## ქსელური ეკრანი - 4 (ოთხი) ცალი ფიზიკური მოწყობილობა

RMG ქსელური ინფრასტრუქტურის ორ ლოკაციაზე, უსაფრთხოების უზრუნველყოფა ახალი თაობის ბრანდმაუერის კლასტერებით:

**მარშრუტიზატორს უნდა გააჩნდეს შემდეგი ტექნიკური მახასიათებლები:**

| | |
|---|---|
| 1. თითოეული კლასტერი უნდა შედგებოდეს არანაკლებ ორი ფიზიკური წევრისგან [ორ ლოკაციაზე ჯამში 4xPhysical Gateway]. | |
| 2. თითოეულ კლასტერს უნდა გააჩნდეს Active-Active და Active-Passive მაღალმდგარად რეჟიმში მუშაობის შესაძლებლობა. | |
| 3. თითოეულ კლასტერის წევრებს შორის უნდა ხდებოდეს სესიებისა და კონფიგურაციის სინქრონიზაცია და თითოეული სესია უნდა დუბლირდებოდეს მის მინიმუმ ერთ წევრზე. | |
| 4. Active-Active რეჟიმში თითოეულ კლასტერში დატვირთულობა უნდა ნაწილდებოდეს ავტომატურ რეჟიმში. | |
| 5. VPN, Networking and Clustering, IPS, Application Control, URL Filtering, Anti-Virus, Anti-Bot, Network Policy Management, Logging and Status, HTTPS Inspection, Sandbox - ჩამოთვლილი ტექნიკური მახასიათებლები მხარდაჭერილ უნდა იქნას გამოყოფილი ან ჩაშენებული ლიცენზიებით. | |
| 6. თითოეულ მოწყობილობაზე SSD ტიპის მონაცემთა სანახი - არანაკლებ 240GB | |
| 7. ლოგების უნდა ინახებოდეს არანაკლებს 30 დღე. ლოგების გაგზანა შესაძლებელი უნდა იყოს იგივე მწარმოებლის ლოგირების სისტემაზე ან Syslog სერვერზე. | |
| 8. თითოეულ კლასტერში არსებულ ყოველ წევრს უნდა გააჩნდეს შემდეგი ფუნქციონალი და ტექნიკური მახასიათებლები: | |
| **Network interfaces** | • არანაკლებ - 4x GE RJ45;<br>• არანაკლებ - 4x GE SFP;<br>• არანაკლებ - 1x GE RJ45 HA/Synch Ports;<br>• არანაკლებ - 1x RJ-45 Serial Console Port;<br>• არანაკლებ - 1x RJ-45 Dedicated Management Port;<br>• არანაკლებ - 1x USB; |
| **Power** | • არანაკლებ 1 x AC ტიპის. [საჭიროების შემთხვევაში შესაძლებელი უნდა იყოს მეორე კვების მოდულის დამატება.] |
| **General Performance** | • Statefull Firewall+Application Control Throughput - **არანაკლებ 1.6 Gbps**<br>• IPS+Application Control+AV+Cloud Sandbox Throughput - **არანაკლებ 900 Mbps;**<br>• IPSec VPN Throughput - **არანაკლებ 1.3 Gbps;**<br>• New HTTP sessions per sec. - **არანაკლებ 8 600;**<br>• Maximum HTTP concurrent sessions - **არანაკლებ 128 000**<br>Insert Details |
| **VPN** | • IPSec VPN:<br>- Topology types: User-to-Site, Site-to-Site, Point-to-Point, Point-to-Multipoint.<br>- Peer authentication methods: certificate, pre-shared key. |

