HCIE-Security 备考指南

SSL VPN（SVN）

HCIE 只是一个开始….

HCIE 仅是一个证书…懂得做人和处事比证书和技能更重要…

希望大家顺利通过 HCIE，取得更好的职业发展！

目 录

HCIE-Security SSL VPN（SVN）需要掌握的知识点

- 掌握 SSL VPN Web 代理技术原理及配置
- 掌握 SSL VPN 文件共享技术原理及配置
- 掌握 SSL VPN 端口转发技术原理及配置
- 掌握 SSL VPN 网络扩展技术原理及配置

Web 代理简介

远程用户（如企业的出差员工、企业分部员工、企业合作伙伴等）想通过 Internet 访问企业内网的 Web 资源，但是 Internet 上潜伏着很多安全风险。在 SVN 上配置 Web 代理功能，可以将企业内网的 Web 资源通过 SVN 网关开放给远程用户访问。由于 SVN 与远程用户之间是通过 SSL VPN 加密隧道来交互信息，经过加密的信息在 Internet 上传输时可以防止被不法用户窃取、篡改，从而消除了安全隐患。

Web 代理应用场景

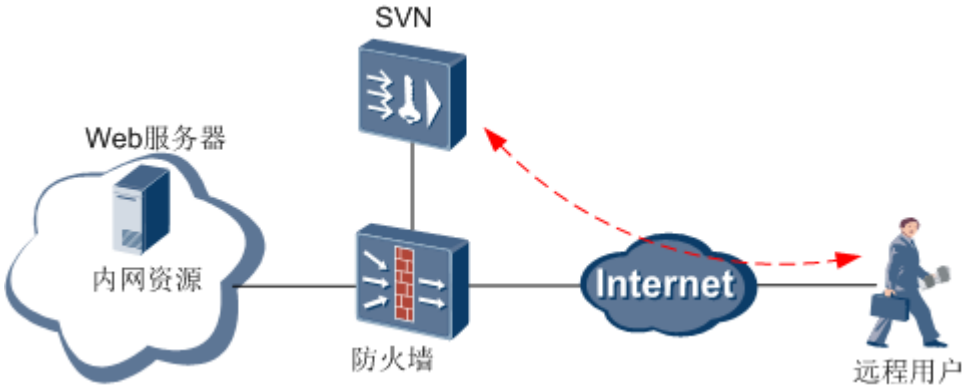
SVN 处于企业内网和 Internet 的边界位置，它以中间人（代理）的身份收集远程用户的 Web 请求，并将此请求转发给内网的 Web 服务器，然后再将 Web 服务器的响应信息回传给远程用户。SVN 启用 Web 代理功能后，远程用户访问企业内网 Web 资源的过程如下：

1. 远程用户通过浏览器访问 SVN 的虚拟网关，进入虚拟网关的登录界面。
2. 远程用户在虚拟网关的登录页面输入用户名和密码，虚拟网关校验该用户的身份信息。

   身份校验通过，远程用户登录虚拟网关成功；身份校验不通过，登录失败。

3. 登录成功的远程用户可以在虚拟网关中看到本用户所能访问的企业内网 Web 资源列表，点击列表中的链接即可访问该资源。

图 1 Web 代理典型组网图



Web 代理原理描述

介绍 Web 代理的业务交互流程以及报文封装原理。

业务交互流程

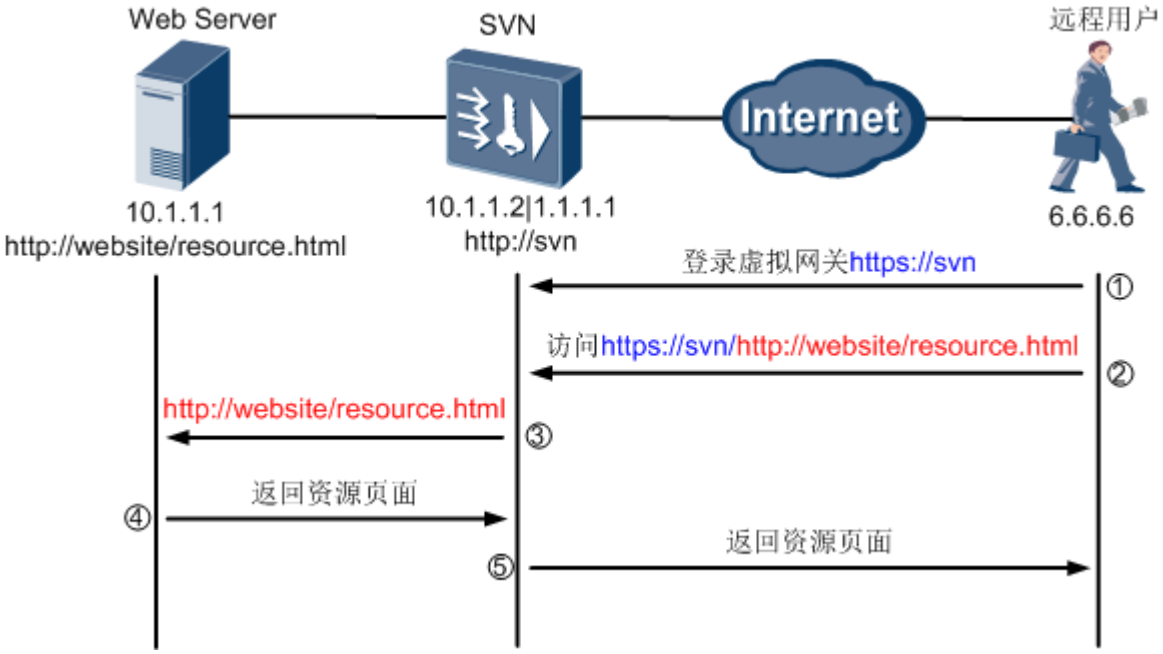
图 1 所示是远程用户通过 Web 代理方式来访问内网 Web Server 的一个业务交互流程。

