draft-mao-ipsecme-ad-vpn-protocol

Yu Mao (H3C)
ZhanQun Wang (H3C)
Vishwas Manral (HP)

IETF 88 – Vancouver, Canada

Content

- Overarching Questions
- How ADVPN Protocol Works
- Important Features
- Compare and contrast

Overarching Questions

- **Does the Control traffic need the same security mechanism as data traffic**?

- **Should the control protocol be extensible or should it be limited to Nexthop resolution only?**

- **Is it better to overload an existing protocol or should we create a new light weight mechanism?**

Overarching Questions- our thoughts

- **Does the Control traffic need the same security mechanism as data traffic**?

We see no reason for the limitation. There could be different mechanisms to do different things and the control plane could reside off-path from the data traffic.

- **Should the control protocol be extensible or should it be limited to Nexthop resolution only?**

Requirements show there is need for more.

- **Is it better to overload an existing protocol or should we create a new light weight mechanism?**

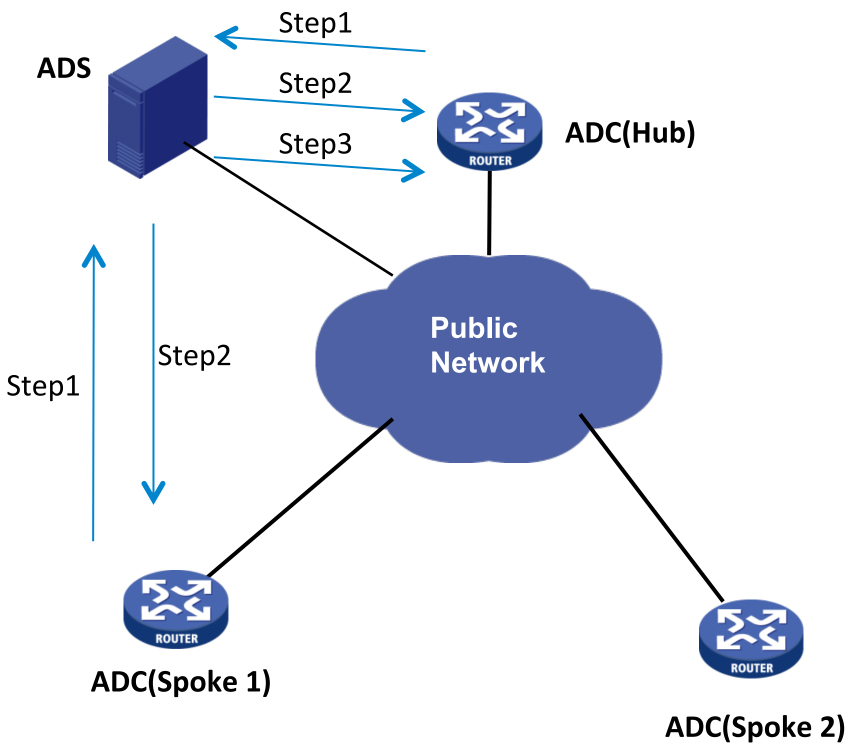
Depends on the number of changes proposed. Newer protocols have a longer deployment cycle.

Registration

Step1: When the ADC (spoke or hub) device comes up, it registers its information to ADS. The information includes the private IP address, the public IP address and the network behind the spoke.

Step2: The ADS sends the Registration Reply message to the ADC(spoke or hub) .

Step3: The ADS sends Shortcut Flow message to hub ADC in order to determine whether sending Redirect message or not.



