ტექნიკური დავალება

1. NGFW ტიპის ბრანდმაუერი 3 (სამი) ცალი

ბრანდმაუერს უნდა გააჩნდეს შემდეგი ტექნიკური მახასიათებლები:

1. ბრანდმაუერის მაქსიმალური წარმადობა: არანაკლებ 5.5 გბ/წმ
2. ერთდროული სესიების რაოდენობა: არანაკლებ 3 მილიონი
3. კავშირების დამყარების სისწრაფე: არანაკლებ 43 000 კავშირი/წამში
4. VLAN ების მაქსიმალური რაოდენობა: არანაკლებ 1024
5. ინტერფეისების რაოდენობა: არანაკლებ 12(თორმეტი) 10/100/1000 მბ/წმ Ethernet ინტერფეისი (RJ-45 ტიპის) და 4 (ოთხი) 10 გბ/წმ ინტერფეისი(SFP+ ტიპის). დამატებით 1(ერთი) 1გბ/წმ წარმადობის მენეჯმენტ პორტი.
6. დამატებითი ქსელური მოდულების საშუალებით პორტების რაოდენობა უნდა გაიზარდოს არანაკლებ 8 (რვა) 10გბ/წმ ინტერფეისით (SFP+ ტიპის)
7. Application Visibility and Control აპლიკაციების მხარდაჭერა: არანაკლებ 4000
8. მაღალი მდგრადობის მხარდაჭერა: Active/Standby
9. ბრანდმაუერს უნდა გააჩნდეს შემდეგი ტექნოლოგიებისა და ოქმების მხარდაჭერა: SSH, SNMP, RADIUS, NAT, IPsec, IKEv2, OSPFv2, OSPFv3, OSPF Gratefull Restart RFC 5187, BGP, OSPFv2, NSF
10. ბრანდმაუერს უნდა შეეძლოს ქსელის ტოპოლოგიის აღმოჩენა
11. IPS სისტემას უნდა ჰქონდეს თვით სწავლის შესაძლებლობა
12. გადაწყვეტილებას უნდა შეეძლოს ფაილების აღმოჩენა და კონტროლი. აღნიშნული ოპერაციების განხორციელება შესაძლებელი უნდა იყოს ფაილების ტიპების, გამოყენებული პროტოკოლისა და ე.წ „ატვირთვა“ „ჩამოტვირთვის“ მიხედვით;
13. 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;
14. გადაწყვეტილება უნდა უზრუნველყოფდეს IDS/IPS სიგნატურების მორგებას ე.წ 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;
15. 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 ;

    1. გადაწყვეტილებას უნდა შეეძლოს, იმ მომხმარებლებისა და მოწყობილობების კარანტინი ან/და ტრაფიკის ღრმა ინსპექტირება, რომლების ქსელში მუშაობა და ქცევა განსხვავდება ბაზურისგან;

    2. 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“;

