# მოთხოვნები ბრანდმაუერის მიმართ (ორი ცალი)

ბრანდმაუერს უნდა გააჩნდეს შემდეგი ტექნიკური მახასიათებლები:

1. ბრანდმაუერის მაქსიმალური წარმადობა: არანაკლებ 10გბ/წმ
2. ერთდროული სესიების რაოდენობა: არანაკლებ 2 მილიონი
3. კავშირების დამყარების სისწრაფე: არანაკლებ 40000 კავშირი/წამში
4. 3DES/AES შიფრაციის წარმადობა: არანაკლებ 1 გბ/წმ
5. IPSec VPN სესიების მაქსიმალური რაოდენობა: არანაკლებ 7500
6. VLAN ების მაქსიმალური რაოდენობა: არანაკლებ 100
7. ბრანდმაუერს უნდა გააჩნდეს A/S და A/A მაღალმდგრადობის რეჟიმებში მუშაობის მხარდაჭერა.
8. ინტერფეისების რაოდენობა არანაკლებ 12(თორმეტი) 1გბ/წმ, დამატებით 1(ერთი) 10/100/1000მბ/წმ წარმადობის მენეჯმენტ პორტი. 4 (ოთხი) x 1/10გბ SFP ფორმ ფაქტორის პორტი.
9. ბრანდმაუერს უნდა გააჩნდეს შემდეგი ტექნოლოგიებისა და ოქმების მხარდაჭერა: SSH, SNMP, RADIUS, CoA, TACACS+, NAT, IKEv1, IKEv2, EIGRP, OSPFv2, OSPFv3, OSPFv2 and OSPFv3 NSF, BGP, BGP NSF
10. ბრანდმაუერში შესაძლებელი უნდა იყოს ე.წ “Context” ქვე ვირტუალური ბრანდმაუერების შექმნა. ბრანდმაუერს უნდა გააჩნდეს არანაკლებ 2(ორი) ვირტუალური ბრანდმაუერის შექმნის შესაძლებლობა. მომავალში შესაბამისი ლიცენზიის დამატებით შესაძლებელი უნდა იყოს არანაკლებ 30(ოცდაათი) ვირტუალური ბრანდმაუერის გააქტიურება
11. ბრანდმაუერს უნდა მოყვებოდეს 1500(ათას ხუთასი) აქტიური VPN კლიენტის ლიცენზია 5 წლის ვადით.
12. არაუმეტეს: 1 RU ზომის
13. კვება: AC ტიპის
14. მწარმოებლის ერთ წლიანი მხარდაჭერა. მოწყობილობის დაზიანების მიზეზის დადგენის შემდეგ, მოწყობილობის შეცვლა შემდეგ სამუშაო დღეს
15. **მომწოდებელმა უნდა წარმოადგინოს მწარმოებლის ავტორიზაციის წერილი (Manufacturers Authorization Form)**

# აუტენთიფიკაციის და ავტორიზაციის სერვერი

ტექნიკური მოთხოვნები:

1. სისტემას უნდა გააჩნდეს RADIUS პროტოკოლი ფუნქიონალი, authentication, authorization და accounting მხარდაჭერით.
