## A ტიპის ბრანდმაუერი 2(ორი ცალი)

ბრანდმაუერს უნდა გააჩნდეს შემდეგი ტექნიკური მახასიათებლები:

1. ბრანდმაუერის მაქსიმალური FW(Firewall Layer1-4)+AVC (Application Visibility and Control) 1024B წარმადობა: არანაკლებ 12გბ/წმ
2. ბრანდმაუერის მაქსიმალური FW+AVC+IPS(Intrusion Prevention System) წარმადობა: არანაკლებ 10გბ/წმ
3. ერთდროული სესიების რაოდენობა: არანაკლებ 9 მილიონი (with AVC)
4. კავშირების დამყარების სისწრაფე: არანაკლებ 68000 კავშირი/წამში (with AVC)
5. IPsec VPN შიფრაციის წარმადობა: არანაკლებ 6 გბ/წმ (1024B TCP w/Fastpath)
6. IPSec VPN სესიების მაქსიმალური რაოდენობა: არანაკლებ 10000
7. VLAN ების მაქსიმალური რაოდენობა: არანაკლებ 1024
8. ინტერფეისების რაოდენობა: არანაკლებ 8(რვა) 10 გბ/წმ ინტერფეისი(SFP+ ტიპის). დამატებით 1(ერთი) 1გბ/წმ წარმადობის (RJ-45 და SFP) მენეჯმენტ პორტი.
9. ქსელური მოდულის სლოტების რაოდენობა: არანაკლებ 2(ორი) Network Module სლოტი
10. დამატებითი ქსელური მოდულების საშუალებით პორტების რაოდენობა უნდა იყოს არანაკლებ 24(ოცდაოთხი) 10გბ/წმ ინტერფეისი (SFP+ ტიპის) ან 8(რვა) 40გბ/წმ ინტერფეისი (QSFP+ ტიპის)
11. Application Visibility and Control აპლიკაციების მხარდაჭერა: არანაკლებ 4000
12. მაღალი მდგრადობის მხარდაჭერა: Active/Standby
13. კლასტერიზაციის მხარდაჭერა: არანალებ 6(ექვსი) ერთეული
14. ბრანდმაუერს უნდა გააჩნდეს შემდეგი ტექნოლოგიებისა და ოქმების მხარდაჭერა: SSH, SNMP, RADIUS, NAT, IPsec, IKEv2, EIGRP(using FlexConfig), OSPF, BGP, PxGrid.
15. ბრანდამაუერს უნდა მოყვებოდეს შესაბამისი 1(ერთი) წლიანი ლიცენზია Intrusion Prevention System(IPS) მხარდაჭერისთვის
16. დამატებითი ლიცენზიების საშუალებით ბრანდმაუერს უნდა ქონდეს URL კატეგორიების ფილტრაციის საშუალება
17. დამატებითი ლიცენზიების საშუალებით ბრანდმაუერს უნდა ქონდეს Advance Malware Protection(AMP) და Cloud Sandboxing მხარდაჭერა
18. არაუმეტეს: 1 RU ზომის
19. ბრანდმაურს უნდა მოყვებოდეს 5(ხუთი) მეტრიანიანი 10(ათი) ცალი SFP+ Twinax Copper კაბელი.
20. კვება: AC ტიპის
21. ბრანდმაუერს უნდა მოყვებოდეს 2(ორი) ცალი კვების ბლოკი
22. ბრანდმაუერზე უნდა ვრცელდებოდეს მწარმოებლის ერთ წლიანი საგარანტიო მომსახურეობა, ტექნიკური მხარდაჭერა და პროგრამული უზრუნველყოფის განახლება. მოწყობილობის დაზიანების მიზეზის დადგენის შემდეგ, მოწყობილობა უნდა შეკეთდეს ან შეცვალოს შემდეგ სამუშაო დღეს.

## B ტიპის ბრანდმაუერი 2(ორი ცალი)

ბრანდმაუერს უნდა გააჩნდეს შემდეგი ტექნიკური მახასიათებლები:

1. ბრანდმაუერის მაქსიმალური FW(Firewall Layer1-4)+AVC (Application Visibility and Control) 1024B წარმადობა: არანაკლებ 4.75გბ/წმ
2. ბრანდმაუერის მაქსიმალური FW+AVC+IPS(Intrusion Prevention System) წარმადობა: არანაკლებ 4.75გბ/წმ
3. ერთდროული სესიების რაოდენობა: არანაკლებ 2 მილიონი (with AVC)
4. კავშირების დამყარების სისწრაფე: არანაკლებ 24000 კავშირი/წამში (with AVC)
5. IPsec VPN შიფრაციის წარმადობა: არანაკლებ 1.5 გბ/წმ (1024B TCP w/Fastpath)
6. IPSec VPN სესიების მაქსიმალური რაოდენობა: არანაკლებ 7500
7. VLAN ების მაქსიმალური რაოდენობა: არანაკლებ 1024
8. ინტერფეისების რაოდენობა: არანაკლებ 12(თორმეტი) 1 გბ/წმ Ethernet ინტერფეისი (RJ-45 ტიპის) და 4 (ოთხი) 10 გბ/წმ ინტერფეისი(SFP+ ტიპის). დამატებით 1(ერთი) 1გბ/წმ წარმადობის (RJ-45 და SFP) მენეჯმენტ პორტი.
9. ქსელური მოდულის სლოტების რაოდენობა: არანაკლებ 1(ერთი) Network Module სლოტი
10. დამატებითი ქსელური მოდულების საშუალებით პორტების რაოდენობა უნდა იყოს არანაკლებ 12(თორმეტი) 10გბ/წმ ინტერფეისი (SFP+ ტიპის)
11. Application Visibility and Control აპლიკაციების მხარდაჭერა: არანაკლებ 4000
12. მაღალი მდგრადობის მხარდაჭერა: Active/Standby
13. ბრანდმაუერს უნდა გააჩნდეს შემდეგი ტექნოლოგიებისა და ოქმების მხარდაჭერა: SSH, SNMP, RADIUS, NAT, IPsec, IKEv2, EIGRP(using FlexConfig), OSPF, BGP, PxGrid.
14. ბრანდამაუერს უნდა მოყვებოდეს შესაბამისი 1(ერთი) წლიანი ლიცენზია Intrusion Prevention System(IPS) მხარდაჭერისთვის
15. დამატებითი ლიცენზიების საშუალებით ბრანდმაუერს უნდა ქონდეს URL კატეგორიების ფილტრაციის საშუალება
16. დამატებითი ლიცენზიების საშუალებით ბრანდმაუერს უნდა ქონდეს Advance Malware Protection(AMP) და Cloud Sandboxing მხარდაჭერა
17. არაუმეტეს: 1 RU ზომის
18. კვება: AC ტიპის
19. ბრანდმაუერს უნდა მოყვებოდეს 2(ორი) ცალი კვების ბლოკი
20. ბრანდმაუერზე უნდა ვრცელდებოდეს მწარმოებლის ერთ წლიანი საგარანტიო მომსახურეობა, ტექნიკური მხარდაჭერა და პროგრამული უზრუნველყოფის განახლება. მოწყობილობის დაზიანების მიზეზის დადგენის შემდეგ, მოწყობილობა უნდა შეკეთდეს ან შეცვალოს შემდეგ სამუშაო დღეს.

## მოთხოვნები მართვისა და მონიტორინგის სისტემის მიმართ (ერთი ცალი)

მოთხოვნები მართვისა და მონიტორინგის სისტემის მიმართ:

1. მართვისა და მონიტორინგის სისტემინდან შესაძლებელი უნდა იყოს მოთხოვნილი A და B ტიპის NGFW ბრანდმაუერების მართვა. მათ შორის:
	1. გადაწყვეტილებას უნდა ჰქონდეს User Intelligence რეპორტები
	2. ქსელის ტრაფიკი უნდა იყოს მიბმული მომხმარებლის ობიექტზე და მასთან ასოცირებულ მოწყობილობებზე (კომპიუტერი, მობილური და ა.შ.) შემდეგი შესაძლებლობებით:
		1. Workstations login events (including RDP, Telnet and SSH sessions)
		2. User application traffic statistics (application type, traffic volume, source and destination)
		3. User-details associated with the particular network traffic
		4. User-details associated with the particular network object (workstation)
	3. შესაძლებელი უნდა იყოს NGFW პოლიტიკების კონფიგურაცია მონიტორინგი და მართვა. წესებისა და სიგნატურების კონფიგურაცია.
2. ცენტრალიზირებული და ადვილად მართვადი მენეჯმენტ პორტალი
3. მომხმარებლის მოთხოვნებზე მორგებადი მართვის პანელი
4. მართვისა და მონიტორინგის სიტემის მართვა შესაძლებელი უნდა იყოს ვებ ბრაუზერიდან
5. მართვისა და მონიტორინგის სისტემა უნდა წარმოადგენდეს მზა ე.წ ‘virtual appliance’ გადაწყვეტილებას
6. გამოყოფილი მართვისა და მონიტორინგის სისტემის გამართვა შესაძლებელი უნდა იყოს ინფრასტრუქტურეში არსებულ ESXi ვირტუალურ გარემოში
7. მართვისა და მონიტორინგის სისტემინდან შესაძლებელი უნდა იყოს ათი NGFW ბრანდმაუერის მართვა.
8. მართვისა და მონიტორინგის სისტემაზე უნდა ვრცელდებოდეს 1 წლიანი მწარმოებლის მხარდაჭერა პროგრამულ ნაწილზე.

