

ΕΚΔΟΣΕΙΣ ΚΛΕΙΔΑΡΙΘΜΟΣ

ΑΣΦΑΛΕΙΑ ΥΠΟΛΟΓΙΣΤΩΝ

ΑΡΧΕΣ ΚΑΙ ΠΡΑΚΤΙΚΕΣ

3η αμερικανική έκδοση



William Stallings • Lawrie Brown



Κεφάλαιο 9

Τείχη προστασίας και συστήματα
αποτροπής εισβολών



Η ανάγκη για τείχη προστασίας



- Πλέον η σύνδεση στο Διαδίκτυο είναι απαραίτητη για τους οργανισμούς
 - Ωστόσο συνιστά απειλή
- Αποτελεσματικά μέσα προστασίας τοπικών δικτύων
- Εισάγεται μεταξύ του δικτύου μιας κτιριακής εγκατάστασης και του Διαδικτύου προκειμένου να δημιουργηθεί ένας ελεγχόμενος σύνδεσμος
 - Ενδέχεται να αποτελείται από ένα μόνο υπολογιστικό σύστημα ή από ένα σύνολο δύο ή περισσότερων συστημάτων τα οποία συνεργάζονται μεταξύ τους
- Χρησιμοποιείται ως περιμετρική άμυνα
 - Παροχή ενός μόνο κομβικού σημείου για την επιβολή της ασφάλειας και της διαχειριστικής παρακολούθησης
 - Απομονώνει τα εσωτερικά συστήματα από εξωτερικά δίκτυα

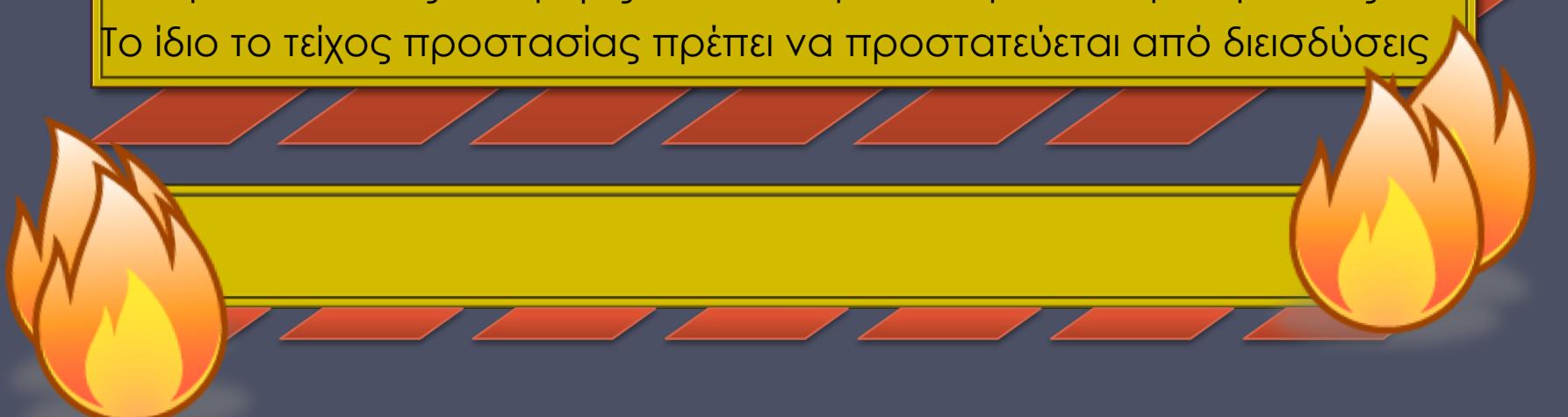
Χαρακτηριστικά τειχών προστασίας

Σχεδιαστικοί στόχοι

Όλη η κυκλοφορία από μέσα προς τα έξω, και αντίστροφα, πρέπει να περνά από το τείχος προστασίας

Πρέπει να επιτρέπεται η διέλευση μόνο εξουσιοδοτημένης κυκλοφορίας δεδομένων, όπως αυτή ορίζεται από την τοπική πολιτική ασφαλείας

Το ίδιο το τείχος προστασίας πρέπει να προστατεύεται από διεισδύσεις



Πολιτική πρόσβασης τείχους προστασίας

- Ένα κρίσιμο κομμάτι στον σχεδιασμό και την υλοποίηση ενός τείχους προστασίας είναι ο ορισμός κατάλληλης πολιτικής πρόσβασης
 - Σε αυτή θα ορίζονται οι τύποι της κυκλοφορίας που είναι εξουσιοδοτημένοι να διέρχονται από το τείχος προστασίας
 - Περιλαμβάνει συγκεκριμένα πρωτόκολλα, εφαρμογές, εύρος διευθύνσεων και τύπους περιεχομένου
- Αυτή η πολιτική πρέπει να αναπτυχθεί με βάση την εκτίμηση κινδύνου και τη σχετική πολιτική ασφαλείας των πληροφοριών του οργανισμού
- Πρέπει επίσης να αναπτυχθεί με βάση μια γενική προδιαγραφή η οποία θα καθορίζει τους τύπους κυκλοφορίας που πρέπει να υποστηρίζει ο οργανισμός
 - Στη συνέχεια μπορεί να αποσαφηνιστεί περαιτέρω ώστε να ορίζει λεπτομερώς τα στοιχεία φίλτρων τα οποία μπορούν να υλοποιηθούν με τη μορφή μιας κατάλληλης τοπολογίας τείχους προστασίας

Χαρακτηριστικά φίλτρων τείχους προστασίας

- Χαρακτηριστικά τα οποία θα μπορούσε να χρησιμοποιεί η πολιτική πρόσβασης ενός τείχους προστασίας για να φιλτράρει την κυκλοφορία:

Τιμές
διευθύνσεων IP
και
πρωτοκόλλων

Τύπος φιλτραρίσματος που νιοθετείται από τείχη προστασίας με φίλτρα πακέτων και τείχη προστασίας με καταστασιακή επιθεώρηση

Συνήθως περιορίζει την πρόσβαση σε συγκεκριμένες υπηρεσίες

Πρωτόκολλα εφαρμογών

Χρησιμοποιείται από μια πύλη επιπέδου εφαρμογών η οποία αναμεταδίδει και παρακολουθεί την ανταλλαγή πληροφοριών για συγκεκριμένα πρωτόκολλα εφαρμογών

Ταυτότητα χρηστών

Συνήθως προορίζεται για χρήστες εκ των έσω οι οποίοι ταυτοποιούνται με κάποια μορφή ασφαλούς τεχνολογίας πιστοποίησης ταυτότητας

Δραστηριότητα δικτύου

Η πρόσβαση ελέγχεται με βάση παράγοντες όπως ο χρόνος της αίτησης, ο ρυθμός των αιτήσεων, ή άλλα μοτίβα δραστηριότητας

