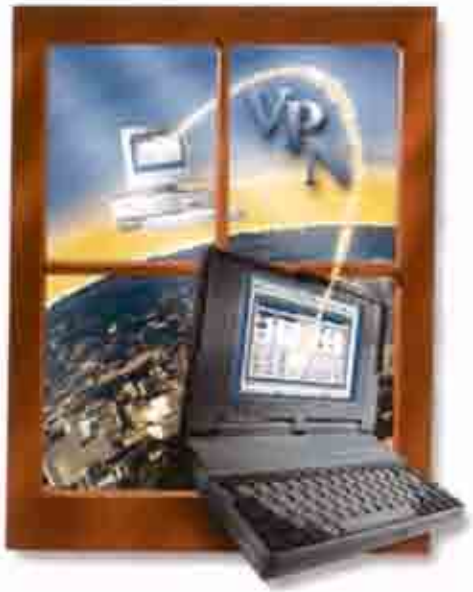
VIRTUAL PRIVATE NETWORKs

ΜΑΤΖΑΒΙΝΟΥ ΠΑΝΑΓΙΩΤΑ
ΜΙΧΕΛΑΚΗ ΕΛΕΥΘΕΡΙΑ

Α.Τ.Ε.Ι. ΠΑΤΡΑΣ
ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΥ ΣΧΕΔΙΑΣΜΟΥ & ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΚΑΤΑΓΡΑΦΗ ΤΩΝ ΔΙΑΔΙΚΑΣΙΩΝ ΣΧΕΔΙΑΣΜΟΥ, ΕΓΚΑΤΑΣΤΑΣΗΣ ΚΑΙ ΛΕΙΤΟΥΡΓΙΑΣ ΕΝΟΣ ΕΙΚΟΝΙΚΟΥ ΙΔΙΩΤΙΚΟΥ ΔΙΚΤΥΟΥ



ΣΠΟΥΔΑΣΤΡΙΕΣ
ΜΑΤΖΑΒΙΝΟΥ ΠΑΝΑΓΙΩΤΑ
ΜΙΧΕΛΑΚΗ ΕΛΕΥΘΕΡΙΑ

ΕΙΣΗΓΗΤΗΣ
κ. ΔΗΜΗΤΡΙΟΣ ΚΑΝΕΛΛΟΠΟΥΛΟΣ

ΠΑΤΡΑ, ΝΟΕΜΒΡΙΟΣ 2003

Αφιερωμένη στους γονείς μας.

ΠΡΟΛΟΓΟΣ

Δεδομένου ότι ολοένα και περισσότεροι χρήστες είναι υποχρεωμένοι να μετακινούνται συχνά, η απομακρυσμένη πρόσβαση στον κύριο υπολογιστή, εκτός από επιθυμητή, είναι πλέον και αναγκαία.

Στο σύγχρονο, ανταγωνιστικό επιχειρηματικό περιβάλλον η δυνατότητα ενός χρήστη να προσπελάσει με ασφάλεια τον προσωπικό υπολογιστή του στο χώρο εργασίας του, ενόσω βρίσκεται έξω από το δίκτυο της εταιρίας, αποτελεί σημαντικό πλεονέκτημα. Τα VPNs επιτρέπουν στο χρήστη να εργάζεται στον υπολογιστή του από απόσταση μέσω ενός προστατευόμενου περιβάλλοντος.

Προσπαθήσαμε λοιπόν, να καταγράψουμε τις διαδικασίες σχεδιασμού, εγκατάστασης και λειτουργίας ενός Εικονικού Ιδιωτικού Δικτύου με σκοπό να βοηθήσουμε τον αναγνώστη να αποκτήσει μια πλήρη και σαφή εικόνα για τον κόσμο των Virtual Private Networks.

Καθ'ότι ο χώρος των Εικονικών Ιδιωτικών Δικτύων δεν είναι ευρέως διαδεδομένος στη χώρα μας, αντιμετωπίσαμε δυσκολίες στη συγκέντρωση απαραίτητων πληροφοριών για την πλήρη καταγραφή τους. Παρόλα αυτά θέλουμε να πιστεύουμε ότι η εργασία αυτή αποτελεί έναν χρήσιμο οδηγό για όποιον επιθυμεί να ασχοληθεί με τα Εικονικά Ιδιωτικά Δίκτυα.

Τέλος, θα θέλαμε να ευχαριστήσουμε τον καθηγητή κ. Δημήτριο Κανελλόπουλο για την ουσιαστική και πολύτιμη βοήθειά του στην προσπάθειά μας αυτή.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 1°

1.1 ΕΙΣΑΓΩΓΗ

Μέχρι σήμερα υπήρχε μια σαφής διάκριση μεταξύ των δημόσιων και ιδιωτικών δικτύων. Ένα δημόσιο δίκτυο, όπως το δίκτυο μεταγωγής πακέτων και το Διαδίκτυο, είναι μια μεγάλη συλλογή από ανεξάρτητους κόμβους που ανταλλάσσουν πληροφορίες μεταξύ τους. Οι άνθρωποι που έχουν πρόσβαση στο δημόσιο δίκτυο μπορεί να έχουν κάτι κοινό, μπορεί και όχι, και κάθε χρήστης αυτού του δικτύου μπορεί να επικοινωνήσει μόνο με ένα μικρό αριθμό των πιθανών χρηστών του.

Ένα ιδιωτικό δίκτυο (υπολογιστών) αποτελείται από υπολογιστές που ανήκουν σε έναν απλό οργανισμό και μοιράζονται πληροφορίες μεταξύ τους. Σε ένα ιδιωτικό δίκτυο διασφαλίζεται ότι ο εκάστοτε χρήστης πρόκειται να είναι ο μόνος που χρησιμοποιεί το δίκτυο. Το χαρακτηριστικό εταιρικό τοπικό δίκτυο (LAN) ή το δίκτυο ευρείας περιοχής (WAN) είναι ένα παράδειγμα ενός ιδιωτικού δικτύου. Η γραμμή μεταξύ ενός ιδιωτικού και δημόσιου δικτύου κάνει χρήση ενός router, όπου μια επιχείρηση θα δημιουργήσει ένα firewall για να κρατήσει τους εισβολείς του δημόσιου δικτύου έξω από το ιδιωτικό δίκτυό τους, ή για να κρατήσει τους εσωτερικούς χρήστες τους έξω από το δημόσιο δίκτυο.

Στο παρελθόν, οι επιχειρήσεις επέτρεπαν στα τοπικά δίκτυά τους να λειτουργούν ξεχωριστά. Κάθε υποκατάστημα της επιχείρησης μπορούσε να έχει το δικό του τοπικό δίκτυό, με τη δική του επωνυμία, το ηλεκτρονικό του ταχυδρομείο, και ακόμη και το αγαπημένο του πρωτόκολλο δικτύου-κανένα από τα οποία δεν ήταν απαραίτητο να είναι συμβατό με τις οργανώσεις άλλων καταστημάτων. Καθώς οι περισσότερες πηγές πληροφόρησης της επιχείρησης έπαιρναν υπολογιστική μορφή, προέκυψε η ανάγκη για "γραφεία διασύνδεσης". Αυτό γινόταν παραδοσιακά χρησιμοποιώντας μισθωμένες τηλεφωνικές γραμμές ποικίλων ταχυτήτων. Χρησιμοποιώντας μισθωμένες γραμμές, μια επιχείρηση μπορεί να διασφαλίσει ότι η σύνδεση είναι πάντα διαθέσιμη, και ιδιωτική. Οι μισθωμένες τηλεφωνικές γραμμές, εντούτοις, μπορεί να είναι ακριβές. Τιμολογούνται τυπικά βάση μιας σταθερής μηνιαίας τιμής, συν τις δαπάνες απόστασης (σε χιλιόμετρα). Εάν μια επιχείρηση έχει γραφεία σε ολόκληρη τη χώρα, αυτό το κόστος μπορεί να είναι απαγορευτικό.

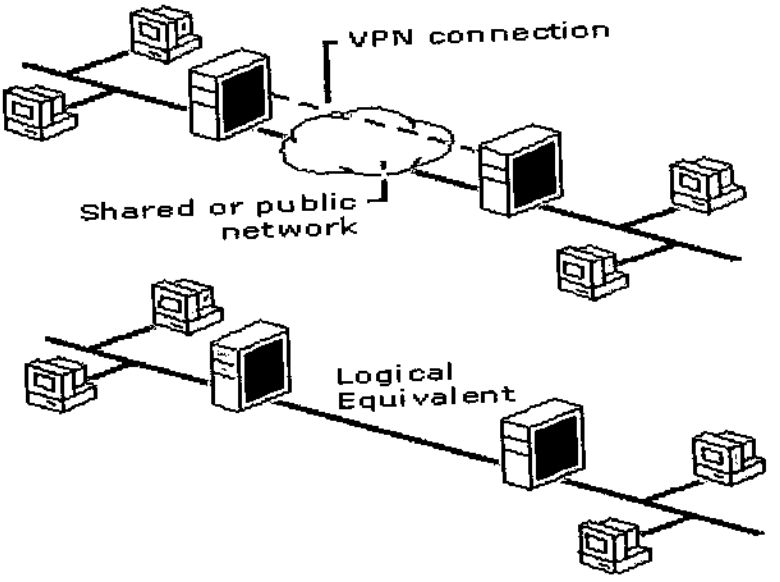
Τα ιδιωτικά δίκτυα έχουν επίσης να αντιμετωπίσουν το πρόβλημα των υπαλλήλων που εργάζονται εκτός καταστημάτων, όπως είναι οι αντιπρόσωποι πωλήσεων. Για παράδειγμα εάν ένας πωλητής δεν είναι κοντά σε έναν υπολογιστή ενός υποκαταστήματος, θα πρέπει να συνδεθεί με ένα απομακρυσμένο modem της εταιρίας, πρόταση η οποία είναι εξαιρετικά ακριβή.

Εμείς θα ασχοληθούμε με το εικονικό ιδιωτικό δίκτυο (VPN), μια έννοια που συγχέεται συχνά με τα δημόσια και τα ιδιωτικά δίκτυα και θα προσπαθήσουμε να αναλύσουμε όσο το δυνατόν σαφέστερα τι είναι και τι κάνει ένα VPN. Ακόμα, θα

αναλύσουμε τις βασικές τους τεχνολογίες, αρχιτεκτονικές και τοπολογίες, θα δούμε βήμα βήμα τη διαμόρφωση και δοκιμή συνδέσεων VPN και τη συντήρηση αυτού, και θα συγκρίνουμε διάφορους τύπους VPNs.

1.2 ΤΙ ΕΙΝΑΙ ΕΝΑ VPN;

Τα Εικονικά Ιδιωτικά Δίκτυα (Virtual Private Networks-VPNs) είναι μια νέα περιοχή της τεχνολογίας των δικτύων υπολογιστών και έχουν σα στόχο να παρέχουν ασφαλή πρόσβαση μεταξύ των μελών ενός οργανισμού που βρίσκονται σε διαφορετικά μέρη σε όλο τον κόσμο. Αυτό το επιτυγχάνουν εξομοιώνοντας ένα ιδιωτικό δίκτυο πάνω από ένα άλλο δημόσιο δίκτυο (π.χ. το Internet). Χρησιμοποιώντας αυτή τη μέθοδο τα VPNs επιτρέπουν στο χρήστη να επικοινωνεί με τέτοιο τρόπο ώστε να του παρέχεται η ίδια ασφάλεια που παρέχεται στους χρήστες των ιδιωτικών δικτύων. Αποκαλείται εικονικό (virtual) διότι βασίζεται στη χρήση εικονικών συνδέσεων (δηλαδή προσωρινές συνδέσεις χωρίς φυσική υπόσταση - Σχήμα 1.1). Ασφαλείς εικονικές συνδέσεις μπορούν να υπάρξουν μεταξύ δύο υπολογιστών, ενός υπολογιστή και ενός δικτύου και μεταξύ δικτύων.



Σχήμα 1.1 Παράδειγμα ενός Εικονικού Ιδιωτικού Δικτύου

Τα VPNs επιτρέπουν σε απομακρυσμένους εργαζόμενους όπως πωλητές ή και σε υποκαταστήματα κάποιας εταιρίας (clients) να συνδέονται με ασφαλή τρόπο στον κεντρικό server ο οποίος είναι τοποθετημένος στην άκρη του τοπικού δικτύου (Local Area Network-LAN), χρησιμοποιώντας την υποδομή που παρέχεται από το δημόσιο δίκτυο (π.χ. Internet). Από την πλευρά του χρήστη, το VPN είναι ένα δίκτυο σύνδεσης point-to-point μεταξύ του client και του κεντρικού server. Η φύση του ενδιάμεσου διαδικτύου δεν ενδιαφέρει τον χρήστη καθώς σε αυτόν φαίνεται σαν ένα ενιαίο δίκτυο. Η σύνδεση που επιτελεί ένα VPN λειτουργεί με τον ίδιο τρόπο που ένα Wide Area Network (WAN) συνδέει δύο πόλεις.

1.2.1 Ποιος το χρειάζεται και γιατί να μπει στη διαδικασία;

Σήμερα, οι περισσότερες επιχειρήσεις έχουν ως κύριο μέλημα τη γεωγραφική τους επέκταση και σε άλλες γεωγραφικές περιοχές πέρα από την έδρα τους. Αρκετές εταιρίες διατηρούν κτίρια και εγκαταστάσεις σε πολλά σημεία της ίδιας χώρας ή ακόμα και του εξωτερικού. Κατά συνέπεια όλες επιθυμούν να διατηρούν ένα γρήγορο, αξιόπιστο και ασφαλή τρόπο επικοινωνίας με τα γραφεία τους. Για να καλύψουν λοιπόν τις ανάγκες των εργαζομένων τους για επικοινωνία, αρκετές επιχειρήσεις άρχισαν να δημιουργούν τα δικά τους εικονικά ιδιωτικά δίκτυα.

Τα VPNs είναι σχεδιασμένα έτσι ώστε να προσφέρουν λύσεις στις αυξημένες ανάγκες για απομακρυσμένη πρόσβαση που υπάρχουν σήμερα, όπου υπάλληλοι πρέπει να συνδεθούν με τον κεντρικό server της εταιρίας, να επικοινωνήσουν μεταξύ τους ή για παράδειγμα να ελέγχουν τα αποθέματα μιας αποθήκης ώστε να γνωρίζουν ανά πάσα χρονική στιγμή τι υπάρχει σε αυτήν. Για να παρέχεται στους εργαζόμενους η δυνατότητα αυτής της απομακρυσμένης πρόσβασης, ανεξαρτήτως απόστασης και τοποθεσίας, η εταιρία πρέπει να αναπτύξει ένα αξιόπιστο και εύκολα επεκτάσιμο σύστημα.

Τα VPNs τα χρειάζονται οι εταιρίες που θέλουν δικτυακή υποδομή, αλλά δεν είναι διατεθειμένες να πληρώσουν για να απολαμβάνουν μια τηλεπικοινωνιακή γραμμή που θα είναι "όλη δική τους", καθώς το κόστος κτήσης ενός Ιδιωτικού Δικτύου είναι μεγάλο. Από την άλλη πλευρά, η δημιουργία, η συντήρηση και η υποστήριξη επί 24ώρου βάσεως ενός ιδιωτικού δικτύου απαιτεί εξειδικευμένο και πάντα διαθέσιμο προσωπικό και είναι γνωστό ότι δεν έχουν όλες οι εταιρίες την 'πολυτέλεια' να στελεχώσουν μια τέτοια εγκατάσταση.

1.2.2 Η εταιρεία ανάλογα με τις ανάγκες της έχει τη δυνατότητα να δημιουργήσει:

- Intranet IP-VPN (ενδοεταιρικό). Είναι η πλέον συνηθισμένη περίπτωση, κατά την οποία ανταλλάσσεται εταιρική κίνηση μεταξύ των Κεντρικών Γραφείων και των τοπικών υποκαταστημάτων ή παραρτημάτων της εταιρείας.
- Extranet IP-VPN. Χρησιμοποιείται στις περιπτώσεις που υπάρχει η ανάγκη διασύνδεσης των δικτύων διαφορετικών εταιρειών που συνεργάζονται μεταξύ τους.
- VPDN (Απομακρυσμένη πρόσβαση μέσω Τηλεφωνικού Δικτύου): Σε αυτή την περίπτωση η σύνδεση με το ενδοεταιρικό περιβάλλον δεν επιτυγχάνεται με μόνιμη γραμμή, αλλά πραγματοποιείται με τηλεφωνική κλήση από τον χρήστη, όταν αυτό απαιτηθεί.

1.2.3 Απαιτήσεις από ένα VPN

Τα VPNs αποτελούνται από υλικό και λογισμικό το οποίο καλείται να ικανοποιήσει ένα σύνολο απαιτήσεων που θα κάνουν το VPN εύκολο στη χρήση και στη συντήρηση, ασφαλές και διαθέσιμο στους χρήστες. Μέσα από μια μελέτη των αναγκών του οργανισμού θα προκύψει ένα σύνολο χαρακτηριστικών για το VPN που θα εγκαταστήσει. Ο οργανισμός μπορεί, είτε να υλοποιήσει το VPN με δικά του μέσα είτε να αναθέσει την υλοποίηση σε έναν παροχέα VPN υπηρεσιών, που μπορεί να είναι ένας παροχέας υπηρεσιών Internet (ISP).

Στην τελευταία περίπτωση υπάρχουν ειδικές συμφωνίες (Service Level Agreements - SLAs) μεταξύ του χρήστη και του ISP, που περιέχουν τις απαιτήσεις του πρώτου και τις αντίστοιχες δεσμεύσεις του δεύτερου. Τα SLAs είναι το μοναδικό μέσο στη διάθεση του χρήστη με το οποίο θα εξασφαλίσει την παροχή των υπηρεσιών από τον παροχέα. Ο χρήστης πρέπει να βρει τρόπους μέτρησης και παρακολούθησης αν όντως ο παροχέας εκπληρώνει τις υποχρεώσεις του. Αν η υλοποίηση του VPN αφορά πολλούς ISP, τότε ο χρήστης στη σύνταξη του SLA θα πρέπει να προνοήσει για την εξασφάλιση της διασύνδεσής τους και της απόδοσης του τελικού συστήματος. Από την άλλη μεριά, ο παροχέας βρίσκεται αντιμέτωπος με την πρόκληση της τήρησης των διαφόρων SLAs που έχει αναλάβει. Το μεγάλο πρόβλημα που αποτελεί τροχοπέδη στην τήρηση κάποιων απαιτήσεων των SLAs είναι το χαρακτηριστικό του best effort, όπως προκύπτει από την TCP ανάλυση του Internet. Έτσι ο παροχέας πρέπει να αναπτύξει τεχνικές διαφοροποίησης των υπηρεσιών που προσφέρει ή να κατασκευάσει το δίκτυό του με τέτοιο τρόπο ώστε να εξασφαλίσει ένα καλό λόγο των απαιτήσεων των χρηστών του προς τις δυνατότητες διαχείρισης του φορτίου που περνά από αυτόν.

Η υλοποίηση ενός VPN πρέπει να υποστηρίζει τα παρακάτω χαρακτηριστικά:

☞ *Διαθεσιμότητα (Availability)*

Το VPN πρέπει να προσφέρει πρόσβαση καθ' όλη τη διάρκεια του 24ώρου. Αυτό συνεπάγεται ότι θα πρέπει να ικανοποιεί κάθε αίτηση για σύνδεση, οποτεδήποτε αυτή εμφανιστεί. Η διαθεσιμότητα δεν εξαρτάται μόνο από την ικανότητα του παροχέα να κρατά το δίκτυό του σε συνεχή λειτουργία, καθώς κάποια προβλήματα οφείλονται σε παράγοντες εκτός ελέγχου του. Η περίπτωση χρήσης του Internet ως υποδομή είναι ένα τέτοιο παράδειγμα.

☞ *Έλεγχος (Control)*

Ένα VPN μπορεί να βρίσκεται είτε κάτω από τον έλεγχο του παροχέα, είτε κάτω από τον έλεγχο του Τομέα Υποστήριξης Δικτύου της εταιρείας. Συνήθως υπάρχει η αντίληψη από τα διοικητικά στελέχη ότι η διαχείριση του VPN από προσωπικό εκτός

εταιρείας δημιουργεί περισσότερους κινδύνους επιθέσεων. Στην πραγματικότητα η επιλογή της διαχείρισης από τρίτους και συγκεκριμένα από τον φορέα υλοποίησης του VPN έχει πολλά πλεονεκτήματα. Η μεγάλη εμπειρία και εξειδίκευση των τεχνικών εξασφαλίζει γρήγορη υλοποίηση και καλή λειτουργία του VPN. Οι εφαρμογές επόπτευσης της κυκλοφορίας και συναγερμού μπορούν να εξασφαλίσουν ένα καλό επίπεδο ασφάλειας. Η δεύτερη περίπτωση έχει το πλεονέκτημα του πλήρη ελέγχου του VPN, αλλά θα πρέπει να ληφθούν σοβαρά υπόψη ο χρόνος εκπαίδευσης του προσωπικού, το κόστος απόκτησης του εξοπλισμού και ο χρόνος μέχρι να κριθεί επιχειρησιακό το δίκτυο.

☞ *Συμβατότητα (Compatibility)*

Το VPN πρέπει να είναι συμβατό με το ήδη υπάρχον δίκτυο του χρήστη. Όταν υπάρχει χρήση διαφορετικών πρωτοκόλλων, θα πρέπει να γίνουν οι απαραίτητες ενέργειες έτσι ώστε τα δύο δίκτυα να διασυνδεθούν. Για παράδειγμα μπορεί το VPN να στηρίζεται στο IP, ενώ το δίκτυο του χρήστη στο IPX. Η χρήση ενός gateway λύνει το πρόβλημα συμβατότητας προσθέτοντας ένα ακόμη επίπεδο στο σχεδιασμό και την υλοποίηση. Επίσης το δίκτυο πρέπει να φτάνει μέχρι το επίπεδο δικτύου (network layer) του μοντέλου αναφοράς OSI του οργανισμού ISO.

☞ *Ασφάλεια (Security)*

Ένα VPN δεν αποτελεί ένα ιδιωτικό δίκτυο του χρήστη όπως ήδη έχει αναφερθεί. Η χρήση της κοινής υποδομής για τη μεταφορά πληροφοριών καθιστά δυνατή την υποκλοπή τους από τρίτους. Η ασφάλεια αναφέρεται σε όλες τις ενέργειες που εκτελούνται από τα στοιχεία του VPN, όπως για παράδειγμα είναι η διαδικασία κρυπτογράφησης των δεδομένων ή η διαδικασία πιστοποίησης των χρηστών του δικτύου. Βέβαια οι απαιτήσεις για ασφάλεια μπορεί να μην ικανοποιούνται αν η πλατφόρμα που θα εγκατασταθεί το VPN παρουσιάζει αδυναμίες. Αν ένα VPN υλοποιηθεί πάνω σε κάποιο λειτουργικό σύστημα, τότε θα πρέπει να αντιμετωπιστούν τα πιθανά του προβλήματα ασφαλείας, διαφορετικά η χρήση του VPN θα είναι ανώφελη. Είναι φανερό ότι οι απαιτήσεις ασφάλειας δεν αφορούν μόνο την πολιτική του VPN στο θέμα αυτό αλλά και τα μέσα του χρήστη τα οποία θα υποστηρίξουν το δίκτυο.

☞ *Διαλειτουργικότητα (Interoperability)*

Καθώς τα VPNs είναι μια νέα τεχνολογία από πλευράς υλοποίησης, προκύπτουν πολλά θέματα συμβατότητας από τη χρήση διαφόρων προτύπων κρυπτογράφησης και ασφαλείας. Υπάρχουν πολλά προϊόντα στην αγορά με αποτέλεσμα να είναι δύσκολη η επιλογή κάποιου από αυτά. Η έλλειψη πιστοποίησης σε κάποια από αυτά δεν εξασφαλίζει το ότι καλύπτουν τα πρότυπα ασφαλείας. Υπάρχουν βέβαια οργανισμοί

πιστοποίησης που αναλαμβάνουν τον έλεγχο των προϊόντων και εκδίδουν πιστοποιητικά που δείχνουν τη συμφωνία του προϊόντος με τα διάφορα πρότυπα.

☞ *Αξιοπιστία (Reliability)*

Ένα VPN πρέπει να προσφέρει εγγυήσεις για αξιόπιστη λειτουργία ειδικά όταν υλοποιείται από κάποιον ISP, καθώς τότε η λειτουργία του εξαρτάται σε ένα σημαντικό βαθμό από αυτόν. Αν το δίκτυο σταματήσει να λειτουργεί τότε ο χρήστης το μόνο που μπορεί να κάνει είναι να περιμένει από τον ISP να λύσει το πρόβλημα. Ο χρόνος εξυπηρέτησης εξαρτάται από τον αριθμό των χρηστών που υποστηρίζει ο ISP και από το πόσο εύκολα μπορεί να διαθέσει πόρους για τη λύση του προβλήματος.

☞ *Πιστοποίηση δεδομένων και χρηστών (Data and User authentication)*

Σε κάθε υλοποίηση ενός VPN, είναι πολύ σημαντικό να προσφέρονται και οι δύο υπηρεσίες, επειδή αποτελούν σημαντικές πτυχές της ασφάλειας που θα προσφέρεται. Η πιστοποίηση δεδομένων (data authentication) αφορά την επιβεβαίωση ότι τα δεδομένα έχουν ληφθεί στο σύνολό τους και ότι δεν έχουν μεταβληθεί κατά τη μεταφορά τους. Πιστοποίηση χρήστη (user authentication) είναι η διαδικασία χορήγησης άδειας πρόσβασης στο δίκτυο. Αν ο χρήστης βρίσκεται εκτός του εταιρικού δικτύου, τότε πρέπει να γίνεται ασφαλής και αξιόπιστη εξακρίβωση της ταυτότητάς του πριν του παραχωρηθεί το δικαίωμα της πρόσβασης. Επίσης πρέπει να εξακριβωθούν και τα δικαιώματα που έχει από τη στιγμή που θα συνδεθεί στο δίκτυο, έτσι ώστε να περιορίζεται μόνο στις υπηρεσίες που του έχουν αποδοθεί.

☞ *Επιβάρυνση φορτίου (Traffic Overhead)*

Σε κάθε τεχνολογία υπάρχει εξισορρόπηση των παραγόντων λειτουργίας της και τα VPNs δε θα μπορούσαν να μην ακολουθούν τον κανόνα. Συγκεκριμένα, τα αλληλοσυγκρουόμενα χαρακτηριστικά είναι η **ευελιξία** και **ευχρηστία** απέναντι στην **ασφάλεια**, η **ταχύτητα** απέναντι στην **απόδοση** της επικοινωνίας. Η επιβάρυνση αφορά είτε το κόστος που υπεισέρχεται από την κρυπτογράφηση των δεδομένων που μεταφράζεται στο πόση υπολογιστική ισχύς καταναλώνεται, είτε στο ποσό του παραπάνω εύρους ζώνης (bandwidth) που απαιτείται για τη μετάδοση των μεγαλύτερου μεγέθους πακέτων που προκύπτουν μέσω της ενθυλάκωσης πακέτων (encapsulation). Θα πρέπει, λοιπόν, το VPN να μπορεί να είναι ευέλικτο στη διαμόρφωσή του, έτσι ώστε να καλύπτει τις διάφορες ανάγκες που θα προκύψουν κατά τη διάρκεια χρήσης του. Για παράδειγμα, θα μπορούσε να γίνεται κατηγοριοποίηση των δεδομένων ανάλογα με την αξία τους και έτσι άλλα να κρυπτογραφούνται, άλλα απλώς να πιστοποιούνται και άλλα να αποστέλλονται χωρίς να υποστούν καμία επεξεργασία.

☞ *Nonrepudiation (Μη αποποίηση ευθύνης)*

Ένα VPN πρέπει να έχει τη δυνατότητα θετικής αναγνώρισης ενός χρήστη χωρίς αυτός να μπορεί να αρνηθεί την αναγνώριση που έγινε. Η απαίτηση αυτή έχει μεγάλη σημασία για τις εφαρμογές του ηλεκτρονικού εμπορίου, διότι αν υπάρχει έστω και μια μικρή αμφιβολία για το ποιος έχει κάνει μία παραγγελία, τότε αυτή δεν μπορεί να εκτελεστεί για ευνόητους λόγους. Η εξασφάλιση αυτής της ιδιότητας μπορεί να γίνει με τη χρήση ψηφιακής υπογραφής (digital signature).

1.3 ΟΙ ΚΙΝΔΥΝΟΙ ΑΣΦΑΛΕΙΑΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Η μεγάλη έκρηξη του Παγκόσμιου Ιστού (WWW) έδωσε το έναυσμα σε απειράριθμους παροχείς συνδεσιμότητας να παρουσιάσουν σε ευρεία κλίμακα τη δυνατότητα φτηνής διαδικτύωσης με τη χρήση ενός απλού modem. Οι διορατικοί υπεύθυνοι μηχανοργάνωσης είδαν στο νέο μέσο, που έπαιρνε μορφή με ταχύτατους ρυθμούς, τον τρόπο να υλοποιήσουν εύκολα και γρήγορα το όνειρο της διαδικτύωσης πολλών γεωγραφικά διάσπαρτων υποκαταστημάτων των εταιριών τους, μέσω συνεργασίας με κάποιον παροχέα Internet, αρκεί να έχει σημεία παρουσίας (POPs) στις περιοχές που τους ενδιέφερε.

Ωστόσο, η λύση αυτή εμπεριέχει κάποια σημαντικά προβλήματα : Τα μονοπάτια μεταφοράς της πληροφορίας είναι, κατά ένα τρόπο, «δημόσια» αφού ο παροχέας χρησιμοποιεί τα κυκλώματά του για τη μεταφορά δεδομένων και άλλων πελατών του, ένα γεγονός που σίγουρα αποτελεί σημαντικό ανασταλτικό παράγοντα για μια εταιρία που θέλει να προστατεύσει αποτελεσματικά τα δεδομένα της από τα περίεργα μάτια του ανταγωνισμού.

Τα κλεμμένα ή διαγραμμένα εταιρικά στοιχεία μπορούν να έχουν σημαντικές επιπτώσεις και να κοστίσουν χρήματα στην επιχείρηση. Εάν κλαπούν τα αρχεία προγραμμάτων ή η βάση δεδομένων των πελατών μιας μικρής επιχείρησης, τότε η επιχείρηση μπορεί και να σταματήσει τη λειτουργία της.

Δεδομένου ότι το Διαδίκτυο είναι ένα δημόσιο δίκτυο μεταγωγής πακέτων, υπάρχει πάντα ο κίνδυνος κάποιος να έχει πρόσβαση στο δίκτυο της εταιρίας και να "σπάσει" ένα μέρος του δικτύου. Εάν το εταιρικό δίκτυό σας συνδέεται πάνω στο Διαδίκτυο και η ασφάλειά σας είναι αμελής, αυτός που θα θέλει να "σπάσει" το σύστημα μπορεί να είναι σε θέση να έχει πρόσβαση στο δίκτυό σας χρησιμοποιώντας μια οποιαδήποτε σύνδεση ενός οποιουδήποτε ISP στον κόσμο. Ακόμα και οι απλοί χρήστες μπορούν να λάβουν και να χρησιμοποιήσουν τα αυτοματοποιημένα εργαλεία "ελέγχου ασφάλειας" για να αναζητήσουν τις οπές στο δίκτυο μιας επιχείρησης. Το χειρότερο είναι ότι κανείς δεν ξέρει ποτέ τι μπορεί να γίνει και καλύτερα να σιγουρευόμαστε ότι ένα VPN είναι αρκετά καλό για να προστατεύσει τα δεδομένα της επιχείρησης.

1.3.1 Τι προστατεύουμε με τα VPNs ;

Τα πρώτα πράγματα που έχουν άμεση ανάγκη προστασίας και ασφάλειας είναι τα αρχεία στους δικτυωμένους υπολογιστές μιας εταιρίας: έγγραφα που περιέχουν α) τα μελλοντικά σχέδια της επιχείρησης, β) υπολογισμούς με λογιστικό φύλλο (spreadsheet) που περιγράφουν την οικονομική ανάλυση μιας νέας εισαγωγής προϊόντων, γ) βάσεις δεδομένων των αρχείων των μισθοδοτικών καταστάσεων και των φόρων της, ή ακόμα και δ) μια αξιολόγηση ασφάλειας του δικτύου της επισημαίνοντας τις οπές και τα προβληματικά μηχανήματα. Ακόμα ε)αρχεία που αφορούν τις υπηρεσίες που χορηγεί η εταιρία στους υπαλλήλους και τους πελάτες της, στ) τα υπολογιστικά στοιχεία που είναι διαθέσιμα για χρήση, καθώς επίσης και ζ) τη φήμη της. Παραδείγματος χάριν, μια αποτυχία ασφάλειας μπορεί να προκαλέσει το ηλεκτρονικό ταχυδρομείο των προμηθευτών της να επιστρέψει πίσω σε αυτούς, ή να εμποδίσει τους χρήστες της να συνδεθούν με άλλες σελίδες.

Το ευκολότερο πράγμα θα ήταν η εταιρία να απομονώσει, να ταξινομήσει σε πίνακες, και να κλειδώσει τα ιδιωτικά στοιχεία της. Παραπάνω από τα μισά από τα στοιχεία που διαχειρίζεται και διανέμει μπορεί να χρειάζονται κάποιο είδος ασφάλειας. Αρκεί να σκεφτούμε, ακόμα και κάτι τόσο αβλαβές όπως τα αρχεία και οι διευθύνσεις των πελατών ότι θα μπορούσαν να χρησιμοποιηθούν ενάντια στην ίδια την εταιρία με μια αρνητική εκστρατεία διαφήμισης. Αυτό μπορεί να την βλάψει πολύ χειρότερα από μια αρνητική εκστρατεία που στοχεύει σε ένα τυχαίο κομμάτι του πληθυσμού.

Δυστυχώς, δεν είναι τόσο εύκολο να κρατηθούν όλα τα ιδιωτικά στοιχεία κλειδωμένα σε μια ενιαία, προστατευμένη περιοχή. Ο κύριος οικονομικός υπάλληλος μιας επιχείρησης μπορεί να χρειάζεται να έχει πρόσβαση στις οικονομικές πληροφορίες όταν ταξιδεύει, ή ένας προγραμματιστής που εργάζεται από το σπίτι μπορεί να πρέπει να έχει πρόσβαση στον κώδικα ενός προγράμματος. **Τα VPNs βοηθούν στην ασφαλή διαβίβαση αρχείων έξω από το δίκτυό σας ανάλογα με την πολιτική ασφάλειας που ακολουθείται.**

1.3.2 Πώς τα VPNs λύνουν τα ζητήματα ασφάλειας Διαδικτύου;

Τα VPNs χρησιμοποιούν διάφορες τεχνολογίες για να προστατεύσουν τα στοιχεία που "ταξιδεύουν" σε ολόκληρο το Διαδίκτυο. Οι σημαντικότερες είναι τα firewalls, η πιστοποίηση ταυτότητας, η κρυπτογράφηση και το tunneling.

☑ Firewalls

Το Firewall (δικτυακό ανάχωμα) είναι ένα φράγμα μεταξύ ενός ιδιωτικού και προστατευόμενου δικτύου (το οποίο υποθέτουμε ότι είναι ασφαλές) και ενός άλλου δικτύου συνήθως δημόσιου, όπως το Internet (το οποίο υποθέτουμε ότι δεν είναι

ασφαλές). Ο σκοπός ενός Firewall είναι να εμποδίσει την ανεπιθύμητη και μη εξουσιοδοτημένη επικοινωνία προς ή από το προστατευόμενο δίκτυο.

Αν και τα περισσότερα πακέτα VPN από μόνα τους δεν εφαρμόζουν άμεσα τα Firewalls, αυτά θα πρέπει να είναι ένα αναπόσπαστο μέρος ενός VPN. Η ιδέα είναι να χρησιμοποιηθεί το Firewall για να κρατήσει τους ανεπιθύμητους επισκέπτες έξω από το δίκτυο της εταιρίας, ενώ να επιτρέπει την πρόσβαση στους χρήστες του VPN.

Ο δρομολογητής του δικτύου μπορεί να παίξει ακόμα και το ρόλο του Firewall. Ο Router μπορεί να προγραμματιστεί με τέτοιο τρόπο, έτσι ώστε να απαγορεύει την πρόσβαση στο εσωτερικό του δικτύου σε ομάδες χρηστών ή και σε όλους τους χρήστες του διαδικτύου.

Για παράδειγμα, δρομολογητές που υποστηρίζουν τις τεχνολογίες VPN είναι ο Private Internet Exchange (PIX) της Cisco και ο Robotics Total Control της 3Com/U.S..

Εκτός όμως από αυτή τη λύση, και για περισσότερη ευελιξία στην ασφάλεια του δικτύου, μπορούν να χρησιμοποιηθούν ειδικά εργαλεία λογισμικού (software firewalls) που συνεργάζονται με το λειτουργικό σύστημα του server ή έχουν το δικό τους λειτουργικό σύστημα. Ένα software firewall θα πρέπει να λειτουργεί σε έναν ανεξάρτητο ηλεκτρονικό υπολογιστή, η αποστολή του οποίου θα είναι αποκλειστικά και μόνο η λειτουργία του Firewall.

Τέλος, ως εναλλακτική και ακριβότερη λύση μπορεί να χρησιμοποιηθεί ένα hardware firewall, μια ειδική συσκευή με μοναδική λειτουργία την παροχή ασφάλειας υψηλού επιπέδου στο δίκτυο της επιχείρησης.

Επίσης, μια κοινή μέθοδος προστασίας ενός δικτύου η οποία επιτρέπει την πρόσβαση στις υπηρεσίες VPN, είναι τα proxies. Οι κεντρικοί υπολογιστές proxies είναι χαρακτηριστικά μια λύση λογισμικού που τρέχει μέσω ενός λειτουργικού συστήματος δικτύου, όπως το Unix, τα Windows NT, ή το Novell Netware.

☑ Πιστοποίηση ταυτότητας

Οι τεχνικές πιστοποίησης ταυτότητας είναι ουσιαστικές στα VPNs, δεδομένου ότι εξασφαλίζουν στα συμβαλλόμενα μέρη ότι ανταλλάσσουν τα στοιχεία με το σωστό χρήστη. Η πιστοποίηση ταυτότητας είναι ανάλογη με "την καταγραφή" σε ένα σύστημα του ονόματος χρήστη και ενός κωδικού πρόσβασης ανά χρήστη. Τα VPNs, εντούτοις, απαιτούν πιο αυστηρές μεθόδους πιστοποίησης ταυτότητας για να επικυρωθούν οι ταυτότητες. Τα περισσότερα συστήματα ελέγχου γνησιότητας VPN είναι βασισμένα σε ένα σύστημα μοιραζόμενου κλειδιού (shared key). Τα κλειδιά τρέχουν μέσω ενός hash αλγορίθμου (hash algorithm: αλγόριθμος κατακερματισμού)*, ο οποίος παράγει μια hash αξία. Το άλλο συμβαλλόμενο μέρος κρατώντας τα κλειδιά θα παραγάγει τη hash αξία του και θα την συγκρίνει με αυτήν που έλαβε από την άλλη πλευρά. Η hash αξία που στέλνεται σε ολόκληρο το

Διαδίκτυο δεν έχει νόημα για έναν παρατηρητή, έτσι κάποιος που θέλει να «εισβάλλει» στο δίκτυο δεν θα ήταν σε θέση να βρει έναν κωδικό πρόσβασης. Το πρωτόκολλο πρόκλησης πιστοποίησης ταυτότητας χειραψιών (CHAP) είναι ένα καλό παράδειγμα μιας μεθόδου πιστοποίησης ταυτότητας που χρησιμοποιεί αυτό το σχέδιο. Ένα άλλο κοινό σύστημα ελέγχου γνησιότητας είναι το RSA (Rivest Shamir Adlemen – βλ. Κεφάλαιο 2).

Η πιστοποίηση ταυτότητας εκτελείται χαρακτηριστικά στην αρχή μιας περιόδου επικοινωνίας, και έπειτα τυχαία κατά τη διάρκεια μιας περιόδου επικοινωνίας για να εξασφαλίσει ότι "δεν μπήκε" στη συνομιλία κάποιος υποκλοπέας. Η πιστοποίηση ταυτότητας μπορεί επίσης να χρησιμοποιηθεί για να εξασφαλίσει την ακεραιότητα στοιχείων. Τα ίδια τα στοιχεία μπορούν να σταλούν μέσω ενός hashing αλγορίθμου για να παραγάγουν μια αξία που είναι συμπεριλαμβανόμενη ως checksum στο μήνυμα. Λέγοντας checksum (άθροισμα ελέγχου) εννοούμε το πεδίο ελέγχου της επικεφαλίδας του μηνύματος και είναι χρήσιμο για την ανίχνευση λαθών που δημιουργούνται από χαλασμένες λέξεις μνήμης μέσα σ' έναν δρομολογητή. Οποιαδήποτε απόκλιση στο checksum που στέλνεται από τον έναν κόμβο στον επόμενο σημαίνει πως τα δεδομένα αλλοιώθηκαν κατά τη διάρκεια της μεταφοράς, ή παρεμποδίστηκαν και τροποποιήθηκαν στη διαδρομή.

*Οι Hash αλγόριθμοι χρησιμοποιούνται χαρακτηριστικά για να παρέχουν ένα ψηφιακό δακτυλικό αποτύπωμα του περιεχομένου ενός αρχείου, που χρησιμοποιείται συχνά για να εξασφαλίσει ότι το αρχείο δεν έχει αλλάξει από έναν εισβολέα ή έναν ιό. Οι Hash λειτουργίες υιοθετούνται συνήθως από πολλά λειτουργικά συστήματα για να κρυπτογραφήσουν τους κωδικούς πρόσβασης.

☑ Κρυπτογράφηση

Όλα τα VPNs υποστηρίζουν κάποιον τύπο τεχνολογίας κρυπτογράφησης, ο οποίος ουσιαστικά "συσκευάζει" τα στοιχεία σε έναν ασφαλή φάκελο. Η κρυπτογράφηση θεωρείται συχνά τόσο ουσιαστική όσο η πιστοποίηση ταυτότητας, γιατί προστατεύει τα μεταφερόμενα στοιχεία από υποκλοπή. Υπάρχουν δύο δημοφιλείς τεχνικές κρυπτογράφησης που υιοθετούνται στα VPNs: η κρυπτογράφηση μέσω μυστικού ή ιδιωτικού κλειδιού και η κρυπτογράφηση μέσω δημόσιου κλειδιού.

Στην κρυπτογράφηση μέσω ιδιωτικού κλειδιού, υπάρχει ένας κοινός μυστικός κωδικός πρόσβασης ή ένα σύνθημα που είναι γνωστό σε όλα τα συμβαλλόμενα μέρη που χρειάζονται πρόσβαση στις κρυπτογραφημένες πληροφορίες. Αυτό το ενιαίο κλειδί χρησιμοποιείται για να κρυπτογραφήσει και για να αποκρυπτογραφήσει τις πληροφορίες. Τα πρότυπα κρυπτογράφησης στοιχείων (DES – Data Encryption Standard), που το σύστημα Unix crypt χρησιμοποιεί για να κρυπτογραφήσει τους κωδικούς πρόσβασης, είναι ένα παράδειγμα μιας μεθόδου κρυπτογράφησης μέσω ιδιωτικού κλειδιού.

Ένα πρόβλημα που δημιουργείται με τη χρήση του ιδιωτικού κλειδιού κρυπτογράφησης για τα κοινά δεδομένα είναι ότι όλα τα συμβαλλόμενα μέρη που χρειάζονται την πρόσβαση στα κρυπτογραφημένα στοιχεία πρέπει να ξέρουν το ιδιωτικό αυτό κλειδί. Ενώ αυτό μπορεί να θεωρηθεί χρήσιμο για μια μικρή ομάδα ανθρώπων, μπορεί να γίνει ακατόρθωτο για ένα μεγάλο δίκτυο. Τι θα γίνει όμως αν κάποιος από την ομάδα φύγει; Η απάντηση είναι ότι θα πρέπει να καταργηθεί το παλιό κλειδί, να καθιερωθεί ένα νέο και με ασφάλεια να ειδοποιηθούν οι χρήστες για την αλλαγή του κλειδιού.

Η κρυπτογράφηση δημοσίου κλειδιού περιλαμβάνει ένα δημόσιο και ένα ιδιωτικό κλειδί. Το δημόσιο κλειδί γίνεται γνωστό σε όλους ενώ μόνο ο χρήστης γνωρίζει το ιδιωτικό κλειδί. Εάν ο χρήστης θέλει να στείλει ευαίσθητα δεδομένα σε κάποιον, τα κρυπτογραφεί με έναν συνδυασμό ιδιωτικού και δημόσιου κλειδιού. Όταν ο παραλήπτης το λάβει το αποκρυπτογραφεί χρησιμοποιώντας το δημόσιο και το ιδιωτικό κλειδί. Το μέγεθος του δημόσιου και του ιδιωτικού κλειδιού μπορεί να είναι πολύ μεγάλο, τόσο ώστε να μη μπορεί κάποιος να το θυμάται και εξαρτάται από το λογισμικό. Γι' αυτό καταχωρούνται συχνά στον σκληρό δίσκο εκείνου που κρυπτογραφεί τα δεδομένα. Λόγω αυτού, τα ιδιωτικά κλειδιά καταχωρούνται χαρακτηριστικά χρησιμοποιώντας μια μυστική βασική μέθοδο κρυπτογράφησης, όπως η DES, και έναν κωδικό πρόσβασης ή ένα σύνθημα που μπορεί κανείς να θυμηθεί, έτσι ώστε ακόμα κι αν κάποιος μπει στο σύστημα, δεν θα είναι σε θέση να δει ποιο είναι το ιδιωτικό κλειδί.

Το Pretty Good Privacy(PGP) είναι ένα γνωστό πρόγραμμα ασφάλειας δεδομένων που χρησιμοποιεί δημόσιο κλειδί κρυπτογράφησης. Είναι ένα από τα ευρύτερα χρησιμοποιούμενα δημόσια προγράμματα συστήματος κρυπτογραφίας σήμερα. Αναπτυγμένο από τον Philip Zimmermann, το PGP είναι διαθέσιμο ως σύνδεση για πολλούς χρήστες ηλεκτρονικού ταχυδρομείου, όπως το Microsoft Exchange και Outlook, και Qualcomm's Eudora. Το PGP μπορεί να χρησιμοποιηθεί για να υπογράψει ή να κρυπτογραφήσει τα μηνύματα ηλεκτρονικού ταχυδρομείου μόνο με το στιγμιαίο πάτημα του ποντικιού.

Το RSA είναι ένα άλλο σύστημα δημόσιου κλειδιού που είναι ιδιαίτερα δημοφιλές στις εμπορικές συναλλαγές. Το βασικό μειονέκτημα του δημόσιου κλειδιού κρυπτογράφησης είναι ότι, για ένα συγκεκριμένο όγκο δεδομένων, η διαδικασία κρυπτογράφησης είναι χαρακτηριστικά πιο αργή απ' ότι με την κρυπτογράφηση ιδιωτικού κλειδιού.

Τα VPNs, εντούτοις, χρειάζεται να κρυπτογραφούν τα δεδομένα σε άμεσο χρόνο, παρά να αποθηκεύουν τα δεδομένα σαν αρχείο όπως θα γινόταν με τη χρήση του PGP. Εξαιτίας αυτού, τα κρυπτογραφημένα μηνύματα που περνούν από ένα δίκτυο, όπως ένα VPN, κρυπτογραφούνται χρησιμοποιώντας το ιδιωτικό κλειδί που χρησιμοποιείται μόνο όσο διαρκεί η επικοινωνία που απαιτείται για τη μεταγωγή των

δεδομένων. Το ιδιωτικό αυτό κλειδί (χαρακτηριστικά μικρότερο από τα δεδομένα) κρυπτογραφείται χρησιμοποιώντας δημόσιο κλειδί κρυπτογράφησης και στέλνεται κατά τη διάρκεια της σύνδεσης.

Το επόμενο βήμα για τα VPNs είναι το ασφαλές IP (Internet Protocol), ή IPSec. Το IPSec είναι μια σειρά διάταξης των προτάσεων από το IETF (Internet Engineering Task Force) περιγράφοντας ένα ασφαλές πρωτόκολλο IP για IPv4 και IPv6. Αυτές οι επεκτάσεις θα παρείχαν την κρυπτογράφηση στο επίπεδο IP, παρά στα υψηλότερα επίπεδα που η SSL (Secure Socket Layer)που τα περισσότερα πακέτα VPN παρέχουν. Το IPSec δημιουργεί ανοικτά πρότυπα για VPNs.