    3. 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 სისტემები და მათი ვერსიები
    2. გამოყენებული პროტოკოლები IPv6, IPv4
    3. აქტიური სერვისები HTTPS, SSH
    4. ღია პორტები, მაგალითად TCP 443
    5. დაინსტალირეუბლი, კლიენტური აპლიკაციები
    6. გამოყენებული ვებ აპლიკაციები
    7. თითოეული აპლიკაციისთვის უნდა იქნეს მისადაგებული რისკი და ბიზნეს რელევანტურობა
    8. მოწყობილობაზე არსებული სისუსტეები ე.წ vulnerabilities
    9. მოწყობილობაზე აქტიური მომხმარებელი
    10. მოწყობილობის ტიპი
    11. მოწყობილობაზე გადაგზავნილი ფაილები
2. გადაწყვეტილებას უნდა შეეძლოს პასიურად განახორციელოს ქსელური სესიებისა და ნაკადების შესახებ შემდეგი სახის ინფორმაციის შეგროვება:
    1. ნაკადის დაწყების და დამთავრების დრო
    2. ნაკადზე განხორციელებული ქმედება, ბლოკირება ან ნების დართვა
    3. ნაკადის ბლოკირების მიზეზე
    4. საწყისის და დანიშნულების IP მისამართები
    5. შემომავალი და გამავალი ზონების სახელები
    6. საწყისის და დანიშნულების პორტის მისამართები
    7. აპლიკაციის პროტოკოლი
    8. კლიენტის აპლიკაცია და მისი ვერსია
    9. ვებ აპლიკაცია
    10. აპლიკაციის რისკი და ბიზნეს რელევანტურობა
    11. URL მისამართი და მისი კატეგორია
    12. ნაკადის ინიციატორი მომხმარებელი
    13. დაფიქსირებული IPS მოვლენა
    14. ნაკადის ფარგლებში გადაცემული ფაილები
    15. შემომავალი და გამავალი ინტერფეისები
    16. გადაცემული პაკეტების რაოდენობა
    17. გადაცემული მონაცემების მოცულობა
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, ქსელში აღმოჩენილ აპლიკაციებს მიუსადაგოს რისკის დონე და ბიზნესის რელევანტობა;
5. 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;
6. გადაწყვეტილებას უნდა შეეძლოს პასიურად განახორციელოს ინფორმაციის შეგროვება ქსელური ნაკადების შესახებ, მათ შორის სესიის დაწყებისა და დამთავრების დრო, კომუნიკაციის პორტები, სერვისები, გადაცემული ინფორმაციის მოცულობა;
7. გადაწყვეტილებას უნდა შეეძლოს პასიურად განახორციელოს მომხმარებლების მაიდენტიფიცირებელი ინფორმაციის შეგროვება. მას უნდა შეეძლოს IP მისამართების მისადაგება მომხმარებლების სახელებზე;
8. გადაწყვეტილებას უნდა შეეძლოს დაადგინოს თუ როგორ გამოიყენებენ ქსელურ რესურსებს მომხმარებლები, მოწყობილობები და აპლიკაციები;

4. გადაწყვეტილებას უნდა გააჩნდეს უსაფრთხოების ინციდენტებზე ავტომატური საპასუხო ქმედებების გაშვების მექანიზმი. მათ შორის ბრანდმაუერებთან და მარშრუტიზატორებთან 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;

5. აღმოჩენის წესები უნდა ეფუძნებოდეს გაფართოებად ღია სტანდარტს, რომლის მეშვეობითაც მომხმარებელს უნდა შეეძლოს როგორც მწარმოებლის მიერ შემუშავებული წესების მოდიფიცირება ასევე ახალი, მისთვის სასურველი წესების შექმნა;

6. სისტემას უნდა ჰქონდეს შესაძლებლობა მოახდინოს ტრაფიკის ინსპექტირება ქცევის მიხედვით, მათ შორის:
   1. Worms, Trojans, Malware, Backdoor, Spy-wares, DoS, Buffer overflows, P2P, SQL Injections, Exploit, Blended, Rate-based ტიპის შეთევები
   2. პორტის სკანირება
   3. VoIP შეტევები
   4. შეტევები IPv6 ქომზე
   5. სტატისტიკური, პროტოკოლის და აპლიკაციების ანომალიები
   6. მოდიფიცირებული ტრაფიკი
   7. დამახინჯებული თავსართები
   8. Evasion აღმოჩენის შესაძლებლობა

7. HTTP პროტოკოლის (5-ფაზიანი) ინსპექტირება:
   1.მოთხოვნის თავსართი ე.წ Header
   2.მოთხოვნის ძირითადი ნაწილი ე.წ Body
   3.პასუხის თავსართი ე.წ headers
   4.პასუხის ძირითადი ნაწილი ე.წ Body
   5.ლოგირება

8. შეტევების აღმომჩენ ძრავს უნდა გააჩნდეს შეტევების აღმოჩენის რამდენიმე მექანიზმი, მათ შორის ე.წ „exploit" ებზე დაფუძნებული სიგნატურები, სისტემების ე.წ „სისუსტეებზე" დაფუძნებული წესები, ოქმების ანომალიები და ქცევის ანომალიების მიხედვით;

9. გადაწყვეტილებას უნდა შეეძლოს ქსელის სხვადასხვა სეგმენტების ტრაფიკის ინსპექტირება სხვადასხვა პოლიტიკებით. ერთ ინტერფეისზე შესაძლებელი უნდა იყოს სხვადასხვა უსაფრთხოების პოლიტიკების გამართვა;

10. გადაწყვეტილებას უნდა შეეძლოს IPv6 ოქმით მიმდინარე შეტევების აღმოჩენა, ვებ ტრაფიკის და აპლიკაციების ფილტრაცია;

11. 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;

12. 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;

