| 1.2 IP სატელეფონო სადგურის როლის შესრულების შესაძლებლობა:  1.2.1 IP ტელეფონების მიერთება და მათი მართვა;  1.2.2 სატელეფონო ნომრების მინიჭება, IP ტელეფონებზე;  1.2.3 IP სათელეფონო სადგურის მართვა შესაძლებელი უნდა იყოს გრაფიკული ინტერფეისიდან; |
| 1.3 ახალი თაობის NGFW/NGIPS ბრანდმაუერის მხარდაჭერა:  1.3.1 დაცვა რეალურ დროში;  1.3.2 პასიური და აქტიური რეჟიმების მხარდაჭერა;  1.3.3 ქსელის ტოპოლოგიის აღმოჩენა;  1.3.4 დაცვის რეჟიმი: 2-დან 7-ე შრემდე (Layer);  1.3.5 SSL ტრაფიკის დეშიფრაციის მხარდაჭერა და მისი შიგთავსისი ინსპექტირების საშუალება;  1.3.6 უნდა უზრუნველყოფდეს ე.წ IDS/IPS Tuning-ს, ადამიანის მინიმალური ჩარევით (მაგ.: წესების შერჩევის, პოლიტიკების კონფიგურაცია, პოლიტიკების განახლება და ა.შ.);  1.3.7 უნდა შეეძლოს ფაილების აღმოჩენა და კონტროლი. აღნიშნული ოპერაციების განხორციელება შესაძლებელი უნდა იყოს ფაილების ტიპების, გამოყენებული პროტოკოლისა და ე.წ „ატვირთვა“ „ჩამოტვირთვის“ მიხედვით;  1.3.8 უნდა შეეძლოს პასიურად შეაგროვოს ინფორმაცია ქსელის ჰოსტებისა და მათი ქცევის შესახებ. მათ შორის: ოპერაციული სისტემები, სერვისები, ღია პორტები, აპლიკაციები, სისუსტეები( vulnerabilities). აღნიშნული ინფორმაციის გამოყენება შესაძლებელი უნდა იყოს, უსაფრთხოების ინციდენტების კორელაციისთვის, ე.წ „false positives“ ინციდენტების შესამცირებლად და პოლიტიკების შესაბამისობაში მოყვანისთვის;  1.3.9 გადაწყვეტილებამ უნდა უზრუნველყოს რეალურ დროში ქსელური აქტივების გზამკვლევის აგება. მას უნდა შეეძლოს ისეთი დეტალური ინფორმაციის დადგენა აქტივების შესახებ, როგორიცაა, აქტივის მომხმარებლები, აქტივის მიერ უზრუნველყოფილი სერვისები და გამოყენებული აპლიკაციები.  1.3.10 გადაწყვეტილებას უნდა შეეძლოს, ქსელში აღმოჩენილ აპლიკაციებს მიუსადაგოს რისკის დონე და ბიზნესის რელევანტობა;  1.3.11 გადაწყვეტილებას უნდა შეეძლოს ქსელური ნაკადებში ამოიცნოს სხვადასხვა აპლიკაციები და თვალყური ადევნოს მათ. გადაწყვეტილებას უნდა შეეძლოს ამოიცნოს, მომხმარებლის აპლიკაციები, სერვერის აპლიკაციები, ვებ აპლიკაციები და აპლიკაციების ოქმები;  1.3.12 გადაწყვეტილებას უნდა შეეძლოს პასიურად განახორციელოს ინფორმაციის შეგროვება ქსელური ნაკადების შესახებ, მათ შორის სესიის დაწყებისა და დამთავრების დრო, კომუნიკაციის პორტები, სერვისები, გადაცემული ინფორმაციის მოცულობა;  1.3.13 გადაწყვეტილებას უნდა შეეძლოს პასიურად განახორციელოს მომხმარებლების მაიდენტიფიცირებელი ინფორმაციის შეგროვება. მას უნდა შეეძლოს IP მისამართების მისადეგება მომხმარებლების სახელებზე, აღნიშნული ინფორმაცია ხელმისაწვდომი უნდა იყოს შეტყობინების მენეჯმენტისთვის;  1.3.14 გადაწყვეტილებას უნდა შეეძლოს დაადგინოს თუ როგორ გამოიყენებენ ქსელურ რესურსებს მომხმარებლები, მოწყობილობები და აპლიკაციები;  1.3.15 გადაწყვეტილებას უნდა შეეძლოს დროში გავრცობილად ახორციელოს ქსელის პროფილირება და შესაბამისი რეკომენტაციების გაწევა ახალი და განახლებული უსაფრთხოების წესებისთვის. გადაწყვეტილებას უნდა შეეძლოს ახალი სიგნატურების ავტომატურად მიღება და უცნობი აპლიკაციების ბლოკირება;  1.3.16 ქსელური შეტევების აღმოჩენის წესები უნდა ეფუძნებოდეს გაფართოებად ღია სტანდარტს, რომლის მეშვეობითაც მომხმარებელს უნდა შეეძლოს როგორც მწარმოებლის მიერ შემუშავებული წესების მოდიფიცირება ასევე ახალი, მისთვის სასურველი წესების შექმნა;  1.3.17 გადაწყვეტილებას უნდა გააჩნდეს SNORT ენაზე დაფუქნებული სრულფასოვანი წესების მხარდაჭერა. გადაწყვეტილებაში შესაძლებელი უნდა იყოს არანაკლებ 2000 SNORT წესის გამოყენება;  1.3.18 სისტემას უნდა ჰქონდეს შესაძლებლობა მოახდინოს ტრაფიკის ინსპექტირება ქცევის მიხედვით;  1.3.19 შეტევების აღმომჩენ ძრავს უნდა შეეძლოს როგორც ცნობილი საფრთხეების, ასევე ახალი, ჯერ უცნობი საფრთხეების აღმოჩენა;  1.3.20 შეტევების აღმომჩენ ძრავს უნდა გააჩნდეს შეტევების აღმოჩენის რამოდენიმე მექანიზმი, მათ შორის ე.წ „exploit” ებზე დაფუძნებული სიგნატურები, სისტემების ე.წ „სისუსტეებზე“ დაფუძნებული წესები, ოქმების ანომალიები და ქცევის ანომალიების მიხედვით;  1.3.21 გადაწყვეტილებას უნდა შეეძლოს ქსელის სხვადასხვა სეგმენტების ტრაფიკის ინსპექტირება სხვადასხვა პოლიტიკებით. ერთ ინტერფეისზე შესაძლებელი უნდა იყოს სხვადასხვა უსაფრთხოების პოლიტიკების გამართვა;  1.3.22 გადაწყვეტილებას უნდა შეეძლოს IPv6 ოქმით მიმდინარე შეტევების აღმოჩენა;  1.3.23 გადაწყვეტილებას უნდა შეეძლოს პასიურად, უწყვეტ რეჟიმში ახორციელოს ქსელური ჰოსტების შესახებ ინფორმაციის შეგროვება. მათ შორის კლიენტის ოპერაციული სისტემების, ე.წ „ვებ ბრაუზერი“-ს, ვირტუალური გარემოს და მობილური მოწყობილობების აღმოჩენა;  1.3.24 გადაწყვეტილებას უნდა შეეძლოს გარე შეერთებების რეპუტაციის დადგენა. გადაწყვეტილება რეგულარულად და ავტომატურად უნდა ანახლებდეს რეპუტაციის ინფორმაციას. სისტემის ადმინისტრატორს უნდა შეეძლოს საკუთრივ განსაზღვროს ე.წ „blacklists/whitelists“ სიები. გადაწყვეტილებას უნდა შეეძლოს საჯარო და კერძო რეპუტაცის ე.წ „Feed” სერვისებთან მიერთება;  1.3.25 გადაწყვეტილებას უნდა შეეძლოს სხვადასხვა მომხმარებლებისთვის ან მათი ჯგუფებისთვის განისაზღვროს სხვადასხვა უსაფრთხოების პოლიტიკები. მომხმარებლების მაიდენტიფიცირებელი ინფორმაციის დადგენა შესაძლებელი უნდა იყოს Active Directory, LDAP სერვერებიდან;  1.3.26 გადაწყვეტილებას უნდა გააჩნდეს უნივერსალური და მოქნილი უსაფრთხოების პოლიტიკების აგების შესაძლებლობა. პოლიტიკებში შესაძლებელი უნდა იყოს სხვადასხვა სახის ინფორმაციის მითითება მათ შორის: ქსელების, ზონების, აპლიკაციების კონტროლის, მომხმარებლების კონტროლის, ფაილების კონტროლის, ჰოსტების წვდომის და IPS სისტემის პოლიტიკების; |
| 1. **მოთხოვნები ქსელური ინტერფეისების მიმართ:** |
