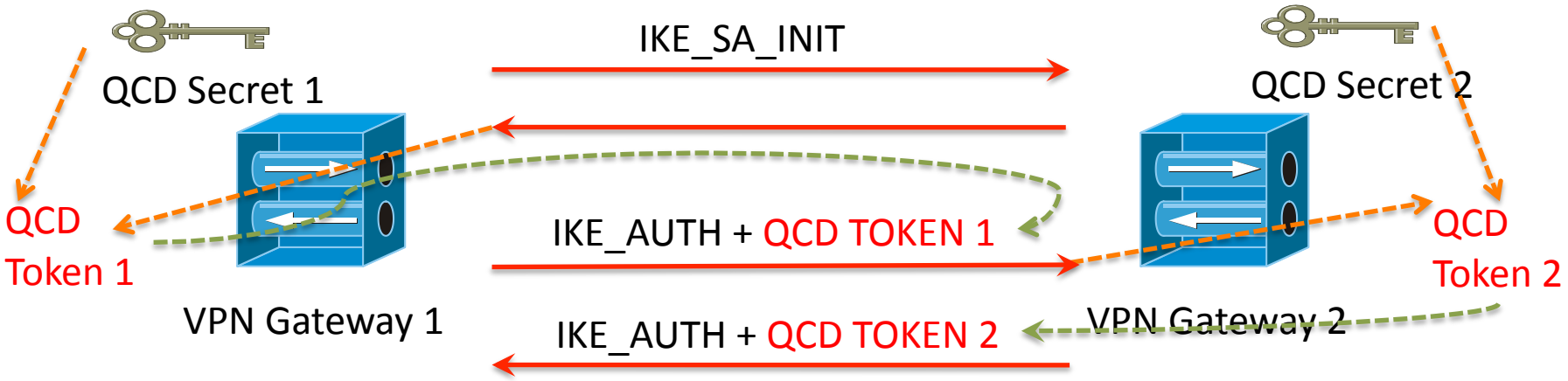
Failure Detection
draft-ietf-ipsecme-failure-detection-02

