**VPN – virtual private network**

על מנת לייצר קשר P2P בין שני נתבים שבבעלותי לצורך הרשת הפרטית שלי אבל הנתבים יושבים בשני מקומות גיאוגרפים שונים ומחוברים לרשת האינטרנט אני צריך ליצור קישור וירטואלי בין שני הנתבים על גבי האינטרנט, כלומר לייצר לי רשת פרטית וירטואלית על גבי האינטרנט.

* נשתמש בפרוטוקול GRE כדי לייצר TUNNEL בין שני הנתבים של הרשת הפרטית שלנו,  
  הגדרות חשובות כדי שה-TUNNEL יעלה: SRC וDES יוגדרו בהצלבה בין שני הנתבים
  + Tunnel source
  + Tunnel destination
  + Ip address
  + שניתוב לtunnel destination לא יהיה דרך הTUNNEL על מנת שלא יוצר לנו recursive route, ניתן לעשות זאת על ידי הגדרת הניתוב לDES ואת הניתוב לכתובת של הTUNNEL עצמו בפרוטוקולים נפרדים.
* על מנת שיהיה לנו קישור מאובטח על גבי הVPN נרצה להשתמש בהצפנה מסוימת, נשתמש בIPSec
  + **נקודה חשובה לגבי IPSec היא שהוא מעביר רק מידע מסוג Unicast ולא מעביר Multicast**
  + IPSec הוא לא בדיוק פרוטוקול מכיוון שהוא מורכב ממספר אלגוריתמים כלומר, זה Framework ולא פרוטוקול. הפרוטוקולים בהם IPSec משתמש הם:
    - הבסיס של הפרוטוקול שיכול להיות מורכב משני אלגוריתמים – הencapsulation של הפרוטוקול:
      * Authentication Header – אימות בלבד
      * ESP – אימות שכולל גם הצפנה
      * ניתן להשתמש בשילוב של 2 האלגוריתמים
    - Confidentiality – חסיון, הצפנה. ככל שכמות הביטים של ההצפנה גבוה אז ההצפנה טובה יותר יש מספר אפשרויות:
      * DES
      * 3DES
      * AES – 255 ביטים
      * SEAL
    - Integrity – יושרה, לוודא שהמידע לא שונה בדרך ושהגיע כמו שנשלח, יש 2 אפשרויות לשימוש:
      * MD5
      * SHA
    - Authentication – אימות נתונים, ישנם 2 אפשרויות:
      * PSK
      * RSA
    - Diffie-Hellman – שיטה להעברת מפתחות הצפנה,   
      ניתן להשתמש באחת מהגרסאות שיש באלגוריתם זה.
  + כאשר נרים את הIPSEC המידע יעבור על גבי רשת ציבורית, על מנת למנוע את השליחה של המידע שאמור להיות מוצפן משתמשים בפרוטוקול שנקרא IKE אשר מייצר סוג של TUNNEL של גביו יוקם הIPsec
  + IPSEC מאפשר לי את האופציה שנקראת replay detection שבה ניתן למספר פקטות וככמה לדעת שבאמת הכמות הנכונה של פקטות והסדר הנכון של הפקטות מגיעות ושלא מישהו מכניס פקטות בדרך.
  + ישנם שני מצבים שבהם ניתן לעבוד בIPSEC:
    - Tunnel modes – מצב שבו מצפינים את המידע שעובר וגם את הTUNNEL שעל גביו עובר המידע, במצב זה משתמשים בTUNNEL של IPSEC
    - Transport mode – מצב בו מצפינים רק את המידע ולא את הTUNNEL על גביו עובר המידע, במצב זה משתמשים בTUNNEL של פרוטוקול אחר (לדוגמא: GRE)
  + מתווסף לנו ESP Header
  + IKE – TUNNEL שמוקם בIPSEC לטובת החלפת מפתחות בין הנתבים, יוקם ישר לפני שהIPSEC עולה
    - לIKE יש 2 שלבים(PHASE):
      * V1 – הקמה של הIKE עצמו, לשלב זה יש 2 אפשרויות למצבי עבודה
        + MAIN MODE – MM – המצב הרגיל שלוקח טיפה יותר זמן להקים את הIKE
        + AGGRESSIVE MODE – AM – שולח בצורה מהירה יותר את ההודעות על מנת להקים את הIKE יותר מהיר
      * V2 – העברת מפתחות של הIPSEC על הIKE שהקמנו
  + ישנם סוגים שונים של IPSEC:
    - Site To Site IPsec VPNs –
    - Cisco Dynamic Multipoint VPN (DMVPN) –
    - Cisco Group Encrypted Transport VPN (GET VPN) –
    - Cisco FlexVPN –
    - Remote VPN access –
* ניתן לראות את הPOLICY של הIPsec על ידי הפקודה : show crypto isakmp policy
* ניתן לראות סטטוס של IPsec על ידי הפקודה: show crypto ipsec sa address

**הגדרות:**

יש שתי דרכים להגדיר את הIPsec על גבי GRE TUNNEL

* Profile – שבה מגדירים את האלגוריתמים בהם נשתמש לIPsec, דרך פשוטה להגדרה
  + נייצר POLICY של IPSEC בה נגדיר את האלגוריתמים שנשתמש
  + נייצר "משתנה" שיגדיר לנו באיזה סוג של IPsec אנחנו משתמשים tunnel/transport
  + נייצר פרופיל של IPsec שבו נגדיר את הסוג של הIPsec על ידי "המשתנה" שיצרנו לפני
  + נכיל את הפרופיל על הGRE TUNNEL
* Crypto Map – הגדרת הIPsec בשימוש עם ACL, טיפה יותר מסובך להגדיר