# **ტენდერი**

**ქსელური აპარატურის და მასთან დაკავშირებული თანმდევი საინსტალაციო/საკონფიგურაციო მომსახურების შესყიდვაზე**

# **ტექნიკური დავალება, აღწერა და რაოდენობები**

# **მოთხოვნები A ტიპის კომუტატორის მიმართ (4 ცალი)**

კომუტატორს უნდა გააჩნდეს შემდეგი ტექნიკური მახასიათებლები:

1. კომუტატორის მინიმალური წარმადობა არანაკლებ: 3.6 ტბ/წმ, 1.2 bpps;
2. ინტერფეისები: არანაკლებ 48(ორმოცდარვა) – 1/10/25 გბ/წმ SFP+ ინტერფეისი, არანაკლებ 6 (ექვსი) 40/100 გბ/წმ QSFP28 ტიპის პორტი;
3. Latency: არაუმეტეს 1 მიკროწამი;
4. პროცესორი: არანაკლებ 6 ბირთვით;
5. სისტემური მეხსიერება: არანაკლებ 24 გბ;
6. SSD დისკი: არანაკლებ 128 გბ;
7. კომუტატორს უნდა გააჩნდეს L2 ტექნოლოგიების და პროტოკოლების მხარდაჭერა, მათ შორის:
   1. RSTP ტიპის ოქმების მხარდაჭერა
   2. CDP
   3. Link Aggregation Control Protocol (LACP)
   4. Static Etherchannel
8. მომავალში მხოლოდ პროგრამული ლიცენზიის დამატების შემთხვევაში კომუტატორს უნდა გააჩნდეს შემდეგი ოქმების მხარდაჭერა:

8.1 Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), Border Gateway Protocol (BGP), RIPv2, PIM-SM, SSM, MSDP, Segment routing, MPLS, VXLAN, EVPN(Multi Pod and Multi Site), VRF, HSRP.

8.2 VXLAN tunnel endpoints (VTEP) რაოდენობა არანაკლებ 256

* 1. VRF რაოდენობა არანაკლებ 1000
  2. IPv4 მარშრუტების ჩანაწერების რაოდენობა არანაკლებ: 896,000

8.5 MACSEC ოქმის მხარდაჭერა

1. კომუტატორს უნდა გააჩნდეს ე.წ „Multichassis Link Aggregation (MLAG)” ტექნოლოგიის მხარდაჭერა. აღნიშნული ტექნოლოგია საშუალებას უნდა იძლეოდეს ორი დამოუკიდებელი და ავტომონიური ე.წ „control-plane” ის მქონე კომუტატორიდან გაიმართოს, ე.წ „Link Aggregation“ ტექნოლოგია
2. ინტეგრირებული DevOps, ხელსაწყოები, მათ შორის: Puppet, Chef, Ansible, Python, ღია API.
3. ფორმფაქტორი: 1 RU;
4. 100 გბ/წმ წარმადობის მქონე 1 მეტრის სიგრძის კაბელი. 1 (ერთი) ცალი;
5. დუბლირებული კვება, AC ტიპის;
6. მოწყობილობაზე უნდა ვრცელდებოდეს მწარმოებლის 1 წლიანი გარანტია და პროგრამული უზრუნველყოფის განახლების სერვისი. დაზიანების შემთხვევაში მოწყობილობა უნდა შეკეთდეს ან შეიცვალოს დაზიანების მიზეზის დადგენიდან მომდევნო სამუშაო დღეს. გარანტია არ მოქმედებს იმ შემთხვევაში თუ დაზიანება გამოწვეულია ფიზიკური ზეგავლენით ან არასწორი ექსპლუატაციით.
7. მომწოდებელმა უნდა წარმოადგინოს მწარმოებლის ავტორიზაციის ფორმა (MAF).

# **2.** **მოთხოვნები B ტიპის კომუტატორის მიმართ (4 ცალი)**

კომუტატორს უნდა გააჩნდეს შემდეგი ტექნიკური მახასიათებლები:

1. კომუტაციის წარმადობა: არანაკლებ 208 გბ/წმ, 150 მილიონი პაკეტი წამში
2. მეხსიერება: არანაკლებ 16 გბ FLASH /8 გბ RAM ან მეტი
3. ინტერფეისები: 24 (ოცდაოთხი) - 10/100/1000T მბ/წმ პორტი და 8(რვა) SFP+ 1/10გბ/წმ პორტი ან მეტი
4. სტეკირების მხარდაჭერა:
   1. სტეკირების წარმადობა: არანაკლებ 480 Gbps
   2. სტეკში შესაძლებელი უნდა იყოს არანაკლებ 8(რვა) კომუტატორის გაერთიანება
   3. აღჭურვილი სტეკირების მოდულით
5. კომუტატორს უნდა გააჩნდეს ე.წ „line rate” წარმადობა
6. თავსებადი პროტოკოლები და ტექნოლოგიები: RSTP, MSTP, LACP, 802.1Q, QOS, RADIUS, TACACS+, Static Routing, SSH, SNMP Version 1,2c,3; UDLD, DHCP Snooping, ARP პროტოკოლის დინამიური ინსპექტირების საშუალება, IGMP v1,2,3 Snooping, MLD v1 and v2 snooping, MACSEC, EIGRP, OSPF, ISIS, BGP, PBR, ვირტუალური მარშუტიზაციის ცხრილები, OSPFv3, HSRP, IPv6, WCCP, HSRP v6, VRRPv3, IPv6 PBR, PIM‑SM, PIM-DM, PIM sparse-dense mode, და source-specific multicast (SSM)
7. კომუტატორს უნდა გააჩნდეს მომხმარებლების მოქნილი აუტენტიფიკაციის მექანიზმების მხარდაჭერა:
   1. 802.1X ტექნოლოგიის მხარდაჭერა
   2. ე.წ “MAB” ტექნოლოგიის მხარდაჭერა
   3. კომუტატორს უნდა გააჩნდეს ე.წ „Multidomain authentication“ ის მხარდაჭერა, რათა განახორციელოს ერთ პორტზე მიერთებული სამუშაო კომპიუტერისა და ტელეფონის ინდივიდუალური აუტენტიფიკაცია და მოათავსოს ისინი სხვადასხვა VLAN-ებში
   4. კომუტატორს უნდა გააჩნდეს „web authentication“ ის მხარდაჭერა
8. კომუტატორს საკუთრივ უნდა გააჩნდეს ქსელში სხვადასხვა ტიპის მოწყობილობის ამოცნობის და პორტების მიერთების დინამიური კონფიგურაციის ფუნქცია, იგი უნდა ახდენდეს სხვადასხვა ტიპის ტრაფიკის გარჩევას (როგორიცაა ვიდეო, აუდიო და სხვა) და შესაბამისი პრიორიტეტების განსაზღვრას
9. კომუტატორს უნდა გააჩნდეს სპეციალური მექანიზმები, რათა განახორციელოს ქსელში კავშირის ხარისხის შეფასება სხვადასხვა სახის აპლიკაციებისათვის
10. კომუტატორს უნდა გააჩნდეს ტრაფიკის ნაკადების აღრიცხვის ტექნოლოგიის მხარდაჭერა. კომუტატორს უნდა შეეძლოს ნაკადების აღრიცხვა ე.წ „Full” და “Sampled” რეჟიმში. 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 შემდგომ აღრიცხვა:
    1. შაბლონის ფარგლებში შესაძლებელი უნდა იყოს, მოთხოვნისამებრ იმ თავსართების ველებისა და პარამეტრების აღწერა, რის მიხედვითაც განხორციელდება ტრაფიკის ნაკადის დადგენა. შემდეგი ველებისა და პარამეტრების აღწერის შესაძლებლობა:
       1. მეორე დონის პარამეტრები: dot1q, ethertype, source mac, destination mac, vlan
       2. IPv4 მესამე დონის პარამეტრები: destination ip, source ip, protocol, tos, ttl, version
       3. IPv6 მესამე დონის პარამეტრები: destination ipv6, source ipv6, protocol
       4. მეოთხე დონის პარამეტრები: destination-port, source-port, icmp, igmp
       5. დამატებითი პარამეტრები: flow direction, interface input, interface output
    2. შაბლონის ფარგლებში, მოთხოვნისამებრ შესაძებელი უნდა იყოს, იმ პარამეტრების აღწერა, რისი აღრიცხვის განხორციელებაც არის საჭირო, დადგენილი ნაკადიდან:
       1. გადაცემული პაკეტების რაოდნობა, გადაცემული ინფორმაციის მოცულობა
       2. input და output ინტერფეისები
       3. ე.წ „timestamp absolute“ ის მითითების შესაძლებლობა, რათა აღირიცხოს ნაკადის პირველი ან/და ბოლო პაკეტი
       4. მეოთხე დონის კონტროლ-პარამეტრების აღრიცხვის შესაძლებლობა: ack, cwr, ece, fin, psh, rst, syn, urg
    3. შესაძლებელი უნდა იყოს ნაკადების აღრიცხვა შემდეგი სახის ინტერფეისებიდან: Layer 2, VLAN, WLAN, Layer 3 interface
    4. ინტერფეისზე ე.წ „ingress“ და „egress“ აღრიცხვის მხარდაჭერა
    5. არანაკლებ 24,000 ნაკადის აღრიცხვის საშუალება
11. კომუტატორზე ადმინისტრატორს მოთხოვნისამებრ უნდა შეეძლოს ე.წ „სკრიპტების“ პოლიტიკების დაწერა, აღნიშნული ფუნქციონალით შესაძლებელი უნდა იყოს გარკვეული ამოცანების ავტომატიზება კომუტატორში. აღნიშნულ პოლიტიკებს უნდა შეეძლოს კომუტატორში გარკვეული ინფორმაციის მონიტორინგი და მათ საფუძველზე წინასწარ განსაზღვრული ქმედებების შესრულება კომუტატორში:
    1. აღნიშნულ პოლიტიკებს უნდა შეეძლოს შემდეგი სახის ინფორმაციის მონიტორინგი და წინასწარ განსაზღვრული პოლიტიკის მიხედვით კომუტატორში სკრიპტის აქტივაცია:
       1. Counter - წინასწარ განსაწღვრული მთვლელის მონიტორინგი
       2. Interface Counter - ინტერფეისზე სხვადასხვა სტატისტიკებისთვის 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. SNMP– SNMP Object და SNMP Trap ის მონიტორინგი
       8. Routing – მარშუტიზაციის ცხრილის მონიტორინგი, მარშუტიზაციის ოქმის მონიტორინგი
    2. სკრიპტით შესაძლებელი უნდა იყოს შემდეგი ქმედებების განხორციელება:
       1. წინასწარ განსაზღვრული ბრძანებების გაშვება კომუტატორში
       2. შეტყობინების გენერაცია SYSLOG და SNMP ოქმების საშუალებით
    3. ე.წ “if” და ”goto” ლოგიკური ოპერაციების მხარდაჭერა
12. კომუტატორს უნდა გააჩნდეს ე.წ ტექსტური ინტერფეისი კონფიგურაციის განსახორციელებლად
13. კომუტატორს უნდა გააჩნდეს QoS პოლიტიკების განხორციელების საშუალებები:
    * 1. მარტივი და მოდულარული QoS პოლიტიკების აღწერის მხარდაჭერა
      2. ე.წ HQoS ტექნოლოგიის მხარდაჭერა
      3. შემდეგი სახის QoS ტექნოლოგიების მხარდაჭერა:
         1. Queuing
         2. Policing
         3. Shaping
14. ფორმფაქტორი: 1 RU
15. კვება: AC დუბლირებული
16. 19-იან სატელეკომუნიკაციო რეკში დასაფიქსირებელი საშუალებით აღჭურვილი
17. მოწყობილობაზე უნდა ვრცელდებოდეს მწარმოებლის 1 წლიანი გარანტია და პროგრამული უზრუნველყოფის განახლების სერვისი. დაზიანების შემთხვევაში მოწყობილობა უნდა შეკეთდეს ან შეიცვალოს დაზიანების მიზეზის დადგენიდან მომდევნო სამუშაო დღეს. გარანტია არ მოქმედებს იმ შემთხვევაში თუ დაზიანება გამოწვეულია ფიზიკური ზეგავლენით ან არასწორი ექსპლუატაციით.
18. მომწოდებელმა უნდა წარმოადგინოს მწარმოებლის ავტორიზაციის ფორმა (MAF)

# **მოთხოვნები A ტიპის ბრანდმაუერის მიმართ (2 ცალი)**

ბრანდმაუერს უნდა გააჩნდეს შემდეგი ტექნიკური მახასიათებლები:

1. NGFW და NGIPS წარმადობა: არანაკლებ 2.2 გბ/წმ(1024 ბაიტიანი HTTP ტრაფიკის პროფილი);
2. NGFW ერთდროული სესიების რაოდენობა: არანაკლებ 400 000;
3. NGFW კავშირების დამყარების სისწრაფე: არანაკლებ 22,000 კავშირი/წამში;
4. 3DES/AES შიფრაციის წარმადობა: არანაკლებ 1.2 გბ/წმ;
5. IPSec VPN სესიების მაქსიმალური რაოდენობა: არანაკლებ 400;
6. ინტერფეისების რაოდენობა არანაკლებ 8(რვა) 10/100/1000მბ/წმ წარმადობის Rj-45 ტიპის პორტი. დამატებით 4 x 1 გბ/წმ წარმადობის SFP ტიპის პორტი
7. ბრანდმაუერს უნდა გააჩნდეს შემდეგი ტექნოლოგიებისა და ოქმების მხარდაჭერა: SSH, SNMP, RADIUS, CoA, NAT, IKEv1, IKEv2, EIGRP, OSPF, BGP;
8. ბრანდმაუერს უნდა გააჩნდეს A/S მაღალმდგრადობის რეჟიმებში მუშაობის მხარდაჭერა.
9. 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 (OSI Layer);
   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. გადაწყვეტილებას უნდა შეეძლოს შესაბამისი დონის უსაფრთხოების უზრუნველყოფა თითოეული აპლიკაციისთვის. მათ შორის, ტრაფიკისთვის ნების დართვა, ინსპექტირების გარეშე ან ღრმა ინსპექტირებით, შეერთების მონიტორინგი ან ტრაფიკის ბლოკირება. ტრაფიკის ბლოკირებისთვის გადაწყვეტილებას უნდა გააჩნდეს მოქნილი მექანიზმები. მათ შორის: უზრუნველყოფილი უნდა იყოს სრულყოფილი ბლოკირება, ბლოკირება შეერთების გაწყვეტის გზავნილის საშუალებით, ინტერაქტიული ბლოკირება, როდესაც მომხმრებელი გადამისამართდება სპეციალურ ვებ გვერდზე სადაც აღწერილი იქნება უსაფრთხოების პოლიტიკა და პასუხისმგებლობა. თანხმობის შემთხვევაში შესაძლებელი უნდა იყოს აღნიშნული ვებ გვერდის შედგენა სურვილისამებრ;
   7. 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;
   8. გადაწყვეტილებას უნდა შეეძლოს დროში გავრცობილად ანხორციელოს ქსელის პროფილირება და შესაბამისი რეკომენდაციების გაწევა ახალი და განახლებული უსაფრთხოების წესებისთვის. გადაწყვეტილებას უნდა შეეძლოს ახალი სიგნატურების ავტომატურად მიღება და უცნობი აპლიკაციების ბლოკირება;
   9. გადაწყვეტილებას უნდა შეეძლოს, იმ მომხმარებლებისა და მოწყობილობების კარანტინი ან/და ტრაფიკის ღრმა ინსპექტირება, რომლების ქსელში მუშაობა და ქცევა დიდად განსხვავდება ბაზურისგან;
   10. 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;
   11. 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“;
   12. გადაწყვეტილებას უნდა შეეძლოს ავტომატურად უზრუნველყოს შესაბამისი დონის ინსპექტირება და უსაფრთხოება ტრაფიკისთვის, რომელიც მიმდინარეობს არასტანდარტულ საკომუნიკაციო პორტებზე;
   13. 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:
       1. გადაწყვეტილებას უნდა შეეძლოს პასიურად შეაგროვოს ინფორმაცია ქსელური მოწყობილობების შესახებ, მათ შორის:
          1. Operating system vendor
          2. Operating system version
          3. Network protocols used, e.g. IPv6, IPv4
          4. Network services provided, e.g. HTTPS, SSH
          5. Open ports, e.g. TCP:80
          6. Client applications installed and type, e.g. Chrome - web browser
          7. Web applications access, e.g. Facebook, Gmail
          8. Risk and relevance ratings must be available for all applications
          9. Potential vulnerabilities
          10. Current User
          11. Device type, e.g. Bridge, Mobile device
          12. Files transferred by this device / user
       2. 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. 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.
    2. გადაწყვეტილებას უნდა შეეძლოს ისეთი მობილური მოწყობილობების აღმოჩენა და კლასიფიცირება, როგორებიცაა iPad, iPhone, Blackberry. გადაწყვეტილებას უნდა შეეძლოს აღმოჩენილი მოწყობილობების დაკავშირება მომხმარებლებთან და აპლიკაციებთან.
    3. გადაწყვეტილებას უნდა შეეძლოს, ქსელში აღმოჩენილ აპლიკაციებს მიუსადაგოს რისკის დონე და ბიზნესის რელევანტობა
    4. 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
    5. გადაწყვეტილებას უნდა შეეძლოს პასიურად განახორციელოს ინფორმაციის შეგროვება ქსელური ნაკადების შესახებ, მათ შორის სესიის დაწყებისა და დამთავრების დრო, კომუნიკაციის პორტები, სერვისები, გადაცემული ინფორმაციის მოცულობა
    6. გადაწყვეტილებას უნდა შეეძლოს პასიურად განახორციელოს მომხმარებლების მაიდენტიფიცირებელი ინფორმაციის შეგროვება. მას უნდა შეეძლოს IP მისამართების მისადეგება მომხმარებლების სახელებზე, აღნიშნული ინფორმაცია ხელმისაწვდომი უნდა იყოს შეტყობინების მენეჯმენტისთვის.
    7. გადაწყვეტილებას უნდა შეეძლოს დაადგინოს თუ როგორ გამოიყენებენ ქსელურ რესურსებს მომხმარებლები, მოწყობილობები და აპლიკაციები
  1. მართვისა და მონიტორინგის სისტემას უნდა გააჩნდეს უსაფრთხოების ინციდენტებზე ავტომატური საპასუხო ქმედებების გაშვების მექანიზმი. მათ შორის ბრანდმაუერებთან და მარშუტიზატორებთან ინტეგრაცია, რათა მათზე განხორციელდეს შესაბამისი საპასუხო ქმედებები. სისტემის ადმინისტრატორს სურვილისამებრ უნდა შეეძლოს ე.წ სკრიპტების დაწერა, რითიც შესაძლებელი იქნება სხვადასხვა ქსელურ კომპონენტებთან ინტეგრაცია და სასურველი ქმედებების გაშვება. სისტემაში უნდა არსებობდეს თანდაყოლილი Cisco-ს მარშუტიზატორებზე ე.წ “Null Route” საპასუხო ქმედების გაშვების სკრიპტი და Cisco ბრანდმაუერზე ე.წ “shun” საპასუხო ქმედების გაშვების სკრიპტი
  2. აღმოჩენის წესები უნდა ეფუძნებოდეს გაფართოებად ღია სტანდარტს, რომლის მეშვეობითაც მომხმარებელს უნდა შეეძლოს როგორც მწარმოებლის მიერ შემუშავებული წესების მოდიფიცირება ასევე ახალი, მისთვის სასურველი წესების შექმნა
  3. გადაწყვეტილებას უნდა გააჩნდეს SNORT ენაზე დაფუქნებული სრულფასოვანი წესების მხარდაჭერა.
  4. სისტემას უნდა ჰქონდეს შესაძლებლობა მოახდინოს ტრაფიკის ინსპექტირება ქცევის მიხედვით:
     1. Worms
     2. Trojans
     3. Malware
     4. Backdoor attacks
     5. Spy-wares
     6. Port Scans
     7. VoIP attacks
     8. IPv6 attacks
     9. DoS attacks
     10. Buffer overflows
     11. P2P attacks
     12. SQL Injections
     13. Exploit Attacks
     14. Statistical anomalies
     15. Protocol anomalies
     16. Application anomalies
     17. Malformed traffic
     18. Invalid headers
     19. Blended threats
     20. Rate-based threats
     21. TCP segmentation and IP fragmentation
     22. Evasion detection
  5. HTTP პროტოკოლის (5-ფაზიანი) ინსპექტირება:
     1. Request Header
     2. Request Body
     3. Response headers
     4. Response Body
     5. Logging
  6. შეტევების აღმომჩენ ძრავს უნდა შეეძლოს როგორც ცნობილი საფრთხეების, ასევე ახალი, ჯერ უცნობი საფრთხეების აღმოჩენა
  7. შეტევების აღმომჩენ ძრავს უნდა გააჩნდეს შეტევების აღმოჩენის რამოდენიმე მექანიზმი, მათ შორის ე.წ „exploit” ებზე დაფუძნებული სიგნატურების, სისტემების ე.წ „სისუსტეებზე“ დაფუძნებული წესების, ოქმების ანომალიების და ქცევის ანომალიების მიხედვით
  8. გადაწყვეტილებას უნდა შეეძლოს ქსელის სხვადასხვა სეგმენტების ტრაფიკის ინსპექტირება სხვადასხვა პოლიტიკებით. ერთ ინტერფეისზე შესაძლებელი უნდა იყოს სხვადასხვა უსაფრთხოების პოლიტიკების გამართვა
  9. გადაწყვეტილებას უნდა შეეძლოს IPv6 ოქმით მიმდინარე შეტევების აღმოჩენა
  10. 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. 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
  11. 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
  12. 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.
  13. გადაწყვეტილებას უნდა გააჩნდეს აპლიკაციების კონტროლის ღრმა შესაძლებლობები. აპლიკაციის შიდა ოპერაციების ამოცნობა და კონტროლი. შესაძლებელი უნდა იყოს დეტალური პოლიტიკების შედგენა თუ რა ოპერაციების განხორციელება შეუძლიათ აპლიკაციებს ან ვებ აპლიკაციებს
  14. გადაწყვეტილებას უნდა შეეძლოს DHCP და Active Directory რესურსებთან ინტეგრაცია, რათა ავტომატურად განახორციელოს მომხმარებლებისა და მოწყობილობების ასოცირება უსაფრთხოების ინციდენტებთან
  15. გადაწყვეტილებას უნდა შეეძლოს საფრთხეების კორელაცია ჰოსტების სისუსტეებთან, ქსელის ტოპოლოგიასა და შეტევის კონტექსტთან, რათა უზრუნველყოს უსაფრთხოების ინციდენტების რელევანტობის დადგენა. აღნიშნული ფუნქციონალი რეალიზირებული უნდა იყოს IPS სისტემასა და „მართვისა და მონიტორინგის სისტემაში“, იგი არ უნდა საჭიროებდეს დამატებით პროგრამულ/აპარატურულ კომპონენტებს, რათა არ გართულდეს სისტემის ადმინისტრირება და მონიტორინგი
  16. მომავალში, მხოლოდ პროგრამული ლიცენზიის დამატების საშუალებით, გადაწყვეტილებამ უნდა უზრუნველყოს უცნობი ბოროტმოქმედი პროგრამული უზრუნველყოფის ე.წ APT –ს დან დაცვის მხარდაჭერა:

1. გადაწყვეტილებას უნდა შეეძლოს ბოროტქმედი პროგრამული უზრუნველყოფით ინფიცირებული ფაილების აღმოჩენა და ბლოკირება.
2. გადაწყვეტილებას უნდა შეეძლოს, ბოროტქმედი პროგრამული უზრუნველყოფით ინფიცირებული ფაილების აღმოჩენა და ბლოკირება, რომლებიც ცდილობენ განახორციელონ უკუკავშირი ე.წ “C&C” სერვერებთან
3. ბოროტქმედი პროგრამული უზრუნველყოფით ინფიცირებული ფაილების განსაზღვრისთვის გადაწყვეტილება უნდა იყენებდეს ე.წ „cloud” სისტემას. უცნობი ფაილების ანალიზი შესაძლებელი უნდა იყოს ე.წ „sandbox“გარემოში
4. „cloud” სისტემა უნდა ახორციელებდეს ფაილების ანალიზსა და მონიტორინგს. მათ შორის იმ ფაილების, რომელთა თავდაპირველი ქსელში მოხვედრის დროს განხორციელებულმა ანალიზმა დაადგინა, რომ ფაილი იყო ლეგიტიმირებული. გადაწყვეტილებას უნდა შეეძლოს შეტყობინების გენერაცია იმ შემთხვევაში თუ ფაილის თავდაპირველი მნიშვნელობა შეიცვალა. მაგალითად, თავდაპირველად ფაილის ანალიზისას, მისი მდგომარეობა დადგინდა, როგორც ლიგიტიმირებული, ხოლო შემდეგ დროთა განმავლობაში ფაილის მდგომარეობა შეიცვალა როგორც, ბოროტქმედი პროგრამული უზრუნველყოფით ინფიცირებული. გადაწყვეტილებას უნდა შეეძლოს შეაფასოს ბოროტმოქმედი პროგრამული უზრუნველყოფის გავრცელების არეალი, შემოსვლის წერტილი, დაინფიცირებული მომხმარებლები და ჰოსტების იდენტიფიცირება.
5. გადაწყვეტილებას უნდა შეეძლოს ქსელში გადაცემული ფაილების რუქის შედგენა
6. გადაწყვეტილებას უნდა შეეძლოს ბოროტმოქმედი პროგრამული უზრუნველყოფის ქსელში გავრცელების რუქის შედგენა
7. გადაწყვეტილებას უნდა შეეძლოს ქსელური კომპრომიტირების ინფორმაციისა და ბოროტქმედი პროგრამული უზრუნველყოფით ინფიცირებული განსაზღვრების ინფორმაციის მიმოცვლა ქსელურ და კლიენტურ უსაფრთხოების სისტემებს შორის. ქსელური და კლიენტური უსაფრთხოების სისტემები უნდა იყენებდენ ერთიან კონსისტენტურ უსაფრთხოების ინფორმაციას
   1. მწარმოებლის მხარდაჭერა NGIPS -ს პროგრამულ უზრუნველყოფაზე, 1 წლიანი განახლებები, „წესებისა და სიგნატურების“, და აპლიკაციების ამოცნობისა და კონტროლის ფუნქციონალზე;
   2. ფორმფაქტორი: 1 RU;
   3. კვება: AC ტიპის;
8. მოწყობილობაზე უნდა ვრცელდებოდეს მწარმოებლის 1 წლიანი გარანტია და პროგრამული უზრუნველყოფის განახლების სერვისი. დაზიანების შემთხვევაში მოწყობილობა უნდა შეკეთდეს ან შეიცვალოს დაზიანების მიზეზის დადგენიდან მომდევნო სამუშაო დღეს. გარანტია არ მოქმედებს იმ შემთხვევაში თუ დაზიანება გამოწვეულია ფიზიკური ზეგავლენით ან არასწორი ექსპლუატაციით.
9. მომწოდებელმა უნდა წარმოადგინოს მწარმოებლის ავტორიზაციის ფორმა (MAF)

# **მოთხოვნები B ტიპის ბრანდმაუერის მიმართ (2 ცალი)**

ბრანდმაუერს უნდა გააჩნდეს შემდეგი ტექნიკური მახასიათებლები:

1. NGFW და NGIPS წარმადობა: არანაკლებ 5 გბ/წმ(1024 ბაიტიანი HTTP ტრაფიკის პროფილი);
2. NGFW ერთდროული სესიების რაოდენობა: არანაკლებ 2 მილიონი;
3. NGFW კავშირების დამყარების სისწრაფე: არანაკლებ 27,000 კავშირი/წამში;
4. 3DES/AES შიფრაციის წარმადობა: არანაკლებ 1.6 გბ/წმ;
5. IPSec VPN სესიების მაქსიმალური რაოდენობა: არანაკლებ 7500;
6. ინტერფეისების რაოდენობა არანაკლებ 12 (თორმეტი) 10/100/1000მბ/წმ წარმადობის Rj-45 ტიპის პორტი. დამატებით 4 x 10 გბ/წმ წარმადობის SFP+ ტიპის პორტი. გაფართოების სლოტის არსებობა. მომავალში შესაძლებელი უნდა იყოს დამატებით 8 x 10 გბ/წმ წარმადობის SFP+ ტიპის პორტის დამატება;
7. ბრანდმაუერს უნდა გააჩნდეს შემდეგი ტექნოლოგიებისა და ოქმების მხარდაჭერა: SSH, SNMP, RADIUS, CoA, NAT, IKEv1, IKEv2, EIGRP, OSPF, BGP;
8. ბრანდმაუერს უნდა გააჩნდეს A/S მაღალმდგრადობის რეჟიმებში მუშაობის მხარდაჭერა.
9. 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 (OSI Layer);
   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. გადაწყვეტილებას უნდა შეეძლოს შესაბამისი დონის უსაფრთხოების ;უზრუნველყოფა თითოეული აპლიკაციისთვის. მათ შორის, ტრაფიკისთვის ნების დართვა, ინსპექტირების გარეშე ან ღრმა ინსპექტირებით, შეერთების მონიტორინგი ან ტრაფიკის ბლოკირება. ტრაფიკის ბლოკირებისთვის გადაწყვეტილებას უნდა გააჩნდეს მოქნილი მექანიზმები. მათ შორის: უზრუნველყოფილი უნდა იყოს სრულყოფილი ბლოკირება, ბლოკირება შეერთების გაწყვეტის გზავნილის საშუალებით, ინტერაქტიული ბლოკირება, როდესაც მომხმრებელი გადამისამართდება სპეციალურ ვებ გვერდზე სადაც აღწერილი იქნება უსაფრთხოების პოლიტიკა და პასუხისმგებლობა თანხმობის შემთხვევაში შესაძლებელი უნდა იყოს აღნიშნული ვებ გვერდის შედგენა სურვილისამებრ;
   7. 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;
   8. გადაწყვეტილებას უნდა შეეძლოს დროში გავრცობილად ანხორციელოს ქსელის პროფილირება და შესაბამისი რეკომენდაციების გაწევა ახალი და განახლებული უსაფრთხოების წესებისთვის. გადაწყვეტილებას უნდა შეეძლოს ახალი სიგნატურების ავტომატურად მიღება და უცნობი აპლიკაციების ბლოკირება;
   9. გადაწყვეტილებას უნდა შეეძლოს, იმ მომხმარებლებისა და მოწყობილობების კარანტინი ან/და ტრაფიკის ღრმა ინსპექტირება, რომლების ქსელში მუშაობა და ქცევა დიდად განსხვავდება ბაზურისგან;
   10. 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;
   11. 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“;
   12. გადაწყვეტილებას უნდა შეეძლოს ავტომატურად უზრუნველყოს შესაბამისი დონის ინსპექტირება და უსაფრთხოება ტრაფიკისთვის, რომელიც მიმდინარეობს არასტანდარტულ კომუნიკაციის პორტებზე;
   13. 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:
       1. გადაწყვეტილებას უნდა შეეძლოს პასიურად შეაგროვოს ინფორმაცია ქსელური მოწყობილობების შესახებ, მათ შორის:
          1. Operating system vendor
          2. Operating system version
          3. Network protocols used, e.g. IPv6, IPv4
          4. Network services provided, e.g. HTTPS, SSH
          5. Open ports, e.g. TCP:80
          6. Client applications installed and type, e.g. Chrome - web browser
          7. Web applications access, e.g. Facebook, Gmail
          8. Risk and relevance ratings must be available for all applications
          9. Potential vulnerabilities
          10. Current User
          11. Device type, e.g. Bridge, Mobile device
          12. Files transferred by this device / user
       2. გადაწყვეტილებას უნდა შეეძლოს პასიურად განახორციელოს ქსელური სესიებისა და ნაკადების შესახებ შემდეგი სახის ინფორმაციის შეგროვება:
          1. 1.Flow start time
          2. 2.Flow end time
          3. 3.Action (allow, deny)
          4. 4.Reason for being denied
          5. 5.Source address
          6. 6.Destination address
          7. 7.Ingres zone
          8. 8.Egress zone
          9. 9.Source port
          10. 10.Destination port
          11. 11.Application Protocol, e.g. HTTP
          12. 12.Client Application, e.g. Chrome
          13. 13.Client version, e.g. v23
          14. 14.Web application, e.g. Facebook
          15. 15.Application Risk
          16. 16.Business Relevance
          17. 17.URL (if HTTP)
          18. 18.URL Category (e.g. Social Networking)
          19. 19.Initiator User
          20. 20.IPS Events (if any)
          21. 21.Files transmitted (if any)
          22. 22.Device
          23. 23.Ingress Interface
          24. 24.Egress Interface
          25. 25.Number of packets
          26. 26.Size of transfer
       3. 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.
       4. გადაწყვეტილებას უნდა შეეძლოს ისეთი მობილური მოწყობილობების აღმოჩენა და კლასიფიცირება, როგორებიცაა iPad, iPhone, Blackberry. გადაწყვეტილებას უნდა შეეძლოს აღმოჩენილი მოწყობილობების დაკავშირება მომხმარებლებთან და აპლიკაციებთან.
       5. გადაწყვეტილებას უნდა შეეძლოს, ქსელში აღმოჩენილ აპლიკაციებს მიუსადაგოს რისკის დონე და ბიზნესის რელევანტობა
       6. 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
       7. გადაწყვეტილებას უნდა შეეძლოს პასიურად განახორციელოს ინფორმაციის შეგროვება ქსელური ნაკადების შესახებ, მათ შორის სესიის დაწყებისა და დამთავრების დრო, კომუნიკაციის პორტები, სერვისები, გადაცემული ინფორმაციის მოცულობა
       8. გადაწყვეტილებას უნდა შეეძლოს პასიურად განახორციელოს მომხმარებლების მაიდენტიფიცირებელი ინფორმაციის შეგროვება. მას უნდა შეეძლოს IP მისამართების მისადეგება მომხმარებლების სახელებზე, აღნიშნული ინფორმაცია ხელმისაწვდომი უნდა იყოს შეტყობინების მენეჯმენტისთვის.
       9. გადაწყვეტილებას უნდა შეეძლოს დაადგინოს თუ როგორ გამოიყენებენ ქსელურ რესურსებს მომხმარებლები, მოწყობილობები და აპლიკაციები