| | |
|---|---|
| | - Peer identification methods Distinguished Name (Subject), FQDN (hostname), IP address or User FQDN (email address).<br>- IKEv1, IKEv2 support.<br>- Supported cryptography algorithms: DES, 3DES, AES128. AES192, AES256.<br>- Supported hashing algorithms: MD5, SHA1, SHA256; SHA384, SHA512.<br>- Diffie-Hellman Groups: 1, 2, 5, 14, 19, 20.<br>- NAT Traversal support.<br>• SSL VPN:<br>- SSL VPN connection methods: via VPN User Agent, via Web-browser (agentless).<br>- VPN user authentication: local, external, multifactor, SSO.<br>- User security policy compliance check support.<br>- User access restrictions support considering used applications and SaaS.<br>- Captive Portal customization support.<br>- Split Tunneling option support.<br>• Encapsulation and inspection abilities:<br>- GRE<br>- Optional - Non-encrypted IPSec, Transport mode AH IPSec, General Packet Radio Service (GPRS) Tunneling Protocol for User Data (GTP-U). |
| **Network and other technologies** | • Supported L2/L3 features: VLAN, L2/L3 Subinterfaces, LACP, Jumbo Frames, LLDP, Loopback Interfaces;<br>• Static/dynamic routing, PBR, VRF and Path monitoring support;<br>• Supported dynamic routing protocols and features: RIPv2, OSPF v2/v3, BGP4, Route Redistribution, BFD;<br>• Multicast options: IGMP, PIM-SM, PIM-ASM, PIM-SSM, SPT, RPF;<br>• IPv6 support: IPv6 management, IPv6 routing, IPv6 VPN, full IPv6 NGFW, NAT46, NAT64, IPv6 IPsec VPN;<br>• Interface operational modes: Span Monitoring, Virtual Wire Pair, L2 Transparent, L3/NAT; |

| | |
|---|---|
| | • NAT features supported: SNAT, DNAT, static/dynamic NAT, PAT, DNAT with DNS Rewrite, DHCP Relay;<br>• Built-in DHCP and DNS servers;<br>• Statefull Firewall functionality;<br>• QoS support regarding applications, users, URL or other conditions;<br>• SD-WAN options:<br>- Support latency, delay and packet loss conditions for path selection;<br>- SD-WAN monitoring support for VPN connections;<br>- Support ZTP feature and automatic devices to SD-WAN inclusion<br>- Supported Forward Error Correction and Packet Deduplication features<br>- SaaS direct connection monitoring feature support<br><br>• Web-interface or CLI<br>- Read-only, restricted or read-write modes support<br>• IoT access control:<br>- Automatic detection and classification of IoT devices.<br>- Automatic vulnerability determination and evaluation of risk.<br>- Automatic policy applying to IoT devices on the firewall.<br>• Optional<br>- ALG role supported for: SIP, SCCP, MGCP, FTP, RTSP, MySQL, Oracle/SQLNet/TNS, RPC, RSH, UNIStim, H.225, H.248;<br>- Ability to add X-Forwarded For header to HTTP packets;<br>- Dedicated separate resources for management tasks. |
| **Authentication and PKI** | • Local user database;<br>• Ability to authenticate users via open XML API, Captive Portal, WMI polling, NetBios and WinRM methods;<br>• Supported authentication protocols: LDAP, Radius, TACACS+, Kerberos;<br>• Single-Sign-On and SAML features support; |

| | |
|---|---|
| | • Multifactor authentication features: integrated token-server, SMS, Voice, Push, OTP delivery methods. Integration with public authentication services (eg, OKTA, DUO, UbiKey, RSA);<br>• PKI and certificates features: X.509 standard, SCEP, CSR, OCSP support;<br>• Third party HSM integration support;<br>• SSL Inspection:<br>- Exceptions for certificate check for known services.<br>- Flexible settings for certificates that do not pass validation<br>- Port mirroring option;<br>- TLS 1.3 support<br>• SSH inspection support. |
| **High Availability** | • Supported HA modes: active/active, active/passive;<br>• Link and connections monitoring;<br>• Configuration, routing table and connection table synchronization support;<br>• Virtual appliances clustering support;<br>• Geo clustering feature support. |
| **Application Control** | • Defining type of application that uses standard, non-standard and dynamic TCP/UDP ports using: application signatures, protocol decoders, context signatures, heuristic and behavioral analysis;<br>• Ability to define types of applications which use HTTP 2.0;<br>• Custom application signatures creating support;<br>• Ability to block files depending on their extensions and applications that allow them to be transferred. Ability to customize user warnings about trying to download files that may contain malicious content; |
| **Security Systems** | • **IPS:**<br>- Vulnerability protection using various sources of signatures (eg, third-party sources, own team of developers, Cyber Threat Alliance).<br>- Blocked packets/files logging.<br>- Ability to create custom IPS signatures.<br>- Ability to make exceptions for certain IPS signatures.<br>- Brute-Force attack signatures. |