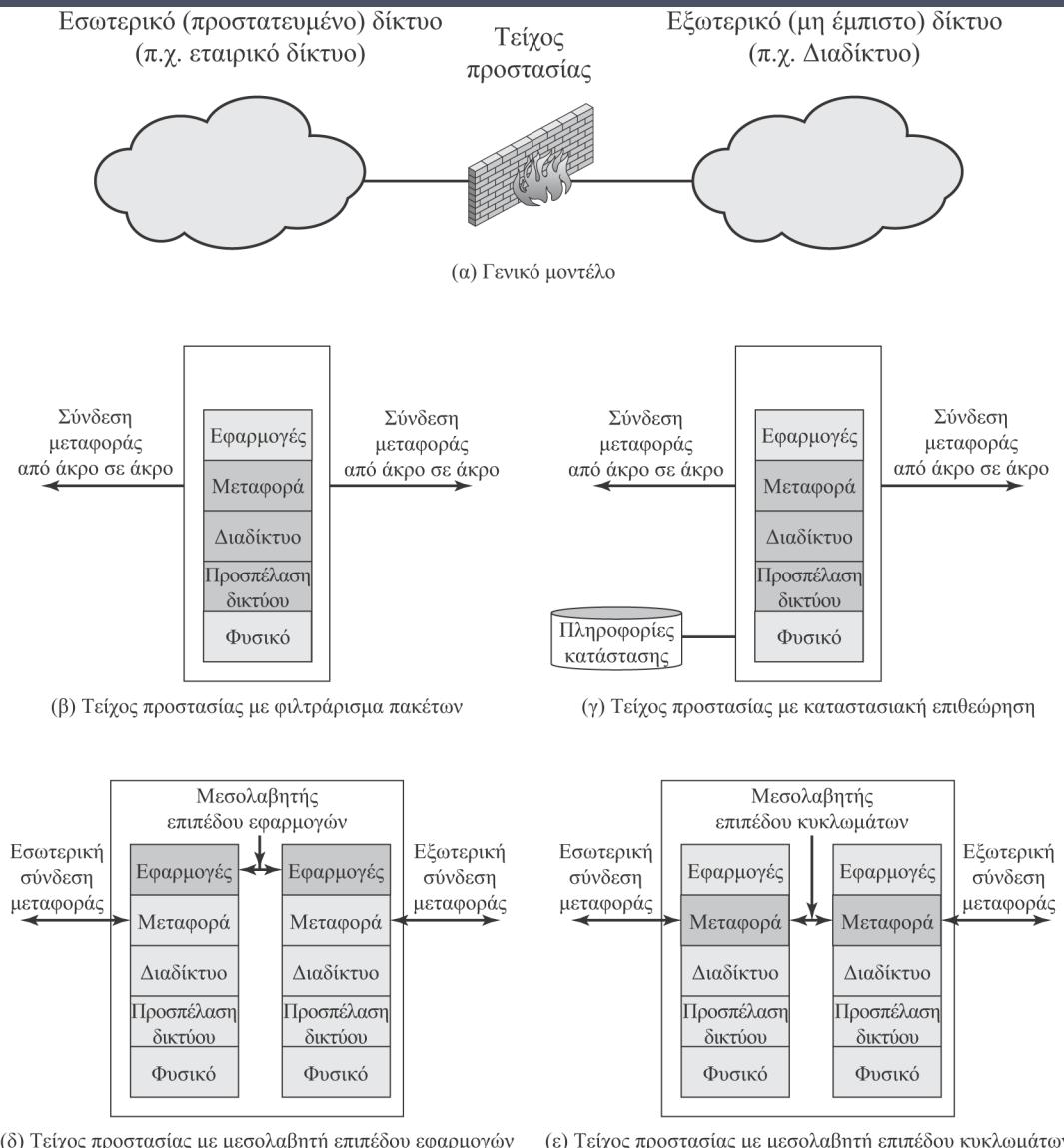
Δυνατότητες και περιορισμοί ενός τείχους προστασίας

Δυνατότητες:

- Ορίζει ένα μοναδικό κομβικό σημείο
- Παρέχει μια τοποθεσία για την παρακολούθηση συμβάντων ασφαλείας
- Βολικό περιβάλλον για αρκετές λειτουργίες του Διαδικτύου οι οποίες δεν σχετίζονται με την ασφάλεια
- Μπορεί να χρησιμεύσει ως περιβάλλον για την Ασφάλεια IP (IPSec)

Περιορισμοί:

- Δεν παρέχει προστασία από επιθέσεις που το παρακάμπτουν
- Ενδέχεται να μην προστατεύει πλήρως από εσωτερικές απειλές
- Ένα ασύρματο LAN με ελλιπή ασφάλεια ενδέχεται να προσπελαστεί από σημεία εκτός του οργανισμού
- Φορητοί υπολογιστές, PDA, ή φορητές συσκευές αποθήκευσης μπορεί να μολυνθούν κάπου έξω από το εταιρικό δίκτυο και κατόπιν να χρησιμοποιηθούν μέσα στο δίκτυο



Εικόνα 9.1 Τύποι τειχών προστασίας

Τείχος προστασίας με φιλτράρισμα πακέτων

- Εφαρμόζει κανόνες σε κάθε εισερχόμενο και εξερχόμενο πακέτο IP
 - Συνήθως μια λίστα κανόνων που βασίζονται σε ταιριάσματα με πεδία της κεφαλίδας IP ή TCP
 - Προωθεί ή απορρίπτει το πακέτο με βάση τους κανόνες που ταιριάζουν

Οι κανόνες φιλτραρίσματος βασίζονται σε πληροφορίες που περιέχονται σε ένα πακέτο δικτύου

- Διεύθυνση προέλευσης IP
 - Διεύθυνση προορισμού IP
 - Διεύθυνση προέλευσης και διεύθυνση προορισμού επιπέδου μεταφοράς
 - Πεδίο πρωτοκόλλου IP
 - Διασύνδεση
- Δύο προεπιλεγμένες πολιτικές:
 - Απόρριψη - απαγορεύεται οτιδήποτε δεν επιτρέπεται ρητά
 - Πιο συντηρητική, ελεγχόμενη, ορατή στους χρήστες
 - Προώθηση - επιτρέπεται οτιδήποτε δεν απαγορεύεται ρητά
 - Ευκολότερη διαχείριση και χρήση, μειωμένη ασφάλεια

Πίνακας 9.1

Παραδείγματα φιλτραρίσματος πακέτων

Κανόνας	Κατεύθυνση	Διεύθυνση προέλευσης	Διεύθυνση προορισμού	Πρωτόκολλο	Θύρα προορισμού	Ενέργεια
1	Εισερχόμενη	Εξωτερική	Εσωτερική	TCP	25	Επιτρέπεται
2	Εξερχόμενη	Εσωτερική	Εξωτερική	TCP	>1023	Επιτρέπεται
3	Εξερχόμενη	Εσωτερική	Εξωτερική	TCP	25	Επιτρέπεται
4	Εισερχόμενη	Εξωτερική	Εσωτερική	TCP	>1023	Επιτρέπεται
5	Οποιαδήποτε	Οποιαδήποτε	Οποιαδήποτε	Οποιοδήποτε	Οποιαδήποτε	Απαγορεύεται

Φίλτρο πακέτων – Πλεονεκτήματα και αδυναμίες

- Πλεονεκτήματα
 - Απλότητα
 - Συνήθως είναι διαφανή στους χρήστες και πολύ γρήγορα
- Αδυναμίες
 - Δεν αποτρέπουν επιθέσεις που εκμεταλλεύονται ευπάθειες ή λειτουργίες συγκεκριμένων εφαρμογών
 - Περιορισμένη λειτουργικότητα καταγραφής
 - Δεν υποστηρίζουν προχωρημένες μεθόδους πιστοποίησης ταυτότητας χρηστών
 - Είναι ευάλωτα σε επιθέσεις που εκμεταλλεύονται σφάλματα του πρωτοκόλλου TCP/IP
 - Εσφαλμένες διευθετήσεις μπορούν να οδηγήσουν σε παραβιάσεις

Τείχος προστασίας με καταστασιακή επιθεώρηση

Ορίζει πιο αυστηρούς κανόνες για την κυκλοφορία TCP δημιουργώντας έναν κατάλογο εξερχόμενων συνδέσεων TCP

- Υπάρχει μία καταχώριση για κάθε ήδη εγκαθιδρυμένη σύνδεση
- Το φίλτρο πακέτων επιτρέπει την εισερχόμενη κυκλοφορία προς θύρες με μεγάλους αριθμούς μόνο για εκείνα τα πακέτα που ταιριάζουν με το προφίλ μίας από τις καταχωρίσεις του καταλόγου

Εξετάζει πληροφορίες πακέτων αλλά καταγράφει επίσης πληροφορίες για τις συνδέσεις TCP

- Παρακολουθεί τους αριθμούς ακολουθίας TCP ώστε να αποτρέπει επιθέσεις οι οποίες εξαρτώνται από τον αριθμό ακολουθίας
- Επιθεωρεί τα δεδομένα αναζητώντας εντολές πρωτοκόλλων όπως τα FTP, IM και SIPS



