University of M’sila
Faculty of Mathematics and Computer Science
Department of Computer Science

Virtual Private Network
VPN

Academic Year 2025-2026

Prepared and presented by SAOUDI Lalia

What’s a VPN

- **Definition**: A Virtual Private Network (VPN) creates a secure, encrypted connection over a public network (typically the internet).
- **Analogy**: Think of a VPN as a secure, private tunnel through a public highway.

Why Use VPNs?

- Core Purposes:
- **Security**: Protect data from eavesdropping
- **Privacy**: Hide your IP address and location
- **Access**: Bypass geographical restrictions
- **Anonymity**: Mask online activities

Threat Scenarios :

- Threat Scenarios :
- 1. Public WiFi at coffee shop
- 2. ISP tracking and selling browsing data
- 3. Working from home
- 4. Corporate espionage on business trips
- 5. Location tracking possible

Questions to Answer:

- What PII (Personally Identifiable Information) does a VPN hide?
- How do VPNs prevent tracking by advertisers?
- Can VPNs provide complete anonymity? Why/why not?

PII a VPN DOES Hide/Protect:

- **Your IP Address:** Your IP address can reveal your approximate geographical location (city/region)). With a VPN, websites and online services see the IP address of the VPN server, not yours.
- Y**our Internet Traffic from Local Eavesdroppers:** The encryption protects the content of your data (what you're doing) from:
  - Your ISP: They cannot see which specific websites you visit, what you search for, or what you download—only that you're connected to a VPN server.
  - Anyone on your local network (like public Wi-Fi at a café or airport): They cannot intercept your login credentials, messages, or any unencrypted data.
  - Local network administrators.
- **Your Browsing Activity from Your ISP:** Tied to the above, your ISP's view of your activity is obscured. They see encrypted traffic to a single point (the VPN server), not the myriad of destinations you visit.

PII a VPN DOES NOT Hide/Protect:

- **Information You Voluntarily Provide:** If you log into Facebook, Google, Amazon, or any online account, that service knows exactly who you are and can track your activity within their platform (searches, purchases, likes), regardless of your VPN.
- **Device Fingerprinting:** Websites can collect detailed information about your device (browser type, version, screen resolution, fonts, plugins, etc.).
- **Cookies and Tracking Scripts:** VPNs do not block cookies. Advertisers and websites can still track your activity across their sites using cookies and other tracking technologies. To combat this, you need browser tools
- **II from Endpoint Threats:** A VPN does not protect you from malware, keyloggers, or phishing attacks.

