|  |
| --- |
| **ქსელური ბრანდმაუერი (Firewall) A ტიპის****(3 ერთეული)** |
| **ტექნიკური სპეციფიკაციები** |
| **ინტერფეისების რაოდენობა:*** არანაკლებ 8x 1GE RJ45 ინტერფეისი
* არანაკლებ 1x RJ45 მართვის პორტი
* არანაკლებ 4x 10GE SFP+ ინტერფეისი
* არანაკლებ 1x Console ინტერფეისი
 |
| კვება - hotswappable დუბლირებული 220VAC კვების ბლოკები.  |
| გაგრილების სისტემა-ინტეგრირებული ქულერი. |
| **სამუშაო გარემო:*** ტემპერატურა არანაკლებ 0 - 40 გრადუსი
* ტენიანობა არანაკლებ 20% - 90%
 |
| SSD სანახი ლოგირებისთვის |
| IPv4 Firewall გამტარუნარიანობა - არანაკლებ 15 Gbps (Internet Mix) |
| IPS რეჟიმში გამტარობა - არანაკლებ 2 Gbps (Internet Mix) |
| NGFW რეჟიმში (როდესაც გააქტიურებულია Firewall, IPS და Application controll ფუნქციონალი) გამტარობა - არანაკლებ 2 Gbps (Internet Mix) |
| Threat Protection რეჟიმში (როდესაც გააქტიურებულია Firewall, IPS, Application controll, URL ფილტრაცია და მავნე პროგრამებისგან (Malware) დაცულობა sandbox ფუნქციონალით) გამრატობა - არანაკლებ 2გბ/წმ (Internet Mix) |
| ერთდროული სესიების რაოდენობა - არანაკლებ 1 მილიონი |
| წამში დაგენერირებული ახალი სესიების რაოდენობა - არანაკლებ 50000 სესია |
| SSL ინსპექტირებისას გამტარობა - არანაკლებ 2 Gbps (Internet Mix) |
|  |
| **მაღალმდგრადობა:*** აქტიური/პასიური
* Virtual Router Redundancy Protocol (VRRP)
 |
| **მართვა:*** WEB GUI საშუალებით
* ადმინისტრატორებისა და მომხმარებლების რამდენიმე დონის მხარდაჭერის ფუნქცია
* ცენტრალიზირებული ავტორიზაციის მხარდაჭერა (AD, LDAP, RADIUS)
* ცენტრალური მართვის სისტემის საშუალებით
* ცენტრალურ მართვის სისტემას უნდა შეეძლოს შემოთავაზებული ქსელური ბრანდმაუერის (Firewall)კონფიგურაცია და მონიტორინგი
 |
| ბრანდმაუერის მუშაობის რეჟიმები - NAT და Transparent რეჟიმების მხარდაჭერა |
| **მარშრუტიზაცია:*** სტატიკური მარშრუტების მხარდაჭერა
* დინამიური მარშრუტიზაციის პროტოკოლების მხარდაჭერა: OSPF, BGP, RIP
* Multicast ტრაფიკის მარშრუტიზაცია
* ვირტუალური მარშრუტიზაცია Virtual Routing and Forwarding (VRF) მხარდაჭერა. VRF დომენებს შორის მარშრუტების გაცვლის (Route leaking between VRF) მხარდაჭერა
* Policy Based მარშრუტიზაცია
 |
| **ლოგირება და ანგარიშების გენერირება:** * შესაძლებელი უნდა იყოს ლოკალურად ტრაფიკის live ლოგების ნახვა
* ტრაფიკის და სისტემური ლოგების remote server-ზე გაგზავნა
 |
| **სიჩქარის შეზღუდვა Shaper:*** Shared packet shaper-ი ან per policy / per application სიჩქარის შეზღუდვის პოლიტიკა, სადაც შესაძლებელი უნდა იყოს ტრაფიკის პრიორიტეტის, მინიმუმ გარანტირებული სიჩქარის / მაქსიმალური სიჩქარეების კონფიგურირება
* Per-ip shaper ფუნქციონალი - შესაძლებელი უნდა იყოს უსაფრთხოების პოლიტიკებში მითითებული ქვექსელის თითოეული IP მისამართისთვის (ან მომხმარებლისათვის) ტრაფიკის შეზღუდვა, ისე რომ ერთმა მომხმარებელმა ვერ შეეძლოს მთლიანი ხელმისაწვდომი ტრაფიკის დაკავება. ამავე ფუნქციონალის ფარგლებში შესაძლებელი უნდა იყოს თითოეულ IP მისამართზე მაქსიმალური დასაშვები სიჩქარისა და სესიების რაოდენობის შეზღუდვის დაწესება
 |
| **ვებ ტრაფიკის ფილტრაცია:*** URL ფილტრაცია დომენის სახელის მიხედვით
* ფილტრაცია regular expression მიხედვით
* შესაძლებელი უნდა ოყოს სპეციფიიური URL-ების ან კატეგორიების დაბლოკვა, გამონაკლისის სახით დაშვება და მონიტორინგის რეჟიმში მეთვალყურეობა(ლოგირებით).
* შესაძლებელი უნდა იყოს სპეციფიურ ვებ გვერდებზე წვდომის მცდელობისას შეტყობინების გამოტანა აღნიშნული ვებ გვერდის ჩატვირთვამდე
* ვებ ტრაფიკის ფილტრაციის სერვისს უნდა გააჩნდეს ვებ გვერდების კატეგორიები, რომელთა სისტემატიურ განახლებას უნდა აწარმოებდეს შემოთავაზებული პროდუქტის მწარმოებელი
* შემოთავაზებაში გათვალისწინებული უნდა იყოს ყველა საჭირო ლიცენზია აღნიშნული ფუნქციონალის გასააქტიურებლად
* SSL-ზე დაფუძნებული Botnet კავშირების ფილტრაციის მხარდაჭერა და ბლოკირების შესაძლებლობა(optional)
 |
| **აპლიკაციების ფილტრაცია:*** შემოთავაზებულ Firewall-ს უნდა შეეძლოს SSL დაშიფრული აპლიკაციების ფილტრაცია (დაბლოკვა და მონიტორინგი)
 |
| **Intrusion Prevention System (IPS):*** ქსელური შეტევებისგან თავდაცვის მხარდაჭერა სიგნატურების გამოყენებით
* IPS სიგნატურების ავტომატური განახლება
 |
| Internet Content Adaptation Protocol (ICAP) პროტოკოლის მხარდაჭერა |
| ანტივირუსული დაცვა:* ანტივირუსული ბაზების ავტომატური განახლება
* Content disarm and reconstruction (CDR) - Microsoft Office და PDF დოკუმენტებიდან აქტიური შიგთავსის წაშლა, როგორიცაა hyperlink, მედია, JavaScript, macros და ტექსტური შინაარსის დამახინჯების გარეშე ფაილების რეკონსტრუქცია (Optional)
 |
| **Sandbox Cloud(optional):*** ნულოვანი დღის, უახლესი მავნე პროგრამების მოწყვლადობის აღმოჩენა, ანალიზი და ჩახშობა
* SSL შიფრაციის მქონე პროგრამების მხარდაჭერა
* ანგარიშების გენერირება მავნე ფაილების შესახებ
 |
| Firewall-ზე უნდა ვრცელდებოდეს მწარმოებლის არანაკლებ სამ წლიანი საგარანტიო მომსახურეობა, ტექნიკური მხარდაჭერა და პროგრამული უზრუნველყოფის განახლება |
| Firewall-ს უნდა მოყვებოდეს არანაკლებ სამ წლიანი პროგრამული პაკეტის ლიცენზიები შემდეგ მოდულებზე: application controll, IPS, Antivirus, WEB ფილტრაცია |
|  |
| **ცენტრალური მართვის სისტემა** |
| **მხარდაჭერილი პლატფორმა:*** VMware ESXi, ცენტრალური მართვის სისტემა უნდა იყოს ვირტუალური მანქანა და გაიმართოს დამკვეთის არსებულ ინფრასტრუქტურაში
 |
| **ლიცენზია:** * უნდა მოიცავდეს არანაკლებ 3 ცალი Next Generation Firewall-ის ერთდროულ მართვას
 |
| **ლოგირება:*** 1 თვის ისტორიული ლოგების შენახვა
 |
| ცენტრალურმა მართვის სისტემამ უნდა უზრუნველყოს შემოთავაზებული ქსელური ბრანდმაუერების მართვა და კონფიგურაცია |
| **მართვის ფუნქციონალი:*** ცენტრალურ მართვის სისტემიდან შესაძლებელი უნდა იყოს ქსელური დაცვის ეკრანის (Firewall) კონფიგურაცია და მონიტორინგი
 |
| ცენტრალურ მართვის სისტემაზე უნდა ვრცელდებოდეს მწარმოებლის არანაკლებ 3 ან 5 წლიანი საგარანტიო მომსახურეობა, ტექნიკური მხარდაჭერა და პროგრამული უზრუნველყოფის განახლება |