Πίνακας 9.2

Παράδειγμα πίνακα κατάστασης συνδέσεων
ενός καταστασιακού τείχους προστασίας

Διεύθυνση προέλευσης	Θύρα προέλευσης	Διεύθυνση προορισμού	Θύρα προορισμού	Κατάσταση σύνδεσης
192.168.1.100	1030	210.9.88.29	80	Εγκαθιδρυμένη
192.168.1.102	1031	216.32.42.123	80	Εγκαθιδρυμένη
192.168.1.101	1033	173.66.32.122	25	Εγκαθιδρυμένη
192.168.1.106	1035	177.231.32.12	79	Εγκαθιδρυμένη
223.43.21.231	1990	192.168.1.6	80	Εγκαθιδρυμένη
219.22.123.32	2112	192.168.1.6	80	Εγκαθιδρυμένη
210.99.212.18	3321	192.168.1.6	80	Εγκαθιδρυμένη
24.102.32.23	1025	192.168.1.6	80	Εγκαθιδρυμένη
223.21.22.12	1046	192.168.1.6	80	Εγκαθιδρυμένη

Πύλη επιπέδου εφαρμογών

- Γνωστή και ως μεσολαβητής επιπέδου εφαρμογών
- Λειτουργεί ως αναμεταδότης της κυκλοφορίας επιπέδου εφαρμογών
 - Ο χρήστης επικοινωνεί με την πύλη χρησιμοποιώντας μια εφαρμογή TCP/IP
 - Πιστοποιείται η ταυτότητα του χρήστη
 - Η πύλη επικοινωνεί με την εφαρμογή στον απομακρυσμένο υπολογιστή υπηρεσίας και αναμεταδίδει τμήματα TCP μεταξύ διακομιστή και χρήστη
- Πρέπει να έχει κώδικα μεσολάβησης για κάθε εφαρμογή
 - Μπορεί να περιορίζει τις υποστηριζόμενες δυνατότητες της εφαρμογής
- Τείνει να είναι πιο ασφαλής από τα φίλτρα πακέτων
- Ένα μειονέκτημα είναι η πρόσθετη επεξεργαστική επιβάρυνση για κάθε σύνδεση

Πύλη επιπέδου κυκλωμάτων

Μεσολαβητής
επιπέδου κυκλωμάτων

- Η πύλη διαμορφώνει δύο συνδέσεις TCP, μία μεταξύ της ίδιας και ενός χρήστη TCP σε κάποιον εσωτερικό και εξωτερικό υπολογιστή υπηρεσίας, αντίστοιχα
- Αναμεταδίδει τμήματα TCP από τη μία σύνδεση προς την άλλη χωρίς να εξετάζει τα περιεχόμενα
- Η λειτουργία ασφαλείας ισοδυναμεί με τον προσδιορισμό των επιτρεπόμενων συνδέσεων

Συνήθως χρησιμοποιείται όταν οι εσωτερικοί
χρήστες θεωρούνται έμπιστοι

- Μπορεί να χρησιμοποιεί πύλη επιπέδου εφαρμογών και κυκλωμάτων στις εσωτερικές και εξωτερικές συνδέσεις, αντίστοιχα
- Μικρότερες επιβαρύνσεις

Πύλη επιπέδου κυκλωμάτων SOCKS

- Η έκδοση 5 του SOCKS ορίζεται στο RFC1928
- Σχεδιασμένο να παρέχει ένα πλαίσιο εργασίας για εφαρμογές πελάτη-διακομιστή σε περιοχές TCP και UDP, με απώτερο σκοπό τη βολική και ασφαλή χρήση των υπηρεσιών ενός τείχους προστασίας δικτύου
- Η εφαρμογή πελάτη επικοινωνεί με τον διακομιστή SOCKS, πιστοποιεί την ταυτότητά της και στέλνει αίτηση αναμετάδοσης
 - Ο διακομιστής την αξιολογεί και είτε πραγματοποιεί την κατάλληλη σύνδεση είτε αρνείται



Οχυρωματικός υπολογιστής υπηρεσίας

- Σύστημα το οποίο καθορίζεται ως κρίσιμο κομβικό σημείο της ασφάλειας του δικτύου
- Χρησιμεύει ως περιβάλλον μιας πύλης επιπέδου εφαρμογών ή κυκλωμάτων
- Τυπικά χαρακτηριστικά:
 - Ασφαλές λειτουργικό σύστημα, μόνο βασικές υπηρεσίες
 - Ενδέχεται να απαιτεί πιστοποίηση ταυτότητας για πρόσβαση στον μεσολαβητή ή υπολογιστή υπηρεσίας
 - Κάθε μεσολαβητής μπορεί να περιορίζει τις υποστηριζόμενες δυνατότητες, και να επιτρέπει την πρόσβαση μόνο σε συγκεκριμένους υπολογιστές υπηρεσίας
 - Κάθε μεσολαβητής είναι ένα μικρό, απλό πακέτο ελεγμένο ως προς την ασφάλειά του
 - Κάθε μεσολαβητής είναι ανεξάρτητος, και εκτελείται με δικαιώματα μη προνομιακού χρήστη
 - Περιορισμένη χρήση του δίσκου, άρα κώδικας μόνο για ανάγνωση

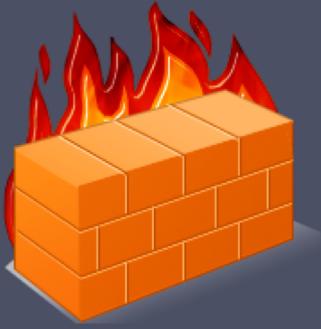


Τείχη προστασίας βασισμένα σε υπολογιστές υπηρεσίας

- Χρησιμοποιούνται για την προστασία μεμονωμένων υπολογιστών υπηρεσίας
- Είναι ενσωματωμένα στα λειτουργικά συστήματα ή μπορούν να παρέχονται ως πρόσθετα πακέτα
- Φιλτράρουν και περιορίζουν τη ροή των πακέτων
- Δημοφιλής θέση: διακομιστές

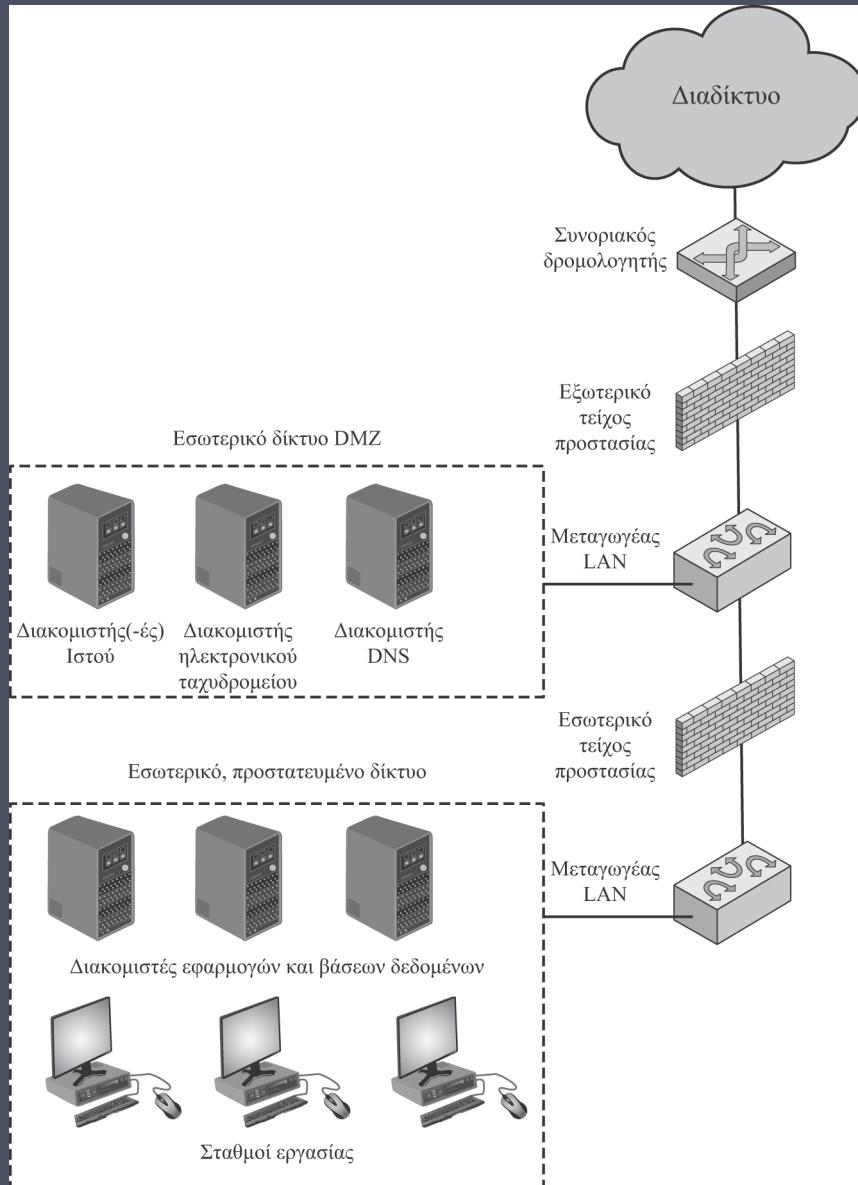
Πλεονεκτήματα:

- Οι κανόνες φιλτραρίσματος μπορούν να προσαρμοστούν ειδικά για το περιβάλλον του υπολογιστή υπηρεσίας
- Παρέχεται προστασία ανεξαρτήτως τοπολογίας
- Παρέχουν ένα πρόσθετο επίπεδο προστασίας

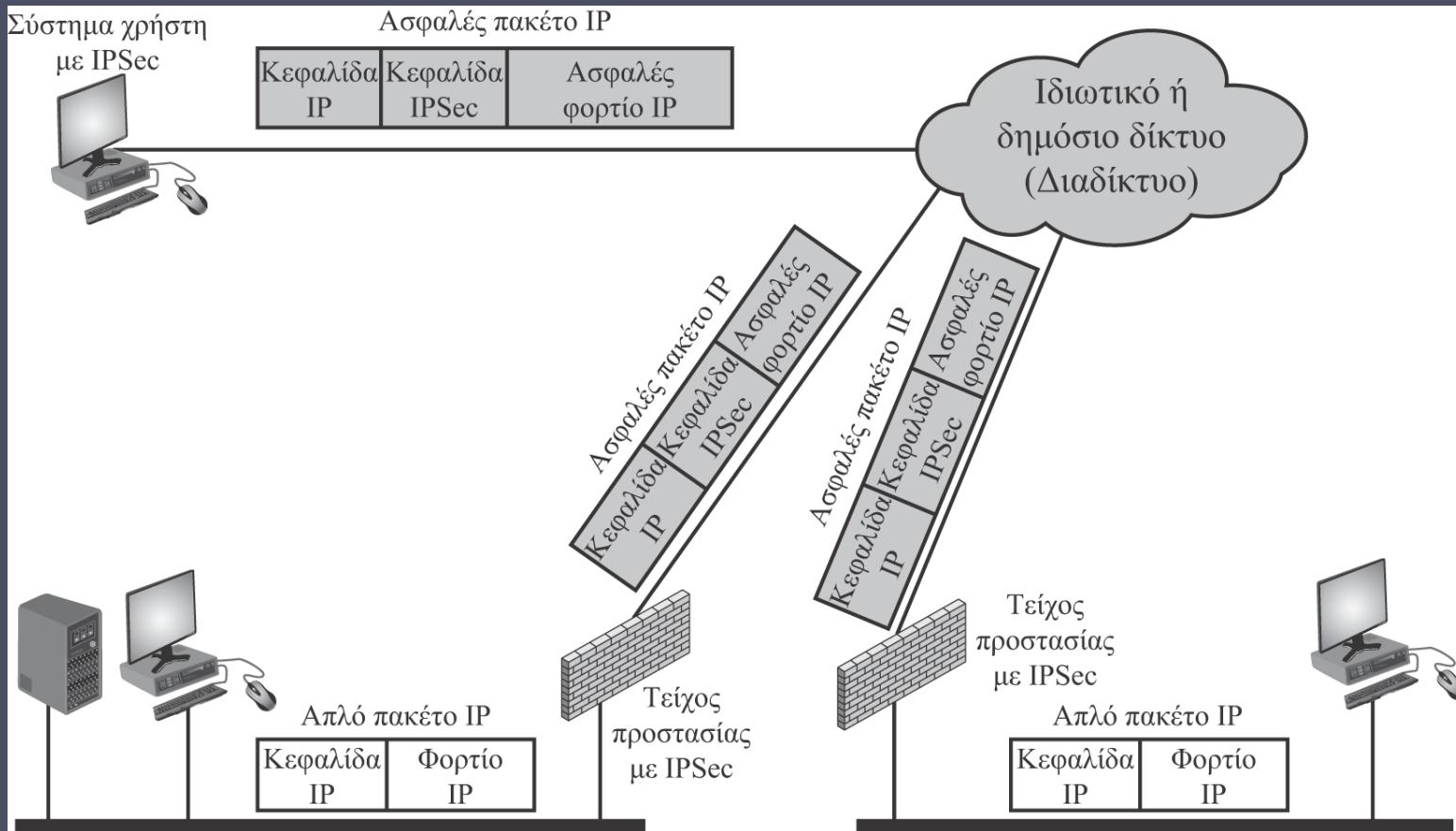


Προσωπικό τείχος προστασίας

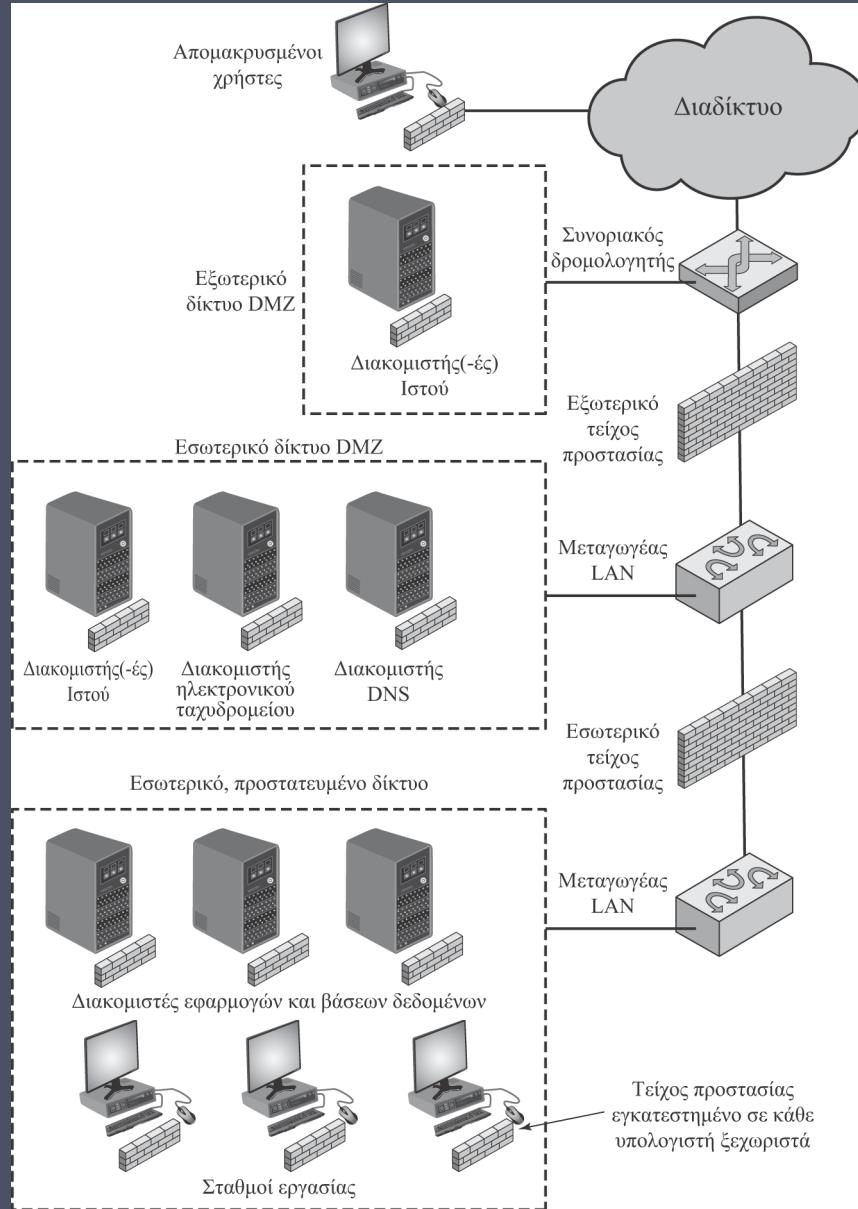
- Ελέγχει την κυκλοφορία μεταξύ ενός προσωπικού υπολογιστή ή σταθμού εργασίας και του Διαδικτύου ή εταιρικού δικτύου
- Χρήση σε οικιακά περιβάλλοντα και σε εταιρικά ενδοδίκτυα
- Συνήθως είναι μια υπομονάδα λογισμικού στο PC
- Μπορεί να φιλοξενείται σε έναν δρομολογητή που συνδέει όλους τους οικιακούς υπολογιστές σε μια γραμμή DSL, ένα καλωδιακό μόντεμ, ή άλλη διασύνδεση Διαδικτύου
- Συνήθως είναι λιγότερο πολύπλοκα από αυτόνομα τείχη προστασίας ή τείχη προστασίας βασισμένα σε διακομιστές
- Ο κύριος ρόλος του είναι να μην επιτρέπει την απομακρυσμένη πρόσβαση χωρίς εξουσιοδότηση
- Μπορεί επίσης να παρακολουθεί την εξερχόμενη δραστηριότητα προκειμένου να ανιχνεύει και να εμποδίζει την εξάπλωση σκουληκιών και άλλου κακόβουλου λογισμικού



