SSL VPN 技术白皮书

目录

1 概述

1.1 产生背景

随着互联网的日益普及，用户可以随时随地接入网络资源。对于企业而言，分支机构及出差员工快速、便捷地通过远程接入 VPN 技术实现远程办公，成为迫切的需求。

传统的 VPN 技术，诸如 IPsec、L2TP 等虽然满足远程接入需求，但是随着网络资源的不断多元化，企业需要针对特定的资源进行用户管理和访问权限控制，此类 VPN 技术难以满足企业的需求。为了解决以上问题 SSL VPN 技术应运而生。SSL VPN 使用简单，任何安装浏览器的终端均可以使用。SSL VPN 还具有丰富的资源访问控制功能，可以基于用户进行管理，并为用户提供不同类型的资源访问需求。

SSL VPN 是以 SSL（Secure Sockets Layer，安全套接字层）为安全基础的远程接入 VPN 技术，可以提供远程的安全连接服务。

1.2 技术优点

相比传统的 IPsec、L2TP 等 VPN 技术，SSL VPN 具有以下优点：

- 操作简单，用户无需安装任何客户端软件，直接使用 Web 浏览器即可安全、便捷地访问企业内网资源。
- 基于用户或用户组对用户进行权限管理，不同的用户或用户组对内网资源有着不同的访问权限。基于用户进行权限控制，更加简单和方便。
- 支持三种接入方式，满足不同用户的访问需求。通过为用户分配不同方式的资源，对用户访问资源的权限进行高细粒度的控制。
- 提供丰富的用户认证方式，包括用户名密码认证、证书认证、企业微信认证等，且各种认证方式可以组合使用，保证合法用户安全接入 SSL VPN。
- 支持各种应用协议。SSL 位于传输层和应用层之间，任何一个应用程序都可以直接享受 SSL VPN 提供的安全性。
- 支持多种操作系统。SSL 协议已被集成到大部分的浏览器，如 IE、Chrome、Firefox 等。这就意味着几乎任意一台装有浏览器的计算机都支持 SSL 连接。任何支持 SSL 协议的操作系统，均可以运行 SSL VPN 客户端。
- SSL VPN 的部署不会影响现有的网络拓扑结构。SSL 协议工作在传输层之上，不会改变 IP 报文头和 TCP 报文头，因此，SSL 报文对 NAT 来说是透明的；SSL 固定采用 443 号端口，只需在设备上打开该端口，不需要根据应用层协议的不同来修改设备上的设置，不仅减少了网络管理员的工作量，还可以提高网络的安全性。

2 技术实现

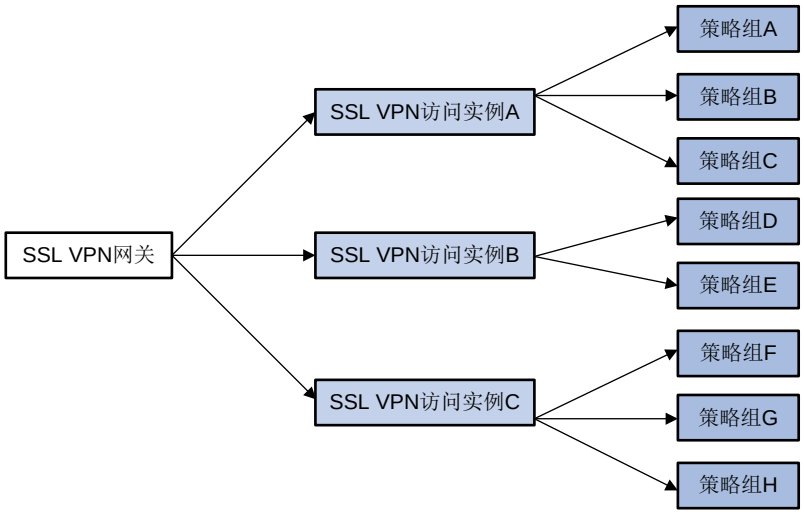
2.1 SSL VPN基本概念

SSL VPN 基本概念如下：

- SSL VPN 网关：提供 SSL VPN 服务的网络设备，位于客户端与内网服务器之间，用于转发用户的访问请求，并为用户提供可访问的内网服务器资源。
- SSL VPN 访问实例：用来管理用户会话、用户认证方式以及用户可以访问的资源等。
- SSL VPN 策略组：策略组是内网资源的集合，用于关联用户可以访问的资源，是用户和访问资源之间的桥梁。当 SSL VPN 用户被授权某个策略组后，该策略组引用的资源将被授权给用户访问。

如图 1 所示，SSL VPN 网关上可以创建多个访问实例，在访问实例中创建策略组，通过策略组关联不同的访问资源。SSL VPN 网关将特定的策略组授权给用户后，该用户将能够访问特定的资源。

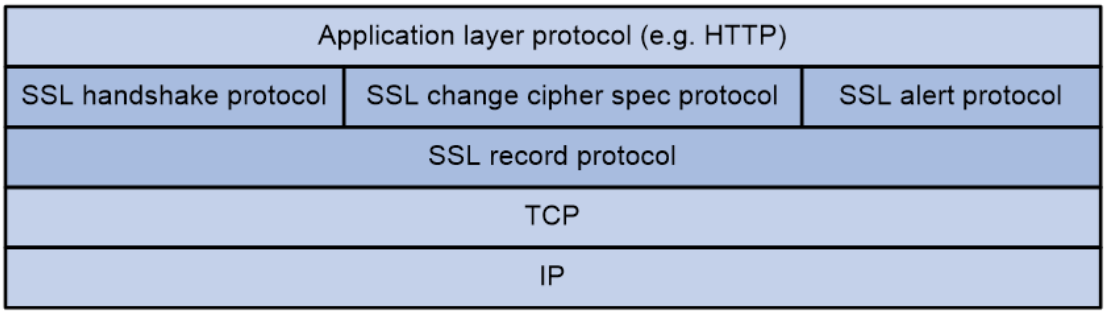
图1 SSL VPN 基本概念示意图



2.2 SSL协议基本原理

SSL VPN 的实现基础是 SSL 协议。SSL 协议在 TCP/IP 协议栈中位于传输层和应用层之间，可为基于 TCP 的应用层协议（如 HTTP 协议）提供安全连接服务。经过 SSL 协议加密后的 HTTP 协议称为 HTTPS，HTTPS 是目前最常用的应用层安全协议。实际应用中，HTTPS 可为网页浏览、电子邮件、即时通讯以及其它的数据交互提供可靠的安全保障。