☑ Tunneling

Ένα tunnel (σήραγγα) είναι ένας όρος δικτύωσης με ένα κατάλληλο όνομα. Αναφέρεται σε μια σύνδεση, κρυπτογραφημένη συνήθως, η οποία συνδέει δύο υπολογιστές μαζί μέσω ενός άλλου, συνήθως μη-έμπιστο δίκτυο. Φανταστείτε ότι υπάρχει πολύ "κίνηση" μεταξύ του lap-top σας και ενός κεντρικού υπολογιστή στο εσωτερικό, προστατευμένο δίκτυό σας. Δεν θέλετε να "ρίξετε" τα αρχεία σας στην "κίνηση" με την ελπίδα ότι θα φτάσουν εκεί που θέλετε. Θέλετε πρώτα να σχεδιάσετε σε πρώτη μορφή μια προστατευμένη σήραγγα από σας στη μηχανή σας, και να στέλνετε έπειτα αυτά που θέλετε μέσω αυτής της σήραγγας (tunnel).

Πάρτε αυτό το χαρακτηριστικό σενάριο: Είστε στη δουλειά σας ή στο σπίτι, δακτυλογραφώντας στο lap-top σας. Θέλετε να ανακτήσετε το ηλεκτρονικό ταχυδρομείο σας από το γραφείο σας με έναν POP client (Netscape Mail, Eudora, fetchmail, κ.λ.π.). Εάν συνδεθείτε με τη μηχανή άμεσα, ο χρήστης του ηλεκτρονικού ταχυδρομείου σας (e-mail client) θα στείλει την άδεια εισόδου και τον κωδικό πρόσβασής σας. Αυτό σημαίνει ότι ένας επιτήδειος κάπου ανάμεσα σε σας και στον κεντρικό υπολογιστή ταχυδρομείου σας (είτε αλλού στο ασύρματο δίκτυό σας, ή ακόμα και "στο καλώδιο" εάν χωρίζεστε από ένα μη-έμπιστο δίκτυο) θα μπορούσε να επιλέξει ένα αντίγραφο των πληροφοριών σας που βρίσκεται καθ' οδόν. Αυτή η άδεια εισόδου θα μπορούσε έπειτα να χρησιμοποιηθεί όχι μόνο για να κερδίσει ο "εισβολέας" την αναρμόδια πρόσβαση στο ηλεκτρονικό ταχυδρομείο σας, αλλά και σε πολλές άλλες περιπτώσεις.

Για να το αποτρέψετε αυτό, μπορείτε να χρησιμοποιήσετε τις δυνατότητες κάλυψης του tunneling του SSH. Μια σήραγγα SSH λειτουργεί κάπως έτσι: Αντί να συνδεθούμε με τον κεντρικό υπολογιστή ταχυδρομείου άμεσα, καθιερώνουμε μια σύνδεση SSH στο εσωτερικό δίκτυο που βρίσκεται ο κεντρικός υπολογιστής ταχυδρομείου (συχνά, ο ίδιος ο κεντρικός υπολογιστής ταχυδρομείου). Το λογισμικό χρηστών SSH σας εγκαθιστά έναν μηχανισμό διαβίβασης, έτσι ώστε η κυκλοφορία που πηγαίνει στο POP του lap-top σας διαβιβάζεται μέσω του κρυπτογραφημένου tunnel και τελειώνει στο POP του κεντρικού υπολογιστή ταχυδρομείου. "Σημαδεύετε"

έπειτα το χρήστη ηλεκτρονικού ταχυδρομείου σας στο τοπικό POP λιμένα σας, και σκέφτεται ότι μιλά στο απομακρυσμένο τέλος (μόνο αυτή τη φορά, ολόκληρη η περίοδος επικοινωνίας κρυπτογραφείται).

Με το tunnel, καθένας που προσπαθεί να ελέγξει τη συνομιλία μεταξύ του lap-top σας και του κεντρικού υπολογιστή ταχυδρομείου θα πάρει ως αποτέλεσμα κάτι που μοιάζει με το θόρυβο γραμμών.

Πολλά πακέτα VPN χρησιμοποιούν το tunneling για να δημιουργήσουν ένα ιδιωτικό δίκτυο, συμπεριλαμβάνοντας τα: AltaVista Tunnel, το Point-to-Point Tunneling Protocol (PPTP), το Layer 2 Forwarding Protocol και το IPSec's tunnel mode.

1.4 ΟΙ ΛΥΣΕΙΣ ΤΟΥ VPN

Ένα VPN είναι ένα σύνολο από χρήσιμες τεχνολογίες. Τώρα οι επιχειρήσεις δικτύωσης και οι ISPs έχουν συνειδητοποιήσει την αξία ενός VPN και προσφέρουν προϊόντα που κάνουν για σας τη "χοντρή" δουλειά. Επιπλέον, υπάρχει μια κατάταξη από ελεύθερο λογισμικό διαθέσιμη στο Διαδίκτυο (συνήθως για τα συστήματα Unix) που μπορεί να χρησιμοποιηθεί για να δημιουργήσει ένα VPN. Παρακάτω θα δούμε μερικές εμπορικές και ελεύθερες λύσεις λεπτομερώς. Το ποιο λογισμικό θα επιλέξει μια εταιρία για το δίκτυό της θα εξαρτηθεί από τις πηγές (χρήματα) που είναι διαθέσιμες, τις πλατφόρμες που χρησιμοποιεί, την τοπολογία του δικτύου, το χρόνο που επιθυμεί να ξοδέψει για την εγκατάσταση και τη διαμόρφωση του λογισμικού και το εάν θέλει εμπορική υποστήριξη ή όχι. Δεν μπορούμε να καλύψουμε κάθε προμηθευτή και προϊόν, αλλάζουν πολύ γρήγορα. Αντ' αυτού, προσφέρουμε οδηγίες που οι εταιρίες μπορούν να χρησιμοποιήσουν σε όλα τα δίκτυα και λεπτομέρειες μερικών "σταθερών" προϊόντων.

Τα πακέτα VPN κυμαίνονται από λύσεις λογισμικού που τρέχουν ή ενσωματώνονται σε ένα λειτουργικό σύστημα του δικτύου (όπως το AltaVista Tunnel ή το CheckPoint Firewall-1 στα Windows ή στη Unix), από routers και firewalls hardware (όπως εκείνοι της Cisco και της Ascend), μέχρι και ενσωματωμένες λύσεις hardware που σχεδιάζονται συγκεκριμένα για τις λειτουργίες του VPN (όπως το VPNet και το Bay Networks Extranet Switch). Μερικά πρωτόκολλα VPN, όπως το SSH ή το SSL, απέκτησαν δημοτικότητα για την εκτέλεση άλλων λειτουργιών, αλλά από τότε χρησιμοποιούνται και για τα VPNs επίσης.

Εκτός από τα προϊόντα, οι ISPs προσφέρουν επίσης υπηρεσίες VPN στους πελάτες τους. Το Tunneling πραγματοποιείται συνήθως στον ISP εξοπλισμό. Εάν και τα δύο άκρα της σύνδεσης είναι μέσω του ίδιου ISP, εκείνο το ISP μπορεί να προσφέρει μια συμφωνία επιπέδων υπηρεσίας (SLA – Service Level Agreement) που εγγυάται ένα ορισμένο μέγιστο ποσό λάθους.

1.4.1 Η ποιότητα των υπηρεσιών

Η χρήση ενός VPN πέρα από το Διαδίκτυο αυξάνει το ζήτημα της αξιοπιστίας. Το Διαδίκτυο δεν είναι πάντα το πιο αξιόπιστο δίκτυο, εκ φύσεως. Δρομολογώντας ένα πακέτο από ένα σημείο σε ένα άλλο, αυτό μπορεί να περάσει μέσω πολλών διαφορετικών δίκτυα ποικίλων ταχυτήτων, αξιοπιστίας και χρήσης – το καθένα "τρέχει" από μια διαφορετική επιχείρηση. Οποιοδήποτε από αυτά τα δίκτυα θα μπορούσε να προκαλέσει προβλήματα για ένα VPN.

Η έλλειψη αξιοπιστίας του Διαδικτύου, και το γεγονός ότι καμία οντότητα δεν το ελέγχει, καθιστούν τα προβλήματα ανίχνευσης λαθών ενός VPN δύσκολα για έναν χειριστή δικτύων. Εάν ένας χρήστης δεν μπορεί να συνδεθεί με έναν απομακρυσμένο server στην εταιρική έδρα, ή υπάρχει πρόβλημα με μια σύνδεση μισθωμένης γραμμής, ο χειριστής δικτύων ξέρει ότι υπάρχει ένας περιορισμένος αριθμός πιθανοτήτων για το που το πρόβλημα μπορεί να εμφανιστεί: στη μηχανή ή το δρομολογητή του απομακρυσμένου χρήστη, στην επιχείρηση τηλεπικοινωνιών που παρέχει τη σύνδεση, ή στη μηχανή ή το δρομολογητή της εταιρικής έδρας. Για ένα VPN πέρα από το Διαδίκτυο, το πρόβλημα θα μπορούσε να είναι στη μηχανή του απομακρυσμένου χρήστη, στο απομακρυσμένο ISP, σε ένα από τα ενδιάμεσα δίκτυα, στο ISP της εταιρικής έδρας, ή στη μηχανή ή το δρομολογητή της ίδιας της εταιρίας. Αν και μερικά μεγάλα ISPs προσφέρουν εγγυήσεις για την ποιότητα των υπηρεσιών με την υπηρεσία VPN τους (εάν όλα τα συμβαλλόμενα μέρη συνδέονται με το δίκτυό τους), τα μικρότερα ISPs δεν μπορούν να προσφέρουν μια τέτοια εγγύηση.

1.5 ΒΙΒΛΙΟΓΡΑΦΙΑ

1.Virtual Private Networks
Second Edition
Charlie Scott, Paul Wolfe and Mike Erwin

2.Δίκτυα Η/Υ
Andrew S. Tanenbaum
Third Edition

3.Περιοδικό OPEN newsletter
(έκδοση της OPEN SERVICES)
Φεβρουάριος 2000

4.ΔΙΕΥΘΥΝΣΕΙΣ ΣΤΟ INTERNET:

www.technojunkie.gr

www.shmoo.com

www.it.uom.gr

ΚΕΦΑΛΑΙΟ 2°

2.1 ΒΑΣΙΚΕΣ ΤΕΧΝΟΛΟΓΙΕΣ ΤΩΝ VPNs

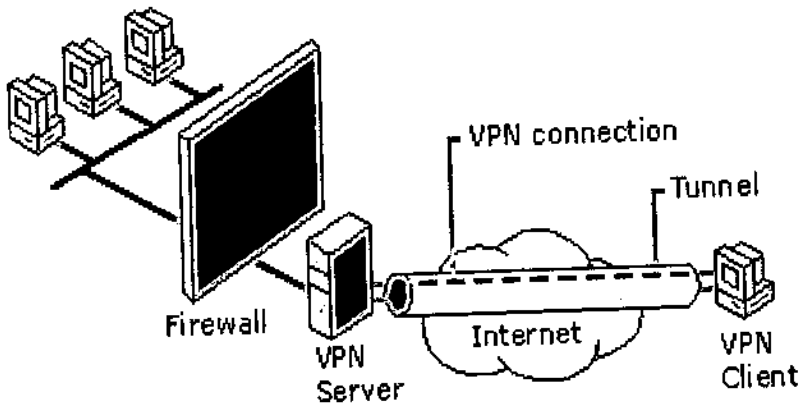
Στο κεφάλαιο αυτό θα εστιάσουμε στις τεχνολογίες που χρησιμοποιούνται για να "χτίσουν" ένα εικονικό ιδιωτικό δίκτυο. Δεδομένου ότι συζητήσαμε στο κεφάλαιο 1, (γιατί να σχεδιάσουμε ένα εικονικό ιδιωτικό δίκτυο), υπάρχουν δύο ανταγωνιστικά στρατόπεδα όταν μιλάμε για τη σύνδεση των δικτύων. Το πρώτο στρατόπεδο θεωρεί ως πιο σημαντικό τη δυνατότητα πρόσβασης στα δεδομένα οπουδήποτε κι αν βρίσκεται ο χρήστης και οπουδήποτε μπορεί να είναι τα στοιχεία. Το δεύτερο υπογραμμίζει ότι η προστασία των ίδιων των δεδομένων, του περιεχομένου, είναι το πιο σημαντικό και πρέπει να προστατευθούν για να μην έχουν πρόσβαση σε αυτά κάποια αναρμόδια πρόσωπα. Όπως μπορείτε να δείτε, αυτές οι δύο έννοιες δεν αποκλείουν η μια την άλλη. Καθώς όλες οι εταιρίες εστιάζουν στο να μοιράζονται όλο και περισσότερες πληροφορίες έτσι ώστε η καθεμιά να μπορεί να βρει αυτό που θέλει, πρέπει επίσης να εστιάζουν στην προστασία αυτών των πληροφοριών έτσι ώστε οι άλλες εταιρίες να μην τις εκμεταλλευθούν.

Επειδή το Διαδίκτυο είναι μια απέραντη συλλογή δεδομένων και πηγών, είναι σαφές ότι το να μοιράζεται κανείς πληροφορίες με άλλους συμμετέχοντες μπορεί να τον βοηθήσει να ευημερήσει. Δεν είναι σαφές, εντούτοις, σε τι κίνδυνο θέτει κανείς τον εαυτό του όταν συνδέεται. Μερικές επιχειρήσεις βλέπουν το Διαδίκτυο ως τεράστια αναξιοποίητη αγορά, γεμάτη από καταναλωτές και ευκαιρίες διαφήμισης, αλλά δεν συνειδητοποιούν ότι το Διαδίκτυο έχει και την όψη ενός "υπόκοσμου" επίσης. Αυτό είναι που αναγκάζει τον καθένα να προστατεύσει τα δεδομένα του. Η προστασία των ιδιωτικών δεδομένων είναι ο πυρήνας του εικονικού ιδιωτικού δικτύου και οι δύο πιο σχετικές τεχνολογίες (τα firewalls και η κρυπτογράφηση) υπάρχουν γι' αυτό το σκοπό.

Σε αυτό το κεφάλαιο, θα παρουσιάσουμε μια επισκόπηση και ένα υπόβαθρο των τεχνολογιών που χρησιμοποιούνται για να "χτίσουν" ένα ασφαλές VPN, και το πώς ενσωματώνονται στα προϊόντα και τις υπηρεσίες. Θα ξεκινήσουμε με το πως οι τεχνικές των firewalls χρησιμοποιούνται για να προστατεύσουν ένα ολόκληρο δίκτυο στους δρομολογητές πυλών του. Έπειτα, θα σας παρουσιάσουμε το υπόβαθρο της πιστοποίησης ταυτότητας: πώς χρησιμοποιείται με μια παραδοσιακή λογική και πώς θα επεκταθεί χρησιμοποιώντας ένα VPN. Μετά από αυτό, θα αναλύσουμε τις τεχνικές κρυπτογράφησης και πώς χρησιμοποιούνται σε συνδυασμό με τους αλγόριθμους κρυπτογράφησης με VPNs. Επίσης, θα ερευνήσουμε τα πρωτόκολλα που έχουν προκύψει από την αύξηση των VPNs.

2.2 Η ΕΠΕΚΤΑΣΗ ΤΩΝ FIREWALLS

Η πρώτη, από τις σχετικές με την ασφάλεια, τεχνολογία που καλύπτουμε είναι το firewall. Ένα firewall είναι ένα σύστημα που στέκεται ανάμεσα στο εσωτερικό δίκτυο και στον έξω κόσμο. Τα firewalls έχουν υιοθετηθεί στα μεγάλα δημόσια δίκτυα εδώ και πολλά χρόνια και είναι ένα καλό ξεκίνημα στην ανάπτυξη μιας στρατηγικής ασφάλειας. Ο λόγος που ξεκινάμε με τα firewalls είναι ότι τοποθετούνται γενικά στο σημείο στο οποίο το ιδιωτικό δίκτυο διασυνδέεται με ένα δημόσιο δίκτυο, όπως το Διαδίκτυο. Αν και όχι τέλεια στρατηγική, ένα firewall είναι εύκολο να διαμορφωθεί επειδή απαιτεί μόνο την τροποποίηση ενός δρομολογητή πυλών.



Σχήμα 2.1 VPN με τη χρήση Firewall

Φυσικά, εάν μια εταιρία έχει ένα μεγάλο, πολλαπλά-συνδεδεμένο WAN, με πολλά "μονοπάτια" στο Διαδίκτυο, πρέπει να σημειωθεί ότι θα χρειαστεί να δημιουργήσει ένα firewall για κάθε σημείο διασύνδεσης.

2.2.1 Τι ακριβώς είναι ένα firewall;

Το Αμερικανικό Τμήμα Υπεράσπισης (U.S. Department of Defense), πιθανώς η παγκόσμια αρχή στους ελέγχους ευαισθησίας και ασφάλειας δεδομένων, χρησιμοποίησε ένα σύστημα από οντότητες που καθορίστηκαν ως επίπεδα ασφάλειας για να περιορίσουν την πρόσβαση στα ταξινομημένα έγγραφα. Υποστηρίζεται ότι για να εξασφαλιστούν τα ιδιαίτερα ευαίσθητα δεδομένα, δεν πρέπει ποτέ να συνδεθεί ο υπολογιστής με ένα εξωτερικό δίκτυο. Αυτή είναι φυσικά η καλύτερη στρατηγική firewall που υπάρχει, αλλά είναι πολύ περιοριστική για να είναι πρακτική. Ξέρουμε την αξία της διασύνδεσης, απλά το καλύτερο firewall για τα εξαιρετικά ευαίσθητα "δεδομένα" είναι να τα απομονώσουμε σε έναν υπολογιστή χωρίς καμία σύνδεση δικτύου.

Τα firewalls εξυπηρετούν συνήθως δύο βασικές λειτουργίες για έναν χειριστή δικτύων. Η πρώτη είναι να ελέγξει ποιες μηχανές μπορεί να δει ένας "ξένος" και τις υπηρεσίες σε εκείνες τις μηχανές στις οποίες μπορεί να έχει κάποιος πρόσβαση. Η

δεύτερη ελέγχει ποιες μηχανές μπορεί να δει στο Διαδίκτυο ένας εσωτερικός χρήστης, όπως και ποιες υπηρεσίες μπορεί να χρησιμοποιήσει.

2.2.2 Πολιτικές firewalls

Η ουσιαστική λειτουργία ενός firewall είναι ο περιορισμός της ανεξέλεγκτης ροής πληροφοριών μεταξύ δύο δικτύων. Για να εγκαταστήσουμε ένα firewall πρέπει να ορίσουμε τα είδη των δεδομένων που επιτρέπουμε να περάσουν και αυτά που απαγορεύουμε. Αυτό καλείται "Ορισμός Πολιτικής για το firewall". Μετά τον ορισμό κάποιας πολιτικής πρέπει να δημιουργηθούν οι κατάλληλοι μηχανισμοί που θα τη θέσουν σε εφαρμογή.

Υπάρχουν δύο βασικές στρατηγικές στο καθορισμό πολιτικής για firewalls:

- *Default Permit* - με αυτή τη στρατηγική δίνουμε στο firewall ένα σύνολο προϋποθέσεων αποτέλεσμα των οποίων θα είναι το μπλοκάρισμα κάποιων δεδομένων. Κάθε υπολογιστής ή πρωτόκολλο το οποίο καλύπτεται από αυτές τις προϋποθέσεις περνάει χωρίς επιπλοκές και άλλες διαδικασίες.
- *Default Deny* - με αυτή τη στρατηγική περιγράφουμε συγκεκριμένα πρωτόκολλα τα οποία μπορούν να περάσουν από το firewall και συγκεκριμένους υπολογιστές που μπορούν να διακινήσουν δεδομένα και να επικοινωνήσουν με το εσωτερικό δίκτυο—όλοι οι άλλοι υπολογιστές και πρωτόκολλα απορρίπτονται.

Υπάρχουν τόσο πλεονεκτήματα όσο και μειονεκτήματα και για τις δύο στρατηγικές. Το κυριότερο πλεονέκτημα της Default Permit είναι η ευκολία με την οποία μπορούν να γίνουν οι ρυθμίσεις. Το μόνο που έχει να κάνει κανείς είναι να απαγορεύσει τη χρήση των "επικίνδυνων" πρωτοκόλλων και βασίζεται επιπλέον στην ετοιμότητα του διαχειριστή του firewall να μπλοκάρει νέα επικίνδυνα πρωτόκολλα που αναπτύσσονται ή ανακαλύπτονται.

Με τη Default Deny απλά ενεργοποιούνται πρωτόκολλα κατά βούληση—μόνο αυτά που είναι αναγκαία για την επιτέλεση συγκεκριμένων διεργασιών που είναι γνωστό από πριν ότι θα γίνουν. Κάθε άλλο πρωτόκολλο δεν περνάει το firewall.

Τόσο η Default Permit όσο και η Default Deny δεν αποτελούν πανάκεια—και με τις δύο πολιτικές μπορεί κανείς να δημιουργήσει ένα firewall το οποίο θα είναι ασφαλές ή και όχι, επιτρέποντας ή αποτυγχάνοντας να απαγορεύσει τα "επικίνδυνα" πρωτόκολλα.

2.2.3 Χρήσεις των firewalls

Τα firewalls είναι ένα καλό όπλο μιας μελετημένης πολιτικής άμυνας. Η όλη ιδέα είναι η τοποθέτηση πολλαπλών επιπέδων προστασίας μεταξύ των μηχανών που θέλουμε να προστατέψουμε και των πιθανών απειλών. Υπάρχουν ορισμένες οφθαλμοφανείς εξωτερικές απειλές οπότε θα πρέπει να παρεμβάλλεται κάποιο firewall μεταξύ αυτών και του υπό προστασία εσωτερικού δικτύου.

Επειδή τα firewalls τοποθετούνται στη διαχωριστική γραμμή μεταξύ εσωτερικού και εξωτερικού δικτύου, μπορούν να χρησιμοποιηθούν και για άλλες λειτουργίες εκτός από τον έλεγχο πρόσβασης.

Για παράδειγμα:

↳Τα firewalls μπορούν να χρησιμοποιηθούν για την απαγόρευση πρόσβασης σε συγκεκριμένα sites στο Internet ή για την αποτροπή σύνδεσης με συγκεκριμένους servers ή υπηρεσίες από κάποιους συγκεκριμένους χρήστες.

↳Μπορούν να χρησιμοποιηθούν για την παρακολούθηση των επικοινωνιών μεταξύ εσωτερικού και εξωτερικού δικτύου. Για παράδειγμα θα μπορούσαμε να χρησιμοποιήσουμε ένα firewall για την καταγραφή των προορισμών και των δεδομένων που αποστέλλονται σε αυτούς μέσω TCP/IP συνδέσεων που εγκαθίστανται μεταξύ κάποιου σημείου του εσωτερικού και του εξωτερικού δικτύου.

↳Μπορούν να χρησιμοποιηθούν για την κρυφή παρακολούθηση, υποκλοπή και καταγραφή όλων των επικοινωνιών και της κίνησης από και προς το προστατευόμενο δίκτυο. Μία αφιερωμένη γραμμή 56KB με ποσοστό χρήσης 100% μπορεί να περάσει 605MB ημερησίως που σημαίνει ότι η αξία της κίνησης στο Internet μιας εβδομάδας μπορεί εύκολα να χωρέσει σε ένα δίσκο.

↳Εάν η εταιρεία έχει παραπάνω από μία φυσική τοποθεσία και υπάρχει ένα firewall για κάθε μια από αυτές, μπορούμε να προγραμματίσουμε τα firewalls να κρυπτογραφούν τα πακέτα που στέλνονται από τη μια τοποθεσία στην άλλη. Έτσι μπορούμε να μετατρέψουμε το Internet σε ένα προσωπικό WAN, δηλαδή να δημιουργήσουμε ένα VPN, αν και θα είμαστε ακόμα ευάλωτοι σε κάποιες μορφές επιθέσεων όπως traffic analysis και denial of service.

2.2.4 Η Ανατομία ενός firewall

Όλα τα firewalls αποτελούνται ουσιαστικά από δύο ειδών μέρη:

☒ Chokes:

Συσκευές επικοινωνίας ή υπολογιστικά συστήματα που σαν στόχο έχουν τον περιορισμό της ροής των πακέτων μεταξύ των δικτύων. Τα chokes υλοποιούνται συνήθως από routers αν και αυτό δεν είναι αναγκαίο. Η χρήση του όρου "choke" έχει παρθεί από τα ηλεκτρονικά—μια συσκευή που φέρει μεγάλη αντίσταση σε συγκεκριμένους μόνο τύπους σημάτων.

☒ Gates:

Ειδικά σχεδιασμένα προγράμματα, συσκευές ή υπολογιστές μέσα στην περίμετρο του firewall οι οποίες λαμβάνουν συνδέσεις από έξω και τις διαχειρίζονται κατάλληλα. Το σωστό, από άποψη ασφάλειας, είναι να μην υπάρχουν λογαριασμοί χρηστών σε

μηχανήματα που δρουν ως Gates. Στα Gates μηχανήματα μπορούν να τρέξουν τα παρακάτω είδη προγραμμάτων:

- Network Client Software

Προγράμματα όπως τα ftp, telnet και mosaic. Ο πιο απλός τρόπος παροχής περιορισμένης πρόσβασης στο Internet για τους χρήστες είναι να τους επιτρέπεται να μπαίνουν στο μηχάνημα που λειτουργεί σαν Gate και να τρέχουν δικτυακό λογισμικό απ' ευθείας. Αυτή η τεχνική έχει το μειονέκτημα ότι ο διαχειριστής του συστήματος πρέπει να δημιουργήσει είτε ξεχωριστούς λογαριασμούς, είτε έναν που να τον μοιράζονται.

- Proxy server

Ο Proxy είναι ένα πρόγραμμα το οποίο προσποιείται ότι είναι κάποιο άλλο. Στην περίπτωση των firewalls ο Proxy είναι ένα πρόγραμμα που προωθεί μια αίτηση, μέσω του firewall, από το εσωτερικό δίκτυο στο εξωτερικό. (Η χρήση των Proxy servers θα αναλυθεί εκτενέστερα παρακάτω.)

- Network Servers

Μπορούμε, επίσης, να τρέξουμε δικτυακούς servers στο Gate μηχάνημα. Για παράδειγμα, μπορούμε να εγκαταστήσουμε έναν SMTP server όπως το sendmail ή το smap έτσι ώστε να είμαστε σε θέση να λαμβάνουμε e-mail. Το σίγουρο είναι ότι απαγορεύεται να τρέξουμε κάποιον HTTP server στο μηχάνημα που λειτουργεί ως Gate. Πολλοί δικτυακοί servers μπορούν να δράσουν σαν Proxies. Μπορούν να το κάνουν διότι υλοποιούν απλά μοντέλα αποθήκευσης και προώθησης μηνυμάτων που δεν μπορούν οι ίδιοι να επεξεργαστούν.

2.2.5 Ποιοι τύποι firewalls υπάρχουν;

Δεδομένου ότι σχεδόν όλες οι τεχνικές firewall σχεδιάζονται γύρω από ένα παρόμοιο μοντέλο, ένα συγκεντρωμένο σημείο ελέγχου, υπάρχουν μόνο μερικές παραλλαγές που χρειάζεται να εξερευνηθούν. Σε αυτό το σημείο θα αναλυθεί η λειτουργία και η διαμόρφωση πέντε αρχιτεκτονικών firewalls. Υπάρχουν πολλές παραλλαγές των πέντε αρχιτεκτονικών που μπορεί κάποιος να έχει δει εφαρμοσμένες, και βεβαίως παραλείπονται αρκετές από τις πιο σύνθετες και προηγμένες αρχιτεκτονικές. Αλλά ελπίζουμε να σας εξοικειώσουμε με αυτό που είναι ένα firewall, με το πώς λειτουργεί, πώς μπορεί κάποιος να το εγκαταστήσει και πώς "ταιριάζει" στον κόσμο του εικονικού ιδιωτικού δικτύου.

Δρομολογητής φιλτραρίσματος πακέτων

Ο δρομολογητής φιλτραρίσματος πακέτων (Packet Filtering Router) εφαρμόζει ένα σύνολο κανόνων σε κάθε εισερχόμενο πακέτο IP και στη συνέχεια προωθεί ή απορρίπτει το πακέτο.

Ο δρομολογητής συνήθως είναι διαμορφωμένος για να φιλτράρει πακέτα που πηγαίνουν και προς τις δυο διευθύνσεις (από και προς το εσωτερικό δίκτυο). Οι κανόνες φιλτραρίσματος βασίζονται σε πεδία της επικεφαλίδας IP και της επικεφαλίδας μεταφοράς (TCP ή UDP, ανάλογα), που περιλαμβάνουν τις διευθύνσεις πηγής και προορισμού IP (που ορίζει το πρωτόκολλο μεταφοράς) και τον αριθμό θύρας TCP ή UDP (που ορίζει την εφαρμογή, π.χ. SNMP ή TELNET).

Αν τα περιεχόμενα κάποιας επικεφαλίδας αντιστοιχούν μ' αυτά κάποιου κανόνα, ο κανόνας ενεργοποιείται για να καθορίσει αν το πακέτο πρέπει να προωθηθεί ή να απορριφθεί. Αν δε βρεθεί κανόνας με κατάλληλα περιεχόμενα, εκτελείται μια προκαθορισμένη ενέργεια. Οι προκαθορισμένες πολιτικές είναι δυο:

1. Ότι δεν επιτρέπεται ρητά, απαγορεύεται.
2. Ότι δεν απαγορεύεται ρητά, επιτρέπεται.

Η πρώτη πολιτική είναι, βέβαια, η πιο συντηρητική. Αρχικά, τα πάντα είναι απαγορευμένα και οι επιτρεπόμενες υπηρεσίες πρέπει να προσθέτονται μία – μία, ανά περίπτωση. Η πολιτική αυτή είναι περισσότερο αντιληπτή από χρήστες, που ενδέχεται και να δουν το firewall ως εμπόδιο στην καθημερινή τους δουλειά. Αντίθετα, η δεύτερη πολιτική αυξάνει την ευκολία χρήσης, αλλά έχει μειωμένη ασφάλεια. Ο διαχειριστής ασφάλειας πρέπει, βασικά, να αντιδρά σε κάθε νέα απειλή, καθώς αυτή γίνεται γνωστή.

Πλεονεκτήματα αυτού του τύπου firewall είναι η απλότητά του, η διαφάνεια που παρέχει στους χρήστες και η μεγάλη του ταχύτητα. Τα μειονεκτήματα περιλαμβάνουν τη δυσκολία της κατασκευής σωστών κανόνων φιλτραρίσματος πακέτων και την έλλειψη αυθεντικοποίησης.

Επιθέσεις που μπορούν να εκδηλωθούν εναντίον τέτοιων firewalls και τα αντίστοιχα αντίμετρα είναι οι εξής:

- Παραποίηση διεύθυνσης IP: Ο επιτιθέμενος μεταδίδει πακέτα από το εξωτερικό δίκτυο με πεδίο διεύθυνσης IP που περιέχει τη διεύθυνση ενός εσωτερικού συστήματος, με την ελπίδα ότι η χρήση της παραποιημένης διεύθυνσης θα επιτρέψει την παραβίαση συστημάτων που χρησιμοποιούν απλά μέτρα ασφαλείας ως προς τη διεύθυνση προέλευσης. Δηλαδή στα συστήματα εκείνα στα οποία πακέτα προερχόμενα από κάποια έμπιστα συστήματα γίνονται αποδεκτά. Το αντίμετρο είναι να απορρίπτουμε τα πακέτα που έχουν εσωτερική διεύθυνση αποστολέα αλλά φτάνουν σε εξωτερική διεπαφή.

- Επιθέσεις δρομολόγησης αποστολέα: Ο σταθμός αποστολής καθορίζει το δρομολόγιο που το κάθε πακέτο θα πάρει στη διαδρομή του μέσα στο διαδίκτυο, ελπίζοντας ότι η πρακτική αυτή θα παρακάμψει μέτρα ασφάλειας που δεν αναλύουν την πληροφορία δρομολόγησης από τον αποστολέα. Το αντίμετρο είναι να απορρίπτονται όλα τα πακέτα που χρησιμοποιούν την επιλογή αυτή.

- Επιθέσεις απειροελάχιστων τμημάτων: Ο επιτιθέμενος χρησιμοποιεί την επιλογή τμηματοποίησης IP για να δημιουργήσει τμήματα εξαιρετικά μικρά σε μέγεθος και να επιβάλλει έτσι την τοποθέτηση της πληροφορίας που περιέχει η επικεφαλίδα TCP σε ξεχωριστό τμήμα πακέτου. Η επίθεση αυτή στοχεύει στην παράκαμψη κανόνων φιλτραρίσματος που βασίζονται στην πληροφορία αυτή. Ο επιτιθέμενος ελπίζει ότι ο δρομολογητής φιλτραρίσματος εξετάζει μόνο το πρώτο τμήμα κι ότι τα υπόλοιπα περνούν χωρίς έλεγχο. Η επίθεση αποκρούεται απορρίπτοντας όλα τα πακέτα με τύπο πρωτοκόλλου TCP και IP Fragment Offset ίσο με 1.

Proxy Servers - Πύλες επιπέδου εφαρμογής

Οι πύλες επιπέδου εφαρμογής (Application Level Gateways), που ονομάζονται επίσης και πληρεξούσιοι εξυπηρετητές (proxy servers), λειτουργούν ως αναμεταδότες της κίνησης στο επίπεδο εφαρμογής.

Ο χρήστης επικοινωνεί με την πύλη μέσω μιας εφαρμογής TCP/IP (π.χ. Telnet, FTP) και η πύλη του ζητάει το όνομα του απομακρυσμένου συστήματος που πρέπει να προσπελαστεί. Όταν απαντήσει ο χρήστης και δώσει τις απαραίτητες και έγκυρες πληροφορίες αυθεντικοποίησης που τον αφορούν, η πύλη επικοινωνεί με την εφαρμογή στο απομακρυσμένο σύστημα και αναμεταδίδει όλα τα μηνύματα TCP που περιέχουν τα δεδομένα της εφαρμογής μεταξύ των δυο άκρων. Αν η πύλη δεν υποστηρίζει τον κώδικα πληρεξουσίου για μια συγκεκριμένη εφαρμογή, η υπηρεσία δεν παρέχεται και δεν μπορεί να διακινηθεί δια μέσου του firewall. Επιπλέον, η πύλη μπορεί να διαμορφωθεί έτσι ώστε να υποστηρίζει μόνο συγκεκριμένα χαρακτηριστικά μιας εφαρμογής, τα οποία ο διαχειριστής δικτύου κρίνει απαραίτητα, απορρίπτοντας όλα τα υπόλοιπα.

Τα firewalls αυτά είναι περισσότερο ασφαλή από τους δρομολογητές φιλτραρίσματος πακέτων. Αντί να προσπαθούν να χειριστούν τους απειράριθμους πιθανούς συνδυασμούς που πρέπει να επιτρέπονται ή να απαγορεύονται στα επίπεδα και TCP και IP, η πύλη επιπέδου εφαρμογής χρειάζεται μόνο να εξετάζει εξονυχιστικά ένα μικρό αριθμό επιτρεπόμενων εφαρμογών. Επιπλέον, είναι εύκολο να καταγράφεται και να ελέγχεται όλη η εισερχόμενη κίνηση στο επίπεδο εφαρμογής.

Ένα βασικό μειονέκτημα των firewalls αυτού του τύπου είναι η επιπλέον επιβάρυνση της επεξεργασίας σε κάθε σύνδεση. Στην πραγματικότητα υπάρχουν δύο

τμήματα σύνδεσης μεταξύ των τελικών χρηστών. Η πύλη αποτελεί το σημείο τομής τους, δημιουργώντας τα δύο τμήματα αυτά, και η πύλη αυτή πρέπει να εξετάζει και να διακινεί όλη την κίνηση και προς τις δυο κατευθύνσεις.

☞ Πύλη επιπέδου κυκλώματος

Μια πύλη επιπέδου κυκλώματος (Circuit Level Gateway) μπορεί να είναι ένα αυτόνομο σύστημα ή μπορεί να είναι μια ειδική λειτουργία που εκτελείται από μια πύλη επιπέδου εφαρμογής για συγκεκριμένες εφαρμογές.

Μια τέτοια πύλη δεν επιτρέπει συνδέσεις TCP απ' άκρη σ' άκρη. Αντίθετα, εγκαθιστά δυο συνδέσεις TCP, μία μεταξύ της ίδιας και ενός χρήστη TCP σε κάποιο εσωτερικό σύστημα και μια άλλη μεταξύ της ίδιας και ενός χρήστη TCP σε κάποιο εξωτερικό σύστημα.

Από τη στιγμή που θα εγκατασταθούν και οι δυο συνδέσεις, η πύλη συνήθως αναμεταδίδει τμήματα TCP από τη μια σύνδεση στην άλλη χωρίς να εξετάζει τα περιεχόμενά τους. Η λειτουργία ασφάλειας συνίσταται στον καθορισμό του ποιες συνδέσεις επιτρέπονται.

Τυπική χρήση τέτοιων firewalls είναι μια κατάσταση στην οποία ο διαχειριστής συστήματος εμπιστεύεται τους εσωτερικούς χρήστες. Η πύλη μπορεί να διαμορφωθεί έτσι ώστε να λειτουργεί ως πύλη επιπέδου εφαρμογής ή ως πληρεξούσιος εξυπηρετητής για τις εισερχόμενες συνδέσεις και ως πύλη επιπέδου κυκλώματος για τις εξερχόμενες συνδέσεις. Στη διαμόρφωση αυτή, η πύλη επιβαρύνεται με την εξέταση της εισερχόμενης πληροφορίας, αλλά όχι με αυτήν της εξερχόμενης. Παράδειγμα τέτοιου firewall αποτελεί το πακέτο SOCKS.

☞ Bastion hosts

Οι επάλξεις (Bastion hosts) είναι μηχανές που έχουν αναγνωρισθεί από τον υπεύθυνο ασφάλειας του δικτύου ως ισχυρά και κρίσιμα σημεία για την ασφάλεια του δικτύου.

Τυπικά, η έπαλξη χρησιμοποιείται ως πλατφόρμα για μια πύλη επιπέδου εφαρμογής ή μια πύλη επιπέδου κυκλώματος. Τα κυριότερα χαρακτηριστικά των bastion hosts είναι:

☒ Στην πλατφόρμα υλικού τους τρέχει ασφαλής έκδοση του λειτουργικού συστήματος.

☒ Μόνο οι υπηρεσίες που ο διαχειριστής συστήματος θεωρεί βασικές είναι εγκατεστημένες στην έπαλξη. Αυτές περιλαμβάνουν πληρεξούσιες εφαρμογές, όπως Telnet, DNS, FTP, SMTP και αυθεντικοποίηση χρήστη.

☒ Η έπαλξη μπορεί να απαιτεί επιπρόσθετη αυθεντικοποίηση πριν επιτρέψει την πρόσβαση ενός χρήστη στις πληρεξούσιες υπηρεσίες. Επιπλέον, κάθε πληρεξούσια υπηρεσία μπορεί να απαιτεί τη δική της αυθεντικοποίηση πριν επιτρέψει την πρόσβαση σε κάποιο χρήστη.

☒ Κάθε πληρεξούσια υπηρεσία είναι διαμορφωμένη έτσι ώστε να υποστηρίζει μόνο ένα υποσύνολο του κανονικού συνόλου εντολών της εφαρμογής.

☒ Κάθε πληρεξούσια υπηρεσία είναι διαμορφωμένη έτσι ώστε να επιτρέπει πρόσβαση μόνο σε συγκεκριμένα συστήματα. Αυτό σημαίνει ότι το περιορισμένο σύνολο χαρακτηριστικών / εντολών μπορεί να εφαρμοστεί σε περιορισμένο μόνο υποσύνολο συστημάτων του προστατευόμενου δικτύου.

☒ Κάθε πληρεξούσια υπηρεσία διατηρεί λεπτομερείς πληροφορίες ελέγχου καταγράφοντας όλη την κίνηση, κάθε σύνδεση και τη διάρκειά της. Το ίχνος ελέγχου είναι ένα βασικό εργαλείο για τον εντοπισμό και τερματισμό επιθέσεων.

☒ Κάθε σπόνδυλος υπηρεσίας πληρεξουσίου είναι ένα πολύ μικρό πακέτο λογισμικού ειδικά σχεδιασμένο για να παρέχει ασφάλεια δικτύου. Λόγω της σχετικής τους απλότητας, είναι ευκολότερο να ελέγξουμε τέτοιους σπονδύλους για ελαττώματα σχετικά με την ασφάλεια. Για παράδειγμα, μια τυπική εφαρμογή ταχυδρομείου στο Unix μπορεί κάλλιστα να περιέχει 20.000 γραμμές κώδικα, ενώ μια αντίστοιχη υπηρεσία πληρεξουσίου λιγότερες από 1.000.

☒ Κάθε πληρεξούσια υπηρεσία είναι ανεξάρτητη από τις άλλες που βρίσκονται στην ίδια έπαλξη. Αν υπάρξει κάποιο πρόβλημα με τη λειτουργία μιας υπηρεσίας ή αν ανακαλυφθεί μια ευπάθεια, η υπηρεσία μπορεί να απεγκατασταθεί χωρίς να επηρεαστεί η λειτουργία των υπολοίπων. Επίσης, αν οι χρήστες απαιτούν την υποστήριξη μιας νέας υπηρεσίας, ο διαχειριστής δικτύου μπορεί εύκολα να εγκαταστήσει τη νέα πληρεξούσια υπηρεσία στην έπαλξη.

☒ Κάθε πληρεξούσια υπηρεσία προσπελάζει το δίσκο μόνο για να διαβάσει το αρχείο αρχικής της διαμόρφωσης. Έτσι, είναι δύσκολο στον επιτιθέμενο να εγκαταστήσει Δούρειους Ίππους ή άλλα επικίνδυνα αρχεία στην έπαλξη.

☒ Κάθε πληρεξούσια υπηρεσία εξυπηρετεί τους μη προνομιούχους χρήστες χρησιμοποιώντας έναν ιδιωτικό και ασφαλή κατάλογο στην έπαλξη.

☞ NAT (Network Address Translation)

Ο Μεταφραστής Διευθύνσεων Δικτύου σχεδιάστηκε για απλοποίηση και διατήρηση των IP διευθύνσεων αφού αυτό που κάνει είναι να επιτρέπει σε ιδιωτικά δίκτυα που χρησιμοποιούν μη εγγεγραμμένες IP διευθύνσεις να έχουν σύνδεση με το Internet.

Το σύστημα NAT λειτουργεί σε κάποιον δρομολογητή, ο οποίος συνδέει συνήθως δύο δίκτυα και μεταφράζει τις ιδιωτικές (μη μοναδικές στον παγκόσμιο ιστό) διευθύνσεις του εσωτερικού δικτύου σε νόμιμες διευθύνσεις προτού τα πακέτα προωθηθούν σε άλλο δίκτυο. Σαν μέρος αυτής της λειτουργίας το NAT μπορεί να ρυθμιστεί να κάνει γνωστή μόνο μία διεύθυνση στον έξω κόσμο για ολόκληρο το δίκτυο που συνδέεται με αυτόν. Αυτό το χαρακτηριστικό παρέχει επιπλέον ασφάλεια αφού κρύβει ολόκληρο το εσωτερικό δίκτυο από τον κόσμο πίσω από μία διεύθυνση.

Επιπλέον, μία επιχείρηση μπορεί να θέλει να έχει σύνδεση με το Internet χρησιμοποιώντας όμως παραπάνω από έναν παροχέα υπηρεσιών Internet (ISP) για διάφορους λόγους. Το να διατηρεί κανείς σύνδεση στο Internet μέσω παραπάνω του ενός ISP μπορεί να θεωρηθεί σαν ένας τρόπος αύξησης της αξιοπιστίας της σύνδεσης στο Internet. Τέτοιου είδους sites με πολλαπλές συνδέσεις ονομάζονται "multi-homed". Όταν η σύνδεση από τον ένα παροχέα πέφτει τότε η εταιρία περνάει σε κάποιον άλλο διατηρώντας έτσι πάντα τη σύνδεσή της. Ακόμα ένα πλεονέκτημα αυτού του σχήματος είναι το ότι η επιχείρηση μπορεί να διανείμει το φορτίο της σε διαφορετικές συνδέσεις. Για επιχειρήσεις μάλιστα που εκτείνονται σε μεγάλη γεωγραφική περιοχή ένα τέτοιο σχήμα θα σήμαινε και καλύτερη διαδικασία δρομολόγησης.

Όλες οι παραπάνω σκέψεις συνδυαζόμενες και με τις συνεχώς μειούμενες τιμές των Internet συνδέσεων δίνουν κίνητρο σε όλο και περισσότερες εταιρίες να γίνουν "multi-homed". Την ίδια στιγμή, ο φόρτος που τέτοιες εταιρίες επιβάλλουν στους δρομολογητές στο Internet αυξάνεται και γίνεται ολοένα και πιο σημαντικός. Πρέπει λοιπόν να βρεθεί ένας τρόπος κλιμακοποίησης του internet και υποστήριξης αυτών των επιχειρήσεων. Μία λύση θα ήταν οι δρομολογητές της ελεύθερης ζώνης του Internet να διατηρούσαν μία διαδρομή για κάθε "multi-homed" επιχείρηση που συνδέεται με παραπάνω του ενός ISP στο Internet. Αυτή η λύση όμως δεν παρέχει επαρκή κλιμακοποίηση. Επιπλέον μία λύση για τη διαχείριση της δρομολόγησης τέτοιων εταιριών θα πρέπει να ενσωματώνει το σκεπτικό ότι ο απαιτούμενος βαθμός συνεργασίας των ISPs θα πρέπει να είναι όσο το δυνατόν μικρότερος και ιδιαίτερα αυτών που δεν συνδέονται άμεσα με τις επιχειρήσεις αυτές.

☞ DMZ ή δίκτυο περιμετρικής ζώνης

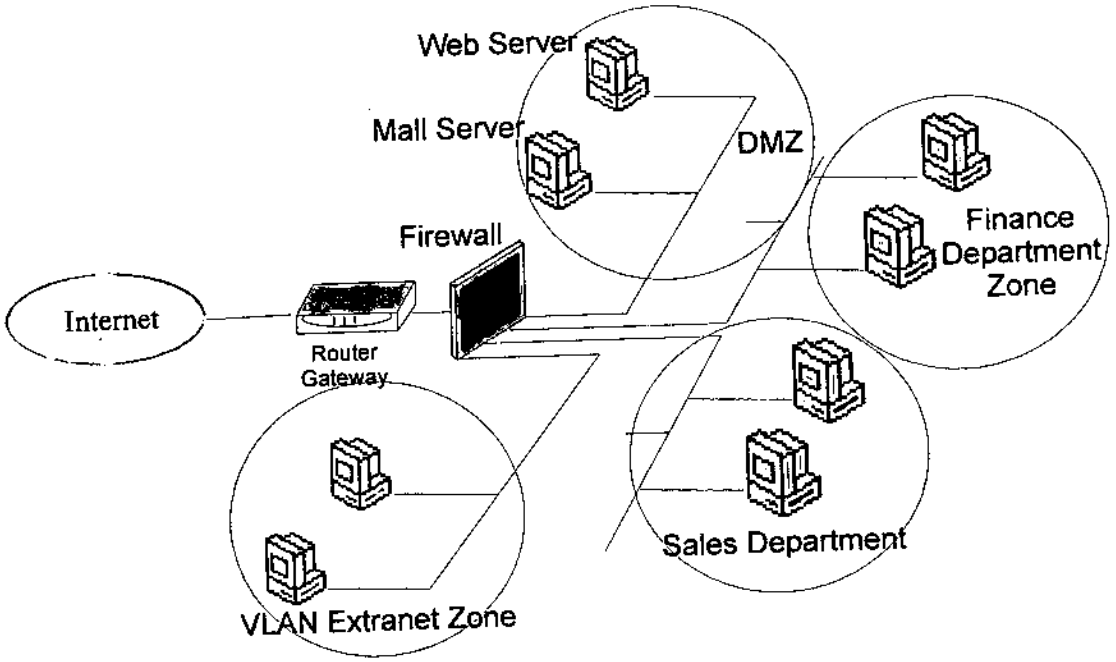
Μια περιμετρική ζώνη απομονώνει τους hosts που είναι προσιτοί από το εξωτερικό περιβάλλον του δικτύου (π.χ. έναν web server ή έναν ftp server) από τους εσωτερικούς servers. Οι εξωτερικοί hosts είναι τοποθετημένοι σε μια ξεχωριστή ζώνη του δικτύου, σε έναν ξεχωριστό προσαρμογέα που είναι συνδεδεμένος με το firewall. Αυτό κατορθώνεται εύκολα με ένα firewall με τρεις ή παραπάνω διεπαφές.

Κάθε υποδίκτυο είναι επίσης διαμορφωμένο με τη δικιά του ζώνη ασφαλείας (π.χ. δίκτυο λογιστηρίου, δίκτυο πωλήσεων κ.τ.λ.) συνδέοντάς το σε ξεχωριστούς προσαρμογείς firewall. Η επικοινωνία μεταξύ των ζωνών, αλλά και η επικοινωνία από το Internet προς όλες τις ζώνες ελέγχεται από το Firewall.

