### ლოტი #6

### აპლიკაციების მიწოდების და მათი დაცვის მოწყობილობა (ADC) – 2 ცალი

წარმოდგენილი შემოთავაზება უნდა შეიცავდეს 2 ცალ მოწყობილობას და თითოეული მოწყობილობა დამატებითი კომპონენტების გარეშე უნდა აკმაყოფილებდეს ქვევით მოცემულ ტექნიკურ მახასიათებლებს:

1. მოწყობილობის მახასიათებლები
	1. მინიმუმ 4 ფიზიკური ბირთვი
	2. 32 GB მინიმალური მეხსიერბა
	3. ქსელური შეერთება
		* 2 x 10 Gbps პორტი - გაფართოვებადი 4 x 10Gbps პორტამდე
		* 4 x 1 Gbps ქსელური პორტი - გაფართოვებადი 8 x 1 Gbps პორტამდე
	4. წარმადობა
		* 20 Gbps - L4/L7 ტრაფიკის გამტარუნარიანობა
		* L7 მოთხოვნა წამში 600K
		* L4 შეერთება წამში 250K
		* 10 Gbps - ჯამური დაშიფრეულიტრაფიკის გამტარუნარიანობა
		* 10K დაშიფრული ტრანზაქცია წამში
2. მოწყობილობას უნდა შეეძლოს როგორც Active/Acitve, ისე Active/Passive მაღალმდგრადობის რეჟიმში მუშაობა. აღნიშნულ რეჟიმში შესაძლებელი უნდა იყოს 8 მოწყობილობის გაერთიანება და შესაძლებელი უნდა იყოს მათ შორის SSL და TCP სესიების სინქრონიზაცია. ასევე შესაძლებელი უნდა იყოს ფიზიკური მოწყობილობების, იგივე მწარმოებლის ვირტუალურ მოწყობილობასთან მაღალმდგრადობის აგება.
3. უნდა ჰქონდეს ქსელში გამართვის შემდეგი რეჟიმების მხარდაჭერა:
4. L2 Forwarding
5. L3 IP Forwarding (Routing)
6. Packet Based Layer 4 traffic processing
7. Reverse Proxy and Forward Proxy (Layer 7)
8. SSL Forward Proxy
9. აუცილებელია შემდეგი ქსელური ტექნოლოგიების მხარდაჭერა
	1. L2 კომუტაცია: Vlan, Vlan Groups, VXLAN.
	2. L3 მარშუტიზაცია: IPV4, IPV6, NAT, SNAT, ასევე საჭიროების შემთხვევაში დამატებით ლიცენზიით BGP, OSPF დინამირუი მარშუტიზაციის პროტოკოლების გააქტიურების შესაძლებლობა
10. სისტემას უნდა გააჩნდეს მომხმარებელთა შემდეგი ავტორიზაციის წყაროს მხარდაჭერა:
11. მომხმარებელთა ლოკალური ბაზა
12. LDAP
13. Microsoft Active Directory
14. RADIUS
15. TACACS+
16. HSM Systems
17. სისტემას უნდა შეეძლოს ვებ აპლიკაციებზე წვდომის დაშვება შემდეგი აუტენტიფიკაციის მექანიზმების გამოყენებით:
18. Kerberos
19. NTLM v1, v2
20. SAML 2.0
21. Smart Card
22. Security Token
23. კლიენტის სერტიფიკატი
24. nFactor აუტენტიფიკაცია
25. უნდა ჰქონდეს 1000 კონკრენტული მომხმარებლისთვის, გარე ქსელიდან კავშირის შემდეგი ფუნქციონალის მხარდაჭერა:
	1. SSL VPN
	2. Microsoft Exchange Server და Microsoft SharePoint Server-ზე გარე ქსელიდან მომხმარებელთა აუტეტიფიცირებული წვდომის უზრუნველყოფა, SSO-ის გამოყენებით.
	3. წვდომის გახსნამდე, მომხმარებელთა მოწყობილობების ორგანიზაციის უსაფრთხოების სტანდარტებთან თავსებადობის შემოწმება
	4. Client-side პროგრამული უზრუნველყოფა Windows, Linux და MacOS ოპერაციული სისტემებისთვის ასევე iOS და Android მობილური ოპერაციული სისტემებისთვის.
26. უნდა ჰქონდეს მომხმარებელთა აპლიკაციებზე წვდომის პოლიტიკების შექმნის შესაძლებლობა:
	1. მომხმარებელთა წვდომის მართვა როგორც ინდივიდუალური სააღრიცხვო ჩანაწერის ისე მომხმარებელთა ჯგუფების მიხედვით.
	2. შესაძლებელი უნდა იყოს, ერთი პოლიტიკის ფარგლებში, სხვადასხვა HTTP პარამეტრის მიხედვით (Host Name, URI, Source IP, Source Browser), ავტორიზაციის სხვადასხვა მეთოდის გამოყენების, ასევე მომხმარებელთა სხვადასხვა ჯგუფის წევრობის შემოწმება.
	3. მომხმარებელთა რესურსებზე წვდომის მართვა აუტენტიფიკაციის პორტალის მეშვეობით. შესაძლებელი უნდა იყო აღნიშნული პორტალის ვიზუალური ნაწილის შეცვლა.