Εικόνα 9.2 Παράδειγμα διευθέτησης ενός τείχους προστασίας



Εικόνα 9.3 Σενάριο ασφάλειας μέσω VPN



Εικόνα 9.4 Παράδειγμα κατανεμημένης διευθέτησης τειχών προστασίας

Τοπολογίες τειχών προστασίας

Τείχος προστασίας εγκατεστημένο σε υπολογιστή υπηρεσίας

- Περιλαμβάνει λογισμικό προσωπικών τειχών προστασίας και λογισμικό τειχών προστασίας σε διακομιστές

Δρομολογητής διαλογής

- Ένας (και μόνο) δρομολογητής μεταξύ εσωτερικών και εξωτερικών δικτύων με μη καταστασιακό ή πλήρες φιλτράρισμα πακέτων

Μονή εμβόλιμη οχυρωματική συσκευή

- Μία συσκευή τείχους προστασίας μεταξύ ενός εσωτερικού και ενός εξωτερικού δρομολογητή

Μονή οχυρωματική συσκευή σε διάταξη T

- Διαθέτει και τρίτη διασύνδεση δικτύου που λειτουργεί οχυρωματικά για ένα DMZ στο οποίο τοποθετούνται διακομιστές ορατοί στον έξω κόσμο

Διπλή εμβόλιμη οχυρωματική συσκευή

- To DMZ είναι στριμωγμένο μεταξύ οχυρωματικών τειχών προστασίας

Διπλή οχυρωματική συσκευή σε διάταξη T

- To DMZ βρίσκεται σε ξεχωριστή διασύνδεση δικτύου του οχυρωματικού τείχους προστασίας

Κατανεμημένη διευθέτηση τειχών προστασίας

- Χρησιμοποιείται από μεγάλες επιχειρήσεις και κρατικούς οργανισμούς

Σύστημα αποτροπής εισβολών (IPS)

- Γνωστό και ως σύστημα ανίχνευσης και αποτροπής εισβολών (IDPS)
- Αποτελεί επέκταση των IDS η οποία περιλαμβάνει τη δυνατότητα μπλοκαρίσματος ή αποτροπής της ανιχνευόμενης κακόβουλης δραστηριότητας
- Μπορεί να είναι βασισμένο σε υπολογιστή υπηρεσίας, βασισμένο σε δίκτυο, ή κατανεμημένο/υβριδικό
- Μπορεί να χρησιμοποιεί ανίχνευση ανωμαλιών για να αναγνωρίζει συμπεριφορές που δεν συνάδουν με έγκυρους χρήστες, ή ανίχνευση υπογραφών/ευρετική ανίχνευση για να αναγνωρίζει κακόβουλες συμπεριφορές
- Μπορεί να μπλοκάρει επιμέρους κυκλοφορία, όπως τα τείχη προστασίας· για να προσδιορίσει πότε πρέπει να κάνει κάτι τέτοιο όμως, χρησιμοποιεί τους τύπους αλγορίθμων που έχουν αναπτυχθεί για συστήματα IDS

IPS βασισμένο σε υπολογιστή υπηρεσίας (HIPS)

- Κάνει χρήση είτε μεθόδων ανίχνευσης ανωμαλιών είτε μεθόδων που βασίζονται σε ανίχνευση υπογραφών/ευρετική ανίχνευση προκειμένου να αναγνωρίζει επιθέσεις
 - Υπογραφές: Εστιάζει στο συγκεκριμένο περιεχόμενο της κυκλοφορίας δικτύου των εφαρμογών, ή των ακολουθιών κλήσεων συστήματος, αναζητώντας μοτίβα τα οποία έχουν αναγνωριστεί ως κακόβουλα
 - Ανωμαλίες: Το IPS ψάχνει μοτίβα συμπεριφοράς που παραπέμπουν σε κακόβουλο λογισμικό
- Παραδείγματα των τύπων κακόβουλης συμπεριφοράς που μπορεί να χειριστεί με επιτυχία ένα σύστημα HIPS:
 - Τροποποίηση πόρων συστήματος
 - Εκμετάλλευση ευπαθειών παροχής αυξημένων προνομίων
 - Εκμετάλλευση ευπαθειών υπερχείλισης περιοχών προσωρινής αποθήκευσης
 - Απόκτηση πρόσβασης στη λίστα επαφών ηλεκτρονικού ταχυδρομείου
 - Προσπέλαση καταλόγων

HIPS

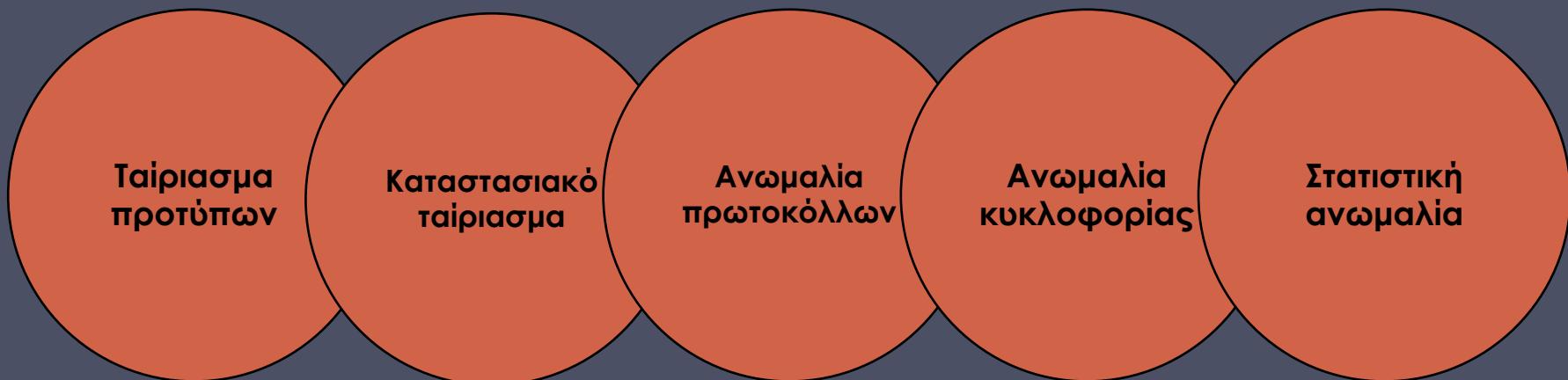
- Μπορεί να προσαρμοστεί για συγκεκριμένο υπολογιστικό περιβάλλον
- Μπορεί να χρησιμοποιηθεί ένα σύνολο εργαλείων γενικής χρήσης
- Μερικά πακέτα HIPS είναι σχεδιασμένα να προστατεύουν συγκεκριμένους τύπους διακομιστών (Ιστού, βάσεων δεδομένων)
 - Σε αυτή την περίπτωση, το HIPS παρακολουθεί για επιθέσεις εναντίον συγκεκριμένων εφαρμογών
- Μπορεί να υιοθετήσει την προσέγγιση της ελεγχόμενης περιοχής
 - Οι ελεγχόμενες περιοχές (sandboxes) είναι ιδιαίτερα κατάλληλες για κινητό κώδικα, όπως οι μικροεφαρμογές Java και οι γλώσσες σεναρίων
 - Το HIPS θέτει τον κώδικα σε καραντίνα, σε κάποια απομονωμένη περιοχή του συστήματος, και μετά τον εκτελεί και παρακολουθεί τη συμπεριφορά του
- Τυπική προστασία που μπορεί να παρέχει ένα σύστημα HIPS σε επιτραπέζια περιβάλλοντα:
 - Κλήσεις συστήματος
 - Προσπέλαση συστήματος αρχείων
 - Ρυθμίσεις μητρώου συστήματος
 - Είσοδος/έξοδος υπολογιστή υπηρεσίας

