אבטחת מחשבים ורשתות

203.4448

סמסטר חורף תשע"ב (2011)

הרצאה 8 – הגנה ברמת הרשת

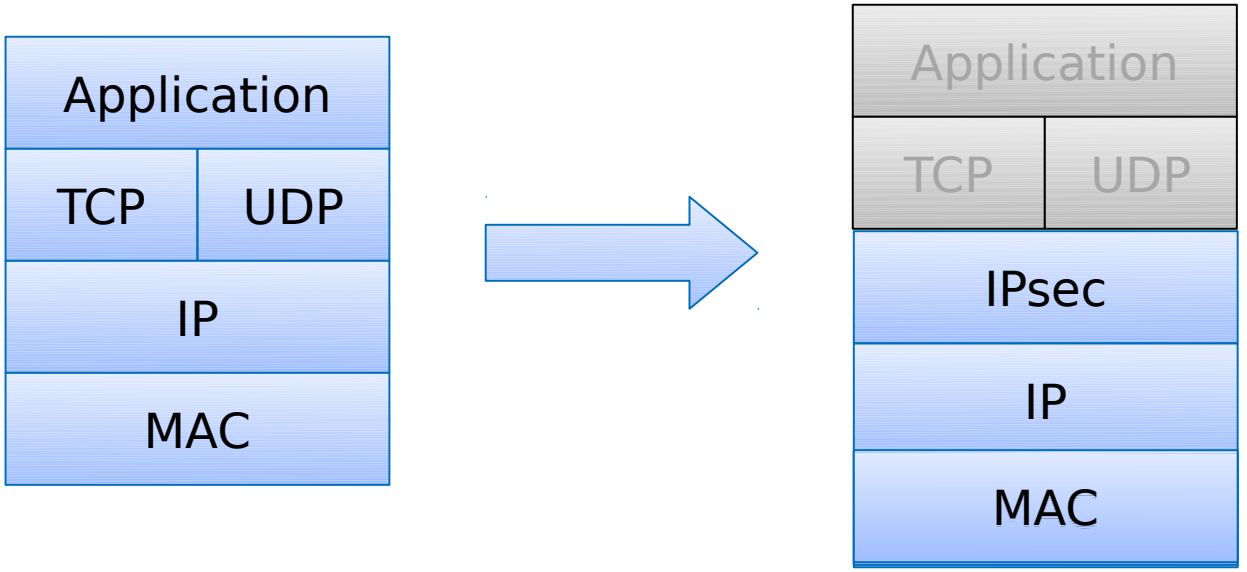
IPsec

מבוא

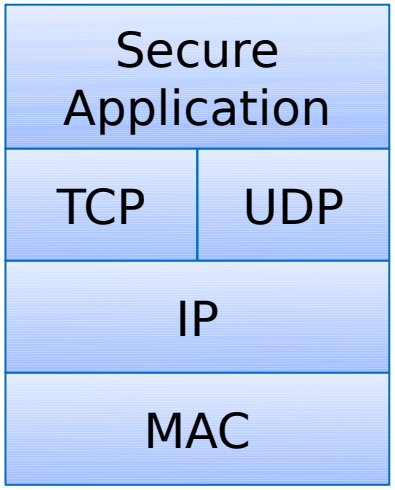
- Firewalls מספקים הגנה על נתונים/משאבים "נייחים" בתוך הרשת המוגנת
- המטרה של פרוטוקולי אבטחה: להגן על נתונים בזמן מעבר ברשת (לספק סודיות, שלמות, אימות השולח ועוד)
- מטרה נוספת: מניעת התקפות נוספות: למשל, התקפות כגון חטיפת הקשר ו-syn attack

באיזו שכבה להוסיף שירותי אבטחה?

הגדרה: נאמר שפרוטוקול אבטחה עובד ברמה x אם הוא מגן על המידע של השכבות שמעל x, לדוגמא הוספת הגנה ברמת הרשת:

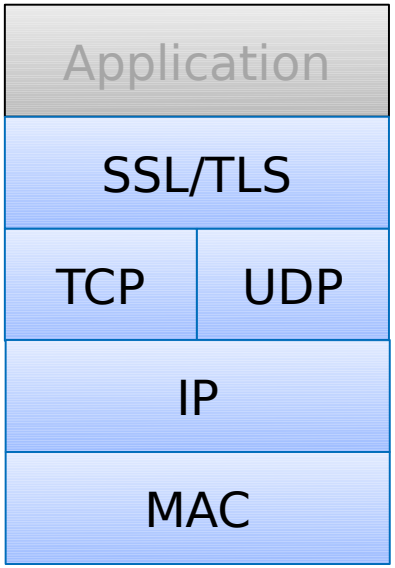


פרוטוקול אבטחה ברמת Application



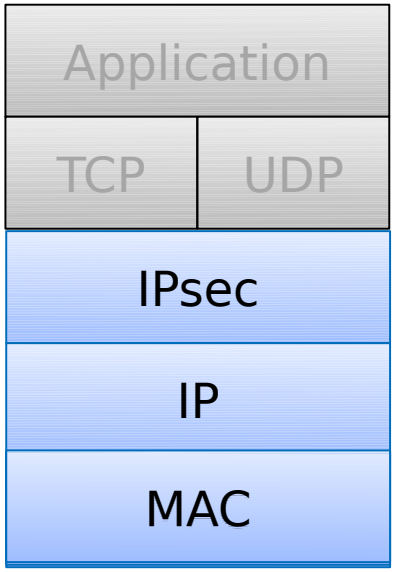
- ניתן לספק סודיות, שלמות, אי-הכחשה, הגנה נגד שידור חוזר ואימות השולח (ברמת האפליקציה)
- איננו פוגע בניתוב
- מסופק end to end
- איננו משבש בדיקות של firewalls
- איננו מגן כנגד התקפות כדוגמת Syn attack
- מחייב שינוי/עדכון האפליקציה
- דוגמאות: PGP, SSH

פרוטוקול אבטחה ברמת Transport



- ניתן לספק סודיות, שלמות, הגנה נגד שידור חוזר ואימות השולח
- איננו פוגע בניתוב
- ניתן לספק end to end
- איננו משבש בדיקות של firewalls
- איננו מגן כנגד התקפות על שכבות התובלה כדוגמת Syn attack
- שקוף לאפליקציה
- דוגמאות: SSL, TLS

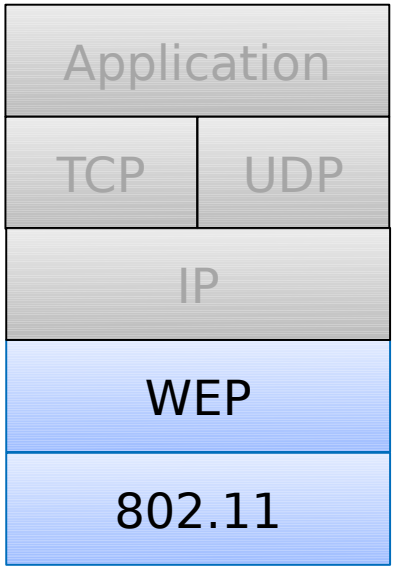
פרוטוקול אבטחה ברמת Network



- ניתן לספק סודיות, שלמות, הגנה נגד שידור חוזר ואימות השולח (ברמת ה-IP)
- איננו פוגע בניתוב
- ניתן לספק end to end או gateway to gateway
- משבש בדיקות של firewalls
- שקוף ל-transport ולאפליקציה
- ניתן להגן נגד התקפות על שכבת התובלה (כגון syn attack)
- דוגמא: IPsec

