SWINBURNE UNIVERSITY OF TECHNOLOGY

VPNs

Lecture fourteen

Outline of Lecture

- Tunnelling protocols
- IPSec
- Internet Key Exchange (IKE)

Learning objectives

- You should be able to:
  - Explain the basics of tunnelling technology
  - Describe the main components and functions of the IPSec protocol
  - Explain in general terms Internet Key Exchange

Basics of tunnelling

- Tunneling the most important component of VPN technology
- The technique for encapsulating an entire data packet in the packet of another protocol
  - The header of the tunnelling protocol is prepended to the original packet
- Three protocols in a tunnel
  - The carrier protocol
  - The encapsulating protocol
  - The passenger protocol

Components of tunnelling

- Target network
- Initiator node
- Home Agent (HA)
- Foreign Agent (FA)

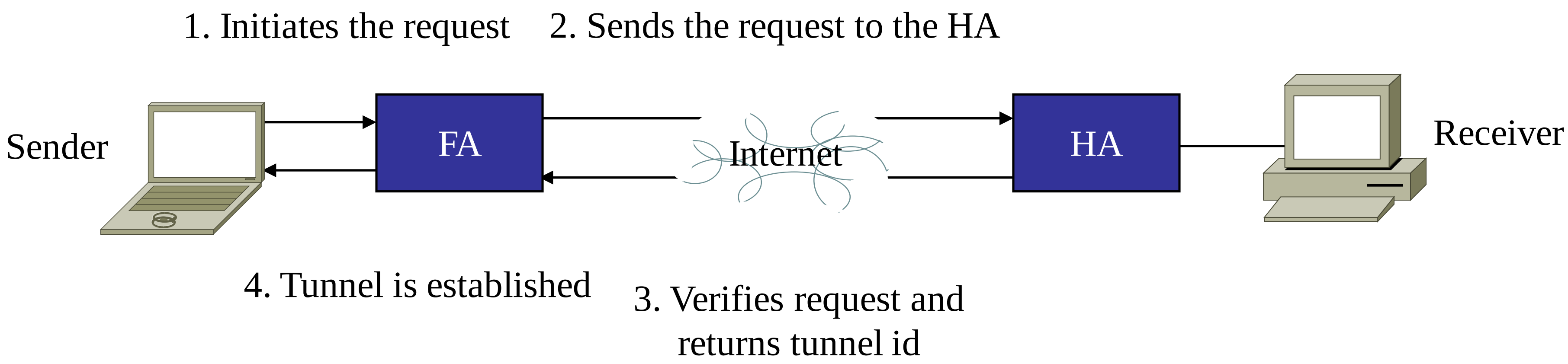
Tunnel operations

- Two phases
  1. Initiator node requests a VPN session and is authenticated by the corresponding Home Agent (HA)
  2. Data transfer occurs across the tunnel

Phase 1: Initiation

1. Initiator sends the connection request to the Foreign Agent (FA) in the local network
2. The FA authenticates the request
3. If successfully authenticated, the FA sends the request to the target network Home Agent (HA)
4. If the request is accepted by the HA the FA sends the encrypted login id and password
5. The HA verifies the login. If successful the HA sends a Register Reply message and tunnel id to the FA
6. The tunnel is established when the FA receives the Register Reply

