**Πίνακας Συμμόρφωσης τεχνικών προδιαγραφών Web Application Firewalls**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **A/A** | **Τεχνικές Προδιαγραφές** | **Απαίτηση** | **Απάντηση** | **Παραπομπή** |
| **1** | **Γενικά** |   |   |   |
| 1.1 | Η προσφερόμενη λύση θα πρέπει να είναι φυσικό μηχάνημα | NAI |   |   |
| 1.2 | Το προσφερόμενο σύστημα θα αποτελείται από 2 ιδίου τύπου Web Application Firewalls (cluster των 2 συσκευών) | NAI |   |   |
| 1.3 | Υποστήριξη εύκολης πρόσβασης στην κονσόλα διαχείρισης μέσω Web interface | NAI |   |   |
| 1.4 | Υποστήριξη υψηλής διαθεσιμότητας HA | NAI |   |   |
| 1.5 | Υποστήριξη SNMP | NAI |   |   |
| 1.6 | Θα πρέπει να καταγράφει όλα τα authenticated events τοπικά και μέσω syslog server | Να αναφερθεί |   |   |
| 1.7 | Υποστήριξη backup του πλήρες configuration | NAI |   |   |
| 1.8 | Υποστήριξη τοπικής βάσης χρηστών | Να αναφερθεί |   |   |
| 1.9 | Υποστήριξη REST API για διασύνδεση με άλλες εφαρμογές. | Να αναφερθεί |   |   |
| **2** | **Φυσικά χαρακτηριστικά και επιδόσεις** |   |   |   |
| 2.1 | HTTP Throughput | >= 1 Gbps |   |   |
| 2.2 | Max HTTP trans/sec | >= 35.000 |   |   |
| 2.3 | Max new HTTP connections/sec | >= 30.000 |   |   |
| 2.4 | Max HTTP concurrent connection | >=700.000 |   |   |
| 2.5 | HTTPS Throughput (2048 Key) | >= 700 Mbps |   |   |
| 2.6 | Max HTTPS trans/sec | >= 15.000 |   |   |
| 2.7 | Max new HTTPS connections/sec | >= 10.000 |   |   |
| 2.8 | Max HTTPS concurrent connection | >= 500.000 |   |   |
| 2.9 | Network Interfaces (GE RJ45) | >= 6 |   |   |
| 2.10 | Network Interfaces (SFP) | Να αναφερθούν |   |   |
| 2.11 | Η προτεινόμενη λύση θα πρέπει να υποστηρίζει τους παρακάτω τρόπους λειτουργίας:* Inline Transparent
* True Transparent Proxy
* Reverse Proxy
* Non-Inline Sniffing.

Περιγράψτε τους τρόπους λειτουργίας αναλυτικά |     NAI |   |   |
| 2.12 | Υποστήριξη κεντρικής διαχείρισης | NAI |   |   |
| 2.13 | Υποστήριξη multi-tenancy | Να αναφερθεί  |   |   |
| **3** | **Χαρακτηριστικά ασφάλειας** |   |   |   |
| 3.1 | Προστασία των web εφαρμογών και της υποδομής  | NAI |   |   |
| 3.2 | Η λύση θα πρέπει να υποστηρίζει το positive security model, δηλαδή να έχει τη δυνατότητα να κάνει ένα δυναμικό προφίλ (dynamic profiling/Auto learning) των εφαρμογών web που προστατεύει. Περιγράψτε πως αυτό υλοποιείται. | NAI |   |   |
| 3.3 | Η λύση θα πρέπει να μπορεί να ενεργοποιεί Protection και Dynamic Profiling ταυτόχρονα χωρίς το ένα να επηρεάζει τη λειτουργία του άλλου. |  ΝΑΙ |   |   |
| 3.4 | Η λύση θα πρέπει να υποστηρίζει το negative security model, δηλαδή την προστασία των web εφαρμογών με βάση signatures. |  ΝΑΙ |   |   |
| 3.5 | Υποστήριξη εξαιρέσεων ανά signature | ΝΑΙ |   |   |
| 3.6 | Τα signatures θα πρέπει να είναι σε γκρουπ και να δίνεται η δυνατότητα αναζήτησης.  |  ΝΑΙ |   |   |
| 3.7 | Θα πρέπει να υπάρχει signatures οι οποίες προστατεύουν κατ’ ελάχιστο από τις παρακάτω απειλές:* Cross Site Scripting
* SQL Injection
* Generic Attacks
* Known Exploits
* Trojans
* Information Disclosure
* Bad Robot
* Credit Card Detection
 |      ΝΑΙ |   |   |
| **4** | **Anti-DDoS** |   |   |   |
| 4.1 | Η λύση θα πρέπει να προσφέρει Anti-DDoS προστασία σε layer 7 | NAI |   |   |
| 4.2 | Η προστασία από DDoS θα πρέπει να υποστηρίζει κατ’ ελάχιστον τα παρακάτω:* HTTP Request limit per source
