ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΟΙΚΟΝΟΜΙΚΩΝ ΚΑΙ ΚΟΙΝΩΝΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΕΙΔΙΚΑ ΣΕΜΙΝΑΡΙΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Virtual Private Networks
(Εικονικά Ιδιωτικά Δίκτυα)

Καθηγητής: Οικονομίδης Αναστάσιος

Φοιτητής: Βλαχόπουλος Σπύρος

ΘΕΣΣΑΛΟΝΙΚΗ 2002

ΠΕΡΙΕΧΟΜΕΝΑ

Σελ.

ΟΡΙΣΜΟΣ

Τα Ιδιωτικά Εικονικά Δίκτυα (Virtual Private Networks ή VPN) αποτελούν ασφαλείς ιδιωτικές συνδέσεις χτισμένες πάνω σε προσιτή από το κοινό υποδομή, όπως το διαδίκτυο ή το τηλεφωνικό δίκτυο. Τα VPN διακατέχονται από ένα συνδυασμό κωδικοποίησης απόκρυψης, ψηφιακών πιστοποιητικών, αυστηρότητα στην αναγνώριση χρήστη (user authentication) και στον έλεγχο πρόσβασης, έτσι ώστε να αποδώσουν ασφάλεια στα δεδομένα που διακινούν.

ΙΣΤΟΡΙΑ

Η τεχνολογία των Εικονικών Ιδιωτικών Δικτύων (**Virtual Private Networking, VPN**) αν και αντικειμενικά καινούργια έλαβε πολύ γρήγορα μεγάλες διαστάσεις στην αγορά των δικτύων. Η τεχνολογία **VPN** πρωτοϋιοθετήθηκε από κάποιους που χρησιμοποίησαν την τεχνολογία για να προσφέρουν ελεύθερα δοκιμαστικά προϊόντα (trials) κι έτσι να ενημερώσουν το κοινό περί του σχεδίου αυτού. Εφόσον η επιχειρηματική κοινωνία αναζητούσε έναν οικονομικό και ασφαλή τρόπο για να συνδέσει τις σελίδες της, πολλοί εμπορικοί οίκοι ξεκίνησαν να χρησιμοποιούν αυτήν την καινούργια τεχνολογία. Με αργά βήματα επέκτειναν αυτήν την υποδομή με στόχο να διευκολύνουν τους υπαλλήλους τους να συνδεθούν στην εταιρική σελίδα από τα σπίτια τους ή και κατά την διάρκεια ταξιδιών. Αυτό προετοίμασε τον δρόμο για την δεύτερη φάση της ανάπτυξης των Ιδιωτικών Εικονικών Δικτύων. Η τεχνολογία εφαρμόστηκε σε κάποιες όχι και τόσο κρίσιμες εφαρμογές και αργότερα σε άλλες κατεξοχήν σημαντικές, οι οποίες απαιτούσαν ανυπέρβλητη ασφάλεια στις πληροφορίες που περιείχαν. Οι ποικίλες φάσεις της ανάπτυξης της τεχνολογίας **VPN** παραθέτονται στον παρακάτω πίνακα:

ΧΡΟΝΙΚΟ ΠΛΑΙΣΙΟ	ΦΑΣΗ ΑΓΟΡΑΣ	ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΑΓΟΡΑΣ
	ΦΑΣΗ 1η : Πρώιμοι ενστερνιστές	• Δοκιμαστικά υπηρεσιών • Τηλεταξιδευτές (Telecommuters) • Ad-hoc employment
1998	ΦΑΣΗ 2η : ΚΛΗΣΗ ΑΠΟ ΕΞΩΤΕΡΙΚΟΥΣ ΕΡΓΑΖΟΜΕΝΟΥΣ	• Εργαζόμενοι από το σπίτι • Κινητές μονάδες εργαζομένων • Παραδοσιακή κλήση για την δημιουργία αντιγράφων ασφαλείας
1999	Φάση 3η : ΔΙΑΚΛΑΔΩΣΗ ΚΛΗΣΗΣ ΕΞΩΤΕΡΙΚΩΝ ΕΡΓΑΖΟΜΕΝΩΝ	• Χρήση για ανεφοδιασμό και για δημιουργία αντιγράφων ασφαλείας • Μερικά «tunnels», πολύ χρήστες • Μη κρίσιμη LAN-to-LAN κίνηση δεδομένων
2000	ΦΑΣΗ 4η : EXTRANETS	• End to end QoS & SLAs • Πολλά Tunnels, πολύ χρήστες • Μεγάλης κρισιμότητας LAN-LAN κίνηση δεδομένων • Ασφαλή Extranets