2. სისტემას უნდა გააჩნდეს გარე აუტენტიფიკაციის ბაზის მხარდაჭერა, რომელიც ბაზირებულია MS AD ის შემდეგ ოპერაციულ სისტემებზე:
* Microsoft Windows Active Directory 2003
* Microsoft Windows Active Directory 2003 R2
* Microsoft Windows Active Directory 2008
* Microsoft Windows Active Directory 2008 R2
* Microsoft Windows Active Directory 2012
* Microsoft Windows Active Directory 2012 R2
* Microsoft Windows Active Directory 2016
1. სისტემას უნდა გააჩნდეს გარე აუტენტიფიკაციის ბაზის მხარდაჭერა, რომელიც ბაზირებულია LDAP სერვერებზე:
* SunONE LDAP Directory Server
* OpenLDAP Directory Server
1. სისტემას უნდა გააჩნდეს გარე აუტენტიფიკაციის ბაზის მხარდაჭერა, რომელიც ბაზირებულია Token სერვერებზე:
* RSA ACE/Server
* RSA Authentication Manager
* ნებისმიერი გარე RADIUS სერვერი რომელიც თავსებადია RFC 2865
1. სისტემას უნდა გააჩნდეს გარე აუტენტიფიკაციის ბაზის Security Assertion Markup Language (SAML) Single Sign-On (SSO) მხარდაჭერა:
* Microsoft Azure
* Oracle Access Manager (OAM)
* Oracle Identity Federation (OIF)
* PingFederate Server
* PingOne Cloud
* Secure Auth
* SAMLv2 სთან თავსებადი ნებისმიერი პროვაიდერი
1. სისტემას უნდა გააჩნდეს გარე აუტენტიფიკაციის ბაზის Open Database Connectivity (ODBC) მხარდაჭერა:
* Microsoft SQL Server
* Oracle
* PostgreSQL
* Sybase
* MySQL
1. სისტემას უნდა გააჩნდეს გარე აუტენტიფიკაციის ბაზის მხარდაჭერა, რომელიც ბაზირებულია Facebook სოციალურ ქსელზე, სტუმრების აუტენტიფიკაციისთვის.
2. სისტემას უნდა გააჩნდეს RADIUS პროტოკოლის მხარდაჭერა, რათა უზრუნველყოს ქსელში წვდომის მხარდაჭერა, მათ შორის შემდეგი სტანდარტების:
	* RFC 2138—Remote Authentication Dial In User Service (RADIUS)
	* RFC 2139—RADIUS Accounting
	* RFC 2865—Remote Authentication Dial In User Service (RADIUS)
	* RFC 2866—RADIUS Accounting
	* RFC 2867—RADIUS Accounting Modifications for Tunnel Protocol Support
	* RFC 5176—Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)
3. სისტემას უნდა გააჩნდეს TACACS+ პროტოკოლის და აუტენტიფიკაციისა, ავტორიზაციის და აღრიცხვის სერვისების მხარდაჭერა, რათა განახორციელოს ადმინისტრატორების კონტროლი ქსელურ მოწყობილობებზე წვდომის დროს.
4. სისტემის გამართვა შესაძლებელი უნდა იყოს როგორც სპეციალიზირებულ აპარატურულ ე.წ appliance, ასევე ვირტუალურ გარემოში. შემდეგი ვირტუალიზაციის პლატფორმების მხარდაჭერა:
	* Vware ESXi 5. x, 6. x
	* KVM ბაზირებული RHEL 7.0 და Ubuntu 14.04 LTS
	* Microsoft Hyper-V ის არაუგვიანეს Microsoft Windows Server 2012 R2
5. სისტემას უნდა გააჩნდეს შემდეგი აუთენთიკაციის პროტოკოლების მხარდაჭერა: PAP, PEAP, MS-CHAPv1, MS-CHAPv2, EAP-MD5, EAP-TLS, EAP-FAST, EAP-TTLS, PEAP-TLS, EAP-GTC, EAP-Chaining
6. სისტემაზე შესაძლებელი უნდა იყოს დაშვების წესების შექმნა შემდეგი ატრიბუტების მიხედვით: მომხმარებელი, მოწყობილობა, ლოკაცია, აუთენთიკაციის პროტოკოლი, მოწყობილობის უსაფრთხოების მდგომარეობა.
7. სისტემას უნდა გააჩნდეს RestAPI ინტერფეისი, გარე ფუნქციების რეალიზაციისთვის.
8. სისტემას უნდა გააჩნდეს სტანდარტიზირებული პროგრამული ინტერფეისი, რომლითაც განახოერციელებს ინტეგრაციას სხვადასხვა მწარმოებლების უსაფრთხოების კომპონენტებთან. აღნიშნული ინტერფეისის საშუალებით სისტემას უნდა შეეძლოს გადასცეს კონტექსტური ინფორმაცია ქსელზე მიერთებული საბოლოო წერტილების შესახებ. ასევე შესაძლებელი უნდა იყოს აღნიშნული ინტერფეისის საშუალებით მიიღოს ინფორმაცია გარე უსაფრთხოების კომპონენტებისაგან, რათა გაზარდოს კონტექსტუალური ინფორმაციის რაოდენობა.
