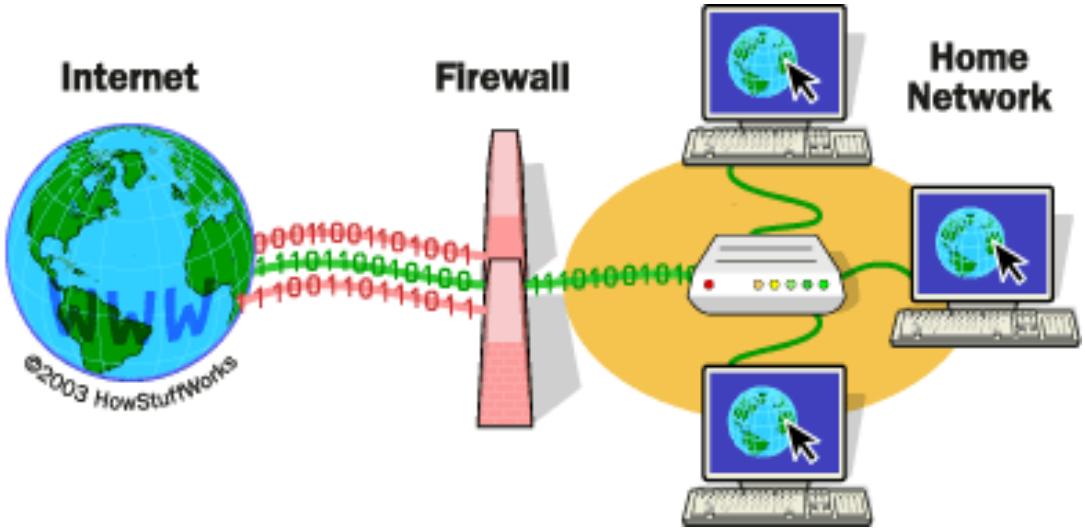
NETWORK FIREWALL

McAfee FIREWALL v 4.0



ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΚΑΡΑΧΡΗΣΤΟΥ ΜΑΡΓΑΡΙΤΑ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ

ΤΣΙΑΝΤΗΣ ΛΕΩΝΙΔΑΣ

ΠΕΡΙΕΧΟΜΕΝΑ

1. ΕΙΣΑΓΩΓΗ

Η τεχνολογία του firewall έχει περάσει από διάφορες φάσεις ανάπτυξης τα τελευταία χρόνια και τα προϊόντα των τειχών προστασίας των Windows έχουν αλλάξει με σκοπό να την φτάσουν και τα έχουν καταφέρει πολύ καλά μέχρι τώρα.

Σε αυτήν την εργασία θα αναφερθούμε γενικότερα για τα τείχη προστασίας, τι είναι, τι κάνουν, ποιοι τύποι υπάρχουν, τοπολογίες και πολλά άλλα.

Θα αναλύσουμε την λειτουργία ενός τοίχου προστασίας και συγκεκριμένα του MCA Firewall v 4.0 .

2.ΕΞΑΣΦΑΛΙΣΗ ΤΟΥ ΕΓΧΩΡΙΟΥ ΔΙΚΤΥΟΥ ΣΑΣ

Εισαγωγή

Οι περισσότεροι άνθρωποι που χρησιμοποιούν τους υπολογιστές αυτές τις μέρες έπρεπε να εξετάσουν ένα ζήτημα ασφάλειας με κάποιον τρόπο – ποτέ πρέπει να ανησυχούν και ποτέ όχι. Ο καθένας έχει μολυνθεί από ένα από τα πολλά σκουλήκια ή τους ιούς που επιπλέουν γύρω από το Διαδικτύο, ή κάποιος είχε χρησιμοποιήσει τον κωδικό πρόσβασής σας. Οι περισσότεροι χρήστες εγχώριων υπολογιστών είναι θύματα των επιθέσεων ότι δεν έχουν καμία ιδέα σχετικά με αυτό.

Παραδείγματος χάριν, ορισμένα προγράμματα αποκαλούμενα ‘ spyware έρχονται συσκευασμένα στα φαινομενικά φιλικά προγράμματα που κατεβάζετε, αυτό το spyware μπορεί να κάνει διάφορα πράγματα, αν και συχνότερα στέλνουν τις προσωπικές πληροφορίες σας (όπως το όνομα και τη διεύθυνση του ηλεκτρονικού ταχυδρομείου) και τις πληροφορίες για ποιες περιοχές επισκέπτεστε σε ορισμένες επιχειρήσεις.

Αυτοί στη συνέχεια θα πωλήσουν τις προσωπικές πληροφορίες σας στα spammers και οι έμποροι ηλεκτρονικού ταχυδρομείου που θα προχωρήσουν να φράξουν το inbox σας με τα παλιοπράματα σκεφτόμενοι ότι ίσως σας ενδιαφέρει. Για να καταλάβετε πώς λειτουργεί αυτή η εργασία, κατεβαστέ ένα πρόγραμμα – π.χ. ένα video – από το Διαδίκτυο και κάντε εγκατάσταση. Στο υπόβαθρο εγκαθιστά κάποιο spyware. Τώρα αρχίζετε να σερφάρετε στις περιοχές αυτοκινήτων, σύντομα μπορείτε να αναμείνετε το ηλεκτρονικό ταχυδρομείο σας inbox για να είστε πλήρες από spam που σας προσφέρει τις μεγάλες διαπραγματεύσεις στα χρησιμοποιημένα αυτοκίνητα κ.λπ.

Πολλοί άνθρωποι πιστεύουν στην αρχή ότι ο εγχώριος υπολογιστής τους δεν περιέχει τίποτα που να ενδιαφέρει αρκετά έναν επιτιθέμενο, δεν συνειδητοποιούν ότι ένας επιτιθέμενος δεν μπορεί να στοχεύσει στο σύστημά σας συγκεκριμένα, είναι πολύ κοινό για αυτούς να χρησιμοποιήσουν τα προγράμματα που θα ανιχνεύσουν τις απέραντες σειρές του Διαδικτύο που ψάχνει τα τρωτά συστήματα, εάν το δικό σας συμβαίνει να είναι ένα από αυτά , αυτό θα αναληφθεί αυτόματα και θα τοποθετηθεί στην εντολή επιτιθεμένων. Από εδώ μπορεί να κάνει ποικίλα πράγματα, όπως τη χρησιμοποίηση του υπολογιστή σας για να επιτεθεί σε άλλες περιοχές στο Διαδικτύο ή τη σύλληψη όλων των κωδικών πρόσβασής σας.

Τα σκουλήκια και οι ιοί ηλεκτρονικού ταχυδρομείου λειτουργούν με τον ίδιο τρόπο, μολύνουν μια μηχανή, και διαδίδουν έπειτα προσπαθώντας να σταλθεί μήνυμα με το ηλεκτρονικό ταχυδρομείο σε η καθεμία στο βιβλίο φιλοξενουμένων σας, ή τη μετατροπή της μηχανής σας σε σύστημα ανίχνευσης για να βρουν άλλους στόχους. Μπορούν ακόμη και να περιέχουν ένα κακόβουλο ωφέλιμο φορτίο που μπορούν να καταστρέψουν τα αρχεία σας, ή ακόμα και το χειρότερο ηλεκτρονικό ταχυδρομείο – τα ιδιωτικά έγγραφά σας στον καθένα που ξέρετε (αυτό συνέβη με ένα σκουλήκι μερικά έτη πριν).

Δεδομένου ότι τα πράγματα που χρησιμοποιούμε τον υπολογιστή τα τελευταία

χρόνια όπως να ψωνίσουμε on-line βιβλία ή η μουσική, οι ηλεκτρονικές τραπεζικές εργασίες κ.λπ., αυτές οι απειλές έχουν μια σοβαρότερη επίπτωση από τους περισσότερους ανθρώπους που τα χρησιμοποιούν. Δεν μπορείτε να έχετε τίποτα σημαντικό στον υπολογιστή σας, αλλά γιατί ένας επιτιθέμενος είναι σε θέση να κλέψει τις πληροφορίες πιστωτικών καρτών σας όταν αγοράζετε ένα βιβλίο από το Amazon.com, ή κλέβετε τον κωδικό πρόσβασης στο σε απευθείας σύνδεση τραπεζικό απολογισμό σας;

Ευτυχώς τα παρακάτω βήματα που πρέπει να κάνετε για να εξασφαλίσουν το PC σας είναι αρκετά απλά και μπορούν να ολοκληρωθούν από τους μη τεχνικούς χρήστες παρέχοντας τις σωστές οδηγίες. Εάν ακολουθείτε τις οδηγίες που δίνονται εδώ, θα είστε ασφαλείς από τις περισσότερες μορφές βασισμένων στο Διαδίκτυο απειλών.

Εδώ είναι μερικά μέτρα που μπορείτε να λάβετε:

- Ασφάλεια ηλεκτρονικού ταχυδρομείου
- Εγκαταστήστε ένα λογισμικό αντιιών
- Θέστε εκτός λειτουργίας τη διανομή αρχείων παραθύρων
- Ενημερώστε το λειτουργικό σύστημα
- Εγκαταστήστε μια προσωπική αντιπυρική ζώνη

ZoneAlarm – πολύ εύκολο να εγκατασταθεί και να χρησιμοποιηθεί, υπάρχει μια ελεύθερη έκδοση με μερικά λιγότερα χαρακτηριστικά γνωρίσματα από την επαγγελματική έκδοση. Σας δίνει πολύ καλές πληροφορίες για τις επιφυλακές που παράγουν. Εξέτασε τον πρωτοπόρο στην αγορά.

Το BlackICE – μια άλλη πολύ ιδιαίτερα εκτιμημένη προσωπική αντιπυρική ζώνη, αυτό δεν είναι τόσο φιλικό προς το χρήστη όσο το ZoneAlarm, αλλά επιτρέπει μερικές περαιτέρω επιλογές διαμόρφωσης

Η προσωπική αντιπυρική ζώνη – Sygate επίσης λιγότερο φιλική προς το χρήστη, αλλά αυτό επιτρέπει σε σας να κάνετε μερικές πολύ ισχυρές αλλαγές διαμόρφωσης και περιέχει ένα στοιχειώδες σύστημα ανίχνευσης παρείσφρησης για να σας προειδοποιήσει για τις κοινές επιθέσεις.

- Ανίχνευση για Spyware
- Επιλέξτε τους ισχυρούς κωδικούς πρόσβασης

3.ΕΙΣΑΓΩΓΗ ΣΤΟ ΤΕΙΧΟΣ ΠΡΟΣΤΑΣΙΑΣ

Εισαγωγή

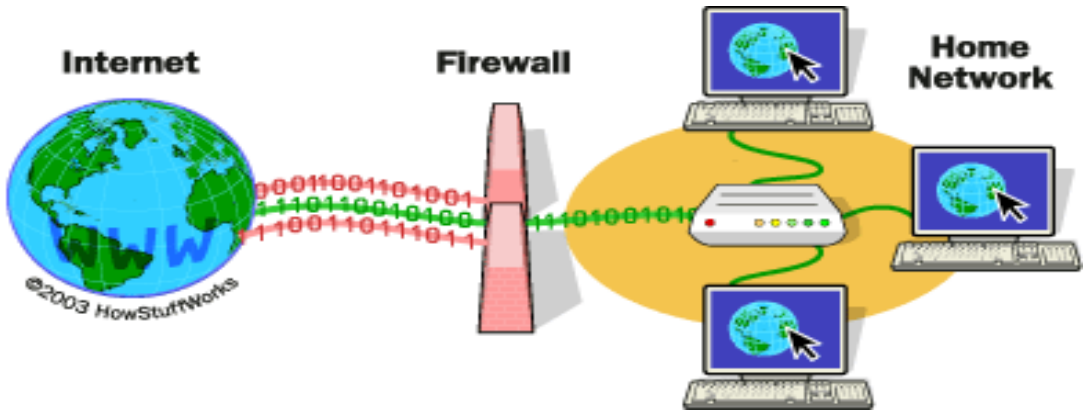
Ένα τείχος προστασίας (firewall) είναι απλά ένα σύστημα με σκοπό να αποτρέψει την αναρμόδια πρόσβαση σε ή από ένα ιδιωτικό δίκτυο. Τα τείχη προστασίας μπορούν να εφαρμοστούν και στο υλικό και στο λογισμικό, ή σε συνδυασμό και των δύο. Τα τείχη προστασίας χρησιμοποιούνται συχνά για να αποτρέψουν τους αναρμόδιους χρήστες του Διαδικτύο από την πρόσβαση στα ιδιωτικά δίκτυα που συνδέονται με το Διαδίκτυο. Όλα τα δεδομένα εισάγονται ή 'πετιόνται' στο πέρασμα ενδοδικτύου μέσω του τοίχου προστασίας ,το οποίο εξετάζει κάθε πακέτο και εμποδίζει εκείνα που δεν ικανοποιούν τα διευκρινισμένα κριτήρια ασφάλειας.

Γενικά, τα τείχη προστασίας διαμορφώνονται για να προστατεύσουν από τα μη αυθεντικά(πλαστά) διαλογικά logins από τον εξωτερικό κόσμο . Αυτό βοηθά στο να αποτρέψει «τους χάκερ» από το να συνδεθούν στα μηχανήματα του δικτύου σας. Τα πιο περίπλοκα τείχη προστασίας εμποδίζουν την κυκλοφορία από το εξωτερικό στο εσωτερικό, αλλά επιτρέπουν στους χρήστες στο εσωτερικό για να επικοινωνήσουν λίγο πιο ελεύθερα με το εξωτερικό.

Τα τείχη προστασίας είναι ζωτικής σημασίας, δεδομένου ότι μπορούν να παρέχουν ένα ενιαίο σημείο φραγμών όπου η ασφάλεια και ο λογιστικός έλεγχος μπορούν να επιβληθούν. Τα τείχη προστασίας παρέχουν μια σημαντική λειτουργία καταγραφής και ελέγχου, συχνά παρέχουν περιλήψεις στον διαχειριστή για ποιο τύπο/όγκο της κυκλοφορίας που έχει υποβληθεί σε επεξεργασία μέσω του. Αυτό είναι ένα σημαντικό σημείο: η παροχή αυτού του σημείου φραγμών μπορεί να εξυπηρετήσει τον ίδιο σκοπό (στο δίκτυό σας) όπως μια οπλισμένη φρουρά μπορεί (για τις φυσικές εγκαταστάσεις).

4.ΤΡΟΠΟΣ ΛΕΙΤΟΥΡΓΙΑΣ ΕΝΟΣ ΤΕΙΧΟΥΣ ΠΡΟΣΤΑΣΙΑΣ

Εάν χρησιμοποιείς το Διαδίκτυο εδώ και πολύ καιρό, ειδικά όταν δουλεύεις σε μια μεγάλη εταιρία και μπαίνεις στο Ντε κατά τη διάρκεια της δουλείας ,λογικά θα έχεις ακούσει τον όρο «τείχος προστασίας» να χρησιμοποιείται. Για παράδειγμα, συχνά ακούμε υπάλληλους σε εταιρίες να λενε ότι 'δεν μπορώ να μπω σε αυτήν την ιστοσελίδα επειδή το τείχος προστασίας δεν επιτρέπει την πρόσβαση.'
Αν έχεις γρήγορη σύνδεση στο Νετ από το σπίτι σου (είτε σύνδεση DSL είτε cable modem),θα έχεις ακούσει,επίσης, σχετικά με το τείχος προστασίας για το δίκτυο σπιτιού. Αυτό αποδεικνύει ότι ένα μικρό δίκτυο στο σπίτι έχει πολλά από τα ίδια θέματα προστασίας από ότι ένα μεγάλο συνεταιριστικό δίκτυο έχει. Μπορείς να χρησιμοποιήσεις ένα τείχος προστασίας για να προστατέψεις το δίκτυο του σπιτιού από επιθετικές ιστοσελίδες και πιθανούς χάκερς.



Βασικά, ένα τείχος προστασίας είναι ένα φραγμός για να κρατάει καταστρεπτικές δυνάμεις μακρυά από την ιδιοκτησία σου. Στην πραγματικότητα ,για αυτό το λόγο καλείται και τείχος προστασίας. η δουλεία του είναι ίδια με εκείνη του φυσικού τείχους προστασίας το οποίο κρατάει τη φωτιά από το να εξαπλωθεί από το ένα μέρος στο άλλο. Θα μάθουμε πολλά σχετικά με τα τείχη προστασίας ,πως λειτουργούν και από ποια είδη απειλών μπορούν να σε προστατέψουν.

5.ΤΙ ΚΑΝΕΙ ΕΝΑ ΤΕΙΧΟΣ ΠΡΟΣΤΑΣΙΑΣ

Ένα firewall είναι ένα απλό πρόγραμμα ή μια συσκευή υλικού που φιλτράρει την πληροφορία που εισέρχεται μέσα από την σύνδεση του διαδικτύου στο ιδιωτικό σας δίκτυο ή το σύστημα του υπολογιστή σας. Εάν ένα εισερχόμενο πακέτο πληροφορίας επισημανθεί από τα φίλτρα, δεν θα του επιτραπεί να 'περάσει'.

Εάν έχετε διαβάσει το άρθρο για το πώς λειτουργούν οι Web Servers ,τότε θα γνωρίζετε ότι ένα καλό bit σχετικά με το πώς τα δεδομένα μετακινούνται στο διαδίκτυο, και μπορείς εύκολα να δεις πως ένα firewall προστατεύει τον υπολογιστή σας μέσα σε μια μεγάλη εταιρία. Ας υποθέσουμε ότι δουλεύετε σε μια εταιρία με 500 υπαλλήλους. η εταιρία θα έχει εκατοντάδες υπολογιστές των οποίων οι κάρτες δικτύου θα συνδέονται μεταξύ τους. επί πρόσθετα, η εταιρία θα έχει μια ή περισσότερες συνδέσεις στο διαδικτυο μέσω γραμμών σαν T1 ή T3. Χωρίς την εγκατάσταση ενός firewall ,όλα αυτοί οι εκατοντάδες υπολογιστές θα είναι άμεσα προσβάσιμοι στον καθένα από το διαδικτυο. κάποιος που γνωρίζει τι κάνει μπορεί να προβεί σε αυτούς τους υπολογιστές ,να προσπαθήσει να κάνει συνδέσεις FTP ή TELNET με αυτούς και πολλά αλλά. Εάν ένας υπάλληλος κάνει ένας λάθος και αφήσει ένα κενό ασφάλειας ,οι χάκερς μπορούν να μπουν στο μηχάνημα και να εκμεταλλευτούν το κενό.

Με την εγκατάσταση ενός firewall ,τα πράγματα είναι πολύ διαφορετικά. μια εταιρία θα εγκαταστήσει ένα firewall σε κάθε σύνδεση στο διαδικτυο(για παράδειγμα, σε κάθε γραμμή T1 που έρχεται στην εταιρία.). το firewall μπορεί να θέσει σε εφαρμογή κανόνες ασφάλειας. Για παράδειγμα, ένας από τους κανόνες ασφάλειας μέσα στην εταιρία μπορεί να είναι :

Από τους 500 υπολογιστές μέσα στην εταιρία ,μόνο σε έναν από αυτούς του επιτρέπεται να λάβει δημόσια κυκλοφορία FTP. Επιτρέπει συνδέσεις FTP μόνο σε εκείνον τον υπολογιστή και τις αποτρέπει από όλους τους άλλους.

Μια εταιρία μπορεί να δημιουργήσει κανόνες όπως αυτούς για FTP servers, Web servers, Telnet servers και πολλούς άλλους. Επί προσθετά, η εταιρία μπορεί να ελέγχει πως οι υπάλληλοι συνδέονται στις ιστοσελίδες, ποτέ αρχεία επιτρέπονται να βγουν μέσα από την εταιρία στο διαδικτυο και πολλά άλλα. Ένα firewall δίνει σε μια εταιρία καταπληκτικό έλεγχο στο πως οι άνθρωποι χρησιμοποιούν το διαδικτυο.

Τα Firewalls χρησιμοποιούν μια ή περισσότερες από τρεις μεθόδους για να ελέγχουν την κυκλοφορία που ρέει μέσα και έξω από το διαδικτυο:

- Packet filtering-πακέτα (μικρά κομμάτια δεδομένων) αναλύονται ενάντια σε ένα σύνολο από φίλτρα. Τα πακέτα που περνούν μέσα από τα φίλτρα στέλνονται σε ένα σύστημα αιτήσεως και όλα τα αλλά 'πετιούνται'.
- Proxy server-πληροφορία από το διαδικτυο αποκαθιστάται από το firewall και έπειτα στέλνεται στο σύστημα αιτήσεως και αντιστρόφως.
- Stateful inspection-μια νεότερη μέθοδος που δεν εξετάζει τα στοιχεία του κάθε

πακέτου αλλά αντίθετα συγκρίνει το ασφαλές κλειδί των μερών του πακέτου σε μια βάση δεδομένων εμπιστευόμενης πληροφορίας. η πληροφορία ταξιδεύει μέσα από το firewall προς τα έξω ελέγχοντας για ορισμένα συγκεκριμένα χαρακτηριστικά., έπειτα η εισερχόμενη πληροφορία συγκρίνεται με αυτά τα χαρακτηριστικά. Εάν η σύγκριση αποδίδει ένα λογικό ταίριασμα, η πληροφορία επιτρέπεται, διαφορετικά ‘πετιέται’.

6.ΤΥΠΟΙ ΤΟΙΧΩΝ ΠΡΟΣΤΑΣΙΑΣ

Θεωρητικά, υπάρχουν δύο τύποι τειχών προστασίας:

1. Στρώμα δικτύων

2. Στρώμα εφαρμογής

Δεν είναι τόσο διαφορετικοί όσο πιστεύουμε, όπως περιγράφεται κατωτέρω.

Το ποιος είναι ποιος εξαρτάται από τι μηχανισμούς χρησιμοποιεί το τείχος προστασίας για να περάσει την κυκλοφορία από μια ζώνη ασφάλειας σε άλλη. Το πρότυπο διασύνδεσης ανοικτών συστημάτων οργάνωσης διεθνών προτύπων (ISO) (OSI) για τη δικτύωση καθορίζει επτά στρώματα, όπου κάθε στρώμα παρέχει τις υπηρεσίες ότι τα υψηλότερου επιπέδου στρώματα εξαρτώνται από. Το σημαντικό πράγμα που αναγνωρίζει είναι ότι το επίπεδο ο μηχανισμός αποστολής, η λιγότερη εξέταση που η αντιπυρική ζώνη μπορεί να εκτελέσει.