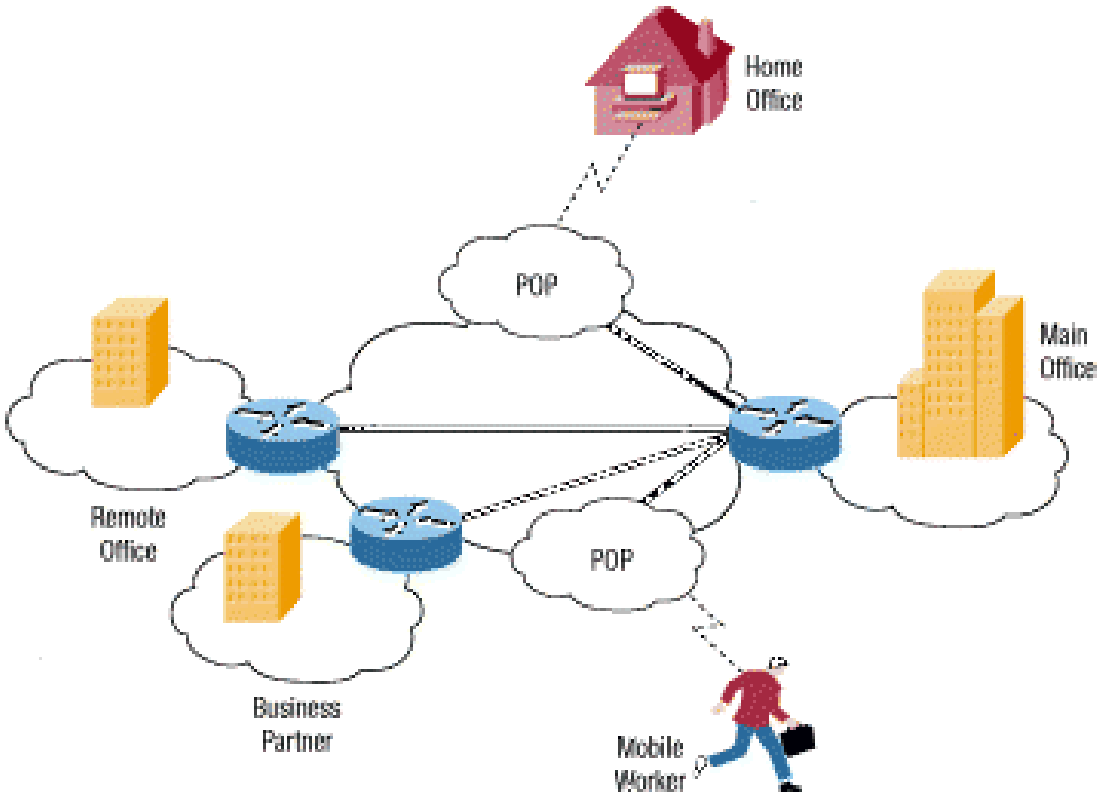
ΕΙΣΑΓΩΓΗ ΣΤΑ ΕΙΚΟΝΙΚΑ ΙΔΙΩΤΙΚΑ ΔΙΚΤΥΑ

Ο κόσμος των υπολογιστών έχει αλλάξει σημαντικά τις τελευταίες δύο δεκαετίες. Πολλές επιχειρήσεις, αντί απλά να ασχολούνται με τοπικά ή εθνικά θέματα, σήμερα θα πρέπει να σκεφτούν την παγκόσμια αγορά και οικονομία. Πολλές εταιρίες έχουν εγκαταστάσεις εκτός της μητρικής χώρας, σε πολλά μέρη του κόσμου. Είναι σίγουρο ότι αυτές αποζητούν το εξής: Τον τρόπο να πετύχουν γρήγορο, ασφαλή και έγκυρη επικοινωνία μεταξύ των γραφείων τους σε οποιοδήποτε σημείο της γης κι αν βρίσκονται αυτά.

Μέχρι και αρκετά πρόσφατα αυτό είχε ως επακόλουθο την **χρήση μισθωμένων γραμμών (leased lines)** με σκοπό την **δημιουργία WAN (wide area network)**. Μια από τις πρώτες εταιρίες στη Ελλάδα που δημιούργησε δίκτυο μέσω μισθωμένης γραμμής ήταν η Shell (Πετρέλαια), την δεκαετία του '90. Αυτές οι μισθωμένες γραμμές είχαν εύρος (bandwidth) από απλή **ISDN (integrated services digital network, 128 Kbps)** ως και OC3 (Optical Carrier-3, 155 Mbps) και παρείχαν στις εταιρίες την δυνατότητα να μεγαλώσουν το ιδιωτικό δίκτυό τους πέρα από μία μέση μικρή γεωγραφική περιοχή. Ένα WAN έχει προφανή πλεονεκτήματα, εν συγκρίσει με ένα δημόσιο δίκτυο, όπως το **INTERNET,** όσον αφορά την αποτελεσματικότητα, την ασφάλεια, την εγκυρότητα και τις επιδόσεις. Αλλά η διατήρηση ενός WAN, ιδιαίτερα όταν χρησιμοποιούνται μισθωμένες γραμμές, αποτελεί μεγάλο έξοδο, το οποίο σταδιακά αυξάνεται όσο μεγαλώνει η απόσταση των γραφείων της επιχείρησης.

Καθώς η δημοτικότητα του διαδικτύου μεγάλωνε, οι εταιρίες στράφηκαν προς αυτό, με σκοπό την επέκταση του προσωπικού τους ιδιωτικού δικτύου. Αρχικά εμφανίστηκαν τα **intranets**, τα οποία είναι σελίδες προστατευμένες με κωδικό, σχεδιασμένα για να χρησιμοποιούνται μόνο από τους υπαλλήλους των εταιριών. Σήμερα πολλές επιχειρήσεις δημιουργούν το δικό τους εικονικό προσωπικό δίκτυο (**virtual private networks, VPN**), για να προσαρμοστεί στις ανάγκες των απομακρυσμένων υπαλλήλων και γραφείων.

Βασικά, ένα ιδιωτικό εικονικό δίκτυο είναι το δίκτυο που χρησιμοποιεί ένα δημόσιο δίκτυο, (συνήθως το internet), για να συνδέσει απομακρυσμένες σελίδες ή χρήστες. Αντί της χρήσης μίας μοναδικά αφιερωμένης γι' αυτό τον σκοπό, πραγματικής σύνδεσης, όπως η μισθωμένη γραμμή (leased line), το **VPN** χρησιμοποιεί εικονικές συνδέσεις δρομολογημένες μέσω του διαδικτύου, από το ιδιωτικό δίκτυο της εταιρίας προς την απομακρυσμένη σελίδα ή εργαζόμενο.



Εικόνα 1

Ένα τυπικό εικονικό ιδιωτικό δίκτυο ένα κεντρικό, κύριο τοπικό δίκτυο (LAN) στα κεντρικά γραφεία της εταιρίας, άλλα LAN σε απομακρυσμένα γραφεία και εγκαταστάσεις και μεμονωμένους χρήστες που συνδέονται εξωτερικά στο πεδίο.

ΠΩΣ ΧΤΙΖΕΤΕ ΕΝΑ ΕΙΚΟΝΙΚΟ ΙΔΙΩΤΙΚΟ ΔΙΚΤΥΟ

Υπάρχουν κυρίως δύο διαδεδομένοι τύποι εικονικών ιδιωτικών δικτύων:

- **Remote – Access** – Επίσης αποκαλείτε και **virtual private dial-up network** (**VPDN**). Αυτό αποτελεί μία σύνδεση από τον χρήστη προς το τοπικό δίκτυο, που χρησιμοποιείτε από μια εταιρία των οποίων οι υπάλληλοι χρειάζεται να συνδεθούν στο ιδιωτικό δίκτυο από διάφορες απομακρυσμένες τοποθεσίες. Τυπικά, μια επιχείρηση που επιθυμεί να εγκαταστήσει ένα μεγάλο **remote – access VPN** θα απευθυνθεί σε έναν **ESP** (**enterprise service provider**). Στην Ελλάδα δεν υπάρχουν

