Ολοκληρωμένη λύση Ασφάλειας στην ΑΝΔΡΟΜΕΔΑ Α.Ε. από την Datelec Hellas

Άρθρο του **Δημήτρη Παρώνη**
Network Security Department
Datelec Hellas
e-mail: d.paronis@datelec.gr

CASE STUDY

Το έργο αφορά την συνολική ασφάλεια του δικτύου της ΑΝΔΡΟΜΕΔΑ Α.Ε. και υλοποιήθηκε από την εταιρεία Datelec Hellas.

Η **ΑΝΔΡΟΜΕΔΑ Α.Ε**. είναι μια από τις κορυφαίες πέντε εταιρίες στο χώρο της Ελληνικής Ιχθυοκαλλιέργειας. Η θέση αυτή κατακτήθηκε, ανάμεσα σε 250 διαφορετικές εταιρίες, χάρη στην ανάπτυξη της Ανδρομέδα Α.Ε., η οποία βασίστηκε στο τρίπτυχο Ποιότητα Προϊόντος,Εξυπηρέτηση Πελατών & Καινοτομίες. Η Ανδρομέδα Α.Ε. ιδρύθηκε το 1998, με κεντρικά γραφεία στο Ρίο Πατρών Αχαΐας, από τον κ. Γιαννόπουλο, τον ιδρυτή της Riopesca Α.Ε. (1988-1998), η οποία ήταν η μεγαλύτερη μονάδα παραγωγής γόνου τσιπούρας και λαβρακιού στην Ευρώπη, στις αρχές του ’90.

Η **Datelec Hellas** είναι πρωτοπόρος στην ασφάλεια δικτύων, παρέχει ολοκληρωμένες λύσεις στους μεγαλύτερους “system integrators” της Ελληνικής αγοράς. Με ευρεία γκάμα εξειδικευμένων προϊόντων δίνει λύσεις προσαρμοσμένες στις ανάγκες των πελατών όπως επίσης παρέχει υψηλού επιπέδου συμβουλευτικές υπηρεσίες και service.

Περιγραφή του έργου

Η παράμετρος της ασφάλειας είναι ο πιο σημαντικός παράγοντας στην υλοποίηση και την διαχείριση ενός σύγχρονου δικτύου. Η διαφύλαξη των εταιρικών δεδομένων, που μας παρέχεται από μια ολοκληρωμένη λύση ασφαλείας είναι άρρηκτα συνδεδεμένη με την απροβλημάτιστη πρόσβαση των χρηστών στις παρεχόμενες, από την εταιρεία, υπηρεσίες (λογιστικές εφαρμογές, υπηρεσίες τηλεφωνίας-εικόνας, WEB services, WEB Mail Access κα). Η πρόσβαση αυτή θα πρέπει να είναι εφικτή για τους χρήστες είτε αυτοί βρίσκονται στο εσωτερικό δίκτυο (LAN) είτε η σύνδεσή τους γίνεται από τα υποκαταστήματα είτε, τέλος, συνδέονται μέσω του Internet από οποιοδήποτε σημείο στον κόσμο. Ταυτόχρονα θα πρέπει να συνυπολογισθεί η αναντίρρητη απαίτηση για γρήγορη, και πάντοτε ασφαλή, πρόσβαση στο διαδίκτυο. Τέλος θα πρέπει να ληφθεί ιδιαίτερη μέριμνα για την ασφάλεια στην επικοινωνία μέσω του ηλεκτρονικού ταχυδρομείου. Οι παράμετροι εδώ που θα πρέπει να λάβουμε υπόψη μας είναι η μη παραβίαση των προσωπικών δεδομένων, η ασφαλής και απρόσκοπτη επικοινωνία ενώ ταυτόχρονα θα πρέπει να σταματάμε τα e-mails με κακόβουλο περιεχόμενο (ιούς, fishing κλπ.) στην περίμετρο του δικτύου μας πριν αυτά εισέλθουν στο εσωτερικό του δικτύου της εταιρείας. Επιπλέον στον σχεδιασμό μας λαμβάνουμε υπόψη την καλή και εύχρηστη διαχείριση της ανεπιθύμητης αλληλογραφίας (spam mails).

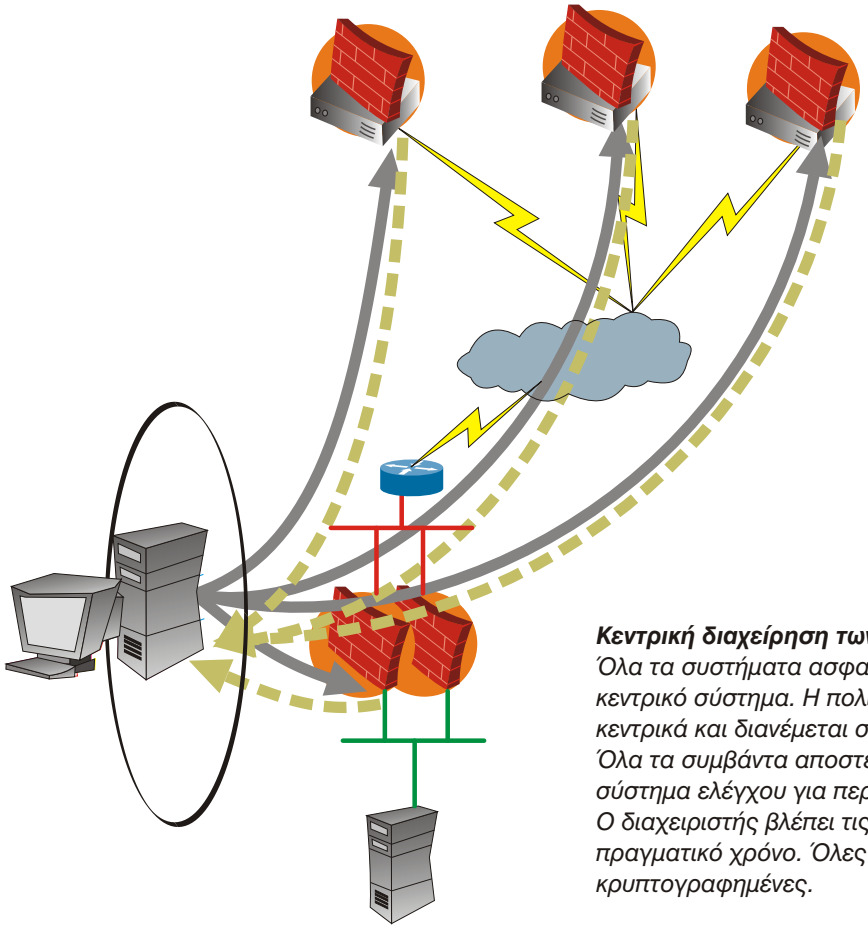
Κεντρικό Κατάστημα (ΠΑΤΡΑ - PIO)