| 2.1 ინტერფეისების რაოდენობა არანაკლებ 4(ოთხი)10/100/1000მბ/წმ წარმადობის:  2.1.1 მათ შორის - 4 (ოთხი)RJ-45 ტიპის, 4 (ოთხი)SFP ტიპის; **[ორმაგი დანიშნულების];**  2.1.2 მენეჯმენტ პორტი RJ-45 to DB9 (Console) ან USB-C Console Port - არანაკლებ 1 ცალი  2.1.3 მართვის პორტი - RJ-45 კონექტორით - არანაკლებ 1 ცალი  2.2 მარშრუტიზატორს უნდა გააჩნდეს გაფართოების სლოტების მხარდაჭერა, არანაკლებ 3 (სამი) ქსელური და სერვისების სლოტის მხარდაჭერა. აღნიშნული სლოტების საშუალებით მომავალში შესაძლებელი უნდა იყოს ინტერეფეისების რაოდენობის გაზრდა, მათ შორის:  2.2.1 არანაკლებ 8 (რვა) x 100/1000 მბ/წმ წარმადობის მქონე პორტის, POE+ ტექნოლოგიით აღჭურვილი კომუტაციის მოდულის მხარდაჭერა. არანაკლებ 3 ასეთი მოდულის მხარდაჭერა;  2.2.2 არანაკლებ 2 (ორი) x 100/1000 მბ/წმ წარმადობის, Rj-45 და SFP (ორმაგი დანიშნულების) პორტის მქონე მარშრუტიზაციის მოდულის მხარდაჭერა. არანაკლებ 3 ასეთი მოდულის მხარდაჭერა;  2.2.3 არანაკლებ 2 (ორი) ცალი მე-4 თაობის LTE მოდულის მხარდჭერა;  2.2.4 არანაკლებ 8 (რვა) E1/T1 ცალი პორტის მქონე მოდულის მხარდაჭერა. არანაკლებ 3 ასეთი მოდულის მხარდაჭერა;  2.2.5 არანაკლედ 4 (ოთხი) FXS ტიპის პორტით. არანაკლებ 3 ასეთი მოდულის მხარდაჭერა;  2.2.6 არანაკლედ 4 (ოთხი) FXO ტიპის პორტით. არანაკლებ 3 ასეთი მოდულის მხარდაჭერა; |
| 1. **მარშრუტიზატორის წარმადობა, არანაკლებ 500მბ. მომავალში მხოლოდ პროგრამული ლიცენზიის დამატებით შესაძლებელი უნდა იყოს მარშრუტიზატორის წარმადობის გაზრდა 4000მბ-მდე. IPSec შიფრაციის წარმადობაზე არ უნდა ვრცელდებოდეს პროგრამული შეზღუდვა.** |
| 1. **DRAM ტიპის მეხსიერება არანაკლებ 4გბ. მომავალში გაფართოებადი 16გბ მდე.** |
| 1. **მარშრუტიზატორს უნდა გააჩნდეს ქსელური ბრანდმაუერის ფუნქციონალის მხარდაჭერა:** |
| 5.1. მარშრუტიზატორს უნდა გააჩნდეს ე.წ „stateteful” ბრანდმაუერის ფუნქციონალი;  5.2. ბრანდმაუერზე შესაძლებელი უნდა იყოს, რამოდენიმე უსაფრთხოების ზონების განსაზღვრა და მათი გათვალისწინებით ტრაფიკის ინსპექტირება;  5.3. ბრანდმაუერს უნდა გააჩნდეს აპლიკაციის დონეზე(Layer 7) ოქმების ინსპექტირებისა და კონტროლის შესაძლებლობა, ე.წ “Application Layer Gateway (ALG)” და „Application Inspection and Control(AIC)” ფუნქციონალი; |
| 1. **მომავალში შესაძლებელი უნდა იყოს მარშრუტიზატორის ფუნქციონალის გაზრდა, მხოლოდ პროგრამული ლიცენზიის დამატების საშუალებით, რის შემთხვევაშიც მას გაუაქტიურდება ე.წ “Application Visibility and Control(AVC)” ფუნქციონალი:** |
| 6.1 AVC ფუქნციონალს უნდა შეეძლოს ქსელური აპლიკაციების ამოცნობა „Deep Packet Inspection (DPI)” ტექნოლოგიით. განურჩევლად იმისა თუ რომელ პორტზე მუშაობს აპლიკაცია. მარშრუტიზატორს უნდა გააჩნდეს არანაკლებ 800 აპლიკაციის ამოცნობის შესაძლებლობა. აპლიკაციების სიგნატურების განახლება არ უნდა აფერხებდეს მარშრუტიზატორის მუშაობას;  6.2 აღნიშნული ფუნქციონალის ფარგლებში შესაძლებელი უნდა იყოს აპლიკაციების გამოყენებისა და ქსელური წარმადობის შეფასების სტატისტიკის შეგროვება;  6.3 აღნიშნული ფუნქციონალის ფარგლებში შესაძლებელი უნდა იყოს თითოეული აპლიკაციისთვის QoS ქსელური რესურსების გამოყენების პოლიტიკების დაწესება. ისეთი პოლიტიკების მხარდაჭერა, როგორებიცაა shape, police, priority;  6.4 შესაძლებელი უნდა იყოს აპლიკაციების გონიერი და ოპტიმალური მარშრუტიზაცია. მარშრუტიზაცია უნდა ხორციელდებოდეს მარშრუტის მიმდინარე წარმადობაზე დაყრდნობით; |
| 1. **მომავალში შესაძლებელი უნდა იყოს მარშრუტიზატორის ფუნქციონალის გაზრდა, მხოლოდ პროგრამული ლიცენზიის დამატების საშუალებით, რის შემთხვევაშიც საკუთრივ უნდა გააჩნდეს სპეციალური მექანიზმები, რათა განახორციელოს ქსელში კავშირის ხარისხის შეფასება, სხვადასხვა სახის აპლიკაციებისათვის. შესაძლებელი უნდა იყოს აღნიშნული მექანიზმის გაშვება პერიოდული განრიგის მიხედვით ან მუდვიმად:** |
| 7.1 აღნიშნულ მექანიზმებს უნდა გააჩნდეს, შემდეგი სახის ქსელის წარმადობის პარამეტრების დადგენის შესაძლებლობა:  7.1.1 Delay (round-trip და one-way)  7.1.2 Jitter (directional)  7.1.3 Packet loss (directional)  7.1.4 Packet sequencing (packet ordering)  7.1.5 Path (per hop)  7.1.6 Connectivity (directional)  7.1.7 Server or website download time  7.2 აღნიშნული მექანიზმით შესაძლებელი უნდა იყოს შემდეგი სახის ოქმებისა და აპლიკაციებისთვის, კავშირის ხარისხის შეფასება და წარმადობის პარამეტრების დადგენა:  7.2.1 TCP  7.2.1.1 response time  7.2.2 UDP  7.2.2.1 round-trip delay  7.2.2.2 one-way delay  7.2.2.3 one-way jitter  7.2.2.4 one-way packet loss  7.2.2.5 connectivity  7.2.3 ICMP  7.2.3.1 response time  7.2.3.2 end-to-end და hop-by-hop response time  7.2.4 HTTP  7.2.4.1 response time between to retrieve a web page from HTTP server  7.2.5 FTP  7.2.5.1 response time to retrieve a file from FTP server  7.2.6 DHCP  7.2.6.1 measure the response time to obtain an IP address from DHCP server  7.2.7 DNS  7.2.7.1 difference between the time taken to send a DNS request and receive a reply  7.3 აღნიშმულ მექანიზმს უნდა შეეძლოს MPLS ქსელში, Label Switched Path (LSP) ის მუშაობის შეაფასება:  7.3.1 მონაწილე „Provider Edge (PE)“ მარშრუტიზატორებს შორის, შესაძლებელი უნდა იყოს ყველა „Label Switched Path (LSP)“ ის „control-plane” და “data-plane” ის მუშაობის შემოწმება;  7.4 აღნიშნულ მექანიზმს უნდა შეეძლოს, ზუსტად შეაფასოს ქსელის მუშაობის შემდეგი პარამეტრები:  7.4.1 Per-direction jitter (source to destination and destination to source)  7.4.2 Per-direction packet loss  7.4.3 Per-direction delay (one-way dely)  7.4.4 Round-trip delay (average round-trip time)  7.5 აღნიშნული მექანიზმის მონიტორინგი შესაძლებელი უნდა იყოს SNMP ოქმის საშუალებით |