Yoav Nir
David Wierbowski
Frederic Detienne
Pratima Sethi

v01

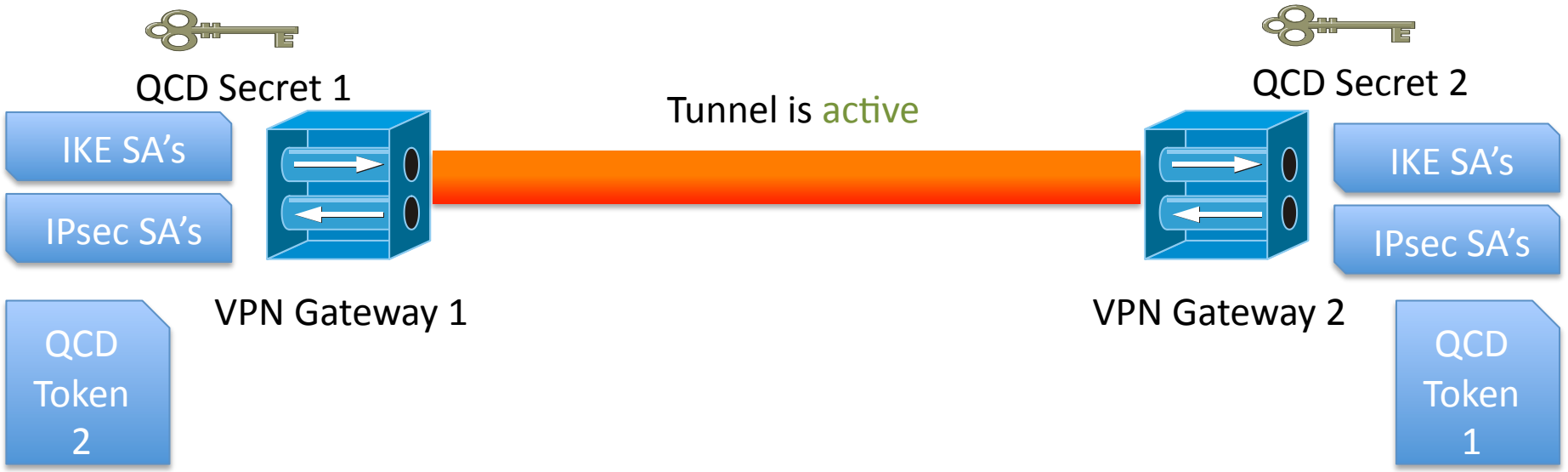
Ipsecme-failure-detection
How it works

- Staging



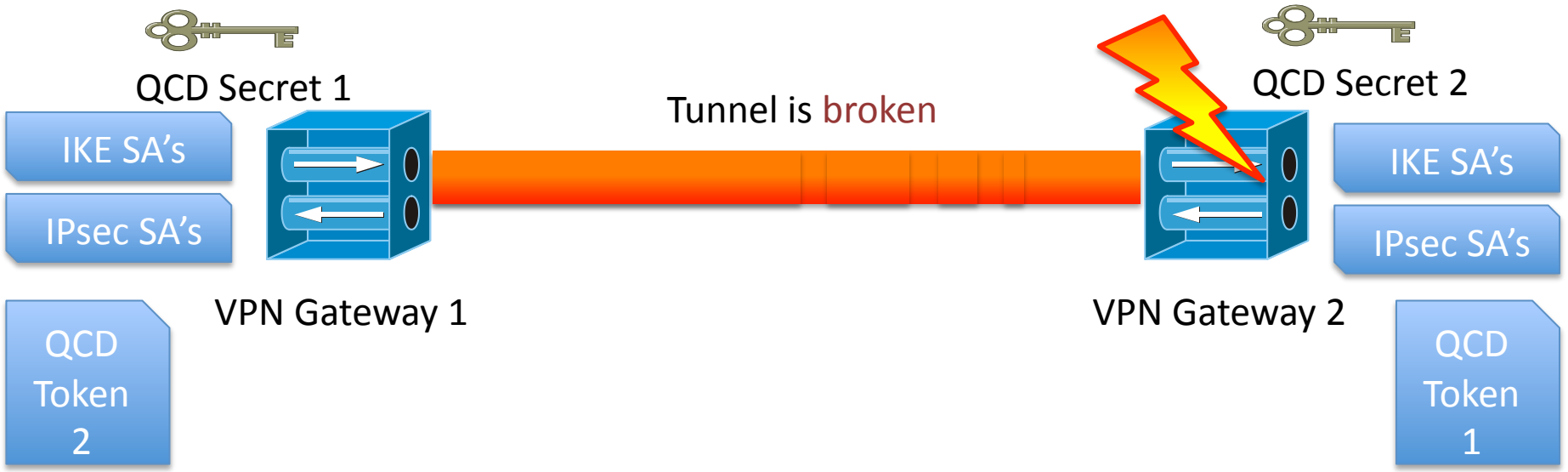
