

ΠΡΟΣΚΛΗΣΗ ΥΠΟΒΟΛΗΣ ΠΡΟΣΦΟΡΑΣ

Το ΤΕΙ Κεντρικής Μακεδονίας αφού έλαβε υπόψη:

1. Το Ν. 4412/2016 (ΦΕΚ-147 Α/8-8-16-Διορθ.Σφαλμ. Στα ΦΕΚ-200 Α/24-10-16 και ΦΕΚ-206 Α/3-11-16): Δημόσιες Συμβάσεις Έργων, Προμηθειών και Υπηρεσιών (προσαρμογή στις Οδηγίες 2014/24/ΕΕ και 2014/25/ΕΕ),
2. τα προβλεπόμενα στην παρ. 17 του άρθρου 22 του Ν.4441/2016, ΦΕΚ-227 Α/6-12-16
3. τα προβλεπόμενα στο άρθρο 22 του Ν.4144/13
4. τα προβλεπόμενα στο άρθρο 84 του Ν.4485/17 (ΦΕΚ 114 Α/04-08-2017) «Οργάνωση και λειτουργία της ανώτατης εκπαίδευσης, ρυθμίσεις για την έρευνα και άλλες διατάξεις»,
5. τα προβλεπόμενα στο άρθρο 107 του Ν.4497/17 (ΦΕΚ 171 Α/13-11-2017): Άσκηση υπαίθριων εμπορικών δραστηριοτήτων, εκσυγχρονισμός της επιμελητηριακής νομοθεσίας και άλλες διατάξεις,
6. την Υ.Α. 209650/Ζ1/30-11-2017 (ΦΕΚ 642/Υ.Ο.Δ.Δ./4-12-2017) με την οποία διαπιστώνεται η εκλογή του κ. Δ. Χασάπη ως Πρύτανη του Ιδρύματος,
7. την αριθ. πρωτ. 4531/7.12.2017 (ΑΔΑ: 715Γ469143-ΨΜΑ) Απόφαση του Πρύτανη του ΤΕΙ ΚΜ, Καθηγητή Δημητρίου Χασάπη, με θέμα: “Καθορισμός τομέων ευθύνης – αρμοδιοτήτων των Αντιπρυτάνεων του Τ.Ε.Ι. ΚΜ-Σειρά αναπλήρωσης του Πρύτανη του ΤΕΙ ΚΜ”, η οποία δημοσιεύθηκε στην Εφημερίδα της Κυβερνήσεως (Αρ. Φύλλου 4431/τ.Β’/15.12.2017),
8. Τη διόρθωση σφάλματος στην αριθμ.4531/7.12.2017 απόφαση του Πρύτανη του Τεχνολογικού Εκπαιδευτικού Ιδρύματος Κεντρικής Μακεδονίας, που δημοσιεύθηκε στο ΦΕΚ 4431/τ.Β’/15.12.2017
9. το αριθ. 1582/10-04-2019 αίτημα προμήθειας αγαθών (ΑΔΑΜ:19REQ004768590 2019-04-10)
10. την με αρ. πρωτ. 1588/10-04-2019(α/α 188, ΑΔΑ: 63ΜΞ469143-1ΜΩ, ΑΔΑΜ: 19REQ004771061 2019-04-10) απόφαση δέσμευσης σε βάρος του προϋπολογισμού του Ιδρύματος οικονομικού έτους 2019 (ΚΑΕ 7127.01)

καλεί

τους ενδιαφερόμενους οικονομικούς φορείς να υποβάλλουν προσφορά, για την δαπάνη προμήθειας «Κεντρικού Συστήματος FIREWALL για τις ανάγκες του ΤΕΙ Κεντρικής Μακεδονίας» συνολικού προϋπολογισμού 5.952,00€ (καθαρό ποσό 4.800,00€ + Φ.Π.Α 24%)

Η δαπάνη θα βαρύνει τις πιστώσεις του προϋπολογισμού εξόδων του Ιδρύματος οικονομικού έτους 2019, ΚΑΕ 7127.01

Κριτήριο κατακύρωσης : η πλέον συμφέρουσα από οικονομική άποψη προσφορά βάσει τιμής.