1. 远程用户通过域名（http://svn）来访问虚拟网关。
2. 登录虚拟网关成功后，远程用户会在虚拟网关中看到自己有权访问的 Web 资源列表，然后单击要访问的资源链接。

   SVN 在将内网资源（http://website/resource.html）呈现给远程用户时，会改写该资源的 URL。远程用户点击资源链接后，发送给 SVN 的 HTTPS 链接请求就是虚拟网关改写以后的 URL，改写后的 URL 实质上是由 https://svn 和 http://website/resource.html 这两个 URL 拼接而成。

3. SVN 收到上述 URL 后，会向 web Server 重新发起一个 HTTP 请求，这个 HTTP 请求就是 Web 资源实际的 URL（http://website/resource.html）。
4. Web Server 以 HTTP 方式向 SVN 返回资源页面。
5. 虚拟网关将 Web Server 返回的资源页面，再经过 HTTPS 方式转发给远程用户。

图 1 Web 代理业务交互流程



从业务交互流程可以看出，Web 代理功能的基本实现原理是将远程用户访问 Web Server 的过程被分成了两个阶段。首先是远程用户与 SVN 虚拟网关之间建立 HTTPS 会话，然后 SVN 虚拟网关再与 Web Server 建立 HTTP 会话。虚拟网关在远程用户访问企业内网 Web Server 中起到了改写、转发 Web 请求的作用。

Web 代理按照实现方式的不同分为了 Web 改写和 Web link 两种。

- Web 改写

  Web 改写中的“改写”包含两层含义。第一层含义是加密，即远程用户在点击虚拟网关资源列表中的链接时，虚拟网关会将用户要访问的真实 URL 进行加密。例如，在图 1 的第二步中，用户要访问的真实 URL 是 *http://website/resource.html*，而经过 Web 改写以后 URL 可能会显示为 *http://website/D%3A/0-2+resource.html*。通过 Web 改写，起到隐藏内网 Web 资源真实 URL 的目的，从而保护内网 Web 服务器的地址安全。在 Web 改写中，这种加密不仅体于此，包括用户要访问的 Web 资源页面链接对象（例如 Flash、PDF、Java Applet 等）的 URL 也会被一并加密。

  第二层含义是适配。随着网络技术不断的发展，远程用户接入 Internet 的终端类型也变得丰富起来，如智能手机、PAD、便携机等越来越普及。这些不同的终端设备使用着不同的操作系统和的浏览器，这就使得它们在 Web 资源的支持上存在差异。为了解决终端类型差异对业务的影响，这就需要 SVN 不仅能将内网 Web 资源转发给远程用户，而且还要对 Web 资源进行“改写”，使之能够适配这些不同的终端。启用 Web 代理功能以后，SVN 设备会自动对 Web 资源进行改写。对于个别 HTML 对象和 ActiveX 控件如果在启用 Web 代理以后，仍然出现显示异常的情况，则可以通过手动配置的方法进行精确改写，解决此问题。

- Web link

Web Link 不会进行加密和适配，只做单纯“转发”远程用户的 Web 资源请求。

由于 Web Link 少了加密和适配的环节，因此业务处理效率较之 Web 改写要高。而 Web 改写由于做了加密和适配，因此在安全性和适用性方面要比 Web Link 高。

