# **NGFW ტიპის ბრანდმაუერი 1 (ერთი) ცალი**

ბრანდმაუერს უნდა გააჩნდეს შემდეგი ტექნიკური მახასიათებლები:

1. ბრანდმაუერის მაქსიმალური წარმადობა NGFW რეჟიმში: არანაკლებ 16.5 გბ/წმ (ტესტი 1024 ბაიტიანი პაკეტების)
2. ბრანდმაუერის მაქსიმალური წარმადობა NGIPS რეჟიმში: არანაკლებ 16.5 გბ/წმ (ტესტი 1024 ბაიტიანი პაკეტების)
3. ერთდროული სესიების რაოდენობა NGFW რეჟიმში: არანაკლებ 2 მილიონი
4. კავშირების დამყარების სისწრაფე NGFW რეჟიმში: არანაკლებ 129 000 კავშირი/წამში
5. TLS აპარატურული დეშიფრაციის წარმადობა, არანაკლებ 4.5 გბ/წმ
6. IPsec VPN შიფრაციის წარმადობა: არანაკლებ 7.9 გბ/წმ (ტესტი 1024 ბაიტიანი პაკეტების)
7. IPSec VPN სესიების მაქსიმალური რაოდენობა: არანაკლებ 2900
8. SSD დისკის მოცულობა: არანაკლებ 900 GB
9. ინტერფეისების რაოდენობა: არანაკლებ 8(რვა) 1 გბ/წმ Ethernet ინტერფეისი (RJ-45 ტიპის) და 8 (რვა) 1/10 გბ/წმ ინტერფეისი(SFP+ ტიპის). დამატებით 1(ერთი) 1/10გბ/წმ წარმადობის (RJ-45 და SFP) მენეჯმენტ პორტი.
10. ქსელური მოდულის სლოტების რაოდენობა: არანაკლებ 1(ერთი) Network Module სლოტი
11. ქსელური მოდულის ინტერფეისების მხარდაჭერა: 8 x 1/10G
12. დამატებითი ქსელური მოდულების საშუალებით პორტების რაოდენობა უნდა იყოს არანაკლებ 24 (ოცდაოთხი) ინტერფეისი (8x1G RJ-45, 8x1/10G SFP, and network module)
13. Application Visibility and Control აპლიკაციების მხარდაჭერა: არანაკლებ 4000
14. მაღალი მდგრადობის მხარდაჭერა: Active/Standby
15. შემდეგი NGFW/NGIPS ფუნქციონალის მხარდაჭერა
    1. დაცვა რეალურ დროში
    2. პასიური და აქტიური რეჟიმების მხარდაჭერა
    3. ქსელის ტოპოლოგიის აღმოჩენა
    4. დაცვის რეჟიმი: 3-დან 7-ე შრემდე.
    5. გადაწყვეტილებას უნდა შეეძლოს ფაილების აღმოჩენა და კონტროლი. აღნიშნული ოპერაციების განხორციელება შესაძლებელი უნდა იყოს ფაილების ტიპების, გამოყენებული პროტოკოლისა და ე.წ „ატვირთვა“ „ჩამოტვირთვის“ მიხედვით;
    6. გადაწყვეტილება უნდა უზრუნველყოფდეს ე.წ. IDS/IPS Tuning-ს, ადამიანის მინიმალური ჩარევით(მაგ. წესების შერჩევის პოლიტიკების კონფიგურაცია, პოლიტიკების განახლება და ა.შ) აღნიშნული ფუნქციონალი რეალიზებული უნდა იყოს მართვისა და მონიტორინგის სისტემაში იგი არ უნდა საჭიროებდეს დამატებით პროგრამულ/აპარატურულ კომპონენტებს, რათა არ გართულდეს სისტემის ადმინისტრირება და მონიტორინგი.
    7. გადაწყვეტილებას უნდა შეეძლოს დროში გავრცობილად ახორციელოს ქსელის პროფილირება და შესაბამისი რეკომენდაციების გაწევა ახალი და განახლებული უსაფრთხოების წესებისთვის. გადაწყვეტილებას უნდა შეეძლოს ახალი სიგნატურების ავტომატურად მიღება და უცნობი აპლიკაციების ბლოკირება;
    8. გადაწყვეტილებას უნდა შეეძლოს, იმ მომხმარებლებისა და მოწყობილობების კარანტინი ან/და ტრაფიკის ღრმა ინსპექტირება, რომლების ქსელში მუშაობა და ქცევა დიდად განსხვავდება ბაზურისგან;
    9. მართვისა და მონიტორინგის სისტემას უნდა გააჩნდეს სხვადასხვა ქსელურ უსაფრთხოების კომპონენტებთან ინტეგრაციის მექანიზმები. ინტეგრაციის მექანიზმები რეალიზებული უნდა იყოს ე.წ “API” ის ან სტანდარტული ინტერფეისების სახით, რათა მომხდარ უსაფრთხოების ინციდენტებზე უზრუნველოფილი იყოს ავტომატური რეაგირება გარე ქსელური კომპონენტების საშუალებით. ინტეგრაცია შესაძლებელი უნდა იყოს მარშუტიზატორებთან, ბრანდმაუერებთან, ე.წ „remediation applications“, „patch management systems“ და “ network access control“ სისტემებთან;
    10. მართვის პლატფორმას უნდა გააჩნდეს სხვადასხვა ქსელური უსაფრთხოების კომპონენტებთან ინტეგრაციის მექანიზმები. ინტეგრაციის მექანიზმები რეალიზებული უნდა იყოს ე.წ “API” ის ან სტანდარტული ინტერფეისების სახით, რათა მიღებულ იქნეს ინფორმაცია ისეთი გარე წყაროებიდან, როგორებიცაა: ე.წ „configuration management databases“, „vulnerability management tools“, და „patch management systems“;
    11. გადაწყვეტილებას უნდა შეეძლოს ავტომატურად უზრუნველყოს შესაბამისი დონის ინსპექტირება და უსაფრთხოება ტრაფიკისთვის, რომელიც მიმდინარეობს არასტანდარტულ კომუნიკაციის პორტებზე;
    12. გადაწყვეტილებას 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. აღნიშნული ფუნქციონალი რეალიზებული უნდა იყოს IPS სისტემასა და „მართვისა და მონიტორინგის სისტემაში“, იგი არ უნდა საჭიროებდეს დამატებით პროგრამულ/აპარატურულ კომპონენტებს, რათა არ გართულდეს სისტემის ადმინისტრირება და მონიტორინგი. დეტალური მოთხოვნები აღნიშნული ფუნქციონალის მიმართ:
    13. გადაწყვეტილებას უნდა შეეძლოს პასიურად შეაგროვოს ინფორმაცია ქსელური მოწყობილობების შესახებ, მათ შორის:
    14. Operating system vendor
    15. Operating system version
    16. Network protocols used, e.g. IPv6, IPv4
    17. Network services provided, e.g. HTTPS, SSH
    18. Open ports, e.g. TCP:80
    19. Client applications installed and type, e.g. Chrome - web browser
    20. Web applications access, e.g. Facebook, Gmail
    21. Risk and relevance ratings must be available for all applications
    22. Potential vulnerabilities
    23. Current User
    24. Device type, e.g. Bridge, Mobile device
    25. Files transferred by this device / user
    26. გადაწყვეტილებას უნდა შეეძლოს პასიურად განახორციელოს ქსელური სესიებისა და ნაკადების შესახებ შემდეგი სახის ინფორმაციის შეგროვება.