Μ' αυτόν τον τρόπο, κάθε ζώνη είναι απομονωμένη και το σύστημα κάθε ζώνης εμπιστεύεται μόνο τα συστήματα που περιλαμβάνονται στην ίδια ζώνη. Γι' αυτό εάν ένας hacker καταφέρει να «μπει» σε έναν προσιτό host, οι υπόλοιποι hosts του δικτύου εξακολουθούν να είναι ασφαλείς.

Τα DMZs χρησιμοποιούνται συχνά από ειδικούς servers όπως είναι οι web servers, οι οποίοι πρέπει να είναι προσπελάσιμοι από δυο ξεχωριστά δίκτυα. Συνήθως μια επιχείρηση έχει μια σύνδεση Internet, ένα τοπικό δίκτυο και ένα DMZ με servers οι οποίοι πρέπει να είναι και εσωτερικά και εξωτερικά προσπελάσιμοι. Αυτό φαίνεται στο σχήμα 2.2.

Σε μια πρότυπη κατασκευή περιμετρικής ζώνης, οι πιο σύνθετοι και προσεκτικοί έλεγχοι τοποθετούνται στον εσωτερικό δρομολογητή, ο οποίος είναι αυτός που χωρίζει το εσωτερικό δίκτυο και από το δίκτυο περιμέτρου και από το εξωτερικό δίκτυο. Είναι μια πολύ κοινή πρακτική να δημιουργηθεί το δίκτυο DMZ με αυτό τον τρόπο, επειδή αυτή η διαμόρφωση μπορεί να παρομοιαστεί με τις σειρές των ομόκεντρων κύκλων – όσο πάμε προς τα έξω, τόσο λιγότερη ασφάλεια έχουμε. Επίσης, γίνεται κοινή πρακτική να χρησιμοποιηθεί το NAT (Network Address Translation)-η μετάφραση διευθύνσεων δικτύων -στον εσωτερικό δρομολογητή για να περιπλέξει περαιτέρω την εντόπιση και την πειρατεία των εσωτερικών επικοινωνιών. Το NAT παρέχει ασφάλεια μεταφράζοντας τις μη-δρομολογήσιμες διευθύνσεις (όπως η 192.168.0.0 σειρά) σε πραγματικές διευθύνσεις Διαδικτύου, με ένα δυναμικό τύπο. Δεν υπάρχει κανένας εύκολος τρόπος να ανταλλαχθεί η κυκλοφορία με τους εσωτερικούς hosts εκτός από την παράκαμψη της μηχανής που κάνει τη NAT μετάφραση.



Σχήμα 2.2 Δίκτυο Περιμετρικής Ζώνης

Η μεγαλύτερη ασφάλεια που μπορείτε να έχετε με ένα DMZ είναι ότι μπορεί να απαγορεύσει όλη την εξερχόμενη κυκλοφορία στο εσωτερικό δίκτυο από τον εξωτερικό δρομολογητή, και να απαγορεύσει όλη την εισερχόμενη κυκλοφορία στο εσωτερικό δίκτυο από το Διαδίκτυο. Στην ουσία, αυτό κάνει όλη την κυκλοφορία μια διαδικασία δυο βημάτων (σταδίων). Οι χρήστες στο Διαδίκτυο μπορούν να "κοιτάξουν αδιάκριτα" μόνο με μηχανές που βρίσκονται στο περιμετρικό δίκτυό σας, και οι χρήστες που είναι βαθιά μέσα στο εσωτερικό δίκτυο δεν μπορούν να δουν το Διαδίκτυο άμεσα. Αυτοί επίσης χρειάζεται να χρησιμοποιήσουν έναν μεσάζοντα μέσω bastion host στο DMZ.

Εσωτερικοί Firewalls

Αντί να βάζουμε όλους τους υπολογιστές του δικτύου σε ένα και μόνο τοπικό δίκτυο, μπορούμε να τους χωρίσουμε σε πολλά μικρότερα ανεξάρτητα τοπικά δίκτυα τα οποία μπορούν να επικοινωνούν μέσω δρομολογητών ή μηχανών gateways ή και firewalls. Εναλλακτικά μπορούν να επικοινωνήσουν μέσω ανεξάρτητων διασυνδέσεων (links) στο Internet χρησιμοποιώντας ένα κατάλληλο σύστημα κρυπτογράφησης.

Τα εσωτερικά firewalls έχουν μεγάλη σημασία για το εσωτερικό δίκτυο ενός οργανισμού. Δεν υπάρχει κανένας λόγος, χρήστες από διαφορετικούς τομείς της εταιρίας να έχουν πρόσβαση σε πόρους συναδέλφων τους που βρίσκονται σε τομείς μακριά από το αντικείμενο εργασίας τους. Έτσι με ένα εσωτερικό firewall ενισχύουμε την ασφάλεια του συστήματος.

Ένα firewall που είναι σχεδιασμένο για τέτοιου είδους χρήση μοιάζει πολύ με αυτό που χρησιμοποιείται για την προστασία από εξωτερικές επιθέσεις. Ωστόσο, επειδή η ίδια ομάδα διαχείρισης μπορεί να είναι υπεύθυνη για πολλά από τα δίκτυα ενός οργανισμού υπάρχει μεγάλος "πειρασμός" στο να γίνει κάποιου είδους μοιρασιά πληροφοριών και υπηρεσιών μέσω ενός εσωτερικού firewall τη στιγμή που τέτοιες πληροφορίες θα έπρεπε να μπλοκάρονται.

2.2.6 Μια συνοπτική κατάταξη των πιο γνωστών firewalls είναι η παρακάτω:

✓ Cisco's PIX Firewall : Το δικτυακό αυτό firewall είναι μια πύλη επιπέδου εφαρμογής που χρησιμοποιεί τις τεχνικές stateful inspection και cut through proxy. Η πρώτη αναφέρεται στη δυνατότητα καταγραφής όλων των δραστηριοτήτων που συμβαίνουν κατά τη διάρκεια μιας σύνδεσης, ενώ η δεύτερη στην αποκατάσταση της απ' ευθείας σύνδεσης μεταξύ πελάτη και εξυπηρετητή, χωρίς την παρεμβολή του δικτυακού firewall, μετά την αρχική αυθεντικοποίηση του χρήστη.

✓ Guardian Firewall – 5 : Το προϊόν αυτό είναι μια πύλη επιπέδου εφαρμογής. Θεωρείται ως ένα από τα καλύτερα προϊόντα από πλευράς διεπαφής χρήστη.

✓ Gauntlet Internet Firewall : Το δικτυακό αυτό firewall είναι μια πύλη επιπέδου εφαρμογής που χρησιμοποιεί αντιπροσώπους (agents) για την εγκατάσταση συνδέσεων. Μπορεί να χρησιμοποιηθεί και για τη χρήση μηχανισμών ισχυρής αυθεντικοποίησης.

✓ SecureIT : Το δικτυακό αυτό firewall αποτελεί ένα συνδυασμό τύπου πύλης κυκλώματος και πύλης επιπέδου εφαρμογής με χρήση αντιπροσώπων εξυπηρετητών (proxy servers). Έχει σχεδιαστεί με βάση την πολιτική ολικής άρνησης και η χρήση του μπορεί να βελτιστοποιηθεί.

2.3 ΚΡΥΠΤΟΓΡΑΦΙΑ

Ένα από τα κυριότερα θέματα για τα VPNs είναι η ασφαλής μετάδοση των δεδομένων χωρίς να παρέχεται η δυνατότητα σε τρίτους να υποκλέψουν τα δεδομένα της επικοινωνίας. Έτσι πρέπει να γίνουν κάποια βήματα προς την μεριά της ασφάλειας των δεδομένων. Όπως θα δούμε παρακάτω υπάρχει μια ευρεία γκάμα αλγορίθμων κρυπτογράφησης σχεδόν για όλα τα επίπεδα του OSI και αυτό που απομένει στον χρήστη του VPN είναι να διαλέξει το επίπεδο ασφαλείας που επιθυμεί σύμφωνα με τις εφαρμογές που χρησιμοποιεί. Παρακάτω θα κάνουμε μια εισαγωγή στους κυριότερους κρυπτογραφικούς αλγορίθμους για να πάρουμε μια πρώτη ιδέα του θεωρητικού υπόβαθρού τους.

Η ασφάλεια των VPNs βασίζεται στην κρυπτογραφική δυνατότητα των αλγορίθμων κρυπτογράφησης. Θεωρούμε ότι είναι ανάγκη να παρουσιασθούν

ορισμένα βασικά στοιχεία των διαφόρων αλγορίθμων ούτως ώστε να μπορούμε να δούμε το θέμα της ασφάλειας των VPNs και πιο σφαιρικά.

Μια κρυπτογραφική διαδικασία είναι η μετατροπή ενός απλού κειμένου σε ένα κρυπτογραφημένο κείμενο όπως για παράδειγμα η πρόταση: "Η ασφάλεια στα VPNs είναι ζωτικής σημασίας" στην κρυπτογραφημένη πρόταση "ςεθ235φ5345η55θ67ε5ηφ675ςε78ηηβ6". Αποκρυπτογράφηση είναι η ακριβώς αντίθετη διαδικασία, δηλαδή η μετατροπή της κρυπτογραφημένης πρότασης "ςεθ235φ5345η55θ67ε5ηφ675ς-ε78ηηβ6" στην μη κρυπτογραφημένη πρόταση "Η ασφάλεια στα VPNs είναι ζωτικής σημασίας". Όπως έχουμε δει τα δυο κείμενα (απλό, κρυπτογραφημένο) δεν φαίνονται να έχουν κάποια σχέση μεταξύ τους. Το κρυπτογραφημένο φαίνεται εκ πρώτης όψεως ότι είναι μια "ασυναρτησία". Αυτά τα δύο κείμενα τα συνδέει μεταξύ τους μια συνάρτηση f(x) η οποία είναι το κλειδί της κρυπτογράφησης.

Ένα άλλο μεγάλο θέμα για τα VPNs είναι αν ένας κρυπτογραφικός αλγόριθμος μπορεί να « σπάσει », αν δηλαδή τα δεδομένα του είναι ασφαλή από την επίδραση τρίτων και αν ο αποστολέας είναι πραγματικά αυτός που ισχυρίζεται ότι είναι. Παρακάτω θα δούμε διάφορους αλγορίθμους οι οποίοι μπορούν να το κάνουν αυτό.

2.3.1 Private Key

Σε αυτόν τον αλγόριθμο ο αποστολέας και ο παραλήπτης ενός κειμένου χρησιμοποιούν το ίδιο κλειδί το οποίο μόνο αυτοί οι δύο γνωρίζουν (ιδιωτικό κλειδί). Ο αποστολέας χρησιμοποιεί το μυστικό κλειδί για να κρυπτογραφήσει το κείμενο και ο παραλήπτης χρησιμοποιεί το ίδιο κλειδί για να το αποκρυπτογραφήσει. Αυτή η μέθοδος κρυπτογραφίας ονομάζεται μυστικού κλειδιού (secret key) ή συμμετρική κρυπτογραφία και θεωρείται μία από τις πιο ασφαλείς μεθόδους. Όμως ένα σοβαρό πρόβλημα της μεθόδου αυτής είναι με πιο τρόπο ο αποστολέας και ο παραλήπτης θα συμφωνήσουν για το κλειδί, και πώς θα το ανταλλάξουν μεταξύ τους. Το πρόβλημα γίνεται πιο οξύ όταν ο αποστολέας και ο παραλήπτης βρίσκονται σε διαφορετική γεωγραφική περιοχή. Σε αυτή την περίπτωση τίθεται ένα πιο γενικό θέμα, αν μπορούν να εμπιστευτούν είτε το δίκτυο, είτε το ταχυδρομείο, είτε το τηλέφωνο. Αν και αυτή η μέθοδος θεωρείται αρκετά ασφαλής είναι δύσκολο να εφαρμοσθεί σε δίκτυα VPN όπου οι διάφοροι hosts δε βρίσκονται στην ίδια γεωγραφική περιοχή. Αν λάβουμε υπόψη ότι τα περισσότερα δίκτυα VPN συνδέουν υπολογιστές που βρίσκονται σε πολύ μακρινές αποστάσεις (διαφορετικές γεωγραφικές περιοχές) μπορούμε να θεωρήσουμε ότι σπάνια χρησιμοποιείται και σε πολύ εξειδικευμένες περιπτώσεις π.χ. στρατιωτικές εφαρμογές ή σε δίκτυα VPN που χρησιμοποιούνται σε κλειστά τραπεζικά συστήματα όπου ο διαχειριστής όλων των κλειδιών είναι ένας και μοναδικός.

2.3.2 Public Key

Οι Whitfield Diffie και Martin Hellman το 1976 παρουσίασαν την κρυπτογραφική μέθοδο δημόσιου κλειδιού (public key) που σκοπό είχε να λύσει το πρόβλημα που παρουσιαζόταν στην μετάδοση του κλειδιού της μεθόδου private key. Σε αυτήν την μέθοδο ο αποστολέας και ο παραλήπτης έχουν από ένα public και ένα private κλειδί. Το public κλειδί είναι σε όλους γνωστό (μπορεί να βρεθεί σε διάφορα ευρετήρια), ενώ το private κλειδί το γνωρίζει μόνο ο κάτοχός του. Σε αυτό το είδος κρυπτογράφησης δεν είναι ανάγκη τα κανάλια επικοινωνίας να είναι ασφαλή γιατί ουσιαστικά μόνο ο κατάλληλος παραλήπτης μπορεί να αποκρυπτογραφήσει το μήνυμα και άρα να το δει.

Τα πλεονεκτήματα της χρήσης public κλειδιού είναι η ασφάλεια και η ευκολία που παρέχεται σε αντίθεση με το private κλειδί το οποίο δεν είναι σωστό να μεταδίδεται μέσω του δικτύου ή να δίδεται σε άλλο τρίτο άτομο. Ένα άλλο πλεονέκτημα του public κλειδιού είναι η δυνατότητα παροχής αξιόπιστων ηλεκτρονικών υπογραφών.

Ένα σοβαρό μειονέκτημα των public key αλγορίθμων είναι η πολύ μικρή ταχύτητά τους ενώ αντίθετα οι private key αλγόριθμοι είναι σημαντικά γρηγορότεροι. Έτσι, εκμεταλλευόμενοι τα πλεονεκτήματα των δύο πιο πάνω κρυπτογραφικών αλγορίθμων έχουμε δημιουργήσει διάφορες "digital envelope" (ψηφιακού φακέλου) μεθόδους οι οποίες συνδυάζουν τις δύο ανωτέρω μεθόδους.

2.3.3 Block Ciphers

Block Cipher είναι ένας αλγόριθμος κρυπτογράφησης ο οποίος επαναλαμβάνει διάφορες λειτουργίες όπως αντικατάσταση, μετάθεση, πολλαπλασιασμό, και γραμμικούς μετασχηματισμούς δημιουργώντας έτσι ένα πολύ πιο δυνατό αλγόριθμο. Η αποκρυπτογράφηση αυτής της μεθόδου γίνεται με τον αντίστροφο αλγόριθμο της κρυπτογράφησης.

2.3.4 Data Encryption Standards - DES

Ο Data Encryption Standards έχει αναπτυχθεί στην IBM και είχε αρχικά ονομασθεί Lucifer. Ο DES είναι ένας αλγόριθμος ο οποίος χρησιμοποιεί 64 bit μέγεθος block και ένα κλειδί 56bit.

Γενικά ο αλγόριθμος αυτός δεν είναι εύκολο να δεχθεί επιθέσεις, αλλά υπάρχει ένας μηχανισμός ο οποίος μπορεί να τον σπάσει. Ένας τέτοιος μηχανισμός είναι η "brute-force attack", η οποία προσπαθεί να βρει όλους τους δυνατούς συνδυασμούς που μπορούν να γίνουν και άρα να βρει και τον σωστό συνδυασμό. Μια άλλη τεχνική ονομάζεται "sustained data analysis", την οποία βλέπουμε παρακάτω:

Wfhrhewpfwe fhwefh8**eem**gwergwe7n13-8 132jgk4kh2Ij8@-76&1

&)0-7-31mfd**eem**mqp8j03mdasx
unfw2y067109760)asdsa(&^%**eem**aca$$gxoasg

7@#7^ypo**eem**iuw2-wefwef3wee-kin0f9qb**eem**upouthf30-53^&^))P**eem**6p4c23

Εδώ βλέπουμε τρία κρυπτογραφημένα μηνύματα τα οποία έχουν κρυπτογραφηθεί με το ίδιο κλειδί. Αν παρατηρήσουμε προσεκτικά βλέπουμε ότι και στα τρία κρυπτογραφημένα μηνύματα υπάρχουν ορισμένοι χαρακτήρες που είναι με την ίδια σειρά και άρα έχουν προέλθει από το ίδιο κλειδί. Αν αυτοί οι χαρακτήρες έχουν μεγάλη συχνότητα εμφάνισης τότε κάποιος μπορεί να συμπεράνει με μεγάλη πιθανότατα ποια είναι αυτή η λέξη. Αυτή η λέξη μπορεί να αντιστοιχεί σε μια λέξη που παρουσιάζει μεγάλη συχνότητα εμφάνισης όπως για παράδειγμα η λέξη "και". Με αυτό τον τρόπο μπορεί κανείς να σπάσει το DES. Η λύση σε αυτό το πρόβλημα είναι βεβαίως η συχνή αλλαγή των κλειδιών.

2.3.5 Hash Functions (Συναρτήσεις Κατακερματισμού)

Οι hash συναρτήσεις, είναι συναρτήσεις οι οποίες παίρνουν ένα μεταβλητού μεγέθους μήνυμα και μας δίνουν ένα μεταβλητού μεγέθους μήνυμα, συνήθως 128 bit ή περισσότερα, το οποίο αναφέρεται σαν hash τιμή. Οι hash συναρτήσεις είναι μονόδρομες (one way) δηλαδή είναι πολύ δύσκολο να βρεθεί η αντίστροφη συνάρτηση τους και άρα να σπάσουν. Δηλαδή αν δοθεί ένα μήνυμα και μια hash συνάρτηση και δημιουργηθεί μια hash τιμή θα πρέπει να είναι αδύνατη η αναπαραγωγή του κλειδιού από την hash τιμή. Όταν σε ένα έγγραφο εφαρμοσθεί η hash συνάρτηση το αποτέλεσμα είναι ένα δακτυλικό αποτύπωμα του αρχικού εγγράφου. Έτσι, αυτή η μέθοδος χρησιμοποιείται ευρέως σε ηλεκτρονικές υπογραφές. Υπάρχουν αρκετές υλοποιήσεις των hash συναρτήσεων όπως για παράδειγμα τα Message Digest 2,4,5 (MD2), (MD4), (MD5) και ο Secure hash αλγόριθμος (SHA και SHA-1).

2.4 ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΣΤΑ VPNS

Στην προηγούμενη ενότητα, έγινε μια εισαγωγή στις έννοιες της κρυπτογραφίας και στις διάφορες υλοποιήσεις που έχουν αναπτυχθεί μέχρι σήμερα. Η κρυπτογραφία αποτελεί μια διαδικασία επίλυσης δύσκολων προβλημάτων. Σε αυτή την ενότητα θα μελετηθεί το πως αυτή εφαρμόζεται στα VPNs, στα διάφορα πρότυπα των VPNs, όπως και στα διάφορα πρωτόκολλα που χρησιμοποιούνται.

2.4.1 Private key encryption

Η κρυπτογράφηση μέσω ιδιωτικού κλειδιού βασίζεται στη λογική του private key όπου το ίδιο κλειδί κωδικοποιεί και αποκωδικοποιεί το μήνυμα. Όπως έχουμε ήδη αναφέρει αν και αυτή η μέθοδος είναι πάρα πολύ καλή, το μεγαλύτερο πρόβλημά της είναι το πώς θα παραλάβει ο παραλήπτης το κρυπτογραφημένο κλειδί.

Εκτός αυτού του σοβαρού μειονεκτήματος, σε τέτοιου είδους συστήματα ο αριθμός των κλειδιών είναι υπερβολικά μεγάλος γιατί κάθε ζεύγος χρηστών πρέπει να έχει και από ένα κλειδί. Όσο περισσότερα κλειδιά χρειάζονται, τόσο η διαχείριση και η διανομή των κλειδιών γίνεται δυσκολότερη. Για παράδειγμα, αν ένας οργανισμός έχει 100 χρήστες VPN τότε απαιτούνται 4950 κλειδιά (100*99/2). Τι γίνεται στην περίπτωση που ένας οργανισμός έχει 1000 χρήστες; Τότε απαιτείται το εξωπραγματικό νούμερο των 499,500 κλειδιών. Άρα παρατηρούμε ότι είναι αδύνατο αυτή η μέθοδος να υλοποιηθεί σε πραγματικά εμπορικά VPN.

2.4.2 Public key encryption

Στην κρυπτογράφηση μέσω δημόσιου κλειδιού, όπως έχουμε αναφέρει στην προηγούμενη ενότητα, απαιτούνται δύο κλειδιά, ένα ιδιωτικό το οποίο είναι γνωστό μόνο στο χρήστη του και σε κανέναν άλλον και ένα δημόσιο το οποίο είναι διαθέσιμο στον καθένα και μπορεί να βρεθεί σε διάφορα ευρετήρια. Το private key που αναφέρουμε εδώ δεν σχετίζεται με το private key που αναφέρεται στην προηγούμενη παράγραφο (μέθοδος private κλειδιού), αλλά αυτό το ιδιωτικό κλειδί απλά αποκρυπτογραφεί μηνύματα τα οποία έχουν κρυπτογραφηθεί με το σχετικό δημόσιο κλειδί.

Δύο πολύ γνωστά συστήματα δημόσιου κλειδιού που χρησιμοποιούνται σήμερα στα VPNs είναι το Rivest Shamir Adlemen (RSA) και το Diffie- Hellman (DH).

Ένα παράδειγμα του Diffie Hellman είναι η παρακάτω διαδικασία: Ο αποστολέας μπορεί να πάρει το δημόσιο κλειδί του παραλήπτη από διάφορες πηγές, στη συνέχεια κωδικοποιεί το μήνυμα χρησιμοποιώντας αυτό το κλειδί. Ακολούθως, το κρυπτογραφημένο μήνυμα στέλνεται στον παραλήπτη μέσω ενός δημόσιου δικτύου. Ο παραλήπτης λαμβάνει το μήνυμα και το αποκρυπτογραφεί χρησιμοποιώντας το ιδιωτικό κλειδί του.

Όμως, όπως έχει αναφερθεί, αυτή η μέθοδος είναι πολύ αργή και έτσι χρησιμοποιείται ένας συνδυασμός των δύο πιο πάνω μεθόδων, δηλαδή του ιδιωτικού και του δημόσιου κλειδιού, ο οποίος βελτιώνει κατά πολύ την κατάσταση χρησιμοποιώντας τα πλεονεκτήματα της κάθε μεθόδου. Δηλαδή, η επικοινωνία των κωδικοποιημένων μηνυμάτων θα γίνεται με κρυπτογράφηση ιδιωτικού κλειδιού, αφού είναι πολύ πιο γρήγορη η αποκρυπτογράφηση, αλλά η αρχική μεταφορά του

μηνύματος και του ιδιωτικού κλειδιού θα γίνεται με κρυπτογράφηση δημόσιου κλειδιού και άρα λύνεται το πρόβλημα της αξιόπιστης μεταφοράς του κλειδιού.

2.4.3 Ψηφιακές Υπογραφές (Digital Signatures)

Για να αυξηθεί η αξιοπιστία των VPNs, οι χρήστες τους μπορούν να χρησιμοποιούν ψηφιακές υπογραφές και με αυτόν τον τρόπο να ελέγχουν την πιστότητα των δεδομένων αλλά και των προσώπων που βρίσκονται στο άλλο άκρο. Οι ψηφιακές υπογραφές είναι ένα είδος κρυπτογράφησης το οποίο χρησιμοποιεί hash συναρτήσεις. Η διαδικασία δημιουργίας μιας ψηφιακής υπογραφής είναι περίπου η παρακάτω: Ο χρήστης Α περνάει το μήνυμα από μια hash συνάρτηση, μετά το μειώνει στα 128-bits και το κρυπτογραφεί με το private key του. Μέχρι εδώ ο χρήστης Α έχει δημιουργήσει την ψηφιακή του υπογραφή. Τώρα η υπογραφή του μαζί με το αρχικό μήνυμα κρυπτογραφούνται ξανά και στέλνονται στον παραλήπτη. Ο παραλήπτης τότε κάνει τις εξής δύο λειτουργίες: πρώτα αποκρυπτογραφεί το αρχικό μήνυμα και ακολούθως την υπογραφή του αποστολέα και τα συγκρίνει και έτσι μπορεί να γνωρίζει αν πράγματι ο αποστολέας του μηνύματος είναι αυτός που ισχυρίζεται ότι είναι και ότι το μήνυμα στάλθηκε από το σωστό άτομο.

2.4.4 RSA αλγόριθμος δημόσιου κλειδιού (Rivest Shamir Adlemen)

Το RSA είναι ένα ευρέως γνωστό σύστημα και χρησιμοποιείται πάρα πολύ στα VPNs όπως και σε πολλές άλλες εφαρμογές στο Internet. Βασίζεται σε δύο μαθηματικές φόρμουλες: την συνάρτηση κρυπτογράφησης, η οποία είναι CT=PTPub mod N, και τη συνάρτηση αποκρυπτογράφησης CT=CTPriv mod N, όπου PT είναι το κείμενο, CT το κρυπτογραφημένο κείμενο, Pub το public key, και Priv το private key.

Τα βήματα του RSA υπολογισμού είναι τα εξής:

I. Πάρε δύο μεγάλους πρώτους αριθμούς, έστω P1 και P2, και πολλαπλασίασε τους, βρες το γινόμενο τους. Το γινόμενο το ονομάζουμε M.

II. Ακολούθως επιλέγουμε ένα αριθμό, τον Pub, ο οποίος είναι μικρότερος από το M, αλλά σχετικά πρώτος στους (P1-1) (P2-1).

III. Βρες ακόμη ένα αριθμό, τον Priv, με τον περιορισμό ότι (PubPriv-1) είναι διαιρετέος από το (P1-1) (P2-1).

IV. Priv είναι ο private εκθέτης του private κλειδιού (M, Priv) και Pub είναι ο public εκθέτης του public κλειδιού (m, Pub).

V. Οι δύο μεγάλοι πρώτοι δεν χρειάζονται πλέον και μπορούν να καταστραφούν.

Ο RSA, όπως θα δούμε παρακάτω, χρησιμοποιείται μαζί με τα κατεξοχήν πρωτόκολλα του VPN, τα IPSec και PPTP, για να προσφέρει κρυπτογράφηση.

2.4.5 Pretty Good Privacy (PGP)

Το PGP, που στα ελληνικά μπορεί να αποδοθεί ως Αρκετά Καλή Προστασία του Απορρήτου, χρησιμοποιείται σήμερα ευρέως όχι μόνο από χρήστες των VPNs, αλλά και από κάθε είδους χρήστη σε αρκετές εφαρμογές όπως π.χ. το ηλεκτρονικό ταχυδρομείο. Το PGP υποστηρίζει υπηρεσίες εμπιστευτικότητας δεδομένων, καθώς και αυθεντικοποίησης μηνύματος, ακεραιότητας δεδομένων και μη αμφισβήτησης αποστολής, μέσω κρυπτογράφησης και ψηφιακών φακέλων. Είναι ένα υβριδικό κρυπτοσύστημα, καθώς συνδυάζει τον αλγόριθμο δημόσιου κλειδιού και τον αλγόριθμο ιδιωτικού κλειδιού. Το PGP λειτουργεί όπως όλα τα υπόλοιπα κρυπτοσυστήματα δημόσιου κλειδιού χρησιμοποιώντας τον RSA public key αλγόριθμο και τον IDEA για κρυπτογράφηση. Ο IDEA είναι ένας αλγόριθμος που χρησιμοποιεί κλειδιά μήκους 128 bits και θεωρείται ισχυρότερος από τον DES που χρησιμοποιεί κλειδιά μήκους μόνο 56 bits. Ένα IDEA κλειδί χρησιμοποιείται για κρυπτογράφηση αλλά και για αποκρυπτογράφηση του μηνύματος και ο RSA χρησιμοποιείται για να κρυπτογραφήσει το IDEA κλειδί μαζί με το δημόσιο κλειδί του παραλήπτη. Ο παραλήπτης, χρησιμοποιεί το δικό του ιδιωτικό κλειδί για να αποκρυπτογραφήσει το κατά RSA κρυπτογραφημένο μήνυμα που έχει λάβει. Χρησιμοποιώντας το αποκρυπτογραφημένο IDEA κλειδί, το οποίο προέκυψε από την αποκρυπτογράφηση του RSA μηνύματος, μπορεί να αποκρυπτογραφήσει το μήνυμα και να το διαβάσει. Παρατηρούμε ότι με αυτό τον τρόπο έχουμε έναν απλό, ασφαλή και γρήγορο τρόπο να κρυπτογραφούμε μηνύματα και να τα στέλνουμε με ασφάλεια γνωρίζοντας ότι ο παραλήπτης θα τα λάβει και θα τα διαβάσει χωρίς κανένα πρόβλημα υποκλοπής.

Αν ο Α θέλει να στείλει ένα μήνυμα στον Β μέσω μιας PGP επικοινωνίας ακολουθεί τα εξής βήματα :

1. Ο χρήστης Α κρυπτογραφεί το μήνυμα με το κλειδί κρυπτογράφησης IDEA.
2. Ο χρήστης Α κωδικοποιεί το IDEA key χρησιμοποιώντας το δημόσιο κλειδί του Β.
3. Το μήνυμα αποστέλλεται στον παραλήπτη που στην προκειμένη περίπτωση είναι ο Β.
4. Ο χρήστης Β χρησιμοποιεί το δικό του RSA ιδιωτικό κλειδί για να αποκρυπτογραφήσει το κρυπτογραφημένο IDEA κλειδί.
5. Ο χρήστης Β αποκρυπτογραφεί το μήνυμα χρησιμοποιώντας το IDEA κλειδί.

2.5 ΠΡΩΤΟΚΟΛΛΑ ΑΣΦΑΛΕΙΑΣ

2.5.1 IPSec

Όταν σχεδιάστηκε το IPv6, πριν από μερικά χρόνια, υπήρχαν ισχυρές πιέσεις να συμπεριληφθούν σ' αυτό λειτουργίες ασφάλειας. Ο βασικός στόχος ήταν να εξασφαλιστεί ότι η επόμενη γενιά του IP θα είχε διαθέσιμους ισχυρούς κρυπτογραφικούς μηχανισμούς για τους χρήστες εκείνους που θα επιθυμούσαν να τους χρησιμο-

ποιήσουν. Σύμφωνα με τους στόχους σχεδίασης, οι μηχανισμοί αυτοί έπρεπε να είναι ανεξάρτητοι από αλγόριθμους, έτσι ώστε να είναι δυνατή η αλλαγή των αλγορίθμων χωρίς να επηρεάζεται η υπόλοιπη υλοποίηση. Οι μηχανισμοί θα έπρεπε, επίσης, να είναι χρήσιμοι στην επιβολή μιας μεγάλης ποικιλίας πολιτικών ασφάλειας, αλλά, ταυτόχρονα, θα έπρεπε να σχεδιαστούν με τέτοιον τρόπο ώστε να αποφευχθούν δυσμενείς επιπτώσεις στους χρήστες του Internet που δεν χρησιμοποιούν καθόλου μηχανισμούς ασφάλειας για τη διακίνηση των δεδομένων τους. Το αποτέλεσμα της προσπάθειας αυτής ήταν η προδιαγραφή μιας ολοκληρωμένης αρχιτεκτονικής ασφάλειας για το IPv6, η οποία συνδυάζει μηχανισμούς αυθεντικοποίησης και κρυπτογράφησης.

Στο τέλος του 1992, η Internet Engineering Task Force (IETF) συγκρότησε μια ομάδα εργασίας με στόχο την προτυποποίηση ενός πρωτοκόλλου ασφάλειας IP (IP Security Protocol — IPSP) και ενός πρωτοκόλλου διαχείρισης κλειδιών Internet (Internet Key Management Protocol - IKMP). Σύντομα έγινε αντιληπτό ότι η ίδια αρχιτεκτονική που σχεδιαζόταν για το IPv6 μπορούσε να χρησιμοποιηθεί και για το IPv4. Η βασική διαφορά είναι ότι οι μηχανισμοί ασφάλειας που περιγράφονται στην αρχιτεκτονική πρέπει εκ των υστέρων να ενταχθούν στις υλοποιήσεις του IPv4, ενώ ενυπάρχουν στις υλοποιήσεις του Ipv6 εξ αρχής.

Τα IPSP και IKMP συνδέονται μόνο μέσω *συνάψεων ασφάλειας* (Security Associations - SAs), στις οποίες γίνονται αναφορές από *δείκτες παραμέτρων ασφάλειας* (Security Parameter Indices - SPIs). Βασικά, το IKMP χρησιμοποιείται για να εγκατασταθούν SAs και να αρχικοποιηθούν SPIs, ενώ το IPSP χρησιμοποιεί αυτές τις SAs και τους SPIs για να κρυπτογραφήσει πακέτα IP.

2.5.1.1 Επισκόπηση της αρχιτεκτονικής

Κάθε υποσύστημα υλοποίησης IPsec περιέχει υλοποιήσεις του IPSP και του IKMP, μια βάση δεδομένων πολιτικής ασφάλειας και μια βάση δεδομένων συνάψεων ασφάλειας. Το IPSP περιέχει τα πρωτόκολλα Authentication Header Protocol (AHP) και *Encapsulating Security Payload Protocol* (ESP) τα οποία, είτε μεμονωμένα είτε σε συνεργασία, παρέχουν τις αντίστοιχες υπηρεσίες στη σύναψη ασφάλειας.

Αν απαιτείται προστασία και με το AHP και με το ESP, τα επικοινωνούντα υποσυστήματα υλοποίησης IPsec πρέπει να εγκαταστήσουν και να συντηρήσουν δύο συνάψεις ασφάλειας. Ομοίως, προκειμένου να επιτευχθεί αμφίδρομη επικοινωνία μεταξύ δύο κεντρικών συστημάτων, το υποσύστημα υλοποίησης IPsec πρέπει να εγκαταστήσει και να συντηρήσει δύο συνάψεις ασφάλειας, μία για κάθε κατεύθυνση επικοινωνίας.

Τόσο το AHP όσο και το ESP υποστηρίζουν δύο τρόπους λειτουργίας: λειτουργία σήραγγας (tunnel mode) και λειτουργία μεταφοράς (transport mode). Στη *λειτουργία μεταφοράς* προστατεύουν κυρίως πρωτόκολλα ανώτερων επιπέδων. Ο τρόπος αυτός είναι ο απλούστερος και ο πιο συνηθισμένος για χρήση μεταξύ τελικών συστημάτων. Στη

λειτουργία σήραγγας προστατεύουν σειρές πακέτων IP χρησιμοποιώντας ενσωμάτωση IP.

Η βάση δεδομένων πολιτικής ασφάλειας, την οποία εγκαθιστά και συντηρεί ένας χρήστης ή ένας διαχειριστής συστήματος μέσα στο υποσύστημα υλοποίησης IPsec, περιέχει απαιτήσεις για το συγκεκριμένο επίπεδο προστασίας. Ο συγκεκριμένος τρόπος επεξεργασίας των πακέτων κάθε εφαρμογής επιλέγεται ταυτίζοντας πληροφορίες των επικεφαλίδων επιπέδου IP και επιπέδου μεταφοράς (διευθύνσεις IP πομπού και δέκτη, αριθμοί θυρών κτλ.) με εγγραφές της βάσης. Μια σύναψη ασφάλειας είτε αποδέχεται τις υπηρεσίες ασφάλειας IPsec κάθε πακέτου, είτε το απορρίπτει, είτε του επιτρέπει να παρακάμψει πλήρως τα πρωτόκολλα IPsec.

Κάθε σύναψη ασφάλειας αναγνωρίζεται μοναδικά από μια τριάδα αριθμών που αποτελείται από ένα δείκτη παραμέτρων ασφάλειας, μια IP διεύθυνση προορισμού και ένα όνομα, που καθορίζει το AHP ή το ESP ως πρωτόκολλο ασφάλειας. Η βάση δεδομένων σύναψης ασφάλειας περιέχει μια εγγραφή για κάθε σύναψη, που ορίζει τις παραμέτρους ασφάλειας της.

2.5.1.2 Προβλήματα που παρουσιάζονται στο IPSec

Γενικά, το IPSec μπορούμε να πούμε ότι δεν αντιμετωπίζει αρκετά προβλήματα. Ένα από τα αυτά όμως είναι η περίπτωση όπου τα κλειδιά είναι στατικά κατά την διάρκεια της επικοινωνίας και δεν υπάρχει μηχανισμός για ανταλλαγή αυτών των κλειδιών. Ένα άλλο σημαντικό πρόβλημα για το IPSec είναι η δυσκολία χειρισμού του μεγάλου αριθμού των κρυπτογραφικών κλειδιών στα μεγάλα δίκτυα. Μία λύση σε αυτό το πρόβλημα είναι το Certificate Enrollment Protocol (CEP) το οποίο έχει αναπτυχθεί από την Cisco και την VeriSign και επιτρέπει την ανταλλαγή μεγάλου αριθμού κλειδιών.

Μέχρι σήμερα, έχουν γίνει αρκετές αλλαγές στο αρχικό IPSec πρότυπο. Δεδομένου ότι πολλοί χρήστες των VPN χρησιμοποιούν dial-up συνδέσεις στο δίκτυο, το IPSec χρειάζεται να γνωρίζει πώς να διαχειρίζεται τις δυναμικές διευθύνσεις. Έτσι μία από αυτές τις αλλαγές είχε σαν κύριο στόχο να υποστηρίξει δυναμικές client διευθύνσεις.

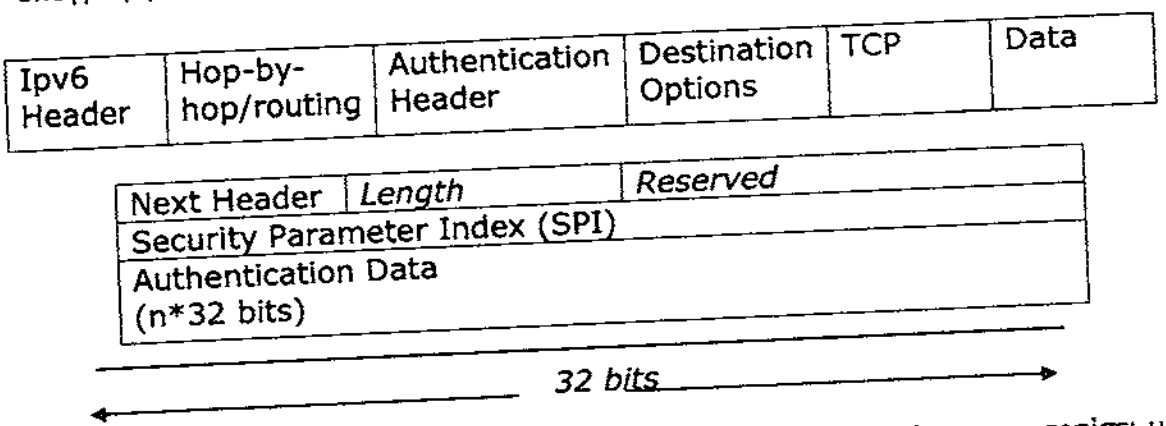
2.5.2 Πρωτόκολλο AHP (Authentication Header Protocol – Πρωτόκολλο Πιστοποίησης Επικεφαλίδας)

Το πρωτόκολλο αυτό χρησιμοποιείται όταν η ακεραιότητα και αυθεντικότητα του πακέτου IP ή του περιεχομένου του πρέπει να προστατευτούν, αλλά όχι απαραίτητα η εμπιστευτικότητα του ίδιου του πακέτου. Το πρωτόκολλο AHP παρέχει μια επιπλέον επικεφαλίδα μεταξύ των επικεφαλίδων των επιπέδων IP και μεταφοράς, η οποία περιέχει κάποια δεδομένα αυθεντικοποίησης τα οποία ο αποδέκτης επαληθεύει, ώστε να διαπιστώσει αν ο αποστολέας ήταν πράγματι αυτός που ισχυρίζεται πως ήταν. Για

το σκοπό αυτό χρησιμοποιείται μια μονόδρομη *συνάρτηση σύνοψης* (hash function) με κλειδί, όπως η MD5 με κλειδί ή ο SHA (Secure Hash Algorithm) με κλειδί. Ο υπολογισμός και η επαλήθευση δεδομένων αυθεντικοποίησης με τον τρόπο αυτό γίνονται πολύ αποτελεσματικότερα απ' ό,τι αν κρυπτογραφούσαμε και αποκρυπτογραφούσαμε όλο το πακέτο.

Στο παρακάτω σχήμα φαίνεται η δομή της επικεφαλίδας αυτής και η θέση της μέσα σε ένα πακέτο IPv6. Κάθε γραμμή της επικεφαλίδας αντιστοιχεί σε λέξη 32 bits.

Το πεδίο Next Header (μήκους 8 bits) χρησιμοποιείται για την αναγνώριση του τύπου των δεδομένων που ακολουθούν την επικεφαλίδα αυθεντικοποίησης. Το πεδίο Payload Length (μήκους 8bits) καθορίζει το μήκος της επικεφαλίδας αυθεντικοποίησης σε λέξεις *32 bits*, μειωμένο κατά 2. Για παράδειγμα, αν η τιμή αυθεντικοποίησης είναι μήκους 96 bits, το πραγματικό μήκος της επικεφαλίδας θα είναι 6, αλλά η τιμή του πεδίου αυτού θα είναι 4. Η τιμή 2 σημαίνει ότι δεν χρησιμοποιείται αλγόριθμος αυθεντικοποίησης. Το πεδίο Reserved (μήκους 16 bits) είναι δεσμευμένο για μελλοντική χρήση. Το πεδίο Security Parameter Index (SPI) (μήκους *32 bits*) καθορίζει τη σύναψη ασφάλειας του πακέτου. Η τιμή 0 σημαίνει ότι δεν υπάρχει σύναψη ασφάλειας. Το πεδίο Authentication Data περιέχει ένα μεταβλητό πλήθος λέξεων μήκους *32 bits* που περιγράφουν τα δεδομένα αυθεντικοποίησης, π.χ. έναν κώδικα αυθεντικοποίησης μηνύματος ή μια ψηφιακή υπογραφή.



Για να αυθεντικοποιηθεί ένα πακέτο, ο αποστολέας πρέπει πρώτα να εντοπίσει μια σύναψη ασφάλειας, καθορίζοντας παραμέτρους όπως ο αλγόριθμος ελέγχου ακεραιότητας, το κρυπτογραφικό κλειδί και το μήκος των δεδομένων αυθεντικοποίησης. Κανονικά, η ταυτότητα του χρήστη, η διεύθυνση προορισμού και ο δείκτης παραμέτρων ασφάλειας (SPI) καθορίζουν ποια σύναψη ασφάλειας θα χρησιμοποιηθεί.

Συνήθως, για αυθεντικοποίηση, χρησιμοποιείται ένας αλγόριθμος κώδικας αυθεντικοποίησης μηνύματος. Οι προκαθορισμένες επιλογές που πρέπει να υποστηρίζονται από όλες τις υλοποιήσεις IPsec είναι ο HMAC με τον MD5 και τον SHA-1. Ωστόσο, μπορούν να χρησιμοποιηθούν και άλλες συναρτήσεις ελέγχου ακεραιότητας. Ο υπολογισμός των δεδομένων αυθεντικοποίησης θεωρεί τα πεδία του

πακέτου, όπως αυτά εμφανίζονται στην πλευρά του δέκτη. Μερικά πεδία θα αλλάξουν κατά τη μετάδοση, όπως το hop limit στην επικεφαλίδα IP. Μερικά πεδία δεν είναι ακόμη γνωστά, όπως τα δεδομένα αυθεντικοποίησης στην επικεφαλίδα αυθεντικοποίησης. Τα πεδία αυτά γεμίζουν με μηδενικά κατά τον υπολογισμό του κώδικα αυθεντικοποίησης του μηνύματος. Ο κώδικας αυτός εισάγεται στη συνέχεια στο κατάλληλο πεδίο δεδομένων της επικεφαλίδας αυθεντικοποίησης.

Ο δέκτης του πακέτου αναφέρεται στο SPI και στη διεύθυνση προορισμού για να εντοπίσει τη σχετική σύναψη ασφάλειας και να επαληθεύσει τα δεδομένα αυθεντικοποίησης. Αν αποτύχει η αυθεντικοποίηση, η αποτυχία πρέπει να καταγραφεί και το πακέτο να απορριφθεί.

Σ' αυτόν τον αλγόριθμο, κάποια πεδία της επικεφαλίδας IP δεν καλύπτονται από το μηχανισμό προστασίας. Για περισσότερη προστασία, η λειτουργία σήραγγας προσθέτει μια εξωτερική IP επικεφαλίδα που περιέχει κάποια άλλη διεύθυνση IP, συνήθως τη διεύθυνση ενός ηλεκτρονικού αναχώματος (firewall). Η εσωτερική επικεφαλίδα IP περιέχει τις αρχικές διευθύνσεις προορισμού και προέλευσης και προστατεύεται πλήρως από την επικεφαλίδα αυθεντικοποίησης, όπως φαίνεται στο σχήμα.

Επικεφαλίδα AHP σε λειτουργία σήραγγας:

New IP Header	External Header(if present)	Authentication Header	Original IP Header	External Header(if present)	TCP	Data

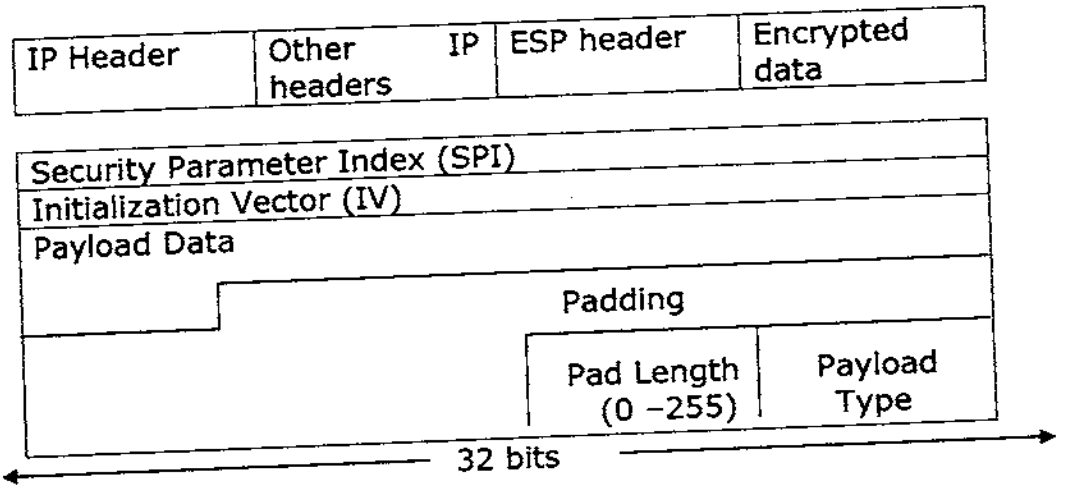
2.5.3 Πρωτόκολλο ESP (Encapsulating Security Payload Protocol - Ενσωμάτωση Επικεφαλίδας Ασφαλείας)

Το πρωτόκολλο αυτό χρησιμοποιείται για να κρυπτογραφήσει και να ενσωματώσει είτε μόνο το περιεχόμενο επιπέδου μεταφοράς είτε ολόκληρο το πακέτο IP, ανάλογα με τον τρόπο χρήσης, όπως θα δούμε αμέσως μετά. Το υποσύστημα υλοποίησης IP πρέπει να περιέχει μια επικεφαλίδα IP και να κρυπτογραφεί τμήματα του πακέτου IP, αντίστοιχα. Η κρυπτογράφηση γίνεται στην πλευρά του αποστολέα και η αποκρυπτογράφηση στην πλευρά του δέκτη. Η ακριβής μορφή των δεδομένων περιεχομένου εξαρτάται από τον συγκεκριμένο αλγόριθμο κρυπτογράφησης και το συγκεκριμένο μετασχηματισμό που χρησιμοποιείται.

