Ασφάλεια Συστημάτων

Τζέριες Μπεσαράτ, PhD

1 Απριλίου 2022, Άρτα

Στο προηγούμενο μάθημα αναπτύξαμε

- Βασικές Έννοιες και Ζητήματα Ασφαλείας
- Βήματα για την ασφάλεια
- Ζητήματα ασφάλειας στο Διαδίκτυο
- Δίκτυα και Διαδίκτυο
- Κατηγορίες Δικτύων
- Διαστρωμάτωση
- Τέσσερα επίπεδα του Μοντέλου του Διαδικτύου
- Συστήματα Διάχυτου Υπολογισμού

Στόχος του διαχειριστή ασφαλείας

Στόχος του διαχειριστή ασφάλειας ενός δικτύου είναι:

- να αναπτύξει την κατάλληλη αμυντική στρατηγική, έτσι ώστε το δίκτυό του να είναι σε θέση να ανταπεξέρχεται σε τέτοιες επιθέσεις, καθώς και
- να καταγράφονται όλες οι λεπτομέρειες της διεξαγωγής τους.

Σε αυτό το μάθημα

- Προφίλ επιτιθεμένων
  - Hackers
  - Script Kiddies
  - Κυβερνο-κατάσκοποι
  - Κυβερνο-εγκληματίες
  - Insiders
- Μεθοδολογία επίθεσης
- Αμυντικά μοντέλα
  - Lollipop model
  - Onion model
- Ασφάλεια περιμέτρου
  - Τείχος προστασίας
  - Είδη Firewall
  - Bastion host

Προφίλ επιτιθέμενων - Hackers

Οι Hackers διαθέτουν εξειδικευμένες γνώσεις και δεξιότητες στις τεχνολογίες ΤΠΕ και, ανάλογα με τα κίνητρά τους, μπορούν να κατηγοριοποιηθούν σε:

- Black-Hat hackers: Στόχος τους είναι το προσωπικό, συνήθως οικονομικό, όφελος. Αναφέρονται συχνά και με τον όρο crackers.
- White-Hat hackers: Στόχος τους είναι ο εντοπισμός ευπαθειών, με σκοπό την αποκάλυψη και την μείωση ή απαλοιφή τους. Ως εκ τούτου, φροντίζουν να μην προκαλέσουν ζημία σε συστήματα ή δεδομένα, αλλά να κοινοποιήσουν το πρόβλημα στις αρμόδιες αρχές και οργανισμούς για να αντιμετωπιστεί.
- Grey-Hat hackers: Στόχος τους είναι, επίσης, ο εντοπισμός ευπαθειών. Η διαφορά με τους White-Hat hackers έγκειται στο ότι δεν τις αποκαλύπτουν στις αρμόδιες αρχές και οργανισμούς (π.χ. στις κατασκευάστριες εταιρείες), αλλά είτε παίρνουν την κατάσταση στα χέρια τους και αντεπιτίθενται σε τυχόν επιθέσεις που προσπαθούν να εκμεταλλευτούν τις ευπάθειες αυτές, είτε τις κοινοποιούν σε επιλεγμένο κοινό με κίνητρα που δεν περιορίζονται πάντα μέσα στα όρια της νομιμότητας.

Προφίλ επιτιθέμενων - Script Kiddies

Συνήθως, δεν διαθέτουν εξειδικευμένες γνώσεις, όπως οι hackers, αλλά χρησιμοποιούν έτοιμα εργαλεία (hacking tools), δηλαδή εργαλεία που έχουν κατασκευαστεί από άλλους, για να προκαλέσουν τη μέγιστη δυνατή ζημιά με στόχο τη δυσφήμιση ή απλά για να διασκεδάσουν.

Είναι ιδιαίτερα επικίνδυνοι, καθώς δεν έχουν επίγνωση της κρισιμότητας της κατάστασης και συνήθως, όντας μικροί σε ηλικία και χωρίς να υπολογίζουν τις σχετικές ευθύνες, δεν υπολογίζουν τις συνέπειες για τους ίδιους.

