AR Feature Description-A2A VPN

Issue v1.0

Date December-09-2013

Contents

List of Tables

A2A VPN

About This Chapter

1.1 Introduction

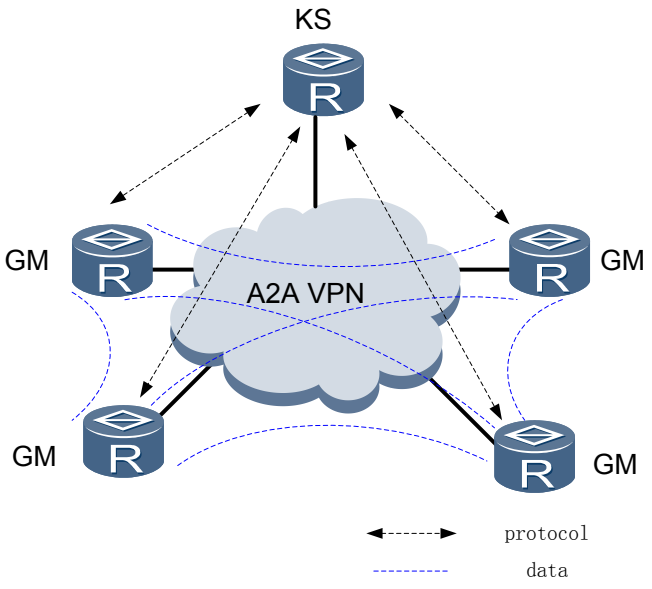
Definition

A2A VPN is the abbreviation of Any to Any VPN. It is a VPN technology solution in the use of GDOI (Group Domain of Interpretation) protocol.

Purpose

Distributed computing, voice, video and other services needed to run anywhere between branches, Hub-Spoke and peer IPSec tunnel solution in the traditional sense do not meet the needs of users. GDOI protocol proposed KS (Key Server) and GM (Group Member) of the group encryption deployment model. The entire network consultates Group SA, using Group SA to encrypt and decrypt traffic between nodes, to make IP secure communications between any nodes possible. A2A VPN network is shown in Figure 1-1.

Figure 1-1 A2A VPN network structure



Benefits

- Compared with traditional VPN, A2A VPN deployment without changing the original route, the traffic is routed directly between nodes forwarding, seamless integration with multicast technology.

- A2A VPN uses Group SA to encrypt and decrypt the data traffic between nodes without tunnel creation, it simplifies network deployment and enhances the network security of data transmission services.

1.2 References

Document	Description	Remarks
RFC6407/RFC3547	The Group Domain of Interpretation	

1.3 Availability

Involving Network Element

Key Server, Group Member, and other enterprises export routers.

Version Support

Product	Version
AR	V200R007

Feature Dependency

- A2A VPN is used in enterprise private networks, companies generally use to build enterprise private network by MPLS technology.
- A2A VPN multicast SA Rekey depends on the multicast tree constructed by PIM, IGMP multicast protocols. When you enable multicast SA Rekey feature, Key Server and Group Member must be the corresponding network node of multicast domain, to ensure GM can receive multicast Rekey message from KS.
- A2A VPN general uses ACL to define network traffic policy to set specified traffic data encrypted by IPSec.
- A2A VPN supports VRF multi-instance.

Hardware Support

None

1.4 Principle Description

1.4.1 GDOI Protocol

Contents

GDOI protocol defines the interaction between KS and GM distribution group policies and group keys. It includes two phases: IKE negotiation and GDOI negotiation.

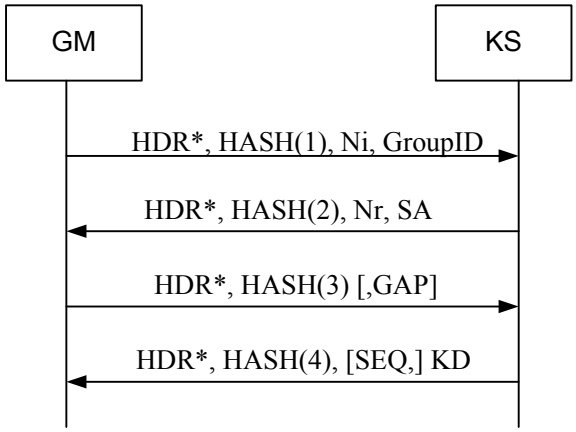
Phase I includes IKE negotiation: GM and KS negotiation with each other, and confirm the Identity. After authentication, it will generate a IKE SA to protect the process of GDOI negotiation.

