ქსელური ინფრასტრუქტურის განახლების პროექტი

1. ქსელური მოწყობილობები _ ფაირვოლები ტიპი I – 2 ც.
2. ქსელური მოწყობილობები _ ფაირვოლები ტიპი II - 7 ც.
3. ლიცენზია არსებული მენეჯმენტის სისტემისთვის - 2 ც.
4. საინსტალაციო სამუშაოები

შეთავაზების ზოგადი ტექნიკური მოთხოვნები

1. ფაირვოლი _ ტიპი I

1.1. შემოთავაზება უნდა მოიცავდეს არანაკლებ 2 ცალი ქსელური უსაფრთხოების ფიზიკურ მოწყობილობას (Hardware Appliance).

1.2. შემოთავაზებული აპარატურა უნდა ინტეგრირდებოდეს არსებულ ვირტუალური მენეჯმენტის სისტემასთან (Check Point Next Generation Security Management Software).

მინიმალური ტექნიკური მახასიათებლები

აპარატურის ტიპი	○ Next Generation Firewall
წარმადობა	○ არანაკლებ 15 Gbps Threat Prevention გამტარუნარიანობა ○ არანაკლებ 35 Gbps IPS გამტარუნარიანობა ○ არანაკლებ 435,000 შეერთება წამში (Connections/sec) ○ არანაკლებ 16,000,000 ერთდროული სესია (Concurrent conn)
ქსელური ინტერფეისები	○ არანაკლებ 8x 1GbE copper ports ○ არანაკლებ 8x 10GbE SFP+ ports ○ არანაკლებ 8x SR Transceivers
მყარი დისკი	○ არანაკლებ 2 ცალი 480GB SSD
ცენტრალური პროცესორი	○ არანაკლებ ორი პროცესორი (CPU), ჯამურად 24 ფიზიკური ბირთვი (physical cores)
ოპერატიული	○ არანაკლებ 64 GB (Memory)
კვების წყარო	○ დუბლირებული

მაღალმდგრადობა	○ Active/Active and Active/Passive ○ Session failover for routing change, device and link failure ○ ClusterXL or VRRP
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 ○ Antivirus, Anti-bot ან Anti-Malware

ტექნიკური მოთხოვნები ფუნქციონალის მიმართ

- **ფაირვოლის 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.
  - ფაიერვოლს უნდა ჰქონდეს შესაძლებლობა მაღალმდგრადობის უზრუნველყოფის, ასევე დატვირთვების გადანაწილების და მდგომარეობის სინქრონიზაციის (State Synchronization).

- **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.

- **შეღწევადობის პრევენცია**
  - IPS და ფაიერვოლის 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-ს უნდა შეეძლოს ქსელის გამონაკლისების დაშვება source, destination, service ან ამ სამივე კომპონენტის კომბინირების საშუალებით.
  - IPS-ს უნდა ქონდეს შესაძლებლობა რომ აღმოაჩინოს და დაბლოკოს Application 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.

- **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.

შესაძლებელი უნდა იყოს შემდეგი ფუნქციონალის დამატება

<u>აპარატურული-პროგრამული გაფართოების შესაძლებლობა:</u>

- აპარატურაში შესაძლებელი უნდა იყოს შემდეგი მოდულის ჩამატება:
  - არანაკლებ 2 Port 40G QSFP28 interface card.
  - არანაკლებ 2 Port 100/25G QSFP28 interface card.

- აპარატურაში მხარდაჭერილი უნდა იყოს Fail Open ან Bypass ტექნოლოგიის ქსელური ბარათის ჩამატება:
  - არანაკლებ 2 Port 10GE Short-range Fiber Bypass (Fail-Open) Network interface card (10GBase-SR).

- მხარდაჭერილი უნდა იყოს ერთდროული სესიების (Concurrent conn) გაფართოება არანაკლებ 32,000,000-მდე.

- ოპერატიული მეხსიერების გაფართოება შესაძლებელი უნდა იყოს არანაკლებ 128 GB-მდე (Memory).

- მხარდაჭერილი უნდა იყოს მონაცემთა გაჟონვის პრევენციის ფუნქციონალი (Data Loss Prevention), რომელსაც თან ახლავს არანაკლებ 700 წინასწარ განსაზღვრული მონაცემთა ტიპი (Data type).

