ΑΠΟΤΕΛΕΣΜΑΤΑ ΔΗΜΟΣΙΑΣ ΔΙΑΒΟΥΛΕΥΣΗΣ

Διάρκεια: 19.10.2022 – 03.11.2022

Μοναδικός Κωδικός : 22DIAB000025242

ΗΛΕΚΤΡΟΝΙΚΟΥ ΑΝΟΙΚΤΟΥ ΔΙΕΘΝΟΥΣ ΑΝΩ ΤΩΝ ΟΡΙΩΝ ΔΙΑΓΩΝΙΣΜΟΥ, ΣΕ ΤΜΗΜΑΤΑ

για το Έργο

ΠΡΟΜΗΘΕΙΑ ΕΞΟΠΛΙΣΜΟΥ ΤΠΕ ΓΙΑ ΤΗΝ ΑΝΑΒΑΘΜΙΣΗ ΤΩΝ ΚΕΝΤΡΙΚΩΝ ΔΙΚΤΥΑΚΩΝ ΥΠΟΔΟΜΩΝ ΤΟΥ ΠΑΝΕΛΛΗΝΙΟΥ ΣΧΟΛΙΚΟΥ ΔΙΚΤΥΟΥ

της Πράξης

«Αναβάθμιση και εμπλουτισμός του οικοσυστήματος ψηφιακών υπηρεσιών του Πανελλήνιου Σχολικού Δικτύου / Επέκταση των λειτουργιών του συστήματος myschool και ολοκλήρωση του περιβάλλοντος παροχής προηγμένων ψηφιακών υπηρεσιών στο σύνολο των μελών της εκπαιδευτικής κοινότητας» (MIS/ΟΠΣ 5168211)

CPV:

32413100-2 Δρομείς δικτύου (Δρομολογητής Ευρυζωνικών Προσβάσεων)

32420000-3 Εξοπλισμός δικτύου (Σύστημα Next-Generation Firewall / Μεταγωγείς Δικτύου (Multigigabit Ethernet / Δικτυακές συσκευές καταμερισμού φορτίου Load Balancers / παρελκόμενα δρομολογητών)

Προϋπολογιζόμενης Δαπάνης: 524.460,00 € πλέον ΦΠΑ

Κριτήριο Ανάθεσης:

Η ΠΛΕΟΝ ΣΥΜΦΕΡΟΥΣΑ ΑΠΟ ΟΙΚΟΝΟΜΙΚΗ ΑΠΟΨΗ ΠΡΟΣΦΟΡΑ ΒΑΣΕΙ ΒΕΛΤΙΣΤΗΣ ΣΧΕΣΗΣ ΠΟΙΟΤΗΤΑΣ-ΤΙΜΗΣ ΑΝΑ ΤΜΗΜΑ

Πάτρα, Μάρτιος 2023

ΙΤΥΕ ΔΙΟΦΑΝΤΟΣ

Πίνακας Περιεχομένων

1 Φορέας 1 3
1.1 ΤΜΗΜΑ 2 3
1.1.1 Σχόλιο 1 3
1.1.2 Σχόλιο 2 3
2 Φορέας 2 4
2.1 ΠΤΧ 1. Σύστημα Προστασίας Δικτύου 4
2.1.1 Σχόλιο 1 4
2.1.2 Σχόλιο 2 4
2.1.3 Σχόλιο 3 5
2.1.4 Σχόλιο 4 5
2.1.5 Σχόλιο 5 5
3 Φορέας 3 6
3.1 Παρατήρηση 1 6
3.2 Παρατήρηση 2 6
3.3 Παρατήρηση 3 7
3.4 Παρατήρηση 4 7
3.5 Παρατήρηση 5 8
3.6 Παρατήρηση 6 8
3.7 Παρατήρηση 7 9
3.8 Παρατήρηση 8 10
4 Φορέας 4 11
4.1 Σχόλιο 1ο 11
4.2 Σχόλιο 2ο 12
5 Φορέας 5 12
5.1 Σχόλιο 1ο 12
5.2 Σχόλιο 2ο 13
5.3 Σχόλιο 3ο 13
6 Επιπλέον αλλαγές 14
6.1 Τμήμα 2, ΠΤΧ 1. Σύστημα Προστασίας Δικτύου – Firewall (Next Generation) 14
6.2 Τμήμα 2, ΠΤΧ 2 Δικτυακές συσκευές καταμερισμού φορτίου Load Balancers (LB) 14

1 Φορέας 1

1.1 ΤΜΗΜΑ 2

1.1.1 Σχόλιο 1

Γενικό Σχόλιο για το τμήμα 2 «Εξοπλισμός Κέντρου Δεδομένων ΠΣΔ» της Διαβούλευσης και πιο συγκεκριμένα για το Σύστημα προστασίας Δικτύου και Κέντρου Δεδομένων ΠΣΔ – Next Generation Firewall.

Λαμβάνοντας υπόψη τις ανάγκες ενός σύγχρονου οργανισμού καθώς και την αναγραφόμενη εκτιμώμενη αξία του συγκεκριμένου τμήματος προτείνουμε την αύξηση του ζητούμενου Next Generation Firewall (NGFW) throughput, όπως αυτό αναφέρεται στην σελίδα 80 προδιαγραφή με αύξων αριθμό fw 5.2, στα 10 Gbps από 6 Gbps.