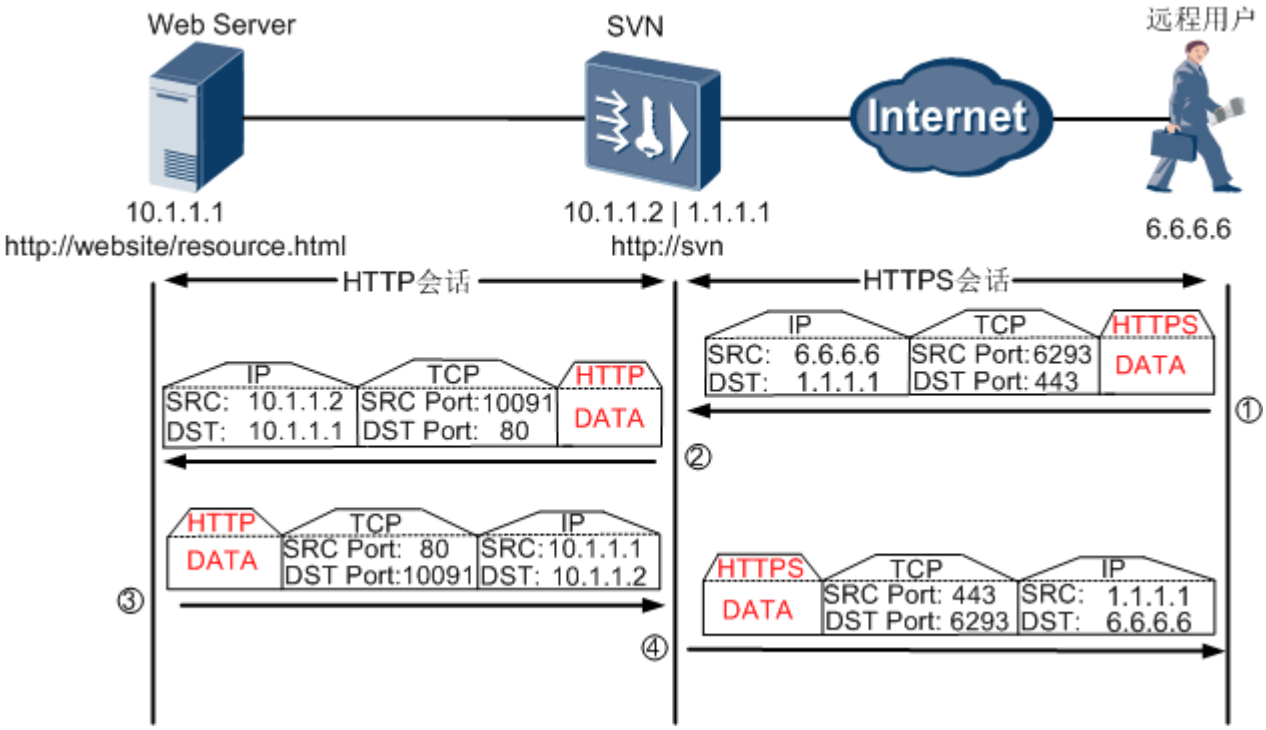
说明：

- 图 1 所示是 Web 改写的业务流程，Web link 的业务交互流程与 Web 改写的类似。所不同的是 Web link 不会对资源进行改写。
- 需要注意的是，Web link 只适合在用户使用 Window 操作系统+IE 浏览器的终端上使用。非此场景，只能使用 Web 改写。

Web 代理报文封装原理

图 1 所示是远程用户访问内网 Web 资源时的报文封装过程，从图中可以看出远程用户的访问过程本质上是由 HTTPS 和 HTTP 这两个会话衔接而成。其中，远程用户与虚拟网关建立 HTTPS 会话时，使用的源端口为 6293，这个源端口是一个随机端口；目的端口是 443。虚拟网关与 Web Server 建立 HTTP 会话时，源端口是 10091，这个源端口也是随机端口，目的端口为 80。

图 2 Web 代理报文封装原理



配置 Web 代理

介绍 Web 代理功能的配置方法。

配置 Web 代理的基本功能，包括以下几个步骤：

1. 启用 Web 代理功能。

   只有启用 Web 代理功能后，用户才能使用 Web 代理业务。

2. 新建 Web 代理资源。

   添加终端用户可以访问的内网 Web 资源。

3. 新建虚拟网关下的用户。

   该用户就是访问企业内网 Web 资源的远程用户。

4. 配置用户访问内网 Web 资源的权限。

   角色是权限的集合，通过为用户分配角色，使其具有访问不同资源的权限。例如用户 A 的角色名称是 role，角色 role 的权限是可以访问 *http://www.svn/resource.html* 这条资源。则将用户 A 的角色配置为 role 以后，该用户就可以访问此资源。

5. 配置虚拟网关的安全策略。

Web 代理除了一些基本功能配置以外，还提供了一些高级选项配置作为对 Web 代理功能的补充。

Web 代理基本配置

1. 启用 Web 代理功能。

   a. 创建虚拟网关，并进入虚拟网关配置界面。详细步骤略，具体配置请参见创建虚拟网关。

   b. 选择“SSL VPN > 资源 > Web 代理”。

   c. 在“配置 Web 代理”区域框中，选中“Web 代理功能”后的“启用”。

   - Web link

     Web Link 是 Web 代理功能的一个辅助功能。启用 Web 代理并不能保证内网所有的 Web 资源都可以经过虚拟网关改写后完整无误的呈现给远程用户。这是因为 Web 应用随着业务需求的发展，在不断的更新、变化，导致部分元素存在改写失败的风险。而 Web Link 的实现机制是真实呈现内网资源给外网用户（无需改写），因此不存在改写失败的问题。如果某些 Web

资源通过 Web 代理无法正常访问时，可以将此资源配置为 Web link 资源，然后启用 Web link 功能解决该问题。

- 例外 URL

  如果某些 Web 资源不需要 Web 代理进行改写，则可将该资源配置到“例外 URL”中。

d. 单击“应用”，启用 Web 代理功能。

2. 新建 Web 代理资源。

a. 在“Web 代理资源列表”区域框中，单击“新建”，配置 Web 代理资源的基本参数。

参数	说明
资源名	为用户可访问的 Web 代理资源定义一个名称。
描述	资源的简要描述。
类型	Web 代理功能对 Web 资源的处理方式。 • Web 改写：通过对 Web 资源页面中的元素进行改写，实现 Web 代理功能。推荐使用此方式。 • Web link：通过在虚拟网关客户端页面中安装 ActiveX 控件，实现对资源页面的转发。 **说明：** 只有启用了 Web Link 功能后，才能选择 Web Link 资源类型。
URL	Web 资源的 URL 地址。
所属资源组	选择资源所在的资源组。 资源组是 Web 资源的集合，一条资源只能加入到一个资源组。资源加入资源组后，配置的资源组信息可对组内各资源生效。资源组可以设置优先级，优先级决定了各个资源组在用户界面中的显示顺序。优先级高的资源组显示在用户界面的左边，随着优先级的降低，资源组依次向右排列。
资源图标	配置智能手机上显示的资源图标。管理员可以通过上传自定义图标的方式，指定资源在智能手机上的显示图标。
门户链接	• 选中“门户链接”对应的复选框后，在虚拟网关客户端页面上正常显示所添加的资源链接。 • 取消选中“门户链接”对应的复选框后，在虚拟网关客户端页面上隐藏所添加资源的链接。用户可以在虚拟网关客户端页面右上方的文本框中输入 Web 资源的 URL 链接，并单击“浏览”访问 Web 资源。

