draft-mao-ipsecme-ad-vpn-protocol

Yu Mao (H3C)
ZhanQun Wang (H3C)
Vishwas Manral (HP)
Presented by Mauricio Sanchez (HP)

IETF 87 Berlin

Content

- Work status
- Protocol overview
- Quick compare and contrast
- Next Steps

Work status

In the ADVPN solution, ADVPN protocol defined in this draft uses the IPsec data plane, as well as routing protocols to fulfill the ADVPN function. The ADVPN function can meet the ADVPN requirements defined in the draft-ietf-ipsecme-ad-vpn-problem.

In the current draft, the following requirements have been satisfied: Requirement #1, #2, #3,#4,#5,#6,#7,#10,#11,#14,#16. However, the solution about #8,#9 ,#12,#13, ,#15 is not included in the current proposal as result of "short time", and we will fix it in the next version. The missing contents are about multicast, NAT issue, QoS and some log events.

In the next update, the conformance description for each requirement will also be included in the draft.

ADVPN Protocol Overview

- The ADVPN protocol is a client and server protocol based on HP/H3C DVPN solution and has been successfully deployed in numerous customer sites. However, it has been simplified and optimized to meet the requirements.

- The ADVPN protocol provides the control plane of ADVPN and uses a solution approach and not just a protocol extension approach.

- Complete solution providing not only the shortcut path establishment for the IPsec data path, but also exchange of ADVPN network information, including how routing/ packet forwarding works.

ADVPN Protocol Design Consideration(1)

- Central management and control of connectivity and security policies through ADVPN server (ADS)
- Minimal information overload of the Spoke devices ADVPN Client (ADC - just as much information as necessary).
- Central controller (ADS) configures ADVPN clients SPD and PAD. If the ADVPN client tries to setup an IPsec tunnel with an ADVPN peer, it queries the ADS and obtains the client information of the peer.
- Clear demarcation/ separation between control plane and data plane topology.
- To discover the remote ADVPN peer information, a private IP address (which does not change) is used as the identifier.
- Routing Protocol can run over the IPsec tunnels between the ADCs for exchanging Private IP Routing information . The routing protocol helps distribute routing information to all ADC's towards about the destination network behind the ADCs.

ADVPN Protocol Design Consideration(2)

- The ADC registers its private IP address and public IP address to the ADS. In the medium and large scale ADVPN network, the ADC also registers its private IP address and network behind the ADC to the ADS .

- In the small scale ADVPN network, with routing information exchanged between the hub and spoke , ADVPN network can be full-mesh or partially full-mesh topology. The ADC queries the ADS to obtain the shortcut ADVPN peer by the private IP address.

- In the medium and large ADVPN network, the network is as a hub-and-spoke network initially after routing information exchanged, the traffic from source ADVPN peer to destination ADVPN peer is forwarded to hub first. When needed to establish a shortcut path, the ADC queries the ADS to obtain the shortcut ADVPN peer by the destination IP address.

ADVPN Protocol Model

ADVPN Server - This is an entity as ADVPN network controller. It maintains ADVPN client information database. It also can decide whether the spoke can directly communicate with the other spoke.

ADVPN Client - This is an entity as ADVPN peer. It registers its information to ADVPN server.

ADVPN protocol is implemented between ADC and ADS. All the ADCs register information on the ADS. When the ADC tries to build a shortcut IPsec tunnel with another ADC, it sends a message to ADS to query the information.

ADVPN protocol can also be implemented between ADC and ADC. The ADC sends the Session message to another ADC to transfer ADC information ; The hub ADC sends Redirect message to spoke ADC to trigger the shortcut path query.