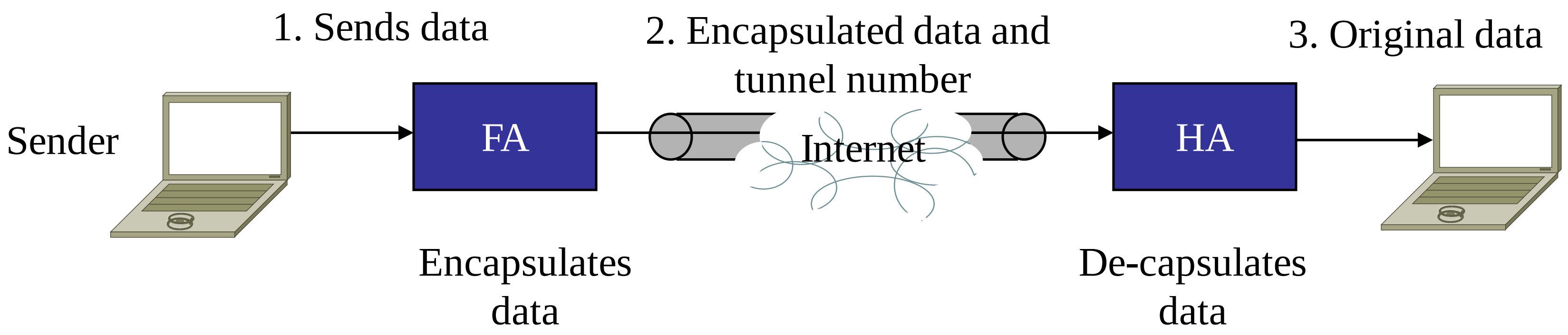
Phase 1: Initiation



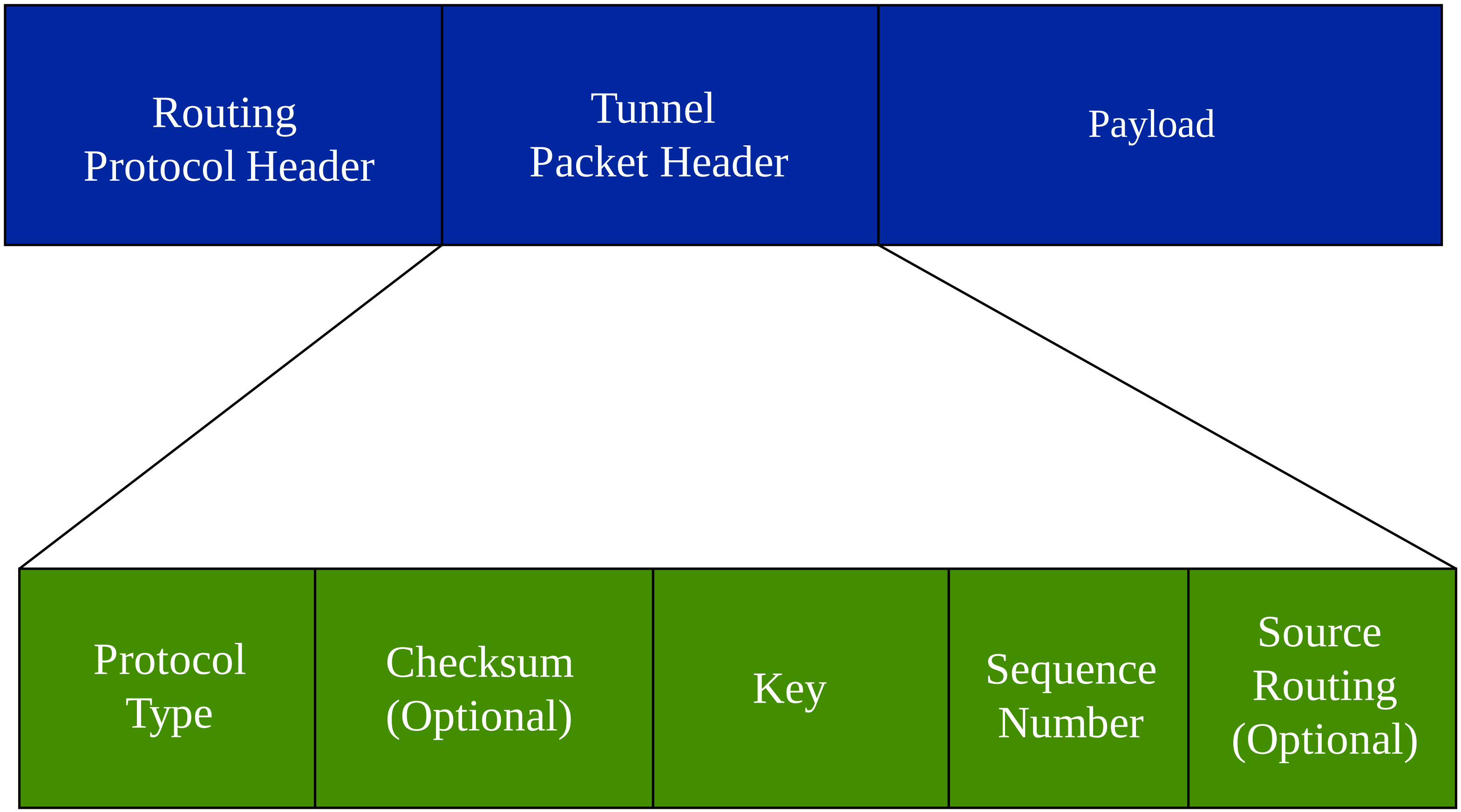
Phase 2: Data transfer

1. The initator starts sending data packets to the FA
2. The FA creates the tunnel header and a header of a routable protocol and prepends it to the data packet
3. The FA forwards the resulting routable encrypted packet to the HA using the supplied tunnel id
4. On receiving the encrypted information the HA strips off the tunnel header and routable protocol header
5. The original data is then forwarded to the intended destination node