| | |
|---|---|
| | - Optional - Cisco Trustsec integration support (SGT tags reading and applying to information-based security policies).<br><br>• **Antivirus:**<br>- Inspected protocols: HTTP, FTP, SMTP, POP3, IMAP, SMB.<br>- Built-in machine learning techniques to detect and block PowerShell and JavaScript scripts.<br>- Cloud file behavior analysis service support (Cloud Sandbox) and ability to receive signatures in real-time.<br>- Flow scanning antivirus mode without file caching<br>• URL-filtering:<br>- Real-time DNS/URL filtering using cloud or local databases.<br>- Comprehensive URL categorization.<br>- Custom URL categories support.<br>- Ability to grant access to individual blocked web pages using an additional password<br>- Safe Search support (Google, Yahoo,Yandex, Youtube)<br>- Customizable web-block pages<br>- Ability to request the URL category change directly from the device web interface.<br>- User credentials theft protection.<br>- Optional - Using external dynamic URL/DNS/IP addresses lists from external sourses (e.g. Spamhaus, etc.).<br>- Optional - Use built-in machine learning for detection of malicious and phishing URLs.<br>• DNS Security<br>- Malicious domain name database updated from a variety of sources, including the vendor's security research center and third-party sources.<br>- Optional - DGA and Fast Flux attack prevention using machine learning techniques.<br>- Optional - Tunneled DNS traffic inspection |

| | |
|---|---|
| | - Ability to analyse suspicious DNS queries and localize compromised hosts using DNS server response substitution feature or similar to it.<br><br>• (Optional) DLP:<br>- Supported protocols: HTTP, FTP, SMB<br>- Object inspection by: file extension types, custom templates using regular expressions<br>- Ability to use pre-defined filters and templates for third-party cloud services (eg, Microsoft Azure, Titus)<br>• DoS/DDoS protection:<br>- IPv4 and IPv6 DOS/DDoS attack and scan protection, such as: TCP/UDP/SCTP port scan, ICMP sweep, TCP/UDP/SCTP/ICMP flood (source/destination), etc. by limiting the amount of traffic of the protocols or limiting the number of TCP connections for each individual source.<br>- Syn-Cookie feature support |
| **Management, monitoring and diagnostics** | • System access support via: HTTPS, SSH, Telnet, serial;<br>• SNMPv2/3 and Syslog (BSD, IETF extensions) support;<br>• Netflow v9.0 support;<br>• Integration with the centralized management, monitoring and reporting system;<br>• E-mail notifications and alerts. Ability to self-determination of the risk level for various event types;<br>• Advanced visibility and individual dashboards by categories:<br>- Used applications<br>- User activity<br>- Tunnel and VPN activity<br>- Activity on SSL traffic (used cipher suites, connection errors, etc.)<br>- Threats.<br>• Advanced logging by categories:<br>- System events<br>- Traffic events<br>- Security events |

