The AutoVPN Architecture: *draft-sheffer-autovpn-00*

Yaron Sheffer and Yoav Nir

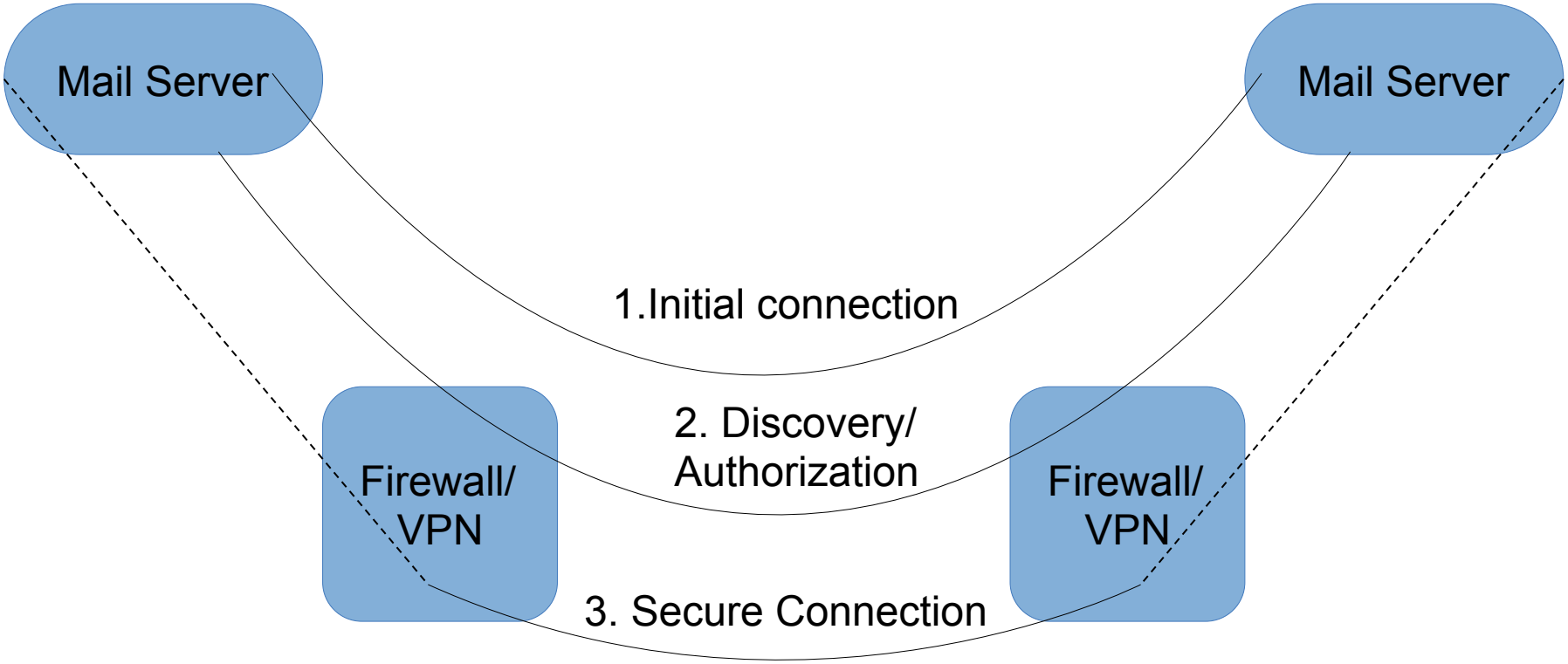
IETF-89, London

Overview

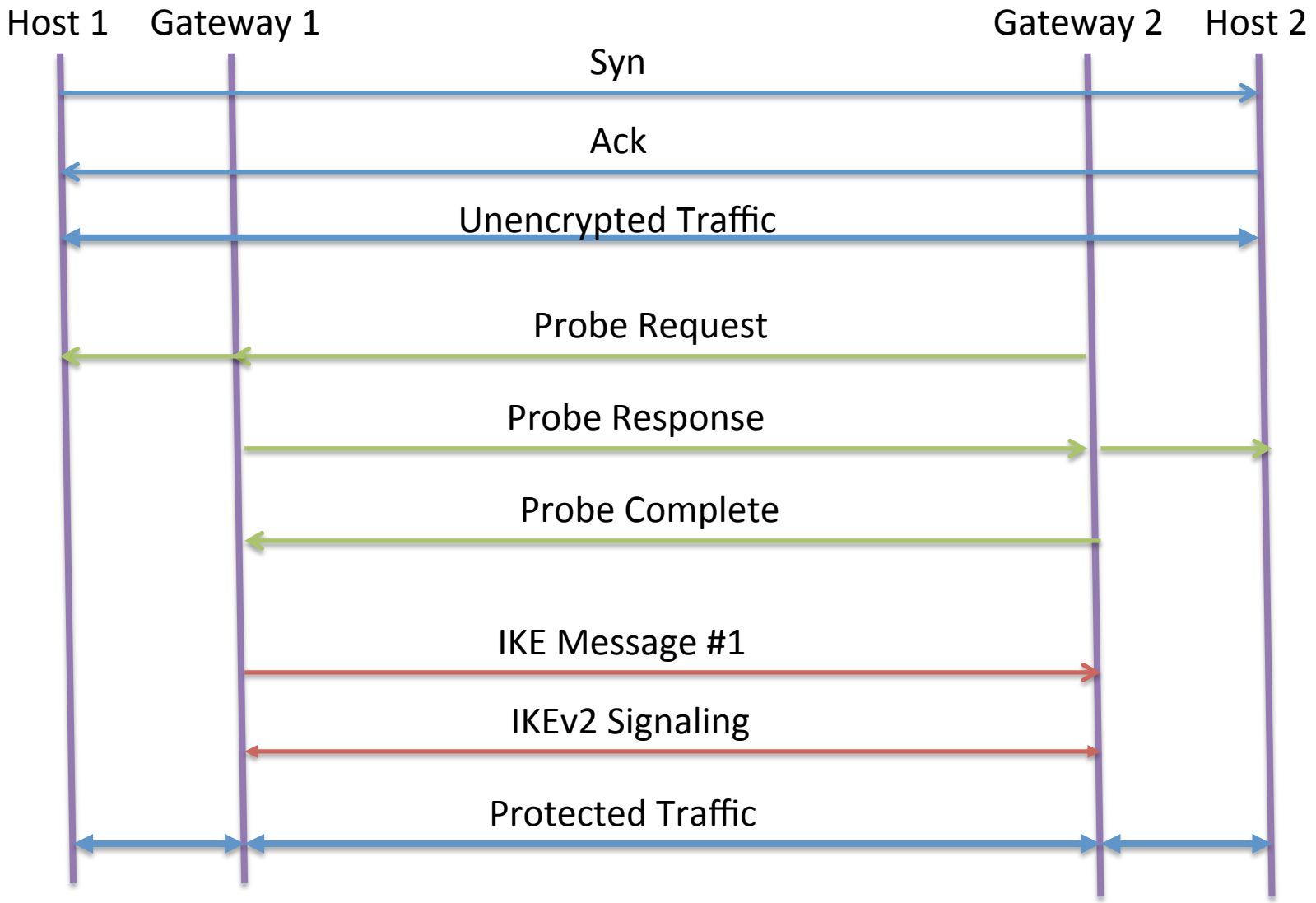
- Opportunistic IKE/IPsec between two gateways
  - Each one representing one host
  - A host may be collocated with a gateway
- ICMP used to discover IPsec entities
- Endpoints are identified by certificates
  - Typically, self-signed certificates
  - Optionally bound to the identity (verified) by off-line means
- Unlike alternatives, AutoVPN has nothing to do with DNS