Ipsecme-failure-detection
How it works

- Steady state



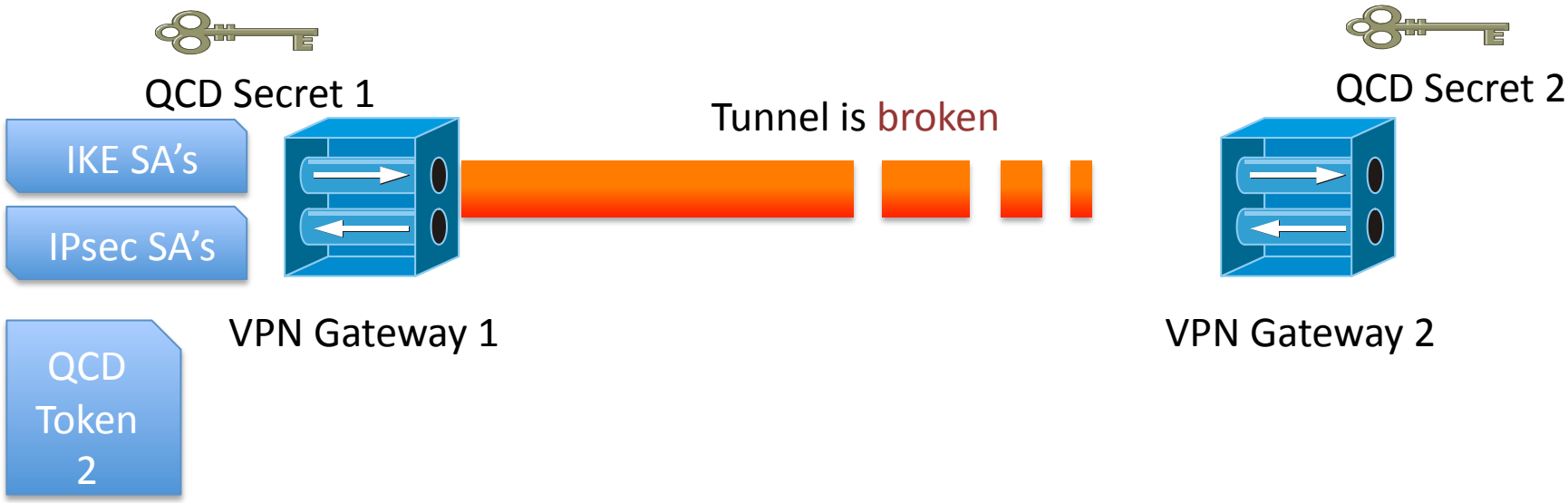
Ipsecme-failure-detection
How it works

- One gateway crashes (here GW 2)