图2 SSL 协议示意图



如图 2 所示。SSL 协议可以分为两层：

- 上层协议：SSL 握手协议（SSL Handshake Protocol）、SSL 密码变化协议（SSL Change Cipher Spec Protocol）和 SSL 告警协议（SSL Alert Protocol）。
- 下层协议：SSL 记录协议（SSL Record Protocol）。

SSL 上层协议：

- SSL 握手协议：用来协商通信过程中使用的加密套件（数据加密算法、密钥交换算法和 MAC 算法等），实现服务器和客户端的身份验证，并在服务器和客户端之间安全地交换密钥。客户端和服务器通过握手协议建立会话。
- SSL 密码变化协议：客户端和服务器端通过密码变化协议通知对端，随后的报文都将使用新协商的加密套件和密钥进行保护和传输。
- SSL 告警协议：用来向对端报告告警信息，以便对端进行相应的处理。告警消息中包含告警的严重级别和描述。

SSL 下层协议：

- SSL 记录协议：主要负责对上层的数据进行分块、计算并添加 MAC、加密，最后把加密后的记录块传输给对方。

目前，SSL 协议版本主要有 SSL2.0、SSL3.0、TLS1.0（TLS1.0 对应 SSL 协议的版本号为 3.1）、TLS1.1 和 TLS1.2。

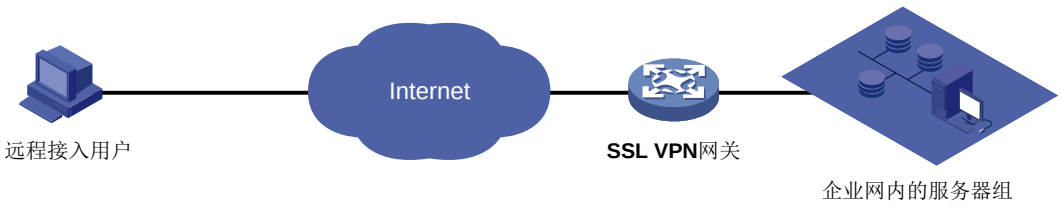
SSL 之所以能够让 VPN 接入具有安全性，在于它提供的全面的安全机制：

- 保证数据传输的机密性：利用对称密钥算法对传输的数据进行加密，并利用密钥交换算法，如 RSA，加密传输对称密钥算法中使用的密钥。
- 验证数据源的身份：基于数字证书，利用数字签名方法对 SSL 服务器和 SSL 客户端进行身份验证。
- 保证数据的完整性：消息传输过程中使用 MAC（Message Authentication Code，消息验证码）来检验消息的完整性。在杂凑算法的参与下，任意长度的原始数据被转换为固定长度的数据，原始数据的任何变化都会导致计算出的固定长度数据发生变化。

2.3 SSL VPN运行机制

SSL VPN 服务通过 SSL VPN 网关来提供。SSL VPN 网关位于远端接入用户和企业内部网络之间，负责在二者之间转发报文。企业网络管理员需要在 SSL VPN 网关上创建与企业网内服务器对应的资源。

图3 SSL VPN 运行机制示意图



如图 3 所示，SSL VPN 的工作机制可以概括如下：

(1) 远程接入用户与 SSL VPN 网关建立 HTTPS 连接，通过 SSL 提供的基于证书的身份验证功能，SSL VPN 网关和远程接入用户可以验证彼此的身份。

(2) 远程接入用户输入用户名、密码等身份信息，SSL VPN 网关对用户的身份进行认证，并对用户可以访问的资源进行授权。

(3) 用户获取到可以访问的资源，通过 SSL 连接将访问请求发送给 SSL VPN 网关。

(4) SSL VPN 网关将资源访问请求转发给企业网内的服务器。

(5) SSL VPN 网关接收到服务器的应答后，通过 SSL 连接将其转发给用户。

2.4 SSL VPN接入方式

SSL VPN 具有三种接入方式，分别为 Web 接入方式、TCP 接入方式和 IP 接入方式。三种接入方式提供不同粒度的资源访问控制，且具有不同的应用兼容性。其中 Web 接入方式资源访问控制粒度最细，可以对用户访问资源进行精细控制，只需要终端安装浏览器即可，其应用兼容性最高；IP 接入方式是基于网络层对内网资源进行控制，资源控制方式简单，易于管理，需要安装 IP 接入客户端软件，其应用兼容性较低。

2.4.1 Web 接入方式

1. Web 接入方式的总体流程

Web 接入方式是指用户使用网页浏览器，通过 HTTPS 协议访问 SSL VPN 网关提供的 Web 资源。用户登录并通过身份认证后，Web 页面上会显示用户可访问的资源列表，用户可以选择需要访问的资源直接访问。Web 接入方式中，所有数据的显示和操作都是通过 Web 页面进行的。这种接入方式不需要安装特殊软件，因此应用较为广泛。