Τείχη προστασίας στρώματος δικτύων

Αυτός ο τύπος καθιστά γενικά τις αποφάσεις τους βασισμένες στη διεύθυνση προέλευσης, τη διεύθυνση προορισμού και τις θύρες στα μεμονωμένα πακέτα IP. Ένας απλός δρομολογητής είναι το παραδοσιακό τείχος προστασίας στρώματος δικτύων, δεδομένου ότι δεν είναι ικανό να λάβει ιδιαίτερα τις περίπλοκες αποφάσεις για αυτό που ένα πακέτο μιλά πραγματικά ή όπου προήλθε πραγματικά .Τα σύγχρονα τείχη προστασίας δικτύων έχουν γίνει όλο και περισσότερο περιπλοκότερα, και διατηρούν τώρα εσωτερικές πληροφορίες για την κατάσταση των συνδέσεων που περνούν μέσω τους οποιαδήποτε στιγμή.

Ένα πράγμα που είναι μια σημαντική διαφορά για πολλά τείχη προστασίας δικτύων είναι ότι καθοδηγούν την κυκλοφορία κατευθείαν μέσω αυτών, έτσι για να χρησιμοποιήσει το ένα ,εσείς είτε πρέπει να έχετε έναν εγκύρως ορισμένο φραγμό διευθύνσεων IP είτε να χρησιμοποιήσετε έναν ιδιωτικό φραγμό διευθύνσεων Διαδικτύου. Τα τείχη προστασίας στρώματος δικτύων τείνουν να είναι πολύ γρήγορα και τείνουν να είναι συνήθως διαφανείς στους χρήστες τους.

Τείχη προστασίας στρώματος εφαρμογής

Αυτοί είναι γενικά οικοδεσπότες που τρέχουν τους proxy servers, οι οποίοι δεν επιτρέπουν καμία άμεση κυκλοφορία μεταξύ των δικτύων, και εκτελούν επιμελημένες αναγραφές και εξέταση της κυκλοφορίας που περνά μέσω τους. Δεδομένου ότι οι εφαρμογές του proxy είναι απλά ένα λογισμικό που τρέχει στο τείχος προστασίας, είναι μια καλή θέση για να κάνεις πολλά logins και ελέγχους πρόσβασης. Τα τείχη προστασίας στρώματος εφαρμογής μπορούν να χρησιμοποιηθούν ως μεταφραστές διευθύνσεων δικτύων, δεδομένου ότι η κυκλοφορία πηγαίνει σε μια πλευρά και έξω άλλη, μετά από να έχε περάσει μέσω μιας εφαρμογής που καλύπτει αποτελεσματικά την προέλευση της σύνδεσης έναρξης.

Η κατοχή μιας εφαρμογής με τον τρόπο μπορεί σε μερικές περιπτώσεις να

προσκρούσει στην απόδοση και μπορεί να καταστήσει το τείχος προστασίας λιγότερο διαφανή. Τα πρόωρα τείχη προστασίας στρώματος εφαρμογής δεν είναι ιδιαίτερα διαφανή στους τελικούς χρήστες και μπορούν να απαιτήσουν κάποια κατάρτιση. Εντούτοις τα πιο σύγχρονα τείχη προστασίας στρώματος εφαρμογής είναι συχνά συνολικά διαφανή. Τα τείχη προστασίας στρώματος εφαρμογής τείνουν να παρέχουν τις πιο λεπτομερείς εκθέσεις λογιστικού ελέγχου και να τείνουν να επιβάλουν τα πιο συντηρητικά πρότυπα ασφάλειας από τα τείχη προστασίας στρώματος δικτύων.

Το μέλλον των τειχών προστασίας κάθεται κάπου και μεταξύ των τειχών προστασίας στρώματος δικτύων και των τειχών προστασίας στρώματος εφαρμογής. Είναι πιθανό ότι τα τείχη προστασίας στρώματος δικτύων θα γίνουν όλο και περισσότερο ενήμερα για τις πληροφορίες που περνούν από τους, και τα τείχη προστασίας στρώματος εφαρμογής θα γίνουν όλο και περισσότερο διαφανεί. Το τελικό αποτέλεσμα θα είναι καλό ενός γρήγορου συστήματος πακέτο-διαλογής που καταγράφει και ελέγχει τα στοιχεία καθώς περνούν μέσω.

7.ΤΟΠΟΛΟΓΙΕΣ ΤΕΙΧΩΝ ΠΡΟΣΤΑΣΙΑΣ

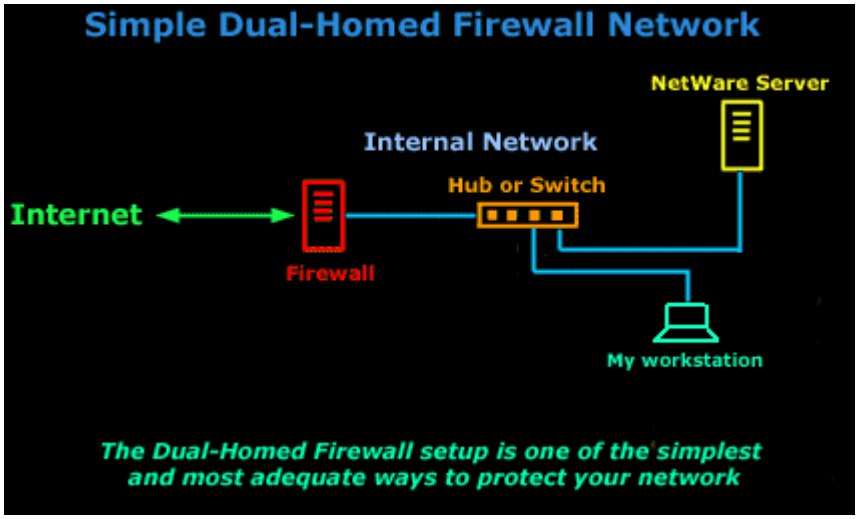
Εισαγωγή

Σε αυτό το τμήμα πρόκειται να μιλήσουμε για τους διαφορετικούς τρόπους που ένα τείχος προστασίας μπορεί να οργανωθεί. Ανάλογα με τις ανάγκες σας, μπορείτε να έχετε μια πολύ απλή οργάνωση τειχών προστασίας που θα παράσχει αρκετή προστασία για τον προσωπικό υπολογιστή ή το μικρό δίκτυό σας, ή μπορείτε να επιλέξετε μια πιο περίπλοκη οργάνωση που θα παράσχει περισσότερη προστασία και ασφάλεια.

Ρίχνει μια ματιά που αρχίζει από τις απλές λύσεις, και κινηθείτε έπειτα προς τις πιο περίπλοκες. Ακριβώς λάβετε υπόψη δεν μιλάμε για ένα τείχος προστασίας που είναι μόνο ένα κομμάτι του λογισμικού που τρέχει στον ίδιο υπολογιστή που χρησιμοποιείτε για να συνδέσετε με το Διαδίκτυο και να κάνετε την εργασία σας, αλλά μιλάμε για έναν φυσικό υπολογιστή που είναι ένα αφιερωμένο στο τείχος προστασίας.

Ένα απλό διπλό κατευθυνόμενο αυτομάτως τείχος προστασίας

Το διπλό κατευθυνόμενο αυτομάτως τείχος προστασίας είναι ένας από τον απλούστερο και ενδεχομένως πιο κοινό τρόπο να χρησιμοποιηθεί ένα τείχος προστασίας. Το Διαδίκτυο μπαίνει στον τείχος προστασίας άμεσα μέσω ενός διαποδιαμορφωτή διεπιλογών ή μέσω κάποιου άλλου τύπου σύνδεσης όπως έναν διαποδιαμορφωτή γραμμών ή καλωδίων ISDN. Δεν μπορείτε να έχετε ένα DMZ (δείτε τη σελίδα DMZ για περισσότερες πληροφορίες) σε αυτόν τον τύπο μιας διαμόρφωσης.



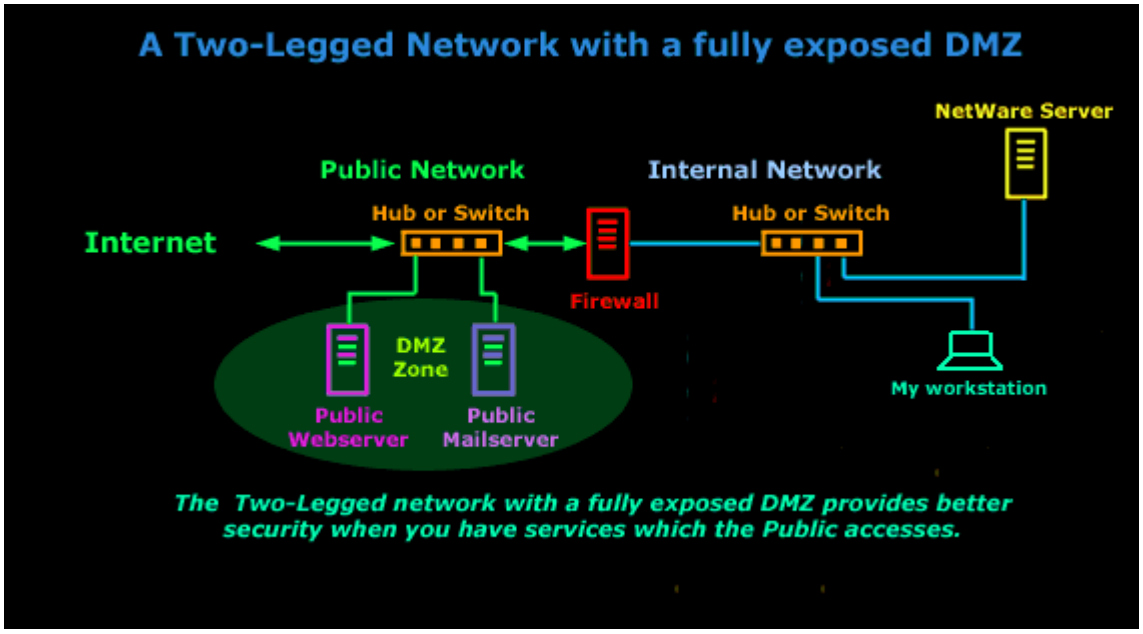
Το τείχος προστασίας φροντίζει τη διάβαση των πακέτων που περνούν τους

κανόνες φιλτραρίσματός του μεταξύ του εσωτερικού δικτύου και του Διαδικτύου, και αντίστροφα. Μπορεί να χρησιμοποιήσει τη IP που μεταμφιέζει και αυτή είναι όλη που. Αυτό είναι γνωστό ως διπλός κατευθυνόμενος αυτομάτως οικοδεσπότης. Τα δύο «σπίτια» αναφέρονται στα δύο δίκτυα ότι η μηχανή τειχών προστασίας είναι μέρος - μια διεπαφή που συνδέεται με το σπίτι εξωτερικών όψεων, και άλλη που συνδέεται με το εσωτερικό σπίτι.

Αυτή η ιδιαίτερη οργάνωση έχει το πλεονέκτημα της απλότητας και εάν η σύνδεση με το Διαδίκτυό σας είναι μέσω ενός διαποδιαμορφωτή και έχετε μόνο μια διεύθυνση IP, είναι αυτό που πρόκειται πιθανώς για να πρέπει να ζήσετε με εκτός αν δημιουργείτε ένα πιο σύνθετο δίκτυο όπως αυτό που πρόκειται να μιλήσουμε για.

Ένα Two-Legged δίκτυο με ένα σύνολο εξέθεσε DMZ

Σε αυτήν την πιο προηγμένη διαμόρφωση, που παρουσιάζεται στην εικόνα κατωτέρω, ο δρομολογητής που συνδέει με την εργασία εξωτερικών όψεων συνδέεται με μια πλήμνη (ή το διακόπτη).



Οι μηχανές που θέλουν την άμεση πρόσβαση στον κόσμο εξωτερικών όψεων, unfiltered από τον τείχος προστασίας, συνδέουν με αυτήν την πλήμνη. Ένας από τους προσάρμοσες δικτύων της αντιπυρικής ζώνης συνδέει επίσης με αυτήν την πλήμνη. Ο άλλος προσαρμοσθείς δικτύων συνδέει με την εσωτερική πλήμνη. Μηχανές που πρέπει να προστατευθούν από την ανάγκη τειχών προστασίας να συνδέσουν με αυτήν την πλήμνη. Οποιεσδήποτε από αυτές τις πλήμνες θα μπορούσαν να αντικατασταθούν με τους διακόπτες για την προστιθέμενες ασφάλεια και την ταχύτητα, και θα ήταν αποτελεσματικότερο να χρησιμοποιήσει έναν διακόπτη

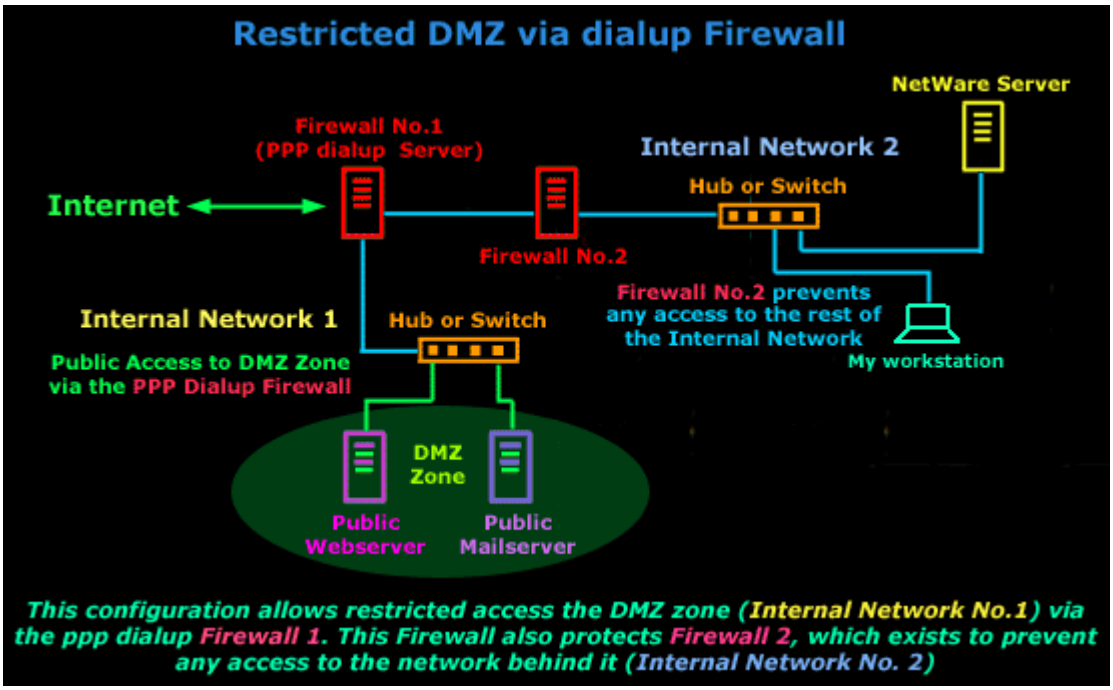
για την εσωτερική πλήμνη.

Υπάρχουν καλά πράγματα για την εκτεθειμένη διαμόρφωση DMZ.Το τείχος προστασίας χρειάζεται μόνο δύο κάρτες δικτύων. Αυτό απλοποιεί τη διαμόρφωση του. Επιπλέον, εάν ελέγχετε το δρομολογητή έχετε πρόσβαση σε ένα δεύτερο σύνολο ικανοτήτων πακέτο-φιλτραρίσματος. Χρησιμοποιώντας αυτών, μπορείτε να δώσετε σε DMZ σας κάποια περιορισμένη προστασία απολύτως χωριστή από το τείχος προστασίας σας.

Αφ' ενός, εάν δεν ελέγχετε το δρομολογητή, DMZ σας εκτίθεται συνολικά στο Διαδίκτυο. Η σκλήρυνση μιας αρκετά μηχανής να ζήσει στο DMZ χωρίς να πάρει τακτικά συμβιβασμένη μπορεί να είναι δυσνόητη.

Η εκτεθειμένη διαμόρφωση DMZ εξαρτάται από δύο πράγματα: 1) εξωτερικός δρομολογητής, και 2) πολλαπλάσιες διευθύνσεις IP.

Εάν συνδέσετε μέσω του PPP (διεπιλογή διαποδιαμορφωτών), ή δεν ελέγχετε τον εξωτερικό δρομολογητή σας, ή θέλετε να μεταμφιέσετε DMZ σας, ή έχετε μόνο 1 διεύθυνση IP, θα πρέπει να κάνετε το κάτι άλλο. Υπάρχουν δύο απλές λύσεις σε αυτό, ανάλογα με το ιδιαίτερο πρόβλημά σας.



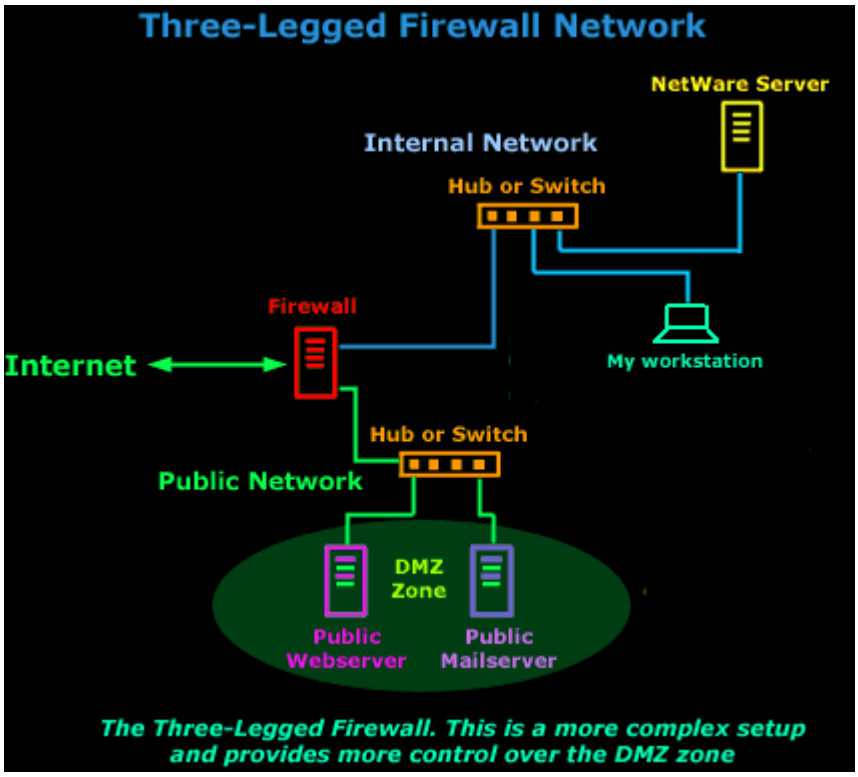
Μια λύση είναι να χτιστεί ένας δεύτερος δρομολογητής/ένας τοίχος προστασίας. Αυτό είναι χρήσιμο εάν συνδέετε μέσω του PPP. Μια μηχανή είναι το εξωτερικό τείχος προστασίας δρομολογητών (τείχος προστασίας κανένα). Αυτή η μηχανή είναι αρμόδια για τη δημιουργία της σύνδεσης PPP και ελέγχει την πρόσβαση στη ζώνη DMZ μας. Το άλλο τείχος προστασίας (τείχος προστασίας κανένα) είναι τυποποιημένος διπλός κατευθυνόμενος αυτομάτως οικοδεσπότης ακριβώς όπως αυτόν που μιλήσαμε για στην αρχή της σελίδας, και η εργασία της είναι να προστατεύσει το εσωτερικό δίκτυο. Αυτό είναι ίδιο με την κατάσταση ενός διπλού

κατευθυνόμενου αυτομάτως τείχους προστασίας όπου η μηχανή PPP σας είναι ο τοπικός εξωτερικός δρομολογητής.

Η άλλη λύση είναι να δημιουργήσει ένα τρίποδο τείχος προστασίας, το οποίο είναι αυτό που πρόκειται να μιλήσουμε για έπειτα.

Το τρίποδο τείχος προστασίας

Αυτό σημαίνει ότι χρειάζεστε έναν πρόσθετο προσαρμοστή δικτύων στο κιβώτιο τειχών προστασίας σας για DMZ σας. Το τείχος προστασίας διαμορφώνεται έπειτα στα πακέτα διαδρομών μεταξύ του κόσμου εξωτερικών όψεων και του DMZ διαφορετικά απ' ότι μεταξύ του κόσμου εξωτερικών όψεων και του εσωτερικού δικτύου. Αυτό είναι μια χρήσιμη διαμόρφωση, και έχω δει πολλοί από τους πελάτες μας χρησιμοποιώντας την.



Η τρίποδος οργάνωση μπορεί επίσης να σας δώσει τη δυνατότητα να έχει ένα DMZ εάν είστε κολλημένοι με την απλή τοπολογία που περιγράφεται πρώτα (διπλό κατευθυνόμενο αυτομάτως τείχος προστασίας). Αντικαταστήστε «το δρομολογητή» με «το διαποδιαμορφωτή,» και μπορείτε να δείτε πώς αυτό είναι παρόμοιο με την απλή τοπολογία (διπλό κατευθυνόμενο αυτομάτως τείχος προστασίας), αλλά με ένα τρίτο πόδι που κολλιέται στην πλευρά:)

Εάν αναγκάζεστε ή έχετε επιλέξει στη μεταμφίεση IP, μπορείτε να μεταμφιέσετε τη μηχανή ή τις μηχανές στο DMZ επίσης, κρατώντας τους λειτουργικά χωριστούς από τις προστατευμένες εσωτερικές μηχανές. Οι άνθρωποι που έχουν τους

διαποδιαμορφωτές καλωδίων ή τις στατικές συνδέσεις PPP μπορούν να χρησιμοποιήσουν αυτό το σύστημα για να τρέξουν τους διάφορους κεντρικούς υπολογιστές μέσα σε ένα DMZ καθώς επίσης και ένα ολόκληρο εσωτερικό δίκτυο από μια ενιαία διεύθυνση IP. Είναι μια πολύ οικονομική λύση για τις μικρές επιχειρήσεις ή τα Υπουργεία Εσωτερικών.

Το αρχικό μειονέκτημα στον τρίποδο τείχος προστασίας είναι η πρόσθετη πολυπλοκότητα. Η πρόσβαση σε και από το DMZ και σε και από το εσωτερικό δίκτυο ελέγχεται από ένα μεγάλο σύνολο κανόνων. Είναι αρκετά εύκολο να αποκτηθούν αυτοί οι κανόνες λανθασμένοι εάν δεν είστε προσεκτικοί!

Αφ' ενός, εάν δεν έχετε οποιοδήποτε έλεγχο του δρομολογητή Διαδικτύου, μπορείτε να ασκήσετε πολύ περισσότερο έλεγχο της κυκλοφορίας σε και από το DMZ αυτός ο τρόπος. Είναι καλό να αποτραπεί η πρόσβαση στο DMZ εάν μπορείτε.