Παρακαλούμε για την προμήθεια των αγαθών του παρακάτω πίνακα:

A/A	Περιγραφή	Ποσότητα	CPV	Προϋπολογισμός χωρίς Φ.Π.Α	Φ.Π.Α.	Συνολικός Προϋπολογισμός με Φ.Π.Α	Κ.Α.Ε.
1	Κεντρικό Σύστημα Firewall	1	32420000-3	4.800,00	1.152,00	5.952,00	7127.01
	ΣΥΝΟΛΟ			4.800,00	1.152,00	5.952,00	

Τακτικός Προϋπολογισμός

Πρόγραμμα Δημοσίων Επενδύσεων

Αναλυτικές τεχνικές προδιαγραφές των υπό προμήθεια αγαθών:

1. Κεντρικό Σύστημα Firewall

	ΠΕΡΙΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ
	ΓΕΝΙΚΑ	
1.	Λειτουργία μη βασισμένη σε ευρέως διαδεδομένες γενικής χρήσης πλατφόρμες λειτουργικών συστημάτων.	ΝΑΙ
2.	Δυνατότητα διασύνδεσης σε τοπολογία active/active και active/standby χωρίς την ανάγκη επιπλέον αδειών ή λογισμικού.	ΝΑΙ
3.	Αριθμός συσκευών	1
4.	Να αναφερθεί Τύπος – Κατασκευαστής – Σειρά – Μοντέλο.	ΝΑΙ
5.	Δυνατότητα εγκατάστασης σε ικρίωμα.	ΝΑΙ
6.	Διεπαφές Gigabit Ethernet ανά συσκευή.	>=8
7.	Μνήμη DRAM ανά συσκευή.	>= 8GB
8.	Μνήμη Flash ανά συσκευή.	>= 8GB
9.	Μέγιστο throughput του κόμβου Firewall ανά συσκευή.	>=1.8Gbps
10.	Μέγιστο Throughput του κόμβου Firewall (multiprotocol) ανά συσκευή.	>=900 Mbps
11.	Μέγιστο Throughput του κόμβου Firewall σε 3DES/AES VPN ανά συσκευή.	>=250 Mbps
12.	Μέγιστο Throughput του κόμβου με application control (AVC) ανά συσκευή	>= 850 Mbps
13.	Μέγιστο Throughput του κόμβου με application control (AVC) και Intrusion Prevention (IPS) ανά συσκευή.	>= 450 Mbps
14.	Μέγιστο Throughput του κόμβου με application control (AVC) και Intrusion Prevention (IPS) ανά συσκευή (440 byte HTTP).	>=300Mbps
15.	Ρυθμός δημιουργίας νέων συνδέσεων (CPS) ανά συσκευή.	>=20.000
16.	Ελάχιστος υποστηριζόμενος αριθμός ταυτόχρονων συνδέσεων ανά συσκευή.	>=250.000

