# ტექნიკური დავალება

**ქსელური უსაფრთხოების გადაწყვეტილების მიწოდება-ინსტალაცია**

## ზოგადი ტექნიკური მოთხოვნები

1. შემოთავაზება უნდა მოიცავდეს მინიმუმ 2 ქსელური უსაფრთხოების ფიზიკურ მოწყობილობას (Appliance).
2. შემოთავაზება უნდა მოიცავდეს მინიმუმ 1 ვირტუალური მენეჯმენტის სისტემის ლიცენზიას, საიდანაც შესაძლებელი იქნება ზემოთ აღნიშნული ქსელური უსაფრთხოების ფიზიკური მოწყობილობების (Appliances) მართვა და მოვლენების ცენტრალური კორელაცია.

## 2 ცალი მოწყობილობა - მინიმალური ტექნიკური მახასიათებლები

|  |  |
| --- | --- |
| აპარატურის ტიპი | * Next Generation Firewall
 |
| წარმადობა | * არანაკლებ 15 Gbps Threat Prevention გამტარუნარიანობა
* არანაკლებ 35 Gbps IPS გამტარუნარიანობა
* არანაკლებ 435,000 ახალი შეერთება წამში (Connections/sec)
* არანაკლებ 16,000,000 ერთდროული სესია (Concurrent conn)
 |
| ქსელური ინტერფეისები | * არანაკლებ 8x 1GbE copper interface
* არანაკლებ 8x 10GbE fiber interface
* არანაკლებ 8x SFP+ SR Transceivers
 |
| მყარი დისკი | * არანაკლებ 2 ცალი 480GB SSD
 |
| ოპერატიული  | * არანაკლებ 64 GB (Memory)
 |
| კვების წყარო | * დუბლირებული
 |
| მაღალმდგრადობა | * Active/Active and Active/Passive
* Session failover for routing change
* Device and link failure detection
 |
| ქსელური კავშირი | * IPv4 and IPv6
* 802.3ad Passive and Active Link Aggregation
* Layer 2 (Transparent) and Layer 3 (Routing) mode
 |
| მარშუტიზაციის პროტოკოლები | * OSPF v2 and v3, BGP, RIP
* Static routes, Multicast routes
* PIM-SM, PIM-SSM, PIM-DM, IGMP v2, and v3
 |
| აუცილებელი ფუნქციონალი, რომელიც უნდა იყოს შემოთავაზებაში | * Firewall
* IPS
* Application Control
* URL Filtering
* Anti-bot
* Antivirus ან Anti-Malware
* Threat Emulation ან Sandboxing
 |

## 1 ცალი მართვის სისტემა - მინიმალური ტექნიკური მახასიათებლები

|  |  |
| --- | --- |
| სისტემის ტიპი | უსაფრთხოების მენეჯმენტი |
| მხარდაჭერილი პლათფორმა | VMware |
| მოთხოვნები მართვისა და ლოგირების მიმართ | ლიცენზია უნდა მოიცავდეს არანაკლებ 5 ცალი Next-Generation Firewall-ის ერთდროულ მართვას და ლოგების ცენტრალურად ანალიზს |
| აუცილებელი ფუნქციონალი, რომელიც უნდა იყოს შემოთავაზებაში | * Policy Management
* Logging
* Reporting
* Event Correlation
* User Identity
 |