Απάντηση

Με βάση την πρόταση σας, σε συνδυασμό με την πρόταση του Φορέα 2 και επανεκτιμώντας τις ανάγκες και τις σύγχρονες προσφερόμενες λύσεις των κατασκευαστών, η προδιαγραφή προσαρμόζεται ως ακολούθως:

> ***fw 5.2*** *Υποστηριζόμενη διαμεταγωγή σε λειτουργία NGFW (Firewall, Application Control, IPS) ≥ 12,5 Gbps*

1.1.2 Σχόλιο 2

Σε συνέχεια των ανωτέρω καθώς και σύμφωνα με την περιγραφή της σελίδας 56 και πιο συγκεκριμένα στην παράγραφο «1. Σύστημα προστασίας Δικτύου και Κέντρου Δεδομένων ΠΣΔ – Next Generation Firewall», ζητείται ζεύγος συσκευών ίδιους τύπου σε διάταξη υψηλής διαθεσιμότητας, ενώ στο στον πίνακα «Πίνακας Εξοπλισμού ΤΜΗΜΑ 2: Εξοπλισμός Κέντρου Δεδομένων ΠΣΔ» και πιο συγκεκριμένα στην στήλη «Τεμάχια» αναφέρεται ποσότητα 1. Παρακαλούμε, όπως διορθωθεί η σχετική ζητούμενη ποσότητα.

Απάντηση

Η περιγραφή της αναφερόμενης παραγράφου μιλάει για σύστημα προστασίας όπως και ο πίνακας προσφερόμενου εξοπλισμού. Η ως άνω αναφερόμενη παράγραφος θεωρούμε ότι είναι σαφής όπως έχει διατυπωθεί:

> *«*
> ***Σύστημα προστασίας Δικτύου και Κέντρου Δεδομένων ΠΣΔ – Next Generation Firewall***
>
> *Σύστημα προστασίας Δικτύου – Firewall (επόμενης γενιάς – Next Generation) με πλήρη προστασία έναντι κινδύνων (threat prevention), τύπου sandboxing εναντίον zero-day επιθέσεων, το οποίο θα έχει τη μορφή ενός ζεύγους συσκευών ιδίου τύπου σε διάταξη υψηλής διαθεσιμότητας.*
> *»*

Ενώ ο Πίνακας Εξοπλισμού αναφέρεται σε σύστημα και όχι σε συσκευές *«Σύστημα προστασίας Δικτύου και Κέντρου Δεδομένων ΠΣΔ – Next Generation Firewall»* το οποίο σύμφωνα και με την προδιαγραφή fw1.3 του ΠΤΧ1 απαιτείται να είναι ζεύγος συσκευών. Συγκεκριμένα η προδιαγραφή αναφέρει σα*φώς :*

> *«**fw 1.3** - Το προσφερόμενο σύστημα θα έχει τη μορφή ενός ζεύγους συσκευών ιδίου τύπου σε διάταξη υψηλής διαθεσιμότητας (High Availability»)*

Στο αναφερόμενο σημείο του πίνακα προσφερόμενου εξοπλισμού προστέθηκε σχετική διευκρίνιση και λαμβάνει τη μορφή:

> *Σύστημα προστασίας Δικτύου και Κέντρου Δεδομένων ΠΣΔ – Next Generation Firewall (σύστημα ζεύγους συσκευών)*

2 Φορέας 2

2.1 ΠΤΧ 1. Σύστημα Προστασίας Δικτύου

2.1.1 Σχόλιο 1

FW 1.6: *Προτείνουμε να τροποποιηθεί ως εξής ‘’Για το προσφερόμενο σύστημα δεν θα πρέπει να έχει ανακοινωθεί από τον κατασκευαστή τέλος του κύκλου ζωής (End of Life) πριν την ημερομηνία κατάθεσης και θα πρέπει αναφερθεί η ημερομηνία πρώτης κυκλοφορίας του προτεινόμενου μοντέλου από τον κατασκευαστή’’*

Απάντηση

Γίνεται δεκτή η εν λόγω πρόταση με τη λογική ότι θεωρείται καλύτερη και εφικτή να απαντηθεί από τους υποψηφίους σε σχέση με την αρχική διατύπωση. Η προδιαγραφή επιμερίζεται σε δύο προδιαγραφές που διαμορφώνονται ως ακολούθως:

«

fw 1.6: *Το προσφερόμενο σύστημα θα πρέπει να είναι σύγχρονης τεχνολογίας με πρόσφατη ημερομηνία πρώτης κυκλοφορίας από τον κατασκευαστή. Να αναφερθεί η ημερομηνία πρώτης κυκλοφορίας του.*

fw 1.7 *Για το προσφερόμενο σύστημα δεν θα πρέπει να έχει ανακοινωθεί από τον κατασκευαστή τέλος του κύκλου ζωής (End of Life) πριν την ημερομηνία κατάθεσης της προσφοράς.*

»

2.1.2 Σχόλιο 2

FW 2.5 *Προτείνουμε να αφαιρεθεί αυτή η προδιαγραφή γιατί η λειτουργία αυτή συναντάται συνήθως σε λύσεις email security καθώς προσθέτει καθυστέρηση*

στην παράδοση ενός attachment, μέχρι να γίνει το attachment reconstruct και reattach, κάτι το οποίο δεν προτείνεται σε λύσεις firewall για την υπόλοιπη κίνηση. Από την άλλη εάν τα αρχεία είναι stored σε OneDrive ή Dropbox χρησιμοποιώντας Client εφαρμογή τα sessions αυτά δεν μπορούν να γίνουν decrypt μέσω firewall.

