დანართი 1 - ტექნიკური დავალება

|  |  |
| --- | --- |
| **1 ) ბრანდმაუერი**  | **რაოდენობა 2 ცალი**  |
| ინტერფეისები: | არანაკლებ 4 ცალი 1G RJ-45არანაკლებ 4 ცალი 1G/10G SFP/SFP+ არანაკლებ 1 ცალი RJ45 მართვის პორტიარანაკლებ 1 ცალი USB ინტერფეისიარანაკლებ 1 ცალი Console ინტერფეისიინტერფეისები უნდა იყოს მინიმუმ მოდულურად გაფართოებადი ან ადგილზე კონფიგურირებადი |
| მუდმივი მეხსიერება | არანაკლებ 240 GB SSD  |
| კვების ბლოკი | დუბლირებული |
| Firewall throughput | არანაკლებ 9 Gbps |
| Threat Prevention throughput | არანაკლებ 6 Gbps |
| IPsec VPN throughput | არანაკლებ 1.5 Gbps |
| მაქსიმალური ერთდროული სესიები | არანაკლებ 1,000,000 |
| ახალი სესიები წამში | არანაკლებ 100,000 |
| ვირტუალური სისტემები | არანაკლებ 5 ვირტუალურ სისტემად გაყოფა, მომავალში ლიცენზიის დამატების საშუალებით |
| მაღალმდგრადობა | * Active/Active და Active/Passive HA რეჟიმის მხარდაჭერა
* Interface Monitoring და Path Monitoring
* Failover რეჟიმი ავტომატური გადართვის შესაძლებლობით
 |
| ზოგადი მოთხოვნები | * შემოთავაზებული ბრანდმაუერი უნდა იყოს ლიდერი Gartner Magic Quadrant for Enterprise Network Firewalls-ში
* შემოთავაზებული ბრანდმაუერი უნდა be ISO 27001, ISO 27017, ISO 27018, ISO 27701, SOC2, FedRAMP, Germany C5, Common Criteria, FIPS 140-2, CMVP, NCSC Foundation, ANSSI, DoDIN, CSfC, USGV6, ICSA და NEBS სერტიფიცირებული
* შემოთავაზებული ბრანდმაუერი არ უნდა საჭიროებდეს გადატვირთვას, უასფრთხოების განახლებების შესამოწმებლად და დასაინსტალირებლად
* შემოთავაზებული ბრანდმაუერი უნდა ჰქონდეს ჩაშენებულად რეპორტების გენერირების მხარდაჭერა, რაიმე დამატებითი აპარატურის გარეშე.
* შემოთავაზებული ბრანდმაუერი უნდა ამოიცნოს აპლიკაციები პორტის, SSL/SSH შიფრაციის, ან თავისარიდების ტექნიკების მიუხედავად
* შემოთავაზებულ ბრანდმაუერს უნდა შეეძლოს უცნობი აპლიკაციების კატეგორიზაცია პოლიტიკის კონტროლისთვის, საფრთხის ანალიზისთვის ან აპლიკაციის იდენტიფიკაციის ტექნოლოგიის განვითარებისათვის.
* შემოთავაზებული ბრანდმაუერი უნდა იყოს ე.წ. Native ინჟინერიული უსაფრთხოების გადაწყვეტა (და არა აპლიკაციების კონტროლის მოდული საფუძველში არსებული Stateful Inspection firewall-ით).
* შემოთავაზებული ბრანდმაუერი უნდა იყოს ე.წ. Native ინჟინერიული მოწყობილობა, რომელიც იყენებს ერთჯერადი გადამუშავების პარალელურ არქიტექტურას ტრაფიკის დამუშავებისთვის.
* შემოთავაზებულ ბრანდმაუერს უნდა ჰქონდეს ინტეგრირებული ტრაფიკის Shaping-ის (QoS) ფუნქციონალი, რომელიც ეფუძნება წყაროს/დანიშნულების IP-ს, პორტს, პროტოკოლს და აპლიკაციას.
* შემოთავაზებულ ბრანდმაუერს უნდა შეეძლოს აპლიკაციის სხვადასხვა ნაწილის გარჩევა, მაგალითად, საშუალებას უნდა აძლევდეს Facebook ჩატის გამოყენებას, მაგრამ ბლოკავდეს ფაილების გადაცემის შესაძლებლობას.
* შემოთავაზებულ ბრანდმაუერს უნდა შეეძლოს წვდომის კონტროლი და პოლიტიკის აღსრულება ვებსაიტებისა და აპლიკაციებისთვის, მათ შორის SaaS აპლიკაციებისთვის.
* შემოთავაზებულ ბრანდმაუერს ყველა ფორმფაქტორზე უნდა ჰქონდეს ერთიანი ოპერაციული სისტემა.
* შემოთავაზებულ ბრანდმაუერს უნდა შეეძლოს უსაფრთხოების პოლიტიკის შექმნა, რათა თავიდან აიცილოს ავთენტიკაციის მონაცემების ქურდობა.
* შემოთავაზებულ ბრანდმაუერს უნდა შეეძლოს შიდა აპლიკაციებისთვის მრავალფაქტორიანი ავთენტიკაციის (MFA) პოლიტიკის აღსრულება.
* შემოთავაზებულ ბრანდმაუერს უნდა ჰქონდეს შეუზღუდავი ღია API, რომლის გამოყენებაც შესაძლებელია დამატებითი გადასახადის (subscription-ის) გარეშე, მათ შორის Dev Toolkit-ის, ხელსაწყოების, სკრიპტებისა და ნიმუშების წვდომისთვის.
* შემოთავაზებულ ბრანდმაუერს უნდა ჰქონდეს უნარი, რომ დინამიურად და ავტომატურად დააჯგუფოს მომხმარებლები უსაფრთხოების მოვლენების საფუძველზე, რომლებიც მათთან არის დაკავშირებული, რისთვისაც არ არის საჭირო ხელით ამის განხორციელება.
* შემოთავაზებულ ბრანდმაუერს უნდა ჰქონდეს ხილვადობა და შესაძლებლობა, შეზღუდოს აპლიკაციები, რომლებიც იყენებენ არასტანდარტულ პორტებს, ერთიანი უსაფრთხოების პოლიტიკის წესის ფარგლებში.
* შემოთავაზებულ ბრანდმაუერს უნდა ჰქონდეს უნარი, ტეგების მიმგრება ობიექტებზე, რათა დინამიურად აღასრულოს პოლიტიკა ნებისმიერ ცვლილებაზე IP-ს, ზონის ან მიმართულების მიუხედავად, საიდანაც ტრეფიკი წამოიშვება, ისე, რომ არ არის საჭირო პოლიტიკის თავიდან დანერგვა.
* შემოთავაზებულ ბრანდმაუერს უნდა ჰქონდეს შესაძლებლობა, დააკმაყოფილოს მანქანური სწავლების(Machine Learning) ალგორითმები მოწინავე დაცვისთვის პირდაპირ ბრანდმაუერი-დან, დამატებითი გარე კავშირების გარეშე.
* შემოთავაზებულ ბრანდმაუერს უნდა ჰქონდეს ადვილად განსახორციელებელი ოპერაციული სისტემის განახლება, რომელიც არ საჭიროებს კონკრეტულ კომბინაციებს, რომ ჰოთფიქსები ან პატჩები იმუშავოს.
* შემოთავაზებულ ბრანდმაუერს უნდა ჰქონდეს ფუნქცია, რომელიც მოიცავს მრავალ ოპერაციულ სისტემის იმიჯს, რათა უზრუნველყოს მდგრადობა და მარტივად წინა ვერსიებზე დაბრუნება(ე.წ. Roll back), ვერსიების განახლების დროს.
* შემოთავაზებულ ბრანდმაუერს უნდა ჰქონდეს შესაძლებლობა, ჩართოს ნებისმიერი ახალი უსაფრთხოების ფუნქცია ტრეფიკის შესრულების გავლენის გარეშე, რომელიც მას ააქვს.
* შემოთავაზებულ ბრანდმაუერს უნდა ჰქონდეს ფუნქცია, რომელიც აიდენტიფიცირებს იმ აპლიკაციებს, რომლებიც არღვევენ უსაფრთხოების პოლიტიკებს, და ამ პოლიტიკების აპლიკაციის ბაზაზე გადმოტანის საშუალებას იძლევა.
 |