## აუთენთიფიკაციის და ავტორიზაციის სერვერი

1. სერვერს უნდა გააჩნდეს RADIUS პროტოკოლის ფუნქიონალი, authentication, authorization და accounting მხარდაჭერით.
2. სერვერს უნდა გააჩნდეს TACACS+ პროტოკოლის მხარდაჭერა დამატებითი ლიცენზიის საშუალებით.
3. სერვერს უნდა გააჩნდეს შემდეგი აუთენთიფიკაციის პროტოკოლების მხარდაჭერა: PAP, MS-CHAP, EAP-MD5, PEAP, EAP-FAST, EAP-TLS და EAP-TTLS.
4. სერვერზე უნდა იყოს შესაძლებელი დაშვების წესების შექმნა შემდეგი ატრიბუტების მიხედვით: მომხმარებელი, მოწყობილობა, ლოკაცია, აუთენთიფიკაციის პროტოკოლი.
5. სერვერს უნდა შეეძლოს დაშვების ატრიბუტების შექმნა დინამიურად, შემდგომ მათი შენახვის და გამოყენების მიზნით.
6. სერვერს უნდა გააჩნდეს შემდეგი დაშვების კონტროლის მექანიზმების მხარდაჭერა: Downloadable access-list(dACL), Vlan assignment, URL redirection, named ACLs and Security Group(SGs)
7. სერვერს უნდა გააჩნდეს Security group tag exchange (SXP) პროტოკოლის მხარდაჭერა.
8. 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.
9. სერვერს უნდა გააჩნდეს WEB პორტალის ფუნქციონალი, მომხმარებლების და მათი მოწყობილობების რეგისტრაციისთვის.
10. სერვერს უნდა გააჩნდეს ჩაშენებულ Guest პორტალი , როგორც მომხმარებლების თვითმომსახურების(self-service) აგრეთვე Sponsored Access ფუნქციონალის მხარდაჭერით.
11. 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.
12. დამატებითი ლიცენზიის შეძენის შემთხვევაში სერვერს უნდა გააჩნდეს ინტეგრაციის მხარდაჭერა mobile device management (MDM/EMM) გადაწყვეტილებებთან.
13. სერვერი უნდა იმართებოდეს ჩაშენებული ცენტრალიზებული web based GUI კონსოლის მეშვეობით.
14. 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.
15. სერვერს უნდა გააჩნდეს ინტეგრაციის მხარდაჭერა შემდეგ სისტემებთან: Microsoft Active Directory, LDAP, RSA SecurID(OTP) და Open Database Connectivity (ODBC).
16. სერვერს უნდა გააჩნდეს ინტეგრაციის მხარდაჭერა არანაკლებს 50(ორმოცდაათი) Microsoft Active Directory სისტემასთან two-way trust მიერთებების გარეშე.
17. სერვერს უნდა გააჩნდეს სხვა სისტემებთან ინტეგრაციის მხარდაჭერა API-ს მეშვეობით.
18. სერვერს უნდა გააჩნდეს ჩაშენებული სერტიფიკაციის ცენტრი (Certificate Authority).
19. სერვერს უნდა შეეძლოს ინტეგრაცია Cisco Firepower Thread Defense ბრანდმაუერებთან ჩაშენებული PxGrid ფუნქციონალის მეშვეობით.
20. სერვერს უნდა შეეძლოს არსებული Cisco Wireless და Anyconnect VPN მომხმარებლების აუთენთიფიკაცია და ავტორიზაცია.
21. სერვერის ინსტალაცია შესაძლებელი უნდა იყოს არსებულ VMware ESXi ინფრასტრუქტურაში.
22. მოთხოვნილ სერვერზე შესაძლებელი უნდა იყოს მიგრაცია მომხმარებლების Base ლიცენზიების, იფრასტრუქტურაში არსებული Cisco ISE (Identity Service Engine) სერვერიდან.
23. მოთხოვნილ სერვერს უნდა მოყვებოდეს 100 მომხმარებლების Plus ტიპის ერთ წლიანი ლიცენზია.
24. მოთხოვნილ სერვერს უნდა მოყვებოდეს დამატებითი ვირტუალური მანქანის ლიცენზია, მაღალმდგრადობის კლასტერის აწყობის მხარდაჭერისთვის.
25. მოთხოვნილ სერვერის ვირტუალური მანქანისთვის საჭირო რესურსები არ უნდა აღემატებოდეს შემდეგ მოთხოვნებს: 12(თორმეტი) ვირტუალური პროცესორი და 16გბ ოპერატიული მეხსირება.
26. მოთხოვნილ სერვერზე უნდა ვრცელდებოდეს მწარმოებლის 1 წლიანი ტექნიკური მხარდაჭერა და პროგრამული უზრუნველყოფის განახლება.

