# 

# ქსელური ინფრასტრუქტურის უსაფრთხოების გადაწყვეტილება

## საკვალიფიკაციო მოთხოვნები კომპანიების მიმართ:

* საინფორმაციო ტექნოლოგიების სფეროში მოღვაწეობის 5 წლიანი გამოცდილება
* ანალოგიურ პროდუქტზე გამოცდილება დასრულებული პროექტების სახით, შესაბამისი რეფერენსებით
* მონაწილის სახელზე გაცემული MAF
* შემოთავაზებული გადაწყვეტილება უნდა იძებნებოდეს Gartner-ის ლიდერებს შორის Application Delivery Controller გადაწყვეტილებებში
* შემოთავაზებული უნდა იქნას ერთდროულად ორი ალტერნატიული კომერციული წინადადება/გადაწყვეტილება
  + ერთი გადაწყვეტილება ფიზიკური მოწყობილობების ბაზაზე
  + მეორე გადაწყვეტილება HyperV-ს ვირტუალური გადაწყვეტილების ბაზაზე
* შემოთავაზებული უნდა იყოს როგორც ვენდორის ასევე ლოკალური მხარდაჭერის შესაძლებლობა, ადგილობრივი ტექნიკოსების კვალიფიკაციის დადასტურებით
* კონტრაქტის დადებამდე კომპანიამ უნდა განახორციელოს შემოთავაზებული სისტემის პილოტის გაშვება და სრული ტესტირება
* წარმოდგენილი უნდა იყოს გადაწყვეტილების მოწოდების ვადები და ინტეგრაციის პირობები საპილოტე ინსტალაციის გაშვების გათვალისწინებით.
* შემოთავაზებაში გათვალისწინებული უნდა იყოს დამკვეთის (ბანკის) 2 თანამშრომლის ტრენინგი

## ძირითადი ტექნიკური ამოცანა არის

1. ონლაინ სერვისების ავტომატური გადართვის ფუნქციონალი მინიმალური down time-ით (არაუმეტეს 30 წამი, უპირატესობა მიენიჭება ნულოვან წყვეტის მქონე გადაწყვეტილებას)
2. ონლაინ სერვისების უსაფრთხოების დაცვა

* Firewall
* IPS/IDS
* Application Layer (WAF)
* Publishing

## მინიმალური ტექნიკური მოთხოვნები:

* ქსელური ნაკადის (traffic) გამტარუნარიანობა:

მინ. 500 MB/Sec ფიზიკური მოწყობილობის შემთხვევაში

მინ. 100 MB/Sec ვირტუალური მანქანის შემთხვევაში

* კონკურენტული მომხმარებლები - მინ. 1000
* ერთდროული შეერთებები - არანაკლებ 20000

## გადაწვეტილების ზოგადი აღწერა

Application Delivery Controller and Web Application Firewall გადაწყვეტილება (შემდგომში „გადაწყვეტილება“) უნდა წარმოადგენდეს მოწყობილობას (Appliance) ან პროგრამულ უზრუნველყოფას ვირტუალური გარემოს მხარდაჭერით (HyperV)

ინტერნეტ მომხმარებლებისთვის ერთდროულად უზრუნველყოს როგორც დატვირთვის გადანაწილება, ასევე მაღალ მდგრადი წვდომა პარალელურად ძირითად და სარეზერვო დატაცენტრში გაშვებულ სერვისებთან.

გადაწყვეტილებას უნდა შეეძლოს სხვადასხვა დონის დაზიანების ავტომატური აღმოჩენა (ქსელის გათიშვა, მოწყობილობის გათიშვა, ვებ სერვისის გათიშვა). ასეთ შემთხვევაში სისტემამ ავტომატურად უნდა გადაამისამართოს მოთხოვნები სარეზერვო სერვისებთან და გააგზავნოს შეტყობინება დაზიანების შესახებ წინასწარ განსაზღვრული სცენარის მიხედვით.