| უსაფრთხოების პოლიტიკის კონტროლი | * შემოთავაზებულ ბრანდმაუერს უნდა ჰქონდეს შესაძლებლობა, შექმნას უსაფრთხოების პოლიტიკები, რომლებიც ეფუძნება Layer 7 აპლიკაციებს, რაც არ არის დამოკიდებული TCP/UDP პორტის ნომერზე (არაპროფილზე დაფუძნებული აპლიკაციების კონტროლი).
* შემოთავაზებულ ბრანდმაუერს უნდა ჰქონდეს მხარდაჭერა უცნობი ტრაფიკის (უცნობი აპლიკაციების) მართვისთვის უსაფრთხოების პოლიტიკების მეშვეობით.
* შემოთავაზებულ ბრანდმაუერს უნდა ჰქონდეს ჩაშენებული უსაფრთხოების პოლიტიკების ოპტიმიზაციის ინსტრუმენტი, რომელიც გაამარტივებს მემკვიდრეობით Layer 4 პორტ-დამოკიდებული უსაფრთხოების პოლიტიკების გადაქცევას Layer 7 აპლიკაციებზე დაფუძნებულ პოლიტიკებში.
* შემოთავაზებულ ბრანდმაუერს უნდა ჰქონდეს მხარდაჭერა უსაფრთხოების პოლიტიკების აღსრულებისთვის, რომელიც ეფუძნება განრიგს.
* შემოთავაზებულ ბრანდმაუერს უნდა ჰქონდეს ფუნქცია, რომელიც გაამარტივებს წესების გამოყენების ტრეკინგს, მოცემული დროით მარკირების საშუალებით, რომელიც აჩვენებს ყველაზე ბოლო წესის შესაბამისობას, პირველი შესაბამისობის დროს და წესის გამოყენების მთვლელს
 |
| მაღალი დონის საფრთხეების პრევენციის ფუნქციები 3 წლიანი ლიცენზიაAdvanced Threat Prevention | * შემოთავაზებულ ბრანდმაუერს უნდა შეეძლოს ქსელების დაცვა მრავალი პრევენციული შრით, რათა შეებრძოლოს საფრთხეებს თითოეული შეტევის ეტაპზე.
* შემოთავაზებულ ბრანდმაუერს უნდა შეეძლოს გამოავლინოს და დაბლოკოს საფრთხეები ნებისმიერ და ყველა პორტზე, და არა მხოლოდ, სიგნატურების გამოყენება მხოლოდ წინასწარ განსაზღვრული პორტების ნაკრების შეზღუდვისთვის
* შემოთავაზებულ ბრანდმაუერს უნდა ჰქონდეს სარგებელი სხვა ღრუბლოვანი უსაფრთხოების გამოწერებიდან, რომლებიც უზრუნველყოფს ყოველდღიურ განახლებებს, რათა შეაჩეროს ექსპლოიტები, მავნე პროგრამები, მავნე URL-ები, ბრძანების და კონტროლის (C2) არხები და ჯაშუშური პროგრამები.
* შემოთავაზებულ ბრანდმაუერს უნდა ჰქონდეს დაცვა უცნობი საფრთხეებისგან, ამისთვის უნდა იყოს ინტეგრირებული მანქანური სწავლება (ML) ბრანდმაუერს ბირთვში, რაც უზრუნველყოფს პირდაპირ(inline)სიგნატურების გარეშე შეტევის პრევენციას.
* შემოთავაზებული ბრანდმაუერს უნდა გამოიყენოს პირდაპირი(inline) მავნე პროგრამების დაცვა—სიგნატურების გამოყენებით, რომლებიც ეფუძნება მონაცემის(Payload) ანალიზს, არა ჰეშს.
* შემოთავაზებულ ბრანდმაუერს უნდა უწყვეტად აგროვებდეს ტელემეტრიას, რათა გახადოს შესაძლებელი მონაცემთა ინტენსიური მანქანური სწავლების პროცესების შედეგად, ავტომატური გამოთვლა და რეკომენდაციები პოლიტიკის ცვლილებებზე.
* შემოთავაზებული ბრანდმაუერი-მა უნდა გამოიყენოს ღრუბლზე დაფუძნებული მანქანური სწავლების (ML) პროცესები, რათა გახდეს შესაძლებელი სიგნატურების და ინსტრუქციების ნულოვანი დაგვიანებით გადატანა ბრანდმაუერი-ზე.
* შემოთავაზებულ ბრანდმაუერი-მა უნდა გამოიყენოს ჰერისტიკური ანალიზი, რათა გამოავლინოს ანომალიურ პაკეტები და ტრაფიკის ნიმუშები, როგორიცაა პორტის სკანირება, ჰოსტების სკანირება და მომსახურების უარყოფის (DoS) შეტევები.
* შემოთავაზებულ ბრანდმაუერს უნდა ჰქონდეს მხარდაჭერა მორგებული სიგნატურების შექმნისთვის, რაც საშუალებას იძლევა შეღწევის პრევენციის შესაძლებლობების მორგებას ქსელის უნიკალური საჭიროებების შესაბამისად.
* შემოთავაზებულ ბრანდმაუერს უნდა ჰქონდეს მხარდაჭერა სხვა თავდაცვის შესაძლებლობებისთვის, როგორიცაა არასწორი ან დეფორმირებული პაკეტების ბლოკირება, IP დეფრაგმენტაცია და TCP-reassembly, თავდაცვა თავისარიდების(evasion) და დამალვის(obfuscation) ტექნიკებისგან.
* შემოთავაზებულ ბრანდმაუერს უნდა ჰქონდეს ინტეგრირებული თავდაცვითი ტექნოლოგიები, რათა უზრუნველყოს, რომ თუ საფრთხე ერთ ტექნოლოგიას აცდება, მეორე მაინც გამოავლენს და შეაჩერებს მას.
* შემოთავაზებულ ბრანდმაუერს უნდა შეეძლოს ტრეფიკის ინსპექტირება და კლასიფიკაცია, ასევე მავნე პროგრამებისა და მოწყვლადობის ექსპლოიტების აღმოჩენა და ბლოკირება ერთჯერადი დამუშავების (single-pass) პროცესში.
* შემოთავაზებულ ბრანდმაუერს უნდა შეეძლოს თითოეული პაკეტის სკანირება პლატფორმის გავლით, ყურადღებით შეისწავლოს ბაიტთა მიმდევრობები როგორც პაკეტის თავსართში(Header), ასევე მონაცემში (Payload)
* შემოთავაზებულ ბრანდმაუერს უნდა შეეძლოს მირებული პაკეტის რიგისა და თანმიმდევრობის კონტექსტის ანალიზი, რათა გამოავლინოს და აღკვეთოს თავის არიდების (evasion) ტექნიკები.
* შემოთავაზებულ ბრანდმაუერს უნდა ჰქონდეს პროტოკოლის დეკოდერზე დაფუძნებული ანალიზის მხარდაჭერა.
* შემოთავაზებულ ბრანდმაუერს უნდა ჰქონდეს პროტოკოლის ანომალიებზე დაფუძნებული დაცვის მექანიზმი.
* შემოთავაზებულ ბრანდმაუერს უნდა შეეძლოს ინლაინ (inline), ნაკადზე (stream-based) დაფუძნებული გამოვლენა და პრევენცია მავნე პროგრამების, რომლებიც დამალულია შეკუმშულ ფაილებსა და ვებ მონაცემში.
* შემოთავაზებულ ბრანდმაუერს უნდა შეეძლოს დაცვა საფრთხის შემცველი მონაცემებისგან(payload), რომლებიც დამალულია გავრცელებულ ფაილურ ფორმატებში, როგორიცაა Office/Microsoft 365 დოკუმენტები და PDF ფაილები.
* შემოთავაზებულ ბრანდმაუერს უნდა შეეძლოს დაკავშირებული საფრთხეების მოვლენების კორელაცია (მაგალითად, Threat Prevention ლოგებიდან), რომლებიც ერთობლივად მიუთითებენ სავარაუდო შეტევაზე.
* შემოთავაზებულ ბრანდმაუერს უნდა ჰქონდეს გამონაკლისების (exception) კონფიგურაციის შესაძლებლობა.
* შემოთავაზებულ ბრანდმაუერს უნდა შეეძლოს მავნე პროგრამების აღმოჩენა და პრევენცია სხვადასხვა ფაილის ტიპების სკანირებით.
* შემოთავაზებულ ბრანდმაუერს უნდა შეეძლოს მავნე პროგრამების იდენტიფიცირება, რომლებიც ინტერნეტიდან ჩამოტვირთული მავნე პროგრამებიდან და ფაილებიდან ცდილობენ შეღწევას.
* შემოთავაზებულ ბრანდმაუერს უნდა ჰქონდეს შესაძლებლობა შექმნას მორგებული სიგნატურები აპლიკაციებისათვის.