* TCP Connections using same cookie
* HTTP requests using the same cookie
* Μηχανισμός challenge response ο οποίος θα είναι τελείως transparent για τον τελικό χρήστη
 |     NAI |   |   |
| **5** | **Προστασία αλλαγής περιεχομένου web-site  (Αnti-web-defacement)** |   |   |   |
| 5.1 | Υποστήριξη anti-web-defacement, δηλαδή θα πρέπει να έχει τη δυνατότητα να αναγνωρίζει και να αποτρέπει τις προσπάθειες αλλαγής του περιεχομένου ενός web site καθώς επίσης να έχει αυτόματους μηχανισμούς επαναφοράς του στην αρχική του μορφή |   NAI |   |   |
| 5.2 | Θα πρέπει να αντιγράφει τα περιεχόμενα του web site στον δίσκο που διαθέτει και να τα συγκρίνει ανά τακτά χρονικά διαστήματα με αυτά που βρίσκονται στο ίδιο το web site |  NAI |   |   |
| 5.3 | Θα πρέπει να δίνεται η δυνατότητα αυτόματης ή ελεγχόμενης επαναφοράς των αρχείων που έχουν αλλαχθεί |  NAI |   |   |
| 5.4 | Για την αντιγραφή αρχείων θα πρέπει να υποστηρίζονται κατ’ ελάχιστον τα FTP/SSH/Windows File Share |  NAI |   |   |
| **6** | **Επιβεβαίωση των HTTP RFC standards** |   |   |   |
| 6.1 | Η λύση θα πρέπει να επιβεβαιώνει τα HTTP RFC standards. | NAI |   |   |
| 6.2 | Nα ελέγχονται και να επιβάλλονται:* Illegal Host Name
* Illegal HTTP Version
* Illegal HTTP Request Method
* Content Length
* Body Length
* Header Length
* Header Line Length
* Number of Header Lines in Request
* Total URL and Body Parameters Length
* Number of URL Parameters
* Number of Cookies in Request
* Number of ranges in Range Header
* Malformed Request
 |        Να αναφερθούν |   |   |
| **7** | **Επιβολή επιχειρησιακής λογικής των εφαρμογών** |   |   |   |
| 7.1 | Επιβολή αρχικών σελίδων. Ο χρήστης θα πρέπει να προσπελάσει την αρχική σελίδα πριν προχωρήσει στην επόμενη |  Να αναφέρεται |   |   |
| 7.2 | Η λύση θα πρέπει να μπορεί να μαθαίνει αυτόματα τις απαιτούμενες παραμέτρους των URLs και να τις επιβάλλει |  NAI |   |   |
| 7.3 | Η λύση θα πρέπει να μπορεί να ανιχνεύει την χρήση cookies σε επίπεδο σελίδας URL |  NAI |   |   |
|   7.4 | Μηχανισμοί τροποποίησης του περιεχομένου:• URL rewriting (obfuscation)• Cookie signing• Cookie encryption• Custom error messages• Error code handling |   Να αναφέρονται |   |   |
| **8** | **Δυνατότητες Application Delivery** | **Εάν παρέχονται, να αναφέρονται** |   |   |
| 8.1 | **Διαμοιρασμός Φορτίου (Load Balancing)** |   |   |   |
| 8.2 | Υποστήριξη Server Load Balancing σε πολλαπλούς servers.  |   |   |   |
| 8.3 | Υποστήριξη των παρακάτω load balancing αλγόριθμων:* Round Robin
* Weighted Round Robin
* Least Connection
 |   |   |   |
| 8.4 | Υποστήριξη server persistence και κατ’ ελάχιστο των παρακάτω persistence δυνατοτήτων:* Persistent IP
* Persistent Cookie
* Insert Cookie
* ASP Session ID
* PHP Session ID
* JSP Session ID
 |   |   |   |
| 8.5 | Υποστήριξη αφαίρεσης ενός server από το Pool με εύκολο τρόπο για λόγους συντήρησης χωρίς αν υπάρχει καμία διατάραξη στο user experience |   |   |   |
| 8.6 | Πραγματοποίηση συνεχών health checks για λόγους αφαίρεσης από το pool των διαθέσιμων servers σε περίπτωση που κάποιος δεν είναι διαθέσιμος.Η λειτουργία αυτή θα πρέπει να είναι διαθέσιμη τόσο σε servers που γίνονται load balanced όσο και σε αυτούς που δεν γίνονται. |   |   |   |
| 9 | **Publishing εφαρμογών** |   |   |   |
