ΒΟΥΛΗ ΤΩΝ ΕΛΛΗΝΩΝ

Δ Ι Α Κ Η Ρ Υ Ξ Η

Α ν ο ι κ τ ο ύ Η λ ε κ τ ρ ο ν ι κ ο ύ Δ η μ ό σ ι ο υ Δ ι α γ ω ν ι σ μ ο ύ για την προμήθεια δύο (2) συσκευών τείχους προστασίας περιμέτρου (firewalls) καθώς και την παροχή υπηρεσιών εγκατάστασης, παραμετροποίησης - βελτιστοποίησης λογικού σχεδιασμού δικτύου και υπηρεσιών τεχνικής υποστήριξης διάρκειας τριών (3) ετών

CPV:	**32420000-3/012** **Συσκευές Firewall**
ΕΚΤΙΜΩΜΕΝΗ ΑΞΙΑ ΣΥΜΒΑΣΗΣ:	**εκατόν σαράντα εννέα χιλιάδες ευρώ (149.000,00 €), πλέον Φ.Π.Α. 24%**
ΑΡΙΘΜΟΣ ΠΡΩΤΟΚΟΛΛΟΥ	**10646/7418-14.10.2025 (ΑΔΑ: 04-0Α06)**

ΑΘΗΝΑ, 23/10/2025

ΠΑΡΑΡΤΗΜΑ Ι

Πίνακας περιεχομένων

ΠΑΡΑΡΤΗΜΑ Ι – Αναλυτική Περιγραφή Φυσικού Αντικειμένου της Σύμβασης

1. Αντικείμενο του έργου

Η Αναθέτουσα Αρχή διαθέτει μια υποδομή πληροφορικής η οποία εξυπηρετεί συνολικά τις ανάγκες της Βουλής των Ελλήνων (ΒτΕ). Προκειμένου για την αποτελεσματικότερη παροχή νέων ηλεκτρονικών υπηρεσιών, η ΒτΕ στοχεύει, με το παρόν έργο, στην προμήθεια εξοπλισμού (υλικό / λογισμικό) με σκοπό την μεγιστοποίηση του επιπέδου ασφαλείας των πολύπλοκων υποδομών του κέντρου δεδομένων και την προστασία από διαρροή δεδομένων.

Η προμήθεια του εξοπλισμού και των υπηρεσιών περιγράφεται συνοπτικά στη συνέχεια.

2. Τεχνική περιγραφή

Ο εξοπλισμός που απαιτείται να προσφερθεί κατ' ελάχιστο από τον ανάδοχο για το κέντρο δεδομένων της ΒτΕ είναι μία λύση Ασφάλειας Δικτύου & Ασφαλούς Πρόσβασης στο Διαδίκτυο για την προστασία των κεντρικών υποδομών της ΒτΕ.

2.1 Λύση Ασφάλειας Δικτύου & Ασφαλούς Πρόσβασης στο Διαδίκτυο

Η προσφερόμενη λύση ασφάλειας θα αντικαταστήσει τους υφιστάμενους front-end firewalls και θα παρέχει προστασία του εταιρικού δικτύου από επιθέσεις και απειλές στο περιεχόμενο των δικτυακών επικοινωνιών, και θα εξασφαλίζει ασφαλή και ελεγχόμενη πρόσβαση των εσωτερικών χρηστών στο Διαδίκτυο. Η λύση θα καλύπτει τον έλεγχο της πρόσβασης των εσωτερικών χρηστών στο Διαδίκτυο και την ανάλυση των επικοινωνιών τους, ασχέτως του πρωτοκόλλου επικοινωνίας με σκοπό τον άμεσο εντοπισμό και καταστολή απειλών στο περιεχόμενο αυτών (π.χ. malware, malicious mobile code κ.α.). Επίσης η προσφερόμενη λύση θα παρέχει προστασία στους servers του εσωτερικού δικτύου της αναθέτουσας αρχής, μέσω Συστήματος Αποτροπής Εισβολών Network IPS , Application Level Firewalling κ.α. σε συνδυασμό με την κατάλληλη διαμόρφωση της δικτυακής αρχιτεκτονικής σε ξεχωριστή ζώνη.

Η προσφερόμενη λύση θα πρέπει κατ' ελάχιστο να περιλαμβάνει τις παρακάτω λειτουργίες:

- Real-time Threat Prevention – έλεγχος όλης της δικτυακής κίνησης ασχέτως του πρωτοκόλλου επικοινωνίας για απειλές με δυνατότητα ανίχνευσης, καταστολής και ενημέρωσης απειλών σε πραγματικό χρόνο.

