Ειρήνη Πετράκη

Πανεπιστήμιο Πειραιώς
University of Piraeus

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

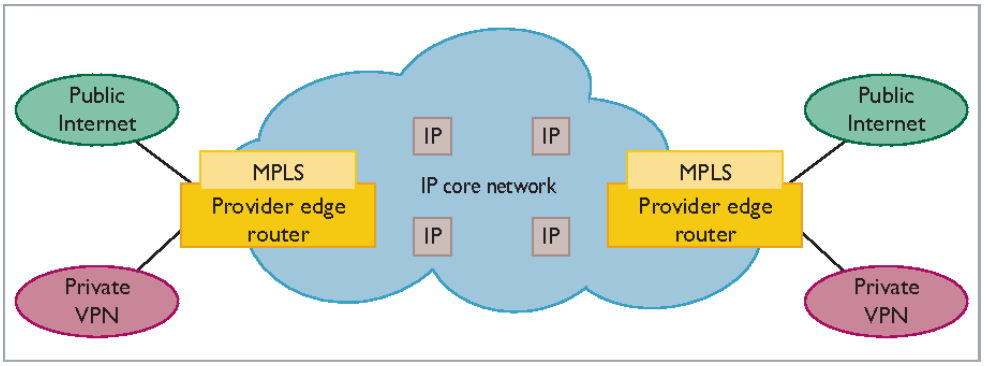
«ΑΣΦΑΛΕΙΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ»

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

«ΜΕΛΕΤΗ ΑΣΦΑΛΕΙΑΣ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ MPLS MULTI-PROTOCOL LABEL SWITCHING»

ΠΕΤΡΑΚΗ ΕΙΡΗΝΗ ΜΤΕ 1825

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΚΩΝΣΤΑΝΤΙΝΟΣ ΛΑΜΠΡΙΝΟΥΔΑΚΗΣ



ΠΕΙΡΑΙΑΣ

ΦΕΒΟΥΡΑΡΙΟΣ 2021

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω τον καθηγητή μου κ. Κωνσταντίνο Λαμπρινουδάκη για τη βοήθεια και την καθοδήγηση που μου παρείχε για την ολοκλήρωση αυτής της εργασίας. Επιπλέον, νιώθω την ανάγκη να ευχαριστήσω τους Σωτήρη Νικολόπουλο και Χρήστο Τζιμούρτο καθώς και όλη την ομάδα του Telco Operation για τη βοήθεια που μου παρείχαν για την παρακολούθηση των μαθημάτων. Τέλος, θα ήθελα ευχαριστήσω την οικογένεια μου και το σύντροφο μου για τη στήριξη τους και τις διευκολύνσεις που μου παρείχαν καθ' όλη τη διάρκεια των σπουδών μου σε αυτό το μεταπτυχιακό.

ΠΕΡΙΛΗΨΗ

Στόχος της παρούσας εργασίας είναι η μελέτη και η ανάλυση της ασφάλειας της τεχνολογίας MPLS (Multi-Protocol Label Switching). Επίσης, θα παρουσιαστεί η μελέτη μιας περίπτωσης υλοποίησης τηλεφωνίας πάνω από το MPLS VPN δίκτυο και θα αναλυθεί η ασφάλεια που παρέχει αυτή η λύση. Η εργασία αποτελείται από τις εξής ενότητες. Στο πρώτο κεφάλαιο γίνεται ανάλυση της τεχνολογίας MPLS, και συγκεκριμένα του τρόπου λειτουργίας και της αρχιτεκτονικής του MPLS αλλά και η παρουσίαση των χαρακτηριστικών - πλεονεκτημάτων του. Στο δεύτερο κεφάλαιο γίνεται η περιγραφή των πιθανών απειλών που μπορεί να αντιμετωπίσει ένα δίκτυο MPLS θέτοντας σε κίνδυνο τόσο το ίδιο το δίκτυο όσο και όλες τις υπηρεσίες που υποστηρίζει. Στο τρίτο κεφάλαιο θα γίνει η ανάλυση της ασφάλειας που παρέχει ένα MPLS δίκτυο, ενώ στο τέταρτο κεφάλαιο θα αναφερθούν ορισμένες προτάσεις για την ενδυνάμωση της. Στο πέμπτο κεφάλαιο γίνεται η ανάλυση του IPsec. Τέλος, στο έκτο κεφάλαιο θα παρουσιαστεί μια πρακτική υλοποίηση ενός MPLS VPN πάνω στο οποίο έχει υλοποιηθεί εσωτερική τηλεφωνία η οποία δρομολογείται πάνω από το κλειστό MPLS κύκλωμα με ασφάλεια.

Λέξεις κλειδιά : MPLS,IP sec,VPN,Voice

ABSTRACT

The aim of this work is to study and analyze the security of MPLS (Multi-Protocol Label Switching) technology. Also, the study of a case of telephony implementation over the MPLS VPN network will be presented and the security provided by this solution will be analyzed. The work consists of the following sections. The first chapter analyzes MPLS technology, and specifically the way of operation and architecture of MPLS and the presentation of its features - advantages. The second chapter describes the potential threats that an MPLS network may face by endangering both the network itself and all the services it supports. The third chapter will analyze the security provided by an MPLS network, while the fourth chapter will mention some suggestions for its strengthening. The fifth chapter analyzes IP sec. Finally, the sixth chapter will present a practical implementation of an MPLS VPN on which internal telephony has been implemented which is routed over the closed MPLS circuit safely.

Keywords: MPLS, IP sec, VPN, Voice

Περιεχόμενα

Πίνακας Εικόνων

Κεφάλαιο 1 - MPLS-VPN

Ιστορική αναδρομή

Τα Εικονικά Ιδιωτικά δίκτυα (Virtual Private Network VPN) στη σημερινή εποχή έχουν αποτελέσει ένα ιδιαίτερα σημαντικό εργαλείο με μεγάλη εφαρμογή κυρίως για τις επιχειρήσεις όπου πολύ συχνά η ανάγκη για απομακρυσμένη σύνδεση των χρηστών κρίνεται απολύτως απαραίτητη. Ένα τέτοιο παράδειγμα υπήρξε , όταν λόγω των έκτακτων μέτρων του COVID 19, προέκυψε η ανάγκη για απομακρυσμένη σύνδεση των χρηστών στην εξ' αποστάσεως εργασία. Η χρήση του VPN έδωσε στις εταιρείες τη δυνατότητα να συνεχίσουν να λειτουργούν κανονικά χωρίς να είναι απαραίτητη η πρόσβαση των χρηστών στις εγκαταστάσεις των εταιριών και οι επιχειρήσεις συνέχισαν να λειτουργούν με τη χρήση VPN χωρίς κανένα πρόβλημα δίνοντας τη δυνατότητα στους εργαζομένους να συνδέονται απομακρυσμένα σαν να βρίσκονται στο lan της εταιρείας. Τα ιδιωτικά δίκτυα VPN στηρίζονται στην πλειονότητα των περιπτώσεών τους σε μισθωμένες γραμμές ενώ έχουν αποτελέσει μία αξιόπιστη εναλλακτική λύση ενός δικτύου WAN επεκτείνοντας έτσι τα ιδιωτικά δίκτυα που κάνουν χρήση μισθωμένων γραμμών και εξυπηρετούν στις τηλεπικοινωνιακές συνδέσεις ενός ή περισσότερων σημείων χρησιμοποιώντας τη δομή που ήδη υπάρχει σε ένα δίκτυο. Τα πρώτα ιδιωτικά δίκτυα εμφανίστηκαν το 1960. Οι μισθωμένες γραμμές κατά τον Peterson P.(2007), μπορούν να χρησιμοποιηθούν για σύνδεση τηλεφωνικών κέντρων, επικοινωνία μέσω τηλεφώνου χρήση fax, μετάδοση δεδομένων, σύνδεση με το διαδίκτυο, σύνδεση με δημόσια ή ιδιωτικά δίκτυα. Το πρωτόκολλο IP αποτελεί το βασικό πρωτόκολλο για τη διασύνδεση ηλεκτρονικών υπολογιστών τα οποία μπορεί να είναι συνδεδεμένα σε ένα δίκτυο, είτε στο ίδιο δίκτυο είτε σε διαφορετικά. Το MPLS στηρίζεται στη λογική διαχείρισης των labels, αποτελείται δηλαδή από μια διαχείριση βασισμένη σε ετικέτες, κατά την οποία τοποθετείται ένα μοναδικό label σε κάθε πακέτο και θα χρησιμοποιείται ώστε να μεταφέρει και να δρομολογήσει το πακέτο μέσω του δικτύου. Παρόμοιες τεχνολογίες που υπήρξαν στο παρελθόν και που βασιζόταν στη διαχείριση ετικετών ήταν το X.25, το Frame Relay και

το ATM. Στα μέσα τις δεκαετίας του ΄90 υπήρξαν διαφορές ενέργειες από εταιρίες όπως η Cisco, η Nokia και η IBM με σκοπό να βελτιώσουν την απόδοση των δρομολογητών και να παρέχουν (QoS). Το 1997 η τεχνολογία μετατροπής ετικετών τυποποιήθηκε από την Internet Engineering Task Force – IETF, η IETF ανέπτυξε το MPLS το οποίο στην πορεία εξελίχθηκε ως μία από τις πιο σημαντικότερες δικτυακές εξελίξεις των τελευταίων χρόνων. Δημιουργήθηκε με σκοπό να τονώσει την απόδοση του παραδοσιακού IP παρέχοντας την ίδια στιγμή καινοτόμες διαδικτυακές υπηρεσίες με τεχνολογικά συστατικά (Susanto et al, 2011). Η υποστήριξη Traffic engineering και του QoS είναι μερικά ενδεικτικά παραδείγματα υπηρεσιών χάρη στα οποία το πρωτόκολλο MPLS έχει επικρατήσει καθώς είναι ανώτερο από οποιαδήποτε υπάρχουσα IP τεχνολογία. Λόγω σχεδιασμού, το πρωτοκόλλου MPLS έχει καταφέρει να είναι ανεξάρτητο από το Επίπεδο 2. Το IPVPN υπήρξε παλαιότερη τεχνολογία δικτύωσης που έδινε στους χρήστες τη δυνατότητα να συνδέονται μέσω μιας δημόσιας σύνδεσης στο διαδίκτυο, με το κύριο δίκτυο τους εξ αποστάσεως. Τα IP VPN ανήκουν στο επίπεδο 3 και 4 του OSI Model, αυτό σημαίνει ότι δημιουργούν μια σύνδεση μέσω δημόσιου διαδικτύου και χρησιμοποιούν μια δημόσια πύλη για σύνδεση. Χρησιμοποιώντας μια δημόσια πύλη, τα IPVPNs ήταν εκτεθειμένα σε επιθέσεις DoS (Denial of Service) με αποτέλεσμα να μειώνουν τις ταχύτητες απόκρισης των συστημάτων έως και την κατάρρευση τους, γιατί γίνεται χρήση του ωφέλιμου εύρους ζώνης. Ένα ακόμη βασικό μειονέκτημα του IPVPNs είναι ότι δεν μπορεί να παρέχει Quality of Services στις διαδικτυακές υπηρεσίες. Σε αντίθεση με το IPVPN το MPLS VPN λειτουργεί στο επίπεδο 2, που σημαίνει ότι αποφεύγει το δημόσιο διαδίκτυο ταξιδεύοντας σε ιδιωτική σύνδεση σε κάθε απομακρυσμένο χώρο, έτσι τα ζωτικά δεδομένα του εκάστοτε οργανισμού παραμένουν ασφαλή. Το MPLSVPN χρησιμοποιεί δυνατότητες του MPLS που δίνουν προτεραιότητα στην κίνηση στο δίκτυο της εταιρείας, έτσι το εύρος ζώνης για σημαντικές εφαρμογές όπως η τηλεδιάσκεψη και η φωνή είναι πλέον εγγυημένα. (Νικολόπουλος, 2019).

Ορολογία και στοιχεία ενός MPLS δικτύου

Είναι ιδιαίτερα σημαντικό πριν προχωρήσουμε στην ανάλυση λειτουργίας της τεχνολογίας του MPLS θα να αναφερθούν ορισμένα από τα βασικά στοιχεία ενός MPLS δικτύου.

• Forwarding Equivalence Class – FEC: Είναι ένα σύνολο πακέτων που προωθούνται με τον ίδιο τρόπο. Τα πακέτα δρομολογούνται από το ίδιο μονοπάτι. Τα FECs βασίζονται στις απαιτήσεις εξυπηρέτησης για σύνολο πακέτων ή κάποιο πρόθεμα της διεύθυνσης.

• MPLS Label: Μια ετικέτα με σταθερού μήκους επικεφαλίδα. Χρησιμοποιείται για την προώθηση των πακέτων στο MPLS δίκτυο. Η διάταξή της εξαρτάται από τα χαρακτηριστικά του δικτύου, και αποτελείται από 32-bit. Η κάθε επικεφαλίδα είναι μοναδική.

• Label Switched Path – LSP: Το μονοπάτι που ορίζεται από όλες τις ετικέτες που ανατίθενται ανάμεσα σε δύο σημεία. Μπορεί να είτε στατικό είτε δυναμικό.

• Label Switched Hop: Το hop μεταξύ δύο MPLS κόμβων στο οποίο η προώθηση γίνεται με χρήση ετικετών.

• Label Distribution Protocol – LDP: Αφορά την επίτευξη της επικοινωνίας μεταξύ των συσκευών που βρίσκονται στα άκρα του δικτύου και των αντίστοιχων που ανήκουν στο δίκτυο κορμού.

• Label Switch Router – LSR: Πρόκειται για τη συσκευή του δικτύου κορμού που πραγματοποιεί τη μεταγωγή των πακέτων που έχουν πλέον ετικέτες σύμφωνα με πίνακες μεταγωγής. Είναι ένας δρομολογητής υψηλής ταχύτητας στον πυρήνα κάποιου MPLS δικτύου ο οποίος συμμετέχει στην αναγνώριση των LSPs χρησιμοποιώντας το κατάλληλο πρωτόκολλο σηματοδοσίας ετικετών και μεταγωγή υψηλής ταχύτητας των δεδομένων που βασίζεται στα εγκατεστημένα μονοπάτια.

• Label Edge Router – LER (ή Edge LSR): Η συσκευή στο άκρο του δικτύου που πραγματοποιεί την αρχική επεξεργασία και κατηγοριοποίηση του πακέτου και εφαρμόζει την πρώτη ετικέτα. Αυτή η συσκευή μπορεί να είναι είτε ένας δρομολογητής, ή ένα switch με ενσωματωμένες ιδιότητες δρομολόγησης. Πρόκειται για τη συσκευή στην οποία ξεκινά και τερματίζεται ένα LSP. Ένας LER υποστηρίζει πολλαπλές θύρες (ports) συνδεδεμένες σε διαφορετικά δίκτυα (όπως Frame Relay, ATM, και Ethernet) και προωθεί την κυκλοφορία πάνω στο MPLS δίκτυο μετά την αναγνώριση των LSPs, χρησιμοποιώντας πρωτόκολλο σηματοδοσίας ετικέτας κατά την είσοδο.

• Ingress LER: Λαμβάνει δεδομένα από την IP πηγή και τα κατηγοριοποιεί για μετάδοση μέσα στο δίκτυο.

• Egress LER: Το αντίστοιχο του ingress LER το οποίο τερματίζει ένα LSP και προωθεί τα IP δεδομένα στον προορισμό.

• Label Information Base - LIB: Η βάση των πληροφοριών σχετικά με τις ετικέτες. Καθένας LSR κατασκευάζει έναν πίνακα για να καθορίσει πώς θα πρέπει να προωθηθεί κάποιο πακέτο. Αυτός ο πίνακας, ο οποίος καλείται Βάση Πληροφοριών Ετικέτας. Αποτελείται από αντιστοιχήσεις ετικετών σε ισοδύναμες κλάσεις προώθησης.

• MPLS Domain: αποτελείται από ένα σύνολο κόμβων που πραγματοποιούν MPLS δρομολόγηση και προώθηση.

• Label merging: Η αντικατάσταση πολλαπλών εισερχόμενων labels για μια FEC από μία μόνο εξερχόμενη ετικέτα.

• Label swap: Η βασική λειτουργία προώθησης που περιλαμβάνει την επεξεργασία μίας εισερχόμενης ετικέτας για να καθορίζει την εξερχόμενη ετικέτα, το port και άλλες πληροφορίες διαχείρισης.

MPLS

Κύριο στόχο του MPLS υπήρξε η επιτάχυνση της προώθησης των πακέτων, στην πορεία όταν το διαδίκτυο μεγάλωσε πολύ και επεκτάθηκε άρχισε να χρησιμοποιείται περισσότερο για την επίτευξη ρητής δρομολόγησης, το σχεδιασμό κίνησης και τη δημιουργία ιδιωτικών νοητών δικτύων καθώς αλλά και για την υποστήριξη κλάσεων υπηρεσίας. Το MPLS προτυποποίηθηκε από την IETF μέσω διαφόρων RFC με κυριότερα :

1. RFC 3031 MPLS Architecture
2. RFC 3032, Label Stack encoding
3. RFC 3036 LDP specification

Για την περίπτωση της μεταγωγής κυκλώματος, οποιοδήποτε μη χρησιμοποιημένο εύρος ζώνης ξοδεύεται άχρηστα και μπορεί να χρησιμοποιηθεί από άλλα πακέτα και από άλλες

πηγές κατευθυνόμενα σε διαφορετικούς προορισμούς και με τους οποίους μοιράζονται ένα μέρος και μόνο της διαδρομής (Νικολόπουλος, 2019). Λόγω του ότι δεν αφιερώνονται κάποια συγκεκριμένα κυκλώματα, υπάρχει πάντα η περίπτωση να υπάρξει ένα απρόσμενο κύμα αυξημένης κίνησης σε κάποια από πολλαπλές εισόδους, κατ' επέκταση να κατακλύσει κάποιες από τις εξόδους ενός κόμβου με αποτέλεσμα να ξεπεραστεί κατά πολύ η διαθέσιμη χωρητικότητα bandwidth της συγκεκριμένης εξόδου. Αυτό λοιπόν έχει ως αποτέλεσμα να προκύψει απώλεια πακέτων. Το πρόβλημα αυτό οφείλεται στην αδυναμία εκτίμησης της κίνησης, διότι δεν έχει προηγηθεί κατά την έναρξη της κλήσης κάποια συνεννόηση και αυτό έχεις ως αποτέλεσμα να υπάρχουν μεγάλες πιθανότητες συμφόρησης και υπερχείλισης των κόμβων. Αντίθετα, με τη χρήση ρητής επιλογής διαδρομών ώστε να μοιραστεί η κίνηση σε διαφορετικές διαδρομές (σχεδιασμός κίνησης - traffic engineering), όπου ο φόρτος των κόμβων γίνεται προβλέψιμος. Αυτό διότι, αφενός γίνεται εφικτή η αναγγελία των απαιτούμενων πόρων κατά την εγκατάσταση του νοητού κυκλώματος και δεν αποφασίζεται ο επόμενος κόμβος με λογική βήμα -βήμα όπως στο IP routing. Σε συνδυασμό με ένα πεδίο που δείχνει την κλάση υπηρεσίας στην ετικέτα και τη χρήση μηχανισμών διαχείρισης προτεραιοτήτων στις ουρές, επιτρέπουν στο MPLS να υποστηρίξει υπηρεσίες φωνής και βίντεο που δεν μπορούν να μεταδοθούν ικανοποιητικά μέσω μηχανισμών που βασίζονται σε απώλειες και αναμεταδόσεις πακέτων. Οι υπηρεσίες αυτές πρέπει να έχουν εξασφαλισμένους πόρους και σε αντίθετη περίπτωση να απορρίπτονται αντί να εμφανίζουν διακοπές που τις καθιστούν δύσχρηστες (Νικολόπουλος, 2019). Με τη χρήση του MPLS μπορούν να υπάρχουν πολλά είδη κυκλοφορίας στο ίδιο δίκτυο και επίσης η διαχείριση της κυκλοφορίας και της καλύτερης απόδοσης μπορούν να γίνουν πιο εύκολα. Το MPLS, ως πρωτόκολλο, έχει τη δυνατότητα να συνδυάζει τη μεταγωγή ετικετών και τη δρομολόγηση του IP. Η μεταγωγή επιτυγχάνεται προσθέτοντας στην αρχή του κάθε πακέτου μια ετικέτα. Όταν αυτό εισέρχεται στο MPLS δίκτυο τότε μια ετικέτα προστίθεται και ορίζει σε κάθε δρομολογητή την απόφαση για το πώς αυτό το πακέτο θα δρομολογηθεί καθορίζοντας έτσι ότι η δρομολόγηση θα εξαρτάται πλέον από αυτήν την ετικέτα. Κάθε δρομολογητής όταν λάβει ένα τέτοιο πακέτο το δρομολογεί με βάση την ετικέτα αυτή και όχι με βάση την διεύθυνση ip. Η τεχνική αυτή τα τελευταία χρόνια έχει γίνει αρκετά δημοφιλής και έχει πολύ μεγάλη χρήση σε δίκτυα κορμού πάνω από τα οποία περνά μεγάλος όγκος κίνησης.

