Hi,
We are using non default leftike port (4500) to connect to Amazon Transit Gateway and rightike port default 500. As an initiator we are being NAT. But AWS Replies to IKE_SA_INIT req on port 500. AWS is on public IP directly.


Have couple of questions here
1. If leftike port is non-default, should right IKE port be always be 4500?
2. The response to IKE_SA_INIT from Transit Gateway does not seem to be received at all by IKE even though tcpdump (above) on shows the packet as received on the kernel interface. We are using default socket plugin. Is this dropped by IKE? netcat on this port combination receives everything. Is this expected? I don't see any counters/stats also. UDP/IP checksums are all correct.

bash-4.3# swanctl --counters
global:
ike-rekey-init : 0
ike-rekey-resp  : 0
child-rekey     : 0
invalid         : 0
invalid-spi     : 0
ike-init-in-req : 0
ike-init-in-resp: 0
ike-init-out-req: 221
ike-init-out-resp: 0
ike-auth-in-req : 0
ike-auth-in-resp: 0
ike-auth-out-req: 0
ike-auth-out-resp: 0
create-child-in-req : 0
create-child-in-resp: 0
create-child-out-req : 0
create-child-out-resp: 0
info-in-req      : 0
info-in-resp     : 0
info-out-req     : 0
info-out-resp    : 0

1. If leftike port is non-default, should right IKE port be always be 4500?

Yes, see NATTraversal.

2. The response to IKE_SA_INIT from Transit Gateway does not seem to be received at all by IKE even though tcpdump (above) on shows the
packet as received on the kernel interface. We are using default socket plugin. Is this dropped by IKE? netcat on this port combination receives everything. Is this expected?

It's dropped by the kernel if it doesn't have a non-ESP marker, see the link above for details.