	* სისტემას უნდა შეეძლოს ქსელური უსაფრთხოების მონიტორინგის სისტემასთან ინტეგრაცია. ინტეგრაციის ფარგლებში, შესაძლებელი უნდა იყოს, ქსელური უსაფრთხოების მონიტორინგის სისტემიდან, საბოლოო მოხმარებლების ავტორიზაციის შესახებ ბრძანებების მიღება, რათა განხორციელდეს ინფიცირებული მომხმარებლების კარანტინი.
	* სისტემას უნდა შეეძლოს მიაწოდოს კონტექსტუალური ინფრომაცია ქსელური უსაფრთხოების მონიტორინგის სისტემას, რათა ცენტრალიზირებულ პანელზე მოხდეს მომხმარებლების ინფორმაციის ასახვა შესაბამის ნაკადებსა და ინციდენტებთან ერთად. მიწოდებული ინფორმაცია, უნდა შეიცავდეს არანაკლებ შემდეგ პარამეტრებს: macaddress, ipAddress, username, securityGroup, vlan, domainName, interfaceDeviceip, lastActiveTime,
	interfaceDevicePortId.
9. შემდეგი აუტენტიფიკაციის მეთოდების მხარდაჭერა:
	* ცენტრალიზირებული WEB აუტენტიფიკაცია, კონფიგურირებადი ფუნქციონალური პორტალების საშუალებით
	* MAB (MAC Authentication Bypass) აუტენტიფიკაცია
	* 802.1x აუტენტიფიკაცია
10. შემდეგი ოპერაციული სისტემების მხარდაჭერა, საბოლოო მომხმარებლების სისტემებზე საპლიკანტების 802.1х (Device Provisioning) ავტომატური კონფიგურირებისათვის:
* Google Android 2.2.x/2.3.x/3.x/4.x/5.x/6.x/7.x
* Apple iOS 5.x/6.x/7.x/8.x/9.x/10.x/11
* Apple MAC OS X 10.9/10.10/10.11/10.12
* Microsoft Windows 7/7x64/8/8x64/8.1/10
* Google ChromeBook
1. სისტემას უნდა გააჩნდეს, მოქნილი, წყობილი პოლიტიკების რეალიზაციის შესაძლებლობა, რათა მარტივად იყოს შესაძლებელი კრიტერიების კომბინაციების აღწერა, ავტორზაციის სესიების საბოლოო შედეგის განსაზღვრისთვის.
2. სისტემას უნდა გააჩნდეს შემდეგი ავტორიზაციის წვდომების მხარდაჭერა:
	* შესაბამისი RADIUS ატრიბუტების განსაზღვრა ლოკალური ბიბლიოთეკიდან
	* VLAN განსაზღვრა
	* ACL ის სახელის განსაზღვრა, რათა მიღებული იქნეს შესაბამის მოწყობილობების მიერთების ინტერფეისებზე
	* dACL ის განსაზღვრა (სერვერიდან ჩამოტვირთვით)
	* ACL ის სახელის განსაზღვრა, რათა მითითებული იქნეს ტრაფიკი რომლის გადამისამართებაც განხორციელდება URL Redirect მიხედვით
	* URL ის განსაზღვრა, რომელზეც განხორციელდება URL Redirect
	* Voice VLANის განსაზღვრა
	* კომუტატორზე პორტის პროფილის კონფიგურაციის განსაზღვრა
3. გამოყენებული RADIUS ატრიბუტები, აუტენტიფიკაციის მეთოდის განსასაზღვრელად ავტომატურად უნდა განისაზღვროს, NAD მწარმოებლის მიხედვით და შეესაბამებოდეს სისტემაში არსებულ თანდაყოლილ NAD პროფილებს.