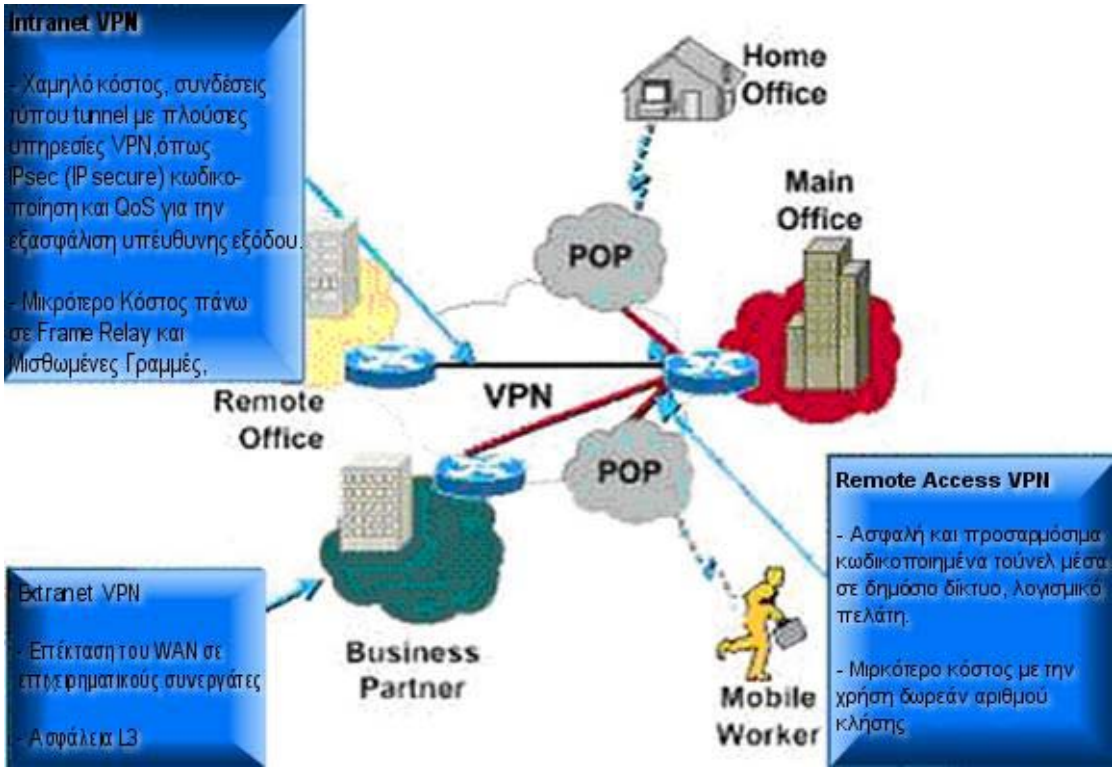
πολλές εταιρίες που να παρέχουν τέτοιες υπηρεσίες, ίσως γιατί είναι ακόμα λίγοι αυτοί που τις ζητάνε. Πάντως VPNs έχουν πραγματωθεί σε ελληνικές εταιρίες (όπως η AlphaNet, στην Θεσσαλονίκη), αλλά ακόμα βρίσκονται σε πρώιμο στάδιο. Ο ESP λοιπόν εγκαθιστά έναν **Εξυπηρέτη Δικτυακής Πρόσβασης** (**Network Access Server, NAS**) και παρέχει στους απομακρυσμένους χρήστες με το κατάλληλο λογισμικό για τους προσωπικούς τους υπολογιστές. Οι telecommuters μπορούν να καλέσουν στην συνέχεια, μέσω τηλεφώνου, έναν αριθμό χωρίς χρέωση, για να επικοινωνήσουν με τον **Εξυπηρέτη Δικτυακής Πρόσβασης (NAS)** και στην συνέχεια χρησιμοποιούν το λογισμικό εικονικών ιδιωτικών δικτύων που τους χορηγήθηκε (VPN client software) για να αποκτήσουν πρόσβαση στο εταιρικό δίκτυο.

Ένα καλό παράδειγμα εταιρίας που χρειάζεται ένα remote – access VPN θα ήταν μια μεγάλη φίρμα με εκατοντάδες πωλητές σε μια περιοχή. Τα remote-access VPNs επιτρέπουν ασφαλή, κωδικοποιημένες συνδέσεις μεταξύ του ιδιωτικού δικτύου μιας επιχείρησης με τους απομακρυσμένους χρήστες, διαμέσου κάποιου τρίτου παροχέα δικτυακών υπηρεσιών.

- **Site – To – Site** – Μέσω της χρήσης αποκλειστικά αφιερωμένου εξοπλισμού και μεγάλου βαθμού κωδικοποίησης, μία εταιρία μπορεί να συνδέσει πολλαπλές σταθερές σελίδες πάνω σε δημόσιο δίκτυο, όπως το internet. Το Site – To – Site VPN μπορεί να είναι:

α) **Intranet – Based** – Αν μια επιχείρηση έχει μία ή παραπάνω τοποθεσίες που θα ήθελε να ενώσει σε ένα μόνο ιδιωτικό δίκτυο, μπορεί να δημιουργήσει ένα VPN βασισμένο σε intranet, έτσι ώστε να ενώσει το ένα τοπικό δίκτυο με το άλλο (LAN to LAN).

β) Extranet – Based – Όταν μια επιχείρηση έχει στενές σχέσεις με μία άλλη (π.χ. αν είναι συνεργάτες ή προμηθευτής ή σημαντικός πελάτης), μπορεί να χτιστεί ένα Εικονικό Ιδιωτικό Δίκτυο βασισμένο σε extranet για να γίνει σύνδεση LAN to LAN. Αυτό επιτρέπει όλες τις εταιρίες που θα δημιουργήσουν μεταξύ τους ένα extranet VPN να μοιραστούν το ίδιο εικονικό περιβάλλον.



Παράδειγμα των τριών τύπων του **VPN**

Ένα καλοσχεδιασμένο VPN μπορεί να ωφελήσει σημαντικότατα μια εταιρία. Παραδείγματος χάρη, θα μπορούσε να:

- Επεκτείνει γεωγραφικά τις συνδέσεις
- Βελτιστοποιήσει την ασφάλεια
- Μειώσει τα λειτουργικά κόστη σε σχέση με τα παραδοσιακά WAN
- Μειώσει χρόνο και το κόστος μεταφοράς για τους απομακρυσμένους χρήστες
- Βελτιώσει την παραγωγικότητα
- Απλουστοποιήσει την διαμόρφωση του δικτύου
- Παράσχει παγκόσμιες δικτυακές ευκαιρίες
- Παράσχει υποστήριξη telecommuter
- Παράσχει ευρείας ζώνης δικτυακή συμβατότητα
- Παράσχει γρηγορότερη απόδοση από την επένδυση, (ROI, return on investment) από ό,τι το παραδοσιακό WAN.