如图 4 所示，Web 接入方式实现过程如下：

(1) 用户使用浏览器，通过 HTTPS 协议登录 SSL VPN 网关。

(2) SSL VPN 网关对用户进行认证，并对允许用户访问的 URL 资源进行授权，授权的 URL 资源以 URL 链接的形式展示在网关的 Web 页面上。

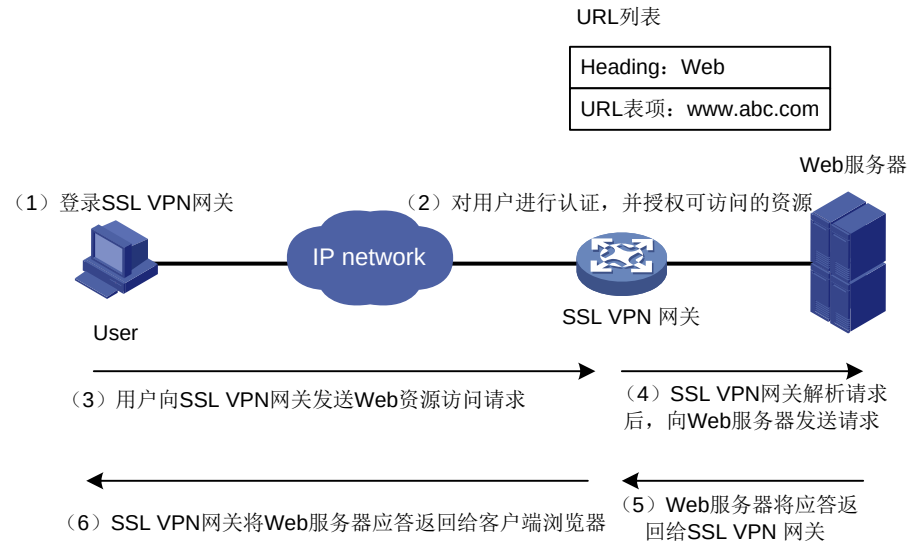
(3) 用户在 SSL VPN 网关的 Web 页面上访问经过授权的 URL 资源。

(4) SSL VPN 网关解析接收到的 Web 请求，并使用 HTTP 或 HTTPS 协议向 Web 服务器发送 Web 请求。

(5) Web 服务器将应答报文返回给 SSL VPN 网关。

(6) SSL VPN 网关接收到 Web 服务器的应答报文后，通过 SSL 连接将其转发给用户浏览器。

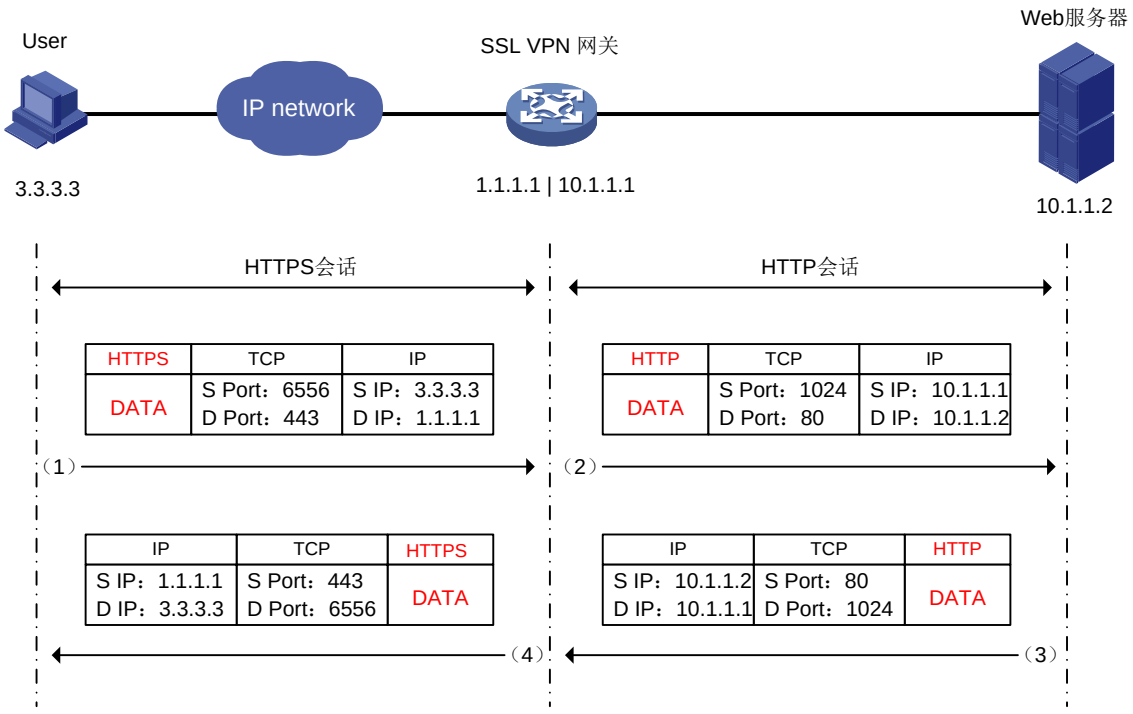
图4 Web 接入方式示意图



2. Web 接入方式的报文封装过程

如图 5 所示，Web 接入方式的报文封装过程，本质上是由一段 HTTPS 会话和一段 HTTP 或 HTTPS 会话组成。用户的访问请求通过 HTTPS 会话发送至 SSL VPN 网关，SSL VPN 网关再通过 HTTP 会话将用户的访问请求转发给 Web 服务器。SSL VPN 网关收到 Web 服务器的应答报文，通过 HTTPS 会话将应答报文转发给用户。

图5 Web 接入方式报文封装示意图



2.4.2 TCP 接入方式

1. TCP 接入方式的总体流程

TCP 接入方式是指用户对企业内部服务器开放端口的安全访问。通过 TCP 接入方式，用户可以访问任意基于 TCP 的服务，包括远程访问服务（如 Telnet）、桌面共享服务、电子邮件服务以及其它使用固定端口的 TCP 服务。

用户利用 TCP 接入方式访问内网服务器时，需要在 SSL VPN 客户端（用户使用的终端设备）上安装专用的 TCP 接入客户端软件，由该软件使用 SSL 连接传送应用层数据，保障数据安全。

