წინამდებარე ტექნიკური დავალებით გათვალისწინებული კომპონენტები და თანმდევი სამუშაოები შემსყიდველს ჩაბარდება ორ ეტაპად, შემდეგი ვადების დაცვით:

I ეტაპი - 2024 წლის 23 დეკემბრამდე;

II ეტაპი - 2025 წლის 31 ივლისამდე.

I ეტაპი

1. A ტიპის კომუტატორი რაოდენობა 6 (ექვსი)

კომუტატორი უნდა იყოს ინდუსტრიული გარემოსთვის თავსებადი	
მოთხოვნები წარმადობის და აპარატურული უზრუნველყოფის მიმართ	
ფიზიკური ინტერფეისები	არანაკლებ 24 x 10/100/1000 მბ/წმ Rj-45 პორტი არანაკლებ 4 x 1 გბ/წმ SFP პორტი
მართვის ინტერფეისები	არანაკლებ 1 x Rj-45 კონსოლის პორტი არანაკლებ 1 x Micro USB კონსოლის პორტი
კომუტაციის წარმადობა	არანაკლებ 55 გბ/წმ
MAC მისამართების რაოდენობა	არანაკლებ 15,000
IPv4 მარშუტების რაოდენობა	არანაკლებ 3,000
IPv6 მარშუტების რაოდენობა	არანაკლებ 1,500
ACL ჩანაწერების რაოდენობა	არანაკლებ 1,400
STP	არანაკლებ 120
ოპერატიული მეხსიერება	არანაკლებ 4 გბ
Flash	არანაკლებ 2 გბ
VLAN IDs	1,024
Switched Virtual Interfaces	არანაკლებ 980
SGT/DGT policies	არანაკლებ 1,980
IPv4 to SGT binding	არანაკლე 9,000
SXP სესიები	არანაკლებ 200
SD Access Fabric-ის მხარდაჭერა	არანაკლებ 32 ვირტუალური ქსელის ბარათი

Rack Unit	1 RU
კომუტატორს უნდა გააჩნდეს 2 კვების ბლოკი თითო კვების ბლოკი უნდა იყოს მინიმუმ 400W სიმძლავრის, რომელიც იმუშავებს როგორც AC ასევე DC კვებაზე.	
მოთხოვნები სამუშაო გარემოს მიმართ: არანაკლებ -40°C დან +75°C	
IEEE 802.3at PoE+ ტექნოლოგიის მხარდაჭრა, არანაკლებ 30 ვატის მიწოდების შესაძლებლობა ერთ პორტზე. POE+ ბიუჯეტი არანაკლებ 380 Perpetual PoE - კომუტატორს უნდა შეეძლოს POE+ მიწოდება კლიენტებზე, კომუტატორის გადატვირთვის დროსაც. • Fast PoE - კომუტატორის უნდა შეეძლოს მყისიერად მიაწოდოს კლიენტებს POE+, ჩართვის მომენტში და არ დაელოდოს ოპერაციული სისტემის ჩატვირთვას.	
მოთხოვნები პროგრამული უზრუნველყოფის, ტექნოლოგიების და ოქმების მიმართ:	
L2 კომუტაცია	• IEEE 802.1D • IEEE 802.1q • IEEE 802.1s • IEEE 802.1w • LACP, PVRST, PVST, RSPAN, VTP, L2PT, SPAN, RSPAN, Selective
L2 multicast	• IGMPv1, v2, v3, Snooping, IGMP filtering, MLD
L3 მარშუტიზაცია	• Static Route, RIP, PBR, OSPF, OSPFv3
უსაფრთხოება	DHCP snooping, Dynamic ARP Inspection, Client Information Signaling Protoco, IP Source Guard, Secure Shell, AAA, , DHCPv6 უსაფრთხოება, 802.1x, IPv6 Snooping, IPv6 Source/Prefix Guard, IPv6 Destination Guard, IP Source Guard, Ipv6 RA guard, TACACS+, TLS 1.3, NEAT,
ქსელის ხილვადობის ტექნოლოგიები	• NetFlow (ან ანალოგი)
მეორე დონის ტრაფიკის შიფრაციის ტექნოლოგები, ყველა პორტზე.	• MACsec-128
მომავალში მხოლოდ პროგრამული ლიცენზიის დამატებით, კომუტატორს უნდა გააჩნდეს შემდეგი ტექნოლოგიების მხარდაჭერა, მათ შორის:	
L3 მარშუტიზაცია	EIGRP, HSRP, BGP, NSF
მეორე დონის ტრაფიკის შიფრაციის ტექნოლოგები, ყველა პორტზე.	• MACsec-256
L3 multicast	MSDP, PIM, IPv6 multicast VRF
კომუტატორს უნდა გააჩნდეს სტეკირების ტექნოლოგია. სტეკში შესაძლებელი უნდა იყოს არანაკლებ 4 კომუტატორის გაერთიანება. კომუტატორისთვის. სტეკირების	

<table>
<tr><td colspan="2">უზრუნველყოფა არ უნდა იკავებდეს კომუტატორზე, მოთხოვნილ 1 გბ/წმ პორტებს. სტეკის ტექნოლოგიისთვის კომუტატორს უნდა მოყვენოდეს 0,5მ ზომის სტეკის კაბელი</td></tr>
<tr><td>ლოგიკურ ჯგუფებზე დაფუძნებული უსაფრთხოების და კონტროლის განსაზღვრა</td><td>კომუტატორს უნდა შეეძლოს ქსელური რესურსების დინამიური და სტატიკური კლასიფიკაცია ლოგიკურ ჯგუფებში, შემდეგი პარამეტრებით:
1. დინამიური კლასიფიკაცია უნდა განისაზღვროს მინიმუმ:
a. 802.1X აუთენტიფიკაციით
b. ვებ აუთენთიფიკაციით
c. MAC მისამართის აუტენტიფიკაციით
2. სტატიკური კლასიფიკაცია უნდა განისაზღვროს მინიმუმ:
a. IP მისამართით
b. VLAN_ით
c. ქვექსელით
d. მესამე დონის ინტერფეისით
• ლოგიკურ ჯგუფში შესაძლებელი უნდა იყოს რესურსების განსაზღვრა/კლასიფიკაცია მიუხედავად მათი ლოკაციისა , ქვექსელის მისამართისა და VLAN ნომრისა.
• ლოგიკური ჯგუფის იდენტიფიკატორის ტრანსპორტირება შესაძლებელი უნდა იყოს როგორც დამატებითი თავსართი ქსელური ნაკადის შესახებ.
• კომუტატორს უნდა შეეძლოს ლოგიკურის ჯგუფების იდენთიფიკატორზე დაფუძნებული უსაფრთხოების/ტრაფიკის ფილტრაციის პოლიტიკების გამართვა.</td></tr>
<tr><td colspan="2">საკუთრივ კომუტატორს უნდა გააჩნდეს სხვადასხვა სახის ავტომატიზაციის მხარდაჭერა, მათ შორის:
1. NETCONF - პროტოკოლის მხარდაჭერა
2. RESTCONF - პროტოკოლის მხარდაჭერა
3. YANG - მონაცემთა მოდელის მხარდაჭერა</td></tr>
<tr><td colspan="2">კომუტატორზე უნდა ვრცელდებოდეს მწარმოებლის სამ წლიანი საგარანტიო მომსახურეობა, ტექნიკური მხარდაჭერა და პროგრამული უზრუნველყოფის განახლება.მოწყობილობის დაზიანების მიზეზის დადგენის შემდეგ, მოწყობილობა უნდა შეკეთდეს ან შეცვალოს შემდეგ სამუშაო დღეს.</td></tr>
</table>

მომწოდებელმა უნდა წარმოადგინოს მწარმოებლის ავტორიზაციის წერილი (Manufacturers Authorization Form) მომწოდებელმა უნდა წარმოადგინოს გადაწყვეტილების მომწოდებლის კომპლექსური კორპორატიული ქსელების სპეციალიზაცია

2. A ტიპის უსადენო წვდომის წერტილი რაოდენობა 5 (ხუთი)

ინტერფეისები	არანაკლებ 1 ცალი 10/100/1000/2500 (RJ-45), Power over Ethernet (PoE) არანაკლებ 1 1გბ/წმ SFP პორტი არანაკლებ 1 ცალი Management console port (RJ-45)
გამოყენების ტიპი	გარე გამოყენების
რადიო ინტერფეისები	არანაკლებ 2.4 GHz, 5 GHz
ჯამური მომხმარებლების რაოდენობა	არანაკლებ 400
IEEE სტანდარტები	არანაკლებ 802.11a, 802.11b/g, 802.11n, 802.11ac Wave 1, 802.11ac Wave 2, 802.11ax
MIMO სივრცული არხი	არანაკლებ 4x4:4
კონტროლერთან თავსებადობა	ფიზიკურ და ვირტუალურ კონტროლერთან თავსებადობა. საჭიროების შემთხვევაში წვდომის წერტილებს უნდა შეეძლოთ არანაკლებ 50 უსადენო წვდომის წერტილის მართვა ცენტრალური კონტროლერის გარეშე
აუთენთიფიკაციის და უსაფრთხოების პროტოკოლები	• 802.11i • WPA2, WPA3 • 802.1X • AES • EAP-TLS • EAP-TTLS ან MSCHAPv2 • EAP-FAST • PEAP ვერსია 1 ან EAP-GTC • EAP-SIM

კონფიგურაციის საშუალება	• Console, Telnet, SSH.
802.11n	• არანაკლებ 4x4 MIMO ოთხი სივცრცული არხით, როგორც 2,4Ghz ასევე 5Ghz-თვის • მაქსიმალური თანაფარდობის კომბინირება • 20 და 40-MHz არხები • ფიზიკური სიჩქარის მონაცემები არანაკლებ 880 მბ/წმ • პაკეტების აგრეგაცია • 802.11 დინამიური სიხშირეების შერჩევა
802.11ac	• არანაკლებ 4x4 MIMO ოთხი სივცრცული არხით, როგორც 2,4Ghz ასევე 5Ghz-თვის • მაქსიმალური თანაფარდობის კომბინირება • 802.11ac სხივის ფორმირება • 20, 40, 80, 160-MHz არხები • ფიზიკური სიჩქარის მონაცემები არანაკლებ 3.40 გბ/წმ • პაკეტების აგრეგაცია • 802.11 დინამიური სიხშირეების შერჩება
802.11ax	• არანაკლებ 4x4 MIMO ოთხი სივრცული არხით როგორც 2,4Ghz ასევე 5Ghz-თვის • მაქსიმალური თანაფარდობის კომბინირება • OFDMA • TWT • BSS coloring • 802.11ax სხივის ფორმირება • 20, 40, 80, 160-MHz არხები • ფიზიკური სიჩქარის მონაცემები არანაკლებ 5.30 Gbps • პაკეტების აგრეგაცია • 802.11 დინამიური სიხშირეების შერჩება

ანტენების განლაგება	შიდა
შიდა ანტენის სიმძლავრე	• 2.4 GHz, მინიმუმ 7 dBi სიმძლავრის • 5 GHz, მინიმუმ gain 6 dBi სიმძლავრის
გადაცემის სიმძლავრე	• 2.4GHz რადიო სიხშირისთვის - არანაკლებ 300 mW • 5 GHz რადიო სიხშირისთვის - არანაკლებ 300 mW
სიმძლავრის რეგულაცია	დაშვების წერტილს უნდა გააჩნდეს გადაცემის სიმძლავრის რეგულაცია “regulatory domain” _ის შესაბამისად.
ელ. კვების მიწოდება:	• 802.3at POE+ • 802.3bt POE++ • 802.3at power injector • DC კვების წყარო
სამუშაო ტემპერატურა	არანაკლებ -40 °C დან +60°C
დაშვების წერტილს ასევე უნდა გააჩნდეს	• Wi-Fi მულტიმედიის ტექნოლოგიის მხარდაჭერა • უსადენო წვდომის წერტილს უნდა გააჩნდეს სპეციალური მოდული რომელიც უზრუნველყოფს რადიო სპექტრის სკანირებას რომელიც იმუშავებს დამოუკიდებლად კლიენტ რადიოებისგან და არ იქონიებს ზეგავლენას მომხმარებლების და უსადენო წვდომის წერტილის მუშაობაზე • უსადენო წვდომის წერტილს უნდა გააჩნდეს WIPS მხარდაჭერა
უსადენო წვდომი წერტილს უნდა მოყვებოდეს სამაგრი რომელიც განკუთვნილი იქნება ვერტიკალურად კედელზე ან ბოძზე ინსტალაციისთვის	

უსადენო წვდომის წერტილეზე უნდა ვრცელდებოდეს მწარმოებლის სამ წლიანი საგარანტიო მომსახურეობა, ტექნიკური მხარდაჭერა და პროგრამული უზრუნველყოფის განახლება.მოწყობილობის დაზიანების მიზეზის დადგენის შემდეგ, მოწყობილობა უნდა შეკეთდეს ან შეცვალოს შემდეგ სამუშაო დღეს. **მომწოდებელმა უნდა წარმოადგინოს მწარმოებლის ავტორიზაციის წერილი (Manufacturers Authorization Form)** **მომწოდებელმა უნდა წარმოადგინოს გადაწყვეტილების მომწოდებლის კომპლექსური კორპორატიული ქსელების სპეციალიზაცია**

3. B ტიპის უსადენო წვდომის წერტილი რაოდენობა 5 (ხუთი)

ინტერფეისები	არანაკლებ 1 ცალი 10/100/1000/2500 (RJ-45), Power over Ethernet (PoE) არანაკლებ 1 1გბ/წმ SFP პორტი არანაკლებ 1 ცალი Management console port (RJ-45)
გამოყენების ტიპი	გარე გამოყენების
რადიო ინტერფეისები	არანაკლებ 2.4 GHz, 5 GHz
ჯამური მომხმარებლების რაოდენობა	არანაკლებ 400
IEEE სტანდარტები	არანაკლებ 802.11a, 802.11b/g, 802.11n, 802.11ac Wave 1, 802.11ac Wave 2, 802.11ax
MIMO სივრცული არხი	არანაკლებ 4x4:4
კონტროლერთან თავსებადობა	ფიზიკურ და ვირტუალურ კონტროლერთან თავსებადობა. საჭიროების შემთხვევაში წვდომის წერტილებს უნდა შეეძლოთ არანაკლებ 50 უსადენო წვდომის წერტილის მართვა ცენტრალური კონტროლერის გარეშე
აუთენთიფიკაციის და უსაფრთხოების პროტოკოლები	• 802.11i • WPA2, WPA3

	• 802.1X • AES • EAP-TLS • EAP-TTLS ან MSCHAPv2 • EAP-FAST • PEAP ვერსია 1 ან EAP-GTC • EAP-SIM
კონფიგურაციის საშუალება	• Console, Telnet, SSH.
802.11n	• არანაკლებ 4x4 MIMO ოთხი სივცრცული არხით, 2,4Ghz რადიოსთვის და არანაკლებ 2x2 MIMO ორი სიცრცული არხით 5Ghz რადიოსთვის • მაქსიმალური თანაფარდობის კომბინირება • 20 და 40-MHz არხები • ფიზიკური სიჩქარის მონაცემები არანაკლებ 880 მბ/წმ • პაკეტების აგრეგაცია • 802.11 დინამიური სიხშირეების შერჩევა
802.11ac	• არანაკლებ 4x4 MIMO ოთხი სივცრცული არხით, 2,4Ghz რადიოსთვის და არანაკლებ 2x2 MIMO ორი სიცრცული არხით 5Ghz რადიოსთვის • მაქსიმალური თანაფარდობის კომბინირება • 802.11ac სხივის ფორმირება • 20, 40, 80, 160-MHz არხები • ფიზიკური სიჩქარის მონაცემები არანაკლებ 3.40 გბ/წმ • პაკეტების აგრეგაცია • 802.11 დინამიური სიხშირეების შერჩება

802.11ax	• არანაკლებ 4x4 MIMO ოთხი სივცრცული არხით, 2,4Ghz რადიოსთვის და არანაკლებ 2x2 MIMO ორი სიცრცული არხით 5Ghz რადიოსთვის • მაქსიმალური თანაფარდობის კომბინირება • OFDMA • TWT • BSS coloring • 802.11ax სხივის ფორმირება • 20, 40, 80, 160-MHz არხები • ფიზიკური სიჩქარის მონაცემები არანაკლებ 5.30 Gbps • პაკეტების აგრეგაცია • 802.11 დინამიური სიხშირეების შერჩება
ანტენების განლაგება	გარე
ანტენის ტიპი	Omni მიმართული
გარე ანტენის სიმძლავრე	• 2,4GHz, მინიმუმ 6 dBi სიმძლავრის • 5 GHz, მინიმუმ gain 7 dBi სიმძლავრის
გადაცემის სიმძლავრე	• 2.4GHz რადიო სიხშირისთვის - არანაკლებ 300 mW • 5 GHz რადიო სიხშირისთვის - არანაკლებ 300 mW
სიმძლავრის რეგულაცია	დაშვების წერტილს უნდა გააჩნდეს გადაცემის სიმძლავრის რეგულაცია “regulatory domain” _ის შესაბამისად.
ელ. კვების მიწოდება:	• 802.3at POE+ • 802.3bt POE++

	• 802.3at power injector • DC კვების წყარო
სამუშაო ტემპერატურა	არანაკლებ -40 °C დან +60°C
დაშვების წერტილს ასევე უნდა გააჩნდეს	• Wi-Fi მულტიმედიის ტექნოლოგიის მხარდაჭერა • უსადენო წვდომის წერტილს უნდა გააჩნდეს სპეციალური მოდული რომელიც უზრუნველყოფს რადიო სპექტრის სკანირებას რომელიც იმუშავებს დამოუკიდებლად კლიენტ რადიოებისგან და არ იქონიებს ზეგავლენას მომხმარებლების და უსადენო წვდომის წერტილის მუშაობაზე • უსადენო წვდომის წერტილს უნდა გააჩნდეს WIPS მხარდაჭერა

უსადენო წვდომი წერტილს უნდა მოყვებოდეს სამაგრი რომელიც განკუთვნილი იქნება ვერტიკალურად კედელზე ან ბოძზე ინსტალაციისთვის

უსადენო წვდომის წერტილეზე უნდა ვრცელდებოდეს მწარმოებლის სამ წლიანი საგარანტიო მომსახურეობა, ტექნიკური მხარდაჭერა და პროგრამული უზრუნველყოფის განახლება.მოწყობილობის დაზიანების მიზეზის დადგენის შემდეგ, მოწყობილობა უნდა შეკეთდეს ან შეცვალოს შემდეგ სამუშაო დღეს.

მომწოდებელმა უნდა წარმოადგინოს მწარმოებლის ავტორიზაციის წერილი (Manufacturers Authorization Form)

მომწოდებელმა უნდა წარმოადგინოს გადაწყვეტილების მომწოდებლის კომპლექსური კორპორატიული ქსელების სპეციალიზაცია

4. A ტიპის უსადენო წვდომის წერტილის კონტროლერი რაოდენობა 1 (ერთი)

კონტორლერის ტიპი	ვირტუალური
გამტარუნარიანობა	არანაკლებ 4 Gbps
WLAN-ების რაოდენობა	არანაკლებ 4000
ვირტუალური ქსელების რაოდენობა	არანაკლებ 4000
რადიო პროფილები	არანაკლებ 11000
ტრაფიკის ფილტრაციის, წვდომის კონტროლის პოლიტიკები	არანაკლებ 250
წვდომის კონტროლის პოლიტიკების ჩანაწერები	არანაკლებ 250
მართვის ინტერფეისები	• HTTP/S • Telnet • SSH • Console • API -ის მხარდაჭერა
უსადენო ქსელის სტანდარტების მხარდაჭერა	IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11d, IEEE 802.11e, IEEE 802.11h, IEEE 802.11n, IEEE 802.11k, IEEE 802.11r, IEEE 802.11u, IEEE 802.11w, IEEE 802.11ac Wave1 და Wave2, IEEE 802.11ax
WLAN - კონფიგურაციის რეჟიმები:	• ე.წ. „Bridge“ რეჟიმის მხარდაჭერა, როდესაც უსადენო წვდომის წერტილი იმართება ცენტრალური კონტროლერის მეშვეობით, მაგრამ მომხამრებლის ტრაფიკის კომუტაცია ხდება ლოკალური

	ქსელურის ინფრასტრუქტურის გავლით. • ე.წ. „Tunnel“ რეჟიმში, როდესაც უსადენო წვდომის წერტილი იმართება ცენტრალური კონტროლერის მეშვეობით და მომხმარებელთა ტრაფიკის კომუტაცია ხდება ამავე კონტროლერის გავლით, ტუნელირების ტექნოლოგიის გამოყენებით. • შესაძლებელი უნდა იყოს ერთდროულად ორივე რეჟიმის სხვადასხვა WLAN-ების გაშვება ერთიდაიგივე უსადენოს წვდომის წერტილზე.
უსაფრთხოების სტანდარტები	• WPA, WPA2, WPA3 • MD5 ალგორითმი • ESP სამმაგი DES ტრანსფორმაცია • HMAC • TLS V1.0 და TLS V1.2 • ტრანსპორტ დონის უსაფრთხოება
შიფრაცია	• WEP RC4 40, 104 და 128 ბიტები • AES, CBC, CCMP • DES: 3DES • IPsec: 3DES, AES-CBC
აუთენტიფიკაცია, ავტორიზაცია და აღრიცხვა	• 802.1X • Microsoft რადიუს ატრიბუტები • EAP-TLS • რადიუს აუთენტიფიკაცია • რადიუსის აღრიცხვა • რადიუსის ტუნელირების აღრიცხვა • რადიუსის-ს მხარდაჭერა EAP-ისთვის • IEEE 802.1X რადიუსი • ვებ-ზე დაფუძნებული ავტორიზაცია

Guest პორტალი	• კონტროლერში ინტეგრირებული უნდა იყოს ე.წ. Guest Portal-ი. • უნდა ხდებოდეს სტუმრებისთვის დროებითი მომხმარებლის და პაროლის შექმნა. მაგ: 1 საათით ან 1 კვირით და ავტომატურად მოხდეს მისი გათიშვა ვადის გასვლის შემდეგ. • კონტროლერზე შესაძლებელი უნდა იყოს Guest Portal-ის მოდიფიკაცია ან ახალი პორტალის ატვირთვა კონტროლერში. ასევე კონტროლერს უნდა შეეძლოს ე.წ. 3rd party პორტალებთან ინტეგრაცია
უსაფრთხოება	• სისტემაში ინტეგრირებული უნდა იყოს, ოპერაციული სისტემის ჩატვირთვის დაცვის მექანიზმი • აპარატურაში ჩატვირთული კოდის დაცვა და შემოწმება, რათა არ მოხდეს აპარატურაში შეცვლილი კოდით ჩატვირთვა • უსადენო ქსელში შეჭრის პრევენციის სისტემა
მაღალ მდგრადობა	• აქტიური კონტოლერიდან სარეზერვო კონტროლერზე გადართვის შემთხვევაში არ უნდა მოხდეს სერვისების და კლიენტების გათიშვა ქსელიდან • პროგრამული უზრუნველყოფის განახლება ქსელის შეფერხების გარეშე

უსადენო წვდომის კონტროლერს უნდა გააჩნდეს შემდეგი ფუნქციონალი:

1. კონტროლერზე შესაძლებელი უნდა იყოს არანაკლებ 5000 ცალი უსადენო წვდომის წერტილის დაერთება, არანაკლებ 6300 ცალი კლიენტ მოწყობილობების დაერთება
2. კონტროლერს უნდა გააჩნდეს ჩაშენებული რადიო რესუსრსების მართვის მექანიზმი.
3. კონტროლერიდან შესაძლებელი უნდა იყოს TCP MSS პარამეტრების ცვლილება გრაფიკული ინტერფეისიდან
4. გრაფიკული ინტერფეისიდან შესაძლებელი უნდა იყოს სამივე რადიოსთვის როგორც 2.4Ghz, 5Ghz ასევე 6Ghz-სთვის:

- როუმინგ პარამეტრების განსაზღვრა როგორიცაა RSSI და Scan Threshold-ები
- ბიკონების ინტერვალის და ფრაგმენტაციის ბარიერის პარამეტრების განსაზღვრა
- SS/MCS პარამეტრების ჩართვა ან გამორთვა გრაფიკული ინტერფეისიდან
- ე.წ. „Data Rate “გასნსაზღვრა, აღნიშნული ფუნქციონალის საშუალებით შესაძლებელი უნდა იყოს განისაზღვროს კონკრეტული კავშირის სისწრაფე, რომელიც მხარდაჭერილი იქნება ან არ იქნება კლიენტისთვის. თუ კლიენტს არ აქვს მხარდაჭერა განსაზღვრული კავშირის სისჩაქრის, აღნიშნული კლეინტის დაერთება ავტომატურად უარყოფილი უნდა იყოს კონტროლერის მიერ.
- მოთხოვნილი ფუნქციონალი გულისხმობს, რომ ადმინისტრატორს შესაძლებლობა ჰქონდეს სამივე რადიო სიხშირეზე არსებული ყველა შეერთების სიჩქარის სტანდარტის მხარდაჭერა ჩართოს ან გამორთოს. მაგალითად 2.4Ghz -ზე გაითიშოს მხოლოდ 1 Mbps ხოლო ყველა სხვა მხარდაჭერილი და აქტიური იყოს, ან მაგალითად 5 Ghz გაითიშოს მხოლოდ 6 მბ/წ და 29 მბ/წ, ამ შემთხვევაშიც ყველა სხვა დაერთების სიჩქარე უნდა იყოს მხარდაჭერილი.