* შემოთავაზებულ ბრანდმაუერს უნდა ჰქონდეს ყველა ძირითადი აპლიკაციის სიგნატურები და უნდა შეძლოს კარგად ცნობილი აპლიკაციების, როგორიცაა P2P და VoIP, გაგება, პორტზე დამოკიდებულების გარეშე.
* შემოთავაზებულ ბრანდმაუერს უნდა შეეძლოს პირდაპირი(Inline) ღრმა სწავლების (deep learning) ტექნოლოგიის გამოყენება რეალურ დროში ახალი და უცნობი ბრძანების და კონტროლის (C2) ტექნიკების აღკვეთისთვის.
* შემოთავაზებული ბრანდმაუერი-ის მანქანური სწავლებისა და ღრმა სწავლების მოდელები უნდა იყოს მორგებული ძირითად პროტოკოლებზე, როგორიცაა SSL, HTTP, უცნობი UDP და უცნობი TCP
* შემოთავაზებული ბრანდმაუერი უნდა იყენებდეს ML-ზე დაფუძნებულ ანალიზს DNS-ზე დაფუძნებული მოწინავე საფრთხეების იდენტიფიცირებისთვის
* შემოთავაზებული ბრანდმაუერი უნდა იყენებდეს ღრუბლოვან მონაცემთა ბაზას, რომელიც შეიცავს ათეულ მილიონობით ცნობილ მავნე დომენს, რაც უზრუნველყოფს ფიშინგის, მავნე პროგრამებისა და სხვა მაღალი რისკის კატეგორიების ბლოკირებას
* შემოთავაზებული ბრანდმაუერი უნდა უზრუნველყოფდეს საფრთხეების შესახებ ანგარიშგების შესაძლებლობებს, რომლებიც იძლევა DNS ტრაფიკის სრულ ხილვადობას, უსაფრთხოების მოვლენების სრულ DNS კონტექსტთან ერთად და ტრაფიკის ტენდენციებს დროთა განმავლობაში
* შემოთავაზებული ბრანდმაუერი უნდა უზრუნველყოფდეს ცნობილი მავნე დომენისთვის DNS მოთხოვნაზე პასუხის გაყალბებას და ამ მავნე დომენის სახელის გადაწყვეტას განსაზღვრად IP მისამართზე, რომელიც მიეწოდება კლიენტს ინფიცირებული ჰოსტების იდენტიფიცირებისთვის
* შემოთავაზებული ბრანდმაუერი უნდა იძლეოდეს ცალკეული პოლიტიკის მოქმედებების განსაზღვრის საშუალებას, ასევე ლოგების სიმძიმის დონეს კონკრეტული ხელმოწერის ტიპისთვის
* შემოთავაზებული ბრანდმაუერი უნდა ახდენდეს DGA-ების გამოყენების იდენტიფიცირებას, რომელიც ქმნის შემთხვევით დომენებს მავნე პროგრამების მიერ C2 სერვერთან დაკავშირებისთვის
* შემოთავაზებული ბრანდმაუერი უნდა ახდენდეს DGA (Domain Generation Algorithms) დომენების იდენტიფიცირებას ლექსიკონის სიტყვებზე დაყრდნობით
* შემოთავაზებული ბრანდმაუერი უნდა აღკვეთდეს DNS გვირაბების გამოყენებას, რომელიც იყენებს DNS პროტოკოლს მავნე პროგრამებისა და სხვა მონაცემების გასატარებლად კლიენტ-სერვერის მოდელის მეშვეობით
* შემოთავაზებული ბრანდმაუერი უნდა შლიდეს ულტრა-დაბალ/ნელ DNS გვირაბებს, რომლებიც ანაწილებენ გვირაბის მონაცემებს და ექსპლოიტებს მრავალ დომენზე და იყენებენ ძალიან ნელ სიჩქარეებს აღმოჩენის თავიდან ასაცილებლად, მონაცემების მოპარვისთვის ან დამატებითი მავნე პეილოადების თქვენს ქსელში გასაგზავნად
* შემოთავაზებული ბრანდმაუერი უნდა იყენებდეს პრედიქტულ ანალიტიკას, რომელიც იცავს მომხმარებლებს იმ დომენებთან დაკავშირებისგან, რომლებიც დარეზერვებული იყო და თვეების განმავლობაში უმოქმედოდ იყო დატოვებული მავნე აქტორების მიერ გამოყენებამდე
* შემოთავაზებული ბრანდმაუერი უნდა აღკვეთდეს სწრაფი ფლუქსის დომენებს
* შემოთავაზებული ბრანდმაუერი უნდა იცავდეს რეპუტაციული დომენების გატეხილ DNS ზონებში ფარულად დამატებული დომენებისგან
* შემოთავაზებული ბრანდმაუერი უნდა აღკვეთდეს DNS რებინდინგის შეტევებს, რომლებიც შეიძლება გამოყენებულ იქნას ლატერალური გადაადგილებისთვის და კორპორატიული ქსელის შიგნით სერვისებზე თავდასხმისთვის ინტერნეტიდან
* შემოთავაზებული ბრანდმაუერი უნდა აღკვეთდეს დანგლინგ DNS შეტევებს
* შემოთავაზებული ბრანდმაუერი უნდა აღკვეთდეს თავდამსხმელების მიერ მომხმარებლების მავნე დომენებზე გადამისამართებას ველდკარდ DNS ჩანაწერის გამოყენებით
* შემოთავაზებული ბრანდმაუერი უნდა აღკვეთდეს მეთოდებს, რომლებიც იყენებენ DNS პროტოკოლს მავნე პეილოადების ქსელში გასატარებლად
* შემოთავაზებული ბრანდმაუერი უნდა იცავდეს მომხმარებლებს იმ დომენებთან დაკავშირებისგან, რომლებიც შეიძლება გამოყენებულ იქნას DDoS შეტევების განსახორციელებლად
* შემოთავაზებული ბრანდმაუერი უნდა უჭერდეს მხარს ტრაფიკის სტატიკურ ანალიზს
* შემოთავაზებული ბრანდმაუერი უნდა უჭერდეს მხარს ტრაფიკის დინამიურ ანალიზს
* შემოთავაზებული ბრანდმაუერი უნდა უჭერდეს მხარს ფაილების მოწინავე ანალიზს URL ქროლინგთან ერთად მრავალეტაპიანი, მრავალნახტომიანი შეტევების პრევენციისთვის
* შემოთავაზებული ბრანდმაუერი-ის ანალიზის გარემო უნდა ახდენდეს macOS, Android, Windows XP/7/10, Linux-ის რეპლიკაციას
* შემოთავაზებული ბრანდმაუერი-ის ფაილების ანალიზმა უნდა უზრუნველყოს PE ფაილების (EXE, DLL და სხვა), ყველა Microsoft Office ფაილის ტიპის, Mac OS X ფაილების, Linux (ELF) ფაილების, Android Package Kit (APK) ფაილების, Adobe Flash და PDF ფაილების, არქივის (RAR და 7-Zip) ფაილების, სკრიპტის (BAT, JS, VBS, PS1, Shell script და HTA) ფაილების, ელ-ფოსტის შეტყობინებებში არსებული ბმულების ანალიზის და დაშიფრული (TLS/SSL) ფაილების მხარდაჭერა
* შემოთავაზებული ბრანდმაუერი-ის მხარდაჭერილი პროტოკოლები უნდა იყოს SMTP, POP3, SMB, FTP, IMAP, HTTP, HTTPS
* შემოთავაზებული ბრანდმაუერი უნდა ქმნიდეს ხელმოწერებს ნიმუშის მავნე პეილოადზე დაყრდნობით და მოწმდებოდეს სიზუსტისა და უსაფრთხოებისთვის
* შემოთავაზებული ბრანდმაუერი უნდა უზრუნველყოფდეს დაცვის განახლებებს უცნობი მავნე პროგრამებისთვის წამების განმავლობაში
* 3 წლიანი ლიცენზია
 |
| Advanced ე.წ. Sandbox ფუნქციონალის 3 წლიანი ლიცენზია | ტრაფიკის ანალიზის საფუძვლები:* შემოთავაზებული ბრანდმაუერი უნდა უჭერდეს მხარს ტრაფიკის სტატიკურ ანალიზს
* შემოთავაზებული ბრანდმაუერი უნდა უჭერდეს მხარს ტრაფიკის დინამიურ ანალიზს
* შემოთავაზებული ბრანდმაუერი უნდა უჭერდეს მხარს ტრაფიკის რეკურსიულ ანალიზს