Phase II includes GDOI negotiation: GDOI negotiation includes GROUPKEY-Pull register exchange protocol and GROUPKEY-PUSH Rekey exchange Protocol.

- Using GROUPKEY-PULL register exchange protocol, GM negotiation finishes identity registration and downloading of KEK SA, TEK SA and traffic policies.
- Starting GROUPKEY-PUSH Rekey exchange protocol repeatedly, KS finishes updating Group SA members.

GROUPKEY-PULL register exchange protocol

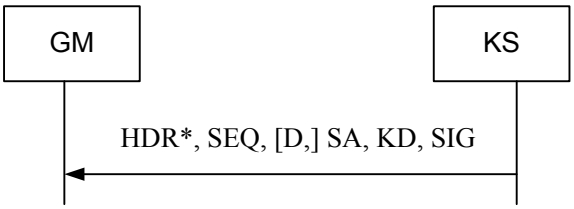
GROUPKEY-PULL interaction is protected by IKE SA. The interaction is showed as following figure:



1. GM sends GDOI messages to KS. It wants to get Group Id that administrator configures.
2. KS analysis and identify the message. KS gets the Group ID and identify whether it has the corresponding Group ID. KS will generate response message after identifying.
3. GM analysis and identify the message from Key server. It analysis the SA payload and get the information of security algorithm. GM generates the response message and answers the KS.
4. KS analysis and identify the GM messages. KS generates KEK SA and TEK SA Secret-key material to GM.
5. GM analysis and identify the message from KS. GM saves the KEK SA and uses it to decrypt the GROUPKEY-PUSH Rekey exchange message. GM also uses it to encrypt and decrypt the data traffic.

GROUPKEY-PUSH Rekey exchange protocol

GROUPKEY-PUSH interaction is protected by KEK SA. The interaction is showed as following figure:



1. Once KS configuration is changed or Key is timeout, KS will generate the Rekey message and notify GM updated the key materials.

   Rekey message will use private key to signature the message.

   GM receives the KS message, then saves the KEK SA and TEK SA.

1.4.2 Group Member

GDOI Policy Configuration

- GM supports to assign the Phase I IKE negotiation parameters. It coordinates with KS and finishes the Phase I IKE SA negotiation.
- GM supports assigning Group ID. The assigned ID need to correspond with KS.
- GM support assigning local ACL policy. It needs adjust GROUP SA encrypt and decrypt policy according the traffic characteristics.
- GM supports assigning packet-forwarding mode. GM need adjusting the packet process methods according the packet-forwarding mode.

GDOI Negotiation

- GM processes the Phase II IKE SA negotiation.
- GM starts GROUPKEY-PULL register exchange protocol. After Phase I IKE negotiation, it sends GDOI registration to KS.
- GDOI registration process is protected by phase I IKE SA. After GDOI registration, GM get KEK SA, TEK SA and KS configuration policy.
- GM uses TEK SA to forward the packet security.

GM Re-registration

- GM starts GROUPKEY-PULL exchange before TEK SA is timeout in 60 seconds, and GM re- register.
- GROUPKEY-PULL is protected by KEK SA. Once KEK SA does not exist, GM will restart Phase I IKE negotiation.
- Before TEK SA is timeout in 30 seconds, GM will use new TEK SA to encrypt and decrypt the packets.

Unicast Rekey

- GM responses KS's Unicast Rekey message, and updates local KEK SA and TEK SA.
- GM generates Rekey ACK message and responses KE's Rekey message.
- Before GM's TEK SA is timeout in 30 seconds, it uses new TEK SA to encrypt and decrypt the packets.

Multicast Rekey

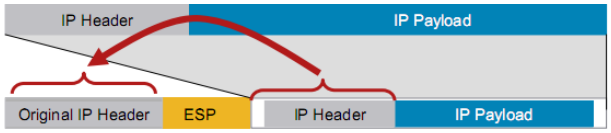
- GM response KS multicast Rekey message, and updates local KEK SA and TEK SA.
- Before TEK SA is timeout in 30 seconds, it uses new TKE SA to encrypt decrypt the packets.

GM Fast-leave

Once GM receive Rekey message, it will reduce SA lifetime, and fulfill GM SA fast-leave and re-registration.