5. კონტროლერის მეშვეობით შესაძლებელი უნდა იყოს უსადენო წვდომის წერტილების რადიო გადამცემის სიმძლავრის ხელით და ავტომატურ რეჯიმში მითითება მინიმალურიდან მაქსიმალურ სიმძლავრემდე. მაგ: უსადენო წვდომის წერტილების რადიო გადამცემის სიმძლავრე უნდა იყოს 18 dBm ან ავტომატურად ხდებოდეს მისი რეგულირება 10 dBm -დან 18 dBm-მდე.
6. კონტროლერს უნდა გააჩნდეს Application Visibility-ის მხარდაჭერა, მის გასააქტიურებლად სისტემა არ უნდა საჭიროებდეს დამატებით ლიცენზიას ან დამატებით პროგრამულ უზრუნველყოფას.
7. კონტროლერს უნდა გააჩნდეს დაშვების წერტილსა და კონტროლერს შორის კომუნიკაციის შიფრაციის შესაძლებლობა CAPWAP პროტოკოლის გამოყენებით ან ანალოგიური
8. კონტროლერზე შესაძლებელი უნდა იყოს ვირტუალური ქსელის ჯგუფების შექმნა.
9. აუთენტიპიკაციის და აღრიცვის შემთხვევაში კონტროლერს უნდა ჰქონდეს სხვადასხვა ატრიბუტების მხარდაჭერა:
10. გრაფიკული ინტერფეისიდან შესაძლებელი უნდა იყოს Called Station Id-ის ატრიბუტების არჩევა აღრიცხვისთვის და აუთენტიპიკაციისთვის როგორიცაა:
    - უსადენო წვდომის წერტილის ჯგუფების სახელები
    - ვირტუალური ქსელის ID
    - უსადენო წვდომის წერტილების ლოკაცია
    - მაკ მისამართები
11. კონტროლერს უდნა გააჩნდეს QOS-ის მხარდაჭერა
12. გრაფიკული ინტერფეისიდან შესაძლებელი უნდა იყოს packet capture, ping,

trace route და რადიოაქტიური ტრეისის ფუნქციის გამოყენება 13. კონტროლერის ინტერფეისიდან შესაძლებელი უნდა იყო კონფიგურაციის შედარება 14. ვირტუალური კონტროლერის ინსტალაცია შესაძლებელი უნდა იყოს შემდეგ პლათფორმებზე: KVM, Hyper-V, ESXI, AWS, Azure და GCP 15. საკუთრივ კონტროლერს უნდა გააჩნდეს სხვადასხვა სახის ავტომატიზაციის მხარდაჭერა, მათ შორის: NETCONF,RESTCONF და YANG
კონტროლერს უნდა მოყვებოდეს შემოთავაზებული წვდომის წერტილების დასაერთებლად და სამართავად საჭირო ყველა ლიცენზია 3 წლის ვადით. ვადის გასვლის შემდგომ უსადენო წვდომის წერტილის ლიცენზიენი უნდა იყოს მუდმივი
უსადენო წვდომის წერტილის კონტროლერზე უნდა ვრცელდებოდეს მწარმოებლის სამ წლიანი საგარანტიო მომსახურეობა, ტექნიკური მხარდაჭერა და პროგრამული უზრუნველყოფის განახლება. **მომწოდებელმა უნდა წარმოადგინოს მწარმოებლის ავტორიზაციის წერილი (Manufacturers Authorization Form)** **მომწოდებელმა უნდა წარმოადგინოს გადაწყვეტილების მომწოდებლის კომპლექსური კორპორატიული ქსელების სპეციალიზაცია**

5. C ტიპის კომუტატორი რაოდენობა 2 (ორი)

მოთხოვნები წარმადობის და აპარატურული უზრუნველყოფის მიმართ	
ფიზიკური ინტერფეისები	არანაკლებ 24 x 10/100/1000 მბ/წმ Rj-45 პორტი არანაკლებ 8 x 1/10 გბ/წმ SFP+ პორტი
მართვის ინტერფეისები	არანაკლებ 1 x 10/100/1000 მბ/წმ Rj-45 პორტი მართვის პორტი არანაკლებ 1 x Rj-45 კონსოლის პორტი არანაკლებ 1 x USB კონსოლის პორტი
კომუტაციის წარმადობა	არანაკლებ 200 გბ/წმ არანაკლებ 150 მილიონი პაკეტი წამში
კომუტაციის წარმადობა სტეკში	არანაკლებ 600 გბ/წმ არანაკლებ 500 მილიონი პაკეტი წამში
ჯამური MAC მისამართების რაოდენობა	არანაკლებ 30,000

IPv4 მარშუტების რაოდენობა	არანაკლებ 30,000
IPv4 Multicast მარშუტების რაოდენობა	არანაკლებ 7,000
IPv6 მარშუტების რაოდენობა	არანაკლებ 15,000
QoS ჩანაწერების რაოდენობა	არანაკლებ 5,000
ACL ჩანაწერების რაოდენობა	არანაკლებ 5,000
ქსელური ნაკადების აღრიცხვის რესურსი	არანაკლებ 60,000 ნაკადის
ოპერატიული მეხსიერება	არანაკლებ 8 გბ
Flash	არანაკლებ 16 გბ
VLAN IDs	4094
Switched Virtual Interfaces	არანაკლებ 900
ე.წ. Jumbo frame ზომა	არანაკლებ 9100 bytes
პაკეტების ბუფერის ზომა	არანაკლებ 16 მბ
Rack Unit	1 RU
კომუტატორს უნდა გააჩნდეს სარეზერვო AC ტიპის კვების ბლოკი.	
მოთხოვნები სამუშაო გარემოს მიმართ: არანაკლებ -5°C დან +45°C	
მოთხოვნები პროგრამული უზრუნველყოფის, ტექნოლოგიების და ოქმების მიმართ:	
კომუტაციის ტექნოლოგიები	• Layer 2, RIP, EIGRP, OSPF, PBR, PIM Stub, PVLAN, VRRP, PBR, QoS, 802.1X, MACsec-128, Control Plane სიბრტყეზე მიმავალი ტრაფიკის კონტროლის შესაძლებლობა, MSTP/IEEE 802.1s, IEEE 802.1w
ტელემეტრიის და ქსელის ხილვადობის ტექნოლოგიები	• Model Driven Telemetry, NetFlow (ან ანალოგი), SPAN, RSPAN
მეორე დონის ტრაფიკის შიფრაციის ტექნოლოგები, ყველა პორტზე.	• MACsec-128
მომავალში მხოლოდ პროგრამული ლიცენზიის დამატებით, კომუტატორს უნდა გააჩნდეს შემდეგი ტექნოლოგიების მხარდაჭერა, მათ შორის:	

დაშიფრული არსების პასიურათ მონიტორინგის ტექნოლოგია	• TLS - დაშიფრული არხების პასიურად, დეშიფრაციის გარეშე მონიტორინგის შესაძლებლობა
	• TLS დაშიფრული ქსელური ნაკადებიდან, სხვადასვა პარამეტრების ექსპორტირების შესაძლებლობა:
	  ○ TLS content ტიპის მნიშნველობა
	  ○ TLS handshake ტიპის მნიშნველობა
	  ○ TLS შიფრაციის ალგორითმების ნაკრები
	  ○ TLS გაფართოების სიგრძე
	  ○ TLS გაფართოების ტიპები
	  ○ TLS ვერსია
	  ○ TLS key length
	  ○ TLS სესიის ID
	  ○ TLS random მნიშნველობა
	• ექსპორტირების შესაძლებლობა NetFlow ან ანალოგიურ პროტოკოლში

აუდიო და ვიდეო კომუტაცია	• IEEE 802.1BA სტანდარტის მხარდაჭერა, ყველა პორტზე
დროის სინქრონიზაციის მხარდაჭრა	• IEEE 1588v2/PTP
NAT სერვისის მხარდაჭერა	• Static ტიპის ტრანსლაცია • Dynamic ტიპის ტრანსლაცია • PAT ტიპის ტრანსლაცია

IPv6 სერვისების მხარდაჭერა	• Dual-stack IPv4/IPv6
	• IPv6 over IPv4 GRE Tunnels
	• Adjusts MSS value of IPv6/TCP
	• IPv6 უსაფრთხოების მხარდაჭერა
	  ○ RA Guard
	  ○ DHCPv6 უსაფრთხოება
	  ○ უცნობი IPv6 მისამართიდან წამოსული ტრაფიკის ბლოკირება
	  ○ მხოლოდ იმ IPv6 მისამართების რესულუცია რომლებიც ატიურია სეგმენტზე
	  ○ ND multicast Neighbor Solicit (NS) ის კონტროლის შესაძლებლობა,

	ე.წ drop და unicast ში გადაყვანის შესაძლებლობა ○ IPv6 ACL - ტრაფიკის ფილტრაციის სიების მხარდაჭერა
მეორე დონის ტრაფიკის შიფრაციის ტექნოლოგები, ყველა პორტზე.	• MACsec-256
ქსელის სეგმენტაციის ტექნოლოგიების მხარდაჭერა	• VRF, VXLAN
ქსელში სერვისების აღმოჩენის მხარდაჭერა	• Multicast DNS (mDNS) gateway
ქსელური პაკეტების მონიტორინგის მხარდაჭერა	• Wireshark
ქსელური მარშრუტიზაციის პროტოკოლების მხარდაჭრა	• BGPv4, BGPv6, OSPFv3, IS-IS, BSR, MSDP, PIM-BIDIR, PIM-SM, PIM-SSM, BGP-EVPN (EVPN VXLAN ფაბრიკის მხარდაჭერა)
ქსელური აპლიკაციების იდენტიფიცირების შესაძლებლობა	• კომუტატორს უნდა გააჩნდეს შესაძლებლობა განახორციელოს ქსელური აპლიკაციების ამოცნობა. არანაკლებ 1000 აპლიკაციის ამოცნობის შესაძლებლობა ქსელურ ტრაფიკში და 100 დაშიფრული აპლიკაციის. • ამოცნობილი აპლიკაციების და მათი წარმადობის ინფორმაციის რეპორტინგის შესაძლებლობა. • აპლიკეციების ინფორმაციის ექსპორტირების შესაძლებლობა NetFlow ან ანალოგიურ პროტოკოლში
კომუტატორს უნდა გააჩნდეს სტეკირების ტექნოლოგია. სტეკში შესაძლებელი უნდა იყოს არანაკლებ 8 კომუტატორის გაერთიანება. სტეკის შეერთების წარმადობა არანაკლებ 460 გბ/წმ. სტეკირების უზრუნველყოფა არ უნდა იკავებდეს კომუტატორზე, მოთხოვნილ 1/10/25 გბ/წმ პორტებს. სტეკირების ტექნოლოგიის ფარგლებში კომუტატორებს ასევე უნდა შეეძლოს სტეკში შემავალი ყველა კვების ბლოკის წყაროს გაერთიანება, ერთიან რესურსად. არანაკლებ 4 კომუტატორისა. ნებისმიერ კომუტატორს აღნიშნულ სტეკში უნდა შეეძლოს კვების რესურსის მიღება საჭიროებისამებს. სტეკში შემავალ ნებისმიერ	

<table>
<tr><td colspan="2">კომუტატორზე კვების ბლოკის მწყობრიდან გამოსვლის შემთხვევაში, კომუტატორს კვების მიღება უნდა შეეძლოს სტეკის ცენტრალური კვების წყაროდან.</td></tr>
<tr><td>ლოგიკურ ჯგუფებზე დაფუძნებული უსაფრთხოებია და კონტროლის განსაზღვრა</td><td>კომუტატორს უნდა შეეძლოს ქსელური რესურსების დინამიური და სტატიკური კლასიფიკაცია ლოგიკურ ჯგუფებში, შემდეგი პარამეტრებით:
3. დინამიური კლასიფიკაცია უნდა განისაზღვროს მინიმუმ:
a. 802.1X აუთენტიფიკაციით
b. ვებ აუთენთიფიკაციით
c. MAC მისამართის აუტენტიფიკაციით
4. სტატიკური კლასიფიკაცია უნდა განისაზღვროს მინიმუმ:
a. IP მისამართით
b. VLAN_ით
c. ქვექსელით
d. მესამე დონის ინტერფეისით
• ლოგიკურ ჯგუფში შესაძლებელი უნდა იყოს რესურსების განსაზღვრა/კლასიფიკაცია მიუხედავად მათი ლოკაციისა , ქვექსელის მისამართისა და VLAN ნომრისა.
• ლოგიკური ჯგუფის იდენტიფიკატორის ტრანსპორტირება შესაძლებელი უნდა იყოს როგორც დამატებითი თავსართი ქსელური ნაკადის შესახებ.
• კომუტატორს უნდა შეეძლოს ლოგიკურის ჯგუფების იდენთიფიკატორზე დაფუძნებული უსაფრთხოების/ტრაფიკის ფილტრაციის პოლიტიკების გამართვა.</td></tr>
<tr><td colspan="2">საკუთრივ კომუტატორს უნდა გააჩნდეს სხვადასხვა სახის ავტომატიზაციის მხარდაჭერა, მათ შორის:
4. NETCONF - პტოკოლის მხარდაჭერა
5. RESTCONF - პტოკოლის მხარდაჭერა
6. gRPC - პტოკოლის მხარდაჭერა
7. YANG - მონაცემთა მოდელის მხარდაჭერა</td></tr>
</table>

8. ZTP - კომუტატორს უნდა შეეძლოს ავტომატურად მიიღოს, სხვადასხვა სახის სტარტაპის პარამეტრები, მათ შორის: ოპერაციული სისტემა, კონფიგურაციის ფაილი, ლიცენზია, წვდომის რეკვიზიტები და სკრიპტები; 9. Linux Shell ის უზრუნველყოფა: a. Linux გარემოზე წვდომა b. Python 2.7 და Python 3.6 ის მხარდაჭერა c. Python PIP install ის მხარდაჭერა d. NCCLIENT ბიბლიოთეკის მხარდა e. Yum ის მხარდაჭერა f. RPM Install ის მხარდაჭერა
საკუთრივ კომუტატორს უნდა გააჩნდეს, კონტეინერული აპლიკაციების გაშვების შესაძლებლობა. 1. Docker - კონტეინერების მხარდაჭერა 2. Flash - მეხსიერებაზე კონტეინერების გაშვების შესაძლებლობა 3. SSD - დისკის დამატების შესაძლებლობა, კონტეინერების გასაშვებად 4. კონსოლზე ლოგირების მხარდაჭერა 5. REST API - არსებობა
კომუტატორზე უნდა ვრცელდებოდეს მწარმოებლის სამ წლიანი საგარანტიო მომსახურეობა, ტექნიკური მხარდაჭერა და პროგრამული უზრუნველყოფის განახლება.მოწყობილობის დაზიანების მიზეზის დადგენის შემდეგ, მოწყობილობა უნდა შეკეთდეს ან შეცვალოს შემდეგ სამუშაო დღეს. **მომწოდებელმა უნდა წარმოადგინოს მწარმოებლის ავტორიზაციის წერილი (Manufacturers Authorization Form)**

6. ქსელური ტრანსივერები

ტრანსივერის ტიპი	რაოდენობა	არხის ტიპი
A ტიპის ტრანსივერი	4	10GBASE-BXU SM
B ტიპის ტრანსივერი	4	10GBASE-BXD SM

7. მონაცემთა ცენტრის მოწყობა

1. მოსაწყობია სასერვერო-სატელეკომუნიკაციო კვანძი:

1.1 სასერვერო კარადა 19“ 42RU 800x1000 მმ. – 1 ცალი;

1.2 უწყვეტი კვების წყარო, On-Line UPS 6 kW – 2 ცალი;

1.3 ოპტიკურ-ბოჭკოვანი 19“ პატჩ-პანელი - 1 ცალი.

1.4 პასიური კომპონენტები - საკაბელო ორგანაიზერები, PDU – 1 კომპლექტი.

1.5 არსებულ სასერვერო ოთახში ჰაერის გაგრილების სისტემის მოწყობა სიმძლავრით 35 kW. რეზერვირება - N+1.
1.6 არსებულ სასერვერო ოთახში თაბაშირ-მუყაოს ტიხრის დემონტაჟი;
1.7 არსებულ სასერვერო ოთახში მინის ვიტრაჟის დემონტაჟი;
1.8 არსებულ სასერვერო ოთახში ფანჯრის ამოშენება თაბაშირ-მუყაოს ფილებით და თბოიზოლაციის მოწყობა მინერალური ბამბით.
2. მოსაწყობია სააბონენტო-სატელეკომუნიკაციო კვანძები - 4 კვანძი:
2.1 სატელეკომუნიკაციო კარადა 19“ 21RU 600x600 მმ. – 1 ცალი;
2.2 უწყვეტი კვების წყარო, On-Line UPS 2 kW – 1 ცალი;
2.3 ოპტიკურ-ბოჭკოვანი 19“ პატჩ-პანელი - 1 ცალი;
2.4 პასიური კომპონენტები - საკაბელო ორგანაიზერები, PDU – 1 კომპლექტი.
3. მოსაწყობია ოპტიკურ-ბოჭკოვანი ქსელი, რომელიც დააკავშირებს სასერვერო კვანძს სააბონენტო კვანძებთან:
3.1 ოპტიკურ-ბოჭკოვანი ქსელის ლოგიკური ტოპოლოგია - ვარსკლავი;
3.2 ოპტიკურ-ბოჭკოვანი კაბელის ტიპი - ADSS;
3.3 ოპტიკური ბოჭკოს სტანდარტი - G.652D;
3.4 ინტერფეისის ტიპი - LC/UPC Duplex.
4. მოსაწყობია სასერვერო-სატელეკომუნიკაციო კვანძის ავტონომური ენერგო მომარაგების სისტემა დიზელ-გენერატორის მეშვეობით:
4.1 დიზელ გენერატორის ძაბვა - 400/230 VAC;
4.2 დიზელ გენერატორის სიმძლავრე - Standby 70 kVA, არა ნაკლები;
4.3 დიზელ გენერატორის შესრულება - Outdoor;
4.4 დიზელ გენერატორის რეზერვის ავტომატური ჩართვა - ჩაშენებული;
4.5 დიზელ გენერატორი მონიტორინგი - WEB/SNMP;
4.6 მოსაწყობია სათანადო ზომის რკინა ბეტონის ბალიში;
4.7 მოსაწყობია დიზელ გენერატორის დამიწების კონტური.
5. საადმინისტრაციო შენობის მეორე სართულზე ლოკალური ქსელის მოწყობა.
5.1 სააბონენტო წერტილების რაოდენობა - 48;
5.2 ქსელის კაბელის სტანდარტი - Cat5e FTP AWG24 100% Copper;
5.3 ქსელის კაბელის საორიენტაციო ჯამური სიგრძე - 2440 - 3050 მეტრი;
5.4 ქსელი მოეწყოს PVC საკაბელო არხების მეშვეობით;
5.5 სააბონენტო როზეტები მოეწყოს საკაბელო არხებში;
5.6 სასერვერო კარადაში კაბელების ტერმინირება მოხდეს Cat5e FTP პატჩ-პანელზე;
5.7 პატჩ-პანელის რაოდენობა - 2 ცალი;
5.8 პასიური კომპონენტები - საკაბელო ორგანაიზერები - 2 ცალი.