## დეტალური ტექნიკური მოთხოვნები ფუნქციონალის მიმართ

1. **Firewall - ფაიერვოლის ფუნქციონალი**
	* უნდა შეეძლოს გადასცეს სტატისტიკა მართვის აპლიკაციას. სტატისტიკური მონაცემები უნდა მოიცავდეს ინფორმაციას იმის შესახებ თუ რამდენჯერ მოხდა უსაფრთხოების წესის (Rule) გამოყენება (hit count statistics).
	* უნდა შეეძლოს ავტომატურად უსაფრთხოების წესის (Rule) აქტივაცია/დეაქტივაცია დროის განსაზღვრულ შუალედებში.
	* მართვის სერვერს და ფაიერვოლს შორის კომუნიკაცია უნდა იყოს დაშიფრული და აუტენთიფიკაცია უნდა ხდებოდეს PKI სერტიფიკატების გამოყენებით.
	* ფაიერვოლს უნდა ჰქონდეს შესაძლებლობა მაღალმდგრადობის უზრუნველყოფის, ასევე დატვირთვების გადანაწილების და მდგომარეობის სინქრონიზაციის (State Synchronization).
2. **Application Control and URL Filtering - აპლიკაციების კონტროლი და URL ფილტრაცია**
	* Application control-ის მონაცემთა ბაზა უნდა მოიცავდეს არანაკლებ 8000 ცნობად აპლიკაციას.
	* უნდა იყოს შესაძლებელი რამოდენიმე კატეგორიის ერთ ფილტრაციის წესში(Rule) გაერთიანების.
	* უნდა იყოს შესაძლებელი ფილტრაციის წესის შექმნა ერთი საიტისთვის რომელიც რამოდენიმე კატეგორიაშია.
	* უნდა იყოს შესაძლებლობა აპლიკაციების და URL-ების რისკის ფაქტორებით კატეგორიზაცია.
	* უნდა იყოს შესაძლებელი Application control-ის და URL ფილტრაციის პოლიტიკებში განიზასღვროს მომხმარებლის საიდენტიფიკაციო პარამეტრები.
	* უნდა იყოს შესაძლებლობა ერთ უსაფრთხოების წესში გაიწეროს Application control-ის და URL ფილტრაციის პოლიტიკები.
	* უნდა იყოს შესაძლებელი შეიზღუდოს კონკრეტული აპლიკაციის მოხმარება სიჩქარის მითითებით
	* ფუნქციონალი უნდა მოიცავდეს თეთრ და შავი სიის მექანიზმს. სადაც შესაძლებელი იქნება ნებისმიერი URL-ის განთავსება მიუხედავად იმისა რომელ კატეგორიას განეკუთვნება ეს URL-ი.
	* გადაწყვეტილებას უნდა ქონდეს კონფიგურირებადი შემოვლითი (bypass) მექანიზმი.
	* უსაფრთხოების პოლიტიკის წესის, რომელიმე სექციაში უნდა შეიძლებოდეს კონკრეტულად ამ უსაფრთხოების წესისთვის უშუალოდ URL Category-ის მითითება ან ცვლილება, იმისათვის რომ ხდებოდეს ე.წ. “Policy match” მითითებული URL კატეგორიების მიხედვით.
3. **Intrusion Prevention System - შეღწევადობის პრევენცია**
	* IPS-ი და ფაიერვოლი ფუნქციონალი უნდა იყოს ინტეგრირებული ერთ პლატფორმაში.
	* შესაძლებელი უნდა იყოს IPS შემოწმების (Inspection) კონფიგურაცია ისე, რომ მხოლოდ შიდა რესურსი (Host) იქნას დაცული.
	* IPS-ის ახალი სიგნატურების (Signatures) და განახლებების აქტივაცია და მართვა უნდა ხდებოდეს ავტომატურად.
	* IPS უნდა ჰქონდეს მექანიზმი, რომლის საშუალებითაც სისტემაში დააკონვერტირებს SNORT-ის სინგატურებს.
	* IPS-ს უნდა შეეძლოს ქსელის გამონაკლისების დაშვება source, destination, service ან ამ სამივე კომპონენტის კომბინირების საშუალებით.
	* IPS-ს უნდა ქონდეს შესაძლებლობა რომ აღმოაჩინოს და დაბლოკოს Аpplication დონის შემოტევები, დაცული უნდა იყოს მინიმუმ შემდეგი სერვისები: email services, DNS, FTP, Windows services, SNMP.
	* შესაძლებელი უნდა იყოს IPS ინსპექტირებიდან გამონაკლისების დაშვება ქსელისთვის და ჰოსტისთვის.
	* შესაძლებელი უნდა იყოს DNS Cache Poisoning -გან დაცვა და აღკვეთოს მომხმარებლების დაშვება დაბლოკილ დომეინების მისამართებზე.
4. **Antivirus (ან Anti-Malware) and Anti-bot- ანტივირუსის სისტემა და ანტი-ბოტი**
	* Antivirus და Anti-bot ფუნქციონალი სრულად უნდა იყოს ინტეგრირებული ფაიერვოლის სხვა დანარჩენ ფუნქციონალთან ერთად .