| 1. **მომავალში შესაძლებელი უნდა იყოს მარშრუტიზატორის ფუნქციონალის გაზრდა, მხოლოდ პროგრამული ლიცენზიის დამატების საშუალებით, რის შემთხვევაშიც მას უნდა გააჩნდეს ტრაფიკის ოპტიმალური მარშრუტიზაციის ტექნოლოგიის მხარდაჭერა. იგი რეალურ დროში უნდა აფასებდეს მარშრუტის ხარისხის ისეთ პარამეტრებს, როგორებიცაა: delay, loss, jitter, throughput, available bandwidth, reachability და მათზე აგებული პოლიტიკების მიხედვით უზრუნველყოფდეს აპლიკაციების ტრაფიკის ოპტიმალურ მარშრუტიზაციას:** |
| 8.1 მარშრუტიზატორს უნდა შეეძლოს, გონივრული, თითოეული აპლიკაციისთვის ოპტიმალური მარშრუტიზაციის განხორციელება, ისეთი პარამეტრების მიხედვით, როგორებიცაა: delay, loss, jitter. მარშრუტიზატორს უნდა შეეძლოს მე - 6 პუქტში აღწერილი, ფუნქციონალის გამოყენება რათა განახორციელოს ქსელური აპლიკაციების ამოცნობა;  8.2 მარშრუტიზატორს უნდა შეეძლოს პასიურად განახორციელოს მარშრუტის შეფასება. ამისათვის ის პასიურად უნდა ახდენდეს ტრანზიტული ტრაფიკის ანალიზს და ისეთი სახის პარამეტრების დადგენას, როგორებიცაა delay, packet loss, reachability, throughput. აღნიშნული სახის პარამეტრების გამოყენებით მარშრუტიზატორს უნდა შეეძლოს ოპტიმალურად განახორციელოს მარშრუტიზაცია;  8.3 მარშრუტიზატორს უნდა შეეძლოს აქტიურად განახორციელოს მარშრუტის შეფასება, მე 7 პუნქტში აღწერილი ტექნოლოგიის გამოყენებით, რათა მის შედეგებზე დაყრდნობით განახორციელოს ტრაფიკის ოპტიმალური მარშრუტიზაცია;  8.4 მარშრუტიზატორს უნდა შეეძლოს კომბინირებულად, როგორც აქტიური ასევე პასიური მარშრუტის შეფასების ტექნოლოგიების გამოყენება ოპტიმალური მარშრუტის ასარჩევად. |
| 1. **მარშრუტიზატორს უნდა გააჩნდეს შემდეგი QoS ტექნოლოგიების მხარდაჭერა: HQoS, Classification, marking, Weighted Random Early Detection (WRED), policing, shaping, priority, and Class-Based Weighted Fair Queuing (CBWFQ) scheduling;** |
| 1. **მომავალში შესაძლებელი უნდა იყოს მარშრუტიზატორის ფუნქციონალის გაზრდა, მხოლოდ პროგრამული ლიცენზიის დამატების საშუალებით, რის შემთხვევაშიც მას უნდა გააჩნდეს Locator/ID Separation Protocol (LISP) ოქმის მხარდაჭერა, რათა უზრუნველყოს IP მისამართის მობილობა;** |
| 1. **საკუთრივ მარშრუტიზატორს უნდა გააჩნდეს სპეციალური დიაგნოსტიკური საშუალება, რომლის მეშვეობითაც ადმინისტრატორს შეეძლება: ტრანზიტული, მოწყობილობაზე მიმართული და მოწყობილობიდან გამოსული ტრაფიკის შეგროვება. შეგროვებული ტრაფიკის ანალიზი შესაძლებელი უნდა იყოს ლოკალურად ან მისი ექსპორტირებით გარე სამუშაო სადგურზე. შეგროვებული ტრაფიკის ანალიზი შესაძლებელი უნდა იყოს Wireshark პროგრამული უზრუნველყოფით;** |
| 1. **საკუთრივ მარშრუტიზატორში მოთხოვნისამებრ ადმინისტრატორს უნდა შეეძლოს ე.წ „სკრიპტი“ -ის პოლიტიკების დაწერა, აღნიშნული ფუნქციონალით შესაძლებელი უნდა იყოს გარკვეული ამოცანების ავტომატიზირება მარშრუტიზატორში. პოლიტიკებს უნდა შეეძლოს მარშრუტიზატორში გარკვეული ინფორმაციის მონიტორინგი და მათ საფუძველზე წინასწარ განსაზღვრული ქმედებების შესრულება:** |
| 12.1. აღნიშნულ პოლიტიკებს უნდა შეეძლოს შემდეგი სახის ინფორმაციის მონიტორინგი და წინასწარ განსაზღვრული პოლიტიკის მიხედვით მარშრუტიზატორში სკრიპტის აქტივაცია:  12.1.1. Counter - წინასწარ განსაწღვრული მთვლელის მონიტორინგი  12.1.2. Interface Counter - ინტერფეისზე სხვადასხვა სტატისტიკური მონაცემისთვის განსაზღვრული მთვლელების მონიტორინგი  12.1.3. Timer - დროის პოლიტიკის მონიტორინგი  12.1.4. Watchdog System Monitor - CPU ან მეხსიერების მონიტორინგი  12.1.5. CLI - ტექსტური ინტერფეისით შეყვენილი ბრძანებების მონიტორინგი  12.1.6. None - შესაძლებელი უნდა იყოს სკრიპტის პოლიტიკის ხელით გაშვება  12.1.7. OIR - Online insertion and removal (OIR) ის მონიტორინგი  12.1.8. SNMP– SNMP Object და SNMP Trap ის მონიტორინგი  12.1.9. Routing – მარშრუტიზაციის ცხრილის მონიტორინგი  12.1.10. მე 7 პუნქტში მოთხოვნილი ტექნოლოგიის მონიტორინგი  12.2. აღნიშნულ ტექნოლოგიას უნდა გააჩნდეს ე.წ “if” და ”goto” ლოგიკური ოპერაციების მხარდაჭერა  12.3. სკრიპტით შესაძლებელი უნდა იყოს შემდეგი ქმედებების განხორციელება:  12.3.1. წინასწარ განსაზღვრული ბრძანებების გაშვება  12.3.2. შეტყობინების გენერაცია SYSLOG, SNMP,Netflow ოქმების საშუალებით; |
| 1. **მომავალში შესაძლებელი უნდა იყოს მარშრუტიზატორის ფუნქციონალის გაზრდა, მხოლოდ პროგრამული ლიცენზიის დამატების საშუალებით, რის შემთხვევაშიც მას უნდა გააჩნდეს ტრაფიკის ნაკადების აღრიცხვის ტექნოლოგიის მხარდაჭერა. ადმინისტრატორს მოთხოვნისამებრ უნდა შეეძლოს მოქნილი შაბლონების განსაზღვრა, რომლებშიც აღწერილი იქნება ნაკადების აღრიცხვის პოლიტიკები. შაბლონის ფარგლებში ადმინისტრატორს უნდა შეეძლოს მოქნილად განსაზღვროს ტრაფიკის ის პარამეტრები, რომელთა მიხედვითაც განხორციელდება ნაკადის დადგენა და შემდგომი აღრიცხვა:** |
| 13.1. მარშრუტიზატორის ადმინისტრატორს უნდა შეეძლოს მოთხოვნისამებრ მოქნილი შაბლონების განსაზღვრა. შაბლონის ფარგლებში უნდა აღიწეროს თავსართების ველები და პარამეტრები რის მიხედვითაც განხორციელდება ტრაფიკის ნაკადის დადგენა. შესაძლებელი უნდა იყოს ისეთი ველებისა და პარამეტრების აღწერა როგორებიცაა:  13.1.1. IPv4 - IP ToS, IP Protocol, IP Source Address, IP Destination Address, Transport Source Port, Transport Destination Port, Interface Input, Interface Output  13.1.2. IPv6 - Traffic Class, Protocol, IP Source Address, IP Destination Address, Transport Source Port, Transport Destination Port, Interface Input, Interface Output  13.1.3. IP Autonomous System - Routing Source AS, Routing Destination AS, IPv4 Next Hop Address, IPv6 Next-hop Address  13.1.4. შაბლონის ფარგლებში შესაძლებელი უნდა იყოს, მე-6 პუნქტში, აღწერილი ტექნოლოგიის გამოყენება, რათა მარშრუტიზატორმა განახორციელოს აპლიკაციის ამოცნობა. აპლიკაციის სახელის გამოყენება შესაძლებელი უნდა იყოს ნაკადის დადგენისათვის.  