**ტექნიკური მახასიათებლები**

| ქსელური მოწყობილობა (ბრანდმაუერი-ფაერვოლი) | |
|---|---|
| **დასახელება** | **მოთხოვნა** |
| **თვისებები და ფუნქციები, რომლებიც მოითხოვება მიწოდებული მოწყობილობების ფუნქციონალისგან** | • IPS/IDS<br>• AntiVirus<br>• Sandbox Cloud<br>• Botnet<br>• AntiSpam<br>• Botnet IP/Domain<br>**ზემოთ ჩამოთვლილი ფუნქციონალის გააქტიურება შესაძლებლებელი უნდა იყოს დამატებითი ლიცენზიის გამოყენებით.**<br>• აღნიშნულ მოწყობილობას უნდა მოყვებოდეს Web-ფილტრაციის და Application-ფილტრაციის 36 თვიანი ლიცენზია<br>• კლასტერი უნდა ფუნქციონირებდეს აქტიურ/პასიურ ან/და აქტიურ/აქტიურ რეჟიმებში.<br>• ვირტუალური დომენებად ან სისტემებად დაყოფის ფუნქცია.<br>• უნდა უზრუნველყოს VPN შეერთება.<br>• უნდა ჰქონდეს დატვირთვის ბალანსირების ფუნქცია.<br>• უნდა უზრუნველყოს traffic shaping ტრაფიკის მართვა<br>• უნდა უზრუნველყოს SSL ინსპექცია.<br>• უნდა უზრუნველყოს IPv4, IPv6 დინამიკური მარშრუტიზაცია.<br>• უნდა უზრუნველყოს შეერთებების WAN-ოპტიმიზაცია.<br>• უნდა უზრუნველყოს ანტივირუსული დაცვა.<br>• უნდა უზრუნველყოს სპამისგან დაცვა. |

| | |
|---|---|
| | • უნდა ჰქონდეს IPS შეჭრის პრევენციის ფუნქცია.<br>• უნდა უზრუნველყოს გამოყენებითი პროგრამების კონტროლი.<br>• უნდა უზრუნველყოს ნულოვანი დღის მოწყვლადობისგან დაცვა მწარმოებლის Sandbox Cloud-ის დახმარებით.<br>• მხარი უნდა დაუჭიროს ინტეგრაციას დომენის კონტროლერთან. |
| **აპარატურული მახასიათებლები** | ქსელთაშორისი ეკრანის ინტერფეისი უნდა იყოს:<br>• არანაკლებ 16x 1G RJ45 ინტერფეისი<br>• არანაკლებ 1x RJ45 კონსოლური ინტერფეისი<br>• არანაკლებ 1 x 1G RJ45 MGMT<br>• არანაკლებ 4 x 10G SFP+ ინტერფეისი<br>• არანაკლებ 8 x 1G SFP ინტერფეისი<br>• არანაკლებ 1xUSB 3.0 ინტერფეისი<br>• არაუმეტეს 2x100-240v AC კვების პორტი<br>• ყველა ფიზიკური ინტერფეისი მოქნილად უნდა ეწყობოდეს ნებისმიერ ფუნქციას (WAN, LAN, DMZ).<br>• ქსელთაშორისი ეკრანის ინტერფეისი უნდა იყოს არაუმეტეს 1U ზომის.<br>• უნდა მოყვებოდეს რეკში ჩასაყენებელი ყველა საჭირო კომპონენტი<br>• ქსელთაშორისი ეკრანის ინტერფეისი მიწოდებული უნდა იქნეს ორ კვების ბლოკთან ერთად რეზერვული კვებისთვის. |
| **მწარმოებლურობა** | Firewall ქსელური ეკრანის გამტარუნარიანობა (1518/512/64 byte RFC 6985, UDP) არანაკლებ 27/27/11 გბიტი/წმ.<br>• IPSec VPN (512 byte) – არანაკლებ 13 გბიტი/წმ.<br>• SSL-VPN Throughput - არანაკლებ 2 გბიტი/წმ.<br>• NGFW გამტარიანობა - არანაკლებ 3.5 გბიტ/წმ.<br>• IPS Throughput (Enterprise AppMix) არანაკლებ 5 გბიტი/წმ. |