17.	Ελάχιστος υποστηριζόμενος αριθμός ταυτόχρονων χρηστών ανά συσκευή.	Χωρίς Όριο
18.	Ελάχιστος υποστηριζόμενος αριθμός ταυτόχρονων συνδέσεων IPSEC site-to-site ανά συσκευή.	>=300
19.	Ελάχιστος υποστηριζόμενος αριθμός ταυτόχρονων συνδέσεων SSL VPN client ανά συσκευή.	>= 300
20.	Ελάχιστος υποστηριζόμενος αριθμός VLANs ανά συσκευή.	>=100
21.	Ελάχιστος υποστηριζόμενος αριθμός VirtualFirewalls ανά συσκευή.	>=2
22.	Ο κάθε κόμβος θα πρέπει να διαθέτει σκληρό δίσκο solidstate.	NAI
23.	Ελάχιστη χωρητικότητα του κάθε σκληρού δίσκου solidstate για κάθε συσκευή.	>= 100GB
24.	Υποστήριξη αρχιτεκτονικής StatefulInspection για κάθε συσκευή.	NAI
25.	Υποστήριξη πρωτοκόλλων IPv4 και IPv6 για κάθε συσκευή.	NAI
26.	Δυνατότητα transparent λειτουργίας (L2 firewall) για κάθε συσκευή.	NAI
27.	Υποστήριξη στατικής δρομολόγησης για κάθε συσκευή.	NAI
28.	Υποστήριξη δυναμικής δρομολόγησης με RIPv2, OSPFv2, ISIS και BGPv4 πρωτοκόλλων για κάθε συσκευή.	NAI
29.	Υποστήριξη δρομολόγησης μέσω πολιτικών (PolicyBasedRouting) για κάθε συσκευή.	NAI
30.	Υποστήριξη δρομολόγησης multicast για κάθε συσκευή.	NAI
31.	Υποστήριξη VXLAN για κάθε συσκευή.	NAI
32.	Υποστήριξη LACP για κάθε συσκευή.	NAI
33.	Υποστήριξη διασύνδεσης με ActiveDirectory, LDAP και RADIUS για κάθε συσκευή.	NAI
34.	Υποστήριξη, για κάθε συσκευή, κανόνων ελέγχου πρόσβασης (Access ControlRules): Έλεγχος εισερχόμενης και εξερχόμενης κίνησης Κανόνες ανά VLAN Κανόνες ανά χρήστη Ομαδοποίηση κανόνων Ενεργοποίηση - απενεργοποίηση κανόνων	NAI
35.	Υποστήριξη παθητικής αναγνώρισης (profiling) των χρηστών, των δικτυακών συσκευών και των επικοινωνιών μεταξύ virtualmachines για κάθε συσκευή.	NAI
36.	Υποστήριξη αναγνώρισης των hosts, του λειτουργικού συστήματος αυτών και των ευπαθειών των εφαρμογών, για κάθε συσκευή.	NAI
37.	Υποστήριξη αναγνώρισης customapplications.	NAI
38.	Υποστήριξη για κάθε συσκευή αναγνώρισης εφαρμογών και εφαρμογή διαφορετικής πολιτικής ανά εφαρμογή / χρήστη.	NAI
39.	Υποστήριξη ελέγχου κίνησης SSL, SMTPS, POPS, FTPS, Telnet και IMAPS.	NAI
40.	Υποστήριξη DNS πολιτικών με δυνατότητα redirect ενός DNS query σε ένα sinkholeserver.	NAI
41.	Υποστήριξη για κάθε συσκευή δημιουργίας customsignatures από τον διαχειριστή.	NAI
42.	Υποστήριξη SSL Decryption σε κάθε συσκευή	NAI
43.	Κάθε συσκευή θα συνεργάζεται με άλλες συσκευές του δικτύου για αποτελεσματικότερη προστασία, συνεργασία μέσω openAPIs με εφαρμογές τρίτων κατασκευαστών όπως vulnerabilitymanagementsystems, securityinformationandeventmanagement (SIEM) applications, networkaccesscontrol (NAC) κ.α.	NAI
44.	Υποστήριξη κρυπτογράφησης δεδομένων με χρήση αλγορίθμου Triple-DES (168-bit) και AES (128, 192, και 256-bit) σε κάθε συσκευή.	NAI
	INTRUSION PREVENTION (IPS)	Τα παρακάτω χαρακτηριστικά δεν απαιτούνται να προσφερθούν αλλά να υποστηρίζονται σε μελλοντική αναβάθμιση με την προσθήκη κατάλληλων αδειών.
45.	Υποστήριξη για κάθε συσκευή ενσωματωμένου μηχανισμού εντοπισμού και αποτροπής επιθέσεων IntrusionPrevention για	Σε μελλοντική αναβάθμιση