II ეტაპი

8. ჰიპერ-კონვერგენტული პროგრამულ-აპარატურული კომპლექსი

№	მოთხოვნა
1.	პროგრამულმა უზრუნველყოფამ უნდა უზრუნველყოს გამოთვლითი რესურსების, მონაცემთა შენახვის სისტემის, ვირტუალიზაციის სისტემის და მართვის პროგრამული უზრუნველყოფის, ასევე კომპლექსის მაჩვენებლების ანალიზისა და მონიტორინგის ერთიან სისტემაში ინტეგრაცია.
2.	პროგრამულმა უზრუნველყოფამ უნდა უზრუნველყოს ჰიპერ-კონვერგენტული პროგრამულ-აპარატული კომპლექსის მარტივი მასშტაბირება, სერვისების მუშაობის შეწყვეტის გარეშე. პროგრამულმა უზრუნველყოფამ უნდა უზრუნველყოს სხვადასხვა დისკური კონფიგურაციის კვანძების გამოყენების შესაძლებლობა (კვანძები SATA/SAS SSD და HDD კვანძებით SATA/SAS SSD დისკებით) ერთ პროგრამულ-აპარატულ კომპლექსში (კლასტერში).
3.	პროგრამულმა უზრუნველყოფამ უნდა უზრუნველყოს სისტემის შეუფერხებელი ფუნქციონირება და თვითაღდგენა, კლასტერში არანაკლებ ორი კვანძის მწყობრიდან გამოსვლის შემთხვევაში.
4.	პროგრამულმა უზრუნველყოფამ უნდა უზრუნველყოს კომპლექსის მიერ დამუშავებული და შენახული მონაცემების დაცვის მექანიზმი, მონაცემთა ასლების შენახვის პოლიტიკის თანახმად. ასლების რაოდენობის დავალების მხარდაჭერა 2 და 3 ასლის ოდენობით.
5.	პროგრამულმა უზრუნველყოფამ უნდა უზრუნველყოს ვირტუალური მანქანების და ვირტუალური მანქანების ჯგუფების მიმართ მონაცემთა დაცვის/მდგრადობის პოლიტიკების გამოყენება.
6.	პროგრამულმა უზრუნველყოფამ უნდა უზრუნველყოს ჰიპერ-კონვერგენტული პროგრამულ-აპარატული კომპლექსის ყველა კომპონენტის პროგრამული უზრუნველყოფის რეკომენდაციების და განახლებისა ჩაშენებული მექანიზმი, ამ კომპლექსის გაჩერების გარეშე, მათ შორის სერვერების კომპონენტების ე.წ firmware ების.
7.	პროგრამულმა უზრუნველყოფამ უნდა უზრუნველყოს, კომპლექსის დისკის ქვესისტემაზე დატვირთვის ოპტიმიზაციის, დისკის სივრცის გამოყენების ოპტიმიზაციის და მონაცემების მრავალდონიანი შენახვისთვის ტექნოლოგიები: • ხშირად გამოყენებადი მონაცემების გადატანა Flash მეხსიერების ბარათებზე (NVMe SSD, SAS და SATA SSD ტიპის) და მონაცემების, რომლებთან წვდომაც ბევრად იშვიათია, მეხსიერების მაგნიტურ დისკზე (HDD); • მონაცემების დედუპლიკაციის ჩაშენებული ფუნქციონალი. ფლეშ-მეხსიერების ბარათების (NVMe SSD, SAS და SATA SSD ტიპის) და მეხსიერების მაგნიტური დისკის (HDD) მხარდაჭრა;

	• მონაცემების კომპრესიის ჩაშენებული ფუნქციონალი. ფლეშ-მეხსიერების ბარათების (NVMe SSD, SAS და SATA SSD) და მეხსიერების მაგნიტური დისკის (HDD) მხარდაჭრა; • Erasure Coding-ის ტიპის დისკური სივრცის ოპტიმიზაციის ჩაშენებული ფუნქციონალი.
8.	პროგრამულმა უზრუნველყოფამ უნდა უზრუნველყოს მონაცემთა ოპტიმიზაციის პოლიტიკების შექმნის შესაძლებლობა (კომპრესაცია, დედუპლიკაცია და Erasure Coding), მათი ვირტუალურ მანქანებზე და ვირტუალური მანქანების ჯგუფებზე გამოყენება.
9.	პროგრამულმა უზრუნველყოფამ უნდა უზრუნველყოს ხშირად გამოყენებული ვირტუალური მანქანების მონაცემების წაკითხვა ლოკალურად, Flash ტიპის დისკებიდან, რომლებზეს გაშვებულია ვირტუალური მანქანა.
10.	პროგრამულმა უზრუნველყოფამ უნდა უზრუნველყოს, კომპლექსის დისკური მასივის მიწოდების ფუნქციონირება iSCSI პროტოკოლით, ვირტუალური დისკების სახით, ჰიპერვიზორის გვერდის ავლით პროგრამულ-აპარატული კომპლექსის კვანძებზე დატვირთვის ბალანსირებით. კომპლექსის დისკური მასივის მიწოდება შესაძლებელი უნდა იყოს იმ ფიზიკური სერვერებისა და ვირტუალური მანქანებისთვის, რომლებიც არ შედიან პროგრამულ-აპარატულ კომპლექსში, და ვირტუალური მანქანებისთვის, რომლებიც გაშვებულია პროგრამულ-აპარატულ კომპლექსზე.
11.	პროგრამულმა უზრუნველყოფამ უნდა უზრუნველყოს ვირტუალური მანქანების ვირტუალური დისკების მყისიერი ასლების შექმნის ფუნქციონალი Redirect on Write ალგორითმის გამოყენებით.
12.	პროგრამულმა უზრუნველყოფამ უნდა უზრუნველყოს ფუნქციონალის არსებობა, რომლის საშუალებითაც შესაძლებელი იქნება შეიზღუდოს დისკური ოპერაციებს მაქსიმალური რაოდენობა ან დისკური რესურსების გამტარუნარიანობა, რომლებიც გაიცემა ვირტუალურ მანქანებზე.
13.	პროგრამულმა უზრუნველყოფამ უნდა უზრუნველყოს მონაცემთა სინქრონული და ასინქრონული რეპლიკაციის ფუნქციონალის არსებობა, ვირტუალური მანქანების, ვირტუალური მანქანების ლოგიკური ჯგუფებისა და iSCSI ვირტუალური დისკების დონეზე.
14.	პროგრამულ უზრუნველყოფას უნდა გააჩნდეს, Recovery Time Objective პარამეტრის კონფიგურაციის შესაძლებლობა 1-დან 15 წუთამდე ასინქრონული რეპლიკაციისთვის.
15.	პროგრამულმა უზრუნველყოფამ უნდა უზრუნველყოს მონაცემთა სინქრონული ან ასინქრონული რეპლიკაციის ტრაფიკის შიფრაციის ფუნქციონალი.
16.	პროგრამულმა უზრუნველყოფამ უნდა უზრუნველყოს მონაცემთა სინქრონული და ასინქრონული რეპლიკაციის ტრაფიკის ცალკე ქსელურ სეგმენტში იზოლაციის ფუნქციონალი.
17.	პროგრამულ უზრუნველყოფას უნდა გააჩნდეს სარეზერვო პროგრამულ-აპარატულ კომპლექსზე რეპლიცირებული ვირტუალური მანქანების აღდგენის ორკესტრაციის ფუნქციონალი. მათ შორის, ვირტუალური მანქანების გაშვების რიგითობა, ქსელების მინიჭება, მანუალურ ან ავტომატურ რეჟიმებში არანაკლებ 1000

	ვირტუალური მანქანისთვის.
18.	პროგრამულმა უზრუნველყოფამ უნდა უზრუნველყოს წაკითხვის ოპერაციის ლოკალიზების ფუნქციონალის არსებობა, კომპლექსის კომუტირებადი ქსელის გამოყენების გარეშე.
19.	პროგრამულ უზრუნველყოფას უნდა შეეძლოს დატვირთვის ოპტიმალურად განაწილება კვანძებს შორის, Dynamic Resource Scheduler ფუნქციონალი.
20.	პროგრამულმა უზრუნველყოფამ უნდა უზრუნველყოს ფუნქციონალის არსებობა, რომლის საშუალებითაც შესაძლებელი იქნება, მხოლოდ FLASH დისკური რესურსების გამოყოფა, ვირტუალურ მანქანების მონაცემების შესანახად.
21.	პროგრამულმა უზრუნველყოფამ უნდა უზრუნველყოს ქსელის ვირტუალიზაციის სერვისი, მათ შორის ვირტუალური ქსელური სეგმენტების შექმნა ჰიპერ-კონვერგენტული პროგრამულ-აპარატული კომპლექსის ფარგლებში, სეგმენტების იზოლაცია და გარე რესურსებზე წვდომის მართვა.
22.	პროგრამულ უზრუნველყოფას უნდა გააჩნდეს ჩაშენებული ქსელის ვირტუალიზაციის სერვისი, რომლის საშუალებითაც შესაძლებელი იქნება ტრაფიკის კონტროლი და მართვა, როგორც ვირტუალური მანქანიდან ასევე ვირტუალურ მანქანებს შორის და ვირტუალური მანქანების ჯგუფებს შორის. აღნიშნული სერვისის ფარგლებში შესაძლებელი უნდა იყოს ვირტუალურ მანქანებს ან მათ ჯგუფებს განესაზღვროს ტეგები, რათა ტეგების საშუალებით განისაზღვროს უსაფრთხოების პოლიტიკები (ტრაფიკის ფილტრაციის პოლიტიკები). ქსელის ვირტუალიზაციის სერვისს უნდა გააჩნდეს Microsoft Active Directory-ის კატალოგების სამსახურთან ინტეგრაცია, რათა უსაფრთხოების პოლიტიკებში შესაძლებელი იყოს მომხმარებლების ჯგუფების და მოხმარებლების განსაზღვრა. ქსელის ვირტუალიზაციის სერვისს უნდა გააჩნდეს ტრაფიკის ვიზუალიზაციის ფუნქციონალი, როგორც ვირტუალი მანქანისკენ ასევე ვირტუალური მანქანიდან და ვირტუალური მანქანების ჯგუფებისთვის. ქსელის ვირტუალიზაციის სერვისს უნდა გააჩნდეს გარე NGFW-ის ტიპის ბრანდმაუერებთან ინტეგრაციის მხარდაჭერა.
23.	პროგრამული უზრუნველყოფის ქსელის ვირტუალიზაციის სერვისის უნდა გააჩნდეს ვირტუალური მანქანებიდან და ვირტუალურ მანქანებამდე ტრაფიკის გამჭვირვალე გადამისამართების ფუნქციონალი, ქსელური სერვისების ვირტუალურ მანქანაზე, როგორიცაა Firewall, IDS, IPS, LB, ქსელის სკანერი და ა.შ.
24.	ქსელის ვირტუალიზაციის სერვისს უნდა გააჩნდეს ე.წ „განაწილებული“ statefull ბრანდმაუერის ფუნქციონალი. უსაფრთხოების პოლიტიკის საშუალებით შესაძლებელი უნდა იყოს თითოეული ვირტუალური მანქანის შემავალი და გამავალი ტრაფიკის გაკონტროლება. შესძლებელი უნდა იყოს პოლიტიკის „დაფიქსირება“ კონკრეტულ ვირტუალურ მანქანაზე იმის მიუხედავად, თუ რომელ ვირტუალიზაციის კვანძზე, რა მომენტში და რომელ მონაცემთა ცენტრში მუშაობს აღნიშნული ვირტუალური მანქანა.
25.	ქსელის ვირტუალიზაციის სერვისს უნდა გააჩნდეს აპლიკაციების მიკროსეგმენტაციის მექანიზმების მხარდაჭრა, მათ შორის ნებისმიერ 2 ვირტუალურ მანქანას შორის გამორიცხოს ყველა ტიპის უკონტროლო ტრაფიკის გატარება, მათ შორის Unicast, Unicast Flood, Broadcast და Multicast, იმ

	შემთხვევაშიც, თუ ეს მანქანები იმყოფებიან საერთო VLAN-ში საერთო ვირტუალიზაციის სერვერზე.

26.	ქსელის ვირტუალიზაციის სერვისს უნდა გააჩნდეს შემდეგი ქსელური სერვისების მხარდაჭერა:
	• ვირტუალური კერძო ქსელების უზრუნველყოფა. თითოეული ვირტუალური კერძო ქსელი უნდა წარმოადგენდეს დამოუკიდებელ ე.წ namespace -ს. სხვადასხვა ვირტუალურ კერძო ქსელებს შორის შესაძლებელი უნდა იყოს IP ქვექსელების გადაფარვა. თითოეულ ვირტუალურ კერძო ქსელს უნდა გააჩნდეს ვირტუალური მარშრუტიზატორის მხარდაჭერა. არანაკლებ 400 ვირტუალური კერძო ქსელის მხარდაჭერა.
	• ტრაფიკის მართვის პოლიტიკები. ვირტუალური კერძო ქსელის დონეზე შესაძლებელი უნდა იყოს ქსელური ტრაფიკის მართვის პოლიტიკების უზრუნველყოფა, მათ შორის ტრაფიკის ფილტრაციის და ტრაფიკის გადამისამართების. ტრაფიკის აღწერა შესაძლებელი უნდა იყოს შემდეგი პარამეტრებით: IPv4 Source (any, IP prefix), Destination (any, IP prefix), Protocol (any, protocol number, tcp, udp, icmp), Source Port Number, Destination Port Number. ტრაფიკზე შესაძლებელი უნდა იყოს შემდეგი ქმედებების განხორციელება: Permit, Deny, Redirect.
	• Network Address Translation - სერვისის უზრუნველყოფა.
	• Static, BGP, OSPF - მარშრუტიზაციის პროტოკოლების მხარდაჭერა.
	• IPSec VPN - სერვისის უზრუნველყოფა.
	• გარე ქსელებთან მიერთების შემდეგი სქემების მხარდაჭერა:
	  ○ Layer 3
	  ○ Layer 2 VXLAN VTEP
	  ○ Layer 2 VXLAN VTEP over IPSec

27.	ქსელის ვირტუალიზაციის სერვისს უნდა გააჩნდეს Citrix VDI გარემოსთან ინტეგრაციის მხარდაჭერა, ვირტუალური სამუშაო მაგიდებისთვის ტრაფიკის კონტროლის, ფილტრაციის მექანიზმების მხარდაჭერა.
28.	პროგრამულმა უზრუნველყოფას უნდა გააჩნდეს სპაციალური უსაფრთხოების ფუნქციონალი, რომლის საშუალებითაც შესაძლებელი იქნება: • პროგრამულ-აპარატული კომპლექსის უსაფრთხოების მიმდინარე მდგომარეობის შეფასება • პროგრამულ-აპარატული კომპლექსის უსაფრთხოების პოტენციური რისკებისა და მოწყვლადობების დადგენა და მათი აღმოფხვრის რეკომენდაციები • ქსელურ და მომხმარებლების ქცევაზე დამოკიდებული ანომალიების აღმოჩენის შესაძლებლობა. შიდა და გარე საფრთხეების დასაფიქსირებლად. • ინფორმაციის ასახვა უსაფრთხოების პანელზე
29.	პროგრამულ უზრუნველყოფას უნდა გააჩნდეს ქსელური ტრაფიკის ანალიზის, ვიზუალიზაცის და კატეგორიზაცის სერვისი რომლის საშუალებითაც სისტემა წარმოადგენს, ტრაფიკის უსაფრთხოების ფილტრაციის პოლიტიკებს და მიკროსეგმენტაციის რეკომენდაციებს.

30.	პროგრამულ უზრუნველყოფას უნდა გააჩნდეს ინტეგრირებული ფაილების და ობიექტების ჩაშენებული სანახი. სანახი ლიცენზირებული უნდა იყოს არანაკლებ 1ტბ მოცულობაზე. ფაილების სანახის ფარგლებში მხარდაჭერილი უნდა იყოს: • SMBv2, SMBv3, NFSv3 და NFSv4 პროტოკოლი • მაღალმდგრადობა • დატვირთვის ბალანსირება, ე.წ scale-up და scaleout • მონაცემების მართვა და ე.წ tiering • ინტეგრაციის არსებობა Microsoft Active Directory-ის კატალოგების სამსახურთან ან სხვა თავსებად OPEN LDAP სერვისთან. • მონაცემთა რეპლიკაციის ფუნქციონალი, ფაილის რესურსის დონეზე (File share) და მტყუნების შემთხვევაში, სარეზერვო პროგრამულ-აპარატულ კომპლექსზე აღდგენის ორკესტრირების შესაძლებლობით. • Internet Content Adaptation Protocol-ის მხარდაჭერა, ფაილური რესურსების სკანირებისთვის ვირუსების არსებობაზე ონლაინ რეჟიმში ფაილის გახსნის, დახურვის, ფაილიდან წაკითხვის და ფაილში ჩაწერის ოპერაციებისთვის. • ფაილური რესურსების გამოყენების ანალიტიკის, სტატისტიკის შეგროვებისა და მათი მონიტორინგის ფუნქციონალი. • Write-once კონფიგურაციის და Read-many პოლიტიკის ფუნქციონალის უზრუნველყოფა, ფაილურ რესურსისთვის (File Share). • მონაცემთა მრავალდონიანი შენახვის ფუნქციონალი ფაილური რესურსებისთვის, S3 მონაცემთა საცავში იშვიათად გამოყენებული ფაილების გადატანის შესაძლებლობით. ობიექტების სანახის ფარგლებში მხარდაჭერილი უნდა იყოს: • S3 პროტოკოლი • Write-Once-Read-Many (WORM) • Immutability • Object Versioning • მონაცემებიც სიცოცხლის ციკლის მართვა • მონაცემების ნაწილებათ ატვირთვის შესაძლებლობა • მონაცემების კრიფტოგრაფიული დაცვა ე.წ "Data-at-Rest Encryption" ინტეგრირებული გასაღებების მართვის შესაძლებლობით • წვდომის და იდენტურობის მართვა
31.	ვირტუალიზაციის ქვესისტემას უნდა გააჩნდეს შემდეგი ვირტუალიზაციის პლათფორმების მხარდაჭერა: VMware vSphere, Microsoft Hyper-V და KVM. გადაწყვეტილება უნდა მოიცავდეს ვირტუალიზაციის ქვესისტემის პროგრამულ

	უზრუნველყოფას.
32.	პროგრამულ უზრუნველყოფას უნდა გააჩნდეს ჰიპერ-კონვერგენტული პროგრამულ-აპარატურული კომპლექსის სხვადასხვა მაჩვენებლების ანალიზის, მონიტორინგის, მართვის და დიაგნოსტიკის (ვირტუალიზაციის სისტემის, ვირტუალური მანქანების, დისკის მასივის, ქსელის ვირტუალიზაციის სერვისის და ა.შ) ფუნქციონალის არსებობა. კომპლექსის ყველა კომპონენტის პროგრამული უზრუნველყოფის განახლება, შესაძლებელი უნდა იყოს ერთიანი მარტივი ინტერფეისის საშუალებით. შესაძლებელი უნდა იყოს ინტერფეისის კასტომიზაცია, საჭირო ინფორმაციის ასახვისთვის.
33.	პროგრამულ უზრუნველყოფას უნდა გააჩნდეს რამოდენიმე ჰიპერ-კონვერგენტული პროგრამულ-აპარატურული კომპლექსის მართვის შესაძლებლობა, მიუხედავად მათი ადგილმდებარეობისა. სხვადასხვა კომპლექსების ცენტრალიზირებული მაჩვენებლების ანალიზი, დიაგნოსტიკა (ვირტუალიზაციის სისტემისა, ვირტუალური მანქანებისა, დისკური მასივისა, ქსელის ვირტუალიზაციის სერვისის და ა.შ), კომპლექსის ყველა კომპონენტის პროგრამული უზრუნველყოფის განახლება ერთიანი მარტივი ინტერფესის საშუალებით. შესაძლებელი უნდა იყოს ინტერფეისის კასტომიზაცია, საჭირო ინფორმაციის ასახვისთვის.
34.	პროგრამულმა უზრუნველყოფამ უნდა უზრუნველყოს კომპლექსის მართვის სისტემის მაღალმდგრადობა.
35.	პროგრამულ უზრუნველყოფას უნდა გააჩნდეს REST API-ის მხარდაჭერა, ჩაშენებული სერვისებისა და ქვესისტემებისათვის.
36.	პროგრამულ უზრუნველყოფამ უნდა უზრუნველყოს პროგრამულ-აპარატული კომლექსის რესურსებისის დროში განვრცობილათ უტილიზაციის ანალიზისა და ვირტუალური მანქანების კონფიგურაციის შეცვლის რეკომენდაციების მიწოდების ფუნქციონალი, ვირტუალური მანქანების რესურსების უტილიზაციის პროფილის შესაბამისად.
37.	პროგრამულ უზრუნველყოფამ უნდა უზრუნველყოს რესურსების მოხმარების პროგნოზების მიწოდების ფუნქციონალი, ისტორიულ მონაცემებზე დაყრდნობით. ასევე პროგრამულ-აპარატული კომპლექსის პოტენციური მასშტაბირების შესახებ რეკომენდაციების მიწოდება.
38.	პროგრამულ უზრუნველყოფამ უნდა უზრუნველყოს პროგრამულ-აპარატული კომლექსის, მისი ქვესისტემებისა და ვირტუალური მანქანების მდგომარეობის შესახებ ანგარიშების შექმნის ფუნქციონალი, ანგარიშების PDF და CSV ფორმატში ჩამოტვირთვის და ელექტრონულ ფოსტაზე ავტომატურად გაგზავნის შესაძლებლობა.
39.	პროგრამულ უზრუნველყოფამ უნდა უზრუნველყოს ამოცანების შესრულების ავტომატიზაციის ფუნქციონალი, რომელიც ეფუძნება შესაბამისი ტრიგერების რეაგირებას მოვლენაზე, შეტყობინებებზე, API ზარებზე და ა.შ.
40.	პროგრამული უზრუნველყოფა უნდა უზრუნველყოფდეს პროგრამულ-აპარატული კომპლექსისთვის Total Cost of Ownership ანგარიშის მიწოდების ფუნქციონირებას.
41.	პროგრამული უზრუნველყოფა უნდა უზრუნველყოფდეს შიფრაციის ფუნქციონალს ვირტუალური მანქანების მონაცემებისთვის, რომლებიც ინახება და

	მუშავდება პროგრამულ-აპარატული კომპლექსის მიერ, ვირტუალურ მანქანებსა და ვირტუალური მანქანების ჯგუფებზე ან/და მთლიანად პროგრამულ-აპარატულ კომპლექსზე, მონაცემთა შიფრაციის პოლიტიკების მინიჭების გზით.
42.	პროგრამულ უზრუნველყოფას უნდა გააჩნდეს მონაცემთა შიფრაციის გასაღების მართვის ჩაშენებული სერვისი.
43.	მონაცემთა შენახვის ქვესისტემის არქიტექტურას უნდა გააჩნდეს მონაცემთა ე.წ Tiering ის მხარდაჭერა (და არა კეშირების, სწრაფ დისკებზეს).
44.	პროგრამულ უზრუნველყოფას უნდა გააჩნდეს ჩაშენებული, ავტომატიზაციის მოდული, რომლის საშუალებითაც შესაძლებელი იქნება შაბლონებზე დაფუძნებით სხვადა სერვისების გამართვა, მათ შორის მონაცემთა ბაზების, ვირტუალური ეპლაინსების და ა.შ.ს
45.	პროგრამულმა უზრუნველყოფამ უნდა უზრუნველყოს პროგრამულ-აპარატული კომპლექსის მდგომარეობის შესახებ დიაგნოსტიკური ინფორმაციის მუდმივი გაგზავნის ფუნქციონალი მწარმოებლის პროაქტიული მხარდაჭერისთვის.
46.	პროგრამული უზრუნველყოფის მწარმოებელმა უნდა უზრუნველყოს დამკვეთის პროგრამულ-აპარატული კომპლექსიდან შეგროვებულ დიაგნოსტიკურ ინფორმაციაზე წვდომა, ასევე რეკომენდაციები რისკების აღმოფხვრისა და ინფრასტრუქტურის ოპტიმიზაციის შესახებ მონაცემების ანალიზზე დაყრდნობით.
47.	პროგრამული უზრუნველყოფის ლიცენზირება, უნდა წარმოადგენდეს ბაზურ ფუნქციონალს და გათვლილი უნდა იყოს არანაკლებ 2 წელზე ვადით.
48.	პროგრამული უზრუნველყოფის მწარმოებლისაგან ტექნიკური მხარდაჭერის ვადა: არანაკლებ 3 წელი, 24 საათი დღე-ღამეში, 7 დღე კვირაში.
49.	პროგრამულ აპარატული კომპლექსის მწარმოებლის, ტექნიკური მხარდაჭერის რეაგირების დრო არაუმეტეს 1 საათისა.
50.	ჰიპერ-კონვერგენტული პროგრამულ-აპარატურული კომპლექსის პროგრამული უზრუნველყოფის ლიცენზიის გადატანა შესაძლებელი უნდა იყოს მწარმოებლის მიერ სერტიფიცირებულ სხვადასხვა სერვერულ პლათფორმებს შორის.
51.	მომწოდებელმა უნდა წარმოადგინო მწარმოებლის ავტორიზაციის წერილი (MAF)

9. ტექნიკური მოთხოვნები ჰიპერ-კონვერგენტული პროგრამულ-აპარატული კომპლექსის კვანძებთან

№	მოთხოვნა
	კვანძების მინიმალური რაოდენობა: არანაკლებ 3 ც.
1.	არანაკლებ 24 ბირთვი ერთ კვანძზე, (HT ტექნოლოგიის არჩათვლით Intel-ის პროცესორებისთვის და AMD-ს პროცესორების ანალოგიური ტექნოლოგიისა).
2.	პროცესორის ბირთვის მინიმალური სიხშირე ერთდროულად ყველა ბირთვისათვის – 2.6 GHz.
3.	პროცესორის ქეშ-მეხსიერების მინიმალური მოცულობა – 60 MB.