b. 单击“确定”。

3. 新建虚拟网关下的用户。

a. 选择“SSL VPN > 用户 > 用户组”。

b. 在“成员管理”页签中，单击“新建”，选择“新建用户”。

参数	说明
登录名	远程用户登录虚拟网关时的名称。
密码	远程用户登录虚拟网关时的密码。
确认密码	重新输入远程用户登录虚拟网关时的密码。

c. 单击“确定”。

4. 配置用户访问内网 Web 资源的权限。

a. 选择“SSL VPN > 角色授权”。

b. 单击“新建”，配置角色所具有资源访问权限。

参数	说明
角色	角色名称。
业务启用	启用该用户的业务功能。例如用户要使用“Web 代理”业务，则需要勾选“Web 代理”后的“启用”。
资源授权列表	单击“选择”，配置该角色所能访问的资源。

5. 配置虚拟网关的安全策略。

a. 配置安全策略，允许用户登录 SVN 虚拟网关。

1. 在界面右上角的“虚拟网关”中选择 root，进入 root 配置界面。

2. 选择“策略 > 安全策略”，单击“新建”，配置安全策略。

参数	说明
源安全区域	选择远程用户所在的安全区域。
目的安全区域	选择“local”。
服务	选择“https”。
动作	选择“允许”。

3. 单击“确定”。

b. 配置安全策略，允许用户访问 Web 代理资源。

0. 选择“策略 > 安全策略”，单击“新建”，配置安全策略。

参数	说明
源安全区域	选择“local”。
目的安全区域	Web 代理资源所在的安全区域。
用户	允许访问此 Web 代理资源的用户或用户组。
动作	选择“允许”。

1. 单击“确定”。

Web 代理高级配置

Web 代理中的高级配置属于可选配置，是在一些特定需要下使用的配置项。展开 Web 代理配置页面中的“高级”折叠按钮即可见，相关配置参数说明如下。

参数	说明
Web 代理选项	Web 代理选项包括： • Flash 改写/PDF 改写/Java Applet 改写 选中表示启用改写功能，SVN 虚拟网关会对 Flash/PDF/Java Applet 文件中的 URL 进行改写。 • HTTP 压缩 选中表示启用 HTTP 压缩功能。SVN 虚拟网关会对 HTML、CSS、JavaScript、XML、VBScript 资源内容进行压缩。 • Web 缓存 选中表示启用 Web 缓存功能。Web 缓存功能是指对 Web 代理改写后的内容进行保存，用于减少终端用户访问内网资源时的响应时间。
URL 隐藏	启用 URL 隐藏后，远程用户在访问内网资源时，其浏览器中该资源的主机地址和端口将被加密显示。加密显示的目的在于隐藏真实的主机地址和端口，保证内网资源安全。
Web 代理日志	启用 Web 代理日志功能可以记录用户访问的 Web 代理资源信息。 • 基本：记录用户通过 Web 代理资源列表页面直接访问的资源信息。 • 详细：记录 Web 代理资源列表页面中包含的其他 Web 资源信息（例如 doc、docx、xls 等），用户可以根据配置项选择记录哪些资源日志。
自定义改写	当远程用户访问内网 Web 资源时，部分 HTML 元素无法正常显示时，可以通过改写该 HTML 元素解决问题。 1. 在“自定义改写列表”区域框中，单击“新建”。 2. 配置要改写的元素。 • 属性：需要改写元素的属性名称。 • HTML 对象：需要改写元素的对象名称。 3. 单击“确定”。 例如：example中，HTML 对象名为“a”，属性名为“href”。定义该改写规则后，对应的属性值“http://www.example.com/”将被改写。

参数	说明
ActiveX 改写	当远程用户访问内网 Web 资源时，某个 ActiveX 控件无法正常使用时，可以通过改写该 ActiveX 控件解决问题。 1. 在“ActiveX 改写”区域框中，单击“新建”。 2. 配置要改写的 ActiveX 控件。 • ClassID：ActiveX 控件都有一个 36 位长度的 ID 号（即 ClassID），当某个 ActiveX 控件无法正常使用而需要改写时，在此输入对应的 ClassID。 • 参数名：需要改写的参数名称。 3. 单击“确定”。 例 如 ： <OBJECT classid=clsid:D27CDB6E-AE6D-11cf-96B8-444553540000><PARAM NAME=movie VALUE="/adv/soft/ss_468X60_Banner.swf"></OBJECT>中，ClassID 为“D27CDB6E-AE6D-11cf-96B8-444553540000”，参数名为“movie”。定义改写规则后，对应的参数值“/adv/soft/ss_468X60_Banner.swf”将被改写。

文件共享简介

文件共享业务是通过将文件共享协议（SMB，NFS）转换成基于 SSL 的超文本传输协议（HTTPS），实现对内网文件服务器的 Web 方式访问。

文件共享业务的主要功能就是让用户直接通过浏览器就能访问内网文件服务器，并能在文件服务器的共享目录中上传/下载文件、删除文件/目录、重命名文件/目录以及新建目录，就像对本机文件系统进行操作一样方便安全。

