Defending against IP forgery

IPsec - Internet Protocol Security provides authentication (AH) (and optionally encryption (ESP)) of IP traffic

➡ Uses SHA2 and AES (previously SHA1 and 3DES)

➡ Built-in support in IPv6

➡ Transport mode and Tunnel mode (most common)

✓ Used usually between routers (link and network layers only)

IPsec encapsulation

| m | IP header | | IPsec header | m | IP header | | m | IP header |

IPsec secure channel

router 1   router 2