	την αποτροπή τόσο γνωστών όσο και αγνώστων απειλών ασφαλείας (knownandunknownthreats)	
46.	Υποστήριξη για κάθε συσκευή αυτοματοποιημένης προτεινόμενης πολιτικής και υπογραφών IPS ανάλογα με το προστατευμένο δίκτυο για να εμποδίσει τις αναδυόμενες επιθέσεις.	Σε μελλοντική αναβάθμιση
47.	Να είναι δυνατή για κάθε συσκευή η δημιουργία διαφορετικής πολιτικής IPS για διαφορετική κίνηση ανάμεσα σε διαφορετικά source/destination.	Σε μελλοντική αναβάθμιση
48.	Για κάθε συσκευή οι υπογραφές του IPS θα πρέπει να ανανεώνονται τακτικά και αυτόματα, με πρόβλεψη του κατασκευαστή του εξοπλισμού ασφαλείας, ώστε να προστατεύουν ουσιαστικά από νέες απειλές	Σε μελλοντική αναβάθμιση
	ANTI-MALWARE	Τα παρακάτω χαρακτηριστικά δεν απαιτούνται να προσφερθούν αλλά να υποστηρίζονται σε μελλοντική αναβάθμιση με την προσθήκη κατάλληλων αδειών.
49.	Υποστήριξη ενσωματωμένου μηχανισμού εντοπισμού και αποτροπής malware τόσο γνωστών όσο και αγνώστων (knownandunknownmalwares)	NAI
50.	Υποστήριξη malwareinspection για αρχεία nested μέσα σε archives (για παράδειγμα .zip ή .rar).	NAI
51.	Υποστήριξη Sandboxing σε κάθε συσκευή.	NAI
	URL FILTERING	Τα παρακάτω χαρακτηριστικά δεν απαιτούνται να προσφερθούν αλλά να υποστηρίζονται σε μελλοντική αναβάθμιση με την προσθήκη κατάλληλων αδειών.
52.	Υποστήριξη φίλτρων URL σε κάθε συσκευή	NAI
53.	Υποστήριξη ομαδοποιημένων κατηγοριών φίλτρων URL και ιστότοπων σε κάθε συσκευή	NAI
54.	Υποστήριξη λεπτομερών φίλτρων Web με δυνατότητα δημιουργίας πολιτικών ανά λειτουργία της Web εφαρμογής και όχι μόνο εφαρμογή σε όλη την πολιτική (πχ απαγόρευση πρόσβασης μόνο σε FacebookGames και όχι στο υπόλοιπο Facebook) σε κάθε συσκευή	NAI
	CLIENT VPN	Τα παρακάτω χαρακτηριστικά δεν απαιτούνται να προσφερθούν αλλά να υποστηρίζονται σε μελλοντική αναβάθμιση με την προσθήκη κατάλληλων αδειών.
55.	Δυνατότητα point-to-point και απομακρυσμένης σύνδεσης VPN (Remote Access VPN) με την χρήση λογισμικού Client σε κάθε συσκευή.	NAI
56.	Υποστήριξη VPN Client πολλαπλών λειτουργικών συστημάτων με κατ' ελάχιστον Windows, MAC OS και Linux VPN Clients σε κάθε συσκευή.	NAI
57.	Υποστήριξη MobileClients (π.χ. iPhone, Android κ.α.) σε κάθε συσκευή.	NAI
58.	Για κάθε συσκευή να υποστηρίζεται και να αναφερθεί ο τρόπος παραμετροποίησης διαφορετικής πολιτικής VPN ανάλογα με τον χρήστη και το λειτουργικό της συσκευής.	NAI
	ΚΕΝΤΡΙΚΗ ΔΙΑΧΕΙΡΙΣΗ	Τα παρακάτω χαρακτηριστικά δεν απαιτούνται να προσφερθούν αλλά να υποστηρίζονται σε μελλοντική αναβάθμιση με την προσθήκη κατάλληλων αδειών.
59.	Δυνατότητα κεντρικής διαχείρισης μέσω γραφικού περιβάλλοντος (GUI) και μέσω γραμμής εντολών (CLI).	NAI
60.	Υποστήριξη ανάλυσης της επίπτωσης κάθε απειλής (ImpactAnalysis) με διαχωρισμό των απειλών σε διαφορετικές κατηγορίες	NAI
61.	Το λογισμικό θα πρέπει να εγκαθίσταται σε υποδομή VMware.	NAI