13.2. მარშრუტიზატორის ადმინისტრატორს შაბლონის ფარგლებში უნდა შეეძლოს მოქნილად განსაზღვროს, თუ რა სახის ინფორმაციის აღრიცხვა სურს დადგენილი ტრაფიკის ნაკადის ფარგლებში. შესაძლებელი უნდა იყოს შემდეგი სახის პარამეტრების აღრიცხვა:  13.2.1. IPv4 - Routing Source AS, Routing Destination AS, Next Hop Address, TCP Flags, Interface Input, Interface Output, Counter Bytes, Counter Packets, Time Stamp First, Time Stamp Last  ii. IPv6 - Routing Source AS, Routing Destination AS, Next-hop Address, TCP Flags, Interface Input, Interface Output, Counter Bytes, Counter Packets, Time Stamp First, Time Stamp Last  13.2.2. შაბლონის ფარგლებში შესაძლებელი უნდა იყოს, მე-6 პუნქტში, აღწერილი ტექნოლოგიის გამოყენება, რათა მარშრუტიზატორმა განახორციელოს აპლიკაციის წარმადობის აღრიცხვა. აპლიკაციების ფარგლებში შესაძლებელი უნდა იყოს ისეთი პარამეტრების აღრიცხვა როგორებიცაა:  1. Application Usage  2. HTTP Hostname  3. HTTP URI  4. TCP Application – response time, transaction time, network delay, and application delay  5. RTP – jitter, packet loss, per-stream byte count and packet count  13.3. ტრაფიკის ნაკადების აღრიცხვის განხორციელება შესაძლებელი უნდა იყოს, როგორც ინტერფეისზე შემომავალი ასევე ინტერფეისიდან გამავალი ნაკადების  13.4. ტრაფიკის ნაკადების შესახებ შეგროვილი სტატისტიის გადაცემა შესაძლებელი უნდა იყოს ქსელის ნაკადების მონიტორინგის სერვერზე. |
| 1. **მარშრუტიზატორს უნდა გააჩნდეს მარშრუტიზაციის და კომუტაციის შემდეგი ოქმების მხარდაჭერა: EIGRP, EIGRP IPv6, OSFP, OSFPv3, IS-IS, IS-IS IPV6, BGP, BGP Route Reflector, BGP IPv6, BFD, PBR,** **EtherChannel Configuration.** |
| 1. **მარშრუტიზატორს უნდა გააჩნდეს შემდეგი MPLS ოქმების მხარდაჭერა: MPLS L3 VPN, ტექნოლოგიის მხარდაჭერა;** |
| 1. **მარშრუტიზატორს უნდა გააჩნდეს შემდეგი Multicast ოქმების მხარდაჭერა: PIM Dense Mode, PIM Sparse Mode, PIM Source Specific Multicast (SSM), Bidirectional PIM, HSRP aware PIM, PIMv2 for IPv6 და Multicast Listener Discovery (MLD) version 1 და MLDv2, MLDP, IGMP.** |
| 1. **მარშრუტიზატორს უნდა გააჩნდეს შემდეგი VPN ტექნოლოგიების მხარდაჭერა უსაფრთხო კავშირის გასამართად: IPSec, IKEv1, IKEv2, DMVPN.** |
| 1. **კვება - არანაკლებ 2 ცალი AC** |
| 1. **ზომა არაუმეტეს 1RU. 19-ინჩიან საკომუნიკაციო კარადაში მონტაჟის საშაუალებით (უნდა მოყვებოდეს რეკში ჩასაყენებელი ყველა საჭირო კომპონენტი)** |
| 1. **მარშრუტიზატორზე უნდა ვრცელდებოდეს მწარმოებლის არანაკლებ 1 (ერთ) წლიანი საგარანტიო მომსახურეობა, ტექნიკური მხარდაჭერა და პროგრამული უზრუნველყოფის განახლება.მოწყობილობის დაზიანების მიზეზის დადგენის შემდეგ, მოწყობილობა უნდა შეკეთდეს ან შეიცვალოს არაუმეტეს 5 სამუშაო დღეში (8x5xNBD).** |

**პროდუქციის მოწოდების და ინსტალიციის ვადაა 120 კალენდარული დღე**

|  |
| --- |
| **B ტიპის მარშუტიზატორი - ორი ცალი** |
| **მარშრუტიზატორს უნდა გააჩნდეს შემდეგი ტექნიკური მახასიათებლები:** |
| 1. **მარშრუტიზატორი უნდა იყოს მულტისერვისული, მომავალში პროგრამული და აპარატურული კომპონენტების დამატებით, საკუთრივ მარშრუტიზატორს უნდა გააჩნდეს:** |
| 1.1 ხმოვანი მარშრუტიზატორის მხარდაჭერა:  1.1.1 უნდა შეეძლოს ხმოვანი სიგნალიზაციის (SIP და H323) ოქმებით განხორციელებული ზარების მარშრუტიზაცია;  1.1.2 უნდა შეეძლოს ხმოვანი სიგნალიზაციის (SIP და H323) ოქმების უსაფრთხოების უზრუნველყოფა;  1.1.3 საჭიროების შემთხვევაში უნდა გააჩნდეს სპეციალური აპარატურული მოდულების მხარდაჭერა, რათა აღნიშნული მოდულების დონეზე განხორციელდეს სატელეფონო ზარების დამუშავება. მათ შორის ხმოვანი კოდეკების ტრანსლირება, DTMF -ის კონვერტირება, ციფრული PSTN ქსელიდან TDM ტექნოლოგიით მიღებული ზარის კონვერტაცია IP ქსელში; |
| 1.2 IP სატელეფონო სადგურის როლის შესრულების შესაძლებლობა:  1.2.1 IP ტელეფონების მიერთება და მათი მართვა;  1.2.2 სატელეფონო ნომრების მინიჭება, IP ტელეფონებზე;  1.2.3 IP სათელეფონო სადგურის მართვა შესაძლებელი უნდა იყოს გრაფიკული ინტერფეისიდან; |
| 1.3 ახალი თაობის NGFW/NGIPS ბრანდმაუერის **მხარდაჭერა:**  1.3.1 დაცვა რეალურ დროში;  1.3.2 პასიური და აქტიური რეჟიმების მხარდაჭერა;  1.3.3 ქსელის ტოპოლოგიის აღმოჩენა;  1.3.4 დაცვის რეჟიმი: 2-დან 7-ე შრემდე (Layer);  1.3.5 SSL ტრაფიკის დეშიფრაციის მხარდაჭერა და მისი შიგთავსისი ინსპექტირების საშუალება;  1.3.6 უნდა უზრუნველყოფდეს ე.წ IDS/IPS Tuning-ს, ადამიანის მინიმალური ჩარევით (მაგ.: წესების შერჩევის, პოლიტიკების კონფიგურაცია, პოლიტიკების განახლება და ა.შ.);  1.3.7 უნდა შეეძლოს ფაილების აღმოჩენა და კონტროლი. აღნიშნული ოპერაციების განხორციელება შესაძლებელი უნდა იყოს ფაილების ტიპების, გამოყენებული პროტოკოლისა და ე.წ „ატვირთვა“ „ჩამოტვირთვის“ მიხედვით;  1.3.8 უნდა შეეძლოს პასიურად შეაგროვოს ინფორმაცია ქსელის ჰოსტებისა და მათი ქცევის შესახებ. მათ შორის: ოპერაციული სისტემები, სერვისები, ღია პორტები, აპლიკაციები, სისუსტეები( vulnerabilities). აღნიშნული ინფორმაციის გამოყენება შესაძლებელი უნდა იყოს, უსაფრთხოების ინციდენტების კორელაციისთვის, ე.წ „false positives“ ინციდენტების შესამცირებლად და პოლიტიკების შესაბამისობაში მოყვანისთვის;  1.3.9 გადაწყვეტილებამ უნდა უზრუნველყოს რეალურ დროში ქსელური აქტივების გზამკვლევის აგება. მას უნდა შეეძლოს ისეთი დეტალური ინფორმაციის დადგენა აქტივების შესახებ, როგორიცაა, აქტივის მომხმარებლები, აქტივის მიერ უზრუნველყოფილი სერვისები და გამოყენებული აპლიკაციები.  