Απάντηση

Γίνεται δεκτή η πρόταση και αφαιρείται η εν λόγω προαιρετική προδιαγραφή.

2.1.3 Σχόλιο 3

FW 2.6 *Προτείνουμε να προστεθεί και η απαίτηση για antimalware προστασία με δυναμική ανάλυση αρχείων με χρήση sandbox όπως αναγράφεται και στην προδιαγραφή FW 9.1*

Απάντηση

Η απαίτηση για antimalware προστασία έχει συμπεριληφθεί ήδη στην προδιαγραφή fw 4.4 η οποία προβλέπει:

« fw 4.4 εξελιγμένο σύστημα προστασίας από κινδύνους (Threat Protection) που υποστηρίζει ταυτόχρονα μηχανισμούς FW, Application Control, IPS και προστασία από zero day και malware με χρήση sandbox NAI»

Θεωρούμε επομένως ότι δεν χρειάζεται να προστεθεί το σημείο αυτό στην προδιαγραφή fw 2.6 (πλέον 2fw2.5) της οποίας άλλωστε η εκπλήρωση είναι προαιρετική. Η προδιαγραφή παραμένει ως έχει.

2.1.4 Σχόλιο 4

FW 4.7 *Το email θεωρείται νο1 vector of attack και είναι best practice να υπάρχει αποκλειστική λύση τύπου Email Security Gateway για την προστασία από επιθέσεις μέσω email και δεν συνιστάται η χρήση firewall. Η συγκεκριμένη απαίτηση δεν πληρείται από όλους τους κατασκευαστές σε firewall και προτείνουμε να αφαιρεθεί εφόσον δεν συνάδει και με τα γενικότερα best practices.*

Απάντηση

Αν και η εκπλήρωση της προδιαγραφής είναι προαιρετική, γίνεται δεκτή η παρατήρηση και αφαιρείται η εν λόγω προδιαγραφή.

2.1.5 Σχόλιο 5

Fw 5.2 *Εφόσον υπάρχει η απαίτηση για 10G διασύνδεση και το έργο αναφέρεται σε νέας γενιάς multigigabit ethernet switches καθώς επίσης και το firewall θα είναι NGFW (θα έχει ενεργοποιημένες υπηρεσίες security όπως IPS, application control) είναι*

προτεινόμενο η απαίτηση του Throughput του NGFW με λειτουργίες IPS και application control να είναι ισάξια του Firewall throughput 15Gbps ή τουλάχιστον ισάξια της φυσικής διασύνδεσης >=10Gbps.

Απάντηση

Με βάση την πρόταση σας και επανεκτιμώντας τις ανάγκες και τις σύγχρονες προσφερόμενες λύσεις των κατασκευαστών, η προδιαγραφή προσαρμόζεται ως ακολούθως:

***fw 5.2** Υποστηριζόμενη διαμεταγωγή σε λειτουργία NGFW (Firewall, Application Control, IPS) ≥ 12,5 Gbps*

3 Φορέας 3

3.1 Παρατήρηση 1

Πίνακας Συμμόρφωσης ΠΤΧ1. Συγκεντρωτής ευρυζωνικών προσβάσεων

***Εδάφιο:** ΤΧ 6.12*

***Απαίτηση:** Υποστήριξη πρωτοκόλλου δρομολόγησης IPv4 EIGRP*

Παρατήρηση

Το EIGRP δεν είναι ευρέως αποδεκτό από όλους τους κατασκευαστές Datacom προϊόντων και δεν έχει αναπτυχθεί ευρέως παγκοσμίως. Το OSPF είναι το τυπικό πρωτόκολλο που χρησιμοποιείται από περισσότερους πελάτες παγκοσμίως. Επιθυμητή αλλαγή: Προτείνουμε να αλλάξει από EIGRP σε OSPF." Επικαιροποιημένη Διατύπωση Απαίτηση: Υποστήριξη πρωτοκόλλου δρομολόγησης IPv4 OSPF

Απάντηση

Η εκπλήρωση της προδιαγραφής δεν είναι υποχρεωτική. Παρόλα αυτά γίνεται δεκτή η εν λόγω παρατήρηση και αφαιρείται η προδιαγραφή ΤΧ 6.12 με τη λογική να μην υπάρχει πλεονεκτική θέση κάποιων κατασκευαστών, σε συνδυασμό με τη μη χρήση στην υφιστάμενη δομή του δικτύου του EIGRP.
Σε σχέση με την υποστήριξη OSPF αυτό προβλέπεται στην προδιαγραφή ΤΧ 6.1 “Υποστήριξη πρωτόκολλου δρομολόγησης IPv4 OSPF και OSPF v2 (συμμόρφωση με το RFC 1793)”