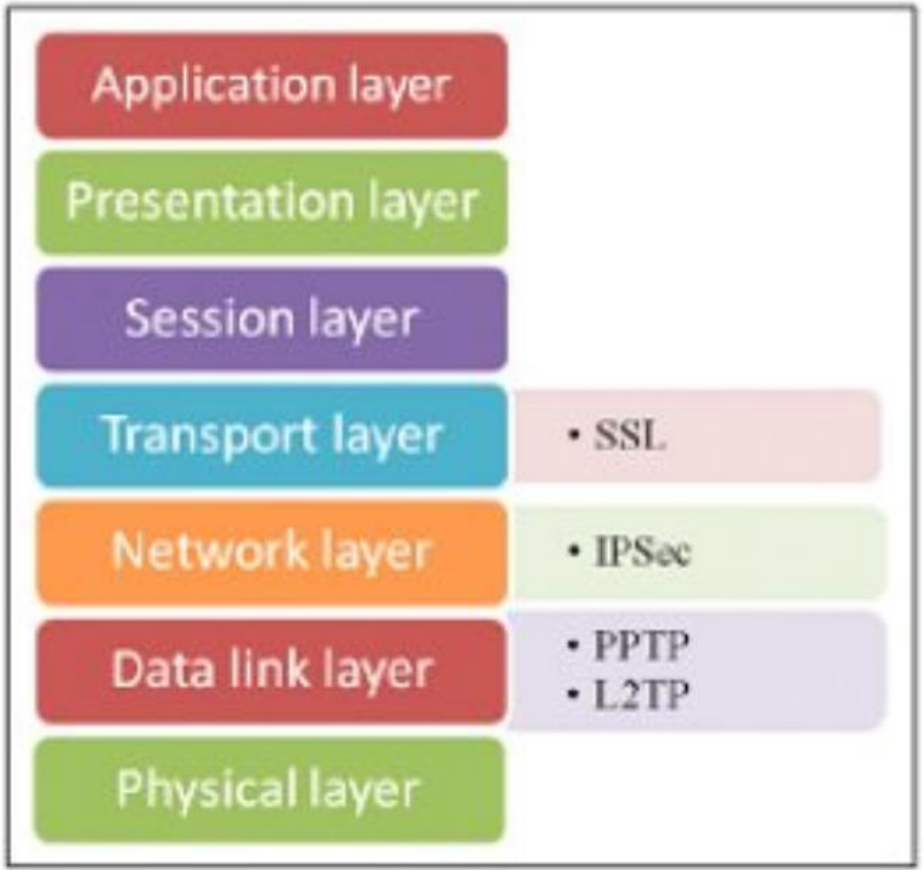
VPN Classification Overview

- **1. BY USAGE:**
  - Site-to-Site VPN (S2S VPN)
  - Client to site VPN
  - Mobile VPN
  - Clientless VPN
- **2. BY PROTOCOL & TECHNOLOGY**
  - IPsec VPN (Internet Protocol Security)
  - RGE VPN
  - PPTP (Point-to-Point Tunneling Protocol):

3.BY TOPOLOGY & ARCHITECTURE; Point 2Point , full mesh , partial mesh

- **4. BY DEPLOYMENT MODEL:** cloud VPN, managed VPN

At what level to deploy a VPN?

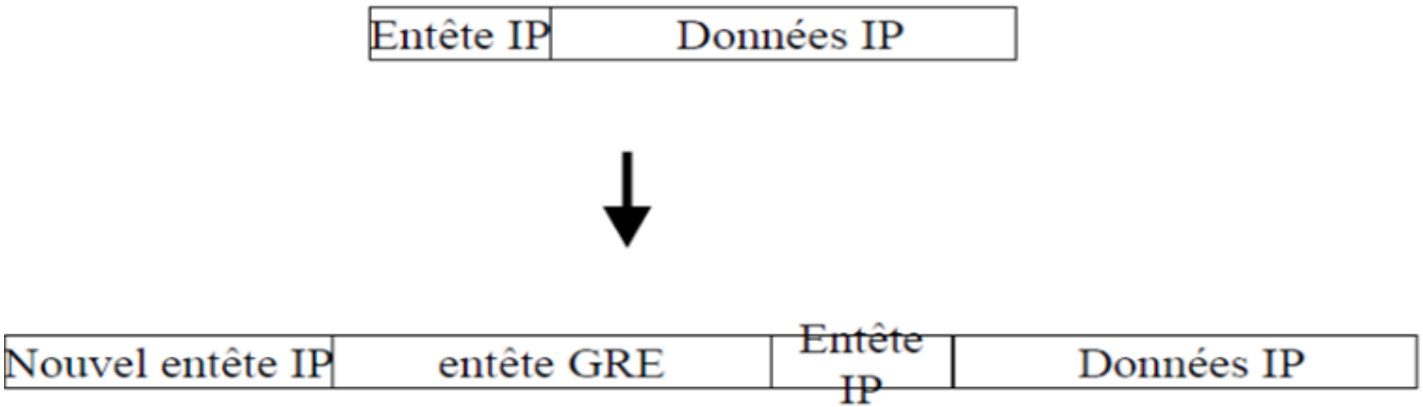


Physical Level

- Encrypting box: encrypts all IP packets that pass through.

