ლოტი I - მონაცემთა გამოთვლითი ქსელის და უსაფრთხოების სისტემების აგება

#

# მონაცემთა გამოთვლითი ქსელის და უსაფრთხოების სისტემების აგების მიზნები

 პროექტის მიზანია „პაშა ბანკი“-ის სამომხმარებლო და მონაცემთა გამოთვლითი ქსელის წარმადობის და უსაფრთხოების გაუმჯობესება, თანამედროვე საქსელო და უსაფრთხოების მართვის სისტემების გამოყენებით.

გადაწყვეტილება ეფუძნება IT უსაფრთხოების თანამედროვე მოდელსა და პრინციპებს.

**მხარეების განმარტება**

სერვისის მიმღები კომპანია - სს „პაშა ბანკი“-ის IT დეპარტამენტი

სერვისის მიმწოდებელი კომპანია - საქართველოში რეგისტრირებული და მწარმოებლის მიერ სერვისზე ავტორიზებული IT კომპანია

## პროექტის ჩარჩო

პროექტის ფარგლებში დაგეგმილია შემდეგი ICT კომპონენტების დანერგვა:

* დატაცენტრის პერიმეტრის მარშუტიზატორები და კომუტატორები
* დატაცენტრის ფაირვოლები
* პერიმეტრის ფაირვოლები
* ფაირვოლების ცენტრალიზებული მართვის პროგრამული უზრუნველყოფა
* ფაირვოლების ლოგების მონიტორინგის და მართვის პროგრამული უზრუნველყოფა

## ქსელის ლოგიკური ბლოკ-დიაგრამა



მოცემულ თავში წარმოდგენილია IT სისტემები/კომპონენტები, რომელთა დანერგვა საჭიროა აღნიშნული ბლოკ-დიაგრამის მიხედვით.

##

## პერიმეტრის ფაირვოლები

|  |  |
| --- | --- |
| კატეგორია | სპეციფიკაცია |
| ფორმ-ფაქტორი | მინიმუმ 1 Rack Unit შასი (უნდა მოყვებოდეს რეკში ჩასაყენებელი სამაგრები) |
| ინტეფეისები (პორტები) | მინიმუმ 1x GE მენეჯმენტ პორტიმინიმუმ 1x GE RJ45 პორტი HA-სთვისმინიმუმ 8x GE RJ45 პორტიმინიმუმ 2x 10 GE SFP+ სლოტიმინუმუმ 8x GE SFP სლოტი |
| გამტარუნარიანობა | Firewall Throughput მინიმუმ 3.5 Gbps (NGFW რეჟიმში)Threat Prevention Throughput მინიმუმ 3 GbpsIPS Throughput მინიმუმ 5 GbpsIPsec VPN Throughput მინიმუმ 6 GbpsSSL-VPN Throughput მინიმუმ 2 GbpsSSL Inspection Throughput მინიმუმ 3 Gpbs |
| მაღალმდგრადობა | უნდა ჰქონდეს Active/Active, Active/Passive HA-ს და Clustering-ის მხარდაჭერა |
| ახალი სესიების რაოდენობა  | არანაკლებ 200000 სესია წამში  |
| ჯამური სესიების რაოდენობა | არანაკლებ 3 მილიონი სესია |
| უსაფრთხოების ფუნქციონალი | IPS, AV, URL Filtering, DNS Filtering, Application Control (Firewall-ს უნდა მოყვებოდეს მოცემული ფუნქციონალის ლიცენზია და არ უნდა იყოს საჭირო ცალკე შეძენა) , Cloud Sandboxing - სასურველია |
| პროტოკოლები და ფუნქციონალი | SSL Certificate Inspection, Active Directory Integration, OSPFv2/v3, BGP, static routing, Policy-based Routing, Point-to-Point Protocol over Ethernet (PPPoE) Multicast: PIM-SM, PIM-SSM, LACP, IGMP v1, v2, and v3, NAT, VLANS, IKEv1 and IKVEv2 IPSEC VPN, Remote Access VPN. |
| პროტოკოლები და ფუნქციონალი  | Active Directory integration, Vlans, Static Routing, Advanced routing features (Dynamic and Policy Based Routing), AAA, Radius, Logging |
| კვების ბლოკი | უნდა მოყვებოდეს მინიმუმ 2 ცალი დუბლირებული კვების ბლოკი |
| ცენტრალიზებული მართვა | ფაირვოლებს უნდა მოყვებოდეს ცენტრალიზებული მართვის სისტემა. მართვის სისტემას უნდა ჰქონდეს ვირტუალიზირებული გარემოს მხარდაჭერა |
| ლოგირების სისტემა | ფაერვოლს უნდა მოყვებოდეს ცენტრალური ლოგ-სერვერი. სისტემის ინსტალაცია შესაძლებელი უნდა იყოს ვირტუალიზირებულ გარემოში. DIsk |
| ლიცენზირება და აპარატულ-პროგრამული მხარდაჭერა | 3 წელი/ 1 წელი |
| რაოდენობა | 3 ცალი |