3.2 Παρατήρηση 2

Πίνακας Συμμόρφωσης ΠΤΧ1. Συγκεντρωτής ευρυζωνικών προσβάσεων

***Εδάφιο:** ΤΧ 8.3*

***Υποχρεωτική Απαίτηση:** Υλοποίηση Application Level Gateway – ALG για τα πρωτόκολλα: NAI ICMP, DNS, FTP, H.323, SIP*

Παρατήρηση

Το Η.323 είναι αρκετά παλιό πρωτόκολλο που αντικαταστάθηκε από το SIP πριν από 15 χρόνια. Επιθυμητή αλλαγή: Να αφαιρεθεί το Η.323, Προτείνεται τη χρήση του NAT ALG για SIP σε φωνητικό σενάριο. Επικαιροποιημένη Διατύπωση Υλοποίηση Application Level Gateway – ALG για τα πρωτόκολλα: NAI ICMP, DNS, FTP, NAT ALG για SIP

Απάντηση

Γίνεται δεκτή η πρόταση και αφαιρείται το Η.323 από τη συγκεκριμένη προδιαγραφή.

3.3 Παρατήρηση 3

Πίνακας Συμμόρφωσης ΠΤΧ1. Συγκεντρωτής ευρυζωνικών προσβάσεων

Εδάφιο: *ΤΧ 13.8 Υποχρεωτική*

Απαίτηση: *Πλήθος υποστηριζόμενων routes IPv4 ≥3.000.000*

Παρατήρηση / Ερώτηση

Το πλήθος υποστηριζόμενων routes IPv4 αφορά Routing Information Base ή αφορά Forwarding Information Base; Επιθυμητή αλλαγή: Αν το πλήθος υποστηριζόμενων routes IPv4 αφορά Routing Information Base, τότε προτείνουμε το πλήθος να είναι ≥ 15M Αν το πλήθος υποστηριζόμενων routes IPv4 αφορά Forwarding Information Base, τότε προτείνουμε το πλήθος να είναι ≥ 3M Επικαιροποιημένη Διατύπωση Πλήθος υποστηριζόμενων routes IPv4 Routing Information Base ≥ 15M ή Πλήθος υποστηριζόμενων routes IPv4 Forwarding Information Base ≥ 3M

Απάντηση

Η προδιαγραφή αφορά το πλήθος υποστηριζόμενων routes IPv4 Forwarding Information Base. Έγινε προσαρμογή της σχετικής προδιαγραφής ως ακολούθως:

> «*ΤΧ 13.8 Πλήθος υποστηριζόμενων routes IPv4, Forwarding Information Base ≥3.000.000»*

3.4 Παρατήρηση 4

Πίνακας Συμμόρφωσης ΠΤΧ1. Συγκεντρωτής ευρυζωνικών προσβάσεων

Εδάφιο: ΤΧ 13.9

Υποχρεωτική Απαίτηση: *Πλήθος υποστηριζόμενων routes IPv6 ≥2.500.000*

Παρατήρηση

Το πλήθος υποστηριζόμενων routes IPv6 αφορά Routing Information Base ή αφορά Forwarding Information Base; Επιθυμητή αλλαγή: Αν το πλήθος υποστηριζόμενων routes IPv6

αφορά Routing Information Base, τότε προτείνουμε το πλήθος να παραμείνει ≥ 2.500.000 Αν το πλήθος υποστηριζόμενων routes IPv6 αφορά Forwarding Information Base, τότε προτείνουμε το πλήθος να είναι ≥ 2.000.000 Επικαιροποιημένη Διατύπωση Πλήθος υποστηριζόμενων routes IPv6 Routing Information Base ≥ 2.500.000 ή Πλήθος υποστηριζόμενων routes IPv6 Forwarding Information Base ≥ 2.000.000

Απάντηση

Η προδιαγραφή αφορά το πλήθος υποστηριζόμενων routes IPv6 Forwarding Information Base. Έγινε προσαρμογή της σχετικής προδιαγραφής ως ακολούθως με δεδομένο ότι το 2.000.000 IPv6 routes θεωρείται επαρκές για το ΠΣΔ:

> «*ΤΧ 13.9 Πλήθος υποστηριζόμενων routes IPv6, Forwarding Information Base ≥2.000.000»*

3.5 Παρατήρηση 5

Πίνακας Συμμόρφωσης ΠΤΧ1. Συγκεντρωτής ευρυζωνικών προσβάσεων

Εδάφιο: *ΤΧ 14.11*

Υποχρεωτική Απαίτηση: *Υποστήριξης ενσωματωμένων λειτουργιών stateful Firewall και NAT*

Παρατήρηση

Απαιτείται ένα ανεξάρτητο τείχος προστασίας (Firewall) στο έντυπο της διαβούλευσης, το δίκτυο μπορεί να ασφαλιστεί από το ζητούμενο τείχος προστασίας (Firewall). Η συγκεκριμένη λειτουργικότητα καλύπτεται από το τείχος προστασίας (Firewall).