8.ΠΡΟΣΑΡΜΟΓΗ ΤΟΥ ΤΕΙΧΟΥΣ ΠΡΟΣΤΑΣΙΑΣ ΑΝΑ ΧΡΗΣΤΗ

Τα τείχη προστασίας μπορούν να προσαρμοστούν ανάλογα με το χρήστη. Αυτό σημαίνει ότι μπορείς να προσθέσεις ή να αφαιρέσεις φίλτρα βασισμένα σε διάφορες καταστάσεις. Μερικές από αυτές είναι:

- IP addresses – Κάθε μηχάνημα στο Ίντερνετ είναι ορισμένο με μια μοναδική διεύθυνση που καλείται IP address. IP addresses είναι 32-bits αριθμός κανονικά εκφράζεται ως τέσσερα «οστάρια»σε ένα δυαδικό σύστημα. Μια τυπική IP address έχει αυτή τη μορφή: 216.27.61.137.Για παράδειγμα, εάν μια συγκεκριμένη IP address εκτός εταιρίας διαβάζει πολλά αρχεία από έναν server, το τείχος προστασίας μπορεί να μπλοκάρει όλη την κυκλοφορία προς ή από αυτήν την IP.
- Domain names –Επειδή είναι δύσκολο να θυμόμαστε εκείνον τον αριθμό που φτιάχνει μια IP address,και επειδή οι IP addresses κάποιες φορές χρειάζεται να αλλάξουν, όλοι οι servers στο Internet έχουν ονόματα που μπορούμε να τα θυμηθούμε τα οποία ονομάζονται domain names. Για παράδειγμα, είναι πιο εύκολο για τους περισσότερους από εμάς να θυμόμαστε www.howstuffworks.com από το να θυμόμαστε 216.27.61.137. μια εταιρία μπορεί να μπλοκάρει εξολοκλήρου την πρόσβαση σε συγκεκριμένα domain names, ή να επιτρέπει πρόσβαση μόνο σε συγκεκριμένα domain names.
- Protocols – Το πρωτόκολλο είναι ένας προκαθορισμένος τρόπος για κάποιον που θέλει να χρησιμοποιεί μια υπηρεσία να επικοινωνεί με μια άλλη υπηρεσία. Ο ‘κάποιος’ μπορεί να είναι άνθρωπος ,αλλά πολύ συχνά μπορεί να είναι ένα πρόγραμμα του υπολογιστή όπως είναι ο Web browser.Τα πρωτοκολλά είναι συχνά κείμενα και απλά περιγράφουν πως ο ‘πελάτης’ και ο server μπορούν να έχουν μεταξύ τους επικοινωνία. Το http είναι το πρωτόκολλο του Web. Μερικά κοινά πρωτοκολλά τα οποία μπορούμε να θέσουμε ως φίλτρα τειχών προστασίας :
- IP (Internet Protocol) - the main delivery system για πληροφορίες σε όλο το 'Ιντερνετ
- TCP (Transmission Control Protocol) - used to break apart and rebuild information that travels over the Internet
    - HTTP (Hyper Text Transfer Protocol) – χρησιμοποιείται για Web pages
    - FTP (File Transfer Protocol) – χρησιμοποιείται για να ανεβάζεις και να κατεβάζεις αρχεία.
    - UDP (User Datagram Protocol) – χρησιμοποιείται για πληροφορίες που δεν απαιτούν απάντηση ,όπως είναι streaming audio και video
    - ICMP (Internet Control Message Protocol) – χρησιμοποιείται από έναν router για να εξάγει πληροφορία σε άλλους
    - SMTP (Simple Mail Transport Protocol) – χρησιμοποιείται για να στέλνει πληροφορίες βασισμένες σε κείμενα (e-mail)
    - SNMP (Simple Network Management Protocol) – χρησιμοποιείται για να μαζέψει πληροφορίες από έναν απομακρυσμένο
    - Telnet – χρησιμοποιείται για να εκτελεί εντολές σε έναν απομακρυσμένο υπολογιστή.

Μια εταιρία συνήθως στήνει μόνο ένα ή δυο μηχανήματα για να χειριστούν το συγκεκριμένο πρωτόκολλο και καταργεί αυτό το πρωτόκολλο από τα αλλά μηχανήματα.

- Ports –Οποιοδήποτε server κάνει διαθέσιμες τις υπηρεσίες του στο Internet χρησιμοποιώντας αριθμημένα ports, ένα για κάθε υπηρεσία είναι διαθέσιμο στο server (see How Web Servers Work for details). Για παράδειγμα, αν ένας server τρέχει έναν Web (HTTP)server και έναν FTP server Web server μπορεί τυπικά να είναι διαθέσιμος στο port 80 και ο FTP server μπορεί να είναι διαθέσιμος στο port 21.Μια εταιρία μπορεί να μπλοκάρει τη πρόσβαση σε όλα τα μηχανήματα στο port 21 αλλά ένα μέσα στην εταιρία. Συγκεκριμένες λέξεις και φράσεις -Μπορεί να είναι οτιδήποτε. Το τείχος προστασίας θα ψάξει διεξοδικά κάθε πακέτο πληροφορίας για ένα ακριβές ταίριασμα του κειμένου το οποίο είναι καταχωρημένο στο φίλτρο. Για παράδειγμα, μπορείς να δώσεις εντολή στο firewall να μπλοκάρει κάθε πακέτο με την λέξη 'Χ-βαθμό' μέσα σε αυτή. Το κλειδί εδώ είναι ότι αυτό πρέπει να ταιριάζει ακριβώς. το φίλτρο "Χ-βαθμου" δεν μπορεί να πιάσει το 'Χ βαθμό'(χωρίς να υπάρχει η ενωτική παύλα). Αλλά μπορείς να συμπεριλαμβάνεις τόσες πολλές λέξεις, φράσεις και ποικιλίες από αυτά όσες χρειάζεσαι.

Σε μερικά λειτουργικά συστήματα υπάρχει εγκατεστημένο το firewall. Διαφορετικά ,ένα λογισμικό firewall πρέπει να εγκατασταθεί στον υπολογιστή σας το οποίο είναι συνδεδεμένο στο Διαδικτύο. Αυτός ο υπολογιστής εξετάζει την πύλη, επειδή παρέχει το μόνο σημείο πρόσβασης ανάμεσα στο δίκτυο του σπιτιού σας και στο Ίντερνετ.

Με ένα firewall υλικού ,το μέρος του firewall από μόνο του είναι κανονικά η πύλη. Ένα καλό παράδειγμα είναι ο Διεπιλογής/DSL router Linksys.Αν το έχει πάνω του μια Ethernet κάρτα και ένα hub. Οι υπολογιστές στο δίκτυο του σπιτιού σας συνδέονται με ένα router ,το οποίο με τη σειρά του συνδέεται είτε με διεπιλογικό είτε με DSL modem. Μπορείτε να διαμορφώσετε το router μέσω μιας διεπαφής που είναι βασισμένη στο Web που είναι προσβάσιμη μέσω του browser του υπολογιστή σας. Έπειτα μπορείτε να θέσετε κάποια φίλτρα ή επιπλέον πληροφορίες .Επίσης είναι απίστευτα ασφαλή και όχι πολύ ακριβά και βρίσκονται σε διάθεση από διάφορες εταιρίες:

ZoneAlarm – πολύ εύκολο να εγκαταστήσει και να χρησιμοποιήσει, υπάρχει μια ελεύθερη έκδοση με μερικούς λιγότερα χαρακτηριστικά γνωρίσματα από την επαγγελματική έκδοση. Σας δίνει τις πολύ καλές πληροφορίες για τις επιφυλακές που παράγουν. Εξέτασε τον πρωτοπόρο στην αγορά.

Το BlackICE – μια άλλη πολύ ιδιαίτερα εκτιμημένη προσωπική αντιπυρική ζώνη, αυτό δεν είναι τόσο φιλικό προς το χρήστη όσο ZoneAlarm, αλλά επιτρέπει μερικές περαιτέρω επιλογές διαμόρφωσης

Η προσωπική αντιπυρική ζώνη – Sygate επίσης λιγότερο φιλική προς το χρήστη, αλλά αυτό επιτρέπει σε σας για να κάνει μερικές πολύ ισχυρές αλλαγές διαμόρφωσης και περιέχει ένα στοιχειώδες σύστημα ανίχνευσης παρείσφρησης για να σας προειδοποιήσει για τις κοινές επιθέσεις.

McAfee Firewall v.4.O-, το McAfee Firewall σας δίνει τη δύναμη που χρειάζεται για να ελέγχετε τις επικοινωνίες σε και από το PC σας ,εξασφαλίζοντας ότι εμπειρία σας στο Διαδικτυο είναι τόσο ασφαλής όσο και ευχάριστη.

9.McAfee Firewall 4.0

Α.ΚΑΛΩΣΗΡΘΑΤΕ ΣΤΟ McAfee Firewall 4.0

Προστατευθείτε ενώ βρισκόσαστε στο Ιντερνετ με την προηγμένη ασφάλεια του McAfee Firewall. Εύχρηστο, παρ'όλα αυτά ιδιαίτερα διαμορφώσιμο, το McAfee Firewall εξασφαλίζει τη σύνδεση των PC σας στο Διαδίκτυο είτε συνδέεστε μέσω DSL, διαποδιαμορφωτή καλωδίων ή διεπιλογή. Με την ανίχνευση απρόσκλητης επίσκεψης, κωδικοποιημένες με χρώμα επιφυλακές ασφάλειας, εξατομικεύσιμες ευδιάκριτες επιφυλακές, λεπτομερής αναγραφή, και μια ανίχνευση εφαρμογής για Διαδίκτυο που επιτρέπεται οι εφαρμογές,

McAfee Firewall:

- Έλεγχος αρχείων και πρόσβαση σε κοινή χρήση σε εκτυπωτή
- Εμφανίζει το ποιος συνδέεται με τον υπολογιστή σας εάν επιτρέπεται η κοινή χρήση.
- Σταματά τις πλημμύρες και άλλα πακέτα επίθεσης να λαμβάνονται από το Λειτουργικό σύστημα.
- Μπλοκάρει τις μη αξιόπιστες εφαρμογές με την επικοινωνία πέρα από το δίκτυο.
- Παρέχει αναλυτικές πληροφορίες σχετικά με ποιες περιοχές έχετε επικοινωνήσει και το τύπο σύνδεσης που πραγματοποιήθηκε.
- Μπορείτε να θέσετε να εμποδίσει όλη την κυκλοφορία ή την κυκλοφορία από μια συγκεκριμένη διεύθυνση IP άμεσα.

Τι καινούριο σε αυτήν την απελευθέρωση;

- Έλεγχος ασφάλειας του Firewall: Εξετάζει τις επιλογές της ασφάλειάς σας για πιθανές ευπάθειες.
- Ενισχυμένη ανεύρεση χάκερ χρησιμοποιώντας από το McAfee την τεχνολογία Οπτικής Ανεύρεσης.
- Σύστημα ανίχνευσης απρόσκλητης επίσκεψης : Ανιχνεύει τους κοινούς τύπους επίθεσης και την ύποπτη δραστηριότητα.
- Μάγος εγχώριας δικτύωσης: Οργανώστε προστασία για τους προσωπικούς υπολογιστές διαμοιράζοντας μια σύνδεσης με το Διαδίκτυο.
- Μάγος για τη δημιουργία των συνηθισμένων κανόνων: Δημιουργεί τις συνηθισμένες διαμορφώσεις για συγκεκριμένα προγράμματα.
- Προστασία κωδικού πρόσβασης: Αποτρέψτε τους άλλους από το να πειράξουν με τις ρυθμίσεις του Firewall σας χρησιμοποιώντας προστασία κωδικού πρόσβασης.
- Βελτιωμένη υποστήριξη για τις ευρυζωνικές συνδέσεις.
- Αυξήσεις δυνατότητας χρησιμοποίησης: Το McAfee Firewall 4.00 περιλαμβάνει πολλές ενισχυμένες για το χρήστη διεπαφες ώστε να το καταστήσει ευκολότερο από ποτέ προστατεύοντας τον υπολογιστή σας.

Πώς το McAfee Firewall λειτουργεί

Το McAfee Firewall είναι απλό λειτουργικό εργαλείο ασφάλειας που δυναμικά διαχειρίζεται την ασφάλεια υπολογισμού σας πίσω από τις σκηνές.

Εγκατάσταση

Κατά τη διάρκεια της εγκατάστασης ,ο βοηθός διαμόρφωσης σας προτρέπει με βασικές ερωτήσεις για την εγκατάσταση του McAfee Firewall για να κάνει συγκεκριμένες δουλείες -σύμφωνα με τις ανάγκες σας (π.χ. επιτρέπει την κοινή χρήση των αρχείων ή όχι).

Λειτουργία

Το McAfee Firewall φιλτράρει την κυκλοφορία στις συσκευές που το σύστημά σας χρησιμοποιεί – κάρτες δικτύου και διαποδιαμορφωτές. Αυτό σημαίνει ότι μπορεί να απορρίψει την εισερχόμενη κυκλοφορία πριν αυτή η κυκλοφορία μπορέσει να φθάσει στις ζωτικής σημασίας λειτουργίες μέσα στον υπολογιστή σας και να σπαταλήσει πολύτιμους πόρους από το σύστημα σας .

McAfee Firewall- Ο Φύλακας

Όταν McAfee Firewall τρέχει, ελέγχει τα αξιόπιστα και μη αξιόπιστα προγράμματα που επικοινωνούν χρησιμοποιώντας το Διαδικτύο. Εάν μια αξιόπιστη εφαρμογή προσπαθεί να επικοινωνήσει, το McAfee Firewall επιτρέπει στο πρόγραμμα να λειτουργήσει χωρίς περιορισμούς. Εάν ένα αναξιόπιστο πρόγραμμα προσπαθεί να επικοινωνήσει μέσα στο ή έξω από τον υπολογιστή σας, το McAfee Firewall εμποδίζει την προσπάθεια του προγράμματος να επικοινωνήσει μέσω του Διαδικτύου.

Διαμόρφωση

Μερικές επικοινωνίες δικτύων απαιτούνται για να διατηρήσουν τις υπηρεσίες που βασίζονται στο διαδικτυο.
Αυτές ρυθμίζονται μέσω των καθορισμένων από το χρήστη κανόνων στο πλαίσιο των ρυθμίσεων του συστήματος του McAfee Firewall. Το προεπιλεγμένο χαρακτηριστικό γνώρισμα των ρυθμίσεων του συστήματος παρέχει ανώτερη προστασία από τις εχθρικές απειλές.

Σχετικά με αυτό το εγχειρίδιο

Αυτό το εγχειρίδιο παρέχει τις βασικές πληροφορίες που χρειάζεστε για να εγκαταστήσετε, στήσετε και να ξεκινήσετε με το McAfee Firewall. Περισσότερες αναλυτικές πληροφορίες για το πώς θα εκτελέσετε κάποιες δουλείες μέσα στο McAfee Firewall παρέχονται μέσω της σε απευθείας σύνδεση βοήθειας. Μπορείτε να πάρετε τη βοήθεια ενώ εργαζόσαστε με διαφορετικά παράθυρα και με τα πλαίσια διαλόγου. Μπορείτε επίσης να κάνετε ανασκόπηση στο αρχείο του Readme.txt που περιέχει άλλες γενικές πληροφορίες, γνωστά ζητήματα, κ.λπ., για αυτό το προϊόν.

Συχνές ερωτήσεις

Τα ακόλουθα είναι μερικές συχνές ερωτήσεις που μπορείτε να κάνετε μια σύντομη ανασκόπηση:

Πώς το McAfee Firewall θα με βοηθήσει;

Το McAfee Firewall προστατεύει τον υπολογιστή σας στο επίπεδο δικτύων. Ενεργεί ως φύλακας , που ελέγχει κάθε πακέτο στοιχείων που πηγαίνει σε ή από το PC σας. Επιτρέπει μόνο ότι του λετε να επιτρέψει.

Το McAfee Firewall έχει σχεδιαστεί για να είναι εύχρηστο, καθώς παρέχει ανώτερη προστασία. Μόλις το εγκαταστήσετε και το τρέξετε, είναι διαμορφωμένο για να εμποδίζει τις γνωστές επιθέσεις και για να σας ρωτάει πριν επιτρέψει στις εφαρμογές την επικοινωνία.

Πώς βρίσκεται το PC μου σε κίνδυνο στο διαδίκτυο;

Όταν συνδέστε με το Διαδίκτυο, μοιράζεστε ένα δίκτυο με εκατομμύρια ανθρώπους από όλον τον κόσμο. Αν και το
Διαδίκτυο είναι ένα θαυμάσιο και καταπληκτικό κατόρθωμα ,αυτό φέρνει μαζί του όλα τα προβλήματα που είναι προσιτά σε εντελώς ξένους.
Επικοινωνώντας μέσω του Διαδικτύου, πρέπει να πάρετε προφυλάξεις ασφάλειας για να προστατεύσετε το υπολογιστικό περιβάλλον σας. Εάν χρησιμοποιείτε IRC (Internet Relay Chat) προγράμματα, να είστε καχύποπτοι με τα αρχεία που σας στενού εντελώς ξένοι. Προγράμματα που δίνουν σε άλλους εξ'
αποστάσεως πρόσβαση στον υπολογιστή σας, όπως το Back Orifice (BO), είναι συχνά διασκορπισμένο κατά αυτόν τον τρόπο. Είναι μια καλή πολιτική να σκαννάρεις τα ληφθέντα
αρχεία χρησιμοποιώντας antivirus προγράμματα όπως το McAfee
VirusScan πριν ανοίξεις ή δεις τα αρχεία και τα συνημμένα τους.

Όταν βρίσκεσαι στο διαδίκτυο, κάποιοι μπορεί να προσπαθήσουν να έχουν πρόσβαση στα κοινά αρχεία σας . Επομένως, εσείς πρέπει να ελέγξετε ότι είναι μόνο προσβάσιμα σε εκείνους που εμπιστεύεστε. Διαφορετικά, μη αξιόπιστα
μέρη μπορούν να διαβάσουν και να διαγράψουν ότι υπάρχει στον υπολογιστή σας.

Τι άλλη προστασία χρειάζομαι;

Το McAfee Firewall παρέχει προστασία στο επίπεδο των δικτύων. Άλλοι σημαντικοί τύποι προστασίας είναι:

- Προγράμματα antivirus για προστασία στο επίπεδο εφαρμογής.
- Οθόνες σύνδεσης και κωδικοί πρόσβασης προφύλαξης οθονών για να αποτρέψει από αναρμόδια πρόσβαση.
- Κρυπτογράφηση αρχείων ή κρυπτογραφημένα αρχεία συστήματος για να κρατήσουν τις πληροφορίες μυστικές.
- Boot-time κωδικοί πρόσβασης για να σταματήσει κάποιον άλλο να ξεκινήσει το PC σας.
- Φυσική πρόσβαση στον υπολογιστή, π.χ. κλέβοντας το σκληρό δίσκο.

Ένα χωριστό αλλά επίσης σημαντικό ζήτημα είναι να ελέγχεις την πρόσβαση στις πληροφορίες, παραπληροφόρηση και«βρωμιά» που είναι ευρέως διαθέσιμα στο Διαδίκτυο. Μπορείτε να χρησιμοποιήστε έναν αριθμό από περιεχόμενα-φιλτράροντας υπηρεσίες ή προγράμματα όπως το McAfee's Internet Security που μπορεί να φιλτράρει το περιεχόμενο από τα στοιχεία των πακέτων ή να περιορίσει την πρόσβαση σε ορισμένες περιοχές.

Υπάρχουν πακέτα στοιχείων που το McAfee Firewall δεν μπορεί να σταματήσει;

Εισερχόμενα στοιχεία: Όχι. Εφ' όσον το McAfee Firewall υποστηρίζει και τρέχει μια συσκευή δικτύων ,παρεμποδίζει όλα τα εισερχόμενα πακέτα και θα επιτρέψει ή θα εμποδίσει

σύμφωνα με τον τρόπο που το έχετε διαμορφώσει. Εάν επιλέγετε να τα εμποδίσετε όλα, αυτό θα γίνει.

Εξερχόμενα στοιχεία: Ναι και όχι. Το McAfee Firewall παρεμποδίζει τα εξερχόμενα στοιχεία των πακέτων καθώς αυτά περνούν στον οδηγό συσκευών δικτύων. Όλες οι δημοφιλείς εφαρμογές επικοινωνούν με αυτόν τον τρόπο. Ένα κακόβουλο πρόγραμμα θα μπορούσε να επικοινωνήσει με άλλα μέσα, εντούτοις.

Ποιες συσκευές δικτύων το McAfee Firewall υποστηρίζει;

Το McAfee Firewall υποστηρίζει Ethernet και συσκευές όμοιες του Ethernet. Αυτό περιλαμβάνει συνδέσεις διεπιλογών, οι Περισσότερους διαποδιαμορφωτές και ISDN μόντεμ και περισσότερες κάρτες Ethernet. Δεν υποστηρίζει Token Ring, FDDI, ATM,Frame Relay και άλλα δίκτυα.

Ποια πρωτόκολλα μπορεί το McAfee Firewall να φιλτράρει;

Το McAfee Firewall μπορεί να φιλτράρει TCP/IP, UDP/IP, ICMP/IP και ARP. Παρεμποδίζει όλα τα πρωτόκολλα, αλλά άλλα, όπως το IPX, πρέπει είτε να επιτραπούν είτε να εμποδιστούν – δε γίνεται φιλτράρισμα. Το Διαδίκτυο χρησιμοποιεί τα πρωτόκολλα IP.

Κανένας άλλος δεν στέλνεται. Επίσης, Τα δίκτυα IP είναι τα πιο κοινά.

Πώς μπορώ να παρενοχληθώ ακόμα, ακόμη και με το McAfee Firewall;

Πολλοί άνθρωποι χρησιμοποιούν το McAfee Firewall για να εμποδίσουν τις «καταστροφές» που προκαλούν τις IRC να σπάσουν. Καθώς το McAfee Firewall εμποδίζει τις καταστροφές, υπάρχουν άλλοι τρόποι ώστε οι εισβολείς μπορούν ακόμα να σπάσουν τις συνδέσεις:

Υπολογιστής-δευτερεύον ατομικό όπλο. Τότε είναι που οι «καταστροφές» στέλνονται στον κεντρικό υπολογιστή IRC, όχι στον υπολογιστή σας, που λεει στον κεντρικό υπολογιστή ότι δεν μπορείτε πλέον να είστε επιτευγμένος. Για να το αποτρέψουμε αυτό, ο κεντρικός υπολογιστής IRC χρειάζεται ένα firewall.