Sandblast (Threat Emulation) ან Sandboxing ფუნქციონალი:

- ფუნქციონალის 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)

- მხარდაჭერილი ოპერაციული სისტემები უნდა იყოს არანაკლებ: Windows 10

- შესაძლებელი უნდა იყოს IPS, Antivirus და Application Control ფუნქციონალისთვის უსაფრთხოების განახლების ბაზების offline რეჟიმში განახლება დამატებითი ფიზიკური მოწყობილობის საშუალებით.

2. ფაირვოლი _ ტიპი II

ზოგადი ტექნიკური მოთხოვნები

1.1. შემოთავაზება უნდა მოიცავდეს არანაკლებ 7 ცალი ქსელური უსაფრთხოების ფიზიკურ მოწყობილობას (Hardware Appliance).

1.2. ქსელური უსაფრთხოების ფიზიკურ მოწყობილობას (Hardware Appliance) უნდა მოყვებოდეს ვირტუალური სისტემების (Virtual System) ლიცენზიები. თითოეულ ფიზიკურ აპარატურას უნდა მოყვებოდეს არანაკლებ 10 ცალი ვირტუალური სისტემა ან ანალოგიური ფუნქციონალი

1.3. შემოთავაზებული აპარატურის ინტეგრაცია უნდა შეიძლებოდეს არსებული ვირტუალური მენეჯმენტის სისტემასთან (Check Point Next Generation Security Management Software).

მინიმალური ტექნიკური მახასიათებლები

აპარატურის ტიპი	○ Next Generation Firewall
წარმადობა	○ არანაკლებ 7.4 Gbps Threat Prevention გამტარუნარიანობა ○ არანაკლებ 19 Gbps IPS გამტარუნარიანობა ○ არანაკლებ 230,000 შეერთება წამში (Connections/sec) ○ არანაკლებ 8,000,000 ერთდროული სესია (Concurrent conn)
ქსელური ინტერფეისები	○ არანაკლებ 24x 1GbE copper ports ○ არანაკლებ 1x 10/100/1000 Base-T port for Sync ○ არანაკლებ 1x 10/100/1000 Base-T port for Management
მყარი დისკი	○ არანაკლებ 2 ცალი 480GB SSD

ცენტრალური პროცესორი	○ არანაკლებ ერთი პროცესორი (CPU), ჯამურად 8 ფიზიკური ბირთვი (physical core)
ოპერატიული	○ არანაკლებ 32 GB (Memory)
კვების წყარო	○ დუბლირებული
მაღალმდგრადობა	○ Active/Active and Active/Passive ○ Session failover for routing change, device and link failure ○ ClusterXL or VRRP
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 ○ Antivirus, Anti-bot ან Anti-Malware

დეტალური ტექნიკური მოთხოვნები ფუნქციონალის მიმართ

- **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.
  - ფაიერვოლს უნდა ჰქონდეს შესაძლებლობა მაღალმდგრადობის უზრუნველყოფის, ასევე დატვირთვების გადანაწილების და მდგომარეობის სინქრონიზაციის (State Synchronization).

- **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.

- **შეღწევადობის პრევენცია**
  - IPS და ფაიერვოლის 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-ს უნდა შეეძლოს ქსელის გამონაკლისების დაშვება source, destination, service ან ამ სამივე კომპონენტის კომბინირების საშუალებით.
  - IPS-ს უნდა ქონდეს შესაძლებლობა რომ აღმოაჩინოს და დაბლოკოს Application 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.

- 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.

შესაძლებელი უნდა იყოს შემდეგი ფუნქციონალის დამატება

- აპარატურაში შესაძლებელი უნდა იყოს შემდეგი ქსელური ბარათის ჩამატება/ჩანაცვლება - არანაკლებ 2 Port 40G QSFP28 interface card.

- აპარატურაში მხარდაჭერილი უნდა ოყოს Fail Open ან Bypass ტექნოლოგიის ქსელური ბარათის ჩამატება/ჩანაცვლება - არანაკლებ 2 Port 10GE Short-range Fiber Bypass (Fail-Open) Network interface card (10GBase-SR).

    - მხარდაჭერილი უნდა იყოს ერთდროული სესიების (Concurrent conn) გაფართოება არანაკლებ 16,000,000-მდე.

    - ოპერატიული მეხსიერების გაფართოება შესაძლებელი უნდა იყოს არანაკლებ 64 GB-მდე (Memory).