TCP 接入方式下，管理员需要在 SSL VPN 网关上创建端口转发规则，将企业网内部服务器的 IP 地址（或域名）和端口号映射为 SSL VPN 客户端的本地 IP 地址（或主机名）和本地端口号。

如图 6 所示，以用户访问内网 Telnet 服务器举例，TCP 接入方式实现过程如下：

(1) 用户使用浏览器，通过 HTTPS 协议登录 SSL VPN 网关。

(2) SSL VPN 网关对用户进行认证，并对允许用户访问的 TCP 接入服务（即端口转发规则）进行授权。

(3) 用户在 SSL VPN 网关的 Web 页面上下载 TCP 接入客户端软件

(4) 用户在 SSL VPN 客户端上启动 TCP 接入客户端软件，可以看到授权访问的 TCP 接入服务。TCP 接入客户端软件在 SSL VPN 客户端上打开授权的端口转发规则中指定的本地端口号。

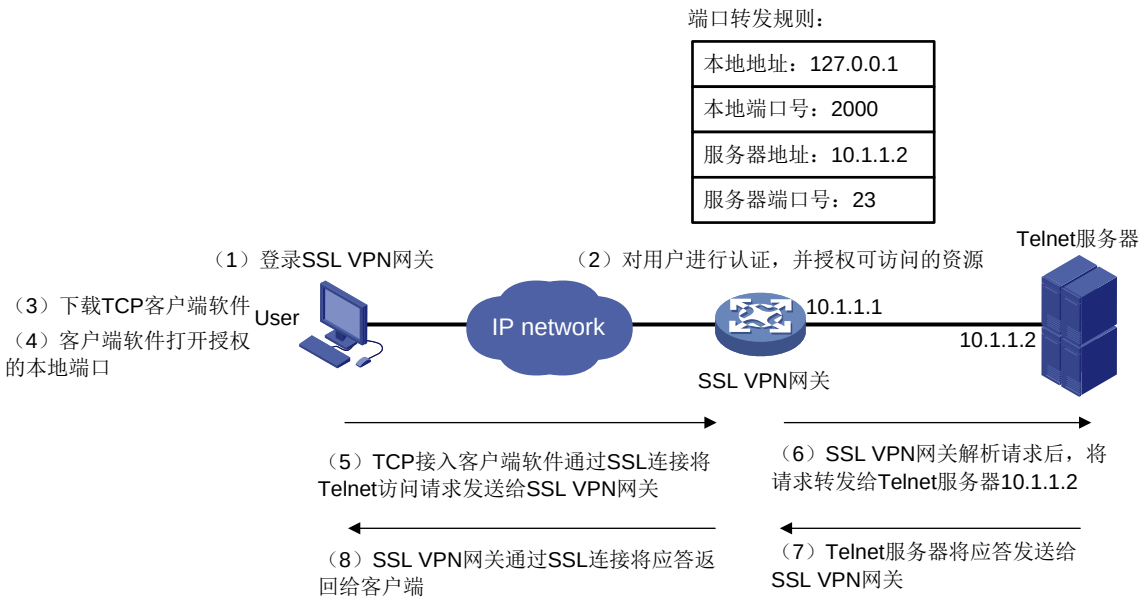
(5) 用户访问本地 IP 地址（或主机名）和本地端口号时，TCP 接入客户端软件将访问请求通过 SSL 连接发送给 SSL VPN 网关。