|  |
| --- |
| დატაცენტრის ISP კომუტატორები |
| კატეგორია | სპეციფიკაცია |
| ფორმ-ფაქტორი | 1 Rack Unit ან Half-Unit შასი |
| ინტეფეისები (პორტები) | მინიმუმ 24 x 100/1000 Mbps RJ-45 portsმინიმუმ 2 x 1G-RJ-45 Uplink portsმინიმუმ 2 x 1G SFP Uplink Ports |
| გამტარუნარიანობა |  Switching Capacity: 12 Gbps (Gigabits per second) |
| მეხსიერება |  ოპერატიული მეხსიერება - 512MB ფლეშ-მეხსიერება: 128MB |
| მხარდაჭერილი პროტოკოლები და სტანდარტები | STP, LACP, SPAN, RSPAN, AAA/RADIUS/TACACS, SNMP Agent, SSHv2, LLDP, NTP Agent, Logging |
| ელ.კვება | შესაბამისი ელ. კვების მოდულები |
| ლიცენზირება და აპარატულ-პროგრამული მხარდაჭერა | 3 წელი/ 1 წელი |
| რაოდენობა | 4 ცალი |

|  |
| --- |
| დატაცენტრის მარშუტიზატორები  |
| კატეგორია | სპეციფიკაცია |
| ფორმ-ფაქტორი | 1 Rack Unit შასი |
| ინტეფეისები (პორტები) | Dual Personality პორტები:მინიმუმ 4 x 10/100/1000 RJ-45 portsმინიმუმ 4 x 10/100/1000 SFP Ports |
| გამტარუნარიანობა |  საწყისი გამტარობა: 500 Mbps ლიცენზიით გაზრდადი 1 Gbps წარმადობამდე |
| მეხსიერება |  ოპერატიული მეხსიერება - 2GB Data Plane, 4GB - Control/Services Plane ფლეშ-მეხსიერება: 8GB, გაზრდადი 32GB-მდე |
| მაღალმდგრადობა | HSRP ან ანალოგიური ტექნოლოგიების მხარდაჭერა |
| მხარდაჭერილი პროტოკოლები და სტანდარტები |  - IPv4, IPv6, static routes, RIP and RIPv2, OSPF, eigrp, BGP, BGP Router Reflector, IGMPv3, PIM SM & SSM, RSVP, ERSPAN, IPSLA, Call Home, EEM, IKE, ACL, EVC, DHCP, FR, DNS, LISP, RADIUS, AAA, AVC, Distance Vector Multicast Routing Protocol (DVMRP), IPv4-to-IPv6 Multicast, MPLS, Layer 2 and Layer 3 VPN, IP sec, L2TPv3, BFD, IEEE802.1ag, and IEEE802.3ah - GRE, Ethernet, 802.1q VLAN, Point-to-Point Protocol (PPP), Multilink Point-to-Point Protocol (MLPPP), Frame Relay, Multilink Frame Relay (MLFR) (FR.15 and FR.16), High-Level Data Link Control (HDLC), Serial (RS-232, RS-449, X.21, V.35, and EIA-530), and PPP over Ethernet (PPPoE) - QoS, Class-Based Weighted Fair Queuing (CBWFQ), Weighted Random Early Detection (WRED), Hierarchical QoS, Policy-Based Routing (PBR), Performance Routing, and NBAR - Encryption: DES, 3DES, AES-128 or AES-256 (in CBC and GCM modes); Authentication: RSA (748/1024/2048 bit), ECDSA (256/384 bit); Integrity: MD5, SHA, SHA-256, SHA-384, SHA-512 |
| გაგრილება | Front-to-Back გაგრილების პრინციპით  |
| ელ.კვება | სარეზერვო კვების მოდულის შასიში დამატების შესაძლებლობით |
| ლიცენზირება და აპარატულ-პროგრამული მხარდაჭერა | 3 წელი / 1წელი |
| რაოდენობა  | 2 ცალი |