მრავალპროტოკოლური მონიტორინგი:* შემოთავაზებული ბრანდმაუერი უნდა ახდენდეს საფრთხეების იდენტიფიცირებას ყველა ტრაფიკში ასობით აპლიკაციის მასშტაბით, მათ შორის ვებ ტრაფიკში; ელ-ფოსტის პროტოკოლებში როგორიცაა SMTP, IMAP და POP; და ფაილების გაზიარების პროტოკოლებში როგორიცაა SMB და FTP, პორტებისა და დაშიფვრის მიუხედავად

საეჭვო აქტივობის მონიტორინგი:* შემოთავაზებული ბრანდმაუერი უნდა აკონტროლებდეს ყველა ქსელურ აქტივობას, რომელიც წარმოიქმნება საეჭვო ფაილისგან, მათ შორის უკანა კარის შექმნას, შემდგომი ეტაპის მავნე პროგრამების ჩამოტვირთვას, დაბალი რეპუტაციის მქონე დომენების მონახულებას და ქსელის დაზვერვას
* შემოთავაზებული ბრანდმაუერი უნდა ახდენდეს პოტენციურად მავნე სკრიპტების, როგორიცაა JScript და PowerShell, ქსელში გადაადგილების იდენტიფიცირებას

მოწინავე საფრთხეების პრევენცია:* შემოთავაზებული ბრანდმაუერი უნდა აჩერებდეს უცნობ საფრთხეებს ფაირვოლის დონეზე ინლაინური მანქანური სწავლების გამოყენებით
* შემოთავაზებული ბრანდმაუერი უნდა ახდენდეს მაღალი თავის არიდების უნარის მქონე მავნე პროგრამების პრევენციას ფარული დაკვირვების, ავტომატური გახსნის, დამოკიდებულების ემულაციის, მავნე პროგრამების ხელმოწერებისა და ჭკვიანი მეხსიერების ანალიზის გამოყენებით

