დასახელება	ტექნიკური პარამეტრები
გათვალისწინებული აპარატურის ფუნქციონალი და თვისებები	• NGFW მოწყობილობა სერვისებით: - AntiVirus - IPS/IDS - AntiSpam - Web-ფილტრაცია - აპლიკაციების კონტროლი • უნდა აერთიანებდეს კლასტერში არანაკლებ 2 და არაუმეტეს 4 მოწყობილობას. • კლასტერი უნდა ფუნქციონირებდეს აქტიურ-პასიური ან აქტიურ-აქტიურ რეჟიმში. • უნდა ჰქონდეს Firewall ფუქნცია • VPN • დატვირთვის ბალანსირება • traffic shaping • WLAN ის კონტროლერი • SSL inspection • დინამიური მარშრუტიზაცია IPv4, IPv6. • WAN კავშირის ოპტიმიზაცია • DLP • ანტივირუსული დაცვა with hardware acceleration • სპამისგან დაცვა (antispam). • დომენის კონტროლერთან ინტეგრაცია • Web-Proxy • მინიმუმ 10 ვირტუალური დომენის (სრულ-ფუნქციური ვირტუალური utm ერთი მოწყობილობის შიგნით) არსებობა.
ინტერფეისები	• არანაკლებ : 16x LAN GE RJ45; 1x RJ45 კონსოლის ინტერფეისი; 1x RJ45 MGMT ინტერფეისი 1x RJ45 HA ინტერფეისი 2x 10GE SFP+ ინტერფეისი 8x GE SFP ინტერფეისები 1x USB ინტერფეისი;
წარმადობა	• არანაკლებ : Firewall Throughput (1518 / 512 / 64 byte UDP packets) 27/27/11 Gbps; Firewall Throughput (Packets Per Second) 16.5 Mpps; Concurrent Sessions (TCP) 3 Million; New Sessions/Second (TCP) 280 000; Firewall Latency (64 byte UDP packets) 4.78 µs; IPsec VPN Throughput (512 byte) 13 Gbps; IPS Throughput 5 Gbps; SSL Inspection Throughput (IPS, avg. HTTPS) 2 Gbps; Firewall Policies 10,000; Virtual Domains (Default / Maximum) 10 / 10; Application Control Throughput (HTTP 64K) 13 Gbps; შეუზღუდავი მომხმარებლის ლიცენზია;

დასახელება	ტექნიკური პარამეტრები
VPN	• PPTP, IPSec და SSL. • Dedicated tunnels • დაშიფვრა (DES, 3DES, AES). • აუთენტიფიკაცია SHA-1 / MD5. • დასრულებული PPTP VPN კლიენტი, L2TP. • მხარდაჭერა იერარქიული (hub and spoke) VPN- • კავშირების. • აუთენტიფიკაცია IKE სერთიფიკატით. • IPSec NAT Traversal პროტოკოლი. • Dead Peer Detection მექანიზმი.
ქსელური სერვისები	• Support for connecting multiple WAN-networks. • Support for PPPoE protocol. • Support DHCP protocol in configuration • Client / Server. • Policy based routing. • Dynamic routing (RIP v1 and v2, OSPF, BGP, • Multicast). • Support for multiple zones. • Routing between zones. • Routing between virtual networks.
ადმინისტრირება / მენეჯმენტი / მომხმარებლების აუთენთიფიკაცია	• Role based management. • Several levels of administrators and users. • Update and change via TFTP protocol and web user interface. • Return to the previous state in the system software. • Built-in database. • Windows Active Directory Service Database. • External RADIUS / LDAP database. • Binding by IP / MAC address. • Xauth via RADIUS for IPSEC VPN protocol.
ბრანდმაუერი	• NAT, PAT, transparent (bridge). • Router mode (RIP v1 and v2, OSPF, BGP, Multicast). • Policy-based NAT. • Virtual domains (NAT / transparent mode) • VLAN Tagging (802.1Q). • Authentication based on user groups • SIP / H.323 NAT Traversal. • WINS support. • Customizable security profiles.
ვებ – კონტენტის ფილტრაცია	• Blocking by URL / Keyword / Phrase. • Whitelist URLs. • Content profiles. • Blocking Java applets, Cookies, elements. • ActiveX controls. • Service support - web filtering • Content, Internet filter, firewall and proxies. • An online reputation database of web resources with more than 250 million web sites divided into more than 78 categories.

დასახელება	ტექნიკური პარამეტრები
Intrusion Prevention System (IPS / IDS)	• Custom dynamic signature list Detection • Automatic update of the attack database.
შეტევებისგან დაცვა	• Verification of HTTP, SMTP, POP3, IMAP, FTP protocols and • IM services, checking encrypted VPN tunnels. • Automatic “prompt delivery” of updates • anti-virus databases. • Quarantined infected messages. • Blocking depending on file size. • Blocking depending on the type of file.
სპამისგან დამცავი მოდული	• Blacklist support real-time / database server "open repeaters. " • Checking MIME headers. • Filtering by keywords / phrases. • Support for "black" / "white" lists of IP addresses. • Automatic, in real time,Receive updates from the update services network.
ლოგინგი და მონიტორინგი	• Internal logging. • Sending protocols to a remote Syslog / WELF server. • Graphical tools for Real-time monitoring and viewing history. • Email notification of viruses and attacks. • Monitoring VPN tunnels. • Optional logging using additional hardware solution. • Ability to store and process logs in the cloud.
ტრაფიკის კონტროლი (Traffic shaping)	• Policy-based traffic shaping. • Setting up various types of services of different types of traffic. • Guaranteed / Maximum / Priority Bandwidth Modes
Proxy-server	• The function of local storage of Web content ,requested by users to optimize the bandwidth
გარანტია და სერვისი	• მოწყობილობას უნდა ჰქონდეს მწარმოებლისგან გარანტია არა ნაკლებ 12 თვის განმავლობაში. • ინციდენტების გახსნის საშუალებით და განახლებების განხორციელებით, 24/7 წვდომა მწარმოებლის საიტზე • არანაკლებ 3 წლიანი უნივერსალური ლიცენზირება

როუტერი (თავსებადი უნდა იყოს გარემოს დაცვისა და სოფლის მეურნეობის სამინისტროში არსებულ ცენტრალური მართვის სისტემა Fortimanager -თან).