Phase 2: Data transfer



Tunnelled packet format

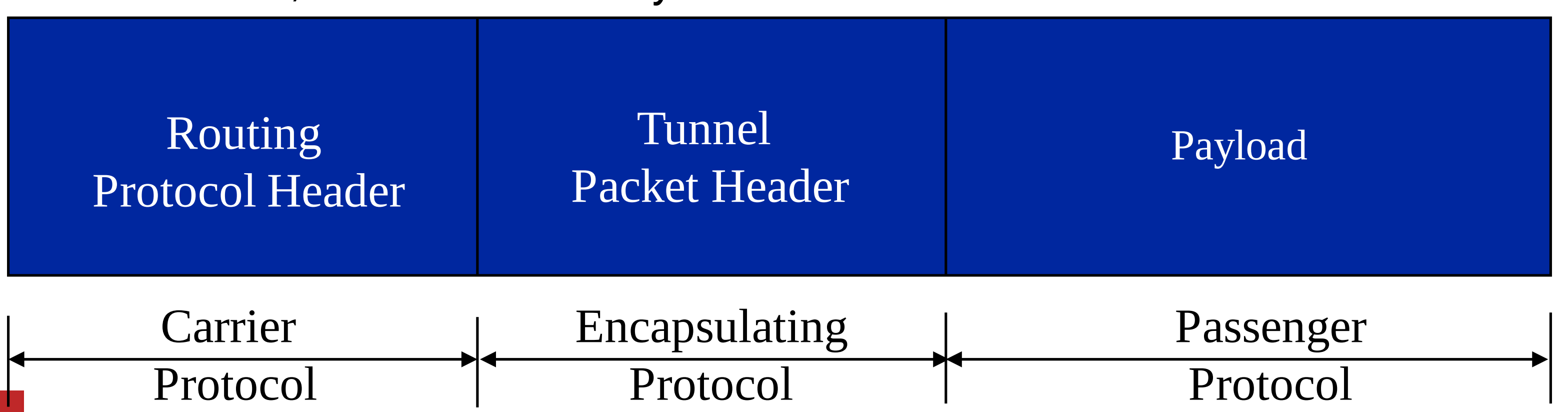


Tunnelled packet format

- Header of routable protocol
  - Addresses of source (FA) and destination (HA)
  - Usually the standard IP packet header
- Tunnel packet header
  - Protocol type of payload
  - Checksum
  - Key
    - identification of initiator
  - Sequence number
  - Source routing
- Payload
  - Original packet sent by the initiator to the FA

Tunnelling Protocols

- Carrier protocol
  - Used to route tunnelled packets to destination across the network
  - Usually IP
- Encapsulating protocol
  - The protocol used to encapsulate the payload
- Passenger protocol
  - The original data that needs to be encapsulated
  - PPP, IP most commonly used



Tunnel types

- Voluntary tunnels
  - end to end tunnels
  - created at the request of one of the end-points
  - exclusive use by a single communication
- Compulsory tunnels
  - created and configured by an intermediate device
  - typically used to transmit authentication information
    - eg Before a tunnel is created all communications go to a NAS
  - usually shared by multiple communications

Question

- Which of the following statements about compulsory tunnels is true?:
  - They are known as end-to-end tunnels
  - The number of tunnels depends on the number of communicating pairs
  - An intermediate device plays an important role in these tunnels

IPSec

- Internet Protocol Security (IPSec)
- A suite of protocols
  - AH: Authentication Header
  - ESP: Encapsulating Security Payload
  - FIP-140-2 and others
- Operates at layer 3
  - Tightly integrated with IP
  - Can be used with IPv4
  - Integrated into IPv6
- Very flexible
  - able to integrate into many different authentication and encryption schemes and use many different tunneling technologies

IPSec

- Developed by IETF
- RFC2401
  - Security Architecture for the Internet Protocol
- RFC2402
  - IP Authentication Header
- RFC2406
  - IP Encapsulating Security Payload
- RFC1852
  - IP Authentication using Keyed SHA
- RFC3602
  - The ESP AES-CBC transform

IPSec Security Associations (SAs)

- Security Associations (SAs) a fundamental concept of IPSec
- An SA is a logical unidirectional connection between two entities that uses IPSec services
- SAs are unidirectional
  - bi directional communication requires two SAs to be defined
- An SA defines:
  - Authentication protocol, keys and algorithms
  - Mode and keys for Authentication Header (AH) or Encapsulation Security Payload (ESP) protocols of IPSec suite
  - Key related information
  - SA information
  - Cryptographic synchronisation

IPSec Security Associations (SAs)

- SAs are made up of three fields
  - Security Parameter Index
    - 32 bit field that identifies the security protocol
  - Destination IP address
    - Always a unicast address
  - Security protocol
    - AH or ESP
- Each SA defines a security association in one direction only for either authentication (AH) or encryption and authentication(ESP)
- To define authentication and encryption in a bidirectional link will require 2 SAs
  - Sometimes an “SA bundle”