Στο κεντρικό κατάστημα προτείνεται η εγκατάσταση ενός Firewall-1 (FW-1 UTM Appliance) της Checkpoint, σύστημα δικτυακής προστασίας υψηλής ασφαλείας με ενσωματωμένο σύστημα ανίχνευσης και αποτροπής επιθέσεων σε πραγματικό χρόνο (IPS). Το FW-1 έρχεται προεγκατεστημένο στην συσκευή (Appliance) με δικό του λειτουργικό (SecurePlatform της Checkpoint) που εξασφαλίζει υψηλή ασφάλεια και ευκολία στην αναβάθμιση του συστήματος.

Το σύστημα εμπεριέχει IPS (Intrusion Prevention System-Smart Defense) με συνέπεια να αναγνωρίζει αυτόματα την προσπάθεια επίθεσης, ή την τυχόν παραβίαση των κανόνων που διέπουν τους κανόνες δικτυακής επικοινωνίας, και τις αποτρέπει άμεσα. Η βάση δεδομένων του συστήματος ενημερώνεται από το Internet.

Κεντρική Διαχείριση

Έχοντας υπόψη ότι υφίστανται πολλά απομακρυσμένα σημεία-συνδέσεις ανά την Ελλάδα θα πρέπει να ενσωματωθεί στο σύστημα μας η δυνατότητα της κεντρικής διαχείρισης όλων των συστημάτων ασφαλείας-FWs σε όλα τα απομακρυσμένα σημεία που παρέχουν πρόσβαση στο δίκτυο της εταιρείας και το Internet.



Κεντρική διαχείρηση των συστημάτων ασφαλείας
Όλα τα συστήματα ασφαλείας ελέγχονται από το κεντρικό σύστημα. Η πολιτική ασφαλείας καθορίζεται κεντρικά και διανέμεται σε όλα τα FWs αυτόματα. Όλα τα συμβάντα αποστέλλονται στο κεντρικό σύστημα ελέγχου για περαιτέρω ανάλυση. Ο διαχειριστής βλέπει τις καταγραφές σε πραγματικό χρόνο. Όλες οι επικοινωνίες είναι κρυπτογραφημένες.

Με αυτό τον τρόπο εξασφαλίζεται η άμεση απόκριση, από τον διαχειριστή του συστήματος, σε περίπτωση που προκύψει έκτακτη ανάγκη - κενό ασφάλειας. Ταυτόχρονα διευκολύνεται με αυτό τρόπο η διαχείριση του ελέγχου πρόσβασης των χρηστών, αφού πλέον δεν απαιτείται από τον διαχειριστή η τροποποίηση της πολιτικής ασφαλείας του κάθε συστήματος ξεχωριστά. Αντίθετα οι απαραίτητες τροποποιήσεις γίνονται στη κεντρική πολιτική ασφαλείας και αποστέλλονται αυτόματα σε όλα τα σημεία παρουσίας. Με βάση τα παραπάνω επιτυγχάνεται αφενός η ελαχιστοποίηση των κινδύνων που προέρχονται από ανθρώπινο λάθος, αφετέρου ελαχιστοποιείται ο χρόνος απόκρισης (πρακτικά υποδεκαπλασιάζεται).

Καταγραφή συμβάντων

Σημαντικό μέρος της ασφάλειας των συστημάτων και δικτύων αποτελεί και η γνώση των τεκταινομένων στο δίκτυο. Μια συστηματική επίθεση περιλαμβάνει μεγάλο αριθμό αποτυχημένων επιθέσεων προς το προστατευόμενο δίκτυο. Η μελέτη των δεδομένων που προέρχονται από τις επιθέσεις αυτές μας δίνουν τον απαραίτητο χρόνο αλλά και τα εφόδια για να αντιμετωπίσουμε τον οποιοδήποτε επιτιθέμενο. Το FW-1 της Checkpoint έρχεται με ενσωματωμένο ένα εξαιρετικό σύστημα καταγραφής των γεγονότων. Στο σύστημα αυτό ενσωματώνεται η δυνατότητα παρακολούθησης των δεδομένων ή δικτυακών συνδέσεων σε πραγματικό χρόνο. Με βάση τα παραπάνω εξασφαλίζονται οι προϋποθέσεις που απαιτούνται για την άμεση απόκριση των διαχειριστών σε περίπτωση εμφάνισης ανωμαλιών στις δικτυακές επικοινωνίες. Στα παραπάνω θα πρέπει να συνυπολογισθούν και τα πλεονεκτήματα που προκύπτουν από την κεντρική διαχείριση η οποία αναφέρθηκε παραπάνω. Τούτο συνεπάγεται την δυνατότητα καταγραφής γεγονότων-συμβάντων από όλα τα σημεία παρουσίας.

Κρυπτογράφηση (VPN)

Μολονότι η λέξη κρυπτογράφηση εμπεριέχει την έννοια της ασφάλειας δυστυχώς έχει κακοποιηθεί κατ' επανάληψη τόσο από χρήστες όσο και από κατασκευαστές δικτυακών συσκευών. Για να θεωρήσουμε την υλοποίηση μιας διαδικασίας κρυπτογράφησης ασφαλή θα πρέπει να πληρούνται μια σειρά από προϋποθέσεις, που πολλάκις δεν ικανοποιούνται:

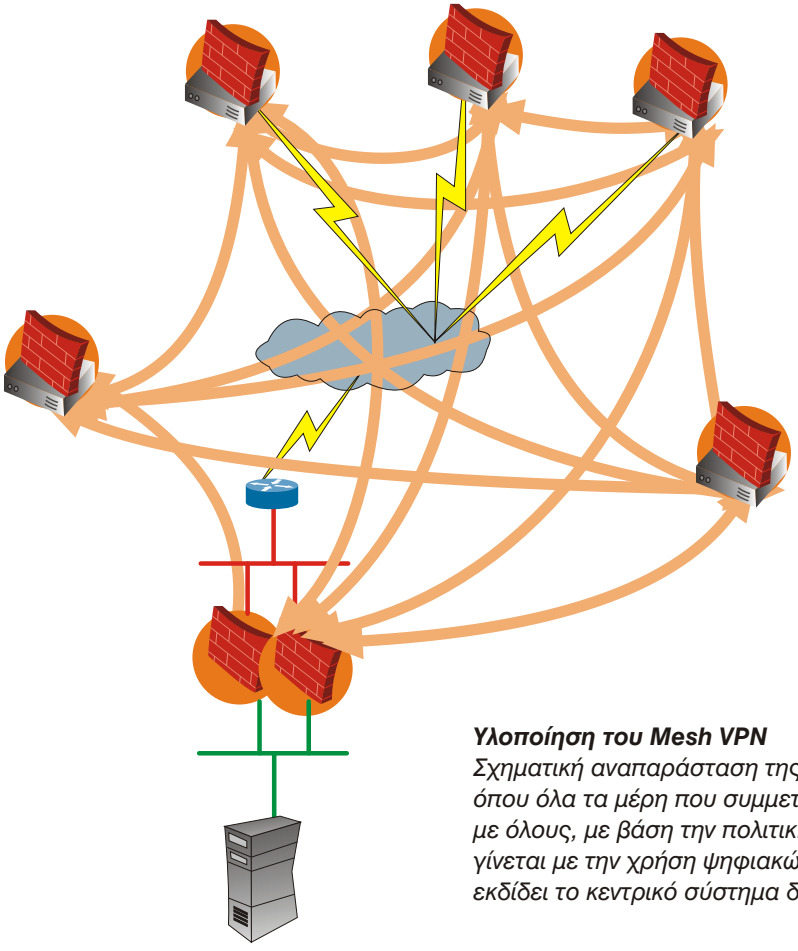
Αλγόριθμος κρυπτογράφησης. Πολλές από τις συσκευές (routers) του εμπορίου, δεν υποστηρίζουν τους σύγχρονους και ταυτόχρονα ισχυρούς αλγόριθμους κρυπτογράφησης. Σε αντίθεση το FW-1 παρέχει στο διαχειριστή την δυνατότητα να επιλέξει ανάμεσα από τους ισχυρότερους αλγόριθμους που ικανοποιούν τις απαιτήσεις ασφάλειας του συστήματος μας. Στην συγκεκριμένη περίπτωση προτείνεται η χρήση του αλγόριθμου Advanced Encryption Standard στα 256bit ο οποίος ικανοποιεί επαρκώς την απαίτηση για ισχυρή κρυπτογράφηση σε συνάρτηση με την υψηλή ταχύτητα.

Διαδικασία Πιστοποίησης Χρήστη ή VPN Gateway. Εν προκειμένω συνιστάται να εκμεταλλευτούμε μια από τις δυνατότητες που μας παρέχει το FW-1 και να χρησιμοποιήσουμε την Certificate Authority που έχει ενσωματωμένη, για την διαδικασία της πιστοποίησης των άκρων του VPN με την χρήση ψηφιακών πιστοποιητικών. Το παραπάνω ισχύει υπό την προϋπόθεση ότι θα επιλεγούν τα Edges της CheckPoint που προτείνονται -δες παρακάτω- (ή άλλες συσκευές ασφαλείας που υποστηρίζουν ψηφιακά πιστοποιητικά) για την προστασία των καταστημάτων. Σε αντίθετη περίπτωση,

κατά ανάγκη θα χρησιμοποιηθούν preshared secrets. Σε αυτή την περίπτωση προτείνεται η επιλογή του ισχυρότερου δυνατού Diffie-Hellman Group (κατά προτίμηση Group 14 - 2048bit) ώστε να ελαχιστοποιήσουμε την πιθανότητα επιθέσεων τύπου Man in the Middle.

Πέρα από την ασφάλεια που μας παρέχει η χρήση του ψηφιακού πιστοποιητικού, μας παρέχεται η δυνατότητα, εφόσον το επιτρέψουμε μέσα από την πολιτική ασφαλείας, της απευθείας κρυπτογραφημένης επικοινωνίας μεταξύ των καταστημάτων χωρίς να απαιτείται η δρομολόγηση των πακέτων μέσω του κεντρικού συστήματος (Mesh VPN όπως ορίζεται από την CheckPoint). Με αυτό τον τρόπο εξασφαλίζουμε μεγαλύτερη ταχύτητα και εξοικονόμηση πολύτιμου bandwidth. Το παραπάνω θεωρείται απαραίτητη προϋπόθεση για ευαίσθητες στην καθυστέρηση δικτυακές επικοινωνίες όπως η τηλεφωνία ή Video κλήσεις.

Για να επιτύχουμε τον ίδιο στόχο με τις "συμβατικές" μεθόδους πιστοποίησης θα απαιτείτο να υλοποιήσουμε ξεχωριστό τούνελ κρυπτογράφησης μεταξύ δύο (όποιων) συσκευών κάτι που συνεπάγεται ότι για το πρώτο εκ των απομακρυσμένων σημείων (έστω ότι έχουμε 10 τέτοια) θα έπρεπε να ορισθούν και να παραμετροποιηθούν 10 τούνελ, για το δεύτερο 9 κοκ. ήτοι θα απαιτούντο συνολικά 10+9+8+7+..+2= **54 (πενήντα τέσσερα)** διαφορετικά τούνελ έναντι **ενός**! Γίνεται εύκολα αντιληπτό ότι ο απαιτούμενος χρόνος εγκατάστασης **αλλά το κυριότερο ο απαιτούμενος χρόνος διαχείρισης, συντήρησης αλλά και η διαδικασία αντιμετώπισης προβλημάτων μειώνεται στο ελάχιστο.**



Υλοποίηση του Mesh VPN
Σχηματική αναπαράσταση της υλοποίησης του Mesh VPN, όπου όλα τα μέρη που συμμετέχουν σε αυτό επικοινωνούν με όλους, με βάση την πολιτική ασφαλείας. Η υλοποίηση γίνεται με την χρήση ψηφιακών πιστοποιητικών που εκδίδει το κεντρικό σύστημα διαχείρισης.