62.	Κάθε συσκευή θα διατηρεί σε πραγματικό χρόνο λίστα με όλα τα hosts, applications, connections και χρήστες	ΝΑΙ
63.	Υποστήριξη συσχετισμού απειλών (correlation) με user, device, service και application.	ΝΑΙ
64.	Η εφαρμογή διαχείρισης πρέπει να υποστηρίζει μηχανισμό παραγωγής αναφορών σε επίπεδο χρήστη και εφαρμογής.	ΝΑΙ
65.	Η εφαρμογή διαχείρισης πρέπει να υποστηρίζει την δημιουργία customizabledashboard.	ΝΑΙ
66.	Η εφαρμογή διαχείρισης πρέπει να υποστηρίζει την δημιουργία custom και template-based reports.	ΝΑΙ
67.	Η εφαρμογή διαχείρισης πρέπει να υποστηρίζει προκαθορισμένες αναφορές που να μπορούν να γίνουν scheduled.	ΝΑΙ
68.	Η εφαρμογή διαχείρισης πρέπει να υποστηρίζει τον συσχετισμό συμβάντων (correlation).	ΝΑΙ
69.	Η εφαρμογή διαχείρισης πρέπει να υποστηρίζει OpenAPIs για την διασύνδεση με λύσεις άλλων κατασκευαστών logmanagement, security information and event management (SIEM), trouble ticketing, and patch management	ΝΑΙ
70.	Η εφαρμογή διαχείρισης πρέπει να υποστηρίζει λογαριασμούς ανάλογα με το ρόλο του διαχειριστή.	ΝΑΙ
71.	Μέσω του γραφικού περιβάλλοντος να είναι άμεση η ενημέρωση για την κατάσταση λειτουργίας των επί μέρους λειτουργιών και διεργασιών.	ΝΑΙ
ΕΓΚΑΤΑΣΤΑΣΗ - ΠΑΡΑΜΕΤΡΟΠΟΙΗΣΗ		
72.	Εργασίες εγκατάστασης, παραμετροποίησης και προσθήκης των απαραίτητων security policies και access lists σύμφωνα με τις ανάγκες του Ιδρύματος.	ΝΑΙ
ΕΓΓΥΗΣΗ ΚΑΙ ΣΥΝΔΡΟΜΕΣ		
73.	Να συνοδεύεται από 3 έτη εγγύηση (με αντικατάσταση την επόμενη εργάσιμη ημέρα) του κατασκευαστή για το λογισμικό και το υλικό συμπεριλαμβανομένης της τεχνικής υποστήριξης.	ΝΑΙ
74.	Η προσφερόμενη τεχνική υποστήριξη (περιλαμβάνεται και η παροχή και εγκατάσταση νέων ενημερώσεων/αναβαθμίσεων λογισμικού/drivers) θα παρέχεται από κατάλληλα πιστοποιημένα πρόσωπα από τον κατασκευαστή.	ΝΑΙ
75.	Προτεινόμενο μοντέλο	Cisco ASA 5516-Χή καλύτερο

Φάκελος Προσφοράς

Οι οικονομικοί φορείς θα πρέπει να προσκομίσουν τις προσφορές τους στο Τμήμα Διοικητικής Μέριμνας και Πρωτοκόλλου του Τ.Ε.Ι. Κεντρικής Μακεδονίας (Τέρμα Μαγνησίας, Σέρρες), **μέχρι και την Δευτέρα 22/04/2019 και ώρα 12:00 π.μ.**

Ο φάκελος της προσφοράς θα πρέπει να περιλαμβάνει τις παρακάτω ενδείξεις:

«ΣΤΟΙΧΕΙΑ ΤΟΥ ΥΠΟΨΗΦΙΟΥ» (Πλήρης Επωνυμία, Ταχυδρομική Διεύθυνση, τηλέφωνο, fax, διεύθυνση ηλεκτρονικού ταχυδρομείου, εφόσον υπάρχει.

