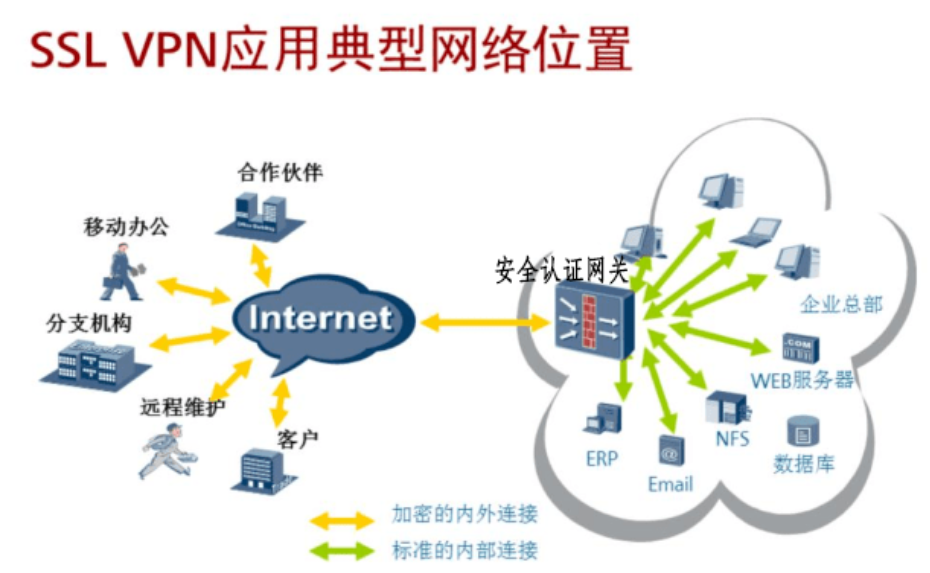
安全接入网关需求分析

# 概念

安全认证网关是采用数字证书为应用系统提供用户管理、身份鉴别、单点登录、传输加密、访问控制和安全审计服务的产品。安全认证网关的部署模式分为物理串联和物理并联两种方式：

物理串联：指从物理网络拓扑上，用户必须经过网关才能访问受保护的应用；

物理并联：指从物理网络拓扑上，用户可以不经过网关就访问到受保护的应用，可以由应用或防火墙上进行某种逻辑判断，来识别出未经网关访问的用户（比如通过来源IP），以达到逻辑上串联的效果



SSL VPN网关多部署于企业的网络出入口，应用服务器之前，介于远程用户和服务器之间，控制两者的通信。实现内部网络的安全访问，使得来自外网的请求可以访问内网的资源。

# 术语解释

VPN: Virtual Private Network，[虚拟专用网络](https://baike.so.com/doc/5351399-5586857.html" \t "_blank)

VPN客户端：在用户端（客户端）使用的vpn软件，与vpn服务端通信，完成相关策略的实现、路由转发等。

VPN服务端：在网关设备中启动的vpn软件，与vpn客户端通信，完成相关策略实现、路由转发等。

VPN配置管理工具：网关设备的配置管理工具，正常情况下通过与网关内网网口直连的方式访问该配置管理工具，实现用户管理配置、相关访问策略的配置等。

# 网关硬件配置

硬件要求：至少具备2个工作网口，分别为内网接口和外网接口。还应提供一个管理接口，可以是网口或串口与管理设备连接。

以东进设备为例，下图为东进网关设备后视图

1. USB接口，2个（上：USB 2；下：USB1）

2.COM接口，管理口：可对 VPN网关设备进行配置

3. LAN1接口，业务口：与 Internet 接入设备相连接，做VPN的外网口

4. LAN2 接口，业务口：与 Internet 接入设备相连接，做IPSEC VPN的外网口

5. LAN4 接口，业务口：与内部局域网相连接，做SSL 和IPSEC VPN的内网口

6. LAN8接口，管理口：可对 VPN网关设备进行配置

# 安全认证网关软件配置

## 软件组成

安全认证网关软件分为如下三个部分。

其中：

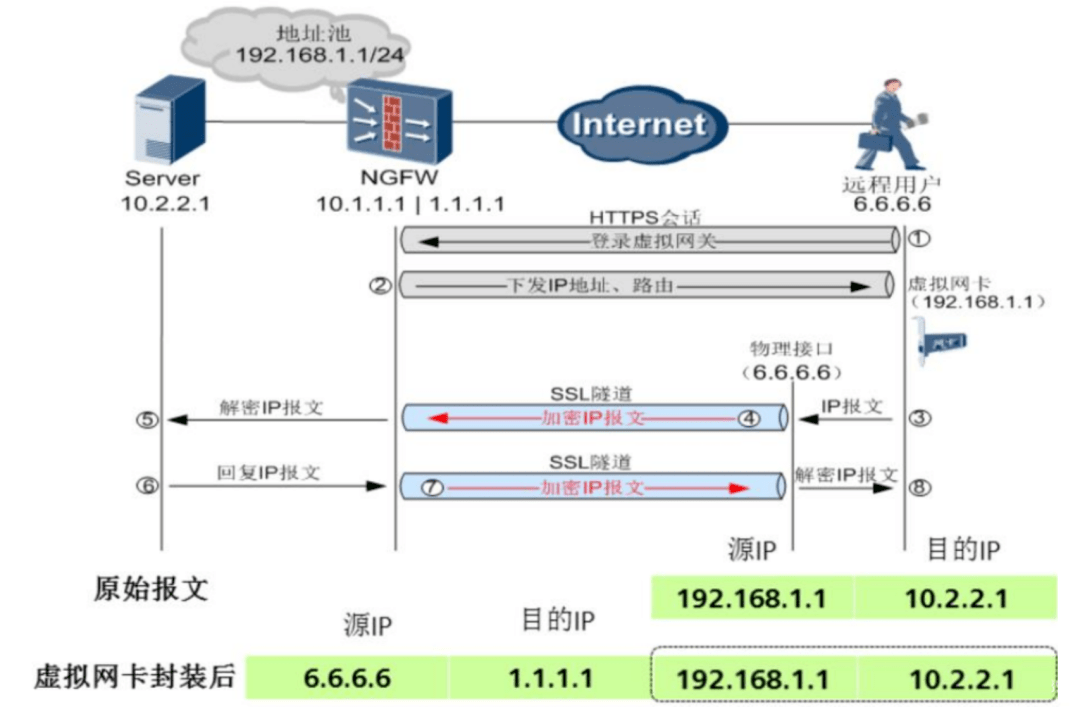
VPN客户端：完成客户端系统自检、VPN系统登录、虚拟网卡路由、用户策略查询等功能。