| 9.1 | Υποστήριξη publishing web εφαρμογών και παροχή δυνατοτήτων SSO πρόσβασης | NAI |   |   |
| 9.2 | Υποστήριξη των πιο συνηθισμένων εφαρμογών * Microsoft ActiveSync
* Microsoft Outlook Web Access
* Microsoft SharePoint
* Microsoft Lync
* Other off-the-shelf applications
 |   |   |   |
| **10** | **Monitoring and reporting** | NAI |   |   |
| 10.1 | Logging and Reporting | NAI |   |   |
| 10.2 | Αποθήκευση πληροφορίας των events | NAI |   |   |
| 10.3 | Αποθήκευση πληροφορίας των alerts | NAI |   |   |
| 10.4 | Αποθήκευση πληροφορίας της κίνησης | NAI |   |   |
| 10.5 | Αποστολή όλης της παραπάνω πληροφορίας σε εξωτερικό σύστημα συλλογής του ίδιου κατασκευαστή ή 3rd party | NAI |   |   |
| 10.6 | Αποστολή όλης της παραπάνω πληροφορίας σε syslog server | NAI |   |   |
| 10.7 | Τα μηνύματα alert να περιλαμβάνουν τα παρακάτω:* Source και Destination της σύνδεσης
* Εκτενές packet header πληροφορία
* Raw and Hex body presentation for POST parameters
* Full Parameter view
* Highlighting the attack in the attack log
* With cookie alerts show the alerted cookie and changed values
* The solution should aggregate logging per day and per attack type
* The log should show both original encoding and decoded values for analysis
 |       Να αναφέρονται |   |   |
| 10.8 | Υποστήριξη της υφιστάμενης λύσης SIEM IBM QRadar  | ΝΑΙ |   |   |
| **11** | **Ανάλυση δεδομένων** |   |   |   |
| 11.1 | Dashboard μέσω του οποίου θα φαίνονται οι παρακάτω πληροφορίες:* Attacks per Country
* Hits per Country
* Data per Country
* Exportable to PDF
* Clickable view of the various attacks per website
* Zoom-able world map with color coding of attacks
 |     Να αναφέρεται |   |   |
| **12** | **Αποκλεισμός IP διευθύνσεων**  |  |   |   |
| 12.1 | Θα πρέπει να παρέχεται η δυνατότητα αποκλεισμού των IP διευθύνσεων | ΝΑΙ |   |   |
| 12.2 | Θα πρέπει να παρέχει μια εικόνα όλων των IP διευθύνσεων που έχουν που έχουν αποκλειστεί, καθώς επίσης και του χρονικού διαστήματος που θα είναι αποκλεισμένες. |   Να αναφέρεται |   |   |
| 12.3 | Να είναι δυνατή η ελευθέρωση μιας IP διεύθυνσης που έχει αποκλειστεί | NAI |   |   |
| **13** | **Συμμόρφωση** |   |   |   |
| 13.1 | Η λύση θα πρέπει να μπορεί να προστατεύει τις web εφαρμογές από τις πιο γνωστές απειλές όπως αυτές περιγράφονται στο OWASP 10. | NAI |   |   |
| 13.2 | Θα πρέπει να διαθέτει πιστοποίηση από ICSA | NAI |   |   |
| **14** | **Προδιαγραφές τεχνικής υποστήριξης και ειδικοί όροι** |   |   |   |
| 14.1 | Υπηρεσίες εγκατάστασης, παραμετροποίησης, πιλοτικής λειτουργίας και εκπαίδευσης. Η εγκατάσταση θα πρέπει να ολοκληρωθεί το αργότερο εντός 25 εργάσιμων ημερών από την έναρξη της υλοποίησης. Η εκπαίδευση θα διαρκέσει 1 εργάσιμη ημέρα (8 ώρες) και θα λάβει χώρα μετά την ολοκλήρωση της εγκατάστασης | NAI |   |   |
| 14.2 | Ο Ανάδοχος καλείται να προσφέρει ένα (1) έτος εγγύηση καλής λειτουργίας της προσφερόμενης λύσης η οποία θα αρχίζει από την υπογραφή του Πρωτοκόλλου Οριστικής Παραλαβής |   NAI |   |   |
| 14.3 | Ο Ανάδοχος θα προσφέρει υπηρεσίες συντήρησης, τεχνικής υποστήριξης (9x5 NBD) και ενημερωμένων εκδόσεων για ένα (1) έτος από την υπογραφή του Πρωτοκόλλου Οριστικής Παραλαβής | NAI |   |   |
| 14.4 | Ο Ανάδοχος θα πρέπει να είναι πιστοποιημένος στη διαχείριση της ασφάλειας κατά ISO/IEC 27001 | NAI |   |   |