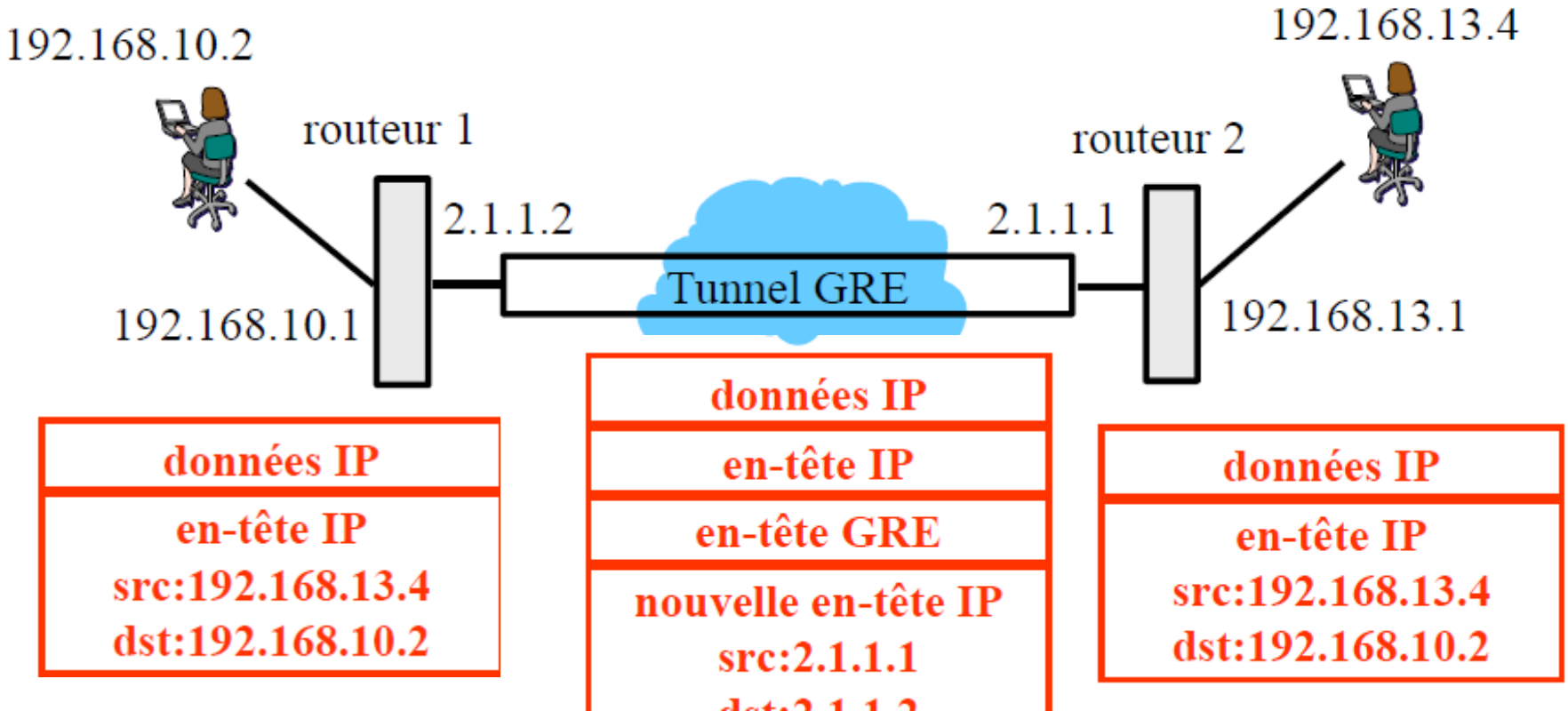
• GRE Generic Routing Encapsulation

- Purpose: Creates tunnels to encapsulate various network protocols
-



• GRE Generic Routing Encapsulation

- Purpose: Creates tunnels to encapsulate various network protocols



• GRE Generic Routing Encapsulation

Pros:
Supports multiple protocols (IP, IPX, AppleTalk)
Supports multicast traffic
Simple configuration
Low overhead
Cons:
No built-in encryption
Vulnerable to attacks
Limited error checking

• IP sec protocol

- IPsec = Internet Protocol Security
- is a standard that defines a security extension for the internet protocol (IP):
  - Packet listening
  - Address spoofing
- to enable the securing of networks based on this protocol.
  - Confidentiality:, Authentication:, Integrity, Protection against replay
- The security is implemented at the IP level,
- IPsec can be deployed on all network devices and provide a unique means of

• IP sec architecture

Security protocols:

- Authentication Header (AH) : authentification only
- Encapsulation Security Payload (ESP) : encryption+authentification