Πλημμύρα που εμποδίζει μια σύνδεση TCP. Εάν μια πλημμύρα πακέτων σας στέλνεται από μια υψηλότερη ταχύτητα σύνδεσης ,το McAfee Firewall μπορεί να σταματήσει τα πακέτα, αλλά η πλημμύρα καταλαμβάνει όλο το εύρος ζώνης σας. Το σύστημά σας δεν έχει πιθανότητα να στείλει τίποτα. Οι χρήστες διεπιλογών είναι ιδιαίτερα τρωτοί εάν έχουν χαμηλότερες ταχύτητες σύνδεσης.

ΠΛΗΡΟΦΟΡΙΑ

Για να διαβάσετε περισσότερες συχνές ερωτήσεις, αναφερθείτε στο αρχείο του Readme.txt.

Β.ΕΓΚΑΘΙΣΤΩΝΤΑΣ ΤΟ McAfee Firewall

Το CD που περιέχει το πρόγραμμα εγκατάστασης για το McAfee Firewall 4.0 σας επιτρέπει την εύκολη εγκατάσταση του προγράμματος στον υπολογιστή σας. Η εγκατάσταση πρέπει να αρχίσει αυτόματα όταν εισάγετε το CD στο CD-ROM του υπολογιστή σας. Οι πληροφορίες στις ακόλουθες παραγράφους θα σας βοηθήσουν να εγκαταστήσετε και να αρχίσετε να χρησιμοποιείτε το McAfee Firewall.

Απαιτήσεις συστημάτων

Για να χρησιμοποιήσετε το McAfee Firewall χρειάζεστε:

- Microsoft Windows XP Home Edition, Windows XP Professional Edition, Windows 2000 Professional, Windows Me, Windows98, Windows 98 SE.

- Internet Explorer 4.01, Service Pack 2 or higher required; IE 5.01 or later recommended.

- Προσωπικός υπολογιστής με ένα Pentium 100 MHZ ή υψηλότερο επεξεργαστή.
- 32MB RAM.
- 30 MB ελεύθερο χώρο στο σκληρό δίσκο.
- CD-ROM drive.
- Πρόσβαση στο Διαδίκτυο απαιτείται για τα διάφορα χαρακτηριστικά γνωρίσματα.

Σχετικά με τα Winsock 2

Το McAfee Firewall χρησιμοποιεί ένα API (διεπαφή προγραμματισμού εφαρμογής) που δεν είναι υποστηρίζεται από τις εκδόσεις Winsock προγενέστερες του v2.0. Το McAfee Firewall ελέγχει για την παρουσία του Winsock 2 κατά τη διάρκεια της διαδικασίας εγκαταστάσεων και θα σας ενημερώσει εάν το σύστημα δεν το έχει. Εάν έχετε την πιο πρόσφατη μηχανή αναζήτησης (π.χ., Internet Explorer 6), αυτό το συστατικό είναι ήδη ενσωματωμένο και δεν θα λάβετε αυτήν την υπαγόρευση. Διαφορετικά, μπορείτε να πάρετε μια ελεύθερη βελτίωση η οποία είναι διαθέσιμη από το http://www.microsoft.com καθώς επίσης και από άλλους ιστοχώρους.

Βήματα εγκατάστασης

Για να αποφύγετε τα προβλήματα της εγκατάστασης, κλείστε όλα τα ανοικτά προγράμματα προτού να εγκαταστήσετε το McAfee Firewall, συμπεριλαμβανομένων των προγραμμάτων που τρέχουν στο υπόβαθρο, όπως προφύλαξη οθόνης ή ελεγκτές ιών.

Αφού εισάγετε το CD εγκατάστασης του McAfee Firewall 4.0 στο CD-ROM driver του υπολογιστή σας, μια εικόνα αυτόματης εκτέλεσης θα εμφανιστεί. Για να εγκαταστήσετε άμεσα το λογισμικό του McAfee Firewall, κλικάρετε το Εγκατάσταση του McAfee Firewall, έπειτα προχωρήστε στο βήμα 5 για να συνεχιστεί η εγκατάσταση.

Χρησιμοποιήστε τα κατωτέρω βήματα για να εγκαταστήσετε το λογισμικό σας.

1. Εάν ο υπολογιστής σας τρέχει τα Windows 2000 Professional, ή τα Windows XP, συνδεθείτε στον υπολογιστή σας ως χρήστης με διαχειριστικά δικαιώματα. Πρέπει να έχετε διαχειριστικά δικαιώματα για να εγκατασταθεί αυτό το λογισμικό.
2. Εισάγετε το CD του McAfee Firewall 4.0 στο CD-ROM του υπολογιστή σας. Εάν ο μάγος εγκατάστασης δεν εμφανιστεί αυτόματα, πηγαίνετε στο βήμα Διαφορετικά, προχωρήστε στο βήμα 4.
3. Χρησιμοποιήστε την ακόλουθη διαδικασία εάν το μενού αυτόματης εγκατάστασης δεν εμφανιστεί, ή, εάν λάβατε το λογισμικό μέσω κατεβάσματος από τον ιστιοχώρο του McAfee.
   - Από το μενού έναρξης των Windows, επιλέξτε το Run(Εκτέλεση). Το πλαίσιο διαλόγου Run (Εκτέλεση) εμφανίζεται.
   - Πληκτρολογείστε <X> : \ SETUP.EXE στο παράθυρο κειμένου που έχει, κατόπιν κάντε κλικ στο OK (Εντάξει)

4. Εδώ, το <X>αντιπροσωπεύει το γράμμα του driver (οδηγού) για τον οδηγό του CD-ROM σας ή το μονοπάτι του φακέλου που περιέχει τα εξαγόμενα αρχεία του McAfee Firewall σας. Για να αναζητήσετε τα σωστά αρχεία στο σκληρό δίσκο ή στο CD-Rom σας, κάντε κλικ στο Browse.
   - Πριν συνεχίσετε με την εγκατάσταση, στην αρχή το πρόγραμμα εγκατάστασης ελέγχει για να δει που ο υπολογιστής σας έχει το Microsoft Windows Installer (MSI) χρησιμότητα που τρέχει ως τμήμα του λογισμικού συστήματος σας. Εάν ο υπολογιστής σας τρέχει τα Windows XP, η τρέχουσα έκδοση MSI υπάρχει ήδη στο σύστημά σας. Εάν ο υπολογιστής σας τρέχει μια προηγούμενη έκδοση των Windows, μπορεί ακόμα να έχετε το MSI στον υπολογιστή σας εάν είχατε εγκαταστήσει προηγουμένως άλλο λογισμικό που χρησιμοποιεί το MSI. Σε καθεμία από αυτές τις περιπτώσεις , η πρώτη εγκατάσταση εμφανίσει άμεσα το πρώτο της wizard panel . Προχωρήστε στο βήμα 5 για να συνεχίσετε.

- Εάν το πρόγραμμα εγκατάστασης δεν βρίσκει το MSI ή μια προηγούμενη έκδοση του MSI εγκατεστημένη στον υπολογιστή σας, εγκαθιστά αρχεία απαραίτητα για

να συνεχίσει η εγκατάσταση, έπειτα σας προτρέπει να κάνετε επανεκκίνηση στον υπολογιστή σας. Κάντε κλικ στο Restart System(Επανεκκίνηση συστήματος). Όταν ο υπολογιστής ξεκινήσει πάλι, το πρόγραμμα εγκατάστασης θα συνεχίσει από εκεί που είχε μείνει.

5. Αναφέρεται στα βήματα που εμφανίζονται στο μάγο εγκατάστασης για να ολοκληρώσουν την εγκατάσταση.

ΠΛΗΡΟΦΟΡΙΑ

Εάν ο υπολογιστής σας δεν έχει τις απαραίτητες πηγές για να δει το End User's License Agreement(EULA), έπειτα εσείς μπορείτε να εγκαταστήσετε το κατάλληλο EULA στο CD εγκατάστασης λογισμικού του McAfee σας. Πρέπει να διαβάσετε και να
συμφωνήσετε με τους όρους της συμφωνίας για να ολοκληρωθεί η εγκατάσταση.

ΣΗΜΕΙΩΣΗ

Για όλα τις εγκαταστάσεις των Windows 2000 Professional, το McAfee Firewall απαιτεί έναν μοναδικό οδηγό προκειμένου να λειτουργήσει. Κατά τη διάρκεια της διαδικασίας εγκαταστάσεως , θα έρθετε αντιμέτωποι με αρκετά προειδοποιητικά μηνύματα που σας ειδοποιούν ότι προσπαθείτε να εγκαταστήσετε έναν μη ορισμένο οδηγό. Επομένως, παρακαλώ κάντε κλικ στο OK μέχρις ότου εγκαταστήσετε τον οδηγό και κάντε επανεκκίνηση στον υπολογιστή σας εάν χρειάζεται.

Προβλήματα κατά την εγκατάσταση

Μια αποτυχημένη εγκατάσταση μπορεί να προκαλέσει προβλήματα λογισμικού που είναι δύσκολο να εντοπιστούν. Οι σημαντικότερες αιτίες της αποτυχίας εγκαταστάσεων είναι:

- Προσπαθεί να εγκαταστήσει ενώ άλλο λογισμικό τρέχει.
- Προσωρινά αρχεία που συγκρούονται με την εγκατάσταση.
- Λάθη σκληρού δίσκου.

Ακολουθήστε τη διαδικασία που περιγράφεται κατωτέρω για να ελαχιστοποιήσετε την επιρροή που αυτοί οι κοινοί όροι μπορούν να έχουν στην εγκατάστασή σας.

Βήμα 1: Κλείστε άλλο λογισμικό

Θέστε εκτός λειτουργίας όλα το λογισμικά που τρέχουν στην επιφάνεια εργασίας :

1 Πατήστε συγχρόνως τα CTRL και ALT από το πληκτρολόγιό σας, και πιέστε έπειτα το πλήκτρο Delete μία φορά. Το πλαίσιο διαλόγου για το κλείσιμο προγράμματος εμφανίζεται.

2 Κάντε κλικ στο τέλος εργασίας για καθένα που βρίσκεται στη λίστα εκτός από τον Internet Explorer.

3 Επαναλάβετε τα βήματα 2 και 3 έως ότου τα έχετε κλείσει όλα εκτός από τον Explorer.

4 Όταν στη λίστα απομείνει μόνο ο Explorer κάντε Cancel(Ακύρωση).

Βήμα 2: Αφαιρέστε τα προσωρινά αρχεία

Διαγράψτε τα προσωρινά αρχεία από το φάκελο Temp των Windows:

1 Κάντε διπλό κλικ στο εικονίδιο My Computer(Ο Υπολογιστής μου)που βρίσκεται στην επιφάνεια εργασίας . Στο παράθυρο που θα ανοίξει, κάντε διπλό κλικ στο C: drive. Τώρα μπορείτε να δείτε τα περιεχόμενα του σκληρού δίσκου σας.

2 Κάντε διπλό κλικ στο φάκελο των Windows.
3 Στο φάκελο των Windows, κάντε διπλό κλικ στο φάκελο Temp.

4 Στις επιλογές, κάντε κλικ στο Edit, και έπειτα στο Select All. Όλα τα στοιχεία που υπάρχουν στο φάκελο Temp είναι τονισμένα.

5 Πατήστε το πλήκτρο Delete από το πληκτρολόγιό σας για να διαγράψετε τα αρχεία. Εάν τα Windows ρωτούν για τη διαγραφή των αρχείων, πατά ναι.

6 Στο μενού έναρξη των Windows,κάντε κλικ στην έναρξη(Start) και κατόπιν κλείσιμο(Shut Down).

7 Επιλέξτε επανεκκίνηση(Restart) του υπολογιστή, κατόπιν πατήστε Yes για να κλείσει το πλαίσιο διαλόγου των Windows ώστε να ξαναξεκινήσει το PC σας.

Βήμα 3: Καθαρίστε το σκληρό δίσκο σας

Τρέξτε τις χρησιμότητες του σκληρού δίσκου των Windows, το ScanDisk και το Disk Defragmenter εντοπίζει και φτιάχνει οποιαδήποτε λάθη στο σκληρό δίσκο σας:

1.Start->Programs->Accessories->System Tools->Scan Disk.

2.Στο παράθυρο ScanDisk, επιλέξτε να κάνει Standard και Automatically fix errors.

3.Επιλέξτε Advanced .Στο πλαίσιο διαλόγου Advanced Settings,επιβεβαιώστε ότι οι ακόλουθες επιλογές έχουν επιλεχθεί:

- Μόνο εάν έχουν βρεθεί λάθη
- Αντικαταστήστε το ημερολόγιο
- Διαγράψτε
- Ελευθερώστε

4. Αγνοήστε τις άλλες επιλογές, και πατήστε ΕΝΤΑΞΕΙ. Πατήστε έναρξη. Το ScanDisk αρχίζει την ανίχνευση στον σκληρό σας για λάθη. Ανάλογα με το μέγεθος του σκληρού δίσκου σας, Το ScanDisk μπορεί να πάρει αρκετό χρόνο για να ολοκληρώσει την εργασία του.

5. Όταν το ScanDisk τελειώσει, κλείστε το ScanDisk.

6.Start->Programs->Accessories->System Tools->Disk Defragmenter.

7. Πατήστε OK για να ξεκινήσει το Disk Defragmenter. Ανάλογα με την ταχύτητα του υπολογιστή σας και το μέγεθος του σκληρού σας, αυτό μπορεί να πάρει αρκετό χρόνο για να ολοκληρωθεί.

8. Κλειστέ το Disk Defragmenter όταν τελειώσει ο δίσκος σας την ανασυγκρότηση.

Αφαιρώντας ή τροποποιώντας την εγκατάσταση του McAfee Firewall σας .....

Εάν το λειτουργικό σύστημα του υπολογιστή σας είναι…

- Windows 2000 Professional
- Windows XP Home Edition
- Windows XP Professional Edition

πρέπει να συνδεθείτε στον υπολογιστή σας χρησιμοποιώντας ένα προφίλ με διαχειριστικά δικαιώματα.

Κατόπιν κάνετε τα εξής:

1. Από τον Πίνακα Ελέγχου των Windows, αρχίστε την Προσθήκη/Αφαίρεση applet.

2. Επιλέξτε το McAfee Firewall και κάντε κλικ:
   - Πατήστε την αφαίρεση για να Αφαιρέσετε το McAfee Firewall από τον υπολογιστή σας.
   - Πατήστε την Αλλαγή για να τροποποιήσετε την εγκατάσταση του McAfee Firewall σας.

3.Αναφερθείτε στα βήματα που εμφανίζονται στο μάγο εγκατάστασης McAfee Firewall για να ολοκληρώσετε τις αλλαγές σας.

Ξαναξεκινήστε τον υπολογιστή σας όπως οδηγείστε από το πρόγραμμα εγκατάστασης.

Σημαντικές πληροφορίες για τα Windows XP migration

Αναβαθμίζοντας το λειτουργικό σύστημα του υπολογιστή σας από οποιαδήποτε έκδοση των Windows σε Windows XP προκαλεί όλα τα προϊόντα του McAfee να εγκατασταθούν πριν από τη μετανάστευση γίνοντας εκτός λειτουργίας μετά από τη μετανάστευση στα παράθυρα XP.

Θα ενημερωθείτε για αυτήν την κατάσταση όταν κάνετε την πρώτη προσπάθειά σας να ξεκινήσετε ένα προϊόν McAfee (μετά από τη μετανάστευση) - θα καθοδηγηθείτε για να επαναγκαταστήσετε το προϊόν.
Υπό αυτήν τη μορφή, θα πρέπει να απεγκαταστήσετε όλα τα προϊόντα McAfee και να επανατοποθετήσετε χρησιμοποιώντας το CD εγκατάστασης σας ή το λογισμικό που λαμβάνεται από το McAfee μέσω κατεβάσματος**.**

Γ.ΞΕΚΙΝΩΝΤΑΣ ΜΕ ΤΟ McAfee Firewall

Μετά από την εγκατάσταση του McAfee Firewall, θα πρέπει να διαμορφώσετε το λογισμικό σας για την πρώτη χρήση του. Οι βοηθοί διαμόρφωσης σας οδηγούν μέσω αυτής της διαδικασίας.

Ο βοηθός διαμόρφωσης

Οθόνη καλωσορίσματος

Ο βοηθός διαμόρφωσης του McAfee Firewall εμφανίζεται την πρώτη φορά που ξεκινάτε το McAfee Firewall. Αυτός ο μάγος σας καθοδηγεί μέσω του αρχικού προγράμματος εγκατάστασης και ενεργοποιεί το McAfee Firewall στον υπολογιστή σας.
Επιλέξτε Bace(πίσω), Next(επόμενος),Cancel (ακυρώστε), και Finish(τελειώστε)για να πλοηγηθείτε στις βοηθητικές οθόνες διαμόρφωσης.

Εάν επιλέξετε Cancel ή οποιαδήποτε βοηθητική οθόνη διαμόρφωσης, η ενεργοποίηση και οι διαδικασίες Διαμόρφωσης σταματούν. Πρέπει να ολοκληρώσετε το βοηθό διαμόρφωσης στην πρώτη χρήση προκειμένου να ενεργοποιηθεί και να χρησιμοποιηθεί το McAfee Firewall.

Ρυθμίσεις του ελέγχου δικτύων

Οι ρυθμίσεις του ελέγχου δικτύων αναγνωρίζουν πώς θέλετε το McAfee Firewall να ανταποκρίνεται όταν ένα πρόγραμμα προσπαθεί να έχει πρόσβαση στο Διαδίκτυο είτε μέσα είτε έξω από τον υπολογιστή σας .

1.Για να θέσετε τις ρυθμίσεις του ελέγχου δικτύων σας, από την οθόνη Καλωσήρθατε στο McAfee Firewall,επιλέξτε ένα από τα ακόλουθα.

Πίνακας 3-1. Ρυθμίσεις του ελέγχου δικτύων του McAfee Firewall

Ρύθμιση κυκλοφορίας Διαδίκτυο	Περιγραφή
Εμποδίζει όλη την κυκλοφορία	Διαμορφώνει το McAfee Firewall για να εμποδίσει όλη την κυκλοφορία του Διαδίκτυο σε και από τον υπολογιστή σας. Αυτή είναι η πιο ασφαλής ρύθμιση του firewall εντούτοις, προγράμματα στον υπολογιστής σας δεν μπορούν να έχουν πρόσβαση στο Διαδίκτυο.

Φιλτράρει όλη την κυκλοφορία	Σας δίνει την ευκαιρία να αποφασίσετε ποτέ μια εφαρμογή ή ένα πρόγραμμα στον υπολογιστή σας μπορεί να του επιτραπεί να έχει πρόσβαση στο Διαδίκτυο. Εάν ένα μη αναγνωρισμένο πρόγραμμα προσπαθεί να έχει πρόσβαση στον υπολογιστή σας από το διαδικτυο, σας έχει επίσης δοθεί η ευκαιρία να επιτρέψετε ή να μπλοκάρετε την πρόσβαση στον υπολογιστή σας.
Επιτρέπει όλη την κυκλοφορία	Διαμορφώνει το MCA Firewall για να όλη την κυκλοφορία του διαδίκτυο μέσα και έξω από τον υπολογιστή σας .όλα τα προγράμματα στον υπολογιστή σας θα επιτραπεί η πρόσβαση στο διαδίκτυο, τα προγράμματα που θα προσπαθούν να έχουν πρόσβαση από τον υπολογιστή σας στο διαδικτυο δεν θα μπλοκαριστούν. επιτρέπει όλη την κυκλοφορία , θέτει εκτός λειτουργίας όλων τα χαρακτηριστικά γνωρίσματα προστασίας του MCA Firewall και πρέπει μόνο να χρησιμοποιηθείτε για διαγνωστικούς λόγους.

2.Καντε κλικ στο Next.

Επιλογές ξεκινήματος

Αυτή η οθόνη σας επιτρέπει να επιλέξετε το πώς θέλετε το McAfee Firewall να ανταποκριθεί καθώς ξεκινά ο υπολογιστή σας.

Για δική σας ευκολία, οι συνιστώμενες επιλογές φορτώματος ξεκινήματος είναι προεπιλεγμένες.

1. Επιλέξτε να φορτώνεται αυτόματα το McAfee Firewall στο ξεκίνημα εάν θέλετε να προστατεύεστε από το firewall καθώς ξεκινάτε τον υπολογιστή σας, διαφορετικά ξεκλικάρετε την επιλογή.
2. Εάν θέλετε να υπάρχει συντόμευση του McAfee Firewall στην επιφάνεια εργασίας σας ,τότε επιλέξτε Place a MCA Firewall Icon ,διαφορετικά ξεκλικάρετε την επιλογή.
3. Πατήστε Next.

Πρόσβαση στα κοινά

Εάν ο υπολογιστής σας είναι μέρος μιας ομάδας εργασίας, όπως ένα εγχώριο δίκτυο, μπορείτε να διαμορφώσετε το McAfee Firewall για να επιτρέψετε την πρόσβαση στα κοινά δίκτυα του υπολογιστή σας όπως και να επιτρέψτε στον υπολογιστή σας για να έχετε πρόσβαση στα κοινά άλλου υπολογιστή. Ένα μερίδιο είναι ένας πόρος όπως ένας οδηγός , ένας κατάλογος, ένα αρχείο, ή ένας εκτυπωτής διαθέσιμος σε μια ομάδα εργασίας ή εγχώριοι δικτυωμένοι υπολογιστές.

1. Πρόσβαση σε άλλα κοινά: Τσεκάρετε την επιλογή Allow my computer to access other computer's shares εάν θέλετε να επιτρέψετε στον υπολογιστή σας να έχει πρόσβαση σε κοινούς οδηγούς , κατάλογους, φακέλους, και εκτυπωτές, κ.λπ. σε άλλους υπολογιστές στο δίκτυό σας ομάδων εργασίας ή σπιτιών.

2.Πρόσβαση στα κοινά μου: Τσεκάρετε την επιλογή Allow other computers to access my shares για να επιτραπεί σε άλλους υπολογιστές της ομάδα εργασίας ή του εγχωρίου δικτύου σας να έχει πρόσβαση Σούσα κοινούς οδηγούς σας, κατάλογους, φακέλους, και εκτυπωτές, κ.λπ.

3.Πατήστε Next.

Επιτρεπόμενες εφαρμογές

Κατά τη διάρκεια της διαδικασίας διαμόρφωσης, το McAfee Firewall σκαννάρει το σκληρό δίσκο του υπολογιστή σας για να προσδιορίσει τα προγράμματα που χρησιμοποιούν το Διαδίκτυο. Παραδείγματος χάριν, προγράμματα αυτού του τύπου θα μπορούσαν να συμπεριληφθούν οι μηχανές αναζήτησης Διαδίκτυο, τα προγράμματα ηλεκτρονικού ταχυδρομείου Διαδίκτυο, και το FTP (πρωτόκολλο μεταφοράς αρχείων) πελάτες. Σε αυτήν την οθόνη, θα προσδιορίσετε τα προγράμματα που θα επιτρέψετε να έχουν πρόσβαση στο Διαδίκτυο μέσω του McAfee Firewall.