Παλαιότερα, είχε πολύ μεγάλη χρήση στα δίκτυα X.25 και ATM δίκτυα ενώ μετέπειτα πήρε μια διαφορετική μορφή στο MPLS η οποία ήταν προσαρμοσμένη στις συνθήκες των δικτύων κορμού και στη διαβίβαση των πακέτων IP. Το πρωτόκολλο MPLS συνδυάζει τη διαχείριση του εύρους ζώνης (bandwidth) αλλά και τις απαιτήσεις εξυπηρέτησης για IP δίκτυα. Το MPLS έχει αποτελέσει μια τεχνολογία η οποία ενοποιώντας τη λειτουργικότητα των επιπέδων δικτύου (network layer στο μοντέλο ISO/OSI) και διασύνδεσης δεδομένων στοχεύει στη βελτίωση της απόδοσης και της προώθησης των IP πακέτων και στην υποστήριξη των εξελιγμένων χαρακτηριστικών του επιπέδου δικτύου. Σε συνδυασμό με τα υπάρχοντα δίκτυα IP, μπορεί να προσφέρει αξιοπιστία, ποιότητα υπηρεσίας αλλά και χαρακτηριστικά όπως η προσανατολισμένη προώθηση στη σύνδεση των τεχνολογιών μεταγωγής του επιπέδου διασύνδεσης δεδομένων, ενώ παράλληλα μπορεί να διατηρεί και την ευελιξία της δρομολόγησης. Η αρχιτεκτονική του MPLS έχει ομοιότητες σε ορισμένα σημεία με αυτή του DiffServ (Differentiated Services).Λόγω αυτού του μαρκαρίσματος που πραγματοποιείται, το MPLS πρωτόκολλο στην αρχιτεκτονική του θα μπορούσε να ειπωθεί ότι έχει ορισμένες ομοιότητες με αυτή του DiffServ. Η κίνηση που μεταφέρεται μέσα στο δίκτυο MPLS εισέρχεται μαρκαρισμένη ενώ κατά την έξοδο από αυτό, την επαναφέρει στην αρχική της μορφή. Το πρωτόκολλο MPLS έχει την ιδιαιτερότητα ότι δεν ελέγχεται ούτε εξαρτάται από τις εφαρμογές. Το MPLS θα μπορούσε να ειπωθεί ότι ανήκει μόνο στους δρομολογητές και είναι ανεξάρτητο από τα δικτυακά πρωτόκολλα, ενώ έχει τη δυνατότητα να χρησιμοποιηθεί με αρκετά από αυτά (ATM, PPP, Frame-Relay, Ethernet και Token ring). Μπορεί επίσης και συνδυάζει την τεχνολογία μεταγωγής του επιπέδου διασύνδεσης δεδομένων με τις δικτυακές υπηρεσίες του επιπέδου δικτύου, ενώ παράλληλα μειώνει την πολυπλοκότητα. Το MPLS δεν αντικαθιστά την IP δρομολόγηση, αλλά μπορεί να λειτουργήσει παράλληλα με υπάρχουσες και μελλοντικές τεχνολογίες δρομολόγησης με κύριο στόχο την προώθηση δεδομένων με υψηλή ταχύτητα και τη δέσμευση του εύρους ζώνης για ροές κυκλοφορίας οι οποίες έχουν διαφορετικές απαιτήσεις και ποιότητα υπηρεσίας. Το MPLS δίνει στα σημερινά δίκτυα τη δυνατότητα να αντιμετωπίσουν ορισμένες μεγάλες προκλήσεις όπως είναι για παράδειγμα η λειτουργικότητα, η κλιμάκωση (Scalability) και η δυνατότητα αλλαγής και επέκτασης των δικτύων αποφεύγοντας τη μεγάλη αποδιοργάνωση ή διακοπή τους.

Για τη σωστή λειτουργία ενός MPLS δικτύου θα πρέπει να πληρούνται όμως ορισμένες προϋποθέσεις έτσι ώστε να μπορεί να επιφέρει τα επιθυμητά αποτελέσματα. Πιο συγκεκριμένα, οι τεχνολογίες κορμού από τη μεριά του παρόχου θα πρέπει να μπορούν να λειτουργούν ανεξάρτητα από τα υποκείμενα πρωτόκολλα δρομολόγησης και θα πρέπει να υπάρχει μηχανισμός έτσι ώστε να αποφεύγονται τα routing loops. Επίσης, πρέπει να επιτρέπεται 'προώθηση συνόλων' (aggregate forwarding) των δεδομένων, να επιτρέπει δηλαδή τη μεταφορά πολλαπλών ροών δεδομένων ώστε να εξασφαλίζει ότι το σύνολο των συγκεκριμένων ροών θα ακολουθεί ένα συγκεκριμένο μονοπάτι. Οι MPLS τεχνολογίες του δικτύου κορμού θα πρέπει να μπορούν να λειτουργούν και με unicast αλλά και multicast ροές δεδομένων. Επιπλέον τα MPLS switches θα πρέπει να μπορούν να συνυπάρχουν με non-MPLS switches στο ίδιο δίκτυο, χωρίς να τους προσθέτουν απαίτηση για επιπλέον διαμόρφωση και τέλος, το MPLS πρέπει να μπορεί να χρησιμοποιηθεί στο ίδιο δίκτυο στο οποίο λειτουργούν ταυτόχρονα πρωτόκολλα επιπέδου διασύνδεσης δεδομένων.

Αρχιτεκτονική MPLS

Κύρια στοιχεία στην αρχιτεκτονική του MPLS αποτελούν τα εξής:

1. Πρωτόκολλα δρομολόγησης
2. Προώθηση επιπέδου δικτύου
3. Μεταγωγή βασισμένη σε ετικέτες
4. Σχηματισμός ετικετών
5. Πρωτόκολλο σηματοδοσίας για διανομή ετικετών
6. Έλεγχος κυκλοφορίας
7. Συμβατότητα με διάφορες τεχνολογίες (ATM, frame relay, PPP)

Η δρομολόγηση στο MPLS γίνεται είτε στατικά είτε με κάποιο δυναμικό πρωτόκολλο όπως για παράδειγμα OSPF, BGP, EIGRP.κλπ. Για να επιτύχει μια αξιόπιστη μετάδοση δεδομένων κατά τη διάρκεια μιας συνόδου από έναν LSR σε έναν άλλο, το LDP χρησιμοποιεί το πρωτόκολλο TCP. Το LDP συντηρεί επίσης την LIB ενώ χρησιμοποιεί το πρωτόκολλο UDP κατά τη διάρκεια της αναζήτησης. Ο LSR ανταλλάσσει πακέτα hello και προσπαθεί να βρει την ταυτότητα των γειτόνων του καθώς επίσης και να σηματοδοτεί

την παρουσία του στο δίκτυο. Το IP Fwd είναι το κλασικό πρωτόκολλο προώθησης σε IP δίκτυα, το οποίο αναζητά το επόμενο βήμα χρησιμοποιώντας ταίριασμα της μεγαλύτερου μεγέθους διεύθυνσης (longest match address) στον πίνακά του. Σε ένα MPLS αυτό γίνεται από τους ακραίους δρομολογητές (LERs). Το MPLS Fwd είναι πρωτόκολλο προώθησης που συνδυάζει την ετικέτα της θύρας εισόδου με μια θύρα εξόδου για κάποιο δεδομένο πακέτο. Οι βασικές εφαρμογές του MPLS είναι:

1. IP over ATM
2. Traffic Engineering
3. MPLS VPNs
4. Class of Service / QoS

Πλεονεκτήματα

Τα σημαντικότερα πλεονεκτήματα του MPLS στα σημερινά δίκτυα είναι η υποστήριξη πολλαπλών πρωτοκόλλων (FECs) τα οποία βασίζονται σε πρωτόκολλα επιπέδου δικτύου και σε πληροφορίες που σχετίζονται με πρωτόκολλα δρομολόγησης, παρέχει επίσης ανεξαρτησία του επιπέδου διασύνδεσης δεδομένων και έχει συνεργασία με κάθε τεχνολογία επιπέδου διασύνδεσης, όπως το ATM, το Frame Relay, το Packet-over-SONSET, το Ethernet, έχει επίσης αυξημένη απόδοση λόγω της απλοποιημένης προώθησης πακέτων, σημαντικό πλεονέκτημα επίσης αποτελεί η ρητή δρομολόγηση, ακόμη να σημειωθεί ότι δεν υπάρχει η επιβάρυνση της επεξεργασίας των επικεφαλίδων για κάθε πακέτο. Το MPLS καθιστά την εξέλιξη των δικτύων αρκετά εύκολη, με λιγότερο κόστος. Επίσης είναι λιγότερο ευάλωτο σε λάθη. Ο έλεγχος κυκλοφορίας που παρέχει αφορά κυρίως στη διαδικασία της επιλογής των μονοπατιών για την κυκλοφορία των δεδομένων ώστε να εξισορροπηθεί ο φόρτος της κυκλοφορίας σε διάφορες συνδέσεις, δρομολογητές, και μεταγωγές μέσα στο δίκτυο. Αυτό έχει ως αποτέλεσμα την αυξανόμενη σπουδαιότητα εξαιτίας της αστραπιαίας ανάπτυξης του Internet και την αντίστοιχη απαίτηση για εύρος ζώνης.

Οι στόχοι του ελέγχου κυκλοφορίας μπορούν να ταξινομηθούν ως εξής:

- Προσανατολισμός στην κυκλοφορία

- Προσανατολισμός στους πόρους
- Έλεγχος κυκλοφορίας.

Τα ρητά μονοπάτια μεταγωγής ετικετών μπορούν να συσχετίζονται με κάποια από τις πολλές ιδιότητες κυκλοφορίας που υπάρχουν στο MPLS για την υποστήριξη διαφορετικών τύπων κυκλοφορίας. Βασικές λειτουργίες όπως η δημιουργία, η ενεργοποίηση, η απενεργοποίηση, η μεταβολή ιδιοτήτων, η επαναδρομολόγηση και η καταστροφή γραμμής κυκλοφορίας. Επίσης η ροή δεδομένων από οποιοδήποτε κόμβο εισόδου σε οποιοδήποτε κόμβο εξόδου μπορούν να προσδιοριστούν αυτόνομα με υποστήριξη των πολλαπλών τύπων κυκλοφορίας διότι υποστηρίζει όλους τους τύπους προώθησης, Unicast και Multicast και μπορεί να ελέγχει ολόκληρο το μονοπάτι ενός πακέτου χωρίς να καθορίζει ρητώς τους ενδιάμεσους δρομολογητές.

Μειονεκτήματα

Το MPLS όπως και οι άλλες τεχνολογίες δεν έχει μόνο πλεονεκτήματα, αλλά και μειονεκτήματα. Ορισμένα από αυτά είναι η υψηλή χρήση σε μνήμη αλλά και σε επεξεργαστή για το δρομολογητή. Παρέχεται επίσης με πολύ υψηλότερο κόστος σε σχέση με την παροχή Internet διότι παρέχει εγγυημένο bandwidth και κλάσεις ανά υπηρεσία. Κάθε VRF, αποτελεί ένα κλειστό ιδεατό δίκτυο και είναι τοπολογίας full mesh. Επίσης σε περίπτωση που υπάρξει ανάγκη πρόσβασης στο διαδίκτυο για τους χρήστες του συγκεκριμένου VRF, τότε θα πρέπει να έχει προβλεφθεί και να υλοποιηθεί μια ξεχωριστή δρομολόγηση σε κάποιον δρομολογητή που έχει πρόσβαση στο διαδίκτυο με εσωτερική διασύνδεση στο κεντρικό σημείο ή με τη χρήση NAT over proxy καθώς στο MPLS αφορά μόνο κλειστού τύπου VPN και επιτρέπει την επικοινωνία αποκλειστικά και μόνο εντός του συγκεκριμένου VRF. Το NAT over Proxy, είναι μια αρχιτεκτονική που επιτρέπει κατ' επιλογή του διαχειριστή να υπάρχει μερική πρόσβαση προς συγκεκριμένους προορισμούς του διαδικτύου. Αυτό οφείλεται στο γεγονός ότι το MPLS είναι Private VPN.

Λειτουργία του MPLS

Η ταμπέλα (tag) που τοποθετεί το MPLS σε κάθε πακέτο όπως φαίνεται στην παρακάτω εικόνα ξεκινά πάντα με το πεδίο της ετικέτας το οποίο αποτελείται από 20 bits και στη συνέχεια ακολουθεί το πεδίο που περιλαμβάνει το CoS (Class of Service) 3 bits έπειτα ακολουθεί το πεδίο S (stack) 1 bit και τέλος υπάρχει το πεδίο TTL, 8 bits.

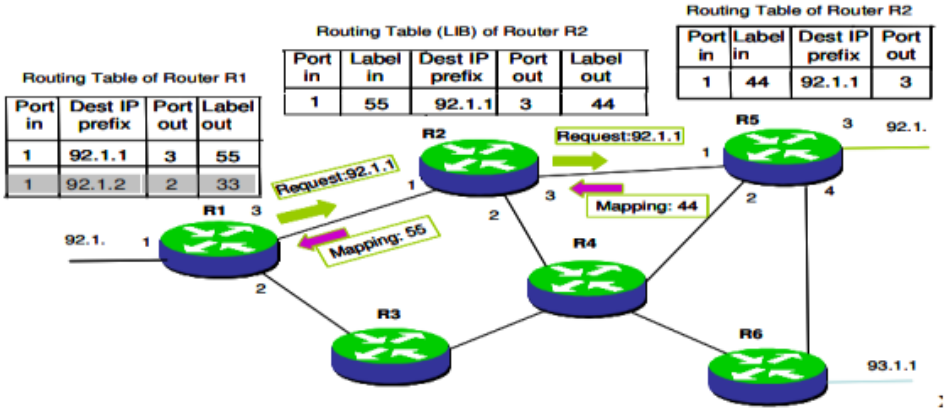
Εικόνα 1 Μορφή ετικέτας MPLS

S (stack): Επιτρέπει την προσθήκη πολλών ετικετών οι οποίες είναι ενθυλακωμένες η μία μέσα στην άλλη, όταν το πεδίο παίρνει τιμή 1 στον πάτο της στοίβας, ενώ παίρνει τιμή 1 στην πιο εσωτερική ετικέτα.

TTL: Μειώνεται με κάθε προώθηση και εάν φθάσει στο 0, τότε το πακέτο απορρίπτεται, ενώ το CoS ορίζει οκτώ επίπεδα προτεραιότητας έτσι ώστε τα πιο σημαντικά πακέτα να προωθούνται πρώτα.

Η μετάδοση δεδομένων στο MPLS επιτυγχάνεται με μονοπάτια μεταγωγής ετικέτας (LSPs - Label Switched Paths) τα οποία δημιουργούνται είτε πριν την εκπομπή δεδομένων ή με την ανίχνευση του πρώτου πακέτου μιας ροής δεδομένων. Οι δρομολογητές αυτοί διακρίνονται στους ακραίους (LER- Label Edge Routers) και στους εσωτερικούς που ονομάζονται LSR (Label Switched Routers). Η αρμοδιότητα των εσωτερικών είναι η επιλογή της πόρτας εξόδου και η επικόλληση της ετικέτας εξόδου βάσει της πόρτας εισόδου αλλά και της τιμής της ετικέτας εισόδου. Οι ετικέτες διανέμονται μέσω του πρωτόκολλου διανομής ετικετών (LDP – Label Distribution Protocol) ενώ όλα τα πακέτα τα οποία ανήκουν στην ίδια ροή, που χαρακτηρίζεται στο IP από το κοινό πρόθεμα της αρχικής διεύθυνσης IP, δρομολογούνται με τον ίδιο τρόπο μέχρι να φτάσουν στον τελικό τους προορισμό και θεωρούνται ότι ανήκουν στην ίδια κλάση ισοδύναμης προώθησης, FEC Forwarding Equivalence Class. Το FEC προσδιορίζει διαδοχή ζεύξεων, των ετικετών που χρησιμοποιούνται σε κάθε ζεύξη και μία διαδρομή που διασχίζει το υποδίκτυο MPLS

από ένα ακραίο LER σε ένα άλλο. Όταν ένας ακραίος δρομολογητής λαμβάνει το πακέτο, πραγματοποιείται ένας έλεγχος στο πρόθεμα προορισμού IP έτσι ώστε να αποδώσει μία ετικέτα, εκτός βέβαια εάν έχει ήδη δημιουργηθεί η FEC και οι ετικέτες είναι πλέον γνωστές. Σε ένα πακέτο που έχει τοποθετηθεί μια ετικέτα, η διαδρομή του δικτύου καθορίζεται αυτόματα και είναι η συγκεκριμένη FEC. Οι ετικέτες έχουν μόνο τοπικό χαρακτήρα και αλλάζουν σε κάθε βήμα δρομολόγησης.



Εικόνα 2Λειτουργία MPLS

Βάσει της παραπάνω εικόνα 2 οι ενέργειες που πραγματοποιούνται για τη δρομολόγηση ενός πακέτου μέσω των δρομολογητών R1-R2-R5, οι R1και R5 είναι LER και LSR είναι ο R2. Στην εικόνα 2 παρατηρούμε ότι , οι LSR είναι περισσότεροι γιατί μία περιοχή MPLS αποτελείται από πολλούς δρομολογητές και όχι μόνο από 6, έτσι ένα πακέτο IP φθάνει στον δρομολογητή R1 υποθέτοντας ότι όλοι οι πίνακες είναι συνήθεις πίνακες IP όπου έχουν δημιουργηθεί με το δυναμικό πρωτόκολλο OSPF. Οι θέσεις των ετικετών είναι κενές εφόσον ακόμα δεν έχει δημιουργηθεί κάποια καταχώρηση ετικετών. Έτσι, ο R1 βλέπει το πρόθεμα 92.1 από την πύλη 1. Βλέπει επίσης ότι πρέπει να το προωθήσει προς το R2 και ταυτόχρονα ζητά με το πρωτόκολλο LDP να γίνει εκχώρηση ετικέτας από τον δρομολογητή R2, ο οποίος ανταποκρίνεται βάζοντας την ετικέτα 55 την οποία στη συνέχεια ο R1 της καταχωρεί στον πίνακα δρομολόγησης ενώ πλέον προωθεί το πακέτο έχοντας πλέον επισυνάψει την ετικέτα. Το ίδιο στη συνέχεια γίνεται και μεταξύ του δρομολογητή R2 και του δρομολογητή R5 που καταλήγει στην ετικέτα 44 για τη ζεύξη μεταξύ τους. Πλέον έχει δημιουργηθεί μία κλάση προώθησης (FEC) μεταξύ των δρομολογητών R1-R2-R5 με ετικέτες 55 για το πρώτο σκέλος και 44 για το δεύτερο

σκέλος. Από εδώ και στο εξής οι δρομολογητές LSR μπορούν πλέον να δρομολογούν με μια απλή ανάγνωση του πίνακα δρομολόγησης και ανταλλαγή των ετικετών. Αυτό αποτελεί μια αναζήτηση με ακριβή ταύτιση που μπορεί να γίνει με μια απλή και φθηνή RAM όπου η διεύθυνση είναι η πόρτα και η ετικέτα εισόδου και τα περιεχόμενα δίνουν την πόρτα εξόδου και την νέα ετικέτα. οι ακραίοι (LER) θα εξακολουθήσουν να λειτουργούν σαν απλοί δρομολογητές IP και θα εκτελούν προώθηση με μεγίστου μήκους ταύτιση που είναι ακριβή και χρησιμοποιεί ειδικά πολύπλοκα κυκλώματα. Σε ένα τέτοιο περιβάλλον, η διαδρομή που θα ακολουθήσει ένα πακέτο είναι ίδια με αυτή που θα ακολουθούσε εάν δε χρησιμοποιούνταν η μέθοδος αυτή. Αυτό που είναι διαφορετικό είναι ουσιαστικά ο αλγόριθμος προώθησης που έγινε πιο απλός αλλά και πιο φθηνός. Μία άλλη σημαντική συνέπεια είναι ότι οι συσκευές που δεν ήξεραν μέχρι πρότινος πώς να προωθήσουν πακέτα IP πλέον μπορούν να χρησιμοποιηθούν και να προωθήσουν την κυκλοφορία IP σε ένα MPLS δίκτυο.