გადაწყვეტილებაში რეალიზებული უნდა იყოს მინიმუმ შემდეგი ფუნქციონალი:

1. Network Integration
2. Firewall
3. Network Load Balancing (Global Traffic Manager)
4. Web Application Firewall
5. Publishing
6. IPS/IDS Features
7. Support

## Network Integration

* ტრაფიკის გამტარუნარიანობა ფიზიკური/ვირტუალური 500/100 MB/Sec
* კონკურენტული შეერთებების მინიმალური რაოდენობა - 20000

მაღალმდგრადობა

* ავტომატური გადართვის შესაძლებლობა (Active/Passive).
* კლასტერში (Active/Passive) შემავალი მოწყობილობების რაოდენობის მხარდაჭერა – 4 (2-2 თითო საიტზე)
* დატვირთვის გადანაწილება (Active/Active).
* ფიზიკური და ვირტუალური მოწყობილობის ერთიან კლასტერში გაერთიანების შესაძლებლობა.
* კლასტერში გაერთიანებულ მოწყობილობებს შორის SSL სესიის სინქრონიზაცია.
* კლასტერში გაერთიანებულ მოწყობილობებს შორის TCP სესიის სინქრონიზაცია.
* აქტიური სესიების კორექტული გათიშვის შესაძლებლობა.

L2 კომუტაცია:

* VLAN
* STP
* LACP (802.1ad).
* LLDP

L3 მარშუტიზაცია:

* IPv4, IPv6.
* NAT, PAT, SNAT.
* BGP, OSPFv2/v3, RIPv2/RIPNG, Static.

ლოგირება:

* რეალურ დროში სისტემის ლოგის ატვირთვა მოშორებულ ლოგირების სერვერებზე
* ლოგების ფილტრაციის შესაძლებლობა
* ლოგებზე წვდომა მომხმარებელთა როლების მიხედვით

რეპორტინგი

* RAM Usage, CPU Performance, System Utilization,
* Active/New Sessions,
* Throughput bps/pps,
* HTTP Requests,
* SSL TPS.

სისტემის მონიტორინგის შესაძლებლობა

* SNMP v1/2c/3,
* SNMP Traps;
* sFlow/Netflow.

## Firewall

ბრენდმაუერი Statefull ინსპექტირების ფუნქციით

* L3/L4 full firewall features (filter by source/dest/port etc)

ტრაფიკის ფილტრაციის წესების მართვა:

* წესის მოქმედების ვადის მითითების შესაძლებლობა.
* წესის ამოქმედების დროის მითითების შესაძლებლობა (scheduler).

ბრენდმაუერის წესების მონიტორინგი:

* ბრენდმაუერის წესის გამოყენების სტატისტიკა. (Hit count statistics).
* ბრენდმაუერის წესების ინდივიდუალური ლოგირების საშუალება
* წესების ამოქმედების (Rule Hit) ინდივიდუალური ლოგირების საშუალება.

## Network Load Balancing

დატვირთვის გადანაწილება გეორგაფიულ ლოკაციებს შორის:

* დატვირთვის გადანაწილების მხარდაჭერა გეოგრაფიული ლოკაციის მიხედვით (By Source Location) DNS პროტოკოლის საშუალებით
* დატვრითვის გადანაწილების და მაღალმდგრადობის უზრუნველყოფის საშუალება გეოგრაფიულად დაშორებულ დატანცეტრებს შორის.
* DNS ჩანაწერების რეპლიკაცია მოწყობილობებს შორის
* DNS სერვერების დატვირთვის გადანაწილების შესაძლებლობა

დატვირთვის გადანაწილებისას მოწყობილობების/სერვისების მონიტორინგი:

* სერვერის მონიტორინგის საშუალებები: ICMP, TCP Echo.
* სერვისის მონიტორინგის შემდეგი საშუალებები : TCP, HTTP/S, Full URL, FTP, IMAP, LDAP, MSSQL, RADIUS, SMTP, SOAP, UDP, WMI.
* სერვისის მონიტორინგის “custom” წესების აგების შესაძლებლობა.
* Application availability and balancing Reporting.

Microsoft NLB-ის ჩანაცვლების ფუნქციონალი (optional):

დატვირთვის გადანაწილების შემდეგი რეჟიმების მხარდაჭერა:

* TCP სესიების გამიჯვნის შესაძლებლობით.
* L2 Forwarding რეჟიმი.
* L3 (IP) Forwarding რეჟიმი.
* L4 (TCP) Forwarding რეჟიმი.
* L4 (HTTP) Forwarding რეჟიმი.
* L4 (UDP) Forwarding რეჟიმი.