ფაილების ანალიზი და გარემო:* შემოთავაზებული ბრანდმაუერი უნდა უჭერდეს მხარს ფაილების მოწინავე ანალიზს URL ქროლინგთან ერთად მრავალეტაპიანი, მრავალნახტომიანი შეტევების პრევენციისთვის
* შემოთავაზებული ბრანდმაუერი-ის ანალიზის გარემო უნდა ახდენდეს macOS, Android, Windows XP/7/10, Linux-ის რეპლიკაციას
* შემოთავაზებული ბრანდმაუერი-ის ფაილების ანალიზმა უნდა უზრუნველყოს PE ფაილების (EXE, DLL და სხვა), ყველა Microsoft Office ფაილის ტიპის, Mac OS X ფაილების, Linux (ELF) ფაილების, Android Package Kit (APK) ფაილების, Adobe Flash და PDF ფაილების, არქივის (RAR და 7-Zip) ფაილების, სკრიპტის (BAT, JS, VBS, PS1, Shell script და HTA) ფაილების, ელ-ფოსტის შეტყობინებებში არსებული ბმულების ანალიზის და დაშიფრული (TLS/SSL) ფაილების მხარდაჭერა

ხელმოწერების გენერაცია და განახლებები:* შემოთავაზებული ბრანდმაუერი უნდა ქმნიდეს ხელმოწერებს ნიმუშის მავნე პეილოადზე დაყრდნობით და მოწმდებოდეს სიზუსტისა და უსაფრთხოებისთვის
* შემოთავაზებული ბრანდმაუერი უნდა უზრუნველყოფდეს დაცვის განახლებებს უცნობი მავნე პროგრამებისთვის წამების განმავლობაში

ინტეგრაცია:* შემოთავაზებული ბრანდმაუერი უნდა ინტეგრირდებოდეს შეუფერხებლად მორგებული აპლიკაციებისა და არსებული უსაფრთხოების ინსტრუმენტების გასამდიდრებლად, როგორიცაა SIEM, TIP, თიქეთინგი, SOAR, XDR ინსტრუმენტები API-ის გამოყენებით კომპრომეტირების ინდიკატორების (IOC) დასამუშავებლად
 |
| მომხმარებლის იდენტიფიკაცია და ავტენტიფიკაციაUser Identification & Authentication Features | მომხმარებლის იდენტიფიკაციის შესაძლებლობები:* შემოთავაზებული ბრანდმაუერი უნდა უჭერდეს მხარს მომხმარებლის ID-ის იდენტიფიცირებას Active Directory-სთან ინტეგრაციით WinRM-ისა და WMI-ის მეშვეობით
* შემოთავაზებული ბრანდმაუერი უნდა უჭერდეს მხარს მომხმარებლის ID-ის იდენტიფიცირებას Exchange-თან ინტეგრაციით WinRM-ისა და WMI-ის მეშვეობით
* შემოთავაზებული ბრანდმაუერი უნდა უჭერდეს მხარს მომხმარებლის ID-ის იდენტიფიცირებას syslog მიმღებად მუშაობით
* შემოთავაზებული ბრანდმაუერი უნდა უჭერდეს მხარს მომხმარებლის ID-ის იდენტიფიცირებას მესამე მხარის გადაწყვეტილებებთან XML API-ების მეშვეობით ინტეგრაციით
* შემოთავაზებული ბრანდმაუერი უნდა უჭერდეს მხარს მომხმარებლის ID-ის იდენტიფიცირებას კაპტიური პორტალის მეშვეობით
* შემოთავაზებული ბრანდმაუერი უნდა უჭერდეს მხარს მომხმარებლის ID-ის იდენტიფიცირებას ტერმინალურ სერვერებში
* შემოთავაზებული ბრანდმაუერი უნდა უჭერდეს მხარს მომხმარებლის ID-ის იდენტიფიცირებას მომხმარებლის კომპიუტერებზე აგენტის გაშვებით

ავთენტიფიკაციის მხარდაჭერა:* შემოთავაზებულ ბრანდმაუერს უნდა ჰქონდეს პირდაპირი მრავალფაქტორიანი ავთენტიფიკაციის ინტეგრაცია RSA-სთან, Okta-სთან, PingID-სთან და Duo-სთან
* შემოთავაზებული ბრანდმაუერი უნდა უჭერდეს მხარს SSO ავთენტიფიკაციას
* შემოთავაზებული ბრანდმაუერი უნდა უჭერდეს მხარს მრავალ სერვერის პროფილს, როგორიცაა SAML 2.0, Radius, LDAP, Tacacs+ და Kerberos
 |
| მართვა, ლოგირება და რეპორტინგიManagement, Logging & Reporting Features | შემოთავაზებული ბრანდმაუერი უნდა აკმაყოფილებდეს შემდეგ მოთხოვნებს: * ბრძანებების სტრიქონის ინტერფეისი (CLI): უნდა უზრუნველყოს CLI-ს მხარდაჭერა კონფიგურაციისა და მართვისთვის.
* ჩაშენებული ვებ-ინტერფეისი (GUI): უნდა უზრუნველყოს Java-ზე დაუფუძნებელი გრაფიკული ინტერფეისი.
* XML Rest API-ზე დაფუძნებული მართვა: მხარდაჭერა უნდა ჰქონდეს XML Rest API-ს მეშვეობით სისტემის მართვისთვის.
* კონფიგურაციის დასტური (Commit-Based): კონფიგურაციის ცვლილებები უნდა გამოყენებულ იქნას მხოლოდ დასტურის (commit) შემდეგ.
* კონფიგურაციის აუდიტი: უნდა შეიძლებოდეს მიმდინარე და კანდიდატური კონფიგურაციების შედარება.
* ინტერაქტიული გრაფიკული ანალიტიკა: უნდა უზრუნველყოს ვიზუალური შეჯამება აპლიკაციების, მომხმარებლების, URL-ების, საფრთხეებისა და ქსელში გამავალი კონტენტის შესახებ.
* მორგებული გრაფიკული ქსელის აქტივობა:

 - არასტანდარტული პორტების გამოყენებით მომუშავე აპლიკაციების ვიზუალიზაცია.  - ბლოკირებული აქტივობების ანალიტიკა (აპლიკაციები, მომხმარებლები, კონტენტი, საფრთხეები, პოლიტიკები).  - VPN ტუნელების აქტივობების დეტალები (ტუნელის ID/ტაგი, აპლიკაციის/მომხმარებლის/IP წყარო/დანიშნულების მონაცემები). * მორგებული ანგარიშგება:

 - ანგარიშების გენერირება მომხმარებლის, მომხმარებელთა ჯგუფის ან აპლიკაციის მიხედვით.  - ანგარიშების PDF-ში ექსპორტი და ელექტრონული ფოსტით გაგზავნა.  - SaaS აპლიკაციების გამოყენების დედიკირებული ანგარიში. * ლოგების მართვა: გამოყოფილი ლოგების ნაკრებები ტრაფიკის, საფრთხეების, URL ფილტრაციის, მონაცემთა ფილტრაციის, ფაილების კონტროლის, მომხმარებლის ID-ის, ავთენტიფიკაციის, კონფიგურაციის, სისტემის და გაფრთხილებებისთვის.
* ადმინისტრატორის როლები: მხარდაჭერა უნდა ჰქონდეს მორგებული ადმინისტრატორის როლებისთვის.

- \*\*პირდაპირი მართვა მოწყობილობაზე\*\*: - ადმინისტრატორებს შეეძლებათ კონფიგურაციის ცვლილებები პირდაპირ მოწყობილობაზე (ცენტრალური მენეჯერის გარეშე). - ცენტრალურმა ადმინისტრატორებმა უნდა შეძლონ ლოკალური ცვლილებების მონიტორინგი. * კონფიგურაციის კონტროლი:

 - არჩევანი, თუ რომელი ადმინისტრატორის ცვლილებები დაიკომიტება ფაირვოლზე. - ცვლილებების სწრაფი გაუქმება/კონფიგურაციის აღდგენა კონკრეტული მომხმარებლების მიერ განხორციელებული მოქმედებებისთვის. * კლიენტგარეშე მართვა: მართვა უნდა ხორციელდებოდეს პირდაპირ მოწყობილობაზე დამატებითი კლიენტების ან ვირტუალური მანქანების ინსტალაციის გარეშე.
* ეს ფორმატი ხაზს უსვამს თითოეულ ფუნქციონალს და აადვილებს მოთხოვნების სტრუქტურირებულად წარმოჩენას.
 |
| პროტოკოლების და ტექნოლოგიების მხარდაჭერა | * Interface Modes: L2, L3, tap, transparent mode.
* OSPFv2/v3 with graceful restart, BGP with graceful restart, RIP, static routing, Policy-based forwarding, Point-to-Point Protocol over Ethernet (PPPoE), Multicast: PIM-SM, PIM-SSM, IGMP v1, v2, and v3.
* Path quality measurement (jitter, packet loss, latency), Initial path selection (PBF), Dynamic path change.
* Key exchange: manual key, IKEv1, and IKEv2 (pre-shared key, certificate-based authentication), Encryption: 3des, AES (128-bit, 192-bit, 256-bit), Authentication: MD5, SHA-1, SHA-256, SHA-384, SHA-512, Large Scale VPN for simplified configuration and management, Secure access over IPsec and SSL VPN tunnels using gateway and portals.
* 802.1Q VLAN tags per device/per interface: 4,094/4,094, Aggregate interfaces (802.3ad), LACP.
* NAT modes (IPv4): static IP, Dynamic IP, Dynamic IP and Port (port address translation), NAT64, NPTv6, Additional NAT features: Dynamic IP reservation, tunable Dynamic IP and Port oversubscription.
* Modes: active/active, active/passive, Failure detection: path monitoring, interface monitoring.
 |
| გარანტია | არანაკლებ 3 წლიანი გარანტია, მწარმოებლის ვებ-გვერდიდან განახლებების გადმოწერის საშუალებით. |