Ρητή Δρομολόγηση

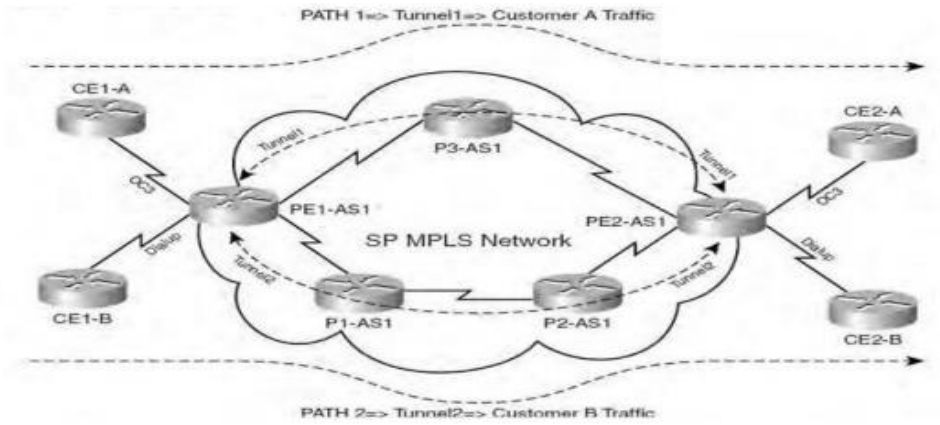
Αρχικά, το IP είχε μία δυνατότητα δρομολόγησης προέλευσης (source routing) οπου η πηγή μπορούσε να προσδιορίσει εξ αρχής τη διαδρομή και να μην αφήσει να γίνει η επιλογή της από το OSPF. Αυτό όμως περιορισμένη χρήση κυρίως για λόγους δυσκολίας στον εντοπισμό προβλημάτων από τους διαχειριστές. Η MPLS τεχνολογία δίνει πλεόν τη δυνατότητα αυτή άλλα με έναν πιο ευέλικτο τρόπο. Η δρομολόγηση αυτή ονομάζεται ρητή δρομολόγηση (explicit routing). Υπάρχει διαφορά στο ότι δεν είναι συνήθως η προέλευση του πακέτου που θα καθορίζει τη διαδρομή. Αυτό γίνεται συνήθως σε κάποιον από τους δρομολογητές εντός του δίκτυου υπηρεσιών του παρόχου (Internet Service Provider). Όπως φαίνεται στο σχήμα της εικόνας 2 , υπάρχουν δύο διαδρομές για το πρόθεμα 92.1 έτσι διαμοιράζεται η κίνηση μέσω των δρομολογητών R1- R2-R5 για το πρόθεμα 92.1.1 και μέσω των δρομολογητών R1-R3-R4-R6 για το 92.1.2. παρατηρείται ότι αυτό μπορεί να γίνει προσθέτοντας τη δεύτερη καταχώρηση στον πίνακα προώθησης του δρομολογητή R1 και δημιουργώντας μια δεύτερη FEC ακολούθως δημιουργώντας τις κατάλληλες ετικέτες στους πίνακες των δρομολογητων R3-R4. Αυτό θα ήταν δύσκολο να γίνει για το IP στην κανονική δρομολόγηση IP, επειδή ο R1 κανονικά δεν εξετάζει την προέλευση της

κυκλοφορίας όταν γίνεται λήψη των αποφάσεων προώθησης. Έτσι, το πρωτόκολλο που χρησιμοποιείται για την εργασία αυτή είναι το Πρωτόκολλο δέσμευσης Πόρων (Resource Reservation Protocol, RSVP). Το πρωτόκολλο αυτό δίνει τη δυνατότητα να σταλεί ένα μήνυμα RSVP κατά μήκος μίας καθορισμένης διαδρομής και να χρησιμοποιηθεί ώστε να διαμορφωθούν οι καταχωρίσεις του πίνακα προώθησης ετικετών για τη συγκεκριμένη διαδρομή σε όλο το μήκος της. Η ρητή δρομολόγηση συμβάλει αρκετά στο να γίνουν τα δίκτυα πιο ανθεκτικά σε περίπτωση κάποια αστοχίας, λόγω της δυνατότητας επαναδρομολόγησης που παρέχει. Είναι δυνατό να υπολογίσει εκ των προτέρων τις εναλλακτικές διαδρομές που θα χρησιμοποιηθούν εάν υπάρξει αστοχία σε κάποια ζεύξη. Χάρη στις δύο αυτές δυνατότητες που παρέχει την εκ των προτέρων εναλλακτική διαδρομή αλλά και τη ρητή δρομολόγηση πακέτων σε όλο το μήκος της διαδρομής, σημαίνει ότι η πρώτη δε θα χρειάζεται να περιμένει ώστε να διασχίσουν το δίκτυο τα πακέτα των πρωτοκόλλων δρομολόγησης, ή να εκτελεστούν αλγόριθμοι δρομολόγησης από διάφορους άλλους κόμβους στο δίκτυο. Μπορεί επομένως να μειώσει κατά πολύ το χρόνο που απαιτείται για την επαναδρομολόγηση των πακέτων με μια μόνο παράκαμψη συγκεκριμένου σημείου αστοχίας. Οι δρομολογητές έχουν τη δυνατότητα να χρησιμοποιήσουν αλγορίθμους ώστε να υπολογίσουν με αυτόματο τρόπο τις διαδρομές όπως για παράδειγμα το RSVP-TE (RSVP with Traffic Engineering) ή CSPF (constrained shortest path first). Πρώτα η υπολογίζεται η συντομότερη διαδρομή υπό περιορισμούς, η οποία έχει αρκτες ομοιότητες με το πρωτόκολλο OSPF λαμβάνει όμως υπόψη της και ορισμένους περιορισμούς που σχετίζονται με τη μέγιστη μεταφορική ικανότητα ή ακόμη και τις ιδιότητες των οπτικών ζεύξεων.

MPLS Traffic Engineering

Το MPLS Traffic Engineering (MPLS TE) πραγματοποιεί καταμερισμό της κίνησης μέσα στο δίκτυο έτσι ώστε να μπορούν να ικανοποιηθούν οι απαιτήσεις των εφαρμογών. Βασικός στόχος του είναι να δρομολογηθεί η κίνηση με τέτοιο τρόπο ώστε να μην υπάρχει συμφόρηση στο δίκτυο και να μην παρουσιαστεί ανάγκη για εφαρμογή άλλων σχημάτων QoS. Το MPLS χρησιμοποιεί την ικανότητα αυτή για να λαμβάνει πληροφορίες που παρέχονται από τα πρωτόκολλα δρομολόγησης layer 3 και λειτουργεί όπως το layer 2 του

δικτύου ATM. Βελτιστοποιεί την απόδοση λόγω της αντιστοίχισης των ροών κυκλοφορίας στην τοπολογία του δικτύου. Οι ικανότητες του είναι ενσωματωμένες στο layer 3 και μπορούν να εφαρμοστούν έτσι ώστε να είναι πιο αποδοτική η χρήση εύρους ζώνης μεταξύ των δρομολογητών στο δίκτυο των παρόχων υπηρεσιών. Τα δίκτυα αυτά απαιτείται να κάνουν υψηλή χρήση της δυνατότητας μετάδοσης και πρέπει να είναι πολύ ελαστικά, ώστε να μπορούν να αντιμετωπίσουν αποτυχίες συνδέσεων και κόμβων. Το Traffic Engineering είναι η μια ιδιότητα που η κίνηση κατευθύνεται πάνω στο κεντρικό δίκτυο κορμού (backbone) με σκοπό να γίνει η πιο αποδοτική χρήση του διαθέσιμου εύρους ζώνης μεταξύ των δρομολογητών. Πριν το MPLS Traffic Engineering, η λειτουργία αυτή γινόταν ή από το IP ή από το ATM. Εξαρτιόταν από το πρωτόκολλο που χρησιμοποιούνταν ανάμεσα στους 2 εξωτερικούς (edge) δρομολογητές του δικτύου. Αν και ο όρος «traffic engineering» έγινε γνωστός με την τεχνολογία του MPLS, το Traffic Engineering πρωτοεμφανίσθηκε στα δίκτυα IP και δίκτυα ATM. Στο IP εφαρμόστηκε για τη διαχείριση του κόστους των διεπαφών όταν υπήρχαν πολλά μονοπάτια μεταξύ δυο άκρων σε ένα δίκτυο. Οι στατικές δηλώσεις, αντίθετα, δρομολογούσαν την κίνηση πάνω σε ένα συγκεκριμένο μονοπάτι προς έναν προορισμό.



Εικόνα 3 Βασικό IP δίκτυο 2 πελατών

Το βασικό πλεονέκτημα του MPLS Traffic Engineering είναι ότι παρέχει συνδυασμό από των δυνατοτήτων των ATM Traffic Engineering και class of service (CoS). Στο MPLS Traffic Engineering, ο κεντρικός router στο δίκτυο ελέγχει τη διαδρομή που θα

ακολουθήσει η κίνηση προς έναν συγκεκριμένο προορισμό το δικτύου. Η εφαρμογή πλήρους πλέγματος VCs, όπως στο ATM, δεν υπάρχει όταν εφαρμόζεται MPLS Traffic Engineering. Για το λόγο αυτό, όταν εφαρμόζεται MPLS Traffic Engineering στο IP δίκτυο, μεταμορφώνεται σε μια περιοχή μεταφοράς ετικέτας, όπως φαίνεται στην τοπολογία της εικόνας 3, όπου τα μονοπάτια μεταφοράς Traffic Engineering (TE tunnels) (Tunnel1 and Tunnel2) καθορίζουν τις διαδρομές που μπορεί να χρησιμοποιηθούν για κίνηση μεταξύ των PE1-AS1 και PE2-AS1. Στην περίπτωση της δρομολόγησης IP προώθησης, τα πακέτα προωθούνται ανά hop και γίνεται ο έλεγχος της διαδρομής σε κάθε δρομολόγηση από την πηγή στον προορισμό. Η προώθηση επειδή είναι βασισμένη στον προορισμό οδηγεί στη χαμηλή αξιοποίηση του διαθέσιμου εύρους ζώνης ανάμεσα σε δύο δρομολογητές. Για την αποφυγή της απώλειας πακέτων λόγω ανεπαρκούς χρήσης του διαθέσιμου εύρους ζώνης αλλά και για την παροχή καλύτερης απόδοσης, εφαρμόζεται το Traffic Engineering ώστε να κατευθυνθεί μέρος της κίνησης από την κατάλληλη διαδρομή και να ενεργοποιείται η καλύτερη διαχείριση και χρήση του διαθέσιμου εύρους ανάμεσα σε ένα ζεύγος δρομολογητών. Το Traffic Engineering χαρτογραφεί τις ροές μεταξύ δύο δρομολογητών για να επιτρέψει κατάλληλα την αποδοτική χρήση του ήδη διαθέσιμου εύρους ζώνης στο δίκτυο κορμού. Σημαντικό επίσης για την εφαρμογή μιας αποδοτικής μεθοδολογίας Traffic Engineering στο δίκτυο κορμού είναι να συγκεντρωθούν οι πληροφορίες έτσι ώστε οι εγγυήσεις εύρους ζώνης να μπορούν να καθιερωθούν όπως φαίνεται στην τοπολογία τα Traffic Engineering (Tunnel 1 και Tunnel 2), μπορεί να καθοριστούν στο δρομολογητή PE1-AS1, να διαχωρίζουν τα πακέτα σε ξεχωριστά μονοπάτια (PATH1, PATH2) ενεργοποιώντας έτσι την αποδοτικότερη χρήση του διαθέσιμου εύρους. Τα Traffic Engineering Tunnels που ορίζονται στους δρομολογητές είναι μονής κατεύθυνσης. Έτσι, για να επιτευχθούν διπλής κατεύθυνσης Traffic Engineering τούνελ ανάμεσα στους δρομολογητές PE1-AS1 και PE2-AS1 ένα ζεύγος τούνελ πρέπει να καθοριστεί επίσης στον PE2-AS1 ομοίως με το Tunnel 1 και Tunnel 2 που ορίστηκαν στο PE1-AS1. Σε ένα MPLS δίκτυο, όλες οι σχετικές διαμορφώσεις τούνελ εκτελούνται πάντα στους δρομολογητές άκρων (PE) του παρόχου. Τα Traffic Engineering τούνελ ή LSPs θα χρησιμοποιηθούν για να συνδέσουν τους δρομολογητές άκρων μέσα από τον πυρήνα του δικτύου φορέων παροχής υπηρεσιών. Το MPLS Traffic Engineering μπορεί επίσης να καταταχτεί σε ορισμένες κατηγορίες κυκλοφορίας σε σχέση με τους

προορισμούς. Αν οι δρομολογητές του πελάτη A (CE routers) είναι συνδεδεμένοι στο δίκτυο του φορέα παροχής (SP) χρησιμοποιώντας κυκλώματα τύπου OC3 (ρυθμό μεταφοράς δεδομένων μέχρι 155,52 Mbit/s) σύνδεση και ο χρήστης B συνδέεται επίσης με το δίκτυο SP με 64 K dialup link, μπορεί να εφαρμοστεί προνομιακή μεταχείριση στα TE Tunnels ώστε το TE Tunnel 1 να μεταφέρει την κίνηση του πελάτη A και το Tunnel 2 αντίστοιχα την κίνηση του πελάτη B. Έτσι τα TE tunnels είναι ροές δεδομένων μεταξύ μιας συγκεκριμένης πηγής ενός προορισμού και μπορεί να διαθέτουν συγκεκριμένες ιδιότητες. Οι ιδιότητες αυτές που έχει ένα tunnel, εκτός από τα σημεία εισόδου και εξόδου του δικτύου, μπορεί να περιλαμβάνουν απαιτήσεις εύρους ζώνης και CoS (Class of Service) για τα δεδομένα που θα προωθηθούν. Η κίνηση προωθείται μέσω της διαδρομής που καθορίζεται ως TE tunnel, με τη χρήση του MPLS. Ως εκ τούτου, για τα TE tunnels ορίζονται συγκεκριμένα LSPs στο δίκτυο από την πηγή στον προορισμό, τα οποία είναι συνήθως συνδεδεμένα στα PE routers. Τα MPLS LSPs έχουν μια προς μία συσχέτιση με τα TE tunnels, και τα TE tunnels είναι συνδεδεμένα με μια συγκεκριμένη διαδρομή μέσω του Service Provider του δικτύου προς ένα PE router. Αν δεν καθοριστούν ρητά (explicitly), τα TE tunnels μπορούν να επαναδρομολογήσουν πακέτα μέσω οποιασδήποτε διαδρομής στο δίκτυο συσχετισμένης με ένα MPLS LSP. Αυτό το μονοπάτι μπορεί να καθοριστεί από το IGP που χρησιμοποιείται στο Core δίκτυο. Ο κύριος λόγος εφαρμογής του MPLS TE είναι να ελέγχονται τα μονοπάτια από τα οποία διακινείται η κίνηση μέσα στο δίκτυο. Το MPLS TE προσδίδει μία ελαστική σχεδίαση στην οποία μια εναλλακτική πορεία μπορεί να χρησιμοποιηθεί όταν αποτυγχάνει η βασική πορεία μεταξύ δύο δρομολογητών σε ένα δίκτυο. Όταν ένα πακέτο φτάσει στον PE δρομολογητή από έναν CE, του προστίθενται labels και προωθείται στους PE δρομολογητές εξόδου. Εκεί γίνεται αφαίρεση των labels και προωθείται προς τον κατάλληλο προορισμό ως IP πακέτο πλέον. Τα πρωτόκολλα OSPF και BGP με TE «προεκτάσεις» χρησιμοποιούνται για να πραγματοποιούν δρομολογήσεις στα τούνελ που έχουν καθοριστεί σε έναν δρομολογητή. Αυτές οι προεκτάσεις περιέχουν πληροφορίες σχετικά με τους διαθέσιμους πόρους για την δημιουργία ενός τούνελ, όπως είναι το εύρος ζώνης μίας σύνδεσης. Ως αποτέλεσμα αυτού , μια σύνδεση που δεν έχει τους απαιτούμενους πόρους δεν επιλέγεται να γίνει μέρος του LSP ή TE τούνελ. Η σηματοδοσία σε ένα MPLS TE περιβάλλον χρησιμοποιεί πρωτόκολλα κατοχύρωσης πόρων (όπως το RSVP) με τις κατάλληλες προεκτάσεις ώστε να

υποστηρίζονται τα χαρακτηριστικά των TE tunnel. Ο δρομολογητής εισόδου στο MPLS δίκτυο χρειάζεται να ξέρει πληροφορίες σχετικά με τη διαθεσιμότητα των πόρων για κάθε σύνδεση που είναι ικανή να γίνει μέλος του MPLS TE tunnel. Αυτές οι πληροφορίες παρέχονται από τα IGPs όπως το OSPF και το BGP λόγω της έμφυτης τους λειτουργίας να παρέχουν πληροφορίες σχετικά με τις συνδέσεις όλους τους δρομολογητές του IGP domain. Έτσι, ο δρομολογητής εισόδου συλλέγει πληροφορίες για όλους τους διαθέσιμους πόρους στο δίκτυο καθώς και την τοπολογία που περιγράφει τα τούνελ μέσα στο δίκτυο μεταξύ των MPLS δρομολογητών. Η βάση του MPLS TE είναι η δρομολόγηση βάσει περιορισμών (Constraint Based Routing - CBR), όπου λαμβάνεται υπόψη η πιθανότητα ύπαρξης πολλαπλών διαδρομών, μεταξύ μιας πηγής και ενός προορισμού σε ένα δίκτυο. Με το CBR, η λειτουργία ενός IP δικτύου ενισχύεται ώστε να δημιουργείται η μικρότερη σε κόστος διαδρομή και να ευνοούνται οι ήδη διαθέσιμες διαδρομές. Το CBR απαιτεί ένα IGP πρωτόκολλο, όπως το OSPF ή το BGP, για τη λειτουργία του. Το CBR χρησιμοποιείται για την εύρεση της συντομότερης διαδρομής σε ένα δίκτυο, οπότε είναι η βάση του TE tunnel και καθορίζεται στον δρομολογητή είσοδο της MPLS περιοχής όταν εφαρμόζουμε MPLS TE. Η διαθεσιμότητα των πόρων και ο πληροφορίες κατάστασης των συνδέσεων υπολογίζονται χρησιμοποιώντας τον CSPF (Constrained Shortest Path First) υπολογισμό όπου μεταβλητές όπως εύρος ζώνης , πολιτικές και τοπολογία λαμβάνονται υπόψη για να καθοριστούν οι πιθανές διαδρομές από μια πηγή σε έναν προορισμό. Τα αποτελέσματα του CSPF υπολογισμού μαζί με ένα καθορισμένο σύνολο IP διευθύνσεων που υποδεικνύουν την διεύθυνση των δρομολογητών, του επόμενου άλματος (hop), δημιουργούν ένα LSP Πρωτόκολλο RSVP

RSVP

Το RSVP καταλαμβάνει ένα ορισμένο εύρος ζώνης σε ένα κανάλι από μια πηγή προς έναν προορισμό. Τα RSVP μηνύματα στέλνονται, από τον κύριο δρομολογητή στο δίκτυο για να προσδιοριστεί η διαθεσιμότητα των πόρων πάνω στη διαδρομή. Ο κύριος δρομολογητής είναι πάντα η πηγή στο MPLS TE tunnel και ο ακραίος δρομολογητής λειτουργεί ως σημείο τερματισμού. Τα RSVP μηνύματα εφόσον σταλούν, οι πληροφορίες κατάστασης των δρομολογητών και η διαθεσιμότητα πόρων, αποθηκεύονται στα

μηνύματα πορείας path messages καθώς διαπερνούν το δίκτυο. Το RSVP έχει ως στόχο να ενημερώνει το δίκτυο για τις απαιτήσεις μιας συγκεκριμένης ροής κίνησης και να συλλέγει πληροφορίες για το αν οι απαιτήσεις αυτές μπορεί να εκπληρωθούν από το δίκτυο. Τα κύρια μηνύματα που χρησιμοποιούνται είναι τέσσερα όπως φαίνεται παρακάτω και είναι τα εξής:

1. RSVP PATH message
2. RSVP RESERVATION messages
3. RSVP error messages
4. RSVP tear messages

Στο MPLS TE, το RSVP χρησιμοποιείται προκειμένου να εξασφαλισθεί και να ελεγχθεί η διαθεσιμότητα των πόρων αλλά και να εφαρμόσει τα MPLS labels ώστε να ορίσει το MPLS TE LSP ανάμεσα στους δρομολογητές του δικτύου.