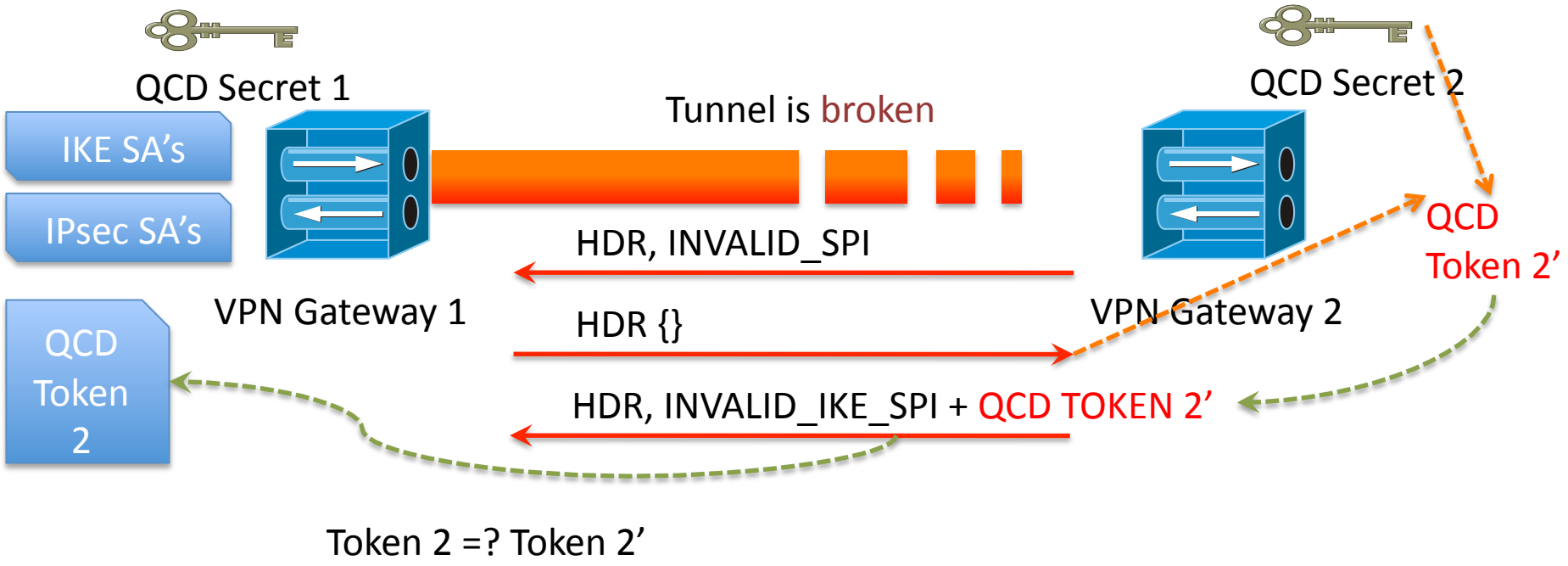
Ipsecme-failure-detection
How it works

- Gateway reboots



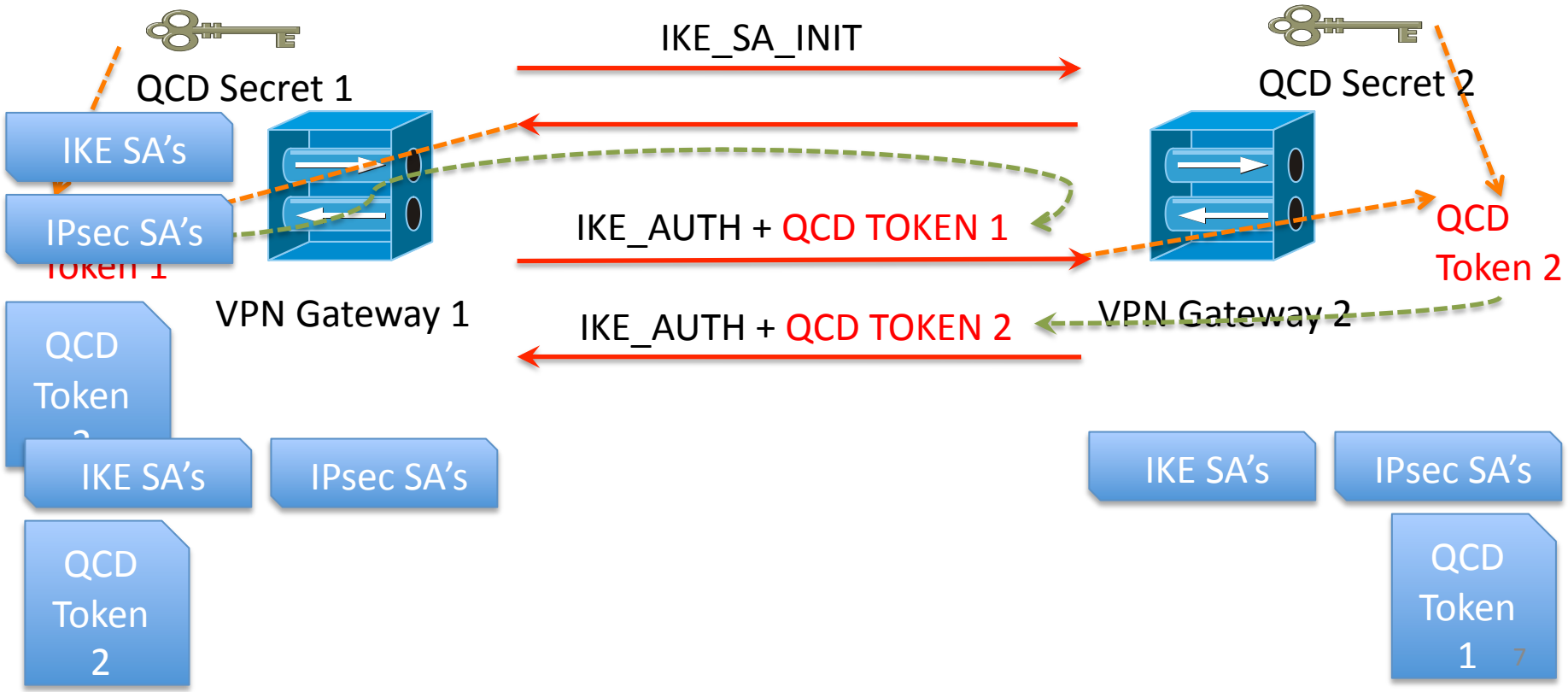
Ipsecme-failure-detection
How it works

- Crashed gateway triggers detection/proof
- INVALID_SPI + TOKEN sent in the clear