- URL Filtering – έλεγχος της πρόσβασης των χρηστών σε συγκεκριμένες κατηγορίες ιστοσελίδων με δυνατότητα εφαρμογής διαφορετικών πολιτικών ανά domain user/group

- Application Identification & Control – αναγνώριση και έλεγχος των εφαρμογών που δραστηριοποιούνται στο εταιρικό δίκτυο ανεξαρτήτως πρωτοκόλλου επικοινωνίας με έμφαση στις εφαρμογές που συνδέονται στο Διαδίκτυο.

- Antivirus & Antimalware Protection – έλεγχος όλης της δικτυακής κίνησης ασχέτως του πρωτοκόλλου επικοινωνίας για πιθανή διακίνηση κακόβουλου λογισμικού

- File Type Filtering - έλεγχος της δικτυακής διακίνησης αρχείων ασχέτως πρωτοκόλλου επικοινωνίας και εφαρμογής διαφορετικών πολιτικών ανά τύπο αρχείου αναγνωρίζοντας τα αρχεία από το payload τους και όχι μόνο από την κατάληξή τους.

• Quality-of-Service – δυνατότητα εφαρμογής πολιτικών ορθής χρήσης των δικτυακών πόρων με καθορισμό συγκεκριμένου δικτυακού εύρους και προτεραιότητας ανά χρήστη και εφαρμογή

• SSL Scanning: Ανάλυση και έλεγχος ασφάλειας των κρυπτογραφημένων Web επικοινωνιών (SSL traffic)

• Real-time Monitoring & Statistics – δυνατότητα παρακολούθησης της κατάστασης ασφάλειας του δικτύου σε πραγματικό χρόνο, παροχή στατιστικών όσων αφορά τις προσβάσεις των χρηστών, τις εφαρμογές που χρησιμοποιούνται, το όγκο των επικοινωνιών που αναπτύσσουν, τις απειλές που εντοπίζονται, τα δεδομένα που διακινούνται κ.α.

• Logging & Reporting - Παραγωγή συγκεντρωτικών και αναλυτικών αναφορών με βάσει πολλαπλά κριτήρια όπως συγκεκριμένος χρήστης, εφαρμογή, σύστημα, είδος απειλής κ.α. και μετέπειτα αποστολή τους στο υφιστάμενο σύστημα SIEM.

• SPAM Detection & Filtering- θα πρέπει να υποστηρίζεται και να είναι ενσωματωμένη στα gateways, για την ανίχνευση και αποτροπή απειλών στην email κίνηση, από το επίπεδο της περιμέτρου.

• Patient zero σύστημα - θα πρέπει να ανιχνεύονται και να αποτρέπονται μολύνσεις ακόμα και στο patient-zero σύστημα, χωρίς να βασίζεται στη δημιουργία υπογραφών (signatures).

• Content inspection - θα πρέπει να υποστηρίζεται και να διατίθεται ενσωματωμένο, για την ανίχνευση και αποτροπή συγκεκριμένων data types, κατ' ελάχιστο PCI, IBAN, JAVA.

3. Υπηρεσίες του Έργου

Για την ολοκλήρωσης της εγκατάστασης της προσφερόμενης λύσης ο Ανάδοχος υποχρεούται να παρέχει τις παρακάτω υπηρεσίες ενός τουλάχιστον ανθρωπομήνα (1 ΑΜ) και να μεριμνήσει για τη μετάπτωση (migration) όπως αυτή θα πρέπει να έχει περιγραφεί αναλυτικά στην μελέτη εφαρμογής.

Οι υπηρεσίες που θα πρέπει να προσφέρει ο Ανάδοχος στο πλαίσιο του έργου, διακρίνονται στις παρακάτω κατηγορίες:

- Υπηρεσίες Μελέτης Εφαρμογής
- Υπηρεσίες Εγκατάστασης – Μετάπτωσης
- Υπηρεσίες Εκπαίδευσης
- Υπηρεσίες Υποστήριξης Πιλοτικής Λειτουργίας και
- Εγγύηση - Υπηρεσίες Υποστήριξης Παραγωγικής Λειτουργίας

Οι υπηρεσίες του Αναδόχου θα προσφερθούν στα κεντρικά γραφεία της ΒτΕ. Οποιαδήποτε μετακίνηση ή άλλου τύπου έξοδα που αφορούν στο Έργο και απαιτούνται για την επίτευξη των σκοπών του έργου βαρύνει τον Ανάδοχο. Η ΒτΕ θα φροντίσει, εφόσον ο Ανάδοχος το επιθυμεί και το προσδιορίσει, να του διατεθούν χώροι στους ανωτέρω χώρους κατά τη διάρκεια της εκτέλεσης συγκεκριμένων εργασιών.