4. შემდეგი მწარმოებლების, NAD მოწყობილობების პროფილების არსებობა:
	* Alcatel Wired
	* Aruba Wireless
	* Brocade Wired
	* Cisco
	* HP Wired
	* HP Wireless
	* Motorolla Wireless
	* Ruckus Wireless
5. სისტემას უნდა გააჩნდეს პროფილირების ფუნქციონალი. რის ფარგლებშიც სისტემას უნდა შეეძლოს ავტომატურად განახორციელოს ქსელზე მიერთებული მოწყობილობების მოდელების და ტიპების ამოცნობა, მათ შორის ოპერაციული სისტემების, როგორიცაა სამუშაო კომპიუტერებე, ნოუთბუქები, მობილური მოწყობილობები, IP ტელეფონები, ვიდეო კონფერენციის სისტემები, ვიდეო კამერები, პრინტერები და ასე შემდეგ. აღნიშნული ინფორმაციის დადგენა შესაძლებელი უნდა იყოს შიდა დინამიური ბაზის მიხედვით. რომელიც აწყობილია კომპლექსური მეტრიკებისა და პროფილების მიხედვიდ და პერიოდულად ნახლდება.
6. პროფილირების ფუნქციას უნდა შეეძლოს მიერთებული მოწყობილობის პროფილის დადგება, შემდეგი წყაროების მიხედვით:
	* Netflow Protocol
	* DHCP
	* HTTP
	* RADIUS
	* NMAP Scan
	* DNS
	* SNMP Trap/Query
	* Active Directory Probe
	* CDP/LLDP
7. პროფილირების ფუნქციონალის ფარგლებში ადმინისტრატორს უნდა შეეძლოს საკუთადი მოწყობილობების პროფილების შედგენა, მათ შორის პროფილების ლოგიკური ჯგუფების.
8. ავტორიზაციის პოლიტიკებს განსაზღვრა შესაძლებელი უნდა იყოს კომპლექსური, წყობილი, ბულური ლოგიკის მიხედვით და მოიცავდეს შემდეგ კრიტერიუმებს:
	* მომხმარებლის/ჯგუფის სახელი
	* მოწყობილობის ტიპი/მოდელი/ოპერაციული
	* ქსელში დაშვების ტიპი სადენიანი/უსადენო/VPN
	* დაშვების დრო
	* სერტიფიკატების პარამეტრები
	* ადგილდებარეობის პარამეტრები, NAD ზე მიბმა, მის ჯგუფზე და ატრიბუტებზე
	* საბოლოო წერტილის მდგომარეობის პარამეტრები
	* მომხმარებლის/მოწყობილობის აუტენტიფიკაციის პარამეტრები
9. სისტემას უნდა შეეძლოს უზრუნველყოს როლებზე დაფუქნებული წვდომა სტუმრებისთვის:
	* სხვადასხვა სტუმრების WEB პორტალების შექმნა
	* ინტეგრირებული ხელსაწყოს არსებობა, რათა შესაძლებელი იყოს პორტალების დიზაინის ცვლილება სხვადასხვა პლატფორმებისთვის მობილური/კომპიუტერი
	* სტუმარი მომხმარებლების სხვადასხვა როლების შექმნა
	* სისტემაში შესვლის პოლიტიკების და პაროლების შექმენა სტუმრებისთვის
	* უზრუნველყოს სტუმრის ლოგინის გაცემა SMS/Email/Print ის საშუალებით
	* სოციალუ ქსელებთან ინტეგრაციის შესაძლებლობა OAuth ის საშუალებით
	* სპონსორების სხვადასხვა როლების შექმნა, შესაბამისის სტუმრების ავტორიზაციების პოლიტიკებთან მიბმით
10. სტუმრების ქსელში დაშვების სერვისის ფარგლებში, სისტემას უნდა გააჩნდეს შემდეგი მეთოდების მხარდაჭერა:
	* Hotspot
	* სპონსორის მიერ გაცემული ანგარიში
	* სტუმრის მიერ პირადათ დარეგისტრირებული ანგარიში, რომელიც დამოწმებულია სპონსორის მიერ
	* სტუმრის მიერ პირადათ დარეგისტრირებული ანგარიში
	* სტუმრის მიერ პირადათ დარეგისტრირებული ანგარიში, რომელიც ინტეგრირებულია სოციალური ქსელის საშუალებით
	* ქსელში დაშვება წინასწარ განსაზღვრული კოდის (Access Code) საშუალებით
11. ინტეგრირებული CA სერვერი, PKI ინფრასტრუქტურის გასამართად BYOD სცენარებისათვის. რათა შესაძლებელი იყოს კლიენტური მოწყობილობებისთვის სერტიფიკატების გაცემა. ასევე სერტიფიკატების განსაზღვრა API სთვის, კონტექსტის გაცვლისთვის.