Εύκολα γίνονται αντιληπτά τα πλεονεκτήματα της προτεινόμενης λύσης τουλάχιστον όσον αφορά την ασφάλεια και την ευκολία διαχείρισης. Εναλλακτικά θα μπορούσε κανείς να χρησιμοποιήσει VPDNs για την διασύνδεση του κεντρικού καταστήματος τα οποία δεν τα χρησιμοποιούμε στην λύση μας για τους παρακάτω λόγους.

- Αρκετοί πάροχοι δεν υλοποιούν κρυπτογράφηση κατά την υλοποίηση του τούνελ αλλά απλώς δρομολογούν τα πακέτα μεταξύ των δύο άκρων. Συνεπώς δεν ικανοποιείται η απαίτηση της εμπιστευτικότητας και της ακεραιότητας των δεδομένων.
- Τα σημεία τερματισμού του VPDN είναι routers οι οποίοι δεν είναι αμιγώς συσκευές ασφαλείας κάτι που θα μπορούσε να θεωρηθεί εν δυνάμει κενό ασφαλείας.
- Στους routers που υλοποιούν το tunneling έχουν πρόσβαση και προσωπικό (μηχανικοί) του παρόχου.
- Η εμπειρία έχει δείξει ότι οι πάροχοι δεν έχουν ικανοποιητικό χρόνο απόκρισης σε περίπτωση προβλήματος.
- Τα απομακρυσμένα σημεία έχουν πρόσβαση αποκλειστικά στο κεντρικό σημείο πρόσβασης και όχι κατευθείαν Internet κάτι που συνεπάγεται τη αύξηση των απαιτήσεων των επικοινωνιών σε bandwidth και κατά συνέπεια υψηλότερο μηνιαίο κόστος (δεδομένου ότι απαιτούνται για την κάλυψη των αναγκών μεγαλύτερου εύρους (bandwidth) γραμμές).
- Σε αρκετές περιπτώσεις οι συνδέσεις θεωρούνται a-priori ασφαλείς με συνέπεια την ευκολότερη εξάπλωση ιών στα επιμέρους τμήματα του δικτύου.
- Υψηλότερο μηνιαίο κόστος.

Υποκαταστήματα

Τα υποκαταστήματα όσον αφορά την ασφάλεια εξοπλίζονται με συσκευές της Checkpoint, τα Edges, που παρέχουν την απαιτούμενη ασφάλεια για την ασφαλή πρόσβαση στο Internet ενώ ταυτόχρονα συνεργάζονται αρμονικά με τα κεντρικά FW-1 ώστε να επιτευχθεί το απαιτούμενο επίπεδο κρυπτογράφησης. Τα παραπάνω σε συνδυασμό με το γεγονός, που ήδη αναφέραμε, της κεντρικής διαχείρισης εξασφαλίζουν την απαιτούμενη επικοινωνία με όλα τα σημεία παρουσίας. Αυτό έχει σαν αποτέλεσμα το δίκτυο της επιχείρησης συμπεριλαμβανομένων όλων των καταστημάτων να φαίνεται ενιαίο για τον χρήστη. Το παραπάνω συνδυάζεται με τον πλήρη έλεγχο, από πλευράς ασφαλείας, των επικοινωνιών. Συνεπώς είμαστε σε θέση να αποτρέψουμε κακόβουλες ενέργειες είτε αυτές προέρχονται από το Internet είτε ακόμα-ακόμα και από τα εσωτερικά σημεία του δικτύου.

Ιδιαίτερη αναφορά πρέπει να γίνει στο γεγονός ότι με τον παραπάνω σχεδιασμό και επιλογή προϊόντων εκμεταλλευόμαστε τον "έξυπνο" τρόπο με τον οποίο η Checkpoint διαχειρίζεται τα τούνελ κρυπτογράφησης (VPN Tunnels). Ποιο συγκεκριμένα, μέσω ειδικών πρωτοκόλλων, για μια δεδομένη επικοινωνία μεταξύ δύο συγκεκριμένων σημείων επιλέγεται η βέλτιστη όσον αφορά την ταχύτητα ενώ μειώνεται και ο κίνδυνος αστοχίας στην επικοινωνία. Επιπλέον η επικοινωνία διατηρείται ανοικτή μόνιμα ακόμα και αν δεν υπάρχουν δεδομένα στην γραμμή επιτυγχάνοντας χαμηλό χρόνο στην αρχικοποίηση των επικοινωνιών, μειώνοντας τα λάθη στην διαδικασία κρυπτογράφησης και τέλος δίνοντας στον διαχειριστή την δυνατότητα έγκαιρου εντοπισμού προβλημάτων - πχ. πτώση γραμμής, αστοχία στην επικοινωνία κλπ.

Edges (Περιμετρικές συσκευές)

Στις συσκευές ασφαλείας που προτείνουμε ενσωματώνεται όλη η τεχνολογία της Checkpoint. Αναφέρουμε ενδεικτικά κάποιες από τις δυνατότητές τους. Statefull Inspection Firewall, IPS (Intrusion Prevention System-Smart Defense) με ανανέωση της βάσης δεδομένων από το κεντρικό FW, Policy based Routing, δυνατότητα λειτουργίας σε Cluster Mode, δυνατότητα διαχείρισης δύο ISPs (HOT-Standby), δυνατότητα dialup μέσω modem κ.α.

Πρόσβαση στο Internet

Καίριο σημείο στην ασφάλεια του δικτύου μας θα πρέπει να θεωρήσουμε την επικοινωνία μέσω ηλεκτρονικής αλληλογραφίας και την πρόσβαση στο WEB. Τούτο γιατί είναι τα δύο πρωτόκολλα μέσω των οποίων εισέρχονται δεδομένα (αρχεία) από το Internet στο εσωτερικό μας δίκτυο τα οποία θα πρέπει να θεωρήσουμε ότι με μεγάλη πιθανότητα περιέχουν κακόβουλο περιεχόμενο (ιούς, spywares, δούρειους ίππους κλπ). Συνεπώς θα πρέπει να θωρακίσουμε την περιμετρική ασφάλειά μας εστιάζοντας στα δύο αυτά σημεία.