Στοιχεία που θα πρέπει απαραίτητα να ενσωματώνει ένα καλοσχεδιασμένο VPN είναι:

- Ασφάλεια
- Εγκυρότητα
- Ευελιξία
- Διαχείριση δικτύου
- Διαχείριση τακτικής

ΚΑΘΕ ΤΟΠΙΚΟ ΔΙΚΤΥΟ ΚΙ ΕΝΑ ΝΗΣΙ

Ας υποθέσουμε πως ζούμε σε ένα μικρό νησί και γύρω από αυτό υπάρχει ένας τεράστιος ωκεανός. Τριγύρω υπάρχουν κι άλλα νησιά, άλλα πιο μακριά κι αλλά πιο κοντά. Ο πιο απλός τρόπος να επισκεφτούμε ένα από αυτά τα νησιά θα ήταν με ένα πλοίο. Αυτό βέβαια θα σήμαινε πως όλοι σχεδόν οι συνεπιβάτες μας θα μπορούσαν να γνωρίζουν πως ταξιδεύουμε σε αυτό το πλοίο.

Ας υποθέσουμε πως κάθε νησί αντιπροσωπεύει ένα ιδιωτικό τοπικό δίκτυο (LAN) και πως ο ωκεανός είναι το Internet. Ταξιδεύοντας με πλοίο είναι σαν να συνδεόμαστε με έναν Web server ή κάποια άλλη συσκευή στο Internet. Δεν υπάρχει κανένας έλεγχος στα καλώδια και στα routers κάτι που κάνει το Internet να μοιάζει με το πλοίο, όπου δεν υπάρχει έλεγχος πάνω στους συνεπιβάτες μας. Αυτό μας κάνει ευάλωτους όσον αφορά την ασφάλεια αν προσπαθήσουμε να συνδεθούμε μεταξύ δύο ιδιωτικών δικτύων χρησιμοποιώντας δημόσιο μέσο.

Συνεχίζοντας με την μεταφορά μας, αν το νησί μας αποφασίσει να χτίσει γέφυρα προς ένα άλλο νησί τότε θα είναι πιο εύκολη η μετακίνηση, πιο ασφαλή και ευθεία η οδός για να ταξιδέψει ο κόσμος ανάμεσα σε αυτά τα δύο νησιά. Είναι δαπανηρό το να χτίσουμε και να διατηρήσουμε μια γέφυρα, ακόμα κι αν το νησί με το οποίο θα γίνει η σύνδεση με την γέφυρα είναι πολύ κοντά. Όμως η ανάγκη για μια αξιόπιστη, ασφαλή οδό είναι τόσο μεγάλη που την φτιάχνουμε όπως και να έχει. Το νησί μας θα ήθελε να συνδεθεί τώρα και με ένα δεύτερο νησί που είναι ακόμα πιο απομακρυσμένο αλλά αποφασίζει πως το κόστος είναι πάρα πολύ μεγάλο για να το καλύψει.

Κάτι τέτοιο μοιάζει πολύ με την τεχνολογία της μισθωμένης γραμμής. Οι γέφυρες (μισθωμένες γραμμές) είναι διαχωρισμένες από τον ωκεανό (Internet), αλλά παρόλα αυτά είναι ικανές να ενώσουν τα νησιά (LANs). Πολλές εταιρίες διάλεξαν αυτόν τον δρόμο λόγω της ανάγκης για ασφάλεια και αξιοπιστία στη σύνδεση με τα απομακρυσμένα γραφεία τους. Αν όμως τα γραφεία βρίσκονται σε πολύ μεγάλη απόσταση, το κόστος μπορεί να γίνει απαγορευτικά υψηλό, ακριβώς σαν να προσπαθήσουμε να χτίσουμε μια γέφυρα η οποία εκτείνεται σε μεγάλο μήκος.

Εδώ έρχεται να δώσει την λύση το εικονικό ιδιωτικό δίκτυο. Συνεχίζοντας με την μεταφορά μας, θα μπορούσαμε να δώσουμε σε κάθε κάτοικο του νησιού μας ένα μικρό υποβρύχιο. Ας υποθέσουμε πως το υποβρύχιό μας διαθέτει κάποιες σημαντικές ιδιότητες:

- Είναι γρήγορο.
- Μπορείς να το πάρεις μαζί σου όπου κι αν ταξιδεύεις.
- Μπορεί να μας κρύψει από άλλες βάρκες ή υποβρύχια.
- Είναι αξιόπιστο.
- Το κόστος για να προστεθεί κι άλλο υποβρύχιο στον στόλο μας είναι πάρα πολύ μικρό από την στιγμή που γίνουμε κάτοχοι του πρώτου μας υποβρυχίου.

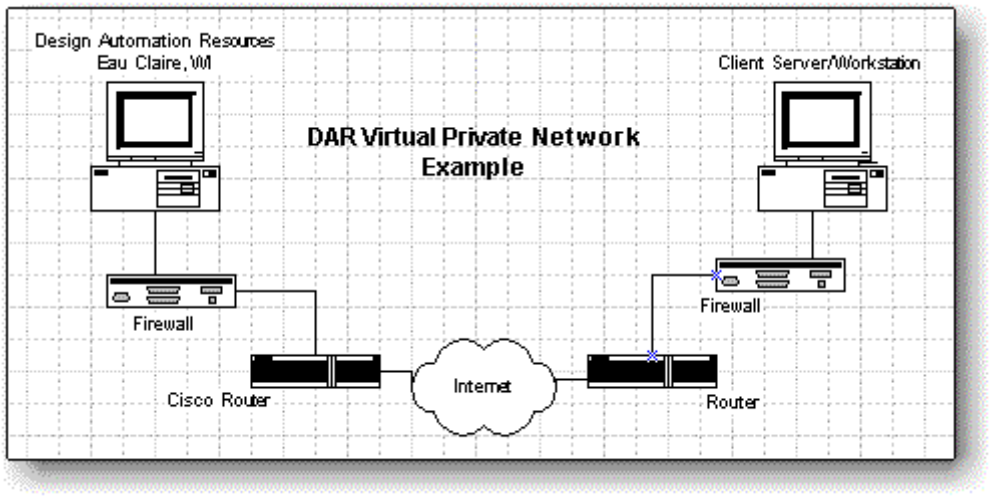
Στην μεταφορά μας, το να έχει ο κάθε άνθρωπος ένα υποβρύχιο είναι σαν κάθε απομακρυσμένος χρήστης να έχει πρόσβαση στο ιδιωτικό δίκτυο της εταιρίας.