Ο ρόλος των HIPS

- Πολλοί παρατηρητές του κλάδου θεωρούν το εταιρικό ακραίο σημείο, συμπεριλαμβανομένων των επιτραπέζιων και φορητών συστημάτων, ως τον κύριο στόχο των χάκερ και των εγκληματιών
 - Επομένως, οι κατασκευαστές επικεντρώνονται περισσότερο στην ανάπτυξη προϊόντων ασφαλείας για ακραία σημεία
 - Παραδοσιακά, η ασφάλεια των ακραίων σημείων παρέχεται από μια συλλογή διαφορετικών προϊόντων, όπως προϊόντα προστασίας από ιούς, κακόβουλο λογισμικό και ενοχλητικά μαζικά μηνύματα, καθώς και προσωπικά τείχη προστασίας
- Αποτελούν προσπάθεια δημιουργίας μιας ενοποιημένης σουίτας λειτουργιών με τη μορφή ενός μόνο προϊόντος
 - Πλεονεκτήματα της ενοποιημένης προσέγγισης: Τα διάφορα εργαλεία συνεργάζονται στενά μεταξύ τους, η αποτροπή απειλών είναι πιο διεξοδική, και η διαχείριση είναι πιο εύκολη
- Μια πιο συνετή προσέγγιση του ζητήματος είναι η χρήση συστημάτων HIPS στα πλαίσια μιας στρατηγικής άμυνας σε βάθος η οποία περιλαμβάνει και συσκευές επιπλέον δικτύου, όπως τείχη προστασίας ή συστήματα IPS βασισμένα σε δίκτυα

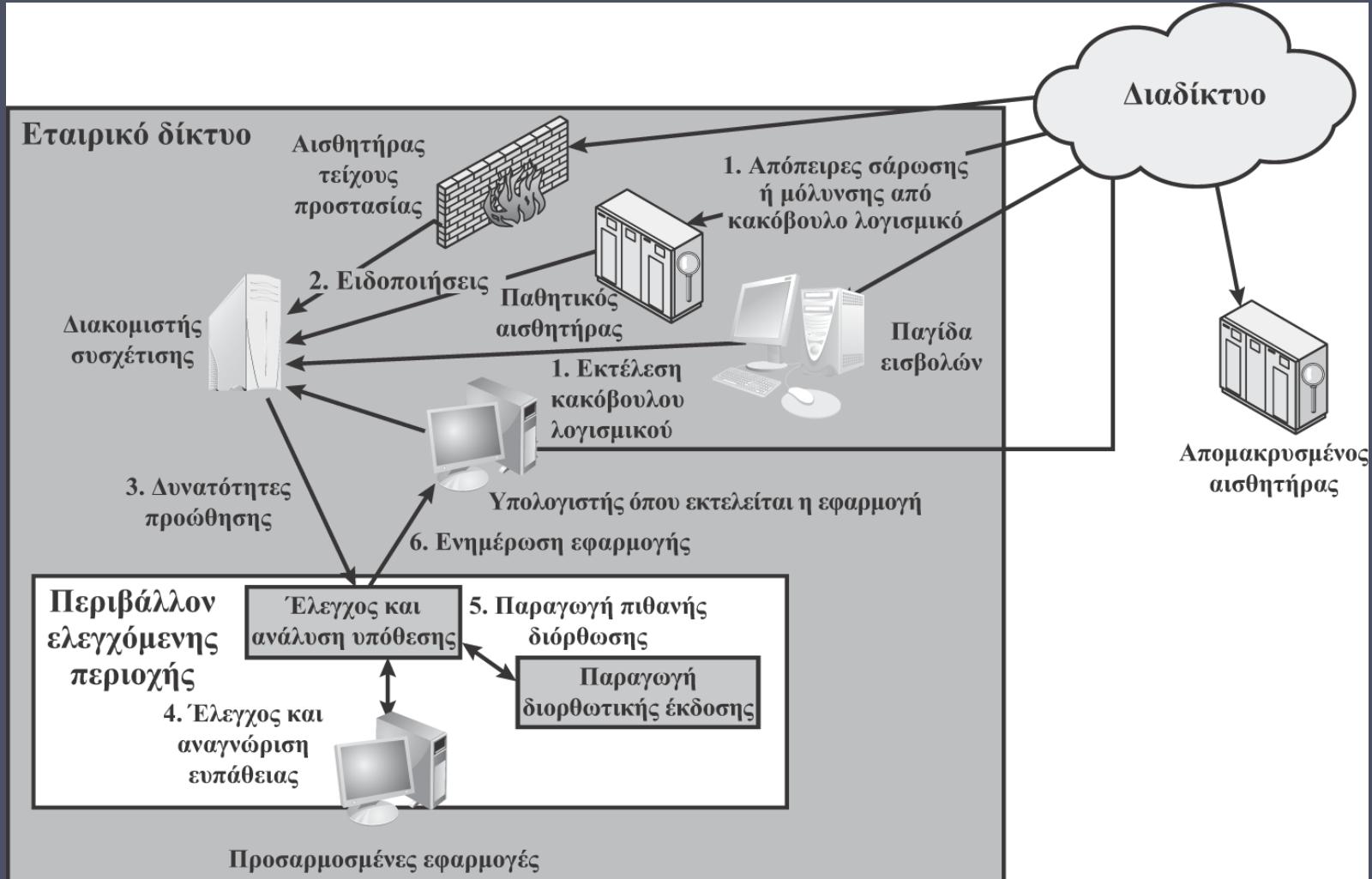
IPS βασισμένο σε δίκτυο (NIPS)

- Εμβόλιμο NIDS με εξουσία να τροποποιεί ή να απορρίπτει πακέτα και να καταστρέψει συνδέσεις TCP
- Χρησιμοποιεί τεχνικές όπως η ανίχνευση υπογραφών /ευρετική ανίχνευση και η ανίχνευση ανωμαλιών
- Ενδέχεται να παρέχει προστασία δεδομένων ροής
 - Αυτό απαιτεί την ανασυναρμολόγηση του φορτίου της εφαρμογής σε μια ακολουθία πακέτων
- Μέθοδοι για την αναγνώριση κακόβουλων πακέτων:



Ψηφιακό ανοσοποιητικό σύστημα

- Αναλυτική αμυντική λύση κατά της κακόβουλης συμπεριφοράς που προκαλείται από κακόβουλο λογισμικό
- Αναπτύχθηκε από την IBM και αργότερα βελτιώθηκε από τη Symantec
- Στα κίνητρα πίσω από την ανάπτυξή του περιλαμβάνονταν η ανερχόμενη απειλή του βασισμένου στο Διαδίκτυο κακόβουλου λογισμικού, η αυξανόμενη ταχύτητα της εξάπλωσής του λόγω του Διαδικτύου, καθώς και η ανάγκη να σχηματιστεί μια συνολική εικόνα της κατάστασης
- Η επιτυχία του ψηφιακού ανοσοποιητικού συστήματος εξαρτάται από την ικανότητα του συστήματος ανάλυσης κακόβουλου λογισμικού να ανιχνεύει νέα και πρωτότυπα στελέχη κακόβουλου λογισμικού