27. სისტემა უნდა უზრუნველყოფდეს ვებ აპლიკაციებს შორის L4/L7 დონეზე, დატვირთვის განაწილებას და მაღალმდგრადობას:
	1. დატვირთვის გადანაწილების შემდეგი მეთოდების გამოყენებით:
		* Round Robin.
		* Ratio Round Robin.
		* Least Connections.
		* Weighted Least Connections
		* Least Sessions
		* Predictive
	2. ვებ აპლიკაციის მონიტორინგისთვის შემდეგი მექანიზმების მხარდაჭერა:
		* ICMP, ICMP Gateway, TCP, HTTP, HTTPS, URL, LDAP, MSSQL, RADIUS, SOAP,WMI, ასევე დამატებით „Custom“ მონიტორინგის მექანიზმის შექმნის შესაძლებლობა.
	3. სისტემა უნდა უზრუნველყოფდეს სესიების მდგრადობას შემდეგი პარამეტრების მიხედვით:
		* Source or Destination IP
		* Session ID Persistence
		* Cookie Persistence
		* MSRDP Sessions Persistence
	4. ასევე სისტემას უნდა შეეძლოს შემომავალი ტრაფიკის ოპტიმიზაცია:
		* HTTP კომპრესია
		* HTTP სესიების, სერვერის მხარეს ერთ TCP სესიაში აგრეგირების შესაძლებლობა
		* HTTP შიგთავსის ქეშირება
28. სისტემას უნდა შეეძლოს “reverse proxy” რეჟიმში მუშაობისას განახორციელოს შემდეგი ოპერაციები: „rewrite URLs“ და “Rewrite Response URLs”
29. სისტემას უნდა გააჩნდეს სპეციალური ანგარიშის მოდული ანალიტიკური შესაძლებლობებით, რომელიც შეაფასებს დაცულობის დონეს სხვადასხვა უსაფრთხოების სტანდარტებთან მიმართებაში
30. მართვა და ნომიტორინგი:
	1. სისტემის მართვა უნდა შესაძლებელი უნდა იყოს როგორც ვებ ინტერფეისიდან ასევე „CLI“-ის მეშვეობით
	2. სისტემას უნდა შეეძლოს, მოთხოვნისამებრ რეპორტების გენერირება. რეპორტების გენერირება ასევე შესაძლებელი უნდა იყოს წინასწარ განსაზღვრული გრაფიკის მიხედვით
	3. სისტემას უნდა შეეძლოს მომხდარი უსაფრთხოების ინციდენტების ლოგირება.
31. სისტემის ინტეგრაცია შესაძლებელი უნდა იყოს, ქსელის ცენტრალიზებული მონიტორინგისა და შეტყობინებების შემგროვებელ სისტემებთან, შემდეგი ტექნოლოგიების საშუალებით:
	1. SNMP
	2. Syslog
	3. SFlow
	4. Integration with leading SIEM vendors
	5. Email to data owners and other stakeholders
	6. Custom followed action
	7. Integrated graphical reporting
	8. Real-time dashboard
	9. Metadata and content-based via integration with third party Data Loss Prevention (DLP) vendors such as RSA, Websense, McAfee, and Symantec
	10. REST, SOAP API - მხარდაჭერა
32. სისტემას უნდა გააჩნდეს აუდიტ ლოგირება და შესაძლებელი უნდა იყოს შემდეგი ლოგების ნახვა:
* Role based access controls to view audit data (read-only)
* Real-time visibility of audit data
1. სისტემაზე უნდა ვრცელდებოდეს მწარმოებლის 1 წლიანი 24/7-ზე მხარდაჭერის მომსახურება, როგორც აპარატურაზე ასევე პროგრამულ უზრუნველყოფაზე.

**საინსტალაციო სამუშაოები:**

* 1. უნდა მოხდეს მოწოდებული მოწყობილობის გაშვება და მაღალმდგრადობის აგება;
	2. მოხდეს არსებულ ქსელთან ინტეგრაცია;
	3. მოხდეს ათი სერვისის მიგრაცია და შესაბამისი ტრაფიკის პოლიტიკების კონფიგურაცია
	4. ცოდნის გადაცემის ერთ დღიანი ვორკშოპი 3 თანამშრომლისთვის

**საკვალიფიკაციო მოთხოვნები:**

1. პრეტენდენტმა უნდა წარმოადგინოს მწარმოებლის ავტორიზაციის ფორმა (Manufacturers Authorization Form).
2. პრეტენდენტმა უნდა წარმოადგინოს ინფორმაცია შემოთავაზებული მწარმოებლის იგივე პროდუქტის გამოყენებით დასრულებული პროექტის/პროექტების შესახებ.

**პროქტის დასრულების ვადაა 2020 წლის ივლისი**