**პასიური მოწყობილობების მოთხოვნები:**

* არანაკლებ 12x 10GBASE-SR SFP+ 850nm 300m თავსებადი შემოთავაზებულ აპარატურასთან
* არანაკლებ 12 x 3 მეტრი სიგრძის Multi Mode OM3 ოპტიკური პაჩკორდი

**დამატებითი მოთხოვნები:**

* შემოთავაზებული ბრანდმაუერის აპარატურა უნდა იყოს ერთი და იმავე მწარმოებლის.
* ყველა მოთხოვნილ აპარატურაზე მომწოდებელმა უნდა წარმოადგინოს მწარმოებლის ავტორიზაციის წერილი (Manufacturers Authorization Form).
* მომწოდებელმა უნდა წარმოადგინოს მოთხოვნილი კომუტატორების ვენდორის არანაკლებ ორი სერთიფიცირებული ინჟინრის სერტიფიკატი.
* მომწოდებელმა უნდა განახორციელოს მოთხოვნილი აპარატურის იმპლემენტაციის დაგეგმვა, კონფიგურაცია და სრული ინტეგრაცია ბანკის ქსელურ ინფრასტრუქტურაში, HA ტესტირება და უნდა შეასრულოს ეს ყველაფერი აპარატურის მოწოდებიდან 2 თვეში