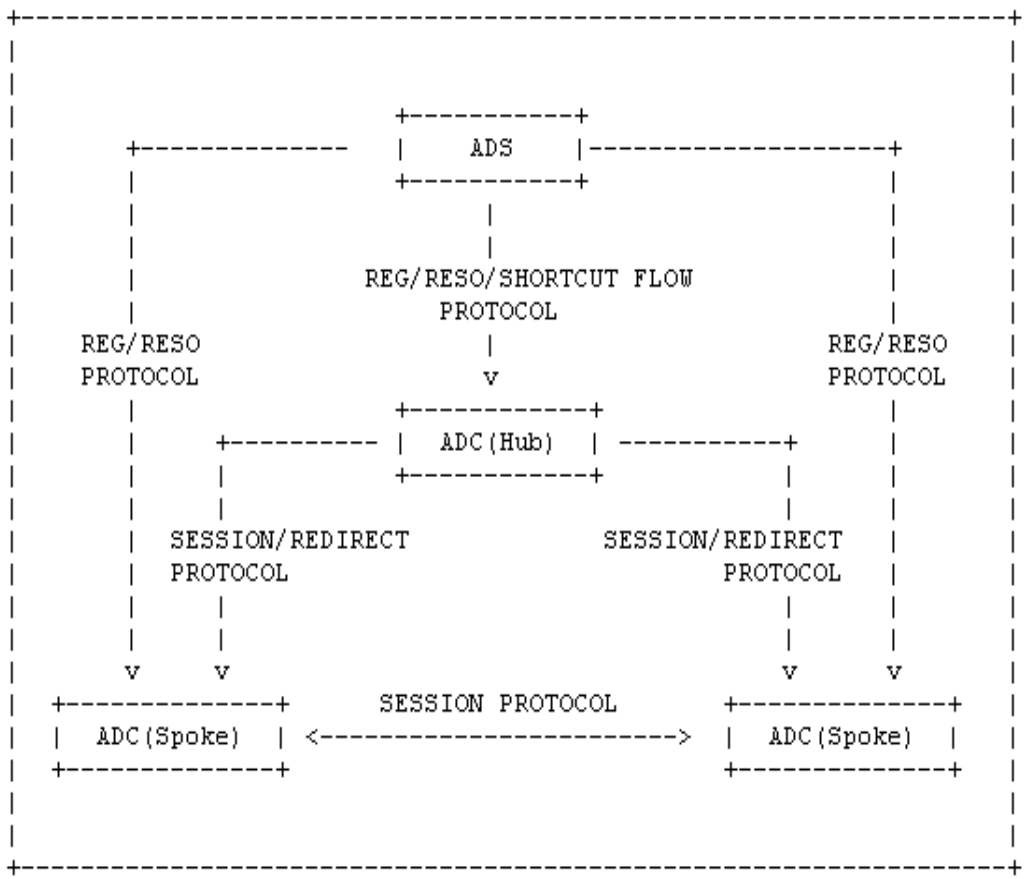


Figure 1. ADVPN Protocol Model

Security Considerations

- The ADVPN protocol has no protocol-internal security mechanism, it relies on other security protocol to protect the ADVPN messages.

- The messages between the ADC and ADS can be protected by the IPsec (or can optionally use SSL/TLS/DTLS). The messages between ADCs are protected by IPsec. Idea being clear separation of the control and data plane.

Notable differences to other ADVPN proposal

1. Solution approach not a small extension to a protocol
2. Clear separation of control and data planes
3. Real-world deployment of protocol
4. Take care of Routing/ NAT security needs to satisfy requirements.
5. Highly scalable solution using an SDN like approach with central ADS controller.

Next Steps

1. Add the content to meet all the requirements, such as multicast, NAT issue , QoS and the log events.
2. Add the conformance description for each requirement.
3. Update by the WG feedback and comments.
4. Submit the -02 draft by the end of August.