Το ESP προστατεύει την εμπιστευτικότητα. Ανάλογα με τον αλγόριθμο κρυπτογράφησης που χρησιμοποιείται, μπορεί επίσης να προστατεύει την ακεραιότητα και την αυθεντικότητα. Η επικεφαλίδα ESP συνήθως τοποθετείται μπροστά από τα κρυπτογραφημένα δεδομένα, όπως φαίνεται στο παρακάτω σχήμα, και περιέχει το SPI. Η δομή της έχει ως εξής: Το πεδίο Security Parameter Index (μήκους 32 bits) αναφέρεται στο δείκτη παραμέτρων ασφάλειας του δέκτη. Το πεδίο Initialization Vector αποτελείται από μεταβλητό πλήθος λέξεων μήκους

32 bits, των οποίων το ακριβές πλήθος ορίζεται ως παράμετρος της σύναψης ασφάλειας. Το περιεχόμενο του πεδίου αυτού είναι κανονικά το αποτέλεσμα μιας γεννήτριας τυχαίων αριθμών. Το πεδίο Payload Data περιέχει τα κρυπτογραφημένα δεδομένα. Το πεδίο Padding (μεταβλητού μήκους) συνήθως γεμίζει με τυχαία bits. Το μήκος του πεδίου επιλέγεται έτσι ώστε το συνολικό μήκος των πεδίων Payload Data και Padding mod 8 να ισούται με 6.

Δομή και θέση της επικεφαλίδας ESP



Το πεδίο Pad Length (μήκους 8 bits) καθορίζει το μήκος του πεδίου Padding. Το πεδίο Payload Type (μήκους 8 bits) περιέχει τον κωδικό του πρωτοκόλλου των δεδομένων του περιεχομένου.

Πριν κρυπτογραφήσουμε ένα πακέτο, ο πομπός πάλι εντοπίζει μια σύναψη ασφάλειας για να καθορίσει ποιον αλγόριθμο κρυπτογράφησης και ποιο κλειδί θα χρησιμοποιήσει. Η σύναψη αυτή είναι διαφορετική από εκείνη που χρησιμοποιείται με το AHP.

Ο πομπός έχει στη συνέχεια δύο επιλογές τρόπου λειτουργίας του ESP:

- Σε λειτουργία μεταφοράς, ένα πλαίσιο από ανώτερο πρωτόκολλο, όπως, π.χ. από το TCP ή το UDP, ενσωματώνεται στο ESP. Η επικεφαλίδα IP δεν κρυπτογραφείται. Η λειτουργία αυτή παρέχει προστασία των πακέτων που μεταδίδονται μεταξύ δύο κόμβων απ' άκρη σε άκρη.

- Σε λειτουργία σήραγγας, ολόκληρο το IP πακέτο ενσωματώνεται στο ESP. Αυτό το ESP μεταδίδεται μέσα σε ένα άλλο πακέτο IP με μη κρυπτογραφημένες επικεφαλίδες. Επομένως, η λειτουργία αυτή μπορεί να ονομαστεί «IP μέσα στο IP». Η λειτουργία αυτή μπορεί να εφαρμοστεί μεταξύ ηλεκτρονικών αναχωμάτων για να δημιουργήσει ένα ιδεατό ιδιωτικό δίκτυο (Virtual Private Network - VPN).

Ο δέκτης του πακέτου εντοπίζει τη σχετική σύναψη ασφάλειας και αποκρυπτογραφεί το κρυπτογραφημένο περιεχόμενο. Αν η αποκρυπτογράφηση αποτύχει, το γεγονός καταγράφεται και το πακέτο απορρίπτεται.

Μέχρι τώρα έχουμε ξεπεράσει τη συζήτηση των ζητημάτων των σχετικών με τη διαχείριση κλειδιών μέσα στο IPsec. Αυτό έγινε γιατί το IPsec προδιαγράφει υπηρεσίες αυθεντικοποίησης και κρυπτογράφησης ανεξάρτητα από τα πρωτόκολλα διαχείρισης κλειδιών, που διαμορφώνουν τις σχέσεις ασφάλειας και τα κλειδιά των συνόδων. Έτσι, οι υπηρεσίες του IPsec δε συσχετίζονται με κάποιο συγκεκριμένο πρωτόκολλο διαχείρισης κλειδιών. Αν ένα τέτοιο πρωτόκολλο βρεθεί ελαττωματικό, μπορεί να αντικατασταθεί χωρίς περαιτέρω επιπτώσεις στην υλοποίηση του IPsec.

2.5.4 Πρωτκολλο IKMP (Internet Key Management Protocol)

Το IPSP προϋποθέτει ότι υπάρχουν συνάψεις ασφάλειας μεταξύ των οντοτήτων που επιθυμούν να χρησιμοποιήσουν το IPsec. Ο σκοπός του πρωτοκόλλου IKMP είναι να διαπραγματευτεί τις κρυπτογραφικές δυνατότητες και των δύο μερών, ώστε να συμφωνήσουν σε αλγόριθμους και παραμέτρους και να ανταλλάξουν κλειδιά. Με άλλα λόγια, το πρωτόκολλο εγκαθιστά και συντηρεί τις συνάψεις ασφάλειας που θα χρησιμοποιήσουν τα πρωτόκολλα AHP και ESP.

Η τρέχουσα έκδοση του πρωτοκόλλου συνδυάζει το πρωτόκολλο Internet Security Association Key Management Protocol (ISAKMP), που αναπτύχθηκε από την NSA, και το πρωτόκολλο καθορισμού κλειδιού Oakley, που αναπτύχθηκε από το Πανεπιστήμιο της Αριζόνα. Το ISAKMP χρησιμοποιείται για τη διαπραγμάτευση αμοιβαία υποστηριζόμενων αλγόριθμων και μαθηματικών δομών για την ανταλλαγή κλειδιών Diffie - Hellman και το επακόλουθο βήμα αυθεντικοποίησης. Πρόσφατα, το ISAKMP/Oakley μετονομάστηκε σε *Internet Key Exchange (IKE)* και πιθανόν κάποτε θα αντικαταστήσει το IKMP.

Η πρόταση ISAKMP/Oakley (IKE) συνδυάζει ανταλλαγή κλειδιών Diffie - Hellman και επακόλουθη αυθεντικοποίηση των παραμέτρων Diffie - Hellman. Η ανταλλαγή κλειδιών επέρχεται σε τρεις φάσεις. Στην πρώτη φάση, τα δύο μέρη ανταλλάσσουν cookies ώστε να προστατευτούν από επιθέσεις συμφόρησης πόρων (resource – clogging attacks) — μια ειδική μορφή επιθέσεων άρνησης παροχής υπηρεσίας (denial– of – service attacks), κατά την οποία ο επιτιθέμενος κατακλύζει το θύμα με υπολογισμούς μεγάλης πολυπλοκότητας, όπως, π.χ. η εκτέλεση πολλών ανταλλαγών κλειδιών Diffie - Hellman ταυτόχρονα. Στη δεύτερη φάση, εκτελούν μια ανταλλαγή κλειδιών Diffie - Hellman, ώστε αμοιβαία να υπολογίσουν το κλειδί μιας συνόδου. Το κλειδί αυτό μπορεί στη συνέχεια να χρησιμοποιηθεί μέσα στα πρωτόκολλα IPsec, έτσι ώστε να προστατευτούν οι μετέπειτα επικοινωνίες. Τα δύο μέρη, προκειμένου να αυθεντικοποιηθούν αμοιβαία και να προστατευτούν από ανεπιθύμητες επιθέσεις (Man – in – the - middle attack), καταλήγουν με την ανταλλαγή ψηφιακών υπογραφών για αυθεντικοποίηση.

Τόσο η μαθηματική δομή, στην οποία θα πραγματοποιηθεί η ανταλλαγή Diffie - Hellman όσο και η μέθοδος της επακόλουθης αυθεντικοποίησης είναι διαπραγματεύσιμες.

2.5.5 Public Key Infrastructure (PKI)

Το σύστημα αυτό και τα σχετικά πρωτόκολλα σχεδιάστηκαν από την IBM Research Division. Το πιο σημαντικό χαρακτηριστικό του συστήματος είναι ότι παρέχει πλήρη κρυπτογραφική προστασία των δεδομένων και επίσης έλεγχο, που μπορεί να χρησιμοποιηθεί για την επίλυση διαφορών.

Το PKI είναι ένα σύστημα ψηφιακών πιστοποιήσεων (digital certificates), πιστοποιήσεων εξουσιών (authorities certificates), πιστοποιήσεων διαχείρισης υπηρεσιών (certificate management services), και directory services (LDAP, X.500) το οποίο εξακριβώνει την ταυτότητα και την εξουσία του κάθε χρήστη που λαμβάνει μέρος σε κάθε συναλλαγή στο Διαδίκτυο.

Ο όρος IKP είναι τα αρχικά των λέξεων Internet Keyed Payments Protocol ή i-key-protocol, όπου i=1,2 ή 3. Η τιμή του i καθορίζει το πλήθος των μερών που κατέχουν ζεύγος δημόσιου – ιδιωτικού κλειδιού και το αντίστοιχο πιστοποιητικό.

Μερικές χρήσεις του PKI είναι:

- ❑ Αυθεντικοποίηση και πιστοποίηση
- ❑ Ιδιωτικότητα και Εμπιστευτικότητα
- ❑ Ακεραιότητα δεδομένων
- ❑ Directory Services π.χ. X.500, LDAP
- ❑ Μεταφορά Εγγράφων
- ❑ Νομικές και Οικονομικές Συναλλαγές
- ❑ Αρχειοθέτηση και Επαναφορά Εγγράφων

Το PKI έχει υλοποιηθεί για εφαρμογές οι οποίες υποστηρίζουν ασφάλεια στις υπηρεσίες του Internet όπως για παράδειγμα e-mail, έγγραφα στο WWW και ηλεκτρονικό εμπόριο.

Οι πληροφορίες οι οποίες περιέχονται σε ένα PKI πιστοποιητικό (certificate) περιλαμβάνουν :

- ◈ Την ταυτότητα του ιδιοκτήτη του πιστοποιητικού
- ◈ Το serial number του πιστοποιητικού
- ◈ Οι ημερομηνίες λήξης του πιστοποιητικού
- ◈ Αντίγραφο του δημόσιου κλειδιού και την ψηφιακή υπογραφή του χρήστη.
- ◈ Το όνομα της αρχής πιστοποίησης και την ψηφιακή υπογραφή του.

2.5.6 Point-to-Point Protocol (PPP)

Το PPP σχεδιάστηκε για να αποστέλλει δεδομένα μεταξύ dial-up ή μισθωμένων point-to-point συνδέσεων. Το PPP ενσωματώνει IP, IPX και NetBEUI πακέτα μέσα σε PPP πλαίσια και έπειτα αποστέλλει τα PPP ενσωματωμένα πακέτα που προέκυψαν σε μια point-to-point σύνδεση. Το PPP χρησιμοποιείται μεταξύ ενός χρήστη που συνδέεται τηλεφωνικά και ενός NAS. Υπάρχουν τέσσερις ξεχωριστές φάσεις κατά την εγκατάσταση μιας PPP dial-up σύνδεσης. Κάθε μια από τις τέσσερις αυτές φάσεις πρέπει να ολοκληρωθεί πριν η PPP σύνδεση είναι σε θέση να μεταφέρει δεδομένα. Αυτές είναι:

Φάση 1: Εγκαθίδρυση PPP Σύνδεσης

Το PPP χρησιμοποιεί το Link Control Protocol (LCP) για να εγκαταστήσει, να διατηρήσει και να τελειώσει τη φυσική σύνδεση. Κατά την αρχική LCP φάση, επιλέγονται οι βασικές παράμετροι της επικοινωνίας. Επίσης, κατά τη διάρκεια εγκατάστασης της σύνδεσης επιλέγονται τα πρωτόκολλα πιστοποίησης, αλλά δεν εκτελούνται μέχρι τη φάση πιστοποίησης της σύνδεσης (Connection Authentication Phase). Όμοια, κατά την LCP φάση επιλέγεται εάν θα χρησιμοποιηθεί συμπίεση και κρυπτογράφηση των δεδομένων.

Φάση 2: Πιστοποίηση Χρήστη

Στη δεύτερη φάση, ο client δίνει τα στοιχεία του στον απομακρυσμένης πρόσβασης server. Ένα πρόγραμμα ασφαλούς πιστοποίησης (Secure Authentication Protocol) προστατεύει από *replay attacks* και *remote client impersonation*. (Μια *replay attack* συμβαίνει όταν ένας τρίτος παρακολουθεί την επιτυχημένη σύνδεση και προσπαθεί να υποκλέψει τους κωδικούς για να επιτύχει μια πιστοποιημένη σύνδεση. *Remote client impersonation* συμβαίνει όταν ένας τρίτος καταλαμβάνει μια πιστοποιημένη σύνδεση. Στην περίπτωση αυτήν, ο εισβολέας περιμένει μέχρι η σύνδεση να πιστοποιηθεί και έπειτα παγιδεύει τις παραμέτρους της σύνδεσης, αποσυνδέει τον πιστοποιημένο χρήστη και παίρνει τον έλεγχο της πιστοποιημένης σύνδεσης).

Οι περισσότερες εφαρμογές πάνω στο PPP παρέχουν περιορισμένες μεθόδους πιστοποίησης μερικές από τις οποίες είναι:

- **Password Authentication Protocol-PAP.** Το PAP είναι ένα απλό πρόγραμμα πιστοποίησης. Ο NAS ζητά το όνομα του χρήστη (user name) και το password και αφού ο PAP τα επεξεργαστεί, τα επιστρέφει σε απλό κείμενο (μη κρυπτογραφημένο). Προφανώς, η μέθοδος αυτή δεν είναι ασφαλής, διότι ένας τρίτος που παρακολουθεί την διαδικασία θα μπορούσε να τα υποκλέψει και να τα χρησιμοποιήσει για να έχει πρόσβαση στον NAS και κατά συνέπεια σε όλες τις απόρρητες πληροφορίες. Δηλαδή, το PAP δεν παρέχει προστασία εναντίον replay

attacks ή client impersonation από την στιγμή που το password του χρήστη είναι εκτεθειμένο.

- **Challenge-Handshake Authentication Protocol (CHAP).** Το CHAP είναι ένας μηχανισμός πιστοποίησης του client που χρησιμοποιεί την κρυπτογραφία ώστε να αποφεύγεται η μεταφορά του πραγματικού password κατά την σύνδεση. Για τον λόγο αυτό ο client και ο server έχουν ένα συμφωνημένο τρόπο εξακρίβωσης του password του client, ώστε να μη στέλνεται το πραγματικό password. Ο NAS στέλνει ένα αίτημα πιστοποίησης (challenge) στον client. Ο client ανταποκρινόμενος στο παραπάνω αίτημα στέλνει τον κωδικό του χρησιμοποιώντας τον RSA MD5 one-way hashing αλγόριθμο. Ο αλγόριθμος αυτός, χρησιμοποιώντας μαθηματικές και τυχαίες συναρτήσεις, τροποποιεί το password του client και έπειτα το αποστέλλει στο διαδίκτυο. Ο server αφού ακολουθήσει την αντίστροφη διαδικασία αναδημιουργεί το password και το συγκρίνει με αυτό που έχει στη βάση δεδομένων του. Το όνομα του χρήστη στέλνεται μη κρυπτογραφημένο. Το CHAP είναι μια βελτίωση του PAP όπου το password του χρηστή δε στέλνεται κατά τη σύνδεση. Επιπρόσθετα, το CHAP προστατεύει από replay attacks χρησιμοποιώντας ένα αυθαίρετο μήνυμα για κάθε προσπάθεια σύνδεσης του client. Το CHAP προστατεύει και την περίπτωση του client impersonation στέλνοντας απρόβλεπτα επαναλαμβανόμενα αιτήματα πιστοποίησης στον απομακρυσμένο client κατά τη διάρκεια της σύνδεσης .
- **Microsoft Challenge-Handshake Authentication Protocol.** Το MS-CHAP είναι ένας μηχανισμός πιστοποίησης παρόμοιος με το CHAP. Όπως και στο CHAP, ο NAS στέλνει ένα αίτημα πιστοποίησης. Ο client στέλνει τον κωδικό του χρησιμοποιώντας τον MD4 αλγόριθμο και ακολουθείται η παραπάνω διαδικασία. Αυτή η διαδικασία έχει ένα επιπλέον πλεονέκτημα, ότι επιτρέπει στον server να αποθηκεύει τα passwords κωδικοποιημένα. Επίσης παρέχει επιπλέον κώδικες διόρθωσης λαθών, έλεγχο για ληγμένα passwords και μηνύματα που επιτρέπουν στους χρήστες την αλλαγή του password.

Κατά την φάση 2 διαμόρφωσης της σύνδεσης του PPP, ο NAS παίρνει τα δεδομένα για την πιστοποίηση και έπειτα τα συγκρίνει με αυτά που έχει σε κάποια βάση δεδομένων.

Φάση 3: PPP Ρύθμιση Ανακοίνωσης Επιστροφής

Η εφαρμογή PPP της Microsoft περιλαμβάνει μια προαιρετική επιλογή Callback Control Phase. Αυτή η φάση χρησιμοποιεί το Callback Control Protocol (CBCP) αμέσως μετά την φάση πιστοποίησης. Εάν έχει επιλεγεί το callback (ανακοίνωση επιστροφής), τότε η σύνδεση τερματίζεται και ο client και ο server αποσυνδέονται. Έπειτα, ο NAS καλεί τον client σε ένα συγκεκριμένο τηλεφωνικό αριθμό, γεγονός που παρέχει επιπλέον προστασία.

Φάση 4: Ενεργοποίηση των πρωτοκόλλων του επιπέδου Δικτύου

Όταν οι προηγούμενες φάσεις ολοκληρωθούν, το PPP επικαλείται τα Network Control Protocols (NCPs) τα οποία έχουν επιλεγεί κατά την εγκατάσταση της σύνδεσης στη φάση 1, για να γίνει η διαμόρφωση (configuration) των πρωτοκόλλων που χρησιμοποιεί ο client. Για παράδειγμα, σε αυτήν την φάση το πρωτόκολλο ελέγχου IP Control Protocol (IPCP) καθορίζει μια διεύθυνση στο χρήστη που επιχειρεί να συνδεθεί. Στην εφαρμογή PPP της Microsoft το πρωτόκολλο ελέγχου συμπίεσης (compression control protocol) χρησιμοποιείται για να συμπιέσει τα δεδομένα (χρησιμοποιώντας το MPPC) και για να τα κρυπτογραφήσει (χρησιμοποιώντας το MPPE).

Φάση μεταφοράς δεδομένων

Αφού οι τέσσερις προηγούμενες φάσεις έχουν ολοκληρωθεί, το PPP αρχίζει τη μεταφορά των δεδομένων. Σε κάθε μεταφερόμενο πακέτο ενσωματώνεται μία επικεφαλίδα PPP (PPP header) η οποία απομακρύνεται από το σύστημα που λαμβάνει τα δεδομένα. Εάν η συμπίεση δεδομένων είχε επιλεγεί στη φάση 1 και όλες οι παράμετροι είχαν συμφωνηθεί στη φάση 4, τα δεδομένα θα συμπιεσθούν πριν τη μεταφορά τους. Το ίδιο συμβαίνει και με την κρυπτογράφηση.

2.5.7 Point-to-Point Tunneling Protocol (PPTP)

Το PPTP είναι ένας συνδυασμός του Point-to-Point Protocol και του Transmission Control Protocol / Internet Protocol (TCP/IP). Το PPTP συνδυάζει τα χαρακτηριστικά του PPP (π.χ. privacy με συμπίεση πακέτων δεδομένων) και του TCP/IP (κυρίως τη δυνατότητα για δρομολόγηση των πακέτων στο Internet). Μαζί με το IPSec είναι ένα από τα κύρια VPN πρωτόκολλα που χρησιμοποιούνται σήμερα.

Το PPTP μπορεί να πάρει πακέτα όπως IP, IPX, NetBios, SNA και να τα μετατρέψει σε ένα καινούριο IP πακέτο για μεταφορά. Χρησιμοποιεί το Generic Routing Protocol (GRE) για μεταφορά των PPP πακέτων. Χρησιμοποιεί επίσης κρυπτογράφηση για ενσωματωμένα δεδομένα τα οποία παρέχει για πιστοποίηση. Η κίνηση του PPTP αποτελείται από δύο είδη πακέτων για διαφορετικούς τύπους δεδομένων: data packets και control packets. Τα πακέτα ελέγχου χρησιμοποιούνται για σηματοδότηση, ενώ τα πακέτα δεδομένων για να μεταφέρουν τα δεδομένα του χρήστη. Τα πακέτα δεδομένων είναι πακέτα τα οποία έχουν υποστεί την διαδικασία του encapsulation χρησιμοποιώντας το Internet Generic Routing Encapsulation Protocol Version 2 (GRE v2).

Η PPTP σύνδεση ξεκινά σαν ένα handshake (χειραψία) μεταξύ δύο απομακρυσμένων σημείων με σκοπό την επίτευξη συμφωνίας στο συμπιεστικό σχήμα και στη μέθοδο για encapsulation που θα χρησιμοποιηθεί. Κατά την διάρκεια της

επικοινωνίας αυτά τα πακέτα μπορούν, αν απαιτηθεί, να τμηματοποιηθούν και ένα PPP header προσθέτει ένα serialization αριθμό για την εξακρίβωση χαμένων πακέτων.

Τα PPTP και IPSec μπορούν να επιτύχουν παρόμοια αποτελέσματα. Μπορούμε να έχουμε ένα IPSec client για την εγκατάσταση ασφαλούς session (τμήματος) σε ένα firewall και την δημιουργία ενός VPN ή να έχουμε ένα PPTP client για την εγκατάσταση ενός session στο firewall. Όμως, το PPTP χρειάζεται ένα NT-based firewall αφού τρέχει μόνο σε NT servers. Το PPTP εμφανίζεται με δύο τρόπους, ο πρώτος είναι ο υποχρεωτικός τρόπος όπου η PPTP σύνδεση γίνεται στο σημείο σύνδεσης του ISP. Επομένως, ο ISP θα χρειαστεί ένα ειδικό επεξεργαστή για να χειριστεί τις PPTP συνδέσεις. Ο δεύτερος τρόπος είναι ο εθελοντικός τρόπος κατά τον οποίο η PPTP σύνδεση γίνεται στο άκρο, για παράδειγμα client-to-server.

Το PPTP αποτελείται από τρία είδη επικοινωνίας:

- PPTP σύνδεση: Αυτή γίνεται όταν ο client εγκαταστήσει ένα PPP ή ISDN σύνδεσμο με τον ISP του.
- PPTP σύνδεση ελέγχου (control connection): Χρησιμοποιώντας το Internet ο χρήστης δημιουργεί την PPTP σύνδεση στον VPN server και θέτει τα PPTP χαρακτηριστικά του tunnel.
- PPTP data tunnel: Ο client και ο server επικοινωνούν μεταξύ τους μέσω του κρυπτογραφημένου tunnel.

Η ασφάλεια στο PPTP είναι ολοκληρωμένη με το Windows NT RAS security. Η επικοινωνία μεταξύ απομακρυσμένων χρηστών και το ιδιωτικό δίκτυο της εταιρείας τους γίνεται με RAS κρυπτογράφηση και πιστοποίηση. Τα πρωτόκολλα πιστοποίησης που χρησιμοποιούνται είναι τα PAP, CHAP και MS-CHAP. Τα πρωτόκολλα κρυπτογράφησης είναι κλειδιών των 40-bit όπως RSA-RC4 και DES. Η 128-bit κρυπτογράφηση είναι διαθέσιμη μόνο για χρήση στις ΗΠΑ και Καναδά.

2.5.8 Layer 2 Forwarding Protocol (L2F)

Το L2F είναι ένα από τα πρωτόκολλα που χρησιμοποιούνται σήμερα στα VPNs σε συνδυασμό με το PPTP. Λόγω της μεγάλης ανάπτυξης των dial-up υπηρεσιών και την παροχή πολλών διαφορετικών πρωτοκόλλων χρειαζόταν ένας τρόπος για να δημιουργείται ένα εικονικό dial-up σενάριο όπου οποιοδήποτε από τα μη-IP πρωτόκολλα να μπορεί να χρησιμοποιεί τα πλεονεκτήματα που παρέχει το Internet. Οι χρήστες μπορούν να κάνουν μία PPP ή SLIP σύνδεση σε έναν dial-up ISP παροχέα υπηρεσιών και χρησιμοποιώντας το L2F πρωτόκολλο να συνδεθούν στα μηχανήματα της εταιρείας τους.

Ορισμένα από τα οφέλη που προσφέρει το L2F είναι :

- Ανεξαρτησία πρωτοκόλλων (IPX, SNA)

- Αυθεντικοποίηση (PPP, CHAP, TACACS)
- Διαχείριση διευθύνσεων
- Δυναμικά και ασφαλή tunnels
- Accounting
- Ανεξαρτησία των media

2.5.8.1 Από κοινού L2F tunneling και τοπική πρόσβαση στο Internet

Σε μία τυπική εγκατάσταση ο χρήστης κάνει μία PPP ή άλλη παρόμοια σύνδεση στον ISP και κατά την διάρκεια της αίτησης το NAS, χρησιμοποιώντας το λογισμικό του L2F, αρχικοποιεί ένα tunnel προς τον προορισμό του χρήστη. Στη συνέχεια, ο προορισμός απαιτεί το password του χρήστη και αφού γίνει πιστοποίηση παραχωρείται στο χρήστη η IP διεύθυνση σαν μία τυπική dial-up απομακρυσμένη πρόσβαση.

2.5.9 Layer 2 Tunneling Protocol (L2TP)

Λόγω του ότι μεγάλες εταιρείες όπως η Microsoft, Ascend και 3Com, δούλευαν με το PPTP ενώ η Cisco με το L2F αποφάσισαν για λόγους συμβατότητας να ορίσουν ένα νέο πρότυπο, το L2TP το οποίο είναι το αποτέλεσμα της συγχώνευσης του PPTP και του L2F.

Το L2TP παρέχει συμπίεση βασισμένη στο λογισμικό η οποία συμπυκνώνει τα πακέτα των χρηστών. Επίσης, ένας μικρός αριθμός τεχνικών συμπίεσης έχει προστεθεί στο επίπεδο της κρυπτογράφησης. Το L2TP χρησιμοποιεί δύο συναρτήσεις: την client-like line server η οποία αναφέρεται ως LAC και είναι ένας L2TP συγκεντρωτής πρόσβασης και τον server-side network server ο οποίος καλείται LNS. Όταν ένα PC κάνει PPP σύνδεση στον ISP, μία LAC συνάρτηση αρχικοποιεί το tunnel, προσθέτει διάφορους headers στο PPP payload και εγκαθιδρύει το tunnel στην LNS τερματική συσκευή – αυτή η συσκευή μπορεί να είναι router, server ή συσκευή πρόσβασης. Αφού έχει εγκαθιδρυθεί το tunnel, εγκαθίσταται ένας μηχανισμός πιστοποίησης του χρήστη για να πιστοποιείται η ταυτότητα των χρηστών. Επίσης, το L2TP χρησιμοποιεί μηνύματα ελέγχου για την βελτιστοποίηση του tunnel.

Το L2TP είναι ένα πρωτόκολλο επιπέδου-2 σχεδιασμένο για την ενσωμάτωση στο επίπεδο-2. Επομένως, το IPSec το οποίο είναι ένα πρωτόκολλο επιπέδου-3 μπορεί να χρησιμοποιηθεί μαζί με το L2TP για περισσότερη ασφάλεια (στην πραγματικότητα αυτό συνίσταται).

2.5.10 Secure Wide Area Network (S/WAN)

Το Secure Wide Area Network (S/WAN) πρωτόκολλο είναι ένα πρωτόκολλο το οποίο παρέχει ενδολειτουργικότητα. Ακόμη αυτό το πρωτόκολλο δεν έχει υλοποιηθεί. Αν γίνει αποδεκτό και υλοποιηθεί από τις εταιρίες, θα επιτρέψει σε διάφορους οργανισμούς να διασταυρώσουν και να ταιριάξουν προϊόντα από διάφορες εταιρίες για να δημιουργήσουν κρυπτογραφημένα tunnels. Σκοπός του είναι να βάλει την ασφάλεια όσο πιο χαμηλά γίνεται στο επίπεδο OSI. Το S/WAN περιλαμβάνει όλους τους γνωστούς αλγορίθμους συμπεριλαμβανομένων των RSA, DES, RC4 και RC5, και κλειδιά των 40 και 128 bits.

Το Internet Security Protocol (IPSec) δεν προτείνει κάποιους συγκεκριμένους κρυπτογραφικούς και πιστοποιητικούς αλγορίθμους για να χρησιμοποιηθούν. Επομένως, ακόμη και αν πολλές εταιρίες παροχής VPN υποστηρίζουν IPSec, μπορεί το δίκτυο να μην είναι συμβατό λόγω των κρυπτογραφικών και πιστοποιητικών αλγορίθμων που έχουν χρησιμοποιηθεί. Έτσι, το S/WAN βρίσκεται στο κάτω σημείο του επιπέδου όπου βρίσκονται τα πρωτόκολλα κρυπτογράφησης. Για παράδειγμα, το SSL-SOCKS θα βρίσκεται στην κορυφή του επιπέδου που βρίσκεται το S/WAN. Έτσι, αν όλοι οι vendors (πωλητές – αντιπρόσωποι) υποστηρίξουν το S/WAN, τότε θα έχουμε VPN ενδολειτουργικότητα με τους διάφορους vendors που υποστηρίζουν το IPSec. Δυστυχώς, αυτό θα αργήσει να γίνει γιατί υπάρχουν αρκετοί vendors που δεν υποστηρίζουν το IPSec.

2.6 ΣΥΓΚΡΙΤΙΚΟΣ ΠΙΝΑΚΑΣ ΠΡΩΤΟΚΟΛΛΩΝ

Χαρακτηριστικό Γνώρισμα	Περιγραφή	PPTP/ PPP	L2TP/ PPP	L2TP/ IPSec	IPSec Tunnel
Πιστοποίηση Χρήστη	Μπορεί να πιστοποιήσει το χρήστη που αρχίζει την επικοινωνία.	NAI	NAI	NAI	WIP[1]
Πιστοποίηση Hardware	Πιστοποιεί τις μηχανές που παίρνουν μέρος στην επικοινωνία.	NAI	NAI	NAI	NAI
Υπηρεσία NAT	Μπορεί να περάσει μέσω του NAT (μεταφραστή διευθύνσεων δικτύων) για να κρύψει το ένα ή και τα δυο άκρα της επικοινωνίας.	NAI	NAI	OXI	OXI
Υποστήριξη Πολλαπλής Διανομής	Καθορίζει μια πρότυπη μέθοδο για τη μεταφορά IP και μη- IP κυκλοφορίας.	NAI	NAI	NAI	WIP
Ανάθεση Δυναμικών Διευθύνσεων IP	Καθορίζει έναν πρότυπο τρόπο να διαπραγματεύεται μια διεύθυνση IP για το ανοιγμένο (tunneled) μέρος της επικοινωνίας. Αυτό είναι σημαντικό γιατί καθοδηγεί τα επιστρεφόμενα πακέτα πίσω μέσω του ίδιου καναλιού επικοινωνίας και όχι μέσω ενός μη-ανοιγμένου(tunneled) και μη ασφαλούς μονοπατιού (path).	NAI	NAI	NAI	WIP
Κρυπτογράφηση	Μπορεί να κρυπτογραφήσει την κυκλοφορία που μεταφέρει.	NAI	NAI	NAI	NAI
Υπηρεσία PKI	Μπορεί να χρησιμοποιήσει το PKI για να εφαρμόσει την κρυπτογράφηση ή/και την πιστοποίηση ταυτότητας.	NAI	NAI	NAI	NAI
Πιστοποιησιμότητα Πακέτων	Παρέχει μια μέθοδο πιστοποίησης για να εξασφαλίσει ότι το περιεχόμενο των πακέτων δεν αλλάζει κατά τη μεταφορά.	OXI	OXI	NAI	NAI
Πολλαπλή Υποστήριξη	Μπορεί να μεταφέρει την πολλαπλής διανομής κυκλοφορία IP εκτός από την απλή κυκλοφορία IP.	NAI	NAI	NAI	NAI

[1] Η υποστήριξη δεν παρέχεται ακόμα εντούτοις, υπάρχει εργασία υπό εξέλιξη (WIP – Work In Progress) από το IPSec Working Group της IETF.

2.7 ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Virtual Private Networks
Second Edition
Charlie Scott, Paul Wolfe and Mike Erwin

2. Ασφάλεια στο Internet
Ελληνικό Ανοικτό Πανεπιστήμιο Πάτρας

3. Πτυχιακή Εργασία: Ιδεατά Ιδιωτικά Δίκτυα
Καλλίγερος Εμμανουήλ
Μπέλλος Μάτσιεϊ
Νεάρχου Μιχάλης

4. ΧΡΗΣΙΜΕΣ ΔΙΕΥΘΥΝΣΕΙΣ ΣΤΟ INTERNET:
www.cisco.com

www.microsoft.com

www.oreilly.com

www.vpn.org

ΚΕΦΑΛΑΙΟ 3

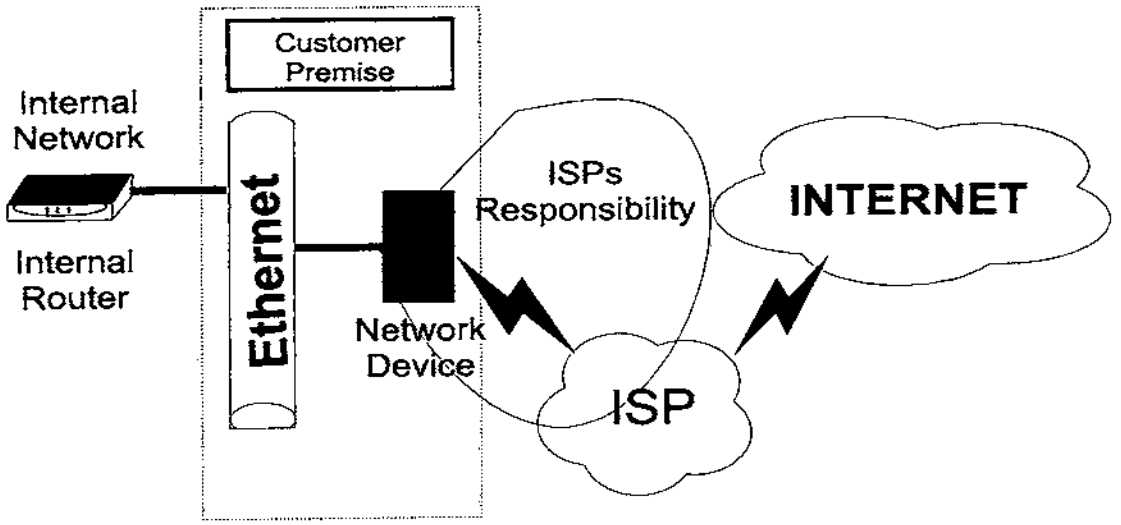
3.1 VPN ΑΡΧΙΤΕΚΤΟΝΙΚΕΣ

Στο κεφάλαιο αυτό θα αναφερθούμε στις διάφορες αρχιτεκτονικές με τις οποίες μπορούμε να δημιουργήσουμε ένα VPN. Το ποια από αυτές τελικά θα επιλέξουμε εξαρτάται από πολλούς παράγοντες και πρώτα πρώτα από τις ανάγκες του οργανισμού που θέλει να εγκαταστήσει το VPN. Με άλλα λόγια, θα πρέπει να λάβουμε υπ' όψιν μας παράγοντες όπως το πόσους χρήστες θα πρέπει να εξυπηρετεί το VPN του οργανισμού και πόσο αναμένεται να αυξηθεί στο μέλλον ο φόρτος του δικτύου από την προσθήκη νέων χρηστών. Πόση ανάγκη για ασφάλεια υπάρχει, για ποιους σκοπούς θα χρησιμοποιείται το VPN (π.χ. e-commerce) κ.ά. Επίσης, η επιλογή που θα κάνουμε, θα εξαρτάται και από τις δυνατότητες του οργανισμού, δηλαδή από την υποδομή που έχει σε hardware, καθώς και από το πόσο και έως ποιο βαθμό μπορεί το τεχνικό προσωπικό του να υποστηρίξει τη λύση VPN που θα επιλεγεί. Έτσι λοιπόν, μπορούμε να ξεχωρίσουμε τις ακόλουθες αρχιτεκτονικές VPN:

3.1.1 VPNs υποστηριζόμενα από κάποιον Παροχέα Πρόσβασης στο Internet (ISP)

Αυτός είναι ο πιο απλός τρόπος να εγκαταστήσει ένας οργανισμός ένα Virtual Private Network. Ο οργανισμός απευθύνεται σε κάποιον ISP ο οποίος εγκαθιστά στο κτήριο του οργανισμού κάποια συσκευή δικτύωσης η οποία θα αναλάβει να δημιουργήσει τα tunnels που χρειάζονται για το VPN. Η συσκευή αυτή θα έχει κάποιο λειτουργικό σύστημα, όπως για παράδειγμα το Unix, επειδή έτσι θα μπορεί κανείς να τη διαχειριστεί εξ αποστάσεως (remote managing). Επίσης, πολύ πιθανή είναι και η χρησιμοποίηση κάποιου firewall (μετά από τη συσκευή δικτύωσης). Ένα γενικό σχήμα αυτής της VPN αρχιτεκτονικής φαίνεται στο σχήμα 3.1. Παρατηρούμε ότι μία εταιρεία, με τη συγκεκριμένη VPN αρχιτεκτονική, έχει τη μικρότερη δυνατή εμπλοκή μιας και η συσκευή δικτύωσης αυτή καθεαυτή καθώς και η επικοινωνία της προς τα έξω αναλαμβάνονται εξ ολοκλήρου από τον Παροχέα Πρόσβασης στο Internet.

Παρόλο που ο τρόπος αυτός φαίνεται να είναι ο πιο απλός, αφού ο οργανισμός μετατρέπεται σε απλό χρήστη του VPN, αυτό δεν είναι απόλυτα σωστό. Υπάρχει μία σειρά από προβλήματα τα οποία για να λυθούν απαιτούν επέμβαση από τη μεριά του χρήστη του VPN.



Σχήμα 3.1 VPN παρεχόμενο από ISP

Το πρώτο και κυριότερο είναι το θέμα της ασφάλειας. Είναι πολύ αμφίβολο το αν ο ISP θα είναι υπεύθυνος για την ασφάλεια, παρόλο που είναι αυτός που «δίνει» τη συσκευή δικτύωσης και παρέχει τελικά το VPN. Οι ISPs είναι κατά πρώτο λόγο παροχείς πρόσβασης στο Internet και κατά δεύτερο παροχείς VPN υπηρεσιών. Έτσι λοιπόν, αν κάποιος χρήστης δημιουργήσει, μέσω ενός VPN, κάποιο πρόβλημα ασφάλειας, τότε είναι πολύ πιθανό ότι το πρόβλημα αυτό δε θα εμποδιστεί από τον ISP. Στην περίπτωση αυτή, θα πρέπει ο οργανισμός – χρήστης του VPN, να προσλάβει μία εξωτερική ομάδα για να δημιουργήσει μία πολιτική ασφαλείας η οποία θα πρέπει στη συνέχεια να εφαρμοστεί από τον ISP.

Ένα άλλο πρόβλημα αφορά το ποιος και πόσο γρήγορα μπορεί να αλλάξει την πολιτική πρόσβασης στο VPN. Ο ISP μπορεί να μην έχει τον απαραίτητο χρόνο να κάνει τέτοιες αλλαγές. Έτσι κάποιος χρήστης μπορεί να ζητήσει να προσπελάσει κάποιον προορισμό ή κάποια υπηρεσία, η οποία μέχρι εκείνη τη στιγμή δεν διατίθεται. Στην περίπτωση αυτή θα χρειαστούν κάποιες μέρες για να εξασφαλισθούν οι απαραίτητες άδειες πρόσβασης και στη συνέχεια θα πρέπει να συμπληρωθούν κάποιες φόρμες οι οποίες θα ζητούν από τον ISP να αλλάξει τη διαμόρφωση του δικτύου. Είναι προφανές ότι η διαδικασία αυτή είναι αρκετά δύσκαμπτη και χρονοβόρα. Επίσης, επειδή για να προστεθεί κάποια καινούρια υπηρεσία, είναι πιθανό να χρειάζεται να γίνουν αρκετές αλλαγές στη διαμόρφωση του VPN, θα πρέπει για κάθε αλλαγή να ενημερώνεται ο χρήστης, αφενός ότι η αλλαγή έγινε και αφετέρου για τον τρόπο με τον οποίο αυτή έγινε.

Μεγάλη προσοχή θα πρέπει να δοθεί επίσης και στην περίπτωση του εντοπισμού και της αντιμετώπισης των βλαβών. Αν προκύψει κάποια βλάβη και το τεχνικό προσωπικό του οργανισμού δεν έχει αντιμετωπίσει κάτι παρόμοιο, τότε τα πράγματα μπορεί να γίνουν πολύ δύσκολα. Μπορεί να χρειαστούν ακόμα και εβδομάδες, ειδικά για προβλήματα τα οποία δεν είναι συνεχή, δηλαδή εμφανίζονται κατά διαστήματα και

στη συνέχεια εξαφανίζονται. Για να προληφθούν τέτοιες περιπτώσεις, είναι προτιμότερο κανείς να πληρώσει παραπάνω χρήματα σε κάποιον ISP, έτσι ώστε να εξασφαλίσει υποστήριξη σε περιπτώσεις βλαβών.

Πολύ σημαντικό θέμα, επίσης, είναι και αυτό της αυθεντικοποίησης, δηλαδή του ποιοι χρήστες επιτρέπεται να δημιουργήσουν ένα tunnel προς το VPN κάποιου οργανισμού. Η βάση δεδομένων που χειρίζεται αυτή την πληροφορία θα βρίσκεται στην πλευρά του ISP ή στην πλευρά του χρήστη του VPN; Αυτό είναι πολύ σημαντικό στην περίπτωση που κάποιος υπάλληλος απολυθεί ή παραιτηθεί από τη θέση του. Καταλαβαίνουμε ότι θα θέλαμε άμεσα να μην του ξαναδώσουμε την ευκαιρία να χρησιμοποιήσει το δίκτυό μας, κάτι το οποίο είναι ιδιαίτερα δύσκολο όταν δεν μπορούμε να προσπελάσουμε αυτές τις βάσεις γρήγορα.

Θα πρέπει επίσης, με κάποιο τρόπο, ο οργανισμός που χρησιμοποιεί το VPN να μπορεί να παρακολουθεί τη χρήση του (utilization) καθώς και τη χρήση της συσκευής δικτύωσης. Έτσι μόνο θα μπορεί να ξέρει έγκαιρα πότε θα χρειαστεί να αναβαθμίσει κάποιο από τα δύο, έτσι ώστε να μην δημιουργηθεί κάποιο πρόβλημα λόγω μεγάλου φόρτου.

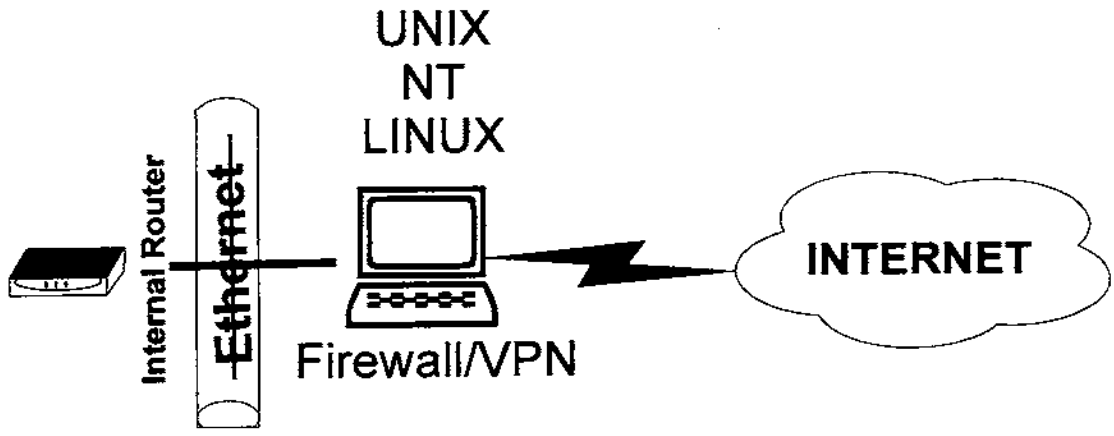
Ένα τελευταίο, αλλά πολύ σημαντικό θέμα, αφορά την ασφάλεια των κλειδιών. Θα πρέπει τα κλειδιά να φυλάσσονται σε κάποιο «σίγουρο» μέρος, όχι μόνο για λόγους ασφαλείας, αλλά και για να ξέρει κανείς που μπορεί να τα βρει αν χρειαστεί κάποιο από αυτά. Για παράδειγμα, τα κλειδιά κρυπτογράφησης μπορεί να χρειάζονταν στην περίπτωση που η συσκευή δικτύωσης χαλάσει και πρέπει να αντικατασταθεί. Συνήθως, σε τέτοιες περιπτώσεις, ακυρώνονται τα παλιά κλειδιά και δημιουργούνται καινούρια. Για να μπορέσουμε όμως να τα ακυρώσουμε θα πρέπει να τα γνωρίζουμε και άρα να τα επαναφέρουμε από κάποιο ασφαλές μέρος στο οποίο τα έχουμε κρατήσει.

3.1.2 VPNs βασισμένα σε Firewalls (Firewall-Based)

Τα VPNs τα οποία βασίζονται σε Firewalls είναι ίσως ο πιο διαδεδομένος τύπος VPN. Αυτό δεν σημαίνει βέβαια ότι αυτού του τύπου τα VPNs υπερτερούν σε σχέση με τα υπόλοιπα, απλά οι περισσότεροι οργανισμοί που αυτή τη στιγμή είναι συνδεδεμένοι στο Internet διαθέτουν firewalls. Έτσι, το μόνο που χρειάζεται από την πλευρά τους είναι να προσθέσουν το κατάλληλο λογισμικό που θα κάνει την κρυπτογράφηση. Μάλιστα, αν κάποια εταιρεία ή οργανισμός διαθέτει κάποιο πρόσφατα αγορασμένο firewall, τότε είναι πολύ πιθανό αυτό να έχει ενσωματωμένη τη δυνατότητα να πραγματοποιεί κάποια κρυπτογράφηση για VPN.

Μεγάλη σημασία, από άποψη ασφάλειας, πρέπει να δώσει κανείς στο λειτουργικό σύστημα του firewall και πιο συγκεκριμένα στα τρωτά σημεία που πιθανώς αυτό να έχει. Κανένα σύστημα δεν είναι εκατό τοις εκατό ασφαλές και έτσι, αν θέλουμε να δημιουργήσουμε ένα VPN, θα πρέπει το λειτουργικό σύστημα της συσκευής

δικτύωσης να είναι όσο το δυνατόν ασφαλέστερο. Στο σχήμα 3.2 φαίνεται ένα firewall-based VPN. Σημειώνουμε εδώ και πάλι, ότι η υλοποίηση ενός τέτοιου τύπου VPN δεν είναι απλή, αλλά βολεύει πολύ τις εταιρείες οι οποίες διαθέτουν ήδη τέτοιες συσκευές.

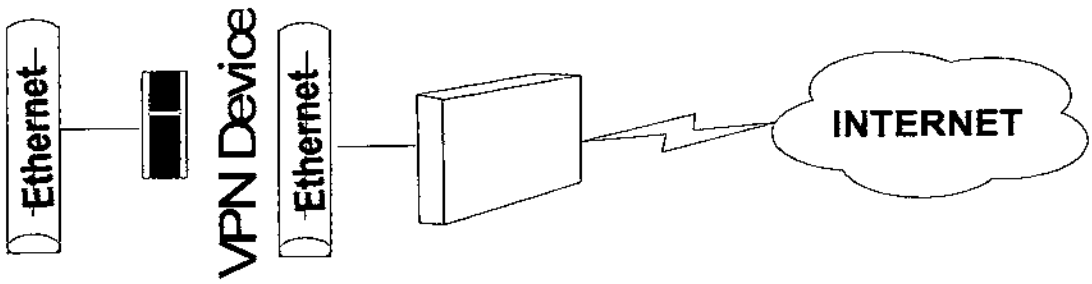


Σχήμα 3.2 VPN βασισμένο σε Firewall

Θα πρέπει, τέλος, να διευκρινίσουμε το εξής: υπάρχουν τρία είδη firewalls στην αγορά: τα stateful-inspection, τα proxies και τα packet filtering. Μιλώντας για προσθήκη VPN τεχνολογίας σε ένα firewall αναφερόμαστε στον πρώτο από τους τρεις τύπους. Αυτός «τρέχει» στα επίπεδα 2 και 3 του OSI protocol stack. Ένας proxy server τρέχει στο επίπεδο εφαρμογών, ενώ ο packet filtering πρέπει να ελέγχει το πλήρες πακέτο που περνάει κάθε στιγμή. Επειδή, όμως, όσο κατεβαίνουμε πιο χαμηλά στα επίπεδα του protocol stack τόση μεγαλύτερη ασφάλεια μπορούμε να πετύχουμε, όταν μιλάμε για προσθήκη VPN τεχνολογίας, αναφερόμαστε πάντα στα stateful-inspection firewalls τα οποία τρέχουν σε επίπεδα χαμηλότερα από τα υπόλοιπα.