Για να επιτρέψετε σε συγκεκριμένα προγράμματα να έχουν πρόσβαση στο Διαδίκτυο, κάντε τα εξής:

1. Από τον κατάλογο εφαρμογών που εμφανίζονται σε αυτό, τσεκάρετε στο παράθυρο ελέγχου το αντίστοιχο πρόγραμμα που εσείς θέλετε να έχει πρόσβαση στο Διαδίκτυο.

Πατήστε κλικ στο Search all drivers(αναζήτηση όλων των δίσκων)για να ψάξετε τα χωρίσματα όλου του υπολογιστή σας, λογικούς δίσκους, και φυσικούς σκληρούς δίσκους για τα προγράμματα που επικοινωνούν με το Διαδίκτυο.

Εάν δεν επιτρέπετε σε οποιοδήποτε ή σε όλα τα προγράμματα που εμφανίζονται σε αυτήν την οθόνη να επικοινωνήσουν, θα ειδοποιηθείτε όταν κάποιο θα προσπαθήσει να το κάνει και θα αποφασίσετε ποτέ θα επιτρέψετε την πρόσβαση στο Διαδίκτυο εκείνη τη στιγμή.

2.Πατήστε Finish.

Τι συμβαίνει έπειτα;

Αφότου ολοκληρώσετε τα βήματα που σχετίζονται με το στήσιμο της αρχική σας η διαμόρφωσης , τα ακόλουθα γεγονότα πραγματοποιούνται:

1. Η υπηρεσία του firewall ξεκινά.

2. Εμφανίζεται η αρχική σελίδα του McAfee Firewall.

Τώρα είστε έτοιμοι να χρησιμοποιήσετε το McAfee Firewall!

ΣΗΜΕΙΩΣΗ

Οι προηγούμενες εκδόσεις του McAfee Firewall δεν σας επέτρεπαν να τρέξει ο Βοηθός διαμόρφωσης περισσότερο από μία φορά. Εντούτοις, το McAfee Firewall 4.0 σας επιτρέπει να τρέξετε το βοηθό διαμόρφωσης με τη βοήθεια ενός προσβάσιμου συνδέσμου που βρίσκεται στην αρχική σελίδα του McAfee Firewall.

Η ΑΡΧΙΚΗ ΣΕΛΙΔΑ ΤΟΥ McAfee Firewall

Σχήμα 3-1. Η αρχική σελίδα του McAfee Firewall

Το κύριο παράθυρο του McAfee Firewall είναι το κεντρικό σημείο εισόδων σας σε όλα τα επιμέρους του McAfee Firewall , Στόχοι για προχωρημένους και κοινά χαρακτηριστικά γνωρίσματα. Η διεπαφή του McAfee Firewall εμφανίζει τρεις περιοχές κοινές για όλες τις οθόνες του McAfee Firewall.

Η μπάρα τίτλου και εργαλείων

Μπάρα τίτλου

Η αρχική σελίδα εμφανίζει τα περισσότερα από τα τυποποιημένα στοιχεία των Windows σας, που περιλαμβάνει:

- Η μπάρα τίτλου εμφανίζει το όνομα του προγράμματος που τρέχει τη δεδομένη στιγμή.
- Κλείστε και ελαχιστοποιήστε τα κουμπιά. Η διεπαφή του McAfee Firewall έχει σταθερό μήκος και πλάτος. Δεν μπορείτε να κάνετε επαναφορά μεγέθους στη διεπαφή.

Μπάρα εργαλείων

Η μπάρα εργαλείων εμφανίζει τέσσαρες μηχανές αναζήτησης-όπως κουμπιά που είναι κοινά για όλες τις οθόνες.

- Back(Πίσω).

Πατήστε πίσω για να επιστρέψετε στην τελευταία οθόνη που είχατε δει.

- Home(Αρχική σελίδα). Πατήστε Home για να πάτε στην αρχική σελίδα του McAfee Firewall από οποιασδήποτε οθόνη.
- Net(Επόμενο). Από κοινού με το Back(Πίσω) κουμπί, χρησιμοποιήστε το Next(Επόμενο) για να πατε σε οποιαδήποτε

προηγουμένη οθόνη κατά τη διάρκεια της τρέχουσας session .

- Help(Βοήθεια). Πατήστε τη βοήθεια για να δείτε το δευτερεύον

μενού του.

Ειπωμένου βοηθείας	Επιλέξτε αυτό το στοιχείο για να…
Help on this page	Δείτε την απευθείας σύνδεση βοήθεια για την οθόνη που ήδη βρίσκεστε
Contents and index	Δείτε την απευθείας σύνδεση βοήθεια για το McAfee Firewall
Help on the web	Ξεκινήστε τη μηχανή αναζήτησης και πήγαινε κατευθείαν στη σελίδα βοηθείας του McAfee στη σελίδα McAfeeHelp.com
McAfee at Home on the Web	Ξεκινήστε τη μηχανή αναζήτησης και πήγαινε κατευθείαν στη σελίδα McAfeeHelp.com
About McAfee Firewall	Πληροφορίες έκδοσης σχετικά με το McAfee Firewall.

Πληροφορίες κατάστασης

Ανάλογα με τη διαμόρφωσή σας, η αρχική σελίδα του McAfee Firewall εμφανίζει άλλες χρήσιμες πληροφορίες όπως:

- Κατάσταση του Firewall: Τρέχει ή σταματά. Πατήστε τη σύνδεση κάτω από την κατάσταση για να αρχίσετε ή σταματήστε το McAfee Firewall.
- Ειδοποιήσει αρχικής σελίδας. Εάν υπάρχει μια αναβάθμιση στην έκδοση του McAfee Firewall σας διαθέσιμη για να την κατεβάσει , επιλέξτε αυτήν την εργασία.
- Ο αριθμός προγραμμάτων που επικοινωνούν τη συγκεκριμένη στιγμή. Εάν θέλετε να προσδιορίσετε την επικοινωνία του προγράμματος, επιλέξτε αυτήν την εργασία για να δείτε την τρέχουσα δραστηριότητα.

- Πληροφορίες προειδοποίησης του Firewall. Εάν υπάρχει οποιαδήποτε προειδοποίηση για επικοινωνία, επιλέξτε αυτήν την εργασία για να δείτε το προειδοποιητικό κείμενο.

Ρυθμίσεις της κυκλοφορίας του Διαδίκτυο

Το πλαίσιο ρυθμίσεων της κυκλοφορίας Διαδίκτυο εμφανίζει την τρέχουσα ρύθμιση φιλτραρίσματός σας. Εδώ καθορίζετε εάν θέλετε να τα εμποδίσετε όλα, να τα επιτρέψετε , ή να φιλτράρετε την κυκλοφορία Διαδίκτυο . Για περισσότερες πληροφορίες για αυτές τις ρυθμίσεις , αναφέρονται στον πίνακα 3-1 στη σελίδα 23.

Για να αλλάξετε μια ρύθμιση στην κυκλοφορία του Διαδικτύο, πατήστε απλά την επιθυμητή ρύθμιση. Οι αλλαγές είναι σε πραγματικό χρόνο και άμεσα αποτελεσματικές .

Η Κατάσταση του McAfee Firewall

Αυτή η περιοχή της αρχικής σελίδας εμφανίζει την τρέχουσα κατάσταση του McAfee Firewall. Είτε τρέχει είτε δεν τρέχει.

Εάν η κατάσταση του McAfee Firewall έχει το μήνυμα…	Τότε…
Το McAfee τρέχει…	Πατά stop McAfee Firewall για να απενεργοποιήσετε την προστασία του Firewall
Το McAfee είναι σταματημένο…	Πατήστε Start McAfee Firewall για να ενεργοποιήσετε την προστασία

Όργανο ελέγχου της κυκλοφορίας των δικτύων

Το όργανο ελέγχου κυκλοφορίας δικτύων εμφανίζει μια γραφική απεικόνιση του πραγματικού χρόνου της δραστηριότητα των δικτύων. Το όργανο ελέγχου είναι κωδικοποιημένο δια χρώματος για να σας βοηθήσει να προσδιορίσετε την κανονική κυκλοφορία των δικτύων, ανιχνεύει τη θύρα, και χειρότερα από όλα, τις επιθέσεις.

- Πράσινη ζώνη: Η δραστηριότητα που εμφανίζεται σε αυτήν την ζώνη είναι η κανονική δραστηριότητα των δικτύων. Δεν είναι ασυνήθιστο να δείτε αυτή τη δραστηριότητα να φθάνει στην κίτρινη περιοχή.
- Κίτρινη ζώνη: Αυτό είναι η ζώνη προσοχής. Μπορείτε να δείτε το κείμενο δραστηριότητας για να αναλύσετε τα στοιχεία για αυτήν την κυκλοφορία. Η δραστηριότητα στην κίτρινη ζώνη θα μπορούσε να αντιπροσωπεύσει μια ανίχνευση θυρών.
- Κόκκινη ζώνη: Το κόκκινο αντιπροσωπεύει το χειρότερο επίπεδο δραστηριότητας δικτύων και συνήθως αντιπροσωπεύει μια επίθεση. Μπορείτε να δείτε τις λεπτομέρειες της επίθεσης με την πρόσβαση του κειμένου δραστηριότητας του McAfee Firewall. Εάν η διεύθυνση IP του επιτιθεμένου είναι διαθέσιμη, μπορείτε να προσπαθήσετε να ανιχνεύσετε τον επιτιθέμενο χρησιμοποιώντας τον Οπτικό τμήμα ιχνών McAfee Firewall.

Το πλακάκι στόχου

Το πλακάκι εργασίας εμφανίζει τις συνδέσεις που σας επιτρέπει
Να ξεκινήσετε τις εργασίες του McAfee Firewall και προηγμένες εργασίες . Ανάλογα με τη διαμόρφωσή σας, το πλακάκι εργασίας μπορεί ή δεν μπορεί να εμφανίζει έναν McAfee κατάλογο . Ο κατάλογος McAfee εμφανίζει τις συνδέσεις που σας επιτρέπουν την έναρξη της αρχικής σελίδας οποιουδήποτε Άλλου τρέχοντος προϊόντος McAfee που έχει εγκατασταθεί στον υπολογιστή
σας.

Σχετικά με τις εργασίες

Η έναρξη μιας εργασίας είναι τόσο εύκολη όπως Πατάτε έναν σύνδεσμο. Ο κατάλογος εργασιών σας επιτρέπει
Να ξεκινήσετε τα Σημαντικά τμήματα του McAfee Firewall. Αν και οι εργασίες σας μπορούν να εκτελεστούν, θα ποικίλουν ανάλογα το λειτουργικό σύστημα του υπολογιστή σας και τη διαμόρφωσή του, οι αρχικές εργασίες περιλαμβάνουν:

- Control Intranet Programs: Αυτή η εργασία σας επιτρέπει να εμποδίσετε ρητά ή να επιτρέψτε συγκεκριμένα προγράμματα να έχουν πρόσβαση στο Διαδίκτυο.
- View Network Activity :Επιλέξτε αυτήν την εργασία για να δείτε τη δραστηριότητα του δικτύου σε πραγματικό χρόνο και για να δείτε το κείμενο της τρέχουσας δραστηριότητάς σας.
- Set Alert Preferences: Επιλέξτε πώς θέλετε το McAfee Firewall να σας ειδοποιεί όταν μια πιθανή παραβίαση ασφάλειας εμφανίζεται.
- Set up Home Networking: Οι βοήθειες κάνουν την προστασία καθιέρωσης για το σας PC που μοιράζονται μια σύνδεση με το Διαδίκτυο ένα αεράκι.
- Perform a security check:Αυτή η εργασία επιτρέπει σε σας να ξεκινήσετε τη διαδικασία του ελέγχου ασφάλειας του McAfee Firewall.
- Set startup options:Επιλέξτε πώς θέλετε να ξεκινάει το McAfee Firewall.
- Configuration assistant: Αυτή η εργασία ξεκινά το βοηθό διαμόρφωσης.

Σχετικά με τις προηγμένες εργασίες

Παρόμοιος με τον αρχικό κατάλογο εργασίας , ο προηγμένος κατάλογος εργασίας μπορεί να ποικίλει ανάλογα με την έκδοση των Windows, τη διαμόρφωσή του, και άλλο λογισμικό που μπορεί να έχει εγκατασταθεί στον υπολογιστή σας.

Οι προηγμένοι εργασίες του McAfee Firewall περιλαμβάνουν:

- Advanced options and logging: Επιλέξτε αυτόν την εργασία για να διαμορφωθούν οι αμυντικοί μηχανισμοί επίθεσης ,για να εγκατασταθεί η αυτόματη διαμόρφωση των κανόνων φιλτραρίσματος , και να προσδιοριστεί ο τύπος κυκλοφορίας που θέλετε να καταγράψετε.
- Configure network adapters: Επιλέξτε αυτήν την εργασία για να δείτε τον τρέχων προσαρμοστεί δικτύων και διαμορφώστε τις ρυθμίσεις επικοινωνίας τους.
- Intrusion detection settings: Επιλέξτε αυτήν την εργασία για να διαμορφώσετε πώς θέλετε το McAfee Firewall να αποκριθεί όταν ανιχνεύει μια επίθεση.
- Block IP address: Εάν υπάρχει μια συγκεκριμένη διεύθυνση IP που θέλετε να εμποδίσετε στο να έχει πρόσβαση στον υπολογιστή σας, ή, εάν υπάρχει μια διεύθυνση IP που είναι ήδη αυτήν την περίοδο μπλοκαρισμένη και θέλετε να την επιτρέψετε, επιλέξτε αυτήν την εργασία.
- Set up password: Αυτή η εργασία σας βοηθά για να προστατεύσετε τις ρυθμίσεις του McAfee Firewall σας με την ασφάλεια κωδικού πρόσβασης.

- Άλλες εργασίες : Επιλέξτε αυτήν την εργασία για να σας πλοηγήσει σε μια οθόνη που σας επιτρέπει να ξεκινήσετε τα κοινά χαρακτηριστικά γνωρίσματα του McAfee Firewall.

Σχετικά με τον κατάλογο του McAfee

Ο κατάλογος του McAfee εμφανίζει τις συνδέσεις για να αρχίσει η αρχική σελίδα σε οποιοδήποτε άλλο πρόγραμμα που υποστηρίζει προγράμματα McAfee.

ΑΛΛΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΓΝΩΡΙΣΜΑΤΑ ΤΟΥ McAfee Firewall

McAfee Firewall settings security check

Εξετάζει τις ρυθμίσεις ασφάλειας των Firewall σας, επιτρέποντας σε σας να αποκαταστήσετε πιο αδύνατες ρυθμίσεις πρώτου οι χάκερ προσπαθήσουν να τα εκμεταλλευτούν. Ο έλεγχος ασφάλειας των ρυθμίσεων του MCA Firewall flags και προτείνει αλλαγές για να σας βοηθήσει να κρατήσετε το καθορισμένο σύστημα σας σε βέλτιστη ασφάλεια.

Εάν ο έλεγχος ασφάλειας ανιχνεύει ένα ζήτημα, πατήστε Fix και το McAfee Firewall σας βοήθα για να αναλύσετε και να διορθώστε τα πιθανά προβλήματα.

Home Networking Wizard

Οι βοήθειες φτιάχνουν προστασία για τα PC σας που μοιράζονται μια σύνδεση με το Διαδίκτυο ένα αεράκι, που παρέχει τους χρήσιμους μάγους για να σας ‘’περπατήσει’’ μέσω της διαδικασίας.

Όλα τα μέσα δικτύωσης και το υλικό (όπως τα καλώδια και οι προσάρμοσες δικτύων)πρέπει να εγκαταστίθονται σε κάθε υπολογιστή ώστε αυτός ο μάγος να τα εντοπίζει στους υπολογιστές σας.

Password protection

Αποτρέψτε άλλους από το να πειράξουν τις ρυθμίσεις των firewall σας κλειδώνοντας την πρόσβαση σε αυτούς με την ασφάλεια του κωδικού πρόσβασης. Επίσης οι βοήθειες κρατούν την προστασία του firewall σας ασφαλή παρεμποδίζοντας να κλείσει το firewall χωρίς να βάλετε τον κωδικό πρόσβαση σας .

Σχετικά με την οπτική ανίχνευση

Η οπτική ανίχνευση είναι ένα εργαλείο του διαδίκτυο για πολλές χρήσεις που χρησιμοποιείται για την ανεύρεση των πληροφοριών και προβλήματα σύνδεσης . Στο απλούστερο επίπεδο η οπτική ανίχνευση σας παρουσιάζει πώς τα πακέτα (στοιχεία) παίρνουν από το σας υπολογιστής σε έναν άλλο υπολογιστή στο διαδίκτυο. Βλέπετε όλους τους κόμβους (εξοπλισμός των διάφορων τύπων στο διαδίκτυο που περνά την κυκλοφορία) μεταξύ του υπολογιστής σας και του στόχου ανίχνευσης.

Υπάρχουν πολλές καταστάσεις όπου χρειάζεστε αυτές τις πληροφορίες. Η οπτική ανίχνευση είναι ένα χρήσιμο εργαλείο όταν έχετε προβλήματα με τις συνδέσεις ή απλώς επαληθεύετε ότι όλα λειτουργούν ΕΝΤΑΞΕΙ. Υπάρχει επίσης ένας πλούτος πληροφοριών που παρουσιάζονται από την οπτική ανίχνευση, συμπεριλαμβανομένων των ιδιοκτητών περιοχών, σχετικές θέσεις, και σε πολλές περιπτώσεις, τη θέση των κόμβων.

Εκτός από τη χρησιμοποίηση της οπτικής ανίχνευσης για να ψάξετε τα αδύνατα σημεία σε μια σύνδεση μπορείτε να χρησιμοποιήσετε το παρακάτω για να:

- Ανακαλύψτε ποτέ δεν μπορείτε να φθάσετε σε μια περιοχή λόγω μιας αποτυχίας στον Παροχές υπηρεσιών Διαδίκτυο (ISP) ή περαιτέρω μέσα στο Διαδίκτυο
- Καθορίστε το σημείο μιας αποτυχίας δικτύων που σας αποτρέπει από το να μπείτε σε ένα ισόχωρο.
- Καθορίστε τη θέση των περιοχών και των χρηστών τους, αποκαλύπτοντας τους ιδιοκτήτες του μιας περιοχής , και βοηθείστε στην ανίχνευση της προέλευσης των ανεπιθύμητων μηνυμάτων ηλεκτρονικού ταχυδρομείου («spam»).
- Πάρτε τα λεπτομερή στοιχεία επαφής για τις περιοχές όλες πέρα από όλον τον κόσμο (όπου είναι διαθέσιμα)

Πώς να ξεκινήσετε την οπτική ανίχνευση

Μπορείτε να ξεκινήσετε την οπτική ανίχνευση άμεσα από τις επιλογές έναρξης παραθύρων. Μπορείτε επίσης αν την ξεκινήσετε από την οθόνη λεπτομερής δραστηριότητας του McAfee Firewall, ο φραγμός Πλαίσιο διαλόγου IP, και εάν επιτίθεστε, από το δίσκο του συστήματος των Windows υπερεμφανιζόμενο ανακοίνωση.

Για περισσότερες πληροφορίες για την οπτική ανίχνευση, παρακαλώ αναφερθείτε στην σε απευθείας σύνδεση βοήθεια για την Οπτική Ανίχνευση.

Δ.ΔΙΑΜΟΡΦΩΣΕΙΣ ΤΟΥ McAfee Firewall

Επισκόπηση

Η διαμόρφωση του McAfee Firewall διαιρείται σε δύο ταξινομήσεις – εφαρμογή (πρόγραμμα) και σύστημα. Με την εγκατάσταση, ένα βασικό σύνολο κανόνων για τις υπηρεσίες συστημάτων όπως ICMP, το DHCP και ARP εγκαθίστανται (αυτές είναι εξεταζόμενες ρυθμίσεις προεπιλογής).

Αφ' ενός, η ταξινόμηση προγραμμάτων είναι εξατομικευμένη. Όποτε εσείς τρέξετε ένα νέο πρόγραμμα που προσπαθεί να επικοινωνήσει μέσω του Διαδίκτυο, το McAfee Firewall θα προτρέψει και θα σας ρωτήσει εάν θέλετε να εμπιστευθείτε το πρόγραμμα ή όχι.

Παραδείγματος χάριν, χρησιμοποιώντας τον Internet Explorer, εισάγετε μια διεύθυνση Διαδίκτυο ή ένα URL(δηλ.: http://www.mcafee-at-home.com) στην μπάρα διευθύνσεων της μηχανής αναζήτησης σας και πιέστε ENTER. Ο Internet Explorer θα προσπαθήσει να συνδεθεί με εκείνο το URL πέρα από Διαδίκτυο. Την πρώτη φορά που θα το κάνετε αυτό, το McAfee Firewall θα σας ρωτήσει εάν «εμπιστεύεστε» τον Internet Explorer. Εάν λετε «ναι» το MCA Firewall σημειώνει ότι δώσατε πρόσβαση στον Internet Explorer και όποτε θα χρησιμοποιείτε τον Internet Explorer στο μέλλον, το McAfee θα επιτρέψει την κυκλοφορία του.

Δεδομένου ότι επιτρέπετε τα προγράμματα για να χρησιμοποιούν το Διαδίκτυο, το McAfee Firewall «μαθαίνει» τους κανόνες που δημιουργείτε για το πρόγραμμα και τους σώζετε για μελλοντική χρήση. Εάν ένα πρόγραμμα δούρειων ίππων προσπαθεί να επικοινωνήσει έξω από τον υπολογιστή σας, το McAfee Firewall θα τα προτρέψει επίσης σε εσάς για το αν τους εμπιστεύεστε ή όχι, και την απόφαση για να εμποδιστεί το πρόγραμμα αυτό από την επικοινωνία είναι εύκολο και στιγμιαίο.

Διαμόρφωση προγράμματος

Κατά τη διάρκεια της πρώτης προσπάθειάς σας να ξεκινήσετε το McAfee Firewall , Ο βοηθός διαμόρφωσης σας ζήτησε να προσδιορίσετε τα προγράμματα στα οποία θέλετε να επιτρέψετε να επικοινωνήσουν. Εκείνη τη στιγμή, το McAfee Firewall δημιούργησε ένα σύνολο προεπιλογής για κανόνες επικοινωνίας για τα προγράμματα (εφαρμογές), χαρακτηρισμένα για να μπορούν να επικοινωνήσουν.

Βασισμένος στον τύπο προγράμματος, παραδείγματος χάριν, Internet Browsers, ηλεκτρονικό ταχυδρομείο, FTP, IRC,και το αρχείο που μοιράζεται τα προγράμματα, το McAfee Firewall προσδιορίζει τον τύπο του προγράμματος και δημιουργεί ένα σύνολο προεπιλογής κανόνων επικοινωνίας για κάθε πρόγραμμα που έχει μέσα ο υπολογιστής σας. Αυτό είναι, είτε να μπλοκάρει, είτε να επιτρέψει, είτε να φιλτράρει ενός προγράμματος τις προσπάθειες για επικοινωνία μέσω του Διαδίκτυο.