Packet encryption and decryption

GM uses original source and destination address as new IP header. And GM uses original payload to ESP security exchange by Group SA. It shows as following figures:



Packets forwarding exchange supports three modes:

- Receive Only Model: GM send plain-text and receives cipher-text and plain-text.
- Receive Option Model: Once local configuration is received option, GM sends cipher text and receives plain-text and cipher-text.
- Normal Model: GM only sends and receives Cipher text.

1.4.3 Key Server

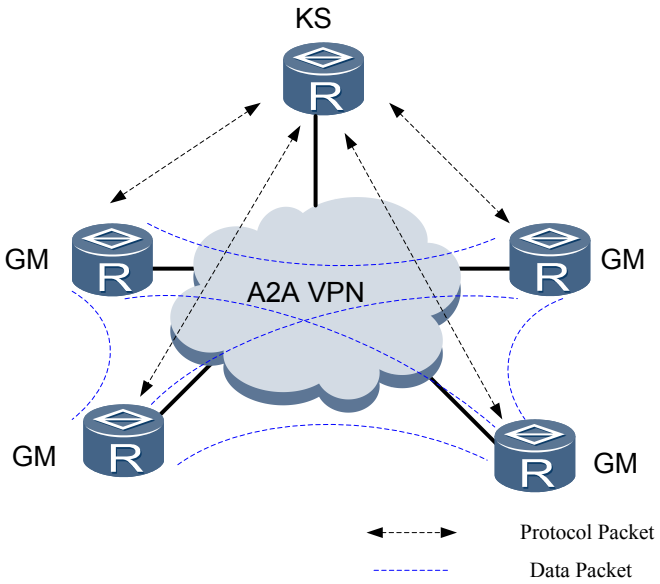
AR can do as GM and it can interconnection with Cisco's Key server.

1.5 Application

1.5.4 Unicast RekyA2AVPN Deployment

As shown in figure**Error! Reference source not found.**, A2AVPN is built in enterprise network to implement the security protection of unicast traffic between different subnets.

图1-1 Unicast RekyA2AVPN Deployment



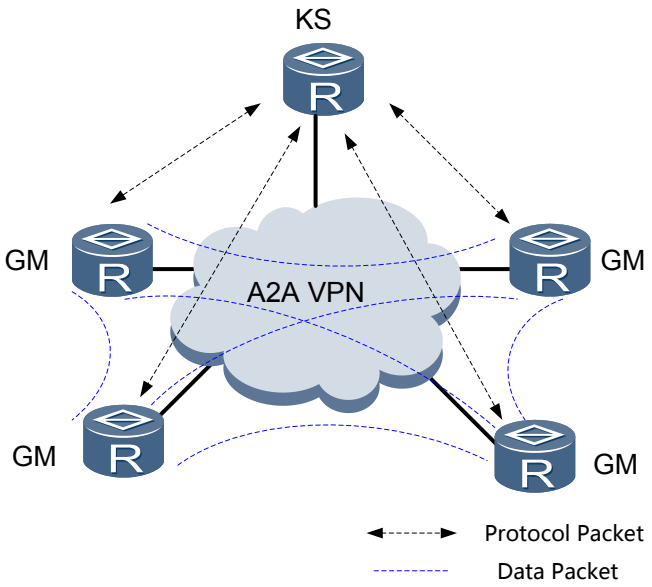
Procedure:

1. Configure A2A VPN on KS
2. Configure A2A VPN on GM
3. GMs register on KS
4. GM send unicast Rekey to Key Server and update Group SA
5. Traffic between GMs are securely transmited with Group SA

1.5.5 Multicast RekyA2AVPN Deployment

As shown in figure**Error! Reference source not found.**, A2AVPN is built in enterprise network to implement the security protection of multicast traffic between different subnets.

图1-2 Multicast RekyA2AVPN Deployment



Procedure:

1. Configure A2A VPN on KS
2. Configure A2A VPN on GMs
3. GMs register on KS
4. GMs send multicast Rekey to Key Server and update Group SA
5. Traffic between GMs are securely transmited with Group SA

1.6 Influence

1.6.6 Influence on System Performance

None

1.6.7 Influence on Other Features

None

1.6.8 Other Defects

None

1.7 Terms and abbreviations

Table1-1 Abbreviations

Abbreviation	Full Name
IKE	The Internet Key Exchange

ISAKMP	The Internet Security Association and Key Management Protocol
IPSec	The Internet security protocol
GDOI	The Group Domain of Interpretation
A2A VPN	Any to Any VPN
SA	Security Association
KEK	Key Encryption Key
TEK	Traffic Encryption Key