

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ

ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ, ΕΡΕΥΝΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ

ΓΕΝΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΕΡΕΥΝΑΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ

**ΙΔΡΥΜΑ ΤΕΧΝΟΛΟΓΙΑΣ ΚΑΙ ΕΡΕΥΝΑΣ**

**Ινστιτούτο Πληροφορικής**

Ταχ. Διεύθυνση: Ν. Πλαστήρα 100, Βασιλικά Βουτών

ΤΚ 70013, Ηράκλειο Κρήτης

 Αρ. πρωτ. 1031

 Ηράκλειο: 14/06/2016

**Προμήθεια εξοπλισμού “Web Application Firewall”**

Το ΙΠ/ΙΤΕ προτίθεται να προμηθευτεί με απευθείας ανάθεση εξοπλισμό τύπου “Web Application Firewall”.

Προϋπολογισμός δαπάνης **15.000** ευρώ μη συμπεριλαμβανομένου του ΦΠΑ. Κριτήριο για την ανάθεση της προμήθειας είναι η συμφερότερη προσφορά.

Οι προσφορές πρέπει να κατατεθούν με email στην διεύθυνση **procurement at ics dot forth dot gr** έως την 27/06/2016 – 12:00 σε θέμα (subject) “Προσφορά Εξοπλισμού Web Application Firewall”.

Ο εξοπλισμός θα πρέπει να είναι επώνυμου κατασκευαστή διεθνούς εμβέλειας. Ο προσφερόμενος εξοπλισμός θα πρέπει να παραδοθεί σαν ενιαίο λειτουργικό σύνολο. Όλος ο εξοπλισμός θα πρέπει να είναι του ίδιου κατασκευαστή και να περιλαμβάνει τα απαραίτητα εξαρτήματα για την διασύνδεση του, να είναι καινούργιος και αμεταχείριστος, κατάλληλος για εγκατάσταση σε standard rack 19”.

Η διαχείριση του εξοπλισμού θα πρέπει να μπορεί να γίνει μέσω web interface και remote shell μεσω ssh και σειριακής θύρας.

Να διαθέτει τουλάχιστον:

* τέσσερις (4) θύρες δικτυακής διασύνδεσης RJ45 10/100/1000
* τέσσερις (4) θύρες SPF / GE
* μία θύρα USB,
* εσωτερικό δίσκο SSD 240GB τουλάχιστον
* σειριακή θύρα (console port)

Η ταχύτητα επεξεργασίας θα πρέπει να διασφαλίζει διαμεταγωγή (firewall throughput) 100Mbps/10.000 transactions/sec σε πλήρες φορτίο HTTP και 70Mbps/5.000 transactions/sec σε πλήρες φορτίο HTTPS, ενώ η εισαγόμενη καθυστέρηση θα πρέπει να είναι μικρότερη του msec.

Θα πρέπει να παρέχει εξειδικευμένη προστασία και αναγνώριση απειλών (threat detection/prevention) σε επίπεδο εφαρμογής (application layer) για υπηρεσίες HTTP/HTTPS όπως Tomcat/nginx/MS IIS/Outlook WebApp/Joomla και άλλες. Θα πρέπει να περιλαμβάνει λογισμικό web vulnerability scanning, HTTP firewall, denial of service attack prevention. Θα πρέπει να μπορεί να προστατεύσει τους web server από απειλές τύπου SQL injection και cross-site scripting.

Θα πρέπει να μπορεί να ρυθμιστεί έτσι ώστε:

* Να παρέχει δυνατότητα blocking μέσω ip-reputation lists
* Geo-information (source address geo location)
* Connection number limit
* http request limit

Θα πρέπει να προστατεύει web services από τουλάχιστον:

* BEAST
* AMF protocol attacks
* Brute force login attacks on forms
* Cookie tampering
* XSS
* HTTP header overflow
* SQL Injection
* Malformed XML
* DoS Attacks
	+ Botnets
	+ Low rate Dos
	+ Slow post
	+ Syn flood

O ανάδοχος θα πρέπει να εγκαταστήσει και θέσει σε λειτουργία τον εξοπλισμό κάνοντας τις απαραίτητες παραμετροποιήσεις.

 Από την κατασκευάστρια εταιρία θα πρέπει να παρέχονται online ενημερώσεις των signatures και η συσκευή θα πρέπει να παρέχεται με συνδρομή ενός έτους τουλάχιστον.

**Πληροφορίες:**

**Ίδρυμα Τεχνολογίας και Έρευνας**

**Ινστιτούτο Πληροφορικής**

**Ταχ. Διεύθυνση: Ν. Πλαστήρα 100, Βασιλικά Βουτών**

**ΤΚ 70013, Ηράκλειο Κρήτης**

**Συκάς Παναγιώτης**

**email: sikas at ics dot forth dot gr**

**τηλ: 2810391647**