1.3.10 გადაწყვეტილებას უნდა შეეძლოს, ქსელში აღმოჩენილ აპლიკაციებს მიუსადაგოს რისკის დონე და ბიზნესის რელევანტობა;  1.3.11 გადაწყვეტილებას უნდა შეეძლოს ქსელური ნაკადებში ამოიცნოს სხვადასხვა აპლიკაციები და თვალყური ადევნოს მათ. გადაწყვეტილებას უნდა შეეძლოს ამოიცნოს, მომხმარებლის აპლიკაციები, სერვერის აპლიკაციები, ვებ აპლიკაციები და აპლიკაციების ოქმები;  1.3.12 გადაწყვეტილებას უნდა შეეძლოს პასიურად განახორციელოს ინფორმაციის შეგროვება ქსელური ნაკადების შესახებ, მათ შორის სესიის დაწყებისა და დამთავრების დრო, კომუნიკაციის პორტები, სერვისები, გადაცემული ინფორმაციის მოცულობა;  1.3.13 გადაწყვეტილებას უნდა შეეძლოს პასიურად განახორციელოს მომხმარებლების მაიდენტიფიცირებელი ინფორმაციის შეგროვება. მას უნდა შეეძლოს IP მისამართების მისადეგება მომხმარებლების სახელებზე, აღნიშნული ინფორმაცია ხელმისაწვდომი უნდა იყოს შეტყობინების მენეჯმენტისთვის;  1.3.14 გადაწყვეტილებას უნდა შეეძლოს დაადგინოს თუ როგორ გამოიყენებენ ქსელურ რესურსებს მომხმარებლები, მოწყობილობები და აპლიკაციები;  1.3.15 გადაწყვეტილებას უნდა შეეძლოს დროში გავრცობილად ახორციელოს ქსელის პროფილირება და შესაბამისი რეკომენტაციების გაწევა ახალი და განახლებული უსაფრთხოების წესებისთვის. გადაწყვეტილებას უნდა შეეძლოს ახალი სიგნატურების ავტომატურად მიღება და უცნობი აპლიკაციების ბლოკირება;  1.3.16 ქსელური შეტევების აღმოჩენის წესები უნდა ეფუძნებოდეს გაფართოებად ღია სტანდარტს, რომლის მეშვეობითაც მომხმარებელს უნდა შეეძლოს როგორც მწარმოებლის მიერ შემუშავებული წესების მოდიფიცირება ასევე ახალი, მისთვის სასურველი წესების შექმნა;  1.3.17 გადაწყვეტილებას უნდა გააჩნდეს SNORT ენაზე დაფუქნებული სრულფასოვანი წესების მხარდაჭერა. გადაწყვეტილებაში შესაძლებელი უნდა იყოს არანაკლებ 2000 SNORT წესის გამოყენება;  1.3.18 სისტემას უნდა ჰქონდეს შესაძლებლობა მოახდინოს ტრაფიკის ინსპექტირება ქცევის მიხედვით;  1.3.19 შეტევების აღმომჩენ ძრავს უნდა შეეძლოს როგორც ცნობილი საფრთხეების, ასევე ახალი, ჯერ უცნობი საფრთხეების აღმოჩენა;  1.3.20 შეტევების აღმომჩენ ძრავს უნდა გააჩნდეს შეტევების აღმოჩენის რამოდენიმე მექანიზმი, მათ შორის ე.წ „exploit” ებზე დაფუძნებული სიგნატურები, სისტემების ე.წ „სისუსტეებზე“ დაფუძნებული წესები, ოქმების ანომალიები და ქცევის ანომალიების მიხედვით;  1.3.21 გადაწყვეტილებას უნდა შეეძლოს ქსელის სხვადასხვა სეგმენტების ტრაფიკის ინსპექტირება სხვადასხვა პოლიტიკებით. ერთ ინტერფეისზე შესაძლებელი უნდა იყოს სხვადასხვა უსაფრთხოების პოლიტიკების გამართვა;  1.3.22 გადაწყვეტილებას უნდა შეეძლოს IPv6 ოქმით მიმდინარე შეტევების აღმოჩენა;  1.3.23 გადაწყვეტილებას უნდა შეეძლოს პასიურად, უწყვეტ რეჟიმში ახორციელოს ქსელური ჰოსტების შესახებ ინფორმაციის შეგროვება. მათ შორის კლიენტის ოპერაციული სისტემების, ე.წ „ვებ ბრაუზერი“-ს, ვირტუალური გარემოს და მობილური მოწყობილობების აღმოჩენა;  1.3.24 გადაწყვეტილებას უნდა შეეძლოს გარე შეერთებების რეპუტაციის დადგენა. გადაწყვეტილება რეგულარულად და ავტომატურად უნდა ანახლებდეს რეპუტაციის ინფორმაციას. სისტემის ადმინისტრატორს უნდა შეეძლოს საკუთრივ განსაზღვროს ე.წ „blacklists/whitelists“ სიები. გადაწყვეტილებას უნდა შეეძლოს საჯარო და კერძო რეპუტაცის ე.წ „Feed” სერვისებთან მიერთება;  1.3.25 გადაწყვეტილებას უნდა შეეძლოს სხვადასხვა მომხმარებლებისთვის ან მათი ჯგუფებისთვის განისაზღვროს სხვადასხვა უსაფრთხოების პოლიტიკები. მომხმარებლების მაიდენტიფიცირებელი ინფორმაციის დადგენა შესაძლებელი უნდა იყოს Active Directory, LDAP სერვერებიდან;  1.3.26 გადაწყვეტილებას უნდა გააჩნდეს უნივერსალური და მოქნილი უსაფრთხოების პოლიტიკების აგების შესაძლებლობა. პოლიტიკებში შესაძლებელი უნდა იყოს სხვადასხვა სახის ინფორმაციის მითითება მათ შორის: ქსელების, ზონების, აპლიკაციების კონტროლის, მომხმარებლების კონტროლის, ფაილების კონტროლის, ჰოსტების წვდომის და IPS სისტემის პოლიტიკების; |
| 1. **მოთხოვნები ქსელური ინტერფეისების მიმართ:** |
| 2.1 ინტერფეისების რაოდენობა არანაკლებ 4(ოთხი)10/100/1000მბ/წმ წარმადობის:  2.1.1 მათ შორის - 4(ოთხი)RJ-45 ტიპისა და 4(ოთხი)SFP ტიპის**[ორმაგი დანიშნულების];**  2.1.2 დამატებითი მოდული - არანაკლებ 1 ცალი. მოდულის ინტერფეისების რაოდენობა - **2** (ორი)RJ-45 ტიპისა და 2 (ორი) SFP ტიპის**[ორმაგი დანიშნულების];**  2.1.2 მენეჯმენტ პორტი RJ-45 to DB9 (Console) ან USB-C Console Port - არანაკლებ 1 ცალი  2.1.3 მართვის პორტი - RJ-45 კონექტორით - არანაკლებ 1 ცალი  2.2 მარშრუტიზატორს უნდა გააჩნდეს გაფართოების სლოტების მხარდაჭერა, არანაკლებ 3 (სამი) ქსელური სლოტის მხარდაჭერა. აღნიშნული სლოტების საშუალებით მომავალში შესაძლებელი უნდა იყოს ინტერეფეისების რაოდენობის გაზრდა, მათ შორის:  2.2.1 არანაკლებ 8 (რვა) x 100/1000 მბ/წმ წარმადობის მქონე პორტის, POE+ ტექნოლოგიით აღჭურვილი კომუტაციის მოდულის მხარდაჭერა. არანაკლებ 3 ასეთი მოდულის მხარდაჭერა;  2.2.2 არანაკლებ 2 (ორი) x 100/1000 მბ/წმ წარმადობის, Rj-45 და SFP (ორმაგი დანიშნულების) პორტის მქონე მარშრუტიზაციის მოდულის მხარდაჭერა. არანაკლებ 3 ასეთი მოდულის მხარდაჭერა;  2.2.3 არანაკლებ 1 (ერთი) ცალი მე-4 თაობის LTE მოდულის მხარდჭერა;  2.2.4 არანაკლებ 8 (რვა) E1/T1 ცალი პორტის მქონე მოდულის მხარდაჭერა. არანაკლებ 1 ასეთი მოდულის მხარდაჭერა;  2.2.5 არანაკლედ 4 (ოთხი) FXS ტიპის პორტით. არანაკლებ 1 ასეთი მოდულის მხარდაჭერა;  2.2.6 არანაკლედ 4 (ოთხი) FXO ტიპის პორტით. არანაკლებ 1 ასეთი მოდულის მხარდაჭერა; |
| 1. **მარშრუტიზატორის წარმადობა, არანაკლებ 500მბ. მომავალში მხოლოდ პროგრამული ლიცენზიის დამატებით შესაძლებელი უნდა იყოს მარშრუტიზატორის წარმადობის გაზრდა 4000მბ-მდე. IPSec შიფრაციის წარმადობაზე არ უნდა ვრცელდებოდეს პროგრამული შეზღუდვა.** |
| 1. **DRAM ტიპის მეხსიერება არანაკლებ 4გბ. მომავალში გაფართოებადი 16გბ მდე.** |
| 1. **მარშრუტიზატორს უნდა გააჩნდეს ქსელური ბრანდმაუერის ფუნქციონალის მხარდაჭერა:** |