Επιθυμητή αλλαγή: *Να αφαιρεθεί το stateful Firewall από την απαίτηση*

Επικαιροποιημένη Διατύπωση: *Υποστήριξης ενσωματωμένων λειτουργιών NAT*

Απάντηση:

Το ανεξάρτητο τείχος προστασίας (Firewall) αφορά το κέντρο δεδομένων και όχι τη διασύνδεση των μονάδων στο ΠΣΔ μέσω του συγκεντρωτή ευρυζωνικών προσβάσεων. Με βάση αυτό θεωρούμε την υποστήριξη των λειτουργιών του stateful Firewall απαραίτητη για τον ορισμό κανόνων προστασίας του δικτύου και των διασυνδεομένων μονάδων. Με βάση αυτό η προδιαγραφή ΤΧ 14.11 για *«Υποστήριξη ενσωματωμένων λειτουργιών stateful Firewall και NAT»* παραμένει όπως είναι.

3.6 Παρατήρηση 6

Πίνακας Συμμόρφωσης: ΠΤΧ 2. Μεταγωγείς υψηλής ταχύτητας – Multigigabit Ethernet Switches

Εδάφιο: S10G 7.2

Υποχρεωτική Απαίτηση: *Εύρος ζώνης διάταξης stacking ≥ 1000 Gbps*

Παρατήρηση:

*Το προτεινόμενο Switch θα χρησιμοποιεί διεπαφή 100G για stacking, δυο (2) συνδέσεις για redundancy. Έτσι, το εύρος ζώνης stacking θα είναι 400 Gbps. Στο μεγαλύτερο μέρος του σεναρίου, η κίνηση east-west traffic μεταξύ των μελών στο σύστημα stacking είναι περιορισμένη. Η κυκλοφορία South-north tracffic είναι η κύρια κυκλοφορία εντός του campus. Το προτεινόμενο downlink Switch έχει ζεύξη 24 θυρών 25G, το maximum traffic μπορεί να είναι 24*25 = 600 Gbps, οπότε το εύρος ζώνης stacking 400 Gbps είναι αρκετό για αυτό το σενάριο.*

Επιθυμητή αλλαγή: *Το Εύρος ζώνης διάταξης stacking να ισοδυναμεί με 400 Gbps* ***Επικαιροποιημένη Διατύπωση:*** *Εύρος ζώνης διάταξης stacking 400 Gbps*

Απάντηση

Ο αναφερόμενος αριθμός θυρών και ο τύπος για stacking δεν προκύπτει από τις προδιαγραφές αλλά είναι επιλογή του προτείνοντος. Έτσι η επιλογή των 400 Gbps είναι πολύ κατώτερη του ζητούμενου εύρους ζώνης 1 Tbps.

Σε σχέση με το ζητούμενο εύρος ζώνης stacking έχουμε τα ακόλουθα:

Ο ζητούμενος αριθμός θυρών είναι 24 X 25 Gbps (=600 Gbps) με δυνατότητα επέκτασης με επιπλέον 2*100Gbps = 200Gbps, δηλαδή 800 Gbps ή 1600 Gbps full duplex κίνηση. Με βάση αυτό θεωρούμε ότι η επικοινωνία μεταξύ των δύο stacking switches δεν μπορεί να είναι κατώτερη του 50 % του συνολικού εύρους ζώνης, καθώς υπάρχουν ακραίες περιπτώσεις που η κίνηση που εξυπηρετείται από το ένα switch του stack θα πρέπει να μεταχθεί στο άλλο διαμέσου της σύνδεσης stacking. Με αυτή τη λογική το ελάχιστο ανεκτό όριο τους εύρους ζώνης σε διάταξη stacking δεν μπορεί να είναι κατώτερο των 800 Gbps.

Η προδιαγραφή μετριάζεται ως ακολούθως:

«S10G 7.2 Εύρος ζώνης διάταξης stacking ≥ 800 Gbps»

3.7 Παρατήρηση 7

Πίνακας Συμμόρφωσης: ΠΤΧ 2. Μεταγωγείς υψηλής ταχύτητας – Multigigabit Ethernet Switches

Εδάφιο: S10G 7.3

Υποχρεωτική Απαίτηση: *Ρυθμός προώθησης (forwarding rate) για πακέτα μεγέθους 64 bytes ≥ 1400 Mpps*

Παρατήρηση:

Στα πλαίσια του συγκεκριμένου έργου θεωρούμε ότι η απαίτηση για τον ρυθμό προώθησης πακέτων μεγέθους 64 bytes είναι αρκετά αυξημένη και δεν ανταποκρίνεται στις τωρινές και μελλοντικές ανάγκες. Επιθυμητή αλλαγή: Ο Ρυθμός προώθησης (forwarding rate) για πακέτα μεγέθους 64 bytes να είναι στα 490 Mpps Επικαιροποιημένη Διατύπωση: Ρυθμός προώθησης (forwarding rate) για πακέτα μεγέθους 64 bytes 490 Mpps