12. სისტემას უნდა შეეძლოს გამართოს საბოლოო მომხმარებლის 802.1Х საპლიკანტი, ცენტრალიზირებულად განსაზღვრული შაბლონის საშუალებით, შიდა CA დან დაგენირირებული სერტიფიკატით, ან კორპორატიული CA დან PKI ინფრასტრუქტურის გამოყენების საშუალებითა და SCEP-Proxy ფუნქციონალით.
13. სისტემას უნდა გააჩნდეს ქსელზე მიერთული მოწყობილობების უსაფრთხოების დონის შემოწმების შესაძლებლობა. შემოწმება შესაძლებელი უნდა იყოს ორი საშუალებით, მათ შორის პერმანენტული და დროებითი აგენტით. დროებითი აგენტის გაშვება არ უნდა საჭიროებდეს ადმინისტრატორის უფლებას. დროექბით და პერმენეტულ აგენს უნდა გააჩნდეს ერთნერი შემოწმების კრიტერიუმების მხარდაჭერა. პერმანენტულ აგენტი უნდა მუშაობდეს, გრაფიკული ინტერფეისის ასახვის გარეშე.
14. უსაფრთხოების დონის შემოწმების ფარგლებში, შესაძლებელი უნდა იყოს სხვადასხვა ტიპის შემოწმების კატეგორიების განსაზღვრა:
	* აუცილებელი შემოწმებები
	* ოპციონალური შემოწმებები
	* აუდიტის შემოწმებები
15. უსაფრთხოების დონის შემოწმების ფარგლებში, სისტემას უნდა გააჩნდეს შემდეგი ტიპის შემოწმებების მხარდაჭერა:
	* ოპერაციულ სისტემაზე პაჩების არსებობა
	* საბოლოო წერტილებზე ხვრელების არსებობა, აღნიშნული ინფორმაციის მიღების შესაძლებლობა გარე სკანერებთან ინტეგრაციით, მათ შორის (Rapid 7, Qualys, Tenable)
	* ოპერაციული სისტემის რეესტრში, შესაბამისის ჩანაწერების არსებობა
	* ფაილური ატრიბუტების შემოწმების შესაძლებლობა
	* დაინსტალირებული პროგრამების შემოწმება
	* დაინსტალირებული ანტივირუსის შემოწმება, მისი ვერსიის და განახლებების
	* ლოკალური ფაირვოლის მუშაობის შემოწმება
	* დისკის შიფრაციის შემოწმება
	* MDM/EDM ატრიბუტების შემოწმება
	* USB დამგროვებლის აღმოჩენა
	* გაშვებული და შეჩერებული სერვისების შემოწმება
	* მიერთებული მოწყობილობების აპარატურული მახასიეთებლების ამოცნობა:
		1. BIOS S/N
		2. Number of CPU
		3. CPU Utilization
		4. Number of HDD
		5. HDD Utilization
16. უსაფრთხოების დონის შემოწმების ფარგლებში, შესაძლებელი უნდა იყოს დონის ჩასწორება როგორც ხელით ასევე ავტომატურად.