Αν και ταξιδεύουν στο ωκεανό μαζί με άλλους, οι κάτοικοι των δύο νησιών μας θα μπορούν να ταξιδεύουν από το ένα νησί στο άλλο όποτε θελήσουν με ασφάλεια και μυστικότητα. Ουσιαστικά αυτός είναι ο τρόπος με τον οποίο λειτουργούν τα εικονικά ιδιωτικά δίκτυα (VPN). Κάθε απομακρυσμένο μέλος του δικτύου μας μπορεί να επικοινωνεί μέσω ενός ασφαλούς και αξιόπιστου μέσου χρησιμοποιώντας το Διαδίκτυο για να συνδεθεί σε ένα ιδιωτικό τοπικό δίκτυο (LAN). Ένα VPN μπορεί να μεγαλώσει έτσι ώστε να διευκολύνει περισσότερους χρήστες σε διαφορετικές τοποθεσίες πολύ πιο εύκολα από ό,τι μια μισθωμένη γραμμή. Για την ακρίβεια, η ευελιξία και προσαρμοστικότητα είναι κάποια από τα μεγαλύτερα προτερήματα των VPNs σε σχέση με τις τυπικές μισθωμένες γραμμές. Αντίθετα με τις μισθωμένες γραμμές, όπου το κόστος ανεβαίνει όσο μεγαλώνουν οι αποστάσεις, οι γεωγραφική τοποθεσία του κάθε γραφείου διαδραματίζει πολύ μικρό ρόλο στην δημιουργία ενός VPN.

VPN & ΑΣΦΑΛΕΙΑ

Ένα καλοσχεδιασμένο Εικονικό Ιδιωτικό Δίκτυο (VPN) χρησιμοποιεί διάφορες μεθόδους για να διατηρήσει την σύνδεση και τα δεδομένα ασφαλή:

Firewalls – Το firewall (ή πύρινο τοίχος ή τοίχος προστασίας) αποτελεί έναν σημαντικό φύλακα ανάμεσα στο ιδιωτικό δίκτυο και το Internet. Τα firewalls μπορούν να ρυθμιστούν έτσι ώστε να περιορίζουν τον αριθμό των ανοιχτών θυρών, τι είδος πακέτων επιτρέπεται να περάσουν στο LAN, ακόμα και το ποια θα είναι τα επιτρεπόμενα πρωτόκολλα. Μερικά προϊόντα VPN, όπως τα 1700 routers της Cisco, μπορούν να αναβαθμιστούν ώστε να συμπεριλαμβάνουν δυνατότητες firewall, τρέχοντας το κατάλληλο Cisco IOS σε αυτά. Θα πρέπει να υπάρχει τοποθετημένο ένα καλό firewall πριν μπει σε λειτουργία ένα Εικονικό Ιδιωτικό Δίκτυο (VPN). Ένα firewall μπορεί επίσης να χρησιμοποιηθεί για να τερματίσει μια περίοδο ενός Εικονικού Ιδιωτικού Δικτύου.



Και το πιο απλό VPN πάντα έχει Firewall

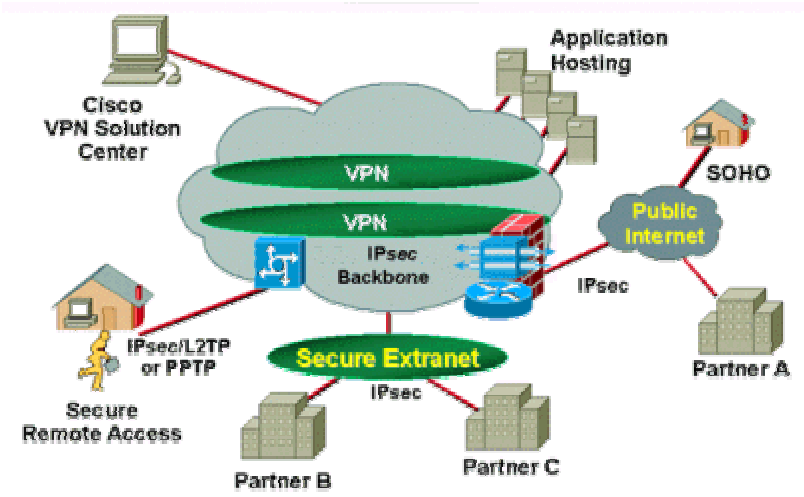
Απόκρυψη Κώδικα (Encryption) - Με αυτήν την διαδικασία παίρνουμε όλα τα δεδομένα που ένας υπολογιστής στέλνει σε έναν άλλον, κωδικοποιώντας τα σε μια φόρμα που μόνο ο άλλος υπολογιστής θα είναι σε θέση να αποκωδικοποιήσει. Τα περισσότερα Συστήματα Απόκρυψης Κώδικα για Υπολογιστή (computer encryption systems) ανήκουν σε μια από τις δύο παρακάτω κατηγορίες:

- Symmetric-key encryption

- Public-key encryption

Στην **symmetric-key encryption**, κάθε υπολογιστής έχει ένα κρυφό κλειδί (κώδικα) το οποίο μπορεί να χρησιμοποιήσει για να αποκρύψει ένα πακέτο πληροφοριών πριν σταλεί μέσω δικτύου σε κάποιον άλλο υπολογιστή. Το Symmetric-key προϋποθέτει ότι υπάρχει γνώση για το ποιοι υπολογιστές θα «συνομιλήσουν» έτσι ώστε να μπορέσεις να εγκαταστήσεις το κλειδί στον καθένα. Η Symmetric-key απόκρυψη δεδομένων είναι συνήθως σαν ένας κρυφός κώδικας που και οι δύο υπολογιστές θα πρέπει να γνωρίζουν, για να μπορέσουν να αποκωδικοποιήσουν τις πληροφορίες. Ο κώδικας παρέχει το κλειδί για την αποκωδικοποίηση του μηνύματος. Είναι σαν να δημιουργούμε ένα κωδικοποιημένο μήνυμα για να αποσταλεί σε έναν φίλο, στο οποίο κάθε γράμμα είναι αντικατεστημένο με το γράμμα που βρίσκετε 2 θέσεις πιο πριν στο αλφάβητο. Έτσι το "A" γίνεται "C," και το "B" γίνεται "D", κ.ο.κ.. Βέβαια εμείς έχουμε πληροφορήσει τον φίλο μας πως να αποκωδικοποιήσει το γράμμα. Έτσι αυτός όταν παίρνει το γράμμα μπορεί και το διαβάζει. Για τους υπόλοιπους το περιεχόμενο του γράμματος δεν είναι κατανοητό.