Απάντηση

Ο ζητούμενος αριθμός θυρών είναι 24 X 25 Gbps (=600 Gbps) με δυνατότητα επέκτασης με 200Gbps. Ο ρυθμός προώθησης (forwarding rate) οφείλει να είναι ίσο ή μεγαλύτερο του (600+200)*1.488 = 1190 Mpps ώστε να μην υπάρχουν καθυστερήσεις σε περίπτωση υψηλής χρήσης. Ο ρυθμός προώθησης που έχει οριστεί σχετίζεται άμεσα με το συνολικό bandwidth με την παραπάνω λογική, έχει σκοπό την διασφάλιση ενός ισχυρού συστήματος το οποίο θα μπορεί να ανταπεξέλθει αποδοτικά σε κάθε ενδεχόμενο κίνησης στα πλαίσια του συνολικού εύρους ζώνης (bandwidth). Η προδιαγραφή S10G 7.3 προσαρμόζεται σε *«S10G 7.2 Ρυθμός προώθησης (forwarding rate) για πακέτα μεγέθους 64 bytes ≥ 1190 Mpps».*

3.8 Παρατήρηση 8

Πίνακας Συμμόρφωσης: ΠΤΧ 1. Σύστημα Προστασίας Δικτύου – Firewall (Next Generation)

Εδάφιο: *fw 3.1, fw 3.2, fw 3.3, fw 3.4*

Υποχρεωτική Απαίτηση:

fw 3.1 Το προσφερόμενο σύστημα θα πρέπει να εκπληρώνει τα ακόλουθα χαρακτηριστικά οριζόντιας κλιμάκωσης:

fw 3.2 Διαμόρφωση σε ενιαίο σύστημα (cluster) με αξιοποίηση της δυναμικότητας και των δύο προσφερόμενων συσκευών

fw 3.3 Δυνατότητα επαύξησης της δυναμικότητας με προσθήκη επιπλέον συσκευής

fw 3.4 Σύστημα ενιαίας διαχείρισης σε όλες τις συσκευές του cluster

Παρατήρηση:

Ο ζητούμενος τρόπος οριζόντιας κλιμάκωσης με ενιαίο σύστημα (cluster) υποστηρίζεται από συγκεκριμένο κατασκευαστή και δεν είναι ο μοναδικός τρόπος. Η απαίτηση εν προκειμένω αφορά την υψηλή διαθεσιμότητα, την επεκτασιμότητα και την κοινή διαχείριση των ζητούμενων Firewalls.

Επιθυμητή αλλαγή:

Να δοθεί η δυνατότητα σε όλους του μεγάλους κατασκευαστές συστημάτων προστασίας δικτύου να προσφέρουν τις λύσεις τους που καλύπτουν την απαίτηση για υψηλή διαθεσιμότητα, την επεκτασιμότητα και την κοινή διαχείριση της προσφερόμενης διάταξης

Προτεινόμενη Διατύπωση:

fw 3.1 Το προσφερόμενο σύστημα θα πρέπει να εκπληρώνει τα ακόλουθα χαρακτηριστικά οριζόντιας κλιμάκωσης:

fw 3.2 Διαμόρφωση σε διάταξη με αξιοποίηση της δυναμικότητας και των δύο προσφερόμενων συσκευών

fw 3.3 Δυνατότητα επαύξησης της δυναμικότητας με προσθήκη επιπλέον συσκευής

fw 3.4 Σύστημα ενιαίας διαχείρισης σε όλες τις συσκευές της προσφερόμενης διάταξης

Απάντηση

Γίνεται δεκτή η εν λόγω πρόταση και προσαρμόζονται οι αναφερόμενες προδιαγραφές ως ακολούθως.

fw 3.1	Το προσφερόμενο σύστημα θα πρέπει να εκπληρώνει τα ακόλουθα χαρακτηριστικά οριζόντιας κλιμάκωσης:	**ΝΑΙ**
fw 3.2	Διαμόρφωση σε διάταξη υψηλής διαθεσιμότητας με αξιοποίηση της δυναμικότητας και των δύο προσφερόμενων συσκευών.	**ΝΑΙ**
fw 3.3	Δυνατότητα επαύξησης της δυναμικότητας με προσθήκη επιπλέον συσκευής ή συσκευών έχοντας κοινή διαχείριση.	**ΝΑΙ**
fw 3.4	Ενιαία διαχείριση σε όλες τις συσκευές της διάταξης.	**ΝΑΙ**

4 Φορέας 4

4.1 Σχόλιο 1ο

Κεφάλαιο 7.

ΠΑΡΑΡΤΗΜΑ Ι – ΑΝΑΛΥΤΙΚΗ ΠΕΡΙΓΡΑΦΗ ΦΥΣΙΚΟΥ ΑΝΤΙΚΕΙΜΕΝΟΥ ΤΗΣ ΣΥΜΒΑΣΗΣ, Παράγραφος ΤΜΗΜΑ, Σελ. 56 της Διαβούλευσης αναφέρεται «Σύστημα προστασίας Δικτύου – Firewall (επόμενης γενιάς – Next Generation)… το οποίο θα έχει τη μορφή ενός ζεύγους συσκευών ιδίου τύπου σε διάταξη υψηλής διαθεσιμότητας.», όμως στον πίνακα της ίδια σελίδας ο αριθμός των τεμαχίων είναι 1. Προτείνεται να αντικατασταθεί ο αριθμός των τεμαχίων από 1 σε 2, ώστε να είναι ξεκάθαρο ότι το ζητούμενο είναι 2 Τεμάχια Firewalls τα όποια θα είναι ίδιου τύπου σε διάταξη υψηλής διαθεσιμότητας. Επίσης, προτείνεται να προστεθεί σχετική προδιαγραφή και στον πίνακα προδιαγραφών 'Πίνακας Εξοπλισμού ΤΜΗΜΑ 2: Εξοπλισμός Κέντρου Δεδομένων ΠΣΔ'.