3.1 Υπηρεσίες Μελέτης Εφαρμογής

Ο Ανάδοχος θα πρέπει να εκπονήσει μελέτη εφαρμογής, που θα συνιστά τον «οδηγό υλοποίησης» και τη βάση αναφοράς για την παρακολούθηση της προόδου των εργασιών και όλων των επί μέρους δραστηριοτήτων καθ' όλη την διάρκεια υλοποίησης του Αντικειμένου της Σύμβασης.

Στην μελέτη εφαρμογής θα πρέπει να συμπεριλαμβάνονται η προτεινόμενη από τον Ανάδοχο τμηματοποίηση (Segmentation) του δικτύου της ΒτΕ, η παραμετροποίηση, η μεθοδολογία μετάπτωσης και οι δοκιμές που πρέπει να γίνουν για την αξιολόγηση και αποδοχή των προσφερόμενων υπηρεσιών.

3.2 Υπηρεσίες Εγκατάστασης -Μετάπτωσης

Οι υπηρεσίες εγκατάστασης-μετάπτωσης που πρέπει να προσφερθούν από τον Ανάδοχο αφορούν την εγκατάσταση της προσφερόμενης λύσης καθώς και την παραμετροποίησή της, ώστε να γίνει η ένταξη της στο ήδη υπάρχον δίκτυο της ΒτΕ σύμφωνα με τον σχεδιασμό και τη μελέτη εφαρμογής.

Στην συνέχεια θα πρέπει να λάβει χώρα η μετάπτωση από την υφιστάμενη λύση ASA-5585 στην νέα λύση χωρίς να υπάρχει downtime.

Κατά την μετάπτωση θα ληφθεί μέριμνα και ο εξοπλισμός θα παραμετροποιηθεί κατάλληλα ώστε να αναλάβει και την λειτουργικότητα της υφιστάμενης υποδομής Checkpoint που εξυπηρετεί το δίκτυο της ΥΑΒΕ.

Ο Ανάδοχος υποχρεούται να οργανώσει και να συμμετέχει σε δοκιμές αποδοχής προκειμένου για την επιβεβαίωση της συμβατής λειτουργίας της προσφερόμενης λύσης, σύμφωνα με τις τεχνικές προδιαγραφές τους αλλά και τις απαιτήσεις διαθεσιμότητας, απόδοσης, αξιοπιστίας, ασφάλειας και επεκτασιμότητας που έχουν οριστεί από την ΒτΕ. Παράλληλα, θα πρέπει να διαπιστωθεί η βέλτιστη διαλειτουργικότητα της λύσης καθώς και η εύρυθμη επικοινωνία και διασύνδεση με την υπάρχουσα υποδομή. Οι δοκιμές αποδοχής θα ολοκληρώνονται κατόπιν πιστοποίησης των αποτελεσμάτων αποδοχής από την ΒτΕ και αφού κριθούν σύμφωνες με τις προδιαγραφές και τις απαιτήσεις της.

Όλες οι πλευρές θα συνεργαστούν για να ανταλλάξουν πληροφορίες σχετικά με τις ήδη υπάρχουσες και σε λειτουργία λύσεις και υποδομές, τη δικτυακή υποδομή και τις διασυνδέσεις, τη διαδικασία διαχείρισης αλλαγών, τη διαδικασία παραμετροποίησης του υπάρχοντος εξοπλισμού όσο και για τη διαδικασία επίλυσης προβλημάτων και συντήρησης. Σημειώνεται, ότι ενδεχόμενο κόστος που τυχόν προκύψει από την ως άνω συνεργασία του αναδόχου με τρίτους δεν βαρύνει την ΒτΕ.

Σε περίπτωση που κάποιες από τις εργασίες που θα πραγματοποιηθούν από τον Ανάδοχο, δύναται να προκαλέσουν την διατάραξη της ομαλής λειτουργίας (ή και διακοπή) ήδη υφιστάμενων υπηρεσιών της ΒτΕ, τότε οι εργασίες αυτές θα εκπονηθούν με τη σύμφωνη γνώμη της ΒτΕ και πιθανά εκτός των εργάσιμων ωρών και ημερών μετά από σχετική απαίτηση.

Σε περίπτωση που κατά την περίοδο εγκατάστασης, εμφανισθούν προβλήματα ή διαπιστωθεί ότι δεν πληρούνται κάποιες από τις προδιαγραφόμενες απαιτήσεις, ο Ανάδοχος οφείλει να προβαίνει άμεσα στις απαραίτητες βελτιωτικές παρεμβάσεις και αναπροσαρμογές.