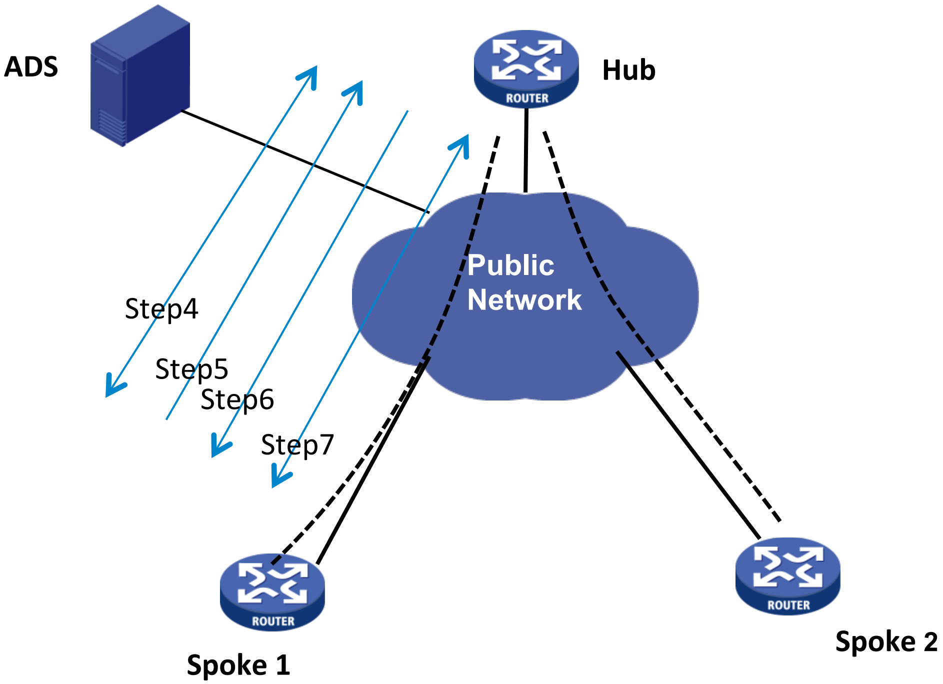
Spoke-Hub Topology Establishment

Step4: The spoke ADC obtains the information of hub ADC after registration. The spoke creates the hub session in the session table. After that, the spoke establishes an IPsec tunnel with hub ADC.

Step5: The spoke ADC send a Session Setup message to hub ADC protected by IPsec tunnel, the hub ADC has the spoke ADC's information.

Step6: The hub ADC send a Session Setup Response message to spoke ADC .

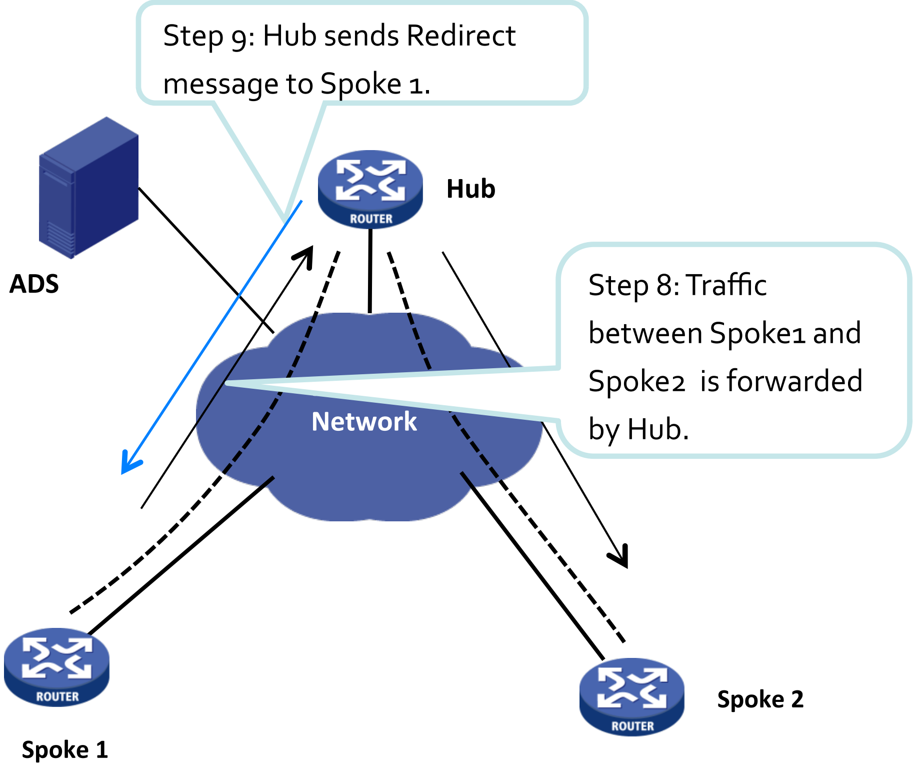
Step7: All the routing protocol packets run over IPsec tunnel between the spoke ADC and hub ADC. The routing protocol packet is copied and sent to hub ADC. The ADVPN network has spoke-hub topology.



Redirect

Step 8: When the traffic towards destination ADVPN peer arrives in the source ADVPN peer device, from the routing table, the next hop is the private IP address of hub ADVPN peer. Match the private IP address in the session table to obtain the public IP address of hub ADVPN peer. By the public IP address, the spoke-to-hub IPsec SA is chosen to encapsulate the traffic.

Step 9: The traffic arrives in the hub, after processing IPsec packet, the hub looks up routing table to determine if incoming and outgoing interface is in the same ADVPN network. If it is, this traffic is transferred through hub towards the destination spoke and there should be a shortcut path between them. If the traffic matches the Shortcut Flow table , the hub sends a redirect message to source ADVPN peer.