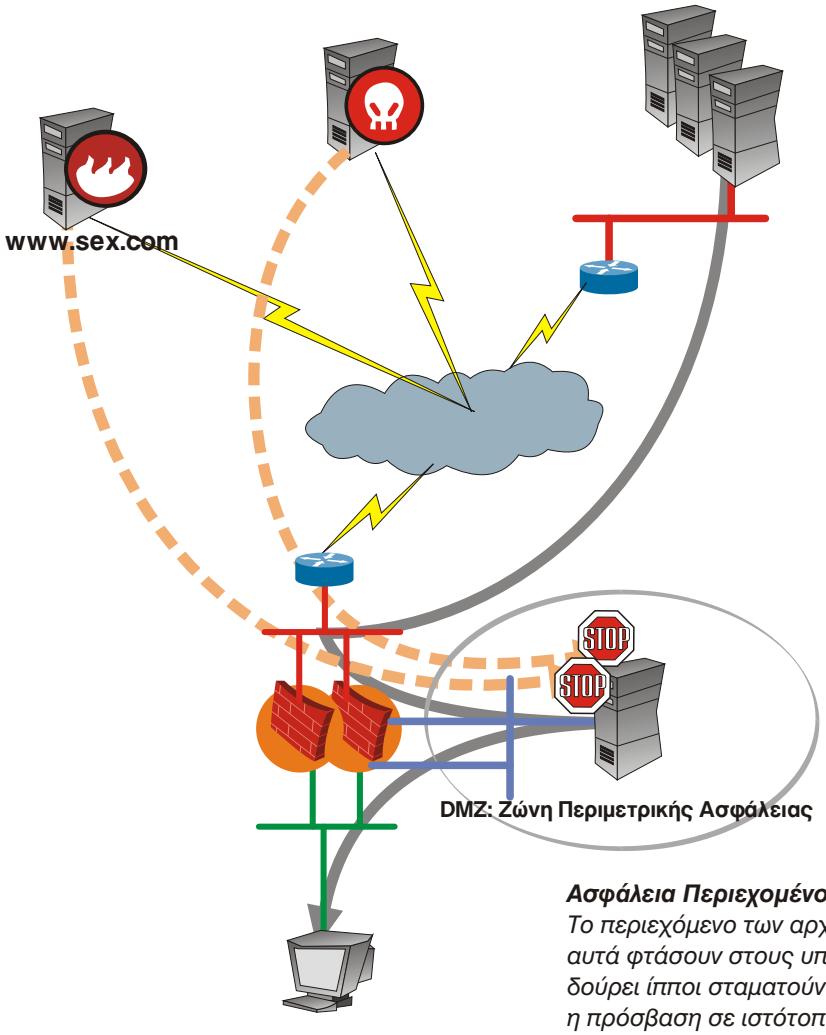
Ασφάλεια περιεχομένου

Ο παραπάνω στόχος επιτυγχάνεται κάνοντας χρήση τεχνικών μέσω των οποίων το περιεχόμενο των αρχείων που ανταλλάσσονται ελέγχεται σε πραγματικό χρόνο και σε περίπτωση κινδύνου να διαγράφονται. Όσον αφορά στα δεδομένα που προέρχονται από την περιήγηση στο διαδίκτυο (surf) - εφεξής θα αναφερόμαστε σε αυτό με την ονομασία του πρωτοκόλλου- http και ftp, η ύπαρξη των antivirus προγραμμάτων που είναι εγκατεστημένα στους υπολογιστές των χρηστών εκτιμάται ότι δίνει την απαραίτητη προστασία από τέτοιους κινδύνους. Επικουρικά στα antivirus θα μπορούσαμε να εγκαταστήσουμε το eSafe AV Gateway (http-ftp) της Alladin με την βοήθεια του οποίου ελέγχουμε το περιεχόμενο των αρχείων που κατεβαίνουν σε πραγματικό χρόνο και σε περίπτωση που αυτά περιέχουν κακόβουλο περιεχόμενο διακόπτεται η επικοινωνία.

"Απαγορευμένοι" τόποι...

Πρόσθετο προϊόν στο παραπάνω είναι το Url Filtering. Στο eSafe AV Gateway ενσωματώνεται μια βάση δεδομένων, η οποία ανανεώνεται αυτόματα καθημερινά, και η οποία περιέχει όλους τους ιστότοπους με βάση το περιεχόμενο. Η βάση αυτή χωρίζεται σε μέρη, με βάση το περιεχόμενο όπως αναφέραμε (πχ. Πορνό, Hacking, Τυχερά παιχνίδια, Γνωριμιών, Ραδιοφωνικούς σταθμούς κλπ). Ο διαχειριστής έχει πλέον την δυνατότητα να καθορίσει την πολιτική πρόσβασης στο Διαδίκτυο. Η πολιτική είναι εξαιρετικά ευέλικτη δίνοντάς μας την δυνατότητα να επιτρέπουμε την πρόσβαση ανά χρήστη ή τμήμα (πχ. μπορούμε να επιτρέπουμε μόνο στο Λογιστήριο πρόσβαση σε ιστότοπους με οικονομικό περιεχόμενο). Τα πλεονεκτήματα κάνοντας χρήση αυτής της τεχνολογίας είναι πολλαπλά:

- Εξοικονόμηση bandwidth
- Περιορίζουμε την επισκεψιμότητα στο Internet στην απαραίτητη - αύξηση παραγωγικότητας
- Το κυριότερο όμως, είναι η αύξηση της ασφάλειας, δεδομένου ότι δρούμε προληπτικά, μια και οι χρήστες δεν μπορούν πλέον να "κατεβάσουν" κακόβουλο περιεχόμενο από απαγορευμένους ιστότοπους (οι οποίοι κατά κανόνα είναι υπεύθυνοι για την διάδοση όλων των νέων ιών).