3.3 Υπηρεσίες Εκπαίδευσης

Ο Ανάδοχος θα προσφέρει υπηρεσίες εκπαίδευσης στα στελέχη της ΒτΕ που θα αναλάβουν τη διαχείριση της λύσης. Ο προγραμματισμός της εκπαίδευσης θα γίνει σε συνεννόηση με την ΒτΕ.

Η εκπαίδευση θα έχει τη μορφή:

- Εκπαιδευτικά σεμινάρια και On the job training

Για τη προσφερόμενη λύση, ο Ανάδοχος θα πρέπει να εκπαιδεύσει τρία (3) άτομα από το εξουσιοδοτημένο προσωπικό της ΒτΕ, ώστε να το καταστήσει ικανό να τη χρησιμοποιεί και να τη διαχειρίζεται αποτελεσματικά σύμφωνα με τις Τεχνικές Προδιαγραφές και τις βέλτιστες πρακτικές που προτείνονται. Ο Ανάδοχος, θα πρέπει να παραδώσει όλο το συνοδευτικό υλικό για την υποστήριξη λειτουργίας και συντήρησης της προσφερόμενης λύσης, όπως εγχειρίδια χρήσης, διαχείρισης, προγράμματα εκπαίδευσης, εκπαιδευτικό υλικό και τεχνικές προδιαγραφές.

Τα κόστη παρακολούθησης της εκπαίδευσης επιβαρύνουν τον Ανάδοχο. Μετά το τέλος κάθε εκπαίδευσης, οι εκπαιδευόμενοι θα συμπληρώνουν φόρμα αξιολόγησης σεμιναρίων, η οποία θα αποστέλλεται στον Ανάδοχο. Σε περίπτωση αιτιολογημένης κακής κριτικής, ο Ανάδοχος υποχρεούται να προσφέρει άλλο αντίστοιχου επιπέδου σεμινάριο.

Ο Ανάδοχος θα παρουσιάσει το αναλυτικό περιεχόμενο και χρονοδιάγραμμα της εκπαίδευσης κατά την μελέτη εφαρμογής του έργου. Τα στελέχη της ΒτΕ θα το εγκρίνουν ή θα κάνουν τις αντιπροτάσεις τους, ώστε να οριστικοποιηθεί ένα κοινό χρονοδιάγραμμα και περιεχόμενο εκπαιδεύσεων.

Κατά τη διάρκεια της Σύμβασης, ο Ανάδοχος έχει την υποχρέωση να παραδίδει και να εγκαθιστά όλες τις νέες εκδόσεις για τη λύση που έχει προσφέρει στο παρόν έργο. Αν κάποιες από αυτές τις νέες εκδόσεις έχουν διαφορές στην λειτουργία τους ή στην διαχείρισή τους, ο Ανάδοχος θα πρέπει να παρέχει στους αντίστοιχους διαχειριστές της ΒτΕ την κατάλληλη εκπαίδευση ώστε να κατανοήσουν τις αλλαγές και να είναι ικανοί να συνεχίσουν τη διαχείρισή τους.

3.4 Υπηρεσίες Υποστήριξης Πιλοτικής Λειτουργίας

Σκοπός των υπηρεσιών πιλοτικής λειτουργίας είναι:

- να επιβεβαιώσουν / εξασφαλίσουν την καλή λειτουργία (technical capability & ability to execute) του Έργου σε πραγματικές συνθήκες εργασίας (ευθύνη που βαρύνει τον Ανάδοχο) παρέχοντας πλήρεις υπηρεσίες ασφαλείας με τρόπο ελαστικό και απρόσκοπτο καθώς και

- να θέσουν την προσφερόμενη λύση σε πλήρη παραγωγική λειτουργία.

Στο πλαίσιο των υπηρεσιών πιλοτικής λειτουργίας ο Ανάδοχος θα προσφέρει τις κάτωθι υπηρεσίες:

- την εκτέλεση των τελικών δοκιμών ελέγχου λειτουργικότητας, προσθήκες/ τροποποιήσεις, σύνθεση, πιλοτική χρήση κλπ.) με στόχο να επιβεβαιωθεί η απόλυτα εύρυθμη λειτουργία και καλή συνεργασία των προσφερόμενων λύσεων

- την εκτέλεση των τελικών δοκιμών ασφαλείας με χρήση πραγματικών σεναρίων επίθεσης. Να αναφερθούν.