Δρομολόγηση βάσει περιορισμών

Η κύρια απαίτηση του TE είναι τα χαρακτηριστικά των συνδέσεων του δικτύου, και η διαθεσιμότητα των πόρων, να μπορούν να αναπαράγονται μέσα στο δίκτυο έτσι ώστε να μπορεί να γίνεται ικανοποιητική επιλογή μεταξύ των TE LSP διαδρομών. Στα πρωτόκολλα δρομολόγησης κατάστασης δικτύου (link-state), στην επιλεγμένη διαδρομή συνεχίζει να λαμβάνεται υπόψη το εύρος ζώνης μεταξύ δύο δρομολογητών έτσι ώστε να μπορεί να υπολογίσει το κόστος που σχετίζεται με αυτή πριν από την κατανομή των επιλεγμένων διαδρομών. Με την ενεργοποίηση και χρήση των πρωτοκόλλων link-sate για να αξιοποιηθούν οι πληροφορίες που σχετίζονται με τη διαθεσιμότητα των πόρων, οι ανανεώσεις των διαδρομών εκτελούνται από τη βασική λειτουργία του πρωτοκόλλου κατάστασης σύνδεσης LSA (Link State Advertisements). Οι μηχανισμοί λειτουργίας ενός link-state πρωτοκόλλου περιλαμβάνουν τη διαρκή μετάδοση επικαιροποιημένων πληροφοριών στο δίκτυο σχετικά με την κατάσταση σύνδεσης. Οι δρομολογητές ανακοινώνουν στο δίκτυο τους διαθέσιμους πόρους ώστε να ενημερωθεί ο router του TE tunnel κατά τη διάρκεια υπολογισμού της LSP διαδρομής. Οι ανακοινώσεις κατάστασης

σύνδεσης μεταφέρουν πληροφορίες που εμπεριέχουν τους γειτονικούς δρομολογητές, τα άμεσα συνδεδεμένα δίκτυα, πληροφορίες σχετικά με τους πόρους του δικτύου και άλλες σχετικές πληροφορίες αναφορικά με την πραγματική διαθεσιμότητα πόρων που μπορεί αργότερα να ζητηθεί ώστε να γίνει ένας CSPF υπολογισμός. Τα OSPF και το BGP παρέχονται με προεκτάσεις ώστε να ενεργοποιείται η χρήση τους σε ένα MPLS TE περιβάλλον για να αναπαράγουν πληροφορίες που αφορούν τη διαθεσιμότητα πόρων και τη δυναμική επιλογή LSP διαδρομής. Το MPLS TE απαιτεί έναν αποτελεσματικό τρόπο για να προβλέψει τη ροή της κυκλοφορίας μέσω του δικτύου με βάση τη διαμόρφωση δρομολόγησης. Η γνώση της διαδρομής μεταξύ κάθε ζεύγους κόμβων επιτρέπει στους χειριστές να αναγνωρίζουν την κίνηση που επιβάλλει φορτίο σε έναν συμφωνημένο σύνδεσμο και να αξιολογούν την επίδραση πιθανών αλλαγών στις παραμέτρους IGP. Αυτό απαιτεί ένα ακριβές μοντέλο για τον τρόπο με τον οποίο οι δρομολογητές σε μια διαδρομή από AS (Autonomus System) βασίζονται για τη διαμόρφωση της τοπολογίας του IGP. Όταν όλοι οι σύνδεσμοι ανήκουν σε μια ενιαία περιοχή OSPF ή IS-IS, η επιλογή μονοπατιού περιλαμβάνει τον υπολογισμό της μικρότερης διαδρομής μεταξύ κάθε ζεύγους δρομολογητών με την χρήση των αλγορίθμων. Τα μεγαλύτερα δίκτυα χωρίζονται συνήθως σε πολλές περιοχές (areas) OSPF ή IS-IS. Για τους δρομολογητές σε διαφορετικές περιοχές, η επιλογή διαδρομής εξαρτάται από τις συνοπτικές πληροφορίες που μεταφέρονται μεταξύ των ορίων της περιοχής. Σε ορισμένες περιπτώσεις, το δίκτυο μπορεί να έχει πολλαπλές συντομότερες διαδρομές μεταξύ του ίδιου ζεύγους δρομολογητών. Οι προδιαγραφές πρωτοκόλλου OSPF και IS-IS δεν υπαγορεύουν τον τρόπο με τον οποίο οι δρομολογητές χειρίζονται την παρουσία πολλαπλών συντομότερων διαδρομών. Οι περισσότεροι δρομολογητές εκμεταλλεύονται τις πολλαπλές διαδρομές για να εξισορροπήσουν το φορτίο. Ένας δρομολογητής μοιράζει συνήθως την κυκλοφορία περίπου ομοιόμορφα σε κάθε έναν από τους εξερχόμενους συνδέσμους κατά μήκος μιας μικρότερης διαδρομής προς τον προορισμό. Το μοντέλο δρομολόγησης πρέπει να υπολογίζει ένα σύνολο διαδρομών για κάθε ζεύγος δρομολογητών. Αυτά τα μονοπάτια μπορούν να αναπαρασταθούν με βάση το κλάσμα της κυκλοφορίας που διασχίζει κάθε μια από τις συνδέσεις. Η έξοδος του μοντέλου δρομολόγησης μπορεί να συνδυαστεί με τις απαιτήσεις κυκλοφορίας για την εκτίμηση του όγκου κίνησης σε κάθε σύνδεσμο, με βάση την τοπολογία και τη διαμόρφωση του IGP. Το μοντέλο δρομολόγησης παίζει επίσης ρόλο

στην καταγραφή της αλληλεπίδρασης του IGP με τη δρομολόγηση μεταξύ των διαμεσολαβητών όπως στο πρωτόκολλο BGP. Ένα μόνο μπλοκ διευθύνσεων IP προορισμού μπορεί να είναι προσβάσιμο μέσω πολλαπλών σημείων εξόδου σε γειτονικούς τομείς.

MPLS Precedence

Όταν στέλνονται πακέτα IP από έναν δρομολογητή σε άλλο, στο πεδίο IP Precedence, τα πρώτα τρία bits του πεδίου DSCP στην κεφαλίδα ενός πακέτου IP, καθορίζουν το QoS. Με βάση τη σήμανση προτεραιότητας IP, το πακέτο λαμβάνει την επιθυμητή επεξεργασία όπως την καθυστέρηση ή το ποσοστό του εύρους ζώνης που επιτρέπεται για την ποιότητα της υπηρεσίας. Εάν το δίκτυο παρόχου υπηρεσιών (PE) είναι ένα δίκτυο MPLS, τότε τα bits προτεραιότητας IP αντιγράφονται στο πεδίο MPLS EXP στην άκρη του δικτύου (CE). Ο πάροχος υπηρεσιών ενδέχεται να θέλει να ορίσει QoS για ένα πακέτο MPLS σε μια διαφορετική τιμή που θα καθορίζεται από την υπηρεσία που θέλει να προσφέρει. Η δυνατότητα αυτή επιτρέπει στον πάροχο υπηρεσιών να μπορεί ορίσει ένα πεδίο MPLS χωρίς να αντικαταστήσει την τιμή στο πεδίο προτεραιότητας IP που ανήκει σε έναν τελικό χρήστη. Η επικεφαλίδα IP παραμένει διαθέσιμη για τη χρήση του πελάτη. Το QoS ενός πακέτου IP δεν αλλάζει καθώς το πακέτο ταξιδεύει μέσω του δικτύου MPLS. Τέλος, επιτρέπει στους παρόχους να ταξινομούν τα πακέτα ανάλογα με τον τύπο, τη διασύνδεση εισόδου καθώς και άλλους παράγοντες χαρακτηρίζοντας κάθε πακέτο εντός του MPLS.

MPLS VPN

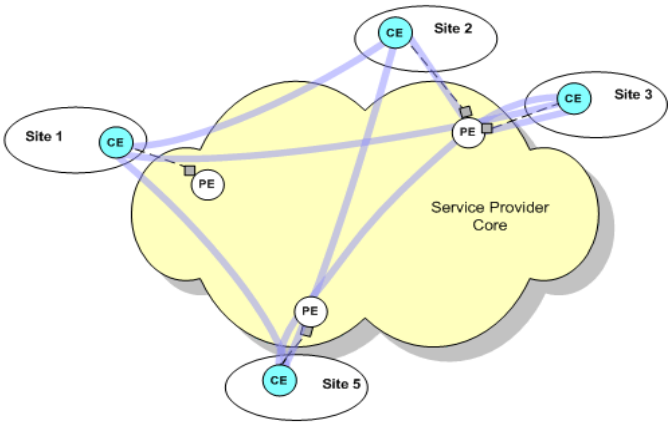
Σε δίκτυα υπολογιστών που βασίζονται σε IP, η εικονική δρομολόγηση και προώθηση (VRF - Virtual Routing and Forwarding) είναι μια τεχνολογία που επιτρέπει την ταυτόχρονη συνύπαρξη πολλαπλών παρουσιών στο πίνακα δρομολόγησης του δρομολογητή. Επειδή οι παρουσίες δρομολόγησης είναι ανεξάρτητες, οι ίδιες ή επικαλυπτόμενες διευθύνσεις IP μπορούν να χρησιμοποιηθούν χωρίς αλληλεπίδραση μεταξύ τους. Η λειτουργία του δικτύου βελτιώνεται καθώς οι διαδρομές δικτύου μπορούν να διαχωριστούν χωρίς να απαιτούνται πολλοί δρομολογητές. Το VRF μπορεί να

υλοποιηθεί σε μια συσκευή δικτύου από συγκεκριμένους πίνακες δρομολόγησης που είναι γνωστοί ως βάσεις πληροφοριών προώθησης (FIBs), μία ανά VRF δρομολόγησης. Εναλλακτικά, μια συσκευή δικτύου μπορεί να έχει τη δυνατότητα να ρυθμίσει διαφορετικούς εικονικούς δρομολογητές, όπου ο καθένας έχει το δικό του FIB που δεν είναι προσβάσιμο σε οποιαδήποτε άλλη παρουσίαση εικονικού δρομολογητή στην ίδια συσκευή. Τα VRFs εισήχθησαν αρχικά σε συνδυασμό με το Multiprotocol Label Switching, αλλά το VRF αποδείχθηκε τόσο χρήσιμο ώστε τελικά εξελίχθηκε για να ζήσει ανεξάρτητα από το MPLS. Η απλούστερη μορφή υλοποίησης του VRF είναι το VRF Lite. Στο VRF Lite, κάθε δρομολογητής εντός του δικτύου συμμετέχει στο περιβάλλον εικονικής δρομολόγησης με έναν ομότιμο τρόπο. Επίσης είναι απλό να αναπτυχθεί για μικρές και μεσαίες επιχειρήσεις και κοινόχρηστα κέντρα δεδομένων, το VRF Lite δεν κλιμακώνεται στο μέγεθος που απαιτείται από τις παγκόσμιες επιχειρήσεις ή τους μεγάλους παρόχους, καθώς υπάρχει ανάγκη γνώσης των δρομολογήσεων του κάθε VRF σε κάθε δρομολογητή, συμπεριλαμβανομένων των ενδιάμεσων δρομολογητών. Οι περιορισμοί επέκτασης του VRF Lite επιλύονται με την υλοποίηση IP VPN. Σε αυτήν την εφαρμογή, ένα δίκτυο κορμού είναι υπεύθυνο για τη διαβίβαση δεδομένων σε όλη την ευρεία περιοχή μεταξύ περιπτώσεων VRF σε κάθε θέση άκρης. Τα MPLS VPNs έχουν αναπτυχθεί παραδοσιακά για να παρέχουν ένα κοινό δίκτυο backbone για πολλούς πελάτες. Είναι επίσης κατάλληλο για τα μεγάλα περιβάλλοντα επιχειρήσεων και κοινόχρηστων κέντρων δεδομένων. Σε μια τυπική ανάπτυξη, οι Customer Edges (CE) δρομολογητές χειρίζονται την δρομολόγηση με παραδοσιακό τρόπο και διαδίδουν τις πληροφορίες δρομολόγησης Provider Edge (PE) όπου οι πίνακες δρομολόγησης είναι εικονικοί. Στη συνέχεια, ο δρομολογητής PE ενσωματώνει την κυκλοφορία, επισημαίνει την αναγνώριση της παρουσίας VRF και τη μεταδίδει μέσω του δικτύου κορμού του παρόχου στο δρομολογητή PE προορισμού. Ο δρομολογητής PE προορισμού κατόπιν μεταφέρει την κίνηση και προωθεί το δρομολογητή CE στον προορισμό. Επιτρέπει σε πολλούς πελάτες ή κοινότητες χρηστών να χρησιμοποιούν το κοινό δίκτυο κορμού, διατηρώντας παράλληλα το διαχωρισμό κυκλοφορίας από άκρο σε άκρο ανά πελάτη. Οι διαδρομές σε ολόκληρο το δίκτυο κορμού του παρόχου διατηρούνται χρησιμοποιώντας ένα πρωτόκολλο εσωτερικής δικτύωσης, το συνηθέστερο είναι το iBGP. Το iBGP χρησιμοποιεί εκτεταμένα χαρακτηριστικά κοινότητας σε έναν κοινό πίνακα δρομολόγησης

για να διαφοροποιήσει τις διαδρομές των πελατών με αλληλεπικαλυπτόμενες διευθύνσεις IP. Το IP VPN χρησιμοποιείται συνήθως σε ένα κορμό MPLS, καθώς η εγγενής επισήμανση των πακέτων στο MPLS προσφέρεται για την αναγνώριση του πελάτη VRF.

Διευθυνσιοδότηση MPLS VPN

Στο MPLS VPNs είναι δυνατό να υπάρχουν επικαλύψεις διευθύνσεων μεταξύ των διαφορετικών VPNs (π.χ. διευθύνσεις 192.168.1.0) καθώς οι ίδιες διευθύνσεις μπορούν να αποδοθούν και να δρομολογηθούν σε πολλαπλά VPN. Το πρόβλημα της επικάλυψης διευθύνσεων αντιμετωπίζεται με τη δημιουργία ενός νέου τύπου διευθύνσεων, των VRFs IP-VPNs. Μία VRF IP-VPN διεύθυνση κατασκευάζεται με την παράθεση ενός πεδίου με σταθερό μήκος, Route Distinguisher, και μιας συνηθισμένης IP διεύθυνσης. Με τον τρόπο αυτό μπορεί μια διεύθυνση ip να αποδοθεί χωρίς κανένα πρόβλημα σε πολλαπλά VPN .

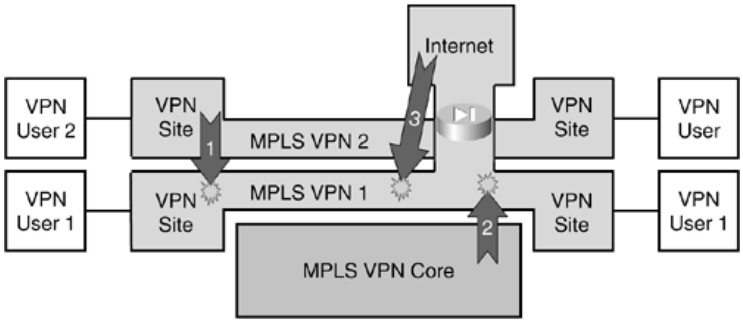


Εικόνα 4 MPLS VPN Τοπολογία

Κεφάλαιο 2 - Απειλές και κίνδυνοι

Σε ένα περιβάλλον MPLS VPN την εκτίμηση της ασφάλειας για να έχουμε μια συνολική εικόνα κρίνεται σκόπιμο να την δούμε από δύο διαφορετικές οπτικές γωνίες: από τον πελάτη VPN και από την μεριά του παρόχου υπηρεσιών. Και στις δύο περιπτώσεις υπάρχουν διαφορετικά μοντέλα απειλών, για παράδειγμα σε έναν πελάτη είναι ιδιαίτερα σημαντικό να έχει προστασία από πιθανές εισβολές δικτύου εκτός του VPN του. Επομένως, μία από τις κύριες απειλές για έναν πελάτη VPN αποτελούν οι εισβολές στο δίκτυο του και θα πρέπει να εξασφαλίσει ότι δεν θα υπάρχουν ανεπιθύμητες εισβολές. Για έναν πάροχο υπηρεσιών αντίστοιχα , ένα από τα βασικότερα και κρίσιμα ζητήματα είναι η διαθεσιμότητα του δικτύου και η εξασφάλιση διαθεσιμότητας του δικτύου και η αποφυγή ανεπιθύμητων εισβολών και επιθέσεων. Μία από τις βασικές προτεραιότητες λοιπόν αποτελεί η πρόληψη από πιθανές απειλές όπως είναι οι επιθέσεις άρνησης υπηρεσίας (DoS). Κατά την μελέτη και το σχεδιασμό ενός δικτύου είναι ιδιαίτερα σημαντικό να έχει προηγηθεί σωστή ανάλυση της ασφάλειας του δικτύου και των πιθανών απειλών έτσι ώστε να διασφαλισθεί η ασφάλεια η διαθεσιμότητα και ακεραιότητα των δεδομένων του από κάθε πιθανή απειλή που μπορεί να παρουσιαστεί. Οι απειλές σε ένα MPLS VPN διακρίνονται με βάση την αρχιτεκτονική του συστήματος στις παρακάτω κατηγορίες.

1. EEσωτερικές παρεμβολές από άλλα vpn ή από δίκτυο κορμού
2. DDos Denial of service (DoS)



Εικόνα 5 Πιθανές απειλές

Κρίσιμο σημείο στην ασφάλεια ενός συστήματος MPLS-VPN αποτελεί η ασφάλεια του PE router καθώς μια πιθανή επίθεση Dos εναντίον ενός PE router μπορεί να επιφέρει καταστροφικά αποτελέσματα και να επηρεάσει τη διαθεσιμότητα πολλών πελατών. Οι βασικότερες απαιτήσεις των ενός πελάτη σε μια MPLS VPN υπηρεσία είναι να μπορεί να εξασφαλίζει**:**

- Διαχωρισμό VPN (διεύθυνση και κίνηση)
- Ανθεκτικότητα έναντι επιθέσεων
- Απόκρυψη της βασικής υποδομής
- Προστασία από πλαστογράφηση VPN

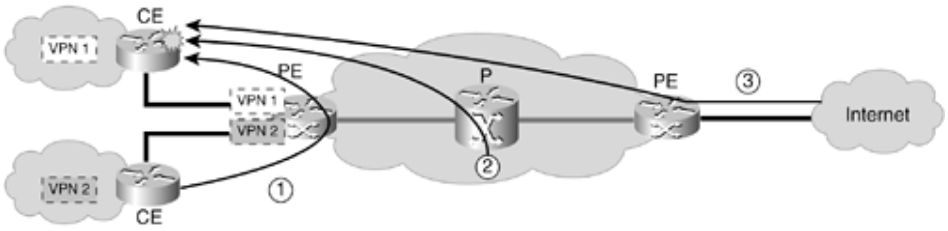
Παρεμβολές

Οι εισβολές μπορούν πρώτα να στοχεύουν σε βασικό εξοπλισμό όπως οι δρομολογητές. Το τεχνικό πεδίο αυτής της απειλής και η προστασία από αυτήν είναι συγκρίσιμο με τα κανονικά δίκτυα του Διαδικτύου. Οι βασικοί δρομολογητές MPLS δεν είναι προσβάσιμοι από συνδεδεμένα VPN ή στο Διαδίκτυο. Εξαιρέσεις είναι μόνο τα πρωτόκολλα που χρησιμοποιεί ένα PE για να επικοινωνήσει εξωτερικά, επειδή στις αντίστοιχες θύρες για κάθε πρωτόκολλο το PE πρέπει να δέχεται πακέτα. Σημαντικό είναι να μειωθεί ο αριθμός των πρωτοκόλλων που χρησιμοποιούνται και να ασφαλισθούν τα πρωτόκολλα. Οι επιτιθέμενοι μπορούν επίσης να έχουν ως στόχο εξοπλισμούς όπως AAA server, server TFTP και FTP και κόμβους διαχείρισης. Ο κίνδυνος είναι υψηλός τόσο για τον ίδιο τον κορμό του δικτύου όσο και για τα συνδεδεμένα VPN. Μια κακόβουλη διαμόρφωση σε έναν PE για παράδειγμα μπορεί να επιτρέψει σε εξωτερικούς ισότοπους να έχουν αποκτήσουν πρόσβαση σε ένα VPN.

Παρεμβολές σε ένα VPN (Intrusions into a VPN)

Οι επιθέσεις αυτές γίνονται όταν ένας επιτιθέμενος σε ένα VPN δίκτυο προσπαθεί να αποκτήσει έλεγχο κίνησης στο συγκεκριμένο VPN όπως για παράδειγμα να μπορέσει να εισάγει ένα πακέτο εντός του VPN. Οι εισβολές θα μπορούσαν να προέρχονται είτε από ένα άλλο VPN είτε τον ίδιο το δίκτυο κορμού αλλά και από το Διαδίκτυο. Στην τοπολογία

της παρακάτω εικόνας μπορούν να διακριθούν τα σημεία στα οποία θα μπορούσε να πραγματοποιηθεί μια επίθεση.