(6) SSL VPN 网关解析接收到的请求，并根据本地配置的端口转发规则，将该请求转发给对应的 Telnet 服务器。

(7) Telnet 服务器将应答报文返回给 SSL VPN 网关。

(8) SSL VPN 网关接收到服务器的应答报文后，通过 SSL 连接将其转发给 SSL VPN 客户端。

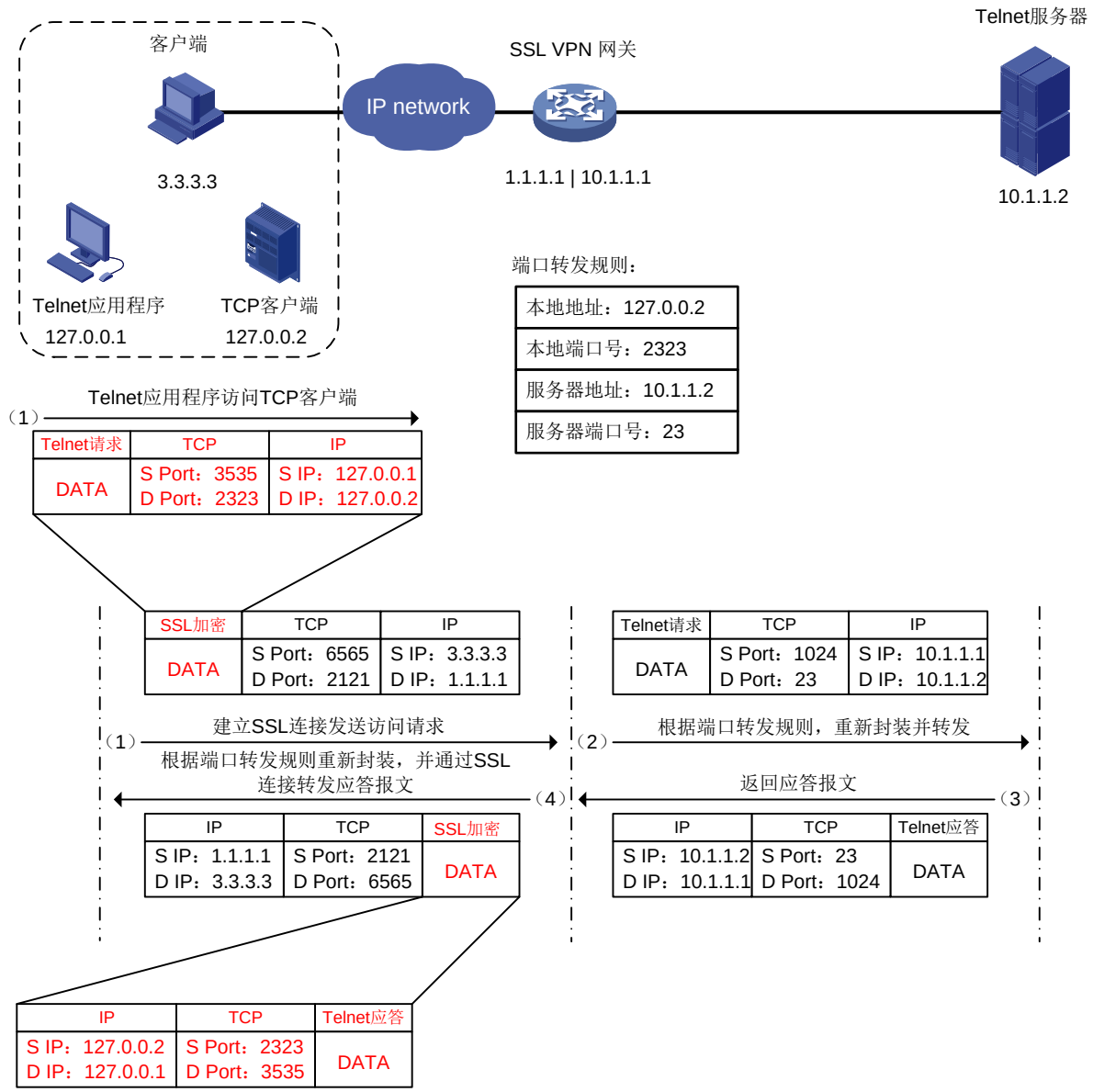
图6 TCP 接入方式示意图



2. TCP 接入方式的报文封装过程

如图 7 所示，以客户端访问内网 Telnet 服务器举例。TCP 客户端软件监听 Telnet 应用程序发送的访问请求，并将访问请求通过 SSL 加密连接，转发至 SSL VPN 网关。SSL VPN 网关将进行 SSL 解密，并根据端口转发规则，重新封装报文向内网 Telnet 服务器发送访问请求。Telnet 服务器将应答报文发送至 SSL VPN 网关，SSL VPN 网关根据端口转发规则，重新封装报文，并通过 SSL 加密连接将应答报文转发给 TCP 客户端。TCP 客户端通过环回地址将应答报文，发送至 Telnet 应用程序。

图7 TCP 接入方式报文封装示意图



2.4.3 IP 接入方式

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 8 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。

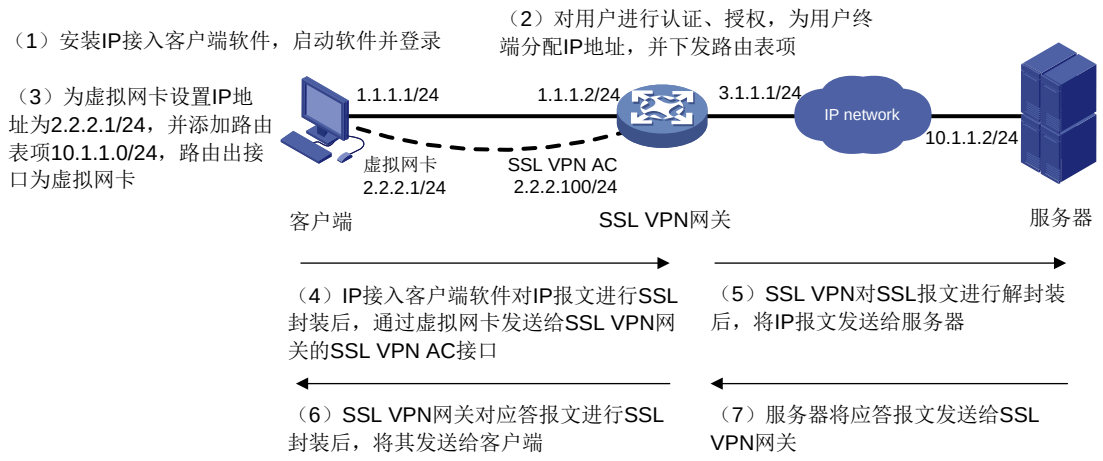
(4) 用户在客户端上访问企业内网服务器时，访问请求报文匹配添加的路由表项，该报文将进行 SSL 封装，并通过虚拟网卡发送给 SSL VPN 网关的 SSL VPN AC 接口。