Εικόνα 9.5 Τοποθέτηση ελεγκτών κακόβουλου λογισμικού
(με βάση το άρθρο [SIDI05])

Snort Inline

- Επιτρέπει στο Snort να λειτουργεί ως σύστημα αποτροπής εισβολών
- Περιλαμβάνει μια επιλογή replace (αντικατάσταση), η οποία επιτρέπει στον χρήστη του Snort να τροποποιεί πακέτα αντί να τα απορρίπτει
 - Χρήσιμη για υλοποίηση παγίδας εισβολών
 - Οι επιτιθέμενοι βλέπουν την αποτυχία, αλλά δεν καταλαβαίνουν γιατί συνέβη

Drop

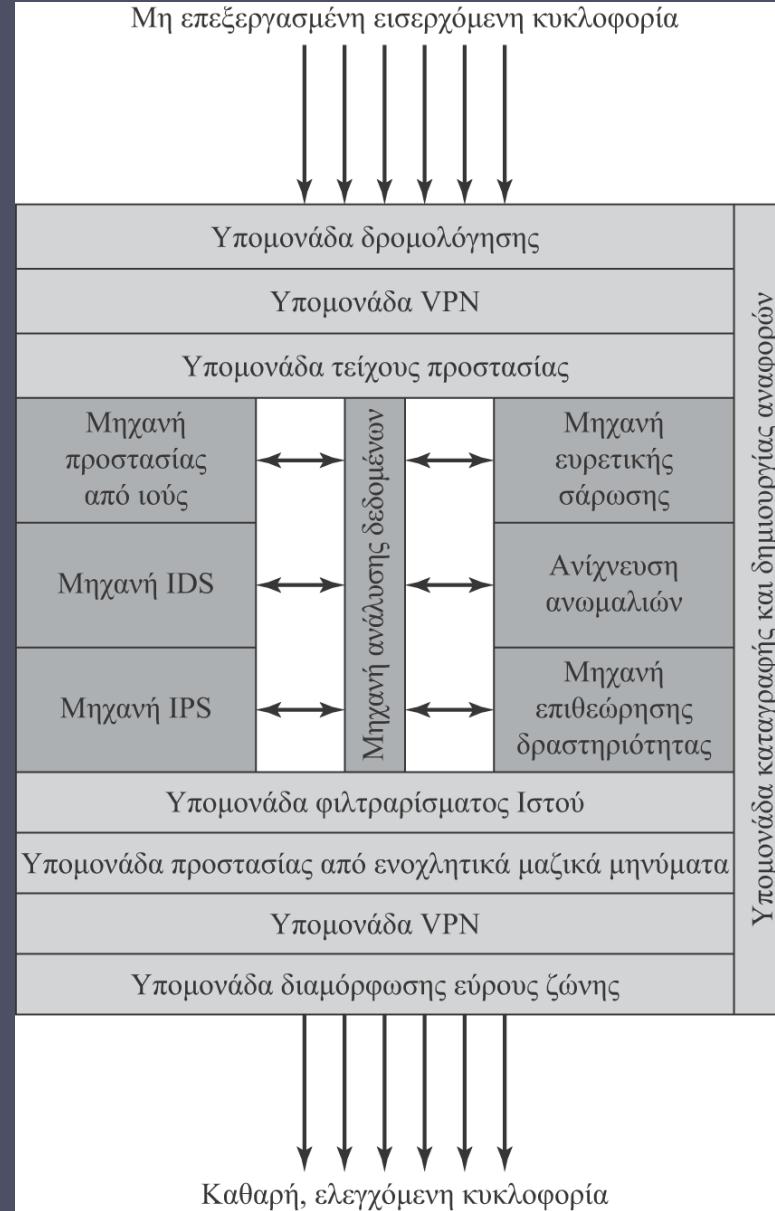
To Snort απορρίπτει ένα πακέτο με βάση τις επιλογές που ορίζονται στον κανόνα, καταγράφει το αποτέλεσμα

Reject

To Snort απορρίπτει ένα πακέτο, καταγράφει το αποτέλεσμα, και επιστρέφει μήνυμα σφάλματος

Sdrop

To Snort απορρίπτει ένα πακέτο, αλλά δεν το καταγράφει



Εικόνα 9.6 Συσκευή ενοποιημένης διαχείρισης απειλών

Πίνακας 9.3

Σύνοψη προστατευτικών μέτρων από επιθέσεις για τη συσκευή ασφαλείας Sidewinder G2 — Παραδείγματα επιπέδου μεταφοράς

Επιθέσεις και απειλές μέσω Διαδικτύου	Προστατευτικά μέτρα		
TCP			
<ul style="list-style-type: none"> • Μη έγκυροι αριθμοί θυρών • Μη έγκυροι αριθμοί ακολουθίας • Κατακλυσμοί SYN • Επιθέσεις «χριστουγεννιάτικου δένδρου» • Μη έγκυρες τιμές CRC • Μηδενικό μήκος • Τυχαία δεδομένα ως κεφαλίδα TCP 	<ul style="list-style-type: none"> • Απόπειρες «πειρατείας» TCP • Απόπειρες παραπλάνησης TCP • Επιθέσεις μικρής PMTU • Επίθεση SYN • Επιθέσεις από «παιδιά των σεναρίων» • «Κατασκευή» πακέτων: ορισμός διαφορετικών επιλογών TCP 	<ul style="list-style-type: none"> • Επιβολή ορθών σημαιών TCP • Επιβολή μήκους κεφαλίδας TCP • Διασφάλιση ορθής τριπλής χειραψίας • Κλείσιμο συνόδου TCP με ορθό τρόπο • Δύο σύνοδοι, μία στο εσωτερικό και μία στο εξωτερικό • Επιβολή ορθής χρήσης σημαιών TCP • Διαχείριση λήξης χρόνων αναμονής συνόδου TCP • Αποκλεισμός επίθεσης SYN 	<ul style="list-style-type: none"> • Ανασυναρμολόγηση πακέτων για διασφάλιση ορθότητας • Ορθός χειρισμός λήξης χρόνων αναμονής του TCP και επαναμετάδοση χρονομέτρων • Προστασία όλων των μεσολαβητών TCP • Έλεγχος κυκλοφορίας μέσω λιστών πρόσβασης • Απόρριψη πακέτων TCP σε θύρες που δεν είναι ανοικτές • Αποκλεισμός «κατασκευής πακέτων» από μεσολαβητές
UDP			
<ul style="list-style-type: none"> • Μη έγκυρα πακέτα UDP • Τυχαία δεδομένα UDP για την παράκαμψη κανόνων 	<ul style="list-style-type: none"> • Πρόβλεψη συνδέσεων • Σάρωση θυρών UDP 	<ul style="list-style-type: none"> • Επαλήθευση ορθότητας πακέτου UDP • Απόρριψη πακέτων UDP σε θύρες που δεν είναι ανοικτές 	

(Ο πίνακας βρίσκεται στη σελ. 363 του βιβλίου.)

Πίνακας 9.4

Σύνοψη προστατευτικών μέτρων από επιθέσεις για τη συσκευή ασφαλείας Sidewinder G2 – Παραδείγματα επιπέδου εφαρμογών (σελ. 1 από 2)

(Ο πίνακας βρίσκεται στις σελ. 363-365 του βιβλίου.)