Ipsecme-failure-detection
How it works

- Assuming Token 2 == Token 2'
- Live gateway deletes old SA's and re-creates tunnel
- New QCD tokens are exchanged



Issue 198 – QCD token only for responder ?

- Q: “do we really need the QCD token for the initiator too? The initiator has already proven to be able to create the IKE SA on its own, and it will have enough information to recreate the IKE SA after the boot. “
- A: Some implementations rely on traffic to trigger the SA (re)creation. This behavior is needed.
- Extra note: always think about gw-gw implementations; not just Remote Access.

Issue 199 – Section 7.4 is mostly wrong

- Note is about rephrasing section 7.4 and actually moving it to section 2 where it really belongs.
- Authors agree. Document will be updated accordingly.

Issue 200 – Section 8 ignores IKEv2 text

- Point is made that in the presence of outgoing IPsec traffic and absence of incoming traffic, a peer should perform a liveness check.
- The picture is also incorrect and should be:

```
HDR, SK {} -->
        <-- HDR, N(INVALID_IKE_SPI), N(QCD_TOKEN)
```

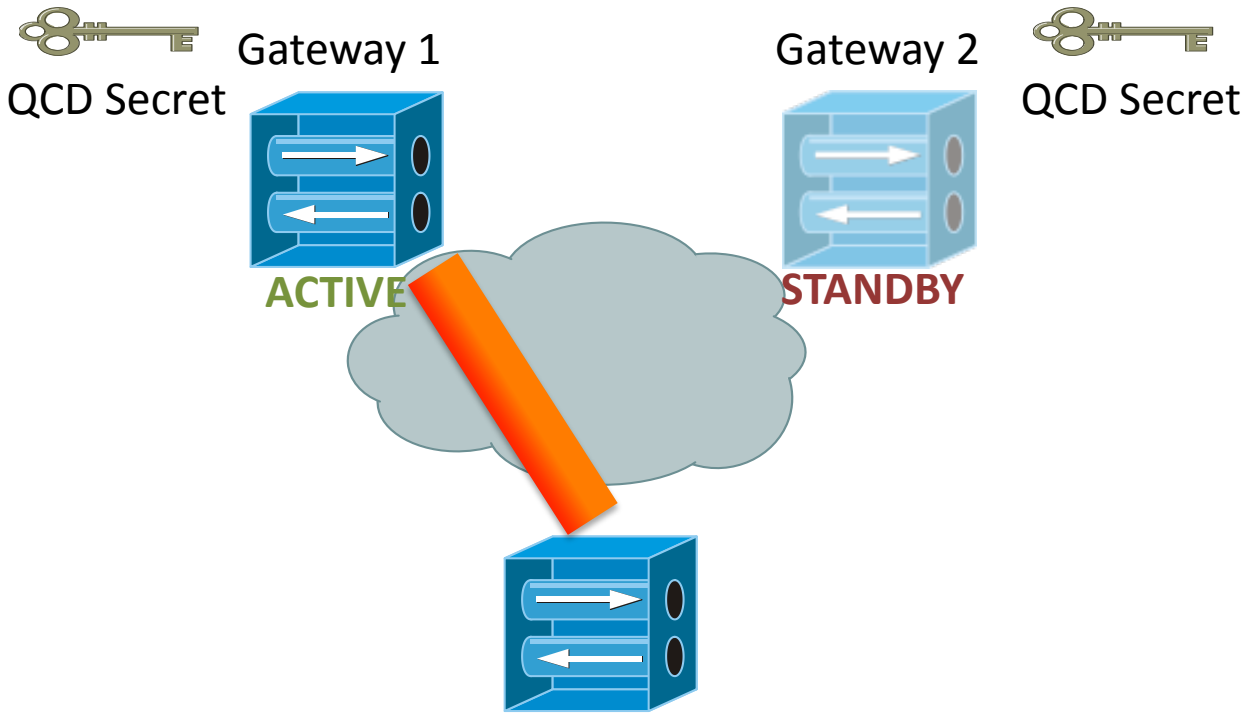
- These points are correct. Document will be fixed.