Προφίλ επιτιθέμενων - Κυβερνο-κατάσκοποι

Σε αντίθεση με τους hackers, στόχος των κυβερνο-κατασκόπων (cyber spies) δεν είναι ο εντοπισμός ευπαθειών σε οποιοδήποτε σύστημα. Οι κατάσκοποι μισθώνονται από τρίτους, με σκοπό να διεισδύσουν σε ένα δίκτυο-στόχο, ώστε να υποκλέψουν συγκεκριμένες πληροφορίες, χωρίς να γίνουν αντιληπτοί από τους διαχειριστές του.

Προφίλ επιτιθέμενων - Κυβερνο-εγκληματίες

Στόχος των κυβερνο-εγκληματιών (cybercriminals) είναι το προσωπικό τους οικονομικό όφελος, ή η οικονομική καταστροφή του ιδιοκτήτη του δικτύου-στόχου. Ενδεικτικά παραδείγματα επιθέσεων από κυβερνοεγκληματίες, είναι το spamming, το phishing και διάφορες απάτες με στόχο πάντα το οικονομικό κέρδος.

Μια υποκατηγορία των κυβερνο-εγκληματιών είναι οι κυβερνο-τρομοκράτες (cyberterrorists), οι οποίοι έχουν ως στόχο την τρομοκράτηση με επιθέσεις, όπως αυτή της κατανεμημένης άρνησης εξυπηρέτησης (DDoS) και της περαιτέρω χρήσης των στόχων για προπαγανδιστικούς ή άλλους παράνομους σκοπούς.

Προφίλ επιτιθέμενων - Insiders

Πολλές επιθέσεις δεν ξεκινούν από επιτιθέμενους εκτός του δικτύου, αλλά από νόμιμους χρήστες που δρουν μέσα από το ίδιο το δίκτυο. Οι εσωτερικοί αυτοί χρήστες είτε ακούσια ή εκούσια αποκαλύπτουν πληροφορίες ή εισάγουν κακόβουλο λογισμικό.

Η μεγάλη ανάπτυξη των ασύρματων δικτύων και η άναρχη υλοποίησή τους, έχει επιτρέψει την εκδήλωση επιθέσεων μέσα από τα δίκτυα ακόμη και από μη νόμιμους χρήστες τους, όπως για παράδειγμα σε περιπτώσεις απρόσκλητων συνδέσεων.

Μεθοδολογία επίθεσης

Οι διαφόρων ειδών επιθέσεις ακολουθούν, συνήθως, μια μεθοδολογία που απαρτίζεται από μια ακολουθία βημάτων, τα οποία σε γενικές γραμμές είναι:

- Αναζήτηση πληροφοριών για το στόχο
- Απόπειρα απόκτησης πρόσβασης
- Τροποποίηση ρυθμίσεων
- Διαγραφή ιχνών
- Αναζήτηση πρόσθετων πληροφοριών μέσα από το δίκτυο
- Πρόκληση ζημιάς

Αναζήτηση πληροφοριών για το στόχο:

Ο επιτιθέμενος προσπαθεί να συλλέξει πληροφορίες για το στόχο, όπως εκδόσεις λειτουργικών συστημάτων, εκδόσεις λογισμικού, τοπολογία δικτύου, διαθέσιμα ασύρματα δίκτυα κ.α., προκειμένου να εντοπίσει πιθανές γνωστές ευπάθειες

Απόπειρα απόκτησης πρόσβασης

Αφού εντοπιστούν κάποιες ευπάθειες, ο επιτιθέμενος προσπαθεί να τις εκμεταλλευτεί, ώστε να αποκτήσει πρόσβαση στο δίκτυο, κατά προτίμηση με όσο το δυνατόν πιο αυξημένα δικαιώματα.

Τροποποίηση ρυθμίσεων

Έχοντας αποκτήσει πρόσβαση, ο επιτιθέμενος τροποποιεί όσες ρυθμίσεις μπορεί, έτσι ώστε η πρόσβασή του σε μελλοντικές απόπειρες να είναι πιο εύκολη, τόσο από πλευράς χρόνου και κόπου, όσο και από πλευράς του να διακινδυνεύσει να εντοπιστεί η εισβολή του από τους διαχειριστές του δικτύου.