|  |  |
| --- | --- |
| **2) მარშრუტიზატორი**  | **რაოდენობა 2 ცალი**  |
| ინტერფეისები: | მინიმუმ 4 Ethernet 10/100/1000 პორტები (მათ შორის 2 ცალი RJ-45 და 2 ცალი SFP სლოტი) |
| ოპერატიული მეხსიერება: | არანაკლებ 8 GB |
| ფლეშ მეხსიერება: | არანაკლებ 16 GB |
| IPsec SVTI Tunnels ინტერფეისების რაოდენბა | არანაკლებ 2500 |
| Number of VRFs | არანაკლებ 4000 |
| IPv4 მარშრუტების რაოდენობა | არანაკლებ 1.6M |
| IPsec Throughput (IMIX 352 Bytes packet size) | არანაკლებ 900 Mbps |
| პროტოკოლების და ტექნოლოგიების მხარდაჭერა: | * IPv4/IPv6, NAT, ACL, VRF, QoS, P2P-IPSec, MACSec
* RIP, OSPF, BGP, EIGRP, IGRP, IS-IS, On-Demand Routing (ODR), Point-to-Point Protocol (PPP), Multi-Link PPP (MLP),TR-069, TR069-CWMP, TCP (ECN, Window scaling, MSS) Stream Control Transmission Protocol (SCTP).
* LACP, PAgP, EtherChannel, LLDP, 802.1Q
* FHRP, GLBP (global load balancing)
* IPSLA responder, echo, jitter, path (ICMP, UDP, and multicast), TCP connect, HTTP, FTP, DHCP, MQC including classification, policing, re-marking, scheduling; HQoS, NBAR2 (standard protocol packs
* NetFlow, Flexible NetFlow (FNF), IPFIX, performance monitoring, Flexible Packet Matching (FPM), Policy-Based Routing (PBR), ACL, ARP, DHCP, BDI, NAT, PAT – IPv4/v6, Reverse Path Forwarding (URPF), 802.1P, Switch Port Analyzer (SPAN)
* NETCONF/YANG support, Zero Touch Support (PnP/ZTP), EEM Support, RESTCONF, TACACS+, AAA, GNMI, gRPC
* Public Key Infrastructure (PKI), Challenge Handshake (CHAP) and Password Authentication (PAP), Certificate Authority (CA)
* Zone-based firewall, ACL, IPsec (point to point).
* MACsec Key Agreement Protocol, LAN MACsec (128-bit), WAN MACSec (125-/256-bit).
* Bi-Di PIM, IGMP, Protocol Independent Multicast (PIM), mVPN, CGMP, AutoRP, Bootstrap Router (BSR), mroute, MLD (v1, v2), extending SSM support (PIM-SSM, IGMPv3 with SSM), SSM-Mapping, Multicast Source Discovery Protocol (MSDP)
* GRE tunnel, IPv6 over v4 and IPv4 over v6 tunnels, per-tunnel QoS.
* Easy Virtual Network (EVN), vRF-Lite, Multi-VRF, VRF support, SGT, SGACL, SGX.
* 802.1X feature support, RADIUS integration, TACACS/ TACACS+ support, SHA-1, SHA-2, MD5
* DMVPN, GETVPN, FLEXVPN, MACSEC, BFD
 |
| ზემოთ ჩამოთვლილი პროტოკოლების მხარდაჭერის ლიცენზია | არანაკლებ 3 წლიანი  |
| საკომუნიკაციო კარადაში ჩასაყენებელი: | სასურველია 1U სივრცის დაკავება. |
| გარანტია | არანაკლებ 3 წელი მწარმოებლის გარანტია, პროგრამულ განახლებებეზე წვდომით და მწარმოებლის ტექნიკურ ჯგუფთან კავშირის უფლებით. |

|  |  |
| --- | --- |
| **3) კომუტატორი “ა“** | **რაოდენობა 2 ცალი**  |
| ინტერფეისები: | მინიმუმ 48-port 1/10/25 Gb/s SFP/SFP+/SFP28, 8x100/40 Gb/s QSFP28/QSFP+ |
| პაკეტის კომუტაციის წარმადობა: | მინიმუმ 2 Tbps (unidirectional), 4 Tbps (bidirectional).  |
| L2/L3 გამტარიანობა: | მინიმუმ 2900 Mpps. (64 ბაიტიანი პაკეტების დროს) |
| „სტეკირება“ | არანაკლებ 4 კომუტატორის ერთ ვირტუალურ კომუტატორად გაერთიანების შესაძლებლობა („სტეკირება“). |
| კომუტატორს უნდა მოყვებოდეს სტეკირებისთვის 100GB სიჩქარის 3 მეტრიანი დაბოლოებული კაბელი. (ე.წ. DAC კაბელი) |
| კვების ბლოკი | უნდა იყოს აღჭურვილი AC ტიპის დუბლირებული კვების ბლოკით, არანაკლებ 650W სიმძლავრის 220/240V, განაწილების და „ცხელი“ გამოცვლის ფუნქციით. |
| კომუტატორის კონსტრუქცია უნდა იყოს განკუთვნილი 19 დუიმიან საკომუნიკაციო კარადაში მონტაჟისათვის. ასევე უნდა მოიცავდეს მის საკომუნიკაციო კარადაში დასამონტაჟებელ აქსესუარების კომპლექტს |
| მოთხოვნილი ფუნქციონალის მისაღები ლიცენზია უნდა იყოს **მუდმივ მოქმედი,** ე.წ. Perpetual. |
| Performance Scale (Unidimensional) | * Layer 2 - MAC addresses per system: 288,000
* VLAN IDs: 4093
* Number of link aggregation groups (LAGs): 80
* Number of ports per LAG: 64
* Multiple Spanning Tree Protocol (MSTP) instances: 64
* Jumbo frame: 9216 bytes
* Firewall filters Ingress: 1500
* Firewall filters Egress: 512
* Layer 3 - IPv4 unicast prefixes: 360,000
* IPv4 unicast routes: 208,000
* IPv4 multicast routes: 104,000
* ECMP paths: 64
* IPv6 unicast prefixes: 170,000
* IPv6 unicast routes: 104,000
* IPv6 multicast routes: 52,000
* ARP entries: 64,000
 |
| Traffic mirroring | * Mirroring destination ports per switch: 4
* Maximum number of mirroring sessions: 4
* Mirroring destination VLANs per switch: 4
 |
| Layer 2 Features | * STP—IEEE 802.1D (802.1D-2004)
* Rapid Spanning Tree Protocol (RSTP) (IEEE 802.1w); MSTP (IEEE 802.1s)
* Redundant Trunk Group (RTG)
* Bridge protocol data unit (BPDU) protect
* Loop protect
* Root protect
* VLAN—IEEE 802.1Q VLAN trunking
* The Routed VLAN Interface (RVI)
* Port-based VLAN • Private VLAN (PVLAN)
* VLAN translation
* Static MAC address assignment for interface
* Per VLAN MAC learning (limit)
* MAC learning deactivate
* Link Aggregation and Link Aggregation Control Protocol (LACP) (IEEE 802.3ad)
 |
| Link Aggregation | * Multichassis link aggregation (MC-LAG)
* EVPN Multihoming (ESI-LAG)
* LAG load-sharing algorithm—bridged or routed (unicast or multicast) traffic: IP: SIP, Dynamic Internet Protocol (DIP), TCP/UDP source port, TCP/UDP destination port. L2 and non-IP: MAC SA, MAC DA, Ethertype, VLAN ID, source port
 |
| Layer 3 Features (IPv4) | * Static routing
* Routing protocols (RIP, OSPF, IS-IS, BGP)
* Virtual Router Redundancy Protocol (VRRP)
* Bidirectional Forwarding Detection (BFD) protocol
* Virtual router
* Dynamic Host Configuration Protocol (DHCP) relay
* Proxy Address Resolution Protocol (ARP)
 |
| Multicast Features | * Internet Group Management Protocol (IGMP): v1, v2, v3
* IGMP snooping: v1, v2, and v3 (L2 only)
* IGMP Filter
* PIM-SM, PIM-SSM, PIM-DM
* Multicast Source Discovery Protocol (MSDP)
 |
| Security and Filters | * Secure interface login and password
* RADIUS
* TACACS+
* Ingress and egress filters: Allow and deny, port filters, VLAN filters, and routed filters, including management port filters
* Filter actions: Logging, system logging, reject, mirror to an interface, counters, assign forwarding class, permit, drop, police, mark
* SSH v1, v2
* Static ARP support
* Storm control, port error deactivate, and autorecovery
* Sticky MAC address
* DHCP snooping
 |
| Quality of Service (QoS) | * L2 and L3 QoS: Classification, rewrite, queuing
* Rate limiting: Ingress policing: Single-rate two-color policer, two-rate three-color policer. Egress policing: Policer, policer mark down action. Egress shaping: Per queue on each port.
* 10 hardware queues per port (8 unicast and 2 multicast)
* Strict-priority queuing (PQ), shaped-deficit weighted roundrobin (SDWRR), weighted random early detection (WRED), weighted tail drop
* FCoE Initialization Protocol (FIP) snooping
* 802.1p remarking
* L2 classification criteria: Interface, MAC address, Ethertype, 802.1p, VLAN
* Congestion avoidance capabilities: WRED
* Trust IEEE 802.1p (ingress) • Remarking of bridged packets
 |
| Data Center Bridging (DCB) | * Priority-based flow control (PFC)—IEEE 802.1Qbb
* Data Center Bridging Capability Exchange (DCBX), DCBx FCoE, and iSCSI type, length, and value (TLVs)
 |
| High Availability | * Bidirectional Forwarding Detection (BFD)
* Uplink failure detection
* Dynamic Load Balancing
 |
| Server Virtualization Management and SDN-Related Protocols | * VXLAN OVSDB
* EVPN-VXLAN
 |
| Device Management and Operations | * Role-based CLI management and access
* CLI via console, telnet, or SSH
* Extended ping and traceroute
* OS configuration rescue and rollback
* Image rollback • SNMP v1/v2/v3
* OS XML management protocol
* sFlow v5
* Beacon LED for port and system
* Zero Touch Provisioning (ZTP)
* OpenStack Neutron Plug-in • Python
* Telemetry Interface
 |
| Traffic Mirroring | * Port-based
* LAG port
* VLAN-based
* Filter-based
* Mirror to local
* Mirror to remote destinations (L2 over VLAN)
 |
| IEEE Standard | * IEEE standard
* IEEE 802.1D
* IEEE 802.1w
* IEEE 802.1
* IEEE 802.1Q
* IEEE 802.1p
* IEEE 802.1ad
* IEEE 802.3ad
* IEEE 802.1AB
* IEEE 802.3x
 |
| მართვის სისტემა 3 წლიანი ლიცენზია | * ე.წ. Cloud მართვის სისტემა
* Day 0/Day 1: Single-Click activation and autoprovisioning of Switches
* გლობალური შაბლონები კონფიგურაციისთვის
* Device, Port, და Interface პროფილები
* Wired Service Level Expectations (SLEs) მონიტორინგის ფუნქციოინალი
* AI-Native Switch Insights მოწყობილობის მდგომარეობის და დატვურთულობის ხილვადობა
* Dynamic Packet Capture(dPCAP) პაკეტების პროაქტიული დაჭერა და ღრუბელში შენახვა პრობლემის დროს, რათა შესაძლებელი იყოს ინციდენტების გამოიძიების დაჩქარება
* Wired Client Health Metrics დაკავშურებული სვიჩებისა და მოწყობილობების სია, ტოპოლოგია, მათში არსებული Firmware-ის გადამოწმება თანამედროვე ვერსიასთან
* Virtual Network Assistant ხელოვნურ ინტელექტზე დაფუძნებული დამხმარე ინტერფეისი პრობლემების აღმოფხვრის ძიების და წარმადობის ანალიზის პროცესში
* ხელოვნურ ინტელექტზე დაფუძნებული ქსელის ანალიზისა და ტესტირების მექანიზმი, რომელიც სამომხმარებლო ტრაფიკის სიმულაციის გზით ამოწმებს ქსელში არსებულ ვითარებას.
* Network Insights 30 დღემდე ინფორმაციის დაგროვება ანალიტიკის შესაძლებობლისთვის
 |
| საკომუნიკაციო კარადაში ჩასაყენებელი: | სასურველია 1U სივრცის დაკავება. |
| გარანტია | არანაკლებ 3 წელი მწარმოებლის გარანტია, პროგრამულ განახლებებეზე წვდომით და მწარმოებლის ტექნიკურ ჯგუფთან კავშირის უფლებით. |