1.Flow start time

2.Flow end time

3.Action (allow, deny)

4.Reason for being denied

5.Source address

6.Destination address

7.Ingres zone

8.Egress zone

9.Source port

10.Destination port

11.Application Protocol, e.g. HTTP

12.Client Application, e.g. Chrome

13.Client version, e.g. v23

14.Web application, e.g. Facebook

15.Application Risk

16.Business Relevance

17.URL (if HTTP)

18.URL Category (e.g. Social Networking)

19.Initiator User

20.IPS Events (if any)

21.Files transmitted (if any)

22.Device

23.Ingress Interface

24.Egress Interface

25.Number of packets

26.Size of transfer

* 1. გადაწყვეტილებას უნდა შეეძლოს ისეთი მობილური მოწყობილობების აღმოჩენა და კლასიფიცირება, როგორებიცაა iPad, iPhone, Blackberry. გადაწყვეტილებას უნდა შეეძლოს აღმოჩენილი მოწყობილობების დაკავშირება მომხმარებლებთან და აპლიკაციებთან.
  2. 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
  3. გადაწყვეტილებას უნდა შეეძლოს დაადგინოს თუ როგორ გამოიყენებენ ქსელურ რესურსებს მომხმარებლები, მოწყობილობები და აპლიკაციები

1. ბრანდმაუერს უნდა გააჩნდეს შემდეგი ტექნოლოგიებისა და ოქმების მხარდაჭერა: SSH, SNMP, RADIUS, NAT, IPsec, IKEv2, EIGRP, OSPF, BGP.
2. სისტემას უნდა გააჩნდეს ე.წ URL ფილტრაციის შესაძლებლობა. სისტემაში უნდა არსებობდეს არანაკლებ 80(ოთხმოცი) URL კატეგორიისა. ასევე ხელმისაწვდომი უნდა იყოს URL კატეგორიები რისკებისა და რეპუტაციების მიხედვით. ფილტრაციის განხორციელება შესაძლებელი უნდა იყოს კატეგორიისა და მისი რეპუტაციის დონის მიხედვით.
3. ბრანდამაუერს უნდა მოყვებოდეს შესაბამისი 3(წლიანი) წლიანი ლიცენზია Intrusion Prevention System(IPS) მხარდაჭერისთვის
4. ბრანდამაუერს უნდა მოყვებოდეს შესაბამისი 3(წლიანი) წლიანი ლიცენზია URL კატეგორიების ფილტრაციის მხარდაჭერისთვის
5. ბრანდამაუერს უნდა მოყვებოდეს შესაბამისი 3(წლიანი) წლიანი ლიცენზია ქსელური ანტივირუსის (Malware Protection) და Cloud Sandboxing ფუნქციონალის მხარდაჭერისთვის
6. შემოთავაზებულ ბრანდმაუერს უნდა გააჩნდეს Cisco Identity Service Engine სერვერთან ინტეგრაციის მხარდაჭერა PxGrid პროტოკოლის საშუალებით, LDAP Passive Identity ფუნქციონალის მხარდაჭერისთვის, დამატებითი Identity აგენტების გარეშე.
7. შემოთავაზებულ ბრანდმაუერს უნდა შეეძლოს უსაფრთხოების პოლიტიკების განსაზთვრა Ethernet  ფრეიმებში უსაფრთხოების ჯგუფების ტეგების (SGT over Ethernet) მიხედვით.
8. შემოთავაზებულ ბრანდმაუერს უნდა გააჩნდეს Snort უსაფრთხოების წესების ინტეგრაციის საშუალება IPS წესების ბაზაში, კონვერტაციის გარეშე.
9. შემოთავაზებულ ბრანდმაუერს უნდა გააჩნდეს ჩაშენებული Snort უსაფრთხოების წესების რედაქტორი.
10. შემოთავაზებულ ბრანდმაუერს უნდა გააჩნდეს open-source OpenAppID აპლიკაციების აღწერის ენის მხარდაჭერა.
11. ზომა: არაუმეტეს 1 RU
12. კვების ტიპი: 100-240V AC ტიპის
13. შემოთავაზებულ ბრანდმაუერს უნდა მოყვებოდეს 2(ორი) ცალი კვების ბლოკი hot-swappable ტიპის (არაუმეტეს 400W per power supply)
14. შემოთავაზებული ბრენდმაუერების მართვა უნდა მოხდეს არსებული მართვის სადგურიდან (FirePOWER Management Center ) მასში არსებული პოლიტიკების და ინტეგრაციების გათვალისწინებით.
15. არსებული მართვის სადგურიდან უნდა მოხდეს როგორც ძველი ასევე შემოთავაზებული ბრენდმაუერების მართვა.
16. ბრანდმაუერზე უნდა ვრცელდებოდეს მწარმოებლის 3(წლიანი) წლიანი საგარანტიო მომსახურეობა, ტექნიკური მხარდაჭერა და პროგრამული უზრუნველყოფის განახლება. მოწყობილობის დაზიანების მიზეზის დადგენის შემდეგ, მოწყობილობა უნდა შეკეთდეს ან შეცვალოს შემდეგ სამუშაო დღეს.