Διαγραφή ιχνών

Κάθε φορά που ολοκληρώνει μια εισβολή, ο επιτιθέμενος φροντίζει ώστε να
σβήνει τα ίχνη του από το σύστημα.

Αναζήτηση πρόσθετων πληροφοριών μέσα από το δίκτυο

Ο επιτιθέμενος, έχοντας αποκτήσει πρόσβαση σε έναν κόμβο του δικτύου, προσπαθεί να εντοπίσει ακόμη περισσότερα συστήματα στο δίκτυο, στα οποία στη συνέχεια θα προσπαθήσει να παρεισφρήσει, χρησιμοποιώντας ως
προκεχωρημένη θέση την τρέχουσα κατάσταση της εισβολή του.

Πρόκληση ζημιάς

Στην περίπτωση που το αποφασίσει, είτε επειδή δεν κατάφερε να αποκτήσει
τα αυξημένα δικαιώματα που ήθελε, είτε για άλλους λόγους, μπορεί να καταφύγει στην τακτική της πρόκλησης ζημιάς, αποκαλύπτοντας, τροποποιώντας ή διαγράφοντας δεδομένα και ρυθμίσεις του δικτύου.

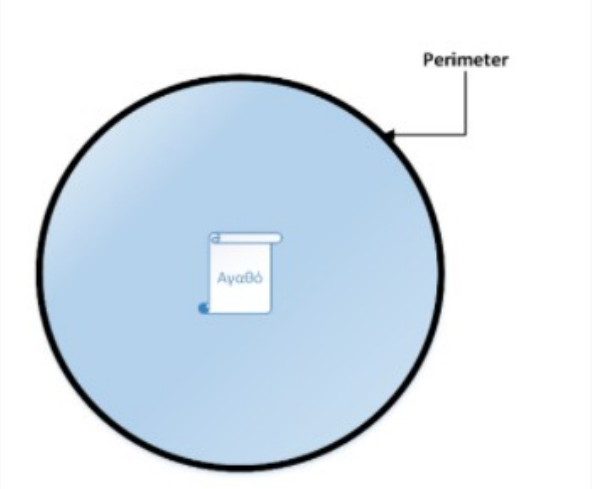
Αμυντικά μοντέλα

Δύο από τις πλέον δημοφιλείς προσεγγίσεις που ακολουθούνται για την αμυντική προστασία ενός δικτύου είναι γνωστές ως αμυντικά μοντέλα, ως εξής:

- Lollipop model: αφορά τη δημιουργία μιας ισχυρής αμυντικής περιμέτρου, θεωρώντας κάθε αντικείμενο εντός αυτής έμπιστο.
- Onion model: αφορά την υλοποίηση μιας πολυεπίπεδης προσέγγισης, γνωστής ως «defense in-depth».

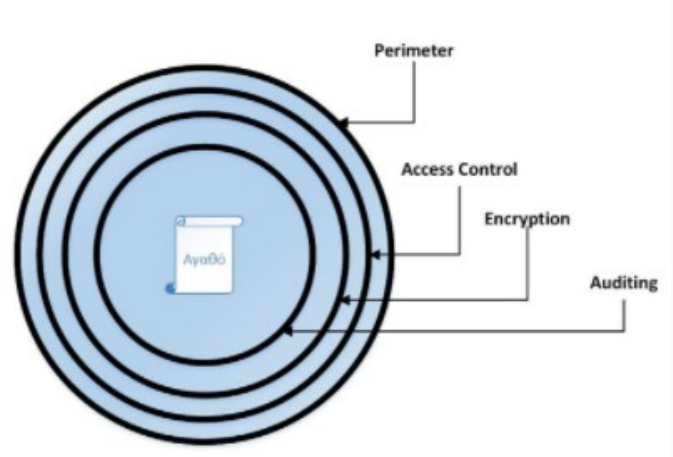
Lollipop model

Το μοντέλο Lollipop, περιγράφει τη δημιουργία μιας ισχυρής περιμέτρου, που συνήθως υλοποιείται με συσκευές που ελέγχουν την είσοδο προς και την έξοδο από το εσωτερικό δίκτυο. Στο μοντέλο αυτό, ισχύει η παραδοχή πως η περίμετρος είναι απαραβίαστη. Αν αυτή όμως παραβιαστεί, τα αντικείμενα που βρίσκονται εντός του δικτύου είναι τελείως απροστάτευτα.