დატვირთვის გადანაწილების მეთოდები:

* Round Robin.
* Ratio Round Robin.
* Least Connections.
* Weighted Least Connections.

სესიის უწყვეტობის შენარჩუნების მეთოდები:

* Source or Destination IP address Persistence.
* Session ID Persistence.
* Cookie Persistence.
* MSRDP sessions Persistence.
* დატვირთვის გადანაწილების გაუქმების შემთხვევაში მომხმარებელთა არსებული სესიების კორექტულად დასრულების შესაძლებლობა.

## Web Application Firewall

ტრაფიკის ბლოკირების შემდეგი მეთოდების მხარდაჭერა:

* Block the HTTP request
* Block the connection
* Block the IP address
* Block the application session
* Block the user
* Send a TCP connection reset (in monitor mode)
* Block the connection (in inline mode)

XML შიგთავსის დაცვა და მთლიანობის უზრუნველყოფა.

წინასწარ გამზადებული და სისტემაში ჩაშენებული უსაფრთხოების პოლიტიკები სერვისის დაცვის გამარტივების მიზნით (MS Exchange, Skype for Business, etc.)

აპლიკაციების დაცვა შემდეგი სახის შეტევებისგან:

* OWASP Top 10
* OS Command Injection
* SQL Injection
* Session Hijacking
* Site Reconnaissance
* Site Scraping
* Cross Site Scripting
* Cross Site Request Forgery
* «Zero Day Web Worm» შეტევებისგან დაცვა.

წესების შექმნის შემდეგი მექანიზმები:

* წესების ავტომატურ რეჟიმში შექმნის შესაძლებლობა „self-learning“ მეთოდის გამოყენების გზით.
* წესების ხელით შექმნის რეჟიმი.
* წესების ხელით შექმნის შესაძლებლობა „Custom“ აპლიკაციებისთვის.

## Publishing

AAA ინტეგრაცია

* AD - სთან ინტეგრაციის შესაძლებლობა

აპლიკაციაზე წვდომის პოლიტიკების მართვა

* წვდომის პოლიტიკის შექმნა მომხმარებლის სააღრიცხვო ჩანაწერის მიხედვით
* წვდომის პოლიტიკის შექმნა მომხმარებელთა ჯგუფების მიხედვით
* ერთი პოლიტიკის ფარგლებში სხვადასხვა მომხმარებლისათვის სხვადასხვა დაშვების შექმნის შესაძლებლობა
* მომხმარებელთა ავტორიზაციის პორტალის შემქნა და მართვა
* მომხმარებელთა ავტორიზაციის პორტალში ცვლილებების შესაძლებლობა
* მომხმარებელთა დაშვების წესების შესაქმნელი ინტერაქტიული მოდული
* მომხმარებელთა დაშვების მართვა

Reverse proxy ფუნქციის მხარდაჭერა

მოშორებული აპლიკაციებისთვის Application Tunneling ფუნქციის მხარდაჭერა

## IPS/IDS Features

* Protocol Anomaly Detection
* Port-misuse protection
* SSL reverse proxy
* IP reputation and geolocation
* Remotely triggered black hole filtering (RTBH)
* DDoS protection
* DNS რეპუტაციის ბაზის გამოყენება მავნე ტრაფიკის დასაბლოკად
* DNS მოთხოვნების RFC სტანდარტებთან შესაბამისობის შემოწმება

## მწარმოებლის მხარდაჭერა / სერვისი

* + მწარმოებლის 1 წლიანი მხარდაჭერა სამუშაო დღეებში 9 დან 6 საათამდე, მნიშვნელოვანი ინციდენტის შემთხვევაში 1 საათიანი რეაგირების დროით
  + 1 წლიანი IPS/IDS ფუნქციონალის განახლების სერვისი
  + ელექტრონული ფოსტის, ვებ-პორტალის და ტელეფონის მეშვეობით დაკავშირების შესაძლებლობა