(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。

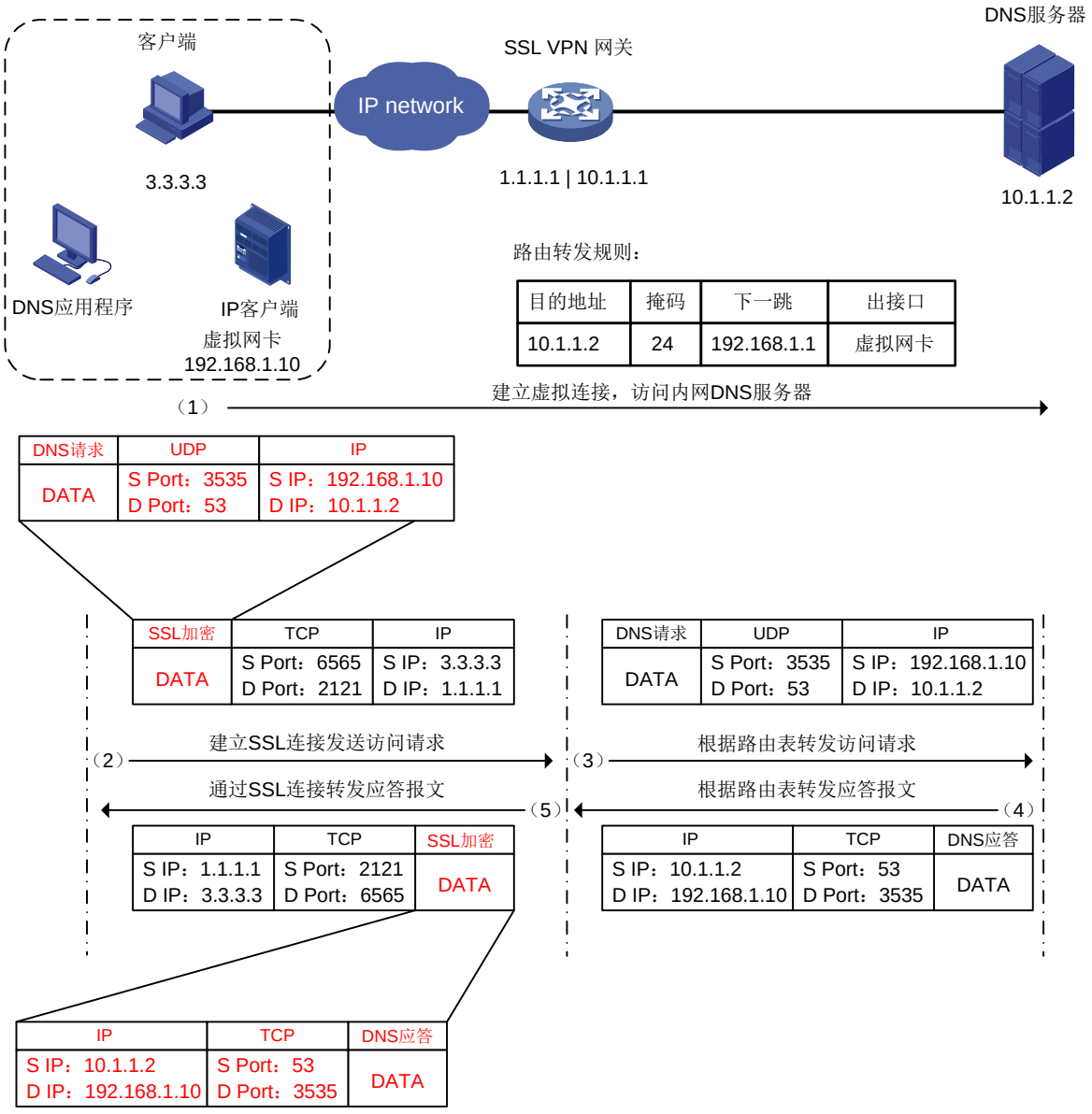
图8 IP 接入方式示意图



2. IP 接入方式的报文封装过程

如图 9 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



2.5 SSL VPN用户认证

SSL VPN 用户认证是 SSL VPN 网关对 SSL VPN 用户身份的认证，用户身份认证通过后，才能访问对应的内网服务器资源。SSL VPN 支持多种用户认证方式，满足用户在不同场景下的需求。多种认证方式可以组合使用，开启多个认证方式时，用户必须同时满足所选认证方式才能登录成功。

SSL VPN 支持如下用户认证方式：

- 用户名密码认证

  SSL VPN 网关在接收到用户发送的用户名和密码后，将这些信息发送至认证模块进行认证。用户认证包括是本地认证和远程认证。本地认证，是指用户名和密码配置在 SSL VPN 网关上，

由 SSL VPN 网关对用户名密码进行认证。远程认证，是指用户名密码将被发送至认证服务器进行认证，认证服务器包括 Radius、LDAP 等。

- 证书认证

  用户在认证时会将证书发送到 SSL VPN 网关。SSL VPN 网关会对证书合法性做验证，如果通过验证，则继续做认证。SSL VPN 网关可以支持软证书，也支持从 USBKey 中读取证书。SSL VPN 网关即可以将证书中的 CN 字段作为认证使用的用户名，也支持将指定的证书某个字段作为用户名。

- 短信认证

  设备使用短信验证码对用户进行身份验证，验证通过后才允许用户登录 SSL VPN 网关。SSL VPN 支持使用 iMC 认证服务器，或者第三方短信网关进行短信认证。

- 自定义认证

  用户根据实际需求，在本地搭建自定义的认证服务器，并配置自定义认证参数，实现对 SSL VPN 登录用户的认证和授权。通过对认证报文格式进行自定义设置，SSL VPN 网关能够适应各种非标准的认证系统，从而极大的扩展 SSL VPN 的应用场景。

- 企业微信认证

  SSL VPN 从第三方企业微信获取企业用户信息，并使用该用户信息对用户进行认证和授权。SSL VPN 网关认证通过后，用户可以通过企业微信访问企业内部资源。借助企业微信强大的终端功能，用户可以轻松的实现移动办公。

3 技术特色

3.1.1 个性化定制用户界面

管理员可以根据需要对 SSL VPN 页面进行定制。支持的页面定制项包括：登录页面欢迎信息、登录页面是否显示密码输入框、页面标题、logo 图标、登录页面和资源页面公告信息、资源页面供用户下载的资源文件、修改密码页面密码复杂度提示信息、改写服务器返回信息。

主要页面定制项如下：

- 页面公告信息

  网络管理员可以在 SSL VPN 登录页面和资源页面配置公告信息，通过 Web 页面统一向用户展示公告信息，具有广泛的应用场景。

- 文档上传和下载

  网络管理员可以将本地文件上传至 SSL VPN 网关，用户可以将上传的文件下载到本地，实现文件的快速分发和共享。

- 密码复杂度提示信息

  用户首次登录 SSL VPN 网关修改密码，或者登录成功后修改密码时，将会在修改密码的界面看到网络管理员设定的密码复杂度提示信息。该提示信息可以帮助用户快速设定符合密码复杂度要求的新密码，方便用户使用。