   14. მართვისა და მონიტორინგის სისტემას უნდა გააჩნდეს უსაფრთხოების ინციდენტებზე ავტომატური საპასუხო ქმედებების გაშვების მექანიზმი. მათ შორის ბრანდმაუერებთან და მარშუტიზატორებთან ინტეგრაცია, რათა მათზე განხორციელდეს შესაბამისი საპასუხო ქმედებები. სისტემის ადმინისტრატორს სურვილისამებრ უნდა შეეძლოს ე.წ სკრიპტების დაწერა, რითიც შესაძლებელი იქნება სხვადასხვა ქსელურ კომპონენტებთან ინტეგრაცია და სასურველი ქმედებების გაშვება. სისტემაში უნდა არსებობდეს თანდაყოლილი Cisco-ს მარშუტიზატორებზე ე.წ “Null Route” საპასუხო ქმედების გაშვების სკრიპტი და Cisco ბრანდმაუერზე ე.წ “shun” საპასუხო ქმედების გაშვების სკრიპტი
   15. აღმოჩენის წესები უნდა ეფუძნებოდეს გაფართოებად ღია სტანდარტს, რომლის მეშვეობითაც მომხმარებელს უნდა შეეძლოს როგორც მწარმოებლის მიერ შემუშავებული წესების მოდიფიცირება ასევე ახალი, მისთვის სასურველი წესების შექმნა
   16. გადაწყვეტილებას უნდა გააჩნდეს SNORT ენაზე დაფუქნებული სრულფასოვანი წესების მხარდაჭერა.
   17. სისტემას უნდა ჰქონდეს შესაძლებლობა მოახდინოს ტრაფიკის ინსპექტირება ქცევის მიხედვით:
       1. Worms
       2. Trojans
       3. Malware
       4. Backdoor attacks
       5. Spy-wares
       6. Port Scans
       7. VoIP attacks
       8. IPv6 attacks
       9. DoS attacks
       10. Buffer overflows
       11. P2P attacks
       12. SQL Injections
       13. Exploit Attacks
       14. Statistical anomalies
       15. Protocol anomalies
       16. Application anomalies
       17. Malformed traffic
       18. Invalid headers
       19. Blended threats
       20. Rate-based threats
       21. TCP segmentation and IP fragmentation
       22. Evasion detection
   18. HTTP პროტოკოლის (5-ფაზიანი) ინსპექტირება:
       1. Request Header
       2. Request Body
       3. Response headers
       4. Response Body
       5. Logging
   19. შეტევების აღმომჩენ ძრავს უნდა შეეძლოს როგორც ცნობილი საფრთხეების, ასევე ახალი, ჯერ უცნობი საფრთხეების აღმოჩენა
   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
   21. გადაწყვეტილებას უნდა შეეძლოს ქსელის სხვადასხვა სეგმენტების ტრაფიკის ინსპექტირება სხვადასხვა პოლიტიკებით. ერთ ინტერფეისზე შესაძლებელი უნდა იყოს სხვადასხვა უსაფრთხოების პოლიტიკების გამართვა
   22. გადაწყვეტილებას უნდა შეეძლოს IPv6 ოქმით მიმდინარე შეტევების აღმოჩენა
   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. 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
   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
   25. 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.
   26. გადაწყვეტილებას უნდა გააჩნდეს აპლიკაციების კონტროლის ღრმა შესაძლებლობები. აპლიკაციის შიდა ოპერაციების ამოცნობა და კონტროლი. შესაძლებელი უნდა იყოს დეტალური პოლიტიკების შედგენა თუ რა ოპერაციების განხორციელება შეუძლიათ აპლიკაციებს ან ვებ აპლიკაციებს
   27. გადაწყვეტილებას უნდა შეეძლოს DHCP და Active Directory რესურსებთან ინტეგრაცია, რათა ავტომატურად განახორციელოს მომხმარებლებისა და მოწყობილობების ასოცირება უსაფრთხოების ინციდენტებთან
   28. გადაწყვეტილებას უნდა შეეძლოს საფრთხეების კორელაცია ჰოსტების სისუსტეებთან, ქსელის ტოპოლოგიასა და შეტევის კონტექსტთან, რათა უზრუნველყოს უსაფრთხოების ინციდენტების რელევანტობის დადგენა. აღნიშნული ფუნქციონალი რეალიზირებული უნდა იყოს IPS სისტემასა და „მართვისა და მონიტორინგის სისტემაში“, იგი არ უნდა საჭიროებდეს დამატებით პროგრამულ/აპარატურულ კომპონენტებს, რათა არ გართულდეს სისტემის ადმინისტრირება და მონიტორინგი
   29. მომავალში მხოლოდ პროგრამული ლიცენზიის დამატების საშუალებით, გადაწყვეტილებამ უნდა უზრუნველყოს უცნობი ბოროტმოქმედი პროგრამული უზრუნველყოფის ე.წ APT –ს დან დაცვის მხარდაჭერა:
       1. გადაწყვეტილებას უნდა შეეძლოს ბოროტმოქმედი პროგრამული უზრუნველყოფით ინფიცირებული ფაილების აღმოჩენა და ბლოკირება.
       2. გადაწყვეტილებას უნდა შეეძლოს, ბოროტმოქმედი პროგრამული უზრუნველყოფით ინფიცირებული ფაილების აღმოჩენა და ბლოკირება, რომლებიც ცდილობენ განახორციელონ უკუკავშირი ე.წ “C&C” სერვერებთან
       3. ბოროტქმედი პროგრამული უზრუნველყოფით ინფიცირებული ფაილების განსაზღვრისთვის გადაწყვეტილება უნდა იყენებდეს ე.წ „cloud” სისტემას. უცნობი ფაილების ანალიზი შესაძლებელი უნდა იყოს ე.წ „sandbox“გარემოში
       4. „cloud” სისტემა უნდა ახორციელებდეს ფაილების ანალიზსა და მონიტორინგს. მათ შორის იმ ფაილების, რომელთა თავდაპირველი ქსელში მოხვედრის დროს განხორციელებულმა ანალიზმა დაადგინა, რომ ფაილი იყო ლეგიტიმირებული. გადაწყვეტილებას უნდა შეეძლოს შეტყობინების გენერაცია იმ შემთხვევაში თუ ფაილის თავდაპირველი მნიშვნელობა შეიცვალა. მაგალითად, თავდაპირველად ფაილის ანალიზისას, მისი მდგომარეობა დადგინდა, როგორც ლიგიტიმირებული, ხოლო შემდეგ დროთა განმავლობაში ფაილის მდგომარეობა შეიცვალა როგორც, ბოროტქმედი პროგრამული უზრუნველყოფით ინფიცირებული. გადაწყვეტილებას უნდა შეეძლოს შეაფასოს ბოროტმოქმედი პროგრამული უზრუნველყოფის გავრცელების არეალი, შემოსვლის წერტილი, დაინფიცირებული მომხმარებლები და ჰოსტების იდენტიფიცირება.
       5. გადაწყვეტილებას უნდა შეეძლოს ქსელში გადაცემული ფაილების რუქის შედგენა
       6. გადაწყვეტილებას უნდა შეეძლოს ბოროტმოქმედი პროგრამული უზრუნველყოს ქსელში გავრცელების რუქის შედგენა
       7. გადაწყვეტილებას უნდა შეეძლოს ქსელური კომპრომიტირების ინფორმაციისა და ბოროტმოქმედი პროგრამული უზრუნველყოფით ინფიცირებული განსაზღვრების ინფორმაციის მიმოცვლა ქსელურ და კლიენტურ უსაფრთხოების სისტემებს შორის. ქსელური და კლიენტური უსაფრთხოების სისტემები უნდა იყენებდენ ერთიან კონსისტენტურ უსაფრთხოების ინფორმაციას.
   30. მწარმოებლის მხარდაჭერა NGIPS -ს პროგრამულ უზრუნველყოფაზე, 1 წლიანი განახლებებზე და აპლიკაციების ამოცნობისა და კონტროლის ფუნქციონალზე;
   31. ფორმფაქტორი: 1 RU;
   32. კვება: დუბლირებული AC ტიპის;
10. მოწყობილობაზე უნდა ვრცელდებოდეს მწარმოებლის 1 წლიანი გარანტია და პროგრამული უზრუნველყოფის განახლების სერვისი. დაზიანების შემთხვევაში მოწყობილობა უნდა შეკეთდეს ან შეიცვალოს დაზიანების მიზეზის დადგენიდან მომდევნო სამუშაო დღეს. გარანტია არ მოქმედებს იმ შემთხვევაში თუ დაზიანება გამოწვეულია ფიზიკური ზეგავლენით ან არასწორი ექსპლუატაციით.
11. მომწოდებელმა უნდა წარმოადგინოს მწარმოებლის ავტორიზაციის ფორმა (MAF)