3.1.3 VPNs βασισμένα σε μαύρα κουτιά (Black-Box Based)

Στην περίπτωση αυτή, ο παροχέας VPN υπηρεσιών προσφέρει ακριβώς αυτό, ένα μαύρο κουτί, δηλαδή μία συσκευή με το απαραίτητο λογισμικό για να δημιουργήσουμε ένα tunnel. Μερικές από τις συσκευές αυτές συνοδεύονται από software το οποίο τρέχει σε κάποιον υπολογιστή και μας βοηθάει να τις διαχειριστούμε, ενώ σε άλλες μπορούμε να αλλάξουμε τη διαμόρφωση μέσω Web. Στην περίπτωση των black boxes χρειαζόμαστε τις περισσότερες φορές έναν ακόμα server για να κάνουμε την πιστοποίηση των χρηστών. Παρά το γεγονός αυτό, ένα ελκυστικό χαρακτηριστικό που έχουν τα black boxes είναι ότι το λογισμικό τους επιτρέπει, για την πιστοποίηση, να χρησιμοποιείται μία ήδη υπάρχουσα βάση δεδομένων, η οποία βρίσκεται σε κάποιον server και έτσι απαλλασσόμαστε από το πρόβλημα του να έχουμε διάφορες βάσεις με χρήστες και να προσπαθούμε να τις κρατάμε συγχρονισμένες.



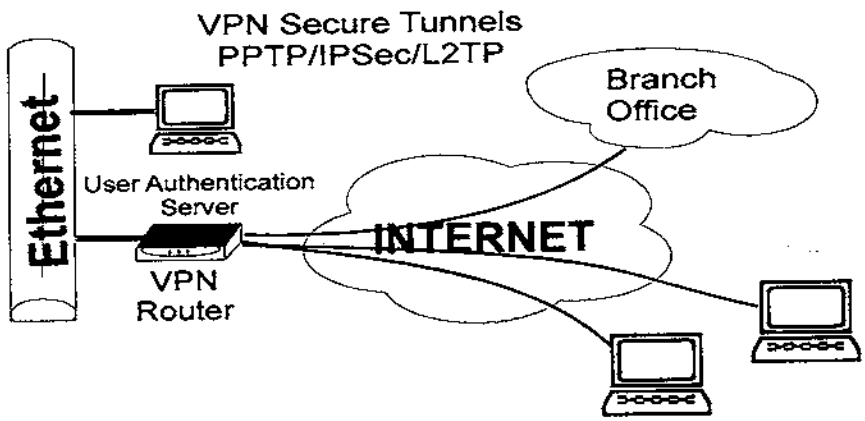
Σχήμα 3.3 VPN βασισμένο σε μαύρο κουτί

Τις περισσότερες φορές, μαζί με τα black boxes χρειαζόμαστε και κάποιο firewall, αν και οι περισσότεροι κατασκευαστές τέτοιων συσκευών έχουν αρχίσει να ενσωματώνουν δυνατότητες firewall σε αυτά. Το firewall παρέχει ασφάλεια στην επιχείρηση, ενώ το VPN ασφάλεια στα δεδομένα. Το μόνο που θα πρέπει να εξασφαλίσουμε σε αυτή την περίπτωση είναι ότι τα κρυπτογραφημένα πακέτα θα μπορούν να περνούν από το firewall. Στο σχήμα 3.3 φαίνεται το διάγραμμα ενός VPN βασισμένου σε μαύρο κουτί.

3.1.4 VPNs βασισμένα σε Routers (Router-Based)

Ο τύπος αυτός των VPNs ταιριάζει σε οργανισμούς οι οποίοι έχουν επενδύσει αρκετά χρήματα σε routers και έχουν τεχνικό προσωπικό εξειδικευμένο σε αυτούς. Υπάρχουν δύο τύποι τέτοιων VPNs. Στον πρώτο εγκαθίσταται στον router λογισμικό που κάνει κρυπτογράφηση, ενώ ο δεύτερος χρησιμοποιεί, για τον ίδιο λόγο, μια κάρτα από έναν τρίτο κατασκευαστή, η οποία τοποθετείται στο σασί του router με αποτέλεσμα να αποδεσμεύεται η CPU από το φόρτο της κρυπτογράφησης. Αυτό είναι πολύ σημαντικό αφού η διαδικασία του routing απαιτεί αρκετούς πόρους, ειδικά όταν οι routers είναι πολλοί και ο routing αλγόριθμος ευαίσθητος.

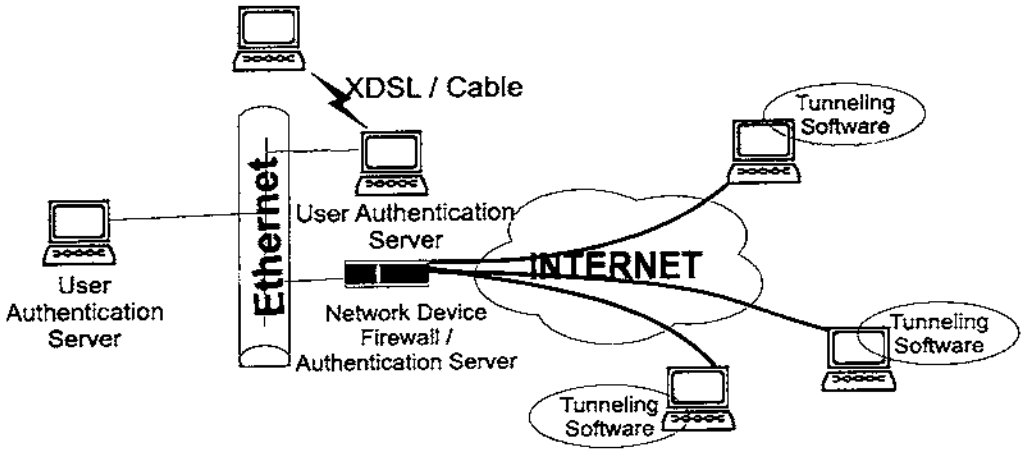
Επίσης, ένα άλλο ζήτημα στα VPNs αυτού του τύπου, είναι αν ο router θα χειρίζεται την πιστοποίηση των χρηστών ή αν θα πρέπει να συνεργάζεται με κάποια άλλη συσκευή που θα κάνει αυτή τη δουλειά. Στο σχήμα 3.4 φαίνεται ένα VPN βασισμένο σε router το οποίο απαιτεί και κάποιον server για πιστοποίηση.



Σχήμα 3.4 VPN βασισμένο σε router

3.1.5 VPNs βασισμένα σε πρόσβαση από απόσταση (Remote Access-Based)

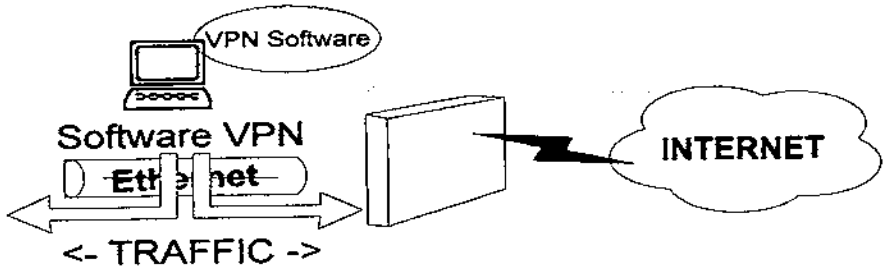
Όπως φανερώνει και το όνομά τους, αυτού του είδους τα Εικονικά Ιδιωτικά Δίκτυα, έχουν να κάνουν με χρήστες οι οποίοι βρίσκονται κάπου εκτός της επιχείρησης και προσπαθούν με τη βοήθεια software να δημιουργήσουν ένα tunnel προς κάποια συσκευή δικτύου η οποία επιτρέπει τη σύνδεση. Το tunnel αυτό μπορεί να δημιουργηθεί μέσω Internet, αλλά και μέσω μίας dial-up ή ISDN γραμμής ή και ενός X.25 δικτύου. Ένα τέτοιο VPN φαίνεται στο σχήμα 3.5.



Σχήμα 3.5 VPN βασισμένο σε πρόσβαση από απόσταση

3.1.6 VPNs βασισμένα στο λογισμικό (Software-based)

Εδώ, χρησιμοποιείται λογισμικό για να γίνει tunneling ή κρυπτογράφηση από κάποιον πελάτη προς κάποιον εξυπηρετητή (client - server). Η διαφορά από τους υπόλοιπους τύπους έγκειται στο γεγονός ότι αντί να έχουμε ένα μοναδικό σημείο πρόσβασης προς το εσωτερικό δίκτυο ενός οργανισμού (π.χ. firewall) και μέσα στο δίκτυο αυτό η πληροφορία να είναι αποκωδικοποιημένη (decrypted), εδώ κάθε σταθμός του εσωτερικού δικτύου μπορεί να έχει ένα δικό του ζευγάρι ιδιωτικού - δημόσιου κλειδιού και η πληροφορία να φτάνει σε αυτόν κρυπτογραφημένη. Φυσικά, και σε αυτή την περίπτωση, θα πρέπει να φροντίσουμε έτσι ώστε αν υπάρχει κάποιο firewall, που δεν παίζει το ρόλο VPN συσκευής, να μπορεί να περνάει μέσα από αυτό η κρυπτογραφημένη πληροφορία. Το σχήμα 3.6 δείχνει έναν τέτοιο τύπο VPN.



Σχήμα 3.6 VPN βασισμένο σε λογισμικό

3.2 ΣΥΓΚΡΙΤΙΚΟΣ ΠΙΝΑΚΑΣ ΤΩΝ ΑΡΧΙΤΕΚΤΟΝΙΚΩΝ VPN

	ΚΡΙΤΗΡΙΑ:	VPN ΥΠΟΣΤΗΡΙΖΟΜΕΝΟ ΑΠΟ ISP	VPN ΒΑΣΙΣΜΕΝΟ ΣΕ FIREWALL	VPN ΒΑΣΙΣΜΕΝΟ ΣΕ BLACK BOX	VPN ΒΑΣΙΣΜΕΝΟ ΣΕ ROUTER	VPN ΒΑΣΙΣΜΕΝΟ ΣΕ REMOTE ACCESS	VPN ΒΑΣΙΣΜΕΝΟ ΣΕ SOFTWARE
1	**ΕΠΙΠΕΔΟ ΑΣΦΑΛΕΙΑΣ**	α. υψηλό όταν την πολιτική ασφάλειας την δημιουργεί η επιχείρηση και έπειτα την εφαρμόζει ο ISP β. υψηλό όταν την πολιτική πρόσβασης την δημιουργεί η επιχείρηση γ.υψηλό όταν ο ISP εξασφαλίζει την υποστήριξη σε περίπτωση βλαβών	υψηλό αν το firewall έχει λειτουργικό σύστημα ασφαλές και περιέχει λογισμικό κρυπτογράφησης	χαμηλό αν ο server που συνεργάζεται με το black box είναι ευαίσθητος σε επιθέσεις	α. χαμηλό αν ο router έχει λογισμικό κρυπτογράφησης β.υψηλό αν χρησιμοποιείται κάρτα κρυπτογράφησης	εξαρτάται από την πολιτική ασφάλειας που εφαρμόζει ο remote access server (RAS)	πολύ υψηλό γιατί η πολιτική ασφάλειας διαμορφώνεται σύμφωνα με τις ανάγκες της επιχείρησης
2	**ΒΑΘΜΟΣ ΔΥΣΚΟΛΙΑΣ ΥΛΟΠΟΙΗΣΗΣ**	χαμηλός	μέτριος	μέτριος	Υψηλός	χαμηλός	υψηλός
3	**ΔΙΑΘΕΣΙΜΟΤΗΤΑ**	εξαρτάται από την διαθεσιμότητα του ISP	εξαρτάται από την υπολογιστική ισχύ του firewall και την ύπαρξη UPS	εξαρτάται από την υπολογιστική ισχύ του server που συνεργάζεται με το black box και την ύπαρξη UPS	εξαρτάται από την υπολογιστική ισχύ του router και την ύπαρξη UPS	εξαρτάται από τον RAS	εξαρτάται από τις παραμέτρους/ περιορισμούς που έχει ορίσει η επιχείρηση
4	**ΕΠΙΒΑΡΥΝΣΗ ΦΟΡΤΙΟΥ**	εξαρτάται από τις υπηρεσίες VPN που προσφέρει ο ISP	εξαρτάται από το λογισμικό κρυπτογράφησης του firewall	εξαρτάται από την υπολογιστκή ισχύ του server που συνεργάζεται με το black box και το λογισμικό που χρησιμοποιείται για την δημιουργία του tunnel	α. χαμηλή αν χρησιμοποέιται κάρτα κρυπτογράφησης β.εξαρτάται από το λογισμικό του router	εξαρτάται από την υπολογιστική ισχύ του RAS	εξαρτάται από τη μέθοδο κρυπτογράφησης που υιοθετείται
5	**ΧΡΟΝΟΣ ΕΛΕΓΧΟΥ ΠΙΣΤΟΠΟΙΗΣΗΣ ΧΡΗΣΤΗ**	α. μικρός όταν η βάση δεδομένων βρίσκεται στον ISP β. μεγάλος όταν η βάση δεδομένων βρίσκεται στην εταιρεία	μικρός	μικρός	μικρός	μικρός	μεγάλος
6	**ΑΞΙΟΠΙΣΤΙΑ**	εξαρτάται από τις δυνατότητες του ISP	υψηλή	μέτρια	υψηλή	μέτρια	χαμηλή
7	**ΒΑΘΜΟΣ ΠΡΟΣΑΡΜΟΓΗΣ ΣΤΙΣ ΑΝΑΓΚΕΣ ΤΗΣ ΕΠΙΧΕΙΡΗΣΗΣ**	χαμηλός (αποτελεί έτοιμη λύση)	χαμηλός (αποτελεί έτοιμη λύση)	μέτριος	χαμηλός (αποτελεί έτοιμη λύση)	χαμηλός (αποτελεί έτοιμη λύση)	υψηλός
8	**ΥΠΑΡΞΗ ΕΞΕΙΔΙΚΕΥΜΕΝΟΥ ΠΡΟΣΩΠΙΚΟΥ**	προτείνεται	όχι απαραίτητη	προτείνεται	απαιτείται	όχι απαραίτητη	απαραίτητη
9	**ΔΙΑΔΕΔΟΜΕΝΗ ΑΡΧΙΤΕΚΤΟΝΙΚΗ**	αρκετά διαδεδομένη	πολύ διαδεδομένη	λίγο διαδεδομένη	λίγο διαδεδομένη	αρκετά διαδεδομένη	ελάχιστα διαδεδομένη

3.3 ΒΑΣΙΚΕΣ ΤΟΠΟΛΟΓΙΕΣ VPN

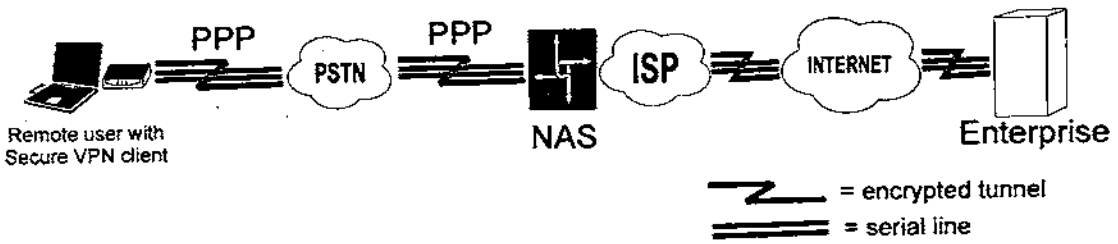
Εδώ θα ασχοληθούμε με τις διάφορες τοπολογίες των Εικονικών Ιδιωτικών Δικτύων. Οι πιο βασικές από αυτές είναι: Remote Access VPN, Intranet VPN, Extranet VPN και Intracompany VPN. Τα VPNs της τελευταίας κατηγορίας δεν είναι ακόμα πολύ διαδεδομένα.

3.3.1 Remote Access VPN

Ένα VPN αυτής της κατηγορίας εξυπηρετεί remote χρήστες. Συγκεκριμένα, παρέχει τη δυνατότητα σύνδεσης αυτού του τύπου χρηστών με τα κεντρικά γραφεία της εταιρείας μέσω ενός tunnel κρυπτογράφησης δεδομένων. Η δημιουργία αυτού, μπορεί να γίνει με ειδικό λογισμικό εγκατεστημένο στον εξοπλισμό του χρήστη. Στην άλλη άκρη του tunnel υπάρχει μια οντότητα που αποτελεί είσοδο στο ιδιωτικό δίκτυο της εταιρείας, που μπορεί να είναι και αυτό ένα VPN.

Τα remote access VPNs χωρίζονται σε δύο κατηγορίες: στα client-initiated και στα network access server (NAS)-initiated.

- **Client initiated:** Στην περίπτωση αυτή, οι απομακρυσμένοι χρήστες χρησιμοποιούν client εφαρμογές για να δημιουργήσουν κρυπτογραφημένα IP tunnels, μέσω του δικτύου ενός ISP, προς το δίκτυο κάποιας εταιρείας. Το πλεονέκτημα των client-initiated VPNs έναντι των NAS-initiated είναι ότι χρησιμοποιούν κρυπτογραφημένο tunneling για τη σύνδεση μεταξύ της client εφαρμογής και του ISP μέσω του δημόσιου τηλεφωνικού δικτύου (PSTN).

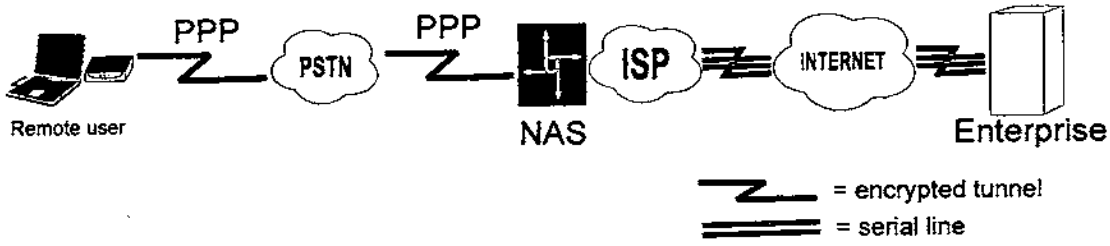


Σχήμα 3.7 Client – initiated remote access VPN

Στο σχήμα 3.7 φαίνεται ένα client-initiated remote access VPN. Η client εφαρμογή δημιουργεί μία PPP σύνδεση με το NAS του ISP και εν συνεχεία σχηματίζεται ένα κρυπτογραφημένο tunnel μέσω του δημόσιου τηλεφωνικού δικτύου.

- **NAS-initiated:** Στην περίπτωση αυτή, οι απομακρυσμένοι χρήστες κάνουν μία κλήση στο Network Access Server του ISP και αυτό δημιουργεί ένα κρυπτογραφημένο tunnel με το VPN της εταιρείας. Τα NAS-initiated VPNs δίνουν τη δυνατότητα στους χρήστες να συνδεθούν σε διάφορα δίκτυα, χρησιμοποιώντας πολλαπλά tunnels, ενώ η client εφαρμογή δεν χρειάζεται να έχει λογισμικό για τη

δημιουργία tunnels. Το αρνητικό στην περίπτωση αυτή, είναι ότι η σύνδεση μεταξύ του χρήστη και του ISP δεν είναι κρυπτογραφημένη και άρα στηρίζεται στο PSTN, το οποίο δυστυχώς δεν παρέχει καμία ασφάλεια. Το διάγραμμα ενός τέτοιου VPN φαίνεται στο σχήμα 3.8.

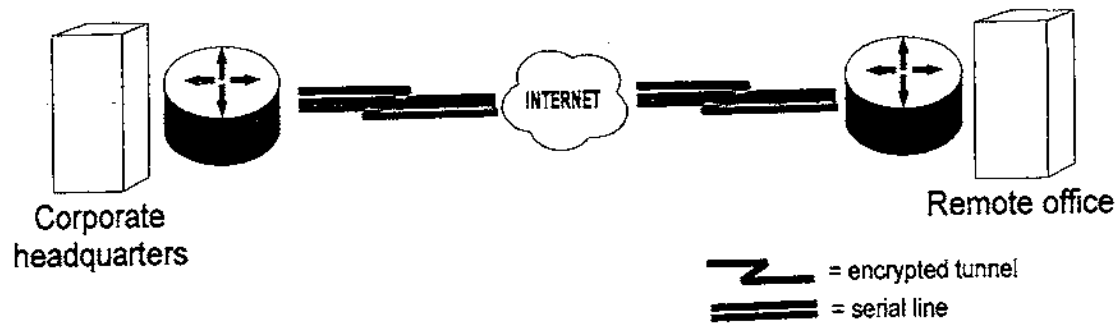


Σχήμα 3.8 NAS – initiated remote access VPN

3.3.2 Intranet VPN

Ένα intranet είναι ένα δίκτυο εργασίας, το οποίο είναι εσωτερικό σε κάποια εταιρεία. Παρέχει τις πιο πρόσφατες πληροφορίες και υπηρεσίες σε όλους τους υπαλλήλους της εταιρείας που συνδέονται σε αυτό. Τα Intranets προσφέρουν ένα κοινό, ανεξάρτητο περιβάλλον διεπαφής, το οποίο είναι λιγότερο ακριβό στην υλοποίηση από μία client/server εφαρμογή. Επιπλέον, τα Intranets αυξάνουν την παραγωγικότητα των υπαλλήλων, επιτρέποντας μία αξιόπιστη σύνδεση. Τα Intranet VPNs, επιτρέπουν την ίδια ασφάλεια και διασυνδεσιμότητα μεταξύ των κεντρικών γραφείων μιας εταιρείας και των απομακρυσμένων γραφείων.

Στο σχήμα 3.9 φαίνεται μία Intranet VPN τοπολογία.



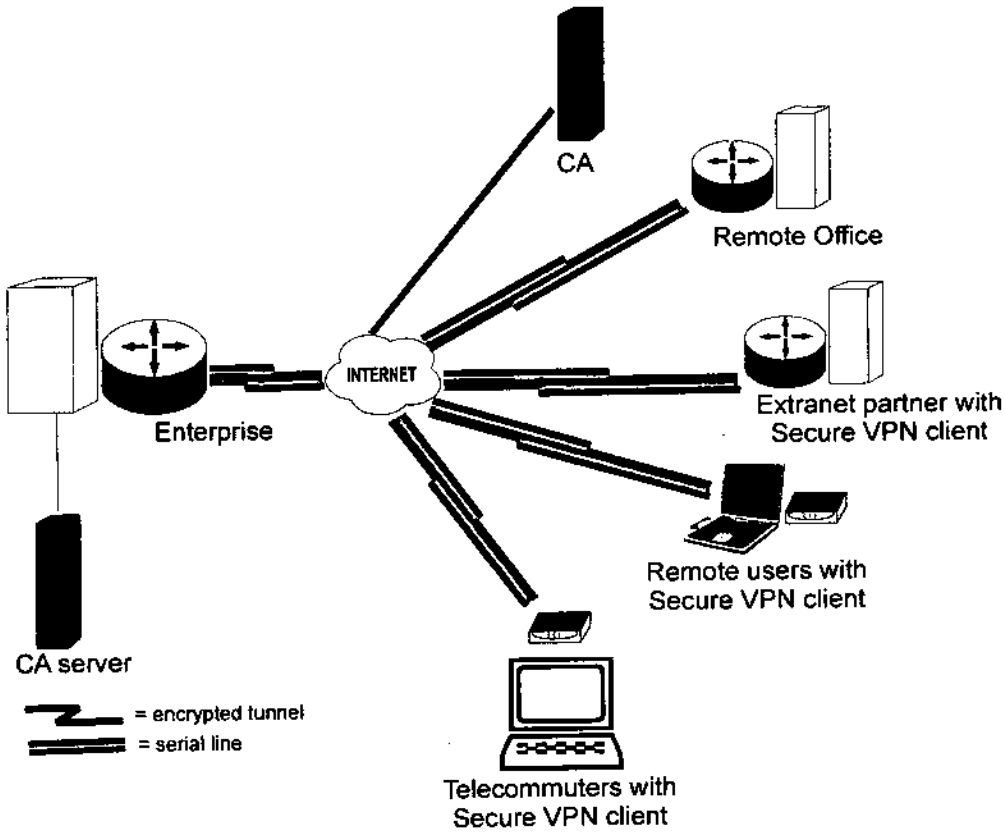
Σχήμα 3.9 Intranet VPN

3.3.3 Extranet VPN

Το extranet είναι ένα intranet το οποίο επιτρέπει και κάποια περιορισμένη πρόσβαση σε πελάτες, προμηθευτές και συνεργάτες της εταιρείας. Τα extranets διαφέρουν από τα intranets στο ότι επιτρέπουν πρόσβαση και σε χρήστες που δεν είναι υπάλληλοι της εταιρείας, είτε μέσω χρήσης του HTTP πρωτοκόλλου, είτε μέσω κάποιου πρωτοκόλλου στο οποίο θα συμφωνούν οι συμβαλλόμενοι στην επικοινωνία

φορείς. Το πεδίο στο οποίο θα εξαπλωθούν ευρέως τα VPNs αυτής της κατηγορίας είναι το ηλεκτρονικό εμπόριο στη γενική του μορφή, καθώς οι εταιρείες αποκτούν τη δυνατότητα ασφαλούς, γρήγορης και αποτελεσματικής εκτέλεσης συναλλαγών με τους εμπορικούς τους συνεργάτες. Επιτρέποντας μεγαλύτερη πρόσβαση στις πηγές τους, οι εταιρείες με extranet VPN βελτιώνουν την εικόνα τους στους πελάτες τους, μειώνοντας ταυτόχρονα τα έξοδά τους.

Στο σχήμα 3.10 φαίνεται μία extranet VPN τοπολογία. Χρησιμοποιώντας ψηφιακά πιστοποιητικά, οι clients δημιουργούν μέσω Internet, ασφαλή tunnels προς το δίκτυο μίας εταιρείας. Κάθε client λαμβάνει από την Αρχή Πιστοποίησης (Certificate Authority - CA) ένα ψηφιακό πιστοποιητικό, το οποίο χρησιμοποιείται για πιστοποίηση από τον server πιστοποίησης της εταιρείας.

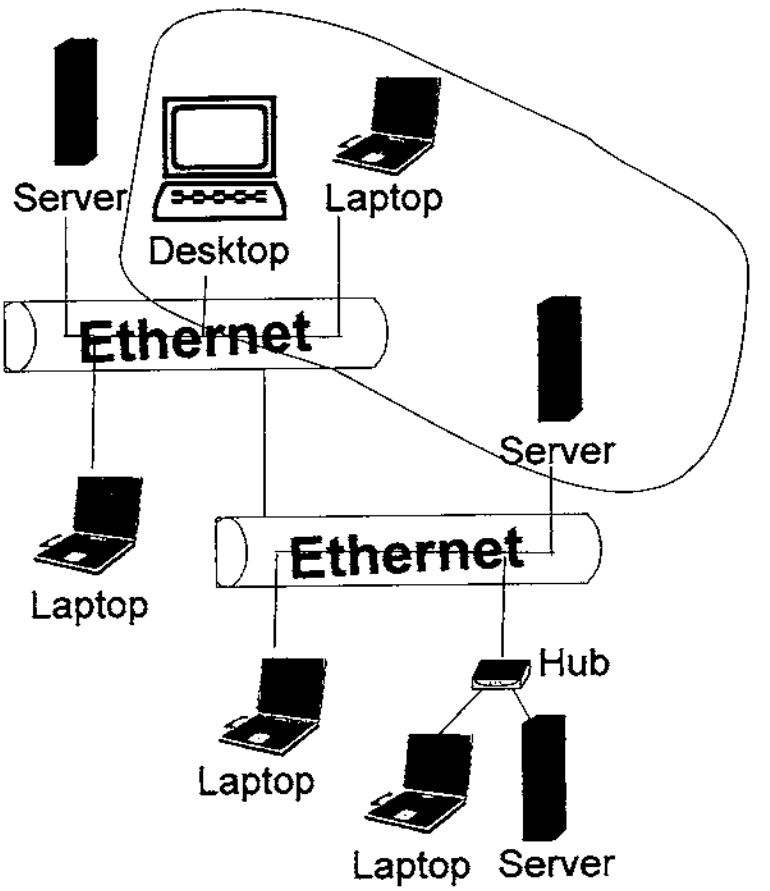


Σχήμα 3.10 Extranet VPN

3.3.4 Intracompany VPN

Η χρήση τέτοιων VPNs δεν έχει διαδοθεί ακόμη, αλλά υπάρχουν διάφοροι λόγοι που θα οδηγήσουν στην εξάπλωσή τους. Η βασική ιδέα της χρήσης τους, είναι η δημιουργία ενός VPN μέσα στο δίκτυο της εταιρείας, το οποίο μπορεί να είναι ένα VPN που θα προσφέρει προστασία σε πολύτιμους πόρους και πληροφορίες σημαντικής αξίας για την εταιρεία. Τέτοιες πληροφορίες μπορεί να είναι στοιχεία ερευνών πάνω σε νέα προϊόντα, οικονομικά στοιχεία, πολιτικές παραγωγής και προώθησης προϊόντων, κλπ. Βασική αιτία χρήσης τους, είναι το γεγονός ότι πολλές παραβιάσεις

στα δίκτυα εταιρειών γίνονται από τους ίδιους τους υπαλλήλους της, οι οποίοι έχουν αποκτήσει πρόσβαση σε μη εξουσιοδοτημένες περιοχές. Οι απώλειες από τέτοιου είδους επιθέσεις δικαιολογούν την υλοποίηση τέτοιων λύσεων. Το παρακάτω σχήμα δείχνει μια απλή περίπτωση εφαρμογής ενός Intracompany VPN, όπου ένας αριθμός συσκευών έχει συνδεθεί με τέτοιο τρόπο, ώστε να αποτελεί ένα εσωτερικό VPN. Όπως φαίνεται από το σχήμα 3.11, οι συσκευές του VPN μπορεί να μην ανήκουν στο ίδιο υποδίκτυο, πράγμα που αποτελεί χαρακτηριστικό της τεχνολογίας αυτής.



Σχήμα 3.11 Intracompany VPN

3.4 ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Πτυχιακή Εργασία: Ιδεατά Ιδιωτικά Δίκτυα
Καλλίγερος Εμμανουήλ
Μπέλλος Μάτσιεϊ
Νεάρχου Μιχάλης

2. ΔΙΕΥΘΥΝΣΕΙΣ ΣΤΟ INTERNET:
www.cisco.com

www.itpapers.com/abstract.aspx?scid=192&docid=58048

www.alliancedatacom.com/vpn-tutorial.htm

ΚΕΦΑΛΑΙΟ 4°

4.1 ΔΙΑΜΟΡΦΩΣΗ ΚΑΙ ΔΟΚΙΜΗ ΣΥΝΔΕΣΕΩΝ 2ου ΕΠΙΠΕΔΟΥ

Στο κεφάλαιο 2, κάναμε μια εισαγωγή στο Point-to-Point Tunneling Protocol, το οποίο μπορεί να χρησιμοποιηθεί για να δημιουργήσει μια ασφαλή σύνδεση μεταξύ των απομακρυσμένων χρηστών και ενός δικτύου. Το PPTP είναι πρώτιστα μια επέκταση των υπηρεσιών απομακρυσμένης πρόσβασης των Windows NT που βοηθά στη δημιουργία ενός VPN μεταξύ ενός χρήστη του Διαδικτύου και ενός δικτύου προορισμού χρησιμοποιώντας τον RAS Server ως πύλη. Το Routing (δρομολόγηση) της Microsoft και η προσθήκη απομακρυσμένης πρόσβασης σε Windows NT server επιτρέπουν τις LAN-to-LAN PPTP συνδέσεις. Αυτό το κεφάλαιο αναφέρεται στο εμπράγματο υλικό για κάποιον που θέλει να δημιουργήσει τις δικές του PPTP συνδέσεις. Η πρώτη διαδικασία είναι πώς θα διαμορφώσει κανείς PPTP στον NT server του. Απ' το να μπαίνουμε σε λεπτομέρειες για τη σύσταση RAS, θα υποθέσουμε ότι την έχετε ήδη κάνει, και θα αναλύσουμε μόνο τα σημεία όπου RAS και PPTP «εμπλέκονται». Όταν κάποιος διαμορφώνει έναν RAS, προσδιορίζει τον αριθμό των ports που θέλει να είναι διαθέσιμα για την πρόσβαση στο VPN. Αν και οι περισσότεροι εγκαθιστούν τους RAS servers τους μόνο για dial-in συνδέσεις, μπορούν επίσης να επιτρέψουν εξερχόμενες συνδέσεις PPTP από τον server.

Ο RAS σας αφήνει επίσης να προσδιορίσετε ποια πρωτόκολλα θα δρομολογήσει ο NT server για να συνδέσει τους χρήστες. Περιορίζοντας τα πρωτόκολλα μπορείτε κάπως να ελέγχετε σε ποιον server μπορούν να έχουν πρόσβαση οι χρήστες που συνδέονται. Παραδείγματος χάριν, αν επιτρέπονται μόνο IP αυτό θα αφήσει τους χρήστες να μπουν σε έναν TCP/IP email server, αλλά θα τους αποτρέψει από το να συνδεθούν σε έναν κοινόχρηστο Novell server χρησιμοποιώντας το IPX. Επιπλέον, εάν οι εσωτερικοί servers δε χρησιμοποιούν καθόλου την IP, μπορεί κάποιος να θέσει εκτός λειτουργίας την IP επιτρέποντας τα άλλα πρωτόκολλα. Παρακάτω στο "Επιλέγοντας τα πρωτόκολλα που ανοίγουν" θα δούμε που μπορεί κάποιος να τα εγκαταστήσει.

Ο RAS server υποστηρίζει επίσης το φιλτράρισμα PPTP, το οποίο σας αφήνει να περιορίσετε το ποιος μπορεί να συνδεθεί με τον προσαρμοστή LAN του συστήματος. Προκειμένου να συνδεθεί, ο χρήστης πρέπει να περάσει μέσω της πιστοποίησης ταυτότητας των NT. Στους πολυκατευθυνόμενους NT servers (κεντρικοί υπολογιστές με δύο προσαρμοστές δικτύων), μπορείτε να χρησιμοποιήσετε το φιλτράρισμα PPTP για να περιορίσετε την πρόσβαση, είτε στα τοπικά δίκτυα, είτε στο Διαδίκτυο. Χρησιμοποιούμενοι σε συνδυασμό με το φιλτράρισμα διευθύνσεων IP και τις σταθερές διευθύνσεις IP, μπορείτε να χρησιμοποιήσετε τον RAS server ως ισχυρό firewall. Εάν προτιμάτε την ευελιξία, τα NT υποστηρίζουν επίσης τη δυναμική ανάθεση διευθύνσεων IP μέσω του Πρωτόκολλου Διαμόρφωσης Δυναμικού Host (Dynamic

Host Configuration Protocol (DHCP)). Σ' αυτό το κεφάλαιο θα ερευνήσουμε πως να διαμορφώσουμε και τους τύπους φιλτραρίσματος και το DHCP.

Κάποιοι ISPs υποστηρίζουν PPTP στον εξοπλισμό πρόσβασής τους, ενώ άλλοι όχι. Σε αυτό το κεφάλαιο, θα σας δείξουμε πώς να χειριστείτε καθεμία δυνατότητα. Επίσης, θα σας δείξουμε πώς να εγκαταστήσετε δύο γνωστούς δρομολογητές για PPTP. Οι ISPs μπορούν να χρησιμοποιήσουν την υποστήριξη του PPTP για να κάνουν τη σύνδεση με το VPN ευκολότερη για τους πελάτες τους, ενώ οι διαχειριστές δικτύων μπορούν να τη χρησιμοποιήσουν για να «ξεφορτώσουν» κατά κάποιο τρόπο τους RAS servers τους από την επεξεργασία κλήσης.

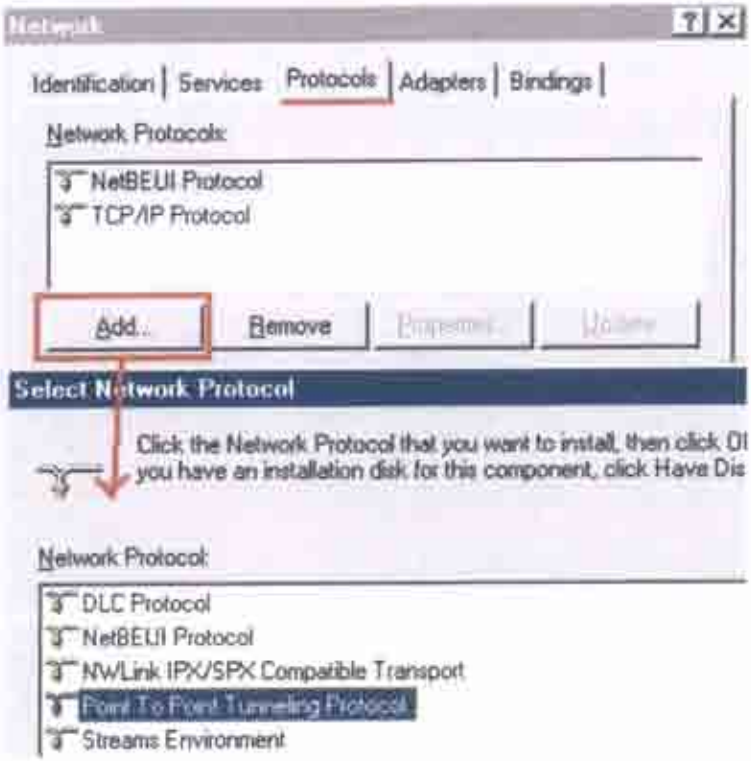
4.2 ΕΓΚΑΘΙΣΤΩΝΤΑΣ ΚΑΙ ΔΙΑΜΟΡΦΩΝΟΝΤΑΣ PPTP ΣΕ ΕΝΑΝ WINDOWS NT RAS SERVER

Η εγκατάσταση και η διαμόρφωση PPTP σε Windows NT 4.0 είναι τόσο απλή όσο το να εγκαθιστάς οποιοδήποτε άλλο «συστατικό» σε Windows NT. Υπάρχουν τρία βασικά βήματα: η εγκατάσταση του πρωτοκόλλου, η εγκατάσταση του RAS, και η διαμόρφωση των χρηστών για dial-up πρόσβαση.

4.2.1 Εγκαθιστώντας το PPTP

Το πρωτόκολλο PPTP δεν εγκαθίσταται αυτόματα σε έναν Windows NT 4.0 server. Εξαρτάται από τον διαχειριστή αν θα το προσθέσει στον κατάλογο πρωτοκόλλων του δικτύου, που είναι ενεργά στο σύστημα και θα χρειαστείτε το CD-ROM των NT 4.0 ή την ιεραρχία εγκαταστάσεων NT (π.χ., "\I386 " για τους επεξεργαστές της Intel). Τα βήματα για την εγκατάσταση του πρωτοκόλλου PPTP είναι απλά:

- Κάτω από το μενού έναρξης στη μπάρα ελέγχου, επιλέγετε Settings και μετά Control Panel.
- Όταν εμφανιστούν οι επιλογές του Control Panel κάνετε διπλό κλικ στο εικονίδιο του δικτύου (Network).
- Όταν «μπείτε» στο Network ανοίγετε την επιλογή Protocols.
- Στον κατάλογο των πρωτοκόλλων δικτύου θα δείτε τα πρωτόκολλα που εγκαταστάθηκαν πρόσφατα στο σύστημά σας. Κάντε κλικ στο κουμπί Add που βρίσκεται κάτω κάτω στη λίστα.
- Θα εμφανιστεί ένα κουτί διαλόγου για την επιλογή πρωτοκόλλου δικτύου (Select Network Protocol), παρουσιάζοντας έναν κατάλογο διαθέσιμων πρωτοκόλλων. Κυλήστε προς τα κάτω τη μπάρα μέχρι να δείτε το Point to Point Tunneling Protocol. Επιλέξτε το και πατήστε OK.(Εικόνα 4.1)



Εικόνα 4.1

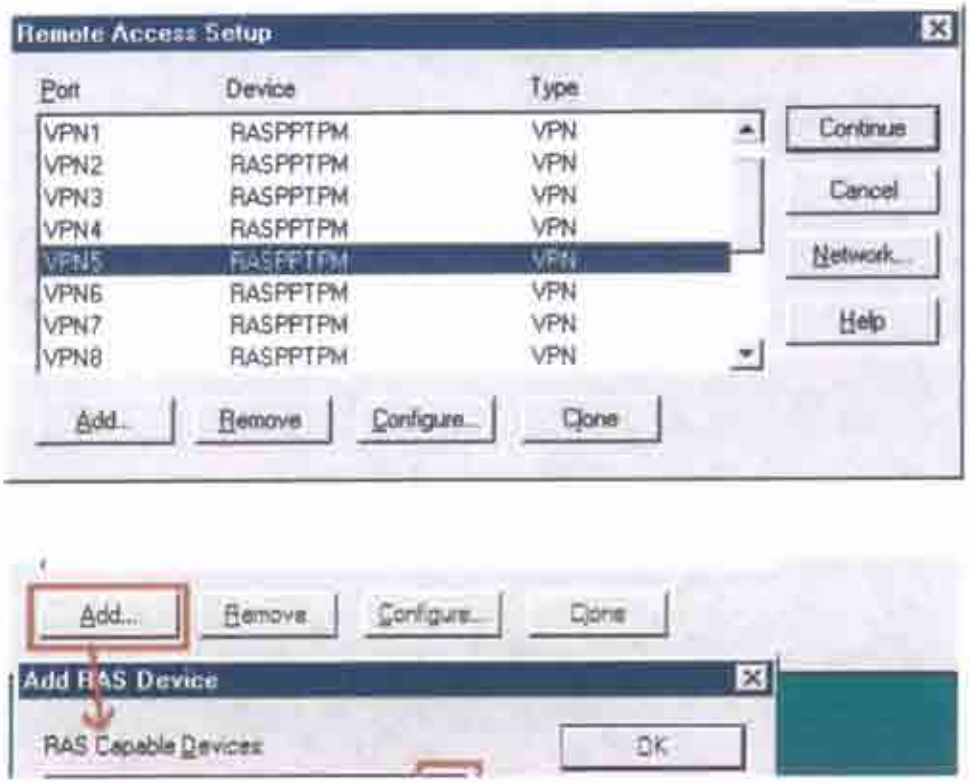
Θα εμφανιστεί ένα άλλο κουτί διαλόγου με την ονομασία PPTP Configuration (Διαμόρφωση PPTP) (Εικόνα 4.2). Εδώ πρέπει να επιλέξετε τον αριθμό των εικονικών ιδιωτικών δικτύων που θέλετε να υποστηρίξετε (δηλ., τον αριθμό των ταυτόχρονων συνδέσεων PPTP που επιτρέπονται στον RAS). Αυτός είναι ένας πολύ καλός τρόπος να προφυλάξετε τον Server από το να «κολλήσει» από τους πολλούς χρήστες. Η έκταση των επιλογών είναι από 1 ως 256. Για παράδειγμα, θα επιλέξουμε 2 και θα πατήσουμε OK. Το πρόγραμμα εγκαταστάσεων θα ψάξει έπειτα στο CD-ROM των NT 4.0 για τα απαιτούμενα αρχεία, ή θα σας ρωτήσει για τη θέση εκείνων των αρχείων.

Εικόνα 4.2

4.2.2 Εγκαθιστώντας έναν RAS

Αφότου εγκατασταθεί το PPTP, η διαδικασία συνεχίζει αυτόματα με τη διαμόρφωση του RAS. Θα λάβετε ένα μήνυμα εγκατάστασης (setup) που θα δηλώνει την έναρξη εγκατάστασης του RAS. Πατήστε OK σε αυτό το μήνυμα για να συνεχίσετε. Τα βήματα που εγκαθιστούν έναν RAS για εικονική ιδιωτική δικτύωση είναι τα εξής:

1. Θα εμφανιστεί το εικονίδιο Remote Access Setup (εγκατάσταση απομακρυσμένης πρόσβασης) (Εικόνα 4.3) και θα σας δώσει μια λίστα των υπαρχόντων ports του RAS και των συσκευών. Εάν έχετε ήδη διαμορφώσει ένα modem για RAS, θα εμφανιστεί σε αυτό το εικονίδιο. Για να διαμορφώσετε τον RAS έτσι ώστε να χρησιμοποιεί τις συσκευές PPTP, πατήστε το κουμπί Add.



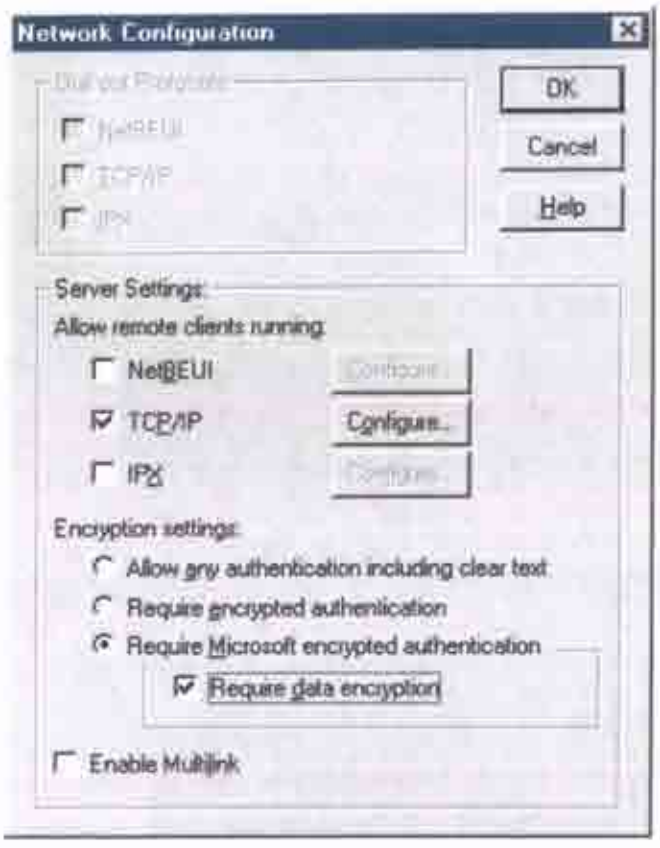
Εικόνα 4.3

2. Τότε θα εμφανιστεί το παράθυρο για την προσθήκη της συσκευής του RAS. Χρησιμοποιήστε τον κατάλογο για να επιλέξετε μια συσκευή ικανή για RAS. Εκτός από τα ports του συστήματός σας, πρέπει να δείτε έναν κατάλογο συσκευών VPN που βρίσκεται κάτω από τον τίτλο Ports.
3. Κάθε συσκευή θα αριθμηθεί από 1 έως το μέγιστο αριθμό VPN ports που διαμορφώσατε (ορίσατε) κατά την εγκατάσταση του πρωτοκόλλου PPTP. Στην περίπτωσή μας, θα δούμε μια συσκευή για κάθε έναν από τα δύο ports που διαμορφώσαμε. Ενώ ο RAS περιέλαβε αυτόματα τα ports που του ορίσαμε, μας επιτρέπει να επιλέξουμε από τη λίστα μόνο ένα κάθε φορά. Μόλις επιλέξετε το port που θέλετε να προστεθεί, πατήστε το OK. Θα πρέπει έπειτα να πατήσετε πάλι το Add στο Remote Access Setup για να ξαναρχίσετε τη διαδικασία.
4. Τα νέα VPN ports διαμορφώνονται μόνο για dial-in συνδέσεις. Εάν επιθυμείτε να εγκαταστήσετε τα ports και για dial-out (όπως θα δούμε παρακάτω στο "διαμόρφωση PPTP για Dial-up δικτύωση σε έναν χρήστη Windows NT"), πατήστε το κουμπί Configure στο Remote Access Setup.
5. Επίσης, από το μενού του Remote Access Setup, μπορείτε να πατήσετε το κουμπί Network που σας στέλνει στη «Διαμόρφωση Δικτύου» (Network

Configuration) για ένα επιλεγμένο VPN port. Θα συζητήσουμε τις επιλογές που παρουσιάζει σε επόμενες παραγράφους. Όπως θα δείτε, αφού δεν υπάρχει κανένας τρόπος να «πιέσουμε» έναν συγκεκριμένο χρήστη να συνδεθεί με ένα συγκεκριμένο VPN port, μπορείτε να θέσετε όλους τους χρήστες στην ίδια κατηγορία. Οι πεπειραμένοι διαχειριστές RAS θα αναγνωρίσουν αυτό το «κουτί διαλόγου» ως σχεδόν ίδιο με αυτό που χρησιμοποιείται για να διαμορφώσει μια κανονική dial-up σύνδεση RAS.