Απάντηση

Η περιγραφή της αναφερόμενης παραγράφου μιλάει για σύστημα προστασίας όπως και ο πίνακας προσφερόμενου εξοπλισμού. Η ως άνω αναφερόμενη παράγραφος θεωρούμε ότι είναι σαφής όπως έχει διατυπωθεί:

> *«*
> ***Σύστημα προστασίας Δικτύου και Κέντρου Δεδομένων ΠΣΔ – Next Generation Firewall***
>
> *Σύστημα προστασίας Δικτύου – Firewall (επόμενης γενιάς – Next Generation) με πλήρη προστασία έναντι κινδύνων (threat prevention), τύπου sandboxing εναντίον*

> *zero-day επιθέσεων, το οποίο θα έχει τη μορφή ενός ζεύγους συσκευών ιδίου τύπου σε διάταξη υψηλής διαθεσιμότητας.*
> *»*

Ενώ ο Πίνακας Εξοπλισμού αναφέρεται σε σύστημα και όχι συσκευές *«Σύστημα προστασίας Δικτύου και Κέντρου Δεδομένων ΠΣΔ – Next Generation Firewall»* το οποίο σύμφωνα και με την προδιαγραφή fw1.3 του ΠΤΧ1 απαιτείται να είναι ζεύγος συσκευών. Συγκεκριμένα η προδιαγραφή αναφέρει σα*φώς :*

> *«**fw 1.3** - Το προσφερόμενο σύστημα θα έχει τη μορφή ενός ζεύγους συσκευών ιδίου τύπου σε διάταξη υψηλής διαθεσιμότητας (High Availability»*

Στο αναφερόμενο σημείο του πίνακα προσφερόμενου εξοπλισμού προστέθηκε σχετική διευκρίνιση και λαμβάνει τη μορφή:

> *Σύστημα προστασίας Δικτύου και Κέντρου Δεδομένων ΠΣΔ – Next Generation Firewall (σύστημα ζεύγους συσκευών)*

4.2 Σχόλιο 2ο

Κεφάλαιο 8.

ΠΑΡΑΡΤΗΜΑ ΙΙ – ΥΠΟΔΕΙΓΜΑ ΤΕΧΝΙΚΗΣ ΠΡΟΣΦΟΡΑΣ σελ. 58 Προτείνεται η προσθήκη οδηγίας η οποία να διευκρινίζει «Σε κάθε προδιαγραφή των πινάκων συμμόρφωσης στην οποία ζητείται η συμμόρφωση με χαρακτηριστικά και τα αντίστοιχα RFCs , να ικανοποιείται η απαίτηση της προδιαγραφής με παραπομπή που τεκμηριώνει το χαρακτηριστικό ή το RFC ή και τα δύο.»

Απάντηση

Προστέθηκε η προτεινόμενη οδηγία.

5 Φορέας 5

5.1 Σχόλιο 1ο

Σχετικά με την προδιαγραφή 3.3. Δυνατότητα επαύξησης της δυναμικότητας με προσθήκη επιπλέον συσκευής Επειδή υπάρχουν λύσεις στην αγορά που στο active-active cluster ομαδοποιούνται ανά δυο συστήματα, θα θέλαμε αυτή η προδιαγραφή να είναι πιο ανοικτή ώστε να μπορούν να συμμετέχουν και αυτές οι προσεγγίσεις. Η πρόταση μας είναι να «υπάρχει Δυνατότητα επαύξησης της δυναμικότητας με προσθήκη επιπλέον συσκευής έχοντας κοινή διαχείριση.

Απάντηση

Γίνεται δεκτή η παρατήρηση και γίνεται προσαρμογή των σχετικών προδιαγραφών ως ακολούθως σε συνδυασμό με σχετική παρατήρηση του φορέα 3, παρατήρηση 8.

fw 3.1	Το προσφερόμενο σύστημα θα πρέπει να εκπληρώνει τα ακόλουθα χαρακτηριστικά οριζόντιας κλιμάκωσης:	**ΝΑΙ**
fw 3.2	Διαμόρφωση σε διάταξη υψηλής διαθεσιμότητας με αξιοποίηση της δυναμικότητας και των δύο προσφερόμενων συσκευών	**ΝΑΙ**
fw 3.3	Δυνατότητα επαύξησης της δυναμικότητας με προσθήκη επιπλέον συσκευής ή συσκευών έχοντας κοινή διαχείριση.	**ΝΑΙ**
fw 3.4	Ενιαία διαχείριση σε όλες τις συσκευές της διάταξης	**ΝΑΙ**

5.2 Σχόλιο 2ο

Υπάρχουν προσεγγίσεις στην αγορά που δεν υποστηρίζουν την λογική κατακερματισμό σε λογικά τείχη προστασίας μέσα στο appliance αλλά υποστηρίζουν μηχανισμούς κατακερματισμού σε επίπεδο διαχείρισης.