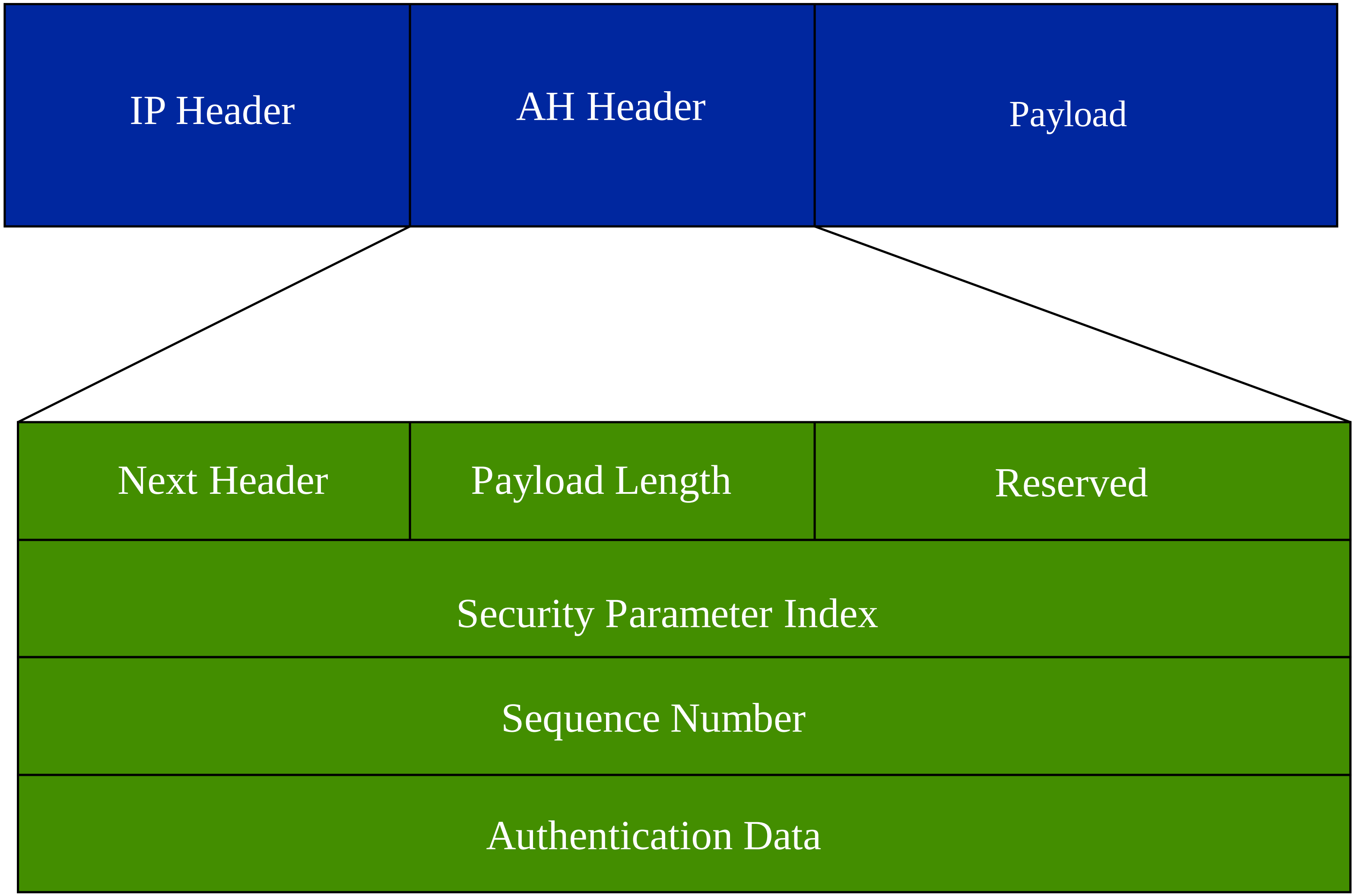
IPSec Security Associations (SAs)

- An SA uses two databases
  - Security Association Database (SAD)
    - keeps track of information related to each SA
  - Security Policy Database
    - specifies what traffic is carried across the tunnel
    - similar to firewall rules

Authentication Header (AH) Protocol

- Used to ensure integrity of packet
  - not confidentiality
- An authentication header is prepended to the payload
- Uses a shared secret key to construct a hash of the contents of the payload
  - Hash based Message Authentication Code (HMAC)
- Destination uses key to calculate the hash
  - if the same then payload has not been changed
- Most commonly used hash algorithms
  - SHA1 (HMAC-SHA1)
  - SHA256 (HMAC-SHA256)