| 5.1. მარშრუტიზატორს უნდა გააჩნდეს ე.წ „stateteful” ბრანდმაუერის ფუნქციონალი;  5.2. ბრანდმაუერზე შესაძლებელი უნდა იყოს, რამოდენიმე უსაფრთხოების ზონების განსაზღვრა და მათი გათვალისწინებით ტრაფიკის ინსპექტირება;  5.3. ბრანდმაუერს უნდა გააჩნდეს აპლიკაციის დონეზე(Layer 7) ოქმების ინსპექტირებისა და კონტროლის შესაძლებლობა, ე.წ “Application Layer Gateway (ALG)” და „Application Inspection and Control(AIC)” ფუნქციონალი; |
| 1. **მომავალში შესაძლებელი უნდა იყოს მარშრუტიზატორის ფუნქციონალის გაზრდა, მხოლოდ პროგრამული ლიცენზიის დამატების საშუალებით, რის შემთხვევაშიც მას გაუაქტიურდება ე.წ “Application Visibility and Control(AVC)” ფუნქციონალი:** |
| 6.1 AVC ფუქნციონალს უნდა შეეძლოს ქსელური აპლიკაციების ამოცნობა „Deep Packet Inspection (DPI)” ტექნოლოგიით. განურჩევლად იმისა თუ რომელ პორტზე მუშაობს აპლიკაცია. მარშრუტიზატორს უნდა გააჩნდეს არანაკლებ 800 აპლიკაციის ამოცნობის შესაძლებლობა. აპლიკაციების სიგნატურების განახლება არ უნდა აფერხებდეს მარშრუტიზატორის მუშაობას;  6.2 აღნიშნული ფუნქციონალის ფარგლებში შესაძლებელი უნდა იყოს აპლიკაციების გამოყენებისა და ქსელური წარმადობის შეფასების სტატისტიკის შეგროვება;  6.3 აღნიშნული ფუნქციონალის ფარგლებში შესაძლებელი უნდა იყოს თითოეული აპლიკაციისთვის QoS ქსელური რესურსების გამოყენების პოლიტიკების დაწესება. ისეთი პოლიტიკების მხარდაჭერა, როგორებიცაა shape, police, priority;  6.4 შესაძლებელი უნდა იყოს აპლიკაციების გონიერი და ოპტიმალური მარშრუტიზაცია. მარშრუტიზაცია უნდა ხორციელდებოდეს მარშრუტის მიმდინარე წარმადობაზე დაყრდნობით; |
| 1. **მომავალში შესაძლებელი უნდა იყოს მარშრუტიზატორის ფუნქციონალის გაზრდა, მხოლოდ პროგრამული ლიცენზიის დამატების საშუალებით, რის შემთხვევაშიც საკუთრივ უნდა გააჩნდეს სპეციალური მექანიზმები, რათა განახორციელოს ქსელში კავშირის ხარისხის შეფასება, სხვადასხვა სახის აპლიკაციებისათვის. შესაძლებელი უნდა იყოს აღნიშნული მექანიზმის გაშვება პერიოდული განრიგის მიხედვით ან მუდვიმად:** |
| 7.1 აღნიშნულ მექანიზმებს უნდა გააჩნდეს, შემდეგი სახის ქსელის წარმადობის პარამეტრების დადგენის შესაძლებლობა:  7.1.1 Delay (round-trip და one-way)  7.1.2 Jitter (directional)  7.1.3 Packet loss (directional)  7.1.4 Packet sequencing (packet ordering)  7.1.5 Path (per hop)  7.1.6 Connectivity (directional)  7.1.7 Server or website download time  7.2 აღნიშნული მექანიზმით შესაძლებელი უნდა იყოს შემდეგი სახის ოქმებისა და აპლიკაციებისთვის, კავშირის ხარისხის შეფასება და წარმადობის პარამეტრების დადგენა:  7.2.1 TCP  7.2.1.1 response time  7.2.2 UDP  7.2.2.1 round-trip delay  7.2.2.2 one-way delay  7.2.2.3 one-way jitter  7.2.2.4 one-way packet loss  7.2.2.5 connectivity  7.2.3 ICMP  7.2.3.1 response time  7.2.3.2 end-to-end და hop-by-hop response time  7.2.4 HTTP  7.2.4.1 response time between to retrieve a web page from HTTP server  7.2.5 FTP  7.2.5.1 response time to retrieve a file from FTP server  7.2.6 DHCP  7.2.6.1 measure the response time to obtain an IP address from DHCP server  7.2.7 DNS  7.2.7.1 difference between the time taken to send a DNS request and receive a reply  7.3 აღნიშმულ მექანიზმს უნდა შეეძლოს MPLS ქსელში, Label Switched Path (LSP) ის მუშაობის შეაფასება:  7.3.1 მონაწილე „Provider Edge (PE)“ მარშრუტიზატორებს შორის, შესაძლებელი უნდა იყოს ყველა „Label Switched Path (LSP)“ ის „control-plane” და “data-plane” ის მუშაობის შემოწმება;  7.4 აღნიშნულ მექანიზმს უნდა შეეძლოს, ზუსტად შეაფასოს ქსელის მუშაობის შემდეგი პარამეტრები:  7.4.1 Per-direction jitter (source to destination and destination to source)  7.4.2 Per-direction packet loss  7.4.3 Per-direction delay (one-way dely)  7.4.4 Round-trip delay (average round-trip time)  7.5 აღნიშნული მექანიზმის მონიტორინგი შესაძლებელი უნდა იყოს SNMP ოქმის საშუალებით |
| 1. **მომავალში შესაძლებელი უნდა იყოს მარშრუტიზატორის ფუნქციონალის გაზრდა, მხოლოდ პროგრამული ლიცენზიის დამატების საშუალებით, რის შემთხვევაშიც მას უნდა გააჩნდეს ტრაფიკის ოპტიმალური მარშრუტიზაციის ტექნოლოგიის მხარდაჭერა. იგი რეალურ დროში უნდა აფასებდეს მარშრუტის ხარისხის ისეთ პარამეტრებს, როგორებიცაა: delay, loss, jitter, throughput, available bandwidth, reachability და მათზე აგებული პოლიტიკების მიხედვით უზრუნველყოფდეს აპლიკაციების ტრაფიკის ოპტიმალურ მარშრუტიზაციას:** |
| 8.1 მარშრუტიზატორს უნდა შეეძლოს, გონივრული, თითოეული აპლიკაციისთვის ოპტიმალური მარშრუტიზაციის განხორციელება, ისეთი პარამეტრების მიხედვით, როგორებიცაა: delay, loss, jitter. მარშრუტიზატორს უნდა შეეძლოს მე - 6 პუქტში აღწერილი, ფუნქციონალის გამოყენება რათა განახორციელოს ქსელური აპლიკაციების ამოცნობა;  8.2 მარშრუტიზატორს უნდა შეეძლოს პასიურად განახორციელოს მარშრუტის შეფასება. ამისათვის ის პასიურად უნდა ახდენდეს ტრანზიტული ტრაფიკის ანალიზს და ისეთი სახის პარამეტრების დადგენას, როგორებიცაა delay, packet loss, reachability, throughput. აღნიშნული სახის პარამეტრების გამოყენებით მარშრუტიზატორს უნდა შეეძლოს ოპტიმალურად განახორციელოს მარშრუტიზაცია;  8.3 მარშრუტიზატორს უნდა შეეძლოს აქტიურად განახორციელოს მარშრუტის შეფასება, მე 7 პუნქტში აღწერილი ტექნოლოგიის გამოყენებით, რათა მის შედეგებზე დაყრდნობით განახორციელოს ტრაფიკის ოპტიმალური მარშრუტიზაცია;  8.4 მარშრუტიზატორს უნდა შეეძლოს კომბინირებულად, როგორც აქტიური ასევე პასიური მარშრუტის შეფასების ტექნოლოგიების გამოყენება ოპტიმალური მარშრუტის ასარჩევად. |