17. შემდეგი უსაფრთხოების დონის შესწორების, ვარიანტების მხარდაჭერა:
	* ოპერაციული სისტემის განახლების პროცედურის გამოძახება
	* ანტივირუსის განახლების პროცედურის გამოძახება
	* პროგრამის წაშლა ხოსტიდან
	* გაშვებული პროცესის გამორთვა
	* გარკვეული პროგრამის გაშვება
	* ტექსტური გზავნილის ასახვა
	* ბრმულის ასახვა
	* ფაილის ასახვა
	* ლოკალური ბრანდმაუერის ჩართვა
18. გადაწყვეტილებას უნდა გააჩნდეს, უსაფრთხობის ჯგუფზე დაფუძნებული ქსელში ავტორიზაციის მეთოდის მხარდაჭერა. უსაფრთხოების ჯგუფების განსაზღვრა შესაძლებელი უნდა იყოს ცენტრალიზირებულად, მოცემული გადაწყვეტილების საშუალებით. უსაფრთხოების ჯგუფების რაოდენობა არანაკლებ 65535, შესაძლებელი უნდა იყოს თვითოეულს ჯგუფს განესაზღვროს აღწერილობა. გადაწყვეტილებას უნდა შეეძლოს ქსელური ინფრასტრუქტურის მოწყობილობებს შორის, ნდობითი დამოკიდებულებების ჩამოყალიბება, მათი აუტენტიფიკაცია EAP-FAST პროტოკოლის საშუალებით, შემდგომი PAC (Protected Access Credentials) ის გაცემით, რითიც განხორციელდება ქსელური მოწყობილობების ურთიერთ აუტენტიფიკაცია, რათა გაიცვალოს მონაცემები საბოლოო მოწყობილობების ავტორიზაციის შესახებ, უსაფრთხოების ჯგუფების საშუალებით. ქსელური ინფრასტრუქტურის მოწყობილობებს შორის ნდობითი დამოკიდებულებების ფარგლებში, უსაფრთხოების ჯგუფების ინფრომაციის მიმოცვლა, ტეგების სახით Ethernet ფრეიმებში და ოპციონალურად კონფიდენციალური არხების გამართვა კომუტატორებს შორის MACSEC ტექნოლოგიის საშუალებით.
19. გადაწყვეტილებას უნდა გააჩნდეს შესაძლებლობა განსაზღვროს უსაფრთხობის ჯგუფები მომხმარებლებისათვის, RADIUS ოქმის საშუალებით ავტორიზაციის ეტაპზე. ასევე შესაძლებელი უნდა იყოს, აქტიური უსაფრთხობის ჯგუფებისა და მათთან ასოცირებული IP ქვექსელების ინფორმაციის მიმოცვლა განახორციელოს, ქსელური ინფრასტრუქტურის კომპონენტაბთან, SXP ოქმის საშუალებით. რათა ქსელურ მოწყობილობებზე განხორციელდეს ტრაფიკის ფილტრაცია.
20. გადაწყვეტილების საშუალებით, შესაძლებელი უნდა იყოს, ცენტრალიზირებულად მატრიცაზე დაფუძნებული ფილტრაციის პოლიტიკების ფორმირება, სისტემაში არსებული ყველა უსაფრთხოების ჯგუფის შორის. მატრიცაში განსაზღვრული პოლიტიკები ავტომატურად უნდა ვრცელდებდეს ყველა, იმ ქსელურ ინფრასტრუქტურის კომპონენტზე, სადაც ფიგურირებენ შესაბამისი უსაფრთხოების ჯგუფებში შემავალი რესურსები. მატრიცაში აღწერილი პოლიტიკები არ უნდა იყოს დაფუძნებული IP მისამართებსა და IP ქვექსელებზე. არამედ ლოგიკურ უსაფრთხოების ჯგუფებზე და ამ ჯგუფებს შორის დაშვებებზე.
21. გადაწყვეტილებაზე ერთდროულად შესაძლებელი უნდა იყოს, რამოდენიმე ერთმანეთისგან განსხვავებული უსაფრთხოების მატრიცის განსაზღვრა. სურვილისამებრ შესაძლებელი უნდა იყოს, საჭირო მატრიცის გააქტიურება, რაც გამოიწვევს, აქტიური მატრიცაში აღწერილი ფილტრაციის პოლიტიკების მინიჭებას, ყველა საჭირო ქსელურ კომპონენტებზე Radius COA საშუალებით. ერთი მარტრიციდან მეორეზე, გადართვა უნდა ხორციელდებოდეს ცენტრალიზირებულად, ინტერფეისიდან მარტივად გადართვის საშუალებით.