- 改写服务器返回信息

  SSL VPN 用户接入过程中，认证服务器可能会返回特定信息。网络管理员可以根据实际情况改写此信息，将晦涩难懂的错误码转换成浅显易懂的语言，展现在登录客户端（例如 iNode 客户端）上，便于用户使用。

3.1.2 多维度、精细化的信息展示

SSL VPN 支持多维度、精细化的信息展示，可以为用户提供详细的用户接入状态监控和查询功能。信息展示内容主要包括：

- 用户接入日志

详细的记录每个用户登录登出 SSL VPN 网关的行为以及结果。当有 SSL VPN 用户登录登出设备时会有相应的日志输出，日志的内容主要包括 SSL VPN 用户的登录时间、登录用户名、登录 IP 地址、所属访问实例、登录登出动作、登录结果等。管理员可以通过查看用户接入日志，了解用户的历史登录登出记录，登录失败原因等信息，有利于管理员管理和维护设备。

- 资源访问日志

清晰的展示每个用户所访问的资源以及访问结果。当 SSL VPN 用户访问内网资源时会有相应的日志输出，日志的内容主要包括 SSL VPN 用户的登录时间、登录用户名、登录 IP 地址、所属访问实例、访问资源类型、访问资源、资源的端口号、访问结果等。管理员可以通过查看访问资源日志，了解用户访问内网资源的具体情况，方便管理员对用户访问的资源进行管理和控制。

- 服务器流量统计

全面的展示SSL VPN用户对内网服务器的流量访问情况，网络管理员可以根据访问流量统计结果，对内网服务器的部署进行调整。

- 在线用户数趋势统计

SSL VPN 在线用户数趋势功能用来对同时登录到设备的 SSL VPN 在线用户数量进行统计，并向用户展示 SSL VPN 在线用户数趋势图和 SSL VPN 接入用户的历史统计数据。方便管理员查看 SSL VPN 在线用户数趋势及历史最大在线用户数，并根据在线用户数趋势，及时进行扩容。

3.1.3 SSO 统一接入管理

SSL VPN 支持 SSO（Single Sign On，单点登录）统一接入管理，是指 SSL VPN 用户只需要完成一次登录认证，即可访问所有相互信任的应用系统。用户无需多次进行身份验证，使用 SSO 统一接入管理功能，即可快速免认证访问内网资源，大大提高了用户访问内网资源的效率和用户体验。

3.1.4 基于 SSL VPN 连接的带宽限速

通过基于 SSL VPN 连接的带宽限速功能，控制单个 SSL VPN 连接的流量，避免单个 SSL VPN 连接占用过多的带宽，影响其它用户使用 SSL VPN，合理有效的进行带宽管理。

3.1.5 基于访问实例的全局带宽限速

IP 接入方式下，SSL VPN 支持基于访问实例的全局带宽限速功能。本功能支持对 SSL VPN 访问实例下所有用户进行带宽限速，同时支持对限速导致的丢包进行统计并生成丢包日志。

3.1.6 内网资源 URL 地址伪装

SSL VPN 支持将资源 URL 地址通过一定的编码处理，转换成新的字符串呈现给用户，从而隐藏真实的资源地址。防止内网服务器资源地址泄露，有效保护内网资源。SSL VPN 支持对某个特定的资源地址进行伪装，或者对访问实例下所有的资源地址进行伪装。

例如，内网服务器真实的资源 URL 地址为 http://www.baidu.fin.com/cn/，伪装后的资源 URL 地址为 http://d3id3dsmgzeYy5jb20=r/cn/。

3.1.7 证书 CRL 吊销信息查询

采用证书认证时，SSL VPN 网关将查询 CRL 吊销列表，判断 SSL VPN 用户证书是否被吊销，如果证书已经被吊销，将禁止用户登录 SSL VPN 网关。有效保证用户证书的可靠性，增强证书认证的安全性。

3.1.8 内网资源快速访问

默认情况下，用户登录 SSL VPN 网关后，需要进入 SSL VPN 资源页面，点击资源链接才能访问资源。内网资源快速访问功能，支持用户登录 SSL VPN 网关后，直接进入访问页面，而不需要在资源页面点击资源链接，可帮助用户快速访问常用的资源。

3.1.9 全面支持国密算法

SSL VPN 全面支持主流的国密算法：SM1、SM2、SM3 和 SM4，满足国密部署场景的要求。

3.1.10 暴力破解攻击防范

暴力破解是指，来自同一 IP 地址的连续登录请求，企图通过穷举密码的方式登录 SSL VPN 网关。一旦用户登录密码被暴力破解，内网服务器资源将会被泄露，用户信息将受到严重威胁。为了阻止暴力破解攻击，SSL VPN 通过限制同一 IP 地址尝试登录 SSL VPN 的次数，降低登录信息被暴力破解的风险，有效保护内网服务器资源。

