დანართი 2

# ბრანდმაუერი(NGFW) - 2 (ორი) ცალი

მოთხოვნები ბრანდმაუერის მიმართ:

1. მოთხოვნები პლატფორმის მიმართ:
   1. მულტი სერვისული არქიტექტურის მხარდაჭერა. ერთი შასის ფარგლებში შესაძლებელი უნდა იყოს სხვადასხვა სერვისების გაშვება, არანაკლებ NGFW, NGIPS, DDoS Appliance;
   2. შესაძლებელი უნდა იყოს წარმადობის გაზრდის მიზნით დამატებითი შასის დამატება და კლასტერიზაციის გამართვა;
   3. სტანდარტულ 19“ ინჩიან სატელეკომუნიკაციო კარადაში, მონტაჟის მხარდაჭედა;
   4. ბრანდმაუერს უნდა შეეძლოს აგრეგირებული ინტერფეისების გამართვა, როგორც LACP ოქმის საშუალებით ასევე სტატიკურად;
   5. ბრანდმაუერის პლატფორმა აღჭურვილი უნდა იყოს არანაკლებ 16(თექვსმეტი) x 1/10გბ/წმ SFP+ ტიპის პორტით;
   6. კვება დუბლირებული, AC ტიპის;
   7. არაუმეტეს 1 RU ზომის;
2. მოთხოვნები მოდულის მიმართ NGFW რეჟიმში:
   1. მაქსიმალური გამტარობა NGFW ფუნქციონალით არანაკლებ: 26გბ/წმ (1024 ბაიტიანი HTTP პაკეტების პროფილი)
   2. მაქსიმალური გამტარობა NGFW+NGIPS ფუნქციონალით არანაკლებ: 25გბ/წმ (1024 ბაიტიანი HTTP პაკეტების პროფილი)
   3. NGFW ერთდროული სესიების რაოდენობა, არანაკლებ: 15 მილიონი
   4. NGFW ახალი სესიები წამში, არანაკლებ: 200 000
   5. TLS დეშიფრაციის მხარდაჭერა აპარატურულ დონეზე. წარმადობა არანაკლებ 6 გბ/წმ
   6. IPSec წარმადობა, არანაკლებ 7 გბ/წმ (1024 ბაიტიანი პაკეტების ტრაფიკის პროფილი);
   7. არანაკლებ 15 000 ერთდროული VPN სესიის მხარდაჭერა;
   8. არანაკლებ: 1024(ათას ოცდაოთხი) Vlan ინტერფეისის მხარდაჭერა;
   9. ბრანდმაუერს უნდა გააჩნდეს ე.წ Active/Active კლასტერიზაციის მხარდაჭერა:
      1. კლასტერი უნდა უზრუნველყოფდეს წარმადობის მასშტაბირებას;
      2. კლასტერის წარმადობა უნდა შეადგენდეს, მასში შემავალი ბრანდმაუერების ჯამური წარმადობის არანაკლებ 90%, UDP ქსელური ნაკადების პროფილით;
      3. ერთ კლასტერში არანაკლებ 6 შასის მხარდაჭერა;
      4. კლასტერს უნდა გააჩნდეს გეოგრაფიულად დაშორებულ ბრანდმაუერებს შორის მოშაობის შესაძლებლობა. არანაკლებ 20ms ე.წ RTT დაყოვნებით დაშორებული ბრანდმაუერების მხარდაჭერა;
      5. კლასტერს უნდა გააჩნდეს ცენტრალიზირებული მართვის მხარდაჭერა;
      6. კლასტერის წევრ ბრანდმაუერებს შორის უნდა მიმდინარეობდეს ქსელური ნაკადების ინფორმაციის სინქრონიზაცია;
      7. კლასტერს უნდა გააჩნდეს ე.წ Transperent რეჟიმში მომუშავე ბრანდმაუერების მხარდაჭერა;
      8. კლასტერს უნდა გააჩნდეს ე.წ Routed რეჟიმში მომუშავე ბრანდმაუერების მხარდაჭერა;
      9. ტრაფიკის ბალანსირება კლასტერში შემავალ ბრანდმაუერებს შორის არ უნდა საჭიროებდეს დამატებითი პროგრამული და/ან აპარატურული კომპონენტის შემოღებას ქსელში;
      10. ტრაფიკის ბალანსირება კლასტერში შემავალ ბრანდმაუერებს შორის, უნდა მიმდინარეობდეს ავტომატურ რეჟიმში ქსელურის კომუტატორის მხრიდან, ინდივიდუალურად თითოეული ნაკადისთვის;
      11. ტრაფიკის ბალანსირება კლასტერში შემავალ ბრანდმაუერებს შორის, არ უნდა იწვევდეს თავდაპირველი გასაფილტრი ტრაფიკის ორჯერ ან მეტჯერ კოპირებას;
      12. ე.წ Transperent რეჟიმში მომუშავე ბრანდმაუერებისგან შემდგარი კლასტერი არ უნდა იწვევდეს ქსელში მარყუჟების ფორმირებას. კლასტერის მუშაობა არ უნდა იყოს დამოკიდებული Spanning Tree ტიპის პროტოკოლზე ან მის ნებისმიერ მოდიფიკაციაზე;
      13. შესაძლებელი უნდა იყოს ე.წ Transperent რეჟიმში მომუშავე კლასტერის წევრ ბრანდმაუერებს შორის ტრაფიკის ბალანსირება ავტომატურ რეჟიმში ქსელურის კომუტატორის მხრიდან, ინდივიდუალურად თითოეული ნაკადისთვის. კლასტერი უნდა წარმოადგენდეს ლოგიკურად ერთი ბრანდმაუერის;