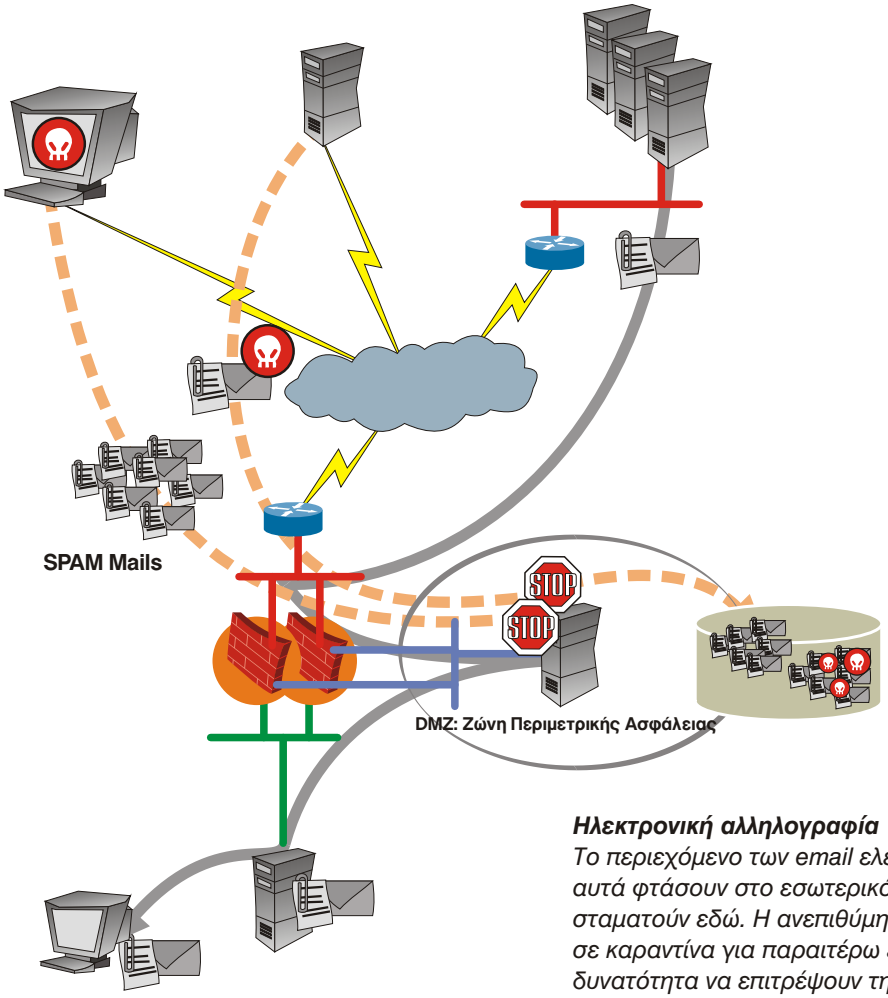


Ασφάλεια Περιεχομένου
Το περιεχόμενο των αρχείων ελέγχεται στην DMZ, πριν καν αυτά φτάσουν στους υπολογιστές των χρηστών. Έτσι, ιοί, δούρει ίπποι σταματούν ενώ ταυτόχρονα απαγορεύεται η πρόσβαση σε ιστότοπους που το περιεχόμενό τους θα μπορούσε να είναι επικύνδυνο (URL filtering).

Ηλεκτρονική Αλληλογραφία

Εξαιρετική προσοχή πρέπει να δοθεί στην υλοποίηση της επικοινωνίας μέσω ηλεκτρονικής αλληλογραφίας (πρωτόκολλο SMTP) δεδομένου ότι μέσω αυτής τίθεται σε καθημερινή βάση σε κίνδυνο η ακεραιότητα του δικτύου μας αλλά και των επικοινωνιών. Για την εξασφάλιση κατά συνέπεια προτείνεται στην περίμετρο ασφαλείας (DMZ) η εγκατάσταση του eSafe Mail Gateway. Το eSafe είναι ένας SMTP Mail Relay Server ο οποίος δέχεται όλα τα εισερχόμενα mails και με τα συστήματα ασφαλείας που περιέχει (AntiBombing, AntiRelay, AntiSpoof κλπ) προστατεύει τον κεντρικό mail Server ο οποίος πλέον δεν είναι εκτεθειμένος άμεσα στο Internet. Το παραπάνω θεωρείται σημαντικό πλεονέκτημα δεδομένου ότι ο Exchange Server είναι νευραλγικό κομμάτι του δικτύου αφού περιέχει τεράστια ποσότητα πληροφορίας. (Όλη την αλληλογραφία, τους λογαριασμούς και τους κωδικούς όλων των χρηστών, πληροφορίες για το Active Directory, άμεση πρόσβαση σε όλα τα συστήματα και αρχεία του δικτύου κλπ).

Το eSafe Mail Gateway επιπλέον ελέγχει για ιούς ή άλλο κακόβουλο περιεχόμενο τα emails, επίσης ελέγχει το περιεχόμενο της αλληλογραφίας για λέξεις ή προτάσεις οι οποίες δεν επιθυμούμε να



Ηλεκτρονική αλληλογραφία
Το περιεχόμενο των email ελέγχεται στην DMZ, πριν καν αυτά φτάσουν στο εσωτερικό δίκτυο. Έτσι, ιοί, δούρει ίπποι σταματούν εδώ. Η ανεπιθύμητη αλληλογραφία αποθηκεύεται σε καραντίνα για παραιτέρω έλεγχο. Οι χρήστες έχουν την δυνατότητα να επιτρέψουν την αποστολή του mail, σε περίπτωση false positive.

περιέχονται σε αυτήν. Με αυτό τον τρόπο όλα τα email σταματούν στη περίμετρο ασφαλείας και δεν εισέρχονται στο εσωτερικό δίκτυο. Επιπλέον εισάγουμε ένα επιπλέον ανάχωμα ασφαλείας προσθέτοντας μια επιπλέον μηχανή antivirus εκμηδενίζοντας την πιθανότητα μόλυνσης των συστημάτων μας σε περίπτωση πχ. που δεν ανανεωθεί εγκαίρως η βάση του antivirus που έχει εγκατασταθεί στους υπολογιστές των χρηστών.

Ένας καινούριος πονοκέφαλος που έχει προστεθεί στους χρήστες είναι αυτή της ανεπιθύμητης αλληλογραφίας (spam mails). Το eSafe, ενσωματώνει μια πλειάδα τεχνολογιών για την εύρεση και την απόρριψη αυτών των mail. Ενδεικτικά αναφέρουμε:

- Έλεγχος μέσω DNS
- RBL (Realtime Blackhole List)
- Ευρεστικοί Αλγόριθμοι
- Λεκτική Ανάλυση - Κατηγοριοποίηση mail με βάση το λεκτικό περιεχόμενο πχ. Ιατρικό, Οικονομικό κλπ.
- Υπογραφές Spam - Μια αυτόματα ανανεούμενη βάση που επιτρέπει την αναγνώριση της

ανεπιθύμητης αλληλογραφίας με βάση την "ψηφιακή υπογραφή" του περιεχομένου. Με αυτό τον τρόπο μπορούν να εντοπιστούν και οι νέοι ιοί για τους οποίους δεν έχουν καν ενημερωθεί οι εταιρείες Anti-Virus.