- την επίλυση προβλημάτων που πιθανά έχουν προκύψει

- τη συλλογή παρατηρήσεων / προτάσεων / σφαλμάτων από όλους τους εμπλεκόμενους και την επίλυσή τους

- την άμεση επίλυση τυχόν προβλημάτων / αποριών των διαχειριστών, σε συνεργασία με εξειδικευμένο προσωπικό του Αναδόχου

- την υλοποίηση ρυθμίσεων, παραμετροποιήσεων, προσαρμογών και τροποποιήσεων που κρίνονται απαραίτητες για τη βελτίωση της απόδοσης της λύσης (fine tuning).

- την επικαιροποίηση της τεκμηρίωσης.

Σε περίπτωση που κατά την περίοδο Πιλοτικής Λειτουργίας, εμφανισθούν προβλήματα ή διαπιστωθεί ότι δεν

πληρούνται κάποιες από τις προδιαγραφόμενες απαιτήσεις, ο Ανάδοχος οφείλει να προβαίνει άμεσα στις απαραίτητες βελτιωτικές παρεμβάσεις και αναπροσαρμογές.

3.5 *Εγγύηση - Υπηρεσίες Υποστήριξης Παραγωγικής Λειτουργίας*

Στο πλαίσιο των υπηρεσιών Παραγωγικής Λειτουργίας ο Ανάδοχος θα προσφέρει τις κάτωθι υπηρεσίες:

- Εγγύηση καλής λειτουργίας που θα είναι back to back με την κατασκευάστρια εταιρία για περίοδο τριών (3) ετών από την ημερομηνία παραλαβής του έργου. Η εγγύηση και η συντήρηση θα περιλαμβάνει επίσης όλες τις συνδρομές λογισμικού (κρίσιμες επιδιορθώσεις, service pack και σημαντικές αναβαθμίσεις, ενημερώσεις και αναβαθμίσεις λογισμικού). Στα πλαίσια της εγγύησης θα περιλαμβάνεται-αντικατάσταση αποτυχημένου υλικού εντός 24 ωρών από την διαπίστωση της αδυναμίας επισκευής του αποτυχημένου υλικού. Οι υπηρεσίες συντήρησης και τεχνικής υποστήριξης θα περιλαμβάνουν και όποια παραμετροποίηση αν απαιτηθεί για τη βελτιστοποίηση της λειτουργικότητας.

- Στον Ανάδοχο θα λειτουργεί Γραφείο Βοήθειας και Υποστήριξης για την εξυπηρέτηση των αιτημάτων υποστήριξης από τη ΒτΕ και θα παρέχεται (εφόσον απαιτείται) πλήρης επιτόπια υποστήριξη εντός 2 ωρών από την επιβεβαιωμένη λήψη του αιτήματος από τον ανάδοχο για βλάβες και επιχειρησιακά ζητήματα όπως και όταν προκύπτουν κατά τις εργάσιμες ημέρες και ώρες 09:00-17:00

4. Χρονοδιάγραμμα

Α.Α	**Υπηρεσία**	Εβδομάδα 1η	Εβδομάδα 2η	Εβδομάδα 3η	Εβδομάδα 4η
1	*Υπηρεσίες Μελέτης Εφαρμογής*	V			
2	*Υπηρεσίες Εγκατάστασης – Μετάπτωσης*		V	V	
3	*Υπηρεσίες Εκπαίδευσης*				V
4	*Υπηρεσίες Υποστήριξης Πιλοτικής Λειτουργίας*				V

