ა(ა)იპ სავალდებულო დაზღვევის ცენტრი აცხადებს ტენდერს ქსელური დაცვის ეკრანის (Firewall), 1 წლიანი ლიცენზიითა და მწარმოებლის მხარდაჭერით

ტენდერის ამოცანა:

შესყიდვის ამოცანას წარმოადგენს - ტექნიკური მოთხოვნების შესაბამისად 2 (ორი) ცალი ქსელური დაცვის ეკრანის (Firewall), 1 წლიანი ლიცენზიითა და მწარმოებლის მხარდაჭერით შესყიდვას.

ქსელური დაცვის ეკრანის (Firewall) შესყიდვასთან დაკავშირებით:

ა(ა)იპ სავალდებულო დაზღვევის ცენტრში დაგეგმილია არსებული ქსელური დაცვის ეკრანის (Firewall) ჩანაცვლება. შესაბამისად დაიგეგმა 2 (ორი) ცალი ქსელური დაცვის ეკრანის (Firewall) შესყიდვა.

ტექნიკური დავალება:

დასახელება	სპეციფიკაცია		რაოდენობა
ქსელური დაცვის ეკრანი (Firewall) – FG-121G - FortiGate-121G 18 x GE RJ45 ports (including 1 x MGMT port, 1 X HA port, 16 x switch ports), 8 x GE SFP slots, 4 x 10GE SFP+ slots, SP5 hardware accelerated, 480GB onboard SSD storage, dual AC power supplies	ფორმ-ფაქტორი	არაუმეტეს 1U	2
	გაგრილების სისტემა	მაქსიმალური კომპლექტაცია, გათვლილი სრულად დატვირთვისთვის	
	პორტების რაოდენობა და პორტის ტიპები	მინიმუმ 16 პორტი არანაკლებ 1Gbps RJ45 ტიპის მინიმუმ 8 პორტი GE SFP ტიპის მინიმუმ 4 პორტი არანაკლებ 10Gbps SFP+ მინიმუმ 1 პორტი მენეჯმენტისთვის RJ45 ტიპის	
	მყარი დისკი	მინიმუმ 1 ცალი 480GB SSD დისკი, ლოგების შესანახად	
	კვების ბლოკები	მინიმუმ 2 ცალი	
	დამატებითი პარამეტრები	მაღალმდგრადობა - Active-Active, Active-Passive, Clustering ვირტუალურ დომენებად ან სისტემებად დაყოფის ფუნქცია Trusted Platform Module (TPM) მხარდაჭერა NAT და Transparent რეჟიმების მხარდაჭერა	
	გამტარუნარიანობა	NGFW რეჟიმში გამტარუნარიანობა - არანაკლებ 3 Gbps Threat Protection რეჟიმში გამტარუნარიანობა - არანაკლებ 2.5 Gbps ჯამური სესიების რაოდენობა - არანაკლებ 3 მილიონი ახალი სესიების რაოდენობა - არანაკლებ 140000 IPsec VPN გამტარუნარიანობა - 30 Gbps ერთდროული SSL-VPN მომხმარებლების რაოდენობა არანაკლებ 500	
	ფუნქციონალი	მაღალმდგრადობა: Active-Active, Active-Passive, Clustering მართვა: - ინტერგირებული WEB GUI საშუალებით - ადმინისტრატორებისა და მომხმარებლების რამდენიმე დონის მხარდაჭერის ფუნქცია - ცენტრალური მართვის სისტემის საშუალებით სიჩქარის შეზღუდვა Shaper:- Shared packet shaper-ი სიჩქარის შეზღუდვის პოლიტიკა სადაც შესაძლებელი უნდა იყოს ტრაფიკის პრიორიტეტის, მინიმუმ გარანტირებული სიჩქარის და მაქსიმალური სიჩქარეების კონფიგურირება.- Per-ip shaper ფუნქციონალი - შესაძლებელი უნდა იყოს უსაფრთხოების პოლიტიკებში მითითებული IP ქვექსელის თითოეული IP მისამართისთვის (ან მომხმარებლისათვის) ტრაფიკის შეზღუდვა, ისე რომ ერთმა მომხმარებელმა ვერ შეძლოს მთლიანი	