Θα θέλαμε την προδιαγραφή αυτή πιο ανοικτή όπως για παράδειγμα Να αναφερθούν οι λογικές καταμερισμού που υποστηρίζονται. Τόσο σε επίπεδο λογικών οντοτήτων όσο και σε επίπεδο επιμερισμού εργασιών και διαχείρισης. Να αναφερθεί εάν υποστηρίζονται virtual firewall , VRF ή virtual domains η αντίστοιχες τεχνολογίες

Απάντηση

Η απαίτηση για λογικό κατακερματισμό είναι απαραίτητη για λειτουργικούς και διαχειριστικούς λόγους του συστήματος προστασίας NGFW και δεν είναι δυνατό να τροποποιηθεί. Ειδικότερα η απαίτηση αυτή είναι απαραίτητη για χρήση του firewall σε διαφορετικά πεδία εφαρμογών πέρα του κέντρου δεδομένων, όπως Intranet, η προστασία δικτύου ή εφαρμογών συγκεκριμένων μονάδων του Πανελληνίου Σχολικού δικτύου, δοκιμαστική εφαρμογή κανόνων και πολιτικών.

Η προδιαγραφή παραμένει ως έχει.

5.3 Σχόλιο 3ο

Σχετικά με την προδιαγραφή 4.6 Δυνατότητα χρήσης μελλοντικά συσκευών sandboxing που θα λειτουργούν στην υποδομή του ΠΣΔ, με σκοπό την λειτουργία σε μεγάλο αριθμό αρχείων Υπάρχουν προσεγγίσεις στην αγορά που χρησιμοποιούν cloud resources για το sandbox με αποτέλεσμα η συγκεκριμένη προδιαγραφή να μην κάνει apply σε αυτές τις προσεγγίσεις. Θα θέλαμε είτε να γίνει προαιρετική η προδιαγραφή αυτή είτε να γραφόταν διαφορετικά ώστε να μπορούν οι προσεγγίσεις αυτές να ικανοποιούν την προδιαγραφή αυτή

Απάντηση

Γίνεται δεκτή η πρόταση και τίθεται προαιρετική η εν λόγω προδιαγραφή fw 4.6.

6 Επιπλέον αλλαγές

Πλέον των μεταβολών που προέκυψαν ως αποτέλεσμα των προτάσεων των ενδιαφερομένων φορέων, έγιναν και οι ακόλουθες αλλαγές:

6.1 Τμήμα 2, ΠΤΧ 1. Σύστημα Προστασίας Δικτύου – Firewall (Next Generation)

Για λόγους σαφήνειας η προδιαγραφή:

fw 4.7	Δυνατότητα ανίχνευσης και αποτροπής επιθέσεων, χωρίς να βασίζεται σε υπογραφές (signatures) ακόμη και σε καταστάσεις “πρώτης εμφάνισης” (patient-zero) μιας απειλής σε χρήστες συστήματα υπηρεσίες

Προσαρμόζεται σε:

fw 4.7	Δυνατότητα ανίχνευσης και αποτροπής επιθέσεων, χωρίς να βασίζεται σε υπογραφές (signatures) ακόμη και σε καταστάσεις “πρώτης εμφάνισης” (patient-zero) μιας απειλής σε χρήστες, συστήματα και υπηρεσίες. *Θα πρέπει να προσφερθεί το απαιτούμενο υλικό (hardware), λογισμικό (software) ή άδειες ή ισοδύναμα virtual appliance ή υπηρεσία cloud που απαιτούνται για τη λειτουργία αυτή.*

Ομοίως για λόγους σαφήνειας προσαρμόζεται η προδιαγραφή

fw 10.1	Η υποστήριξη και οι ανανεωμένες εκδόσεις του λογισμικού θα προέρχονται από τον κατασκευαστή του προϊόντος	ΝΑΙ

Προσαρμόζεται σε:

fw 10.1	Η υποστήριξη του συστήματος όσον αφορά το υλικό λογισμικό και οι ανανεωμένες εκδόσεις του λογισμικού θα προέρχονται από τον κατασκευαστή του προϊόντος	ΝΑΙ

6.2 Τμήμα 2, ΠΤΧ 2 Δικτυακές συσκευές καταμερισμού φορτίου Load Balancers (LB)

1. Οι προδιαγραφές LB 6.3, LB 6.4 γίνονται προαιρετικές καθώς σε έλεγχο που έγιναν σε Data sheets κατασκευαστών δεν φαίνεται να αναφέρονται.
2. Αλλαγές στις προδιαγραφές LB 9.5.2 και LB 9.6 για προστασία από tear drop, ping-of-death
   - Στην προδιαγραφή LB 9.5.2 η απαίτηση για προστασία από tear drop, ping-of-death αφαιρείται.

- Στην προδιαγραφή LB 9.7 προστίθεται η αναφορά σε προστασία από tear drop, ping-of-death.

Μετά τις ως άνω μεταβολές οι προδιαγραφές διαμορφώνονται ως ακολούθως:

LB 9.5.2	• Προστασία από επιθέσεις τύπου Syn-flood.	ΝΑΙ		
LB 9.6	Να αναφερθεί η παρεχόμενη προστασία από επιθέσεις άλλου τύπου όπως Nimda, Smurf, tear drop, ping-of-death. Επιπλέον χαρακτηριστικά προστασίας θα αξιολογηθούν θετικά.	ΝΑΙ		