Μηνύματα ειδοποιήσεων για επικοινωνίας του Firewall

Το μήνυμα ειδοποίησης για επικοινωνία του MCA Firewall εμφανίζει εάν το αναγνωρισμένο πρόγραμμα προσπαθεί να επικοινωνήσει. Υπάρχουν διάφορα σενάρια που θα μπορούσε να προκαλέσει ένα πρόγραμμα το οποίο δεν είναι αναγνωρισμένο.

- Εάν εγκαθιστάτε ένα πρόγραμμα που επικοινωνεί μέσω του Διαδίκτυο κατόπιν της εγκατάστασης του McAfee Firewall, με την πρώτη προσπάθεια του προγράμματος να επικοινωνήσει θα εμφανιστεί ένα μήνυμα ειδοποίησης.
- Αν και ο βοηθός διαμόρφωσης εκτελεί μια λεπτομερή ανάλυση των προγραμμάτων του υπολογιστή σας που χρησιμοποιούν το Διαδίκτυο για να επικοινωνήσουν, αυτό μπορεί να μην είναι σε θέση να προσδιορίσει όλα τα προγράμματα του υπολογιστή σας που χρησιμοποιούν το Διαδίκτυο για να επικοινωνήσουν.

Εάν ένα αναγνωρισμένο πρόγραμμα προσπαθεί να επικοινωνήσει, το μήνυμα ειδοποίησης που θα προκύψει σας ζητά να επιλέξετε μια από τις ακόλουθες επιλογές:

- Όχι, αρνείται αυτή τη στιγμή: Εμποδίζει το παρών πρόγραμμα και όλες τις μελλοντικές προσπάθειες του να επικοινωνήσουν. Το ενεργό πρόγραμμα προστίθεται στον εμπιστευμένο κατάλογο των προγραμμάτων με μια επιτρεπόμενη κατάσταση «μπλοκαρισμένος.»
- Ναι, επιτρέψτε αυτή τη φορά: Η ενεργός προσπάθεια να επικοινωνήσει επιτρέπεται. Το πρόγραμμα δεν προστίθεται στον εμπιστευμένο κατάλογο των προγραμμάτων.
- Εάν αναγνωρίζετε το πρόγραμμα και δεν θέλετε να λάβετε στο μέλλον οποιαδήποτε ειδοποίηση για αυτό το πρόγραμμα, τσεκάρετε το I recognize this program check box.

ΣΗΜΕΙΩΣΗ

Εάν επιτρέψατε ή εμποδίσατε ένα πρόγραμμα την πρώτη φορά που σας πρότρεψε, το McAfee Firewall παρέχει σε σας την ευελιξία να αλλαχτεί αυτή η ρύθμιση και να μπλοκάρετε ή να επιτρέψετε να επικοινωνήσει οποιαδήποτε στιγμή στο μέλλον. Καθώς βγαίνετε από το McAfee Firewall , οι ρυθμίσεις σας σώζονται και θα είναι οι ίδιες την επόμενη φορά που θα το τρέξετε.

Αλλάζοντας την επιτρεπόμενη κατάσταση ενός προγράμματος

Το McAfee Firewall ελέγχει την κυκλοφορία του Διαδίκτυο για να δει ποια προγράμματα είναι σε επικοινωνία. Ανάλογα με τις ρυθμίσεις σας, θα επιτρέψει, θα εμποδίσει, ή θα φιλτράρει την προσπάθεια ενός προγράμματος να επικοινωνήσει.

Εάν έχετε επιλέξει «να επιτραπούν όλα» τα προγράμματα για να επικοινωνούν μέσω του firewall σας, κατόπιν όλα τα προγράμματα που εγκαθίστανται στον υπολογιστή σας μπορούν να επικοινωνήσουν.

Για να δείτε και να διαμορφώσετε τον τρέχοντα κατάλογο των εμπιστευμένων προγραμμάτων

1. Από το Task List, επιλέξτε Control Internet Programs.

2. Επιλέξτε εκείνο το πρόγραμμα του οποίου οι ρυθμίσεις φιλτραρίσματος επιθυμείτε να διαμορφώσετε (ή πατήστε Browse για να προσθέσετε ένα πρόγραμμα στον κατάλογο).

Επιλέξτε μια από τις ακόλουθες επιλογές:

- Φιλτράρετε την πρόσβαση αυτού του προγράμματος στο Διαδίκτυο.
- Επιτρέψτε αυτό το πρόγραμμα για να έχει πλήρης μη φιλτραρισμένη πρόσβαση στο Διαδίκτυο.
- Εμποδίστε αυτό το πρόγραμμα από την πρόσβαση του Διαδίκτυο.

4. Για να προστεθεί ένα πρόγραμμα στον κατάλογο, πατήστε Add και browse για να επιλέξει το πρόγραμμα που θέλετε να προστεθεί. Για να αφαιρέσετε ένα πρόγραμμα από τον κατάλογο, επιλέξτε το πρόγραμμα που θέλετε να αφαιρέσετε και πατήστε Remove.

5.Πατήστε Apply.

Πώς να τυποποιήσουμε τους κανόνες φιλτραρίσματος για ένα συγκεκριμένο πρόγραμμα

Για όλα τα προγράμματα που υποδεικνύονται ως «φιλτραρισμένα,» το McAfee Firewall παρέχει στους power users την ευελιξία να δημιουργήσουν ένα σύνολο από τυποποιημένους κανόνες φιλτραρίσματος για κάθε φιλτραρισμένο πρόγραμμα.

ΣΗΜΕΙΩΣΗ

Το κουμπί Customize γίνεται προσβάσιμο εάν επιλέξετε την επιλογή Filter this program's access to the Internet.

Για να δημιουργήσετε έναν τυποποιημένο κανόνα φιλτραρίσματος

1 από την οθόνη ελέγχου των προγραμμάτων Διαδίκτυο ,επιλέξτε το πρόγραμμα για το οποίο θέλετε να δημιουργήσετε έναν τυποποιημένο κανόνα φιλτραρίσματος.

2.Επιλέξτε το κουμπί Filter this program's access to the Internet.

3.Πατήστε Customize.

Εάν το πρόγραμμα αυτήν την περίοδο διατηρεί ένα σύνολο προεπιλογής κανόνων που δημιουργούνται από το McAfee Firewall, έπειτα εμφανίζεται ένας διάλογος Customize filtering rules. Εάν το πρόγραμμα δεν διατηρεί ένα σύνολο προεπιλογής κανόνων, κατόπιν εμφανίζει ένα διάλογο ¨What do you want this filtering rule to do?"

Αναφέρεται στις οδηγίες που εμφανίζονται στο Custom Filtering rules για να ολοκληρώσει τη τυποποιημένη διαμόρφωση σας.

Πίνακας 4-2. Κουμπιά διάλογου για να τυποποιήσετε τους κανόνες φιλτραρίσματος

Κουμπί	Περιγραφή
Add	Πατήστε Add για να προσθέσετε έναν καινούριο κανόνα και να εμφανιστεί ο διάλογος What do you want this rule to do?
Remove	Πατήστε Remove για να αφαιρέσετε έναν κανόνα από το επιλεγμένο πρόγραμμα Προσοχή:δεν υπάρχει Undo
Edit	Πατήστε Edit για να βελτιώσετε τον κανόνα του φιλτραρίσματος
Restore	Πατήστε Restore για να επαναφέρετε τους προκαθορισμένους κανόνες για το επιλεγμένο πρόγραμμα Σημείωση: Εάν αίρετε ακούσια έναν κανόνα, πατήστε αυτό το κουμπί για να επαναφέρετε τους προεπιλεγμένους κανόνες για το επιλεγμένο πρόγραμμα

OK	Πατήστε OI για να κλείσετε το διάλογο Customize Filtering Rules και αποθηκεύστε τις αλλαγές σας
Cancel	Πατήστε Cancel για να κλείσετε το διάλογο Customize Filtering Rules χωρίς να αποθηκεύσετε τις αλλαγές σας

Αρχικές λειτουργίες

Από τον κατάλογο αρχικών λειτουργιών που εμφανίζεται στο διάλογο Customize Filtering Rules, μπορείτε να επιλέξετε ένα από τα εξής:

Πίνακας 4-3. Αρχικές λειτουργίες

Μπορείτε να επιλέξετε για να…	Από…
Επιτρέπετε την επικοινωνία…	• Protocol(πρωτόκολλο) • Local port(τοπική θύρα) • Remote port(απομακρυσμένη θύρα)
Μπλοκάρετε την επικοινωνία…	• IP address • Domain name • direction

Όροι βελτίωσης

Αφότου επιλέξετε την αρχική λειτουργία για τον κανόνα, μπορείτε περαιτέρω να βελτιώσετε τον κανόνα τσεκάροντας στα αντίστοιχα κουτάκια για οποιαδήποτε ή όλα τα χαρακτηριστικά της επικοινωνίας :

Με…	Χρησιμοποιώντας…
• direction • domain names • IP addresses	• protocols • remote ports • local ports

Για να προσαρμόσετε τον όρο καθαρισμού, πατήστε [click here to select].Εξαρτώμενος επάνω στα χαρακτηριστικά επικοινωνίας που επιλέγονται, ποικίλοι διάλογοι και κείμενα εμφανίζονται. Παραδείγματος χάριν, εάν ένας τυποποιημένος κανόνας δηλώνει«Block this program from communicating and the IP address is» έπειτα ένας Add/Edit κανόνας κειμένου εμφανίζεται επιτρέποντας σας να εισάγετε μια διεύθυνση IP.
Ομοίως, εάν θέλετε να εμποδίσετε ένα πρόγραμμα από το να επικοινωνήσει από το πρωτόκολλο, ένας διάλογος Edit Protocols εμφανίζεται.

Για να σώσετε τις αλλαγές σας, πατήστε OK.

Διαμόρφωση συστημάτων

Το λειτουργικό σύστημα του υπολογιστή σας εκτελεί πολλούς τύπους επικοινωνίας δικτύων χωρίς να αναφερθεί άμεσα σε σας. Το McAfee Firewall ρητά σας αφήνει να επιτρέψτε ή να εμποδίστε διαφορετικές λειτουργίες συστημάτων. Οι ρυθμίσεις μπορούν να είναι διαφορετικές για κάθε δίκτυο η συσκευή, εφ'όσον ένας υπολογιστής, παραδείγματος χάριν, μπορεί να συνδεθεί με ένα εσωτερικό δίκτυο καθώς επίσης και έχοντας μια σύνδεση διεπιλογών στο Διαδίκτυο.

Χρησιμοποιήστε τα κατωτέρω βήματα για να ελέγξετε τις ρυθμίσεις των συστημάτων σας.

1. από το Advanced Task List, επιλέξτε Configure network adapters.
2. Από την οθόνη Configure Network Adapter Settings, επιλέξτε τον προσαρμοστεί που θέλετε να διαμορφώσετε και πατήστε Adapter Settings για να δείτε ή να αλλάξετε τις ιδιότητες του συγκεκριμένου προσαρμοστεί.

Αποτέλεσμα: Το φύλλο ιδιοτήτων για τις επιλεγμένες προσαρμοστώ δικτύων εμφανίζεται.

Μπορείτε έπειτα να επιλέξετε ώστε να επιτρέψετε ή να εμποδίσετε το NetBIOS άνω του TCP, Identification, ICMP, ARP, DHCP, RIP, PPTP και άλλα πρωτόκολλα (IP και μη-IP).

Πίνακας 4-4. Ρυθμίσεις προεπιλογής για τη δραστηριότητα συστημάτων

Τύπος δραστηριότητας συστημάτων	Περιγραφή
NetBios over TCP: Μπλοκαρισμένο	Αυτό θα εμποδίσει όλη τη δραστηριότητα κοινής χρήσης αρχείων άνω του TCP καθώς και τις UDP εκπομπές. Το σύστημά σας δεν θα εμφανιστεί στον οποιοδήποτε «γειτονιά δικτύων» και οι δικές τους δεν θα εμφανιστούν στις δικές σας. Εάν το σύστημά σας είναι διαμορφωμένο για να υποστηρίζει NetBIOS πέρα από άλλα πρωτόκολλα, όπως το IPX ή το NetBEUI, έπειτα η διανομή αρχείων μπορεί να επιτραπεί εάν «τα πρωτόκολλα μη-IP» επιτρέπονται (δείτε «άλλα Πρωτόκολλα» κατωτέρω).
Identification: Μπλοκαρισμένο	Αυτή η υπηρεσία απαιτείται συχνά όταν παίρνεις email και απαιτείται από τους περισσότερους κεντρικούς υπολογιστές IRC.
ICMP: Μπλοκαρισμένο	Αυτό το πρωτόκολλο συχνά δεν

	χρησιμοποιείται σωστά ως μέθοδος το να σπάει συνδέσεις δικτύων των ανθρώπων (ειδικά σε IRC).
ARP: Μπλοκαρισμένο	Είναι ένα απαραίτητο πρωτόκολλο Ethernet και δεν είναι γνωστό ως μια απειλή.
DHCP: Επιτρέπεται αν το σύστημα σας χρησιμοποιεί DHCP	Το πρόγραμμα κοιτάζει στο αρχείο των συστημάτων σας που βλέπει εάν μια από τις συσκευές δικτύων σας χρησιμοποιεί το DHCP. Σε αυτή την περίπτωση, το DHCP επιτρέπεται για όλες τις συσκευές. Εάν όχι, έπειτα είναι μπλοκαρισμένο για όλες τις συσκευές. Εάν έχετε περισσότερες της μιας συσκευές δικτύων και κάποια χρησιμοποιεί το DHCP, πρέπει να ελέγξτε το DHCP που έχει εγκατασταθεί για κάθε συσκευή και επιτρέψτε μόνο για τη συσκευή που το χρησιμοποιεί (συχνότερα καλώδιο ή ADSL διαποδιαμορφωτές και μερικά εσωτερικά δίκτυα, όχι για διεπιλογή).
RIP:Μπλοκαρισμένο	Επιτρέψτε το RIP αν ο διαχειριστής σας ή ο ISP σας το συμβουλεύει.
PTTP:Μπλοκαρισμένο	Αυτό πρέπει να αλλαχτεί μόνο από το διοικητή.
Άλλα πρωτόκολλα:Μπλοκαρισμένα	Εάν είστε σε ένα δίκτυο IPX, πρέπει να επιτρέψετε τα «πρωτόκολλα μη-IP». Εάν χρησιμοποιείτε PPTP, πρέπει να επιτρέψτε τα «άλλα πρωτόκολλα IP». Ρωτήστε το διαχειριστή δικτύου σας πριν να κάνετε οποιαδήποτε αλλαγή εδώ.

Ε.ΣΥΣΤΗΜΑ ΑΝΙΧΝΕΥΣΗΣ ΕΠΙΘΕΣΗΣ ΤΟΥ McAfee Firewall

Σχετικά με την ανίχνευση επίθεσης

Αντίθετα από άλλα εργαλεία ανίχνευσης παρεισφρήσεις, το McAfee Firewall είναι ένα ισχυρό σύστημα ανίχνευσης της επίθεσης(IDS) το οποίο είναι απλό να διαμορφωθεί και να ενεργοποιηθεί. Αντί να απαιτεί στους χρήστες να μάθουν και να καταλάβουν ένα σύνθετο σύνολο επιθέσεων για να χτίσουν τις δικές τους αμυντικές γραμμές ενάντια στις επιθέσεις, η ομάδα ανάπτυξης του McAfee Firewall δημιούργησε ένα εργαλείο που, όταν ενεργοποιείται με το πάτημα ενός κουμπιού, ανιχνεύει κοινούς τύπους επίθεσης και ύποπτη δραστηριότητα.

Οι μη προστατευμένοι υπολογιστές μπορούν να καταστραθούν θύματα. Παραδείγματος χάριν, οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν μια θύρα ανίχνευσης TCP για να ανακαλύψουν ποιες υπηρεσίες τρέχετε στο μηχάνημα σας. Μόλις ολοκληρωθεί αυτό, θα προσπαθήσουν να συνδεθούν με εκείνες τις υπηρεσίες και να επιτεθούν στον υπολογιστής σας. Εάν ο επιτιθέμενος ανακαλύψει ότι τρέχετε ένα TELNET, FTP, ή έναν κεντρικό υπολογιστή δικτύου, ο επιτιθέμενος μπορεί να δοκιμάσει κάθε μια από τις θύρες του υπολογιστή σας διαδοχικά, από 1 έως 65535, μέχρι να βρεθεί μια ανοικτή θύρα βρίσκεται με την οποία μπορούν να συνδεθούν.

Το χαρακτηριστικό γνώρισμα IDS του McAfee Firewall ψάχνει για συγκεκριμένα σχέδια κυκλοφορίας χρησιμοποιούμενα από επιτιθέμενους. Το McAfee Firewall ελέγχει κάθε πακέτο που λαμβάνει το μηχάνημα σας για να ανιχνεύσει την ύποπτη ή γνωστή κυκλοφορία επίθεσης. Παραδείγματος χάριν, εάν το McAfee Firewall βλέπει τα πακέτα ICMP, αναλύει εκείνα τα πακέτα για ύποπτα σχέδια κυκλοφορίας συγκρίνοντας την κυκλοφορίας του ICMP ενάντια στα γνωστά σχέδια επίθεσης. Όταν το McAfee Firewall ταιριάζει πακέτα με ένα γνωστό σχέδιο επίθεσης, το λογισμικό παράγει ένα γεγονός για να σας προειδοποιήσει για μια πιθανή παραβίαση ασφάλειας.

Όταν η ανίχνευση επίθεσης είναι ανοικτή, η κυκλοφορία ελέγχεται από το σύστημα ανίχνευσης επιθέσεως . Όταν η ανίχνευση επιθέσεως είναι ενεργή και το McAfee Firewall ανιχνεύει μια επίθεση, εσείς μπορείτε να εμποδίσετε την περαιτέρω επικοινωνία από μια IP διεύθυνση ενός υποπτευόμενου μηχανήματος αόριστο ή για ένα συγκεκριμένο χρονικό διάστημα. Όταν μια επίθεση ανιχνεύεται, το McAfee Firewall σας προειδοποιεί με μια ανακοίνωση του δίσκου συστήματος των Windows.

ΣΗΜΕΙΩΣΗ

Επειδή το McAfee Firewall αναλύει τα πακέτα και ερευνά σχέδια των πακέτων που προσδιορίζουν τους συγκεκριμένους τύπους επιθέσεων, αυτό το χαρακτηριστικό γνώρισμα μπορεί να οδηγήσει σε έναν πολύ αντίκτυπο προσβολών της απόδοσης του μηχανήματος σας.

Πώς να διαμορφώσετε το σύστημα ανίχνευσης επίθεσης

Χρησιμοποιήστε τα κατωτέρω βήματα για να διαμορφώσετε το σύστημα της ανίχνευσης της επίθεσης του McAfee Firewall :

1 Από την αρχική σελίδα του McAfee Firewall, πατήστε Advanced Tasks.

2 Από τον κατάλογο Advanced Tasks, επιλέξτε Instruction detection settings.

Αναφερθείτε στις οδηγίες που επιδεικνύονται στην οθόνη Configure Intrusion Detection Settings για να ολοκληρώσετε αυτήν την εργασία.

Κοινές επιθέσεις που αναγνωρίζονται από IDS

Ο ακόλουθος πίνακας απαριθμεί τις επιθέσεις που αναγνωρίζονται από το McAfee Firewall's IDS, μια περιγραφή κάθε επίθεσης, και ο παράγοντας κινδύνου που ορίζεται σε κάθε επίθεση.