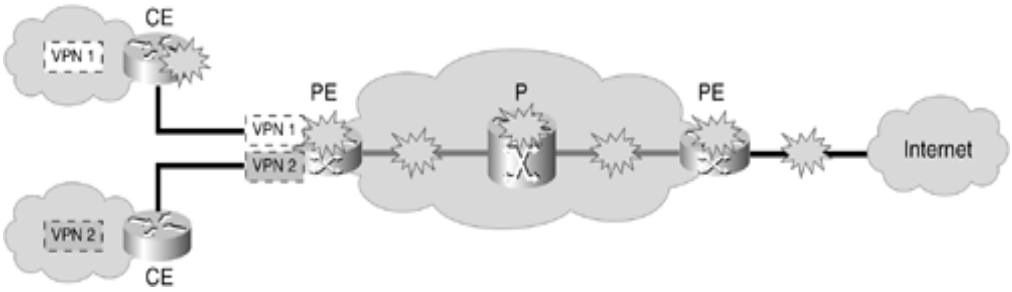


Εικόνα 6 Πιθανά σημεία παρεμβολής

Για να αποφευχθούν τέτοιου είδους παρεμβολές είναι σημαντικό να υπάρχει ένα τείχος προστασίας που θα ελέγχει την κίνηση σε μια τοποθεσία και θα διαχωρίζει το δίκτυο από άλλα εξωτερικά δίκτυα διότι είναι απαραίτητο να αποτραπεί όλη η παράνομη κυκλοφορία δεδομένων και να αποκλειστεί η παράνομη κίνηση.

Άρνηση υπηρεσίας εναντίον VPN (VPN Denial of service)

Πιθανή απειλή επίσης σε ένα MPLS VPN θα μπορούσε να προέρχεται είτε από κάποιο άλλο VPN ή από το Διαδίκτυο. Για να μπορέσει να πραγματοποιηθεί μια τέτοια εισβολή θα πρέπει ο επιτιθέμενος να μπορεί να στέλνει πακέτα προς μια αξιόπιστη ζώνη του VPN που θέλει να εισβάλει. Αυτή η ενέργεια περιλαμβάνει τη διασφάλιση ελέγχου όλων των σημείων εισβολής. Η προστασία ενός VPN από εισβολές θα μπορούσε να χαρακτηρισθεί απλή έχοντας τον έλεγχο των σημείων εισόδου ενός VPN. Η προστασία όμως από μια επίθεση DoS είναι πιο περίπλοκη λόγω της έμμεσης επίδρασης των επιθέσεων DoS στην υποδομή.



Εικόνα 7 Denial of Service Against a VPN

Επιθέσεις DoS Denial of Service

Η απειλή μιας επίθεσης DoS κατά του δικτύου κορμού ενός δικτύου είναι ισοδύναμη με την απειλή μιας επίθεσης DoS σε κανονικά δίκτυα IP. Οποιοδήποτε μέρος του κορμού MPLS είναι ευάλωτο σε μια επίθεση DoS από ένα VPN ή από το Διαδίκτυο, εκτός εάν το τμήμα αυτό έχει ασφαλιστεί και σχεδιαστεί κατάλληλα. Σε έναν σωστά διαμορφωμένο MPLS δίκτυο κορμού είναι αδύνατο από έξω να αποστέλλεται η κυκλοφορία απευθείας σε ένα κομμάτι πυρήνα εξοπλισμού. Η λύση ενάντια σε μια απειλή επίθεσης DoS είναι ο κατάλληλος σχεδιασμός του κεντρικού δικτύου. Οι δρομολογητές και οι γραμμές πρέπει να έχουν τη σωστή σχεδίαση ώστε να υπάρχει προστασία σε κάθε πιθανή απειλή. Ακόμη και αν μια επίθεση από ένα VPN φορτώνει μια γραμμή πρόσβασης αυτού του VPN, με πακέτα ελάχιστου μεγέθους, ο συνδεδεμένος δρομολογητής PE πρέπει να μπορεί να χειρίζεται όλη τη ληφθείσα κίνηση. Όταν η συνολική κίνηση ενδέχεται να υπερβαίνει την προβλεπόμενη χωρητικότητα, πρέπει να ληφθούν κατάλληλα μέτρα ποιότητας υπηρεσίας (QoS) για να διασφαλιστεί ότι η κυκλοφορία διέλευσης πληροί τα απαιτούμενα SLA.

Εσωτερικές απειλές

Η απειλή εναντίον των βασικών δικτύων MPLS είναι οι εσωτερικές επιθέσεις, όπως είναι για παράδειγμα τα λάθη ή οι εσκεμμένες εσφαλμένες διαμορφώσεις που έγιναν από το εσωτερικό προσωπικό του παρόχου υπηρεσιών. Η απειλή σχετίζεται με τον κορμό του δικτύου και το MPLS VPN δίκτυο. Τέτοιες εσφαλμένες διαμορφώσεις ενδέχεται επίσης να επηρεάσουν την ασφάλεια των συνδεδεμένων VPN. Μια σχετικά απλή εσφαλμένη διαμόρφωση ενός στόχου διαδρομής θα μπορούσε να έχει δυνητικά σοβαρές συνέπειες για την ασφάλεια.

Απειλές από μια ζώνη εμπιστοσύνης

Η έρευνα για το έγκλημα και την ασφάλεια υπολογιστών CSI / FBI του 2004 δείχνει ότι περίπου ο ίδιος αριθμός συμβάντων ασφαλείας έχει την προέλευσή του στο εσωτερικό με το εξωτερικό μιας επιχείρησης. Γενικότερα, αυτό αναφέρεται σε μια ζώνη εμπιστοσύνης.

Ορισμένα πιθανά ζητήματα ασφάλειας ενδέχεται να προέρχονται από την ίδια ζώνη εμπιστοσύνης και επομένως δεν σχετίζονται με το γεγονός ότι η υποκείμενη υποδομή είναι ένα δίκτυο MPLS. Παραδείγματα τέτοιων ζητημάτων είναι ενα μη ασφαλές σημείο ασύρματης πρόσβασης σε μια επιχείρηση η οποία διαθέτει υπηρεσία MPLS VPN. Επίσης μια επίθεση DoS από το διαδίκτυο σε έναν διακομιστή ενός δικτύου VPN, όπου το VPN με υπηρεσία διαδικτύου παρέχεται στον ίδιο πυρήνα MPLS. Εάν ένας πυρήνας MPLS παρέχει σύνδεση στο διαδίκτυο με ένα δεδομένο VPN, τότε αυτή η συνδεσιμότητα μπορεί επίσης να χρησιμοποιηθεί για επίθεση το VPN από έξω. Το ίδιο θα ισχύει και σε άλλες αναπτύξεις VPN όπως το Frame Relay ή το ATM. Μια εισβολή από ένα MPLS VPN σε ένα άλλο VPN, όπου η ροή πακέτων πέρασε από σημεία διασύνδεσης που έχουν σχεδιαστεί ειδικά για το σκοπό αυτό, για παράδειγμα Extranets. Τέτοιες αναπτύξεις πρέπει κανονικά να προστατεύονται από τείχος προστασίας.

Επίθεση αναγνώρισης Reconnaissance Attacks

Για την αποτελεσματική εκκίνηση ορισμένων τύπων επιθέσεων, ένας εισβολέας χρειάζεται συνήθως κάποια γνώση σχετικά με την τοπολογία του δικτύου ή το υλικό που χρησιμοποιείται. Η τεχνική που συγκεντρώνει αυτόν τον τύπο πληροφοριών ονομάζεται αναγνώριση . Η αναγνώριση από μόνη της, σε πολλά περιβάλλοντα, δεν αποτελεί απειλή, αλλά η ευφυΐα που χρησιμοποιείται με τη χρήση της χρησιμοποιείται συχνά αργότερα για να επιτεθεί σε ένα σύστημα ή ένα δίκτυο. Έτσι, η απειλή των επιθέσεων αναγνώρισης είναι ως επί το πλείστων έμμεση. Μετά τη σάρωση του δικτύου, αυτές οι πληροφορίες χρησιμοποιούνται στη συνέχεια για επιθέσεις. Στο MPLS, το δίκτυο κορμού είναι ήδη, σε μεγάλο βαθμό προστατευμένο καθώς δεν είναι ορατό προς τα έξω, το μόνο ορατό σημείο είναι οι διευθύνσεις PE-peering. Αυτές οι διεπαφές παρόλο που είναι ορατές, προστατεύονται με ACL, έτσι ώστε ο δρομολογητής PE να μην δέχεται πακέτα που στοχεύουν στον πυρήνα ή να στέλνει οποιαδήποτε απόκριση. Αυτό κρύβει τον πυρήνα και καθιστά πολύ δύσκολη την αναγνώριση από το εξωτερικό του δικτύου.

Κεφάλαιο 3 - Ανάλυση ασφαλείας της τεχνολογίας MPLS

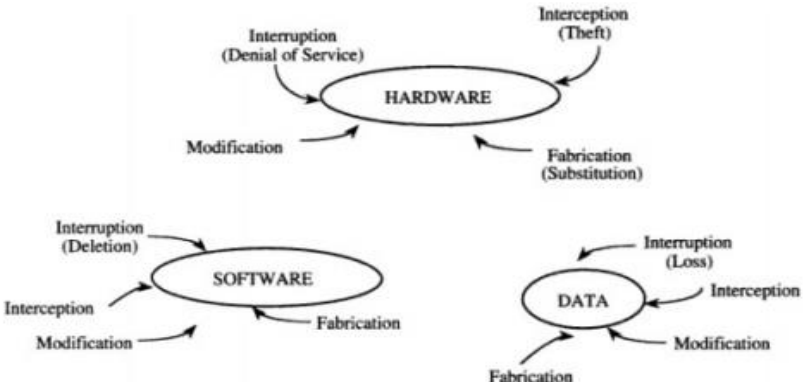
Η πολιτική ασφάλειας σε μια επιχείρηση έπεται της αξιολόγησης του επιπέδου ασφάλειας όλων των συστημάτων. Η αξιολόγηση της ασφάλειας μπορεί να πραγματοποιηθεί με πολλούς τρόπους, όπως για παράδειγμα η χρήση προτύπων διαχείρισης σχετικά με την ασφάλεια. Στη συνέχεια δίνονται οι ορισμοί για την ανάλυση κινδύνων (Spears & Barki, 2010)

1. Απειλή: Ένα μη επιθυμητό γεγονός που μπορεί να προξενήσει μη διαθεσιμότητα του συστήματος

2. Ευπάθεια: Μια σχεδιαστική ατέλεια σε ένα σύστημα, με δυνατότητα παραβίασης της ασφάλειας του συστήματος.

3. Κίνδυνος: Ενδεχόμενο κινδύνου στο να εκμεταλλευτεί μια απειλή μια ευπάθεια.

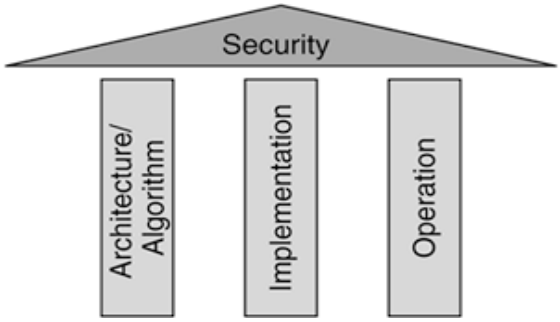
4. Αντίμετρο: Μέτρο που εφαρμόζεται για την προστασία του ΠΣ και την αντιμετώπιση των απειλών.



Εικόνα 8 Ευπάθειες ενός πληροφοριακού συστήματος

Ένα σύστημα θα μπορούσε να χαρακτηριστεί ασφαλές εκείνο στο οποίο κανείς δε θα μπορούσε να εισβάλλει εξωτερικά. Σε ένα MPLS VPN λόγω αρχιτεκτονικής, μπορεί να θεωρηθεί ότι αποτελεί ένα ασφαλές σύστημα λόγω του ότι κανείς δεν μπορεί να εισβάλει σε ένα τέτοιο δίκτυο εξωτερικά. Σε ένα mpls δίκτυο, όλα τα πακέτα εισέρχονται με μια προκαθορισμένη ετικέτα βάση της οποίας γίνεται η δρομολόγηση από το δίκτυο του παρόχου. Ακόμη και αν ένας αλγόριθμος αποδειχθεί ότι είναι 100% ασφαλής στο το συνολικό σύστημα ενδέχεται να υπάρχουν ορισμένες αδυναμίες σε άλλους τομείς. Κατά την ταξινόμηση της συνολικής ασφάλειας ενός συστήματος όπως ένα δίκτυο MPLS VPN

θα πρέπει κανείς να αναλύσει ξεχωριστά τα τρία βασικά μέρη που συνθέτουν το σύστημα τα οποία είναι αφενός η αρχιτεκτονική ή αλγόριθμος. Στην κρυπτογραφία θα μπορούσε να μελετηθεί ο ίδιος ο αλγόριθμος άλλα στην περίπτωση των MPLS VPNs, είναι η τυπική προδιαγραφή όπως ορίζεται στο RFC 2547bis. Αφετέρου, η υλοποίηση αυτής της αρχιτεκτονικής ή αλγορίθμου. Αυτό αναφέρεται στο πώς η αρχιτεκτονική ή ο αλγόριθμος εφαρμόζεται στην πραγματικότητα.



Εικόνα 9 Βασικά στοιχεία ασφαλείας

Η λειτουργία της αρχιτεκτονικής του αλγορίθμου περιλαμβάνει ζητήματα όπως είναι επιλογή αδύναμων κωδικών πρόσβασης σε δρομολογητές ή σταθμούς εργασίας ή τυχαία αποκάλυψη ενός κοινόχρηστου κλειδιού. Κατά την ανάλυση της ασφάλειας ενός συστήματος, είναι πολύ σημαντικός ο διαχωρισμός αυτών των τριών στοιχείων και η ανάλυση της ασφάλειας καθενός από αυτά ξεχωριστά. Είναι αρκετά σημαντικό να γίνει κατανοητό κατά τον καθορισμό των πολιτικών ασφαλείας, ότι ο καλύτερος αλγόριθμος είναι άχρηστος όταν λειτουργεί με αδύναμο τρόπο. Μπορεί κανείς να βρει συστήματα στα οποία καταβλήθηκε πολύ μεγάλη προσπάθεια για τη διασφάλιση της αρχιτεκτονικής, αλλά η λειτουργία της παραμελήθηκε πλήρως. Η διαχείριση κωδικού πρόσβασης στις επιχειρήσεις είναι ένα κλασσικό παράδειγμα. Πολύ καλά συστήματα ασφαλείας καθίστανται μη ασφαλή καθώς οι χρήστες επιλέγουν αδύναμους κωδικούς πρόσβασης. Οι σχεδιαστές τέτοιων συστημάτων θα πρέπει να έχουν κατά νου ότι η συνολική ασφάλεια εξαρτάται και από τα τρία στοιχεία ασφαλείας .Ένα σύστημα θα μπορούσε να θεωρηθεί ότι δεν είναι ασφαλές εάν υπάρχει ένας μόνο τρόπος για να εισέλθουν στο σύστημα. Υπάρχει δηλαδή μια σημαντική λεπτομέρεια σε αυτήν την πρόταση. Απαιτείται μόνο μία αδυναμία για να σπάσει την ασφάλεια ενός ολόκληρου συστήματος. Η κοινή αναλογία που χρησιμοποιείται για να εξηγήσει αυτό είναι μια αλυσίδα. Εάν ένας σύνδεσμος σπάσει,

ολόκληρη η αλυσίδα είναι σπασμένη. Ο πιο αδύναμος κρίκος σε ένα σύστημα είναι συχνά ο ανθρώπινος παράγοντας, άλλα ενδέχεται επίσης να είναι ελαττωματικά και άλλα μέρη ενός συστήματος έκτος από αυτό και θα πρέπει να παρακολουθούνται προσεκτικά. Η πολιτική ασφάλειας ενός συστήματος θα πρέπει να καλύπτει όλα τα μέρη καθώς και τις πιθανές αδυναμίες τους, οι οποίες θα πρέπει να ελέγχονται τακτικά. Επειδή τα ανθρώπινα λάθη αποτελούν σημαντικό κίνδυνο για την ασφάλεια ενός συστήματος, ο πιο ασφαλής τρόπος σχεδιασμού συστημάτων είναι να παρέχεται σε κάθε χειριστή μόνο η άδεια που απαιτείται αυστηρά για την εκτέλεση της εργασίας. Ο χρήστης να μπορεί εκτελέσει συγκεκριμένες πράξεις με αποτέλεσμα να είναι προβλέψιμες οι πιθανές παραβιάσεις της ασφάλειας με αποτέλεσμα κάθε ενέργεια να παρακολουθείται και να ελέγχεται. Κάθε πελάτης έχει την απαίτηση τα δεδομένα του να είναι εμπιστευτικά, έτσι ώστε να μην είναι προσβάσιμα εκτός του VPN τους, όπως επίσης ότι τα δεδομένα δε θα αλλάξουν κατά τη μεταφορά και θα περιμένουν ότι η υπηρεσία VPN MPLS θα έχει εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα. Στην συνέχεια θα προχωρήσουμε στην ανάλυση της ασφάλειας που μας παρέχει ένα MPLS δίκτυο και τα σημεία που το καταστούν να είναι αρκετά ασφαλή.

Προσανατολισμός στη σύνδεση

Πολλές τεχνολογίες VPN είναι προσανατολισμένες στη σύνδεση. Ένας χρήστης VPN μπορεί να έχει σύνδεση με άλλον χρήστη εντός του ίδιου VPN. Οι τεχνολογίες IPsec, GRE και IP-in-IP point-to-multipoint, όπως το GRE multipoint (mGRE), αποτελούν κλασικά παραδείγματα τεχνολογιών προσανατολισμένων στη σύνδεση.

Κρυπτογράφηση

Χρησιμοποιείται όταν απαιτείται εμπιστευτικότητα των δεδομένων όπως είναι για παράδειγμα, στη σύνδεση μέσω ασύρματου δικτύου ή δημόσιου Διαδικτύου. Κλασικό παράδειγμα αποτελεί η τεχνολογία IPsec. Το MPLS είναι μη κρυπτογραφημένο άλλα μπορεί με την χρήση ipsec να γίνει η κρυπτογράφηση. Τα IPsec, GRE, IP-in-IP, TLS, SSH

αποτελούν παραδείγματα τεχνολογιών VPN οι οποίες μπορούν να χρησιμοποιηθούν μέσω του διαδικτύου προσφέροντας το πλεονέκτημα της διαθεσιμότητας και ακεραιότητας.

Ζώνες ασφαλείας

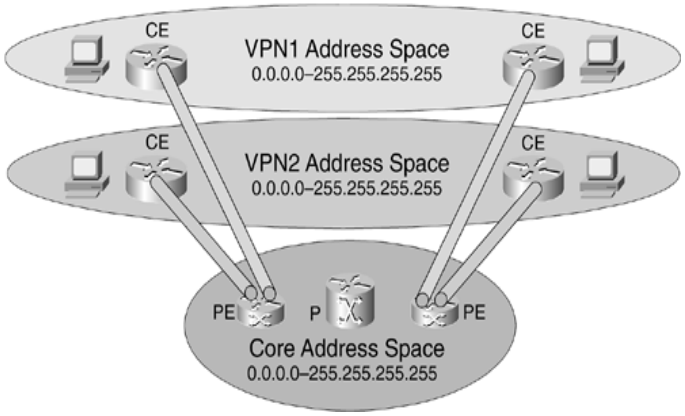
Ένα δίκτυο MPLS αποτελείται από ένα βασικό δίκτυο MPLS και VPN MPLS που διανέμονται σε διάφορες τοποθεσίες VPN. Ένα MPLS VPN είναι μια υπηρεσία που παρέχεται μέσω ενός δικτύου MPLS σε έναν αριθμό χρηστών σε διάφορες τοποθεσίες. Σε αυτό το μοντέλο, υπάρχουν ορισμένοι περιορισμοί όπως είναι για παράδειγμα τα VPN που δεν μπορούν να διασυνδεθούν και δεν υπάρχει σύνδεση στο διαδίκτυο. Ιδιαίτερα σημαντικό επίσης είναι ότι οι ζώνες διαχωρίζονται. Ο διαχωρισμός αυτός σημαίνει ότι δεν είναι δυνατή η αποστολή κίνησης από ένα VPN σε άλλο VPN κάθε VPN είναι ξεχωριστό. Ο κορμός του MPLS core network θα μπορούσε επίσης να παρέχεται από πολλούς παρόχους, μέσω των προηγμένων αρχιτεκτονικών MPLS VPN όπως το Inter-AS ή το Carrier Carrier. Η ύπαρξη ενός ή περισσοτέρων παρόχων είναι κάτι που δεν γίνεται αντιληπτό για τους χρήστες. Οι πάροχοι υπηρεσιών πρέπει να διασφαλίσουν το δικό τους δίκτυο κορμού MPLS από εισβολές. Οι χρήστες VPN πρέπει να εμπιστεύονται όλους τους εμπλεκόμενους παρόχους. Όλα αυτά ορίζουν ζώνες ασφαλείας, ζώνες εμπιστοσύνης, με τις αντίστοιχες συνδέσεις. Επειδή αυτές οι ζώνες δεν συνδέονται, οι εισβολές είναι αδύνατες, για παράδειγμα, είναι αδύνατον να εισβάλουμε από ένα VPN στον πυρήνα MPLS.