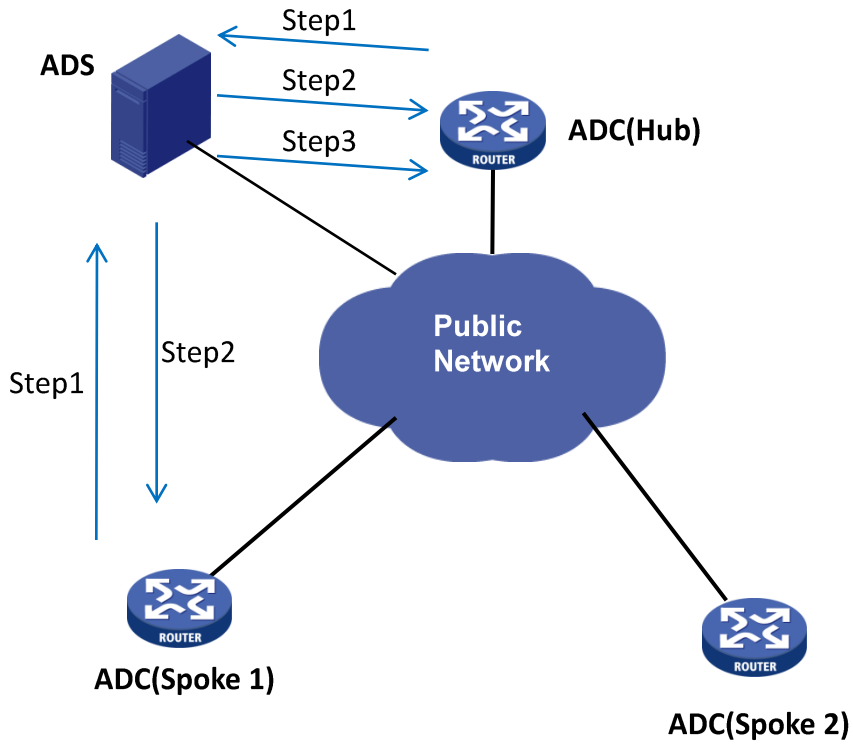
Thank you

How ADVPN Protocol Works

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.

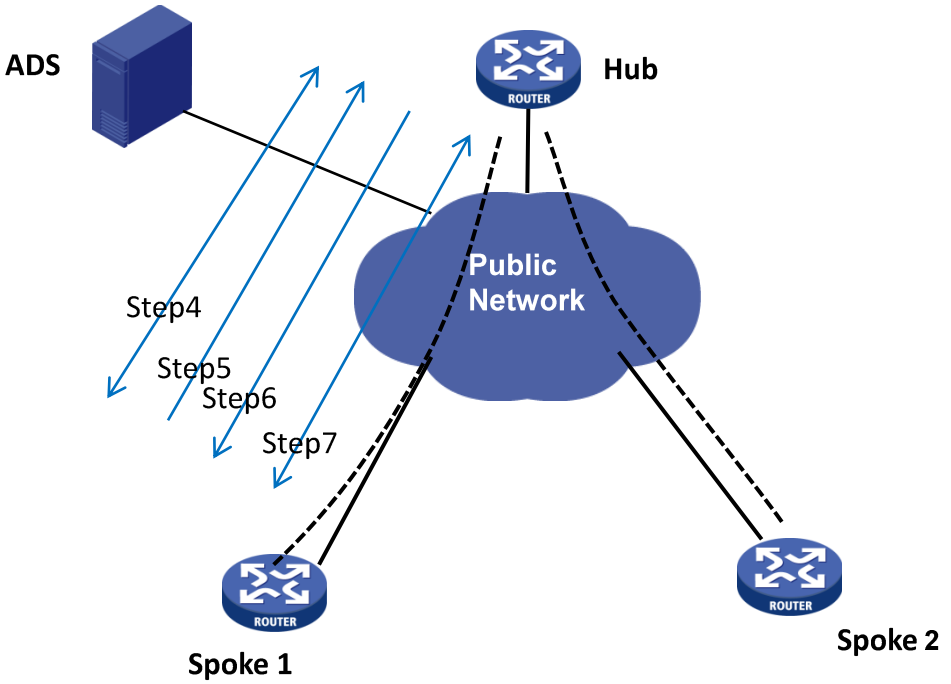


Step4: The spoke ADC obtains the information of hub ADC after registration. The spoke creates the hub session in the session table. After that, the spoke establishes an IPsec tunnel with hub ADC.