4.2.3 Επιλέγοντας τα πρωτόκολλα για tunnel (που ανοίγουν)

Από το Network Configuration, ένα από τα πράγματα που είστε σε θέση να επιλέξετε είναι ποια πρωτόκολλα θα επιτρέπονται για ένα συγκεκριμένο VPN port (Εικόνα 4.4).



Εικόνα 4.4

Οι επιλογές είναι IP, IPX και NetBEUI. Για το παράδειγμά μας, διαλέγουμε το IP έτσι ώστε να μπορεί κάποιος να μπει στον server του ηλεκτρονικού ταχυδρομείου του Διαδικτύου και διαλέγουμε το NetBEUI, έτσι ώστε να μπορεί να συνδεθεί με το κοινόχρηστο desktop της συσκευής, αλλά θέτουμε εκτός λειτουργίας το αχρησιμοποίητο πρωτόκολλο IPX.

Από το ίδιο «παράθυρο διαλόγου» μπορείτε επίσης να περιορίσετε το χρήστη στον RAS server, και να μη του δοθεί πρόσβαση σε ολόκληρο το δίκτυο. Για το σενάριό μας, ο χρήστης θα έχει πρόσβαση σε ολόκληρο το δίκτυο. Δε συστήνουμε την περιορισμένη πρόσβαση για διάφορους λόγους:

- Καταρχήν, δεν είναι ενδιαφέρον. Ένα από τα συναρπαστικά πράγματα των VPNs είναι ότι δίνουν στους χρήστες ασφαλή απομακρυσμένη πρόσβαση σαν να συνδέθηκαν άμεσα με το (τοπικό δίκτυο) LAN. Ο περιορισμός τους στον RAS server σημαίνει ότι περιορίζετε αυτά που τους επιτρέπονται να κάνουν στο δίκτυο, στις υπηρεσίες που εκτελεί ο RAS server.
- Εάν περιορίζετε την απομακρυσμένη πρόσβαση χρηστών στον RAS, αυτό πιθανώς σημαίνει ότι "τρέχετε" άλλες υπηρεσίες στον RAS server, όπως ηλεκτρονικό ταχυδρομείο ή εκτυπώσεις, ή ότι χρησιμοποιείτε τον RAS server ως server εφαρμογών. Αν έχετε παραπάνω από τέσσερις χρήστες στο δίκτυό σας, δε συστήνουμε να χρησιμοποιείτε τον RAS server για τίποτα άλλο παρά ως RAS. Διαφορετικά, μπορεί να «κολλήσει» με το να ενεργεί και ως δρομολογητής (router) και ως server.
- Ένας PPTP RAS server, από τη φύση του, χρειάζεται να είναι, τουλάχιστον μερικώς, προσιτός από το Διαδίκτυο. Κατά συνέπεια, θα είναι επίσης «ανοικτός» σε επιθέσεις από το ίδιο το Διαδίκτυο. Εάν ασχολείστε με πολύ σημαντικές εφαρμογές προς ή από τον RAS server και αυτός είναι ευάλωτος σε τέτοιου είδους επιθέσεις, το αίτημά σας (η εφαρμογή σας) θα αποτύχει.

4.2.4 Επιλέγοντας τη μέθοδο πιστοποίησης της ταυτότητας σας

Στο κεφάλαιο 2, είδαμε τις μεθόδους πιστοποίησης που είναι διαθέσιμες στον RAS: πιστοποίηση ταυτότητας με κρυπτογράφηση (CHAP), πιστοποίηση ταυτότητας με την Microsoft-Challenge Handshake κρυπτογράφηση (MS-CHAP), και Password Authentication Protocol (PAP). Μπορείτε είτε να απαιτήσετε το CHAP, είτε το MS-CHAP, είτε να επιτρέψετε και τις δύο μεθόδους κρυπτογράφησης συν την PAP. Την επιλογή αυτή μπορείτε να την κάνετε στο παράθυρο διαλόγου «Διαμόρφωση Δικτύου» (Network Configuration).

Εάν είναι διαθέσιμο σε όλους τους χρήστες σας (π.χ., εάν είναι όλοι χρήστες Windows ή χρησιμοποιείτε TunnelBuilder στο Macs σας), σας προτείνουμε να χρησιμοποιήσετε το MS-CHAP. Χρησιμοποιώντας το, θα μπορείτε να «ανοίξετε» την κρυπτογράφηση στοιχείων, έτσι ώστε η σύνδεση PPTP να είναι απόλυτα ασφαλής. Η χρήση άλλων μεθόδων είναι βεβαίως πιθανή εάν δεν έχετε χρήστες ικανούς για MS-CHAP, αλλά διατρέχετε τον κίνδυνο να σταλούν μη κρυπτογραφημένα δεδομένα και μη κρυπτογραφημένοι κωδικοί πρόσβασης (στην περίπτωση του PAP) μέσω του Διαδικτύου.

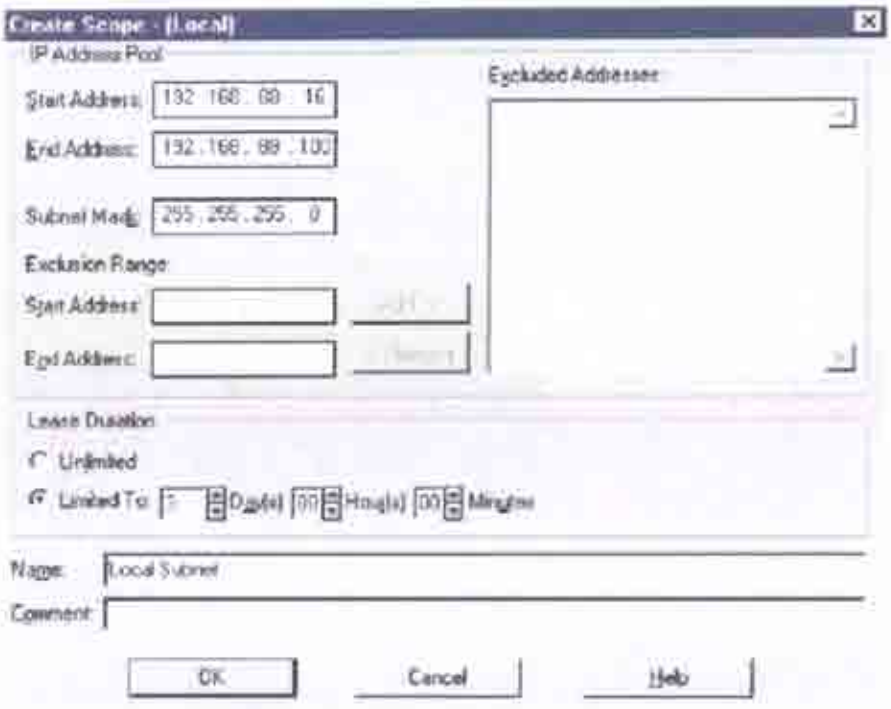
4.2.5 Η διαπραγμάτευση διευθύνσεων IP χρησιμοποιώντας το DHCP

Το DHCP είναι ένας ιδανικός τρόπος να διαμορφωθούν οι εισερχόμενοι χρήστες PPTP με μια δυναμική διεύθυνση IP. Τα Windows NT 4.0 διαθέτουν μια υπηρεσία DHCP server που πρέπει να εγκατασταθεί μέσω του Network Control Panel.

Ακολουθήστε τις οδηγίες για την εγκατάσταση RAS, αλλά εγκαταστήστε την υπηρεσία DHCP server της Microsoft. Μόλις εγκατασταθεί η υπηρεσία, θα εγκατασταθεί επίσης ένα πρόγραμμα διαχείρισης DHCP (DHCP Manager program) κάτω από το μενού έναρξης στα εργαλεία διαχείρισης (Administrative Tools).

Για να διαμορφώσετε το DHCP ακολουθήστε αυτά τα βήματα:

- Αφού πατήσετε Start → Programs→ Administrative Tools ανοίξτε το DCHP Manager.
- Κάτω από τη στήλη DHCP servers, επιλέξτε το "Local Machine". Κατόπιν πηγαίνετε στο μενού Scope (σκοπός) και επιλέξτε Create (δημιουργία).
- Θα εμφανιστεί το παράθυρο διαλόγου «Create Scope» (Εικόνα 4.5). Εισάγετε τη διεύθυνση έναρξης και τη διεύθυνση τέλους για τις εργασίες σας.



Εικόνα 4.5

- Εισάγετε τη μάσκα υποδικτύου (Subnet Mask) για τη σειρά.
- Σε αυτό το σημείο, θα αφήσουμε τις διευθύνσεις σειράς αποκλεισμού κενές. Δεν θέλουμε να αποκλείσουμε οποιεσδήποτε διευθύνσεις από αυτήν την σειρά.
- Θα δώσετε στο σκοπό το όνομα: "Dial-Up Address Range" και θα πατήσετε OK. Όταν το παράθυρο διαλόγου σάς ρωτά εάν θέλετε να ενεργοποιήσετε το πεδίο, πατήστε «Ναι».

4.3 PPTP FILTERING

Για να εγκαταστήσετε το φιλτράρισμα PPTP, ανοίγετε το Network Control Panel, κάνετε κλικ στο κουμπί Protocols και διαλέγετε το TCP/IP, έπειτα πατάτε την επιλογή Properties. Τελικά, πατάτε την επιλογή Advanced στο παράθυρο διαλόγου της

εγκατάστασης του TCP/IP. Στο κάτω κάτω σημείο του παράθυρου διαλόγου του Advanced IP Addressing βρίσκεται η επιλογή Enable PPTP Filtering.

4.3.1 Η εξερχόμενη πιστοποίηση ταυτότητας που χρησιμοποιεί φιλτράρισμα PPTP

Σε πολλαπλούς hosts το PPTP filtering μπορεί επίσης να χρησιμοποιηθεί ως τύπος εξερχόμενου firewall. Οι χρήστες του εσωτερικού δικτύου μπορούν να καλέσουν τον PPTP server όπως θα έκαναν μέσω μιας PPP σύνδεσης, χρησιμοποιώντας την IP διεύθυνση του RAS server ως τηλεφωνικό αριθμό. Θα αναγκάζονταν έπειτα να πιστοποιηθούν στον RAS server προκειμένου να έχουν πρόσβαση στο Διαδίκτυο χρησιμοποιώντας τις δυνατότητες δρομολόγησης του server. Αυτό επιτρέπει σε έναν διαχειριστή δικτύων να περιορίσει την πρόσβαση στο Διαδίκτυο, να ελέγξει ποιοι έχουν πρόσβαση στο Διαδίκτυο και για πόσο, και να περιορίσει τον αριθμό των ταυτόχρονων συνδέσεων στο Διαδίκτυο.

4.3.2 Προειδοποιήσεις φιλτραρίσματος

Η ενεργοποίηση του φιλτραρίσματος PPTP στο σύστημα των Windows NT 4.0 με μια μόνο κάρτα δικτύου μπορεί να κάνει άλλες υπηρεσίες του δικτύου NT που «τρέχετε» (όπως η υπηρεσία DHCP server και η υπηρεσία FTP server) απρόσιτες σε χρήστες που δε χρησιμοποιούν PPTP. Ο προσαρμοστής (adapter) θα ζητήσει πιστοποίηση ταυτότητας PPTP σε οποιοδήποτε «αίτημα» παίρνει. Υπάρχει ένας τρόπος που επιτρέπει στα πακέτα να φθάσουν στον RAS server, χωρίς να διοχετεύονται στο υπόλοιπο δίκτυο. Πρέπει να εγκαταστήσετε τα Windows NT 4.0 Service Pack 3, ή πιο πρόσφατη έκδοση και να προσθέσετε μια ξεχωριστή είσοδο στο Windows NT Registry.

Τρέξτε το Registry Editor επιλέγοντας την επιλογή Run κάτω από το μενού έναρξης και βάλτε REGEDIT.EXE στο πεδίο όνομα αρχείου. Η παράμετρος που προσθέτει είναι κάτω από το ακόλουθο Registry πλήκτρο:

HKEY_LOCAL_MACHINE\SYSTEM\Services\RASPPTPE\Parameters\Configuration

Προσθέστε μια νέα είσοδο Registry με τον τύπο στοιχείων REG_DWORD. Ονομάστε την είσοδο - Allow-PacketsForLocalMachine και δώστε της την τιμή 1, κατόπιν εισάγετε τις αλλαγές και κλείστε τον Registry Editor. Θα πρέπει να κάνετε επανεκκίνηση για να εφαρμοστούν οι αλλαγές.

Παρ' όλα αυτά, δε συνιστούμε να «τρέχετε» υπηρεσίες που μπορούν να προκαλέσουν παραβιάσεις ασφάλειας (ανώνυμο FTP) ή να αναστατώσουν τις εργασίες του εσωτερικού δικτύου σας (DHCP) στον RAS server σας.

4.3.3 Φιλτράρισμα μέσω IP διεύθυνσης

Ένας άλλος τύπος ασφάλειας σάς επιτρέπει να προσδιορίσετε τις διευθύνσεις IP από τις οποίες ο RAS server θα επιτρέπει συνδέσεις PPTP. Προκειμένου να

εφαρμοστεί αυτό, θα πρέπει οι απομακρυσμένοι χρήστες σας να έχουν καθορίσει τις διευθύνσεις IP που ανατίθενται από τους ISPs τους, και θα πρέπει να ξέρετε αυτές τις διευθύνσεις.

Χρησιμοποιούμενο σε συνδυασμό με το φιλτράρισμα PPTP, αυτό μπορεί να καταστήσει τον RAS server ασφαλή και από τις "πλαστές" συνδέσεις και από τις συνδέσεις από αναρμόδιους hosts. Δυστυχώς, αυτό δεν μπορεί να γίνει απλά από ένα παράθυρο διαλόγου, έτσι πρέπει να επιστρέψετε στο Registry των Windows NT 4.0.

Τρέξτε τον Registry Editor ξανά και ακολουθήστε το ακόλουθο Registry key:

HKEY_LOCAL_MACHINE\SYSTEM\Services\RASPPTPE\Parameters\Configuration

Κάτω από αυτό το πλήκτρο, θα χρειαστεί να δημιουργήσετε μια νέα είσοδο για δεδομένα τύπου REG_DWORD. Η νέα είσοδος θα ονομάζεται "AuthenticateIncomingCalls". Κάντε το να δέχεται δεκαδικά ψηφία και δώστε του την τιμή 1. Κάτω από το ίδιο πλήκτρο, δημιουργήστε μια νέα είσοδο για δεδομένα τύπου REG_MULTI_SZ. Δώστε σε αυτήν την είσοδο το όνομα "PeerClientIPAddresses". Εδώ θα θελήσετε να εισάγετε τις έγκυρες IP διευθύνσεις των hosts που θέλετε να είναι σε θέση να συνδεθούν με τον RAS server χρησιμοποιώντας PPTP.

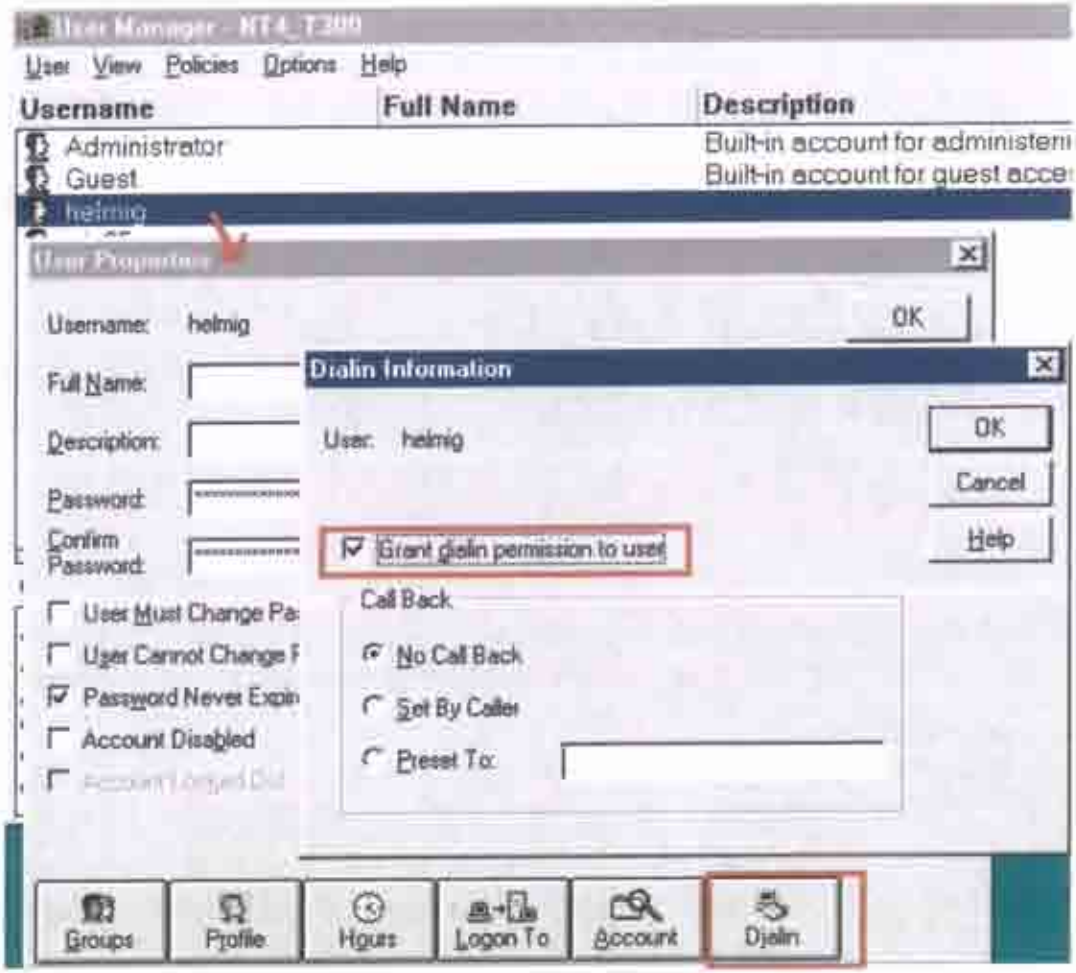
4.4 ΔΙΑΜΟΡΦΩΝΟΝΤΑΣ ΧΡΗΣΤΕΣ ΓΙΑ DIAL-UP ΠΡΟΣΒΑΣΗ

Ένας dial-up χρήστης υποστηριζόμενος από τον Windows NT RAS ουσιαστικά εγκαθίσταται με τον ίδιο τρόπο που εγκαθίσταται ένας κανονικός χρήστης των Windows NT:

☞ Χρησιμοποιήστε το User Manager για Domains, που βρίσκεται κάτω από το μενού Administrative Tools, για να προσθέσετε ή να τροποποιήσετε τον χρήστη.

☞ Όταν διαμορφώσετε τις Ιδιότητες Χρήστη, πατήστε το κουμπί Dialin στην κάτω κάτω δεξιά πλευρά του παράθυρου διαλόγου.

☞ Θα εμφανιστεί το παράθυρο διαλόγου του Dialin Information (Εικόνα 4.6). Για έναν χρήστη PPTP, επιλέξτε το "Grant dial-in permission to user" και από το Call Back το No Call Back.



Εικόνα 4.6

☞ Πατήστε OK για να βγείτε από το παράθυρο διαλόγου του Dial-in Information και του User Properties.

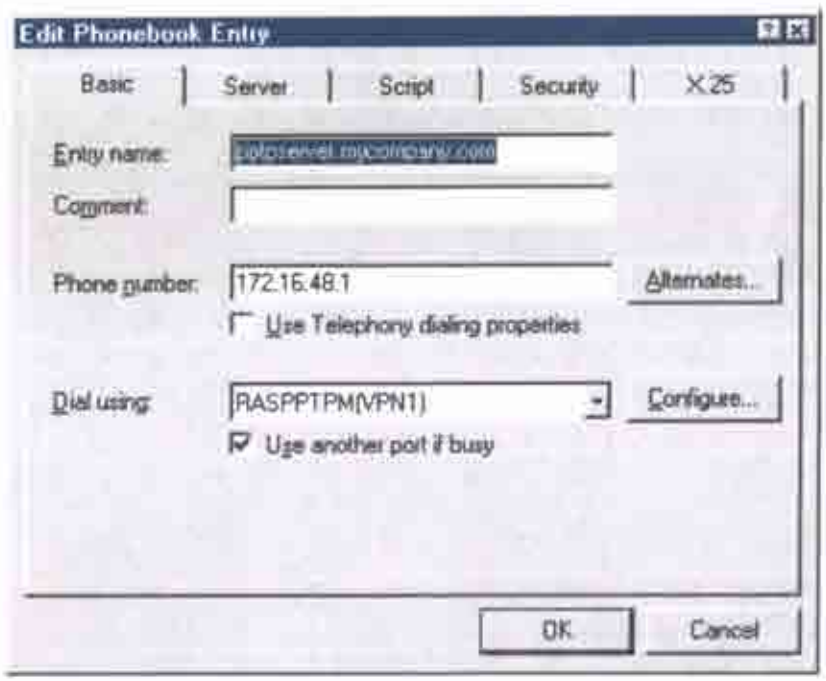
4.5 ΔΙΑΜΟΡΦΩΝΟΝΤΑΣ PPTP ΓΙΑ DIAL-UP ΔΙΚΤΥΩΣΕΙΣ ΣΕ ΕΝΑΝ WINDOWS NT ΧΡΗΣΤΗ

Για να συνδεθείτε με έναν ISP που υποστηρίζει PPTP χρησιμοποιώντας έναν Windows NT Client, απλά διαμορφώνετε το dial-up networking όπως θα κάνατε κανονικά - απλά εγκαθιστάτε επιπλέον δυνατότητες πιστοποίησης ταυτότητας και κρυπτογράφησης. Σε αυτήν την παράγραφο, θα εστιάσουμε στην εγκατάσταση ενός NT χρήστη για να χρησιμοποιήσει το πρωτόκολλο PPTP όταν συνδέεται με έναν provider που δεν το υποστηρίζει.

Παρακάτω δίνουμε τα βήματα για την εγκατάσταση μιας σύνδεσης PPTP. Υποθέτουμε ότι έχετε ήδη διαμορφώσει μια σύνδεση Dial up για να καλέσετε τον ISP και να εγκαταστήσετε μια σύνδεση PPP.

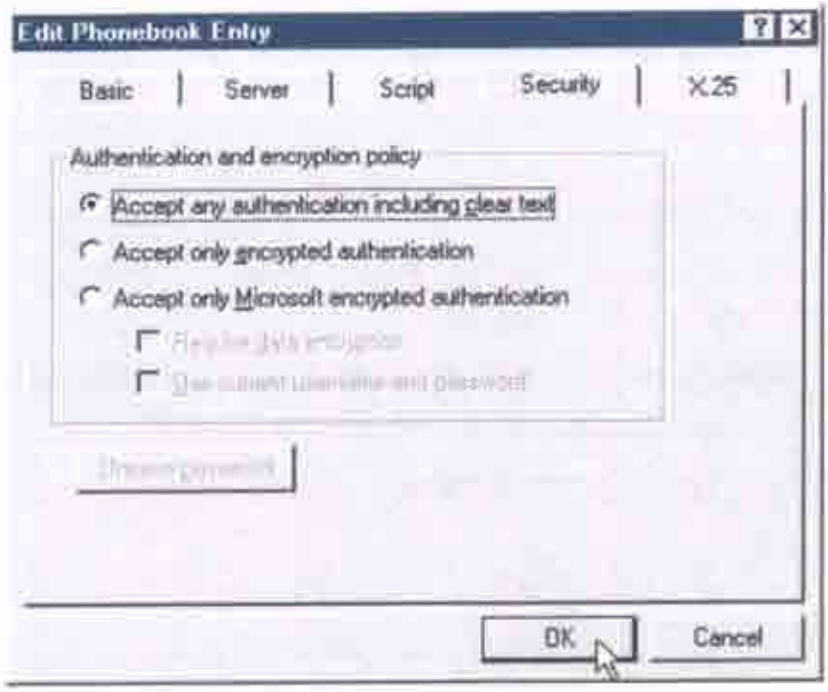
1. Εγκαθιστάτε το πρωτόκολλο PPTP με τον ίδιο τρόπο που το εγκαταστήσατε για τον RAS server με τα βήματα 1 έως 6 στην παράγραφο που αναφεράταν στην εγκατάσταση του PPTP.

2. Η διαμόρφωση του RAS είναι επίσης παρόμοια με τον τρόπο που έγινε στην παράγραφο εγκατάστασης του RAS. Αυτή τη φορά, στο τρίτο βήμα πατήστε το κουμπί Configure (διαμόρφωση) στο παράθυρο διαλόγου "remote access setup". Από εκεί επιλέγετε το dial out, δεδομένου ότι θέλετε να ήσαστε σε θέση να dial out παρά να dial in.
3. Από το μενού Start→ programs → accessories, επιλέξτε το dial up networking. Όταν εμφανιστεί το παράθυρο διαλόγου του dial up networking, κάντε κλικ στο κουμπί new και εισάγετε το όνομα που θέλετε να καλείται τη VPN σύνδεσή σας στο παράθυρο διαλόγου του Phonebook entry. Στην περίπτωση μας θα χρησιμοποιήσουμε το "pptpserver.mycompany.com". Στο πεδίο τηλεφωνικού αριθμού, εισάγετε τη διεύθυνση IP του PPTP RAS server με τον οποίο συνδέεστε. Για το παράδειγμά μας, είναι 172.16.48.1.. Στο πεδίο dial using, επιλέξτε ένα από τα VPN ports που δημιουργήσατε εγκαθιστώντας το PPTP και τον RAS. Θα έχουν το όνομα RASPPTPPM (VPNn), όπου το n είναι ο αριθμός των ports (Εικόνα 4.7).



Εικόνα 4.7

4. Μπορείτε επίσης να προσδιορίσετε ποια μέθοδο πιστοποίησης ταυτότητας θα απαιτείτε, και εάν πρέπει ή όχι να απαιτηθεί κρυπτογράφηση δεδομένων από το χρήστη. Από το ίδιο παράθυρο διαλόγου edit phonebook entry, κάνετε κλικ στην επιλογή security και θα δείτε τις ίδιες επιλογές ασφάλειας που είχατε στον server (Εικόνα 4.8). Για το ασφαλέστερο VPN, επιλέξτε να αποδέχεστε μόνο την κρυπτογραφημένη πιστοποίηση της Microsoft και «τσεκάρετε» την επιλογή "require data encryption". Είτε συνδεθείτε με έναν ISP που υποστηρίζει το PPTP, είτε όχι, θα θέλετε να χρησιμοποιήσετε το MS-CHAP και κρυπτογράφηση εάν την επιτρέπει ο χρήστης σας.



Εικόνα 4.8
(Εδώ είναι επιλεγμένη η επιλογή οποιασδήποτε πιστοποίησης)

4.6 ΔΙΑΜΟΡΦΩΝΟΝΤΑΣ PPTP ΓΙΑ DIAL UP NETWORKING ΣΕ ΕΝΑ ΧΡΗΣΤΗ ΤΩΝ WINDOWS 95 Ή 98.

Όπως έχουμε πει, τα Windows 95 δεν έχουν πάντα εγκατεστημένο το PPTP. Για να το χρησιμοποιήσετε, θα πρέπει να λάβετε το dial up networking update 1.3 από το website της Microsoft. Δεδομένου ότι οι αναπροσαρμογές και τα πακέτα υπηρεσιών αλλάζουν κατά διαστήματα, πρέπει να ελέγξετε το website της Microsoft για να δείτε ποιο επίπεδο λογισμικού μπορεί να χρειαστείτε. Η εγκατάσταση του dial up networking (DUN) update είναι πολύ απλή. Δεν υπάρχουν παράμετροι που πρέπει να εισαχθούν και η Microsoft περιλαμβάνει ένα χρήσιμο έγγραφο με οδηγίες. Εξ αιτίας αυτού, δεν πρόκειται να δώσουμε βήμα προς βήμα τις οδηγίες εγκατάστασης. Όπως έχουμε πει επίσης, τα Windows 98 περιέχουν τις δυνατότητες πρόσβασης VPN σαν αναπόσπαστο μέρος του λειτουργικού συστήματος.

Για να διαμορφώσετε το PPTP για τα Windows 95 ή 98, πρέπει να διαμορφώσετε δύο dial up networking profiles: ένα για τη σύνδεση με τον ISP και ένα για τη σύνδεση με τον PPTP server. Επειδή πολλοί είναι εξοικειωμένοι με τη διαμόρφωση DUN για να συνδεθούν με τον ISP τους, θα προσπεράσουμε εκείνο το βήμα. Εάν δεν το έχετε κάνει ποτέ πριν, μπορείτε να βρείτε τις πληροφορίες για το πώς να εγκαταστήσετε μία DUN entry στο έγγραφο της Microsoft που συμπεριλαμβάνεται στο DUN update.

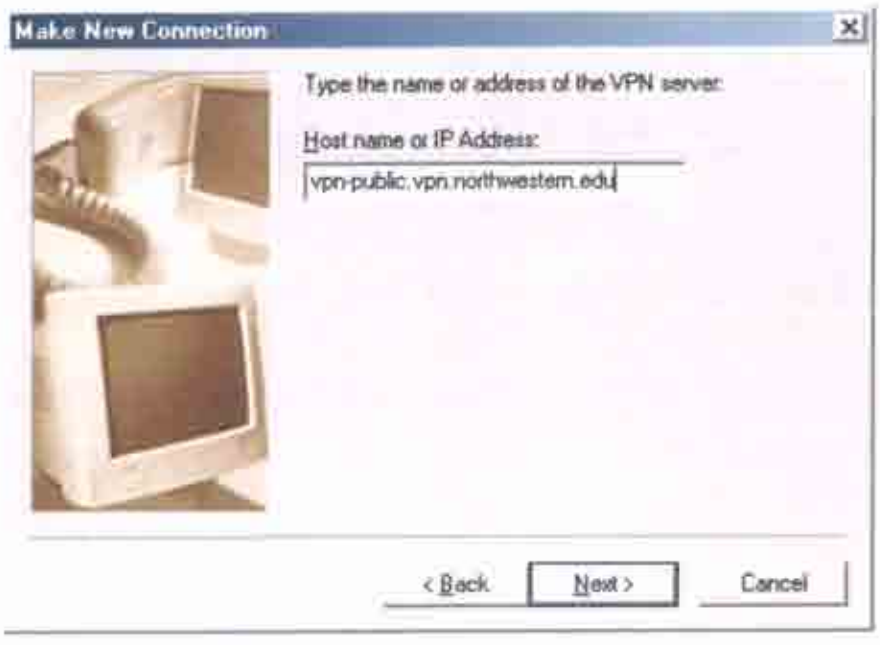
Προκειμένου να εγκαταστήσετε το VPN DUN profile σας, ακολουθήστε αυτά τα βήματα:

1. Πηγαίνετε στο μενού έναρξης, και επιλέξτε programs → accessories → dial up networking.

2. Όταν εμφανιστεί το παράθυρο του Dial-up Networking, πατήστε το make new connection.
3. Θα εμφανιστεί ο οδηγός "Make New Connection wizard". Ονομάστε πως θέλετε να ονομάζεται η σύνδεσή σας στο πεδίο "name of the computer you are dialing". Θα ονομάσουμε το δικό μας "NU VPN" (Εικόνα 4.9). Στο πεδίο select a device διαλέξτε την επιλογή Microsoft VPN adapter.

Εικόνα 4.9

4. Έπειτα θα δείτε ένα παράθυρο διαλόγου το οποίο θα σας ζητάει να πληκτρολογήσετε σε ποιο host name ή IP address του VPN server επιθυμείτε να συνδεθείτε. (Εικόνα 4.10).



Εικόνα 4.10

5. Κάντε κλικ στο Next και μετά στο Finish. Θα εμφανιστεί ένα εικονίδιο του profile σύνδεσής σας στο παράθυρο διαλόγου του Dial Up Networking.
6. Επιλέξτε αυτό το εικονίδιο και κάντε δεξί κλικ σε αυτό. Επιλέξτε τις ιδιότητες (properties) απ' το πτυσσόμενο μενού. Το παράθυρο διαλόγου που θα εμφανιστεί θα δείχνει τις πληροφορίες που εισαγάγατε νωρίτερα για τη VPN σύνδεσή σας. Κάντε κλικ στην επιλογή server types.
7. Στο παράθυρο διαλόγου του Server Type κάτω από τις επιλογές "Advanced" (για προχωρημένους) επιλέξτε το "Log On to Network" εάν το δίκτυο με το οποίο συνδέεστε το απαιτεί, όπως στα Windows NT ή στο δίκτυο Novell NetWare. Μπορεί να είναι τσεκαρισμένη η επιλογή "Enable Software Compression". Η επιλογή "Require encrypted password" δε χρειάζεται να είναι τσεκαρισμένη και τερματίστε το παράθυρο διαλόγου.
8. Κάτω από την επιλογή "Allowed Network Protocols" (επιτρεπόμενα πρωτόκολλα δικτύου) επιλέξτε το πρωτόκολλο που θα χρησιμοποιείτε. Εάν είναι απαραίτητο κάντε κλικ στην επιλογή TCP/IP Settings έτσι ώστε να εισάγετε μια σταθερή διεύθυνση IP, μια Gateway Address και έναν DNS server. Κάντε κλικ στο OK για να σώσετε τις αλλαγές σας.

4.7 ΠΡΑΓΜΑΤΟΠΟΙΩΝΤΑΣ ΚΛΗΣΕΙΣ

Όταν καλείτε έναν ISP που υποστηρίζει ένα PPTP, όλη η "δουλειά" του VPN έχει γίνει για σας από τον ISP. Πρέπει απλά να διαμορφώσετε το χρήστη σας σαν να καλείτε απευθείας τον RAS server σας. Το switch του ISP θα μεταβιβάσει όλες τις πληροφορίες αυθεντικοποίησης σε αυτόν τον RAS server.

Όταν καλείτε έναν ISP που δεν υποστηρίζει PPTP θα πρέπει να κάνετε μια PPP κλήση στον ISP χρησιμοποιώντας το παράθυρο διαλόγου Dial Up Networking. Μόλις συνδεθείτε, αφήστε την PPP ενεργοποιημένη, επιλέξτε το PPTP Entry που είχατε φτιάξει, και κάντε κλικ στην επιλογή Dial. Αυτό θα ξεκινήσει μια κλήση PPTP στον RAS server που συνεργάζεται με την PPP Internet σύνδεσή σας.

4.8 ΠΡΟΒΛΗΜΑΤΑ ΑΝΙΧΝΕΥΣΗΣ ΛΑΘΩΝ

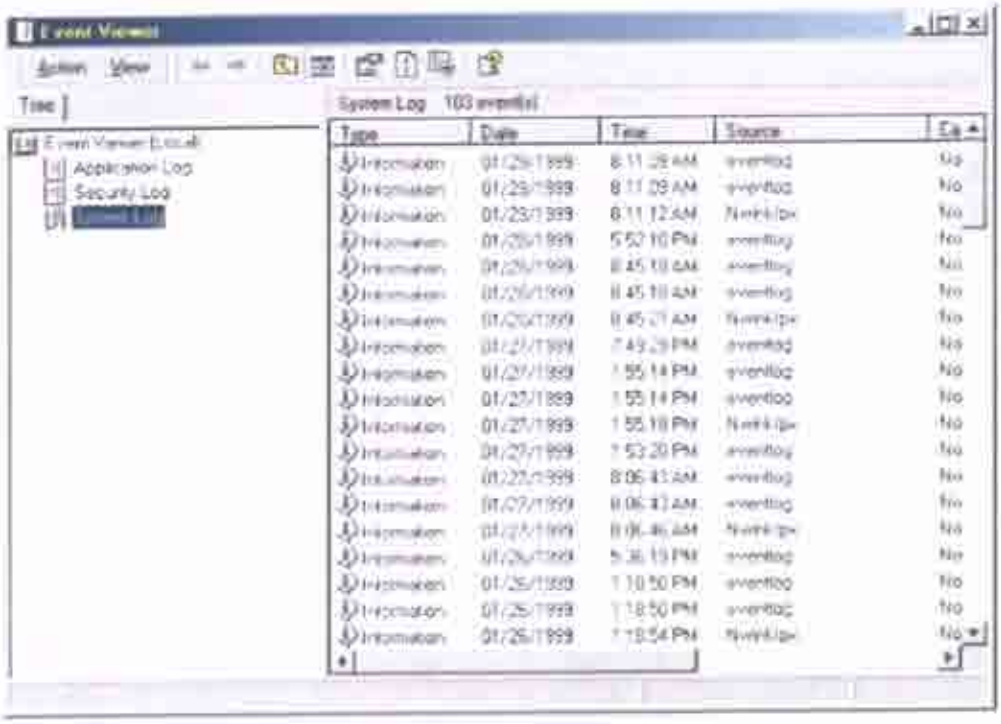
Τι θα κάνετε αν το σύστημά σας δε συνδέεται; Το πρόβλημα είναι ο ISP του απομακρυσμένου χρήστη σας, ο δικός σας ISP, το Internet από μόνο του ή η διαμόρφωση του RAS server; Εξαιτίας όλων των συμβαλλόμενων παραγόντων, τα προβλήματα με τις VPN συνδέσεις είναι δύσκολο να ανιχνευθούν.

4.8.1 Τα προβλήματα άδειας εισόδου

Για τους χρήστες που συνδέονται με RAS server, το πιο κοινό πρόβλημα σύνδεσης είναι να δουλεύουν με modem. Σε αυτή την περίπτωση η ανίχνευση λαθών μπορεί να γίνει από την πλευρά των χρηστών. Τα προβλήματα πιστοποίησης ταυτότητας (λάθος όνομα χρήστη ή λάθος κωδικοί πρόσβασης ή ανακριβής τύποι πιστοποίησης ταυτότητας) απαιτούν κάποιον που θα παρακολουθεί τις εισόδους και τις προσπάθειες σύνδεσης που έχουν προορισμό τον RAS server. Τα Windows NT Event Viewer και Dial-up Networking Monitor σας βοηθούν να απομονώσετε τέτοια προβλήματα άδειας εισόδου.

4.8.2 Event Viewer

Το Event Viewer είναι το κοινό σύστημα άδειας εισόδου σε όλα τα Windows NT. Μπορεί να βρεθεί από το μενού start→ programs → Administrative tools. Υποθέστε ότι έχετε πρόβλημα να συνδεθείτε και δεν γνωρίζετε ακριβώς ποιο είναι το πρόβλημα. Ανοίγετε το event viewer και κοιτάτε στη λίστα πηγών μήπως υπάρχουν μηνύματα απομακρυσμένης πρόσβασης που εμφανίστηκαν τη στιγμή που προσπαθούσατε να συνδεθείτε. Στην αριστερή στήλη, υπάρχουν εικονίδια που ξεχωρίζουν τα ενημερωτικά μηνύματα (ένα μπλε "i"), από τα μηνύματα προειδοποίησης (ένα κίτρινο θαυμαστικό) και από τα μηνύματα σφάλματος (ένα κόκκινο STOP). Βλέπετε ένα μήνυμα κόκκινου STOP στην πηγή απομακρυσμένης πρόσβασης τη στιγμή που εσείς προσπαθούσατε να συνδεθείτε. Κάνοντας ένα διπλό κλικ πάνω του θα εμφανιστεί ένα μήνυμα για το που ακριβώς βρίσκεται το λάθος. Το σφάλμα (για παράδειγμα) φαίνεται να προέρχεται από ένα πρόβλημα διαπραγμάτευσης DHCP. Το επόμενο λογικό βήμα για να είστε σίγουροι είναι να αποκτήσετε μια IP διεύθυνση χρησιμοποιώντας DHCP και να επιβεβαιώσετε ότι ο DHCP server σας είναι κατάλληλα διαμορφωμένος. Το Event Viewer είναι επίσης χρήσιμο στο να διατηρεί χρήσιμες πληροφορίες σχετικά με επιτυχή logins, συμπεριλαμβανομένου του username, του POP number, της ώρας σύνδεσης, της ταχύτητας σύνδεσης και των bytes που στάλθηκαν και ελήφθησαν. Η εικόνα 4.11 δείχνει πληροφορίες μιας επιτυχημένης σύνδεσης από τον Event Viewer.



Εικόνα 4.11

4.8.3 Το Dial Up Networking Monitor

Το Dial Up Networking Monitor βρίσκεται στο μενού Start→Programs→Administrative tools. Μπορεί να χρησιμοποιηθεί για να παρακολουθεί την κατάσταση της τηλεφωνικής σύνδεσης. Εκτός από την παρακολούθηση προβλημάτων πιστοποίησης, μπορείτε επίσης να δείτε αν κάποιο πακέτο στέλνεται ή λαμβάνεται και να κοιτάξετε μήπως υπάρχουν κάποια σφάλματα σύνδεσης. (Η εικόνα 4.12 δείχνει τις πληροφορίες που παρουσιάζονται).

Εικόνα 4.12

4.9 ΕΛΕΓΧΟΣ ΣΥΝΔΕΣΙΜΟΤΗΤΑΣ

Εάν ο χρήστης PPTP έχει πρόβλημα να συνδεθεί, ένα από τα πρώτα πράγματα που πρέπει να ελεγχθεί είναι η συνδεσιμότητα. Αυτό περιλαμβάνει την PPP συνδεσιμότητα μεταξύ του χρήστη και του ISP σας, και μεταξύ του dial-up ISP σας και του ISP με τον οποίο συνδέεται ο RAS server. Σημειώστε ότι ο έλεγχος συνδεσιμότητας θα έχει αποτέλεσμα μόνο για συνδέσεις όπου καλείτε έναν ISP που δεν υποστηρίζει PPTP. Αυτό συμβαίνει γιατί στις περιπτώσεις που καλείτε έναν παροχέα που υποστηρίζει PPTP, δεν είστε πραγματικά «συνδεδεμένος» μέχρι να πιστοποιηθεί η ταυτότητά σας από τον RAS server. Εάν πιστοποιηθεί η ταυτότητά σας, δεν υπάρχει κανένα πρόβλημα συνδεσιμότητας.

4.9.1 Ping and Traceroute

Ο καλύτερος τρόπος για να ελέγξετε τη συνδεσιμότητα είναι να "τρέξετε" την εφαρμογή ping από το Start → Run menu. Αφού συνδεθείτε με τον ISP, μπορείτε να προσπαθήσετε να ελέγξετε τον RAS server με την ακόλουθη εντολή:

"PING IP address of RAS server"

Στην περίπτωσή μας, θα προσπαθήσουμε να ελέγξουμε τη συνδεσιμότητα της διεύθυνσης 2.1.1.60. Εάν η απάντηση είναι θετική, δεν έχετε πρόβλημα συνδεσιμότητας. Εάν η απάντηση δεν είναι θετική, πρέπει να προσπαθήσετε να ελέγξετε κάτι άλλο στο Διαδίκτυο για το οποίο ξέρετε τη διεύθυνση IP ή το hostname - μια άριστη δοκιμή θα ήταν οι DNS servers του ISP σας. Εάν μπορείτε να το ελέγξετε αυτό, από την άλλη πλευρά της σύνδεσής σας, αλλά δεν μπορείτε να ελέγξετε τον RAS server σας, τότε υπάρχει ένα από τα εξής προβλήματα:

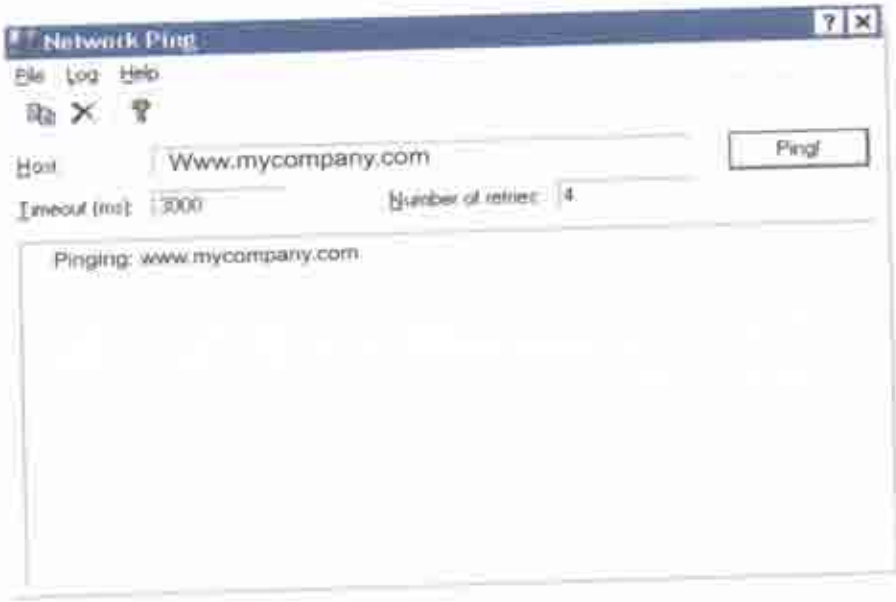
☑ Έχετε αποσυνδεθεί. Μερικές φορές ένα modem μπορεί να σας αποσυνδέσει, αλλά το Dial-Up Networking να σας αναφέρει ότι είστε ακόμα συνδεδεμένοι.

☑ Η PPP σύνδεσή σας έχει διαμορφωθεί λάθος. Ελέγξτε τις πληροφορίες για το PPP και το TCP/IP που σας δίνονται από τον ISP σας. Στην περίπτωση που έχετε μια σταθερή διεύθυνση IP, η διεύθυνση IP και η πύλη σας πρέπει να οριστούν από τον PPP server του ISP σας. Επίσης, σιγουρευτείτε ότι έχετε τους σωστούς DNS servers του ISP σας σε λίστα.

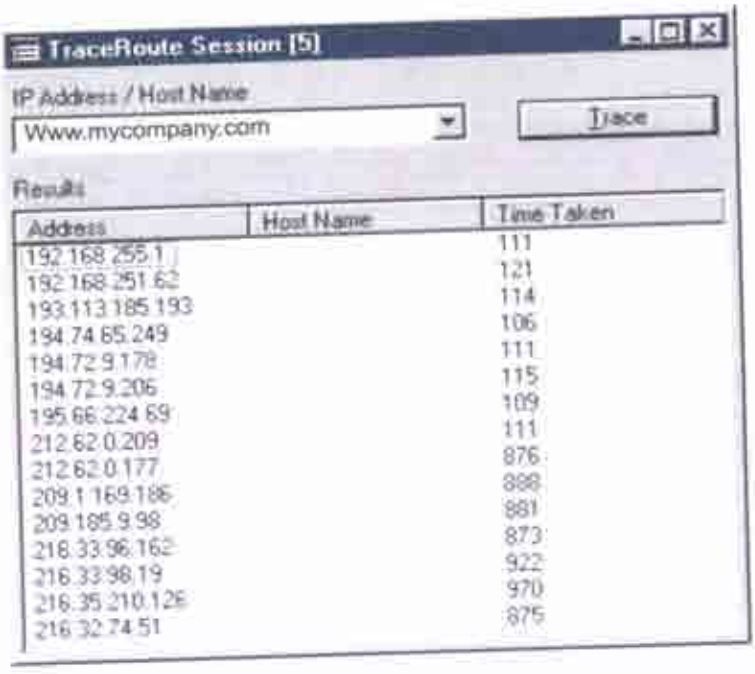
☑ Συνάθροιση (συμφόρηση) ή βασικά προβλήματα δρομολόγησης στο Διαδίκτυο σας αποτρέπουν από την επίτευξη του εταιρικού δικτύου. Μια καλή δοκιμή θα ήταν να προσπαθήσετε να ελέγξετε τη συνδεσιμότητα της διεύθυνσης IP του δρομολογητή πυλών του ISP σας. Εάν μπορείτε να φθάσετε σε αυτό μέσω του Διαδικτύου, τότε μπορείτε πιθανώς να υποθέσετε ότι ο RAS server έχει διαμορφωθεί λάθος ή δε συνδέεται.

Ένα άλλο καλό εργαλείο για τον έλεγχο της συνδεσιμότητας είναι το Traceroute. Το Traceroute είναι οικείο στους χρήστες Unix ως πρόγραμμα traceroute, που ανιχνεύει το μονοπάτι των πακέτων που στέλνονται από τον αρχικό host στον host προορισμού, καταγράφοντας τους "hops" (άλλους δρομολογητές πυλών) κατά μήκος της "διαδρομής". Στα Windows 95/98 και στα συστήματα των Windows NT, το Traceroute ονομάζεται TRACERT. Το μόνο πρόβλημα που μπορεί να έχετε με τη χρήση του Traceroute είναι ότι στέλνει πακέτα UDP σε ένα μη έγκυρο port, και μερικοί ISPs ή επιχειρήσεις δε δέχονται τα εισερχόμενα πακέτα UDP για λόγους ασφάλειας.

Στις παρακάτω εικόνες (Εικόνες 4.13, 4.14) φαίνονται δύο παραδείγματα των παράθυρων διαλόγων του ping και του traceroute.