		ხელმისაწვდომი ტრაფიკის დაკავება. აღნიშნული ფუნქციონალის ფარგლებში შესაძლებელი უნდა იყოს ქვესელის თითოეული მისამართისათვის დასაშვები მაქსიმალური სიჩქარის და კონკურენტული სესიების რაოდენობის დაწესება. DoS ტიპის შეტევისგან თავდაცვის მექანიზმი: კერძოდ, მოწყობილობას უნდა შეეძლოს tcp syn flood-ის, tcp/udp პორტების სკანირების, UDP Flood, icmp Flood ტიპის შეტევების აღმოჩენა ერთი და იგივე სორს ან დესტინეიშენ მისამართებით, tcp/udp პორტების წინასწარ განსაზღვრული სესიის სიხშირის/რაოდენობის მიხედვით, შეტევის აღმოჩენისა და შემდგომი გადაწყვეტილების მიღება (სესიის დაბლოკვა. მისამართის, საიდანაც შეტევა ხორციელდება, განსაზღვრული დროით კარანტინში მოთავსება, ინციდენტის ლოგირება) მარშრუტიზაცია: - სტატიკური მარშრუტები მხარდაჭერა - დინამიური მარშრუტიზაციის პროტოკოლების მხარდაჭერა: OSPF, BGP, RIP - Multicast ტრაფიკის მარშრუტიზაცია - ვირტუალური მარშრუტიზაცია Virtual Routing and Forwarding (VRF) მხარდაჭერა. არანაკლებ 30 VRF-ის მხარდაჭერა - Policy Based მარშრუტიზაცია 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 - შესაძლებელი უნდა იყოს სპეციფიურ ვებ გვერდებზე წვდომის მცდელობისას წინასწარი ავტორიზაციის მოთხოვნა. - ვებ ტრაფიკის ფილტრაციის სერვისს უნდა გააჩნდეს ვებ გვერდების კატეგორიები, რომელთა სისტემატიურ განახლებას უნდა აწარმოებდეს შემოთავაზებული პროდუქტის მწარმოებელი. - SSL-ზე დაფუძნებული Botnet კავშირების ფილტრაციის მხარდაჭერა და ბლოკირების შესაძლებლობა 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 ანტივირუსული დაცვა	

		- 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. - ანტივირუსული ბაზების ავტომატური განახლება - HTTP, SMTP, POP3, IMAP, FTP-პროტოკოლების მხარდაჭერა Sandbox Cloud - ნულოვანი დღის, უახლესი მავნე პროგრამების მოწყვლადობის აღმოჩენა, ანალიზი და ჩახშობა - SSL შიფრაციის მქონე პროგრამების მხარდაჭერა - ანგარიშების გენერირება მავნე ფაილების შესახებ	
	სამაგრი და კაბელები	19“ სასერვერო კარადაში მონტაჟისთვის, სამონტაჟო ყველა აქსესუარით კომპლექტში,	
ზემოთ მითითებული ქსელური ეკრანისათვის მწარმოებლის 1 წლიანი ლიცენზია და გარანტია **FC-10-F121G-950-02-12 - FortiGate-121G 1 Year Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium)**	**ლიცენზია და გარანტია**	ფუნქციონალის ველში აღწერილი შესაძლებლობების სრული ლიცენზია 1 (ერთი) წლის ვადით. მწარმოებლის გარანტია და მხარდაჭერის სერვისი 1 (ერთი) წლის ვადით.	**2**

მომწოდებელმა უნდა განახორციელოს მოწყობილობების მოწოდება და მწარმოებლის მიერ პროდუქტის ლიცენზიების და მხარდაჭერის მოწოდების მხარდაჭერა.

მოთხოვნები პრეტენდენტის მიმართ:

- პრეტენდენტს უნდა გააჩნდეს უკანასკნელი ორი წლის განმავლობაში, არანაკლებ სამი ანალოგიური ქსელური პროექტის წარმატებით შესრულების გამოცდილება.
- პრეტენდენტი კომპანია უნდა იყოს მწარმოებლის პარტნიორი ან რესელერი ან წარმომადგენელი

<u>შესაბამისად პრეტენდენტმა უნდა წარმოადგინოს:</u>

- არანაკლებ სამი ანალოგიური ქსელური პროექტის წარმატებით შესრულების გამოცდილების დასადასტურებლად შესაბამისი ხელშეკრულებები და მიღება ჩაბარების აქტები ან/და SPA/NAT/CMR ნომრები.
- მწარმოებლის პარტნიორობის ან რესელერობის ან წარმომადგენელობის დასადასტურებლად მწარმოებლის ავტორიზაციის ფორმა (ე.წ. MAF - Manufacturer Authorization Form).

- პრეტენდენტმა უნდა წარმოადგინოს ინვოისი.

შემოთავაზებები წარმოადგინეთ ცხრილის სახით სადაც ცალკე-ცალკე პუნქტებად იქნება გაწერილი:

- პროდუქტის დასახელება, ვერსია და ღირებულება (ასევე მითითებული ექნება შედის თუ არა აღნიშნულ ვერსიაში ერთწლიანი ლიცენზია და მწარმოებლის ერთწლიანი მხარდაჭერა);

შემსყიდველის მხრიდან საკონტაქტო ინფორმაცია:

შესყიდვის პროცედურების და შესყიდვების მიმართულებით საკონტაქტო პირი:
ნიკოლოზ მინდიაშვილი,
საკონტაქტო პირის ელ-ფოსტის მისამართი: **nmindiashvili@tpl.ge**
მობ: 591404046

ტექნიკურ საკითხების მიმართულებით საკონტაქტო პირი:
გიორგი გიორგანაშვილი
საკონტაქტო პირის ელ-ფოსტა: **ggiorganashvili@tpl.ge**
მობ:595184444