| | |
|---|---|
| | - Decryption events<br>- URL-filtering<br>- Tunnel and VPN events<br>- User activity and authentication events<br>• Automatic log correlation;<br>• Reports autogeneration and scheduling:<br>- by information categories (blocked threats, user activities, applications, etc.)<br>- Report customization support<br>- Ability to view reports via the device's web interface<br>- Optional - Exporting supported formats: PDF, CSV<br>• Optional - Built-in troubleshooting tools:<br>- Policy optimization tool<br>- Packet capture tool<br>- Active connection monitoring tool<br>- Traffic and threat global map<br>• **Optional** - Ability to use additional tools providing best practices recommendations, converting configuration for easy migration, quick deployment and so on |
| **Sandboxing** | • Sandboxing უნდა უზრუნველყოფდეს ე.წ. Zero Day Attack ტიპის შეტევისგან დაცვას.<br>• Sandbox გადაწყვეტილება უნდა ახდენდეს არქივების, დოკუმენტების, მათ შორის ჯავა და ფლეშ ფაილების ემულაციას, როგორც საფოსტო მიბმული ფაილებიდან ასევე ვებ ტრაფიკიდან: doc, .docx, .exe, .jar (not executable only).PIF, .PDF .pkg, .ppt, .pptx, ps1, RTF .rar, .Seven-Z, .js, .xls, .xlsx, XML .zip,.bat, .vbs, (*)…<br>• ოპერაციული სისტემების მხარდაჭერა მინიმუმ: Windows 10 და Customized Images.<br>• ემულაციის ძრავი უნდა ახდენდეს ინსპექტირებას, ემულაციას, აღკვეთას და მოვლენების გადაგზავნას.<br>• CPU-level, OS-level და სტატიკური ფაილის ანალიზის შესაძლებლობა.<br>• გადაწყვეტილება უნდა ახდენდეს ფაილების ემულაციას ქლაუდში მინიმალური ზომიდან არანაკლებ 15 მბ-დე.<br>• Sandbox გადაწყვეტილებას უნდა გააჩნდეს შეტევის აღმოჩენის შესაძლებლობა |

| | |
|---|---|
| | ექსპლოიტის შესრულების სტადიაში - ანუ მანამ სანამ გაეშვება Shell-Code და მოხდება თავად კოდის ჩატვირთვა/შესრულება.<br>• Sandbox გადაწყვეტილება უნდა ახდენდეს ბმულების სკანირებას ელ. ფოსტაში Zero Day და Malware ტიპის შეტევებისგან თავდასაცავად.<br>• Sandbox გადაწყვეტილება უნდა აგენერირებდეს დეტალურ ანგარიშს თითოეული ფაილის ანალიზის შესახებ.<br>• საჭიროების დადგომის შემთხვევაში, სისტემას უნდა შეეძლოს ამავე მწარმოებლის Sandbox Appliance-სთან ინტეგრაცია კრიტიკული ფაილების (დოკუმენტების) ლოკალური ემულაციისთვის. |

**ცენტრალური მართვისა და ლოგირების სისტემის შემოთავაზების შემთხვევაში, გადაწყვეტილება უნდა აკმაყოფილებდეს შემდეგ ტექნიკურ მოთხოვნებს:**

- გადაწყვეტილება უნდა იყოს ცენტრალიზებული ფიზიკური ან ვირტუალური მოწყობილობა და გააჩნდეს გრაფიკული ინტერფეისი. უნდა მართავდეს ქსელის პერიმეტრზე განთავსებულ ბრანდმაუერების კლასტერს არანაკლებ HTTPS, SSH და SNMP პროტოკოლობით.
- ფაირვოლების მართვის საშუალება - არანაკლებ 5 ფაირვოლი
- ლოგები - არანაკლებ 40 00 წამში
- ინდექსირებული ლოგები - არანაკლებ 3000 წამში
- ე.წ. Sustained ინექსირებული ლოგები - არანაკლებ 1000 წამში
- ყოველდღიური ლოგები - არანაკლებ 6 GB
- ბირთვების როდენობა - არანაკლებ 4
- მონაცემთა სანახი - არანაკლებ 1TB
- მეხსიერება - არანაკლებ 16 GB
- პორტები - არანაკლებ 5 x Copper GbE
- კონსოლის პორტი - არანაკლებ 1
- USB პორტი - არანაკლებ 2
- ასევე გადაწყვეტილებას უნდა გააჩნდეს არანაკლებ შემდეგი ფუნქციონალი:
- უსაფრთოების მართვის ტექნოლოგიებს უნდა გააჩნდეს role-based ადმინისტრირების უფლებების მინიჭების მხარდაჭერა.
- გადაწყვეტილება უნდა ახდენდეს ყველა წესის პროტოკოლირებას და მონიტორინგს.
- გადაწყვეტილება უნდა ახდენდეს მოვლენების პროტოკოლირებას ყველა ინტეგრირებულ უსაფრთხოების ტექნოლიგიიდან.
- მოვლენათა ჟურნალის დათვალიერების საშუალებას უნდა გააჩნდეს საძიებო სისტემა.
- პროტოკოლირების სისტემას უნდა გააჩნდეს უსაფრთხო არხი მონაცემთა გადაცემისთვის, რათა აღკვეთილ იქნას ინფორმაციაზე არასანქცირებული წვდომა, ამიტომ გადაწყვეტილება უნდა იყოს დაშიფრული და გადიოდეს ნამდვილობის შემოწმებას.
- მოვლენათა ჩაწერა, შეტყობინება, SNMP trap, ელექტრონული წერილის გაგზავნა და მომხმარებლის მიერ განხორციელებულ ქმედებაზე გაფრთხილებების გაგზავნ.

