# V7 NGFW SSLVPN实现方式咨询

SSL VPN　王英凯　2023-09-11 发表

## 问题描述

如题，SSL VPN有哪些实现方式?

## 解决方法

适用的产品系列：防火墙M9000系列、M9000-S系列、M9000-X系列、M9000-AI系列、F50X0-D系列、F5000系列、F5000-CN系列、F1000-AK系列、F1000-AI-X系列、F1000-X-G5系列、F1000-X-G2系列、F1000-V系列、F100-WiNet系列、F100-X-G3系列、F1000-C-X系列、F1000-X-XI系列、F100系列、vFW系列、F5000-AK系列、F5000-AI系列、F1000系列、F1000-L系列、F1000-SASE系列、F1000-X-G3系列、F1000-9X0-AI系列、F1000-7X0-HI系列、F100-X-G5系列、F100-X-G2系列、F100-X-XI系列、F100-C-A系列、F1000-T、F1000-K系列。

SSL VPN接入主要有IP资源、WEB资源、TCP资源，目前我司主要使用的方式是IP资源接入。

**1、IP接入方式的总体流程**

IP接入方式用来实现远程主机与企业内部服务器网络层之间的安全通信，进而实现所有基于IP的远程主机与服务器的互通。

用户通过IP接入方式访问内网服务器前，需要安装专用的IP接入客户端软件，该客户端软件会在SSL VPN客户端上安装一个虚拟网卡。H3C通过iMC iNode软件来实现。

IP接入方式下，管理员在SSL VPN网关上创建SSL VPN接入接口，并配置下发给SSL VPN客户端的路由表项。

如图1所示，IP接入方式实现过程如下：

(1) 用户在客户端上安装IP接入客户端软件后，启动该软件并登录。

(2) SSL VPN网关对其进行认证和授权。认证、授权通过后，SSL VPN网关为客户端的虚拟网卡分配IP地址，并将授权用户访问的IP接入资源（即路由表项）发送给客户端。

(3) 客户端为虚拟网卡设置IP地址，并添加路由表项，路由的出接口为虚拟网卡。

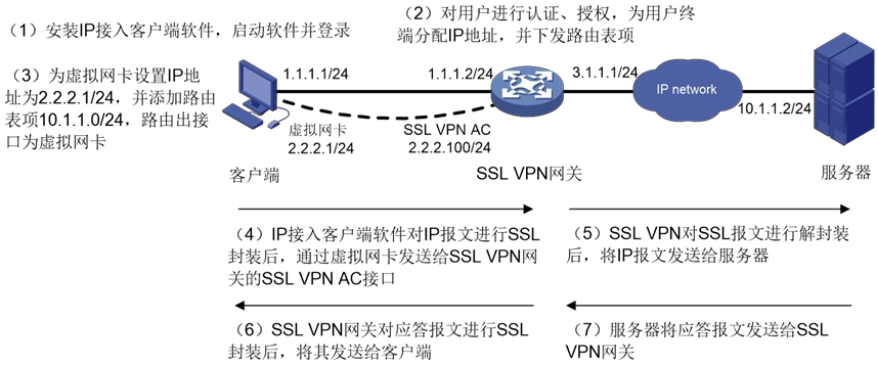
(4) 用户在客户端上访问企业内网服务器时，访问请求报文匹配添加的路由表项，该报文将进行SSL封装，并通过虚拟网卡发送给SSL VPN网关的SSL VPN AC接口。

(5) SSL VPN网关对SSL报文进行解封装，并将IP报文转发给内网服务器。

(6) 内网服务器将应答报文发送给SSL VPN网关。

(7) SSL VPN网关对报文进行SSL封装后，通过SSL VPN AC接口将其发送给客户端。

图8 IP接入方式示意图




**2、IP接入方式的报文封装过程**

如图2所示，以客户端访问内网DNS服务器举例。IP接入方式下，DNS应用程序访问内网DNS服务器的源IP地址为，SSL VPN网关为其分配的虚拟网卡IP地址。当用户访问内网DNS服务器时，客户端通过查找路由表，封装DNS访问请求报文，该报文外层将进行SSL加密封装，并发送至SSL VPN网关。SSL VPN网关通过SSL解密，还原DNS请求，并转发至DNS服务器。内网DNS服务器接受到SSL VPN网关的DNS请求后，将DNS应答发送至SSL VPN网关。SSL VPN网关通过SSL加密连接将DNS应答发送至IP接入客户端。

图9 IP接入方式报文封装示意图


客户端
IP network
SSL VPN 网关
DNS服务器