| 1. **მარშრუტიზატორს უნდა გააჩნდეს შემდეგი QoS ტექნოლოგიების მხარდაჭერა: HQoS, Classification, marking, Weighted Random Early Detection (WRED), policing, shaping, priority, and Class-Based Weighted Fair Queuing (CBWFQ) scheduling;** |
| 1. **მომავალში შესაძლებელი უნდა იყოს მარშრუტიზატორის ფუნქციონალის გაზრდა, მხოლოდ პროგრამული ლიცენზიის დამატების საშუალებით, რის შემთხვევაშიც მას უნდა გააჩნდეს Locator/ID Separation Protocol (LISP) ოქმის მხარდაჭერა, რათა უზრუნველყოს IP მისამართის მობილობა;** |
| 1. **საკუთრივ მარშრუტიზატორს უნდა გააჩნდეს სპეციალური დიაგნოსტიკური საშუალება, რომლის მეშვეობითაც ადმინისტრატორს შეეძლება: ტრანზიტული, მოწყობილობაზე მიმართული და მოწყობილობიდან გამოსული ტრაფიკის შეგროვება. შეგროვებული ტრაფიკის ანალიზი შესაძლებელი უნდა იყოს ლოკალურად ან მისი ექსპორტირებით გარე სამუშაო სადგურზე. შეგროვებული ტრაფიკის ანალიზი შესაძლებელი უნდა იყოს Wireshark პროგრამული უზრუნველყოფით;** |
| 1. **საკუთრივ მარშრუტიზატორში მოთხოვნისამებრ ადმინისტრატორს უნდა შეეძლოს ე.წ „სკრიპტი“ -ის პოლიტიკების დაწერა, აღნიშნული ფუნქციონალით შესაძლებელი უნდა იყოს გარკვეული ამოცანების ავტომატიზირება მარშრუტიზატორში. პოლიტიკებს უნდა შეეძლოს მარშრუტიზატორში გარკვეული ინფორმაციის მონიტორინგი და მათ საფუძველზე წინასწარ განსაზღვრული ქმედებების შესრულება:** |
| 12.1. აღნიშნულ პოლიტიკებს უნდა შეეძლოს შემდეგი სახის ინფორმაციის მონიტორინგი და წინასწარ განსაზღვრული პოლიტიკის მიხედვით მარშრუტიზატორში სკრიპტის აქტივაცია:  12.1.1. Counter - წინასწარ განსაწღვრული მთვლელის მონიტორინგი  12.1.2. Interface Counter - ინტერფეისზე სხვადასხვა სტატისტიკური მონაცემისთვის განსაზღვრული მთვლელების მონიტორინგი  12.1.3. Timer - დროის პოლიტიკის მონიტორინგი  12.1.4. Watchdog System Monitor - CPU ან მეხსიერების მონიტორინგი  12.1.5. CLI - ტექსტური ინტერფეისით შეყვენილი ბრძანებების მონიტორინგი  12.1.6. None - შესაძლებელი უნდა იყოს სკრიპტის პოლიტიკის ხელით გაშვება  12.1.7. OIR - Online insertion and removal (OIR) ის მონიტორინგი  12.1.8. SNMP– SNMP Object და SNMP Trap ის მონიტორინგი  12.1.9. Routing – მარშრუტიზაციის ცხრილის მონიტორინგი  12.1.10. მე 7 პუნქტში მოთხოვნილი ტექნოლოგიის მონიტორინგი  12.2. აღნიშნულ ტექნოლოგიას უნდა გააჩნდეს ე.წ “if” და ”goto” ლოგიკური ოპერაციების მხარდაჭერა  12.3. სკრიპტით შესაძლებელი უნდა იყოს შემდეგი ქმედებების განხორციელება:  12.3.1. წინასწარ განსაზღვრული ბრძანებების გაშვება  12.3.2. შეტყობინების გენერაცია SYSLOG, SNMP, Netflow ოქმების საშუალებით; |
| 1. **მომავალში შესაძლებელი უნდა იყოს მარშრუტიზატორის ფუნქციონალის გაზრდა, მხოლოდ პროგრამული ლიცენზიის დამატების საშუალებით, რის შემთხვევაშიც მას უნდა გააჩნდეს ტრაფიკის ნაკადების აღრიცხვის ტექნოლოგიის მხარდაჭერა. ადმინისტრატორს მოთხოვნისამებრ უნდა შეეძლოს მოქნილი შაბლონების განსაზღვრა, რომლებშიც აღწერილი იქნება ნაკადების აღრიცხვის პოლიტიკები. შაბლონის ფარგლებში ადმინისტრატორს უნდა შეეძლოს მოქნილად განსაზღვროს ტრაფიკის ის პარამეტრები, რომელთა მიხედვითაც განხორციელდება ნაკადის დადგენა და შემდგომი აღრიცხვა:** |
| 13.1. მარშრუტიზატორის ადმინისტრატორს უნდა შეეძლოს მოთხოვნისამებრ მოქნილი შაბლონების განსაზღვრა. შაბლონის ფარგლებში უნდა აღიწეროს თავსართების ველები და პარამეტრები რის მიხედვითაც განხორციელდება ტრაფიკის ნაკადის დადგენა. შესაძლებელი უნდა იყოს ისეთი ველებისა და პარამეტრების აღწერა როგორებიცაა:  13.1.1. IPv4 - IP ToS, IP Protocol, IP Source Address, IP Destination Address, Transport Source Port, Transport Destination Port, Interface Input, Interface Output  13.1.2. IPv6 - Traffic Class, Protocol, IP Source Address, IP Destination Address, Transport Source Port, Transport Destination Port, Interface Input, Interface Output  13.1.3. IP Autonomous System - Routing Source AS, Routing Destination AS, IPv4 Next Hop Address, IPv6 Next-hop Address  13.1.4. შაბლონის ფარგლებში შესაძლებელი უნდა იყოს, მე-6 პუნქტში, აღწერილი ტექნოლოგიის გამოყენება, რათა მარშრუტიზატორმა განახორციელოს აპლიკაციის ამოცნობა. აპლიკაციის სახელის გამოყენება შესაძლებელი უნდა იყოს ნაკადის დადგენისათვის.  13.2. მარშრუტიზატორის ადმინისტრატორს შაბლონის ფარგლებში უნდა შეეძლოს მოქნილად განსაზღვროს, თუ რა სახის ინფორმაციის აღრიცხვა სურს დადგენილი ტრაფიკის ნაკადის ფარგლებში. შესაძლებელი უნდა იყოს შემდეგი სახის პარამეტრების აღრიცხვა:  13.2.1. IPv4 - Routing Source AS, Routing Destination AS, Next Hop Address, TCP Flags, Interface Input, Interface Output, Counter Bytes, Counter Packets, Time Stamp First, Time Stamp Last  ii. IPv6 - Routing Source AS, Routing Destination AS, Next-hop Address, TCP Flags, Interface Input, Interface Output, Counter Bytes, Counter Packets, Time Stamp First, Time Stamp Last  13.2.2. შაბლონის ფარგლებში შესაძლებელი უნდა იყოს, მე-6 პუნქტში, აღწერილი ტექნოლოგიის გამოყენება, რათა მარშრუტიზატორმა განახორციელოს აპლიკაციის წარმადობის აღრიცხვა. აპლიკაციების ფარგლებში შესაძლებელი უნდა იყოს ისეთი პარამეტრების აღრიცხვა როგორებიცაა:  1. Application Usage  2. HTTP Hostname  3. HTTP URI  4. TCP Application – response time, transaction time, network delay, and application delay  5. RTP – jitter, packet loss, per-stream byte count and packet count  13.3. ტრაფიკის ნაკადების აღრიცხვის განხორციელება შესაძლებელი უნდა იყოს, როგორც ინტერფეისზე შემომავალი ასევე ინტერფეისიდან გამავალი ნაკადების  13.4. ტრაფიკის ნაკადების შესახებ შეგროვილი სტატისტიის გადაცემა შესაძლებელი უნდა იყოს ქსელის ნაკადების მონიტორინგის სერვერზე. |
| 1. **მარშრუტიზატორს უნდა გააჩნდეს მარშრუტიზაციის და კომუტაციის შემდეგი ოქმების მხარდაჭერა: EIGRP, EIGRP IPv6, OSFP, OSFPv3, IS-IS, IS-IS IPV6, BGP, BGP Route Reflector, BGP IPv6, BFD, PBR, EtherChannel Configuration.** |