      14. კლასტერს უნდა შეეძლოს, მოშორებული მონაცემთა დამუშავების ცენტრებს შორის მუშაობა. ტრაფიკის ფილტრაცია შესაძლებელი უნდა იყოს როგორც მომხმარებლებსა და სერვერებს შორის, ასევე სერვერული ფერმის შიგნით, სერვერებს შორის;
   10. ბრანდმაუერს უნდა გააჩნდეს ვირტუალიზაციის მხარდაჭერა:
       1. ვირტუალიზაციის არქიტექტურა უნდა უზრუნველყოფდეს დამოუკიდებელი პროგრამული უზრუნველყოფის მქონე ლოგიკური ბრანდმაუერების გაშვებას ერთ ფიზიკურ შასიზე;
       2. ვირტუალიზაციის ფარგლებში შესაძლებელი უნდა იყოს, სხვადასხვა ლოგიკური ბრანდმაუერების გაშვება, სხვადასხა პროგრმული უზრუნველყოფის ვერსიით, დამოუკიდებლად გადატვირთვის შესაძლებლობით;
       3. ვირტუალიზაციის ფარგლებში შესაძლებელი უნდა იყოს CPU ბირთვების მკაცრად განსაზღვრა ლოგიკურ ბრანდმაუერებზე;
       4. ვირტუალიზაციის არქიტექტურა საშუალებას უნდა იძლეოდეს, როგორც ცალკეული ფიზიკური ინტერფეისიბის განსაზღვრა მოხდეს ლოგიკურ ბრანდმაუერებზე, ასევე ქვე ინტერფეისების. შესაძლებელი უნდა იყოს ერთი და იგივე ინტერფეისის/ქვეინტერფეისის მიბმა სხვადასხვა ლოგიკურ ბრანდმაუერებზე. ლოგიკურ ბრანდმაუერებს შორის განაწილებული ინტერფეისებს/ქვეინტერფეისებს უნდა გააჩნდეს ე.წ unicast, multicast და broadcast ტიპის ტრაფიკის მხარდაჭერა;
       5. ვირტუალიზაციის ფარგლებში შესაძლებელი უნდა იყოს, ფიზიკური ბრანდმაუერზე არანაკლებ 7( შვიდი) ლოგიკურ ბრანდმაუერის გაშვება;
   11. ბრანდმაუერს უნდა გააჩნდეს პასიური და აქტიური რეჟიმების მხარდაჭერა სხვადასხვა ინტერფეისებზე. ინტერფეისების კონფიგურაცია შესაძლებელი უნდა იყოს Inline, Passive, Transparent/Bridge, Routed რეჟიმებში;
   12. IPS სისტემას უნდა ჰქონდეს თვით სწავლის შესაძლებლობა;
   13. გადაწყვეტილებას უნდა შეეძლოს ფაილების აღმოჩენა და კონტროლი. აღნიშნული ოპერაციების განხორციელება შესაძლებელი უნდა იყოს ფაილების ტიპების, გამოყენებული პროტოკოლისა და ე.წ „ატვირთვა“ „ჩამოტვირთვის“ მიხედვით;
   14. 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;
   15. გადაწყვეტილება უნდა უზრუნველყოფდეს ე.წ IDS/IPS Tuning-ს, ადამიანის მინიმალური ჩარევით (მაგ.: წესების შერჩევის, პოლიტიკების კონფიგურაცია, პოლიტიკების განახლება) აღნიშნული ფუნქციონალი რეალიზებული უნდა იყოს მართვისა და მონიტორინგის სისტემაში, იგი არ უნდა საჭიროებდეს დამატებით პროგრამულ/აპარატურულ კომპონენტებს, რათა არ გართულდეს სისტემის ადმინისტრირება და მონიტორინგი;
   16. 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 ;
   17. გადაწყვეტილებას უნდა შეეძლოს, იმ მომხმარებლებისა და მოწყობილობების კარანტინი ან/და ტრაფიკის ღრმა ინსპექტირება, რომლების ქსელში მუშაობა და ქცევა განსხვავდება ბაზურისგან;
   18. მართვისა და მონიტორინგის სისტემას 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“;
   19. 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. ოპერაციული სისტემა
          2. ოპერაციული სისტემის ვერსია
          3. ქსელური პროტოკოლები IPv4 და IPv6
          4. ქსელური სერვისები FTP, Telnet, HTTP
          5. ღია პორტები, TCP:3123
          6. კლიენტური აპლიკაციები და მათი ტიპები, FireFox - ვებ ბრაუზერი
          7. ვებ აპლიკაციები, Twitter, Gmail
          8. თითოეული აპლიკაციისთვის უნდა იყოს ასახული რისკი და ბიზნეს რელევანტობა
          9. პოტენციური მოწყვლადობები
          10. მიმდინარე მომხმარებელი
          11. მოწყობილობის ტიპი
          12. მოწყობილობაზე გადაცემული ფაილები
       2. გადაწყვეტილებას უნდა შეეძლოს პასიურად განახორციელოს ქსელური სესიებისა და ნაკადების შესახებ, შემდეგი სახის ინფორმაციის შეგროვება:

1.ქსელური ნაკადის დაწყების დრო

2.ქსელური ნაკადის დამთავრების დრო

3.ქმედება ნაკადზე (ბლოკირება, გატარება)

4.ბლოკირების მიზეზი

5.წყაროს მისამართი

6.დანიშნულების მისამართი

7.შემომავალი ზონა

8.გამავალი ზონა

9.წყაროს პორტის მისამართი

10.დანიშნულების პორტის მისამართი

11. აპლიკაციის პროტოკოლი, მაგ HTTP

12.კლიენტური აპლიკაცია, მაგ Firefox

13.კლიენტის ვერსია, მაგ v33

14.ვებ აპლიკაცია, მაგ Gmail

15.აპლიკაციის ვერსია

16.ბიზნეს რელევანტურობა

17.URL მისამართი

18.URL კატეგორია

19.წამოწყების მომხმარებელი

20.IPS მოვლენა

21.გადაცემული ფაილები

22.მოწყობილობა

23.შემომავალი ინტერფეისი

24.გამავალი ინტერფეისი

25.პაკეტების რაოდენობა

26.გადაცემის მოცულობა

* + 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, ქსელში აღმოჩენილ აპლიკაციებს მიუსადაგოს რისკის დონე და ბიზნესის რელევანტობა;
    3. 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;
    4. გადაწყვეტილებას უნდა შეეძლოს პასიურად განახორციელოს ინფორმაციის შეგროვება ქსელური ნაკადების შესახებ, მათ შორის სესიის დაწყებისა და დამთავრების დრო, კომუნიკაციის პორტები, სერვისები, გადაცემული ინფორმაციის მოცულობა;
    5. გადაწყვეტილებას უნდა შეეძლოს პასიურად განახორციელოს მომხმარებლების მაიდენტიფიცირებელი ინფორმაციის შეგროვება. მას უნდა შეეძლოს IP მისამართების მისადეგება მომხმარებლების სახელებზე;
    6. გადაწყვეტილებას უნდა შეეძლოს დაადგინოს თუ როგორ გამოიყენებენ ქსელურ რესურსებს მომხმარებლები, მოწყობილობები და აპლიკაციები;
  1. გადაწყვეტილებას 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;
  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:
  5. Worms
  6. Trojans
  7. Malware
  8. Backdoor attacks
  9. Spy-wares
  10. Port Scans
  11. VoIP attacks
  12. IPv6 attacks
  13. DoS attacks
  14. Buffer overflows
  15. P2P attacks
  16. SQL Injections
  17. Exploit Attacks
  18. Statistical anomalies
  19. Protocol anomalies
  20. Application anomalies
  21. Malformed traffic
  22. Invalid headers
  23. Blended threats
  24. Rate-based threats
  25. TCP segmentation and IP fragmentation
  26. Evasion detection
  27. HTTP პროტოკოლის (5-ფაზიანი) ინსპექტირება:
      1. Request Header
      2. Request Body
      3. Response headers
      4. Response Body
      5. Logging
  28. შეტევების აღმომჩენ ძრავს უნდა შეეძლოს როგორც ცნობილი საფრთხეების, ასევე ახალი, ჯერ უცნობი საფრთხეების აღმოჩენა;
  29. 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;
  30. გადაწყვეტილებას უნდა შეეძლოს ქსელის სხვადასხვა სეგმენტების ტრაფიკის ინსპექტირება სხვადასხვა პოლიტიკებით. ერთ ინტერფეისზე შესაძლებელი უნდა იყოს სხვადასხვა უსაფრთხოების პოლიტიკების გამართვა;
  31. გადაწყვეტილებას უნდა შეეძლოს IPv6 ოქმით მიმდინარე შეტევების აღმოჩენა;
  32. 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;
  33. 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;
  34. 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;
  35. 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;
  36. გადაწყვეტილებას უნდა გააჩნდეს NAT ფუნქციონალის მხარდაჭერა;
  37. გადაწყვეტილებას უნდა გააჩნდეს სტატიკური და დინამიური მარშუტიზაციისმხარდაჭერა. შემდეგი დინამიური მარშუტიზაციის ოქმების მხარდაჭერა:

1. OSPFv2, NSF
2. OSPFv3, OSPF Gratefull Restart RFC 5187
3. BGP
4. გადაწყვეტილებას უნდა გააჩნდეს აპლიკაციების კონტროლის მოქნილი მექანიზმები. სისტემაში უნდა არსებობდეს აპლიკაციების კატეგორირების რამოდენიმე სქემა, მათ შორის:
5. აპლიკაციები დანიშნულების მიხედვით(თამაშის, ე.წ P2P, anonymizer/proxy, VPN/Tunnel და ა.შ)
6. აპლიკაციები ტიპის მიხედვით (კლიენტური, სერვერული, ვებ)
7. აპლიკაციები ბიზნეს რელევანტობის მიხედვით
8. აპლიკაციები უსაფრთხოების რისკის მიხედვით
9. სისტემის ადმინისტრატორს სურვილისამებრ უნდა შეეძლოს ახალი აპლიკაციის აღმომჩენი წესების შექმნა.
10. მომავალში მხოლოდ პროგრამული ლიცენზიის დამატებით, გადაწყვეტილებას უნდა გააჩნდეს URL ფილტრაციის შესაძლებლობა. სისტემაში უნდა არსებობდეს არანაკლებ 80(ოთხმოცი) URL კატეგორია. ასევე ხელმისაწვდომი უნდა იყოს URL კატეგორიები რისკებისა და რეპუტაციების მიხედვით. ფილტრაციის განხორციელება შესაძლებელი უნდა იყოს კატეგორიისა და მისი რეპუტაციის დონის მიხედვით;
11. მომავალში მხოლოდ პროგრამული ლიცენზიის დამატებით, გადაწყვეტილებას უნდა გააჩნდეს უცნობი ბოროტმოქმედი პროგრამული უზრუნველყოფის ე.წ APT აღმოჩენის შესაძლებლობა. აღნიშნული ფუნქციონალის დამატება არ უნდა საჭიროებდეს დამატებითი აპარატურული საშუალების დამატებას რათა არ გართულდეს სისტემის ადმინისტრირება და მონიტორინგი.
12. გადაწყვეტილებას უნდა შეეძლოს ბოროტქმედი პროგრამული უზრუნველყოფით ინფიცირებული ფაილების აღმოჩენა და ბლოკირება.
13. გადაწყვეტილებას უნდა შეეძლოს, ბოროტქმედი პროგრამული უზრუნველყოფით ინფიცირებული ფაილების აღმოჩენა და ბლოკირება, რომლებიც ცდილობენ განახორციელონ უკუკავშირი ე.წ “C&C” სერვერებთან
14. ბოროტქმედი პროგრამული უზრუნველყოფით ინფიცირებული ფაილების განსაზღვრისთვის გადაწყვეტილება უნდა იყენებდეს ე.წ „cloud” სისტემას. უცნობი ფაილების ანალიზი შესაძლებელი უნდა იყოს ე.წ „sandbox“გარემოში
15. „cloud” სისტემა უნდა ახორციელებდეს ფაილების ანალიზსა და მონიტორინგს. მათ შორის იმ ფაილების, რომელთა თავდაპირველი ქსელში მოხვედრისას განხორციელებულმა ანალიზმა არ დაადგინა ფაილში საფრთხე. გადაწყვეტილებას უნდა შეეძლოს შეტყობინების გენერაცია იმ შემთხვევაში თუ ფაილის თავდაპირველი მნიშვნელობა შეიცვალა. მაგალითად, თავდაპირველად ფაილის ანალიზისას, არ დაადგინა საფრთხე, 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;
16. გადაწყვეტილებას უნდა შეეძლოს ქსელში გადაცემული ფაილების რუქის შედგენა;
17. გადაწყვეტილებას უნდა შეეძლოს ბოროტქმები პროგრამული უზრუნველყოს ქსელში გავრცელების რუქის შედგენა;
18. 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;
19. 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;
20. მომავალშ მხოლოდ პროგრამული ლიცენზიის დამატების საშეალებით, ბრანდმაუერის შასის შიგნით შესაძლებელი უნდა იყოს DDoS შეტევების მოგერიების გადაწყვეტილების გაშვება:
    * + 1. DDoS შეტევების გადაწყვეტილება უნდა იყოს სპეციალიზირებული, DDoS შეტევების მოსაგერიებლად პოზიციონირებული;
        2. NGFW/NGIPS და DDoS გადაწყვეტილების გაშვება შესაძლებელი უნდა იყოს ერთდროულად;
        3. ბრანდმაუერის შასის უნდა გააჩნდეს ე.წ Service Chaining ის შესაძლებლობა, ქსელური ნაკადების გადამისამართება ჯერ უნდა მოხდეს DDoS გადაწყვეტილებაზე ხოლო შემდეგ NGFW/NGIPS სერვისზე;
        4. IPv4 და IPv6 ოქმების მხარდაჭერა;
        5. მულტივექტორული DDoS შეტევების მოგერიება;
        6. IP პაკეტების დეფრაგმენტაციის შესაძლებლობა;
        7. გადაწყვეტილება საშუალებას უნდა იძლეოდეს ახალი DDoS პოლიტიკების ფორმირების და მათი ოპერატიული ცვლილების;
        8. სპეციალიზირებულ DDoS გადაწყვეტილებას უნდა გააჩნდეს შემდეგი ტიპის შეტევების მოგერიების მხარდაჭერა: SYN flood, Network DDoS, IP floods, ICMP floods, TCP floods, UDP floods and IGMP floods, Application DDoS, HTTP floods, DNS query flood, Anomalous flood, nonstandard და malformed packet;
        9. HTTP აუტენტიფიკაციის მხარდაჭერის შესაძლებლობა ე.წ challenge response და 302 Redirect, JAVA;
        10. DNS ტრაფიკის აუნტენტიფიკაციის შესაძლებლობა;
        11. TCP სესიის ლიგიტიმურობის დადგენის შესაძლებლობა Out-of-State Flood Attack Protection;
        12. ქსელური ნაკადების ქცევის ანალიზის საფუძველზე, გადაწყვეტილებას უნდა შეეძლოს ავტომატურად მოახდინოს DDoS შეტევების მოსაგერიებილი სიგნატურების დინამიური ფორმირება;
        13. გადაწყვეტილებას უნდა შეეძლოს, აპლიკაციებზე არაკორექტული მამართვების შემოწმება;
        14. გადაწყვეტილებას უნდა შეეძლოს ვერტიკალური და ჰორიზონდალური პორტების სკანირებისგან დაცვა;
        15. გადაწყვეტილაბას უნდა შეეძლოს დაცვა HTTP, SIP და SMTP აპლიკაციების სკანირებისგან;
        16. გადაწყვეტილებას უნდა შეეძლოს შემდეგი HTTP, DNS, FTP, LDAP, MSSQL, MySQL, POP3, SIP, SMTP, telnet, ssh, NTP, Oracle DB და Postgresql აპლიკაციებისა და სერვისებისთვის დაცვა ე.წ Brute Force ტიპის შეტევებისგან;
        17. გადაწყვეტილებას უნდა შეეძლოს, ბოროტქმედი აპლიკაციების გავრცელების აღკვეთა;
        18. გადაწყვეტილებას უნდა შეეძლოს ე.წ Zero Day შეტევების მოგიება;
21. გადაწყვეტილებას უნდა მოყვებოდეს 7 (შვიდი) ცალი ლოგიკური ბრანდმაუერის მხარდაჭერა;
22. დამატებითი მოთხოვნები:
    * + 1. ბრანდამაუერს უნდა მოყვებოდეს 3(სამ) წლიანი ლიცენზია Intrusion Prevention System სიგნატურების განახლებისთვის;
        2. ბრანდამაუერზე უნდა ვრცელდებოდეს მწარმოებლის 3 წლიანი გარანტია და პროგრამული უზრუნველყოფის განახლების სერვისი. დაზიანების შემთხვევაში მოწყობილობა უნდა შეიცვალოს ან შეკეთდეს დაზიანების მიზეზის დადგენიდან მომდევნო სამუშაო დღეს.
23. **მომწოდებელმა უნდა წარმოადგინოს მწარმოებლის ავტორიზაციის წერილი (Manufacturers Authorization Form),**