4.	ერთ კვანძზე ოპერატიული მეხსირების მინიმალური მოცულობა– 768 GB.
5.	ერთ კვანძზე ქსელური პორტების მინიმალური რაოდენობა – 4 ცალი 10/25გბ/წმ.
6.	Cache-ის ტიპის „ნედლი“ დისკური სივრცის მინიმალური მოცულობა -23.04TB. არაუმეტეს 6 NVMe ტიპის დიკი, 3.84TB მოცულობით, მეოთხე თაობის ე.წ High Performance Read Intensive.
7.	დღეში სულ ცოტა ერთი სრული გადაწერის მხარდაჭერა დისკური სივრცე SSD ბარათისა.
8.	მწარმოებლის ტექნიკური მხარდაჭერია: არანაკლებ 3 წელი, რეაგირების დრო 9x5 დონე. დაზიანებული კომპონენტის შეკეთება ან შეცვლა.
9.	მომწოდებელმა უნდა წარმოადგინო მწარმოებლის ავტორიზაციის წერილი (MAF)

10. მონაცემთა რეზერვირების სისტემა

№	მოთხოვნა
	მონაცემთა რეზერვირების სისტემების მინიმალური რაოდენობა: არანაკლებ 2 ც.
1.	ოპერატიული: არანაკლებ
2.	დრაივების რაოდენობა: არანაკლებ 12, აღჭურვილი არანაკლებ 9(ცხრა) 4 TB, SATA 6 Gb/s, 7200 rpm, 240MB სიჩქარე
3.	ქსელის პორტები: არანაკლებ 2 x 1Gb Rj-45, 1 x 10Gb Rj-45, 2 x 10Gb SFP+
4.	PCIe 3.0 სლოტი
5.	New connections/sec
6.	პროცესორი: არანაკლებ 3.3 GHz, ოთხ ბირთვიანი
7.	ოპერატიული მეხსიერება: არანაკლე 16გბ
8.	ქსელური პროტოკოლები: არანაკლებ SMB, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, Telnet, SSH, SNMP, and VPN (PPTP, OpenVPN™, L2TP)
9.	მონაცემთა სანახის მართვა: • მაქსიმალური ტომის მოცულობა: არანაკლებ 100TB • მაქსიმალური სნეპშორების რაოდენობა: არანაკლებ 65000 • მაქსიმალური შიდა ტომების რაოდენობა: არანაკლებ 64
10.	ფაილების გაზიარების შესაძლებლობები: • ლოკალური მომხმარებლების რაოდენობა: არანაკლებ 2000 • ლოკალური ჯგუფების რაოდენობა: არანაკლებ 356 • ლოკალური გაზირებული ფოლდერების რაოდენობა: არანაკლებ 512 • კონკურენტული SMB/NFS/AFP/FTP შეერთებების რაოდენობა: არანაკლებ 2000
11.	უსაფრთხოების მხარდაჭერა: Firewall, shared folder encryption, SMB encryption, FTP over SSL/TLS, SFTP, rsync over SSH, login auto block, Let's Encrypt support, and HTTPS (customizable cipher suite)
12.	ფაილური სისტემები: არამაკლებ Btrfs, ext4, ext3, FAT32, NTFS, HFS+, exFAT

13.	RAID 5 ის მხარდაჭერა: არანაკლებ JBOD, RAID 0, RAID 1, RAID 5, RAID 6, and RAID 10
14.	რეზერვირებული კვების ბლოკი
15.	მომწოდებელმა უნდა წარმოადგინოს მწარმოებლის ავტორიზაციის წერილი (MAF)

11. მონაცემთა რეზერვირების პროგრამული უზრუნველყოფა

№	მოთხოვნა
	მონაცემთა რეზერვირების პროგრამული უზრუნველყოფის ლიცენზირება გათვლილი უნდა იყოს, 10 ვირტუალურ მანქანაზე 3 წლის ვადით
16.	სისტემამ უნდა უზრუნველყოს ცენტრალიზებული მართვა Web UI ინტერფეისის მეშვეობით;
17.	სისტემა დისკზე უნდა იკავებდეს მცირე ადგილს და ამავე დროს იყოს ძლიერი, ფუნქციონალური და წარმადი;
18.	სისტემის ინტეგრაცია ადვილად უნდა იყოს შესაძლებელი ჰიპერ-კონვერგენტული პროგრამულ-აპარატურული ინფრასტრუქტურაში;
19.	სისტემა უნდა იყოს მარტივი გამოსაყენებელი და მოიცავდეს ყველა აუცილებელ კომპონენტს და ლიცენზიას, რომელიც საჭიროა ინტეგრაციისთვის მათ შორის ისეთ კომპონენტებს, როგორიცაა: ოპერაციული სისტემა, DB ან სხვა კომპონენტები, რომლებიც საჭიროა ტექნიკური გადაწყვეტის ნორმალური ფუნქციონირებისთვის;
20.	სისტემას უნდა ჰქონდეს მონაცემთა დაცვის მხარდაჭერა Linux, Unix და Windows გარემოსთვის;
21.	სისტემამ უნდა უზრუნველყოს მონაცემთა დაცვის აგენტები შემდეგი აპლიკაციებისა და მონაცემთა ბაზებისთვის:MS SQL, PostgreSQL, MongoDB.
22.	სისტემა უნდა იყოს ე.წ multi-cloud ოპტიმიზირებული და იძლეოდეს საშუალებას, განხორციელდეს ორგანიზაციის მონაცემთა ცენტრის ეფექტური გაფართოება ღრუბლოვან გარემომდე, მონაცემების გრძელვადიანი შენარჩუნების, კატასტროფის შემთხვევაში აღდგენის, ბექაფირებას როგორც ღრუბელში ასევე ღრუბლის შიგნით განთავსებულ რესურსებზე;
23.	სისტემამ უნდა უზრუნველყოს ყოველდღიურად სწრაფი და ეფექტური სრული სარეზერვო ასლების დამზადება ;
24.	სისტემამ უნდა უზრუნველყოს გაფართოებული სარეზერვო და აღდგენის შესაძლებლობები, როგორიცაა მყისიერი წვდომა, პირდაპირი აღდგენა ვირტუალიზაციაშ და ვირტუალური ინფრასტრუქტურის გრანულირებული აღდგენა;
25.	მომწოდებელმა უნდა წარმოადგინოს მწარმოებლის ავტორიზაციის წერილი (MAF)

12. ბრანდმაუერი A ტიპის

1	რაოდენობა: 2
2	მოწყობილობის გამტარობა ქსელის დამცავი რეჟიმში აპლიკაციების და მომხმარებლების იდენტიფიკაციით, ლოგირებით - არანაკლებ 2.5 გბ/წმ. (ტრაფიკის პროფილი დამიქსული აპლიკაციებით)
3	მოწყობილობის გამტარუნარიანობა (Application Control, IPS, Anti-Virus, Anti-spyware ან Anti-bot, Zero Day Attacks Detection and Analysis) - არანაკლებ 1 გბ/წმ; (ტრაფიკის პროფილი დამიქსული აპლიკაციებით) ასევე უნდა იყოს გამოქვეყნებული მწარმოებლის ოფიციალურ ვებგვერდზე;
4	IPsec VPN გამტარობა უნდა შეადგენდეს მინიმუმ 1 Gbps;
5	წამში ახალი სესიების მაქსიმალური რაოდენობა არანაკლებ 32000;
6	სესიების მაქსიმალური რაოდენობა არანაკლებ 200,000;
7	სიმაღლე არაუმეტეს 1 Rack Unit
8	მოწყობილობა უნდა შედგებოდეს, მართვის კომპონენტისა და ტრაფიკის დამუშავების დამოუკიდებელი პროგრამული და აპარატული კომპონენტებისგან. თითოეულ კომპონენტს უნდა ჰქონდეს პროცესორების (CPU), RAM (მეხსიერება) და ინტერფეისების (Ethernet პორტი) საკუთარი ნაკრები. აღნიშნული კომპონენტები ერთმანეთისგან დამოუკიდებლად უნდა იყვნენ, რათა შეძლონ მოწყობილობის კონტროლი კრიტიკული დატვირთვის შემთხვევაში, განსაკუთრებით DoS / DDoS შეტევების დროს.
9	არანაკლებ: 8 x 100/1000/10000 მბ/წმ სპილენძის ინტერფეისი არანაკლებ: 1 x 100/1000/10000 მბ/წმ სპილენძის OOB ტიპის ინტერფეისი არანაკლებ: 1 x RJ45 console ინტერფეისი არანაკლებ: 2 x USB ინტერფეისი არანაკლებ: 1 x Micro USB console ინტერფეისი
10	სტატიკური IPv4 / IPv6 მარშრუტიზაციისა და დინამიური მარშრუტიზაციის პროტოკოლების BGPv4, OSPFv2 / v3, RIP v2 მხარდაჭერა. თუ ამ ფუნქციონალისათვის საჭირო დამატებითი ლიცენზია, ის უნდა იყოს შეტანილი შემოთავაზებაში;
11	ქსელის ინტერფეისებს უნდა ჰქონდეს მხარდაჭერა Span- პორტებიდან "დუბლირებული" ტრაფიკის მოსმენის, MAC და IP- მისამართის (Virtual Wire) შეცვლის გარეშე, Layer 2 რეჟიმის, ტრაფიკის მარშრუტიზაციის რეჟიმის (Layer 3);
12	მხარდაჭერა ქსელის სხვადასხვა ინტერფეისების ერთდროულად მუშაობაში ჩამოთვლილ ნებისმიერ რეჟიმში ნებისმიერ კომბინაციაში შეზღუდვების გარეშე ერთი ვირტუალური ბრანდმაუერის შიგნით;

13	პორტის მუშაობის რეჟიმის შეცვლის მხარდაჭერა (Layer 2, Layer 3, გამჭვირვალე რეჟიმი და მოსმენის რეჟიმი) მოწყობილობის გადატვირთვის გარეშე;
14	სტატიკური და დინამიური (Hide) NAT– ის მხარდაჭერა
15	NAT მხარდაჭერა გამჭვირვალე რეჟიმში
16	IPV6 მხარდაჭერა, მათ შორის, პროგრამა და მომხმარებლის იდენტიფიკაცია
17	multicast მარშრუტიზაციის პროტოკოლების მხარდაჭერა - PIM-SM, PIM-SSM, IGMP v1, v2, v3.
18	ბრანდმაუერზე ორგანიზებულ VLAN ქსელებს შორის მარშრუტიზაციის მხარდაჭერა
19	მოწყობილობამ უნდა უზრუნველყოს არანაკლებ 4000 vlan ერთ ინტერფეისზე;
20	NAT ტრანსლაციების, DHCP სერვერის და DHCP relay ფუნქციონირების მხარდაჭერა.
21	802.1-ზე ტეგირებული ფრეიმების მხარდაჭერა.
22	802.3ad ინტერფეისის გაერთიანების მხარდაჭერა (LACP მხარდაჭერა).
23	დიდი პაკეტების (Jumbo frame) გადაცემის მხარდაჭერა.
24	SNMPv3 მხარდაჭერა.
25	Netflow მხარდაჭერა. Netflow პროფილი უნდა განისაზღვროს ფიზიკური პორტების საფუძველზე.
26	LLDP (Link Layer Discovery Protocol) მხარდაჭერა. მოწყობილობას უნდა ჰქონდეს ინფორმაცია სხვა მოწყობილობების შესახებ (MAC მისამართი, სისტემის სახელი, მასთან დაკავშირებული პორტი).
27	Policy Based Forwarding მხარდაჭერა IPv4 და IPv6 პროტოკოლებისთვის.
28	BFD (Bidirectional Forward Detection) მხარდაჭერა
29	არანაკლებ 10 ვირტუალური ბრანდმაუერის მხარდაჭერა მომავალში ლიცენზიის უზრუნველყოფით.
30	site-to-site და client-to-site IPSec VPN მხარდაჭერა.
31	მაქსიმალური შესაძლო Client SSL VPN რაოდენობა - არანაკლებ 1000.
32	მაღალ მდგრადობის კლასტერის შექმნის მხარდაჭერა (HA) - Active/Passive და Active/Active
33	HA კლასტერირების რეჟიმში უნდა იყოს მხარდაჭერილი ბრანდმაუერების ჰორიზონტალური მასშტაბირება, არანაკლებ 6 ბრანდმაუერის გაერთიანება ერთ კლასტერში;
34	HA კლასტერირების რეჟიმს უნდა გააჩნდეს რამდენიმე მოშორებული დატაცენტრებს შორის მუშაობა;
35	კლასტერის კომპონენტებს შორის გადასასვლელად უნდა განხორციელდეს ინტერფეისების მონიტორინგი (interface monitoring) და მითითებული რესურსებისკენ მიმავალი გზები (path monitoring);
36	მოწყობილობა უნდა აკონტროლებდეს სესიების სტატუსს (Stateful inspection) პაკეტების ფილტრაციით და აპლიკაციების იდენტიფიკაციით.

37	მოწყობილობა უნდა იყოს Zone- ებზე (Zone-based) დაფუძნებული. ერთი ან მეტი ინტერფეისი ან ქვე ინტერფეისი შეიძლება მიეკუთვნებოდეს ერთ ზონას. წვდომის (firewall rules) და NAT-ის პოლიტიკები უნდა ებმებოდეს ზონებს;
38	NAT პოლიტიკას უნდა ჰქონდეს საკუთარი წესები, დამოუკიდებელი უნდა იყოს წვდომის პოლიტიკებისაგან (firewall rules);
39	ქსელის ბრენდმაუერზე გატარებული ტრაფიკის OSI მოდელის მეშვიდე დონეზე ქსელის აპლიკაციების ამოცნობა და დაბლოკვა, მათ შორის ინდივიდუალურად ყველა პროგრამისთვის, რომლებიც იყენებენ საერთო პორტებს, (80 და 443), რომლებიც იყენებენ დინამიურ TCP / UDP პორტებს;
40	აპლიკაციების მართვამ უნდა აჩვენოს აპლიკაციის დამოკიდებულება, რომ შეძლოს თეთრი სიების შექმნა.
41	Layer-7 OSI მოდელზე ტრაფიკის აღმოჩენა და ინსპექტირება სიგნატურებით, პროგრამული უზრუნველყოფით, პროტოკოლებითა და სერვისებით: - აუთენტიფიკაციის სერვისები, მათ შორის Microsoft Active Directory, LDAP, RADIUS, TACACS +, Kerberos, SAML, Syslog Monitoring / Parser (Syslog– დან შეტყობინებების დამუშავებისას მოწყობილობამ უნდა უზრუნველყოს user-to-ip რუკების შედგენა); - მონაცემთა ბაზები, მათ შორის Microsoft SQL, Oracle და ა.შ; - ფაილური სერვისები, მათ შორის Microsoft SMB; - ელექტრონული დოკუმენტების მართვისა და გაგზავნის სისტემები, მათ შორის Microsoft Sharepoint, Exchange, Office 365, Google Docs; - ელ.ფოსტის პროტოკოლები: SMTP, POP3, IMAP; - VOIP პროტოკოლები და აუდიო – ვიდეო კონფერენციები, მათ შორის SIP, H.323, H.245, H.225, Webex; - პროგრამული უზრუნველყოფის განახლების სერვისები, მათ შორის Microsoft Update, ანტივირუსული პროგრამა, Adobe, Java; - სარეზერვო სერვისები; - ვირტუალიზაციისა და ტერმინალზე წვდომის სერვისები, მათ შორის VMware, Microsoft RDP; - დისტანციური წვდომის პროტოკოლები, მათ შორის Telnet, SSH, VNC, Radmin; - ქსელის პროტოკოლები, მათ შორის დინამიური მარშრუტიზაციისა და SSL პროტოკოლები, IPSec VPN; - ელექტრონული ფოსტა; - სოციალური ქსელები; - მყისიერი შეტყობინების საშუალებები; - აუდიო – ვიდეო კონფერენციების საშუალებები; - აუდიო-ვიდეოს ნაკადები (ვებსაიტის მიუხედავად), აუდიოსა და ვიდეოს ნაკადი HTTP– ით; - დისტანციური წვდომის საშუალებები, Team-Viewer- ის ჩათვლით;

	- გარე Proxy სერვერები და ანონიმაიზერები, მათ შორის Tor, Ultrasurf, Freegate, SOCKS, PHP Proxy; - ინსტრუმენტები VPN და ტუნელების შესაქმნელად სხვა პროგრამებზე, მათ შორის Freenet, Open-vpn, Vtun, Rdp-to-Tcp, Tcp-over-Dns;
42	გადაწყვეტილებას უნდა ჰქონდეს SafeSearch– ის მხარდაჭერა YouTube– სა და CIPA– ს შესაბამისი Google ძიებისთვის (გადაწყვეტილება არ უნდა მუშაობდეს პროქსი რეჟიმში).
43	ჩაშენებული ხელსაწყოები, საკუთარი სიგნატურების შესაქმენელად, ე.წ Regex ზე დაფუძნებით და HTTP (S), FTP, SMB, SMTP, RPC დეკოდერების გამოყენებით. აგრეთვე ნიღაბი TCP / UDP- პაკეტების შიგთავსისთვის;
44	შესაძლებელი უნდა იყოს ჰოსტის უსაფრთხოების დონეზე დაფუძნებული უსაფრთხოების პოლიტიკების შექმნა;
45	აპლიკაციების აღმოჩენა დაშიფრულ ტრაფიკში, მათ შორის SSL (RSA გასაღებების მხარდაჭერა 2048 ბიტამდე) და SSHv2 ტრაფიკში. ბრანდმაუერში, შემომავალი ან/და გამავალი ტრაფიკის დეშიფრაციის მხარდაჭერა, მოხმარებლებისთვის ტრანსპერენტულად, ინდივიდუალური მიკრო აპლიკაციების კონტროლის შესაძლებლობით, მათ შორის სოციალურ ქსელებში შეტყობინებების გაგზავნის, ფაილების მიმოცვლა, აუდიო და ვიდეოს კონტროლი.
46	ერთ სესიის ფარგლებში სხვადასხვა ტიპის აპლიკაციეს აღმოჩენის შესაძლებლობა;
47	წვდომის კონტროლის პოლიტიკებს, უნდა გააჩნდეს დროის, დღის, თარიღისა და პერიოდის გათვალისწინებით მუშაობა.
48	მომხმარებელთა ამოცნობა, რომლებიც იყენებენ ქსელურ აპლიკაციებს, კორპორატიული აუტენტიფიკაციის სერვისებთან ინტეგრაციის ხარჯზე, ინტეგრაცია: Microsoft Active Directory, Microsoft Exchange, LDAP, Novell eDirectory სთან;
49	მომხმარებელთა ჯგუფებისა და ინდივიდუალური მომხმარებლების საფუძველზე პოლიტიკების შექმნის შესაძლებლობა. სისტემამ უნდა შეინახოს მომხმარებლის ინფორმაცია შესაბამის ჟურნალებში.
50	ინტეგრაცია Microsoft Active Directory– ში უნდა განხორციელდეს Active Directory– ში ცვლილებების გარეშე და არ უნდა იქნას გამოყენებული Active Directory დომენის ადმინისტრატორის ანგარიში;
51	Microsoft Active Directory ინტეგრაცია არ უნდა საჭიროებდეს დამატებით კომპონენტებს, შუამავალ აგენტებსა თუ დამატებითი პროგრამული უზრუნველყოფის ინტალაციას;
52	ავტორიზაციის სერვისებთან (მაგ., უკაბელო ქსელის კონტროლერებთან) ინტეგრირების შესაძლებლობა ღია XML API– ს საშუალებით;
53	User-IP რუკების შექმნის შესაძლებლობა (user-IP mapping) სისტემის მიერ გაგზავნილი syslog შეტყობინებების ანალიზის საშუალებით, რომლებიც ავტორიზაციას უკეთებენ მომხმარებლებს.