# **ბრანდმაუერების მართვისა და მონიტორინგის სისტემა (1ცალი)**

1. მართვისა და მონიტორინგის სისტემიდან შესაძლებელი უნდა იყოს მოთხოვნილი A და B ტიპის NGFW ბრანდმაუერების მართვა;
2. მართვისა და მონიტორინგის სისტემის მართვა შესაძლებელი უნდა იყოს ვებ ბრაუზერიდან;
3. მართვისა და მონიტორინგის სისტემა უნდა წარმოადგენდეს მზა ე.წ ‘virtual appliance’ გადაწყვეტილებას;
4. მართვისა და მონიტორინგის სისტემიდან შესაძლებელი უნდა იყოს ოთხი NGFW ბრანდმაუერის მართვა;
5. სისტემაზე უნდა ვრცელდებოდეს მწარმოებლის 1 წლიანი გარანტია და პროგრამული უზრუნველყოფის განახლების სერვისი. დაზიანების შემთხვევაში სისტემა უნდა შეკეთდეს ან შეიცვალოს დაზიანების მიზეზის დადგენიდან მომდევნო სამუშაო დღეს. გარანტია არ მოქმედებს იმ შემთხვევაში თუ დაზიანება გამოწვეულია ფიზიკური ზეგავლენით ან არასწორი ექსპლუატაციით.
6. მომწოდებელმა უნდა წარმოადგინოს მწარმოებლის ავტორიზაციის ფორმა (MAF)

# **მოთხოვნები C ტიპის კომუტატორის მიმართ (2 ცალი)**

# ტექნიკური მახასიათებლები:

* ინტერფეისების რაოდენობა: 24 – 100/1000 მბ/წმ RJ-45 ტიპის ინტერფეისი. 4 - 1 გბ/წმ SFP ტიპის ინტერფეისი;
* კომუტაციის სიჩქარე: 56 Gbps;
* MAC მისამართების ცხრილის ზომა: არანაკლებ 8000 ჩანაწერი
* მეხსიერება მინიმალური: 256 MB FLASH /512 MB DRAM
* Basic Layer 3 ტექნოლოგიების მხარდაჭერა:
  + Static Routing
  + RIP

კომუტატორს უნდა გააჩნდეს შემდეგი ტექნოლოგიების და პროტოკოლების მხარდაჭერა:

* STP ტიპის ოქმების მხარდაჭერა:
  + IEEE 802.1d STP, IEEE 802.1w RSTP, IEEE 802.1s MSTP, PVRST+
  + 64 instances support
* Dynamic Host Configuration Protocol (DHCP)
* Jumbo Frames - მინიმუმ 10240 ბაიტი
* MTU-L3 packet – 9198 ბაიტი
* IPv4/MAC security ACEs - 384
* IPv4 unicast direct routes – 542
* IPv6 security ACEs – 384
* Active VLANs – 64
* VLAN IDs available – 4094
* Voice VLAN
* Link Layer Discovery Protocol (LLDP)
* CDP
* Port Aggregation Protocol (PAgP)
* Link Aggregation Control Protocol (LACP)
* Dynamic Trunking Protocol (DTP)
* Local Proxy ARP
* VLAN Trunking Protocol (VTP)
* Trivial File Transfer Protocol (TFTP)
* Network Time Protocol (NTP)
* Multicast ტექნოლოგიის მხარდაჭერა:
  + IGMP versions 1, 2, and 3 snooping
  + IGMP/MLD querier
  + MLD v1/2 Snooping (IPv6)
* Layer 2 უსაფრთხოების მექანიზმების მხარდაჭერა:
  + Secure Shell(SSH) Protocol მხარდაჭერა.
  + Multilevel security on console access
  + Secure Sockets Layer (SSL)
  + Port-based ACLs
  + ACLs(Access Control List)
  + TACACS+ and RADIUS authentication
  + Storm control, Broadcast, multicast, and unknown unicast
  + Port Security
  + DHCP Snooping
  + ARP Inspection
  + Switched Port Analyzer(SPAN)
  + BPDU guard
  + Spanning-Tree Root Guard(STRG)
  + Internet Group Management Protocol(IGMP) filtering
* QoS ტექნოლოგიების მხარდაჭერა:
  + 4 egress queues
  + Scheduling:
  + Strict priority and weighted round-robin (WRR)
  + Queue assignment based on DSCP and class of service (802.1p/CoS)
* მართვადიანობა:
  + Web UI
  + Bluetooth
  + CLI
  + SNMP
  + Virtual Stacking
    - მინიმუმ 8 სვიჩის გაერთიანების შესაძლებობა ვირტუალურ სტეკში
    - ვირტუალურ სტეკში არსებული კომუტატორების მართვა შესაძლებელი უნდა იყოს ერთი კომუტატორიდან
    - ვირტუალურ სტეკში არსებული კომუტატორების მართვა შესაძლებელი უნდა იყოს CLI, SNMP ან web UI - დან.
* ფიზიკური მახასიათებლები:
  + არაუმეტეს: 1 RU ზომის
  + 19-იან სატელეკომუნიკაციო რეკში დასაფიქსირებელი, საშუალებით აღჭურვილი
* კვება: 110-220V (ACE ტიპის კვების კაბელით აღჭურვილი)
* კომუტატორზე უნდა ვრცელდებოდეს მწარმოებლის 1 წლიანი საგარანტიო მომსახურეობა, ტექნიკური მხარდაჭერა და პროგრამული უზრუნველყოფის განახლება. მოწყობილობის დაზიანების მიზეზის დადგენის შემდეგ, მოწყობილობა უნდა შეკეთდეს ან შეცვალოს შემდეგ სამუშაო დღეს.