Onion model

Το μοντέλο Onion, ή defense in-depth, δεν περιορίζεται στην ασφάλεια περιμέτρου, αλλά υλοποιεί ένα σύνολο αντιμέτρων σε πολλαπλά επίπεδα, όπως έλεγχο πρόσβασης, τεχνικές κρυπτογραφίας, έλεγχο ανίχνευσης εισβολών, προστασία δικτυακών εφαρμογών κ.ά. Η ασφάλεια περιμέτρου αφορά απλά το «εξωτερικό περίβλημα», ενώ αν ο επιτιθέμενος το παραβιάσει θα πρέπει να αντιμετωπίσει όλα τα αντίμετρα που λειτουργούν στα υπόλοιπα επίπεδα προστασίας.



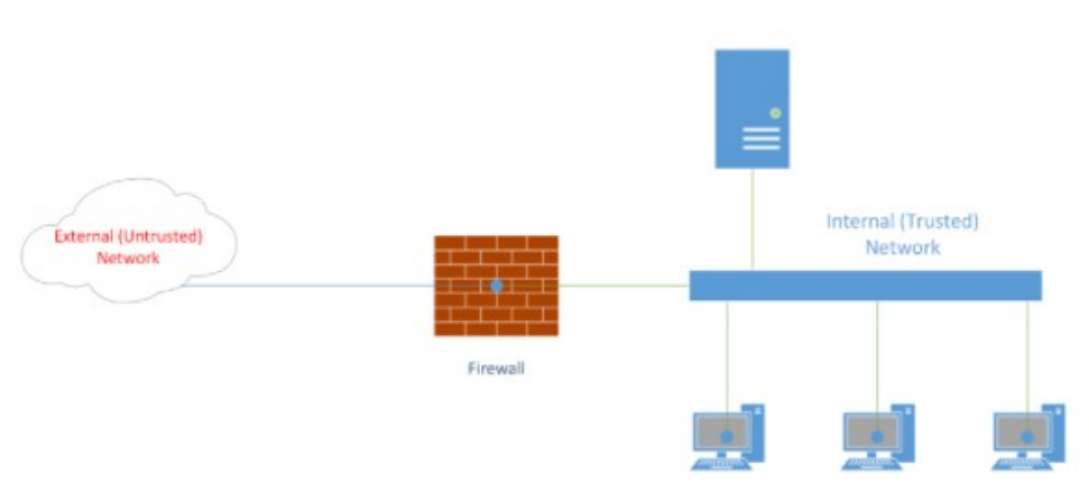
Ασφάλεια Περιμέτρου

Η λέξη «περίμετρος, ίσως να θυμίζει ένα φράκτη, ένα τείχος ή μια ένοπλη στρατιωτική περιπολία. Όταν αναφερόμαστε σε ένα δίκτυο, ως περίμετρο μπορούμε, αντίστοιχα, να θεωρήσουμε κάθε συσκευή, πραγματική ή εικονική, που διαχωρίζει το δίκτυο αναφοράς από όλα τα υπόλοιπα δίκτυα που το περιβάλλουν και, φυσικά, το ίδιο το Διαδίκτυο.

Ως δίκτυο αναφοράς, σε σχέση με την περίμετρο, νοείται το εσωτερικό δίκτυο του οποίου τους πόρους επιθυμούμε να προστατεύσουμε. Για την επίτευξη της προστασίας αυτής χρησιμοποιούνται, σε συνδυασμό ή ξεχωριστά, διατάξεις τείχους προστασίας (firewall) και συστημάτων ανίχνευσης εισβολών (IDS).