Εικόνα 4.12



Εικόνα 4.14

4.10 ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Virtual Private Networks
Second Edition
Charlie Scott, Paul Wolfe and Mike Erwin

2.ΔΙΕΥΘΥΝΣΕΙΣ ΣΤΟ INTERNET:
www.microsoft.com/traincert/mcp

http://howto.lycos.com

www.oucs.ox.ac.uk/network/vpn/microsoft/winnt/index.xml.ID=Installation-de

www.hotspotvpn.com/inwinnt.asp?mm=3

www.cuhk.edu.hk/itsc/network/vpn/winnt/setting.html

www.helpdesk.princeton.edu/remote/VPN/vpn_nt.htm

www.microsoft.com/library/en-us/dnras/html/instpptp.asp

www.twpm.com/internet/downloads/cyberkit.htm

www.oclc.org/oclc/man/10061tcp/tcpchap5.htm

www.wright.edu/cats/docs/docroom/ppp/winntppp.html

www.microsoft.com/mind/0497/sitebuild/sitebuilding2.asp

www.wown.com/j_helmig/vpnrasvc.htm

ΚΕΦΑΛΑΙΟ 5°

5.1 ΔΙΑΧΕΙΡΙΣΗ ΚΑΙ ΣΥΝΤΗΡΗΣΗ ΕΝΟΣ VPN

Τώρα το VPN σας είναι έτοιμο και οι απομακρυσμένοι χρήστες και τα sites είναι συνδεδεμένα με αυτό μέσω του διαδικτύου. Τώρα αρχίζει η προσπάθεια για να κρατήσετε το VPN σας αναβαθμισμένο και να ελέγχετε την ασφάλειά του, επιπλέον από εδώ και πέρα πρέπει να ασχοληθείτε και με προβλήματα όπως, χρήστες που τηλεφωνούν για να παραπονεθούν ότι δεν μπορούν να συνδεθούν. Μερικά από αυτά τα προβλήματα μπορούν να λυθούν με τη χρήση ενός ISP που θα διαχειρίζεται το VPN σας για εσάς. Ακόμα κι αν επιλέξετε αυτή τη λύση, η γνώση του τι μπορεί να πάει στραβά είναι ουσιαστική και χρήσιμη. Γι' αυτό θα μιλήσουμε σ' αυτό το κεφάλαιο.

Αντίθετα από ένα firewall ή έναν proxy server, όπου μπορείτε να τον εγκαταστήσετε μια φορά και να μην τον αγγίξετε για μήνες, το VPN σας είναι ένας δυναμικότερος μηχανισμός ασφάλειας. Ο βασικός λόγος για αυτό είναι ότι οι χρήστες σπάνια συνειδητοποιούν ότι αλληλεπιδρούν με ένα firewall ή έναν proxy server, ενώ αυτό δε συμβαίνει όταν συνδέονται με έναν VPN server. Χρήστες με διάφορους τύπους εξοπλισμού μπορούν να έχουν πρόσβαση στο VPN σας από οποιοδήποτε σημείο στο Διαδίκτυο, οποιαδήποτε ώρα ή ημέρα. Οποιοσδήποτε έχει "τρέξει" έναν server απομακρυσμένης πρόσβασης ξέρει τα διάφορα προβλήματα που μπορεί να έχουν οι χρήστες που συνδέονται.

Σε αυτό το κεφάλαιο, θα δούμε τα προβλήματα που μπορεί να εμφανιστούν και θα ψάξουμε τις πιθανές λύσεις, καθώς επίσης θα φτιάξουμε και κατάλογο με το τι θα πρέπει να εξοπλιστείτε όταν δουλεύετε με ISP σε ζητήματα που αφορούν το VPN.

Παρόλο που σε αυτό το κεφάλαιο δεν μπορούμε να εξετάσουμε τις λεπτομέρειες του δικτύου σας, μπορούμε να σας δώσουμε μερικές γενικές προτάσεις ασφάλειας. Είναι σημαντικό να αναφερθεί ότι κανένα επίπεδο πιστοποίησης ταυτότητας ή κρυπτογράφησης δεν μπορεί να σας προστατεύσει εάν δεν έχετε μια "υγιή" πολιτική ασφάλειας. Αυτό το αναλύσαμε εν συντομία στο κεφάλαιο 1, «Γιατί να κατασκευάσετε ένα εικονικό ιδιωτικό δίκτυο», και στο κεφάλαιο 2, «Βασικές τεχνολογίες VPN».

Τελικά, θα διαπιστώσετε ότι οι πιο πρόσφατες τάσεις, πρότυπα και μορφές ασφαλείας στις τεχνολογίες VPN, θα σας εξασφαλίσουν ένα ενημερωμένο VPN.

5.2 ΕΠΙΛΕΓΟΝΤΑΣ ΕΝΑΝ ISP

Η επιλογή ενός σωστού ISP για τη σύνδεση του VPN σας είναι ίσως ένα από τα σημαντικότερα πράγματα που έχετε να κάνετε εάν επιλέξετε αυτήν την αρχιτεκτονική. Για να παρέχετε την πιο αξιόπιστη σύνδεση που ενδεχομένως μπορείτε, πρέπει να χρησιμοποιήσετε τον ίδιο ISP για κάθε σύνδεση του VPN. Το πρώτο πράγμα που πρέπει να λάβετε υπ' όψιν είναι η γεωγραφία. Θα θελήσετε να επιλέξετε έναν ISP που έχει σημεία παρουσίας σε όλες τις θέσεις που χρειάζεστε. Αν

και οι τοπικοί και περιφερειακοί ISPs μπορεί να είναι τέλειοι για συνδέσεις μέσα στην ίδια πόλη ή ακόμα και στο ίδιο κράτος, εάν χρειάζεστε συνδεσιμότητα σε ολόκληρη τη χώρα πρέπει να επιλέξετε έναν μεγαλύτερο, εθνικό παροχέα (provider).

Κάτι άλλο που πρέπει να λάβετε υπ' όψιν για ένα αξιόπιστο VPN είναι η εγγύηση της ποιότητας των υπηρεσιών (QoS – Quality of Service). Αυτή είναι μια συμφωνία μεταξύ ενός πελάτη και ενός ISP που εγγυάται ένα ορισμένο ποσοστό διαθεσιμότητας και ορισμένο εύρος ζώνης ISP στο δίκτυο. Τυπικά η εγγύηση της ποιότητας των υπηρεσιών εγγυάται ένα ορισμένο ποσοστό λανθάνουσας κατάστασης για την κυκλοφορία σας στο ISP δίκτυο, που μετριέται τυπικά σε δεκάδες χιλιοστά του δευτερολέπτου. Τα περισσότερα εθνικά ISPs εγγυώνται 99,5% διαθεσιμότητα στο δίκτυό τους. Οι εγγυήσεις του QoS θα διαπραγματευτούν κατά την συμφωνία του ISP και του πελάτη.

Υπάρχουν επίσης υπηρεσίες VPN που πωλούν οι ISPs, συμπεριλαμβανομένου του GTE, του UUNET, και άλλων. Με αυτές τις υπηρεσίες, λειτουργούν και διαχειρίζονται το VPN σας για σας. Οι τιμές είναι διάφορες, και είναι τυπικά βασισμένες στον αριθμό των sites και στο συνολικό εύρος ζώνης που χρησιμοποιείται.

5.3 ΛΥΝΟΝΤΑΣ ΤΑ ΠΡΟΒΛΗΜΑΤΑ ΤΟΥ VPN

Υπάρχουν πολλά σημεία στα οποία το VPN σας μπορεί να παρουσιάσει πρόβλημα. Η εύρεση της αιτίας ενός προβλήματος είναι πιο δύσκολη από ότι θα ήταν για ένα κανονικό WAN ή για μια σύνδεση απομακρυσμένης πρόσβασης. Μεταξύ των πιθανών προβλημάτων είναι τα προβλήματα συνδεσιμότητας, τα σφάλματα πιστοποίησης ταυτότητας και τα προβλήματα δρομολόγησης.

5.3.1 Προβλήματα συνδεσιμότητας

Οποιοσδήποτε είναι εξοικειωμένος με τη συντήρηση ή τη σύνδεση με servers απομακρυσμένης πρόσβασης ή με ISPs, είναι επίσης εξοικειωμένος και με προβλήματα κακής σύνδεσης. Η βασική δυσκολία με τα προβλήματα συνδεσιμότητας είναι ότι μπορεί να προέρχονται από πολλές αιτίες. Εδώ βλέπουμε μερικές πιθανότητες:

✧Τεχνικά Προβλήματα:

- Κακές γραμμές
- Απασχολημένες γραμμές

✧Προβλήματα ISP:

- Μη αποκρινόμενος ISP
- Κακό modem ή router

✧Προβλήματα τελικού χρήστη:

- Κακό modem ή router

- Ένα modem ή ένας router μη συμβατός με του ISP
- Πρόβλημα διαμόρφωσης

Εκτός από αυτά τα γενικά προβλήματα επικοινωνίας, μπορεί να ανακαλύψετε προβλήματα με τη χρήση των ports στα firewalls. Όπως έχετε δει, διάφορα πακέτα VPN χρησιμοποιούν συγκεκριμένα TCP ή UDP ports προκειμένου να επικοινωνήσουν (παραδείγματος χάριν, το PPTP χρησιμοποιεί το TCP port 1723). Εάν αυτά τα ports δεν είναι ανοικτά, μπορεί να μην είστε σε θέση να κάνετε μια VPN σύνδεση ή να μεταφέρετε δεδομένα μέσω του VPN. Είναι πιθανό αυτά τα ports να "εγκλωβιστούν" (να μπλοκαριστούν) στον ISP σας ή στους δρομολογητές σας.

5.3.2 Τα προβλήματα πιστοποίησης ταυτότητας

Τα προβλήματα πιστοποίησης ταυτότητας είναι κοινά στις dial-up συνδέσεις, ακόμα και όταν οι συνδέσεις αυτές δεν έχουν να κάνουν με VPNs. Εδώ βλέπετε τα δύο πιο κοινά προβλήματα πιστοποίησης ταυτότητας:

① Λάθος όνομα χρήστη ή κωδικός πρόσβασης. Αυτό μερικές φορές προκαλείται από ένα απλό τυπογραφικό σφάλμα. Επιπλέον, θα μπορούσαν να υπάρξουν λάθος συνδυασμοί κλειδιών σε ένα σύστημα δημόσιου κλειδιού.

②Μη συμβατότητα των μεθόδων πιστοποίησης ταυτότητας. Παραδείγματος χάριν, ο χρήστης μπορεί να προσπαθεί να πιστοποιηθεί με PAP, ενώ το σύστημα προορισμού να αναμένει τη μέθοδο CHAP.

Υπάρχει ένα τρίτο επίπεδο προβλημάτων πιστοποίησης ταυτότητας που περιλαμβάνει τις υποδομές δημόσιου κλειδιού. Είναι σημαντικό να χρησιμοποιηθεί το ίδιο πρωτόκολλο ανταλλαγής κλειδιού. Παραδείγματος χάριν, μερικά προϊόντα IPSec επιτρέπονται για διάφορες δυνατότητες ανταλλαγής κλειδιού: Manual, SKIP ή IPSec.

5.3.3 Προβλήματα δρομολόγησης

Προβλήματα δρομολόγησης εμφανίζονται όταν είστε σε θέση να συνδεθείτε επιτυχώς με τον ISP σας, αλλά έχετε πρόβλημα να "μπείτε" σε ορισμένους hosts του Διαδικτύου, ή να "σερφάρετε" στο Διαδίκτυο γενικά. Αυτά τα προβλήματα οφείλονται συνήθως στα σφάλματα διαμόρφωσης. Είτε η διεύθυνση IP, είτε η subnetmask, είτε η πύλη στο σύστημά σας είναι εγκατεστημένη λάθος, ή ο ISP σας δεν έχει μια "διαδρομή" για σας.

Το πρόβλημα δρομολόγησης θα μπορούσε επίσης να οφείλεται σε οποιοδήποτε από τα πολυάριθμα σημεία σύνδεσης στο εύρος του Διαδικτύου μεταξύ εσάς και του προορισμού. Εσείς, και ο ISP σας, θα ελέγχετε μερικώς αυτά τα προβλήματα, αλλά είναι καλό να ξέρετε που είναι το πρόβλημα, έτσι ώστε να μπορείτε να το αναφέρετε στους κατάλληλους ανθρώπους.

Στο κεφάλαιο 4, "Διαμορφώνοντας και εξετάζοντας συνδέσεις 2ου επιπέδου", στην παράγραφο "έλεγχος συνδεσιμότητας" (4.9) αναφέραμε δύο χρήσιμα βοηθήματα για τη δοκιμή των διαδρομών: ping και traceroute. Και τα δύο αυτά εργαλεία μπορούν επίσης να χρησιμοποιηθούν για να ανιχνεύσουν λάθη σε άλλα VPNs. Το ping είναι ένα βοήθημα που βρίσκεται στο Unix, στα Windows 95/98 και στα συστήματα των Windows NT. Στέλνει τα πακέτα σε ένα συγκεκριμένο προορισμό και αναμένει μια επιστροφή. Δεν σας λέει ποια διαδρομή ακολουθούν τα πακέτα, αλλά σας λέει εάν φτάνουν τελικά στον προορισμό τους και εάν υπάρχει οποιαδήποτε απώλεια πακέτων. Το traceroute είναι ένα πρόγραμμα για τα συστήματα Unix. Το αντίστοιχο των Windows 95/98/NT είναι το TRACERT. Το traceroute θα σας εμφανίσει το "μονοπάτι" που ακολουθούν τα πακέτα για τον προορισμό τους. Αυτές οι πληροφορίες μπορεί να είναι χρήσιμες στο να επισημάνουν που ακριβώς υπάρχει κάποιο πρόβλημα.

Επίσης έχετε υπ' όψιν ότι ένας ISP ή μια επιχείρηση μπορεί να μπλοκάρει τα UDP πακέτα του traceroute στο firewall τους για λόγους ασφάλειας, έτσι μπορεί να θέλετε να συνδεθείτε μ' αυτούς και να δείτε αν πρόκειται γι' αυτήν την περίπτωση. Εάν το πρόβλημα φαίνεται να είναι σε έναν παροχέα του Διαδικτύου, το καλύτερο που έχετε να κάνετε είναι να έρθετε σε επαφή με τον ISP σας.

5.4 ΣΥΝΕΡΓΑΣΙΑ ΜΕ ΤΟΝ ISP

Το να δουλεύεις με έναν ISP για να λύσεις ένα πρόβλημα VPN μπορεί να αποδειχτεί δύσκολο, ειδικά εάν ο ISP δεν υποστηρίζει VPNs. Σαν διαχειριστής δικτύων, επομένως, θα πρέπει να ξέρετε το VPN σας αρκετά καλά. Το σημαντικότερο πράγμα που πρέπει να θυμάστε κατά την ανίχνευση λαθών ενός προβλήματος με ISP είναι να τους δίνετε όσο το δυνατόν περισσότερες πληροφορίες. Τουλάχιστον, δώστε τους αυτές τις πληροφορίες:

- Ποιο προϊόν VPN χρησιμοποιείτε
- Ποια πρέπει να είναι η διεύθυνση IP του συστήματός σας
- Ποια πρέπει να είναι η διεύθυνση IP του VPN server προορισμού ή του δρομολογητή (π.χ., η διεύθυνση του PPTP server σας).
- Τα TCP ή UDP ports που το προϊόν VPN σας χρησιμοποιεί, σε περίπτωση που ο ISP σας έχει μπλοκάρει εκείνα τα ports σε ένα firewall
- Οποιοδήποτε αποτέλεσμα μπορεί να σας δείχνει το ping ή το traceroute για κάποιο πρόβλημα.

Σιγουρευτείτε ότι εμπιστεύεστε τον ISP σας. Κατά τη διάρκεια της περιόδου ανίχνευσης λαθών μπορεί να πρέπει να του δώσετε πληροφορίες ασφάλειας για το δίκτυό σας. Εδώ δίνουμε μερικές προτάσεις για να βρείτε έναν αξιόπιστο ISP, ή για να αποκτήσετε εμπιστοσύνη σε αυτόν που ήδη έχετε:

☒ Χρησιμοποιήστε έναν καθιερωμένο ISP: είτε ένας γνωστός εθνικός provider, ή ένας τοπικός που έχει καλή φήμη και ένα ιστορικό λειτουργίας.

☒ Εάν είναι δυνατό, να επικοινωνείτε πάντα με το ίδιο πρόσωπο υποστήριξης. Αυτό, όχι μόνο θα σας εγγυηθεί καλύτερες υπηρεσίες, - δεδομένου ότι το πρόσωπο αυτό θα γνωρίζει και προηγούμενα τυχόν προβλήματά σας - αλλά θα κρατήσει επίσης χαμηλό τον αριθμό των ανθρώπων που γνωρίζουν ευαίσθητες πληροφορίες του δικτύου.

5.5 Η ΣΥΜΒΑΤΟΤΗΤΑ ΜΕ ΑΛΛΑ ΠΡΟΪΟΝΤΑ

Άλλα προϊόντα στο δίκτυό σας μπορεί να παίξουν σημαντικό ρόλο στην απόδοση του VPN σας. Πριν επενδύσετε χρόνο και χρήματα για να εγκαταστήσετε ένα VPN, πρέπει να κάνετε μια έρευνα για να εξασφαλίσετε ότι το σύστημά σας και η διαμόρφωση δικτύων θα λειτουργήσουν με αυτό - ειδικά εάν έχετε ήδη εγκατάστήσει μέτρα ασφάλειας. Εδώ δίνονται μερικές προειδοποιήσεις κατά την εγκατάσταση ενός VPN ή την προσθήκη ενός νέου προϊόντος στο δίκτυό σας:

☑ Μερικοί δρομολογητές μπορεί να μπλοκάρουν ορισμένα TCP ports ως μέτρο ασφάλειας. Βρείτε ποια ports μπλοκάρει και σιγουρευτείτε ότι δεν είναι ports που χρησιμοποιεί το VPN σας. Μπορείτε επίσης να απενεργοποιήσετε αυτό το φιλτράρισμα.

☑ Όπως έχουμε πει ήδη, μερικά προϊόντα VPN δεν θα λειτουργήσουν σε έναν proxy server. Ο Proxy Server της Microsoft, παραδείγματος χάριν, δεν λειτουργεί με PPTP. Εάν έχετε ήδη έναν proxy server και θέλετε να εφαρμόσετε ένα VPN, μπορεί να θελήσετε να πολυ-κατευθυνθείτε (multi-homed) τον VPN server μεταξύ του Διαδικτύου και του LAN σας, αμέσως μόλις εγκαταστήσετε τον proxy server. Μόνο η κυκλοφορία του VPN δρομολογείται μέσω του VPN server, ενώ όλη η άλλη κυκλοφορία δρομολογείται μέσω του proxy server.

☑ Το Network Address Translation (NAT) είναι ένα πρωτόκολλο που υποστηρίζουν πολλοί δρομολογητές. Το NAT επιτρέπει στις μηχανές να έχουν πρόσβαση στο Διαδίκτυο ακόμα κι αν έχουν εσωτερικές διευθύνσεις IP που δεν είναι χρησιμοποιήσιμες στο ευρύτερο Διαδίκτυο. Ουσιαστικά, σε κάθε μηχανή δίνεται μια nonroutable διεύθυνση, ενώ ο δρομολογητής έχει μια routable διεύθυνση IP. Όταν κάθε μηχανή πίσω από το δρομολογητή θέλει να έχει πρόσβαση στο Διαδίκτυο, προσποιείται ότι έχει τη διεύθυνση IP του δρομολογητή.

Εάν θέλετε να χρησιμοποιήσετε το NAT, προτείνουμε μια εγκατάσταση διπλού-δρομολογητή. Σ' αυτού του τύπου την εγκατάσταση εμφανίζεται ένας δρομολογητής πύλης στο Διαδίκτυο και ένα περιμετρικό δίκτυο με τις routable διευθύνσεις IP του Διαδικτύου. Στο περιμετρικό δίκτυο βρίσκεται ένας πολύ-κατευθυνόμενος δρομολογητής NAT για να έχει διεπαφές και στο περιμετρικό δίκτυο και στο εσωτερικό δίκτυο. Οι μηχανές στο εσωτερικό δίκτυο έχουν μόνο τις nonroutable IP διευθύνσεις Διαδικτύου. Ο VPN server πολυ-κατευθύνεται επίσης μεταξύ των περιμετρικών και

των εσωτερικών δικτύων, και θα δρομολογήσει μόνο την κυκλοφορία του VPN από και σε εκείνα τα δίκτυα.

5.6 QUALITY OF SERVICE (QoS) ΣΤΟ VPN

Έχουμε μιλήσει ήδη για την QoS όταν αναφερόμασταν στην επιλογή του ISP. Εδώ θα αναφερθούμε στη δημιουργία QoS για τη δική σας συνδεσιμότητα. Το QoS σας δίνει τη δυνατότητα να διαχειριστείτε το εύρος ζώνης στο οποίο θα μπορείτε να κινηθείτε. Το κάνει αυτό, επιτρέποντάς σας να ορίσετε προτεραιότητες σε συγκεκριμένους τύπους της κυκλοφορίας των δικτύων που βασίζονται στο χρήστη, την εφαρμογή, τον host, το δίκτυο ή το πρωτόκολλο. Με ένα VPN, μπορείτε να χρησιμοποιείτε επίσης τη VPN σύνδεσή σας στο Διαδίκτυο για την κοινή χρήση του Διαδικτύου, όπως το ηλεκτρονικό ταχυδρομείο, το web browsing, τη μεταφορά αρχείων κ.λ.π.. Μπορείτε να θέσετε σε προτεραιότητα την κυκλοφορία του VPN σας και στη συνέχεια την κυκλοφορία που δεν είναι απαραιτήτως επιχειρησιακού προσανατολισμού, για παράδειγμα η πρόσβαση σε ορισμένα URLs.

Το Resource Reservation Protocol (RSVP) είναι ένα προτεινόμενο πρότυπο για την ποιότητα των υπηρεσιών (QoS) του Διαδικτύου που μπορεί να χρησιμοποιηθεί για να διαχειριστεί την κυκλοφορία IP. Είναι ήδη διαθέσιμο σε κάποιο VPN εξοπλισμό και σε μερικά λειτουργικά συστήματα. Επιπλέον, υπάρχει ένας αριθμός διοικητικών προϊόντων διαθέσιμα από τους προμηθευτές όπως το Packeteer και το Check Point.

5.7 ΠΡΟΤΑΣΕΙΣ ΑΣΦΑΛΕΙΑΣ

Η αρχική πρόταση ασφαλείας μας, είναι να γίνει το VPN το μόνο σημείο εισόδου στο δίκτυό σας από το Διαδίκτυο. Δηλαδή, σιγουρευτείτε ότι όλα τα συστήματά σας μπλοκάρονται, ή αλλιώς, είναι μη προσβάσιμα από το Διαδίκτυο, εκτός κι αν οι εξωτερικοί χρήστες συνδέονται με αυτό μέσω ενός VPN. Το κεφάλαιο 2 περιγράφει τη χρήση των firewalls για αυτόν ακριβώς το λόγο.

5.7.1 Περιορίστε το ποιος θα έχει πρόσβαση στο VPN

Δεν πρέπει να έχει οποιοσδήποτε πρόσβαση στο VPN σας. Εάν η επιχείρησή σας υποβάλλεται σε σταθερές αλλαγές, ή "τρέχετε" μια εικονική εταιρία όπου οι εργαζόμενοι εργάζονται από το σπίτι, μπορεί να σας είναι δύσκολο να περιορίσετε τους χρήστες που έχουν πρόσβαση. Μπορεί να θέλετε να επιτρέπετε απομακρυσμένη πρόσβαση μόνο σε ανθρώπους που πραγματικά τη χρειάζονται. Εδώ δίνουμε μερικά παραδείγματα ανθρώπων που μπορεί να χρειάζονται απομακρυσμένη πρόσβαση VPN:

- Διακινούμενοι πωλητές ή marketers που χρειάζονται πρόσβαση στο ηλεκτρονικό ταχυδρομείο και στα αρχεία.

☞Εργαζόμενοι που εργάζονται από το σπίτι, ή που χρειάζονται πρόσβαση στους servers του δικτύου οποιαδήποτε ώρα της ημέρας. Για παράδειγμα, οι υπεύθυνοι για την ανάπτυξη λογισμικού, ελεγκτές, αυτοί που γράφουν τις αναφορές, ή διευθυντές. Αν κάποιος εργάζεται μόνιμα από το σπίτι ή έχει ανάγκη για μόνιμη πρόσβαση, παραδείγματος χάριν, ένας υπάλληλος που έχει σπάσει το πόδι του και πρέπει να μείνει στο σπίτι για κάποιους μήνες πρέπει να είναι σε θέση να συνδεθεί και να εργαστεί.

☞ Διαχειριστές δικτύου ή συστημάτων.

Επίσης προτείνουμε να εφαρμόσετε μια κοινώς αποδεκτή πολιτική που να διέπει τους λογαριασμούς του VPN σας και την οποία θα πρέπει να γνωρίζει καθένας που έχει πρόσβαση στο VPN. Εδώ είναι μερικές προτεινόμενες οδηγίες:

❁Ο λογαριασμός του VPN δεν είναι ένας γενικός λογαριασμός Διαδικτύου που ένας υπάλληλος μπορεί να τον χρησιμοποιήσει για οτιδήποτε θέλει. Είναι ουσιαστικά μια επέκταση του δικτύου της εταιρίας και του λογαριασμού που ο χρήστης έχει στο εταιρικό σύστημα, ακόμα κι αν η πρόσβαση γίνεται μέσω ενός ISP. Ο χρήστης δεν πρέπει να δώσει πληροφορίες για το λογαριασμό σε παιδιά, συγγενείς, φίλους, ούτε ακόμα και σε συνεργάτες του.

❁ Ο χρήστης πρέπει να κατευθύνει όλα τα προβλήματα τεχνικής υποστήριξης σχετικά με το VPN στο διαχειριστή δικτύων, παρά άμεσα στον σχετικό ISP. Εάν απαιτείται, ο διαχειριστής δικτύων μπορεί να έρθει σε επαφή με τον ISP. Δεν υπάρχει κανένας λόγος για το χρήστη να δώσει τον κωδικό πρόσβασής του ή το domain (την δικτυακή τοποθεσία) του εσωτερικού δικτύου στον ISP .

❁ Οι χρήστες του VPN πρέπει να αλλάζουν τους κωδικούς πρόσβασής τους συχνότερα από άλλους χρήστες του domain του εσωτερικού δικτύου. Πρέπει επίσης να επιλέξουν κωδικούς πρόσβασης χωρίς νόημα, που δε θα περιέχουν ενδεχομένως αλφαβητικούς ή αριθμητικούς χαρακτήρες, οι οποίοι δεν μπορούν να υποτεθούν εύκολα. Παραδείγματα: "xf3Kr!" ή "bat*CORE."

❁ Τέλος, όταν κάποιοι υπάλληλοι φεύγουν από τη δουλειά (π.χ. απόλυση), θυμηθείτε να τους αφαιρέσετε την πρόσβαση στο VPN, ακριβώς όπως θα κάνατε και με τους λογαριασμούς τους στο τοπικό σύστημα. Ακόμα κι αν είναι εύκολο να τους εντοπίσετε αν προσπαθήσουν να το χρησιμοποιήσουν, θα μπορούσαν να προκαλέσουν αρκετό κακό και σύγχυση για να κάνουν τη δουλειά των άλλων υπαλλήλων δυσκολότερη – ακόμα χειρότερα αν έχουν πρόσβαση στο VPN μπορούν ευκολότερα να "κλέψουν" εμπορικά μυστικά ή λογισμικό που χορηγείται με άδεια στην επιχείρησή σας.

5.7.2 Περιορίστε τις δυνατότητες των χρηστών του VPN

Σε μεγάλα εταιρικά LANs, οι διαχειριστές δικτύων δημιουργούν συχνά διάφορα τμήματα δικτύου ξεχωριστά από τους δρομολογητές και τα οποία μπορούν να περιορίσουν την κυκλοφορία του δικτύου σε ορισμένα τμήματα και να παρέχουν τις δυνατότητες των firewalls. Παραδείγματος χάριν, δε χρειάζεται κανένας από το κατασκευαστικό τμήμα να έχει πρόσβαση στον server των μισθοδοτικών καταστάσεων του ανθρώπινου δυναμικού- είτε έχει κωδικό πρόσβασης, είτε όχι.

Επιπλέον, μπορείτε να χρησιμοποιήσετε εσωτερικούς δρομολογητές και firewalls για να περιορίσουν προς τα που μπορούν να πάνε οι χρήστες του VPN. Εδώ δίνουμε μερικά παραδείγματα πληροφοριών που δε θα θέλετε ποτέ να είναι προσιτές σε έναν χρήστη VPN ή σε έναν χρήστη απομακρυσμένης πρόσβασης:

- Πληροφορίες ασφάλειας και κρυπτογράφησης, όπως τα ιδιωτικά κλειδιά RSA και τα πιστοποιητικά SSL.
- Πληροφορίες που αφορούν τα user names και τα passwords.
- Άκρως απόρρητες πληροφορίες ερευνών και πληροφορίες ανάπτυξης.
- Πληροφορίες μισθοδοτικών καταστάσεων.
- Ιδιωτικές πληροφορίες των εργαζομένων, συμπεριλαμβανομένων πληροφοριών που αφορούν την υγεία.
- Οποιεσδήποτε πληροφορίες που οι πελάτες σας σάς έχουν εμπιστευτεί και πρέπει να τις κρατάτε εμπιστευτικά (παραδείγματος χάριν, εάν είστε ένα νοσοκομείο, θα θέλετε να κρατήσετε τα ιατρικά αρχεία εξαιρετικά ασφαλή).

Το ιδανικό θα ήταν να εγκατασταθούν πολλαπλοί VPN servers - ένας για κάθε τμήμα - και να περιοριστεί ο αριθμός αυτών που θα μπορούσαν να τους χρησιμοποιήσουν.

5.7.3 Αποφύγετε να δημοσιεύετε DNS πληροφορίες για τους servers και τους δρομολογητές του VPN

Δεδομένου ότι ο VPN server σας θα είναι ένα προσβάσιμο σημείο εισόδου στο δίκτυό σας, είναι καλύτερο να μην αφήσετε τους "επιτιθέμενους" να ξέρουν τι είναι ή τι κάνει. Το απλούστερο πράγμα που έχετε να κάνετε είναι να μη βάλετε καθόλου DNS hostname στον VPN server σας. Εάν πρέπει να βάλετε ένα (για εσωτερική χρήση, παραδείγματος χάριν), κοιτάξτε να εγκαταστήσετε έναν "πλαστό" DNS server με ασυνάρτητες πληροφορίες που θα είναι προσιτός στο Διαδίκτυο, ενώ θα έχετε έναν server με συγκεκριμένες πληροφορίες που θα τον χρησιμοποιείτε μέσα στο LAN σας. Σε καμία περίπτωση μην αφήσετε τους "έξω" να δουν ένα κατανοητό (με σημασία) όνομα για τον VPN server σας, όπως το avtunnel.caf-feine.net.

5.8 ΚΡΑΤΩΝΤΑΣ ΤΟ VPN ΑΝΑΒΑΘΜΙΣΜΕΝΟ

Το να κρατάτε το VPN σας συνεχώς αναβαθμισμένο είναι πολύ σημαντικό. Εδώ δίνουμε τους βασικούς λόγους για τους οποίους πρέπει να αναβαθμίζεται το λογισμικό του VPN σας:

- Όταν το προϊόν που χρησιμοποιείτε αυτήν την περίοδο δε σας καλύπτει απόλυτα στα θέματα ασφαλείας.
- Όταν υπάρχει ένα προγραμματιστικό λάθος που προκαλεί προβλήματα στο σύστημα (όπως διαρροές μνήμης ή προβλήματα δικτύωσης).
- Όταν η τρέχουσα έκδοση δεν είναι συμβατή με ένα άλλο προϊόν στο δίκτυό σας, ή με ένα προϊόν που έχουν οι απομακρυσμένοι χρήστες, και η νέα έκδοση βελτιώνει την ενδολειτουργικότητα.
- Όταν η νέα έκδοση έχει διάφορες επιπλέον λειτουργίες που είναι σημαντικές για τη λειτουργία του VPN σας.

5.9 ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Virtual Private Networks
Second Edition
Charlie Scott, Paul Wolfe and Mike Erwin

2. ΔΙΕΥΘΥΝΣΕΙΣ ΣΤΟ INTERNET:
www.cisco.com/en/Us/products/sw/securcw/ps2120/products_configuration_guide_chapter09186a0080172787.Html-101k

www.cw.com/services/connectivity/data/ipvpn_qos.html

ΚΕΦΑΛΑΙΟ 6°

6.1 ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΤΩΝ VPNs

Η χρήση VPN αποφέρει σημαντικά οφέλη σε όλα τα μέρη που συμμετέχουν, είτε αυτά αποτελούν την εταιρεία που το χρησιμοποιεί, είτε τον τελικό χρήστη του VPN, είτε τον ISP που παρέχει την υποδομή. Σε γενικές γραμμές τα οφέλη περιλαμβάνουν μείωση των δαπανών για τις τηλεπικοινωνίες, καλύτερη διαχείριση και ευκολότερη συντήρηση, πιο εύκολη κατασκευή του συστήματος.

Άμεσα οικονομικά οφέλη

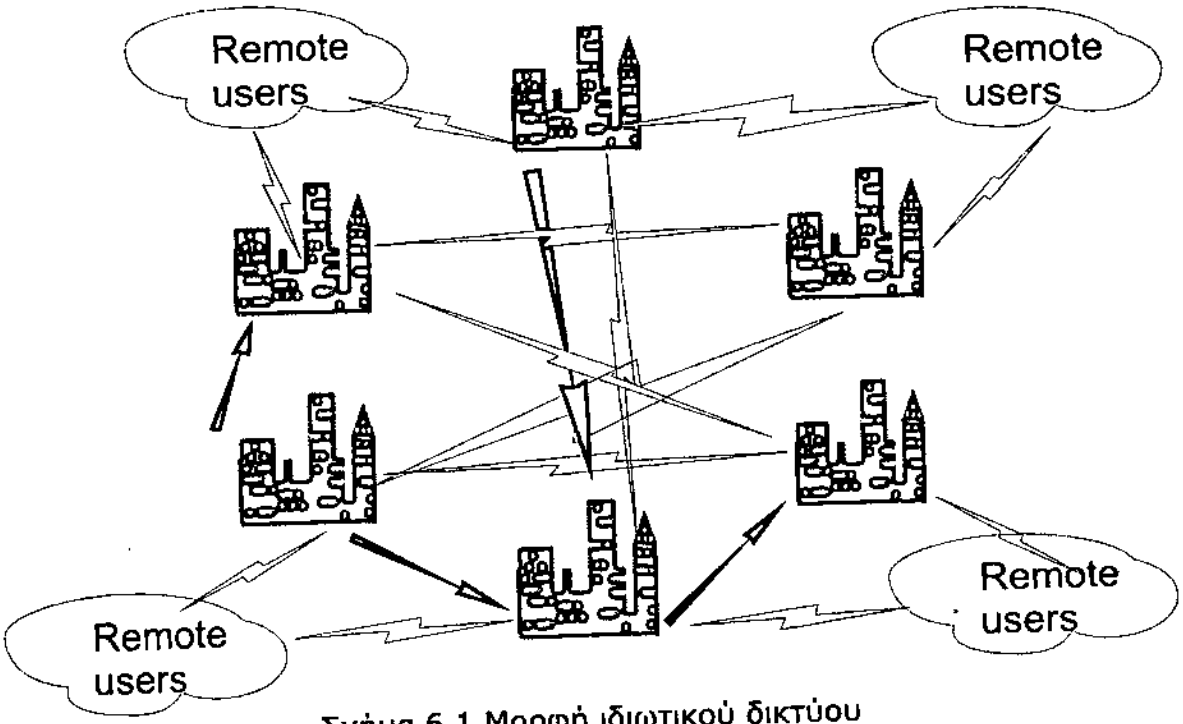
Είναι δυνατό να επιτευχθεί σημαντική μείωση στο συνολικό κόστος που θα επιβαρύνει την εταιρεία αν και το ακριβές ποσοστό θα προκύψει από τον συμψηφισμό του ποσού που η εταιρεία κερδίζει και του ποσού που χρειάζεται για να υλοποιήσει και να συντηρεί το VPN. Έτσι, αν η εταιρεία χρησιμοποιούσε ένα ιδιωτικό δίκτυο, με τη χρήση VPN μπορεί να σταματήσει τη μίσθωση γραμμών και να μειώσει το κόστος από κλήσεις μεγάλων αποστάσεων που γίνονται από απομακρυσμένους χρήστες. Μπορεί, επίσης, να αφαιρέσει τον εξοπλισμό απομακρυσμένης πρόσβασης και παράλληλα όλο τον εξοπλισμό που τον υποστηρίζει (π.χ. UPS) και να μειώσει με αυτό τον τρόπο το προσωπικό που κάνει τη διαχείριση και τη συντήρηση του δικτύου της.

Σχεδιασμός δικτύου

Η τεχνολογία των VPNs αποφέρει μεγάλα οφέλη στον τομέα σχεδιασμού του δικτύου του οργανισμού. Ο οργανισμός δεν είναι επιφορτισμένος με το σχεδιασμό ενός πολύπλοκου WAN, την εύρεση των αναγκαίων επιδόσεων των συνδέσεων μεταξύ των περιοχών ενδιαφέροντος και τον υπολογισμό του απαιτούμενου εύρους ζώνης. Το κύριο ενδιαφέρον του είναι να εξασφαλίσει μια καλή σύνδεση με τον ISP. Πριν την εμφάνιση του Internet ο οργανισμός έπρεπε να εγκαταστήσει έναν αριθμό μισθωμένων γραμμών για να συνδέσει τα διάφορα γραφεία του. Τα θέματα που έπρεπε να ληφθούν υπόψη από τον σχεδιαστή του δικτύου ήταν:

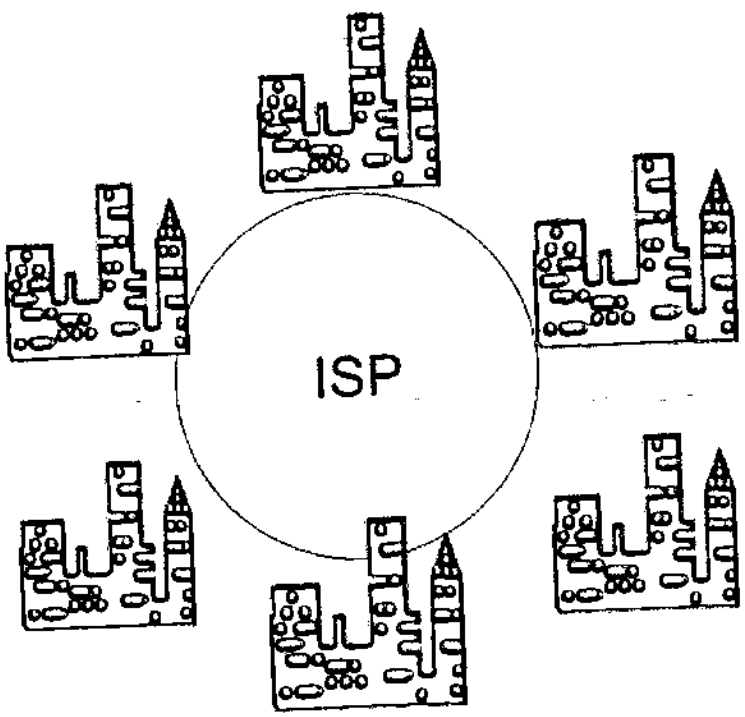
- η χρήση βοηθητικών (backup) γραμμών για να αντιμετωπιστούν περιπτώσεις μη λειτουργίας κάποιων από τις κύριες,
- η δυνατότητα επέκτασής του,
- η παροχή πρόσβασης σε απομακρυσμένους χρήστες και
- ο καθορισμός του μεγέθους της κυκλοφορίας μέσα στο δίκτυο.

Ένα ιδιωτικό δίκτυο που θα υλοποιούνταν με μέσα της εταιρείας θα είχε τη γενική μορφή του παρακάτω σχήματος (Σχήμα 6.1).



Σχήμα 6.1 Μορφή ιδιωτικού δικτύου

Η χρήση ενός VPN μειώνει όλη αυτή την εργασία, καθώς ο ISP είναι αυτός που αναλαμβάνει την μεταφορά των δεδομένων. Έτσι το WAN μπορεί να είναι επεκτάσιμο και βασισμένο πάνω σε ένα πρωτόκολλο. Ο ISP επίσης έχει αναλάβει και τα θέματα που αφορούν πλεονασμό συνδέσεων, ώστε να εξασφαλίζεται η αξιοπιστία του δικτύου. Ο οργανισμός πρέπει να καθορίσει το μέγεθος της σύνδεσης με τον ISP που συνεπάγεται μελέτη της κίνησης μέσα στο εσωτερικό δίκτυο κάθε περιοχής και υπολογισμό του ποσοστού που θα διακινείται μέσω Internet. Το αποτέλεσμα αυτής της μεταφοράς του σχεδιασμού στον ISP είναι το ιδιωτικό δίκτυο της εταιρείας να αποκτά την παρακάτω μορφή (Σχήμα 6.2).



Σχήμα 6.2 Μορφή ιδιωτικού δικτύου με χρήση ISP

Κεντρικοποιημένος έλεγχος

Αρκετοί κατασκευαστές υποστηρίζουν κεντρικοποιημένο έλεγχο των VPNs προϊόντων τους, κάτι το οποίο είναι ένας καλός μηχανισμός ανίχνευσης βλαβών, αλλά και ένα χαρακτηριστικό που προσφέρει μεγαλύτερη ασφάλεια. Αν υποθέσουμε ότι έχει παρουσιαστεί ένα πρόβλημα σύνδεσης μεταξύ μιας εφαρμογής πελάτη σε ένα τμήμα και ενός εξυπηρετητή σε ένα άλλο τμήμα, τότε θα έπρεπε να γίνει συντονισμός του προσωπικού των δύο αυτών τμημάτων για να επιλυθεί το πρόβλημα. Τα πράγματα περιπλέκονται όταν κάποιες λύσεις δεν αποδίδουν και αναγκαστικά στρεφόμαστε στον κατασκευαστή με αποτέλεσμα να καθυστερεί η επίλυση του προβλήματος. Η χρήση κεντρικοποιημένου ελέγχου δεν απαιτεί τέτοια αντιμετώπιση αλλά το μόνο που χρειάζεται είναι ο χρήστης που έχει το πρόβλημα και ένας τεχνικός να είναι on-line και με παρακολούθηση των δύο άκρων του VPN να μπορεί να απομονωθεί η αιτία του. Παράλληλα, η ίδια προσέγγιση μπορεί να εφαρμοστεί στη συντήρηση του VPN. Σε περίπτωση που δεν υπάρχει κεντρικοποιημένος έλεγχος μπορεί να γίνει εγκατάσταση modem με κρυπτογραφικές ιδιότητες σε κάθε κονσόλα συσκευής του VPN και έτσι να μπορεί με ειδικό λογισμικό να γίνεται η διαχείρισή της.

Ευκολίες στον τελικό χρήστη

Ο χρήστης όταν θέλει να συνδεθεί με κάποιον server χρειάζεται μόνο να πληρώνει το κόστος μιας τοπικής κλήσης συν μια μηνιαία συνδρομή στην περίπτωση που το VPN έχει υλοποιηθεί στο Internet. Έτσι υπάρχει σημαντική μείωση του κόστους. Παράλληλα μπορεί πολύ εύκολα να αποκτήσει οποιοδήποτε υλικό κρίνει αναγκαίο για να εξασφαλίσει μια συναλλαγή με κάποιον πελάτη. Το μόνο που πρέπει να κάνει είναι να συνδεθεί με κάποιον εξυπηρετητή της εταιρείας και να κατεβάσει το υλικό αυτό. Επίσης μπορεί να ανήκει σε κάποια κλάση προτεραιότητας οπότε και να μπορεί να εξυπηρετείται πιο γρήγορα. Η κατηγοριοποίηση των χρηστών αλλά και της διακινούμενης πληροφορίας μπορεί να βελτιώσει τη συμπεριφορά του δικτύου, αφού θα γίνεται ορθότερη χρήση των πόρων του, και να κάνει αποδοτική την εκτέλεση των διαφόρων υπηρεσιών που ζητούν οι τελικοί χρήστες.

Σύνδεση σε παγκόσμια βάση (Global reach)

Το Internet παρέχει σύνδεση σε παγκόσμια βάση καθώς ο κάθε χρήστης μπορεί να συνδεθεί με την εταιρεία του με τη βοήθεια κάποιου ISP. Διευκολύνεται σημαντικά η επέκταση της παρουσίας του οργανισμού ανά την υφήλιο που σημαίνει ότι μπορεί πιο εύκολα να προωθήσει τα προϊόντα του. Ακόμη και για εταιρείες με μικρό προϋπολογισμό η χρήση του Internet μπορεί να προσφέρει μια αγορά της τάξεως των εκατομμυρίων πελατών.

Νέοι τομείς δραστηριοποίησης των ISPs

Οι ISPs μπορούν με τη χρήση των VPNs να προσφέρουν στους πελάτες τους οποιεσδήποτε υπηρεσίες τους ζητηθούν. Ακόμη και εφαρμογές τηλεδιάσκεψης μεταξύ κεντρικών πόλεων του πλανήτη είναι εφικτές. Αν ένας ISP μπορεί να προσφέρει και ένα βαθμό Quality of Service για τέτοιες εφαρμογές κάποιου οργανισμού τότε αυτόματα γίνεται στρατηγικός συνεργάτης και ταυτόχρονα ισχυροποιεί τη θέση του στην αγορά υπηρεσιών. Ο τομέας διαχείρισης των VPNs θα γνωρίσει μεγάλη ανάπτυξη στο μέλλον, καθώς οι τεχνολογίες δικτύωσης αναπτύσσονται με ρυθμούς που είναι πολύ γρήγοροι για να τους παρακολουθήσει το προσωπικό ενός οργανισμού. Επίσης, τα θέματα ασφαλείας αποκτούν ιδιαίτερη σημασία ώστε πολλοί χρήστες VPN θα οδηγηθούν στην απόφαση χρησιμοποίησης ISP με εμπειρία στο συγκεκριμένο τομέα.

Προσφορά στρατηγικού πλεονεκτήματος

Η χρήση του Internet μέσω VPN προσφέρει στρατηγικό πλεονέκτημα σε κάθε οργανισμό. Η περαιτέρω αύξηση αυτής της κατηγορίας χρηστών θα οδηγήσει σε βελτίωση των προσφερόμενων υπηρεσιών, καθώς κάθε οργανισμός θα απαιτεί νέες υπηρεσίες που θα τον φέρουν σε μια θέση ισχύος απέναντι στους υπολοίπους. Θα υπάρξει βελτίωση σε θέματα αξιοπιστίας και απόδοσης από πλευράς χρονικής καθυστέρησης.

6.2 ΜΕΙΟΝΕΚΤΗΜΑΤΑ ΤΩΝ VPNs

Η χρήση VPN παρουσιάζει κάποια μειονεκτήματα που αφορούν κυρίως τον τομέα της ασφάλειας. Το κύριο πρόβλημα που παρουσιάζεται είναι το ποιοι αλγόριθμοι κρυπτογράφησης μπορεί να χρησιμοποιηθούν. Υπάρχουν προορισμοί όπου απαγορεύεται η χρήση οποιασδήποτε κωδικοποίησης με αποτέλεσμα η εκάστοτε εταιρεία να βρίσκεται στο δίλημμα να εγκαταστήσει μια ευάλωτη μορφή του δικτύου που ενδεχομένως να προκαλέσει γενικότερα προβλήματα ασφαλείας ή να αγνοήσει την αγορά της συγκεκριμένης περιοχής και να χάσει τα οποιαδήποτε οικονομικά οφέλη που μπορεί να αποκομίσει.

Η χρήση του Internet βάζει και κάποιους περιορισμούς σε θέματα απόδοσης των VPNs. Απαιτητικές εφαρμογές όπως είναι η τηλεδιάσκεψη δεν μπορούν να εφαρμοστούν για κάθε τελικό χρήστη ενός VPN γιατί δεν πληρούνται οι απαιτήσεις απόδοσης του δικτύου. Επίσης, εφαρμογές που αποτελούν απόκριση πραγματικού χρόνου δεν έχουν όφελος από χρήση VPN καθώς εκτός από την καθυστέρηση του Internet υπεισέρχεται και η καθυστέρηση κρυπτογράφησης των δεδομένων.