მომწოდებელმა უნდა წარმოადგინოს მწარმოებლის ავტორიზაციის ფორმა (MAF)

# **WDM ტრანსპონდერ/მუქსპონდერი გადაწყვეტილება (4 ცალი)**

მრავალფუნქციური DWDM მუქსპონდერი შემდეგი მახასიათებლებით:

1. 10 (ათი) x 1/10გბ კლიენტური შეერთების მულტიპლექსირების მხარდაჭერა, მომავალში შესაძლებელი უნდა იყოს დამატებით 6 (ექვსი) კლიენტური არხის დამატება;
2. 3 (სამი) x 10გბ/წმ 40კმ DWDM ტრანსივერი სრულად თავსებადი A და B ტიპის კომუტატორებთან და ანალოგური კლასის კომუტატორებთან. სრულად თავსებადი მულტიპლექსორთან;
3. 2 (ორი) x 1გბ/წმ 40კმ DWDM ტრანსივერი სრულად თავსებადი არსებულ Cisco 3850 სერიის კომუტატორთან. სრულად თავსებადი მულტიპლექსორთან;

# **ტრანსივერი A ტიპის 30 ცალი**

1. ფორმფაქტორი: SFP+
2. წარმადობა: 10გბ/წმ
3. მანძილი არანაკლებ 400(ოთხასი) მეტრი
4. თავსებადი MM ტიპის ოპტიკურ ბოჭკოვან კაბელთან
5. სრულად თავსებადი A, B ტიპის კომუტატორებთან
6. სრულად თავსებადი A, B ტიპის ბრანდმაუერებთან

# **ტრანსივერი B ტიპის 54 ცალი**

1. ფორმფაქტორი: SFP
2. წარმადობა: 1გბ/წმ
3. კონექტორი: Rj-45
4. სრულად თავსებადი A, B ტიპის კომუტატორთან

**1-6 პოზიციები უნდა იყოს ერთი და იგივე მწარმოებლის**

# **ინტეგრაცია და თანმდევი მომსახურება**

პრეტენდენტმა კომპანიამ უნდა განაროხციელოს შემოთავაზებული გადაწყვეტილების ინტეგრაცია. ინტეგრაციის ფარგლებში, პრეტენდენტმა კომპანიამ უნდა განახორციელოს:

1. დეტალური ინტეგრაციის გეგმის და დოკუმენტაციის შემუშავება, მათ შორის ე.წ HLD, L1, L2 და L3 სქემების. სისტემა უნდა იყოს სრულად დუბლირებული, ცალკეული კომპონენტების(კაბელი, ტრანსივერი, მოწყობილობა) მწყობრიდან გამოსვლა არ უნდა იწვევდეს სერვისების მიწოდების შეფერხებას;
2. დეტალური მიგრაციის გეგმის შემუშავება. არსებული მუშა მონაცემთა დამუშავების ცენტრში, მოთხოვნილი მოწყობილობების ეტაპობრივი ინტეგრაციის გეგმის შემუშავება და მათზე მიგრაციის განხორციელება. არსებული სერვისების კრიტიკულობიდან გამომდინარე, მიგრაციის სამუშაოები წინასწარ უნდა იყოს შეთანხმებული ბანკის IT სამსახურთან, ხოლო მიგრაციის სამუშაოები უნდა განხორციელდეს ღამის საათებში ან ისეთ დროს, რომ შეფერხებები იყოს მინიმიზირებული;
3. შემოთავაზებული მოწყობილობები უნდა გაიმართოს მონაცემთა დამუშავების ორ ცენტრში. ქსელის რედიზაინში პირობითად მოიაზრება ძირითად და სარეზერვო დატაცენტრებს/ოფისებს შორის active/active ტოპოლოგიის გაკეთება (ფაირვოლები იმუშავებენ failover რეჟიმში). სერვერები უნდა შეერთდეს სპეციალურად ამ ფუნქციისთვის გამოყოფილ სვიჩებზე. ძირითადი და სარეზერვო დატაცენტრების/ოფისების გადაბმაში მოიაზრება 10G DWDM მულტიპლექსორები, რომლებზეც შეერთდება ქსელის მოდულები - ქორი, დატაცენტრი, მომხმარებელთა დისტრიბუციის დონის აპარატურა. აპარატურის აფგრეიდი გულისხმობს ქორ სვიჩებს (სტეკირების მხარდაჭერით), დატაცენტრის სვიჩებს სერვერებისთვის (10G და VPC/MLAG მხარდაჭერით), პერიმეტრის და შიდა დატაცენტრის ფაირვოლებს, რომელთაც ექნებათ სრული თავსებადობა ორგანიზაციის ქსელში გამოყენებულ პროტოკოლებთან და ტექნოლოგიებთან. შემოთავაზებულ DWDM მულტიპლექსორებს უნდა ჰქონდეთ სრული თავსებადობა ქსელის დანარჩენ კომპონენტებთან. შესასრულებელ სამუშაოებში შედის ქსელის კონფიგურაცია, რათა მიღწეულ იქნას High availability-ის საჭირო დონე დატაცენტრებს/ოფისებს შორის და ინტეგრაციის სქემამ უნდა უზრუნველყოს მონაცემთა დამუშავების ცენტრებს შორის მაღალი მდგრადობისა და მაღალი მიწვდომადობის ურთიერთშეერთება და მათ შორის გადართვის ავტომატიზაციის მაღალი ხარისხი, ასევე ე.წ vMotion მხარდაჭერა მონაცემთა დამუშავების ცენტრებს შორის. განსაკუთრებით აღსანიშნავია, რომ უნდა მოხდეს არსებული Cisco ASA ფაირვოლების მიგრაცია/კონფიგურაციის გადატანა ახალ NG ფაირვოლებზე. ამასთანავე, პერიმეტრის ფაირვოლებზე უნდა ამოქმედდეს IPS ფუნქციონალი;
4. ინტეგრაციამ უნდა გაითვალისწინოს არსებული ქსელური მოწყობილობების რეკონფიგურაცია რათა მიღწეული იქნეს საჭირო შეერთებები და საიმედოობა;
5. BGP ოქმის საშუალებით ტრაფიკის დიტრიბუციის ოპტიმალური სქემის შემუშავება/ ინტერნეტთან საიმედო შეერთების გამართვა;
6. NRFU (Network Ready For Use Test) ტესტირების გეგმის შემუშავება და განხორციელება ხარვეზების გამოსავლენად და ასეთების არსებობის შემთხვევაში მათი აღმოფხვრა;