    - მხარდაჭერილი უნდა იყოს მონაცემთა გაჟონვის პრევენციის ფუნქციონალი (Data Loss Prevention), რომელსაც თან ახლავს არანაკლებ 700 წინასწარ განსაზღვრული მონაცემთა ტიპი (Data type).

- Sandblast (Threat Emulation) ან Sandboxing ფუნქციონალი:

    - ფუნქციონალის 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)
- მხარდაჭერილი ოპერაციული სისტემები უნდა იყოს არანაკლებ Windows 10

შესაძლებელი უნდა იყოს IPS, Antivirus და Application Control ფუნქციონალისთვის უსაფრთხოების განახლების გაზების offline რეჟიმში განახლება

3. ლიცენზია არსებული მენეჯმენტის სისტემისთვის

გადაწვეტილებას უნდა მოყვებოდეს 2 ცალი ლიცენზია (Next Generation Security Management Software License for 50 gateways). თითოეულს უნდა გააჩნდეს მინიმუმ 50 ცალი ფაირვოლის დამატების შესაძლებლობა. შესაძლებელი უნდა იყოს აღნიშნული ლიცენზიების ინტეგრაცია არსებულ ვირტუალური მენეჯმენტის სისტემასთან (Check Point Next Generation Security Management Software).

4. საინსტალაციო სამუშაოები

- მოწოდებული ქსელური მოწყობილობების ინსტალაცია (მწარმოებლის მიერ რეკომენდირებული ბოლო განახლებების (Hot-fix) დაყენებით)
- არსებულ მენეჯმენტის სისტემასთან ინტეგრაცია
- არსებულ მენეჯმენტის სისტემაში ლიცენზიების გაწერა
- არსებული სისტემებიდან Backup ფაილების შექმნა
- მომწოდებლის სერტიფიცირებული ინჟინრის მიერ ტრენინგის ჩატარება სსე-ს მინიმუმ 3 თანამშრომლისთვის

მოთხოვნები გარანტიაზე და სერვისულ მომსახურეობაზე:

- გადაწყვეტილების ფიზიკურ კომპონენტებზე უნდა ვრცელდებოდეს მინიმუმ 2 წლიანი მწარმოებლის გარანტია.

- გადაწყვეტილებაზე უნდა ვრცელდებოდეს პროგრამული უზრუნველყოფის და სხვა აუცილებელი კომპონენტების მინიმუმ 2 წლიანი განახლებების სერვისი.

- მომწოდებელმა კომპანიამ უნდა უზრუნველყოს მოწოდებული პროდუქტის მხარდაჭერა 2 წლის განმავლობაში

- მწარმოებლის ოფიციალურ საიტზე მითითებული უნდა იყოს, რომ პრეტენდენტ კომპანიას აქვს შემოთავაზებული მხარდაჭერის განხორციელების შესაბამისი ავტორიზაცია.

საკვალიფიკაციო მოთხოვნები:

- პრეტენდენტმა კომპანიამ უნდა წარადგინოს მწარმოებლის ავტორიზაციის ფორმა (ე.წ. MAF –Manufacturer Authorization Form)

- გამოცდილების დასადასტურებლად პრეტენდენტმა კომპანიამ უნდა წარადგინოს შემოთავაზებული პროდუქტის შესაბამისად მის მიერ განხორციელებული ბოლო 2 წლის მანძილზე არანაკლებ 2 (ორი) პროექტის შესახებ ინფორმაცია (თითოეული არანაკლებ 1 000 000 ლარის ღირებულების), დამკვეთთან/შემსყიდველთან გაფორმებული ხელშეკრულებები და შესაბამისი მიღება-ჩაბარების აქტები, ან/და შესრულების დამადასტურებელი სხვა დოკუმენტები, ან/და მიუთითოს ელექტრონულ სისტემაში არსებული ელექტრონული ტენდერის ან CMR ნომერი.

- პრეტენდენტ კომპანიაში დასაქმებული უნდა იყოს მინიმუმ ორი ქართულენოვანი, შემოთავაზებულ პროდუქციაზე სერტიფიცირებული ინჟინერი, რის დასადასტურებლად უნდა წარმოადგინონ შესაბამისი სერტიფიკატები.

საქონლის მოწოდების ვადა - 60 კალენდარული დღე.

ინსტალაცია უნდა განხორციელდეს, ჩვენი წერილობითი მოთხოვნიდან 30 კალენდარული დღის განმავლობაში.