Επιθέσεις και απειλές μέσω Λιαδικτύου	Προστατευτικά μέτρα
DNS	
Εσφαλμένες απαντήσεις NXDOMAIN από ερωτήματα AAAA θα μπορούσαν να προκαλέσουν συνθήκες άρνησης εξυπηρέτησης.	<ul style="list-style-type: none">Απαγόρευση αρνητικής χρήσης κρυφής μνήμηςΑποτροπή «δηλητηρίασης» της κρυφής μνήμης DNS
Οι προγενέστερες της 9.2.1 εκδόσεις του πακέτου BIND από τον οργανισμό ISC επιτρέπουν σε αποκρισμένους επιτιθέμενους να προκαλέσουν άρνηση εξυπηρέτησης (τερματισμό) μέσω ενός εσφαλμένα σχηματισμένου πακέτου DNS που ενεργοποιεί μια συνήθη σφάλματος το οποίο δεν αντιμετωπίζεται σωστά ήταν η παράμετρος rdataset που μεταβιβάζεται στη συνάρτηση dns_message_findtype() του αρχείου message.c δεν έχει την τιμή NULL.	<ul style="list-style-type: none">Αποτροπή της κακόβουλης χρήσης εσφαλμένα σχηματισμένων μηνυμάτων DNS με σκοπό να επιτρέπουν λειτουργίες του τείχους προστασίαςΑποτροπή επιθέσεων που βασίζονται σε ερωτήματα DNSΑποτροπή επιθέσεων που βασίζονται σε απαντήσεις DNS
Επιθέσεις και απειλές μέσω Λιαδικτύου	Προστατευτικά μέτρα
Παρεμπόδιση πληροφοριών DNS και άλλες καταχρήσεις του DNS	<ul style="list-style-type: none">Αποτροπή μεταφορών ζώνης και ερωτημάτωνΠραγματική προστασία διαχωρισμένου DNS (split DNS) με την τεχνολογία Επιβολής Τόπου (Type Enforcement) ώστε να επιτρέπονται οι δημόσιες και ιδιωτικές ζώνες DNSΔυνατότητα απενεργοποίησης αναδρομής
FTP	
<ul style="list-style-type: none">Επίθεση ανατρήσης FTPΕπίθεση PASSΕπιθέσεις εισαγωγής θυρών FTPΕπίθεση τημπατοποίησης TCP (TCP segmentation)	<ul style="list-style-type: none">Δυνατότητα φιλτραρίσματος εντολών FTP για την αποτροπή τέτοιων επιθέσεωνΠραγματικός διαχωρισμός δικτύων για αποτροπή επιθέσεων τημπατοποίησης
SQL	
Επιθέσεις μεσάζοντα SQL Net	<ul style="list-style-type: none">Προστασία έξυπνου μεσολαβητή με την τεχνολογία Επιβολής ΤόπουΑπόκρυψη εσωτερικής βάσης δεδομένων μέσω μη διαραύνων συνδέσεων
Πρωτόκολλο Συνεχός Ροής Πραγματικού Χρόνου (Real-Time Streaming Protocol, RTSP)	
<ul style="list-style-type: none">Υπερχείλιση περιοχής προσωρινής αποθήκευσηςΆρνηση εξυπηρέτησης	<ul style="list-style-type: none">Προστασία έξυπνου μεσολαβητή με την τεχνολογία Επιβολής ΤόπουΕπικύρωση πρωτοκόλλωνΑρνηση διέλευσης κυκλοφορίας πολυεκπομπήςΈλεγχος μεθόδων διαώφορωσης και καταστροφήςΕπαλήθευση πρωτοκόλλων PNG και RTSP, απόρριψη όλων των υπολογίστωνΠαρακολούθηση βοηθητικών θυρών
SNMP	
<ul style="list-style-type: none">Επιθέσεις κατακλυσμού SNMPΕπίθεση προεπιλεγμένης κοινότηταςΕπίθεση «ωμής βίας»Επίθεση SNMP put	<ul style="list-style-type: none">Φιλτράρισμα κυκλοφορίας έκδοσης SNMP 1, 2cΦιλτράρισμα μηνυμάτων Read (ανάγνωση), Write (εγγραφή) και Notify (ειδοποίηση)Φιλτράρισμα OIDSΦιλτράρισμα PDU (Protocol Data Unit, Μονάδα Δεδομένων Πρωτοκόλλου)
SSH	
<ul style="list-style-type: none">Υπερχείλιση περιοχών προσωρινής αποθήκευσης με πρόκληση-απάντησηΟ δαίμονας SSHD επιτρέπει σε χρήστες να παρακάμπτουν «έπιτρεπμενές πιστοποιήσεις ταυτότητας» (Allowed Authentications)OpenSSH buffer_append_space: Υπερχείλιση περιοχής προσωρινής αποθήκευσηςOpenSSH/PAM: Υπερχείλιση περιοχής προσωρινής αποθήκευσης με πρόκληση-απάντησηOpenSSH: Ο κοδικός καναλού εμφανίζει απόκλιση κατά ένα	<p>Η ενσωματωμένη τεχνολογία Επιβολής Τόπων των εκδόσεων 6.x του Sidewinder G2 περιορίζει αυστηρά τις δυνατότητες των τροποποιημένων εκδόσεων της εταιρείας Secure Computing για τον κώδικα του δαίμονα OpenSSH.</p>

Πίνακας 9.4

Σύνοψη προστατευτικών μέτρων από επιθέσεις για τη συσκευή ασφαλείας Sidewinder G2 – Παραδείγματα επιπέδου εφαρμογών (σελ. 2 από 2)

Επιθέσεις και απειλές μέσω Διαδικτύου	Προστατευτικά μέτρα
<ul style="list-style-type: none">Sendmail: Υπερχείλιση περιοχών προσωρινής αποθήκευσηςSendmail: Επιθέσεις άρνησης εξυπηρέτησηςSendmail: Απομακρυσμένη υπερχείλιση περιοχής προσωρινής αποθήκευσηςSendmail: Υπερχείλιση περιοχής προσωρινής αποθήκευσης της ανάλυσης διευθύνσεωνΑνοιμαλίες πρωτοκόλλου SMTP	<ul style="list-style-type: none">Προστασία της διαχωρισμένης αρχιτεκτονικής του sendmail με την τεχνολογία Επιβόλης τύπωνΠροσαρμογή του sendmail για ελέγχουςΑποτροπή της υπερχείλισης περιοχών προσωρινής αποθήκευσης μέσω της τεχνολογίας Επιβόλης ΤύπωνΈλεγχος από το sendmail για ανοιμαλίες του πρωτοκόλλου SMTP
<ul style="list-style-type: none">SMTP: Επιθέσεις σκονιληκιώνSMTP: Κατακλυσμός ταχυδρομείουΕπιθέσεις αναμετάδοσης (replay)Ιοι. Λοιφείοι ίπποι, σκονιλήκιαΠαραπλάνηση διευθυνσιοδότησης ηλεκτρονικού ταχυδρομείουΕπιθέσεις MIMEΗλεκτρονικό ταχυδρομείο: Μηνύματα ηλεκτρονικού ψαρέματος	<ul style="list-style-type: none">Επικίνδυνη πρωτοκόλλωνΦύλτρο προστασίας από ενοχλητικά μαζικά μηνύματαΦύλτρα ταχυδρομείου – μέγεθος, λέξη-κλειδίΠροστασία από ιούς με υπογραφέςΠροστασία από αναμετάδοσηΦύλτρο MIME/προστασίας από ιούςΠροστασία από ιούς στο τείχος προστασίαςΠροστασία από ηλεκτρονικό ψάρεμα μέσω σάρωσης για ιούς

Σύνοψη

- Η ανάγκη για τείχη προστασίας
- Χαρακτηριστικά τειχών προστασίας και πολιτική πρόσβασης
- Τύποι τειχών προστασίας
 - Τείχη προστασίας με φίλτραρισμα πακέτων
 - Τείχη προστασίας με καταστασιακή επιθεώρηση
 - Πύλη επιπέδου εφαρμογών
 - Πύλη επιπέδου κυκλωμάτων
- Έδρα τειχών προστασίας
 - Οχυρωματικός υπολογιστής υπηρεσίας
 - Τείχη προστασίας βασισμένα σε υπολογιστές υπηρεσίας
 - Προσωπικά τείχη προστασίας
- Θέση και διευθετήσεις τειχών προστασίας
 - Δίκτυα DMZ
 - Εικονικά ιδιωτικά δίκτυα
 - Κατανεμημένα τείχη προστασίας
 - Σύνοψη θέσεων και τοπολογιών των τειχών προστασίας
- Συστήματα αποτροπής εισβολών
 - IPS βασισμένα σε υπολογιστές υπηρεσίας
 - IPS βασισμένα σε δίκτυα
 - Κατανεμημένα ή υβριδικά IPS
 - Εμβόλιμο Snort
- Παράδειγμα: Προϊόντα ενοποιημένης διαχείρισης απειλών