# მართვისა და მონიტორინგის სისტემა - 1 (ერთი) ცალი

1. მართვისა და მონიტორინგის სისტემიდან შესაძლებელი უნდა იყოს მოთხოვნილი NGFW ბრანდმაუერების მართვა;
2. მართვისა და მონიტორინგის სიტემის მართვა შესაძლებელი უნდა იყოს ვებ ბრაუზერიდან;
3. მართვისა და მონიტორინგის სისტემა უნდა წარმოადგენდეს მზა ე.წ ‘Virtual Appliance’ გადაწყვეტილებას;
4. მართვისა და მონიტორინგის სისტემის გამართვა შესაძლებელი უნდა იყოს VMware გარემოში;
5. გადაწყვეტილებას უნდა ჰქონდეს User Intelligence რეპორტები;
6. ქსელის ტრაფიკი უნდა იყოს მიბმული მომხმარებლის ობიექტზე და მასთან ასოცირებულ მოწყობილობებზე (კომპიუტერი, მობილური და ა.შ.) შემდეგი შესაძლებლობებით:
   * + 1. Workstations login events (including RDP, Telnet and SSH sessions)
       2. User application traffic statistics (application type, traffic volume, source and destination)
       3. User-details associated with the particular network traffic
       4. User-details associated with the particular network object (workstation)
7. შესაძლებელი უნდა იყოს NGFW პოლიტიკების კონფიგურაცია მონიტორინგი და მართვა. წესებისა და სიგნატურების კონფიგურაცია;
8. სისტემას უნდა გააჩნდეს კოორელაციის წესების შექმნის საშუალება უსაფრთხოების მოვლენების მიხედვით. კოორელაციის წესში განსაზღვრული უსაფრთხოების მოვლენის აკტივაციის შემთხვევაში სისტემას უნდა შეეძლოს შემდეგი ამოცანების შესრულება:
9. მართვისა და მონიტორინგის სისტემას უნდა შეეძლოს არანაკლებ 10(ათი) ბრანდმუერის მართვის შესაძლებლობა;
10. იგივე მწარმოებლის რაც ბრანდმაუერი;
11. დამატებითი მოთხოვნები:
    * + 1. მართვისა და მონიტორინგის სისტემაზე უნდა ვრცელდებოდეს მწარმოებლის 3 წლიანი გარანტია და პროგრამული უზრუნველყოფის განახლების სერვისი. დაზიანების შემთხვევაში მოწყობილობა უნდა შეიცვალოს ან შეკეთდეს დაზიანების მიზეზის დადგენიდან მომდევნო სამუშაო დღეს.
12. **მომწოდებელმა უნდა წარმოადგინოს მწარმოებლის ავტორიზაციის წერილი (Manufacturers Authorization Form),**

# კომუტატორი- 2(ორი) ცალი

კომუტატორს უნდა გააჩნდეს შემდეგი ტექნიკური მახასიათებლები:

1. კომუტატორის წარმადობა: არანაკლებ 2 ტბ/წმ, 1 მილიარდი პაკეტი წამში;
2. არანაკლებ 24 (ოცდაოთხი) 1/10/25გბ/წმ წარმადობის SFP+ ფორმ ფაქტორის ინტერფეისის მხარდაჭერა და 4(ოთხი) x 40/100გბ/წმ QSFP ინტერფეისის მხარდაჭერა;
3. კომუტატორს უნდა გააჩნდეს არანაკლებ 80 000 MAC მისამართის მხარდაჭერა;
4. კომუტატორს უნდა გააჩნდეს არანაკლებ 200 000 IPv4 Unicast მარშრუტის მხარდაჭერა;
5. კომუტატორს უნდა გააჩნდეს არანაკლებ 30 000 IPv4 Multicast მარშრუტის მხარდაჭერა;
6. კომუტატორს უნდა გააჩნდეს არანაკლებ 200 000 IPv6 Unicast მარშრუტის მხარდაჭერა;
7. კომუტატორს უნდა გააჩნდეს არანაკლებ 30 000 IPv6 Multicast მარშრუტის მხარდაჭერა;
8. კომუტატორს უნდა გააჩნდეს არანაკლებ 15 000 QoS წვდომის სიების მხარდაჭერა;
9. კომუტატორს უნდა გააჩნდეს არანაკლებ 25 000 უსაფრთხოების წვდომის სიის მხარდაჭერა;
10. ქსელური ნაკადების აღმრიცხველის შესაძლებლობა, არანაკლებ 96 000 ჩანაწერი;
11. RAM ტიპი მეხსიერება: არანაკლებ 16 გბ;
12. Flash ტიპის მეხსიერება: არანაკლებ 16 გბ;
13. გადაწყვეტილებას უნდა გააჩნდეს MACSec ტექნოლოგიის მხარდაჭერა ყველა პორტზე. 256 და 128 ბიტიანი გასაღებით;
14. გადაწყვეტილებას უნდა გააჩნდეს შემდეგი ტექნოლოგიების მხარდაჭერა: BGP, OSPF, RIP, NSF, MPLS, PIM-SM, PIM-SSM, VXLAN, VRF, mVPN, RSPAN, SPAN, NETCONF, YANG, Python;
15. დამატებითი მოთხოვნები:
    * + 1. კომუტატორზე უნდა ვრცელდებოდეს მწარმოებლის 3 წლიანი გარანტია და პროგრამული უზრუნველყოფის განახლების სერვისი. დაზიანების შემთხვევაში მოწყობილობა უნდა შეიცვალოს ან შეკეთდეს დაზიანების მიზეზის დადგენიდან მომდევნო სამუშაო დღეს.
16. **მომწოდებელმა უნდა წარმოადგინოს მწარმოებლის ავტორიზაციის წერილი (Manufacturers Authorization Form),**