内网文件服务器可以是支持 SMB（Server Message Block）协议的 Windows 系统或者支持 NFS（Network File System）协议的 Linux 系统：

- SMB 文件服务器根据登录用户名和密码进行资源访问的权限控制，即用户访问 SMB 类型的文件时需要首先输入正确的用户名、密码登录文件服务器。
- NFS 文件服务器根据用户的 UID（User IDentification）和 GID（Group IDentification）进行资源访问的权限控制。

  管理员可以在 NFS 文件服务器上为共享文件设置以下三种用户群，并为每种用户群定义 GID、UID 以及访问权限，然后在 SVN 上为访问用户指定拥有相应权限的用户群 UID 和 GID 即可：

  - 拥有者

    拥有者即为共享文件的创建者。

  - 同组用户

    同组用户是指与拥有者同组的用户，即与拥有者的 GID 相同，但 UID 可以设置为不同。

- 其他用户

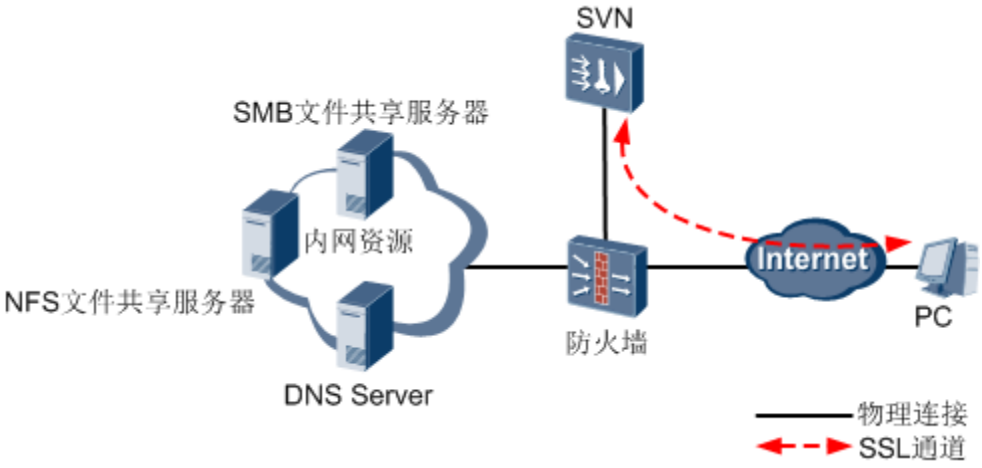
  其他用户是指与拥有者不同组的用户，即 GID、UID 与拥有者的 GID、UID 均不同。