Issue 201 – Interdomain Gateways do not need QCD at all

- “In section 9.1. it says that inter-domain VPN gateways should do both, but I think that inter-domain VPN gateways does not really need this specification as all, as they by configuration do know the other ends IP-addresses etc, thus when the inter-domain VPN gateway gets up, it can immediately create the IKE SAs needed based on the configuration.”
- Answer: same as for issue 198. Traffic-triggered SA’s need this.

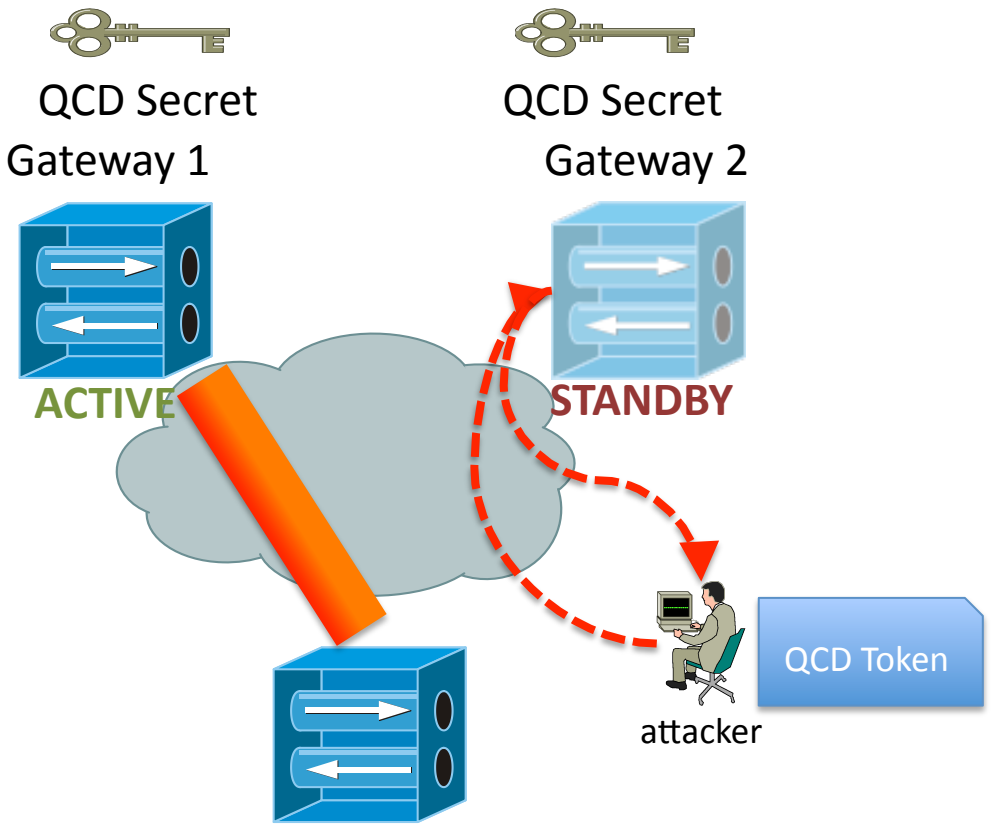
Issue 202 – Token makers generating the same tokens without synchronized DB