Authentication Header (AH) Protocol



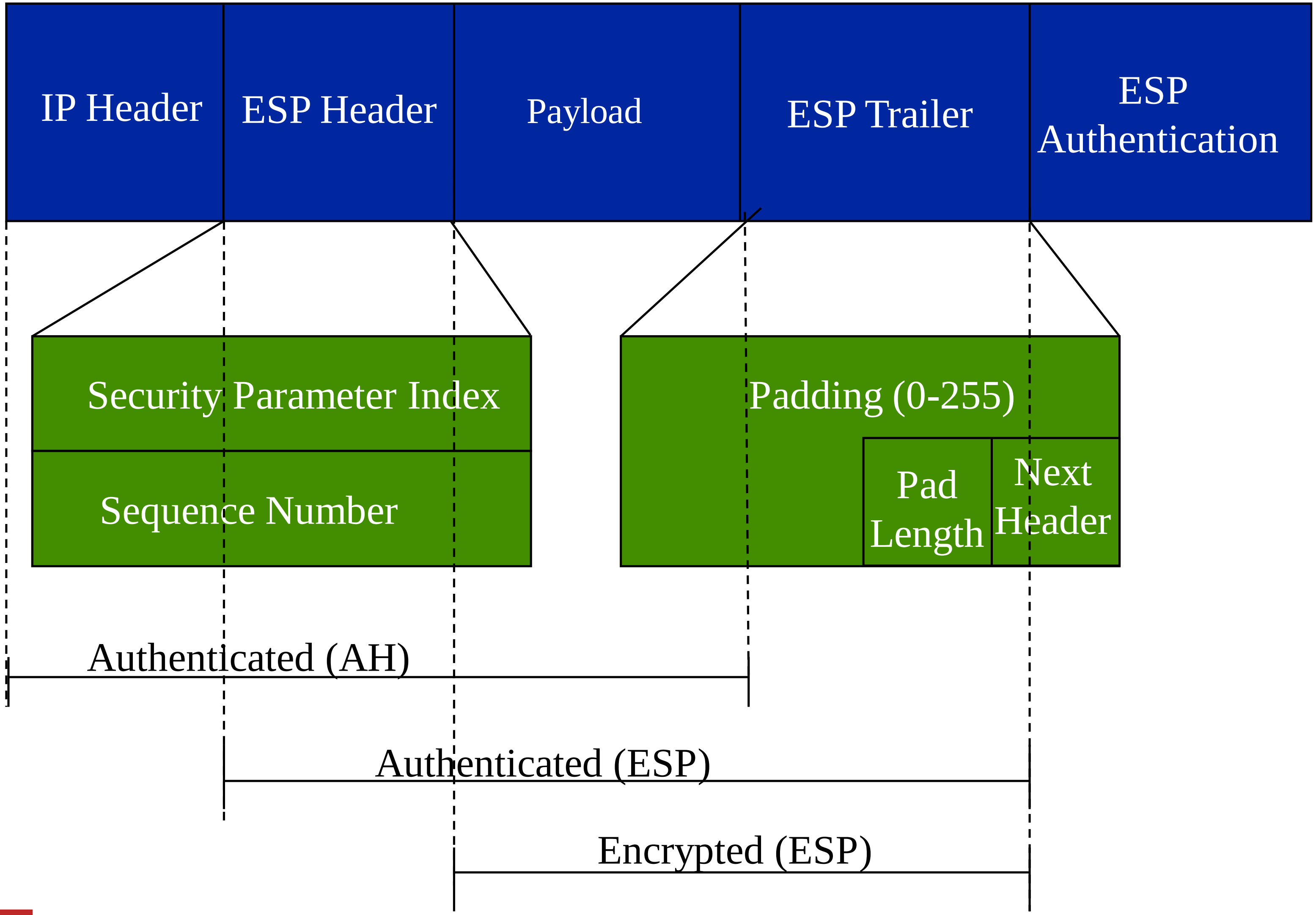
Authentication Header (AH) Protocol

- Next header
  - Protocol number
- Payload length
- Reserved
- SPI
  - index into SAD for Security Association information
- Sequence number
- Authentication data

Encapsulating Security Payload (ESP) Protocol

- Provides both confidentiality AND authentication
- ESP uses encryption for confidentiality and hashing for authentication
- Authentication algorithms used are the same as AH
- Encryption algorithms symmetric
  - use shared secret key
    - CBC-AES, 3DES, IDEA most commonly used
- ESP encrypts and authenticates the payload only

Encapsulating Security Payload (ESP) Protocol



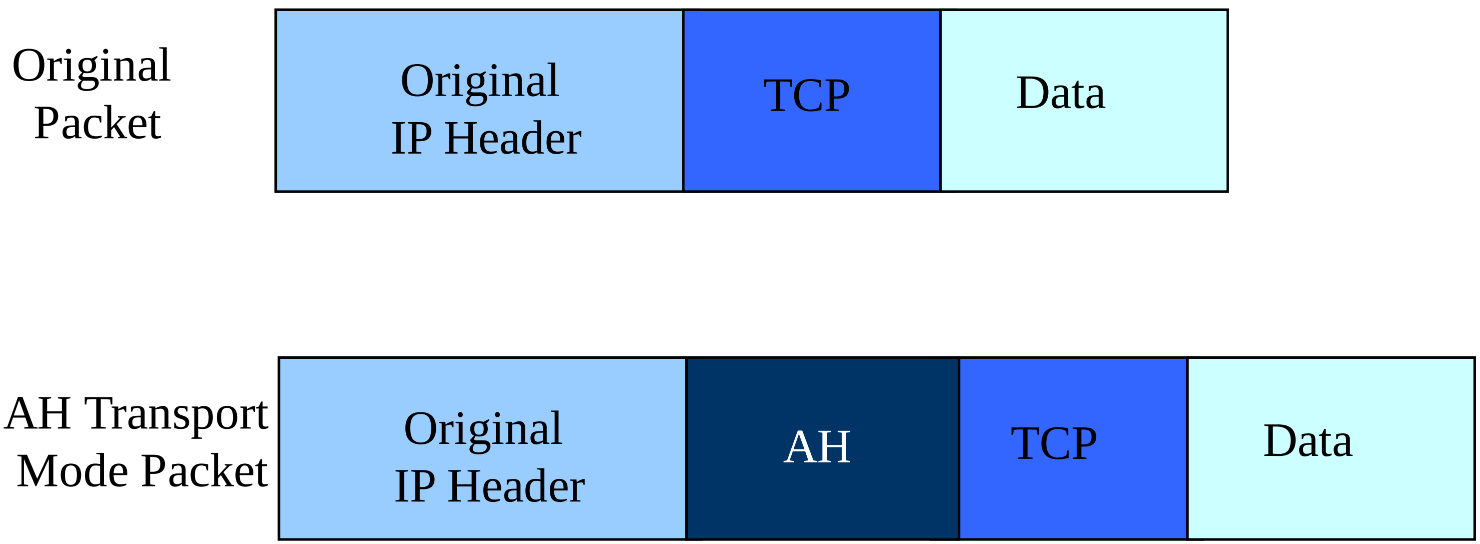
Question

- We only wish to authenticate our data.
  - Which IPSec protocol do we use?
  - How many SAs?
- We wish to encrypt and authenticate our data
  - Which IPSec protocol do we use?
  - How many SAs?