22. სერვერს უნდა შეეძლოს დაშვების ატრიბუტების შექმნა დინამიურად, შემდგომ მათი შენახვის და გამოყენების მიზნით.
23. სერვერს უნდა გააჩნდეს შემდეგი დაშვების კონტროლის მექანიზმების მხარდაჭერა: Downloadable access-list(dACL), Vlan assignment, URL redirection, named ACLs and Security Group(SGs)
24. სერვერს უნდა გააჩნდეს Security group tag exchange (SXP) პროტოკოლის მხარდაჭერა.
25. სერვერს უნდა გააჩნდეს ჩაშენებული პროფილები შემდეგი მოწყობილობებისთვის (Device profiling): IP phones, Printers, IP cameras, smartphones, tablets. პროფილების მეშვეობით უნდა ხორციელდებოდეს ქსელში მიერთებულ მომხმარებლების მოწყობილობების (endpoint) დინამიური იდენტიფიკაცია და პლასიფიკაცია.
26. სერვერს უნდა გააჩნდეს თვითმომსახურების WEB პორტალის ფუნქციონალი, რათა მომხმარებლებმა განახორციელონ თავიანთი საკუთარი მოწყობილობების რეგისტრაცია, სერტიფიკატების და კორპორატიული პროგრამული უზრუნველყოფის ინსტალაციის შესაძლებლობით.
27. სერვერს უნდა გააჩნდეს ჩაშენებულ Guest პორტალი , როგორც მომხმარებლების თვითმომსახურების(self-service) აგრეთვე Sponsored Access ფუნქციონალის მხარდაჭერით.
28. დამატებითი ლიცენზიის შეძენის შემთხვევაში სერვერს უნდა გააჩნდეს Endpoint Posture check პოლიტიკების მხარდაჭერა, რომ მოხდეს მომხმარებლების მოწყობილობების შემოწმება და წვდომების განსაზღვდა შემდეგი კრიტერიუმების მოხედვით: latest OS patch, antivirus and antispyware packages with current definition file variables (version, date), antimalware packages, registry settings (key, value),patch management, disk encryption, mobile PIN-lock or rooted or jailbroken status, application presence, and USB -attached media.
29. დამატებითი ლიცენზიის შეძენის შემთხვევაში სერვერს უნდა გააჩნდეს ინტეგრაციის მხარდაჭერა mobile device management (MDM/EMM) გადაწყვეტილებებთან, არანაკლებ 4 მწარმოებლის.
30. სერვერი უნდა იმართებოდეს ჩაშენებული ცენტრალიზებული web based GUI კონსოლის მეშვეობით. Web ინტერფეისიდან უნდა მიმდინარეობდეს დაშვების პროფილების, უსაფრთხოების მდგომარეობის, სტუმრების დაშვების, აუტენტიფიკაციისა და ავტორიზაციის სერვისების კონფიგურაცია.
31. სერვერს უნდა გააჩნდეს ჩაშენებული web-კონსოლი მონიტორიგისთვის და დიაგნოსტიკისთვის. უნდა გააჩნდეს მომხმარებლების და მათი მოწყობილობების შესახებს მიმდინარე და ისტორიული მონაცემების ნახვის საშუალება, ასევე ინფორმაციის ატრიბუტების შესახებ.
32. სერვერს უნდა გააჩნდეს ინტეგრაციის მხარდაჭერა შემდეგ სისტემებთან: Microsoft Active Directory, LDAP, RSA SecurID(OTP) და Open Database Connectivity (ODBC).
33. სერვერს უნდა გააჩნდეს ინტეგრაციის მხარდაჭერა არანაკლებს 50(ორმოცდაათი) Microsoft Active Directory სისტემასთან two-way trust მიერთებების გარეშე.
34. სერვერს უნდა გააჩნდეს სხვა სისტემებთან ინტეგრაციის მხარდაჭერა API-ს მეშვეობით.