54	უსაფრთხოების პოლიტიკებში, მომხმარებლის დინამიური ჯგუფების შექმნისა და გამოყენების შესაძლებლობა. დინამიური მომხმარებლის ჯგუფების საშუალებით შესაძლებელი უნდა იყოს "მყისიერად" მომხმარებლის ჯგუფში დამატება ან ამოშლა, შესაბამისი დირექტორიის ჯგუფებში (მაგალითად, Active Directory) შეცვლის გარეშე და წესების დაყენების გარეშე. ეს საშუალებას უნდა იძლეოდეს ავტორიზებულ ადმინისტრატორებს ან გარე სისტემებს ამოიღონ მომხმარებელი დინამიური მომხმარებლის ჯგუფიდან, მაგალითად, თუ შესაბამისი მომხმარებელი კომპრომეტირებულია;
55	უსაფრთხოების ერთიან უნიფიცირებული პოლიტიკების შექმნა, გამომგზავნის, მიმღების, გამოყენებული სერვისების (TCP/UDP- პორტები), მომხმარებლის სახელების, მომხმარებლის ჯგუფების და პროგრამების ან პროგრამების კატეგორიების მითითების საშუალებით;
56	პოლიტიკას უნდა შეეძლოს შემდეგი ქმედებების განხორციელება: - ნებართვა ან აკრძალვა; - მიეცეს უფლება კონკრეტულ პროგრამას ან პროგრამის კატეგორიას გამოიყენოს მხოლოდ სტანდარტული ან მკაცრად განსაზღვრული TCP / UDP პორტები. ამასთან, ეს პორტები არ უნდა იქნას გამოყენებული სხვა პროგრამების მიერ ისეთი პოლიტიკის გარეშე, რომელიც აშკარად იძლევა ამგვარი ურთიერთქმედების საშუალებას; - ნებართვები ან უარი დროის გრაფიკის მიხედვით, მომხმარებლების ან მომხმარებლის ჯგუფის საფუძველზე; - DSCP ტეგირებისა და ტრაფიკის შეზღუდვები QOS წესების გამოყენებით, რომლებიც დაფუძნებულია აპლიკაციებზე, IP მისამართებზე, DSCP, მომხმარებლებსა და მომხმარებელთა ჯგუფებზე. - QOS– ის განხორციელება რეალურ დროში აპლიკაციების დონეზე, მხარდაჭერილი უნდა იყოს სხვადასხვა ტიპის აპლიკაციები, მათ შორის ცოლიალური ქსელები, აუდიო, ვიდეო, მესინჯერები, ფაილების მიმოცვლა; - შესაძლებელი უნდა იყოს QOS ის რემარკირების განხორციელება, source/destination IP, პორტისა და აპლიკაციის დონეზე; - ტრაფიკის მარშრუტიზაცია პოლიტიკების მიხედვით (Policy Based Forwarding) IP მისამართის (source ან/და destination), მომხმარებლის, აპლიკაციის ან URL- ის საფუძველზე; - აპლიკაციებში გარკვეული ფუნქციონირების კონტროლის შესაძლებლობა; - ზემოთქმულის ნებისმიერი კომბინაციის გამოყენების შესაძლებლობა; - ინდივიდუალური მომხმარებლებისთვის სიის / შავი სიის პოლიტიკის შექმნის შესაძლებლობა.
57	სხვადასხვა პროტოკოლების ტრაფიკის ინსპექტირების შესაძლებლობა: - Generic Routing Encapsulation; - არა დაშიფრული IPSec ტრაფიკი (NULL Encryption Algorithm for Ipsec and transport mode AH Ipsec).

58	გადაწყვეტილებას უნდა გააჩნდეს უსაფრთხოების პოლიტიკების ოპტიმიზაციის ფუნქციონალი, რომელიც დაფუძნებულია გამოყენებულ აპლიკაციებზე. მათ შორის პოლიტიკების აღმოჩენა და წაშლა რომლებიც არ გამოიყენებიან;
59	მკაცრი უსაფრთხოების პოლიტიკების შესაქმნელად, მოწყობილობის ინტერფეისში ხელმისაწვდომი უნდა იყოს შემდეგი ფუნქციონალი: - განახორციოლოს იმ უსაფრთხოების პოლიტიკების იდენტიფიცირება, რომლებშიც არაა განსაზღვრული აპლიკაციები. მოახდინოს იმ აპლიკაციების იდენტიფიცირება, რომლებიც იყენებენ აღნიშნულ უსაფრთხოების პოლიტიკას და უზრუნველყოს აპლიკაციების მითითება/აქტივაცია აღნუშნულ პოლიტიკაში, წინასწარ აპლიკაციების სიის მოწოდებით რომელშიც მოხდება საჭირო აპლიკაციების არჩევა; - განახორციელოს იმ უსაფრთხოების პოლიტიკების იდენტიფიცირება, რომლებშიც მითითებული აპლიკაცია არ გამოიყენება. გამოუყენებელი აპლიკაციების შესახებ ინფრომაციის ასახვა, ბოლო 7, 15 და 30 დღის განმავლობაში; - განახორციელოს უსაფრთხოების პოლიტიკაში მოხვედრილი აპლიკაციის გამოყენების პირველი და ბოლო თარიღი და აპლიკაციის ტრაფიკის მიერ დაკავებული ქსელური გამტარუნარიანობა; - განახორციელოს უსაფრთხოების პოლიტიკების იდენტიფიცირება რომლებიც არ იყო გამოყენებული ბოლოს 30 და 90 დღის განმავლობაში;
60	უსაფრთხოების პოლიტიკებში შესაძლებელი უნდა იყოს გეოგრაფიული რეგიონების განსაზღვრა;
61	გამტარუნარიანობის შეზღუდვა შესაძლებელი უნდა იყოს მომხმარებლის სახელის/ჯგუფის, საწყისი/მიმღები IP მისამართისა და აპლიკაციის საფუძველზე.
62	გარკვეული წყაროებიდან ტრაფიკის ავტომატურად დაბლოკვის შესაძლებლობა ქსელის ბრანდმაუერის დონეზე, სანამ ეს პაკეტები გამოიყენებენ ბრანდმაუერის მთავარი პროცესორის ან პაკეტის ბუფერის რესურსებს.
63	გადაწყვეტილებას უნდა გააჩნდეს სპეციალური სერვისის მხარდაჭერა, რომელშიც განხორციელდება ახალი პოტენციურად მავნე ფაილების გაშვება Microsoft Windows ის გარემოში, მათ შორის (EXE, DLL, SCR, BAT და ა.შ.) ფაილების, ქსელში გადაცემული ფაილების, SMTP/POP3 ელ.ფოსტის შეტყობინებებში მათ შორის SSL დაშიფრული შეტყობინებებში, საეჭვო ფაილების ქცევის ანალიზი, ბმულების ანალიზი, როგორც კერძო "Sanbox" -ში ასევე ღრუბლოვან "Sanbox" -ში. ახალი მავნე ფაილების აღმოჩენა და ავტომატური სიგნატურების გენერაცია არანაკლებ 24 საათში, ხოლო URL რეპუტაციული ბაზების განახლება არანაკლებ 30 წუთში.
64	ვიზუალიზაციის მოწინავე ფუნქციონალის არსებობა: ვიზუალიზაცია მარტივი და მოსახერხებელი ფორმატით, ქსელური პროგრამების აქტივობა, ქსელური შეტევების აღმოჩენა და ბლოკირება. ინფორმაციის ფილტრაციის შესაძლებლობა, სხვადასვა საკვანძო პარამეტრების გამოყენებით, მათ შორის (პროგრამების,

	საფრთხეების, მომხმარებლების, IP მისამართების, TCP/UDP პორტების, უსაფრთხოების ზონების, საფრთხეების ტიპები და ა.შ.);
65	რეპორტების შექმნის შესაძლებლობა. ბრანდმაუერს უნდა ჰქონდეს რეპორტების ავტომატური წარმოების ფუნქციონალი და მათ შორის განრიგის მიხედვით, ხელით განსაზღვრულ სხვადასხვა თემატურ ფუნქციებზე. რეპორტების ნახვა შესაძლებელი უნდა იყოს, როგორც უშუალოდ ვებ გრაფიკული ინტერფეისით (GUI), აგრეთვე PDF და CSV ფორმატებში ექსპორტის შესაძლებლობით;
66	უნდა შეეძლოს ინტეგრირება იგივე მწარმოებლის ცენტრალიზებული მართვისა და მონიტორინგის სისტემასთან, ლოგირების, პროგრამული უზრუნველყოფის განახლების და რამოდენიმე ბრანდმაუერის მართვის შეასძლებლობით;
67	უნდა შეეძლოს ბრანდმაუერზე ლოკალურად გამოყოფილ დისკებზე ლოგიბის ბუფერიზაცია, იმ შემთხვევაში თუ დაიკარგება წვდომა ცენტრალიზირებული მართვისა და მონიტორინგის სისტემასთან;
68	უნდა შეეძლოს მესამე მხარის SIEM- სისტემებთან ინტეგრირებას Syslog- ის საშუალებით, ლოგის ფორმატის მოქნილი კონფიგურაციის შესაძლებლობით;
69	უნდა შეეძლოს ლოკალური ადმინისტრატორების კონტროლი, როლებზე დაფუძნებით: - შესაძლებელი უნდა იყოს მართვის და კონფიგურაციის ნახვის არიალის შეზღუდვა, როგორც მთლიან მოწყობილობაზე ასევე ცალკეულ კონტექსტზე; - შესაძლებელი უნდა იყოს, კონფიგურაციის ცვლილების, ნახვის ან ნახვის სრული შეზღუდვა ბრანდმაუერის ვებ ინტერფეისის ნებისმიერ ჩანართზე; - შესაძლებელი უნდა იყოს, კონფიგურაციის ცვლილების, ნახვის ან ნახვის სრული შეზღუდვა ბრანდმაუერის CLI ინტერფეისზე;
70	გადაწყვეტილებს უნდა გააჩნდეს ერთიანი მართვის ინტერფეისი, უსაფრთხოების პოლიტიკების სამართავად, მოწყობილობის ქსელური პარამეტრების სამართავად, უსაფრთხოების პროფილების სამართავად, როგორც ლოკალურად ასევე ცალკე მდგომი მართვის და მონიტორინგის სადგურის საშუალებით. ბრანდმაუერის ლოკალური მართვის შემთხვევაში მას უნდა შეეძლოს ლოგირების განხორციელება ლოკალურად;
71	გადაწყვეტილების მართვა შესაძლებელი უნდა იყოს HTTPS და SSH პროტოკოლებზე დაფუძნებით, დამატებითი პროგრამული უზრუნველყოფის ინსტალაციის გარეშე ადმინისტრატორის კომპიუტერზე;
72	ბრანდმაუერის მართვის ლოკალური ინტერფეისი (ვებ და CLI) უნდა იყოს უნიფიცირებული ცენტრალური მართვისა და მონიტორინგის სისტემასთან, რომლიდანაც შეასძლებელია განხორციელდეს ცენტრალიზირებული ლოგირება, რეპორტინგი და პროგრამული უზრუნველყოფის განახლება;
73	Cisco TrustSec SGT ტეგების მხარდაჭერა;
74	გადაწყვეტილებას უნდა გააჩნდეს დინამიური მისამართების ჯგუფებისა (Dynamic Address Group) და დინამიური მომხმარებლების ჯგუფების (Dynamic User Group) მხარდაჭერა. რაც უზრუნველყოფს XML API საშუალებით აღნიშნული

	ჯგუფების განახლებას უსაფრთხოების პოლიტიკებში. აღშნული წცლილებების უნდა ისახებოდეს მყისიერად და არ საჭიროებდეს უსაფრტხოების პოლიტიკების ხელახალ აქტივაციას;
75	გადაწყვეტილებას უნდა გააჩნდეს თანამედროვე პროგრამულ-აპარატურული არქიტექტურა, რომელიც დაფუძნებულია, როგორც სტატიკურ ASIC ზე, ასევე პროგრამირებად FPGA ჩიპებზე. აღნიშნული ჩიპები უნდა ასრულებდენ ცალკეულ ამოცანებს, მათ შორის დაშიფრული ტრაფიკის, მარშრუტიზაციის პროტოკოლების, ARP პაკეტების დამუშავება და სხვა. ბრანდმაუერზე დიდი დატვირთვის დროს ცალკეული აპარატურული ჩიპები უნდა ასრულებდენ კრიტიკულ ამოცანებს ტრაფიკის დამუშავებისგან დამოუკიდებლად;
76	გადაწყვეტილებას უნდა გააჩნდეს შემდეგი NGFW ფუნქციონალი: - მოწყობილობებს უნდა ჰქონდეთ არქიტექტურული შემოწმების შესაძლებლობა, მათ შორის IP პაკეტის ფილტრაციის, აპლიკაციების აღმოჩენის ფუნქციები და ასევე შემდეგი უსაფრთხოების სერვისები: - ახალი თაობის ბრანდმაუერი (NGFW) - IPSEC VPN, SSL VPN - აპლიკაციების კონტროლი(Application Control) - ანტივირუსი(Antivirus/Antimalware) - შეჭრის პრევენცია (IPS) - Antispyware / antibot - უცნობი მავნე ფაილების გამოვლენა და ”ნულოვანი” დღის შეტევების და მოწინავე მუდმივი საფრთხეების პრევენცია (APT) - შეტევების დაბლოკვა DNS პროტოკოლის გამოყენებით (DNS Security) - URL გაფილტვრა(URL filtering) - IoT მოწყობილობების იდენტიფიკაცია და ანალიზი(IoT Security) - დირექტორიების სერვისებთან ინტეგრაცია მომხმარებლების იდენტიფიცირებისთვის (Identity Awareness)
77	გადაცემული ტრაფიკის რეალურ დროში შემოწმების შესაძლებლობა, მათ შორის: სიგნატურული ანალიზი, ქცევის ანალიზი, დაცვა მოწყვლადობებისგან, დაცვა ქსელური შეტევებისგან, მავნე ფაილებისგან დაცვა, ფაილების ტიპების აღმოჩენა, ვირუსების აღმოჩენა სხვადასხვა ტიპის პროტოკოლებში მათ შორის ელექტრონულ ფოსტაში, FTP და SMB პროტოკოლებში, ჯაშუშური პროგრამების აღმოჩენა, ქსელური “worms” ბლოკირება, ქსელურ და აპლიკაციების ტრაფიკში შიგთავსის აღმოჩენა regex საშუალებით, როგორც SSL ასევე SSHv2 დაშიფრულ ტრაფიკში;
78	ანტივირუსული დაცვა, ჯაშუშური პროგრამებისგან დაცვა, მოწყვლადობებისგან და ქსელის შეტევებისგან დაცვა(IPS სისტემა), URL- ფილტრაცია დინამიური რეპუტაციის ბაზის გამოყენებით, რომელიც გააჩნია ერთი და იგივე საიტის ფარგლებში კატეგორიციის მხარდაჭერა, მათ შორის კატეგორიზაცია ერთი და იგივე საიტის სხვადასხვა ენაზე, ფაილების გადაცემის ბლოკირება ტიპებით;

79	დამატებითი სკანირების ფუნქციების გამოყენების შესაძლებლობა Microsoft და Android გარემოში, ახალი პოტენციურად მავნე ფაილების სკანირებისთვის, მათ შორის, ფაილების (EXE, DLL, SCR, BAT და ა.შ.), PDF დოკუმენტების (Adobe Reader– ის სხვადასხვა ვერსიის შემოწმება), MS Office 2003, 2007 და ზემოთ, Java და Flash, Android APK, ბმულები http: // და https: // ახალი მავნე პროგრამების და ანტივირუსული სიგნატურების ავტომატური შექმნის შესაძლებლობა აღმოჩენას რეალურ დროში;
80	სხვადასხვა ტიპის ლოგების ავტომატური კორელაცია, ქსელური ბრანდმაუერის, IPS, ფაილის გადაცემის კონტროლი, URL ფილტრაცია), რომლებიც გენერირებული იქნა ერთი სესიის ფარგლებში;
81	გადაწყვეტილებას უნდა ჰქონდეს შემდეგი IPS სისტემის ფუნქციები: - სხვადასხვა მომხმარებლებისთვის ან მომხმარებელთა ჯგუფებისთვის სხვადასხვა IPS პოლიტიკის შექმნის შესაძლებლობა. - მოწყობილობაზე IPS ხელმოწერების ძებნის შესაძლებლობა CVE, კრიტიკულობის დონის და ჰოსტის ტიპის (კლიენტი / სერვერი) გამოყენებით. - IPS სისტემის სიგნატურების ინდივიდუალურად კონფიგურაციის შესაძლებლობა შეტევებზე რეაგირებისთვის შემდეგნაირად: Allow, Alert, Deny, reset-both, reset-client, reset-server, Block-IP. IP– ზე დაფუძნებული დაბლოკვა უნდა განხორციელდეს როგორც source IP– ს, ასევე source და destination IP– ების საფუძველზე. - IPS სიგნატურები, რომლებიც გამოიყენება შეტევების საწინააღმდეგოდ, უნდა განახლდეს ფაილიდან ან ინტერნეტით. გარდა ამისა, საჭიროების შემთხვევაში, სიგნატურების განახლებები ავტომატურად უნდა განხორციელდეს მომხმარებლის ჩარევის გარეშე. - IPS სისტემა უნდა შეიცავდეს პროტოკოლის ანომალიის გამოვლენის ტექნოლოგიას(Protocol Anomaly Detection), რომელიც ბლოკავს შეტევებს არსებულ სიგნატურებზე დაყრდნობის გარეშე; - IPS უნდა შეეძლოს გაუმკლავდეს შემდეგ შეტევებს: - Brute Force - Code/Command execution - Sql-injection - Exploit-kit - Denial of Service - Info-leak - Overflow - Scan
82	გადაწყვეტილებას უნდა გააჩნდეს შემდეგი DNS უსაფრთხოების ფუნქციონალი: - საეჭვო DNS- მოთხოვნების ანალიზი და ინფიცირებული სადგურების ლოკალიზაცია DNS sinkhole ტექნოლოგიის გამოყენებით (DNS- სერვერის პასუხების ჩანაცვლება);

	- ცნობილი მავნე დომენების სახელების დაბლიკვა რეპუტაციის მონაცემთა ბაზების გამოყენებით; - ფუნქციურმა უნდა გამოიყენოს ღრუბელზე დაფუძნებული მანქანური სწავლების ალგორითმები პოტენციურად მავნე დომენის სახელების დასადგენად; - DNS ტუნელების გამოვლენა და დაბლოკვა (DNS tunneling) მანქანური სწავლების გამოყენებით, რომელიც აანალიზებს DNS მოთხოვნების ხარისხს და ქცევას (მოთხოვნების სიხშირე, ენტროპია და ა.შ.). - DGA (domain generation algorithm) ანალიზი და გამოვლენა, რაც გულისხმობs დომენური სახელების ანალიზს იმის განსასაზღვრელად იყო თუ არა დომენი გენერირებული პროგრამის/მანქანის ან ადამიანის მიერ, უკუინჟინერიაზე დაფუძნებით და სხვა ხშირად გამოყენებული მეთოდების ანალიზით. თუ დადგინდა, რომ დომენი შექმნილია DGA ალგორითმით, მისი დაბლოკვის შესაძლებლობა; - NXNSAttack და DNS Rebinding შეტევების მოგერიება; - Malware, ახალი რეგისტრირებული, Phishing, Grayware , Parked, Proxy Avoidance და Anonymizers ტიპის დომენების აღმოჩენა და ბლოკირება;
83	გადაწყვეტილებას უნდა ჰქონდეს Anti-Spyware / Anti-bot აღმოჩენის და ბლოკირების ფუნქციონალი, შემდეგი შესაძლებლობებით: - აღნიშნული ფუნქციონალი უნდა მუშაობდეს პორტისა და პროტოკოლისგან დამოუკიდებლად და ამოწმებდეს მთელ IP ტრაფიკს. - კონტროლ ცენტრების IP მისამართების განსაზღვრის (resolution requests) მოთხოვნების აღმოჩენა და მათი ბლოკირება DNS მოთხოვნების დონეზე; - DNS Sinkhole ფუნქციონალი, მავნე დომენური სახელის მოთხოვნის შემთხვევაში უნდა გასცეს ადმინისტრატორის მიერ მინიჭებული IP მისამართი, რათა აღმოჩენილი იქნენ ინფიცირებული სისტემები; - სიგნატურების გამოყენებით ცნობილი ბოტნეტების დაბლოკვის ფუნქციონალი. სისტემამ უნდა უზრუნველყოს ადმინისტრატორს botnet სიგნატურების კონფიგურაციის შესაძლებლობა; - სიგნატურებზე შემდეგი ქმედებების განხორციელების შესაძლებლობა: Allow, Alert, Deny, reset-both, reset-client, reset-server, Block-ip. - სხვადასხვა Anti-spyware პოლიტიკები უნდა შეიქმნას სხვადასხვა მომხმარებლებისა და მომხმარებლების ჯგუფებისთვის.
84	Anti-spyware ფუნქციონალი უნდა შეიცავდეს შემდეგი შეტევების იდენტიფიცირებას და დაბლოკვას: - Adware; Botnets; Backdoor; Browser-Hijacker; Data-theft; Keylogger; spyware; net-worm; p2p-communication;
85	მოწყობილობას უნდა ჰქონდეს Anti-Virus ფუნქციონალი, შემდეგი შესაძლებლობებით: - სიგნატურებზე დაფუძნებული ცნობილი მავნე პროგრამების დაბლოკვა.