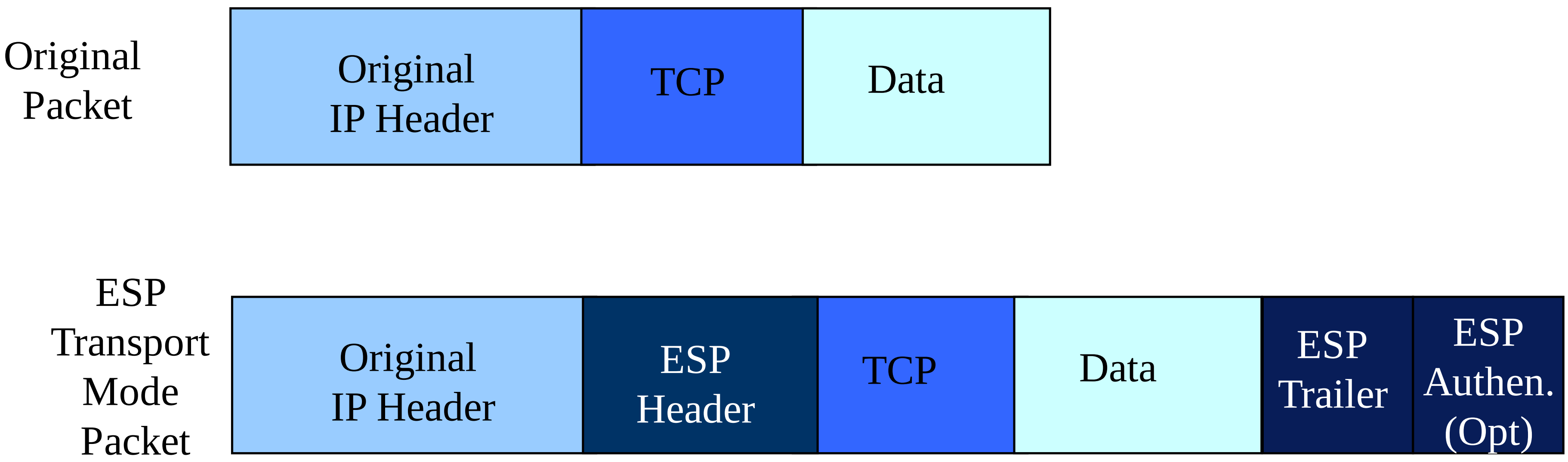
IPSec modes

- SAs in IPSec can operate in two modes
  - Transport mode
    - protects upper layer protocols only
    - IPSec header is inserted between the IP header and the payload
  - Tunnel mode
    - protects the entire IP datagram
    - New IP header is created and the IPSec header is inserted between the new IP header and the old IP header