- გადაწყვეტილებას უნდა გააჩნდეს კონფიგურირებადი გრაფიკები: უსაფრთხოების მთავარი წესები, P2P, VPN ტუნელის ძირითადი მომხმარებლები, ქსელური ტრაფიკი და სხვა სასარგებლო ინფორმაცია.
- გადაწყვეტილებას უნდა შეეძლოს შექმნას ახალი და მომხმარებლზე მორგებული გრაფიკები - დიაგრამების სხვადასხვა ტიპებით.
- გადაწყვეტილება უნდა უზრუნველყოფდეს მოვლენათა კორელაციას და ანგარიშებს.
- კორელაცია შესაძლებელი უნდა იყოს ყველა ტექნოლოგიაზე - Firewall, IPSEC VPN, IPS, მომხმარებელთა იდენტიფიკაცია, მობილური წვდომა, აპლიკაციების კონტროლი, URL-ფილტრაცია, Anti-Bot ან მსგავსი ტექნოლოგია, Anti-Virus, Sandboxing.
- მოვლენების შიგნით ძიების, დეტალებში ჩაღრმავებისა და ინცინდენტების გამოძიების შესაძლებლობა.
- გადაწყვეტილება უნდა უზრუნველყოფდეს რეპორტების ავტომატურ გადაგზავნას ელ. ფოსტის მეშვეობით.
- გადაწყვეტილება უნდა უზრუნველყოფდეს უსაფრთხოების Best Practice შემოთავაზებას.
- გადაწყვეტილებამ უნდა აკონტროლოს ბრანდმაუერის კონფიგურაცია Best Practice ფუნქციონალის დახმარებით.
- უნდა შეეძლოს ავტომატურად უსაფრთხოების წესის (Rule) აქტივაცია/დეაქტივაცია დროის განსაზღვრულ შუალედებში.

• URL ფილტრაცია და Application Control:

- გადაწყვეტილებას უნდა შეეძლოს რამოდენიმე კატეგორიის ერთ ფილტრაციის წესში(Rule) გაერთიანება.
- გადაწყვეტილებას უნდა შეეძლოს ფილტრაციის წესის შექმნა ერთი საიტისთვის რომელიც რამოდენიმე კატეგორიაშია.
- გადაწყვეტილებას უნდა შეეძლოს აპლიკაციების და URL-ების რისკის ფაქტორებით კატეგორიზაცია.
- გადაწყვეტილებას უნდა შეეძლოს Application control-ის და URL ფილტრაციის პოლიტიკებში განსაღვროს მომხმარებლის საიდენტიფიკაციო პარამეტრები.
- გადაწყვეტილებას უნდა შეეძლოს ერთ უსაფრთხოების წესში გაიწეროს Application control-ის და URL ფილტრაციის პოლიტიკები.
- ფუნქციონალი უნდა მოიცავდეს თეთრ და შავი სიის მექანიზმს. სადაც შესაძლებელი იქნება ნებისმიერი URL-ის განთავსება მიუხედავად იმისა რომელ კატეგორიას განეკუთვნება ეს URL-ი.
- უსაფრთხოების პოლიტიკის წესის, რომელიმე სექციაში უნდა შეიძლებოდეს კონკრეტულად ამ უსაფრთხოების წესისთვის უშუალოდ URL Category-ის მითითება ან ცვლილება, იმისათვის რომ ხდებოდეს ე.წ. “Policy match” მითითებული URL კატეგორიების მიხედვით.
- უნდა უზრუნველყოფდეს URL კატეგორიზაციას და უნდა შეიცავდეს არანაკლებ 200 მილიონ URL-ს.