# **კომუტატორი A ტიპის 1 (ერთი) ცალი**

|  |  |
| --- | --- |
| მოთხოვნები წარმადობის და აპარატურული უზრუნველყოფის მიმართ | |
| ფიზიკური ინტერფეისები | არანაკლებ 20 x 1/10გბ/წმ SFP+ ტიპის |
| მართვის ინტერფეისები | არანაკლებ 1 x 10/100/1000 მბ/წმ Rj-45 პორტი მართვის პორტი  არანაკლებ 1 x Rj-45 კონსოლის პორტი  არანაკლებ 1 x USB კონსოლის პორტი  არანაკლებ 1 x USB სანახის დასაერთებელი პორტი |
| კომუტაციის წარმადობა | არანაკლებ 1200 გბ/წმ  არანაკლებ 1000 მილიონი პაკეტი წამში |
| კომუტაციის წარმადობა სტეკში | არანაკლებ 2400 გბ/წმ  არანაკლებ 1700 მილიონი პაკეტი წამში |
| ჯამური MAC მისამართების რაოდენობა | არანაკლებ 30,000 |
| IPv4 მარშუტების რაოდენობა | არანაკლებ 35,000 |
| IPv4 Multicast მარშუტების რაოდენობა | არანაკლებ 7,000 |
| IPv6 მარშუტების რაოდენობა | არანაკლებ 15,000 |
| QoS ACL | არანაკლებ 4,000 |
| Security ACL | არანაკლებ 7,000 |
| ქსელური ნაკადების აღრიცხვის რესურსი | არანაკლებ 60,000 |
| ოპერატიული მეხსიერება | არანაკლებ 16 GB |
| VLAN IDs | არანაკლებ 4094 |
| Switched Virtual Interfaces | არანაკლებ 1000 |
| ე.წ. Jumbo frame ზომა | არანაკლებ 9100 bytes |
| Flash | არანაკლებ 16 GB |
| Rack Unit | არაუმეტეს 1 RU |
| კომუტატორს უნდა გააჩნდეს დუბლირებული AC ტიპის კვების ბლოკი | |
| მოთხოვნები პროგრამული უზრუნველყოფის, ტექნოლოგიების და ოქმების მიმართ: | |
| კომუტაციის ტექნოლოგიები | არანაკლებ Layer 2, PVLAN, VRRP, PBR, 802.1x, |
| მარშუტიზაციის ტექნოლოგიები | არანაკლებ EIGRP, BGP, OSPF, IS-IS, BSR, MSDP, PIM SM, PIM SSM, PIM-BIDIR, IP SLA |
| ქსელის სეგმენტაციის ტექნოლოგბიე | არანაკლებ VRF, VXLAN, MPLS |
| საკუთრივ კომუტატორს უნდა გააჩნდეს არანაკლებ შემდეგი სახის ავტომატიზაციის მხარდაჭერა, მათ შორის:   1. NETCONF - პტოკოლის მხარდაჭერა 2. RESTCONF - პტოკოლის მხარდაჭერა 3. YANG - მონაცემთა მოდელის მხარდაჭერა 4. ZTP - კომუტატორს უნდა შეეძლოს ავტომატურად მიიღოს, სხვადასხვა სახის სტარტაპის პარამეტრები, მათ შორის: ოპერაციული სისტემა, კონფიგურაციის ფაილი, ლიცენზია, წვდომის რეკვიზიტები და სკრიპტები; 5. Linux Shell ის უზრუნველყოფა:    1. Linux გარემოზე წვდომა    2. Python 3.6 ის მხარდაჭერა    3. Python PIP install ის მხარდაჭერა    4. NCCLIENT ბიბლიოთეკის მხარდა    5. Yum ის მხარდაჭერა    6. RPM Install ის მხარდაჭერა | |
| საკუთრივ კომუტატორს უნდა გააჩნდეს, არანაკლებ შემდეგი კონტეინერული აპლიკაციების გაშვების შესაძლებლობა:   1. Docker - კონტეინერების მხარდაჭერა 2. SSD - დისკის დამატების შესაძლებლობა, კონტეინერების გასაშვებად 3. კონსოლზე ლოგირების მხარდაჭერა 4. REST API - არსებობა | |
| ტელემეტრიის და ქსელის ხილვადობის ტექნოლოგიები | არანაკლებ Model Driven Telemetry, NetFlow (ან ანალოგი), SPAN, RSPAN |
| მეორე დონის ტრაფიკის შიფრაციის ტექნოლოგები | არანაკლებ MACsec-256 |
| მესამე დონის ტრაფიკის შიფრაციის ტექნოლოგიები, აპარატურულ დონეზე | IPSec არანაკლებ 100გბ/წმ |
| კომუტატორს უნდა გააჩნდეს სპეციალური ინტეგრირებული და ცენტრალიზებული ქსელისა და აპლიკაციის მონიტორინგის გადაწყვეტილების მხარდაჭერა:   1. გადაწყვეტილების უნდა გააჩნდეს ინტერაქტიული და ცენტრალიზებულ სამართავი პენელი მონიტორინგისთვის ერთი წერტილიდან. 2. გადაწყვეტილების ცენტრალური სამართავი პანელიდან შესაძლებელი უნდა იყოს აპლიკაციის წარმადობის, ქსელის, მარშრუტიზაციის და მოწყობილობების მდგომარეობის შეფასება. 3. გადაწყვეტილების ცენტრალური სამართავი პანელიდან შესაძლებელი უნდა იყოს ვიზუალიზაცია მთლიანი გზის ფილიალიდან/კამპუსიდან დატაცენტრამდე/ღრუბლოვან სივრცემდე. 4. გადაწყვეტილებას უნდა შეეძლოს პრობლემის აღმოჩენა და მითითება მე7 დონიდან მე2 დონემდე. 5. გადაწყვეტილებამ უნდა მოახდინოს მოწყობილობის ავტომატური აღმოჩენა და L2 ტოპოლოგიის რუკების შედგენა, რათა დაეხმაროს რეალურ დროში ცვლილებების იდენტიფიცირებას ქსელის ინფრასტრუქტურაში. 6. გადაწყვეტილებამ უნდა მოახდინოს ქსელური მოწყობილობის ავტომატური იდენტიფიცირება, რომლებიც გავლენას ახდენს აპლიკაციის წარმადობაზე. 7. გადაწყვეტილებამ უნდა განსაზღვროს ძველი და რეალურ დროში ცვლილებები ქსელის ინფრასტრუქტურაში 8. გადაწყვეტილებას უნდა გააჩნდეს მხარდაჭერა გზის ვიზუალიზაციის, რათა მალევე შეძლოს აპლიკაციაში პრობლემის აღმოჩენა, რომელიც გამოწვეულია მოწყობილობის გაუმართაობით. 