| | |
|---|---|
| | • Threat Protection გამტარიანობა - არანაკლებ 3 გბიტი/წმ.<br>• დაყოვნება (64 byte, UDP packets) - არანაკლებ 4,78 µs.<br>• გამტარუნარიანობა (Packets Per Second) - არანაკლებ 16.5 მბიტი/წმ.<br>• ერთდროული სესიების რაოდენობა (TCP) – არანაკლებ 3 მილიონი.<br>• ახალი სესიები (TCP 64byte) – არანაკლებ 280 000 სესია/წმ.<br>• Firewall პოლიტიკების რაოდენობები – არანაკლებ 10 000.<br>• SSL VPN Clients (ერთდროული წვდომა) – 500 (დამატებითი ლიცენზიის გარეშე).<br>• Gateway-to-Gateway IPsec VPN Tunnels - არანაკლებ 2000.<br>• შეუზღუდავი სამომხმარებლო ლიცენზია. |
| **მოდულების აღწერა** | **ანტივირუსული დაცვის / კომპიუტერული ვირუსის აღმოჩენისა და განადგურების მოდულს უნდა ჰქონდეს შემდეგი შესაძლებლობები:**<br>• HTTP, SMTP, POP3, IMAP, FTP-პროტოკოლების მხარდაჭერა<br>• ანტივირუსული ბაზების განახლებების ავტომატური „ოპერატიული მიწოდება“.<br>• ინფიცირებული შეტყობინებების კარანტინში მოთავსება.<br>• ევრისტიკული სკანირება.<br>**ქსელური ფუნქციები**<br>• უნდა ჰქონდეს მრავალი WAN-ქსელის შეერთებების მხარდაჭერის ფუნქცია.<br>• უნდა ჰქონდეს DHCP-პროტოკოლის მხარდაჭერის ფუნქცია კლიენტი/სერვერის კონფიგურაციაში.<br>• უნდა ჰქონდეს პოლიტიკების საფუძველზე მარშრუტიზაციის მხარდაჭერის ფუნქცია. |

| | |
|---|---|
| | • უნდა ჰქონდეს დინამიკური მარშრუტიზაციის მხარდაჭერის ფუნქცია (RIP v1 ან v2, OSPF, BGP, Multicast, Policy-based routing, Virtual Router).<br><br>**ადმინისტრირება / მართვა**<br><br>• უნდა ჰქონდეს როლების საფუძველზე მართვის მხარდაჭერის ფუნქცია.<br><br>• უნდა ჰქონდეს ადმინისტრატორებისა და მომხმარებლების რამდენიმე დონის მხარდაჭერის ფუნქცია.<br><br>უნდა ჰქონდეს მომხმარებლის TFTP,FTP,SSH-პროტოკოლისა და web-ინტერფეისის მეშვეობით განახლებებისა და ცვლილების მხარდაჭერის ფუნქცია.<br><br>**მომხმარებელთა ავთენტურობის შემოწმება**<br><br>• უნდა ჰქონდეს ჩაშენებული მონაცემთა ბაზა.<br><br>• უნდა ჰქონდეს RADIUS/LDAP გარე მონაცემთა ბაზის მხარდაჭერის ფუნქცია.<br><br>• Xauth RADIUS მეშვეობით IPSEC VPN-პროტოკოლებისთვის<br><br>**ქსელთაშორის ეკრანს უნდა ჰქონდეს შემდეგი ფუნქციონალები:**<br><br>• NAT, PAT, „გამჭვირვალე“ (ხიდი).<br><br>• მარშრუტიზატორის რეჟიმი (RIP v1 და v2, OSPF, BGP, Multicast).<br><br>• VLAN Tagging (802.1Q).<br><br>• ავთენტურობის შემოწმება მომხმარებელთა ჯგუფების საფუძველზე.<br><br>• SIP/H.323 NAT Traversal.<br><br>• WINS მხარდაჭერა.<br><br>**VPN**<br><br>• უნდა ჰქონდეს PPTP, IPSec და SSL მხარდაჭერის ფუნქცია<br><br>• უნდა ჰქონდეს დაშიფვრის (DES, 3DES, AES) მხარდაჭერის ფუნქცია |

| | |
|---|---|
| | • უნდა ჰქონდეს SHA-1 / MD5 ავთენტურობის შემოწმების მხარდაჭერის ფუნქცია.<br>• უნდა ჰქონდეს იერარქიული (hub and spoke) VPN-შეერთებების მხარდაჭერის ფუნქცია.<br>• უნდა ჰქონდეს IKE სერტიფიკატის მიხედვით ავთენტურობის შემოწმების მხარდაჭერის ფუნქცია.<br>• უნდა ჰქონდეს IPSec NAT Traversal პროტოკოლის მხარდაჭერის ფუნქცია.<br>• უნდა ჰქონდეს Dead Peer Detection მექანიზმის მხარდაჭერის ფუნქცია.<br>**-შინაარსის ფილტრაცია**<br>• უნდა ჰქონდეს „თეთრი“ URL სიების მხარდაჭერის ფუნქცია.<br>• უნდა ჰქონდეს შინაარსის პროფილების მხარდაჭერის ფუნქცია.<br>• უნდა ჰქონდეს ბლოკირების მხარდაჭერის ფუნქცია.<br>**შეჭრის პრევენციის სისტემა (IPS/IDS)**<br>• უნდა ჰქონდეს დინამიკური აღმოჩენის სიგნატურების გასამართი სიის მხარდაჭერის ფუნქცია.<br>• უნდა ჰქონდეს შეტევების ბაზის ავტომატური განახლების მხარდაჭერის ფუნქცია.<br>**Sandbox Cloud** (დამატებითი ლიცენზიის შემთხვევაში, აღნიშნული ფუნქციონალის შემოთავაზება გამოიყოს ცალკე ველად)<br>• ნულოვანი დღის, უახლესი მავნე პროგრამების მოწყვლადობის აღმოჩენა, ანალიზი და ჩახშობა, მათ შორის, იმ მავნე პროგრამებისა, რომელთა მიზანია გამოძალვა და პაროლით დაცული მავნე პროგრამების ჩახშობა.<br>• კოდის სტატისტიკური ანალიზი, რომელიც განსაზღვრავს შესაძლო საფრთხეებს შეუსრულებად კოდში.<br>• ევრისტიკული / მახასიათებლური / რეპუტაციული ანალიზი. |