פרוטוקול אבטחה ברמת MAC

- ניתן לספק סודיות, שלמות ואימות השולח (ברמת ה-MAC)
- תלוי מדיה פיסית
- hop by hop – כלומר בין כל שתי נקודות בניתוב צריך להחליף את שכבות ההגנה
- מגן על החלק הגדול ביותר מה-datagram
- שקוף ל-IP ומעלה (כי כל תחנה שמטפלת מורידה את שכבות ההגנה ברמת ה-MAC)
- דוגמא : WEP



IPsec

IPsec - IP Security Protocol

מסוגל לספק את שירותי האבטחה הבאים:

- סודיות (ע"י שימוש ב-ESP עם הצפנה)
- שלמות
- אימות השולח
- הגנה כנגד שידור חוזר
- בקרת גישה
- מיזעור החשיפה ל-syn attack
- הגנה נגד session hijacking – ע"י הצפנה ו/או אימות
- הגנה כנגד DoS (במקרים מסוימים)

ארכיטקטורת IPsec

- IPsec מכיל את הפרוטוקולים הבאים
  - שני פרוטוקולים לאבטחת תעבורת IP:
  - ESP – מספק הצפנה ו/או אימות
  - AH – מספק אימות בלבד
  - פרוטוקול לניהול והחלפת מפתחות IKE.
- ניתן להשתמש ב-IPsec בשני אופנים:
  - Transport Mode
  - Tunnel Mode

הקמת ערוץ IPsec

- ערוץ IPsec מוקם רק בין מכונות שיש ביניהן אמון הדדי.
- את האמון ניתן ליצור באמצעות החלפת מפתחות ארוכי טווח.
- מפתחות אלה יכולים להיות מפתחות פומביים (יש שימוש ב-PKI שמוגדר ע"י X.509) או מפתחות סימטריים (מעין "סיסמא" משותפת)
- האמון ההדדי בין המכונות מאפשר צמצום החשיפה ל-syn attack וכנגד DoS
- עם זאת, אם מכונה A ומכונה B בעלות אמון הדדי, ותוקף משתלט על מכונה A, הוא יוכל להשתמש בה לצורך תקיפת B

Security Association Database (SAD)

- כל מחשב שמותקן בו IPsec, מחזיק מבנה נתונים שנקרא Security Association Database, או בקיצור SAD
- מבנה נתונים זה מחזיק רשומות שנקראות Security Association (ובקיצור SA)

Security Association

- רשומת Security Association מכילה את כל הנתונים הדרושים לקיום קשר IPsec בין שני מחשבים. היא כוללת בין השאר נתונים לגבי:
  - האלגוריתמים המשמשים להצפנה/אימות
  - המפתחות הקריפטוגרפיים המשמשים להצפנה/אימות
  - אורך חיים של ה-SA
  - מונה מספר סידורי (sequence number)
  - גודל חלון עבור מספרים סידוריים
  - מוד הפעלה (Tunnel/Transport Mode, ESP/AH)
- כל SA מגדיר קשר חד-כיווני. את ה-SA מגדירים בזוגות, אחד לכל כיוון

מבנה ה-SAD

ה-SAD מורכב מ-

- רשומות SA (Security Associations).
- אינדקסים של הרשומות שנקראים SPI (Security Parameter index).
- מכיוון שהתוכן של SA משותף לשתי מכונות (צד שולח וצד מקבל), לכל SA יש שני SPI, אחד במכונה A והשני במכונה B.

מבנה ה-SAD (המשך)

- לכל כיוון של תעבורה בין אליס לבוב מתאים SA אחד
- ה-SAD מחולק לשני חלקים: טבלת SA לתעבורה יוצאת, וטבלת SA לתעבורה נכנסת
- כל אחד משני הצדדים מחזיק עותק של SA זה
- ה-SA מאליס לבוב מכיל את כל המידע הדרוש לאליס על-מנת לשלוח חבילה מאובטחת ואת כל המידע הדרוש לבוב על-מנת לקרוא ולאמת חבילה זו

Security Parameter Index (SPI)

- ה-SPI הוא מספר באורך 32 סיביות שמשמש כמצביע אל העותק של ה-SA אצל הצד המקבל
- מכיוון שאצל המקבל יש מספר SA-ים שונים, ערך ה- SPI של ה-SA לתעבורה מאליס לבוב, מוקצה ע"י בוב (כדי שלא יווצר מצב של שני SA-ים נכנסים עם אותו SPI)
- הגישה אל טבלת ה-SA הנכנסים נעשית לפי ה-SPI
- כאשר אליס שולחת חבילה לבוב, בתוך החבילה רשום ה-SPI של בוב, על מנת שבוב ידע עם איזה SA לפתוח את החבילה
- למטרות יעילות, ניתן לאחסן ב-SA שמתאים לתעבורה מבוב לאליס, מצביע אל ה-SA התואם מאליס לבוב (שנמצא בטבלת ה-SAD היוצאים)

המחשה

Alice

Incoming SAD

SPI	SA
1	
…	
13	Bob to Alice
…	
21	Chris to Alice

Outgoing SAD

SA	SPI
Alice to Bob	17
…	
Alice to Chris	17

Bob

Incoming SAD

SPI	SA
1	
…	
13	Chris to Bob
…	
17	Alice to Bob

Outgoing SAD

SA	SPI
Bob to Alice	13
…	
Bob to Chris	11

Chris

Incoming SAD

SPI	SA
1	
…	
11	Bob to Chris
…	
17	Alice to Chris

Outgoing SAD

SA	SPI
Chris to Alice	21
…	
Chris to Bob	13

דוגמא

דוגמא ל-SA אצל אליס: מאליס לבוב

Protocol = ESP, transport mode,

Encryption Alg.=AES-128, Integrity Alg. = HMAC-SHA256

Life time = 10 Min

SPI = 17

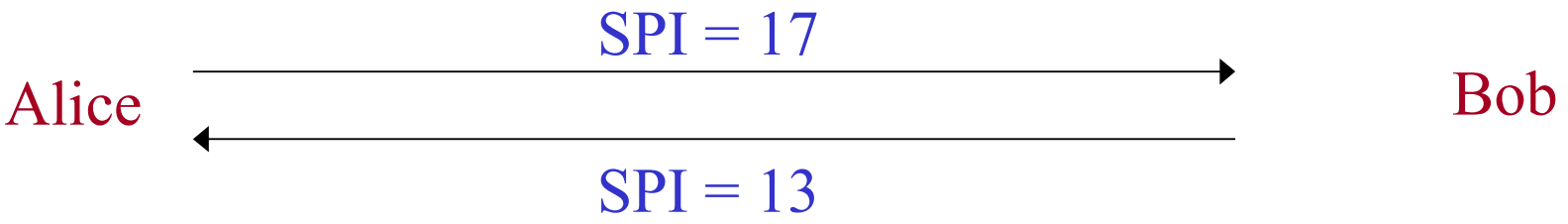
Alice's encryption key =

0xc20c07ab4d2ca5df3027a134d0409416

Alice's integrity key =

0x6cb3df613e590fa095cfa61bebbaf960

Sequence number: 20



בניית וניהול ה-SA

בניית וניהול ה-SA-ים יכולים להיות:

- סטטיים – המפתחות והתכונות האחרות של ה-SA נקבעים מראש (offline) בשני הצדדים (השולח והמקבל), ומוזנים ע"י המשתמש.
- דינמיים – על ידי פרוטוקול לניהול מפתחות בשם IKE (נראה בהמשך).