Τείχος προστασίας

Το τείχος προστασίας (firewall) διαχωρίζει δύο δίκτυα με διαφορετικό βαθμό εμπιστοσύνης, ελέγχοντας την κίνηση δεδομένων μεταξύ τους (από και προς το κάθε δίκτυο).



Τείχος προστασίας

Μπορούμε, αρχικά, να διαχωρίσουμε τα τείχη προστασίας σε δύο βασικές κατηγορίες:

- Προσωπικά, τα οποία στοχεύουν στην προστασία ενός κόμβου (host) από εξωτερικές απειλές και συνήθως υλοποιούνται με μια εφαρμογή λογισμικού.
- Δικτυακά, τα οποία χρησιμοποιούνται για την προστασία ολόκληρου δικτύου από εξωτερικές απειλές και, συνήθως, υλοποιούνται από ένα ανεξάρτητο υπολογιστικό σύστημα ή ενσωματώνονται σε έναν περιμετρικό δρομολογητή.

Τείχος προστασίας

Ο σχεδιασμός μιας διάταξης firewall πρέπει να διέπεται από βασικές αρχές, όπως οι ακόλουθες:

- Όλη η κίνηση μεταξύ των δικτύων πρέπει να διέρχεται μέσα από το firewall.
- Μόνον η κίνηση που καθορίζεται από την πολιτική που εφαρμόζει το firewall, επιτρέπεται να περάσει από αυτό.
- Το firewall πρέπει να είναι απαραβίαστο.

Είδη firewall

Τα τείχη προστασίας (firewalls) ταξινομούνται στις ακόλουθες βασικές κατηγορίες:

- Φιλτράρισμα πακέτων (Packet Filters).
- Πύλες κυκλώματος (Circuit-level Gateways).
- Πύλες εφαρμογών (Application-level Gateways).

Packet Filters

Ένα packet filtering firewall είναι η πιο κοινή διάταξη firewall. Εξετάζει κάθε πακέτο που εισέρχεται (ingress filtering) ή εξέρχεται (egress filtering) από αυτό. Η εξέταση περιορίζεται στις κεφαλίδες του επιπέδου δικτύου (IP headers) και του επιπέδου μεταφοράς (TCP/UDP headers) για να εξαχθούν:

- το πρωτόκολλο επικοινωνίας (protocol field),
- η διεύθυνση της προέλευσης (source address),
- η θύρα προέλευσης (source port),
- η διεύθυνση προορισμού (destination address),
- η θύρα προορισμού (destination port).

Packet Filters

Οι παραπάνω πληροφορίες εξετάζονται στη βάση ενός συνόλου κανόνων, έτσι ώστε να καθοριστεί αν θα επιτραπεί ή θα απαγορευτεί η διέλευση του πακέτου. Συγκεκριμένα, οι κανόνες υλοποιούν μια λίστα ελέγχου πρόσβασης (access control list – ACL):

#	Src Addr	Src Port	Dst Addr	Dst Port	Proto	Action	Comment
1	192.168.0.0/16	*	192.168.1.0/24	*	*	permit	Permit outbound traffic
2	172.16.0.0/12	*	192.168.1.0/24	*	*	permit	Permit outbound traffic
3	10.0.0.0/8	*	192.168.1.0/24	*	*	permit	Permit outbound traffic
4	any	*	192.168.1.21	80	TCP	permit	Access to web server
5	any	*	192.168.1.31	25	TCP	permit	Access to mail server
6	any	500	192.168.1.2	500	UDP	permit	Access to isakmp
7	any	4500	192.168.1.2	4500	UDP	permit	Access to isakmp-nat
8	any	*	192.168.1.0/24	*	*	deny	Deny all

Stateless packet filtering.