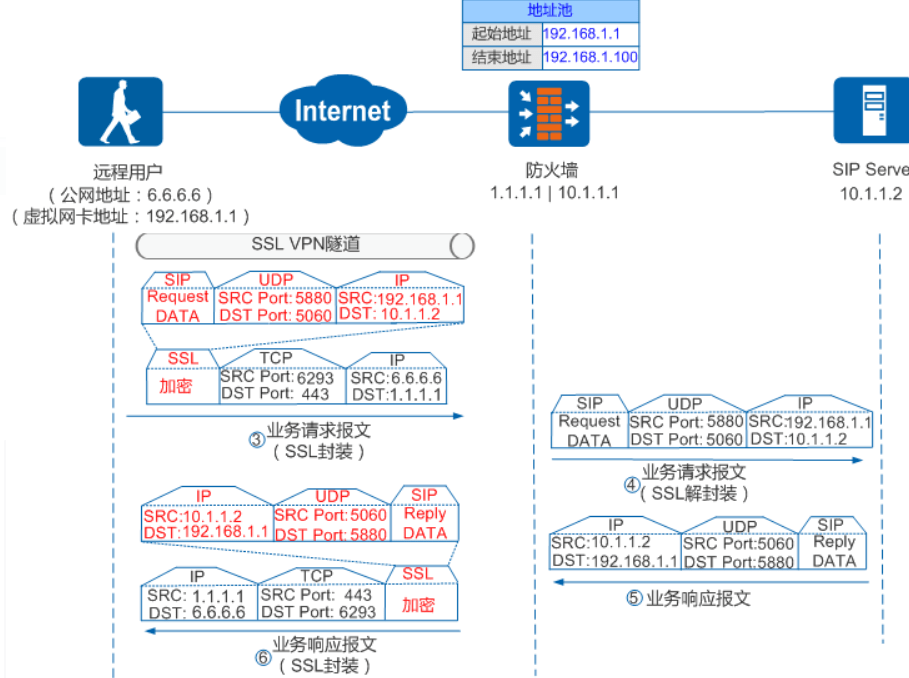
VPN服务端：完成客户端的身份认证，相关用户策略的实现。

配置管理工具：完成网关的配置，包括用户配置、证书配置、策略配置等等。

## 数据链路图

如上图的应用场景中，数据链路如下所示





数据链路说明：

因为虚拟网卡的优先级高于物理网卡，所以请求数据会优先使用虚拟网卡。

用户登录VPN客户端后，SSL VPN即已成功建立。

用户发送请求：用户浏览内网应用时，https请求先经由虚拟网卡进行一次封装，再由虚拟网卡经由物理网卡实际发出到安全认证网关，请求由安全认证网关的外网网口进入后，经由虚拟网卡（vpn服务端程序）解析，如果满足网关配置中配置的用户策略，则将该请求通过安全认证网关的内网网口转发到内网代理服务器，再由内网代理服务器分别路由到各个内网业务系统。

用户请求响应：业务系统的请求返回信息，先经由代理服务器到达安全认证网关的内网网口，再经由虚拟网卡（vpn服务端）进行一次封装后，通过安全认证网关的外网接口发出，同样，在客户端接收时，先经由物理网卡处理后，再通过虚拟网卡（VPN客户端）反馈到应用层程序（如浏览器）。

1. 用户打开vpn客户端，选择用户名和密码的登陆方式或者Ukey登陆方式，登陆vpn系统。登陆时先进行客户端主机安全检查（杀软、防火墙、系统补丁以及），包括需进行身份认证，登陆成功后，从vpn服务端获取相关配置策略参数，并显示。
2. 用户打开浏览器，输入要访问的内网网址，浏览器发送访问请求到虚拟网卡，由vpn客户端控制，在虚拟网卡层对发送数据进行封装、过滤后经由物理网卡发送到安全应用网关。
3. 安全应用网关接收到数据后，解析出虚拟网卡地址，与管理策略中的路由表进行匹配，匹配成功后，路由到业务系统真实网址

# 管理工具配置

通过网关管理口直连后，访问网关出厂IP，根据出厂设置的用户名和密码登陆网关配置管理工具。

在配置管理工具中，

1. 增加用户（VPN客户端），为每个用户分配用户名和密码以及数字证书等，用于用户身份认证。
2. 为每个用户分配可访问策略，比如添加应用，为每个应用设置用户或用户组的访问权限等。

配置管理工具的需求及功能由java端确定及实现。

# VPN客户端

## VPN客户端流程



## VPN客户端模块结构

# VPN服务端