פרוטוקולים לאבטחת תעבורת IP

ל-IPsec שני תתי פרוטוקולים:

- AH - Authentication header

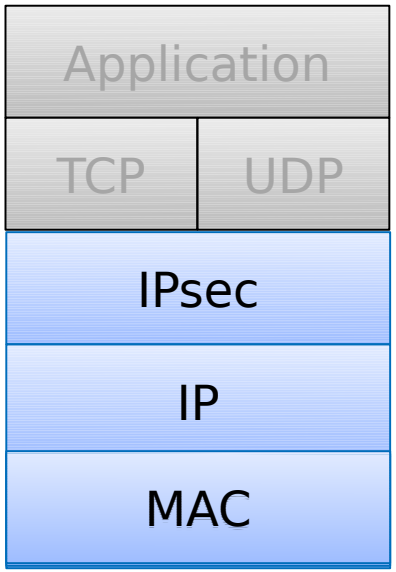
מספק הגנה כנגד שידור חוזר, אימות ושלמות (גם של ה-IP header).

- ESP - Encapsulating Security Payload

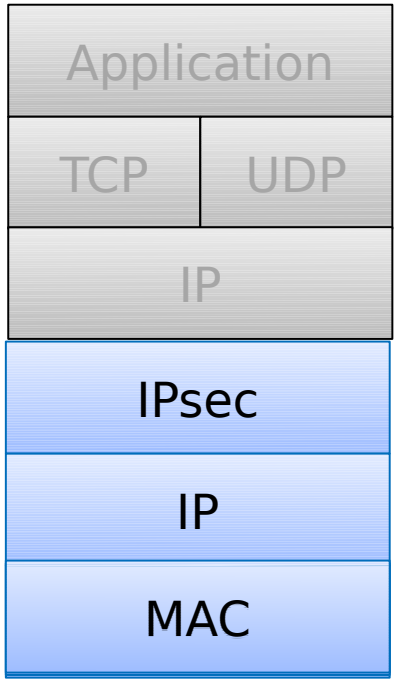
מספק סודיות, אימות, שלמות והגנה כנגד שידור חוזר

מיקום ה-IPsec Header

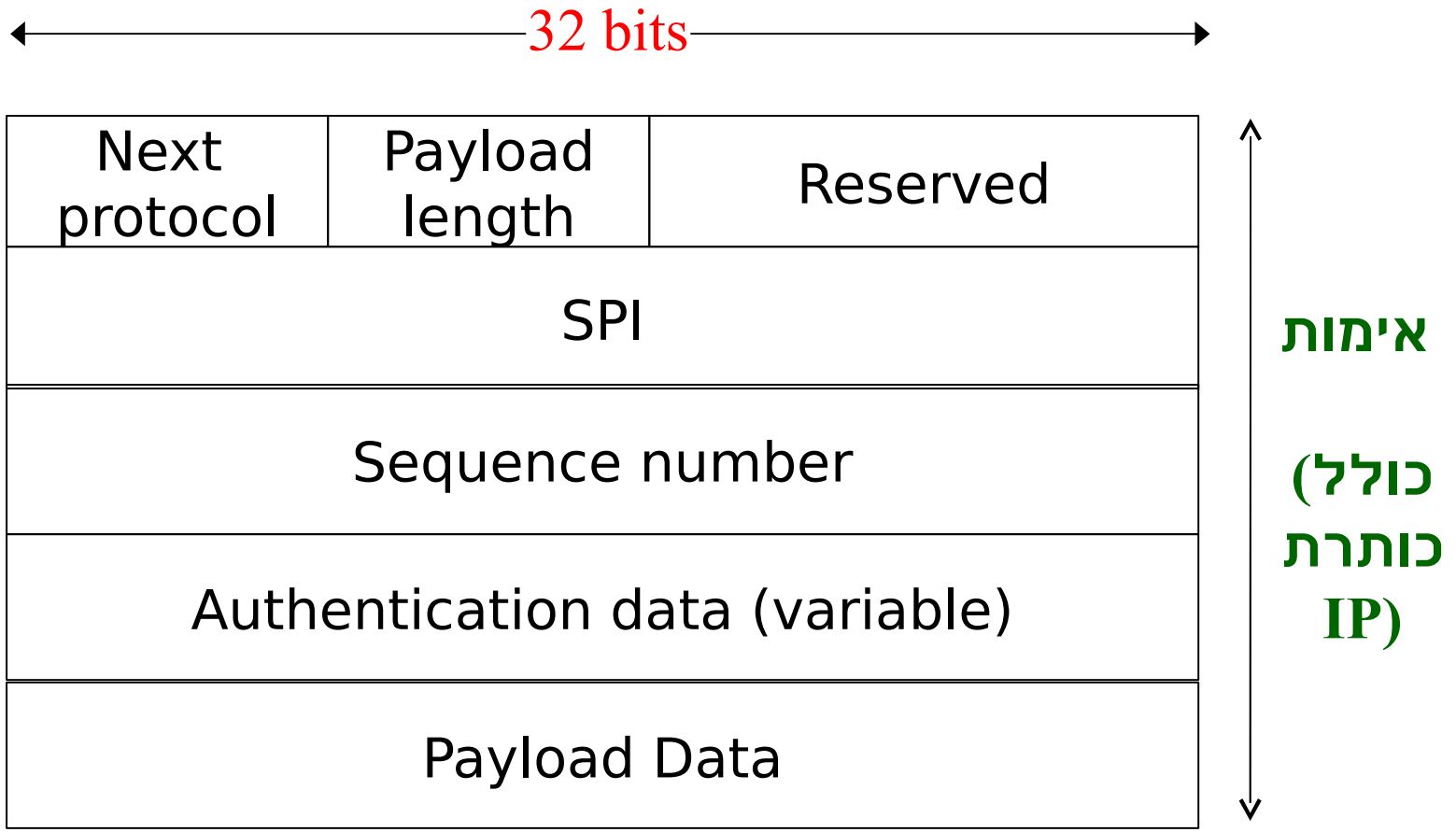
Transport mode



Tunnel mode



AH


32 bits
Next protocol
Payload length
Reserved
SPI
Sequence number
Authentication data (variable)
Payload Data
אימות
(כולל כותרת IP)

כותרי AH

רוב השדות זהים לאלה שב-ESP. עם זאת שדה ה-Authentication Data שונה.

Authentication data – ה-MAC מחושב על שרשור של ה-IP header החיצוני, ה-AH header וה-data payload.
השדות ב-IP header החיצוני שמשתנים בכל hop (דוגמת ה-TTL) מאופסים לשם חישוב ה-MAC. כמו כן מאופס השדה שיכיל את ה-MAC.