	* Antivirus და Anti-bot პოლისები უნდა ადმინისტრირდებოდეს ცენტრალური კონსოლიდან.
	* Antivirus და Anti-bot აპლიკაციას უნდა ქონდეს ცენტრალური ევენთების კორელაციის და რეპორტინგის მექანიზმი.
	* Antivirus და Anti-bot ფუნქციონალს უნდა შეეძლოს SSL დაშიფრული ტრაფიკის ინსპექცია.
5. **Threat Emulation (ან Sandboxing) - საფრთხეების ემულაცია (სენდბოქსი)**
	* ფუქნციონალის მართვა ინტეგრირებული უნდა იყოს ცენტრალურ მენეჯმენტის სისტემაში.
	* სენდბოქსის ფუნქციონალს მხარდაჭერილი უნდა ჰქონდეს ფაილების ემულაცია პროცესორის (CPU-Level) და ოპერაციული სისტემის დონეზე (OS-Level).
	* სენდბოქსის ფუნქციონალში მხარდაჭერილი უნდა იყოს ფაილების სტატიკური ანალიზი და რეკონსტრუქცია (Reconstruction)
	* ფაილის ემულაციის საშუალო დრო უნდა იყოს არაუმეტეს 100 წამი
	* მხარდაჭერილი ოპერაციული სისტემები უნდა იყოს არანაკლებ: Windows 8.1 და 10
6. **Policy Management, Reporting and Event Correlation - ცენტრალური მართვა, რეპორტინგი და მოვლენების კორელაცია**
	* შესაძლებელი უნდა იყოს ყველა ფაიერვოლის ამავე მწარმოებლის ერთ მენეჯმენტ აპლიკაციასთან ინტეგრაცია.
	* მენეჯმენტის აპლიკაციას უნდა შეეძლოს როლების და უფლებების მინიჭება ადმინისტრატორების ექაუნთების მიხედვით, მაგალითად: ადმინისტრატორს ჰქონდეს როლი და უფლება მხოლოდ პოლისების მართვის ან შეეძლოს მხოლოდ ლოგების დათვალიერება.
	* მენეჯმენტის აპლიკაციას უნდა შეეძლოს ადმინისტრატორების კოლაბორატიულად მუშაობის მხარდაჭერა, ისე რომ არ მოხდეს კონფლიქტი (შეუთავსებლობა), როცა რამდენიმე ადმინისტრატორი პარალელურად ახორციელებს უსაფრთხოების სამუშაოებს.
	* ყველა უსაფრთხოების პოლიტიკის მართვა შესაძლებელი უნდა იყოს ცენტრალური კონსოლიდან.
	* მართვის სისტემა უნდა მოიცავდეს ძებნის სწრაფ ინდექსირებულ ოფციას, რომლის საშუალებითაც შესაძლებელი იქნება მოიძებნოს უსაფრთხოების წესები რომლებიც მოიცავენ კონკრეტულ IP-ის ან მის ნაწილს.
	* შესაძლებელი უნდა იყოს ცენტრალიზირებულად ახალი პროგრამული ვერსიების გავრცელება და დაყენება.
	* შესაძლებელი უნდა იყოს ყველა შესაძლო ლიცენზიების ცენტრალიზირებულად მართვა.
	* ლოგირების დათვალიერებისას შესაძლებელი უნდა იყოს ფილტრების დაყენება სხვადასხვა წინასწარ განსაზღვრული ობიექტებით (hosts, network, groups, users...)
	* ფაიერვოლს უნდა ჰქონდეს ხდომილებების კორელაციის საშუალება ჩაშენებული ან იმავე მწარმოებლის დამატებითი ცენტრალიზირებული პროგრამული უზრუნველყოფის საშუალებით.
	* რეპორტინგ სისტემას უნდა შეეძლოს კონსოლიდირებული ინფორმაციის ჩვენება მართვის სისტემაში გაერთიანებული ყველა მოწყობილობიდან.
7. **Logging - ლოგირება**
	* შესაძლებელი უნდა იყოს მოვლენების დახარისხება სხვადასხვა მახასიათებლის მიხედვით.
	* ლოგირების ფუქნციონალს უნდა შეეძლოს შემდეგი ტიპის მოვლენების გენერაცია: Top sources, Top destinations, Top services, Top Actions, Top users, Top Origins, Top Firewall Rules.
	* გადაწყვეტილებას უნდა შეეძლოს იგივე მწარმოებლის რეპორტინგის ცენტრალურ სისტემასთან ინტეგრაცია და გეგმიური რეპორტების დაგენერირება (ყოველდღიური, ყოველკვირეული და ყოველთვიური). მხარდაჭერილი უნდა იყოს არანაკლებ შემდეგი რეპორტინგის ფორმატები: HTML და PDF.
8. **User Identity - მომხმარებელთა იდენტიფიკაცია**
	* სისტემას უნდა შეეძლოს Microsoft Active Directory-სთან ინტეგრაცია.
	* მხარდაჭერილი უნდა იყოს AD მომხმარებლებისა და ჯგუფების ფაიერვოლის წესებში გამოყენება.