Επίθεση	Περιγραφή	Παράγοντας κίνδυνου
1234	Επίσης γνωστός ως επίθεση Flushot, ένας επιτιθέμενος στέλνει ένα μεγάλο μεταλλικό θόρυβο πακέτου που το λογισμικό δικτύωσης δεν μπορεί να χειριστεί. Συνήθως, οι υπολογιστές κρεμούν ή επιβραδύνουν. Εάν μια συνολική στήριξη εμφανίζεται, τα μη σωσμένα στοιχεία μπορεί να χαθούν.	Μεσαίος
Back Orifice	Το Back Orifice είναι ένα πρόγραμμα πίσω πόρτων για τα Windows9x που έχει γραφτεί από μια ομάδα που καλούνται the Cult of the Dead Cow. Αυτή η πίσω πόρτα επιτρέπει την εξ' αποστάσεως πρόσβαση στο μηχάνημα με μία φορά εγκατάσταση, επιτρέποντας στον εφαρμοστή να τρέξει εντολές, να πάρει πυροβολισμούς οθόνης, να τροποποιήσει το ληξιαρχείο, και εκτελέσει άλλες διαδικασίες. Τα προγράμματα πελατών για να έχουν πρόσβαση στο Back Orifice είναι διαθέσιμα για Windows και Unix.	Υψηλός
Bonk	Σχεδιάστηκε με σκοπό να εκμεταλλευτεί ένα λάθος εφαρμογής στο πρώτο patch του Teardrop που κυκλοφόρησε από τη Microsoft, αυτή η επίθεση είναι βασικά ένα Windows-	Υψηλός

	συγκεκριμένη παραλλαγή της αρχικής επίθεσης του Teardrop.	
Fraggle	Αυτή η επίθεση είναι μια παραλλαγή UDP της επίθεσης Smurf. Με την αποστολή ενός πλαστογραφημένου UDP πακέτου σε μια συγκεκριμένη θύρα σε μια διεύθυνση broadcast, συστήματα στο δίκτυο«ενισχυτών» θα αποκριθούν στο μηχάνημα στόχων είτε με UDP απάντηση είτε με ένα ΑΠΡΟΣΙΤΟ πακέτο ICMP. Αυτή η πλημμύρα από αποτελέσματα εισερχόμενων πακέτων σε μια άρνηση της επίθεσης υπηρεσιών ενάντια στο μηχάνημα στόχων.	Υψηλός
IP Spoofing	Η IP Spoofing περιλαμβάνει την αποστολή των στοιχείων με μια πλαστογραφημένη επιστροφή IP διεύθυνσης. Δεν υπάρχει τίποτα ευγενώς επικίνδυνο για να εξαπατηθεί μια διεύθυνση πηγής IP, αλλά αυτή η τεχνική μπορεί να χρησιμοποιηθεί από κοινού με άλλες για να πραγματοποιήσει τις επιθέσεις TCP, ή για να κρύψει την πηγή άρνησης της υπηρεσίας επιθέσεων (SYN flood,PING flood κ.λπ.)	Μεσαίος
Jolt	Η απομακρυσμένη άρνηση της Επίθεσης υπηρεσιών χρησιμοποιεί τα ειδικά επεξεργασμένα τεμάχια πακέτων ICMP. Μπορεί να προκαλέσουν επιβραδύνσεις ή συντριβές στα συστήματα στόχων.	Υψηλός
Jolt 2	Μια απομακρυσμένη επίθεση της άρνηση υπηρεσιών (DOS) παρόμοιας με Jolt που χρησιμοποιεί ειδικά επεξεργασμένα τεμάχια πακέτων ICMP ή UDP.Μπορει να προκαλέσουν επιβραδύνσεις ή συντριβές στα συστήματα στόχων.	Υψηλός
Land	Αυτή η επίθεση εκτελείται με το να στέλνει ένα πακέτο TCP σε μια τρέχων υπηρεσία στον οικοδεσπότη στόχων, με μια διεύθυνση προέλευσης του ίδιου οικοδεσπότη. Το πακέτο TCP είναι ένα πακέτο SYN,που χρησιμοποιείται για να εγκαταστήσει μια νέα σύνδεση, και στέλνεται από την ίδια θύρα πηγής TCP με τη θύρα προορισμού. Όταν γίνεται αποδεκτό από τον οικοδεσπότη στόχων, αυτό το πακέτο προκαλεί έναν	Υψηλός

	βρόχο μέσα στο λειτουργικό σύστημα, ουσιαστικά κλειδώνοντας το σύστημα.	
Nestea	Αυτή η επίθεση στηρίζεται σε ένα λάθος στον υπολογισμό των μεγεθών κατά τη διάρκεια της επανασυναρμολόγησης των τεμαχίων του πακέτου. Στη ρουτίνα επανασυναρμολόγησης των τρωτών συστημάτων, υπήρξε μια αποτυχία στο να μετρήσει το μήκος στο τομέα της IP επικεφαλίδας. Με το να στείλει προσεκτικά τα επεξεργασμένα πακέτα σε ένα τρωτό σύστημα, είναι δυνατόν να συντρίψει το στόχο.	Υψηλός
NetWare	Μια επίθεση άρνησης υπηρεσιών (DOS) προκαλεί συνήθως τους υπολογιστές με ένα λειτουργικό σύστημα βασισμένο στα Windows NT για να συντρίψει. Αν και η επίθεση δεν είναι συνήθως επιβλαβής στον ίδιο τον υπολογιστή, στοιχεία από τρέχουσες εφαρμογές σίγουρα θα χαθούν.	Υψηλός
O'Hare	Μια επίθεση άρνησης υπηρεσιών (DOS) προκαλείται με την αποστολή ενός μοναδικού πακέτου δομής στον υπολογιστή σας. Τα αποτελέσματα αυτών των επιθέσεων μπορούν να ποικίλουν από μια πλήρης συντριβή συστημάτων, αυξανόμενο φορτίο στη CPU, ή στιγμιαίες καθυστερήσεις, ανάλογα με τη διαμόρφωση του υπολογιστή σας. Αυτό έχει επιπτώσεις σχεδόν σε όλες τις εκδόσεις των Windows 98 και των συστημάτων βασισμένα σε NT σε ποικίλους βαθμούς βασισμένο στο υλικό που χρησιμοποιείται.	Υψηλός
Ping Flood	Αυτή η επίθεση περιλαμβάνει την αποστολή των πολύ μεγάλων αριθμών από IMP ECHO (PING) αιτήματα στον οικοδεσπότη κάτω από επίθεση. Αυτή η επίθεση είναι ιδιαίτερα αποτελεσματική όταν ο επιτιθέμενος έχει μια γρηγορότερη σύνδεση δικτύων από το θύμα.	Υψηλός
Ping of Death	Με αυτήν την επίθεση, ένας απομακρυσμένος χρήστης μπορεί να αναγκάσει το σύστημά σας να κάνει επανεκκίνηση ή τον πανικό με την αποστολή ενός μεγάλου μεγέθους πακέτου PING. Αυτό γίνεται στέλνοντας του ένα τεμαχισμένο πακέτο μεγαλύτερο από 65536 bytes στο μήκος, που προκαλεί στο	Υψηλός

	απομακρυσμένο σύστημα να επεξεργαστεί όχι σωστά το πακέτο. Το αποτέλεσμα είναι ότι το απομακρυσμένο σύστημα θα κάνει επανεκκίνηση ή πανικό κατά τη διάρκεια της επεξεργασίας.	
Port Scanning	Όταν όχι μια επίθεση μέσα και έξω από αυτήν, μια ανίχνευση θυρών συχνά εμφανίζει ότι ένας επιτιθέμενος έχει αρχίσει να ψάχνει το σύστημά σας για πιθανές αδυναμίες. Μια ανίχνευση θυρών αποτελείται από τον έλεγχο κάθε θύρας TCP ή/και UDP για να δει τι υπηρεσίες (και ως εκ τούτου, ποιες ευπαθής) μπορεί να είναι παρούσες .	Χαμηλός
Saihyousen	Η επίθεση Saihyousen μπορεί να αναγκάσει μερικά firewall να κρασάρουν. Προκαλείται όταν ένας επιτιθέμενος στέλνει ένα ρεύμα από UDP πακέτα.	Υψηλός
Smurf	Αυτή η επίθεση πραγματοποιείται με την αποστολή ενός ICMP ECHO REQUEST (PING) πακέτο με μια σφυρηλατημένη διεύθυνση προέλευσης που ταιριάζει με αυτής του συστήματος στόχων. Αυτό το πακέτο στέλνεται στα δίκτυα «amplifier» - δίκτυα που επιτρέπουν τη μετάδοση πακέτων σε διευθύνσεις broadcast - έτσι ώστε κάθε μηχάνημα στο amplifier δίκτυο θα αποκριθεί ότι αυτό που σκέφτονται είναι ένα νόμιμο αίτημα από το στόχο. Κατά συνέπεια, το σύστημα στόχων είναι πλημμυρισμένο με μηνύματα ICMP ECHO REPLY, προκαλώντας μια επίθεση άρνησης υπηρεσιών.	Υψηλός
SynDrop	Επικαλύπτοντας τα τεμαχισμένα στοιχεία που στέλνονται από έναν επιτιθέμενο προκαλεί τον υπολογιστή σας να είναι ασταθής και ή να κρασάρει. Τα μη σωσμένα στοιχεία θα μπορούσαν να χαθούν.	Υψηλός
Syn Flood	Αυτή η επίθεση μπορεί να χρησιμοποιηθεί για να θέσει εντελώς εκτός λειτουργίας τις υπηρεσίες δικτύων σας πλημμυρίζοντας τους με αιτήματα σύνδεσης. Αυτό θα γεμίσει τη σειρά αναμονής που διατηρεί ένα κατάλογο από μη καθιερωμένες εισερχόμενες συνδέσεις, αναγκάζοντας το να είναι ανίκανο να δεχτεί πρόσθετες συνδέσεις.	Υψηλός
Teardrop	Στα τρωτά συστήματα, είναι	Υψηλός

	δυνατόν να εκμεταλλευτεί μια ρωγμή στο δρόμο ο σωρός TCP/IP χειρίζεται την επανασυναρμολόγηση των τεμαχισμένων πακέτων που καταναλώνει διαθέσιμους πόρους μνήμης. Με την αποστολή ενός ειδικά επεξεργασμένου IP διαγράμματος, αυτή η επίθεση μπορεί να αναγκάσει πολλά λειτουργικά συστήματα να κρεμάσουν ή κάνουν επανεκκίνηση.	
UDP Flood	Η απομακρυσμένη επίθεση άρνησης υπηρεσιών (DOS) σχεδιάστηκε για να πλημμυρίσει το μηχάνημα στόχου με περισσότερα στοιχεία από αυτά που μπορεί να επεξεργαστεί, με αυτόν τον τρόπο παρεμποδίζει νόμιμες συνδέσεις από το να καθιερωθούν. Το μηχάνημα είναι απρόσιτο μέσω TCP/IP. Εμφανίζεται όταν το μηχάνημα τίθεται σε κατάσταση sleep και έπειτα στην κατάσταση awakened.Σιγουρευτείτε ότι εκείνο το «Load Only When Needed» δεν έχει τσεκαριστεί στον πίνακα ελέγχου του TVT. Κατόπιν το TCP/IP φορτώνεται όλη την ώρα, επιτρέποντας στο McAfee Firewall για να λειτουργήσει ενώ το μηχάνημα είναι σε κατάσταση sleep.	Υψηλός
Winnuke	Αυτή η επίθεση είναι μια επίθεση της άρνησης υπηρεσιών (DOS) που θέτει εντελώς εκτός λειτουργίας τη δικτύωση σε πολλά μηχανήματα Win95 και WinNT. Αν και το Winnuke θα μπορούσε όχι απαραίτητα να βλάψει τον υπολογιστή σας, μπορεί να χάσετε οποιαδήποτε μη σωσμένα στοιχεία κατά το χρόνο της επίθεσης. Μετά την επανεκκίνηση του υπολογιστή σας πρέπει να αποκαταστήσει ολόκληρη τη λειτουργία.	Υψηλός

ΣΤ.ΕΝΗΜΕΡΩΝΟΝΤΑΣ ΤΟ McAfee Firewall

Σχετικά με τη στιγμιαία ενημέρωση

Καθώς οι τεχνολογίες προοδεύουν, παρέχονται συνεχώς ενημερώσεις για το λογισμικό των προϊόντων του MCA. Για να εξασφαλίσετε το πιο υψηλό επίπεδο προστασίας, πρέπει πάντα να λαμβάνετε την πιο πρόσφατη έκδοση του προϊόντος McAfee σας.

Η ενημέρωση του λογισμικού σας είναι απλή χρησιμοποιώντας
Την στιγμιαία ενημέρωση McAfee. Είναι μια ίδια ραφής διαδικασία και απαιτεί την ελάχιστη αλληλεπίδραση από τη μεριά σας.

Η στιγμιαία ενημέρωση είναι επίσης ο μηχανισμός που χρησιμοποιείται για να καταχωρήσει το προϊόν σας McAfee. Προκειμένου να ληφθούν οι ενημερώσεις προϊόντων, πρέπει να καταχωρήσετε το προϊόν σας McAfee.

Γιατί πρέπει να ενημερωθείτε;

- Τα νέα χαρακτηριστικά γνωρίσματα μπορούν να απελευθερωθούν για το προϊόν McAfee σας.
- Οι αποτυπώσεις προϊόντων είναι περιοδικά διαθέσιμες.
- Η περιεκτικότητα σε νέα προϊόντα ενημερώνεται περιοδικά.
- Οι ενημερώσεις στα αρχεία υπογραφής antivirus είναι συχνά διαθέσιμες.

Πώς η διαδικασία ενημέρωσης λειτουργεί;

Η στιγμιαία ενημέρωση σας επιτρέπει να λάβετε και να εφαρμόσετε τις ενημερώσεις στα προϊόντα σας McAfee ,ενώ συνδέεται με το Διαδίκτυο. Εάν μια ενημερώσει υπάρξει, θα λάβετε μια ειδοποίηση. Εκείνη τη στιγμή, μπορείτε να κατεβάσετε και να εφαρμόσετε τις ενημερώσεις στα προϊόντα σας .

Στιγμιαία χαρακτηριστικά γνωρίσματα ενημέρωσης

- Η αυτόματη ενημέρωση είναι ρύθμιση προεπιλογής του στιγμιαίου ενημερωτή.

Ο Στιγμιαίος Updater ψάχνει σιωπηλά για, και ανάλογα με την περίπτωση, εφαρμόζει την ενημέρωση του προϊόντος σας ενώ συνδέεστε στο Διαδίκτυο. Περιστασιακά, ο στιγμιαίος Updater μπορεί να σας ζητήσει για να εφαρμόσετε τις ενημερώσεις να ξαναξεκινήσετε τον υπολογιστή σας . Η αυτόματη ενημέρωση ελέγχει για τις ενημερώσεις για να επιβεβαιώνει καθημερινά ότι το προϊόν McAfee, η περιεκτικότητα σε προϊόντα, και τα σχετικά στοιχεία σας όπως η μηχανή και DATs ανίχνευσης ιών είναι τρέχουσες.

- Αυτόματη διακήρυξη: Εάν η αυτόματη έρευνα επιτρέπεται, επιτρέπει σε σας για να λάβει ανακοίνωση των αναπροσαρμογών προϊόντων ενώ συνδέεται με

το Διαδίκτυο. να μην συστήσει την αυτόματη έρευνα εάν έχετε ένα αργό Διαδίκτυο σύνδεση Εγχειρίδιο που ενημερώνει: Εάν συνδέετε σπάνια με το Διαδίκτυο, μπορείτε να προτιμήσετε για να χρησιμοποιήσει τη χειρωνακτική ενημέρωση με το προϊόν McAfee σας. Μπορείτε με το χέρι ενημερώστε ενώ συνδέεται με το Διαδίκτυο. Για να κάνετε αυτό, επιλέξτε την ΑΝΑΠΡΟΣΑΡΜΟΓΗ λειτουργία από μέσα από το μεμονωμένο προϊόν. Η χειρωνακτική ενημέρωση παρέχει σε σας το ρητό έλεγχο της ενημέρωσης διαδικασία. Ερώτηση αρχικών σελίδων Αφορά στιγμιαίο Updater η ερώτηση αρχικών σελίδων. Αυτό το χαρακτηριστικό γνώρισμα σας επιτρέπει διαμορφώστε την αρχική σελίδα του προϊόντος McAfee σας για να επιδείξετε ένα μήνυμα όταν η αναπροσαρμογή είναι διαθέσιμη. Αφότου εγκαθιστάτε το λογισμικό McAfee σας, ερώτηση αρχικών σελίδων «» είναι η ρύθμιση προεπιλογής. Διαμόρφωση Για τις πρόσθετες πληροφορίες σχετικά με την αυτόματη έρευνα και τις αυτόματες τοποθετήσεις αναπροσαρμογών, παρακαλώ αναφερθείτε στη σε απευθείας σύνδεση βοήθεια.

Z. ΠΩΣ ΜΠΟΡΕΙΣ ΝΑ ΕΡΘΕΙΣ ΣΕ ΕΠΑΦΗ ΜΕ ΤΟ McAfee

- www.McAfee-at-Home.com :Το McAfee είναι διάσημο για την αφιέρωσή του προς την ικανοποίηση των πελατών. Έχουμε συνέχισε αυτήν την παράδοση με να καταστήσει την περιοχή μας στο World Wide Web έναν πολύτιμο πόρος για τις απαντήσεις στις ερωτήσεις σας για τα καταναλωτικά McAfee προϊόντα. Σας ενθαρρύνει να επισκεφτείτε το site http://www.mcafee-at-home.com και να κάνετε ανατρέξετε εκεί για όλες τις ανάγκες υποστήριξης προϊόντων σας.
- Εξυπηρέτηση πελατών :Για να παραγγείλετε τα προϊόντα ή να λάβετε πληροφορίες σχετικά με αυτα, μπορειτε να έρθετε σε επαφή με το τμήμα εξυπηρετήσεων πελατών του McAfee στο (972) σε 308-9960 ή γράφτε στην ακόλουθη διεύθυνση:

Συνεταίροι δικτύων 13465 ευρισκόμενος
στη μέση του δρόμου δρόμος Ντάλλας, TX 75244 U.S.A

Παρακαλώ σημειώστε,(972) 308-9960 είναι τηλέφωνο στις Ηνωμένες Πολιτείες της Αμερικής.

- Τεχνική υποστήριξη: Για πράκτορας τη βοηθημένη τεχνική υποστήριξη, παρακαλώ επισκεφτείτε το http://www.mcafeehelp.com. Ο ιστοχώρος υποστήριξής μας προσφέρει την εικοσιτετράωρη πρόσβαση στις λύσεις στον

πιο κοινό αιτήματα υποστήριξης στον εύχρηστο μάγο απάντησης 3 βημάτων μας. Επιπλέον, εσείς μπορέστε να χρησιμοποιήσετε τις προηγμένες επιλογές μας, οι οποίες περιλαμβάνουν μια αναζήτηση λέξης κλειδιού και μας.Βοηθήστε το δέντρο, τα οποία έχουν σχεδιαστεί με τον πιο πεπειραμένο χρήστη μέσα μυαλό.

Εάν μια λύση στο πρόβλημά σας δεν μπορεί να βρεθεί, μπορείτε επίσης να έχετε πρόσβαση σε εικοσιτετράωρη ΕΛΕΥΘΕΡΗ συνομιλία τώρα! Και το ηλεκτρονικό ταχυδρομείο είναι σαφές! Η συνομιλία και το ηλεκτρονικό ταχυδρομείο επιτρέψτε σε σας για να φθάσετε γρήγορα στους μηχανισμούς κατάλληλης υποστήριξής μας, μέσω Διαδίκτυο, με κανένα κόστος. Οι πληροφορίες τηλεφωνικής υποστήριξης μπορούν επίσης να ληφθούν από το μας ιστοχώρος αυτοβοήθειας σε:

http://www.mcafeehelp.com.

ΕΝΩΠΙΟΝ ΣΑΣ το λογισμικό McAfee ΕΠΑΦΩΝ για την τεχνική υποστήριξη, εντοπίζουν οι ίδιοι στον υπολογιστή το προϊόν McAfee που εγκατέστησαν και ελέγχουν πληροφορίες που απαριθμούνται κατωτέρω:

1. Αριθμός έκδοσης λογισμικού McAfee σας Από την επίλεκτη βοήθεια παραθύρων αντιπυρικών ζωνών McAfee κύρια > περίπου για να βρει αυτό πληροφορίες
2. Πώς να έρθει σε επαφή με McAfee Αριθμός έκδοσης λειτουργικών συστημάτων παραθύρων.
3. Ποσό μνήμης (RAM) Πλήρης περιγραφή του προβλήματος ΑΚΡΙΒΕΣ μήνυμα λάθους όπως στην οθόνη
4. Ποια βήματα εκτελέσθηκαν πριν απο τη λήψη του μηνύματος λάθους;

5. Είναι το λάθος επίμονο μπορείτε να αναπαραγάγετε το πρόβλημα;
6. Πρότυπο όνομα του σκληρού δίσκου (εσωτερικού/εξωτερικού) Πρόσθετο κάρτες, πίνακες, ή υλικό

Για περισσότερες πληροφορίες για προϊόντα, παγκόσμιες υπηρεσίες, και υποστήριξη, έρχεται σε επαφή με εξουσιοδοτημένους πωλητές McAfee. Ο αντιπρόσωπος ή μας επισκέπτεται σε:

Συνεταίροι δικτύων 13465 ευρισκόμενος στη μέση του δρόμου δρόμος Ντάλλας, TX 75244 (972) 308-9960
www.mcafee-at-home.com

10.PROXY SERVERS ΚΑΙ DMZ

Μια λειτουργία που συχνά συνδυάζεται με το firewall είναι ο proxy server. Ο proxy server χρησιμοποιείται για να έχει πρόσβαση στις Web pages των άλλων υπολογιστών. Όταν ένας άλλος υπολογιστής κάνει αίτηση για μια Web page , βρίσκεται από το proxy server και έπειτα στέλνεται στον υπολογιστή που έχει κάνει την αίτηση. Η επιρροή του δικτύου από αυτήν την ενέργεια είναι ότι ο απομακρυσμένος υπολογιστής που φιλοξενεί την Web page δεν έρχεται σε απευθείας επαφή με οτιδήποτε ή με το δίκτυο του σπιτιού σας, εκτός από το proxy server.

Proxy servers μπορούν επίσης να κάνουν την πρόσβαση σας στο διαδικτυο να δουλεύουν αποδοτικότερα. Εάν η πρόσβαση σας σε μια σελίδα σε μια ιστοσελίδα, αυτή αποθηκεύεται στον proxy. Αυτό σημαίνει ότι την επόμενη φορά που θα γυρίσετε σε αυτήν τη σελίδα, κανονικά δεν θα χρειάζεται να τη ξαναφορτώσετε από την ιστοσελίδα. Αντίθετα θα τη φορτώσει στιγμιαία από τον proxy.

Υπάρχουν φορές που ίσως να θέλετε απομακρυσμένοι χρηστές να έχουν πρόσβαση σε διάφορα αντικείμενα στο δίκτυο σας. Μερικά παραδείγματα είναι :

- Web site
- Online business
- FTP download and upload area

Σε περιπτώσεις όπως αυτές , χρειαζόσαστε να δημιουργήσετε ένα DMZ(αποστρατικοποιημένη ζώνη). Παρόλο που ακούγεται αρκετά σοβαρό, στην πραγματικότητα είναι μια περιοχή έξω από το firewall.σκεπτόμενοι το DMZ το πίσω μέρος του σπιτιού σας. Ανήκει σε εσάς και μπορεί να βάλετε κάποια πράγματα εκεί., αλλά πρέπει τα χρήσιμα πράγματα να τα βάλετε μέσα στο σπίτι σας που είναι πιο ασφαλές.

11.Η ΖΩΝΗ DMZ

Εισαγωγή

Από την άποψη της ασφάλειας υπολογιστών μια αποστρατικοποιημένη ζώνη (DMZ) είναι μια περιοχή δικτύων που κάθεται μεταξύ του εσωτερικού δικτύου μιας οργάνωσης και ενός εξωτερικού δικτύου, συνήθως το Διαδίκτυο. Το DMZ επιτρέπει στους περιλαμβανόμενους οικοδεσπότες για να παρέχει τις υπηρεσίες στο εξωτερικό δίκτυο, προστατεύοντας το εσωτερικό δίκτυο από τις πιθανές παρεισφρήσεις σε εκείνους τους οικοδεσπότες. Στους όρους του λαϊκού (μη κληρικού) ένα DMZ είναι όπως ένας μονόδρομος.

Η συνδετικότητα επιτρέπεται από και στο εξωτερικό δίκτυο. Οι συνδέσεις από το εξωτερικό δίκτυο ελέγχονται συνήθως χρησιμοποιώντας τη μετάφραση διευθύνσεων λιμένων .

Η συνδετικότητα επιτρέπεται από το εσωτερικό δίκτυο, αλλά καμία πρόσβαση δεν επιτρέπεται στο εσωτερικό δίκτυο.