ΠΡΟΣΦΟΡΑ

για την προμήθεια «Κεντρικού Συστήματος FIREWALL για τις ανάγκες του ΤΕΙ Κεντρικής Μακεδονίας»

ΑΝΑΘΕΤΟΥΣΑ ΑΡΧΗ: Τεχνολογικό Εκπαιδευτικό Ίδρυμα (Τ.Ε.Ι.)
Κεντρικής Μακεδονίας

ΚΑΤΑΛΗΚΤΙΚΗ ΗΜΕΡΟΜΗΝΙΑ ΚΑΤΑΘΕΣΗΣ ΠΡΟΣΦΟΡΩΝ :

Δευτέρα 22-04-2019 και ώρα 12:00 π.μ.

Να μην ανοιχτεί από την ταχυδρομική υπηρεσία ή το πρωτόκολλο

Ο φάκελος της προσφοράς θα πρέπει να περιλαμβάνει:

- Οικονομική προσφορά από την οποία να προκύπτει με σαφήνεια η προσφερόμενη τιμή.
- Χρόνος παράδοσης: 30ημέρες
- Υπεύθυνος Παραλαβής: Σάββας Πασχαλίδης

Υπεύθυνη δήλωση στην οποία δηλώνεται ότι είναι παραγωγός ή εισαγωγέας και είναι υπόχρεος να τηρεί τις υποχρεώσεις του Ν 2939/2001 και να είναι εγγεγραμμένος στο Εθνικό Μητρώο Παραγωγών(ΕΜΠΑ) με αριθμό _____ ή είναι διακινητής και δεν είναι υπόχρεος να τηρεί τις υποχρεώσεις του Ν 2939/2001 και να είναι εγγεγραμμένος στο Εθνικό Μητρώο Παραγωγών (ΕΜΠΑ) αλλά ο παραγωγός ή εισαγωγέας _____ (αναφέρεται ονομαστικά) των ειδών που θα προμηθεύσει στο πλαίσιο του διαγωνισμού είναι εγγεγραμμένος στο ΕΜΠΑ

Τον ανάδοχο που θα προκύψει βαρύνει κάθε νόμιμη κράτηση.

Κατά την εκτέλεση της παροχής υπηρεσίας ο ανάδοχος οφείλει να τηρεί τις υποχρεώσεις στους τομείς του περιβαλλοντικού, κοινωνικοασφαλιστικού και εργατικού δικαίου, που έχουν θεσπιστεί με το δίκαιο της Ένωσης, το εθνικό δίκαιο, συλλογικές συμβάσεις ή διεθνείς διατάξεις περιβαλλοντικού, κοινωνικοασφαλιστικού και εργατικού δικαίου, οι οποίες απαριθμούνται στο Παράρτημα Χ του Προσαρτήματος Α του ν. 4412/2016.

**Ο ΠΡΥΤΑΝΗΣ
ΤΟΥ Τ.Ε.Ι. ΚΕΝΤΡΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ**

**Χασάπης Δημήτριος
Καθηγητής**

Εσωτ. Διανομή:

- avdelas@teicm.gr, για ανάρτηση στο site του Τ.Ε.Ι. Κεντρικής Μακεδονίας
- Υπεύθυνος Προδιαγραφών Πασχαλίδης Σάββας τηλέφωνο 23210-49331
- Τμήμα Μισθοδοσίας, Αποζημιώσεων, Προμηθειών και Περιουσίας