Διαχωρισμός VPN

Η πιο σημαντική απαίτηση ασφάλειας για τους χρήστες VPN είναι συνήθως ότι η κυκλοφορία τους διατηρείται ξεχωριστή από την άλλη κίνηση VPN και την κύρια κίνηση. Αυτό αναφέρεται τόσο στην επισκεψιμότητα της που δε φαίνεται σε άλλα VPN, όσο και σε άλλες πηγές VPN ή τη βασική κίνηση που δεν εισβάλλει στο VPN τους. Ένα VPN πρέπει να είναι εντελώς ξεχωριστό από άλλα VPN ή τον πυρήνα όσον αφορά το διαχωρισμό κίνησης και το διαχωρισμό χώρου διευθύνσεων.

Διαχωρισμός χώρου διευθύνσεων

Για να μπορεί να κάνει διάκριση μεταξύ διευθύνσεων από διαφορετικά VPN, το RFC 2547bis, δεν χρησιμοποιεί την τυπική διεύθυνση IPv4 (ή IPv6) στο επίπεδο ελέγχου για VPN στον πυρήνα. Εισάγει την έννοια της οικογένειας διευθύνσεων VPN -IPv4. Μια διεύθυνση VPN-IPv4 αποτελείται από ένα διανομέα διαδρομής 8-byte (RD) ακολουθούμενο από μια διεύθυνση IPv4 4-byte. Ο σκοπός του RD είναι να επιτρέψει την χρήση ολόκληρου του χώρου IPv4 σε διαφορετικά περιβάλλοντα. Σε έναν δεδομένο δρομολογητή, ένα μόνο RD μπορεί να ορίσει μια παρουσία δρομολόγησης VPN (VRF), στην οποία ολόκληρος ο χώρος διευθύνσεων IPv4 μπορεί να χρησιμοποιηθεί ανεξάρτητα. Το RFC 2547bis ορίζει ένα σημασιολογικό για RD, αλλά αυτό εξυπηρετεί μόνο διοικητικούς σκοπούς, για να διευκολύνεται η επιλογή μοναδικών RD. Λόγω της αρχιτεκτονικής των VPNIPMPLS, μόνο οι δρομολογητές PE πρέπει να γνωρίζουν τις διαδρομές VPN. Επειδή οι δρομολογητές PE χρησιμοποιούν διευθύνσεις VPN-IPv4 αποκλειστικά για VPN, ο χώρος διευθύνσεων διαχωρίζεται μεταξύ VPN.



Εικόνα 10 διαχωρισμός vpn

Διαχωρισμός κυκλοφορίας

Αυτή η κίνηση VPN είναι ενθυλακωμένη, συνήθως σε LSP και αποστέλλεται από PE σε PE. Λόγω αυτής της ενθυλάκωσης, ο πυρήνας δεν βλέπει ποτέ την κίνηση. Η VPN κίνηση αποτελείται από κίνηση από και προς τερματικούς σταθμούς σε ένα VPN και μεταξύ CE.

Απόκρυψη της βασικής υποδομής

Τα Layer 2 VPN όπως είναι το Frame Relay ή το ATM έχουν το χαρακτηριστικό ότι ο χρήστης VPN δεν μπορεί να "δει" τη βασική υποδομή. Σε αυτές τις περιπτώσεις, ο χρήστης συνδέει μια συσκευή Layer 3 σε ένα δίκτυο Layer 2, έτσι ώστε η υποδομή Layer 2 να είναι κρυμμένη στον χρήστη. Τα δίκτυα MPLSVPN κρύβουν το μεγαλύτερο μέρος της βασικής τους υποδομής στην αρχιτεκτονική. Οι δρομολογητές PE είναι κρυμμένοι. Είναι σημαντικό να γίνει κατανοητό ότι η απόκρυψη του δικτύου κορμού δεν οφείλεται σε ACL αλλά στον εγγενή τρόπο χειρισμού ξεχωριστών χώρων διευθύνσεων σε έναν πυρήνα MPLS. Η μόνη εξαίρεση σε αυτό είναι η διεύθυνση του δρομολογητή PE. Ωστόσο, ο χώρος διευθύνσεων των κυκλωμάτων σύνδεσης CE-PE ανήκει στο VPN.Παρόλο που μια διεύθυνση PE ενδέχεται να είναι ορατή στο VPN δεν διαβιβάζονται βασικές πληροφορίες προς τα έξω επειδή η εν λόγω διεύθυνση είναι χώρος διευθύνσεων VPN. Ο λόγος για την απόκρυψη της βασικής υποδομής είναι η αποφυγή επιθέσεων εναντίον της. Υπάρχει, ωστόσο, ένας τρόπος απόκρυψης εντελώς των δρομολογητών PE από τον χρήστη VPN, χρησιμοποιώντας μη αριθμημένο χώρο διευθύνσεων και στατική δρομολόγηση μεταξύ PE και CE. Εδώ, ένα ACL θα μπορούσε να εφαρμοστεί σε όλες τις διεπαφές peering PE αυτού του VRF. Όσον αφορά την απόκρυψη του core δικτύου , ο κύριος στόχος των παρόχων υπηρεσιών είναι να παρέχουν υψηλότερη αντίσταση ενάντια σε επιθέσεις. Ακόμα και όταν η διεύθυνση PE peering είναι εκτεθειμένη, μπορεί να επιτευχθεί επαρκής ασφάλεια.

Κεφάλαιο 4 - Προτάσεις για αύξηση της ασφάλειας

Η ασφαλής πρόσβαση σε router είναι ένα πολύ σημαντικό κομμάτι και η εξασφάλιση της μέγιστης ασφάλειας παίζει καθοριστικό ρόλο σε ένα δίκτυο, ορισμένα πράγματα που θα πρέπει να ληφθούν υπόψη είναι το Pingability όπου από τον πάροχο υπηρεσιών (service provider) υπάρχει περιορισμός σε δρομολογητές στους οποίους απαιτείται πρόσβαση. Για την πρόσβαση με χρήση SSH και την απομακρυσμένη πρόσβαση στους router ως ασφαλέστερη επιλογή μπορεί να χρησιμοποιηθεί το πρωτόκολλο SSH. Η ασφάλεια και κρυπτογράφηση που παρέχει το SSH το καθιστούν ως το μόνο πρωτόκολλο που θα πρέπει να χρησιμοποιείται σε οποιοδήποτε περιβάλλον δικτύου όπου υπάρχει κίνδυνος. Η SNMP πρόσβαση ανάγνωσης από τον ίδιο τον πελάτη σε εξοπλισμό διαχείρισης πελάτη εάν αυτό ζητηθεί από τον ίδιο. Ιδιαίτερα σημαντικό επίσης είναι να έχει υλοποιηθεί AAA μοντέλο (Authentication, Authorization and Accounting) για τον έλεγχό πρόσβασης στους router καθώς θα υπάρχει μόνο εξουσιοδοτημένη πρόσβαση στους εξοπλισμούς. Ακόμη, η εφαρμογή μιας λίστας πρόσβασης Access List στις θύρες VTY μπορεί να αποτρέψει την πρόσβαση στο router, με τη λέξη-κλειδί καταγραφής που περιλαμβάνεται στη ρητή άρνηση, καταγράφονται ακατάλληλες προσπάθειες. Ο ασφαλέστερος τρόπος αντιγραφής αρχείων από και προς έναν δρομολογητή είναι η δυνατότητα Secure Copy (SCP), η οποία είναι διαθέσιμη σε κάθε image IOS που υποστηρίζει SSH. Το SCP χρησιμοποιεί τους ίδιους ισχυρούς μηχανισμούς ασφαλείας με το SSH όσον αφορά την κρυπτογράφηση και τον έλεγχο. Το πρωτόκολλο Cisco Discovery (CDP) χρησιμοποιείται για ορισμένες λειτουργίες διαχείρισης δικτύου, αλλά είναι επικίνδυνο επειδή επιτρέπει σε οποιοδήποτε σύστημα σε ένα άμεσα συνδεδεμένο τμήμα να μάθει ότι ο δρομολογητής είναι μια συσκευή Cisco και να προσδιορίσει τον αριθμό μοντέλου και την έκδοση λογισμικού Cisco IOS που εκτελείται. Έτσι, αυτές οι πληροφορίες μπορούν να χρησιμοποιηθούν για το σχεδιασμό επιθέσεων εναντίον του δρομολογητή. Οι πληροφορίες CDP του είναι προσβάσιμες μόνο σε άμεσα συνδεδεμένα συστήματα με τον συγκεκριμένο εξοπλισμό. Το πρωτόκολλο CDP ενδέχεται επίσης να απενεργοποιηθεί με την εντολή global configuration χωρίς εκτέλεση CDP. Το CDP μπορεί να απενεργοποιηθεί σε ένα συγκεκριμένο interface μόνο. Το Network Time Protocol (NTP) δεν είναι ιδιαίτερα επικίνδυνο, αλλά οποιαδήποτε περιττή υπηρεσία μπορεί να αντιπροσωπεύει μια πορεία διείσδυσης έτσι εάν το NTP χρησιμοποιείται πραγματικά, είναι σημαντικό να οριστεί ένας

αξιόπιστος server χρόνου και να χρησιμοποιείται επίσης ο κατάλληλος έλεγχος ταυτότητας, επειδή η καταστροφή της βάσης χρόνου είναι ένας τρόπος για να αναγραφούν πρωτόκολλα ασφαλείας. Εάν το NTP δεν χρησιμοποιείται, θα ήταν καλό να απενεργοποιηθεί στο συγκεκριμένο interface. Εάν το interface αποκρίνεται με ένα μήνυμα ICM Pun reachable στον αποστολέα, εάν ένα πακέτο πέσει σε αυτό το interface, μπορεί να οδηγήσει σε κατάχρηση για να αρνηθεί την υπηρεσία σε μια διεπαφή. Επομένως, όταν δεν απαιτείται η δημιουργία μη προσπελάσιμων ICMP, συνιστάται να απενεργοποιείται η δημιουργία ή να περιορίζεται ο ρυθμός δημιουργίας ICMP. Το interface Null 0 δημιουργεί ICM Pun reachable, έτσι ώστε αυτή η εντολή θα πρέπει επίσης να εφαρμοστεί στο Null 0.

Η επαλήθευση διεύθυνσης source IPT αποτελεί το φιλτράρισμα εισόδου το οποίο είναι το κρίσιμο μέρος της διαμόρφωσης δρομολογητή από τον πάροχο υπηρεσιών. Το φιλτράρισμα Ingress εφαρμόζει φίλτρα στην κυκλοφορία που εισέρχεται σε ένα δίκτυο από έξω. Ο στόχος είναι να επαληθευτεί η διεύθυνση προέλευσης των εισερχόμενων πακέτων για να αποφευχθεί η πλαστογράφηση διεύθυνσης προέλευσης. Το Egress filtering εφαρμόζει ένα φίλτρο για όλη την κυκλοφορία που εξέρχεται από το δίκτυο ενός παρόχου υπηρεσιών. Κατά την προστασία και λήψη ACL (rACL), τα δεδομένα που λαμβάνονται από έναν δρομολογητή (GSR) μπορούν να χωριστούν σε δύο κατηγορίες, την κίνηση που περνά μέσω του δρομολογητή μέσω της διαδρομής προώθησης και την κίνηση που πρέπει να σταλεί μέσω της διαδρομής λήψης στον επεξεργαστή δρομολογητή gigabit (GRP) για περαιτέρω ανάλυση. Στο περιβάλλον rACL, το φιλτράρισμα προσθέτει ένα επιπλέον επίπεδο προστασίας έναντι μιας επίθεσης. Η χρήση δήλωσης άρνησης για μη αρχικά τμήματα στην αρχή του rACL απαγορεύει την πρόσβαση στο δρομολογητή. Σε σπάνιες περιπτώσεις, μια έγκυρη περίοδος σύνδεσης ενδέχεται να απαιτεί κατακερματισμό και επομένως να φιλτράρεται εάν υπάρχει μια δήλωση άρνησης θραύσματος στο rACL.

Το CoPP αντιμετωπίζει την ανάγκη προστασίας των επιπέδων ελέγχου και διαχείρισης, διασφαλίζοντας τελικά τη σταθερότητα δρομολόγησης, την προσβασιμότητα και την παράδοση πακέτων. Χρησιμοποιεί μια ειδική διαμόρφωση επιπέδου ελέγχου μέσω (QoS) για να παρέχει δυνατότητες φιλτραρίσματος και περιορισμού τιμών για πακέτα επιπέδου ελέγχου. Το CoPP αξιοποιεί το MQC για να καθορίσει κριτήρια ταξινόμησης επισκεψιμότητας και να καθορίσει διαμορφώσιμες ενέργειες πολιτικής για την

ταξινομημένη κίνηση. Η κίνηση ενδιαφέροντος πρέπει πρώτα να προσδιοριστεί μέσω χαρτών κατηγορίας, οι οποίοι χρησιμοποιούνται για τον καθορισμό πακέτων για μια συγκεκριμένη κατηγορία κυκλοφορίας. Το Cisco Auto Secure είναι μια εντολή Cisco IOS Security Line Interface (CLI). Οι πελάτες μπορούν να αναπτύξουν έναν από τους δύο τρόπους, ανάλογα με τις μεμονωμένες ανάγκες τους. Προτρέπει το χρήστη με επιλογές για ενεργοποίηση και απενεργοποίηση υπηρεσιών και άλλων λειτουργιών ασφαλείας. Εκτελεί αυτόματα την εντολή Cisco Auto Secure με τις προτεινόμενες προεπιλεγμένες ρυθμίσεις Cisco. Συνιστάται επίσης η χρήση του Unicast Reverse Path Forwarding (uRFP) στονPE. Η δυνατότητα αναζήτησης Unicast Reverse Path Forwarding (uRPF) θα πρέπει να είναι ενεργοποιημένη σε κάθε διεπαφή των διεπαφών CE των δρομολογητών PE και στις διεπαφές PE που βλέπουν PE.

Επιπρόσθετα, πραγματοποιείται έλεγχος ταυτότητας γειτονικού δρομολογητή όποτε ανταλλάσσονται ενημερώσεις δρομολόγησης μεταξύ γειτονικών δρομολογητών που βρίσκονται στον έλεγχο του φορέα παροχής υπηρεσιών. Αυτός ο έλεγχος ταυτότητας διασφαλίζει ότι ένας δρομολογητής λαμβάνει αξιόπιστες πληροφορίες δρομολόγησης από μια αξιόπιστη πηγή. Χωρίς έλεγχο ταυτότητας γείτονα, μη εξουσιοδοτημένες ή σκόπιμα κακόβουλες ενημερώσεις δρομολόγησης θα μπορούσαν να θέσουν σε κίνδυνο την ασφάλεια της κυκλοφορίας του δικτύου. Ένας συμβιβασμός ασφαλείας θα μπορούσε να προκύψει εάν ένα εχθρικό συμβαλλόμενο μέρος εκτρέψει ή αναλύσει την κίνηση του δικτύου. Για παράδειγμα, ένας μη εξουσιοδοτημένος δρομολογητής θα μπορούσε να στείλει μια πλασματική ενημέρωση δρομολόγησης για να πείσει το δρομολογητή να στείλει κίνηση σε λανθασμένο προορισμό. Αυτή η εκτροπή της κίνησης θα μπορούσε να αναλυθεί για να γίνουν γνωστές εμπιστευτικές πληροφορίες σχετικά με έναν οργανισμό ή απλώς χρησιμοποιήθηκε για να διαταράξει την ικανότητα του οργανισμού να επικοινωνεί αποτελεσματικά χρησιμοποιώντας το δίκτυο. Χρησιμοποιούνται δύο τύποι ελέγχου ταυτότητας γειτονικών, ο έλεγχος ταυτότητας απλού κειμένου και ο έλεγχος ταυτότητας μηνύματος Digest Algorithm Version 5 (MD5). Και οι δύο φόρμες λειτουργούν με τον ίδιο τρόπο, με την εξαίρεση ότι το MD5 στέλνει ένα "μήνυμα σύνοψης" αντί του ίδιου του κλειδιού ελέγχου ταυτότητας. Η σύνοψη μηνυμάτων δημιουργείται χρησιμοποιώντας το κλειδί και ένα μήνυμα, αλλά το ίδιο το κλειδί δεν αποστέλλεται, εμποδίζοντας την ανάγνωσή του κατά τη μετάδοση. Ο έλεγχος ταυτότητας απλού κειμένου στέλνει το ίδιο

το κλειδί ελέγχου ταυτότητας μέσω του καλωδίου. Όπως συμβαίνει με όλα τα κλειδιά, τον κωδικό πρόσβασης και άλλα μυστικά ασφαλείας, είναι επιτακτική ανάγκη το SP να προστατεύει στενά τα κλειδιά ελέγχου ταυτότητας στον έλεγχο ταυτότητας του γείτονα. Τα οφέλη ασφαλείας αυτής της δυνατότητας εξαρτώνται από το SP διατηρώντας σίγουρα όλα τα κλειδιά ελέγχου ταυτότητας. Επίσης, κατά την εκτέλεση εργασιών διαχείρισης δρομολογητών μέσω SNMP, δεν πρέπει να αγνοείται ο κίνδυνος που σχετίζεται με την αποστολή κλειδιών χρησιμοποιώντας μη κρυπτογραφημένο SNMP.

Με την πρόσβαση SNMP για τους πελάτες υπάρχει κίνδυνος υπερφόρτωσης της CPU με SNMP. Η σύσταση του παρόχου υπηρεσιών είναι να χρησιμοποιηθεί ένας διακομιστή μεσολάβησης SNMP για πρόσβαση πελατών. Ο έλεγχος ταυτότητας MD5 λειτουργεί παρόμοια με τον έλεγχο ταυτότητας απλού κειμένου, εκτός του ότι το κλειδί δεν αποστέλλεται ποτέ μέσω του καλωδίου. Αντ' αυτού, ο δρομολογητής χρησιμοποιεί τον αλγόριθμο MD5 για να παράγει μια "σύνοψη μηνυμάτων" του. Στη συνέχεια, αποστέλλεται το μήνυμα αντί του ίδιου του κλειδιού. Το πρωτόκολλο διανομής ετικετών (LDP) για τα στοιχεία χρησιμοποιεί έλεγχο ταυτότητας Message-Digest 5 (MD5) για να προστατεύεται από πλαστογράφηση ετικετών. Η ενεργοποίηση όλων των περιόδων σύνδεσης LDP για έλεγχο ταυτότητας MD5 ισχύει επίσης για περιβάλλοντα CsC όπου ένας δρομολογητής PE παρέχει στους δρομολογητές CE ετικέτες για διαδρομές IGP στο VPNMD5.

Ο μηχανισμός ασφαλείας TTL BGP. Η λειτουργία BGP Support for TTL Security Check εισάγει έναν μηχανισμό ασφαλείας για την προστασία των περιόδων Exterior Border Gateway Protocol (eBGP) από επιθέσεις με βάση τη χρήση CPU χρησιμοποιώντας πλαστά πακέτα IP. Η ενεργοποίηση αυτής της δυνατότητας αποτρέπει τις απόπειρες παραβίασης της περιόδου ανταλλαγής eBGP από έναν κεντρικό υπολογιστή σε ένα τμήμα δικτύου που δεν αποτελεί μέρος ενός δικτύου BGP ή από έναν κεντρικό υπολογιστή σε ένα τμήμα δικτύου που δε βρίσκεται μεταξύ των eBGP. Ενεργοποιείται η δυνατότητα αυτή διαμορφώνοντας μια ελάχιστη τιμή Time-To-Live (TTL) για εισερχόμενα πακέτα IP που λαμβάνονται από ένα συγκεκριμένο eBGPpeer. Όταν είναι ενεργοποιημένη το BGP θα δημιουργήσει και θα διατηρήσει την περίοδο λειτουργίας μόνο εάν η τιμή TTL στην κεφαλίδα πακέτου IP είναι ίση ή μεγαλύτερη από την τιμή TTL που έχει διαμορφωθεί για

την περίοδο peering. Εάν η τιμή είναι μικρότερη από τη διαμορφωμένη τιμή, το πακέτο απορρίπτεται και δεν δημιουργείται μήνυμα πρωτοκόλλου μηνύματος ελέγχου Internet (ICMP). Το BGP πρέπει να διαμορφωθεί στο δίκτυό και πρέπει να πραγματοποιηθούν συνεδρίες ανταλλαγής δεδομένων eBGP. Αυτή η δυνατότητα πρέπει να ρυθμιστεί σε κάθε δρομολογητή γιατί προστατεύει την ανταλλαγή eBGP peering μόνο στην εισερχόμενη κατεύθυνση και δεν επηρεάζει τα εξερχόμενα πακέτα IP ή τον απομακρυσμένο δρομολογητή. Κατά τη διαμόρφωση της δυνατότητας BGP Support for TTL Security Check, για την υποστήριξη μιας υπάρχουσας συνεδρίας peering πολλαπλών διαδρομών, πρέπει πρώτα να απενεργοποιηθεί η εντολή διαμόρφωσης γειτονικού ebgp-multihop δρομολογητή, εισάγοντας την εντολή no neighbor ebgp-multihop, προτού διαμορφωθεί αυτή η δυνατότητα με το γειτονικό δρομολογητή ttl-security ως εντολή διαμόρφωσης. Αυτές οι εντολές είναι αμοιβαία αποκλειστικές και απαιτείται μόνο μία εντολή για τη δημιουργία μιας συνεδρίας peering πολλαπλών γραμμών. Εάν γίνει προσπάθεια να διαμορφωθούν και οι δύο εντολές για την ίδια περίοδο peering, θα εμφανιστεί ένα μήνυμα σφάλματος στην κονσόλα.. Σε περίπτωση επίθεσης βασισμένης στη χρήση CPU από έναν δρομολογητή BGP που έχει διαμορφωθεί για peering, ίσως χρειαστεί να τερματιστούν οι επηρεαζόμενες συνεδρίες peering για να αντιμετωπιστεί η επίθεση. Αυτή η δυνατότητα δεν είναι αποτελεσματική έναντι επιθέσεων από ομότιμους που έχουν παραβιαστεί στο δίκτυό. Αυτός ο περιορισμός περιλαμβάνει επίσης BGPpeers που δεν αποτελούν μέρος του τοπικού ή εξωτερικού δικτύου BGP αλλά συνδέονται με το τμήμα δικτύου μεταξύ των BGP peers, για παράδειγμα, ένας διακόπτης ή διανομέας που χρησιμοποιείται για τη σύνδεση των τοπικών και εξωτερικών δικτύων BGP.