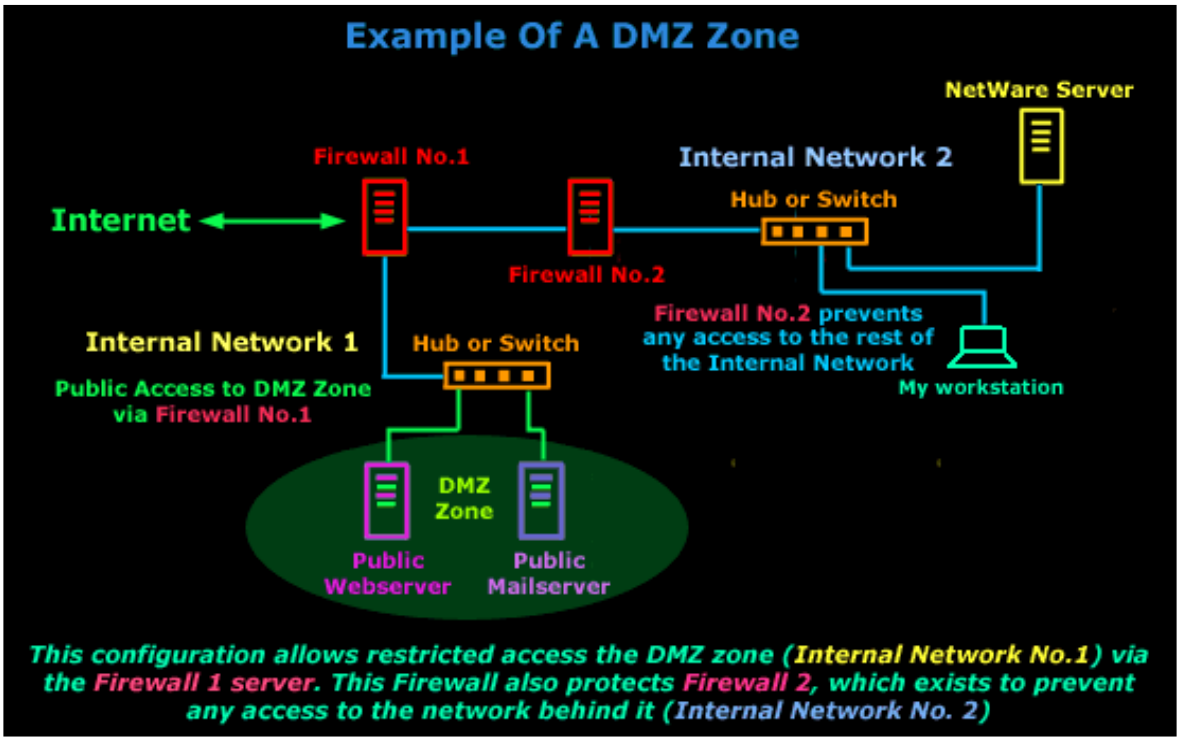
Σημειώστε ότι οι εγχώριοι δρομολογητές αναφέρονται μερικές φορές σε έναν "οικοδεσπότη DMZ". Αυτό δεν είναι ένα αληθινό DMZ εξ ορισμού.

Το δίκτυο geeks το χρησιμοποιεί για να σημαίνει: «μια μερίδα του δικτύου σας που, αν και υπό τον έλεγχό σας, είναι έξω η βαρύτερη ασφάλειά σας.» Έναντι του υπολοίπου του δικτύου σας, οι μηχανές που τοποθετείτε στο DMZ είναι λιγότερο προστατευμένες, ή επίπεδος-έξω μη προστατευμένες, από το Διαδίκτυο.

Μόλις μια μηχανή εισαγάγει το DMZ, δεν πρέπει να επανέλθει μέσα στο δίκτυο πάλι. Υποθέτοντας ότι έχει συμβιβαστεί με κάποιο τρόπο, με το να επανέλθει στο δίκτυο είναι ένας μεγάλος κίνδυνος ασφάλειας.

Χρήση του DMZ

Εάν αποφασίσετε να χτίσετε ένα, τι κάνετε με αυτό; Οι μηχανές που τοποθετούνται στο DMZ συνήθως προσφέρουν υπηρεσίες στο ευρύ κοινό, όπως υπηρεσίες Ιστού, υπηρεσίες ονόματος περιοχών (DNS), αναμετάδοση ταχυδρομείου και υπηρεσίες FTP (οι ορολογίες αυτές θα εξηγηθούν έπειτα). Ο ι Proxy servers μπορούν επίσης να εισάγουν το DMZ. Εάν αποφασίζετε να επιτρέψετε την πρόσβαση Ιστού στους χρήστες σας μόνο μέσω ενός proxy server, μπορείτε να βάλετε τον proxy σε τείχος προστασίας και να θέσετε στους κανόνες του τείχους προστασίας σας, να επιτρέπει εξωτερική πρόσβαση μόνο στον proxy.



Εφ' όσον έχετε ανταποκριθεί στα ακόλουθα σημεία, το DMZ σας πρέπει να είναι εντάξει:

Εάν βάζετε μια μηχανή στο DMZ, πρέπει να είναι για έναν καλό λόγο. Μερικές φορές, οι επιχειρήσεις θα ιδρύσουν μερικούς τερματικούς σταθμούς με την πλήρη πρόσβαση Διαδικτύου μέσα στο DMZ. Οι υπάλληλοι μπορούν να χρησιμοποιήσουν αυτές τις μηχανές για τα παιχνίδια και άλλες επισφαλείς δραστηριότητες. Αυτό είναι ένας καλός λόγος εάν οι εσωτερικές μηχανές δεν έχουν καμία πρόσβαση στο Διαδίκτυο, ή έχουν εξαιρετικά περιορισμένη πρόσβαση. Εάν η πολιτική σας είναι να δώσετε στους υπαλλήλους μέτρια πρόσβαση από τους υπολογιστές γραφείου τους, κατόπιν η δημιουργία των τερματικών σταθμών όπως αυτό στέλνει το λανθασμένο μήνυμα. Σκεφτείτε αυτό: Ο μόνος λόγος για τον οποίο θα χρησιμοποιούσαν μια μηχανή DMZ είναι εάν έκαναν κάτι ακατάλληλο για τον εργασιακό χώρο!

Πρέπει να είναι ένα απομονωμένο νησί,not a stepping stone. Δεν πρέπει να συνδεθεί άμεσα με το εσωτερικό δίκτυο. Επιπλέον, δεν πρέπει να περιέχει τις πληροφορίες που θα μπορούσαν να βοηθήσουν τους χάκερ να τα συνδυάσουν με άλλα μέρη του δικτύου. Αυτό περιλαμβάνει τα ονόματα χρηστών, τους κωδικούς πρόσβασης, τις πληροφορίες σχετικά με τη διαμόρφωση του υλικού δικτύων κ.λ.π.

Δεν πρέπει να περιέχει τίποτα που δεν μπορείτε να αντέξετε να χάσετε. Οποιαδήποτε σημαντικά αρχεία που τοποθετούνται στο DMZ πρέπει να είναι μόνο ανάγνωσης αντίγραφα των πρωτοτύπων που βρίσκονται μέσα στο δίκτυο. Τα αρχεία που δημιουργούνται στο DMZ δεν πρέπει να είναι σε θέση να μεταναστεύσουν στο δίκτυο εκτός αν ένας διαχειριστής τα έχει εξετάσει. Εάν τρέχετε έναν news server και

θα επιθυμούσατε να αρχειοθετήσετε τις ειδήσεις, σιγουρευτείτε ότι το DMZ έχει το δικό του σύστημα αρχείων.

Τι δεν θα έπρεπε να κάνετε; Παράδειγμα: Εάν τρέχετε έναν κεντρικό υπολογιστή FTP στο DMZ, μην αφήστε τους χρήστες να βάλουν τις εμπιστευτικές πληροφορίες εκεί, έτσι ώστε να μπορούν να τις πάρουν από το σπίτι αργότερα.

Πρέπει να είναι τόσο ασφαλής οικοδεσπότης όσο μπορείτε να το κάνετε. Ακριβώς επειδή υποθέτετε ότι είναι ασφαλές δεν εγγυάται κιόλας ότι είναι. Μην το καταστήστε καθόλου ευκολότερο για έναν χάκερ από απολύτως απαραίτητο. Ένας χάκερ μπορεί να μην είναι σε θέση να συμβιβάσει το εσωτερικό δίκτυό σας από DMZ σας, αλλά μπορούν να αποφασίσουν να το χρησιμοποιήσουν στο δίκτυο κάποιου άλλου συμβιβασμού. Δώστε τη προσοχή στο να μην τρέχουν τα Windows στις μηχανές DMZ σας, είναι εγγενώς επισφαλές και πολλοί τύποι παρεισφρήσεων δεν μπορούν να ανιχνευθούν στα Windows. Το Linux ή το openbsd μπορεί να παρέχει των περισσότερων, εάν όχι όλων, την αναγκαία λειτουργία μαζί με ένα ασφαλέστερο περιβάλλον.

12.DOS & ΕΠΙΘΕΣΕΙΣ DDoS

Εισαγωγή

Σε αυτό το τμήμα πρόκειται να ρίξουμε μια γρήγορη ματιά στο DOS και τις επιθέσεις DDoS, πώς εκτελούνται και γιατί προσελκύουν τόσο πολλή προσοχή! Δεν θα μπαίνουμε σε λεπτομέρειες δεδομένου ότι προσπαθούμε ακριβώς να δώσουμε στον καθένα μια καλύτερη κατανόηση του προβλήματος.

Άρνηση των επιθέσεων υπηρεσιών

Η άρνηση των επιθέσεων υπηρεσιών (DOS) μπορεί να είναι ένα σοβαρό ομοσπονδιακό έγκλημα με τις ποινικές ρήτρες που περιλαμβάνουν τα έτη φυλάκισης και πολλές χώρες έχουν τους νόμους που προσπαθούν να τους προστατεύσουν από αυτό. Στο ελάχιστο, οι παραβάτες χάνουν συνήθως τους απολογισμούς φορέων παροχής υπηρεσιών Διαδικτύου τους (ISP), περνούν ανασταλμένοι ή εάν οι σχολικοί πόροι περιλαμβάνονται, κ.λπ.

Υπάρχουν δύο τύποι επιθέσεων DOS:

1) επιθέσεις λειτουργικών συστημάτων: Ποια ζωύφια στόχων στα συγκεκριμένα λειτουργικά συστήματα και μπορεί να φτιαχτεί με τα μπαλώματα(patches).

2) επιθέσεις δικτύωσης: Αυτές που εκμεταλλεύονται τους έμφυτους περιορισμούς της δικτύωσης και μπορούν να απαιτήσουν την προστασία τειχών προστασίας.

Επιθέσεις λειτουργικών συστημάτων

Αυτές οι επιθέσεις εκμεταλλεύονται τα ζωύφια σε ένα συγκεκριμένο λειτουργικό σύστημα (OS), το οποίο είναι το βασικό λογισμικό που τρέχει στον υπολογιστή σας, όπως τα Windows98 ή MacOs. Γενικά, όταν αυτά τα προβλήματα προσδιορίζονται, ο προμηθευτής, όπως η Microsoft, θα απελευθερώσει ένα update ή ένα bug για να τα φτιάξει.

Έτσι, ως πρώτο βήμα, σιγουρευτείτε πάντα ότι έχετε την πολύ πιο πρόσφατη έκδοση του λειτουργικού συστήματός σας, συμπεριλαμβανομένων όλων των bug fixes.Όλοι οι χρήστες των Windows πρέπει τακτικά να επισκεφτούν το Microsoft's Windows Update Site(τουλάχιστον μία φορά την εβδομάδα!) το ποιο ελέγχει αυτόματα εάν χρειάζεστε οποιεσδήποτε αναπροσαρμογές.

Επιθέσεις δικτύωσης

Αυτές οι επιθέσεις εκμεταλλεύονται τους έμφυτους περιορισμούς της δικτύωσης για να σας αποσυνδέσουν από ISP σας, αλλά δεν προκαλούν συνήθως τον υπολογιστή σας συντριβή. Μερικές φορές δεν έχει καν σημασία τι είδους λειτουργικό σύστημα χρησιμοποιείτε και δεν μπορείτε να patch or fix το πρόβλημα άμεσα. Οι επιθέσεις στοYahoo και στο Amazon από το «mafiaboy» ήταν επιθέσεις δικτύωσης μεγάλης κλίμακας και κατέδειξαν ότι κανένας δεν είναι ασφαλής ενάντια σε έναν πολύ καθορισμένο επιτιθέμενο.

Οι επιθέσεις δικτύων περιλαμβάνουν την πλημμύρα ICMP (πλημμύρα μεταλλικού θορύβου) και smurf που είναι ολοκληρωτικές πλημμύρες των στοιχείων για να συντρίψουν την ικανότητα της σύνδεσής σας, εξαπατώ unreach/redirect γνωστό επίσης ως «click» που εξαπατά τον υπολογιστή σας να σκεφτεί ότι υπάρχει μια αποτυχία δικτύων και εθελοντικά σπάσιμο της σύνδεσης (αυτό χρησιμοποιείται για να αποσυνδέσει τους χρήστες MIRC), και ολόκληρη μια νέα γενεά της διανεμημένης άρνησης των επιθέσεων υπηρεσιών (θα μιλήσουμε για αυτό αργότερα).

Το γεγονός ότι αποσυνδεθήκατε με κάποιο ασυνήθιστο μήνυμα λάθους δεν σημαίνει ότι επιτεθήκατε. Σχεδόν όλες οι αποσυνδέσεις οφείλονται σε φυσικές αποτυχίες των δικτύων. Αφ' ενός, πρέπει να υποπτευθείτε εάν αποσυνδεόσαστε συχνά.

Τι μπορείτε να κάνετε για τις επιθέσεις δικτύωσης; Εάν ο επιτιθέμενος σας πλημμυρίζει, ουσιαστικά χρειάζεται να έχετε μια καλύτερη σύνδεση από αυτόν. Διαφορετικά η μόνη προσφυγή σας να είναι ένα τείχος προστασίας που να τρέχει από το ISP σας.

Διανεμημένη άρνηση--υπηρεσία

Μια διανεμημένη επίθεση άρνηση--υπηρεσιών (DDoS) είναι ίδια με την επίθεση DOS που περιγράψαμε ανωτέρω, αλλά περιλαμβάνει ένα πλήθος συμβιβασμένων συστημάτων που επιτίθενται σε έναν ενιαίο στόχο, με αυτόν τον τρόπο προκαλώντας την άρνηση της υπηρεσίας για τους χρήστες του στοχοθετημένου συστήματος. Η πλημμύρα των εισερχόμενων μηνυμάτων στο σύστημα στόχων το αναγκάζει ουσιαστικά για να διακόψει, με αυτόν τον τρόπο αρνείται την υπηρεσία στο σύστημα στους νόμιμους χρήστες.

Ένας χάκερ (ή, εάν προτιμάτε, κροτίδα) αρχίζει μια επίθεση DDoS με την εκμετάλλευση μιας ευπάθειας σε ένα συγκρότημα ηλεκτρονικών υπολογιστών και κάνοντάς το DDoS «master.» Είναι από το κύριο σύστημα ότι ο εισβολέας προσδιορίζει και επικοινωνεί με άλλα συστήματα που μπορούν να συμβιβαστούν. Ο εισβολέας φορτώνει τα cracking εργαλεία διαθέσιμα στο διαδίκτυο στο πολλαπλάσιο -- μερικές φορές χιλιάδες -- συμβιβασμένα συστήματα. Με μια μόνο εντολή, ο εισβολέας καθοδηγεί τις ελεγχόμενες μηχανές για να προωθήσει μιας από πολλές επιθέσεις πλημμύρων ενάντια σε έναν συγκεκριμένο στόχο. Το αποτέλεσμα αυτών των πακέτων που στέλνονται στο στόχο προκαλεί μια άρνηση της υπηρεσίας.

Ενώ ο Τύπος τείνει να εστιάσει στο στόχο των επιθέσεων DDoS ως θύμα, στην πραγματικότητα υπάρχουν πολλά θύματα σε μια επίθεση DDoS -- ο τελικός στόχος καθώς επίσης και τα συστήματα ελέγχονται από τον εισβολέα.

13.ΠΑΡΑΘΥΡΑ ΚΛΕΙΔΩΜΑΤΟΣ

Εισαγωγή

Στατικό IPs είναι μέρος του προβλήματος επίμονος-σύνδεσης, αλλά τα επίμονα παράθυρα τα ίδια πρόκειται επίσης να κατηγορήσουν. (Καταναλωτικές εκδόσεις των παραθύρων, εν πάση περιπτώσει--NT και τα παράθυρα το 2000 είναι ένα διαφορετικό παιχνίδι εξ ολοκλήρου.) WINDOWS.95 και 98 είναι πλήρη των χασμάτων ασφάλειας. Εδώ είναι μερικά πράγματα που πρέπει να κάνετε για να τα κλείσετε επάνω.

Τι να κάνει

Κλείστε το αρχείο μοιρασμένος εάν δεν το χρειάζεστε. Εάν δεν μοιράζεστε τα αρχεία με άλλους υπολογιστές--συνήθως θα κάνατε έτσι πέρα από ένα εγχώριο δίκτυο--κατόπιν να θέσει εκτός λειτουργίας αυτού του χαρακτηριστικού γνωρίσματος κλείνει επάνω την αφθονία των τρυπών. Για να εξασφαλίσει αρχείο η διανομή είναι κλειστή, γειτονιά δικτύων σωστός-κρότου και ιδιότητες επιλογών. Χτυπήστε το κουμπί επονομαζόμενο «το αρχείο και την τυπωμένη ύλη μοιρασμένος» και επιβεβαιώστε ότι και τα δύο παράθυρα
το προκύπτον πλαίσιο διαλόγου είναι ανεξέλεγκτο.

Ιδρύστε το αρχείο μοιρασμένος προσεκτικά εάν πρέπει να το χρησιμοποιήσετε. Η γειτονιά δικτύων σωστός-κρότου, επιλέγει τις ιδιότητες, και χτυπά τη «διανομή αρχείων και τυπωμένων υλών.» Ελέγξτε ότι το παράθυρο δίπλα «θέλω να δώσω σε άλλους την πρόσβαση στα αρχεία μου.» Έπειτα, η επιλογή ή δημιουργεί έναν συγκεκριμένο φάκελο που θα αφήσετε την πρόσβαση ανθρώπων, όπως τα έγγραφα φωτογραφίες του c:\My \. Στον εξερευνητή, τον σωστός-κρότο ο φάκελος και την επιλογή παραθύρων που μοιράζεται από τις επιλογές πλαισίου. Στο πλαίσιο διαλόγου που εμφανίζεται, χτυπήστε το ράδιο κουμπί δίπλα κοινός όπως: και εισάγετε ένα όνομα για το φάκελο στον τομέα στο δικαίωμα. (Το όνομα που επιλέγετε είναι το όνομα που θα εμφανιστεί σε εκείνοι που κοιτάζουν βιαστικά το φάκελο μέσω το δίκτυο ή του Διαδικτύου).

Εάν θέλετε τους ανθρώπους για να είστε σε θέση να προσθέσετε, να αφαιρέσετε, ή τα έγγραφα αλλαγής στο φάκελο, να χτυπήσετε το πλήρες ράδιο κουμπί κάτω από τον τύπο πρόσβασης.

Εάν θέλετε τους ανθρώπους για να είστε σε θέση μόνο να αντιγράψετε ή να εξετάσετε τα αρχεία στο φάκελο, χτυπήστε το διαβασμένο μόνο ράδιο κουμπί.

Σε καθεμία περίπτωση, να είστε βέβαιος να πληκτρολογήσει έναν προσωπικό κωδικό (όχι λιγότεροι από τέσσερις και λιγότερος από οκτώ χαρακτήρες) στον τομέα στο κατώτατο σημείο του πλαισίου διαλόγου. Το πλαίσιο διαλόγου θα επιτρέψει σε σας για να χτυπήσει ΕΝΤΑΞΕΙ χωρίς είσοδό σας έναν κωδικό πρόσβασης, αλλά σε εκείνη την περίπτωση, οποιοσδήποτε που κοιτάζει βιαστικά το φάκελο θα πάρει την πρόσβαση στα αρχεία μέσα.

Ελέγξτε τους κοινούς φακέλους σας χρησιμοποιώντας τη χρησιμότητα παρατηρητών δικτύου παραθύρων. App επιδεικνύει όλους τους χρήστες που συνδέονται αυτήν την περίοδο με τους κοινούς φακέλους και σας αφήνει να τους αποσυνδέσετε εάν είναι απαραίτητο. Η χρησιμότητα δεν είναι μέρος των WINDOWS.95 ή 98's εγκατάσταση προεπιλογής, αλλά μπορείτε να τα εγκαταστήσετε από το CD-Rom παραθύρων σας με την ακολουθία αυτών των βημάτων:

1.Click η έναρξη, τοποθετήσεις, επιτροπή ελέγχου και ανοικτός προσθέτει/αφαιρεί τα προγράμματα.

2.Click η οργάνωση πίν. παραθύρων. Στα παράθυρα 98, τυλίξτε κάτω από τον κατάλογο κατηγοριών οργάνωσης και πιέστε δύο φορές τα εργαλεία συστημάτων. Στα WINDOWS.95, βρείτε και πιέστε δύο φορές τα εξαρτήματα.

3.Check το παράθυρο δίπλα στον παρατηρητή δικτύου, και χτυπά ΕΝΤΑΞΕΙ δύο φορές για να βγει τους διαλόγους.

4.Windows θα εγκαταστήσει τον παρατηρητή δικτύου. Μετά από του συστήματός σας που, επιλέξτε την έναρξη, προγράμματα, εξαρτήματα, εργαλεία συστημάτων, παρατηρητής δικτύου για να προωθήσετε τη χρησιμότητα.

Κατεβάστε τα μπαλώματα συστημάτων. Τα παράθυρα 98 χρήστες μπορούν να διευθύνουν στον ιστοχώρο αναπροσαρμογών παραθύρων για να μεταφορτώσουν αυτόματα τα σχετικά με την ασφάλεια μπαλώματα για το λειτουργικό σύστημά τους. Εάν χρησιμοποιείτε ακόμα τα WINDOWS.95, θα πρέπει να μεταφορτώσετε κάθε μπάλωμα αναπροσαρμογών ασφάλειας με το χέρι στα WINDOWS.95 μεταφορτώνετε τη σελίδα.

Ελέγξτε τις ασπίδες σας. Αφότου έχετε λάβει τα μέτρα ανωτέρω, οι ασπίδες ΕΠΑΝΩ! Ο ιστοχώρος (τρέξιμο από Gibson τη Research εταιρία) μπορεί να εξετάσει τη σύνδεσή σας στον υπόλοιπο κόσμο και να σας ενημερώσει εάν οποιεσδήποτε τρύπες παραμένουν. Η πτώση κοντά και βλέπει εάν έχετε περαιτέρω ευπάθειες. Ασπίδες ΕΠΑΝΩ! επίσης περιέχει κάποιες εξαιρετικά σε βάθος συμβουλές σχετικά με τις τοποθετήσεις δικτύωσης παραθύρων.

14.ΒΙΒΛΙΟΓΡΑΦΙΑ:

1. http://firewall.cx
2. www.mcafeehelp.com
3. www.howstuffworks.com
4. News and Communication-Duke University