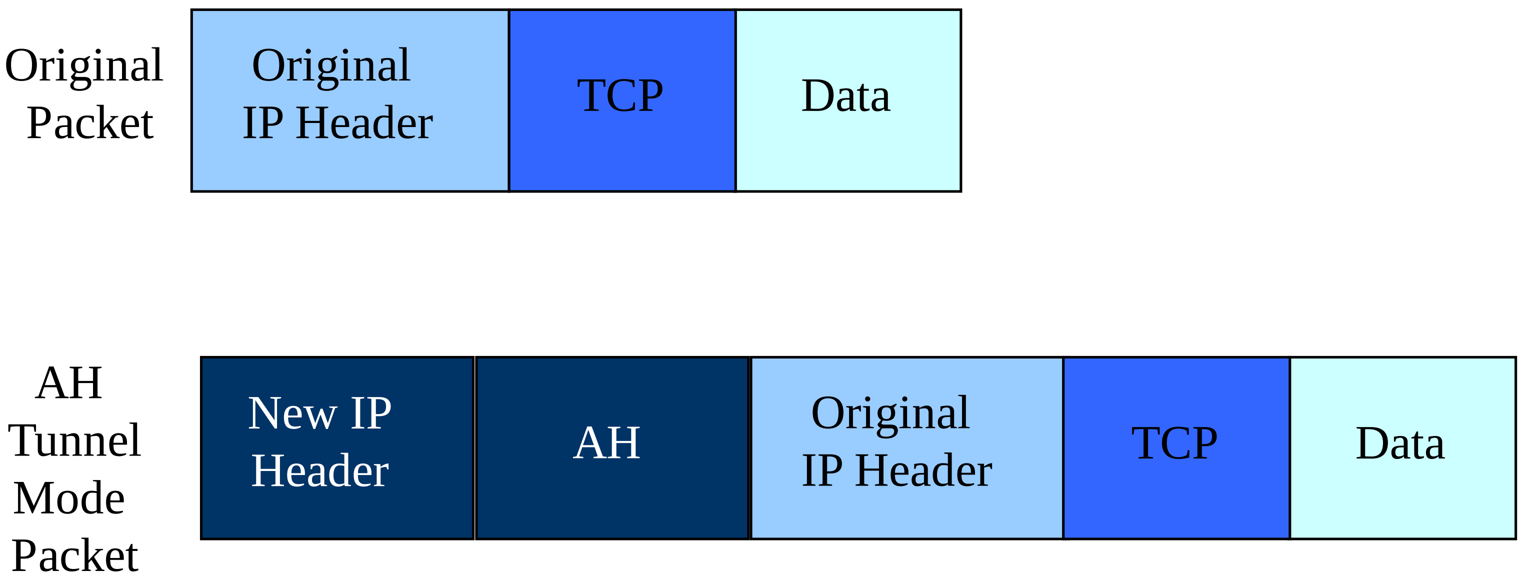
IPSec transport mode with AH



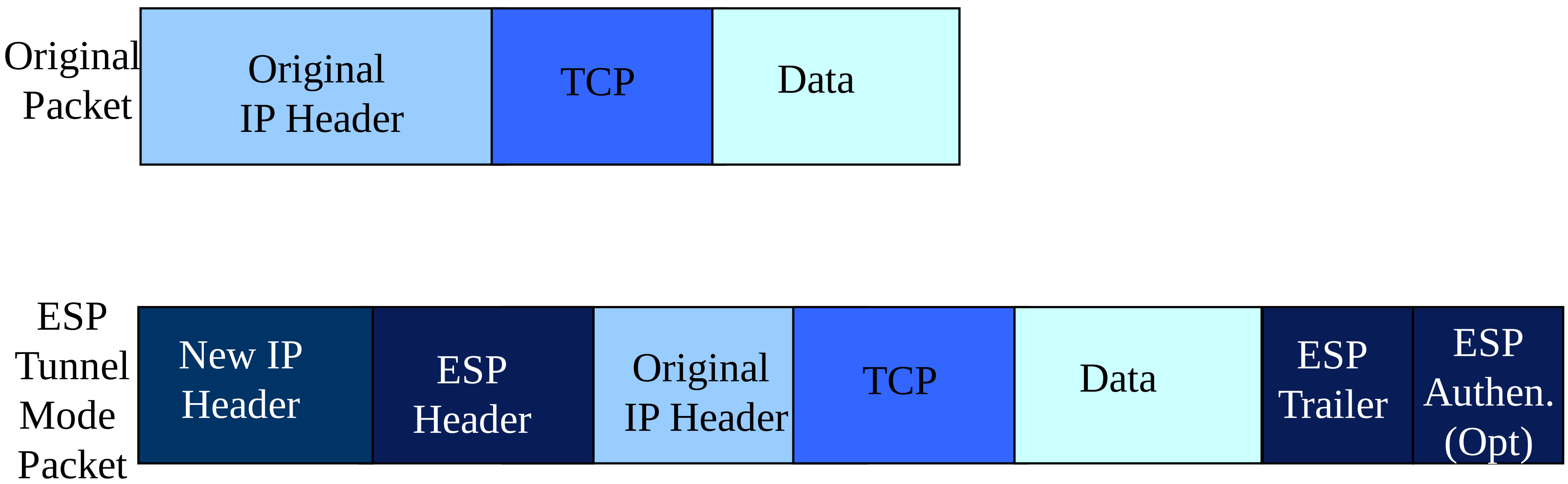
IPSec transport mode with ESP



IPSec tunnel mode with AH



IPSec tunnel mode with ESP



Key management

- AH and ESP each need separate keys for send and receive
  - Potentially 4 keys
    - Sometimes wish to open an authentication tunnel only, sometimes an encryption and authentication tunnel
- Keys can be distributed manually
  - Changed infrequently
    - not every packet or session
- However, automated key management desirable
  - Large number of users manual key exchange a large overhead
  - Need an automated method of key exchange

Internet Key Exchange

- RFC 2409
  - Derived from ISAKMP/ Oakley
  - Not technology dependent
    - Can be used with any security mechanism
- Not fast, but key exchange occurs relatively infrequently
- Assumes a secure channel already exists
  - Usually Diffie-Hellman
    - More later when we talk about cryptography
- IKE has two phases