5. Πίνακες Συμμόρφωσης

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ
	ΤΕΙΧΟΣ ΠΡΟΣΤΑΣΙΑΣ		
	ΓΕΝΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ		
1.	Να αναφερθεί ο κατασκευαστής και το μοντέλο.	ΝΑΙ	
2.	Απαιτούμενος αριθμός συσκευών	≥ 2	
3.	Θύρες 25 GE SFP28	≥ 4	
4.	Θύρες 10 GE SFP+	≥ 4	
5.	Θύρες GE SFP	≥ 8	
6.	Θύρες 2.5 GE RJ45	≥ 1	
7.	Θύρες GE RJ45	≥ 16	
8.	Θύρα κονσόλας (console)	ΝΑΙ	
9.	Θύρα USB	ΝΑΙ	
10.	Κάθε συσκευή συνοδεύεται από δύο (2) SFP transceiver modules του ίδιου κατασκευαστή.	ΝΑΙ	
11.	Παροχή δύο συμβατών (2) τροφοδοτικών εναλλασσόμενου ρεύματος άμεσης αντικατάστασης, χωρίς διακοπή λειτουργίας της συσκευής, με τα αντίστοιχα καλώδια τροφοδοσίας τους.	ΝΑΙ	
12.	Ανάρτηση του εξοπλισμού σε ικρίωμα, να προσφερθούν όλα τα απαραίτητα υλικά ανάρτησης.	ΝΑΙ	
13.	Να αναφερθούν τα ηλεκτρικά χαρακτηριστικά λειτουργίας του κάθε συστήματος (μέγιστο ρεύμα, κατανάλωση ισχύος, έκλυση θερμότητας).	ΝΑΙ	
14.	Λειτουργία σε διάταξη υψηλής διαθεσιμότητας (ομαδοποίηση High Availability). Να περιγραφούν αναλυτικά οι σχετικές αρχιτεκτονικές υψηλής διαθεσιμότητας.	ΝΑΙ	
15.	Υποστήριξη διαμοιρασμού και προτεραιοποίησης με βάση την εφαρμογή του δικτυακού φορτίου πάνω από πολλαπλές γραμμές WAN. Να αναφερθούν οι σχετικές υποστηριζόμενες τεχνικές.	ΝΑΙ	
16.	Υποστήριξη διαμοιρασμού δικτυακού φορτίου μεταξύ πολλαπλών back-end διακομιστών, βάσει πολλαπλών χρονοδιαγραμμάτων διαμοιρασμού φόρτου.	ΝΑΙ	
17.	Κατακερματισμός σε πολλά λογικά τείχη προστασίας (virtual domains).	ΝΑΙ	
18.	Να αναφερθεί η μέγιστη δυνατότητα (πλήθος) υποστήριξης λογικών τειχών προστασίας.	ΝΑΙ	
19.	Το προσφερόμενο σύστημα θα πρέπει να ενσωματώνει τις παρακάτω λειτουργίες προστασίας και εποπτείας, με την προσφορά και των αντίστοιχων αδειών χρήσης: • Intrusion Prevention (IPS) • Application Control (AC) • Web filtering και Video filtering • Antispam • Antivirus, Botnet και Virus outbreak	ΝΑΙ	
20.	Υποστήριξη hardware acceleration με τεχνολογία ASIC. Να περιγραφεί συνοπτικά η σχετική αρχιτεκτονική)	ΝΑΙ	
21.	Ενσωματωμένη υποστήριξη προστασίας σε επιθέσεις άρνησης εξυπηρέτησης (DoS attacks).	ΝΑΙ	
	ΕΠΙΔΟΣΕΙΣ		
1.	Stateful inspection throughput IPv4 και IPv6 (για μέγεθος πακέτου 512-byte και κίνηση UDP)	≥ 163 Gbps	
2.	Ταυτόχρονες TCP συνδέσεις.	≥ 16.000.000	
3.	**Ρυθμός αποκατάστασης νέων TCP συνδέσεων**	**≥ 700.000 per sec**	
4.	IPS throughput σε συνθήκες enterprise mix.	≥ 25 Gbps	
5.	**Next Generation Firewall (NGFW) throughput.** **Ως NGFW θεωρούμε ότι θα πρέπει να περιλαμβάνονται οι υπηρεσίες Stateful firewall, IPS και Application Control.**	**≥ 20 Gbps**	
6.	Threat Protection throughput. Ως Threat Protection θεωρούμε ότι θα πρέπει να περιλαμβάνονται οι υπηρεσίες Stateful firewall, IPS, Application Control και Malware Protection.	≥ 20 Gbps	
7.	IPsec VPN throughput	≥ 55 Gbps	
8.	SSL VPN throughput.	≥ 10 Gbps	
9.	Υποστήριξη ταυτόχρονων IPsec tunnel, site to site.	≥ 2.000	
10.	SSL inspection throughput.	≥ 16 Gbps	
11.	Να αναφερθούν οι πιστοποιήσεις συμμόρφωσης που έχουν λάβει τα προσφερόμενα συστήματα ασφαλείας.	ΝΑΙ	
	ΛΕΙΤΟΥΡΓΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ		
1.	Υποστήριξη διαφανούς λειτουργίας (L2)	ΝΑΙ	
2.	Υποστήριξη λειτουργίας ως δρομολογητής (L3)	ΝΑΙ	
3.	Υποστήριξη ταυτόχρονης λειτουργίας L2 και L3 (σε διαφορετικά λογικά τείχη προστασίας)	ΝΑΙ	