Η **Public-key encryption** χρησιμοποιεί έναν συνδυασμό της private key και της public key. Το private key (ιδιωτικό κλειδί) τώρα είναι γνωστό μόνο στον υπολογιστή μας, καθώς το public key (δημόσιο κλειδί) δίνεται από τον υπολογιστή μας σε κάθε υπολογιστή που θέλει να επικοινωνήσει με ασφάλεια με αυτό. Για να αποκωδικοποιήσει ένα κωδικοποιημένο, κρυφό μήνυμα κάποιος υπολογιστής θα πρέπει να χρησιμοποιήσει το public key (δημόσιο κλειδί), το οποίο παρέχεται από τον υπολογιστή που το δημιούργησε, καθώς και από το δικό του private key. Μια πολύ δημοφιλής εφαρμογή public-key encryption ονομάζεται **Pretty Good Privacy** (PGP), η οποία επιτρέπει να κωδικοποιήσεις σχεδόν τα πάντα.



Ένα remote-access VPN που χρησιμοποιεί IPSec

- **IPSec** – Το Internet Protocol Security Protocol (IPSec) παρέχει εμπλουτισμένα στοιχεία ασφάλειας όπως καλύτερους αλγόριθμους κωδικοποίησης καθώς και πιο εύκολη πιστοποίηση. Το IPSec έχει δύο μεθόδους κωδικοποίησης: **tunnel** και **transport**. Η μέθοδος tunnel κωδικοποιεί την κεφαλή και το ωφέλιμο φορτίο κάθε πακέτου πληροφορίας, ενώ η μέθοδος transport κωδικοποιεί μόνο το πολύτιμο φορτίο. Μόνο τα συστήματα που είναι συμβατά με IPSec μπορούν να εκμεταλλευτούν αυτό το πρωτόκολλο. Ακόμα, όλες οι συσκευές πρέπει να χρησιμοποιούν ένα κοινό κλειδί και τα firewalls του κάθε δικτύου πρέπει να έχει αντίστοιχες τακτικές ασφαλείας. Το IPSec μπορεί να κωδικοποιήσει δεδομένα ανάμεσα σε διάφορες συσκευές, όπως:
    - Router προς router
    - Firewall προς router
    - Η/Υ προς router
    - Η/Υ προς server
- **AAA Server** – Οι εξυπηρέτες AAA (authentication, authorization and accounting) χρησιμοποιούνται για ακόμα πιο ασφαλή πρόσβαση σε ένα απομακρυσμένο περιβάλλον VPN. Όταν λαμβάνεται μια αίτηση για δημιουργία νέας περιόδου σύνδεσης από κάποιον πελάτη μέσω

τηλεφώνου, η αίτηση πηγαίνει από έναν proxy (διαμεσολαβητή) στον εξυπηρέτη AAA. Ο AAA αμέσως μετά κάνει τον ακόλουθο έλεγχο:

- Ταυτότητας (authentication)
- Δικαιωμάτων (authorization)
- Πραγματικών ενεργειών (accounting)

Οι πληροφορίες περί των πραγματικών ενεργειών του χρήστη ενός AAA είναι πολύ χρήσιμες ειδικά για την καταγραφεί των κινήσεων του πελάτη για λόγους ελέγχου, χρέωσης αλλά και για λόγους παιδαγωγικούς.

ΤΕΧΝΟΛΟΓΙΕΣ & VPN

Ανάλογα με τον τύπο του Εικονικού Ιδιωτικού Δικτύου (remote-access ή site-to-site), χρειάζεται και να χρησιμοποιηθούν διάφορα «συστατικά» για να χτιστεί το VPN. Μερικά από αυτά μπορεί να είναι:

- Λογισμικό πελάτη για τους υπολογιστές όλων των απομακρυσμένων χρηστών.
- Ειδικές συσκευές οι οποίες να είναι αφιερωμένες μόνο σε μια εργασία όπως ένας VPN concentrator η ένα ασφαλές PIX firewall.
- Αποκλειστικός εξυπηρέτης VPN για υπηρεσίες από κλίση μέσω τηλεφώνου.
- Ένας NAS (network access server) που θα χρησιμοποιείτε από τον παροχέα υπηρεσιών (service provider) για να επιτευχθεί η απομακρυσμένη πρόσβαση των χρηστών του VPN access
- Κέντρο διαχείρισης θεμάτων δικτύου και πολιτικής του VPN

Επειδή δεν υπάρχει ευρέως αποδεκτό πρότυπο για την υλοποίηση ενός Εικονικού Ιδιωτικού Δικτύου, πολλές εταιρίες έχουν αναπτύξει λύσης κλειδιά μετά από δική τους πρωτοβουλία. Για παράδειγμα, η Cisco προσφέρει αρκετές λύσεις πάνω στο VPN συμπεριλαμβανομένου και τις εξής:

- **VPN concentrator** – Ενσωματώνει τις πιο προοδευτικές τεχνολογίες που υπάρχουν σήμερα πάνω στην κωδικοποίηση. Οι Cisco VPN concentrators έχουν χτιστεί ειδικά για την δημιουργία απομακρυσμένης πρόσβασης Εικονικά Ιδιωτικά Δίκτυα (remote-access VPN). Παρέχουν υψηλή αξιοπιστία, υψηλή απόδοση και ευελιξία και ακόμα περιέχουν ηλεκτρονικές υπομονάδες, που ονομάζονται **scalable encryption**

processing (**SEP**), που επιτρέπουν στους χρήστες με ευκολία να αυξάνουν την χωρητικότητα και την παραγωγή. Οι εστιαστές (concentrators) προσφέρονται σε μοντέλα κατάλληλα για τα πάντα και για όλους, από μικρές εταιρίες των 100 χρηστών remote-access μέχρι μεγάλους οργανισμούς των 10,000 απομακρυσμένων χρηστών.

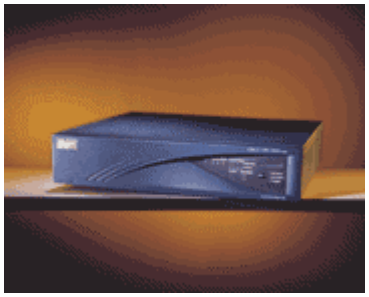


Photo courtesy Cisco Systems, Inc.