Typical Use Case

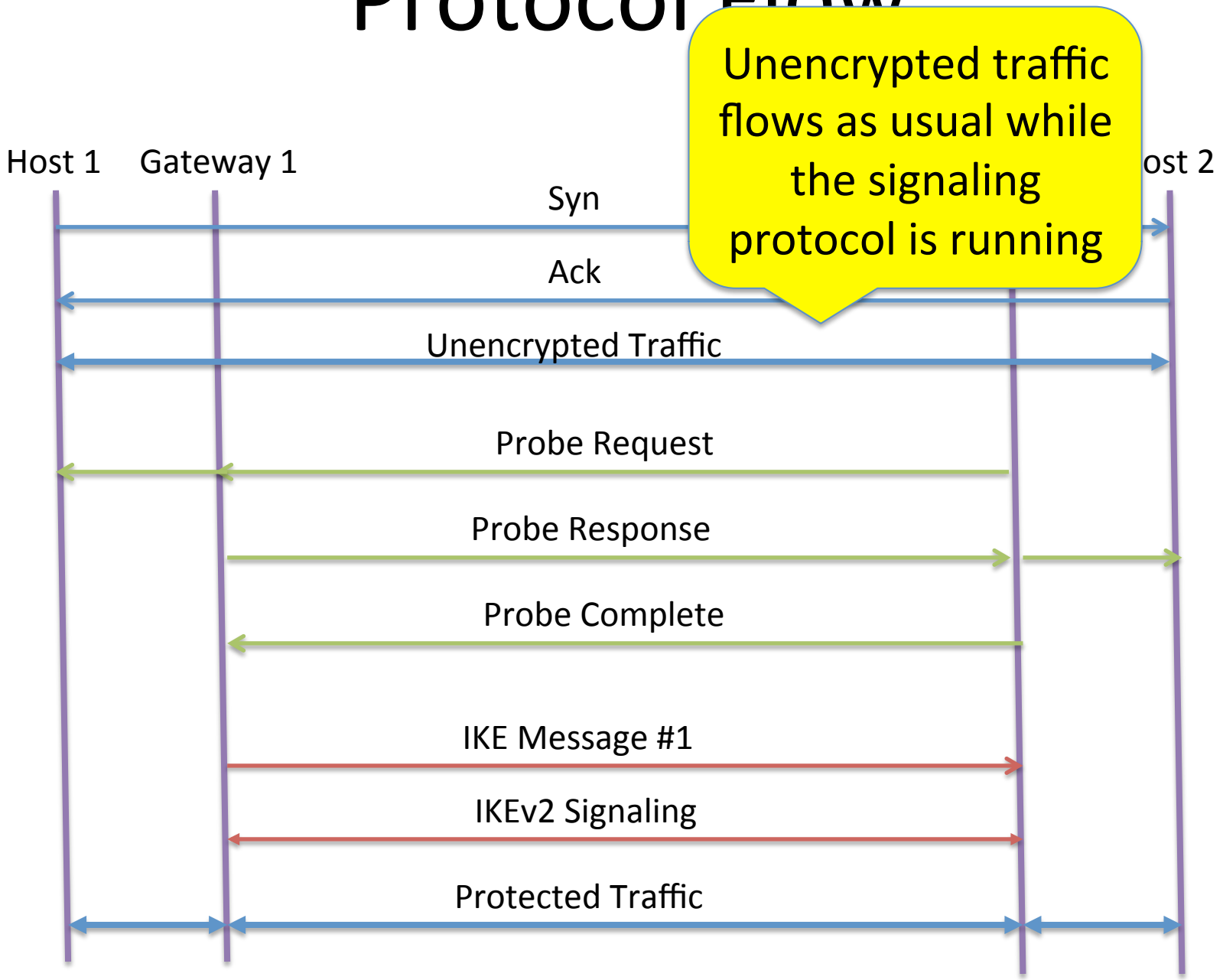
- Two mail servers speaking SMTP
  - Probably with STARTTLS
- Protected by firewall/VPNs