Η λειτουργία BGP Support for TTL Security Check εισάγει έναν μηχανισμό ασφαλείας για την προστασία των ανταλλαγών eBGP peering από επιθέσεις που βασίζονται στη χρήση της CPU. Αυτοί οι τύποι επιθέσεων είναι συνήθως βίαιες επιθέσεις άρνησης υπηρεσίας (DoS) που επιχειρούν να απενεργοποιήσουν το δίκτυο πλημμυρίζοντας το δίκτυο με πακέτα IP που περιέχουν πλαστές διευθύνσεις IP πηγής και προορισμού. Αυτή η δυνατότητα προστατεύει την ανταλλαγή eBGP peering, συγκρίνοντας την τιμή στο πεδίο TTL των ληφθέντων πακέτων IP έναντι ενός αριθμού hop που έχει διαμορφωθεί τοπικά για κάθε συνεδρία peering BGP. Εάν η τιμή στο πεδίο TTL του εισερχόμενου πακέτου IP είναι μεγαλύτερη ή ίση με την τοπικά διαμορφωμένη τιμή, το πακέτο IP γίνεται αποδεκτό

και υποβάλλεται σε επεξεργασία κανονικά. Εάν η τιμή TTL στο πακέτο IP είναι μικρότερη από την τοπικά διαμορφωμένη τιμή, το πακέτο απορρίπτεται και δε δημιουργείται μήνυμα ICMP.

Διαμόρφωση του ελέγχου ασφαλείας TTL για συνεδρίες Peering BGP

Η λειτουργία BGP Support for TTL Security Check έχει διαμορφωθεί με την εντολή ttl-security της γειτονικής σε κατάσταση διαμόρφωσης δρομολογητή ή σε λειτουργία διαμόρφωσης οικογένειας διευθύνσεων. Όταν αυτή η δυνατότητα είναι ενεργοποιημένη, το BGP θα δημιουργήσει ή θα διατηρήσει μια περίοδο λειτουργίας μόνο εάν η τιμή TTL στην κεφαλίδα πακέτου IP είναι ίση ή μεγαλύτερη από την τιμή TTL που έχει διαμορφωθεί για την περίοδο peering. Η ενεργοποίηση αυτής της δυνατότητας διασφαλίζει τη συνεδρία eBGP μόνο στην εισερχόμενη κατεύθυνση και δεν επηρεάζει τα εξερχόμενα πακέτα IP ή τον απομακρυσμένο δρομολογητή. Το όρισμα hop-count χρησιμοποιείται για τη διαμόρφωση του μέγιστου αριθμού λυκίσκου που διαχωρίζουν τους δύο συνομηλίκους. Η τιμή TTL καθορίζεται από το δρομολογητή από τον διαμορφωμένο αριθμό hop. Η τιμή για αυτό το όρισμα είναι ένας αριθμός από το 1 έως το 254.

Διαμόρφωση του TTL Security Check για Multihop BGP Peering Sessions

Η λειτουργία BGP Support for TTL Security Check υποστηρίζει τόσο άμεσα συνδεδεμένες συνεδρίες peering όσο και multihop peering. Όταν αυτή η δυνατότητα έχει διαμορφωθεί για μια συνεδρία peering πολλαπλών διαδρομών, η εντολή διαμόρφωσης του γειτονικού ebgp-multihop router δεν μπορεί να διαμορφωθεί και δεν απαιτείται για τον καθορισμό της συνεδρίας peering. Αυτές οι εντολές είναι αμοιβαία αποκλειστικές και απαιτείται μόνο μία εντολή για τη δημιουργία μιας συνεδρίας peering πολλαπλών γραμμών Εάν επιχειρηθεί να διαμορφωθούν και οι δύο εντολές για την ίδια περίοδο peering, θα εμφανιστεί ένα μήνυμα σφάλματος στην κονσόλα. Αυτή η δυνατότητα πρέπει να ρυθμιστεί σε κάθε δρομολογητή.

Οφέλη από την υποστήριξη BGP για τη λειτουργία ελέγχου ασφαλείας TTL

Η λειτουργία BGP Support for TTL Security Check παρέχει μια αποτελεσματική και εύχρηστη λύση για την προστασία περιόδων ανταλλαγής eBGP από επιθέσεις βάσει CPU. Όταν αυτή η δυνατότητα είναι ενεργοποιημένη, ένας κεντρικός υπολογιστής δεν μπορεί να επιτεθεί σε μια περίοδο λειτουργίας BGP εάν ο κεντρικός υπολογιστής δεν είναι μέλος του τοπικού ή απομακρυσμένου δικτύου BGP ή εάν ο κεντρικός υπολογιστής δεν είναι άμεσα συνδεδεμένος σε ένα τμήμα δικτύου μεταξύ των τοπικών και απομακρυσμένων δικτύων BGP. Αυτή η λύση μειώνει σημαντικά την αποτελεσματικότητα των επιθέσεων DoS κατά ενός αυτόνομου συστήματος BGP.

Διεύθυνση PE-CE

Η χρήση μη αριθμημένων συνδέσμων αντιμετωπίζεται συχνά ως μέσο για την ενίσχυση της ασφάλειας του PE, και σε κάποιο βαθμό του CE, επειδή δεν υπάρχει εκτεθειμένη διεύθυνση Layer 3 για επίθεση. Εάν είναι επιθυμητή μια τέτοια προσέγγιση, πρέπει να ληφθούν υπόψη οι επιπτώσεις στο πρωτόκολλο δρομολόγησης που χρησιμοποιείται μεταξύ των PE και CE. Ένα από τα πιο χρησιμοποιημένα εργαλεία αντιμετώπισης προβλημάτων στον χώρο δικτύου IP είναι η δοκιμή ICMP Echo (ping). Η χρήση μη αριθμημένων συνδέσμων αφαιρεί την ικανότητα του διαχειριστή δικτύου να κάνει ping στην απευθείας ως μεθοδολογία ανάλυσης σφαλμάτων. Περαιτέρω προστασία μπορεί επίσης να είναι διαθέσιμη με την κρυπτογράφηση της κίνησης που περνά πάνω από το σύνδεσμο χρησιμοποιώντας είτε μηχανισμούς κρυπτογράφησης ωφέλιμου φορτίου είτε κρυπτογραφήσεις πλήρους συνδέσμου.

Στατική δρομολόγηση

Η στατική δρομολόγηση παρέχει το πιο σταθερό και ελεγχόμενο σενάριο για τη διασύνδεση PE-CE. Με τους στατικούς ορισμούς διαδρομών, δεν υπάρχουν λανθασμένες διαδρομές που θα εισαχθούν εκτός από πληκτρολογώντας τις απευθείας στις

διαμορφώσεις. Επίσης, υπάρχει μικρότερο αντίκτυπο CPU με στατικές διαδρομές, επειδή δεν υπάρχει δυναμική διαδικασία δρομολόγησης. Επιπλέον, επειδή το CE και το PE χρησιμοποιούν συγκεκριμένες διαδρομές, και κατ' επέκταση η ασφάλεια της διασύνδεσης βελτιώνεται.

Δυναμική δρομολόγηση

Η χρήση ενός δυναμικού πρωτοκόλλου δρομολόγησης μειώνει την προσπάθεια διαμόρφωσης και στους δύο δρομολογητές PE και CE. Επίσης, οι αλλαγές εντός της διεύθυνσης δικτύου του πελάτη προσαρμόζονται εύκολα και η εναλλακτική διαδρομή αναπτύσσεται πιο εύκολα. Εάν πρόκειται να χρησιμοποιηθεί ένα δυναμικό πρωτόκολλο μεταξύ των δρομολογητών PE και CE, τότε το eBGP είναι η συνιστώμενη επιλογή λόγω των εγγενών χαρακτηριστικών σταθερότητας, κλιμάκωσης και ελέγχου. Σε κάθε περίπτωση, η χρήση ενός δυναμικού πρωτοκόλλου επιβάλλει τη χρήση ενός μηχανισμού ελέγχου ταυτότητας μεταξύ των δύο δρομολογητών για λόγους ασφαλείας. Προκειμένου να παρέχεται ένας βαθμός ασφάλειας σε ένα δυναμικά δρομολογημένο περιβάλλον PE-CE σε σχέση με τις ομότιμες σχέσεις μεταξύ των συνδέσμων PE-CE, ο έλεγχος ταυτότητας MD5 (Message Digest 5 Hashed Message Authentication Code [HMAC]) πρέπει να είναι ενεργοποιημένος. Αυτός ο μηχανισμός χρησιμοποιεί έναν εξαιρετικά ανθεκτικό αλγόριθμο κατακερματισμού για να παρέχει κάποια διαβεβαίωση ότι είναι ο επιδιωκόμενος γείτονας. Το MD5 θα πρέπει να χρησιμοποιείται σε αντίθεση με τους άλλους, λιγότερο ανθεκτικούς μηχανισμούς κατακερματισμού. Αυτός ο μηχανισμός είναι διαθέσιμος για όλα τα πρωτόκολλα δρομολόγησης PE-CE που υποστηρίζονται επί του παρόντος, συμπεριλαμβανομένων των ακόλουθων παραδειγμάτων.

CBC

Το μπλοκ Cipher (CBC) είναι ένας τρόπος λειτουργίας για ένα μπλοκ κρυπτογράφησης, στο οποίο μια ακολουθία bits κρυπτογραφείται ως μια απλή μονάδα ή ένα μπλοκ με ένα κλειδί κρυπτογράφησης που εφαρμόζεται σε ολόκληρο το μπλοκ. Το CBC χρησιμοποιεί αυτό που είναι γνωστό ως φορέας αρχικοποίησης (IV) ορισμένου μήκους. Ένα από τα

βασικά χαρακτηριστικά του είναι ότι χρησιμοποιεί έναν μηχανισμό αλυσίδας που κάνει την αποκρυπτογράφηση ενός μπλοκ κειμένου κρυπτογράφησης να εξαρτάται από όλα τα προηγούμενα μπλοκ κρυπτογράφησης. Με το BGP μεταξύ PE και CE, ο έλεγχος ταυτότητας ορίζεται ανά βάση. Επίσης, το BGP δεν υποστηρίζει προς το παρόν τη χρήση των βασικών αλυσίδων. Η βασική αλυσίδα των κατακερματισμών MD5 δεν υποστηρίζεται ακόμη με το BGP.

Δρομολόγηση OSPFPE-CE

Το OSPF καθορίζει επίσης απαιτήσεις ελέγχου ταυτότητας σε βάση ανά διεπαφή. Επιπλέον, ο έλεγχος ταυτότητας πρέπει να είναι ενεργοποιημένος για την περιοχή εντός του AS όπου θα πραγματοποιηθεί έλεγχος ταυτότητας. Όπως με το BGP, το OSPF δεν χρησιμοποιεί τη μεθοδολογία της βασικής αλυσίδας. Προκειμένου να αποφευχθεί η αποδοχή διαδρομών από μη αναγνωρισμένους γείτονες, συνιστάται η χρήση ελέγχου ταυτότητας MD5 μεταξύ PE και CE που χρησιμοποιούν δυναμικά πρωτόκολλα. Μέσα στο BGP, αυτό επιτυγχάνεται εγγενώς μέσω της «γειτονικής» δομής.

Μηχανισμός μέγιστου προθέματος BGP

Το BGP υποστηρίζει την έννοια ενός μέγιστου επιτρεπόμενου προθέματος. Μέσα στο BGP, η κατασκευή μέγιστου προθέματος επιτρέπει στο χρήστη να καθορίσει έναν μέγιστο αριθμό διαδρομών που θα γίνουν αποδεκτοί από το συγκεκριμένο γείτονα με τον οποίο συνδέεται . Μόλις επιτευχθεί αυτό ο δρομολογητής μπορεί να ρυθμιστεί ώστε να εκδίδει ένα προειδοποιητικό μήνυμα ή να κάνει επανεκκίνηση.

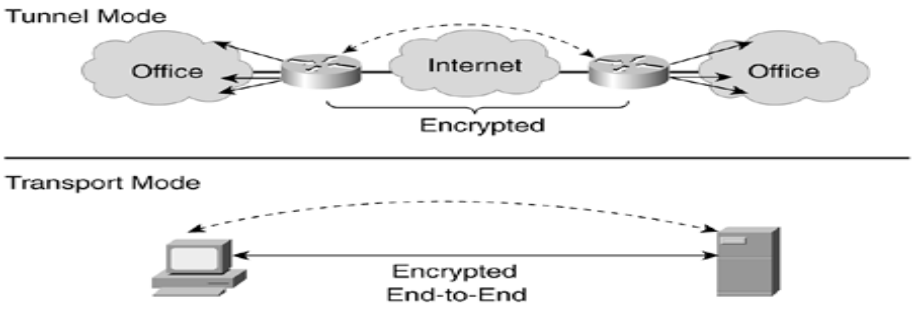
Τείχος προστασίας firewall

Είναι σαφές ότι το τείχος προστασίας πρέπει να θεωρείται ως απαραίτητο στοιχείο οποιασδήποτε πρόσβασης στο διαδίκτυο, είτε επιτυγχάνεται με οποιοδήποτε από τα ακόλουθα μέσα. Τείχος προστασίας σε μια κεντρική τοποθεσία με κεντρική πρόσβαση στο διαδίκτυο, είτε τείχος προστασίας σε κάθε τοποθεσία CE.

Κεφάλαιο 5 - IPsec

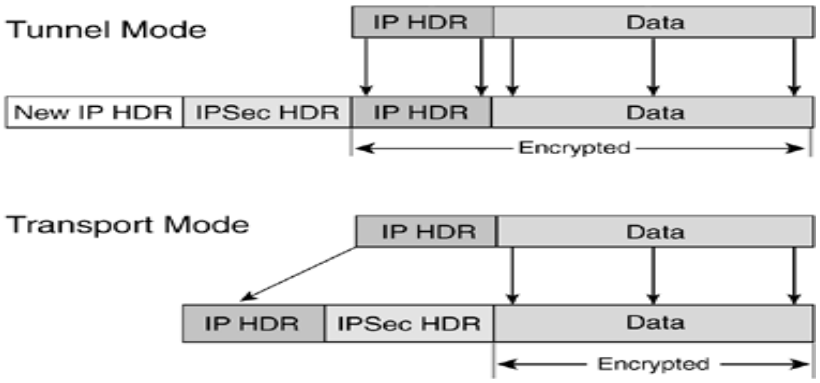
Το IPsec έχει αποτελέσει σημαντικό κομμάτι στην ασφάλεια στο επίπεδο του IP γιατί οι προδιαγραφές του IPsec ορίζουν στα πακέτα δύο τύπους δεδομένων, την επικεφαλίδα πιστοποίησης (AH-Authentication Header), για να παρέχει ακεραιότητα δεδομένων και την ενθυλάκωση ασφάλειας (ESP-Encapsulating Security Payload) όπου παρέχει πιστοποίηση ταυτότητας και την ακεραιότητα των δεδομένων. Περιλαμβάνει επίσης παραμέτρους επικοινωνίας μεταξύ συσκευών όπως διαχείριση των κλειδιών και συσχετισμούς ασφάλειας (security associations). Παρέχει κρυπτογράφηση και πιστοποίηση στο επιπέδου δικτύου, οι εφαρμογές και τα συστήματα που είναι στα άκρα του δικτύου δε χρειάζονται επιπλέον ρυθμίσεις για να έχουν ισχυρή ασφάλεια. Πρόκειται για κρυπτογραφημένα πακέτα τα οποία μοιάζουν όμως με κανονικά IP πακέτα και μπορούν να δρομολογηθούν από οποιοδήποτε IP δίκτυο, όπως χωρίς καμία αλλαγή στον ενδιάμεσο δικτυακό εξοπλισμό. Οι μόνες συσκευές οι που γνωρίζουν για την κρυπτογράφηση είναι αυτές στα δυο ακραία σημεία. Μειώνει έτσι δραστικά τόσο το κόστος της υλοποίησης αλλά και το κόστος της διαχείρισης. Το IPSec συνδυάζει τις τεχνολογίες ασφάλειας σε ένα σύστημα ολοκληρωμένο που παρέχει ακεραιότητα, πιστοποίηση και εμπιστευτικότητα. Οι προδιαγραφές αυτές περιλαμβάνουν κατάλληλο IP πρωτόκολλο ασφαλείας, το οποίο καθορίζει την πληροφορία που πρέπει να προστεθεί σε ένα IP πακέτο για να ενεργοποιηθούν οι έλεγχοι πιστότητας, ακεραιότητας και πιστοποίησης ταυτότητας, όπως επίσης καθορίζει και το πώς πρέπει να γίνει η κρυπτογράφηση των δεδομένων του πακέτου, και ανταλλαγή κλειδιών Internet, το οποίο διαπραγματεύεται το συσχετισμό ασφάλειας μεταξύ δυο οντοτήτων και ανταλλάσσει το υλικό των κλειδιών. Δεν είναι απαραίτητο να χρησιμοποιηθεί το IKE, αλλά το να ρυθμιστούν χειροκίνητα οι συσχετισμοί ασφάλειας είναι μια δύσκολη και επίπονη διαδικασία. Το IKE πρέπει να χρησιμοποιείται στις περισσότερες εφαρμογές για να ενεργοποιεί ασφαλείς επικοινωνίες μεγάλης κλίμακας. Η τεχνολογία IPsec παρέχει υπηρεσίες ασφάλειας σε ένα δίκτυο όπως είναι η αυθεντικότητα, η ακεραιότητα, η εμπιστευτικότητα και το anti-replay. Το σημαντικό πλεονεκτήματα που παρέχει το IPsec είναι ότι όλες οι υπηρεσίες ασφαλείας που εφαρμόζει είναι στο επίπεδο δικτύου, αυτό έχει ως αποτέλεσμα οι υπηρεσίες ασφαλείας να παραμένουν ανεξάρτητες από το μηχανισμό μεταφοράς όπως επίσης και από τα πρωτόκολλα και τις εφαρμογές που χρησιμοποιούνται

στην κορυφή της στοίβας. Μπορεί να εφαρμοστεί από άκρο σε άκρο, μεταξύ πελάτη και διακομιστή.



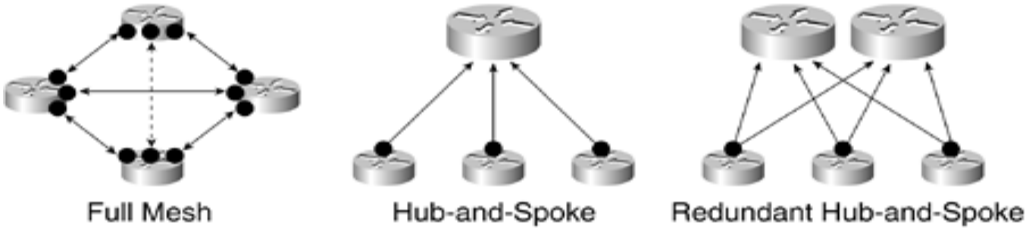
Εικόνα 11 Ip sec tunnel

Με αυτούς τους δύο τρόπους σύνδεσης, υπάρχουν δύο τρόποι αντιστοίχισης πακέτων IP σαφούς κειμένου σε πακέτο IPsec. Ολόκληρο το πακέτο IP κειμένου είναι ασφαλές και προετοιμάζεται μια νέα κεφαλίδα IP, ακολουθούμενη από μια κεφαλίδα IPsec που προσδιορίζει τη λογική σύνδεση μεταξύ των πυλών IPsec. Κατά τη λειτουργία μεταφοράς, διατηρείται η αρχική κεφαλίδα IP και η κεφαλίδα IPsec εισάγεται πριν από το ασφαλές πακέτο.