SSL VPN 支持如下防暴力破解功能：

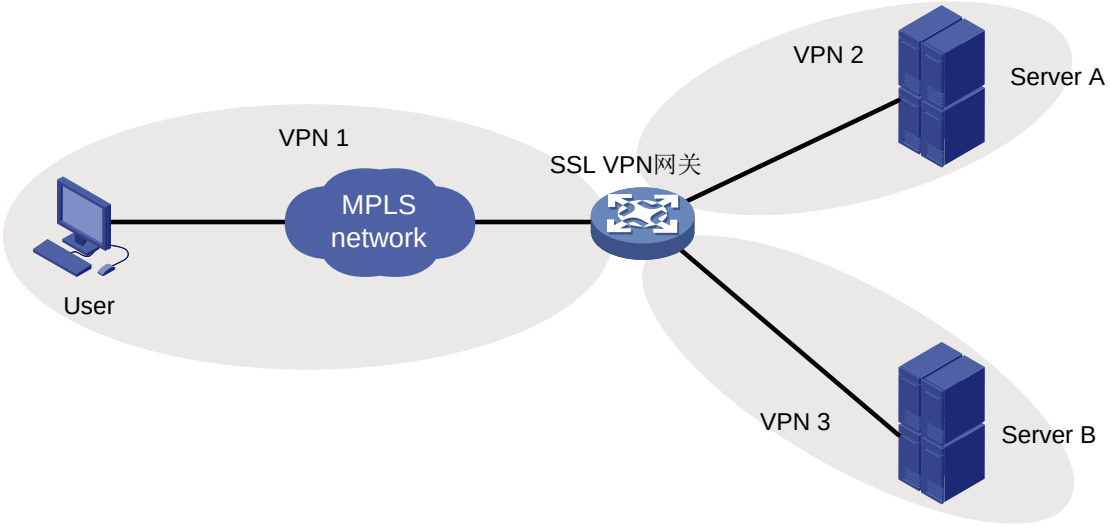
- 登录失败达到限定次数后，SSL VPN 自动开启图形验证码功能。该图形验证功能将在登录成功后自动关闭。
- 登录失败达到限定次数后，SSL VPN 将冻结该 IP 地址，在一定时间内禁止该 IP 地址再次登录。

3.1.11 多业务隔离 VPN 实例

SSL VPN 支持将不同的 SSL VPN 访问实例关联不同的 VPN 实例，可以隔离不同访问实例内的服务器资源，避免非法用户访问特定资源的同时，还可以实现服务器资源的地址重叠。

管理员还可以指定 SSL VPN 网关所属的 VPN 实例。只有属于同一个 VPN 的用户可以访问 SSL VPN 网关，从而避免内部服务器资源泄漏到公网和其它 VPN 中。

图10 SSL VPN 支持 VPN 多实例示意图



3.1.12 深度融合的虚拟化技术

SSL VPN 支持两级虚拟化技术，以应对不同的场景需求。

- 操作系统级虚拟化技术

将一台物理设备划分成多台逻辑设备，每台逻辑设备就称为一个 Context。每个 Context 拥有自己专属的软硬件资源，独立运行。SSL VPN 通过操作系统级别的虚拟化，可以实现在管理、转发上的完全隔离，对外完全呈现为独立的 SSL VPN 网关。这种深度虚拟化技术适用于多租户业务模型，同时也为不同租户管理员提供了独立的管理界面。在这种模式下，不同租户虽然共享硬件资源，但是缺省管理员可以给每一个租户对应的设备（Context）分配独立的安全能力。

- SSL VPN 内部虚拟化技术

针对仅需要提供外部访问及业务隔离的场景，可以通过 SSL VPN 内部虚拟化技术——SSL VPN 访问实例实现。SSL VPN 访问实例将 SSL VPN 各业务进行实例化，实现不同访问实例域之间的配置管理相互独立。用户可以通过不同的访问实例域名进入各个不同的访问实例。在转发层面，可通过 VPN 多实例实现不同访问实例之间的转发隔离。

用户可以在系统级虚拟化设备（Context）内，进一步创建 SSL VPN 访问实例，实现两级虚拟化，满足更加复杂的应用场景需求。同时管理员还可以灵活的分配每个 Context 和 SSL VPN 访问实例支持的最大在线用户数，对接入用户数量进行统一管理。

3.1.13 双机联动的高可靠性

SSL VPN 支持双机热备可以提高 SSL VPN 接入的可靠性。在双机热备组网中，当一台 SSL VPN 网关设备出现故障时，其它网关设备可以继续为用户提供接入服务，已上线用户不掉线，不需要重新认证授权。

4 典型组网应用

SSL VPN 的典型组网方式主要有两种：网关模式和单臂模式。

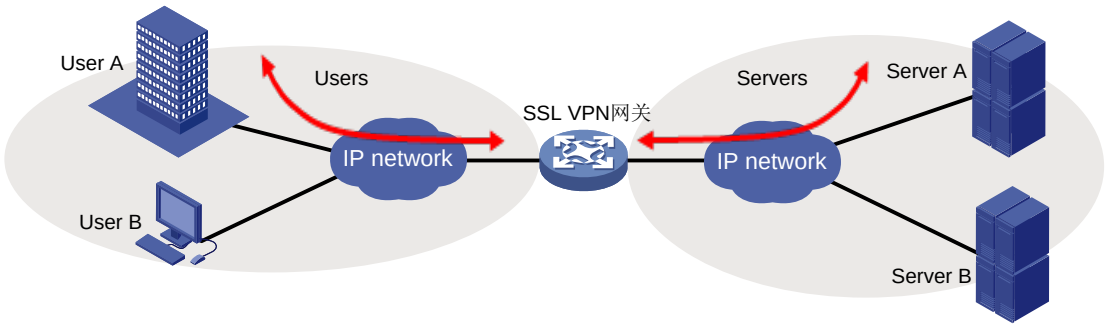
4.1.1 网关模式

网关模式是指，SSL VPN 网关直接作为网关设备连接内外网，所有流量通过 SSL VPN 网关进行转发。

网关模式具有如下特点：

- SSL VPN 网关跨接在内网和外网之间，处在网络出口的枢纽位置，可以保护内外网之间的所有流量。
- 该模式对 SSL VPN 网关的处理能力、抗攻击能力和稳定性有较高的要求。

图11 网关模式



4.1.2 单臂模式

单臂模式是指，SSL VPN 网关旁挂在网关设备之上，流量由网关设备转发至 SSL VPN 网关。

单臂模式具有如下特点：

- SSL VPN 网关不处在网络通信的关键路径上，即使出现故障，也不影响内外网的通信。
- 需要保护的流量先由网关设备转发至 SSL VPN 网关，SSL VPN 网关再将流量转发至内网服务器；不需要保护的流量将由网关设备直接转发至内网服务器。

图12 单臂模式