Η παραπάνω προσέγγιση, όπου πρέπει ρητά να καθοριστούν κανόνες για κάθε είδους εξερχόμενης και εισερχόμενης κίνησης, αποτελεί την υλοποίηση του stateless packet filtering. Όμως, παρουσιάζει τα ακόλουθα προβλήματα:

- Κάθε πακέτο πρέπει να ελέγχεται μέχρι να βρεθεί κανόνας που να ικανοποιείται από το πακέτο αυτό και να ληφθεί η απόφαση για την εφαρμογή της ενέργειας (action) που αναφέρεται στον κανόνα. Αυτός ο τρόπος λειτουργίας σε δίκτυα με συχνή κίνηση και μεγάλο αριθμό πακέτων, μπορεί να προκαλέσει αισθητές καθυστερήσεις στην εξυπηρέτηση της κίνησης αυτής.
- Ο διαχειριστής θα πρέπει να ορίζει κανόνες και για την εισερχόμενη αλλά και για την εξερχόμενη κίνηση, αυξάνοντας έτσι το διαχειριστικό φόρτο.
- Το stateless packet filter είναι επιρρεπές σε επιθέσεις τύπου IP Spoofing και TCP Fragmentation, που υλοποιείται κατακερματίζοντας τα πακέτα σε μικρά τμήματα (fragments) έτσι ώστε το πεδίο κεφαλίδας FLAGS του TCP να μη βρίσκεται στο πρώτο τμήμα αλλά σε ένα από τα υπόλοιπα τμήματα που διέρχονται χωρίς να ελέγχονται από το firewall.

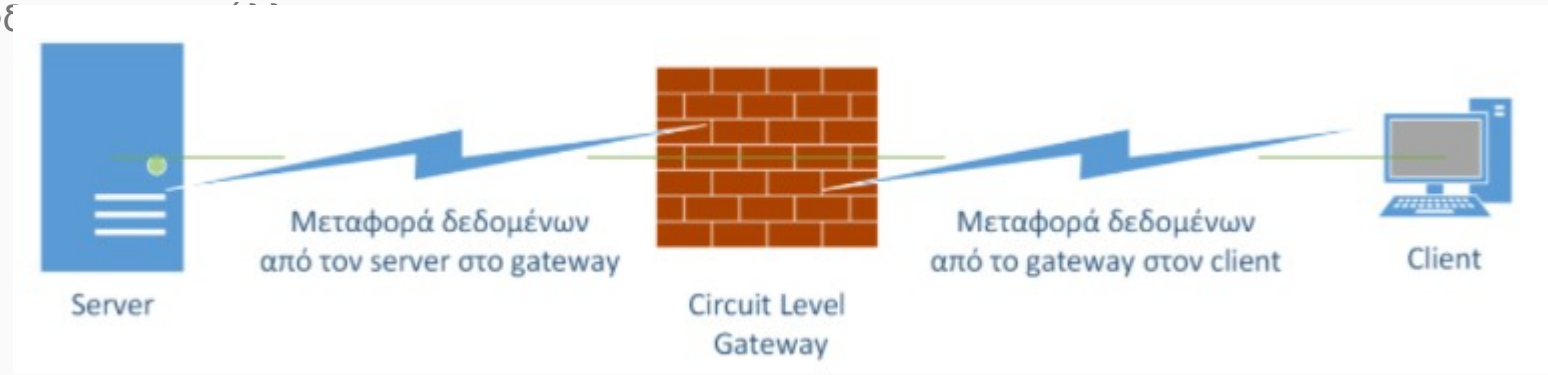
Packet Filters

Όταν ένας κόμβος από το εσωτερικό δίκτυο εκκινεί μια σύνδεση σε έναν άλλο κόμβο εκτός του δικτύου, το firewall καταχωρεί τη σύνδεση αυτή σε ένα πίνακα καταστάσεων (state table). Έτσι, για κάθε νέο εισερχόμενο ή εξερχόμενο από το δίκτυο πακέτο που φτάνει στο firewall:

- Αν το πακέτο αυτό ανήκει σε μια εδραιωμένη (established) σύνδεση επικοινωνίας, η διέλευσή του επιτρέπεται.
- Αν το πακέτο εκκινεί μια νέα σύνδεση (πακέτο τύπου SYN), δημιουργείται νέα εγγραφή στον πίνακα καταστάσεων. Τηρούνται, ακόμη, λίστες πρόσβασης ώστε να καθοριστεί η επιτρεπόμενη κίνηση.
- Αν το πακέτο δεν ανήκει σε μια εδραιωμένη σύνδεση και δεν είναι ένα SYN πακέτο, τότε απορρίπτεται.