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ
4.	Υποστήριξη VLAN IEEE 802.1q	ΝΑΙ	
5.	Υποστήριξη link aggregation IEEE 802.3ad	ΝΑΙ	
6.	Υποστήριξη IPv4 και IPv6	ΝΑΙ	
7.	Υποστήριξη OSPF v.2 και v.3	ΝΑΙ	
8.	Υποστήριξη BGP v.4+	ΝΑΙ	
9.	Υποστήριξη policy routing	ΝΑΙ	
10.	Υποστήριξη NTP	ΝΑΙ	
11.	Υποστήριξη DHCP server/relay	ΝΑΙ	
12.	Υποστήριξη NAT με τις εξής δυνατότητες: • Source/Destination NAT • Port Address Translation (PAT) • Fixed port • Port block allocation	ΝΑΙ	
13.	Υποστήριξη QoS. Να περιγραφούν σύντομα οι υποστηριζόμενες τεχνικές.	ΝΑΙ	
	ΥΠΗΡΕΣΙΕΣ ΑΣΦΑΛΕΙΑΣ		
1.	Υποστήριξη πολιτικών ασφαλείας IPv4 και IPv6.	ΝΑΙ	
2.	Η υπηρεσία προστασίας από ιούς θα πρέπει να υποστηρίζει: • Ανίχνευση ιών μέσω σχετικής, διαρκώς ανανεωμένης, βάσης ιών (Virus Signatures Database) • Ανίχνευση προγραμμάτων ύποπτης συμπεριφοράς (Grayware) • Ανίχνευση ιών μέσω ευρετικών μεθόδων (heuristic scan)	ΝΑΙ	
3.	Υποστήριξη υπηρεσίας προστασίας από έξαρση ιών (virus outbreak protection)	ΝΑΙ	
4.	Η υπηρεσία του προγράμματος προστασίας από ιούς θα πρέπει να δύναται να συνεργαστεί με εξωτερική υπηρεσία απομονωμένης εκτέλεσης λογισμικού (sandbox) είτε τοπικά είτε στο νέφος (cloud).	ΝΑΙ	
5.	Η λειτουργία IPS θα πρέπει να υποστηρίζει δημιουργία IPS φίλτρων μέσω εύχρηστης ενεργοποίησης επιλεκτικών προκατασκευασμένων υπογραφών IPS από τον κατασκευαστή.	ΝΑΙ	
6.	Η λειτουργία IPS θα πρέπει να υποστηρίζει δημιουργία custom υπογραφών από τον διαχειριστή.	ΝΑΙ	
7.	Υποστήριξη φιλτραρίσματος του παγκόσμιου ιστού (web filtering) με στατικά φίλτρα URL	ΝΑΙ	
8.	Υποστήριξη υπηρεσίας φιλτραρίσματος βίντεο (video filtering)	ΝΑΙ	
9.	Να προσφερθεί υπηρεσίας ασφάλειας IPS.	ΝΑΙ	
10.	Δυνατότητα υποστήριξης ανάλυσης πακέτων εις βάθος (deep packet inspection).	ΝΑΙ	
	ΕΠΙΠΡΟΣΘΕΤΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ		
1.	Διαχείριση μέσω γραμμής εντολής (CLI)	ΝΑΙ	
2.	Διαχείριση μέσω ενσωματωμένου γραφικού περιβάλλοντος (GUI)	ΝΑΙ	
3.	Πρόσβαση διαχειριστών μέσω HTTPS και SSH	ΝΑΙ	
4.	Υποστήριξη SNMP v.1, 2c και 3	ΝΑΙ	
5.	Δημιουργία πολιτικής password και επιβολή συμμόρφωσης σε αυτή. Η πολιτική password θα πρέπει να υποστηρίζει υποχρεωτικά τα εξής: • Ελάχιστο μήκος password • Υποχρεωτικά κεφαλαία/μικρά γράμματα • Υποχρεωτική χρήση μη αλφαριθμητικών χαρακτήρων • Υποχρεωτική χρήση αριθμών • Χρονική διάρκεια password • Μη επανάληψη ίδιου password	ΝΑΙ	
6.	Υποστήριξη RADIUS και LDAP.	ΝΑΙ	