|  |  |
| --- | --- |
| **4) კომუტატორი “ბ”** | **რაოდენობა 2 ცალი**  |
| ინტერფეისები: | მინიმუმ 24-port 1 Gb/s 4x1G/10G SFP/SFP+ |
| მეხსიერება: | მინიმუმ DRAM: 4 GB with Error Correcting Code (ECC)მინიმუმ Storage: 8 GB |
| პაკეტის კომუტაციის წარმადობა: | მინიმუმ 64 Gbps (unidirectional)/128 Gbps (bidirectional) |
| L2/L3 გამტარიანობა: | მინიმუმ 95Mpps. (64 ბაიტიანი პაკეტების დროს) |
| „სტეკირება“ | არანაკლებ 6 კომუტატორის ერთ ვირტუალურ კომუტატორად გაერთიანების შესაძლებლობა („სტეკირება“). |
| კომუტატორის კონსტრუქცია უნდა იყოს განკუთვნილი 19 დუიმიან საკომუნიკაციო კარადაში მონტაჟისათვის. ასევე უნდა მოიცავდეს მის საკომუნიკაციო კარადაში დასამონტაჟებელ აქსესუარების კომპლექტს |
| Security | * Media Access Control (MAC) limiting (per port and per VLAN)
* Allowed MAC addresses: 32,000
* Dynamic Address Resolution Protocol (ARP) dynamic ARP inspection (DAI)
* IP source guard
* Local proxy ARP
* Static ARP support
* Dynamic Host Configuration Protocol (DHCP) snooping
* Captive portal
* Persistent MAC address configurations
* Distributed denial of service (DDoS) protection (CPU control path flooding protection)
 |
| Layer 2 Switching | * Maximum MAC addresses per system: 32,000
* Jumbo frames: 9216 bytes
* Concurrent Active VLAN: 1020
* Range of possible VLAN IDs: 1 to 4094
* Virtual Spanning Tree (VST) instances: 253
* Port-based VLAN
* Voice VLAN
* Physical port redundancy: Redundant trunk group (RTG)
* Compatible with Per-VLAN Spanning Tree Plus (PVST+)
* Routed VLAN interface (RVI)
* Uplink failure detection (UFD)
* ITU-T G.8032: Ethernet Ring Protection Switching
* IEEE 802.1AB: Link Layer Discovery Protocol (LLDP)
* LLDP-MED with VoIP integration
* Default VLAN and multiple VLAN range support
* MAC learning deactivate
* Persistent MAC learning (sticky MAC)
* MAC notification
* Private VLANs (PVLANs)
* Explicit congestion notification (ECN)
* Layer 2 protocol tunneling (L2PT)
* IEEE 802.1ak: Multiple VLAN Registration Protocol (MVRP)
* IEEE 802.1p: Class of Service (CoS) prioritization
* IEEE 802.1Q: VLAN tagging
* IEEE 802.1X: Port Access Control
* IEEE 802.1ak: Multiple Registration Protocol
* IEEE 802.3: 10BASE-T
* IEEE 802.3u: 100BASE-T
* IEEE 802.3ab: 1000BASE-T
* IEEE 802.3z: 1000BASE-X
* IEEE 802.3ae: 10-Gigabit Ethernet
* IEEE 802.3by: 25-Gigabit Ethernet
* IEEE 802.3af: Power over Ethernet
* IEEE 802.3at: Power over Ethernet Plus
* IEEE 802.3x: Pause Frames/Flow Control
* IEEE 802.3ah: Ethernet in the First Mile
 |
| Spanning Tree | * IEEE 802.1D: Spanning Tree Protocol
* IEEE 802.1s: Multiple Spanning Tree Protocol (MSTP)
* Number of MSTP instances supported: 64
* Number of VLAN Spanning Tree Protocol (VSTP) instances supported: 253
* IEEE 802.1w: Rapid reconfiguration of Spanning Tree Protocol
 |
| Link Aggregation | * IEEE 802.3ad: Link Aggregation Control Protocol
* 802.3ad (LACP) support:
* Number of LAGs supported: 128
* Maximum number of ports per LAG: 8
* LAG load-sharing algorithm bridged or routed (unicast or multicast) traffic:
* IP: S/D IP
* TCP/UDP: S/D IP, S/D Port
* Non-IP: S/D MAC
* Tagged ports support in LAG
 |
| Layer 3 Features: IPv4 | * Maximum number of ARP entries: 4,000
* Maximum number of IPv4 unicast routes in hardware: 1,000 prefixes; 7,800 host routes
* Maximum number of IPv4 multicast routes in hardware: 3,200 multicast routes
* Routing protocols: RIPv1/v2, OSPF, BGP, IS-IS
* Static routing
* Routing policy
* Bidirectional Forwarding Detection (BFD)
* L3 redundancy: Virtual Router Redundancy Protocol (VRRP)
* VRF-Lite
 |
| Layer 3 Features: IPv6 | * Maximum number of neighbor discovery (ND) entries: 3,000
* Maximum number of IPv6 unicast routes in hardware: 1,000 prefixes; 3,800 host routes
* Maximum number of IPv6 multicast routes in hardware: 1,650 multicast routes
* Routing protocols: RIPng, OSPFv3, IPv6, IS-IS
* Static routing
 |
| Access Control Lists (ACLs) | * ACL entries (ACE) in hardware per system:
* Port-based ACL (PACL) ingress: 510
* VLAN-based ACL (VACL) ingress: 510
* Router-based ACL (RACL) ingress: 510
* Port-based ACL (PACL) egress: 510
* VLAN-based ACL (VACL) egress: 255
* Egress across RACL: 510
* ACL counter for denied packets
* ACL counter for permitted packets
* Ability to add/remove/change ACL entries in middle of list (ACL editing)
* L2-L4 ACL
 |
| Access Security | * 802.1X port-based
* 802.1X multiple supplicants
* 802.1X with VLAN assignment
* 802.1X with authentication bypass access (based on host MAC address)
* 802.1X with VoIP VLAN support
* 802.1X dynamic ACL based on RADIUS attributes
* 802.1X Supported Extensible Authentication Protocol (EAP) types: Message Digest 5 (MD5), Transport Layer Security (TLS), Tunneled TLS (TTLS), Protected Extensible Authenticated Protocol (PEAP)
* MAC authentication (RADIUS)
* Control plane DoS protection
* Radius functionality over IPv6 for authentication, authorization, and accounting (AAA)
* DHCPv6 snooping
* IPv6 neighbor discovery
* IPv6 source guard
* IPv6 router advertisement (RA) guard
* IPv6 Neighbor Discovery Inspection
 |
| High Availability | * GRES for Layer 2 hitless forwarding and Layer 3 protocols on RE failover
* Graceful protocol restart (OSPF, BGP)
* Layer 2 hitless forwarding on RE failover
* Nonstop bridging: LACP, xSTP
* Nonstop routing: PIM, OSPF v2 and v3, RIP v2, RIPng, BGP, BGPv6, IS-IS, IGMP v1, v2, v3
 |
| Quality of Service | * L2 QoS
* L3 QoS
* Ingress policing: 1 rate 2 color
* Hardware queues per port: 12 (8 unicast + 4 multicast)
* Scheduling methods (egress): Strict priority (SP), weighted deficit round-robin (WDRR)
* 802.1p, DiffServ code point (DSCP)/IP precedence trust and marking
* L2-L4 classification criteria: Interface, MAC address, Ethertype, 802.1p, VLAN, IP address, DSCP/IP precedence, TCP/UDP port numbers, and more
* Congestion avoidance capabilities: Tail drop, weighted random early detection (WRED)
 |
| Multicast | * IGMP: v1, v2, v3
* IGMP snooping
* Multicast Listener Discovery (MLD) snooping
* Protocol Independent Multicast-Sparse Mode (PIM-SM), PIM Source-Specific Mode (PIM-SSM), PIM Dense Mode (PIM-DM)
 |
| Device Management and Operations | * Role-based CLI management and access
* CLI via console, telnet, or SSH
* Extended ping and traceroute
* OS configuration rescue and rollback
* Image rollback • SNMP v1/v2/v3
* OS XML management protocol
* sFlow v5
* Beacon LED for port and system
* Zero Touch Provisioning (ZTP)
* OpenStack Neutron Plug-in • Python
* Telemetry Interface
 |
| Traffic Mirroring | * Port-based
* LAG port
* VLAN-based
* Filter-based
* Mirror to local
* Mirror to remote destinations (L2 over VLAN)
 |
| IEEE Standard | * IEEE standard
* IEEE 802.1D
* IEEE 802.1w
* IEEE 802.1
* IEEE 802.1Q
* IEEE 802.1p
* IEEE 802.1ad
* IEEE 802.3ad
* IEEE 802.1AB
* IEEE 802.3x
 |
| Device Management and Operations | * OS CLI
* Out-of-band management: Serial; 10/100/1000BASE-T Ethernet
* Rescue configuration
* Configuration rollback
* Image rollback
* RMON (RFC2819) groups 1, 2, 3, 9
* Remote performance monitoring
* SNMP: v1, v2c, v3
* Network Time Protocol (NTP)
* DHCP server
* DHCP client and DHCP proxy
* DHCP relay and helper
* DHCP local server support
* RADIUS
* TACACS+
* SSHv2
* Secure copy
* HTTP/HTTPs
* Domain Name System (DNS) resolver
* System logging
* Temperature sensor
* Configuration backup via FTP/secure copy
 |
| Troubleshooting | * Debugging: CLI via console, Telnet, or SSH
* Diagnostics: Show and debug command, statistics
* Traffic mirroring (port)
* Traffic mirroring (VLAN)
* IP tools: Extended ping and trace
* commit and rollback
 |
| Traffic Monitoring | * ACL-based mirroring
* Mirroring destination ports per system: 4
* LAG port monitoring
* Multiple destination ports monitored to 1 mirror (N:1)
* Maximum number of mirroring sessions: 4
* Mirroring to remote destination (over L2): 1 destination VLAN
 |
| მართვის სისტემა 3 წლიანი ლიცენზია | * ე.წ. Cloud მართვის სისტემა
* Day 0/Day 1: Single-Click activation and autoprovisioning of Switches
* გლობალური შაბლონები კონფიგურაციისთვის
* Device, Port, და Interface პროფილები
* Wired Service Level Expectations (SLEs) მონიტორინგის ფუნქციოინალი
* AI-Native Switch Insights მოწყობილობის მდგომარეობის და დატვურთულობის ხილვადობა
* Dynamic Packet Capture(dPCAP) პაკეტების პროაქტიული დაჭერა და ღრუბელში შენახვა პრობლემის დროს, რათა შესაძლებელი იყოს ინციდენტების გამოიძიების დაჩქარება
* Wired Client Health Metrics დაკავშურებული სვიჩებისა და მოწყობილობების სია, ტოპოლოგია, მათში არსებული Firmware-ის გადამოწმება თანამედროვე ვერსიასთან
* Virtual Network Assistant ხელოვნურ ინტელექტზე დაფუძნებული დამხმარე ინტერფეისი პრობლემების აღმოფხვრის ძიების და წარმადობის ანალიზის პროცესში
* ხელოვნურ ინტელექტზე დაფუძნებული ქსელის ანალიზისა და ტესტირების მექანიზმი, რომელიც სამომხმარებლო ტრაფიკის სიმულაციის გზით ამოწმებს ქსელში არსებულ ვითარებას.
* Network Insights 30 დღემდე ინფორმაციის დაგროვება ანალიტიკის შესაძლებობლისთვის
 |
| საკომუნიკაციო კარადაში ჩასაყენებელი: | სასურველია 1U სივრცის დაკავება. |
| გარანტია | არანაკლებ 3 წელი მწარმოებლის გარანტია, პროგრამულ განახლებებეზე წვდომით და მწარმოებლის ტექნიკურ ჯგუფთან კავშირის უფლებით. |

