

★ Security Policy:

- It defines the type of Security applied to a packet when it is to be sent or arrived.
- Before using SAD, a host must determine the predefined policy for the packet.

★ SPD: (Security Policy Db)

- Each host using the IPsec needs to keep a Security Policy Database.

- There is a need for
Inbound SPD
Outbound SPD

- Each entry in the SPD can be accessed using

(CP)
<SA, DA, Name, Protocol, Source Port, Destination Port>

SA: Source Address (IP)

DA: Destination Address (IP)

P: Protocol

- SA, DA Can be Unicast, Multicast, or Wildcard addresses.

- The Name defines a DNS entity.
- Protocol is either AH/ESP)

★ Outbound Processing

From Alice

Application Layer

Transport Layer

SA, DA, N, P, Sport DPort	Policy

Outbound SPD

Index of
SAD (Outbound)
= $\langle SPI, DA, P \rangle$



Index	Parameters

Outbound
SAD

IPsec
Layer



IKE

IP Layer

Link &
Physical
Layer

To Bob

IKE:
Internet
Key
Exchange
to create SA

★ Inbound Processing:

- When a packet arrives, the inbound SPD is consulted.
- Each entry in the Inbound SPD is accessed using the same sixtuple.