	- უნდა ჰქონდეს სკანირების შესაძლებლობა ნაკადში. არქივების სკანირების შესაძლებლობა; - Anti-Virus უნდა შეეძლოს ინტეგრაციის განხორციელება Active Directory სთან, რათა Anti-Virus პოლიტიკების განსაზღვრა განხორციელდეს Active Directory- ში მომხმარებლის ან მომხმარებელთა ჯგუფის საფუძველზე. - Anti-Virus სიგნატურების გამორიცხვის შესაძლებლობა; - შესაძლებელი უნდა იყოს განსხვავებული ანტივირუსული პოლიტიკების შეიქმნას სხვადასხვა მომხმარებლებისა და მომხმარებლების ჯგუფებისთვის. - ანტივირუსმა უნდა დაბლოკოს მავნე ფაილები, რომლებიც გადაეცემა FTP, HTTP, SMB, POP3 გზით.
86	მოწყობილობას უნდა ჰქონდეს URL ფილტრაციის მხარდაჭერა შემდეგი ფუნქციონალით: - URL ფილტრაციის ფუნქციონალი უნდა მუშაობდეს Active Directory სთან ინტეგრაციაში, რის ფარგლებშიც შესაძლებელი უნდა იყოს პოლიტიკების აღწერა მომხმარებლებისა და ჯგუფების მიხედვით Active Directory დან; - შესაძლებელი უნდა იყოს ბლოკირების პორტალის ცვლილება, რომელიც ისახება URL ბლოკირების დროს; - C&C (Command and Control) სიების დინამიური განახლება; - URL ფილტრაციის უნდა ჰქონდეს XFF (X-forwarded-for) მხარდაჭერა; - URL კატეგორიაზე შესაძლებელი უნდა იყოს ქსელური ტრაფიკის სიჩქარის შეზღუდვა; - URL- ების კლასიფიკაცია შესაძლებელი უნდა იყოს რისკის მიხედვით, მაღალი რისკი (URL ის მავნე აქტივობა, ბოლო 30 დღის განმავლობაში), საშუალო რისკი (URL ის მავნე აქტივობა, ბოლო 60 დღის განმავლობაში), - ბოლო 30 დღის განმავლობაში რეგისტრირებული URL ების კლასიფიკაცია (ახალი რეგისტრირებული დომენები). - დეტალური ლოგირების წარმოება და გარე syslog მიწოდება, თუ რომელ URL ხორციელდებოდა წვდომა; - URL ფილტრაციის ფუნქციონალს უნდა შეეძლოს მანქანური სწავლების (ML) გამოყენება ვებ გვერდებზე, რათა აღკვეთოს მავნე Javascript ექსპლოიტებისა და ფიშინგის მოხვედრა სისტემაზე. მანქანური სწავლების (ML) ფუნქციონალს, უნდა შეეძლოს, მანქანური სწავლების მოდელებზე დაფუძნებით, რეალურ დროში დინამიური ანალიზი და მავნე შიგთავსის გამოვლენა, ვებ გვერდის სხვადასხვა დეტალების შეფასებით;
87	შემოთავაზებულ გადაწყვეტილებას უნდა ჰქონდეს ნულოვანი დღის შეტევებისგან დასაცავი ფუნქციონალი, ქსელურ ტრაფიკში გადაცემული ფაილების სკანირების საშუალებით: - გადაწყვეტილებას უნდა გააჩნდეს დამატებითი ლოკალური ან ღრუბლოვანი ე.წ sandbox მხარდაჭერა, ფაილების გასაანალიზებლად;

	- გადაწყვეტილებას უნდა შეეძლოს საეჭვო ფაილების გაგზავნა (ფაილის შემდეგი ფორმატები უნდა იყოს მხარდაჭერილი: 7-ZIP, RAR, ZIP, Adobe Flash, APK, JAR, PDF, MS-Office DOC, DOCX, RTF, XLS, XLSX, PPT, PPTX, .exe, .dll, აგრეთვე ბმულები ფოსტაში, Linux ის ELF ფაილის ფორმატი, Mac OS X ფაილების ფორმატები Mach-O, DMG და PKG) ლოკალურ ან ღრუბლოვან ე.წ sandbox ში. - გადაწყვეტილებას უნდა შეეძლოს რეალურ დროში მიიღოს შესაბამისი განახლებები, რომ უზრუნველყოს მავნე ფაილებისგან დაცვა ლოკალურ ან ღრუბლოვანი ე.წ sandbox ში; - გადაწყვეტილებას უნდა შეეძლოს რეალურ დროში ამოიცნოს და დაბლოკოს უცნობი მავნე პორტატული ე.ს „შემსრულებელი“ ტიპის ფაილები და PowerShell სკრიპტები, მანქანური სწავლების (ML) ალგორითმების გამოყენებით, ფაილის დეტალების შეფასების საშუალებით, მათ შორის ველების და დეკოდერების შაბლონების ჩათვლით. ამ დონის დაცვამ უნდა უზრუნველყოს დაცვა იმ მავნე ფაილებისგან რომლებისთვისაც არ არსებობს სიგნატურები; - გადაწყვეტილებს უნდა შეეძლოს მომხმარებლის იდენტიფიცირება, რომელიც ტვირთავს მავნე ფაილს;
88	გადაწყვეტილებას უნდა გააჩნდეს ფიშინგ და ლეგიტიმირებულ საიტებზე, კორპორატიული სახელისა და პაროლის გამოყენების აღკვეთა;
89	გადაწყვეტილებას უნდა გააჩნდეს ფიშინგ ტიპის შეტევებისგან დაცვის მექანიზმები, მომხმარებლის იდენტობის კონტროლის საშუალებით. გადაწყვეტილებას უნდა შეეძლოს HTTP/HTTPS POST ის დონეზე აღკვეთოს მოპარული, მომხმარებლის კორპორატიული სახელისა და პაროლის გადაცემა. მომხმარებლის კორპორატიული სახელისა და პაროლის კონტროლისთვის გადაწყვეტილებას უნდა შეეძლოს ინტეგრაცია Active Directory სთან. გადაწყვეტილება უნდა იყოს აღჭურვილი შესაბამისი ლიცენზიით;
90	გადაწყვეტილებას უნდა გააჩნდეს მონაცემთა ფილტრაციის მხარდაჭერა, სპეციალური პოლიტიკების საშუალებით. ფაილების ტიპების იდენტიფიკაცია შესაძლებელი უნდა იყოს ე.წ regex ის საშუალებით. გადაწყვეტილება უნდა იყოს აღჭურვილი შესაბამისი ლიცენზიით;
91	გადაწყვეტილებას უნდა გააჩნდეს ღრუბლოვანი ინტერნეტი საგნების (IoT Security) დაცვის მექანიზმები: - NGFW გადაწყვეტილებას უნდა შეეძლოს მეტა ინფორმაციის შეგროვება ქსელურ ტრაფიკში, დეტალური ანალიზისთვის; - გადაწყვეტილებას უნდა შეეძლოს IoT მოწყობილობების ამოცნობა და იდენტიფიცირება მანქანურ სწავლბასა და ხელოვნურ ინტელექტზე დაფუძნებით; - გადაწყვეტილებას უნდა შეეძლოს ბაზური ქცევის შაბლონის განსაზღვრა, რათა მომავალში გამოავლინოს ანომალიური აქტივობა, რაც შეიძლება ნიშნავდეს ქსელური შეტევას და დარღვევას. აღნიშნულის შესახებ გადაწყვეტილებას უნდა შეეძლოს ადმინისტრატორის შეტყობინება.

	- გადაწყვეტილებას უნდა შეეძლოს უსაფრთხოების პოლიტიკების რეკომენდაციების ავტომატური გენერაცია, რომლებიც უზრუნველყოფენ IoT მოწყობილობის, ლეგიტიმირებულ მუშაობას და არალეგიტიმირებული მუშაობის აღკვეთას. შესაძლებელი უნდა იყოს აღნიშნული რეკომენდაციების იმპორტირება ბრანდმაუერის პოლიტიკებში; - გადაწყვეტილებას უნდა შეეძლოს, უსაფრთხოების პოლიტიკების განსაზღვრა IoT მოწყობილობის იდენტიფიკატორზე დაფუძნებით, მათ შორის მოწყობილობის იმპორტირებული ატრიბუტები, პროფილი, კატეგორია, მწარმოებელი და მოდელი; - გადაწყვეტილებას უნდა შეეძლოს IoT უსაფრთხოების სერვისიდან რეგულარული განახლება, რათა დადგინდეს IoT მოწყობილობის IP მისამართი და მოწყობილობის პროფილი, უსაფრთხოების პოლიტიკებში გამოსაყენებლად. გადაწყვეტილებას უნდა შეეძლოს მაღალი სიზუსტით არანაკლებ 90%, IP მისამართის შესაბამისობის დადგენა, მოწყობილობებისათვის რომლებიც იყო ქსელში აქტიური ბოლო 1 საათი;
92	გადაწყვეტილებას უნდა შეძლოს SSL/TLS და SSH გაშიფვრა, მათ შორის TLS 1.0, TLS 1.1, TLS 1.2 და TLS 1.3 პროტოკოლების;
93	გადაწყვეტილებას უნდა შეეძლოს HTTPS ტრაფიკზე, სხვადასხვა უსაფრთხოების სერვისების განხორციელება, მათ შორის: IPS, აპლიკაციების კონტროლი, URL ფილტრაცია და ანტივირუსული დაცვა;
94	გადაწყვეტილებას უნდა შეეძლოს HTTPS შემომავალი და გამავალი მიმართულებებით დეშიფრაცია;
95	გადაწყვეტილებას უნდა შეეძლოს HSM- თან (hardware security module) ინტეგრაცია ციფრული გასაღებების სამართავად;
96	VxLAN ტუნელების ინსპექტირების მხარდაჭერა
97	HTTPS ტრაფიკის ინსპექტირების პოლიტიკების განსაზღვრა, შესაძლებელი უნდა იყოს, სახვადასხვა პარამეტრებით, მათ შორის: მომხმარებლის სახელის / მომხმარებლის ჯგუფის, source IP / source ზონის, destination IP) / destination ზონისა და URL კატეგორიის მიხედვით;
98	გადაწყვეტილებას უნდა შეეძლოს HTTPS ტრაფიკზე გამორიცხვის პოლიტიკების განსაზღვრა, რათა მისი დეშიფრაცია არ მოხდეს. გამორიცხვების პოლიტიკების გამართვა შესაძლებელი უნდა იყოს სხვადასხვა პარამეტრებზე დაყრდნობით, მათ შორის source/desination IP, აპლიკაცია, URL/URL კატეგორია, გარე დინამიური სიები, source/desination მოწყობილობა, მომხმარებელი;
99	გადაწყვეტილებას უნდა შეეძლოს HTTPS სესიის სერთიფიკატის შემოწმება ვალიდურობაზე, არვალიდური/არასანდრო სერტიფიკატის შემთხვევაში სესიის პრევენცია;
100	გადაწყვეტილებას უნდა შეეძლოს SSL ტრაფიკის დეშიფრაცია და ასლის გარე ანალიტიკის მოწყობილობაზე გადაცემა. შეთავაზებას უნდა დაერთოს შესაბამისი ლიცენზია.

101	გადაწყვეტილებას უნდა გააჩნდეს packet broker/service chain ფუნქციონალი. აღნიშნული ფუნქციონალის ფარგლებში გადაწყვეტილებას უნდა შეეძლოს SSL ტრაფიკის დეშიფრაცია და დეშიფრირებული ტრაფიკის გადაცემა გარე სერვისულ მოწყობილობაზე (მაგალითად IPS, Network Forensics,) დამატებითი ინსპექტირებისთვის. გარე სერვისული მოწყობილობიდან დაბრუნებული ღია ტრაფიკის თავიდან შიფრაცია და ქსელში გადაცემა. აღნიშნული ფუნქციონალის ფარგლებში, გადაწყვეტილებას უნდა შეეძლოს: - მაღალმდგრადობის რეჟიმის მხარდაჭერა; - გარედან შიდა, სერვერებზე მიმართული SSL ტრაფიკის მხარდაჭერა; - მომხმარებლებიდან, ინტერნეტში მიმავალი SSL ტრაფიკის მხარდაჭერა; - ტრანსპერენტული ე.წ Layer 1 რეჟიმის მხარდაჭერა; - მარშრუტიზაციის ე.წ Layer 3 რეჟიმის მხარდაჭერა; - რამოდენიმე სერვისულ მოწყობილობაზე, ტრაფიკის განაწილების სხვადასხვა რეჟიმების მხარდაჭერა, მათ შორის: - IP Source & IP Destination ჰეში - IP Source & IP Destination & Port ჰეში - Round Robin - დაყოვნების დამოკიდებული;
102	გადაწყვეტილებას უნდა შეეძლოს გეოგრაფიული ზონების მიხედვით პოლიტიკების შექმნა;
103	დამატებითი სავალდებულო მოთხოვნები NGFW– სთვის: - ერთზე მეტ ადმინისტრატორს უნდა შეეძლოს ერთდროულად კონფიგურაციის ცვლილება; - უსაფრთხოების პოლიტიკების აქტივაცია უნდა ხორციელდებოდეს, აქტივაციის ოპერაციის გამოძახების შემდეგ. აქტივაციის ოპერაცია უნდა იძლეოდეს შესაძლებლობას მოინიშნოს სპეციფიური ადმინისტრატორი, რომლის ცვლილებების აქტივაციაცაა საჭიროა, ან ყველა ადმინისტრატორის; - თითოეული აქტივაციის წინ, მოწყობილობა ავტომატურად უნდა ახორციელებდეს, მიმდინარე კონფგურაციის სარეზერვო ასლის შექმნას; - სარეზერვო ასლის პოლიტიკები უნდა აღდგეს და გააქტიურდეს გადატვირთვის აუცილებლობის გარეშე; - გადაწყვეტილებას უნდა გააჩნდეს უსაფრთხოების პოლიკების ოპტიმიზაციის ფუნქცია. რის ფარგლებშიც, უნდა მოხდეს ადმინისტრატორის შეტყობინება თუ პოლიტიკა დუბლირდება ან გადაიფარება უკვე არსებული პოლიტიკით; - ლოგების გადაცემა გარე სისტემებში შესაძლებელი უნდა იყოს SNMP ასევე syslog ის საშუალებით; - ლოგები უნდა ინახებოდეს ლოკალურად. ასევე უნდა არსებობდეს ლოგების გაგზავნის ცენტრალური მართვისა და მონიტორინგის სისტემაზე, მისი არსებობის შემთხვევაში;

	- შემოთავაზებულ სისტემას უნდა ჰქონდეს SSD ტიპის სისტემური დისკი, არანაკლებ 480 (ოთხას ოთხმოცი) გბაიტი ზომის. - მოწყობილობას უნდა ჰქონდეს შესაძლებლობა snmp და syslog ლოგების გადაცემის სპეციალურად განსაზღვრული ფილტრების გამოყენების საშუალებით; - გადაწყვეტილებას უნდა შეეძლოს ავტომატურად განაახლოს მავნე IP მისამართების სია სპეციალური სერვისის მეშვებობით და განახორციელოს მათი ბლოკვა; - გადაწყვეტილებას უნდა გააჩნდეს SYN Flood, UDP Flood, ICMP Flood უსაფრთხოების პოლიტიკების გამართვა, ზღვრული მნიშნველობების მითითებით; - გადაწყვეტილებას უნდა შეეძლოს TCP port scan, UDP Ports scan და sweep scan იდენტიფიცირება და ბლოკირება; - გადაწყვეტილება უნდა ეყრდნობოდეს ე.წ white list უსაფრთხოების მოდელს და გააჩნდეს მარტივი ინტერფეისი უსაფრთხოების პოლიტიკების სამართავად და რედაქტირებისთვის. - გადაწყვეტილებას უნდა შეეძლოს ე.წ portable executable ფაილების გადაცემა ღრუბლოვან Sanbox ში ანალიზისთვის. აღნიშნული ფუნქციონალი არ უნდა საჭიროებდეს დამატებით ლიცენზირებას;
104	გადაწყვეტილება აღჭურვილი უნდა იყოს 3 წლიანი უსაფრთხოების ლიცენზიებით, მათ შორის IPS, URL, DNS, და ანტივირუსული უსაფრთხოების ნაწილში. გადაწყვეტილება აღჭურვილი უნდა იყოს მწარმოებლის 3 წლიანი მხარდაჭერით.
105	მომწოდებელმა უნდა წარმოადგინო მწარმოებლის ავტორიზაციის წერილი (MAF)

13. ბრანდმაუერი B ტიპის

1	რაოდენობა: 1
2	მოწყობილობის გამტარობა ქსელის დამცავი რეჟიმში აპლიკაციების და მომხმარებლების იდენტიფიკაციით, ლოგირებით - არანაკლებ 1.2 გბ/წმ. (ტრაფიკის პროფილი დამიქსული აპლიკაციებით)
3	მოწყობილობის გამტარუნარიანობა (Application Control, IPS, Anti-Virus, Anti-spyware ან Anti-bot, Zero Day Attacks Detection and Analysis) - არანაკლებ 0.6 გბ/წმ; (ტრაფიკის პროფილი დამიქსული აპლიკაციებით) ასევე უნდა იყოს გამოქვეყნებული მწარმოებლის ოფიციალურ ვებგვერდზე;
4	IPsec VPN გამტარობა უნდა შეადგენდეს მინიმუმ 0.5 Gbps;
5	წამში ახალი სესიების მაქსიმალური რაოდენობა არანაკლებ 10,000;
6	სესიების მაქსიმალური რაოდენობა არანაკლებ 62,000;
7	სიმაღლე არაუმეტეს 1 Rack Unit

8	მოწყობილობა უნდა შედგებოდეს, მართვის კომპონენტისა და ტრაფიკის დამუშავების დამოუკიდებელი პროგრამული და აპარატული კომპონენტებისგან. თითოეულ კომპონენტს უნდა ჰქონდეს პროცესორების (CPU), RAM (მეხსიერება) და ინტერფეისების (Ethernet პორტი) საკუთარი ნაკრები. აღნიშნული კომპონენტები ერთმანეთისგან დამოუკიდებლად უნდა იყვნენ, რათა შეძლონ მოწყობილობის კონტროლი კრიტიკული დატვირთვის შემთხვევაში, განსაკუთრებით DoS / DDoS შეტევების დროს.
9	არანაკლებ: 7 x 100/1000/10000 მბ/წმ სპილენძის ინტერფეისი არანაკლებ: 1 x 100/1000/10000 მბ/წმ სპილენძის OOB ტიპის ინტერფეისი არანაკლებ: 1 x RJ45 console ინტერფეისი არანაკლებ: 2 x USB ინტერფეისი
10	სტატიკური IPv4 / IPv6 მარშრუტიზაციისა და დინამიური მარშრუტიზაციის პროტოკოლების BGPv4, OSPFv2 / v3, RIP v2 მხარდაჭერა. თუ ამ ფუნქციონალისათვის საჭირო დამატებითი ლიცენზია, ის უნდა იყოს შეტანილი შემოთავაზებაში;
11	ქსელის ინტერფეისებს უნდა ჰქონდეს მხარდაჭერა Span- პორტებიდან "დუბლირებული" ტრაფიკის მოსმენის, MAC და IP- მისამართის (Virtual Wire) შეცვლის გარეშე, Layer 2 რეჟიმის, ტრაფიკის მარშრუტიზაციის რეჟიმის (Layer 3);
12	მხარდაჭერა ქსელის სხვადასხვა ინტერფეისების ერთდროულად მუშაობაში ჩამოთვლილ ნებისმიერ რეჟიმში ნებისმიერ კომბინაციაში შეზღუდვების გარეშე ერთი ვირტუალური ბრანდმაუერის შიგნით;
13	პორტის მუშაობის რეჟიმის შეცვლის მხარდაჭერა (Layer 2, Layer 3, გამჭვირვალე რეჟიმი და მოსმენის რეჟიმი) მოწყობილობის გადატვირთვის გარეშე;
14	სტატიკური და დინამიური (Hide) NAT– ის მხარდაჭერა
15	NAT მხარდაჭერა გამჭვირვალე რეჟიმში
16	IPV6 მხარდაჭერა, მათ შორის, პროგრამა და მომხმარებლის იდენტიფიკაცია
17	multicast მარშრუტიზაციის პროტოკოლების მხარდაჭერა - PIM-SM, PIM-SSM, IGMP v1, v2, v3.
18	ბრანდმაუერზე ორგანიზებულ VLAN ქსელებს შორის მარშრუტიზაციის მხარდაჭერა
19	მოწყობილობამ უნდა უზრუნველყოს არანაკლებ 4000 vlan ერთ ინტერფეისზე;
20	NAT ტრანსლაციების, DHCP სერვერის და DHCP relay ფუნქციონირების მხარდაჭერა.
21	802.1-ზე ტეგირებული ფრეიმების მხარდაჭერა.
22	802.3ad ინტერფეისის გაერთიანების მხარდაჭერა (LACP მხარდაჭერა).
23	დიდი პაკეტების (Jumbo frame) გადაცემის მხარდაჭერა.
24	SNMPv3 მხარდაჭერა.
25	Netflow მხარდაჭერა. Netflow პროფილი უნდა განისაზღვროს ფიზიკური პორტების საფუძველზე.

26	LLDP (Link Layer Discovery Protocol) მხარდაჭერა. მოწყობილობას უნდა ჰქონდეს ინფორმაცია სხვა მოწყობილობების შესახებ (MAC მისამართი, სისტემის სახელი, მასთან დაკავშირებული პორტი).
27	Policy Based Forwarding მხარდაჭერა IPv4 და IPv6 პროტოკოლებისთვის.
28	BFD (Bidirectional Forward Detection) მხარდაჭერა
29	არანაკლებ 10 ვირტუალური ბრანდმაუერის მხარდაჭერა მომავალში ლიცენზიის უზრუნველყოფით.
30	site-to-site და client-to-site IPSec VPN მხარდაჭერა.
31	მაქსიმალური შესაძლო Client SSL VPN რაოდენობა - არანაკლებ 250.
32	მაღალ მდგრადობის კლასტერის შექმნის მხარდაჭერა (HA) - Active/Passive და Active/Active
33	HA კლასტერირების რეჟიმში უნდა იყოს მხარდაჭერილი ბრანდმაუერების ჰორიზონტალური მასშტაბირება, არანაკლებ 6 ბრანდმაუერის გაერთიანება ერთ კლასტერში;
34	HA კლასტერირების რეჟიმს უნდა გააჩნდეს რამდენიმე მოშორებული დატაცენტრებს შორის მუშაობა;
35	კლასტერის კომპონენტებს შორის გადასასვლელად უნდა განხორციელდეს ინტერფეისების მონიტორინგი (interface monitoring) და მითითებული რესურსებისკენ მიმავალი გზები (path monitoring);
36	მოწყობილობა უნდა აკონტროლებდეს სესიების სტატუსს (Stateful inspection) პაკეტების ფილტრაციით და აპლიკაციების იდენტიფიკაციით.
37	მოწყობილობა უნდა იყოს Zone- ებზე (Zone-based) დაფუძნებული. ერთი ან მეტი ინტერფეისი ან ქვე ინტერფეისი შეიძლება მიეკუთვნებოდეს ერთ ზონას. წვდომის (firewall rules) და NAT-ის პოლიტიკები უნდა ებმებოდეს ზონებს;
38	NAT პოლიტიკას უნდა ჰქონდეს საკუთარი წესები, დამოუკიდებელი უნდა იყოს წვდომის პოლიტიკებისაგან (firewall rules);
39	ქსელის ბრენდმაუერზე გატარებული ტრაფიკის OSI მოდელის მეშვიდე დონეზე ქსელის აპლიკაციების ამოცნობა და დაბლოკვა, მათ შორის ინდივიდუალურად ყველა პროგრამისთვის, რომლებიც იყენებენ საერთო პორტებს, (80 და 443), რომლებიც იყენებენ დინამიურ TCP / UDP პორტებს;
40	აპლიკაციების მართვამ უნდა აჩვენოს აპლიკაციის დამოკიდებულება, რომ შეძლოს თეთრი სიების შექმნა.
41	Layer-7 OSI მოდელზე ტრაფიკის აღმოჩენა და ინსპექტირება სიგნატურებით, პროგრამული უზრუნველყოფით, პროტოკოლებითა და სერვისებით: - აუთენტიფიკაციის სერვისები, მათ შორის Microsoft Active Directory, LDAP, RADIUS, TACACS +, Kerberos, SAML, Syslog Monitoring / Parser (Syslog– დან შეტყობინებების დამუშავებისას მოწყობილობამ უნდა უზრუნველყოს user-to-ip რუკების შედგენა); - მონაცემთა ბაზები, მათ შორის Microsoft SQL, Oracle და ა.შ; - ფაილური სერვისები, მათ შორის Microsoft SMB;