文件共享应用场景

文件共享的应用场景是保证用户能够安全便捷的访问内网文件服务器的共享资源。

SVN 文件共享业务的典型应用场景如图 1 所示。部署了 DNS 服务器后，用户便可通过域名访问文件服务器的共享目录。

图 1 文件共享的典型应用场景

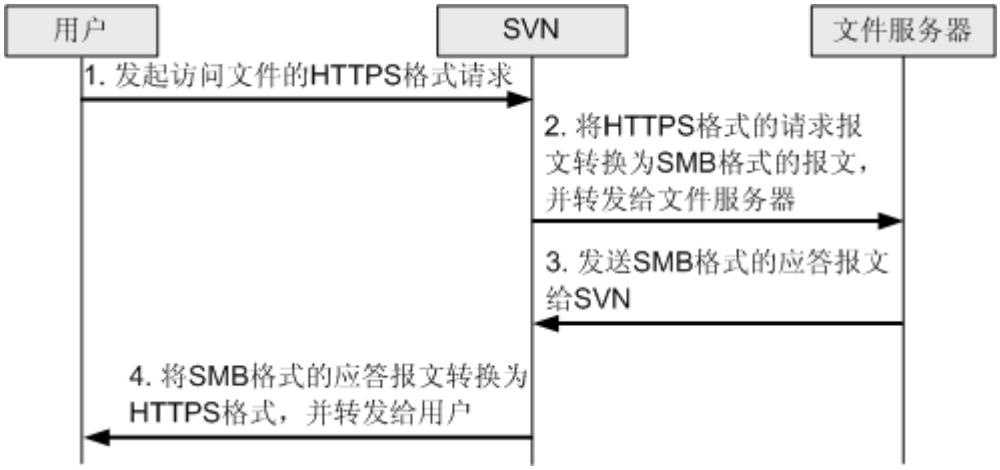


文件共享原理描述

介绍文件共享的实现原理。

在文件共享业务中 SVN 起到了协议转换器的作用，以访问内网 Windows 文件服务器为例，具体实现过程如图 1 所示。

图 1 文件共享的交互过程



配置文件共享

您需要启用文件共享功能，并为用户指定文件共享资源，即内网文件服务器上的文件共享目录。

背景信息

配置文件共享，包括以下几个步骤：

1. 启用文件共享功能。

   只有启用文件共享功能后，用户才能使用文件共享业务。

2. 新建文件共享资源。

   添加终端用户可以访问的文件共享资源。

3. 新建虚拟网关下的用户。

   该用户就是访问企业内网资源的远程用户。

4. 配置用户访问内网资源的权限。

   角色是权限的集合，通过为用户分配角色，使其具有访问不同资源的权限。

操作步骤

1. 在界面右上角的“虚拟网关”中选择虚拟网关名称，进入对应的虚拟网关。
2. 选择“SSL VPN > 资源 > 文件共享”。

3. 启用文件共享功能。

   a. 在“配置文件共享”区域框中，选中“文件共享功能”对应的“启用”。

   b. 单击“应用”。

   c. 在操作成功的提示框中。单击“确定”。

4. 配置文件共享资源

   a. 在“文件共享资源列表”区域框中，单击“新建”。

      如果新建的资源与现有资源的配置有相同之处，可以单击现有资源对应的  ，在现有资源的参数基础上新建文件共享资源。

   b. 配置文件共享资源。

参数	说明
资源名	为用户可访问的文件共享资源定义一个名称。
资源路径	共享资源的路径格式与资源类型有关： • SMB 类型资源的格式为：//IP 地址（主机名）/共享文件夹。SMB 类型资源路径只能有一级共享文件夹目录，不区分大小写。 • NFS 类型资源的格式为：//IP 地址（主机名）/dir1/dir2/共享文件夹。NFS 类型资源路径可以是多级共享文件夹目录，区分大小写。
类型	文件共享资源的协议类型： • Windows 系统下文件共享资源选择 SMB。 • Linux 系统下文件共享资源选择 NFS。
资源描述	文件共享资源的描述信息。对配置不会造成影响。

   c. 单击“确定”。

5. 新建虚拟网关下的用户。

   a. 选择“SSL VPN > 用户 > 用户组”。

   b. 在“成员管理”页签中，单击“新建”，选择“新建用户”。

参数	说明
登录名	远程用户登录虚拟网关时的名称。
密码	远程用户登录虚拟网关时的密码。
确认密码	重新输入远程用户登录虚拟网关时的密码。

   c. 单击“确定”。

6. 配置用户访问内网资源的权限。

   a. 选择“SSL VPN > 角色授权”。

   b. 单击“新建”，配置角色所具有资源访问权限。

参数	说明
角色	角色名称。
业务启用	启用该用户的业务功能。例如用户要使用文件共享业务，则需要勾选“文件共享”后的“启用”。
资源授权列表	单击“选择”，配置该角色所能访问的资源。

端口转发简介

端口转发是通过在客户端上获取指定目的 IP 地址和端口的 TCP 报文，实现对内网指定资源的访问。

端口转发的主要功能就是根据端口控制远程接入用户访问内网服务器，适用于对 TCP 应用的访问。另外，还提供以下功能：

- 客户端自动启用

  客户端登录虚拟网关页面后自动启用端口转发功能。

- 保持连接

  客户端会定时向虚拟网关发送报文，这样客户端和虚拟网关的端口转发连接不会因为 SSL 会话超时而断开，而是一直保持直到该连接的生命周期结束。

SVN 的端口转发可支持多种 TCP 应用服务，按照服务和端口对应关系分为以下几种情况：

- 支持静态端口的 TCP 应用
  - 单端口单服务：一个服务对应一个端口。

    例如：Windows 远程桌面、Telnet、SSH（Secure Shell）、VNC、ERP（Enterprise Resource Planning）、SQL（Structured Query Language） Server、iNotes、OWA（Outlook Web Access）、BOSS（Business and Operation Support System）。

  - 单端口多服务：多个服务对应一个端口。

    例如：Notes（多个数据库服务器对应一个端口）。

  - 多端口单服务：一个服务对应多个端口。

例如：POP3（Post Office Protocol 3） Email（SMTP（Simple Message Transfer Protocol）：25、POP3：110 等）。

- 支持动态端口的 TCP 应用

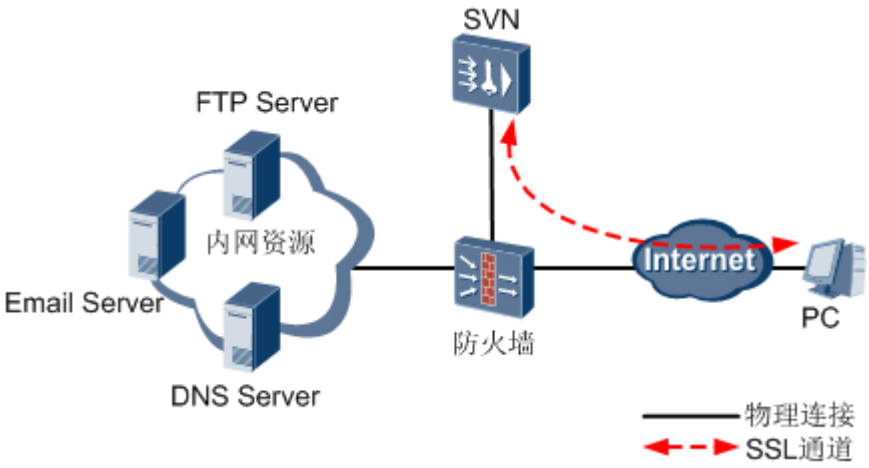
动态端口服务：一个服务对应多个动态变化的端口，例如：FTP 被动模式、Oracle Manager。