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

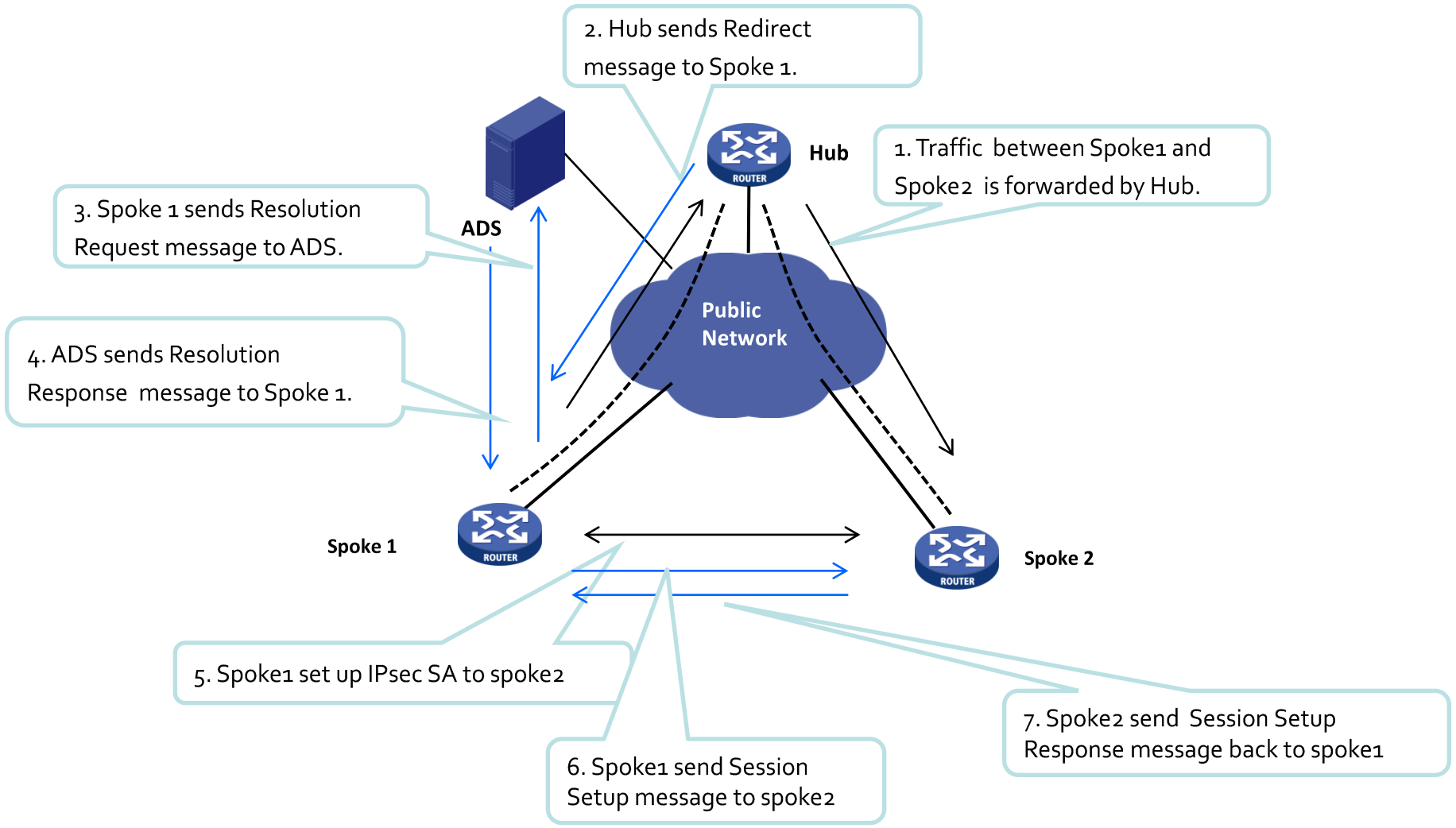


Step 8: When the traffic towards destination ADVPN peer arrives in the source ADVPN peer device, from the routing table, the next hop is the private IP address of hub ADVPN peer. Match the private IP address in the session table to obtain the public IP address of hub ADVPN peer. By the public IP address,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

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.