The Cisco VPN 3000 Concentrator

- **VPN-optimized router** – Τα Cisco's VPN-optimized routers παρέχουν ευελιξία, routing, ασφάλεια και QoS (ποιότητα υπηρεσιών). Είναι βασισμένα πάνω στα Cisco Λειτουργικά Συστήματα Διαδικτύου (**IOS,** Internet Operating System), Έτσι υπάρχει κάποιο router κατάλληλο για κάθε περίπτωση, από πρόσβαση σε μικρό σπίτι / γραφείο (small-office/home-office, **SOHO**) μέχρι κεντρική σελίδα του συνόλου των VPNs, για μεγάλες επιχειρησιακές ανάγκες.

Photo courtesy Cisco Systems, Inc.

The Cisco 1750 Modular Access Router

- **Cisco secure PIX firewall** – Μεγάλο τεχνολογικό επίτευγμα αποτελεί το PIX (private Internet exchange) firewall συνδυάζοντας δυναμικό network address translation, proxy εξυπηρέτη, φιλτράρισμα πακέτων δεδομένων, firewall και ικανότητες VPN σε μια μονάχα συσκευασία.

Photo courtesy Cisco Systems, Inc.

The Cisco PIX Firewall

Αντί της χρήσης του Cisco IOS, αυτή η συσκευή διαθέτει εκσυγχρονισμένο Λειτουργικό Σύστημα το οποίο έχει την ικανότητα να διαχειρίζεται μια ποικιλία πρωτοκόλλων φτάνοντας μεγάλες αποδόσεις με το να συγκεντρώνετε μόνο σε ένα IP.

TUNNELING

Τα περισσότερα Εικονικά Ιδιωτικά Δίκτυα (VPNs) στηρίζονται στο **tunneling** για να δημιουργήσουν ένα ιδιωτικό δίκτυο το οποίο να μπορεί να διασχίσει το Internet. Συνήθως, το tunneling αποτελεί την διαδικασία της τοποθέτησης ενός ολόκληρου πακέτου μέσα σε ένα άλλο πακέτο και της αποστολής του σε ένα δίκτυο. Το πρωτόκολλο του εξωτερικού πακέτου είναι κατανοητό από το δίκτυο κι έτσι αυτό «καταλαβαίνει» για το πότε αυτό μπαίνει ή αποχωρεί. Και οι δύο πλευρές αποκαλούνται **tunnel interfaces**,

Το tunneling απαιτεί τρία διαφορετικά πρωτόκολλα:

- **Carrier protocol** – Το πρωτόκολλο που χρησιμοποιείτε από το δίκτυο επιβεβαιώνοντας πως η πληροφορία ταξιδεύει
- **Encapsulating protocol** – Το πρωτόκολλο (GRE, IPSec, L2F, PPTP, L2TP) το οποίο είναι τυλιγμένο γύρω από τα αρχικά δεδομένα
- **Passenger protocol** – Τα πραγματικά δεδομένα (IPX, NetBeui, IP) τα οποία μεταφέρονται

Το tunneling επιφέρει μεγάλες επιπλοκές στα VPNs. Για παράδειγμα, μπορούμε να τοποθετήσουμε ένα αρχείο που χρησιμοποιεί κάποιο

πρωτόκολλο το οποίο δε υποστηρίζεται από το διαδίκτυο (όπως το NetBeui) μέσα σε ένα IP πακέτο και να το στείλουμε με ασφάλεια μέσω του Internet. Ή ακόμα θα μπορούσαμε να τοποθετήσουμε ένα πακέτο που χρησιμοποιεί μια ιδιωτική (non-routable) IP διεύθυνση μέσα σε ένα πακέτο που χρησιμοποιεί μια παγκόσμια μοναδική IP διεύθυνση (globally unique IP address) έτσι ώστε να επεκτείνουμε ένα ιδιωτικό δίκτυο μέσα στο Internet.

Σε ένα site-to-site VPN, το **GRE** (**generic routing encapsulation**) είναι συνήθως το πρωτόκολλο δημιουργίας της «κάψουλας» που παρέχει το πλαίσιο εργασίας, για το πως θα δημιουργηθεί το πρωτόκολλο επιβάτη, για την μεταφορά μέσω του πρωτοκόλλου του κομιστή, που τυπικά είναι βασισμένο σε IP. Αυτό συμπεριλαμβάνει πληροφορίες πάνω στο είδος του πακέτου που βάζουμε σε «κάψουλα» και πληροφορίες όσον αφορά την σύνδεση μεταξύ τον πελάτη και τον εξυπηρέτη. Αντίθετα με το GRE, το IPSec στην **μέθοδο tunnel** μερικές φορές χρησιμοποιείται ως το πρωτόκολλο της «κάψουλας». Το IPSec δουλεύει σωστά και στα remote-access αλλά και στα site-to-site VPNs. Το IPSec πρέπει να υποστηρίζεται και από τις δύο επιφάνειες tunnel για να χρησιμοποιηθεί.

Σε ένα απομακρυσμένης πρόσβασης (remote-access) VPN, το tunneling κανονικά λαμβάνει χώρα με την βοήθεια του PPP (Place To Place Protocol). Μέρος της δέσμηςTCP/IP, το PPP είναι ο μεταφορέας για άλλα πρωτόκολλα IP όταν υπάρχει επικοινωνία πάνω στο δίκτυο μεταξύ του υπολογιστή που φιλοξενεί και το απομακρυσμένο σύστημα. Το Remote-access VPN tunneling βασίζεται στο PPP.

Όλα τα παρακάτω πρωτόκολλα χτίστηκαν χρησιμοποιώντας την βασική δομή του PPP και χρησιμοποιούνται από τα remote-access VPNs.

- **L2F** (Layer 2 Forwarding) – Αναπτύχθηκε από την Cisco, το L2F χρησιμοποιεί κάθε σχήμα πιστοποίησης που υποστηρίζεται από το PPP.

- **PPTP** (Point-to-Point Tunneling Protocol) – Το PPTP δημιουργήθηκε από το PPTP Forum, μια διεθνής εταιρική συνεργασία των US Robotics, Microsoft, 3COM, Ascend και ECI Telematics. Το PPTP

υποστηρίζει κωδικοποίηση 40-bit and 128-bit και χρησιμοποιεί κάθε σχήμα πιστοποίησης που υποστηρίζεται από το PPP.