	- ელექტრონული დოკუმენტების მართვისა და გაგზავნის სისტემები, მათ შორის Microsoft Sharepoint, Exchange, Office 365, Google Docs; - ელ.ფოსტის პროტოკოლები: SMTP, POP3, IMAP; - VOIP პროტოკოლები და აუდიო – ვიდეო კონფერენციები, მათ შორის SIP, H.323, H.245, H.225, Webex; - პროგრამული უზრუნველყოფის განახლების სერვისები, მათ შორის Microsoft Update, ანტივირუსული პროგრამა, Adobe, Java; - სარეზერვო სერვისები; - ვირტუალიზაციისა და ტერმინალზე წვდომის სერვისები, მათ შორის VMware, Microsoft RDP; - დისტანციური წვდომის პროტოკოლები, მათ შორის Telnet, SSH, VNC, Radmin; - ქსელის პროტოკოლები, მათ შორის დინამიური მარშრუტიზაციისა და SSL პროტოკოლები, IPSec VPN; - ელექტრონული ფოსტა; - სოციალური ქსელები; - მყისიერი შეტყობინების საშუალებები; - აუდიო – ვიდეო კონფერენციების საშუალებები; - აუდიო-ვიდეოს ნაკადები (ვებსაიტის მიუხედავად), აუდიოსა და ვიდეოს ნაკადი HTTP– ით; - დისტანციური წვდომის საშუალებები, Team-Viewer- ის ჩათვლით; - გარე Proxy სერვერები და ანონიმაიზერები, მათ შორის Tor, Ultrasurf, Freegate, SOCKS, PHP Proxy; - ინსტრუმენტები VPN და ტუნელების შესაქმნელად სხვა პროგრამებზე, მათ შორის Freenet, Open-vpn, Vtun, Rdp-to-Tcp, Tcp-over-Dns;
42	გადაწყვეტილებას უნდა ჰქონდეს SafeSearch– ის მხარდაჭერა YouTube– სა და CIPA– ს შესაბამისი Google ძიებისთვის (გადაწყვეტილება არ უნდა მუშაობდეს პროქსი რეჟიმში).
43	ჩაშენებული ხელსაწყოები, საკუთარი სიგნატურების შესაქმენელად, ე.წ Regex ზე დაფუძნებით და HTTP (S), FTP, SMB, SMTP, RPC დეკოდერების გამოყენებით. აგრეთვე ნიღაბი TCP / UDP- პაკეტების შიგთავსისთვის;
44	შესაძლებელი უნდა იყოს ჰოსტის უსაფრთხოების დონეზე დაფუძნებული უსაფრთხოების პოლიტიკების შექმნა;
45	აპლიკაციების აღმოჩენა დაშიფრულ ტრაფიკში, მათ შორის SSL (RSA გასაღებების მხარდაჭერა 2048 ბიტამდე) და SSHv2 ტრაფიკში. ბრანდმაუერში, შემომავალი ან/და გამავალი ტრაფიკის დეშიფრაციის მხარდაჭერა, მოხმარებლებისთვის ტრანსპერენტულად, ინდივიდუალური მიკრო აპლიკაციების კონტროლის შესაძლებლობით, მათ შორის სოციალურ ქსელებში შეტყობინებების გაგზავნის, ფაილების მიმოცვლა, აუდიო და ვიდეოს კონტროლი.
46	ერთ სესიის ფარგლებში სხვადასხვა ტიპის აპლიკაციეს აღმოჩენის შესაძლებლობა;

47	წვდომის კონტროლის პოლიტიკებს, უნდა გააჩნდეს დროის, დღის, თარიღისა და პერიოდის გათვალისწინებით მუშაობა.
48	მომხმარებელთა ამოცნობა, რომლებიც იყენებენ ქსელურ აპლიკაციებს, კორპორატიული აუტენტიფიკაციის სერვისებთან ინტეგრაციის ხარჯზე, ინტეგრაცია: Microsoft Active Directory, Microsoft Exchange, LDAP, Novell eDirectory სთან;
49	მომხმარებელთა ჯგუფებისა და ინდივიდუალური მომხმარებლების საფუძველზე პოლიტიკების შექმნის შესაძლებლობა. სისტემამ უნდა შეინახოს მომხმარებლის ინფორმაცია შესაბამის ჟურნალებში.
50	ინტეგრაცია Microsoft Active Directory– ში უნდა განხორციელდეს Active Directory– ში ცვლილებების გარეშე და არ უნდა იქნას გამოყენებული Active Directory დომენის ადმინისტრატორის ანგარიში;
51	Microsoft Active Directory ინტეგრაცია არ უნდა საჭიროებდეს დამატებით კომპონენტებს, შუამავალ აგენტებსა თუ დამატებითი პროგრამული უზრუნველყოფის ინტალაციას;
52	ავტორიზაციის სერვისებთან (მაგ., უკაბელო ქსელის კონტროლერებთან) ინტეგრირების შესაძლებლობა ღია XML API– ს საშუალებით;
53	User-IP რუკების შექმნის შესაძლებლობა (user-IP mapping) სისტემის მიერ გაგზავნილი syslog შეტყობინებების ანალიზის საშუალებით, რომლებიც ავტორიზაციას უკეთებენ მომხმარებლებს.
54	უსაფრთხოების პოლიტიკებში, მომხმარებლის დინამიური ჯგუფების შექმნისა და გამოყენების შესაძლებლობა. დინამიური მომხმარებლის ჯგუფების საშუალებით შესაძლებელი უნდა იყოს "მყისიერად" მომხმარებლის ჯგუფში დამატება ან ამოშლა, შესაბამისი დირექტორიის ჯგუფებში (მაგალითად, Active Directory) შეცვლის გარეშე და წესების დაყენების გარეშე. ეს საშუალებას უნდა იძლეოდეს ავტორიზებულ ადმინისტრატორებს ან გარე სისტემებს ამოიღონ მომხმარებელი დინამიური მომხმარებლის ჯგუფიდან, მაგალითად, თუ შესაბამისი მომხმარებელი კომპრომეტირებულია;
55	უსაფრთხოების ერთიან უნიფიცირებული პოლიტიკების შექმნა, გამომგზავნის, მიმღების, გამოყენებული სერვისების (TCP/UDP- პორტები), მომხმარებლის სახელების, მომხმარებლის ჯგუფების და პროგრამების ან პროგრამების კატეგორიების მითითების საშუალებით;
56	პოლიტიკას უნდა შეეძლოს შემდეგი ქმედებების განხორციელება: - ნებართვა ან აკრძალვა; - მიეცეს უფლება კონკრეტულ პროგრამას ან პროგრამის კატეგორიას გამოიყენოს მხოლოდ სტანდარტული ან მკაცრად განსაზღვრული TCP / UDP პორტები. ამასთან, ეს პორტები არ უნდა იქნას გამოყენებული სხვა პროგრამების მიერ ისეთი პოლიტიკის გარეშე, რომელიც აშკარად იძლევა ამგვარი ურთიერთქმედების საშუალებას;

	- ნებართვები ან უარი დროის გრაფიკის მიხედვით, მომხმარებლების ან მომხმარებლის ჯგუფის საფუძველზე; - DSCP ტეგირებისა და ტრაფიკის შეზღუდვები QOS წესების გამოყენებით, რომლებიც დაფუძნებულია აპლიკაციებზე, IP მისამართებზე, DSCP, მომხმარებლებსა და მომხმარებელთა ჯგუფებზე. - QOS– ის განხორციელება რეალურ დროში აპლიკაციების დონეზე, მხარდაჭერილი უნდა იყოს სხვადასხვა ტიპის აპლიკაციები, მათ შორის ცოლიალური ქსელები, აუდიო, ვიდეო, მესინჯერები, ფაილების მიმოცვლა; - შესაძლებელი უნდა იყოს QOS ის რემარკირების განხორციელება, source/destination IP, პორტისა და აპლიკაციის დონეზე; - ტრაფიკის მარშრუტიზაცია პოლიტიკების მიხედვით (Policy Based Forwarding) IP მისამართის (source ან/და destination), მომხმარებლის, აპლიკაციის ან URL- ის საფუძველზე; - აპლიკაციებში გარკვეული ფუნქციონირების კონტროლის შესაძლებლობა; - ზემოთქმულის ნებისმიერი კომბინაციის გამოყენების შესაძლებლობა; - ინდივიდუალური მომხმარებლებისთვის სიის / შავი სიის პოლიტიკის შექმნის შესაძლებლობა.
57	სხვადასხვა პროტოკოლების ტრაფიკის ინსპექტირების შესაძლებლობა: - Generic Routing Encapsulation; - არა დაშიფრული IPSec ტრაფიკი (NULL Encryption Algorithm for Ipsec and transport mode AH Ipsec).
58	გადაწყვეტილებას უნდა გააჩნდეს უსაფრთხოების პოლიტიკების ოპტიმიზაციის ფუნქციონალი, რომელიც დაფუძნებულია გამოყენებულ აპლიკაციებზე. მათ შორის პოლიტიკების აღმოჩენა და წაშლა რომლებიც არ გამოიყენებიან;
59	მკაცრი უსაფრთხოების პოლიტიკების შესაქმნელად, მოწყობილობის ინტერფეისში ხელმისაწვდომი უნდა იყოს შემდეგი ფუნქციონალი: - განახორციოლოს იმ უსაფრთხოების პოლიტიკების იდენტიფიცირება, რომლებშიც არაა განსაზღვრული აპლიკაციები. მოახდინოს იმ აპლიკაციების იდენტიფიცირება, რომლებიც იყენებენ აღნიშნულ უსაფრთხოების პოლიტიკას და უზრუნველყოს აპლიკაციების მითითება/აქტივაცია აღნუშნულ პოლიტიკაში, წინასწარ აპლიკაციების სიის მოწოდებით რომელშიც მოხდება საჭირო აპლიკაციების არჩევა; - განახორციელოს იმ უსაფრთხოების პოლიტიკების იდენტიფიცირება, რომლებშიც მითითებული აპლიკაცია არ გამოიყენება. გამოუყენებელი აპლიკაციების შესახებ ინფრომაციის ასახვა, ბოლო 7, 15 და 30 დღის განმავლობაში; - განახორციელოს უსაფრთხოების პოლიტიკაში მოხვედრილი აპლიკაციის გამოყენების პირველი და ბოლო თარიღი და აპლიკაციის ტრაფიკის მიერ დაკავებული ქსელური გამტარუნარიანობა;

	- განახორციელოს უსაფრთხოების პოლიტიკების იდენტიფიცირება რომლებიც არ იყო გამოყენებული ბოლოს 30 და 90 დღის განმავლობაში;
60	უსაფრთხოების პოლიტიკებში შესაძლებელი უნდა იყოს გეოგრაფიული რეგიონების განსაზღვრა;
61	გამტარუნარიანობის შეზღუდვა შესაძლებელი უნდა იყოს მომხმარებლის სახელის/ჯგუფის, საწყისი/მიმღები IP მისამართისა და აპლიკაციის საფუძველზე.
62	გარკვეული წყაროებიდან ტრაფიკის ავტომატურად დაბლოკვის შესაძლებლობა ქსელის ბრანდმაუერის დონეზე, სანამ ეს პაკეტები გამოიყენებენ ბრანდმაუერის მთავარი პროცესორის ან პაკეტის ბუფერის რესურსებს.
63	გადაწყვეტილებას უნდა გააჩნდეს სპეციალური სერვისის მხარდაჭერა, რომელშიც განხორციელდება ახალი პოტენციურად მავნე ფაილების გაშვება Microsoft Windows ის გარემოში, მათ შორის (EXE, DLL, SCR, BAT და ა.შ.) ფაილების, ქსელში გადაცემული ფაილების, SMTP/POP3 ელ.ფოსტის შეტყობინებებში მათ შორის SSL დაშიფრული შეტყობინებებში, საეჭვო ფაილების ქცევის ანალიზი, ბმულების ანალიზი, როგორც კერძო "Sanbox" -ში ასევე ღრუბლოვან "Sanbox" -ში. ახალი მავნე ფაილების აღმოჩენა და ავტომატური სიგნატურების გენერაცია არანაკლებ 24 საათში, ხოლო URL რეპუტაციული ბაზების განახლება არანაკლებ 30 წუთში.
64	ვიზუალიზაციის მოწინავე ფუნქციონალის არსებობა: ვიზუალიზაცია მარტივი და მოსახერხებელი ფორმატით, ქსელური პროგრამების აქტივობა, ქსელური შეტევების აღმოჩენა და ბლოკირება. ინფორმაციის ფილტრაციის შესაძლებლობა, სხვადასვა საკვანძო პარამეტრების გამოყენებით, მათ შორის (პროგრამების, საფრთხეების, მომხმარებლების, IP მისამართების, TCP/UDP პორტების, უსაფრთხოების ზონების, საფრთხეების ტიპები და ა.შ.);
65	რეპორტების შექმნის შესაძლებლობა. ბრანდმაუერს უნდა ჰქონდეს რეპორტების ავტომატური წარმოების ფუნქციონალი და მათ შორის განრიგის მიხედვით, ხელით განსაზღვრულ სხვადასხვა თემატურ ფუნქციებზე. რეპორტების ნახვა შესაძლებელი უნდა იყოს, როგორც უშუალოდ ვებ გრაფიკული ინტერფეისით (GUI), აგრეთვე PDF და CSV ფორმატებში ექსპორტის შესაძლებლობით;
66	უნდა შეეძლოს ინტეგრირება იგივე მწარმოებლის ცენტრალიზებული მართვისა და მონიტორინგის სისტემასთან, ლოგირების, პროგრამული უზრუნველყოფის განახლების და რამოდენიმე ბრანდმაუერის მართვის შეასძლებლობით;
67	უნდა შეეძლოს ბრანდმაუერზე ლოკალურად გამოყოფილ დისკებზე ლოგიბის ბუფერიზაცია, იმ შემთხვევაში თუ დაიკარგება წვდომა ცენტრალიზირებული მართვისა და მონიტორინგის სისტემასთან;
68	უნდა შეეძლოს მესამე მხარის SIEM- სისტემებთან ინტეგრირებას Syslog- ის საშუალებით, ლოგის ფორმატის მოქნილი კონფიგურაციის შესაძლებლობით;
69	უნდა შეეძლოს ლოკალური ადმინისტრატორების კონტროლი, როლებზე დაფუძნებით:

	- შესაძლებელი უნდა იყოს მართვის და კონფიგურაციის ნახვის არიალის შეზღუდვა, როგორც მთლიან მოწყობილობაზე ასევე ცალკეულ კონტექსტზე; - შესაძლებელი უნდა იყოს, კონფიგურაციის ცვლილების, ნახვის ან ნახვის სრული შეზღუდვა ბრანდმაუერის ვებ ინტერფეისის ნებისმიერ ჩანართზე; - შესაძლებელი უნდა იყოს, კონფიგურაციის ცვლილების, ნახვის ან ნახვის სრული შეზღუდვა ბრანდმაუერის CLI ინტერფეისზე;
70	გადაწყვეტილებს უნდა გააჩნდეს ერთიანი მართვის ინტერფეისი, უსაფრთხოების პოლიტიკების სამართავად, მოწყობილობის ქსელური პარამეტრების სამართავად, უსაფრთხოების პროფილების სამართავად, როგორც ლოკალურად ასევე ცალკე მდგომი მართვის და მონიტორინგის სადგურის საშუალებით. ბრანდმაუერის ლოკალური მართვის შემთხვევაში მას უნდა შეეძლოს ლოგირების განხორციელება ლოკალურად;
71	გადაწყვეტილების მართვა შესაძლებელი უნდა იყოს HTTPS და SSH პროტოკოლებზე დაფუძნებით, დამატებითი პროგრამული უზრუნველყოფის ინსტალაციის გარეშე ადმინისტრატორის კომპიუტერზე;
72	ბრანდმაუერის მართვის ლოკალური ინტერფეისი (ვებ და CLI) უნდა იყოს უნიფიცირებული ცენტრალური მართვისა და მონიტორინგის სისტემასთან, რომლიდანაც შეასძლებელია განხორციელდეს ცენტრალიზირებული ლოგირება, რეპორტინგი და პროგრამული უზრუნველყოფის განახლება;
73	Cisco TrustSec SGT ტეგების მხარდაჭერა;
74	გადაწყვეტილებას უნდა გააჩნდეს დინამიური მისამართების ჯგუფებისა (Dynamic Address Group) და დინამიური მომხმარებლების ჯგუფების (Dynamic User Group) მხარდაჭერა. რაც უზრუნველყოფს XML API საშუალებით აღნიშნული ჯგუფების განახლებას უსაფრთხოების პოლიტიკებში. აღშნული წცლილებების უნდა ისახებოდეს მყისიერად და არ საჭიროებდეს უსაფრტხოების პოლიტიკების ხელახალ აქტივაციას;
75	გადაწყვეტილებას უნდა გააჩნდეს თანამედროვე პროგრამულ-აპარატურული არქიტექტურა, რომელიც დაფუძნებულია, როგორც სტატიკურ ASIC ზე, ასევე პროგრამირებად FPGA ჩიპებზე. აღნიშნული ჩიპები უნდა ასრულებდენ ცალკეულ ამოცანებს, მათ შორის დაშიფრული ტრაფიკის, მარშრუტიზაციის პროტოკოლების, ARP პაკეტების დამუშავება და სხვა. ბრანდმაუერზე დიდი დატვირთვის დროს ცალკეული აპარატურული ჩიპები უნდა ასრულებდენ კრიტიკულ ამოცანებს ტრაფიკის დამუშავებისგან დამოუკიდებლად;
76	გადაწყვეტილებას უნდა გააჩნდეს შემდეგი NGFW ფუნქციონალი: - მოწყობილობებს უნდა ჰქონდეთ არქიტექტურული შემოწმების შესაძლებლობა, მათ შორის IP პაკეტის ფილტრაციის, აპლიკაციების აღმოჩენის ფუნქციები და ასევე შემდეგი უსაფრთხოების სერვისები: - ახალი თაობის ბრანდმაუერი (NGFW) - IPSEC VPN, SSL VPN - აპლიკაციების კონტროლი(Application Control)

	- ანტივირუსი(Antivirus/Antimalware) - შეჭრის პრევენცია (IPS) - Antispyware / antibot - უცნობი მავნე ფაილების გამოვლენა და ”ნულოვანი” დღის შეტევების და მოწინავე მუდმივი საფრთხეების პრევენცია (APT) - შეტევების დაბლოკვა DNS პროტოკოლის გამოყენებით (DNS Security) - URL გაფილტვრა(URL filtering) - IoT მოწყობილობების იდენტიფიკაცია და ანალიზი(IoT Security) - დირექტორიების სერვისებთან ინტეგრაცია მომხმარებლების იდენტიფიცირებისთვის (Identity Awareness)
77	გადაცემული ტრაფიკის რეალურ დროში შემოწმების შესაძლებლობა, მათ შორის: სიგნატურული ანალიზი, ქცევის ანალიზი, დაცვა მოწყვლადობებისგან, დაცვა ქსელური შეტევებისგან, მავნე ფაილებისგან დაცვა, ფაილების ტიპების აღმოჩენა, ვირუსების აღმოჩენა სხვადასხვა ტიპის პროტოკოლებში მათ შორის ელექტრონულ ფოსტაში, FTP და SMB პროტოკოლებში, ჯაშუშური პროგრამების აღმოჩენა, ქსელური “worms” ბლოკირება, ქსელურ და აპლიკაციების ტრაფიკში შიგთავსის აღმოჩენა regex საშუალებით, როგორც SSL ასევე SSHv2 დაშიფრულ ტრაფიკში;
78	ანტივირუსული დაცვა, ჯაშუშური პროგრამებისგან დაცვა, მოწყვლადობებისგან და ქსელის შეტევებისგან დაცვა(IPS სისტემა), URL- ფილტრაცია დინამიური რეპუტაციის ბაზის გამოყენებით, რომელიც გააჩნია ერთი და იგივე საიტის ფარგლებში კატეგორიციის მხარდაჭერა, მათ შორის კატეგორიზაცია ერთი და იგივე საიტის სხვადასხვა ენაზე, ფაილების გადაცემის ბლოკირება ტიპებით;
79	დამატებითი სკანირების ფუნქციების გამოყენების შესაძლებლობა Microsoft და Android გარემოში, ახალი პოტენციურად მავნე ფაილების სკანირებისთვის, მათ შორის, ფაილების (EXE, DLL, SCR, BAT და ა.შ.), PDF დოკუმენტების (Adobe Reader– ის სხვადასხვა ვერსიის შემოწმება), MS Office 2003, 2007 და ზემოთ, Java და Flash, Android APK, ბმულები http: // და https: // ახალი მავნე პროგრამების და ანტივირუსული სიგნატურების ავტომატური შექმნის შესაძლებლობა აღმოჩენას რეალურ დროში;
80	სხვადასხვა ტიპის ლოგების ავტომატური კორელაცია, ქსელური ბრანდმაუერის, IPS, ფაილის გადაცემის კონტროლი, URL ფილტრაცია), რომლებიც გენერირებული იქნა ერთი სესიის ფარგლებში;
81	გადაწყვეტილებას უნდა ჰქონდეს შემდეგი IPS სისტემის ფუნქციები: - სხვადასხვა მომხმარებლებისთვის ან მომხმარებელთა ჯგუფებისთვის სხვადასხვა IPS პოლიტიკის შექმნის შესაძლებლობა. - მოწყობილობაზე IPS ხელმოწერების ძებნის შესაძლებლობა CVE, კრიტიკულობის დონის და ჰოსტის ტიპის (კლიენტი / სერვერი) გამოყენებით. - IPS სისტემის სიგნატურების ინდივიდუალურად კონფიგურაციის შესაძლებლობა შეტევებზე რეაგირებისთვის შემდეგნაირად: Allow, Alert, Deny,

	reset-both, reset-client, reset-server, Block-IP. IP– ზე დაფუძნებული დაბლოკვა უნდა განხორციელდეს როგორც source IP– ს, ასევე source და destination IP– ების საფუძველზე. - IPS სიგნატურები, რომლებიც გამოიყენება შეტევების საწინააღმდეგოდ, უნდა განახლდეს ფაილიდან ან ინტერნეტით. გარდა ამისა, საჭიროების შემთხვევაში, სიგნატურების განახლებები ავტომატურად უნდა განხორციელდეს მომხმარებლის ჩარევის გარეშე. - IPS სისტემა უნდა შეიცავდეს პროტოკოლის ანომალიის გამოვლენის ტექნოლოგიას(Protocol Anomaly Detection), რომელიც ბლოკავს შეტევებს არსებულ სიგნატურებზე დაყრდნობის გარეშე; - IPS უნდა შეეძლოს გაუმკლავდეს შემდეგ შეტევებს: - Brute Force - Code/Command execution - Sql-injection - Exploit-kit - Denial of Service - Info-leak - Overflow - Scan
82	გადაწყვეტილებას უნდა გააჩნდეს შემდეგი DNS უსაფრთხოების ფუნქციონალი: - საეჭვო DNS- მოთხოვნების ანალიზი და ინფიცირებული სადგურების ლოკალიზაცია DNS sinkhole ტექნოლოგიის გამოყენებით (DNS- სერვერის პასუხების ჩანაცვლება); - ცნობილი მავნე დომენების სახელების დაბლიკვა რეპუტაციის მონაცემთა ბაზების გამოყენებით; - ფუნქციურმა უნდა გამოიყენოს ღრუბელზე დაფუძნებული მანქანური სწავლების ალგორითმები პოტენციურად მავნე დომენის სახელების დასადგენად; - DNS ტუნელების გამოვლენა და დაბლოკვა (DNS tunneling) მანქანური სწავლების გამოყენებით, რომელიც აანალიზებს DNS მოთხოვნების ხარისხს და ქცევას (მოთხოვნების სიხშირე, ენტროპია და ა.შ.). - DGA (domain generation algorithm) ანალიზი და გამოვლენა, რაც გულისხმობs დომენური სახელების ანალიზს იმის განსასაზღვრელად იყო თუ არა დომენი გენერირებული პროგრამის/მანქანის ან ადამიანის მიერ, უკუინჟინერიაზე დაფუძნებით და სხვა ხშირად გამოყენებული მეთოდების ანალიზით. თუ დადგინდა, რომ დომენი შექმნილია DGA ალგორითმით, მისი დაბლოკვის შესაძლებლობა; - NXNSAttack და DNS Rebinding შეტევების მოგერიება; - Malware, ახალი რეგისტრირებული, Phishing, Grayware , Parked, Proxy Avoidance და Anonymizers ტიპის დომენების აღმოჩენა და ბლოკირება;