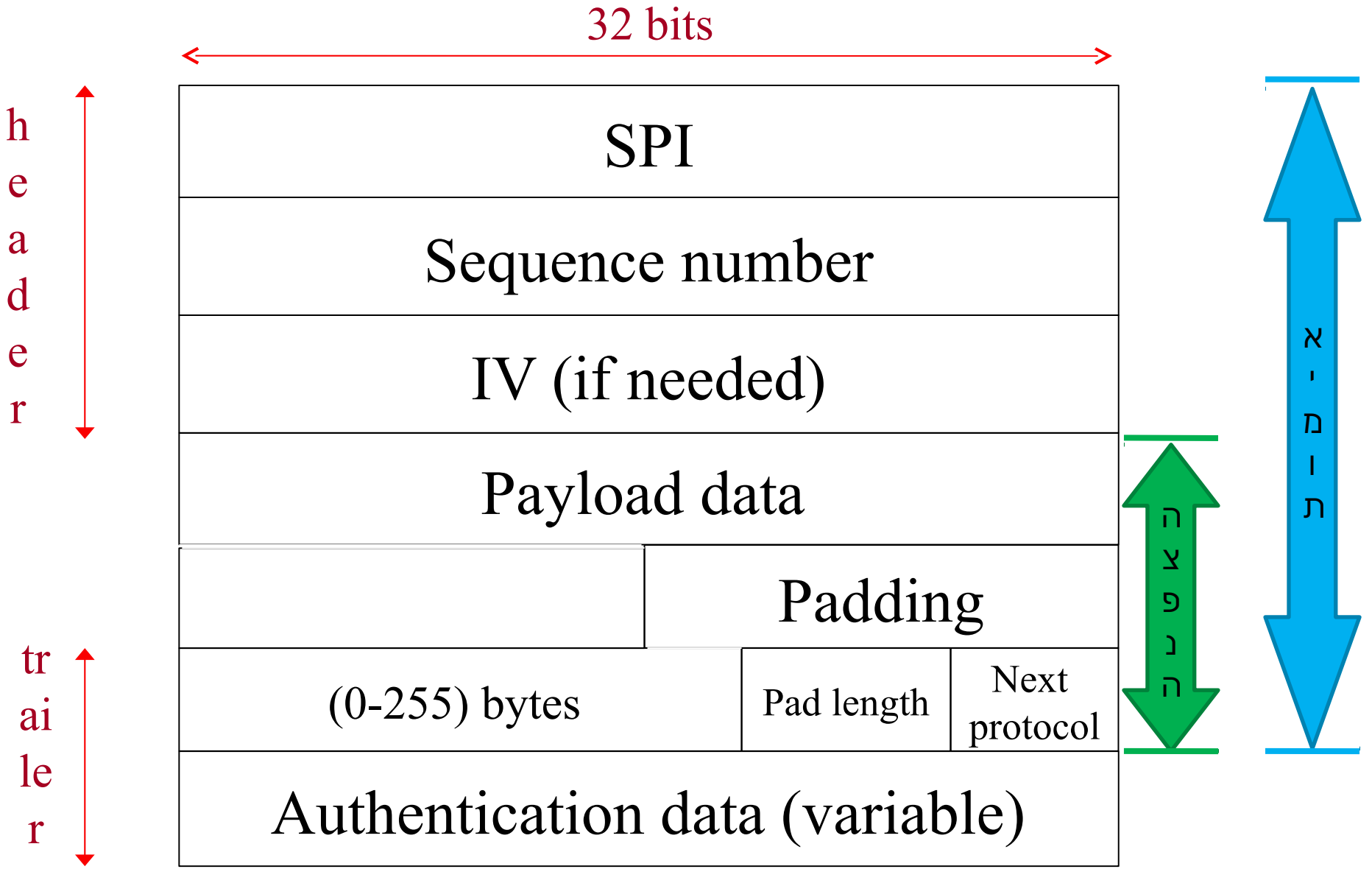
תהליך עיטוף (Encapsulation) המידע

- מציאת ה-SA (פירוט בהמשך)
- שלוף את ה-SPI של הצד השני
- שלוף את ה-Sequence number, והגדל באחד
- בניית ה-AH header
- בניה (מוקדמת) של ה-IP header
- חישוב ה-MAC (תוך איפוס זמני של חלק מהשדות, כפי שתואר בשקף הקודם)

תהליך פתיחת (Decapsulation) המידע

- מציאת ה-SA (ע"ס ה-SPI) ובדיקה ש-SA זה משותף עם השולח ויכול לשמש לצורך הנוכחי.
- בדיקת ה-Sequence number.
- חישוב ובדיקת ה-MAC תוך אפוס זמני של חלק מהשדות.
- אם בדיקה כלשהי נכשלת - זרוק את החבילה.
- אחרת, הגדל את ה-Sequence number ב-SA באחד.
- המשך עיבוד על פי ה-Next protocol.

ESP


32 bits
header
trailer
SPI
Sequence number
IV (if needed)
Payload data
Padding
(0-255) bytes
Pad length
Next protocol
Authentication data (variable)
הצפנה
אי-מות

כותרי ESP

- SPI – מצביע ל-SA אצל המקבל - 32 סיביות
- Sequence number – מונה שמשמש להגנה מפני שידור חוזר - 32 סיביות
- Initialization vector - IV – במידה ואלגוריתם ההצפנה דורש זאת (באורך הנדרש ע"י אלגוריתם ההצפנה)
- Payload data – המידע שעליו מגן ה-SA (באורך משתנה)
- Padding – במידה ודרוש, אם ה-SA מצפין בעזרת צופן בלוקים
- Pad length – אורך ה-padding, מופיע תמיד (גם אם אין צורך) - 8 סיביות

כותרי ESP (המשך)

- מספר הפרוטוקול הבא (שדה ה-Next protocol) באורך 8 סיביות מציין האם החבילה המוגנת היא IP,TCP, או UDP.
- Authentication data – תוצאת MAC על המידע (datagram) ועל ה-ESP headers (כלומר, על כל החבילה מלבד שדה ה-authentication data עצמו) – אורך השדה תלוי באלגוריתם ה-MAC שבשימוש

(כותרת ה-IP אינה מוגנת על ידי ESP)

תהליך עיטוף (Encapsulation) המידע

- מציאת ה-SA (פירוט בהמשך)
- שלוף את ה-SPI של הצד השני
- שלוף את ה-Sequence number, והגדל באחד
- לצורך ההצפנה:
  - קביעת ה-IV (אם נדרש)
  - דיפון המידע (אם נדרש)
- שרשור ה-Pad length וה-Next protocol number
- הצפנה באלגוריתם שנקבע ב-SA (אם הצופן אינו null cipher)
- חישוב האימות (על הכל, פרט לערך האימות [ולכותרת ה-IP שטרם נוצרה]; האלגוריתם נקבע ב-SA)

תהליך פתיחת המידע (Decapsulation)

- מציאת ה-SA (ע"ס ה-SPI) ובדיקה ש-SA זה משותף עם השולח
- בדיקת ה-Sequence number
- בדיקת ה-MAC
- אם בדיקה כלשהי נכשלת - זרוק את החבילה
- פענוח
- בדוק ש-SA זה יכול לשמש לצורך הנוכחי, וזרוק החבילה אם לא (בדיקה זו אינה יכולה להעשות לפני הפענוח)
- המשך עיבוד על פי ה-Next protocol

מבני הנתונים של IPsec

IPsec משתמש בשני מבני נתונים:

- Security Association Data – SAD : מכיל את האלגוריתמים ומפתחות סימטריים שבאמצעותם תאובטח התעבורה של שירות מסוים
- Security Policy Data – SPD : מאפשר למשתמש לבחור את שירותי האבטחה שינתנו לשירות מסוים, ואת האלגוריתמים הקריפטוגרפים שבאמצעותם ימומשו שירותי האבטחה. ה-SPD מוזן ע"י המשתמש, ומייצג את חשיבות האבטחה לכל חיבור אפשרי