13. გადაწყვეტილებას უნდა შეეძლოს სხვადასხვა მომხმარებლებისთვის ან მათი ჯგუფებისთვის განისაზღვროს სხვადასხვა უსაფრთხოების პოლიტიკები. მომხმარებლების მაიდენტიფიცირებელი ინფორმაციის დადგენა შესაძლებელი უნდა იყოს Active Directory სერვერიდან;

14. 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;

15. 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;

16. გადაწყვეტილებას უნდა გააჩნდეს NAT ფუნქციონალის მხარდაჭერა;

34. გადაწყვეტილებას უნდა გააჩნდეს აპლიკაციების კონტროლის მოქნილი მექანიზმები. სისტემაში უნდა არსებობდეს აპლიკაციების კატეგორირების რამოდენიმე სქემა, მათ შორის:

1. აპლიკაციები დანიშნულების მიხედვით(თამაშის, ე.წ P2P, anonymizer/proxy, VPN/Tunnel და ა.შ)
2. აპლიკაციები ტიპის მიხედვით (კლიენტური, სერვერული, ვებ)
3. აპლიკაციები ბიზნეს რელევანტობის მიხედვით
4. აპლიკაციები უსაფრთხოების რისკის მიხედვით
5. სისტემის ადმინისტრატორს სურვილისამებრ უნდა შეეძლოს ახალი აპლიკაციის აღმომჩენი წესების შექმნა

35. გადაწყვეტილებას უნდა გააჩნდეს ტრაფიკის გადაცემის სისწრაფის შეზღუდვის შესაძლებლობა;

37. მომავალში მხოლოდ პროგრამული ლიცენზიის დამატებით, გადაწყვეტილებას უნდა გააჩნდეს ე.წ APT აღმოჩენის შესაძლებლობა. აღნიშნული ფუნქციონალის დამატება არ უნდა საჭიროებდეს დამატებითი აპარატურული საშუალების დამატებას რათა არ გართულდეს სისტემის ადმინისტრირება და მონიტორინგი.

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 მოხვედრისას განხორციელებულმა ანალიზმა არ დაადგინა ფაილში საფრთხე. გადაწყვეტილებას უნდა შეეძლოს შეტყობინების გენერაცია იმ შემთხვევაში თუ ფაილის თავდაპირველი მდგომარეობა 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;
5. გადაწყვეტილებას უნდა შეეძლოს ქსელში გადაცემული ფაილების რუქის შედგენა;
6. გადაწყვეტილებას უნდა შეეძლოს ბოროტქმედი პროგრამული უზრუნველყოს ქსელში გავრცელების რუქის შედგენა;
7. გადაწყვეტილებას უნდა შეეძლოს ქსელური კომპრომეტირების ინფორმაციისა და ბოროტქმედი პროგრამული უზრუნველყოფით ინფიცირებული განსაზღვრების ინფორმაციის მიმოცვლა ქსელურ და კლიენტურ უსაფრთხოების სისტემებს შორის. ქსელური და კლიენტური უსაფრთხოების სისტემები უნდა იყენებდნენ ერთიან კონსისტენტურ უსაფრთხოების ინფორმაციას;

38. გადაწყვეტილებას უნდა შეეძლოს საფრთხეების კორელაცია ჰოსტების სისუსტეებთან, ქსელის ტოპოლოგიასა და შეტევის კონტექსტთან, რათა უზრუნველყოს უსაფრთხოების ინციდენტების რელევანტობის დადგენა. 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;

39. უსაფრთხოების მოვლენების ანალიზისას, შესაძლებელი უნდა იყოს პაკეტის შიგთავსთან წვდომა;

40. სურვილისამებრ შესაძლებელი უნდა იყოს უსაფრთხოების მოვლენების რეპორტების შექმნა სხვადასხვა ფორმატებში, მათ შორის PDF, HTML, CSV;

41. გარე აუტენტიფიკაციის სიტემებთან ინტეგრაციის შესაძლებლობა RADIUS, LDAP, AD;

42. სისტემას უნდა გააჩნდეს ღია API გარე კომპონენტებთან ინტეგრაციისთვის

43. გადაწყვეტილებას უნდა გააჩნდეს API მხარდაჭერა, რისი საშუალებითაც შესაძლებელი იქნება დამატებითი კონტექსტუალური ინფორმაციის დამატება მოწყობილობის პროფილებზე