1. ტრანსივერი A ტიპის 100(ასი) ცალი
2. ფორმ ფაქტორი: SFP+;
3. წარმადობა: 10გბ/წმ;
4. კონექტორი: Dual LC;
5. მანძილი არანაკლებ 400(ოთხასი) მეტრი;
6. თავსებადი MM ტიპის ოპტიკურ ბოჩკოვან კაბელთან;
7. სრულად თავსებადი 1 პუნქტში მოთხოვნილ ბრანდმაუერთან;
8. ტრანსივერი B ტიპის 16(თექვსმეტი) ცალი
9. ფორმ ფაქტორი: SFP;
10. წარმადობა: 1გბ/წმ;
11. კონექტორი: Rj-45;
12. სრულად თავსებადი 1 პუნქტში მოთხოვნილ ბრანდმაუერთან;
13. სრულად თავსებადი 3 პუნქტში მოთხოვნილ კომუტატორთან;
14. ტრანსივერი C ტიპის 18(თვრამეტი) ცალი
15. ფორმ ფაქტორი: SFP;
16. წარმადობა: 1გბ/წმ;
17. კონექტორი: Dual LC;
18. მანძილი არანაკლებ 10 კილომეტრი;
19. თავსებადი SM ტიპის ოპტიკურ ბოჩკოვან კაბელთან;
20. სრულად თავსებადი 3 პუნქტში მოთხოვნილ კომუტატორთან;
21. ტრანსივერი E ტიპის 8(რვა) ცალი
22. ფორმ ფაქტორი: SFP+;
23. წარმადობა: 10გბ/წმ;
24. კონექტორი: Dual LC;
25. მანძილი არანაკლებ 10 კილომეტრი;
26. თავსებადი SM ტიპის ოპტიკურ ბოჩკოვან კაბელთან;
27. სრულად თავსებადი 3 პუნქტში მოთხოვნილ კომუტატორთან;
28. ტრანსივერი F ტიპის 2(ორი) ცალი
29. ფორმ ფაქტორი: SFP+;
30. წარმადობა: 10გბ/წმ;
31. ტიპი: upstream;
32. მანძილი არანაკლებ 40 კილომეტრი;
33. თავსებადი ე.წ single fiber SM ტიპის ოპტიკურ ბოჩკოვან კაბელთან;
34. სრულად თავსებადი 3 პუნქტში მოთხოვნილ კომუტატორთან;
35. ტრანსივერი G ტიპის 2(ორი) ცალი
36. ფორმ ფაქტორი: SFP+;
37. წარმადობა: 10გბ/წმ;
38. ტიპი: downstream;
39. მანძილი არანაკლებ 40 კილომეტრი;
40. თავსებადი ე.წ single fiber SM ტიპის ოპტიკურ ბოჩკოვან კაბელთან;
41. სრულად თავსებადი 3 პუნქტში მოთხოვნილ კომუტატორთან;
42. ოპტიკური პაჩკორდი A ტიპის 32(ოცდათორმეტი) ცალი
43. სიგრძე: არანაკლებ 1 მეტრი
44. კონექტორი: Dual LC
45. ტიპი: Fiber Multi Mode
46. ოპტიკური პაჩკორდი B ტიპის 20 (ოცი) ცალი
47. სიგრძე: არანაკლებ 2 მეტრი
48. კონექტორი: Dual LC
49. ტიპი: Fiber Multi Mode
50. ოპტიკური პაჩკორდი C ტიპის 20 (ოცი) ცალი
51. სიგრძე: არანაკლებ 10 მეტრი
52. კონექტორი: Dual LC
53. ტიპი: Fiber Multi Mode
54. ოპტიკური პაჩკორდი D ტიპის 12 (თორმეტი) ცალი
55. სიგრძე: არანაკლებ 15 მეტრი
56. კონექტორი: Dual LC
57. ტიპი: Fiber Multi Mode
58. ოპტიკური პაჩკორდი E ტიპის 12 (თორმეტი) ცალი
59. სიგრძე: არანაკლებ 15 მეტრი
60. კონექტორი: Dual LC
61. ტიპი: Fiber Single Mode
62. FTP CAT6 პაჩკორდი F ტიპის 20 (ოცი) ცალი
63. სიგრძე: არანაკლებ 1 მეტრი
64. კონექტორი: Rj45
65. FTP CAT6 პაჩკორდი G ტიპის 20 (ოცი) ცალი
66. სიგრძე: არანაკლებ 2 მეტრი
67. კონექტორი: Rj45
68. FTP CAT6 პაჩკორდი H ტიპის 20 (ოცი) ცალი
69. სიგრძე: არანაკლებ 10 მეტრი
70. კონექტორი: Rj45
71. FTP CAT6 პაჩკორდი I ტიპის 12 (თორმეტი) ცალი
72. სიგრძე: არანაკლებ 15 მეტრი
73. კონექტორი: Rj45

დამატებითი მოთხოვნები

1. მიმწოდებელ კომპანიამ უნდა განახორციელოს შემოთავაზებული გადაწყვეტილების ინტეგრაცია;
2. პრეტენდენტმა უნდა წარმოადგინოს ინფორმაცია მის მიერ შემოთავაზებული მწარმოებლის ბრანდმაუერის დანერგვის არანაკლებ 3 (სამი) პროექტის შესახებ, გამოცდილების დამადასტურებელი ინფორმაცია წარმოდგენილ უნდა იქნას ხელშეკრულებებით და წარმოდგენილი ხელშეკრულებების შესაბამისი მიღება-ჩაბარებებით ან/და საგადასახადო ანგარიშ-ფაქტურებით. იმ შემთხვევაში, თუ მოთხოვნილი დოკუმენტაცია ატვირთულია სახელმწიფო შესყიდვების ერთიან ელექტრონულ სისტემაში პრეტენდენტს შეუძლია გამოცდილების შესახებ წარმოადგინოს შესაბამისი SPA ან/და NAT ან/და CMR ნომრები და არ წარმოადგინოს მოთხოვნილი დოკუმენტაცია.
3. 1, 2 და 3 პუნქტებში მოცემული კომპონენტები უნდა იყოს ერთი და იგივე მწარმოებლის;
4. მოწოდებული საქონელი (მისი ყველა კომპონენტი) უნდა იყოს ახალი (არ უნდა იყოს მეორადი გამოყენების);
5. პრეტენდენტმა უნდა წარმოადგინოს მწარმოებლის ავტორიზაციის წერილი (MAF), რომელიც დაადასტურებს შემოთავაზებული საქონლის გაყიდვის ავტორიზაციას, მითითებული იქნება პრეტენდენტის დასახელება და წინამდებარე ტენდერის უნიკალური ნომერი.