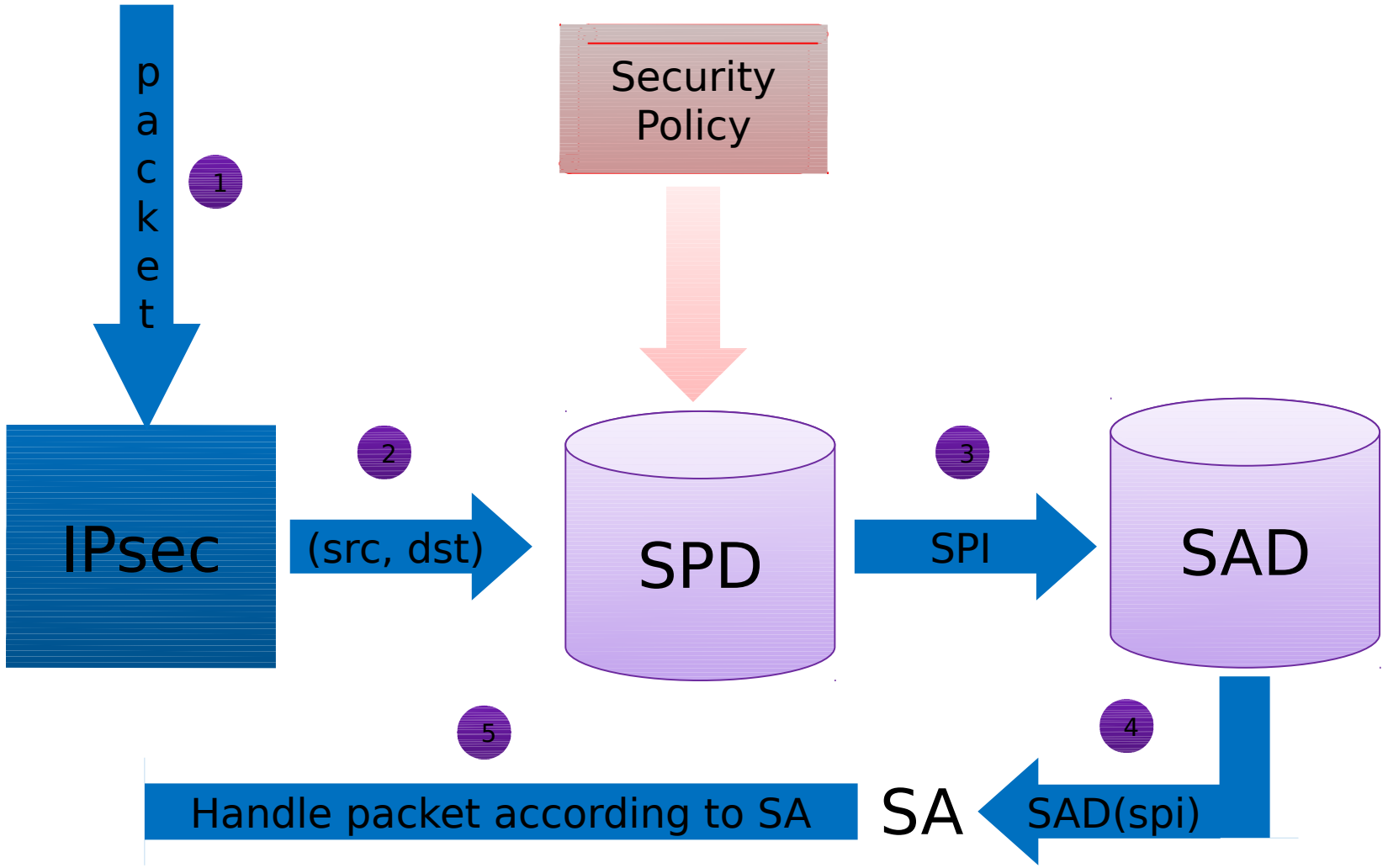
Security Policy Data (SPD)

ה-(Security Policy Data) SPD הינה רשימה של חוקים (דומים לחוקי Firewalls) שמוזנים על ידי המשתמש. כל חוק מורכב מ-selectors ומפעולה.

ה-Selectors – יכולים להיות כתובות IP, טווחים של כתובות IP, מספרי פורטים TCP/UDP ועוד

הפעולה יכולה להיות: זרוק את החבילה, שלח חבילה רגילה, שלח חבילה מוגנת ב-SA נתון, או יצר SA ושלח חבילה מוגנת. במקרה האחרון, הפעולה מפנה לתכונות (אלגוריתמים קריפטוגרפיים) שיש להשתמש בהן ב-SA.

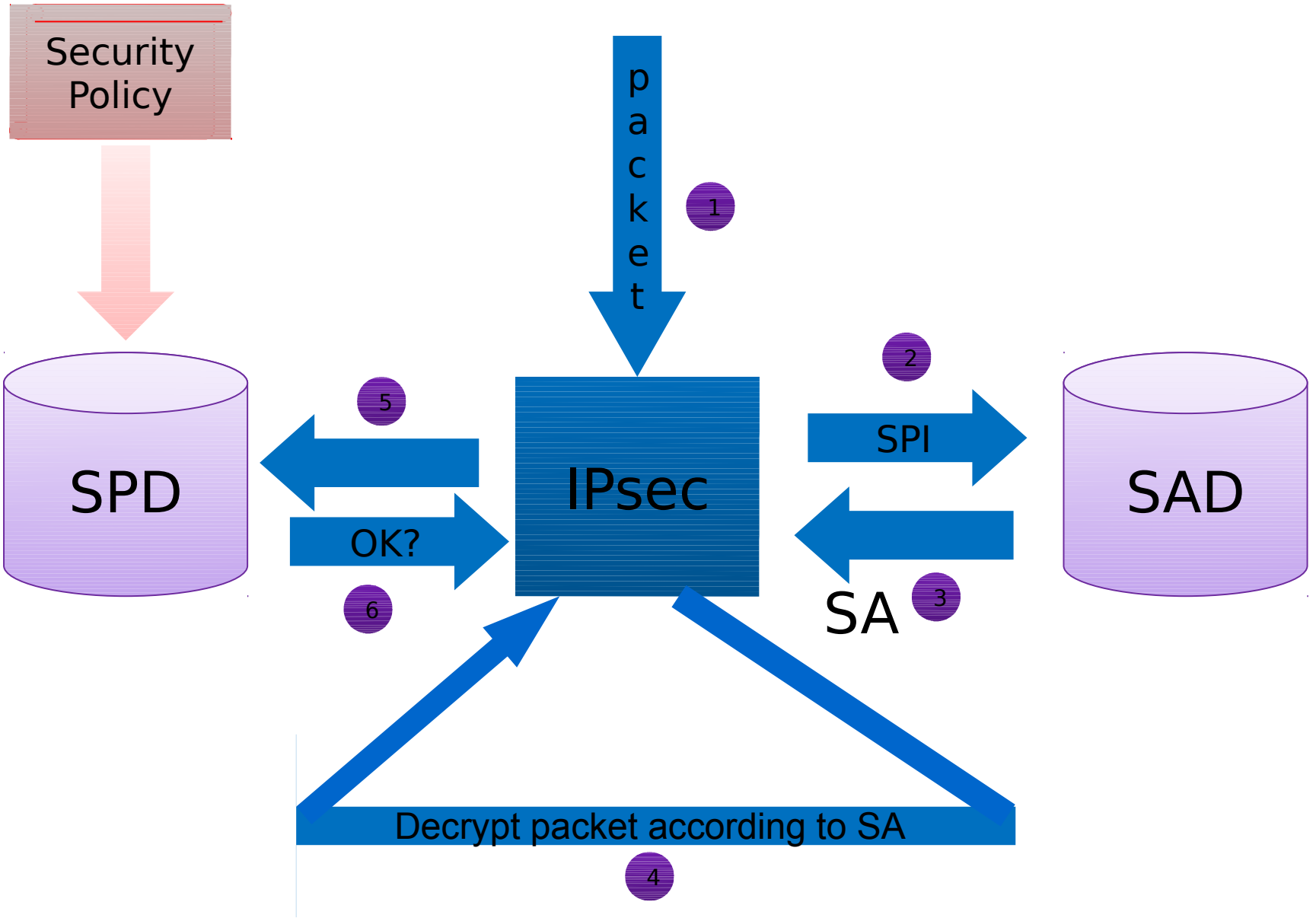
ביצוע עיבוד IPsec (ביציאה)