##

## დატაცენტრის ფაირვოლები

|  |  |
| --- | --- |
| კატეგორია | სპეციფიკაცია |
| ფორმ-ფაქტორი | მინიმუმ 1 Rack Unit შასი (უნდა მოყვებოდეს რეკში ჩასაყენებელი სამაგრები) |
| ინტეფეისები (პორტები) | მინიმუმ 1x GE მენეჯმენტ პორტიმინიმუმ 1x GE RJ45 პორტი HA-სთვისმინიმუმ 2x USB პორტიმინიმუმ 1x RJ45 კონსოლის პორტიმინიმუმ 16x GE RJ45 პორტიმინიმუმ 8x GE SFP სლოტიმინიმუმ 4x 10GE/GE SFP+/SFP სლოტი |
| გამტარუნარიანობა | Firewall Throughput მინიმუმ 9 Gbps (NGFW რეჟიმში)Threat Prevention Throughput მინიმუმ 8 GbpsIPS Throughput მინიმუმ 9 GbpsSSL Inspection Throughput მინიმუმ 8 Gpbs |
| მაღალმდგრადობა | უნდა ჰქონდეს Active/Active, Active/Passive HA-ს და Clustering-ის მხარდაჭერა |
| ახალი სესიების რაოდენობა  | არანაკლებ 400000 სესია წამში |
| ჯამური სესიების რაოდენობა | არანაკლებ 5 მილიონი სესია |
| უსაფრთხოების ფუნქციონალი | IPS, AV, Cloud Sandboxing, URL Filtering, DNS Filtering, Application Control (Firewall-ს უნდა მოყვებოდეს მოცემული ფუნქციონალის ლიცენზია და არ უნდა იყოს საჭირო ცალკე შეძენა) |
| პროტოკოლები და ფუნქციონალი | SSL Certificate Inspection, Active Directory Integration, OSPFv2/v3, BGP, static routing, Policy-based Routing, Point-to-Point Protocol over Ethernet (PPPoE) Multicast: PIM-SM, PIM-SSM, LACP, IGMP v1, v2, and v3, NAT, VLANS, IKEv1 and IKVEv2 IPSEC VPN, Remote Access VPN. |
| პროტოკოლები და ფუნქციონალი  | Traffic Shaping (Per IP), Active Directory integration, Vlans, Static Routing, Advanced routing features (Dynamic and Policy Based Routing), AAA, Radius, Logging |
| კვების ბლოკი | უნდა მოყვებოდეს მინიმუმ 2 ცალი დუბლირებული კვების ბლოკი |
| ლოგირების სისტემა | ფაერვოლს უნდა მოყვებოდეს ცენტრალური ლოგ-სერვერი. სისტემის ინსტალაცია შესაძლებელი უნდა იყოს ვირტუალიზირებულ გარემოში. |
| ცენტრალიზებული მართვა | ფაირვოლებს უნდა მოყვებოდეს ცენტრალიზებული მართვის სისტემა. მართვის სისტემას უნდა ჰქონდეს ვირტუალიზირებული გარემოს მხარდაჭერა |
| ლიცენზირება და აპარატულ-პროგრამული მხარდაჭერა | 3 წელი / 1 წელი |
| რაოდენობა | 3 ცალი |