## პრეტენდენტის მიერ ჩასატარებელი ტექნიკური სამუშაოები

1. აუთენთიფიკაციის და ავტორიზაციის სერვერების ინსტალაცია არსებულ VMware ინფრასტრუქტურაში
2. აუთენთიფიკაციის და ავტორიზაციის სერვერების კლასტერის აწყობა.
3. კონფიგურაციის და ლიცენზიების მიგრაცია ინფრასტრუქტურაში არსებული Cisco ISE (Identity Service Engine) სერვერიდან ახალ აუთენთიფიკაციის და ავტორიზაციის სერვერების კლასტერზე.
4. A და B ტიპის ბრანდმაუერების არსებულ ინფრასტრუქტურაში ინტეგრაციის დაგეგმვა
5. A ტიპის ბრანდმაუერების ბაზური ფიზიკური და ლოგიკური ინსტალაცია შედგენილი გეგმის მიხედვით
6. A ტიპის ბრანდმაუერების და მართვის სისტემის პროგრამულ უზრუნველყოფის განახლება ბოლო ვერსიაზე
7. A ტიპის ბრანდმაუერების ინტეგრაცია მოთხოვნილ მართვის სისტემაში
8. A ტიპის ბრანდმაუერების Active/Standby კლასტერის იმპლემენტაცია
9. არსებული Cisco ASA 5555 ბრანდმაუერებიდან შიდა ინფრასტრუქტურის ნაწილის კონფიგურაციის მიგრაცია და ოპტიმიზაცია ახალ A ტიპის ბრანდმაუერებისთვის
10. A ტიპის ბრანდმაუერების საშუალებით SSL დეშიფრაციის სერვისების დანერგვა
11. A ტიპის ბრანდმაუერების და მართვის სისტემის, მოთხოვნილ აუთენთიფიკაციის და ავტორიზაციის სისტემის და Active Directory სერვერებთან ინტეგრაცია, პასიური აუტენტიფიკაციის მხარდაჭერისთვის
12. A ტიპის ბრანდმაუერების IPS ფუნქციონალის კონფიგურაცია მონიტორინგ რეჟიმში და შემდგომ ნაწილობრივ პრევენციის რეჟიმში გადაყვანა.
13. B ტიპის ბრანდმაუერების ბაზური ფიზიკური და ლოგიკური ინსტალაცია შედგენილი გეგმის მიხედვით
14. არსებული Cisco ASA 5555 ბრანდმაუერებიდან გარე ინფრასტრუქტურის ნაწილის კონფიგურაციის მიგრაცია და ოპტიმიზაცია ახალ B ტიპის ბრანდმაუერებისთვის.
15. B ტიპის ბრანდმაუერების ინტეგრაცია მოთხოვნილ მართვის სისტემაში
16. B ტიპის ბრანდმაუერების Active/Standby კლასტერის იმპლემენტაცია
17. B ტიპის ბრანდმაუერების საშუალებით SSL დეშიფრაციის სერვისების დანერგვა
18. B ტიპის ბრანდმაუერების და მართვის სისტემის, მოთხოვნილ აუთენთიფიკაციის და ავტორიზაციის სისტემის და Active Directory სერვერებთან ინტეგრაცია, პასიური აუტენტიფიკაციის მხარდაჭერისთვის
19. B ტიპის ბრანდმაუერების IPS ფუნქციონალის კონფიგურაცია მონიტორინგ რეჟიმში და შემდგომ ნაწილობრივ პრევენციის რეჟიმში გადაყვანა.

## დამატებითი მოთხოვნები

* პრეტენდენტს უნდა გააჩნდეს კომპლექსური უსაფრთხოებისა და ქსელური ინფრასტრუქტურის სპეციალიზაცია, რაც უნდა დასტურდებოდეს შემოთავაზებული პროდუქციის მწარმოებლის მიერ გაცემული წერილით.
* პრეტენდენტის მიერ შემოთავაზებული აპარატურა უნდა იყოს ერთიდაიგივე მწარმოებლის
* პრეტენდენტმა უნდა მოახდინოს შემოთავაზებული აპარატურის ინსტალაცია და კონფიგურაცია
* მომწოდებელმა უნდა წარმოადგინოს მწარმოებლის ავტორიზაციის ფორმა (Manufacturers Authorization Form)