עיבוד החבילה ביציאה

- ניגשים עם החבילה ל-SPD
- אם תשובת ה-SPD: זרוק או שלח חבילה רגילה, יש לזרוק את החבילה או להעביר לשכבה הבאה בהתאמה
- אם תשובת ה-SPD: צור SA ושלח חבילה מוגנת – מפעילים את IKE לשם בניית ה-SA בהתאם לכללים שה-SPD החזיר
- אם התשובה שלח חבילה מוגנת ב-SA נתון – מבצעים עיבוד החבילה בהתאם

ביצוע עיבוד IPsec (בכניסה)



עיבוד החבילה בכניסה

- ניגשים ל-SAD עם האינדקס SPI שבחבילה ומאמתים/מפענחים את החבילה. אם אין SA מתאים, זורקים את החבילה
- ניגשים עם החבילה וה-SPI ל-SPD. ה-SPD בודק התאמה ביניהם. אם אין התאמה, זורקים את החבילה
- מעלים את החבילה לשכבה הבאה

שימו לב לסעיף השני: חייבים לבדוק התאמה, אך יש לתת חופש לשולח להחליף מפתחות. לכן לא נותנים ל-SPD לנחש איזה SPI צריך לקבל, אלא נותנים לו את ה-SPI לבדיקה.

אופני התפעול של IPsec

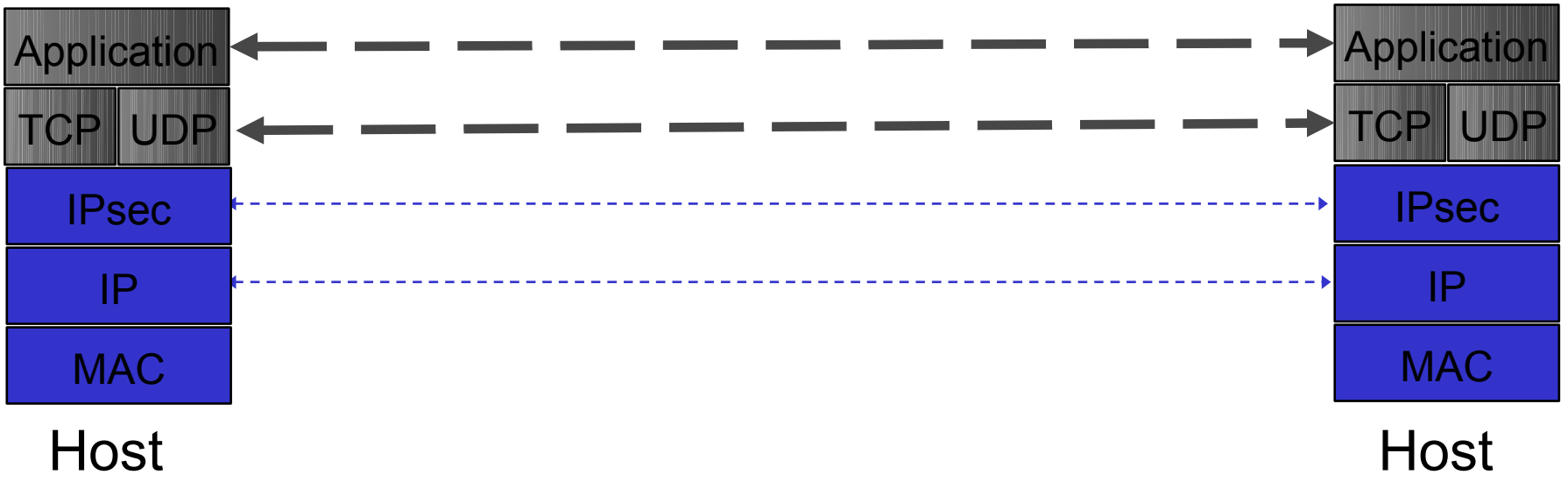
ניתן להשתמש ב-IPsec באחד משני אופני תפעול אפשריים:

- Transport mode – שני מחשבי הקצה מתקשרים ביניהם באמצעות IPsec באופן ישיר. כלומר, בין אליס ובוב מוקם ערוץ IPsec
- Tunnel mode – השימוש ב-IPsec לא בהכרח נעשה ע"י מחשבי הקצה. בצורה זו, בין אליס לבוב קיים קשר IP רגיל, וה-IPsec מולבש עליו באופן שיתואר בהמשך

IPsec Transport Mode

מספק שירותי אבטחה מקצה לקצה (end to end).

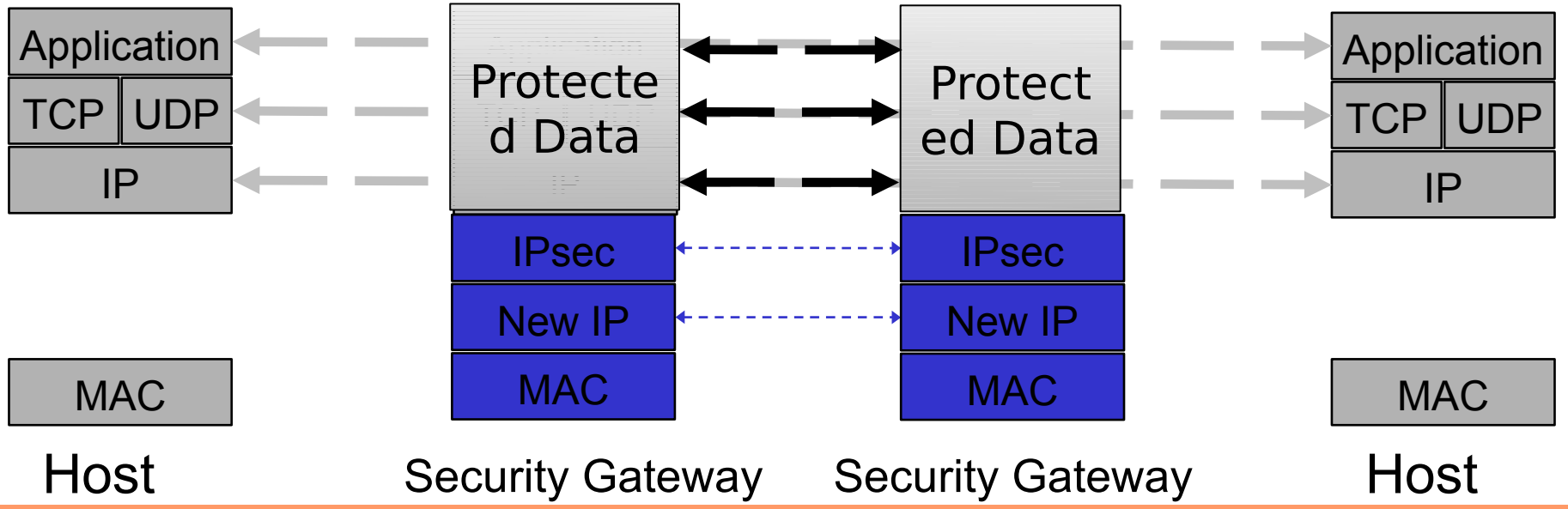
לכן, מחייב את שני הקצוות להפעיל את IPsec בעצמם (כלומר, ה-TCP/IP stack בשני הקצוות צריכה לטפל ב-IPsec).



IPsec Tunnel Mode

מופעל ע"י Security gateways, ולאו דווקא ע"י משתמשי הקצה. כלומר, ניתן למימוש באופן שקוף למשתמשי הקצה.

תכונה נוספת של מוד זה, היא הסתרת כתובות ה-IP האמיתיות של מערכות הקצה, בזמן מעבר החבילה ברשת.