- Spam URL filtering - Έλεγχος στο περιεχόμενο των emails για διασυνδέσεις σε spam ιστότοπους.
- Ανάλυση Φωτογραφιών και αναγνώριση λέξεων μέσα σε αυτές.

Δεν απαιτείται να ληφθούν ιδιαίτερα μέτρα για την υψηλή διαθεσιμότητα αφ' ενός γιατί το SMTP δεν είναι πρωτόκολλο πραγματικού χρόνου και αφ' ετέρου γιατί τροποποιώντας την πολιτική του firewall (FW-1) μπορούμε να τροποποιήσουμε την δρομολόγηση της αλληλογραφίας ώστε να μην έχουμε την απώλεια μηνυμάτων.

Διαχείριση των SPAM

Σε κάθε χρήστη αποστέλλεται ημερησίως αναφορά για το ποια mails κόπηκαν σαν spam ταυτόχρονα του δίνεται η δυνατότητα να ζητήσει από το σύστημα να του αποσταλλεί κάποιο μήνυμα σε περίπτωση false positive.

ΥΠΗΡΕΣΙΕΣ

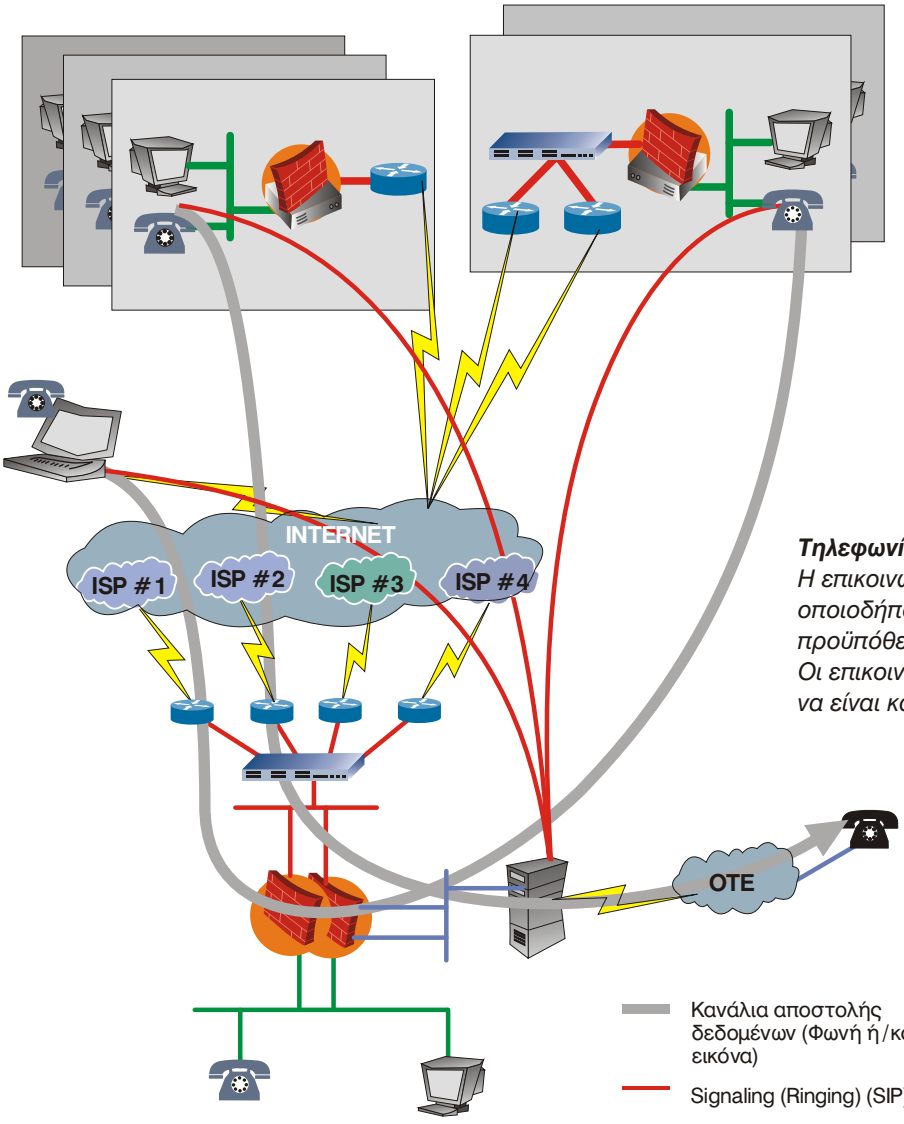
Λογιστικές εφαρμογές

Σε μεγάλο ποσοστό, οι λογιστικές εφαρμογές δεν πληρούν τις απαραίτητες δικτυακές προδιαγραφές με συνέπεια πολλάκις για την υλοποίηση των επικοινωνιών να απαιτούνται πολύ υψηλοί ρυθμοί μεταγωγής δεδομένων (σε ορισμένες περιπτώσεις έχουμε μετρήσει μέχρι και 6Mbit) συνεπώς δεν μπορούμε να εκτιμήσουμε εκ των προτέρων τις απαιτήσεις σε bandwidth τέτοιων εφαρμογών παρά μόνο μετά από μέτρηση. Στην περίπτωση που απαιτείται πολύ υψηλό bandwidth (άνω των 50 - 60kbps/ανά σύνδεση) συνιστάται η επικοινωνία να γίνεται μέσω Terminal Server, για τις συνδέσεις μέσω VPN. Η χρήση Terminal Server, συνιστάται να μείνει, σαν ύστατη εναλλακτική επιλογή με δεδομένο το υψηλό κόστος που απαιτείται για την προμήθεια του σχετικού Hardware αλλά και Software. Πιο συγκεκριμένα απαιτείται πολύ ισχυρό σύστημα για να καλύψει τις μεγάλες ανάγκες σε ταυτόχρονες συνδέσεις. Τέλος σε περίπτωση που επιλεχθεί η λύση αυτή προτείνεται η εγκατάσταση του συστήματος σε Cluster ώστε να μην εισάγουμε στις λογιστικές εφαρμογές αυτό που αποκαλούμε Single Point of Failure.

Σε κάθε περίπτωση η τελική απόφαση μπορεί να ληφθεί μόνο αφού η λογιστική εφαρμογή εγκατασταθεί και τεθεί σε λειτουργία.

