# **Multiple Path IP Security**
# draft-zhang-ipsecme-multi-path-ipsec-02

IETF 85, Atlanta
IPSECME WG

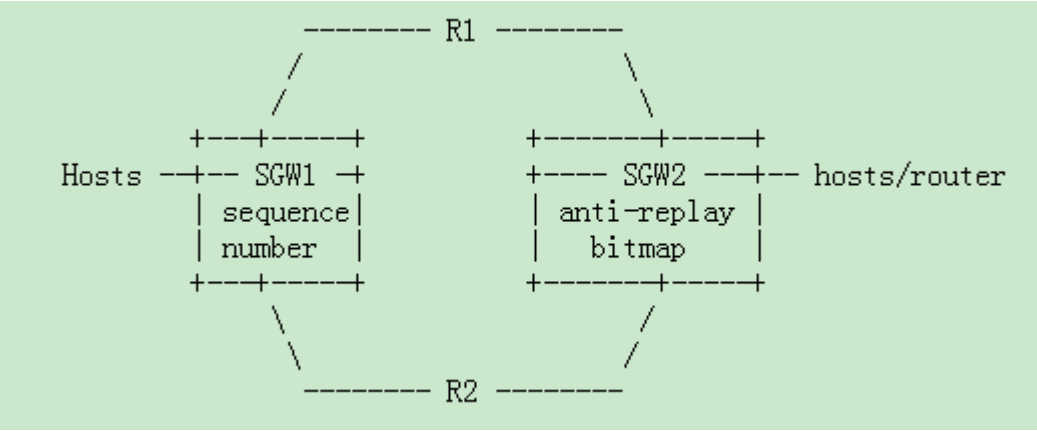
Xiangyang Zhang
Tina Tsou
Will Liu

# Background and Problem

- Security Association (SA)
  - Simplex "connection" affords security services
  - AH, or ESP, but not both – for both, two SAs must be created
- Current IPsec implementation
  - SA - only one same SA for one IPsec tunnel
  - Single SA could not achieve enough protection
- Single route
  - Intercepted easily
  - Low liability to link failure

# Approach overview

- Clustered tunnel - Multiple tunnels between sending and receiving entities
- SA Cluster - a combination of SAs
- Unique sequence number – shared among all sub-tunnels



# Outbound/Inbound processing

- Outbound processing
  - Sending entity splits the IPsec traffic through different sub-tunnels
  - One sub-SA is chosen for outbound IPsec processing only for one packet
- Inbound processing
  - Receiving entity multiplex the traffic from the different IPsec tunnels
- Except that the sequence number is shared among all sub-SAs, all the other processing procedures are not altered.

# Advantages

## Comparing to SA:

- ✓ Enhance the security
  - ✓ Different routes – harder to intercept all the packets
  - ✓ SA cluster – harder for the attacker even with the same route
- ✓ High reliability
- ✓ Provide the option for optimized performance and optimal network control

Thanks!

Comments?