9. გადაწყვეტილებაში მონაცემების დამუშავება უნდა ხდებოდეს ერთიანი სამართავი პანელიდან, რათა შეამციროს პრობლემის მოგვარება და გაზარდოს მუშაობის ეფექტურობა. 10. გადაწყვეტილებას უნდა ქონდეს დეტალური ინფორმაცია ჰოპების მეტრიკების. 11. გადაწყვეტილებას უნდა შეეძლოს მომხმარებლების გამოცდილების ანალიზი. 12. გადაწყვეტილებას უნდა შეეძლოს ტრაფიკის მოძრაობის ვიზუალიზაცია. 13. გადაწყვეტილებას უნდა განსაზღვროს საორიენტაციო ნიშნულები როგორც ქსელი ასევე აპლიკაციის წარმადობის. 14. პროაქტიული გარჩევადობა და გათიშვის გამოვლენა 15. გადაწყვეტილება უნდა მოიცავდეს ინტერფეისის შეცდომების მონიტორინგს MTTR-ის გასაუმჯობესებლად, მოწყობილობის ყველაზე რელევანტურ მეტრიკებზე ფოკუსირებით, რომლებიც გავლენას ახდენენ აპლიკაციის მუშაობაზე. 16. გადაწყვეტილება უნდა ამონიტორებდეს კავშირის მდგომარეობას, გამტარუნარიანობას, შეცდომებს ინტერფეისის მიხედვით, მოწყობილობის გაუმართაობის წარმოსაჩენად. 17. WEB წარმადობის მონიტორინგი: 18. ვებ ტესტები - HTTP, გვერდის დატვირთულობა, ტრანზაქცია 19. მომხმარებლის ქმედების ემულაცია ტრანზაქციის ტესტებთან 20. დეტალური მეტრიკები განსაზღვრა ბრაუზერში უზერის გამოცდილებით, რომელიც ხელმისაწვდომია გვერდის დატვირთულობისა და ტრანზაქციების ტესტირებისას 21. ობიექტების გამოვლენა რომლებიც ხელს უშლიან და ახანგძლივებენ გვერდის ჩამოტვირთვას. 22. HTTP სერვერის წარმადობა - რომელიც ზომავს სერვისის ხელმისაწვდომობას, რეაგირების დროს და გამტარუნარიანობას. 23. DNS წარმადობის მონიტორინგი: 24. DNS - აპლიკაციის მიწოდებისა და უსაფრთხოების მნიშვნელოვანი კომპონენტი. 25. DNS ტესტები - სერვერი, ტრეისი, DNSSEC 26. DNS სერვერების ხელმისაწვდომობა და რეაგირების დრო, DNS პასუხების სისწორე 27. VOIP პრობლემების ხარვეძების აღმოჩენა 28. VoIP ზარების სიმულაცია ფილიალებსა და დატაცენტრებს შორის 29. SIP და RTP სერვერის ხელმისაწვდომობის განსაზღვრა. | |
| კომუტატორს უნდა გააჩნდეს სტეკირების ტექნოლოგია. სტეკში შესაძლებელი უნდა იყოს არანაკლებ 8 კომუტატორის გაერთიანება. სტეკის შეერთების წარმადობა არანაკლებ 1ტბ/წმ, თითოეული კომუტატორისთვის. სტეკირების უზრუნველყოფა არ უნდა იკავებდეს კომუტატორზე, მოთხოვნილ 1/10 გბ/წმ პორტებს.  სტეკირების ტექნოლოგიის ფარგლებში კომუტატორებს ასევე უნდა შეეძლოს სტეკში შემავალი ყველა კვების ბლოკის წყაროს გაერთიანება, ერთიან რესურსად. არანაკლებ 4 კომუტატორისა. ნებისმიერ კომუტატორს აღნიშნულ სტეკში უნდა შეეძლოს კვების რესურსის მიღება საჭიროებისამებს. სტეკში შემავალ ნებისმიერ კომუტატორზე კვების ბლოკის მწყობრიდან გამოსვლის შემთხვევაში, კომუტატორს კვების მიღება უნდა შეეძლოს სტეკის ცენტრალური კვების წყაროდან.  სტეკის გამართვა შესაძლებელი უნდა იყოს B და E ტიპის კომუტატორთან | |
| ლოგიკურ ჯგუფებზე დაფუძნებული უსაფრთხოებია და კონტროლის განსაზღვრა | კომუტატორს უნდა შეეძლოს ქსელური რესურსების დინამიური და სტატიკური კლასიფიკაცია ლოგიკურ ჯგუფებში, შემდეგი პარამეტრებით:   1. დინამიური კლასიფიკაცია უნდა განისაზღვროს მინიმუმ:    1. 802.1X აუთენტიფიკაციით    2. ვებ აუთენთიფიკაციით    3. MAC მისამართის აუტენტიფიკაციით 2. სტატიკური კლასიფიკაცია უნდა განისაზღვროს მინიმუმ:    1. IP მისამართით    2. VLAN\_ით    3. ქვექსელით    4. მესამე დონის ინტერფეისით 3. ლოგიკურ ჯგუფში შესაძლებელი უნდა იყოს რესურსების განსაზღვრა/კლასიფიკაცია მიუხედავად მათი ლოკაციისა , ქვექსელის მისამართისა და VLAN ნომრისა. 4. ლოგიკური ჯგუფის იდენტიფიკატორის ტრანსპორტირება შესაძლებელი უნდა იყოს როგორც დამატებითი თავსართი ქსელური ნაკადის შესახებ. 5. კომუტატორს უნდა შეეძლოს ლოგიკურის ჯგუფების იდენთიფიკატორზე დაფუძნებული უსაფრთხოების/ტრაფიკის ფილტრაციის პოლიტიკების გამართვა. |
| კომუტატორზე უნდა ვრცელდებოდეს მწარმოებლის სამ წლიანი საგარანტიო მომსახურეობა, ტექნიკური მხარდაჭერა და პროგრამული უზრუნველყოფის განახლება.მოწყობილობის დაზიანების მიზეზის დადგენის შემდეგ, მოწყობილობა უნდა შეკეთდეს ან შეცვალოს შემდეგ სამუშაო დღეს.  კომუტატორზე, სასიცოცხლო ცისკლის განმავლობაში უნდა ვრცელდებოდეს მწარმოებლის გარანტია შეზღუდული პირობით. კომუტატორის დაზიანების შემთხვევაში მისი შეცვლით შესაძლებლობით. | |