端口转发应用场景

端口转发的应用场景是保证用户对内网 TCP 应用端口级的安全访问。

端口转发的典型应用场景如图 1 所示，企业的子公司或合作伙伴等远程用户可以访问内网服务器的指定 TCP 应用。

图 1 端口转发的典型应用场景

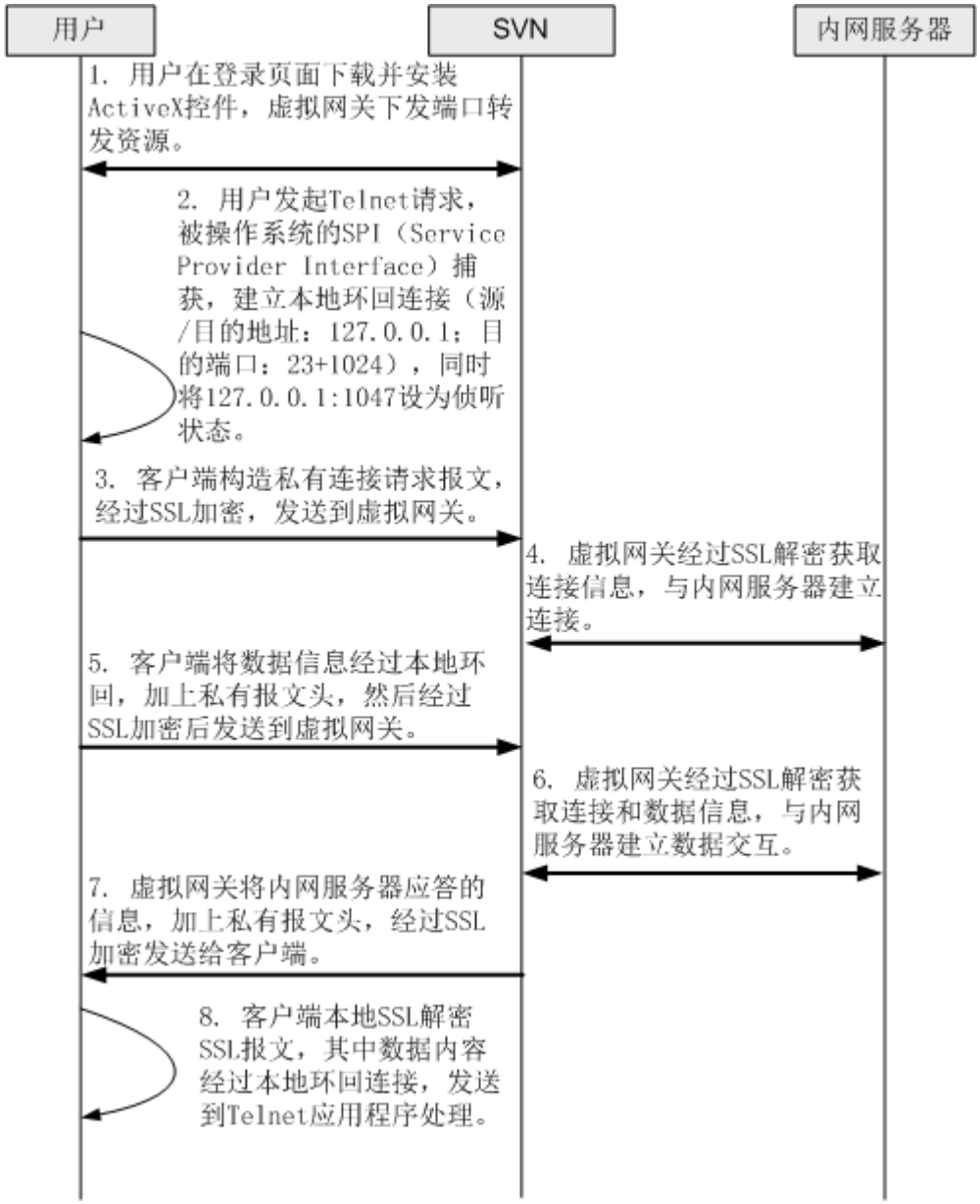


端口转发原理描述

介绍端口转发的实现原理。

端口转发需要在客户端上运行一个 ActiveX 控件作为端口转发器，用于侦听指定端口上的连接。以用户 Telnet 到内网服务器为例，端口转发的实现过程如图 1 所示。

图 1 端口转发的交互过程



配置端口转发

您需要启用端口转发功能，并为用户指定端口转发资源。

背景信息

配置端口转发，包括以下几个步骤：

1. 启用端口转发功能。

   只有启用端口转发功能后，用户才能使用端口转发业务。

2. 新建端口转发资源。

   添加终端用户可以访问的端口转发资源。

3. 新建虚拟网关下的用户。

   该用户就是访问企业内网资源的远程用户。

4. 配置用户访问内网资源的权限。

   角色是权限的集合，通过为用户分配角色，使其具有访问不同资源的权限。

操作步骤

1. 在界面右上角的“虚拟网关”中选择虚拟网关名称，进入对应的虚拟网关。
2. 选择“SSL VPN > 资源 > 端口转发”。
3. 启用端口转发功能
   a. 在“配置端口转发”区域框中，选中“端口转发功能”对应的“启用”。
   b. **可选：**根据需要选中“客户端自动启用”和“保持连接”对应的“启用”。
      - 启用“客户端自动启用”后，客户端登录虚拟网关页面后自动启用端口转发功能。
      - 启用“保持连接”后，客户端会定时向虚拟网关发送报文，这样客户端和虚拟网关的端口转发连接不会因为 SSL 会话超时而断开。
   c. 单击“应用”。
   d. 在操作成功的提示框中。单击“确定”。
4. 配置端口转发资源。
   a. 在“端口转发资源列表”区域框中，单击“新建”。