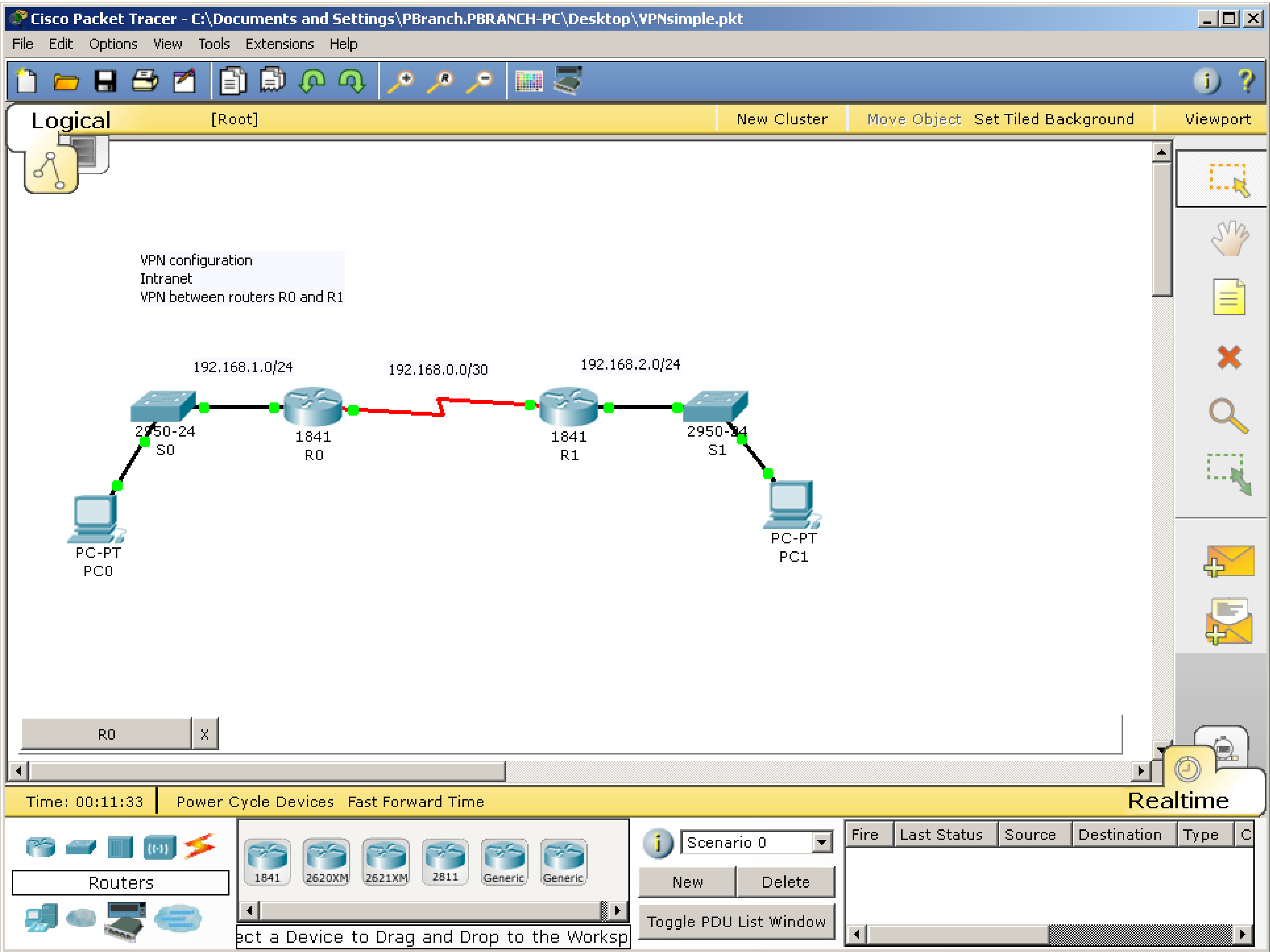
IKE phase 1

- Authenticates communicating ends
- Establishes secure IKE channel for establishing the SA
- ISAKMP SA established
  - Encryption algorithms
  - Hash functions
  - Authentication mechanisms to protect encryption keys
- Generates shared secret key using Diffie-Helman hybrid key exchange

IKE phase 2

- Deals with the establishment of SAs for IPSec
- Establishes SA including
  - Authentication methods
  - Hash functions
  - Encryption algorithms
- Typically occur ever 4 to 5 minutes
  - Much more frequently than IKE phase 1

Cisco IPSec Configuration (Intranet)



Cisco IPSec Configuration

- Extract from R0 running-config

```
crypto isakmp policy 99
 encr aes
 authentication pre-share
 group 5
!
crypto isakmp key cisco address 192.168.0.2
!
!
crypto ipsec transform-set vpntransform esp-aes 128 esp-sha-hmac
!
crypto map vpnmap 999 ipsec-isakmp
 set peer 192.168.0.2
 set transform-set vpntransform
 match address vpnacl
!
!
interface Serial0/0/0
 ip address 192.168.0.1 255.255.255.252
 clock rate 64000
 crypto map vpnmap
!
ip access-list extended vpnacl
 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
!
```

Cisco IPSec Status

Untitled - Notepad

File Edit Format View Help

```
R0#show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: vpnmap, local addr 192.168.0.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
   current_peer 192.168.0.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 0
   #pkts decaps: 6, #pkts decrypt: 6, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 1, #recv errors 0

     local crypto endpt.: 192.168.0.1, remote crypto endpt.:192.168.0.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0x0E535F22(240344866)

     inbound esp sas:
      spi: 0x2D956D44(764767556)
        transform: esp-aes 128 esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2006, flow_id: FPGA:1, crypto map: vpnmap
        sa timing: remaining key lifetime (k/sec): (4525504/3078)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x0E535F22(240344866)
        transform: esp-aes 128 esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2007, flow_id: FPGA:1, crypto map: vpnmap
        sa timing: remaining key lifetime (k/sec): (4525504/3078)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:
```

Problems with IPSec

- Compression
  - Encrypted data does not compress
  - Compression algorithms need to be applied before encryption
- QoS
  - QoS makes use of the DSCP field in the IP header
  - If this is encrypted then it cannot be read by routers on the transmission path
- Firewalls and NAT
  - If the internal packet is encrypted then NAT cannot translate the IP address
  - If internal packet is encrypted then firewall cannot do deep packet inspection or stateful inspection

Summary

- Tunneling protocols
  - Fundamental concept of VPNs
    - Enable private and authenticated communications across public network infrastructure
- IPSec
  - Operates at layer 3
  - Most commonly implemented VPN protocol
  - Authentication Header (AH)
  - Encapsulating Security Payload (ESP)
- IKE
  - Automated exchange of keys