Key exchange protocol:

- Internet Key Exchange (IKE)

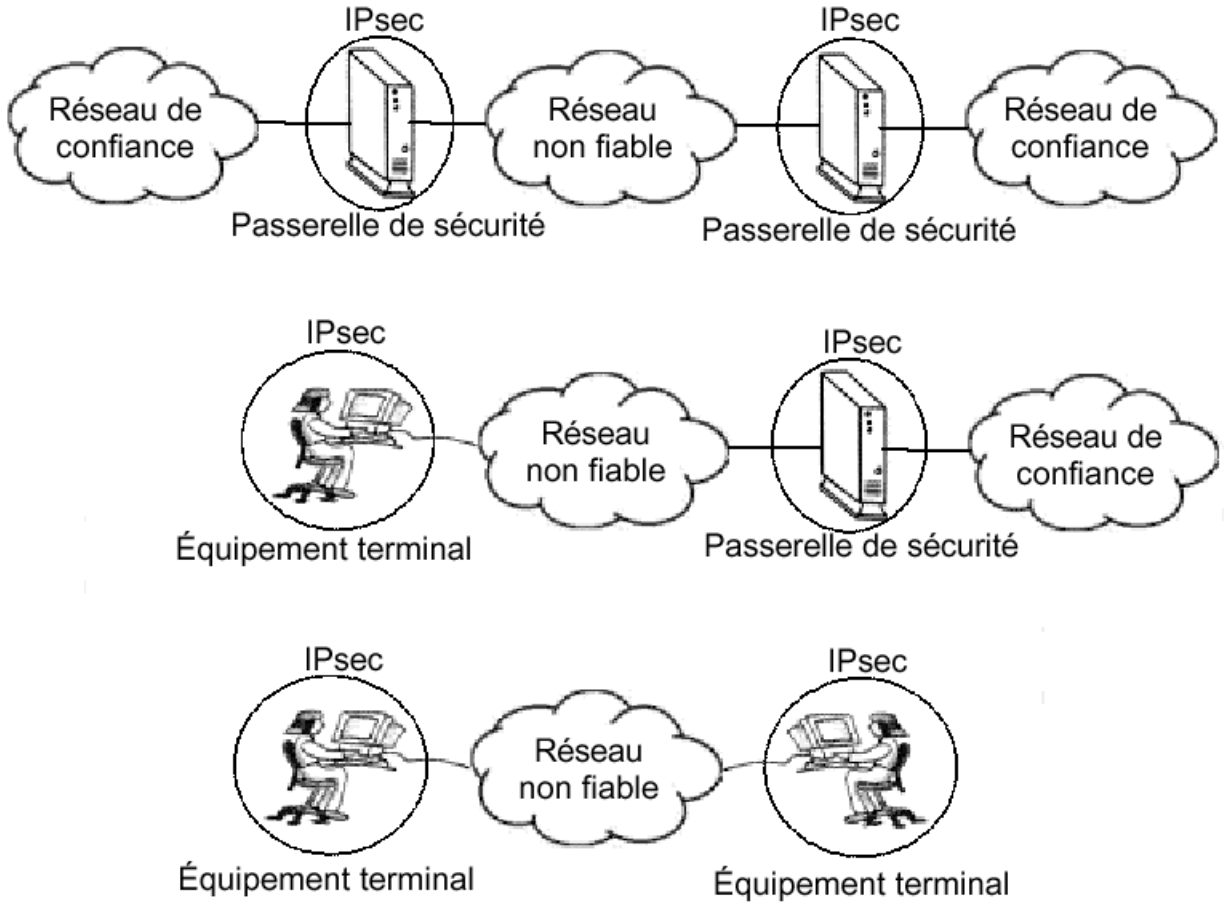
Encryption Algorithms • AES (128/256) • 3DES • DES

Authentication Methods: Pre-shared Keys,RSA,ECDSA

Internal databases:

- Security Policy Database (SPD)
- Security Association Database (SAD)

Where does IPsec come into play?



Advantage

- Ability to use it only on specific communications (without disrupting other communications).
- IPSec is below the transport layer (TCP, UDP); it is therefore transparent to applications (allowing for increased security without modifying higher-level applications).
- Once established, IPSec is transparent to users.