## შესაძლებელი უნდა იყოს შემდეგი ფუნქციონალის დამატება

**აპარატურული-პროგრამული გაფართოების შესაძლებლობა**

1. აპარატურაში შესაძლებელი უნდა იყოს დამატებით შემდეგი მოდულის ჩამატება:
* არანაკლებ 2x 40G QSFP+ port card
* არანაკლებ 2x 100/25G QSFP28 port card
1. აპარატურაში მხარდაჭერილი უნდა ოყოს Fail Open ან Bypass ტექნოლოგიის ქსელური ბარათის ჩამატება:
* არანაკლებ 2x Port 10GE Short-range Fiber Bypass (Fail-Open) Network interface card (10GBase-SR)
1. მხარდაჭერილი უნდა იყოს ერთდროული სესიების (Concurrent conn) გაფართოება არანაკლებ 32,000,000-ამდე.
2. მხარდაჭერილი უნდა იყოს მონაცემთა გაჟონვის პრევენციის ფუნქციონალი (Data Loss Prevention), რომელსაც თან ახლავს არანაკლებ 700 წინასწარ განსაზღვრული მონაცემთა ტიპი (Data type).

## მოთხოვნები საგარანტიო და სერვისულ მომსახურეობაზე

1. გადაწყვეტილების ფიზიკურ კომპონენტებზე უნდა ვრცელდებოდეს მინიმუმ 1 წლიანი მწარმოებლის გარანტია.
2. გადაწყვეტილებაზე უნდა ვრცელდებოდეს პროგრამული უზრუნველყოფის და სხვა აუცილებელი კომპონენტების მინიმუმ 1 წლიანი განახლებების სერვისი.
3. მომწოდებელმა კომპანიამ უნდა უზრუნველყოს მოწოდებული პროდუქტის მხარდაჭერა (Collaborative / Shared Support) 1 წლის განმავლობაში. მწარმოებლის ოფიციალურ საიტზე მითითებული უნდა იყოს, რომ პრეტენდენტ კომპანიას აქვს შემოთავაზებული მხარდაჭერის განხორციელების შესაბამისი ავტორიზაცია.