אופני התפעול של IPsec – הערות

- יתכן שעל אותה חבילה, בזמן הניתוב, מפעילים קודם את IPsec ב-transport mode במחשב הקצה, ולאחר מכן מספר פעמים IPsec ב-tunnel mode ב-Security gateways שבדרך.
- בדרך כלל מחשבי הקצה (hosts) מסוגלים להפעיל IPsec בשני האופנים. ה-Security gateways נדרשים לממש רק tunnel mode.

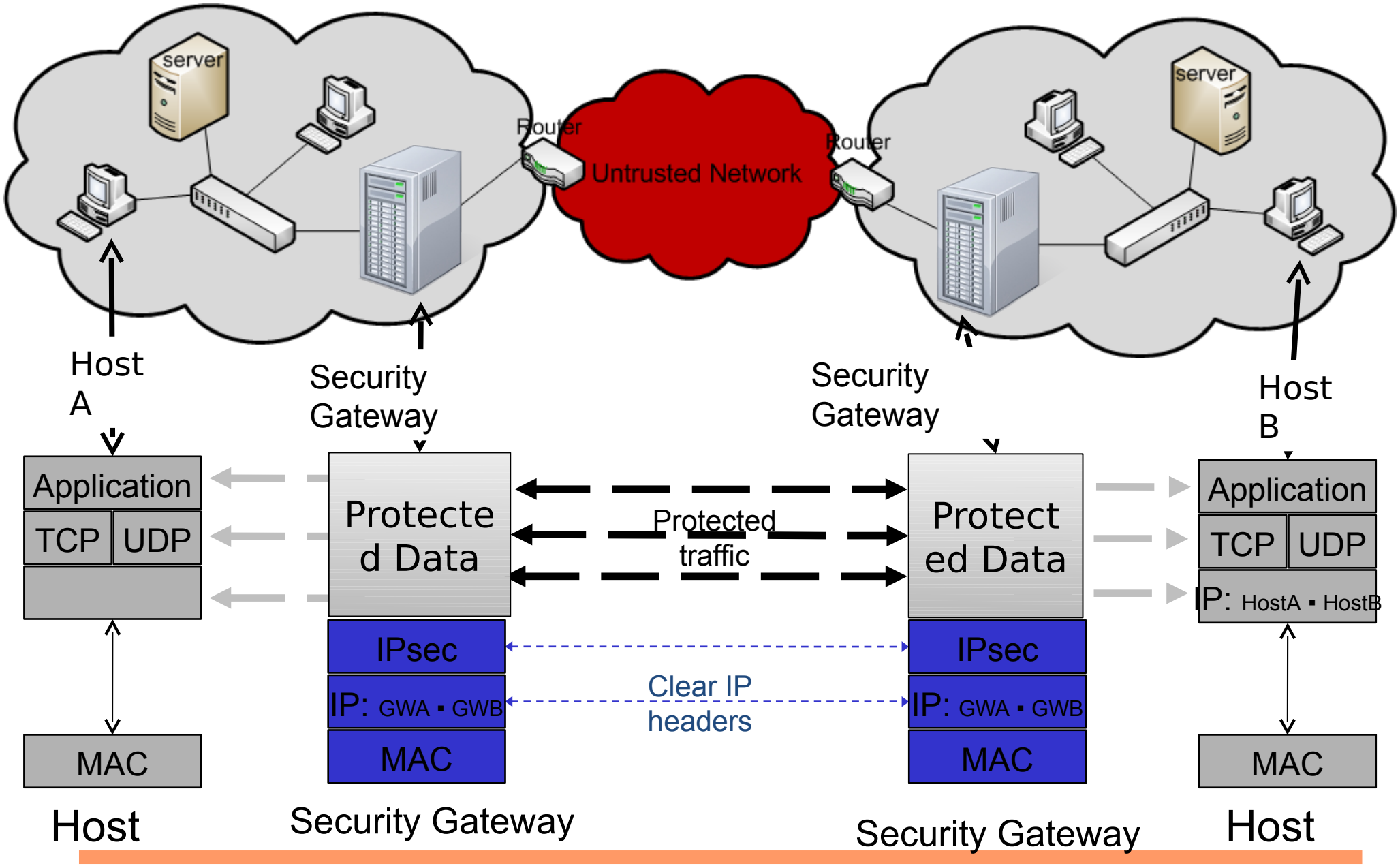
Virtual Private Network (VPN)

רשת פרטית וירטואלית (VPN) היא רשת הנבנית מעל רשת ציבורית (לדוגמא האינטרנט) באופן המשמר את פרטיות משתמשי ה-VPN.

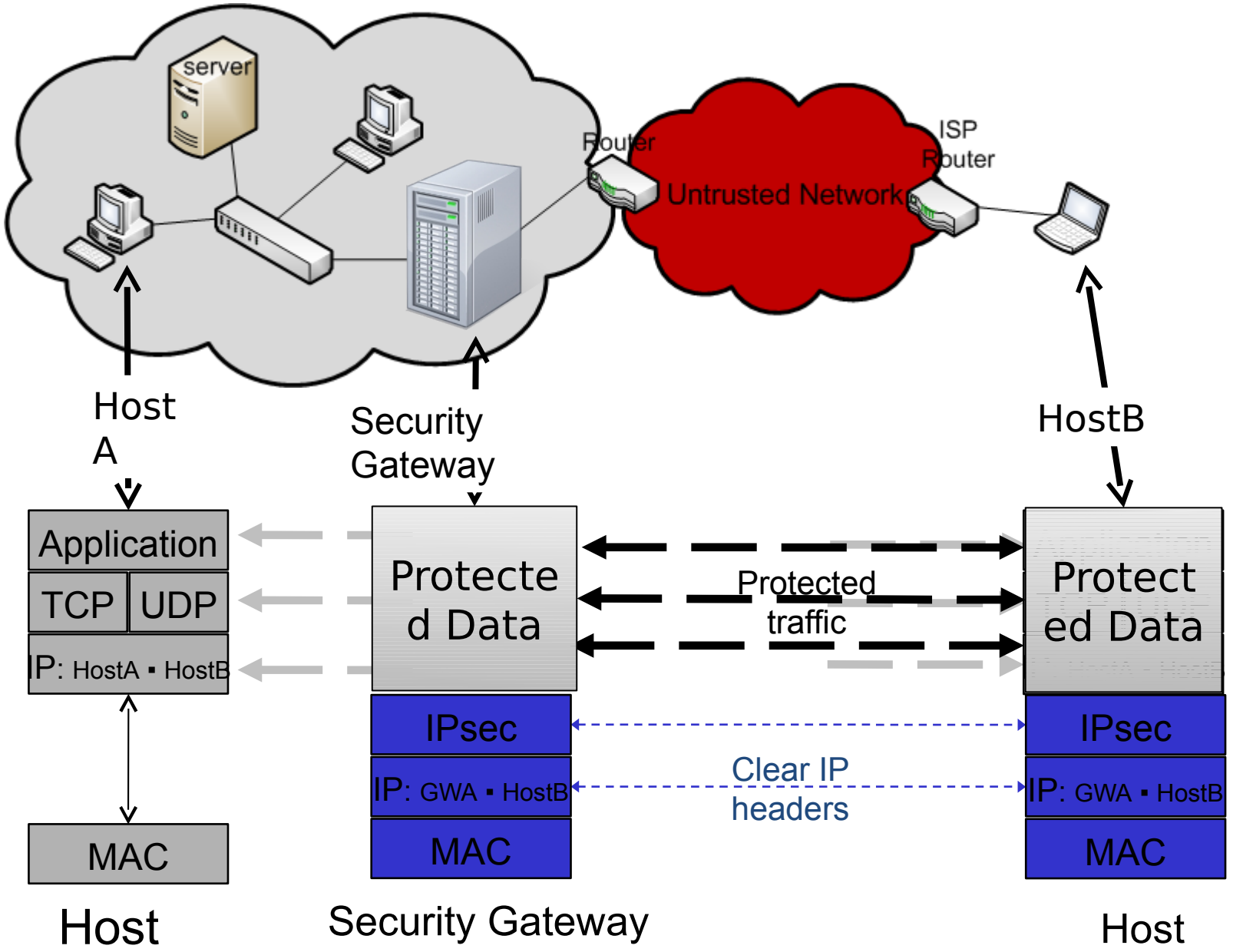
הרעיון הוא שרק המשתמשים המורשים של ה-VPN מסוגלים לדבר אחד עם השני, ורק הם מסוגלים לשלוח ולקבל הודעות ב-VPN (תארו לעצמכם רשת LAN פרטית שאיננה מחוברת לאינטרנט).