How are these services provided?

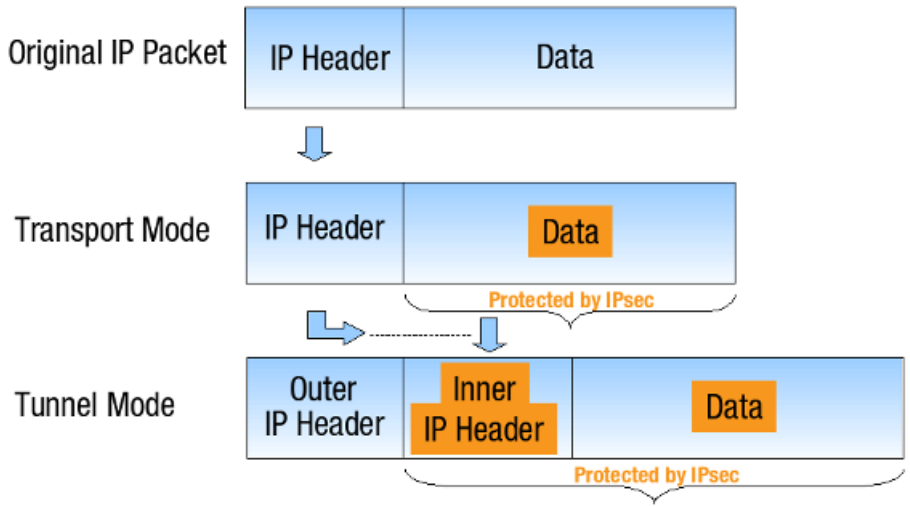
- Security services are provided through two extensions of the IP protocol:
  - AH (Authentication Header)
    - is used to validate the integrity of messages and to prove the identity of the sender, as well as to prevent replay attacks.
  - ESP (Encapsulating Security Payload):
    - *has the primary role of ensuring confidentiality but can also ensure data authenticity.*

IPSEC modes

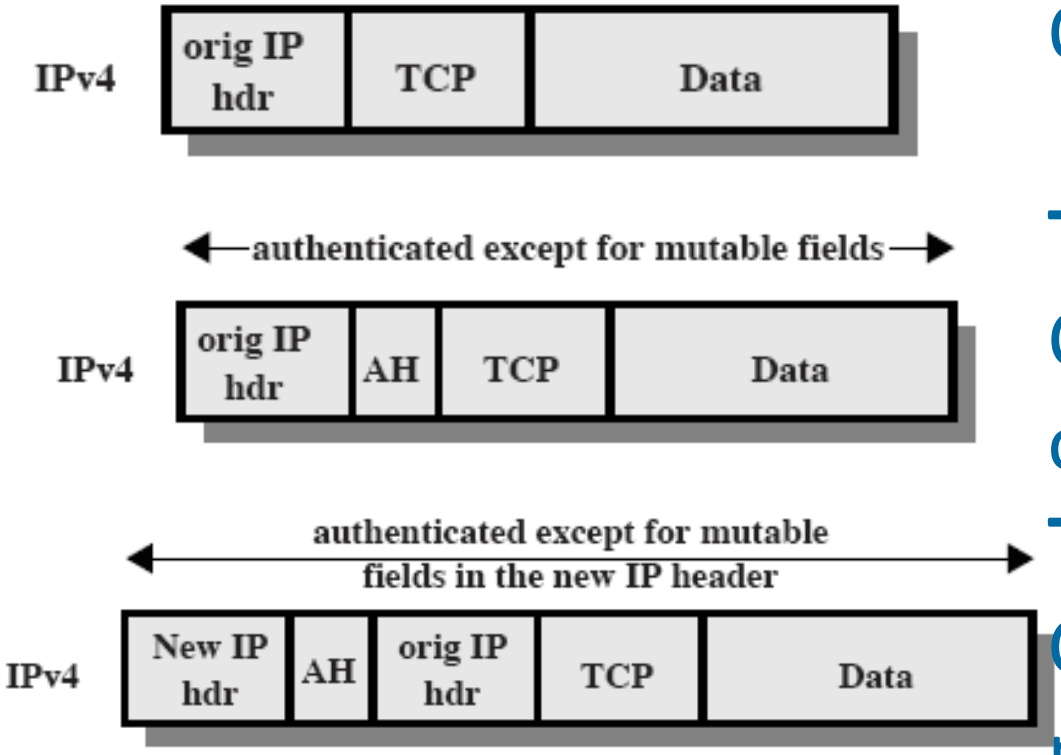
- **The transport mode:** protects only the content of the IP packet without touching the header; this mode can only be used on end devices (client machines, servers). AH, ESP, or both.
- 