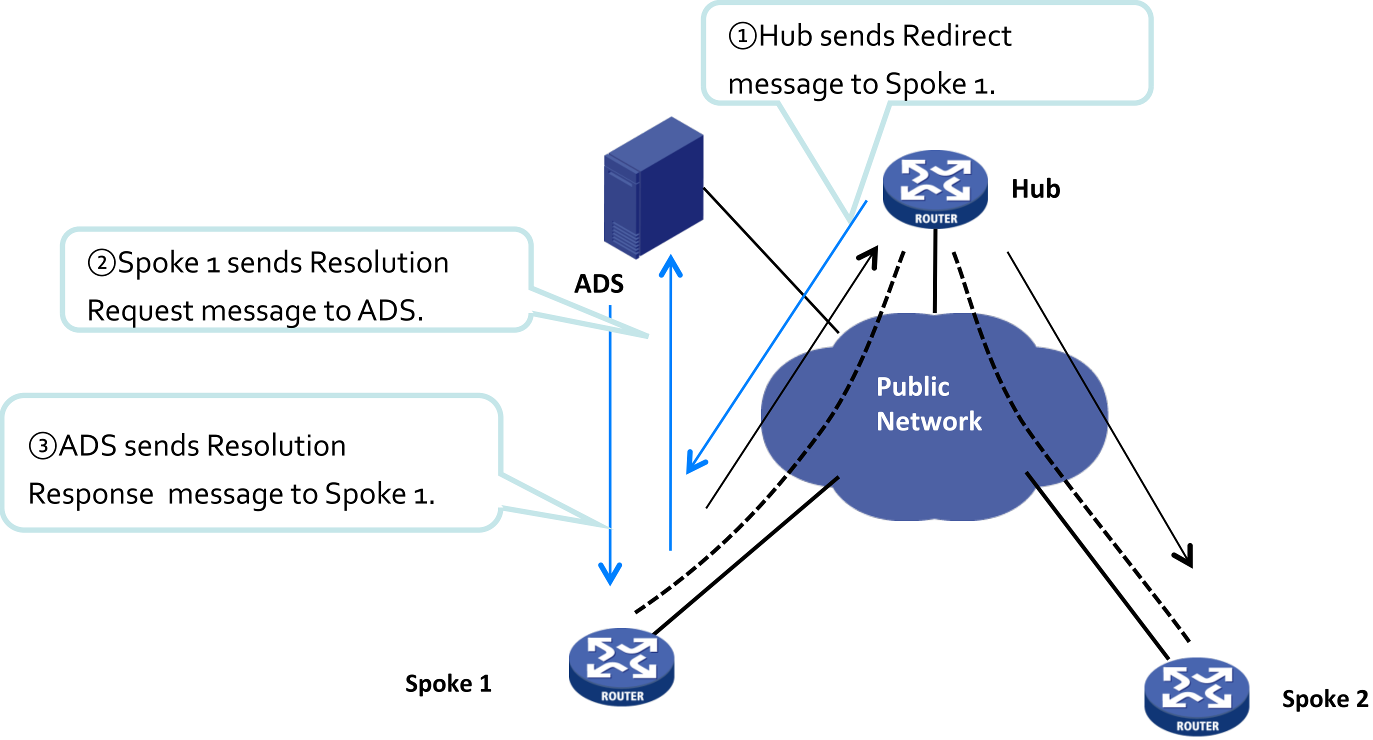


Step 9: Hub sends Redirect message to Spoke 1.

Step 8: Traffic between Spoke1 and Spoke2 is forwarded by Hub.

Resolution

Step10: The source ADVPN peer receives the redirect message, it sends Resolution Request message with destination IP address to ADS. The ADS looks in the ADC information database to find out the next hop to the destination IP address and related network information. The ADS sends a Resolution Response message to the source ADVPN peer.