44. გადაწყვეტილებას უნდა გააჩნდეს ავტომატური და რეგულარული ე.წ თეთრი და შავი სიების განახლების შესაძლებლობა, რომლებიც ბაზირებულია IP, URL, DNS მისამართებზე. სიების განახლება შესაძლებელი უნდა იყოს როგორ მწარმოებლის სერვისით, ასევე მომხმარებელს უნდა შეეძლოს სიების გარე წყაროებიდან განახლება;

45. გადაწყვეტილებას უნდა გააჩნდეს ე.წ DNS sinkholing მექანიზმის მხარდაჭერა, რომელიც დაფუძნებული იქნება დინამიურ DNS ზე;

16. სისტემას უნდა გააჩნდეს ინტეგრაციის საშუალება იმავე მწარმოებლის საფრთხეების რეაგირების ღრუბლოვან გადაწყვეტილებასთან. საფრთხეების რეაგირების გადაწყვეტილებას უნდა გააჩნდეს ბრანდმაუერისგან გამოგზავნილი შემდეგი მოვლენების დამუშავების საშუალება:
    1. IPS უსაფრთხოების მოვლენები
    2. ინფორმაცია ქსელური ნაკადების შესახებ
    3. ინფორმაცია ფაილის და ე.წ malware მოვლენების შესახებ
17. ზომა: არაუმეტეს 1 RU
18. კვების ტიპი: 100-240V AC ტიპის
19. შემოთავაზებულ ბრანდმაუერს უნდა მოყვებოდეს 2(ორი) ცალი კვების ბლოკი hotswappable ტიპის;
20. ბრანდამაუერს უნდა მოყვებოდეს შესაბამისი სამწლიანი ლიცენზია Intrusion Prevention System (IPS) მხარდაჭერისთვის

2. მოთხოვნები ბრანდმაუერების მართვისა და მონიტორინგის სისტემის მიმართ

1. მართვისა და მონიტორინგის სისტემიდან შესაძლებელი უნდა იყოს მოთხოვნილი NGFW ბრანდმაუერების მართვა. მათ შორის:
    1. გადაწყვეტილებას უნდა ჰქონდეს User Intelligence რეპორტები
    2. 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)
    3. შესაძლებელი უნდა იყოს NGFW პოლიტიკების კონფიგურაცია მონიტორინგი და მართვა. წესებისა და სიგნატურების კონფიგურაცია.
2. სისტემას უნდა გააჩნდეს კორელაციის წესების შექმნის საშუალება უსაფრთხოების მოვლენების მიხედვით. კორელაციის წესში განსაზღვრული უსაფრთხოების მოვლენის აქტივაციის შემთხვევაში სისტემას უნდა შეეძლოს შემდეგი ამოცანების შესრულება:
    a) Alert შეტყობინების გაგზავნა შემდეგი მეთოდებით : Email, Syslog, SNMP (v1,v2,v3)
    b) სკანირება NMAP-ის საშუალებით
    c) IOS Null Route კონფიგურაციის გაგზავნა ქსელურ მოწყობილობაზე
3. ცენტრალიზებული და ადვილად მართვადი მენეჯმენტ პორტალი
4. მომხმარებლის მოთხოვნებზე მორგებადი მართვის პანელი
5. მართვისა და მონიტორინგის სიტემის მართვა შესაძლებელი უნდა იყოს ვებ ბრაუზერიდან
6. მართვისა და მონიტორინგის სისტემა უნდა წარმოადგენდეს მზა ე.წ 'virtual appliance' გადაწყვეტილებას
7. გამოყოფილი მართვისა და მონიტორინგის სისტემის გამართვა შესაძლებელი უნდა იყოს ინფრასტრუქტურაში არსებულ ESXi ვირტუალურ გარემოში
8. **შემოთავაზებული ბრენდმაუერი, მართვისა და მონიტორინგის სისტემა დამზადებული უნდა იყოს ერთი მწარმოებლის მიერ.**

3. ტრანსივერი 6 (ექვსი) ცალი

1. ფორმ ფაქტორი: SFP+;
2. წარმადობა: 10გბ/წმ;
3. კონექტორი: Dual LC;
4. მანძილი არანაკლებ 400 (ოთხასი) მეტრი;
5. თავსებადი MM ტიპის ოპტიკურ ბოჭკოვან კაბელთან;