##

## ფაირვოლ(ებ)ის ცენტრალიზებული მართვის პროგრამული უზრუნველყოფა

|  |  |
| --- | --- |
| კატეგორია | სპეციფიკაცია |
| ცენტრალიზებული მართვის პროგრამული უზრუნველყოფა | პერიმეტრის და დატაცენტრის ფაირვოლების მართვა უნდა დებოდეს ცენტრალიზებული მართვის პროგრამული უზრუნველყოფით.  |
| ლოგების შენახვის მინ.მოცულობა | 2 GB დღიური  |
| თავსებადობა | შემოთავაზებული პროგრამული უზრუნველყოფა თავსებადი უნდა იყოს შემდეგ ჰიპერვიზორებთან;VMware ESXiMicrosoft Hyper-V |
| ლიცენზირება და პროგრამული მხარდაჭერა | 3 წელი/ 1 წელი |
| რაოდენობა | 1 ცალი |

##

## ფაირვოლ(ებ)ის ლოგების მონიტორინგის და მართვის პროგრამული უზრუნველყოფა

|  |  |
| --- | --- |
| კატეგორია | სპეციფიკაცია |
| ლოგების მონიტორინგის და მართვის პროგრამული უზრუნველყოფა | პერიმეტრის და დატაცენტრის ფაირვოლების მართვა უნდა ხდებოდეს ცენტრალიზებული მართვის პროგრამული უზრუნველყოფით.  |
| ლოგების შენახვის მინ.მოცულობა | 5 GB დღიური 3 TB ჯამური |
| თავსებადობა | შემოთავაზებული პროგრამული უზრუნველყოფა თავსებადი უნდა იყოს შემდეგ ჰიპერვიზორებთან;VMware ESXiMicrosoft Hyper-V |
| ლიცენზირება და პროგრამული მხარდაჭერა | მინიმუმ 3 წელი / 1 წელი |
| რაოდენობა | 1 ცალი |

## დამატებითი მოთხოვნები

* მოწოდებულ საქსელო კომპონენტებზე უნდა ვრცელდებოდეს მწარმოებლის არანაკლებ 1 წლიანი გარანტია (საქონლის მოწოდების შემდგომ აღნიშნული ინფორმაციის გადამოწმება შესაძლებელი უნდა იყოს მწარმოებლის ოფიციალურ საიტზე), რომლის ათვლაც დაიწყება საქონლის მიწოდების მიღება-ჩაბარების აქტის გაფორმებიდან.
* სასურველია ,რომ პროვაიდერის კომუტატორი და მარშუტიზატირი იყოს ერთი და იგივე მწარმოებლის.
* საგარანტიო პერიოდის მანძილზე, სერვისის მიმღებ კომპანიას უნდა ჰქონდეს ცხელი ხაზით, ელ. ფოსტით და პორტალით მწარმოებელთან ინციდენტის რეგისტრირების საშუალება.( მწარმოებლის გარანტია, მის ტექნიკურ ჯგუფთან კავშირის უფლებითა და პროგრამული განახლებების გადმოწერის საშუალებით მწარმოებლის ვებ გვერდიდან )
* საგარანტიო პერიოდში მოწოდებული საქონლის ნებისმიერი დაზიანების შემთხვევაში, სერვისის მიმწოდებელი კომპანია ვალდებულია საკუთარი ხარჯებით აღმოფხვრას ყველა გამოვლენილი ხარვეზი/დაზიანება.
* სერვისის მიმწოდებელმა კომპანიამ უნდა წარადგინოს მწარმოებლ(ებ)ის ავტორიზაციის ფორმა (MAF).
* სერვისის მიმწოდებელმა კომპანიას უნდა უზრუნველყოს მოწოდებული პროგრამული უზრუნველყოფ(ებ)ის სტაბილურ ვერსიამდე განახლება.
* შემოთავაზებული ფაირვოლები, უნდა ირიცხებოდეს Gartner-ის Magic Quadrant-ში ბოლო 3 წლის განმავლობაში ლიდერებში (2020,2021,2022).
* ტენდერში ყველა მოთხოვნილი კომპონენტი უნდა იყოს ახალი და არ უნდა იყოს მოხსნილი წარმოებიდან.
* მომწოდებელმა ყველა საჭირო ფიზიკური დაერთებისთვის უნდა გაითვალისწინოს საჭირო კაბელების და დამატებითი კომპონენტების არსებობა.