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.


2. Hub sends Redirect message to Spoke 1.
Hub
1. Traffic between Spoke1 and Spoke2 is forwarded by Hub.
ADS
3. Spoke 1 sends Resolution Request message to ADS.
Public Network
4. ADS sends Resolution Response message to Spoke 1.
Spoke 1
Spoke 2
5. Spoke1 set up IPsec SA to spoke2
6. Spoke1 send Session Setup message to spoke2
7. Spoke2 send Session Setup Response message back to spoke1

Backup: Comparing Against Each ADVPN Requirements

Requirement #1:

In this ADVPN protocol, each ADC only needs to configure its own SPD and SAD. Adding or Removing a ADC from ADVPN topology does not need reconfiguration for each ADC.

Requirement #2:

The ADC registers its public address to ADS, and the other ADC query the ADS to obtain the peer address. Therefore, even the peer address is updated every time , the other ADC can communicate with this ADC without any configuration change.

Requirement #3:

This draft allows the other tunneling protocol and routing protocol running over the spoke-to-hub and spoke-to-spoke IPsec tunnel, and has no additional configuration for those protocols.

Requirement #4:

The ADS decides whether the spoke can be allowed to have a direct communication with other spoke. The control policy is pushed to hub from the ADS after the hub ADC finishes registration on the ADS.

Requirement #5:

The ADVPN Peer should not have wildcard pre-shared-key to be used in the IKEv1 or IKEv2. It is recommended that the certificate is as authentication credential for ADVPN peer.

Requirement #6:

When the endpoint is roaming, it is as a new ADC to join ADVPN network. After registering to ADS again, it connects the new hub. The data traffic can be transferred through new spoke-to-hub IPsec tunnel and spoke-to-spoke IPsec tunnel.

Requirement #7:

The all hub ADCs is managed by ADS, if the hub ADC changes, the new hub ADC' information will be pushed to the spoke ADCs, and new IPsec tunnel is established between the ADC and new hub ADC. The traffic is migrated from one gateway to another gateway.

Requirement #8:

In this draft, all the ADVPN peer can be located behind NAT boxes. The ADS can obtain the modifying IP address or port of spoke ADC from hub ADC, therefore, even two spoke are both behind NAT boxes, they can also establish the direct connectivity.

Requirement #9:

This draft will define some events that can be reportable next version, such as: a new IPsec SA establishment, a shortcut route injected into the routing table etc. This draft does not create a MIB.

Requirement #10:

This draft does not have any restriction that the ADVPN peer from different organization can connect to each other.

Requirement #11:

The ADS is the controller of ADVPN network. The administrator can configure the control policy on ADS to determine the ADVPN network is a Star, Full mesh or a partial full mesh topology.

Requirement #12:

The ADVPN protocol can cooperated with IGMP and PIM to provide multicast function. The ADC information includes multicast group. Multicast traffic is replicated to selective ADC.

Requirement #13:

This draft will define some events that can be logged and monitored next version. These event is almost the same as for Requirement #9.

Requirement #14:

When L3VPN operate over IPsec tunnel, GRE or other tunnel protocol can be transport-link protocol. These tunneling protocols can run over the spoke-to-hub and spoke-to-spoke IPsec tunnel in ADVPN network.

Requirement #15:

The ADC can register its QoS policy information to ADS, and when the other ADC query the ADC's information, it can obtain the related QoS policy information.

Requirement #16:

In the ADVPN solution, the administrator can specify more than one hub in the ADS for the ADC. The ADC gets all the hub ADC information after registration and establishes IPsec tunnel with each hub ADC.