# **მარშრუტიატორი A ტიპის - 1 (ერთი) ცალი**

|  |  |  |
| --- | --- | --- |
| მოთხოვნები წარმადობის და აპარატურული უზრუნველყოფის მიმართ | | |
| ფიზიკური ინტერფეისები | | არანაკლებ 6 x 1გბ/წმ  არანაკლებ 2 x 10გბ/წმ |
| IPv4 მარშრუტიზაციის წარმადობა (1400 ბაიტიანი ბაკეტებით) | | არანაკლებ 19 გბ/წმ |
| IPSec მარშრუტიზაციის წარმადობა (1400 ბაიტიანი ბაკეტებით) | | არანაკლებ 6.5 გბ/წმ |
| IPSec ტუნელების რაოდენობა | | არანაკლებ 4000 |
| პაკეტების ფილტრაციის პოლიტიკების რაოდენობა | | არანაკლებ 70 000 |
| IPv4 მარშრუტების რაოდენობა | | არანაკლებ 1.5 მილიონი. მომავალში გაზრდადი 4 მილიონამდე, მეხსიერების მოდულის დამატებით |
| IPv6 მარშრუტების რაოდენობა | | არანაკლებ 1.5 მილიონი. მომავალში გაზრდადი 4 მილიონამდე, მეხსიერების მოდულის დამატებით |
| QOS რიგების რაოდენობა | | არანაკლებ 7 000 |
| NAT სესიების რაოდენობა | | არანაკლებ 1 მილიონი. მომავალში გაზრდადი 2 მილიონამდე, მეხსიერების მოდულის დამატებით |
| ბრანდმაუერის წარმადობა | | არანაკლებ 500 000 სესიის დამუშავების შესაძლებლობა |
| ვირტუალური მარშრუტიზაციის ცხრილების რაოდენობა | | არანაკლებ 4000 |
| მარშრუტიზატორი უნდა იყოს მულტისერვისული, მომავალში პროგრამული და აპარატურული კომპონენტების დამატებით, მარშრუტიზატორს უნდა გააჩნდეს: | | 1. **ხმოვანი მარშრუტიზატორის მხარდაჭერა:**    1. უნდა შეეძლოს ხმოვანი სიგნალიზაციის (SIP და H323) ოქმებით განხორციელებული ზარების მარშრუტიზაცია;    2. უნდა შეეძლოს ხმოვანი სიგნალიზაციის (SIP და H323) ოქმების უსაფრთხოების უზრუნველყოფა;    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; 2. **IP სატელეფონო სადგურის როლის შესრულების შესაძლებლობა:**    1. IP ტელეფონების მიერთება და მათი მართვა;    2. სატელეფონო ნომრების მინიჭება, IP ტელეფონებზე;    3. IP სათელეფონო სადგურის მართვა შესაძლებელი უნდა იყოს გრაფიკული ინტერფეისიდან; |
| მარშუტიზატორს უნდა გააჩნდეს დამატებითი ქსელური მოდულის მხარდაჭერა შემდეგი მახასიათებლებით | 1. 2 პორტიანი SFP ინტერფეისი MACSec ის მხარდაჭერით MACSec ის მხარდაჭერით 2. 1 პორტიანი 10გბ/წმ SFP+ ინტერფეისი MACSec ის მხარდაჭერით 3. 1 პორტიანი სერიული WAN ინტერფეისიანი მოდული 4. 2 პორტიანი სერიული WAN ინტერფეისიანი მოდული 5. 4 პორტიანი სერიული WAN ინტერფეისიანი მოდული 6. 24 არხიანი ასინქრონული სერიული მოდული 7. 16 არხიანი ასინქრონული სერიული მოდული 8. 1 პორტიანი Voice/Clear-channel Data E1 9. 2 პორტიანი Voice/Clear-channel Data E1 10. 4 პორტიანი Voice/Clear-channel Data E1 11. 8 პორტიანი Voice/Clear-channel Data E1 12. 4 პორტი FXO 13. 4 პორტი FXS | | |
| მარშრუტიზატორს უნდა გააჩნდეს შემდეგი ტექნოლოგიების მხარდაჭერა | | 1. ე.წ “Application Visibility and Control(AVC)” ფუნქციონალი:    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;    2. აღნიშნული ფუნქციონალის ფარგლებში შესაძლებელი უნდა იყოს აპლიკაციების გამოყენებისა და ქსელური წარმადობის შეფასების სტატისტიკის შეგროვება;    3. აღნიშნული ფუნქციონალის ფარგლებში შესაძლებელი უნდა იყოს თითოეული აპლიკაციისთვის QoS ქსელური რესურსების გამოყენების პოლიტიკების დაწესება. ისეთი პოლიტიკების მხარდაჭერა, როგორებიცაა shape, police, priority;    4. შესაძლებელი უნდა იყოს აპლიკაციების გონიერი და ოპტიმალური მარშრუტიზაცია. მარშრუტიზაცია უნდა ხორციელდებოდეს მარშრუტის მიმდინარე წარმადობაზე დაყრდნობით; 2. მარშრუტიზატორს უნდა გააჩნდეს სპეციალური მექანიზმები, რათა განახორციელოს ქსელში კავშირის ხარისხის შეფასება, სხვადასხვა სახის აპლიკაციებისათვის. შესაძლებელი უნდა იყოს აღნიშნული მექანიზმის გაშვება პერიოდული განრიგის მიხედვით ან მუდვიმად:    1. აღნიშნულ მექანიზმებს უნდა გააჩნდეს, შემდეგი სახის ქსელის წარმადობის პარამეტრების დადგენის შესაძლებლობა:       1. დაყოვნება (ცალი მხარე და ორივე მხარე)       2. ე.