Υπηρεσίες τηλεφωνίας μέσω δικτύου

Όλο και περισσότερες εταιρείες υλοποιούν υπηρεσίες τηλεφωνίας μέσω δικτύου. Η πρόταση που αναλύουμε εδώ υποστηρίζει πλήρως τέτοιες επικοινωνίες είτε αυτές γίνονται εντός του δικτύου, είτε μέσω VPN είτε ο χρήστης βρίσκεται σε οποιοδήποτε σημείο του κόσμου κάνοντας χρήση των δυνατοτήτων που μας παρέχει η Checkpoint. Έχουμε την δυνατότητα πχ. να επικοινωνήσουμε από οποιοδήποτε hot spot σε ένα αεροδρόμιο, οπουδήποτε στον κόσμο, με οποιοδήποτε εσωτερικό τηλέφωνο, κάνοντας μάλιστα χρήση κρυπτογράφησης, εντελώς δωρεάν.



Τηλεφωνία μέσω δικτύου
Η επικοινωνία μέσω SIP γίνεται από οποιοδήποτε σημείο του κόσμου με την προϋπόθεση σύνδεσης με το Internet. Οι επικοινωνίες αν το επιθυμούμε μπορεί να είναι και μη κρυπτογραφημένες.

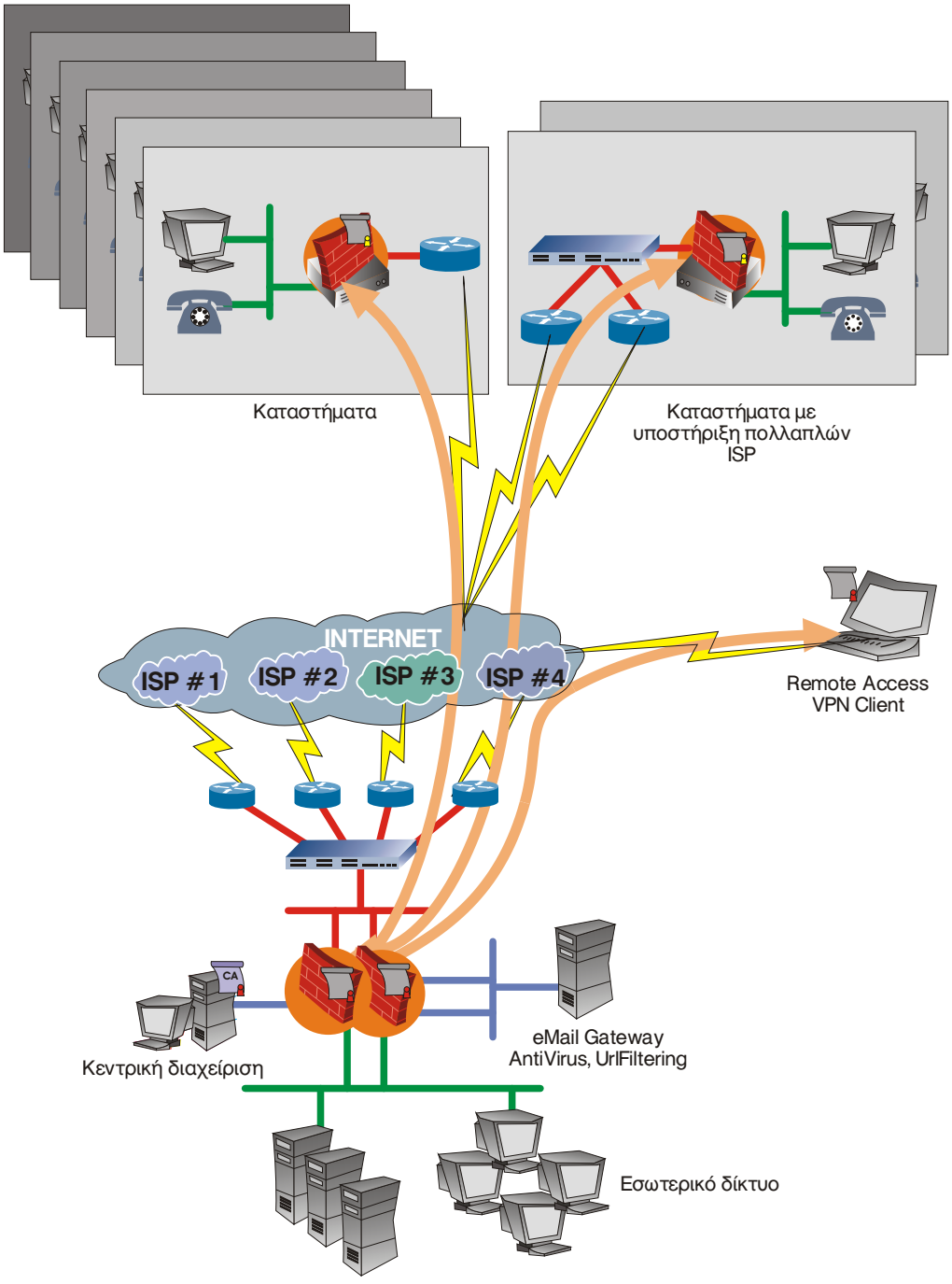
Client to Site VPN

Με τις συσκευές που χρησιμοποιούνται παρέχεται η δυνατότητα στους χρήστες να επικοινωνήσουν με το εσωτερικό δίκτυο κάνοντας χρήση της κρυπτογράφησης από οποιοδήποτε σημείο του κόσμου. Η επικοινωνία είναι πιστοποιημένη από το Firewall (FW-1) και είναι ελεγχόμενη σε όλα τα στάδιά της από αυτό. Αυτό συνεπάγεται υψηλή ασφάλεια ενώ διευκολύνεται και η επικοινωνία με όλα τα σημεία παρουσίας.

Η υλοποίηση αυτή, εκτός της υψηλής ασφάλειας, δεν απαιτεί παρά ελάχιστες ρυθμίσεις από τον χρήστη. Με αυτό τον τρόπο μπορεί κανείς εύκολα και γρήγορα να διαβάσει την αλληλογραφία του ή να εκτυπώσει ένα αρχείο από το σπίτι του.

Τέλος αξίζει να αναφέρουμε την δυνατότητα της υλοποίησης Clientless VPN, η υλοποίηση δηλαδή του VPN γίνεται χωρίς να απαιτείται η εγκατάσταση κανενός είδους Client κάνοντας χρήση του πρωτοκόλλου https.

Η τελική τοπολογία του δικτύου φαίνεται στο παρακάτω σχήμα.



Τελική Τοπολογία