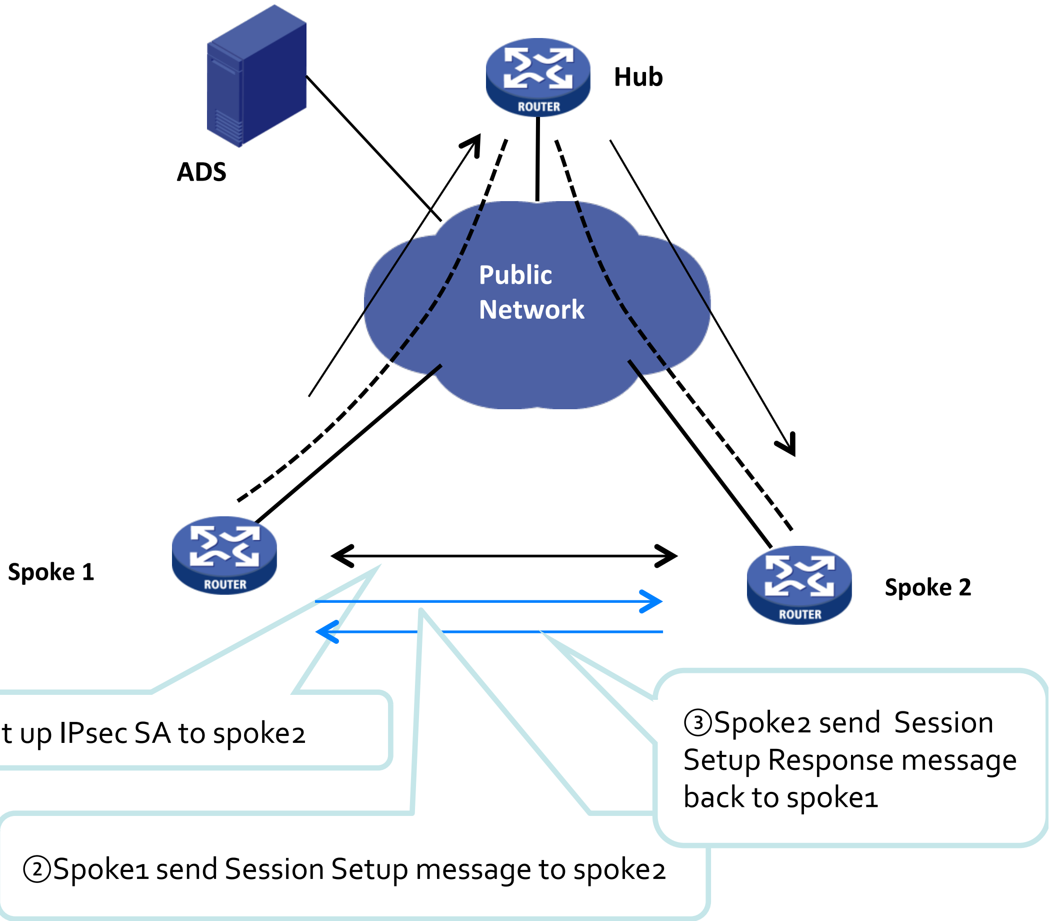
①Hub sends Redirect message to Spoke 1.

②Spoke 1 sends Resolution Request message to ADS.

③ADS sends Resolution Response message to Spoke 1.

Shortcut Path Establishment

Step11 : The source ADVPN peer receives the Resolution Response message. Firstly, a route towards destination network is added into the route table. Secondly, the source ADVPN peer establishes an IPsec tunnel with the destination ADVPN peer. Lastly, the source ADVPN peer send a session message to destination ADVPN peer. The destination ADVPN peer can add the reverse route in its route table and the ADC information in session table.



①Spoke1 set up IPsec SA to spoke2

②Spoke1 send Session Setup message to spoke2

③Spoke2 send Session Setup Response message back to spoke1

NAT Traversal

- All the ADCs and ADS can be located in the NAT box under some restrictions.