წ Jitter       3. პაკეტების დანაკარგები       4. პაკეტების თანმიმდევრობა       5. მარშრუტი       6. სერვერიდან ან ვებსაიტიდან ჩამოტვირთვის ხანგრძლივობა    2. აღნიშნული მექანიზმით შესაძლებელი უნდა იყოს შემდეგი სახის ოქმებისა და აპლიკაციებისთვის, კავშირის ხარისხის შეფასება და წარმადობის პარამეტრების დადგენა:       1. TCP          1. პასუხის ხანგრძლივობა       2. UDP          1. ორმხრივი დაყოვნება          2. ცალმხრივი დაყოვნება          3. ცალმხრივი ე.წ jitter          4. ცალმხრივი პაკეტების დანაკარგები       3. ICMP          1. პასუხის ხანგრძლივობა          2. პასუხის ხანგრძლივობა, მარშრუტზე თითოეულ კვანძამდე          3. end-to-end პასუხის ხანგრძლივობა       4. HTTP          1. HTTP სერვერიდან ვებ გვერდის ჩამოტვირთვის ხანგრძლივობა       5. FTP          1. FTP სერვერიდან ფაილის ჩამოტვირთვის ხანგრძლივობა       6. DHCP          1. IP მისამართის, მინიჭების ხანგრძლივობა          2. DHCP სერვერიდან       7. DNS          1. DNS მოთხოვნისა და პასუხის შორის ხანგრძლივობა    3. აღნიშმულ მექანიზმს უნდა შეეძლოს MPLS ქსელში, Label Switched Path (LSP) ის მუშაობის შეაფასება:       1. მონაწილე „Provider Edge (PE)“ მარშრუტიზატორებს შორის, შესაძლებელი უნდა იყოს ყველა „Label Switched Path (LSP)“ ის „control-plane” და “data-plane” ის მუშაობის შემოწმება;    4. აღნიშნულ მექანიზმს უნდა შეეძლოს, ზუსტად შეაფასოს ქსელის მუშაობის შემდეგი პარამეტრები:       1. ცალმხრივი ე.წ jitter (წყაროდან - ადრესატისკენ და ადრესატიდან წყარომდე)       2. ცალმხრივი, ქსელური პაკეტების დანაკარგები       3. ცალმხრივი დაყოვნება       4. ორმხრივი დაყოვნება    5. აღნიშნული მექანიზმის მონიტორინგი შესაძლებელი უნდა იყოს SNMP ოქმის საშუალებით 3. მარშრუტიზატორს 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:    1. მარშრუტიზატორს უნდა შეეძლოს, თითოეული აპლიკაციისთვის ოპტიმალური მარშრუტიზაციის განხორციელება, ისეთი პარამეტრების მიხედვით, როგორებიცაა: delay, loss, jitter. მარშრუტიზატორს უნდა შეეძლოს AVC ფუნქციონალის გამოყენება რათა განახორციელოს ქსელური აპლიკაციების ამოცნობა;    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;    3. მარშრუტიზატორს უნდა შეეძლოს აქტიურად განახორციელოს მარშრუტის შეფასება, მე 3 პუნქტში აღწერილი ტექნოლოგიის გამოყენებით, რათა მის შედეგებზე დაყრდნობით განახორციელოს ტრაფიკის ოპტიმალური მარშრუტიზაცია;    4. მარშრუტიზატორს უნდა შეეძლოს კომბინირებულად, როგორც აქტიური ასევე პასიური მარშრუტის შეფასების ტექნოლოგიების გამოყენება ოპტიმალური მარშრუტის ასარჩევად 4. 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; 5. 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; 6. 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:    1. აღნიშნულ პოლიტიკებს უნდა შეეძლოს შემდეგი სახის ინფორმაციის მონიტორინგი და წინასწარ განსაზღვრული პოლიტიკის მიხედვით მარშრუტიზატორში სკრიპტის აქტივაცია:       1. Counter - წინასწარ განსაწღვრული მთვლელის მონიტორინგი       2. Interface Counter - ინტერფეისზე სხვადასხვა სტატისტიკური მონაცემისთვის განსაზღვრული მთვლელების მონიტორინგი       3. Timer - დროის პოლიტიკის მონიტორინგი       4. Watchdog System Monitor - CPU ან მეხსიერების მონიტორინგი       5. CLI - ტექსტური ინტერფეისით შეყვენილი ბრძანებების მონიტორინგი       6. None - შესაძლებელი უნდა იყოს სკრიპტის პოლიტიკის ხელით გაშვება       7. OIR - Online insertion and removal (OIR) ის მონიტორინგი       8. SNMP– SNMP Object და SNMP Trap ის მონიტორინგი       9. Routing – მარშრუტიზაციის ცხრილის მონიტორინგი    2. აღნიშნულ ტექნოლოგიას უნდა გააჩნდეს ე.