• ლოგირება:

- Logging - შესაძლებელი უნდა იყოს მოვლენების დახარისხება სხვადასხვა მახასიათებლის მიხედვით.
- Logging - ფუქნციონალს უნდა შეეძლოს არანაკლებ შემდეგი ტიპის მოვლენების გენერაცია: Top sources, Top destinations, Top services, Top Actions, Top users, Top Origins, Top Firewall Rules.
- Logging - ლოგირების დათვალიერებისას შესაძლებელი უნდა იყოს ფილტრების დაყენება სხვადასხვა წინასწარ განსაზღვრული ობიექტებით (hosts, network, groups, users...)

- გადაწყვეტილება უნდა უზრუნველყოფდეს ბრანდმაუერების პროგრამული უზრუნველყოფების განახლების ავტომატურ გავრცელებას და მორგებას.
- გადაწყვეტილებას უნდა გააჩნდეს ბრანდმაუერების ლიცენზიების ცენტრალური მართვის სისტემა.
- გადაწყვეტილება უნდა უზრუნველყოფდეს ანგარიშების ავტომატურ გავრცელებას ელ. ფოსტის მეშვეობით.
- გადაწყვეტილება უნდა უზრუნველყოფდეს მარეგულერებლის მოთხოვნებისადმი შესაბამისობის სტანდარტებით შეფასებას (ISO 27001/27002, PCI-DSS,HiPPA, და სხვ.).

**მხარდაჭრა და ლიცენზიები**

- ლიცენზიების მოქმედების ვადა არანაკლებ 3 წელი
- ტექნიკურ მხარდაჭერაზე არაუმეტეს 4 საათში რეაგირება, არანაკლებ 5x9
- მოწყობილობის შეცვლის გარანტია არაუმეტეს ერთი თვის განმავლობაში, მას შემდეგ რაც მოხდება დაზიანების დადასტურება არაუმეტეს 24 საათისა.
- შემოთავაზებული ლიცენზიები უნდა მუშაობდეს მომხმარებელთა ულიმიტო რაოდენობაზე.

**დამატებითი მოთხოვნები**

- ქსელის რედიზაინი და ყველა სერვისების გადატანა იმპლემენტაცია კომპანია RMG ინფორმაციული ტექნოლოგიების დეპარტამენტის მოთხოვნების შესაბამისად.
- ტექნიკის მონტაჟი და პროგრამული გამართვა "კონფიგურაცია" და არსებულ ქსელში ინტეგრაცია უნდა განხორციელდეს პრეტენდენტი კომპანიის მიერ დამკვეთის საინფორმაციო ტექნოლოგიების დეპარტამენტთან წინასწარი შეთანხმებით.
- პრეტენდენტმა უნდა წარმოადგინოს მწარმოებლის ავტორიზაციის დამადასტურებელი დოკუმენტი(MAF), რომელიც უფლებას აძლევს პრეტენდენტს აღნიშნული პროექტის ფარგლებში საქართველოს ტერიტორიაზე განახორციელოს პროდუქციის გაყიდვა და სერვისული მომსახურება
- პრეტენდენტმა უნდა წარმოადგინოს პრეტენდენტ კომპანიაში დასაქმებული მინიმუმ ერთი თანამშრომლის სერტიფიკატ(ებ)ი, რომელიც გაცემულია შემოთავაზებული პროდუქტის მწარმოებლის მიერ.
- საქონლის მიწოდების ვადა: არაუმეტეს 65 კალენდარული დღე
- ინსტალაცია და იმპლემენტაციის ვადა საქონლის მიწოდებიდან: არაუმეტეს 30 კალენდარული დღე.