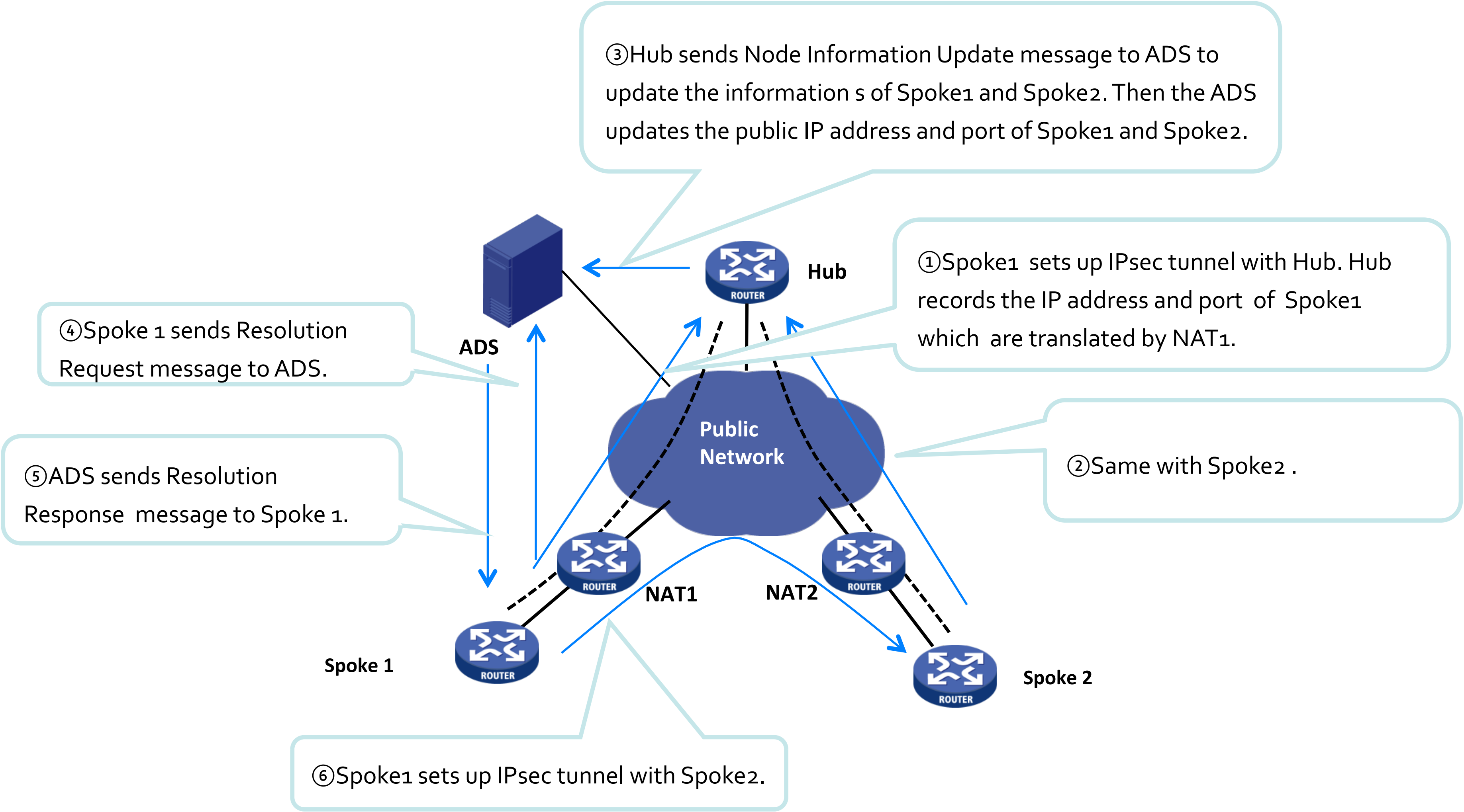
  Restrictions :

  1. The ADS and Hub ADC should be behind the static NAT box.
  2. The NAT box with PAT mode uses the EIM(Endpoint-Independent Mapping) mapping behaviors.

- The NAT box can be No-PAT or PAT(Port Address Translation) mode.

- When the NAT box is PAT mode, the hub ADC updates the source ADC’s IPsec port and address information to ADS, and the spoke ADC can get the ADVPN peer‘s NAT-translated port and address from ADS.

NAT Traversal



①Spoke1 sets up IPsec tunnel with Hub. Hub records the IP address and port of Spoke1 which are translated by NAT1.

②Same with Spoke2 .

③Hub sends Node Information Update message to ADS to update the information s of Spoke1 and Spoke2. Then the ADS updates the public IP address and port of Spoke1 and Spoke2.

④Spoke 1 sends Resolution Request message to ADS.

⑤ADS sends Resolution Response message to Spoke 1.

⑥Spoke1 sets up IPsec tunnel with Spoke2.

IPsec Encryption

IPsec is used to protect the data plane, also can protect the control plane.

- **Works with tunnel protocol : like GRE + IPsec Encapsulation**

  No change to IPsec;

  tunnel encapsulation information is as IPsec selector.

- **Works without any other tunnel protocol : only IPsec Encapsulation**

  small changes:

  1. In the forwarding path of data plane, use the remote public address to find IPsec SA.

  2. IKE traffic selector is ANY port and ANY address on the spoke.

Advantages of the proposal

- Clear separation of control plane and data plane
- Real implementation and deployment of the protocol
- Central ADS controller to implement control and management policy conveniently
- Establish shortcut path only one query from ADS.
- NAT Traverse support – supports all requirements.
- Pure IPsec ADVPN network, no need for the other tunnel protocol encapsulation in the data plane.
- Support for the large scale ADVPN network.