35. სერვერს უნდა გააჩნდეს ჩაშენებული სერტიფიკაციის ცენტრი (Certificate Authority). სერვერს უნდა შეეძლოს მუშაობა როგორც დამოუკიდებელ სერტიფიკაციის ცენტრს ან უკვე არსებული სერტიფიკაციის ცენტრის დაქვემდებარებაში მუშაობა.
36. უნდა გააჩნდეს NTP პროტოკოლის მხარდაჭერა, აუტენტიფიკაციის გასაღებების საშუალებით.
37. სერვერს უნდა გააჩნდეს პორტალის მხარდაჭრა, რომლის საშუალებითაც მომხმარებლები განახორციელებენ საკუთარი მოწყობილობების რეგისტრაციას და მათ კონფიგურაციას.
38. სერვერი უნდა უზრუნველყოფდეს სერვისს, რომლის საშუალებითაც შესაძლებელი იქნება მოწყობილობის ავტორიზაციის ცვლილება, ისე რომ არ მოხდეს საერთო ავტორიზაციის პოლიტიკაში ცვლილების განხორციელება.
39. სერვერს უნდა შეეძლოს ინტეგრაცია PxGrid ტექნოლოგიის საშუალებით სხვადასხვა ტიპის ქსელური უსაფრთხოების კომპონენტაბთან, რათა განახორციელოს ინციდენტების ღრმა ანალიზი და კორელაცია.
40. სერვერის ინსტალაცია შესაძლებელი უნდა იყოს არსებულ VMware ESXi ინფრასტრუქტურაში.
41. სისტემა არქიტექტურულად მზად უნდა იყოს, დიდი ზომის ქსელებში დანერგვაში. არანაკლებ 500 000 საბოლოო მომხმარებლის ზომით.
42. გადაწყვეტილებას უნდა გააჩნდეს კლასტერირების მხარდაჭერა. ასევე მხარდაჭერილი უნდა იყოს კლასტერის წევრების გატანა, გეოგრაფიულად მოშორებულ მანძილზე. კლასტერის წევრებს შორისმ დაყოვნება არანალკედ 300მწ.
43. შესაძლებელი უნდა იყოს გადაწყვეტილების განაწილებულ რეჟიმში გამართვა. რომლის ფარგლებშიც, სხვადასხვა ვირტუალ მანქანებეზე მოხდება ისეთი როლების გატანა, როგორებიცაა ადმინისტრაციული, მონიტორინგის და პოლიტიკის. ასევე შესაძლებელი უნდა იყოს ერთ ვირტუალ მანქანეზე მოხდეს ადმინისტრაციული დამონიტორინგის როლების შეთავსება, ხოლო პოლიტიკების როლის გატანა ცელკე ვირტუალურ მანქანაზე.
44. შემოთავაზებული სპეციფიკაცია უნდა ითვალისწინებდეს:
	* 1 ცალ ვირტუალურ მანქანას
	* არანაკლებ 1500 საბოლოო წერტილის ლიცეინზია
	* შემოთავაზებული ლიცენზიევმა უნდა უზრუნველყონ შემდეგ აქტიური ფუნქციონალი:
		1. Basic RADIUS authentication, authorization, and accounting, including 802.1x, MAC Authentication Bypass. Wired/Wireless/VPN
		2. Web authentication (local, central, device registration)
		3. MACsec
		4. SSO, SAML, ODBC–based authentication
		5. Guest portal and sponsor services
		6. უსაფრთხოების ჯგუფები
		7. TACACS+ ოქმი
45. გადაწყვეტილება აღჭურვილი უნდა იყოს არანაკლებ 1 წლიანი მწარმოებლის მხარდაჭერით, მათ შორის პროგრამული განახლებით;
46. **მომწოდებელმა უნდა წარმოადგინოს მწარმოებლის ავტორიზაციის წერილი (Manufacturers Authorization Form),**

## დამატებითი მოთხოვნები

* ყველა შემოთავაზებული კომპონენტი უნდა იყოს ერთი და იგივე მწარმოებლის
* შემოთავაზება უნდა ითვალისწინებდეს შემოთავაზებული პროდუქტების დანერგვას და ინტეგრაციას