- **L2TP** (Layer 2 Tunneling Protocol) – Το L2TP αποτελεί προϊόν μιας συνεργασίας μεταξύ μελών του PPTP Forum, Cisco και της IETF (Internet Engineering Task Force). Συνδυάζει στοιχεία κι από το PPTP και από L2F και L2TP. Επίσης υποστηρίζει πλήρως το IPSec.

Το L2TP μπορεί να χρησιμοποιηθεί ως πρωτόκολλο tunneling για Εικονικά Ιδιωτικά Δίκτυα τύπου site-to-site καθώς επίσης ως remote-access VPNs. Ακριβέστερα, το L2TP μπορεί να δημιουργήσει tunnel μεταξύ:

- Πελάτη και router
- NAS και router
- Router και router

Το φορτηγό είναι το πρωτόκολλο διακομιστή, το κουτί είναι το πρωτόκολλο «κάψουλας» κι ο υπολογιστής είναι το πρωτόκολλο επιβάτης.

Τα Εικονικά Ιδιωτικά Δίκτυα (VPNs) αποτελούν έναν σπουδαίο τρόπο ώστε να μπορέσει μια εταιρία να κρατήσει τους υπαλλήλους της συνδεδεμένους ανεξάρτητα από το που βρίσκονται αυτοί. Στην Ελλάδα αυτό το μέσω δεν έχει αναπτυχθεί ακόμα και λίγοι είναι οι επιχειρηματίες που γνωρίζουν την ύπαρξή του. Όλες αυτές οι αλλαγές που επέρχονται στην οικονομική και τεχνολογική ζωή του πλανήτη οδηγούν σε ανοιχτή οικονομικά

κοινωνία, όπου ο καθένας θα μπορεί να εργάζεται οπουδήποτε κι αν βρίσκεται αυτός, όσο μακριά κι αν είναι από τον τόπο εργασίας του.

ΟΡΟΛΟΓΙΑ

Όρος	Επεξήγηση
ASN.1	Abstract Syntax Notation (1). A method for describing data that is used in many other standards.
CAST	A cryptographic encryption algorithm that is an optional part of some standards.
CE	Customer edge. The router that is on the customer's side of the customer-provider interface.
CPE	Customer premise equipment. Systems that are at a customer's site (as compared systems that are in a service provider's network).
cryptography	The study and practice of keeping data secure. Two common applications of cryptography are privacy (preventing unauthorized viewing of data) and authentication (proving one's identity to access data or as the source of a message).
DES	Data Encryption Standard. A cryptographic encryption algorithm that is part of many standards.
Diffie-Hellman	A cryptographic key-exchange algorithm that is part of many standards. See also X9.42.
digital signature	A method for proving that the holder of a private key is the originator of a message
DSS	Digital Signature Standard. A cryptographic signature algorithm that is part of many standards. Also called DSA (Digital Signature Algorithm).
FAQ	Frequently Asked Question. Usually, this is a document that lists frequently asked questions on a particular topic and gives answers to the questions.
IAB	Internet Architecture Board. The body that helps define the overall architecture and design of Internet protocols. The IAB is the technical advisory group of the ISOC.
IESG	Internet Engineering Steering Group. The group who oversees the IETF working group process and determines which proposals become standards.

IETF	Internet Engineering Task Force. The main organization that creates protocol standards for the Internet.
IKE	Internet Key Exchange. The protocol used to exchange symmetric keys for performing IPsec.
Internet Draft	A document that is offered for review to the IETF.
IPsec	IP Security. The protocol used to give authentication and/or encryption to IP packets.
ISAKMP	Internet Security Association and Key Manangement Protocol. The basis for IKE.
ISOC	Internet Society. The longest-standing organization promoting the use of the Internet.
L2TP	Layer 2 Tunneling Protocol. Provides a means for tunneling IP traffic in layer 2. Can be used with IPsec to provide authentication.
LDAP	Lightweight Directory Access Protocol. A simpler protocol for directory access than X.500.
LDP	Label distribution protocol
LSR	Label switching router. A router that can read and respond to labelled layer 2 datagrams
MPLS	Multiprotocol label switching protocol
Oakley	A protocol in which two authenticated parties can agree on secret keys.
PE	Provider edge. The router that is on the provider's side of the customer-provider interface.
PKI	Public Key Infrastructure. The mechanisms used both to allow a recipient of a signed message to trust the signature and to allow a sender to find the encryption key for a recipient.
PKIX	Internet X.509 Public Key Infrastructure. The name of the IETF working group creating standards for PKI on the Internet.
PPTP	Point-to-Point Tunneling Protocol. Provides a means for tunneling IP traffic in layer 2.
PPVPN	Provider-provisioned VPN. A VPN that is managed by a service provider, not the user of the VPN.
public key cryptography	A method for creating two keys (also called a *key pair*) that can be used to encrypt and decrypt messages. One of the two keys, the *public key*, is widely published, while the other key, the *private key* is kept secret. When you want to encrypt a message for a recipient, you use that recipient's public key; only someone with the private key can decrypt the message.

	When you want to digitally sign a message, you use your private key; anyone with your public key can then check the signature and verify that only you could have signed the message.
QoS	Quality of Service. There are many meanings for this term, but they generally revolve around guarantees of service levels for Internet connections. With respect to VPNs, QoS generally means the amount of throughput and/or the number of simultaneous connections that can be sustained over a connection that uses IPsec.
RFC	Request For Comments. The primary mechanism used by the IETF to publish documents, including standards.
RSA	Rivest-Shamir-Adelman. The name of a cryptographic key-exchange algorithm popular in many security protocols. Also the name of the company which controls the US patent on the algorithm.
SSL	Secure Sockets Layer. A protocol for encryption and authentication of Internet connections. See TLS.
TLS	Transport Layer Security. The standardized version of SSL.
Triple DES	A cryptographic algorithm for repeated DES operations that have the effect of increasing the security of the encrypted message.
VPN	A private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures.
VPNC	Virtual Private Network Consortium. The trade association for manufacturers and providers in the VPN market.
WG	Working Group. Usually used with reference to the IETF.
X.509	Specification of the format of digital certificates. See also PKIX.
X9.42	A specification for methods of using the Diffie-Hellman algorithms.

ΒΙΒΛΙΟΓΡΑΦΙΑ

VPN INFO OF THE WORLD WIDE WEB - http://www.shmoo.com

Introduction: History Of VPN - http://www.ari.vt.edu/ece5516/vpn/history.html

International Engineering Consortium – http://www.iec.org

Design Automation Resources, Inc - http://www.darinc.com/

RAM, Τεύχος 153, Δεκέμβριος 2001

www.enterasys.com/vpn/