- **The tunnel mode**: allows the creation of tunnels by 'encapsulating' each IP packet in a new packet. Thus, the protection covers all fields of the incoming IP packets at the entrance of a tunnel, including the fields of the headers (source and destination addresses).
- 

IPSEC modes


Original IP Packet
IP Header
Data
Transport Mode
IP Header
Data
Protected by IPsec
Tunnel Mode
Outer IP Header
Inner IP Header
Data
Protected by IPsec

AH: Tunnel and Transport Mode

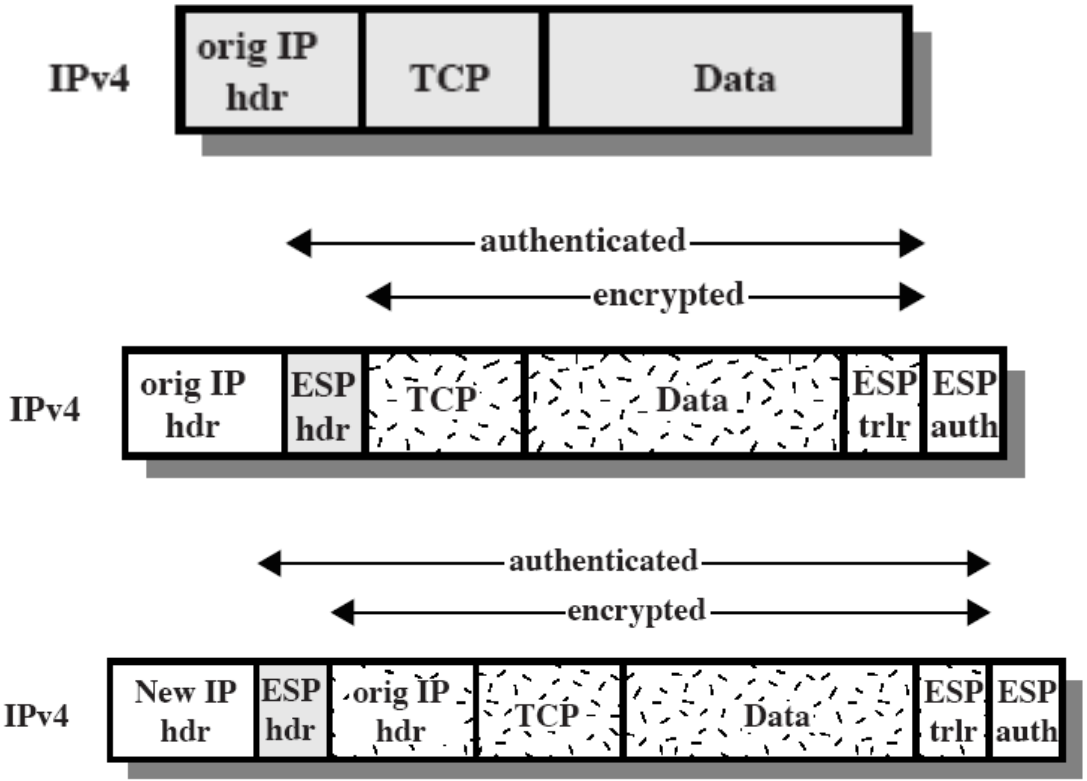


Original

Transport Mode: Cover most of the original packet

Tunnel Mode: Cover entire original packet

ESP: Tunnel and Transport Mode



Transport Mode
Good for host to host traffic
Tunnel Mode
Good for VPNs, gateway to gateway security