6.3 ΚΟΣΤΟΣ ΕΝΟΣ VPN

Το κόστος εγκατάστασης και χρήσης ενός VPN εκτείνεται πάνω σε διάφορους τομείς, μερικοί από τους οποίους είναι αυτοί που αποκομίζουν σημαντικά οφέλη από τα VPNs. Συγκεκριμένα, παρά το γεγονός ότι παρέχεται εύκολη πρόσβαση μέσω του Internet μπορεί το κόστος σύνδεσης με αυτό να είναι σημαντικό για κάποιους απομακρυσμένους χρήστες καθώς μπορεί να κάνουν κλήση μεγάλης απόστασης. Έτσι ίσως θα απαιτείται από τον οργανισμό η παροχή κάποιων γραμμών μηδενικής χρέωσης (0800). Επίσης οι ανάγκες διαχείρισης του VPN μπορεί να απαιτούν ειδικά modems που θα μπορούν να ελέγχουν κάθε συσκευή του.

Το σημαντικότερο κόστος που υπεισέρχεται είναι ο σχεδιασμός του. Όπως αναφέρθηκε, αυτός περνά στα χέρια του ISP, ο οποίος αναλαμβάνει τη μελέτη της κυκλοφορίας του δικτύου της εταιρείας και προσπαθεί να φτάσει σε ένα αποτέλεσμα που θα ικανοποιεί και τις απαιτήσεις για περαιτέρω υπηρεσίες, όπως αυτές ορίζονται στο SLA. Παράλληλα η εταιρεία πρέπει να λάβει σοβαρά υπόψη την ύπαρξη δευτερεύουσας σύνδεσης με το Internet, ώστε να μπορεί να έχει κάποιες εναλλακτικές επιλογές σε περίπτωση που η κύρια σύνδεση παρουσιάζει προβλήματα. Το κόστος μιας ενδεχόμενης απομόνωσης από το παγκόσμιο δίκτυο μπορεί να είναι μεγαλύτερο σε σχέση με αυτό που απαιτείται για τη συντήρηση της σύνδεσης αυτής. Ένας άλλος παράγοντας είναι η ύπαρξη πλεονασμού στις συνδέσεις του ISP με άλλους ISPs καθώς έτσι μπορεί να βελτιωθεί η αξιοπιστία της επικοινωνίας.

Η απόκτηση του εξοπλισμού VPN και των αδειών χρήσης του λογισμικού είναι ένας ακόμη παράγοντας που προστίθεται στο κόστος του VPN. Πρέπει να υπάρχουν οι συσκευές που θα κάνουν πιστοποίηση των χρηστών καθώς και οι συσκευές που θα επιτρέπουν πρόσβαση σε απομακρυσμένους χρήστες με ασφάλεια.

Τέλος, ένας παράγοντας κόστους είναι η ανάγκη συντήρησης και διαχείρισης του δικτύου. Η συντήρηση αφορά αναβάθμιση συσκευών ή λογισμικού που προσδίδουν νέες δυνατότητες στο VPN. Αρκετές φορές το κόστος αναβάθμισης συμπεριλαμβάνεται στην αγορά των αδειών χρήσης των μερών που συνιστούν το VPN. Η διαχείριση συνήθως ανατίθεται στον ISP που έχει αναλάβει και την εγκατάσταση του VPN.

6.4 ΤΥΠΟΙ ΕΙΚΟΝΙΚΩΝ ΙΔΙΩΤΙΚΩΝ ΔΙΚΤΥΩΝ

6.4.1 TRUESPAN (OPENREACH)

Γενικά χαρακτηριστικά

Το OpenReach είναι ένας νέος τύπος VPN που εύκολα και αποτελεσματικά εκμεταλλεύεται τη δύναμη του Internet για προσωπικές συνδέσεις χωρίς την πολυπλοκότητα, το κόστος ή το χρόνο που χρειάζονταν η εγκατάσταση των παραδοσιακών VPNs. Δεν απαιτείται ιδιαίτερο Hardware ή Software.

Τα ελάχιστα τεχνικά χαρακτηριστικά που πρέπει να πληρεί ένα PC είναι:

- Επεξεργαστή Pentium/200 MHz
- Μνήμη RAM 32 MB
- 100 MB κενό χώρο στο σκληρό δίσκο
- Κάρτα Ethernet

Με οποιοδήποτε PC που πληρεί τις παραπάνω προϋποθέσεις μπορεί να δημιουργηθεί ένα δίκτυο ευρείας περιοχής. Ένα PC συνδέει ολόκληρο το τοπικό δίκτυο (LAN) με άλλο γραφείο. Δεν χρειάζονται αλλαγές στα υπάρχοντα PCs, servers, firewalls ή στον δικτυακό εξοπλισμό. Μπορούν να συνδεθούν PCs, Macs, συστήματα Unix και γενικά οτιδήποτε συνδέεται μέσω TCP/IP. Το Network Operations Center ειδοποιεί εάν υπάρχει πρόβλημα στη σύνδεση με άλλο γραφείο. Μπορούν, επίσης, πολύ εύκολα να συνδεθούν στο δίκτυο νέα μέλη. Είναι ένα δίκτυο πολύ εύκολα υλοποιήσιμο και ασφαλές για μικρές ή μεσαίες επιχειρήσεις.

Το OpenReach's TrueSpan Services είναι μια επέκταση του δικτύου ενός γραφείου που μπορεί να συνδέσει διαφορετικά γραφεία και να φαίνονται σαν ένα. PCs, servers και printers «βλέπουν» ο ένας τον άλλον σαν να βρίσκονται στον ίδιο χώρο. Οι εργαζόμενοι μπορούν να επικοινωνούν μεταξύ τους σαν να βρίσκονται στο ίδιο κτίριο. Το TrueSpan συνδέει τις απομακρυσμένες περιοχές μέσω Internet. Αυτή η σύνδεση είναι φθηνότερη, απλούστερη και περισσότερο ευέλικτη από άλλες παραδοσιακές μεθόδους, όπως μισθωμένες γραμμές, κλήσεις μεγάλης απόστασης ή frame relay. Το TrueSpan λειτουργεί με οποιαδήποτε τεχνολογία πρόσβασης στο Internet (DSL, T1 κλπ) και με οποιονδήποτε Internet Service Provider.

Ασφάλεια

Το OpenReach είναι ασφαλές για οτιδήποτε είναι encrypted, tunneled, authenticated και firewalled χρησιμοποιώντας τα ισχυρότερα διαθέσιμα standards.

Ειδικότερα για αυθεντικοποίηση χρησιμοποιεί ψηφιακά πιστοποιητικά.

Ένα ψηφιακό πιστοποιητικό:

- Παρέχει πιστοποίηση και προς τις δύο κατευθύνσεις και εγγυάται για την ταυτότητα και των δύο που βρίσκονται στις άκρες της σύνδεσης.
- Λειτουργεί με διαφάνεια και δεν χρειάζεται οι άνθρωποι να μαθαίνουν τον κωδικό ενός νέου χρήστη.
- Κάνει έλεγχο αυθεντικότητας και για τους δύο απομακρυσμένους χρήστες και τοποθεσίες και εγγυάται ασφάλεια για όλες τις εφαρμογές δικτύου ευρείας περιοχής.

Εγκατάσταση

Η εγκατάσταση του OpenReach TrueSpan Network είναι απλή. Επισκέπτεστε το site του OpenReach (www.openreach.com) και κατεβάζετε το software σε μια δισκέτα.

Τοποθετείτε τη δισκέτα στο διαθέσιμο PC και κάνετε επανεκκίνηση. Το PC επικοινωνεί με έναν VPN router, συνδέεται στο OpenReach Network, κατεβάζει κάποια συμπληρωματικά στοιχεία και ρυθμίζει κάποιες παραμέτρους. Επαναλαμβάνετε αυτή τη διαδικασία σε κάθε θέση και μπορείτε να χρησιμοποιήσετε τη διαμόρφωση του OpenReach web site για την ασφαλή επικοινωνία και σύνδεση μεταξύ των γραφείων.

6.4.2 Virtela Communications

Η Virtela δημιούργησε ένα πολύ προνομιούχο IP VPN Network στη βιομηχανία. Οι κατασκευαστές του Virtela εργάστηκαν από τις αρχές της δεκαετίας του '90 για να σχεδιάσουν και να θεμελιώσουν τα μεγαλύτερα IP Networks. Θεωρούνται πολύ καλοί στον τομέα τους και το αποτέλεσμα ικανοποιεί και τους πιο απαιτητικούς πελάτες.

Προσφέρει μια αποτελεσματική IP VPN λύση για ασφαλή και αξιόπιστη επικοινωνία μιας επιχείρησης. Περιλαμβάνει μεταφορά δεδομένων, φωνής και βίντεο. Παρέχει μια ολοκληρωμένη end-to-end λύση διαχειριζόμενη όλο τον εξοπλισμό, τις υπηρεσίες και τα IP ports. Παρέχει στους πελάτες της όλα τα πλεονεκτήματα του Internet και μια ασφαλή και ευέλικτη IP VPN λύση. Οι πελάτες μπορούν να επιλέξουν από μια ποικιλία μεθόδων σύνδεσης στο Internet ή να χρησιμοποιήσουν την υπάρχουσα πρόσβαση στο Internet με τη μεγαλύτερη δυνατή ευελιξία.

Το πλεονέκτημα του Virtela VPN

Ο Provider IPSF (IP Service Fabric) είναι το βασικό στοιχείο στο οποίο οφείλεται η πιο αποτελεσματική, ασφαλής και αξιόπιστη λύση για VPN. Ο IPSF χρησιμοποιεί τριπλή DES κρυπτογράφηση, firewalls δικτύου, virus detection, Network Address Translation (NAT)/Port Address Translation (PAT), Remote Authentication Dial-In User Service (RADIUS), secure ID κλπ. εξασφαλίζοντας μεγαλύτερη αξιοπιστία από οποιονδήποτε άλλον service provider. Η Virtela μπορεί γρήγορα να προμηθεύσει τους πελάτες της με μια μεγάλη κλίμακα νέων υπηρεσιών και τεχνολογιών χωρίς επιπλέον κόστος και πρόσθετο hardware.

Network Enabled VPN

Κάθε Virtela Network Enables VPN πλεονεκτεί στο ότι η διαχείριση και ο έλεγχος γίνονται κεντρικά. Η διαχείριση του κάθε πελάτη γίνεται κεντρικά, στον πυρήνα του Virtela Network, στο Virtela Network Operations Center (NOC).

Το Virtela Network Enabled VPN προσφέρει ασφάλεια και αξιοπιστία στο χαμηλότερο κόστος από όλα τα παραδοσιακά VPNs. Υποστηρίζει ένα μεγάλο εύρος μεθόδων πρόσβασης, συμπεριλαμβανομένης της DirectVPN Access, CPE VPN Access και Secure Remote VPN Access. Η Direct VPN Access και η CPE VPN Access

προσφέρουν στις επιχειρήσεις φθηνή, αποτελεσματική και ασφαλή site-to-site επικοινωνία δικτύων.

VirtelaVoice και VirtelaVideo

Η Virtela παρέχει τη δυνατότητα στους πελάτες της να έχουν ασφαλείς και αξιόπιστες κλήσεις, τόσο μέσα στην ίδια την επιχείρηση, όσο και με συνεργάτες τους που βρίσκονται σε απομακρυσμένες περιοχές.

Η Virtela παρέχει στις επιχειρήσεις μία ολοκληρωμένη, χαμηλού κόστους, υψηλής ποιότητας videoconferencing λύση. Υποστηρίζει videoconferencing ανάμεσα σε επιχειρήσεις, αλλά και ανάμεσα στα τμήματα μιας επιχείρησης.

Ο συνδυασμός video και μεταφοράς δεδομένων χρησιμοποιώντας έναν απλό provider πάνω σε μια απλή σύνδεση δικτύου παρέχει αυξημένη ασφάλεια, ευελιξία, ευκολία στη διαχείριση, επεκτασιμότητα και αισθητή μείωση του κόστους. Η VirtelaVideo παρέχει IP videoconferencing χωρίς χρονικούς περιορισμούς.

- Standard IP video conferencing

Τα χαρακτηριστικά του είναι: TV-quality video, advanced web management interface, full duplex audio, control από απόσταση. Στο Standard IP video η ταχύτητα μετάδοσης είναι 768/kbps.

- Prenium IP video conferencing

Το Prenium IP video conferencing έχει όλα τα χαρακτηριστικά του Prenium IP video, αλλά έχει επιπλέον τη δυνατότητα μετάδοσης περισσότερων από 2 Mbps. Ακόμη οι επιχειρήσεις μπορούν να συνδεθούν με περισσότερα από τέσσερα sites στα 384kbps ή με τρία sites στα 512kbps.

Ασφάλεια

Οι εταιρείες χρειάζονταν πάντα έναν ασφαλή τρόπο επικοινωνίας. Για να πετύχουν αυτή την επικοινωνία μίσθωναν γραμμές, επιβάρυναν οικονομικά αυτούς που επικοινωνούσαν μαζί τους ή πρόσφεραν ατελώς αυτή την υπηρεσία. Καθεμιά απ' αυτές τις λύσεις έχει αρκετό οικονομικό κόστος και δύσκολη διαχείριση.

Σε ένα Virtela VPN τα στοιχεία που διακινούνται στο δίκτυο φθάνουν πρώτα στον Virtela Service POP και στη συνέχεια γίνεται έλεγχος ασφάλειας από τον IP Service Fabric (IPSF). Χρησιμοποιείται Triple DES encryption, network firewalls, virus detection, Network Address Translation (NAT)/Prot Address Translation (PAT) και έλεγχος αυθεντικότητας του χρήστη Lightweight Directory Access Protocol [LDAP], Remote authentication Dial-In User Service [RADIUS], SecurID κλπ.

6.4.3 GoToMyPC

Το GoToMyPC της εταιρίας Expertcity είναι ένα software το οποίο επιτρέπει στους χρήστες να έχουν πρόσβαση και να εργάζονται σε οποιοδήποτε PC έχει συνδεθεί με το GoToMyPC Web site, (www.gotomypc.com). Με το GoToMyPC, μπορούν να δουν την οθόνη του Η/Υ με τον οποίο είναι συνδεδεμένοι και να χρησιμοποιήσουν τα προγράμματα και τα αρχεία σαν να ήταν σε τοπικό δίκτυο, ακόμα κι αν βρίσκονται χιλιάδες χιλιόμετρα μακριά.

☑ Εγκατάσταση

Η εγκατάσταση είναι απλή. Απλώς εγγράφεστε στο site www.gotomypc.com, κατεβάζετε το host και επιλέγετε ID. Ο host computer πρέπει να είναι μόνιμα συνδεδεμένος, αλλά όχι οι υπόλοιποι υπολογιστές. Για να συνδεθείς πρέπει να επισκεφτείς το www.gotomypc.com και να επιλέξετε το host PC.

Όλες οι συνδέσεις περνάνε από τους ασφαλείς servers επικοινωνίας Expertcity.com. Το GoToMyPC χρησιμοποιεί end-to-end 128bit encryption και password authentication.

☑ Ελάχιστες τεχνικές προδιαγραφές

- Microsoft Windows 95, 98, 2000, Me ή NT4.0
- Host PC: 300MHz επεξεργαστή ή καλύτερο, μόνιμη σύνδεση στο Internet.
- Απλό PC: 28.8kbps modem ή πιο γρήγορο, Internet Explorer ή Netscape Navigator 4.0 ή μεταγενέστερο.

☑ Πλεονεκτήματα

Το GoToMyPC επιτρέπει την πρόσβαση και τον έλεγχο του host computer από οποιονδήποτε άλλον υπολογιστή που είναι συνδεδεμένος στο Internet χωρίς να χρειάζεται να εγκατασταθεί κάποιο software.

Οι απομακρυσμένοι χρήστες συνδέονται με το GoToMyPC Web site και έχουν στη διάθεση τους τη λίστα με όλους τους υπολογιστές με τους οποίους μπορούν να συνδεθούν με ασφάλεια. Δεν χρειάζεται να θυμούνται τίποτα περισσότερο, παρά μόνο το δικό τους user name και τον κωδικό πρόσβασης στον υπολογιστή.

Το GoToMyPC δεν επηρεάζεται καθόλου από θέματα NAT.

Επιτρέπει τη χρήση όλων των πρωτοκόλλων που υποστηρίζονται από τον host computer.

Επειδή η εφαρμογή τρέχει στον host computer ο οποίος είναι στο LAN, οι χρήστες έχουν την αίσθηση ότι πράγματι βρίσκονται στο τοπικό δίκτυο της επιχείρησης.

Το GoToMyPC χρειάζεται password authentication για να μπορεί ο χρήστης να έχει πρόσβαση στο GoToMyPC Web site. Όταν συνδεθεί ο χρήστης έχει τη δυνατότητα να δει τη λίστα με όλους τους υπολογιστές με τους οποίους μπορεί να συνδεθεί. Εάν επιπλέον θέλει να έχει τον έλεγχο κάποιου υπολογιστή, πρέπει να γνωρίζει τον κωδικό του μηχανήματος. (Να σημειώσουμε ότι οι κωδικοί των μηχανημάτων δεν στέλνονται ποτέ μέσω του δικτύου, ούτε κρυπτογραφημένοι).

Το GoToMyPC παρέχει ιδιαίτερη ασφάλεια γιατί ο απομακρυσμένος υπολογιστής δεν είναι ποτέ μέρος του δικτύου, οπότε και να υπάρχει πρόβλημα με κάποιον ιό, αυτό δεν μεταφέρεται στο δίκτυο. Όλοι οι απομακρυσμένοι υπολογιστές έχουν ένα ασφαλές κανάλι για να επικοινωνούν με τους άλλους υπολογιστές του δικτύου.

Το GoToMyPC δεν προσφέρεται για ασφαλή επικοινωνία μεταξύ γραφείων. Υπάρχει ο μηχανισμός ο οποίος επιτρέπει την ασφαλή επικοινωνία μεταξύ host computer και client computer, αλλά όχι μεταξύ των χρηστών.

6.4.4 WorldCom

Η WorldCom δημιούργησε τρεις τύπους VPN. Δίνει τη δυνατότητα σε κάθε εταιρία να επιλέξει το VPN που ταιριάζει στις ανάγκες της. Οι τρεις αυτοί τύποι είναι:

1. Fully managed: είναι η λύση που προσφέρει ασφαλή σύνδεση με το Internet.
2. Customer Directed: Μία site to site VPN λύση που προσφέρει τη δυνατότητα για αυξημένο έλεγχο και αρκετή ευελιξία.
3. Customer Managed: Μία end-to-end λύση.

☒ Fully Managed

Οι εταιρίες οι οποίες διατηρούν γραφεία σε όλες τις πόλεις μιας χώρας, αλλά πολλές φορές και σε ολόκληρο τον κόσμο, ενδιαφέρονται για μια οικονομική και ασφαλή επικοινωνία μεταξύ τους. Δεν είναι βέβαια επιθυμητό να μεταφέρονται στοιχεία που αφορούν την εταιρία, μέσω του Internet

Για αυτές τις περιπτώσεις προσφέρεται το VPN Fully Managed της WorldCom. Προσφέρει:

- Ευελιξία: η ποικιλία των μεθόδων πρόσβασης, το εύρος των ταχυτήτων (από 56kbps μέχρι 115Mbps)
- Ασφάλεια: Κρυπτογράφηση και έλεγχος αυθεντικότητας
- Scalability: Απλή εγκατάσταση, ρύθμιση και επαναρύθμιση εάν χρειαστεί να μεγαλώσει το δίκτυο.
- Ευκολία στη χρήση.
- Απλότητα.

Customer Directed

Το Customer Directed Service δίνει τη δυνατότητα στα γραφεία μιας εταιρίας, στους συνεργάτες τους, στους προμηθευτές κλπ να επικοινωνούν μεταξύ τους και να ανταλλάσουν πληροφορίες με ασφάλεια μέσω του Internet.

Το Customer Directed προσφέρει:

- Ασφάλεια: Internet Protocol Security (IPSec), DES/3DES (data encryption standard), Cisco IOS firewall και IKE Authentication Integration.
- Ευκολία στη χρήση: Είναι σχεδιασμένο έτσι ώστε να μπορεί κάποιος να το χρησιμοποιήσει χωρίς να χρειάζεται να έχει εμπειρία στη χρήση δικτύων και χωρίς να χρειάζεται να προστεθούν κάποιες συσκευές.
- Ευκολία στον έλεγχο: Είναι εύκολο να το ελέγξει κανείς και να το ρυθμίσει ανάλογα με τις ανάγκες του χωρίς να χρειάζεται να περιμένει να το κάνει κάποια εξωτερική εταιρία.
- Ευελιξία: Είναι πολύ εύκολη η προσαρμογή κάθε φορά στις ανάγκες της εταιρίας.

Customer Managed

Το Customer Managed είναι το VPN που επιτρέπει στον κάτοχο του να έχει εξ ολοκλήρου τον έλεγχο του δικτύου. Παρέχει:

- Ασφάλεια: Standards-based Internet Protocol Security (IPSec), Generic Routing Encapsulation (GRE), 3DES encryption. Είναι ιδανικό για εταιρίες στις οποίες είναι απαγορευτικό να έχουν πρόσβαση στα στοιχεία τους τρίτοι.
- Έλεγχος: Μπορεί κανείς να έχει υπό έλεγχο ολόκληρο το VPN με το Cisco Secure Policy Manager (CSPM) tool.

6.4.5 Sprint

Το Sprint Virtual Private Network Voice μπορεί να διευκολύνει την επικοινωνία συνεργατών που βρίσκονται διασκορπισμένοι σε μία χώρα ή ακόμα και στο εξωτερικό. Ακόμα και συνεργάτες που βρίσκονται σε δύο μόνο διαφορετικά γεωγραφικά σημεία, μπορούν να επωφεληθούν από τα χαρακτηριστικά ενός Sprint VPN for Voice. Διευκολύνει την επικοινωνία εργαζομένων, προμηθευτών, πελατών ανά τον κόσμο. Διευκολύνει επίσης την τηλεφωνική επικοινωνία εξοικονομώντας για την επιχείρηση πολύτιμο χρόνο και χρήμα.

Το Sprint VPN for Voice δίνει τη δυνατότητα να ορίσει κανείς παραμέτρους όπως χρόνο, τόπο, έλεγχο για την αυθεντικότητα αυτού με τον οποίον γίνεται η επικοινωνία. Η επέκταση του σε καινούργιες θέσεις είναι πολύ εύκολη. Είναι λύση που

βασίζεται στο software, γι' αυτό είναι ευέλικτη και μπορεί να προσαρμοστεί πολύ εύκολα στις ανάγκες του πελάτη και να του προσφέρει νέες δυνατότητες.

Η επικοινωνία μεταξύ συνεργατών γίνεται πιο γρήγορα και έτσι εξοικονομείται χρόνος από τις εργασίες ρουτίνας. Ακόμη δεν χρειάζεται επιπλέον εξοπλισμός σε hardware.

Τεχνικά πλεονεκτήματα:

- Μπορούν πολύ εύκολα να προστεθούν νέες θέσεις στο δίκτυο, εάν το απαιτεί η επιχείρηση.
- Υπάρχει η δυνατότητα να δοθούν περισσότεροι από 15 εναλλακτικοί προορισμοί όταν είναι απασχολημένη ή γενικά δεν είναι διαθέσιμη η γραμμή που καλούμε.
- Είναι εύκολη η επέκταση του δικτύου σε ολόκληρο τον κόσμο.
- Δίνει τη δυνατότητα στους εργαζόμενους που μετακινούνται να μπορούν να επικοινωνούν με κινητό τηλέφωνο ή χρησιμοποιώντας την κάρτα Sprint VPN PHONECARD.
- Υπάρχει η δυνατότητα για Videoconference με χαμηλό κόστος.
- Μπορούν να δοθούν κωδικοί στους χρήστες του δικτύου και να έχει ο καθένας πρόσβαση μόνο σε συγκεκριμένες θέσεις. Είναι δυνατόν βάσει του κωδικού να γίνεται έλεγχος των κλήσεων και κατά συνέπεια και οικονομικός έλεγχος της επικοινωνίας.
- Είναι δυνατόν να γίνει ταχύτερο το δίκτυο (high-speed bandwidth) εάν η επιχείρηση το χρειαστεί.

Η Sprint είναι πρωτοπόρος στο χώρο των VPNs. Δημιούργησε το πρώτο Voice VPN το 1985 και εξακολουθεί και σήμερα να κατέχει ηγετική θέση στο χώρο των VPNs.

6.4.6 AT & T Worldnet VPN

Η AT & T δημιούργησε ένα Εικονικό Ιδιωτικό Δίκτυο το οποίο υπόσχεται 99.7% διαθεσιμότητα, οικονομική και αξιόπιστη πρόσβαση μεταξύ συνεργατών, προμηθευτών, εργαζομένων σε LAN, intranets και extranets. Οι επιχειρήσεις που χρησιμοποιούν το AT & T VPN παρέχουν στους χρήστες ασφαλή επικοινωνία μεταξύ τους και υπάρχει η δυνατότητα να έχει κάποιος πρόσβαση σε ένα τμήμα της βάσης δεδομένων. Εγγυάται την καλή λειτουργία του δικτύου και σε περίπτωση που το δίκτυο παρουσιάσει πρόβλημα για περισσότερο από δέκα λεπτά στη διάρκεια μιας μέρας, το AT & T μειώνει την μηνιαία συνδρομή του πελάτη κατά 5%.

Πλεονεκτήματα:

- Είναι γρήγορο, αξιόπιστο και ασφαλές.
- Εγγυάται υψηλή διαθεσιμότητα,99,7%
- Έχει υψηλή ταχύτητα.
- Μπορούν εύκολα να προστεθούν χρήστες, εάν μεγαλώσει η εταιρία, χωρίς να

απαιτείται επιπλέον server.

- Παρέχει πρόσβαση στο δίκτυο από οποιαδήποτε χώρα του κόσμου.
- Είναι εύκολη η διαχείριση του δικτύου και μειώνεται το κόστος υποστήριξης των απομακρυσμένων χρηστών.

Ασφάλεια

RADIUS (Remote Authentication Dial-In User Service) επικυρώνουν την αυθεντικότητα των χρηστών μόλις κάποιος συνδεθεί στο δίκτυο μέσω του CHAP (Challenge Handshake Authentication Protocol). Όλα τα passwords σε κρυπτογραφημένη μορφή. Κάθε χρήστης έχει πρόσβαση μόνο σε συγκεκριμένα sites, σ' αυτά που του επιτρέπει ο διαχειριστής του δικτύου.

6.4.7 Equant

Είναι ένα VPN μέσω του οποίου μπορούν να μεταφερθούν δεδομένα, φωνή και βίντεο.

Υπάρχουν τρεις τύποι που μπορούν να καλύψουν τις ανάγκες κάθε επιχείρησης:

- Silver για sites που δεν χρειάζονται διαφοροποίηση
- Gold για sites που χρειάζονται data traffic differentiation
- Platinum που δίνουν τη δυνατότητα μεταφοράς data και Multimedia (Voice/Video).

Προσφέρει:

- Μεταφορά μέσω του προσωπικού δικτύου (όχι μέσω Internet) για μεγαλύτερη αξιοπιστία.
- Εξοικονόμηση χρημάτων γιατί το κόστος των υπηρεσιών του δικτύου είναι μικρότερο.
- Μεταφορά φωνής και fax σε 65 χώρες που μπορούν να είναι συνδεδεμένες στο δίκτυο και σε 240 εκτός δικτύου.
- Σχεδιάστηκε για επιχειρήσεις και η διαχείριση του γίνεται από την Equant με τα υψηλότερα standards.
- Επεκτείνεται εύκολα εάν διευρυνθεί η επιχείρηση.
- Αύξηση της παραγωγικότητας γιατί με την εύκολη και οικονομική επικοινωνία μεταξύ των μελών της επιχείρησης διευκολύνεται η συνεργασία.
- Καλύτερο έλεγχο των εξόδων για επικοινωνία με τις λεπτομερείς αναφορές που μπορεί να δώσει το δίκτυο, βάσει των κωδικών των χρηστών.
- Ασφάλεια: προσφέρει firewall, anti-virus protection, authentication, IPsec, encryption και Intrusion Detection για αποφυγή εισβολέων.

6.5 ΣΥΓΚΡΙΤΙΚΟΣ ΠΙΝΑΚΑΣ ΤΩΝ ΤΥΠΩΝ VPN

	TRUESPAN	VIRTELA	GOTOMY PC	WORLDCOM			SPRINT	AT & T	EQUANT
				FULLY MANAGED	CUSTOMER DIRECTED	CUSTOMER MANAGED			
ΤΗΡΙΑ:									
ΦΑΛΕΙΑ	encryption, authentication (digital certificates), firewall	3 DES encryption, firewall, NAT, PAT, RADIUS	encryption, password authentication	encryption, authentication	IPSec, Cisco IOS firewall, 3DES, IKE authentication integration	IPSec, rooting encapsulation, 3 DES	firewall, Intrusion Detection*, authentication, e-mail protection	RADIUS, CHAP	firewall, anti-virus protection, authentication, IPSec, encryption, Intrusion Detection*
ΚΟΛΙΕΣ ΟΠΟΙ-ΗΣ	εύκολο εγκατάσταση μέσω επίσκεψης στο site	εύκολο εγκατάστα-ση από το site. Επιλογή --> VirtelaView	εύκολο εγγραφή στο site και επιλογή host name και ID	εύκολο εγκατάσταση από το site			μέτριο βασίζεται σε software που προσαρμό-ζεται στις ανάγκες του πελάτη	εύκολο εγκατά-σταση από το site	εύκολο εγκατάστα-ση από το site
ΣΚΟΛΙΑ ΕΚΤΑΣΙ-ΟΤΗΤΑΣ	εύκολο επίσκεψη στο site	εύκολο από το site. Επιλογή --> VirtelaView	δύσκολο επαναρύ-θμιση δικτύου	εύκολο επίσκεψη στο site			εύκολο	εύκολο δεν απαιτείται επιπλέον server	εύκολο
ΙΒΕΛΕΙΑ	παγκόσμια	παγκόσμια	παγκόσμια	παγκόσμια			παγκόσμια	παγκόσμια	voice & data σε 65 συνδεδεμέ-νες χώρες και σε 240 εκτός δικτύου
ΠΑΙΤΗ-ΕΙΣ ARD-ARE	Pentium 200 MHz, RAM 32 MB, Hard Disc 100MB, κάρτα Ethernet		Host PC: Pentium 300MHz, RAM 64MB, Internet Explorer ή Netscape Navigator 4.0, σύνδεση στο Internet Απλά PC: Modem 28,8 Kbps, Internet Explorer ή Netscape Navigator 4.0						
ΥΝΑΤΟ-ΗΤΕΣ	voice	voice, video	voice	voice, video			voice, video	voice	voice, video

6.6 ΑΝΑΦΟΡΑ ΣΤΗΝ ΕΛΛΗΝΙΚΗ ΠΡΑΓΜΑΤΙΚΟΤΗΤΑ

Τα VPNs έχουν αρχίσει να κάνουν αισθητή την παρουσία τους και στην Ελλάδα μέσω κάποιων παροχέων Internet. Συγκεκριμένα εφαρμογές VPN παρέχουν η FORTHnet, η Internet Hellas, η ACN, η Otenet και η HellasOnline, και η καθεμιά τους προσφέρει στους χρήστες έναν αριθμό επιλογών σχετικά με την τεχνολογία υλοποίησης αλλά και την ποιότητα των προσφερόμενων υπηρεσιών.

Το κόστος για τις υπηρεσίες που προσφέρουν οι παραπάνω Providers εξαρτάται από κριτήρια όπως τον αριθμό των κόμβων του VPN, την απόσταση μεταξύ των κόμβων, τον αριθμό των χρηστών του VPN, το μέγεθος των πληροφοριών που θα διακινούνται κ.α.

Επίσης στο συνολικό κόστος σημαντικό ρόλο παίζει αν ο ISP θα παρέχει software και hardware για την επιθυμητή ασφάλεια του δικτύου ή αν θα τα διαθέτει και θα τα διαχειρίζεται η εταιρεία.

6.7 ΒΙΒΛΙΟΓΡΑΦΙΑ

ΔΙΕΥΘΥΝΣΕΙΣ ΣΤΟ INTERNET

www.conta.uom.gr

www.forthnet.gr

www.acn.gr

www.InternetHellas.gr

web.hol.gr

www.virtela.net

www.gotomypc.com

www.worldcom.com

www.openreach.com

www.microsoft.com

www.equant.com

www.spintbiz.com

ΓΛΩΣΣΑΡΙΟ

A

AHP Πρωτόκολλο (Authentication Header Protocol - Επικεφαλίδα Πιστοποίησης) πρωτόκολλο που παρέχει μια επιπλέον επικεφαλίδα μεταξύ των επικεφαλίδων των επιπέδων IP και μεταφοράς, η οποία περιέχει κάποια δεδομένα αυθεντικοποίησης, τα οποία ο αποδέκτης επαληθεύει, ώστε να διαπιστώσει αν ο αποστολέας ήταν πράγματι αυτός που ισχυρίζεται πως ήταν.

Application Level Gateways (Πύλες επιπέδου εφαρμογής), που ονομάζονται επίσης και πληρεξούσιοι εξυπηρετητές **(proxy servers)**, είναι τύπος firewall και λειτουργούν ως αναμεταδότες της κίνησης στο επίπεδο εφαρμογής του OSI.

B

Bastion hosts (Επάλξεις) είναι μηχανές που έχουν αναγνωρισθεί από τον υπεύθυνο ασφάλειας του δικτύου ως ισχυρά και κρίσιμα σημεία για την ασφάλεια του δικτύου.

Black box είναι μία συσκευή με το απαραίτητο λογισμικό για να δημιουργήσουμε ένα tunnel.

Block Cipher είναι ένας αλγόριθμος κρυπτογράφησης ο οποίος επαναλαμβάνει διάφορες λειτουργίες όπως αντικατάσταση, μετάθεση, πολλαπλασιασμό, και γραμμικούς μετασχηματισμούς δημιουργώντας έτσι ένα πολύ πιο δυνατό αλγόριθμο. Η αποκρυπτογράφηση αυτής της μεθόδου γίνεται με τον αντίστροφο αλγόριθμο της κρυπτογράφησης.

C

Certificate Authority - CA (Αρχή Πιστοποίησης) είναι ένα ψηφιακό πιστοποιητικό, το οποίο χρησιμοποιείται για πιστοποίηση από τον server πιστοποίησης της εταιρείας.

Challenge-Handshake Authentication Protocol (CHAP) Πρωτόκολλο πρόκλησης πιστοποίησης ταυτότητας χειραψιών είναι μια μεθόδος πιστοποίησης ταυτότητας που χρησιμοποιεί το σύστημα μοιραζόμενου κλειδιού (shared key). Το CHAP είναι ένας μηχανισμός πιστοποίησης του client που χρησιμοποιεί την κρυπτογραφία ώστε να αποφεύγεται η μεταφορά του πραγματικού password κατά την σύνδεση.

Chokes είναι συσκευές επικοινωνίας ή υπολογιστικά συστήματα που σαν στόχο έχουν τον περιορισμό της ροής των πακέτων μεταξύ των δικτύων.

Circuit Level Gateway (Πύλη επιπέδου κυκλώματος) είναι τύπος firewall που μπορεί να είναι ένα αυτόνομο σύστημα ή μπορεί να είναι μια ειδική λειτουργία που εκτελείται από μια πύλη επιπέδου εφαρμογής για συγκεκριμένες εφαρμογές.

D

Data Encryption Standards (DES) είναι ένας αλγόριθμος κρυπτογράφησης ο οποίος χρησιμοποιεί 64 bit μέγεθος block και ένα κλειδί 56bit.

Default Deny στρατηγική καθορισμού πολιτικής firewall, με αυτή τη στρατηγική περιγράφουμε συγκεκριμένα πρωτόκολλα τα οποία μπορούν να περάσουν από το firewall και συγκεκριμένους υπολογιστές που μπορούν να διακινήσουν δεδομένα και να επικοινωνήσουν με το εσωτερικό δίκτυο—όλοι οι άλλοι υπολογιστές και πρωτόκολλα απορρίπτονται.

Default Permit στρατηγική καθορισμού πολιτικής firewall, με αυτή τη στρατηγική δίνουμε στο firewall ένα σύνολο προϋποθέσεων αποτέλεσμα των οποίων θα είναι το μπλοκάρισμα κάποιων δεδομένων. Κάθε υπολογιστής ή πρωτόκολλο το οποίο καλύπτεται από αυτές τις προϋποθέσεις περνάει χωρίς επιπλοκές και άλλες διαδικασίες.

Diffie- Hellman (DH) είναι σύστημα δημόσιου κλειδιού που χρησιμοποιούνται στα VPN.

Digital IDs (Ψηφιακές Ταυτότητες), ή Digital certificats (Ψηφιακές Βεβαιώσεις) είναι «ταυτότητες» που εκδίδονται από οργανισμούς πιστοποίησης (TTP ή certification authorities – CA) και επιβεβαιώνουν ότι ο παρέχων τα προσωπικά του στοιχεία και το δημόσιο κλειδί του στο Διαδίκτυο είναι ο αυθεντικός και νόμιμος κάτοχος.

DMZ (Δίκτυο περιμετρικής ζώνης). Μια περιμετρική ζώνη απομονώνει τους hosts που είναι προσιτοί από το εξωτερικό περιβάλλον του δικτύου (π.χ. έναν web server ή έναν ftp server) από τους εσωτερικούς servers. Οι εξωτερικοί hosts είναι τοποθετημένοι σε μια ξεχωριστή ζώνη του δικτύου, σε έναν ξεχωριστό προσαρμογέα που είναι συνδεδεμένος με firewall.

E

ESP Πρωτόκολλο (Encapsulating Security Payload Protocol - Ενσωμάτωση Επικεφαλίδας Ασφαλείας), στο πρωτόκολλο αύτό χρησιμοποιείται για να κρυπτογραφήσει και να ενσωματώσει είτε μόνο το περιεχόμενο επιπέδου μεταφοράς είτε ολόκληρο το πακέτο IP, ανάλογα με τον τρόπο χρήσης.

F

Firewall (δικτυακό ανάχωμα) είναι ένα φράγμα μεταξύ ενός ιδιωτικού και προστατευόμενου δικτύου (το οποίο υποθέτουμε ότι είναι ασφαλές) και ενός άλλου δικτύου συνήθως δημόσιου, όπως το Internet (το οποίο υποθέτουμε ότι δεν είναι ασφαλές). Ο σκοπός ενός Firewall είναι να εμποδίσει την ανεπιθύμητη και μη εξουσιοδοτημένη επικοινωνία προς ή από το προστατευόμενο δίκτυο.

G

Gates είναι ειδικά σχεδιασμένα προγράμματα, συσκευές ή υπολογιστές μέσα στην περίμετρο του firewall οι οποίες λαμβάνουν συνδέσεις από έξω και τις διαχειρίζονται κατάλληλα.

H

Hash Functions (Συναρτήσεις Κατακερματισμού) είναι συναρτήσεις κρυπτογράφησης οι οποίες παίρνουν ένα μεταβλητού μεγέθους μήνυμα και μας δίνουν ένα fixed length μήνυμα, συνήθως 128 bit ή περισσότερα, το οποίο αναφέρεται σαν hash τιμή. Οι hash συναρτήσεις είναι μονόδρομες (one way) δηλαδή είναι πολύ δύσκολο να βρεθεί η αντίστροφη συνάρτηση τους και άρα να σπάσουν.

Hash αλγόριθμοι χρησιμοποιούνται για να παρέχουν ένα ψηφιακό δακτυλικό αποτύπωμα του περιεχομένου ενός αρχείου, που χρησιμοποιείται συχνά για να εξασφαλίσει ότι το αρχείο δεν έχει αλλάξει από έναν εισβολέα ή έναν ιό. Οι Hash λειτουργίες υιοθετούνται συνήθως από πολλά λειτουργικά συστήματα για να κρυπτογραφήσουν τους κωδικούς πρόσβασης.

I

IKMP Πρωτόκολλο (Internet Key Management Protocol) εγκαθιστά και συντηρεί τις συνάψεις ασφάλειας που θα χρησιμοποιήσουν τα πρωτόκολλα AHP και ESP.

Internet Key Exchange (IKE), μετονομασία του ISAKMP πρωτόκολλο.

Internet Security Association Key Management Protocol (ISAKMP), πρωτόκολλο που χρησιμοποιείται για τη διαπραγμάτευση αμοιβαία υποστηριζόμενων αλγόριθμων και μαθηματικών δομών για την ανταλλαγή κλειδιών Diffie - Hellman και το επακόλουθο βήμα αυθεντικοποίησης.

IP (Internet Protocol) ή IPSec είναι μια σειρά διάταξης των προτάσεων από το IETF (Internet Engineering Task Force) περιγράφοντας ένα ασφαλές πρωτόκολλο IP για IPv4 και IPv6. Αυτές οι επεκτάσεις θα παρείχαν την κρυπτογράφηση στο επίπεδο IP, παρά στα υψηλότερα επίπεδα που η SSL (Secure Socket Layer)που τα περισσότερα πακέτα VPN παρέχουν.

L

Layer 2 Forwarding Protocol (L2F) πρωτόκολλο που δημιουργεί ένα εικονικό dial-up (virtual) σενάριο όπου οποιοδήποτε από τα μη-IP πρωτόκολλα να μπορεί να χρησιμοποιεί τα πλεονεκτήματα που παρέχει το Internet σε συνδυασμό με το PPTP.

Layer 2 Tunneling Protocol (L2TP) είναι ένα επιπέδου-2 πρωτόκολλο σχεδιασμένο για το encapsulation στο επίπεδο-2. Παρέχει συμπίεση βασισμένη στο λογισμικό η οποία συμπυκνώνει τα πακέτα των χρηστών. Επίσης, ένας μικρός αριθμός τεχνικών συμπίεσης έχει προστεθεί στο επίπεδο της κρυπτογράφησης.

M

Microsoft Challenge-Handshake Authentication Protocol. Το MS-CHAP είναι ένας μηχανισμός πιστοποίησης που επιτρέπει στον server να αποθηκεύει τα passwords κωδικοποιημένα. Επίσης παρέχει επιπλέον κώδικες διόρθωσης λαθών, έλεγχο για ληγμένα passwords και μηνύματα που επιτρέπουν στους χρήστες την αλλαγή του password.

N

NAT (Network Address Translation). Το σύστημα NAT λειτουργεί σε κάποιον δρομολογητή, ο οποίος συνδέει συνήθως δύο δίκτυα και μεταφράζει τις ιδιωτικές (μη μοναδικές στον παγκόσμιο ιστό) διευθύνσεις του εσωτερικού δικτύου σε νόμιμες διευθύνσεις προτού τα πακέτα προωθηθούν σε άλλο δίκτυο.

Network Client Software είναι πρόγραμμα όπως τα ftp, telnet και mosaic που μπορούν να τρέξουν στα Gates μηχανήματα.

NT servers είανι κεντρικοί υπολογιστές με δύο προσαρμοστές δικτύων.

P

Packet Filtering Router (Δρομολογητής φιλτραρίσματος πακέτων) είναι τύπος firewall που εφαρμόζει ένα σύνολο κανόνων σε κάθε εισερχόμενο πακέτο IP και στη συνέχεια προωθεί ή απορρίπτει το πακέτο.

Password Authentication Protocol-PAP είναι ένα απλό πρόγραμμα πιστοποίησης. Ο NAS ζητά το όνομα του χρήστη (user name) και το password και αφού ο PAP τα επεξεργαστεί τα επιστρέφει σε απλό κείμενο (μη κρυπτογραφημένο).

Point-to-Point Protocol (PPP) αποστέλλει δεδομένα μεταξύ dial-up ή μισθωμένων point-to-point συνδέσεων. Το PPP ενσωματώνει IP, IPX και NetBEUI πακέτα μέσα σε PPP πλαίσια και έπειτα αποστέλλει τα PPP ενσωματωμένα πακέτα που προέκυψαν σε μια point-to-point σύνδεση.

POPs σημεία παρουσίας παροχέα Internet

Point-to-Point Tunneling Protocol (PPTP) είναι ένας συνδυασμός του Point-to-Point Protocol και του Transmission Control Protocol / Internet Protocol (TCP/IP). Το PPTP μπορεί να πάρει πακέτα όπως IP, IPX, NetBios, SNA και να τα μετατρέψει σε ένα καινούριο IP πακέτο για μεταφορά.

Prety Good Privacy (PGP), είναι μία ευρέως αποδεκτή τεχνολογία κρυπτογράφησης, γνωστή ως «public key cryptography» στην οποία δύο αλληλοσυμπληρωματικοί κωδικοί χρησιμοποιούνται για να διατηρηθούν ασφαλείς οι επικοινωνίες.

Private Key είναι αλγόριθμος κρυπτογράφησης όπου ο αποστολέας και ο παραλήπτης ενός κειμένου χρησιμοποιούν το ίδιο κλειδί το οποίο μόνο αυτοί οι δύο γνωρίζουν (ιδιωτικό κλειδί).

Proxies είναι μια κοινή μέθοδος προστασίας ενός δικτύου η οποία επιτρέπει την πρόσβαση στις υπηρεσίες VPN. Οι κεντρικοί υπολογιστές proxies είναι χαρακτηριστικά μια λύση λογισμικού που τρέχει μέσω ενός λειτουργικού συστήματος δικτύου, όπως

το Unix, τα Windows NT, ή το Novell Netware.

Public key κρυπτογραφική μέθοδο δημόσιου κλειδιού όπου ο αποστολέας και ο παραλήπτης έχουν από ένα public και ένα private κλειδί. Το public κλειδί είναι σε όλους γνωστό (μπορεί να βρεθεί σε διάφορα ευρετήρια), ενώ το private κλειδί το γνωρίζει μόνο ο κάτοχός του.

Public Key Infrastructure (PKI) είναι ένα σύστημα ψηφιακών πιστοποιήσεων (digital certificates), πιστοποιήσεων εξουσιών (authorities certificates), πιστοποιήσεων διαχείρισης υπηρεσιών (certificate management services), και directory services (LDAP, X.500) το οποίο εξακριβώνει την ταυτότητα και την εξουσία του κάθε χρήστη που λαμβάνει μέρος σε κάθε συναλλαγή στο Διαδίκτυο.

Q

QoS – Quality of Service (Εγγύηση Ποιότητας Υπηρεσιών) είναι μια συμφωνία μεταξύ ενός πελάτη και ενός ISP που εγγυάται ένα ορισμένο ποσοστό διαθεσιμότητας και ορισμένο εύρος ζώνης ISP στο δίκτυο. Τυπικά η εγγύηση της ποιότητας των υπηρεσιών εγγυάται ένα ορισμένο ποσοστό λανθάνουσας κατάστασης για την κυκλοφορία του χρήστη στο ISP δίκτυο, που μετριέται τυπικά σε δεκάδες χιλιοστά του δευτερολέπτου.

R

Rivest Shamir Adlemen (RSA) Αλγόριθμος δημόσιου κλειδιού είναι σύστημα δημόσιου κλειδιού που χρησιμοποιούνται στα VPN και χρησιμοποιεί δύο μαθηματικές φόρμουλες.

Router είναι συσκευές των οποίων η χρήση επιτυγχάνει τη σύνδεση δύο δικτύων μεταξύ τους.

S

Secure Socket Layer (SSL) πρωτόκολλο ασφάλειας το οποίο εξασφαλίζει την απόκρυψη όλων των δεδομένων που διακινούνται προς και από τον server με χρήση της τεχνολογίας κρυπτογράφησης.

Secure Wide Area Network (S/WAN) πρωτόκολλο είναι ένα πρωτόκολλο το οποίο παρέχει ενδολειτουργικότητα. Ακόμη αυτό το πρωτόκολλο δεν έχει υλοποιηθεί.

Service Level Agreements (SLAs) είναι ειδικές συμφωνίες μεταξύ του χρήστη και του ISP, που περιέχουν τις απαιτήσεις του πρώτου και τις αντίστοιχες δεσμεύσεις του δεύτερου.

T

Tunnel (σήραγγα) είναι ένας όρος δικτύωσης με ένα κατάλληλο όνομα. Αναφέρεται σε μια σύνδεση, κρυπτογραφημένη συνήθως, η οποία συνδέει δύο υπολογιστές μαζί μέσω ενός άλλου, συνήθως μη-έμπιστο δίκτυο.

V

Virtual Private Network - VPN (Εικονικό Ιδιωτικό Δίκτυο). Τα VPNs επιτρέπουν σε απομακρυσμένους χρήστες όπως πωλητές ή και σε υποκαταστήματα κάποιας εταιρίας (clients) να συνδέονται με ασφαλή τρόπο στον κεντρικό server ο οποίος είναι τοποθετημένος στην άκρη του τοπικού δικτύου (Local Area Network-LAN), χρησιμοποιώντας την υποδομή που παρέχεται από το δημόσιο δίκτυο (π.χ. Internet).

W

Web hosting, είναι η υπενοικίαση ηλεκτρονικού χώρου, που καλύπτει τη στέγαση, την εξυπηρέτηση και τη συντήρηση του ηλεκτρονικού καταστήματος.

ΚΑΤΑΣΤΑΣΗ ΣΧΗΜΑΤΩΝ