|  |  |
| --- | --- |
| **5) კომუტატორი “გ”** | **რაოდენობა 1 ცალი**  |
| ინტერფეისები: | მინიმუმ 48-port 1 Gb/s 4x1G/10G SFP/SFP+ |
| მეხსიერება: | მინიმუმ DRAM: 4 GB with Error Correcting Code (ECC)მინიმუმ Storage: 8 GB |
| პაკეტის კომუტაციის წარმადობა: | მინიმუმ 88 Gbps (unidirectional)/176 Gbps (bidirectional) |
| L2/L3 გამტარიანობა: | მინიმუმ 130Mpps. (64 ბაიტიანი პაკეტების დროს) |
| „სტეკირება“ | არანაკლებ 6 კომუტატორის ერთ ვირტუალურ კომუტატორად გაერთიანების შესაძლებლობა („სტეკირება“). |
| კომუტატორის კონსტრუქცია უნდა იყოს განკუთვნილი 19 დუიმიან საკომუნიკაციო კარადაში მონტაჟისათვის. ასევე უნდა მოიცავდეს მის საკომუნიკაციო კარადაში დასამონტაჟებელ აქსესუარების კომპლექტს |
| Security | * Media Access Control (MAC) limiting (per port and per VLAN)
* Allowed MAC addresses: 32,000
* Dynamic Address Resolution Protocol (ARP) dynamic ARP inspection (DAI)
* IP source guard
* Local proxy ARP
* Static ARP support
* Dynamic Host Configuration Protocol (DHCP) snooping
* Captive portal
* Persistent MAC address configurations
* Distributed denial of service (DDoS) protection (CPU control path flooding protection)
 |
| Layer 2 Switching | * Maximum MAC addresses per system: 32,000
* Jumbo frames: 9216 bytes
* Concurrent Active VLAN: 1020
* Range of possible VLAN IDs: 1 to 4094
* Virtual Spanning Tree (VST) instances: 253
* Port-based VLAN
* Voice VLAN
* Physical port redundancy: Redundant trunk group (RTG)
* Compatible with Per-VLAN Spanning Tree Plus (PVST+)
* Routed VLAN interface (RVI)
* Uplink failure detection (UFD)
* ITU-T G.8032: Ethernet Ring Protection Switching
* IEEE 802.1AB: Link Layer Discovery Protocol (LLDP)
* LLDP-MED with VoIP integration
* Default VLAN and multiple VLAN range support
* MAC learning deactivate
* Persistent MAC learning (sticky MAC)
* MAC notification
* Private VLANs (PVLANs)
* Explicit congestion notification (ECN)
* Layer 2 protocol tunneling (L2PT)
* IEEE 802.1ak: Multiple VLAN Registration Protocol (MVRP)
* IEEE 802.1p: Class of Service (CoS) prioritization
* IEEE 802.1Q: VLAN tagging
* IEEE 802.1X: Port Access Control
* IEEE 802.1ak: Multiple Registration Protocol
* IEEE 802.3: 10BASE-T
* IEEE 802.3u: 100BASE-T
* IEEE 802.3ab: 1000BASE-T
* IEEE 802.3z: 1000BASE-X
* IEEE 802.3ae: 10-Gigabit Ethernet
* IEEE 802.3by: 25-Gigabit Ethernet
* IEEE 802.3af: Power over Ethernet
* IEEE 802.3at: Power over Ethernet Plus
* IEEE 802.3x: Pause Frames/Flow Control
* IEEE 802.3ah: Ethernet in the First Mile
 |
| Spanning Tree | * IEEE 802.1D: Spanning Tree Protocol
* IEEE 802.1s: Multiple Spanning Tree Protocol (MSTP)
* Number of MSTP instances supported: 64
* Number of VLAN Spanning Tree Protocol (VSTP) instances supported: 253
* IEEE 802.1w: Rapid reconfiguration of Spanning Tree Protocol
 |
| Link Aggregation | * IEEE 802.3ad: Link Aggregation Control Protocol
* 802.3ad (LACP) support:
* Number of LAGs supported: 128
* Maximum number of ports per LAG: 8
* LAG load-sharing algorithm bridged or routed (unicast or multicast) traffic:
* IP: S/D IP
* TCP/UDP: S/D IP, S/D Port
* Non-IP: S/D MAC
* Tagged ports support in LAG
 |
| Layer 3 Features: IPv4 | * Maximum number of ARP entries: 4,000
* Maximum number of IPv4 unicast routes in hardware: 1,000 prefixes; 7,800 host routes
* Maximum number of IPv4 multicast routes in hardware: 3,200 multicast routes
* Routing protocols: RIPv1/v2, OSPF, BGP, IS-IS
* Static routing
* Routing policy
* Bidirectional Forwarding Detection (BFD)
* L3 redundancy: Virtual Router Redundancy Protocol (VRRP)
* VRF-Lite
 |
| Layer 3 Features: IPv6 | * Maximum number of neighbor discovery (ND) entries: 3,000
* Maximum number of IPv6 unicast routes in hardware: 1,000 prefixes; 3,800 host routes
* Maximum number of IPv6 multicast routes in hardware: 1,650 multicast routes
* Routing protocols: RIPng, OSPFv3, IPv6, IS-IS
* Static routing
 |
| Access Control Lists (ACLs) | * ACL entries (ACE) in hardware per system:
* Port-based ACL (PACL) ingress: 510
* VLAN-based ACL (VACL) ingress: 510
* Router-based ACL (RACL) ingress: 510
* Port-based ACL (PACL) egress: 510
* VLAN-based ACL (VACL) egress: 255
* Egress across RACL: 510
* ACL counter for denied packets
* ACL counter for permitted packets
* Ability to add/remove/change ACL entries in middle of list (ACL editing)
* L2-L4 ACL
 |
| Access Security | * 802.1X port-based
* 802.1X multiple supplicants
* 802.1X with VLAN assignment
* 802.1X with authentication bypass access (based on host MAC address)
* 802.1X with VoIP VLAN support
* 802.1X dynamic ACL based on RADIUS attributes
* 802.1X Supported Extensible Authentication Protocol (EAP) types: Message Digest 5 (MD5), Transport Layer Security (TLS), Tunneled TLS (TTLS), Protected Extensible Authenticated Protocol (PEAP)
* MAC authentication (RADIUS)
* Control plane DoS protection
* Radius functionality over IPv6 for authentication, authorization, and accounting (AAA)
* DHCPv6 snooping
* IPv6 neighbor discovery
* IPv6 source guard
* IPv6 router advertisement (RA) guard
* IPv6 Neighbor Discovery Inspection
 |
| High Availability | * GRES for Layer 2 hitless forwarding and Layer 3 protocols on RE failover
* Graceful protocol restart (OSPF, BGP)
* Layer 2 hitless forwarding on RE failover
* Nonstop bridging: LACP, xSTP
* Nonstop routing: PIM, OSPF v2 and v3, RIP v2, RIPng, BGP, BGPv6, IS-IS, IGMP v1, v2, v3
 |
| Quality of Service | * L2 QoS
* L3 QoS
* Ingress policing: 1 rate 2 color
* Hardware queues per port: 12 (8 unicast + 4 multicast)
* Scheduling methods (egress): Strict priority (SP), weighted deficit round-robin (WDRR)
* 802.1p, DiffServ code point (DSCP)/IP precedence trust and marking
* L2-L4 classification criteria: Interface, MAC address, Ethertype, 802.1p, VLAN, IP address, DSCP/IP precedence, TCP/UDP port numbers, and more
* Congestion avoidance capabilities: Tail drop, weighted random early detection (WRED)
 |
| Multicast | * IGMP: v1, v2, v3
* IGMP snooping
* Multicast Listener Discovery (MLD) snooping
* Protocol Independent Multicast-Sparse Mode (PIM-SM), PIM Source-Specific Mode (PIM-SSM), PIM Dense Mode (PIM-DM)
 |
| Device Management and Operations | * Role-based CLI management and access
* CLI via console, telnet, or SSH
* Extended ping and traceroute
* OS configuration rescue and rollback
* Image rollback • SNMP v1/v2/v3
* OS XML management protocol
* sFlow v5
* Beacon LED for port and system
* Zero Touch Provisioning (ZTP)
* OpenStack Neutron Plug-in • Python
* Telemetry Interface
 |
| Traffic Mirroring | * Port-based
* LAG port
* VLAN-based
* Filter-based
* Mirror to local
* Mirror to remote destinations (L2 over VLAN)
 |
| IEEE Standard | * IEEE standard
* IEEE 802.1D
* IEEE 802.1w
* IEEE 802.1
* IEEE 802.1Q
* IEEE 802.1p
* IEEE 802.1ad
* IEEE 802.3ad
* IEEE 802.1AB
* IEEE 802.3x
 |
| Device Management and Operations | * OS CLI
* Out-of-band management: Serial; 10/100/1000BASE-T Ethernet
* Rescue configuration
* Configuration rollback
* Image rollback
* RMON (RFC2819) groups 1, 2, 3, 9
* Remote performance monitoring
* SNMP: v1, v2c, v3
* Network Time Protocol (NTP)
* DHCP server
* DHCP client and DHCP proxy
* DHCP relay and helper
* DHCP local server support
* RADIUS
* TACACS+
* SSHv2
* Secure copy
* HTTP/HTTPs
* Domain Name System (DNS) resolver
* System logging
* Temperature sensor
* Configuration backup via FTP/secure copy
 |
| Troubleshooting | * Debugging: CLI via console, Telnet, or SSH
* Diagnostics: Show and debug command, statistics
* Traffic mirroring (port)
* Traffic mirroring (VLAN)
* IP tools: Extended ping and trace
* commit and rollback
 |
| Traffic Monitoring | * ACL-based mirroring
* Mirroring destination ports per system: 4
* LAG port monitoring
* Multiple destination ports monitored to 1 mirror (N:1)
* Maximum number of mirroring sessions: 4
* Mirroring to remote destination (over L2): 1 destination VLAN
 |
| მართვის სისტემა 3 წლიანი ლიცენზია | * ე.წ. Cloud მართვის სისტემა
* Day 0/Day 1: Single-Click activation and autoprovisioning of Switches
* გლობალური შაბლონები კონფიგურაციისთვის
* Device, Port, და Interface პროფილები
* Wired Service Level Expectations (SLEs) მონიტორინგის ფუნქციოინალი
* AI-Native Switch Insights მოწყობილობის მდგომარეობის და დატვურთულობის ხილვადობა
* Dynamic Packet Capture(dPCAP) პაკეტების პროაქტიული დაჭერა და ღრუბელში შენახვა პრობლემის დროს, რათა შესაძლებელი იყოს ინციდენტების გამოიძიების დაჩქარება
* Wired Client Health Metrics დაკავშურებული სვიჩებისა და მოწყობილობების სია, ტოპოლოგია, მათში არსებული Firmware-ის გადამოწმება თანამედროვე ვერსიასთან
* Virtual Network Assistant ხელოვნურ ინტელექტზე დაფუძნებული დამხმარე ინტერფეისი პრობლემების აღმოფხვრის ძიების და წარმადობის ანალიზის პროცესში
* ხელოვნურ ინტელექტზე დაფუძნებული ქსელის ანალიზისა და ტესტირების მექანიზმი, რომელიც სამომხმარებლო ტრაფიკის სიმულაციის გზით ამოწმებს ქსელში არსებულ ვითარებას.
* Network Insights 30 დღემდე ინფორმაციის დაგროვება ანალიტიკის შესაძლებობლისთვის
 |
| საკომუნიკაციო კარადაში ჩასაყენებელი: | სასურველია 1U სივრცის დაკავება. |
| გარანტია | არანაკლებ 3 წელი მწარმოებლის გარანტია, პროგრამულ განახლებებეზე წვდომით და მწარმოებლის ტექნიკურ ჯგუფთან კავშირის უფლებით. |