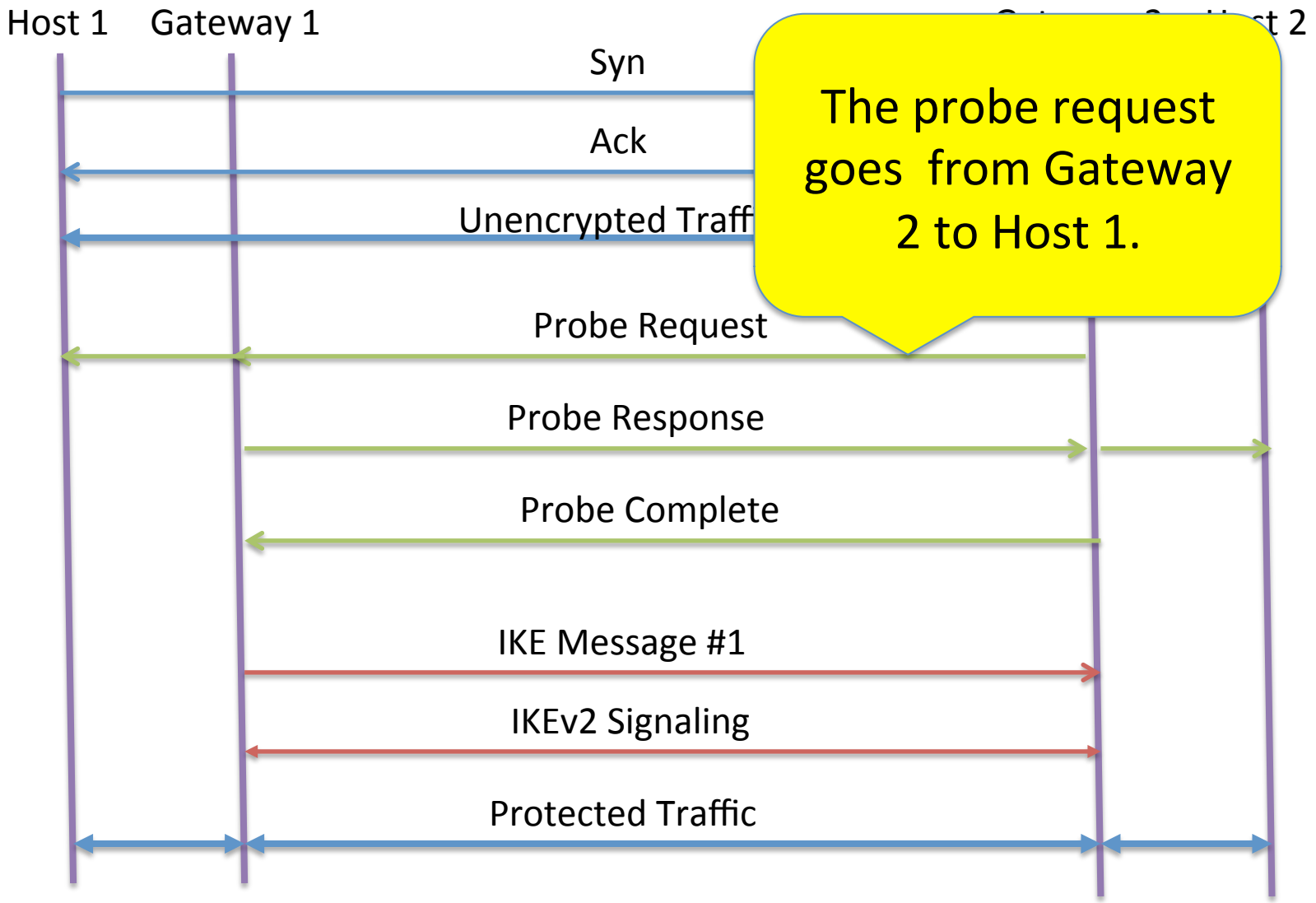
Protocol Flow



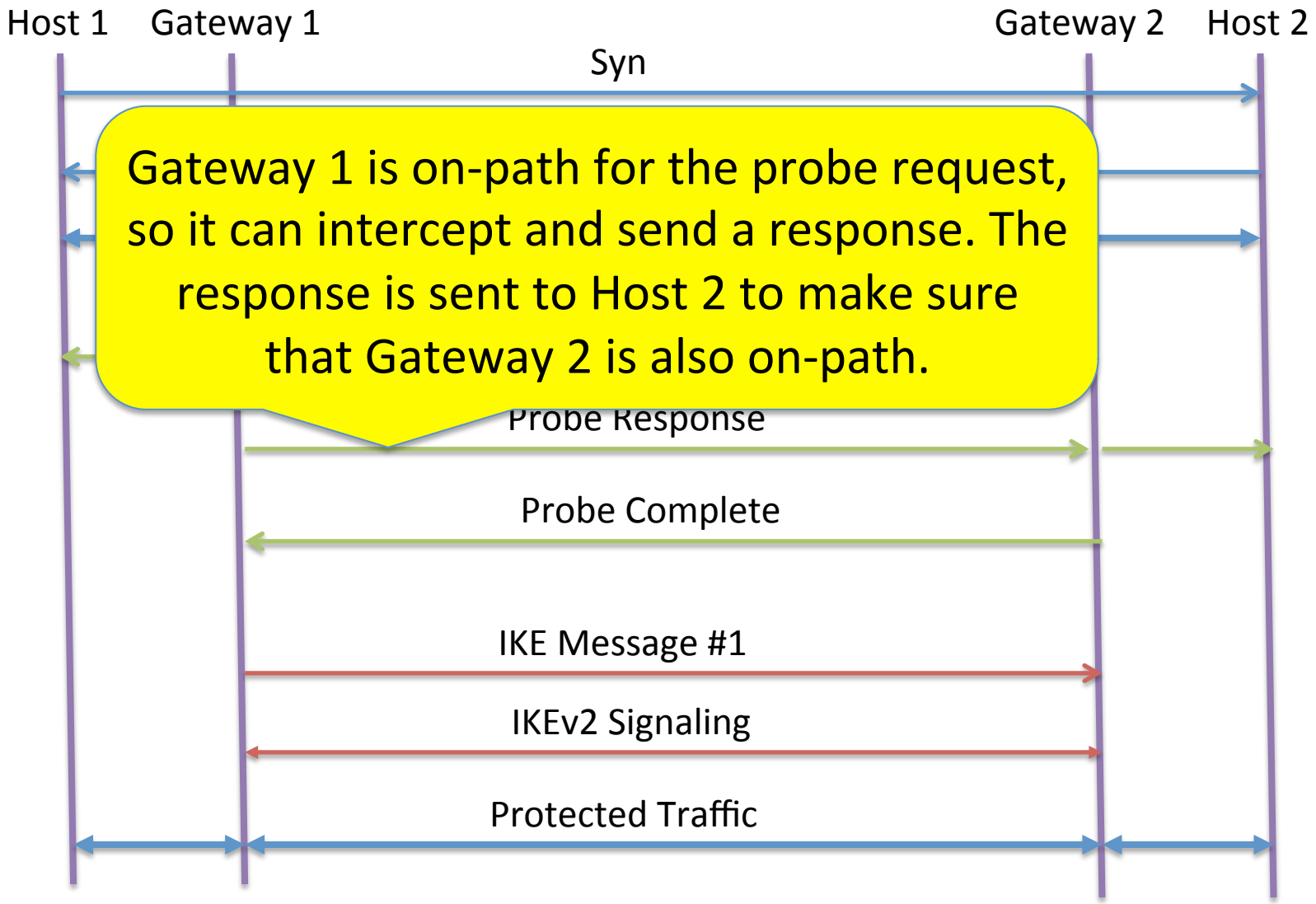
Protocol Flow



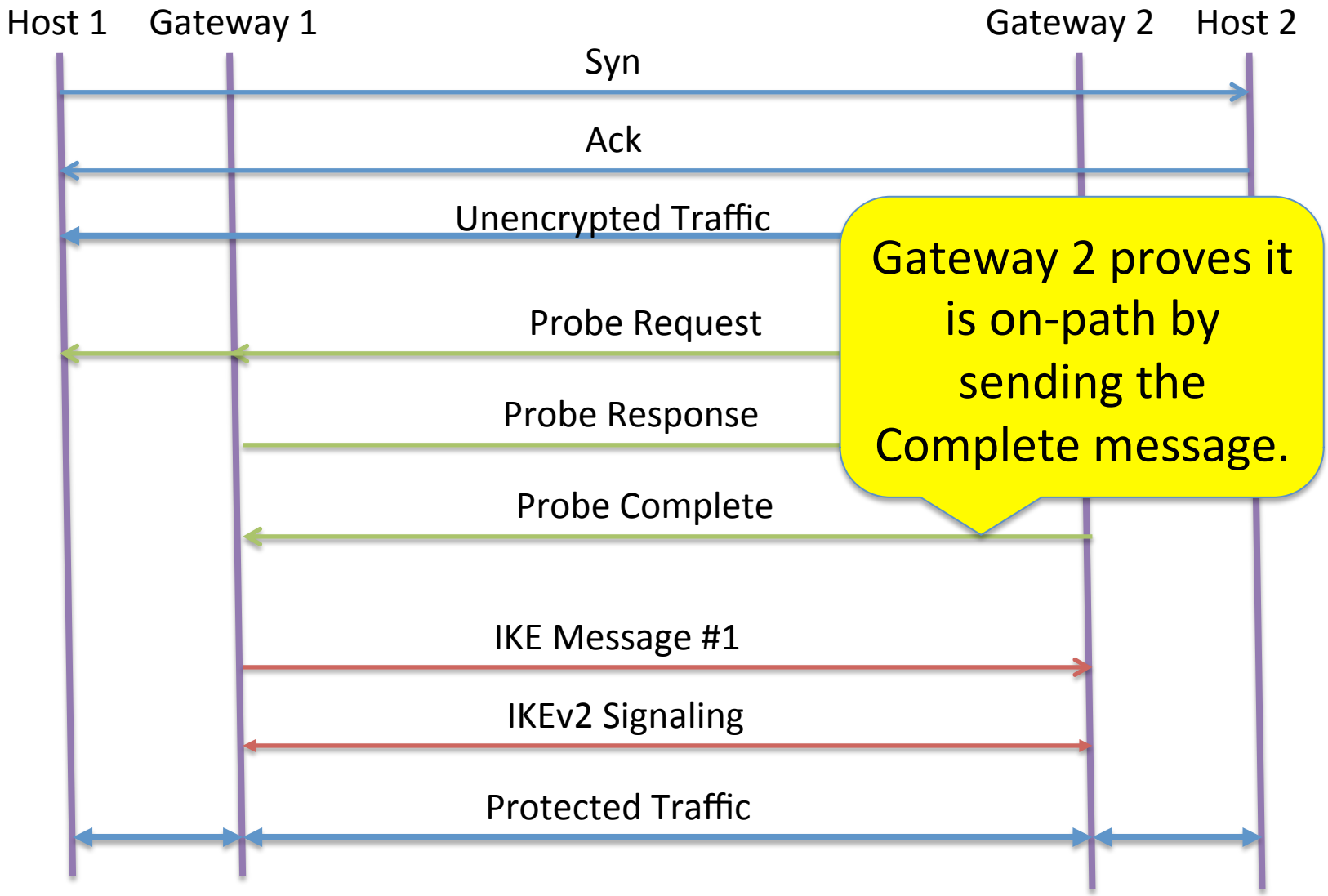
Protocol Flow



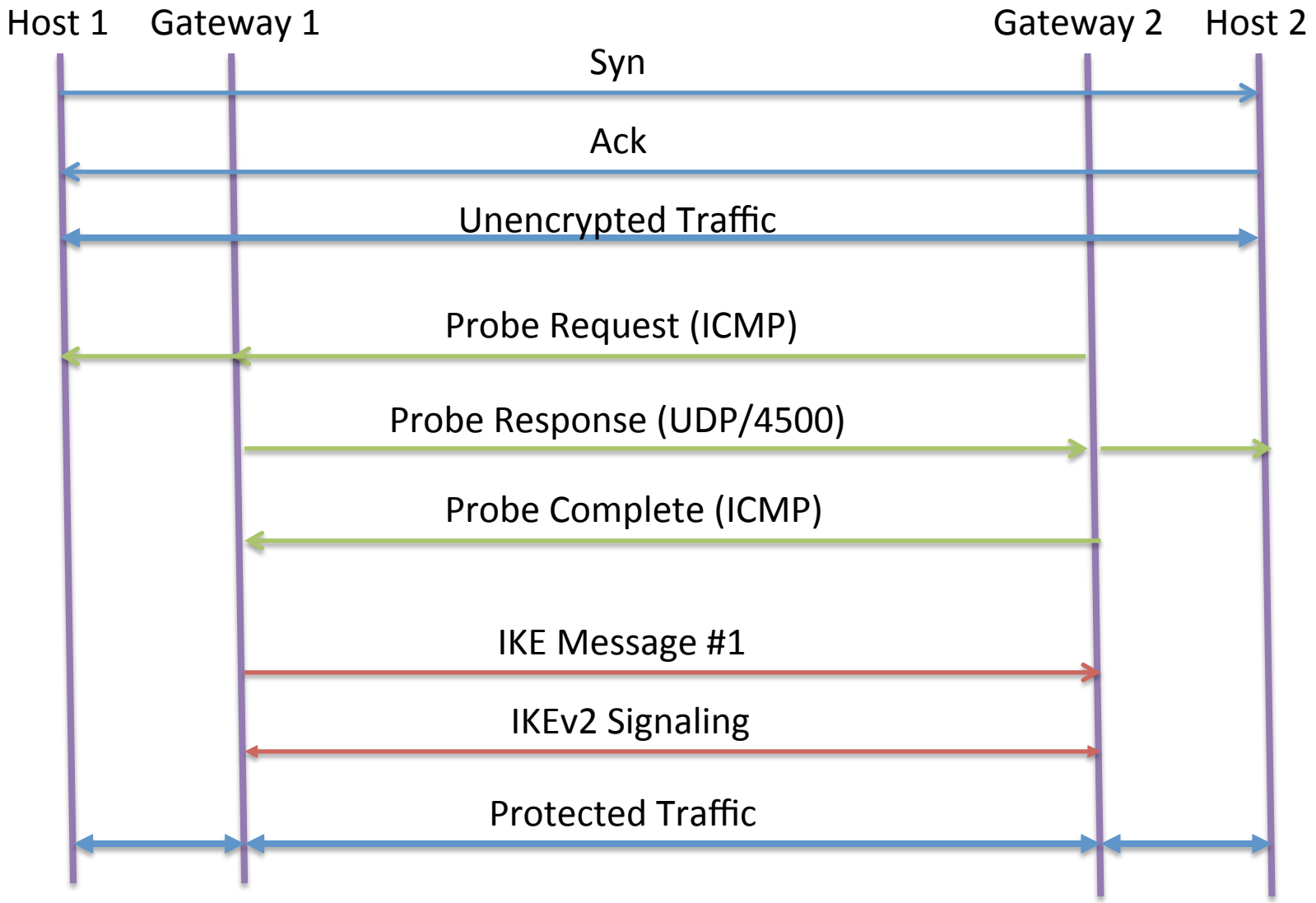
Protocol Flow



Protocol Flow



Protocol Flow



Some Details

- Using ICMP “extension objects”
- Protocol messages bound together with nonces
  - Also bound to IKE message #1
- IKE extended with a nonce and with a human readable “contact details” payload
  - Payload? Notification?

Identity

- The protocol uses IDi/IDr, and endpoints present certificates
- An admin can phone up the other side and validate the fingerprint
  - Identity is important, even in an opportunistic context!
- An optional shared secret allows each side to "roll" its certificate

Next Steps

- This is an early draft, WG feedback is requested
- Coordination with other OE activities