წ “if” და ”goto” ლოგიკური ოპერაციების მხარდაჭერა    3. სკრიპტით შესაძლებელი უნდა იყოს შემდეგი ქმედებების განხორციელება:       1. წინასწარ განსაზღვრული ბრძანებების გაშვება       2. შეტყობინების გენერაცია SYSLOG და SNMP ოქმების საშუალებით 7. მარშრუტიზატორს 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:    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:       1. IPv4 - IP ToS პარამეტრი, IP ოქმი, IP წყაროს მისამართი, IP დანიშნულების მისამართი, მე-4 დონის წყაროს პორტის მისამართი, მე-4 დონის დანიშნულების პორტის მისამართი, შემომავალი ინტერფეისი, გამავალი ინტერფეისი;       2. IPv6 - Traffic Class პარამეტრი, პროტოკოლი, IP წყაროს მისამართი, IP დანიშნულების მისამართი, მე-4 დონის წყაროს პორტის მისამართი, მე-4 დონის დანიშნულების პორტის მისამართი, შემომავალი ინტერფეისი, გამავალი ინტერფეისი;       3. IP ავტონომიური სისტემა - მარშრუტიზაციის წყარო AS, მარშრუტიზაციის დანიშნულება AS, IPv4 Next Hop მისამართი, IPv6 Next-hop მისამართი;       4. შაბლონის ფარგლებში შესაძლებელი უნდა იყოს, AVC ტექნოლოგიის გამოყენება, რათა მარშრუტიზატორმა განახორციელოს აპლიკაციის ამოცნობა. აპლიკაციის სახელის გამოყენება შესაძლებელი უნდა იყოს ნაკადის დადგენისათვის.    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:       1. IPv4 - მარშრუტიზაციის წყარო AS, მარშრუტიზაციის დანიშნულება AS, Next Hop მისამართი, TCP Flag პარამეტრები, შემომავალი ინტერფეისი, გამავალი ინტერფეისი, მთველელი მოცულობით გადაცემულ ტრაფიკი(ბაიტებში), მთვლელი მოცულობით გადაცემული პაკეტები, პირველი და ბოლო დროის პაკეტის ხანგრძლივობა ე.წ Time Stamp;       2. IPv6 - მარშრუტიზაციის წყარო AS, მარშრუტიზაციის დანიშნულება AS, Next-hop მისამართი, TCP Flag პარამეტრები, შემომავალი ინტერფეისი, გამავალი ინტერფეისი, მთველელი მოცულობით გადაცემულ ტრაფიკი(ბაიტებში), მთვლელი მოცულობით გადაცემული პაკეტები, პირველი და ბოლო დროის პაკეტის ხანგრძლივობა ე.წ Time Stamp;       3. შაბლონის ფარგლებში შესაძლებელი უნდა იყოს, „Application Visibility and Control(AVC)” ტექნოლოგიის გამოყენება, რათა მარშრუტიზატორმა განახორციელოს აპლიკაციის წარმადობის აღრიცხვა. აპლიკაციების ფარგლებში შესაძლებელი უნდა იყოს ისეთი პარამეტრების აღრიცხვა როგორებიცაა:          1. აპლიკაციის მიერ ქსელური რესურსების მოხმარება          2. HTTP Hostname პარამეტრი          3. HTTP URI პარამეტრი          4. TCP აპლიკაცია – პასუხის ხანგრძლივობა, ტრანზაქციის ხანგრძლივობა, ქსელური დაყოვნება, აპლიკაციის დაყოვნება;          5. RTP – jitter პარამეტრი          6. ქსელში გადაცემული პაკეტების დანაკარგები, თითოეული ნაკადისთვის          7. ტრაფიკისნაკადების აღრიცხვის განხორციელება შესაძლებელი უნდა იყოს, როგორც ინტერფეისზე შემომავალი ასევე ინტერფეისიდან გამავალი ნაკადების    3. ტრაფიკის ნაკადების შესახებ შეგროვილი სტატისტიის გადაცემა შესაძლებელი უნდა იყოს ქსელის ნაკადების მონიტორინგის სერვერზე 8. მარშრუტიზატორს უნდა გააჩნდეს syslog, NetFlow, SNMP, RMON და IPFIX ოქმების მხარდაჭერა; 9. მარშრუტიზატორს უნდა გააჩნდეს შემდეგი მარშრუტიზაციის ოქმების მხარდაჭერა: EIGRP, OSFP, OSFPv3, IS-IS, IS-IS IPV6, BGP, BGP Route Reflector, BGP IPv6, BFD, PBR; 10. მარშრუტიზატორს უნდა გააჩნდეს შემდეგი MPLS ოქმების მხარდაჭერა: MPLS L3 VPN, L2VPN, VPLS, ტექნოლოგიის მხარდაჭერა; 11. 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, MLDP-Based MVPN, MoFRR, MVPN**,** IGMP;   მარშრუტიზატორს უნდა გააჩნდეს შემდეგი VPN ტექნოლოგიების მხარდაჭერა უსაფრთხო კავშირის გასამართად: IPSec, VTI Tunnel, IKEv1, IKEv2; |
| კვება | | დუბლირებული AC ტიპის |
| ზომა | | არაუმეტეს 1RU |
| მარშრუტიზატორზე უნდა ვრცელდებოდეს მწარმოებლის სამ წლიანი საგარანტიო მომსახურეობა, ტექნიკური მხარდაჭერა და პროგრამული უზრუნველყოფის განახლება.მოწყობილობის დაზიანების მიზეზის დადგენის შემდეგ, მოწყობილობა უნდა შეკეთდეს ან შეცვალოს შემდეგ სამუშაო დღეს. | | |