- Anatomy of the problem:
- Multiple gateways share the same QCD Secret
- Each gateway is a hot standby of other gateways



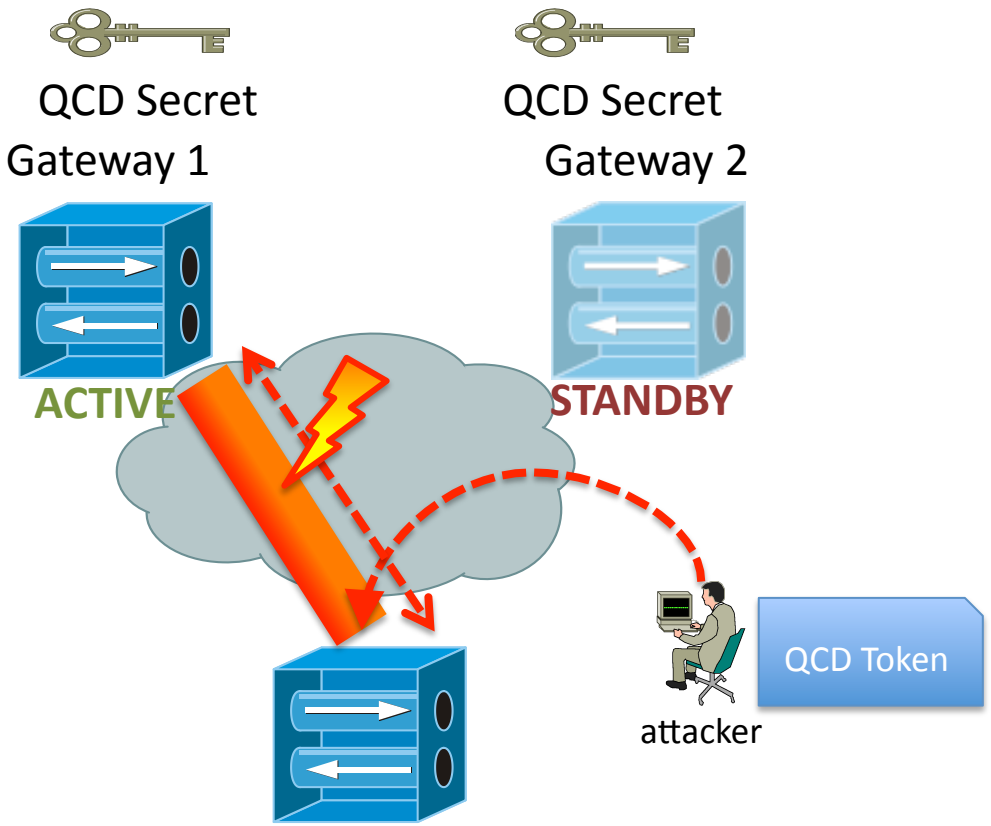
Issue 202 – Token makers generating the same tokens without synchronized DB

- An attacker spoofs an IKE packet to a standby gateway
- The standby gateway responds with the QCD token



Issue 202 – Token makers generating the same tokens without synchronized DB

- The attacker then spoofs an Invalid_IKE_SPI + Token
- Gateway deletes valid SA's and creates new ones



Issue 202 – Token makers generating the same tokens without synchronized DB

- Assumptions on the attacker:
  - knows the IKE SPI's (MitM?)
  - can inject packets to random GW (spoof to gw)
  - can capture the reply
  - Can inject packets to peer (spoof to peer)
- Ease of attack depends on
  - the Token generation method
  - The routing to reach the standby's
  - Additional strengthening of Failure Detection

Issue 202 – Token makers generating the same tokens without synchronized DB

- Proposals to alleviate the issue
  - Peer must not accept QCD token if no pending IKE request
  - Peer should delay before accepting QCD token
    - Gives a chance to real IKE reply to come back
    - Attacker gets caught
  - Rekey before deleting old SA's
  - Dampen SA – wait delay before accepting/ triggering new Failure Detection exchange