技术介绍

ADVPN

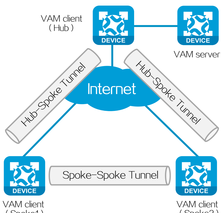
Auto Discovery Virtual Private Network

简介

ADVPN（Auto Discovery Virtual Private Network，自动发现虚拟专用网络）是一种基于VAM（VPN Address Management，VPN地址管理）协议的动态VPN技术。其核心思想是VAM client从VAM sever获取目标VAM client的公网地址，自动建立Hub-Spoke永久隧道以及Spoke-Spoke动态隧道。Spoke-Spoke隧道仅在Spoke之间有数据交互时建立，当Spoke之间没有数据交互时，自动删除隧道，从而避免设备维护大量闲置的隧道表项，有效地提高了设备资源的利用率。

- VAM server：负责收集、维护和分发VAM client的私网地址和公网地址的对应关系。
- VAM client：自动向VAM server注册自己的私网地址和公网地址的对应关系。
- Hub：ADVPN网络的中心设备，通常是企业总部的网关。
- Spoke：ADVPN网络的分支设备，通常是企业分支机构的网关。

本文仅以同一ADVPN域同一个Hub组组网环境为例介绍ADVPN技术。



技术亮点

动态地址接入

在企业分支机构使用动态地址接入公网的环境中，ADVPN可以感知公网地址的变化，在各分支机构之间以及分支与总部之间自动建立VPN隧道。

分支间直接互联

传统的VPN隧道多为总部与分支之间的点到点连接，分支间的通信必须经过总部转发，增加了总部设备的负担。ADVPN可在分支之间直接建立隧道，有利于减轻总部设备的负担和提高分支间的通信效率。

IPsec深度保护

ADVPN支持与IPsec深度融合，借助IPsec的加密和认证技术，可为ADVPN隧道传输数据提供可靠的安全防护。

配置和维护简单

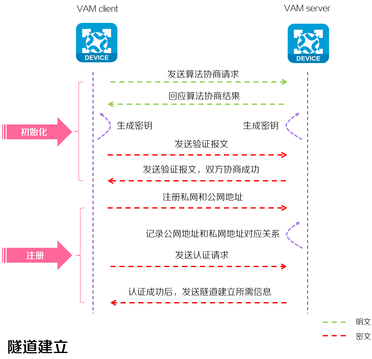
ADVPN支持动态路由协议，管理员只需要简单配置，即可快速实现VAM client之间私网的互通。

运行机制

ADVPN网络的建立过程包括以下步骤：初始化、注册、隧道建立、路由学习。初始化阶段可为注册阶段传输的报文提供加密及认证保护。注册完成后，当有数据需要传输时VAM client之间将建立隧道，并完成路由学习，最后转发报文。

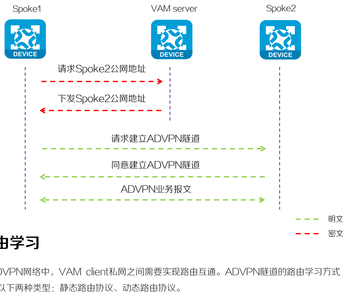
初始化 & 注册

初始化阶段VAM client和VAM server之间协商加密和认证的算法和密钥；注册阶段VAM client向VAM server注册自己的私网地址和公网地址的对应关系。



隧道建立

隧道建立阶段，Hub与Spoke之间将建立永久隧道，Spoke与Spoke之间建立流量触发的动态隧道。本文仅以Spoke-Spoke隧道为例详细介绍隧道的建立过程。如下图所示，Spoke通过VAM server获取对端Spoke的公网地址，从而建立跨越Internet的隧道。



路由学习

在ADVPN网络中，VAM client私网之间需要实现路由互通。ADVPN隧道的路由学习方式包括以下两种类型：静态路由协议、动态路由协议。

静态路由协议	动态路由协议
◆ 适合小型组网 ◆ 需要手工配置	◆ 适合大型组网 ◆ 部署简单

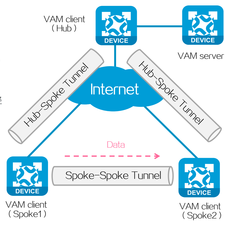
组网模式

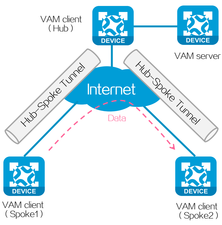
Full-Mesh网络

Full-Mesh（全互联）网络是指，Spoke和Spoke之间可以直接建立隧道进行通信，不需要经过Hub转发。

Full-Mesh模式具有如下特点：

- Spoke之间的流量不需要经过Hub转发，从而减轻了Hub的压力。
- Spoke之间直接通信，数据传输效率较高。
- Spoke需要管理动态建立的隧道表项，因此对Spoke设备的处理能力有较高要求。





Hub-Spoke网络

Hub-Spoke是指，Spoke和Spoke之间不可以直接建立隧道进行通信，必须经过Hub转发。

Hub-Spoke模式具有如下特点：

- Spoke之间的流量需要经过Hub转发，因此对Hub设备的处理能力有较高要求。
- Spoke之间通过Hub通信，数据传输效率较低。
- Spoke无需管理动态建立的隧道表项，从而减轻了Spoke的压力。