Εικόνα 12 Επικεφαλίδα

Ένα tunnel IPsec μπορεί συνδέσει δύο σημεία και με την προσθήκη περισσότερων tunnel, μπορεί να δημιουργηθεί έναVPN μεταξύ των πυλών IPsec. Αυτό μπορεί να γίνει με τις ακόλουθες τοπολογίες full mesh, hub and spoke ή και με redundant hub and spoke.



Εικόνα 13 τοπολογίες με IPsec tunnels

Όταν απαιτείται να υπάρχει ασφάλεια όπως για παράδειγμα, ένα δίκτυο τραπεζών που διασυνδέει τα δύο κεντρικά γραφεία με τα υποκαταστήματα. Οι κύριες επιλογές για τη δημιουργία σηράγγων IPsec είναι οι ακόλουθες.

Στατικό IPsec

ΚάθεσημείοIPsec διαμορφώνεται στατικά με όλα τα IPsec tunnel. Είναι δύσκολο να διαμορφωθεί επειδή κάθε κόμβος IPsec απαιτεί σημαντική διαμόρφωση. Υποστηρίζεται στις περισσότερες πλατφόρμες (RFC 2401-22412). Μπορεί να εφαρμοστεί CE-CE και PE-PE.

Δυναμικό IPsec

Μπορεί να διαμορφωθεί χωρίς συγκεκριμένες πληροφορίες για κάθε ακτίνα. Μόνο οι ακτίνες ξέρουν πώς να φτάσουν στο κέντρο και δημιουργείται μια σήραγγα IPsec μόνο εάν το ακουστικό μπορεί να πιστοποιηθεί. Η IPsec απομακρυσμένης πρόσβασης χρησιμοποιεί μια παρόμοια ιδέα, αλλά ο έλεγχος ταυτότητας γίνεται συνήθως σε διακομιστή AAA. Το Dynamic IPsec μπορεί να χρησιμοποιηθεί τόσο για CE-CE όσο και για PE-PE.

Dynamic Multipoint VPN (DMVPN)

Αυτό το μοντέλο λειτουργεί με την αρχή του Next Hop Resolution Protocol (NHRP). Κάθε κόμβος IPsec περιέχει πληροφορίες σχετικά με τον τρόπο πρόσβασης σε έναν επόμενο διακομιστή hop ο οποίος επιστρέφει τη διεύθυνση του κόμβου IPsec προορισμού στον

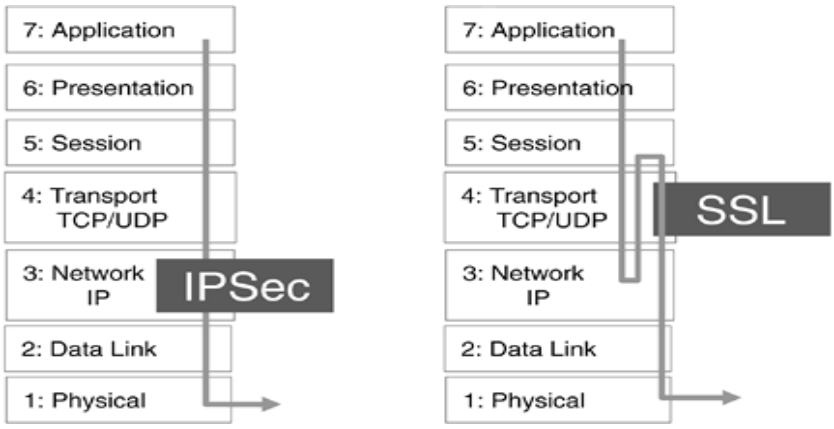
αρχικό κόμβο. Αυτός είναι ένας πολύ επεκτάσιμος τρόπος για τη δυναμική δημιουργία σηράγγων IPsec. Το DMVPN λειτουργεί CE-CE και PE-PE.

Χρήση κρυπτογράφησης

Η κρυπτογράφηση παρέχει μια μεγάλη ποικιλία λύσεων για συγκεκριμένα πρωτόκολλα του επιπέδου σύνδεσης, εξασφαλίζει μόνο έναν σύνδεσμο αλλά δεν παρέχει ασφάλεια από άκρο σε άκρο του VPN.

Secure Sockets Layer (SSL)

Τα SSL όπως και το IPsec εξασφαλίζουν την ασφαλή μεταφορά αλλά σε διαφορετικά σημεία στη στοίβα. Το IPsec ενεργεί στο επίπεδο δικτύου, πράγμα που σημαίνει ότι είναι, όπως το IP, ανεξάρτητο από το μέσο μεταφοράς και από τις εφαρμογές που εκτελούνται στην κορυφή. Το IPsec μπορεί να χρησιμοποιηθεί σε ένα τελικό σημείο χωρίς καμία αλλαγή στις εφαρμογές ή στα χαμηλότερα επίπεδα στη στοίβα. Το SSL αντίθετα στηρίζεται στην ασφάλεια επιπέδου μεταφοράς και βρίσκεται στο επίπεδο 4 στη στοίβα. Αυτό είναι ιδανικό για εφαρμογές όπως το Hypertext Transport Protocol (HTTP) που βρίσκεται πάνω από το επίπεδο TCP.



Εικόνα 14 ssl & ιp sec

Η SSL έχει βρει εφαρμογή σε πύλες VPN όπου απαιτείται περιορισμένη υποστήριξη εφαρμογών, όπως όταν η πρόσβαση VPN χρησιμοποιείται μόνο για πρόσβαση σε ιστοσελίδες. Το πλεονέκτημα σε αυτά τα σενάρια είναι ότι το SSL δεν απαιτεί πελάτη στον υπολογιστή. Σε περιβάλλοντα MPLSVPN, το SSL δε χρησιμοποιείται για ασφάλεια CE-CE ή PE-PE, αλλά μπορεί να χρησιμοποιηθεί ως τεχνολογία απομακρυσμένης πρόσβασης. Όπου απαιτείται ασφάλεια σε επίπεδο VPN, το IPsec είναι η σημερινή βασική τεχνολογία, με όλες τις επιλογές ανάπτυξης.

Κεφάλαιο 6 - Πρακτικό μέρος

Στην παρακάτω υλοποίηση έχει κατασκευαστεί ένα ασφαλές MPLSVPN πάνω από το οποίο έχει περαστεί εσωτερική sip τηλεφωνία. Το configuration αποτελεί template βάση του οποίου έγινε η συγκεκριμένη υλοποίηση

Customer router (CE)

```
config-register 0x2102
version 12.4
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
hostname eirini

boot-start-marker
boot system flash c2801-entservicesk9-mz.124-15.T10.bin
boot-end-marker

logging count
logging buffered 128000
logging reload informational
logging console errors
enable secret 5 xxxxxx
enable password <removed>

aaa new-model
aaa group server tacacs+ TACACS-AAA-GROUP
 server x.x.x.x
 server x.x.x.x
aaa authentication login default group TACACS-AAA-GROUP enable
aaa authentication login CON-AUX enable
aaa authorization console
```

```
aaa authorization exec default group TACACS-AAA-GROUP if-authenticated
aaa authorization exec CON-AUX if-authenticated
aaa authorization commands 1 default group TACACS-AAA-GROUP none
aaa authorization commands 1 CON-AUX if-authenticated
aaa authorization commands 15 default group TACACS-AAA-GROUP none
aaa authorization commands 15 CON-AUX if-authenticated
aaa session-id common

clock timezone EET 2
clock summer-time EET recurring last Sun Mar 3:00 last Sun Oct 4:00
clock calendar-valid
network-clock-participate wic 0
dot11 syslog
no ip source-route
ip cef

no ip domain lookup
ip domain name abcd.prv
multilink bundle-name authenticated
isdn switch-type basic-qsig
voice-card 0
voice service voip
sip
bind control source-interface Loopback0
bind media source-interface Loopback0

voice class codec 1
codec preference 1 g729br8 bytes 40
 codec preference 2 g729r8 bytes 40
 codec preference 3 g711alaw
 codec preference 4 g711ulaw
rchive
```

```
 log config
logging enable
logging size 500
 hidekeys

ip ssh version 2
class-map match-all GOLD
match access-group name GOLD
class-map match-any BRONZE
match any
class-map match-all SILVER
match access-group name SILVER

policy-map CPE-OUT
class SILVER
set ip precedence 3
bandwidth 1536
class GOLD
priority 512
set ip precedence 5
policy-map MPLS-OUT
class GOLD
priority 1024
set ip precedence 5
class SILVER
set ip precedence 3
bandwidth 2048
class BRONZE
bandwidth 16380
set ip precedence 1
interface Loopback0
 ip adrress x.x.x.x 255.255.255.255
```

```
interface FastEthernet0/0
 no ip address
load-interval 30
speed 100
full-duplex

interface FastEthernet0/0.1
encapsulation dot1Q 1 native
ip address  x.x.x.x 255.255.255.0

interface FastEthernet0/0.10
encapsulation dot1Q 10
 ip address x.x.x.x 255.255.255.224

interface FastEthernet0/1
ip address  x.x.x.x 255.255.255.252
load-interval 30
duplex auto
speed auto
service-policy output MPLS-OUT

interface FastEthernet0/3/0
switchport access vlan x

interface FastEthernet0/3/1
interface FastEthernet0/3/2
interface FastEthernet0/3/3

interface BRI0/0/0
no ip address
no logging event link-status
```

```
isdn switch-type basic-qsig
isdn timer T310 120000
isdn protocol-emulate network
isdn point-to-point-setup
isdn layer1-emulate network
isdn incoming-voice voice
isdn supp-service name calling profile Network-Extension operation-value-tag local
isdn skipsend-idverify
interface BRI0/0/1
no ip address
isdn switch-type basic-qsig
isdn point-to-point-setup

interface ATM0/1/0
no ip address
shutdown
no snmp trap link-status
atm ilmi-keepalive
dsl operating-mode itu-dmt
pvc 8/35
pppoe-client dial-pool-number 1 dial-on-demand

interface Serial0/2/0
no ip address
shutdown
clock rate 2000000

interface Serial0/2/1
no ip address
shutdown
clock rate 2000000
```

```
interface Vlan1
no ip address

nterface Vlan2
ip address  x.x.x.x  255.255.255.0
interface Dialer0
ip address negotiated
ip mtu 1492
ip virtual-reassembly
encapsulation ppp
ip tcp header-compression
ip tcp adjust-mss 1452
load-interval 30
shutdown
dialer pool 1
dialer redial interval 60 attempts 3 re-enable 300
dialer-group 1
no snmp trap link-status
no keepalive
no cdp enable
ppp authentication pap chap callin
ppp chap hostname eirini6%eirini.gr
ppp chap password xxxxxxx
ppp pap sent-username yyyyyy password xxxxxxxx
router bgp 654321
bgp log-neighbor-changes
neighbor x.x.x.x remote-as  x.x.x.x

address-family ipv4
redistribute connected
redistribute static
neighbor x.x.x.x activate
```

```
neighbor x.x.x.x soft-reconfiguration inbound
neighbor x.x.x.x route-map LP-95 in
neighbor x.x.x.x route-map MED-100 out
default-information originate
no auto-summary
no synchronization
exit-address-family

ip forward-protocol nd



no ip http server
no ip http secure-server
ip tacacs source-interface Loopback0
ip access-list extended GOLD
permit tcp any eq 1720 any
permit tcp any any eq 1720
permit ip any host x.x.x.x
permit ip any host x.x.x.x
permit ip any host x.x.x.x
deny   ip any any

ip access-list extended SILVER
permit ip any host x.x.x.x
permit ip any host x.x.x.x
permit ip any host x.x.x.x
deny   ip any any
ip prefix-list ROUTES permit x.x.x.x
ip prefix-list CUSTOMER-ROUTES permit x.x.x.x
ip prefix-list CUSTOMER-ROUTES permit x.x.x.x

ip sla responder
```

```
logging history size 50
logging history informational
logging facility local0
logging source-interface Loopback0

dialer-list 1 protocol ip permit
snmp-server view SAA_VIEW ciscoRttMonObjects included
snmp-server community  RO 99
snmp-server community  rr90
snmp-server trap-source Loopback0
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps envmon
snmp-server enable traps dsp card-status
snmp-server enable traps frame-relay multilink bundle-mismatch
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps ipsla
snmp-server enable traps syslog
snmp-server host x.x.x.x
snmp-server host x.x.x.x
route-map LP-100 permit 10
set local-preference 100

route-map LP-95 permit 10
set local-preference 95
route-map MED-100 permit 10
match ip address prefix-list CUSTOMER-ROUTES
set metric 100

route-map MED-100 deny 20

route-map MED-95 permit 10
```

```
match ip address prefix-list CUSTOMER-ROUTES
set metric 95

route-map MED-95 deny 20

tacacs-server host x.x.x.x
tacacs-server host x.x.x.x
tacacs-server timeout 4
tacacs-server key <removed>

control-plane

voice-port 0/0/0
compand-type a-law
no comfort-noise
cptone GR
description ISDN-1

voice-port 0/0/1
dial-peer cor custom
dial-peer voice 3 voip
destination-pattern 3...
voice-class codec 1
voice-class source interface Loopback0
session protocol sipv2
session target ipv4:x.x.x.x
ip qos dscp cs5 media
ip qos dscp cs5 signaling
no vad

dial-peer voice 4 voip
destination-pattern 26..
```

```
voice-class codec 1
voice-class source interface Loopback0
session protocol sipv2
session target ipv4:x.x.x.x
ip qos dscp cs5 media
ip qos dscp cs5 signaling
no vad

dial-peer voice 5 voip
destination-pattern 96..
voice-class codec 1
voice-class source interface Loopback0
session protocol sipv2
session target ipv4: x.x.x.x
ip qos dscp cs5 media
ip qos dscp cs5 signaling
no vad

dial-peer voice 1 pots
destination-pattern 95..
no digit-strip
direct-inward-dial
port 0/0/0

no vad
dial-peer voice 5 voip
destination-pattern 42..
voice-class codec 1
voice-class source interface Loopback0
session protocol sipv2
session target ipv4:x.x.x.x
ip qos dscp cs5 media
```

```
ip qos dscp cs5 signaling
no vad

 dial-peer voice 100 voip
 destination-pattern 76..
voice-class codec 1
voice-class source interface Loopback0
session protocol sipv2
session target ipv4:x.x.x.x
ip qos dscp cs5 media
ip qos dscp cs5 signaling
no vad

dial-peer voice 110 voip
destination-pattern 24..
voice-class codec 1
voice-class source interface Loopback0
session protocol sipv2
session target ipv4:x.x.x.x
ip qos dscp cs5 media
ip qos dscp cs5 signaling
no vad
dial-peer voice 130 voip
destination-pattern 67..
voice-class codec 1
voice-class source interface Loopback0
session protocol sipv2
session target ipv4:x.x.x.x
ip qos dscp cs5 media
ip qos dscp cs5 signaling
 no vad
```

```
line con 0
session-timeout 30  output
exec-timeout 30 0
authorization commands 1 CON-AUX
authorization commands 15 CON-AUX
authorization exec CON-AUX
logging synchronous
login authentication CON-AUX
transport preferred none
transport output telnet ssh
stopbits 1
flowcontrol hardware
line aux 0
no exec
transport output none
line vty 0 4
access-class 2 in
exec-timeout 30 0
logging synchronous
transport preferred none
 transport input ssh
```

Provider Router

Το παρακάτω configuration αποτελεί template βάση του οποίου δημιουργήθηκε το vrf για την συγκεκριμένη υλοποίηση και αφορά την δημιουργία του mpls από την μεριά του παρόχου. Επιπλέον στον provider router PE υπάρχουν μηχανισμοί και δικλίδες για την ασφάλεια του δικτύου και οι οποίες δεν μπορούν να καταγραφούν

```
ip vrf abcd
rd 1241:2520
export map CPE
route-target export xxxx:yyyy
route-target import xxxx:yyyy
route-target import xxxx:yyyy

interface GigabitEthernet0/0/0.123456
encapsulation dot1Q z second-dot1q 2
ip vrf forwarding abcd
ip address x.x.x.x.x 255.255.255.252
service-policy input ASD_IN
service-policy output ASD_OUT

router bgp z
address-family ipv4 vrf abcd
redistribute connected
redistribute static
neighbor x.x.x.x remote-as y
neighbor x.x.x.x activate
neighbor x.x.x.x as-override
neighbor x.x.x.x soft-reconfiguration inbound
neighbor x.x.x.x prefix-list DEFAULT-ROUTE-PREFIXLIST out
neighbor x.x.x.x maximum-prefix 40 warning-only
exit-address-family
```

Κεφάλαιο 7 – Συμπεράματα

Όπως γίνεται αντιληπτό το MPLS μπορεί να αποτελέσει ένα ασφαλές δίκτυο καθώς πρόκειται για ένα κλειστό κύκλωμα layer 2 που δεν έχει πρόσβαση στο Internet. Με τη χρήση σωστού σχεδιασμού του δικτύου και μελέτη ασφάλειας μπορεί να αποτελέσει μια πολύ αξιόπιστη ασφαλή λύση στα σημερινά δίκτυα. Τα τελευταία χρόνια έχει βρει αρκετά μεγάλη εφαρμογή και έχει αποδειχθεί ότι μπορεί να είναι μια ασφαλή λύση με πολλές δυνατότητες. Βάση της υλοποίησης που πραγματοποιήθηκε στην παρούσα εργασία μπορεί μέσω του MPLS δικτύου να δρομολογηθεί με ασφάλεια οποιοδήποτε είδος κυκλοφορίας τόσο υπηρεσίες δεδομένων mpls αλλά και υπηρεσίες τηλεφωνίας είτε πρόκειται για απλή δρομολόγηση voice κίνησης είτε για την υλοποίηση εσωτερικής τηλεφωνίας μέσω του MPLS VPN. Ένα ακόμη σημαντικό πλεονέκτημα που παρέχει η υλοποίηση τηλεφωνίας πάνω από το MPLS δίκτυο είναι ότι παρέχεται QOS με εγγυημένο bandwidth και καλύτερη ποιότητα κλήσεων έναντι της κλασικής τηλεφωνίας. Επίσης, οι κλήσεις που δρομολογούνται μέσω ενός MPLS δικτύου είναι κρυπτογραφημένες και μπορεί να υλοποιηθεί και ipsec. Στην παρούσα πτυχιακή εργασία έγινε υλοποίηση ενός mpls vpn όπου υπάρχει επικοινωνία μεταξύ των σημείων και επιπλέον δρομολογήθηκε εσωτερική τηλεφωνία μεταξύ των σημείων.

Βιβλιογραφικές Αναφορές

Νικολόπουλος, Σ. (2019). *Μελετη εφαρμογής MPLS σε τοπικά δίκτυα,ΕΑΠ*

Cisco (2021).*Introduction to Cisco MPLS VPN Technology – Cisco,* Retrieved from:

Cisco (2021).*Cisco Press MPLS Fundamentals*

Cisco (2021).*Cisco Press Advanced MPLS Design and Implementation*

Tanenbaum, A. S. (2003). *Computer Networks*, Fourth Edition, Prentice Hall, ISBN 9600133499456.

Tanenbaum, A. S. (2008). *Δίκτυα Υπολογιστών*, 4η έκδοση, Κλειδάριθμος, Αθήνα

http://etutorials.org/

Peterson P.,(2007), The new Banking services, McGraw Hill

Sommestad, T., Ekstedt, M., Holm, H., & Afzal, M. (2011). Security mistakes in information system deployment projects. Information Management & Computer Security

Λιμνιώτης Γ.(2005-2006) Σχεδίαση Εικονικών δικτύων

Τάσσιος Κ.(2004) Υλοποίηση Της Υπηρεσίας Διαλειτουργικότηταςς μεταξύ τεχνικών Circuit Cross Connect & Any Transport over MPLS

Τσώνης Α(2015) Προσομοιώσεις MPLS Δικτύων με χρήση του OMNeT+

Luc De Ghein (2006, November). Cisco Press MPLS Fundamentals ISBN-10: 1-58705-197-4

Μοραντζής Σταύρος, Μελέτη της τεχνολογίας MPLS, Πανεπιστήμιο Πειραιώς

https://tools.ietf.org/html/rfc3031 [25]

https://tools.ietf.org/html/rfc3032 [26]

IEEE: https://tools.ietf.org/html/rfc3036

S. Halabi and D. McPherson, Internet Routing Architectures. Cisco Press, second ed., 2001.

Ivan Pepelnjak and Jim Guichard (2002, May). Cisco Press MPLS and VPN Architectures ISBN-10: 1-58705-081-1

Ivan Pepelnjak, Jim Guichard, Jeff Apsar (2003, June). Cisco Press MPLS and VPN Architectures, Volume II ISBN-10: 1-58705-112-5