83	გადაწყვეტილებას უნდა ჰქონდეს Anti-Spyware / Anti-bot აღმოჩენის და ბლოკირების ფუნქციონალი, შემდეგი შესაძლებლობებით: - აღნიშნული ფუნქციონალი უნდა მუშაობდეს პორტისა და პროტოკოლისგან დამოუკიდებლად და ამოწმებდეს მთელ IP ტრაფიკს. - კონტროლ ცენტრების IP მისამართების განსაზღვრის (resolution requests) მოთხოვნების აღმოჩენა და მათი ბლოკირება DNS მოთხოვნების დონეზე; - DNS Sinkhole ფუნქციონალი, მავნე დომენური სახელის მოთხოვნის შემთხვევაში უნდა გასცეს ადმინისტრატორის მიერ მინიჭებული IP მისამართი, რათა აღმოჩენილი იქნენ ინფიცირებული სისტემები; - სიგნატურების გამოყენებით ცნობილი ბოტნეტების დაბლოკვის ფუნქციონალი. სისტემამ უნდა უზრუნველყოს ადმინისტრატორს botnet სიგნატურების კონფიგურაციის შესაძლებლობა; - სიგნატურებზე შემდეგი ქმედებების განხორციელების შესაძლებლობა: Allow, Alert, Deny, reset-both, reset-client, reset-server, Block-ip. - სხვადასხვა Anti-spyware პოლიტიკები უნდა შეიქმნას სხვადასხვა მომხმარებლებისა და მომხმარებლების ჯგუფებისთვის.
84	Anti-spyware ფუნქციონალი უნდა შეიცავდეს შემდეგი შეტევების იდენტიფიცირებას და დაბლოკვას: - Adware; Botnets; Backdoor; Browser-Hijacker; Data-theft; Keylogger; spyware; net-worm; p2p-communication;
85	მოწყობილობას უნდა ჰქონდეს Anti-Virus ფუნქციონალი, შემდეგი შესაძლებლობებით: - სიგნატურებზე დაფუძნებული ცნობილი მავნე პროგრამების დაბლოკვა. - უნდა ჰქონდეს სკანირების შესაძლებლობა ნაკადში. არქივების სკანირების შესაძლებლობა; - Anti-Virus უნდა შეეძლოს ინტეგრაციის განხორციელება Active Directory სთან, რათა Anti-Virus პოლიტიკების განსაზღვრა განხორციელდეს Active Directory- ში მომხმარებლის ან მომხმარებელთა ჯგუფის საფუძველზე. - Anti-Virus სიგნატურების გამორიცხვის შესაძლებლობა; - შესაძლებელი უნდა იყოს განსხვავებული ანტივირუსული პოლიტიკების შეიქმნას სხვადასხვა მომხმარებლებისა და მომხმარებლების ჯგუფებისთვის. - ანტივირუსმა უნდა დაბლოკოს მავნე ფაილები, რომლებიც გადაეცემა FTP, HTTP, SMB, POP3 გზით.
86	მოწყობილობას უნდა ჰქონდეს URL ფილტრაციის მხარდაჭერა შემდეგი ფუნქციონალით: - URL ფილტრაციის ფუნქციონალი უნდა მუშაობდეს Active Directory სთან ინტეგრაციაში, რის ფარგლებშიც შესაძლებელი უნდა იყოს პოლიტიკების აღწერა მომხმარებლებისა და ჯგუფების მიხედვით Active Directory დან; - შესაძლებელი უნდა იყოს ბლოკირების პორტალის ცვლილება, რომელიც ისახება URL ბლოკირების დროს;

	- C&C (Command and Control) სიების დინამიური განახლება; - URL ფილტრაციის უნდა ჰქონდეს XFF (X-forwarded-for) მხარდაჭერა; - URL კატეგორიაზე შესაძლებელი უნდა იყოს ქსელური ტრაფიკის სიჩქარის შეზღუდვა; - URL- ების კლასიფიკაცია შესაძლებელი უნდა იყოს რისკის მიხედვით, მაღალი რისკი (URL ის მავნე აქტივობა, ბოლო 30 დღის განმავლობაში), საშუალო რისკი (URL ის მავნე აქტივობა, ბოლო 60 დღის განმავლობაში), - ბოლო 30 დღის განმავლობაში რეგისტრირებული URL ების კლასიფიკაცია (ახალი რეგისტრირებული დომენები). - დეტალური ლოგირების წარმოება და გარე syslog მიწოდება, თუ რომელ URL ხორციელდებოდა წვდომა; - URL ფილტრაციის ფუნქციონალს უნდა შეეძლოს მანქანური სწავლების (ML) გამოყენება ვებ გვერდებზე, რათა აღკვეთოს მავნე Javascript ექსპლოიტებისა და ფიშინგის მოხვედრა სისტემაზე. მანქანური სწავლების (ML) ფუნქციონალს, უნდა შეეძლოს, მანქანური სწავლების მოდელებზე დაფუძნებით, რეალურ დროში დინამიური ანალიზი და მავნე შიგთავსის გამოვლენა, ვებ გვერდის სხვადასხვა დეტალების შეფასებით;
87	შემოთავაზებულ გადაწყვეტილებას უნდა ჰქონდეს ნულოვანი დღის შეტევებისგან დასაცავი ფუნქციონალი, ქსელურ ტრაფიკში გადაცემული ფაილების სკანირების საშუალებით: - გადაწყვეტილებას უნდა გააჩნდეს დამატებითი ლოკალური ან ღრუბლოვანი ე.წ sandbox მხარდაჭერა, ფაილების გასაანალიზებლად; - გადაწყვეტილებას უნდა შეეძლოს საეჭვო ფაილების გაგზავნა (ფაილის შემდეგი ფორმატები უნდა იყოს მხარდაჭერილი: 7-ZIP, RAR, ZIP, Adobe Flash, APK, JAR, PDF, MS-Office DOC, DOCX, RTF, XLS, XLSX, PPT, PPTX, .exe, .dll, აგრეთვე ბმულები ფოსტაში, Linux ის ELF ფაილის ფორმატი, Mac OS X ფაილების ფორმატები Mach-O, DMG და PKG) ლოკალურ ან ღრუბლოვან ე.წ sandbox ში. - გადაწყვეტილებას უნდა შეეძლოს რეალურ დროში მიიღოს შესაბამისი განახლებები, რომ უზრუნველყოს მავნე ფაილებისგან დაცვა ლოკალურ ან ღრუბლოვანი ე.წ sandbox ში; - გადაწყვეტილებას უნდა შეეძლოს რეალურ დროში ამოიცნოს და დაბლოკოს უცნობი მავნე პორტატული ე.ს „შემსრულებელი“ ტიპის ფაილები და PowerShell სკრიპტები, მანქანური სწავლების (ML) ალგორითმების გამოყენებით, ფაილის დეტალების შეფასების საშუალებით, მათ შორის ველების და დეკოდერების შაბლონების ჩათვლით. ამ დონის დაცვამ უნდა უზრუნველყოს დაცვა იმ მავნე ფაილებისგან რომლებისთვისაც არ არსებობს სიგნატურები; - გადაწყვეტილებს უნდა შეეძლოს მომხმარებლის იდენტიფიცირება, რომელიც ტვირთავს მავნე ფაილს;
88	გადაწყვეტილებას უნდა გააჩნდეს ფიშინგ და ლეგიტიმირებულ საიტებზე, კორპორატიული სახელისა და პაროლის გამოყენების აღკვეთა;

89	გადაწყვეტილებას უნდა გააჩნდეს ფიშინგ ტიპის შეტევებისგან დაცვის მექანიზმები, მომხმარებლის იდენტობის კონტროლის საშუალებით. გადაწყვეტილებას უნდა შეეძლოს HTTP/HTTPS POST ის დონეზე აღკვეთოს მოპარული, მომხმარებლის კორპორატიული სახელისა და პაროლის გადაცემა. მომხმარებლის კორპორატიული სახელისა და პაროლის კონტროლისთვის გადაწყვეტილებას უნდა შეეძლოს ინტეგრაცია Active Directory სთან. გადაწყვეტილება უნდა იყოს აღჭურვილი შესაბამისი ლიცენზიით;
90	გადაწყვეტილებას უნდა გააჩნდეს მონაცემთა ფილტრაციის მხარდაჭერა, სპეციალური პოლიტიკების საშუალებით. ფაილების ტიპების იდენტიფიკაცია შესაძლებელი უნდა იყოს ე.წ regex ის საშუალებით. გადაწყვეტილება უნდა იყოს აღჭურვილი შესაბამისი ლიცენზიით;
91	გადაწყვეტილებას უნდა გააჩნდეს ღრუბლოვანი ინტერნეტი საგნების (IoT Security) დაცვის მექანიზმები: - NGFW გადაწყვეტილებას უნდა შეეძლოს მეტა ინფორმაციის შეგროვება ქსელურ ტრაფიკში, დეტალური ანალიზისთვის; - გადაწყვეტილებას უნდა შეეძლოს IoT მოწყობილობების ამოცნობა და იდენტიფიცირება მანქანურ სწავლბასა და ხელოვნურ ინტელექტზე დაფუძნებით; - გადაწყვეტილებას უნდა შეეძლოს ბაზური ქცევის შაბლონის განსაზღვრა, რათა მომავალში გამოავლინოს ანომალიური აქტივობა, რაც შეიძლება ნიშნავდეს ქსელური შეტევას და დარღვევას. აღნიშნულის შესახებ გადაწყვეტილებას უნდა შეეძლოს ადმინისტრატორის შეტყობინება. - გადაწყვეტილებას უნდა შეეძლოს უსაფრთხოების პოლიტიკების რეკომენდაციების ავტომატური გენერაცია, რომლებიც უზრუნველყოფენ IoT მოწყობილობის, ლეგიტიმირებულ მუშაობას და არალეგიტიმირებული მუშაობის აღკვეთას. შესაძლებელი უნდა იყოს აღნიშნული რეკომენდაციების იმპორტირება ბრანდმაუერის პოლიტიკებში; - გადაწყვეტილებას უნდა შეეძლოს, უსაფრთხოების პოლიტიკების განსაზღვრა IoT მოწყობილობის იდენტიფიკატორზე დაფუძნებით, მათ შორის მოწყობილობის იმპორტირებული ატრიბუტები, პროფილი, კატეგორია, მწარმოებელი და მოდელი; - გადაწყვეტილებას უნდა შეეძლოს IoT უსაფრთხოების სერვისიდან რეგულარული განახლება, რათა დადგინდეს IoT მოწყობილობის IP მისამართი და მოწყობილობის პროფილი, უსაფრთხოების პოლიტიკებში გამოსაყენებლად. გადაწყვეტილებას უნდა შეეძლოს მაღალი სიზუსტით არანაკლებ 90%, IP მისამართის შესაბამისობის დადგენა, მოწყობილობებისათვის რომლებიც იყო ქსელში აქტიური ბოლო 1 საათი;
92	გადაწყვეტილებას უნდა შეძლოს SSL/TLS და SSH გაშიფვრა, მათ შორის TLS 1.0, TLS 1.1, TLS 1.2 და TLS 1.3 პროტოკოლების;

93	გადაწყვეტილებას უნდა შეეძლოს HTTPS ტრაფიკზე, სხვადასხვა უსაფრთხოების სერვისების განხორციელება, მათ შორის: IPS, აპლიკაციების კონტროლი, URL ფილტრაცია და ანტივირუსული დაცვა;
94	გადაწყვეტილებას უნდა შეეძლოს HTTPS შემომავალი და გამავალი მიმართულებებით დეშიფრაცია;
95	გადაწყვეტილებას უნდა შეეძლოს HSM- თან (hardware security module) ინტეგრაცია ციფრული გასაღებების სამართავად;
96	VxLAN ტუნელების ინსპექტირების მხარდაჭერა
97	HTTPS ტრაფიკის ინსპექტირების პოლიტიკების განსაზღვრა, შესაძლებელი უნდა იყოს, სახვადასხვა პარამეტრებით, მათ შორის: მომხმარებლის სახელის / მომხმარებლის ჯგუფის, source IP / source ზონის, destination IP) / destination ზონისა და URL კატეგორიის მიხედვით;
98	გადაწყვეტილებას უნდა შეეძლოს HTTPS ტრაფიკზე გამორიცხვის პოლიტიკების განსაზღვრა, რათა მისი დეშიფრაცია არ მოხდეს. გამორიცხვების პოლიტიკების გამართვა შესაძლებელი უნდა იყოს სხვადასხვა პარამეტრებზე დაყრდნობით, მათ შორის source/desination IP, აპლიკაცია, URL/URL კატეგორია, გარე დინამიური სიები, source/desination მოწყობილობა, მომხმარებელი;
99	გადაწყვეტილებას უნდა შეეძლოს HTTPS სესიის სერთიფიკატის შემოწმება ვალიდურობაზე, არვალიდური/არასანდრო სერტიფიკატის შემთხვევაში სესიის პრევენცია;
100	გადაწყვეტილებას უნდა შეეძლოს SSL ტრაფიკის დეშიფრაცია და ასლის გარე ანალიტიკის მოწყობილობაზე გადაცემა. შეთავაზებას უნდა დაერთოს შესაბამისი ლიცენზია.
101	გადაწყვეტილებას უნდა გააჩნდეს packet broker/service chain ფუნქციონალი. აღნიშნული ფუნქციონალის ფარგლებში გადაწყვეტილებას უნდა შეეძლოს SSL ტრაფიკის დეშიფრაცია და დეშიფრირებული ტრაფიკის გადაცემა გარე სერვისულ მოწყობილობაზე (მაგალითად IPS, Network Forensics,) დამატებითი ინსპექტირებისთვის. გარე სერვისული მოწყობილობიდან დაბრუნებული ღია ტრაფიკის თავიდან შიფრაცია და ქსელში გადაცემა. აღნიშნული ფუნქციონალის ფარგლებში, გადაწყვეტილებას უნდა შეეძლოს: - მაღალმდგრადობის რეჟიმის მხარდაჭერა; - გარედან შიდა, სერვერებზე მიმართული SSL ტრაფიკის მხარდაჭერა; - მომხმარებლებიდან, ინტერნეტში მიმავალი SSL ტრაფიკის მხარდაჭერა; - ტრანსპერენტული ე.წ Layer 1 რეჟიმის მხარდაჭერა; - მარშრუტიზაციის ე.წ Layer 3 რეჟიმის მხარდაჭერა; - რამოდენიმე სერვისულ მოწყობილობაზე, ტრაფიკის განაწილების სხვადასხვა რეჟიმების მხარდაჭერა, მათ შორის: - IP Source & IP Destination ჰეში - IP Source & IP Destination & Port ჰეში - Round Robin

	- დაყოვნების დამოკიდებული;
102	გადაწყვეტილებას უნდა შეეძლოს გეოგრაფიული ზონების მიხედვით პოლიტიკების შექმნა;
103	დამატებითი სავალდებულო მოთხოვნები NGFW– სთვის: - ერთზე მეტ ადმინისტრატორს უნდა შეეძლოს ერთდროულად კონფიგურაციის ცვლილება; - უსაფრთხოების პოლიტიკების აქტივაცია უნდა ხორციელდებოდეს, აქტივაციის ოპერაციის გამოძახების შემდეგ. აქტივაციის ოპერაცია უნდა იძლეოდეს შესაძლებლობას მოინიშნოს სპეციფიური ადმინისტრატორი, რომლის ცვლილებების აქტივაციაცაა საჭიროა, ან ყველა ადმინისტრატორის; - თითოეული აქტივაციის წინ, მოწყობილობა ავტომატურად უნდა ახორციელებდეს, მიმდინარე კონფგურაციის სარეზერვო ასლის შექმნას; - სარეზერვო ასლის პოლიტიკები უნდა აღდგეს და გააქტიურდეს გადატვირთვის აუცილებლობის გარეშე; - გადაწყვეტილებას უნდა გააჩნდეს უსაფრთხოების პოლიკების ოპტიმიზაციის ფუნქცია. რის ფარგლებშიც, უნდა მოხდეს ადმინისტრატორის შეტყობინება თუ პოლიტიკა დუბლირდება ან გადაიფარება უკვე არსებული პოლიტიკით; - ლოგების გადაცემა გარე სისტემებში შესაძლებელი უნდა იყოს SNMP ასევე syslog ის საშუალებით; - ლოგები უნდა ინახებოდეს ლოკალურად. ასევე უნდა არსებობდეს ლოგების გაგზავნის ცენტრალური მართვისა და მონიტორინგის სისტემაზე, მისი არსებობის შემთხვევაში; - შემოთავაზებულ სისტემას უნდა ჰქონდეს SSD ტიპის სისტემური დისკი, არანაკლებ 480 (ოთხას ოთხმოცი) გბაიტი ზომის. - მოწყობილობას უნდა ჰქონდეს შესაძლებლობა snmp და syslog ლოგების გადაცემის სპეციალურად განსაზღვრული ფილტრების გამოყენების საშუალებით; - გადაწყვეტილებას უნდა შეეძლოს ავტომატურად განაახლოს მავნე IP მისამართების სია სპეციალური სერვისის მეშვებობით და განახორციელოს მათი ბლოკვა; - გადაწყვეტილებას უნდა გააჩნდეს SYN Flood, UDP Flood, ICMP Flood უსაფრთხოების პოლიტიკების გამართვა, ზღვრული მნიშნველობების მითითებით; - გადაწყვეტილებას უნდა შეეძლოს TCP port scan, UDP Ports scan და sweep scan იდენტიფიცირება და ბლოკირება; - გადაწყვეტილება უნდა ეყრდნობოდეს ე.წ white list უსაფრთხოების მოდელს და გააჩნდეს მარტივი ინტერფეისი უსაფრთხოების პოლიტიკების სამართავად და რედაქტირებისთვის.

	- გადაწყვეტილებას უნდა შეეძლოს ე.წ portable executable ფაილების გადაცემა ღრუბლოვან Sanbox ში ანალიზისთვის. აღნიშნული ფუნქციონალი არ უნდა საჭიროებდეს დამატებით ლიცენზირებას;
104	გადაწყვეტილება აღჭურვილი უნდა იყოს მწარმოებლის 3 წლიანი მხარდაჭერით.
105	მომწოდებელმა უნდა წარმოადგინოს მწარმოებლის ავტორიზაციის წერილი (MAF)

14. B ტიპის კომუტატორი რაოდენობა 2 (ორი)

კომუტატორი უნდა იყოს ინდუსტრიული გარემოსთვის თავსებადი	
მოთხოვნები წარმადობის და აპარატურული უზრუნველყოფის მიმართ	
ფიზიკური ინტერფეისები	არანაკლებ 24 x 1/10 გბ/წმ SFP+ პორტი
მართვის ინტერფეისები	არანაკლებ 1 x Rj-45 კონსოლის პორტი არანაკლებ 2 x USB კონსოლის პორტი არანაკლებ 1 x 1-PPS დროის პორტი არანაკლებ 1 x Rj-45 მართვის პორტი
კომუტაციის წარმადობა	არანაკლებ 480 გბ/წმ არანაკლებ 360 მილიონი პაკეტი წამში
MAC მისამართების რაოდენობა	არანაკლებ 62,000
IPv4 მარშუტების რაოდენობა	არანაკლებ 22,000
ACL ჩანაწერების რაოდენობა	არანაკლებ 4000
STP	არანაკლებ 500
ოპერატიული მეხსიერება	არანაკლებ 16 გბ
Flash	არანაკლებ 16 გბ
VLAN IDs	არანაკლებ 4000
Rack Unit	1 RU
კომუტატორს უნდა გააჩნდეს 2 კვების ბლოკი. კომუტატორს უნდა გააჩნდეს არანაკლებ ოთხი გაგრილების მოდული	
მოთხოვნები პროგრამული უზრუნველყოფის, ტექნოლოგიების და ოქმების მიმართ:	
L2 კომუტაცია	• IEEE 802.1D • IEEE 802.1q • IEEE 802.1s • IEEE 802.1w • IEEE 802.3ad • IEEE 802.3ax

L2 multicast	• IGMPv1, v2, v3
L3 მარშუტიზაცია	• Static Route, RIP, PBR, OSPF, OSPFv3
კომუტატორს უნდა გააჩნდეს MLAG ჯგუფის ფორმირების მხარდაჭერა	
მომავალში მხოლოდ პროგრამული ლიცენზიის დამატებით, კომუტატორს უნდა გააჩნდეს შემდეგი ტექნოლოგიების მხარდაჭერა, მათ შორის:	
L3 მარშუტიზაცია	• EIGRP, HSRP, BGP
კომუტატორზე უნდა ვრცელდებოდეს მწარმოებლის სამ წლიანი საგარანტიო მომსახურეობა, ტექნიკური მხარდაჭერა და პროგრამული უზრუნველყოფის განახლება.მოწყობილობის დაზიანების მიზეზის დადგენის შემდეგ, მოწყობილობა უნდა შეკეთდეს ან შეცვალოს შემდეგ სამუშაო დღეს. **მომწოდებელმა უნდა წარმოადგინოს მწარმოებლის ავტორიზაციის წერილი (Manufacturers Authorization Form)** **მომწოდებელმა უნდა წარმოადგინოს გადაწყვეტილების მომწოდებლის კომპლექსური კორპორატიული ქსელების სპეციალიზაცია**	

15. ქსელური ტრანსივერები

ტრანსივერის ტიპი	რაოდენობა	არხის ტიპი
C ტიპის ტრანსივერი	6	1GBASE-T
D ტიპის ტრანსივერი	10	10GB SR
E ტიპის ტრანსივერი	20	10GB Copper Passive Cable 1 Meter

დამატებითი მოთხოვნები (I და II ეტაპი)

1. მომწოდებელმა კომპანიამ უნდა განახორციელოს გადაწყვეტილების სრული ინტეგრაცია.
2. პრეტენდენტს კომპანიას A, B და C ტიპის კომუტატორებზე და A, B ტიპის უსადენო წვდომის წერტილებზე და A ტიპის უსადენო წვდომის წერტილის კონტროლერზე უნდა გააჩნდეს შემოთავაზებული ტექნოლოგიების (ქსელური ინფრასტრუქტურის და კომპლექსური უსაფრთხოები) სპეციალიზაცია, რაც უნდა დასტურდებოდეს შემოთავაზებული პროდუქციის მწარმოებლის მიერ გაცემული წერილით.
3. მოწოდებული საქონელი (მისი ყველა კომპონენტი) უნდა იყოს ახალი (არ უნდა იყოს მეორადი გამოყენების);

4. ჰიპერ-კონვერგენტული ინფრასტრუქტურის კრიტიკულობიდან გამომდინარე, პრეტენდენტს კომპანიას შტატში უნდა გააჩნდეს მინიმუმ ერთი მწარმოებლის მიერ სერთიფიცირებული ინჟინერი.
5. ჰიპერ-კონვერგენტული ინფრასტრუქტურის კრიტიკულობიდან გამომდინარე, პრეტენდენტ კომპანიას უნდა გააჩნდეს მინიმუმ ერთი წარმატებულად დასრულებული პროექტი საქართველოს ტერიტორიაზე. პრეტენდენტმა გამოცდილების დასადასტურებლად უნდა წარმოადგინოს შესაბამისი დოკუმენტაცია.