| 1. **მარშრუტიზატორს უნდა გააჩნდეს შემდეგი MPLS ოქმების მხარდაჭერა: MPLS L3 VPN, ტექნოლოგიის მხარდაჭერა;** |
| 1. **მარშრუტიზატორს უნდა გააჩნდეს შემდეგი Multicast ოქმების მხარდაჭერა: PIM Dense Mode, PIM Sparse Mode, PIM Source Specific Multicast (SSM), Bidirectional PIM, HSRP aware PIM, PIMv2 for IPv6 და Multicast Listener Discovery (MLD) version 1 და MLDv2, MLDP, IGMP.** |
| 1. **კვება - არანაკლებ 2 ცალი AC** |
| 1. **ზომა არაუმეტეს 1RU. 19-ინჩიან საკომუნიკაციო კარადაში მონტაჟის საშაუალებით (უნდა მოყვებოდეს რეკში ჩასაყენებელი ყველა საჭირო კომპონენტი)** |
| 1. **მარშრუტიზატორზე უნდა ვრცელდებოდეს მწარმოებლის არანაკლებ 1 (ერთ) წლიანი საგარანტიო მომსახურეობა, ტექნიკური მხარდაჭერა და პროგრამული უზრუნველყოფის განახლება.მოწყობილობის დაზიანების მიზეზის დადგენის შემდეგ, მოწყობილობა უნდა შეკეთდეს ან შეიცვალოს არაუმეტეს 5 სამუშაო დღეში (8x5xNBD).** |

**პროდუქციის მოწოდების და ინსტალიციის ვადაა 120 კალენდარული დღე**

|  |  |
| --- | --- |
| **C ტიპის კომუტატორი - ოთხი ცალი** | |
| Ethernet პორტების რაოდენობა | არანაკლებ 24 ცალი 10/100/1000მბ/წმ წარმადობის პორტი. |
| 1G SFP პორტი | არანაკლებ 4 ცალი; [არანაკლებ 4 x 10G SFP+ მოდულის მხარდაჭერა] |
| ფორმ-ფაქტორი | კომუტატორი უნდა იყოს 19-ინჩიან საკომუნიკაციო კარადაში მონტაჟის  საშაუალებით. არაუმენტეს - 1RU.  (მოწყობილობას უნდა მოყვებოდეს რეკში სამონტაჟე ყველა საჭირო კომპონენტი) |
| მენეჯმენტ პორტი RJ-45 to DB9 (Console) ან USB-C Console Port | არანაკლებ 1 ცალი |
| მართვის პორტი - RJ-45 კონექტორით | არანაკლებ 1 ცალი |
| USB პორტი | არანაკლებ 1 ცალი |
| კომუტაციის წარმადობა | არანაკლებ 128 გბ/წმ |
| ოპერატიული მეხსიერება | არანაკლებ 4GB |
| Flash მეხსიერება | არანაკლებ 4GB |
| MAC მისამართების ცხრილის მოცულობა | არანაკლებ 32000 MAC მისამართი |
| ACL რაოდენობა | არანაკლებ 1600 |
| IPv4 მარშრუტების  რაოდენობა | არანაკლებ 4000 |
| SVI რაოდენობა | არანაკლებ 1000 |
| VLAN-ID-ების რაოდენობა | არანაკლებ 4096 |
| Jumbo frames | არანაკლებ 9198 bytes |
| კვება | არანაკლებ 1 ცალი AC, საჭიროების შემთხვევაში შესაძლებელი უნდა იყოს მეორე კვების მოდულის დამატება. |
| სტეკირების ფუნქციონალის მხარდაჭერა | დიახ, გამტარობა არანაკლებ 160 გბ/წმ. უნდა მოყვებოდეს სტეკირებისთვის საჭირო ყველა კომპონენტი. (კაბელები და სტეკ მოდულები) |
| Layer 2 ფუნცქიონალი | - Layer 2 switch ports and VLAN trunks  - IEEE 802.1Q VLAN encapsulation  - Rapid Spanning Tree Protocol (RSTP)  - Multiple Spanning Tree Protocol (MSTP)  - EtherChannel Configuration  - Storm control (multicast and broadcast)  - Link-level flow control (IEEE 802.3x) |
| Layer 3 ფუნქციონალი | - static routes  -RIP, OSPF - არანაკლებ 1000 routes |
| Layer 3 და სხვა ფუნქციონალი დამატებითი ლიცენზირების შემთხვევაში | -VRF, VXLAN, LISP, SGT,EIGRP, HSRP, IS-IS, BSR, MSDP, IP SLA. |
| Switch fundamentals | -Layer 2, PBR, PIM, VRRP, QoS, 802.1X |
| Telemetry and visibility | sampled NetFlow(sFlow), SPAN ან ანალოგიური ფუნქციონალი - მაგალთად Port mirroring |
| უსაფრთხოება | - Authentication, Authorization, and Accounting(AAA)  - Access Control Lists (ACLs)  - storm control |
| მართვის ფუნქციონალი | SSH - Telnet - SNMP - syslog - CLI-based console |
| გარანტია/მხარდაჭერა  8X5XNBD | კომუტატორზე უნდა ვრცელდებოდეს მწარმოებლის არანაკლებ 1 (ერთ) წლიანი საგარანტიო მომსახურეობა, ტექნიკური მხარდაჭერა და პროგრამული უზრუნველყოფის განახლება.მოწყობილობის დაზიანების მიზეზის დადგენის შემდეგ, მოწყობილობა უნდა შეკეთდეს ან შეიცვალოს არაუმეტეს 5 სამუშაო დღეში (8x5xNBD). |

|  |
| --- |
| **დამატებითი მოთხოვნები** |
| * შემოთავაზებული A,B, და C ტიპის მოწყობილობები უნდა იყოს ერთი და იგივე მწარმოებლის. |
| * A,B,და C ტიპის მოწყობილობებს უნდა გააჩნდეს მიწოდებიდან არანაკლებ 1 წლიანი მწარმოებლის გარანტია. დაზიანებული ტექნიკის ჩანაცვლება უნდა მოხდეს მწარმოებლის ოფიციალურ ვებ გვერდზე დაზიანების ინციდენტის დაფიქსირებიდან არაუმეტეს 5 სამუშაო დღეში (8x5xNBD). ასევე შესაძლებელი უნდა იყოს პროგრამული უზრვუნველყოფის განახლება აღნიშნულ პერიოდში. |
| * მიღება ჩაბარების აქტის გაფორმების დროს, პრეტენდენტის მიერ მიწოდებული A,B და C ტიპის მოწყობილობების სერიული ნომრები უნდა იძებნებოდეს მწარმოებლის ოფიციალურ ვებ გვერდზე, სადაც ნათლად უნდა ჩანდეს, რომ თითოეული სერიული ნომერი წარმოადგენს A,B და C ტიპის კონკრეტულ მოწუობილობას და მისი საბოლოო მომხმარებელია - „ტერა ბანკი“ |
| * პრეტენდენტი კომპანია უნდა იყოს შემოთავაზებული A,B და C ტიპის მოწყობილობების მწარმოებლის ოფიციალური პარტნიორი საქართველოს ტერიტორიაზე და ეს ინფორმაცია უნდა მოწმდებოდეს მწარმოებლის ოფიციალურ ვებ გვერდზე. |
| * პრეტენდენტ კომპანიას უნდა გააჩნდეს ანალოგიური საქონლის მიწოდების გამოცდილება და უნდა წარმოადგინოს ინფორმაცია მინიმუმ 3 შესრულებულ პროექტზე. |
| * პრეტენდენტ კომპანიაში დასაქმებული უნდა იყოს არანაკლებ ერთი თანამშრომელი, რომელსაც გააჩნია შემოთავაზებული A,B და C ტიპის მოწყობილობების მწარმოებლის მიერ გაცემული, ცოდნის დამადასტურებელი სერტიფიკატი/დიპლომი. |

|  |
| --- |
| **ოპტიკური გამსხივებელი** |
| * DWDM SFP+ channel #a – 2 ცალი * DWDM SFP+ channel #b – 2 ცალი * DWDM SFP+ channel #c - 2 ცალი * 1000BASE-BX-U BiDi 20KM – 4 ცალი * 1000BASE-BX-D BiDi 20KM – 4 ცალი   მოთხოვნილი ოპტიკური გამსხივებლები სრულად თავსებადი უნდა იყოს D ტიპის კომუტატორთან. |

**პროდუქციის მოწოდების და ინსტალიციის ვადაა 120 კალენდარული დღე**