# **ტრანსივერი A ტიპის 20(ორმოცი) ცალი**

* 1. ფორმ ფაქტორი: SFP+
  2. წარმადობა: 10გბ/წმ
  3. კონექტორი: LC
  4. ოპტიკური კაბელის მხარდაჭერა: multimode
  5. სამუშაო მანძილი: არანაკლებ 300მ

# დამატებითი მოთხონები

**1. მიმწოდებელ კომპანიამ უნდა განახორციელოს შემოთავაზებული გადაწყვეტილების**

**ინტეგრაცია;**

**2. მიმწოდებელ კომპანიას უნდა გააჩნდეს მწარმოებლის არანაკლებ 2 სერტიფიცირებული,**

**საქართველოს რეზიდენტი ინჟინერი;**

**3. პრეტენდენტს უნდა გააჩნდეს შემოთავაზებული ტექნოლოგიების (ქსელური ინფრასტრუქტურის) სპეციალიზაცია, რაც უნდა დასტურდებოდეს შემოთავაზებული პროდუქციის მწარმოებლის მიერ გაცემული წერილით;**

**4. შემოთავაზებული მოწყობილობები დამზადებული უნდა იყოს ერთი მწარმოებლის მიერ;**

**5. მოწოდებული საქონელი (მისი ყველა კომპონენტი) უნდა იყოს ახალი (არ უნდა იყოს მეორადი გამოყენების);**

**6. მომწოდებელმა უნდა წარმოადგინოს მწარმოებლის ავტორიზაციის წერილი (Manufacturers Authorization Form)**