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ
7.	Να προσφερθεί πλατφόρμα κεντρικής διαχείρισης για τις διατάξεις ασφαλείας (NGFW) με δυνατότητα διαχείρισης μέχρι δέκα (10) συσκευών, του ίδιου κατασκευαστή. Η πλατφόρμα δύναται να προσφερθεί και με τη μορφή λογισμικού. Στην περίπτωση αυτή να αναφερθούν τα χαρακτηριστικά και οι απαιτήσεις.	ΝΑΙ	
8.	Να παρέχεται επίσης η δυνατότητα επέκτασης του αριθμού συσκευών που δύναται να διαχειριστεί η κεντρική πλατφόρμα διαχείρισης, με προμήθεια σχετικών αδειών. Ζητείται ως δυνατότητα μόνο.	ΝΑΙ	
9.	Να προσφερθεί κεντρική πλατφόρμα ανάλυσης και πληροφόρησης με δυνατότητα υποστήριξης 5 GB/ ημέρα logs, του ίδιου κατασκευαστή. Η πλατφόρμα δύναται να προσφερθεί και με τη μορφή λογισμικού. Σε αυτήν τη περίπτωση να αναφερθούν τα χαρακτηριστικά και οι απαιτήσεις.	ΝΑΙ	
10.	Να παρέχεται επίσης η δυνατότητα επέκτασης του όγκου των logs που δύναται να διαχειριστεί η κεντρική πλατφόρμα ανάλυσης και πληροφόρησης, με προμήθεια σχετικών αδειών. Ζητείται ως δυνατότητα μόνο.	ΝΑΙ	
11.	Η προσφερόμενη πλατφόρμα θα επεξεργάζεται και θα αναλύει τα συλλεγμένα δεδομένα καταγραφής.	ΝΑΙ	
12.	Η προσφερόμενη πλατφόρμα θα παρέχει υπηρεσίες αναγνώρισης ρίσκου μέσω Indicators of Compromise (IoC).	ΝΑΙ	
13.	Η προσφερόμενη πλατφόρμα θα παρέχει υποστήριξη γραφικού περιβάλλοντος (GUI) για την αναζήτηση και παρουσίαση των δεδομένων καταγραφής.	ΝΑΙ	
	ΥΠΟΣΤΗΡΙΞΗ		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ
1.	Ο εξοπλισμός θα πρέπει να προσφερθεί με υπηρεσίες υποστήριξης 24x7 , διάρκειας τουλάχιστον τριών (3) ετών από την ημερομηνία παράδοσης του συνόλου της λύσης (υλικό και λογισμικό). Οι παραπάνω υπηρεσίες θα πρέπει να περιλαμβάνουν: • Τηλεφωνική υποστήριξη 24x7 • Δυνατότητα επίλυσης τεχνικών προβλημάτων μέσω δημιουργίας καρτέλας / ερωτημάτων τεχνικής υποστήριξης (ticket) • Αντικατάσταση του εξοπλισμού σε περίπτωση βλάβης την επόμενη ημέρα. • Τεχνική υποστήριξη και ανταλλακτικά στο εξουσιοδοτημένο επισκευαστικό κέντρο του κατασκευαστή	ΝΑΙ	
2.	Θα πρέπει να προσφερθούν όλες οι άδειες χρήσης που απαιτούνται για την υποστήριξη των υπηρεσίας ασφάλειας που περιγράφονται στον εν λόγω πίνακα, διάρκειας τουλάχιστον τριών (3) ετών από την ημερομηνία παράδοσης του συνόλου της λύσης.	ΝΑΙ	
3.	Ο προσφερόμενος εξοπλισμός θα πρέπει να ενημερώνεται αυτόματα, μέσω αντίστοιχης λειτουργίας του γραφικού περιβάλλοντος διαχείρισης της λύσης, μέσω διαδικτύου και καθ' όλο το 24ωρο, με ανανεωμένες εκδόσεις όλων των παρεχόμενων υποσυστημάτων ανίχνευσης, προστασίας και λοιπών λειτουργιών	ΝΑΙ	

6. Απαιτήσεις που αφορούν τον ανάδοχο και αποτελούν υποχρεωτική ελάχιστη απαίτηση επιλογής (on-off κριτήριο)

Α/Α	Προδιαγραφή	Απαίτηση	Απάντηση	Παραπομπή
Α.Α	**Απαίτηση**	Απάντηση		
1	Ο Ανάδοχος θα πρέπει να διαθέτει ISO/IEC 27001:2013	ΝΑΙ		
2	Ο Ανάδοχος θα πρέπει να έχει υλοποιήσει τουλάχιστον τρία (3) παρόμοια έργα την τελευταία 3-ετία με κόστος άνω των 60.000 €	ΝΑΙ		
3	Ο Ανάδοχος θα πρέπει να διαθέτει τουλάχιστον δύο (2) τεχνικούς που να έχουν πιστοποίηση από τον κατασκευαστή για την συντήρηση τεχνική υποστήριξη της κατηγορίας των υπό προμήθεια συσκευών	ΝΑΙ		