Circuit Level Gateways

Οι πύλες κυκλώματος (circuit gateways) έχουν ως αρχή λειτουργίας την απαγόρευση δημιουργίας απευθείας συνδέσεων μεταξύ ενός κόμβου του προστατευόμενου δικτύου και ενός κόμβου του εξωτερικού δικτύου. Σε αντίθεση δηλαδή με τα packet filters, δεν γίνεται απλά έλεγχος και εδραίωση σύνδεσης μεταξύ των επικοινωνούντων μερών, αλλά δημιουργούνται δύο διαφορετικές συνδέσεις μεταξύ των δύο κόμβων και της πύλης (gateway). Η τελευταία, στη συνέχεια, προωθεί τα segments που λαμβάνει από της μια σύνδ



Circuit Level Gateways

Όταν ένας πελάτης επιθυμεί να εδραιώσει μια σύνδεση με ένα διακομιστή, η διαδικασία που ακολουθείται είναι:

1. Ο πελάτης ζητάει τη σύνδεση στο gateway.
2. Το gateway ελέγχει αν μια τέτοια σύνδεση επιτρέπεται.
3. Αν επιτρέπεται, τότε η σύνδεση εδραιώνεται.
4. Το gateway προωθεί τα πακέτα, χωρίς να τα αλλοιώνει, από το ένα host στο άλλο.
5. Όταν το gateway δεχτεί σχετικό αίτημα, τερματίζει τις συνδέσεις.

Circuit Level Gateways

Ένα πρωτόκολλο που χρησιμοποιείται από τις πύλες κυκλωμάτων είναι το SOCKS. Στην υλοποίησή του ορίζονται:

- Ο SOCKS Server, που εκτελείται στο gateway.
- Ο SOCKS Client, που ενσωματώνεται στις εφαρμογές πελάτη, που κάνουν χρήση τροποποιημένων, για την υποστήριξη του SOCKS, πρωτόκολλων.
- Το SOCKS Client Library, που χρησιμοποιείται από τους διακομιστές που προστατεύονται από το firewall.

Application Level Gateways

Οι πύλες εφαρμογών (application gateways), πιο γνωστές ως proxy servers, υλοποιούνται συνήθως με προϊόντα λογισμικού που εγκαθίστανται σε έναν ή περισσότερους διακομιστές. Οι proxy servers λειτουργούν ως ενδιάμεσοι κόμβοι.

Έτσι, όταν ένας πελάτης επιθυμεί, εκ μέρους ενός χρήστη, πρόσβαση σε μια συγκεκριμένη υπηρεσία, αποστέλλει την αίτηση αυτή στον proxy server, ο οποίος στη συνέχεια αυθεντικοποιεί το χρήστη και προωθεί τα πακέτα που λαμβάνει από τον πελάτη στον διακομιστή προορισμού και τις απαντήσεις του τελευταίου στον πρώτο.

Διαφορές proxy servers - circuit level gateways

- Οι proxy servers έχουν τη δυνατότητα να εξετάσουν το payload των πακέτων (deep inspection). Με τον τρόπο αυτό, μπορούν να εντοπιστούν ίχνη κακόβουλου λογισμικού ή να γίνει κάποια ενέργεια (π.χ. απαγόρευση πρόσβασης σε συγκεκριμένους ιστότοπους) με βάση τα περιεχόμενα του πακέτου.
- Οι proxy servers εξυπηρετούν συγκεκριμένες υπηρεσίες. Για παράδειγμα, ένας εξειδικευμένος proxy server για υπηρεσίες web δεν μπορεί να χρησιμοποιηθεί για άλλες υπηρεσίες. Ο mail server είναι, επίσης, μια κλασσική περίπτωση proxy server.

Οι τρεις διαφορετικοί τύποι firewall που εξετάστηκαν δεν είναι αμοιβαία αποκλειστικοί, αλλά μπορούν να συνδυαστούν σε ένα δίκτυο, όπως φαίνεται στην Εικόνα