| | |
|---|---|
| | • SSL დაშიფვრით პროტოკოლების / გამოყენებითი პროგრამების: HTTP, SMTP, POP3, IMAP,FTP,და ანალოგიური ვერსიების მხარდაჭერის ფუნქცია. (არ გვაქვს აღნიშნული პროტოკოლების მხარდაჭერის ფუნქცია)<br>• დაწვრილებითი ანგარიში მავნე ფაილების შესახებ.<br>• ანალიზის ჩასატარებლად საეჭვო ფაილების ხელით ჩატვირთვის შესაძლებლობა.<br><br>**პროტოკოლირება / მონიტორინგი**<br>• უნდა ჰქონდეს პროტოკოლების დისტანციურ Syslog გადაგზავნის მხარდაჭერის ფუნქცია.<br>• უნდა ჰქონდეს რეალურ დროში მონიტორინგისა და ისტორიის გადახედვის გრაფიკული საშუალებების მხარდაჭერის ფუნქცია<br>• უნდა ჰქონდეს ვირუსებისა და შეტევების შესახებ ელექტრონული ფოსტით შეტყობინების მხარდაჭერის ფუნქცია.<br>• უნდა ჰქონდეს VPN-გვირაბების მონიტორინგის მხარდაჭერის ფუნქცია.<br>**ტრაფიკის ჩამოყალიბება**<br>• უნდა ჰქონდეს გარანტირებული / მაქსიმალური / პრიორიტეტული გამტარუნარიანობის რეჟიმების მხარდაჭერის ფუნქცია.<br>**Proxy-server**<br>• უნდა ჰქონდეს გამტარი ზოლის მუშაობის ოპტიმიზაციისთვის მომხმარებლების მიერ მოთხოვნილი Web-შინაარსის ლოკალურად შენახვის მხარდაჭერის ფუნქცია. |
| **გარანტიები და** | • მოწყობილობა უზრუნველყოფილი უნდა იყოს არანაკლებ 36-თვიანი გარანტიით მწარმოებლისგან. |

| | |
|---|---|
| **მომსახურებით მხარდაჭერა** | • გარანტიის პირობები უნდა შეიცავდეს ვებ-პორტალის, ონლაინ-ჩატის ან ტელეფონის მეშვეობით მწარმოებლის ტექნიკური მხარდაჭერისთვის მიმართვის, მომსახურების შემთხვევათა რეგისტრაციის, მოწყობილობის მწყობრიდან გამოსვლის შემთხვევაში მისი შეცვლის, სისტემის მიკროკოდისა და დაყენებული პროგრამული უზრუნველყოფის ვერსიის განახლების შესაძლებლობას.<br>• მომსახურებით მხარდაჭერა უნდა შეიცავდეს მონაცემთა აქტუალური რეპუტაციული ბაზების, ანტივირუსული სიგნატურებისა და შეჭრის პრევენციის სისტემის სიგნატურების მონაცემთა ბაზების მიღების შესაძლებლობას.<br>• კონსულტაციების გაწევა ტელეფონით, ელექტრონული ფოსტით და მწარმოებლის მხარდაჭერის საიტზე ორშაბათიდან კვირის ჩათვლით 00.00 საათიდან 24.00 საათამდე დღეღამურად.<br>• მუდმივი (24 საათი x 7 დღის განმავლობაში) ავტორიზებული წვდომა მწარმოებლის საიტზე.<br>• პრეტენდენტის კომპანიაში დასაქმებული უნდა იყოს არანაკლებ ერთი თანამშრომელი, რომელსაც უნდა გააჩნდეს შემოთავაზებული ქსელური ეკრანის მწარმოებლის მიერ გაცემული, ინჟინრის ექსპერტის დონის მოქმედი სერტიფიკატი. |