Web Application Firewall

შემოთავაზებული სისტემა უნდა წარმოადგენდეს ვირტუალურ მანქანას.
სისტემა წარმოდგენილი უნდა იყოს ერთიანი იმიჯის სახით.
სისტემას უნდა გააჩნდეს შემდეგი ჰიპერვიზორების მხარდაჭერა:

- VMware ESX/ESXi
- Citrix Xenserver
- Microsoft Hyper-V
- KVM

მინიმალური ბირთვების რაოდენობის მხარდაჭერა - 8.
სისტემას უნდა გააჩნდეს არანაკლებ 500Mbps მონაცემების გატარების შესაძლებლობა.
სისტემას უნდა გააჩნდეს მაღალმდგრადობის მხარდაჭერა(ე.წ. High Availability)

- Active/Passive
- Active/Active

სისტემას უნდა ჰქონდეს როგორც ე.წ. ერთ მხარიანი(one-arm), ასევე ორ მხარიანი(two-arm) reverse proxy რეჟიმში მუშაობის შესაძლებლობა.

სისტემას უნდა შეეძლოს შემდეგი Web - აპლიკაციების უსაფრთხოების ტექნოლოგიების და მექანიზმების გამოყენების შესაძლებლობა:

- განასხვავოს ლეგიტიმური მომხმარებელი ე.წ. spider_ებისგან და ბოტებისგან
- პასუხიდან წაშალოს არასასურველი თავსართის ველები(header fields) და დაბლოკოს შეცდომის შემდეგი კოდები: 4xx და 5xx
- JSON შიგთავსის ინსპექტირება
- OWASP TOP 10 მოწყვლადობებისგან დაცვა
- ჩამოთვლილი ცნობილი შეტევებისგან დაცვა:
    - SQL injection
    - Cross-site scripting
    - Cookie/forms tampering
- ფორმის ველებში შეყვანილი მონაცემების ვალიდურობის შემოწმების
- მონაცემების მოპარვისგან დაცვა (Data Loss Prevention)
    - საკრედიტო ბარათების ნომრები
    - ხელით შექმნილი პატერნები(regex)
- HTTP მოთხოვნის პარამეტრებზე ზომის ლიმიტის დაყენების შესაძლებობა
- XML Schema/WSDL სტრუქტურის დაცვა
- WS-I თავსებადობის შემოწმება (XML)
- ერთი საიტისთვის დაკონფიგურირებული web სერვერებისთვის დატვირთვის გადანაწილება(Load Balancing)
- კონტენტის მარშრუტიზაცია კონფიგურირებადი წესების მიხედვით (host, path, header, client-ip, method, etc)

- სერვისის/საიტის(HTTP/HTTPS) უსაფრთხოების მომართვების ოპტიმიზაციისთვის, სწავლის შესაძლებლობა, წინასწარგანსაზღვრული “კარგი“ მომხმარებლების ტრაფიკის მიხედვით
- ატვირთული ფაილების ანტივირუსით შემოწმება
- URL_ების დაშიფვრის შესაძლებლობა (ე.წ.URL Encryption)
- სერვერებზე დატვირთვის შესამცირებლად, SSL დაშიფრული სესიის ორგანიზება. (ე.წ. SSL Offloading)
- Perfect Forward Secrecy/HSTS/SNI
- TLS 1.1/1.2
- ქეშირება და კომპრესია

პროტოკოლების მხარდაჭერა

- HTTP/S 1.1/2.0
- FTP/S

SIEM სისტემებთან ინტეგრაციის შესაძლებლობა:

- IBM Qradar
- RSA enVision
- HPE/Micro Focus ArcSight
- Splunk
- ლოგ ფორმატის მოდიფიკაცია მანუალურ რეჟიმში

ავთენტიპიკაციისა და ავტორიზაციის მექანიზმების მხარდაჭერა:

- LDAP
- RADIUS
- Local user database
- SAML
- User Certificate Authentication
- Multi-domain/Single Sign-On
- RSA SecurID
- Kerberos

DDoS -სგან დაცვის მექანიზმები:

- CAPTCHA_ს გამოყენება საეჭვო კლიენტებისთვის
- ნელი მოთხოვნებისგან დაცვა (Slowloris, Slow Read, etc)

IP მისამართების რეპუტაციის მიხედვით ბლოკირების ფუნქციონალი:

- გეოგრაფიული ლოკაციის მიხედვით
- proxy/tor სერვერები
- მანუალურად შექმნილი Blacklist
- გამონაკლისის დაშვება/ბლოკირება

ქსელური ფუნქციონალი:

- VLAN
- NAT (SNAT/DNAT)

- Static Routing

მოწყვლადობის სკანერებთან ინტეგრაციის შესაძლებლობა:

- HPE Security WebInspect
- HPE Security Fortify On Demand
- IBM AppScan
- ImmuniWeb

- REST API
- სისტემას უნდა გააჩნდეს მომხმარებლების როლური დაშვების/გრანულარულად უფლებების მინიჭების შესაძლებლობა.
- სანდო ჰოსტების ჯგუფის შექმნა და სერვისებთან ბლოკირების გარეშე დაშვების შესაძლებლობა.

1. კომპანიამ უნდა წარადგინოს შესაბამისი სერთიფიკატები, რომელიც ადასტურებენ მის კომპეტენციას აღშნინული გადაწყვეტილების მხარდაჭერის მომსახურების განსახორციელებლად, კერძოდ:

   Certified Engineer

   Certified Support Technician

   Web Application Firewall Certified Product Specialist

2. მონაწილე კომპანიამ უნდა წარადგინოს მინიმუმ 3 რეკომენდატორი კომპანიების ჩამონათვალი;
3. პრეტენდენტ ორგანიზაციას უნდა გააჩნდეს ბოლო 2 წელიწადში იგივე მწარმოებლის მინიმუმ 3 ანალოგიური პროექტის განხორციელების გამოცდილება
4. მონაწილე კომპანიებმა უნდა წარმოადგინონ მწარმოებლის ავტორიზაციის წერილი (MAF);