כלומר זוהי רשת פרטית, שממומשת מעל רשת ציבורית (ומכאן החלק הוירטואלי בשמה).

Secure VPN Implementation



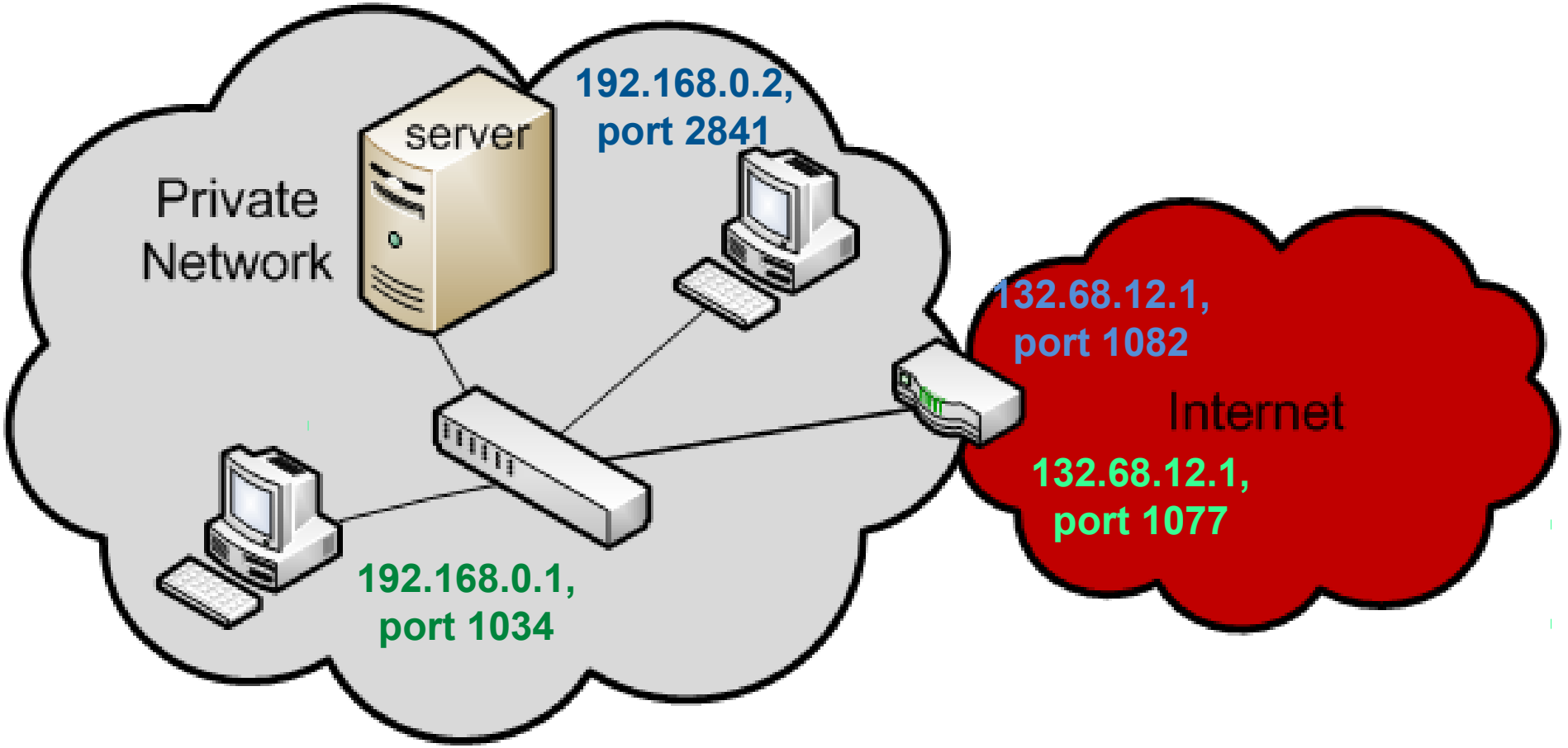
מהבית VPN


server
Router
Untrusted Network
ISP
Router
Host
A
Security
Gateway
HostB
Application
TCP
UDP
IP: HostA ▪ HostB
MAC
Protecte
d Data
IPsec
IP: GWA ▪ HostB
MAC
Protected
traffic
Clear IP
headers
Protect
ed Data
IPsec
IP: GWA ▪ HostB
MAC
Host
Security Gateway
Host

על הקשר בין IPsec ו-NAT

- Network Address Translation (NAT) – פרוטוקול שמאפשר לרשת גדולה לעבוד עם מספר קטן של כתובות IP
- בתוך הרשת יעשה שימוש בכתובות IP "לא חוקיות"
- כאשר מחשב מהרשת הקטנה יוצר קשר עם האינטרנט, ה-gateway מתרגם את כתובתו לכתובת IP חוקית. כמובן, שעל ה-gateway לבצע את תרגום הכתובות גם בכניסה
- לא ניתן להשתמש ב-AH ב-transport mode יחד עם NAT.
- NAT גורם לבעיות רבות נוספות בהקשר של IPsec. זוהי רק דוגמא אחת לבעיות אלו

על הקשר בין IPsec ו-NAT (דוגמא)



סיכום

- פרוטוקול IPsec מספק שירותי אבטחה בשכבת ה-IP. הוא מאפשר למערכת לבחור בפרוטוקולים, ובאלגוריתמים שבעזרתם יאובטח שירות (Service) מסוים, ולנהל את המפתחות הקריפטוגרפיים הדרושים (באמצעות IKE)
- ניתן להשתמש ב-IPsec בכדי לאבטח מסלול (או מספר מסלולים) בין זוג hosts, בין host ובין security gateway, או בין זוג security gateways
- IPsec משתמש בקריפטוגרפיה סימטרית לאבטחת תעבורת IP, והוא מסתמך על מנגנונים חיצוניים שיספקו לו את המפתחות הסימטרים. מנגנונים אילו יכולים להיות ידניים, או אוטמטיים

סיכום (המשך)

פרוטוקול IPsec מספק את שירותי האבטחה הבאים:

- סודיות – ב-ESP תוך שימוש בהצפנה
- שלמות – באמצעות ה-MAC
- אימות השולח – באמצעות ה-MAC
- הגנה כנגד שידור חוזר – באמצעות ה-sequence number
- בקרת גישה – באמצעות דרישת ידיעת ה-SA המתאים לצורך תקשורת
- מיזעור החשיפה ל-syn attack –מכיוון שתוקף אינו יכול לבצע IP spoofing (ודרישת ידיעת ה-SA המתאים)
- הגנה נגד session hijacking – ע"י הצפנה ו/או אימות
- הגנה כנגד DoS – מניעת IP spoofing (ודרישת ידיעת ה-SA המתאים)