      如果新建的资源与现有资源的配置有相同之处，可以单击现有资源对应的  ，在现有资源的参数基础上新建端口转发资源。

   b. 配置端口转发资源。

参数	说明
资源名	为用户可访问的端口转发资源定义一个名称。

参数	说明
主机地址类型	用户通过哪种方式来访问端口转发资源： • 选择“主机名”后，用户可访问内网的指定域名或主机名，而无法访问其他网络中的相同域名。 此时，请确保虚拟网关上已配置 DNS 服务器，并已在 DNS 服务器上做相应配置。 • 选择“主机 IP 地址”后，用户可访问内网的指定 IP 地址，而无法访问其他网络中的对应 IP 地址。 • 选择“任意 IP 地址”后，情况如下： ▪ 如果管理员未在虚拟网关上配置 DNS 服务器，则用户可以通过 IP 地址访问内网任意主机的指定端口以及外网除指定端口外的资源，但不能以域名形式访问所有内外网资源。 ▪ 如果管理员在虚拟网关上配置了 DNS 服务器，则用户可以通过域名形式或 IP 地址访问内网任意主机的指定端口资源，也可以通过 IP 地址访问外网除指定端口外的资源，但仍不能以域名形式访问外网所有资源。 **说明：** 选择“任意 IP 地址”后将影响所有关联该资源的用户都无法使用域名访问外网，请慎重选择该主机地址类型。
主机名	供用户访问的内网主机的域名或者机器名。
主机 IP 地址	供用户访问的内网主机的 IP 地址。
端口	供用户访问的内网资源对应的 TCP 端口号。 在 TCP/IP 协议中，端口是传输层的内容，端口与应用服务一一对应。协议里面小于 1024 的端口号都有确切的定义和规定，称为知名端口。端口转发配置中常用的端口如表 1 所示。 **说明：** 对虚拟网关端口转发资源的访问控制通过目的 IP 型的策略实现。
资源描述	端口转发资源的描述信息。对配置不会造成影响。 建议在“资源描述”中描述资源的主机名或 IP 地址。“资源描述”信息会显示在虚拟网关页面上，方便用户根据主机名或 IP 地址访问。

表 1 常用服务端口号

应用服务	端口号
FTP	21
SSH	22
Telnet	23
SMTP	25
HTTP	80
POP3	110
IMAP	143

参数	说明
SQL Server	1433
Windows 远程桌面	3389
VNC	5900

c. 单击“确定”。

5. 新建虚拟网关下的用户。

a. 选择“SSL VPN > 用户 > 用户组”。

b. 在“成员管理”页签中，单击“新建”，选择“新建用户”。

参数	说明
登录名	远程用户登录虚拟网关时的名称。
密码	远程用户登录虚拟网关时的密码。
确认密码	重新输入远程用户登录虚拟网关时的密码。

c. 单击“确定”。

6. 配置用户访问内网资源的权限。

a. 选择“SSL VPN > 角色授权”。

b. 单击“新建”，配置角色所具有资源访问权限。

参数	说明
角色	角色名称。
业务启用	启用该用户的业务功能。例如用户要使用文件共享业务，则需要勾选“文件共享”后的“启用”。
资源授权列表	单击“选择”，配置该角色所能访问的资源。

网络扩展简介

在远程用户访问公司内网资源的应用场景中，Web 代理业务限制用户只能访问内网的 Web 资源，端口转发限制用户只能访问基于 TCP 的内网资源，然而用户需要访问的企业内网资源远不止这两种。为了满足用户需求，丰富用户访问内网资源的种类，SVN 还提供了网络扩展业务。在网络扩展业务中，SVN 为远程用户开发放了所有的内网资源。SVN 通过为远程用户分配私网 IP 地址，使远程用户如同企业内网用户一样，可以方便、快捷的访问内网资源。

远程用户访问企业内网资源时，其所使用的终端、浏览器、操作系统等不尽相同，为了适应用户的这种差异，

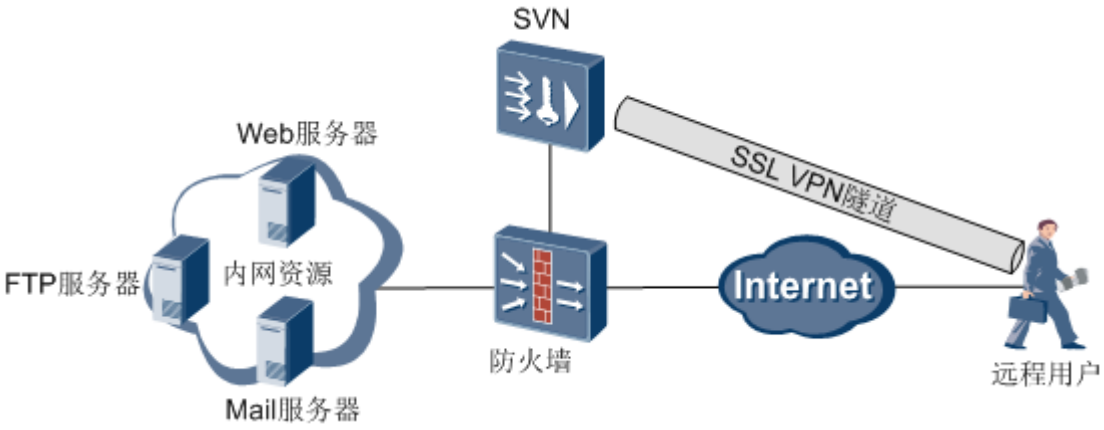
SVN 的网络扩展业务有 SSL 网络扩展和 L2TP over IPSec 网络扩展这两种不同的技术实现方案。

SSL 网络扩展

图 1 所示是 SSL 网络扩展的实现方案，远程用户和 SVN 虚拟网关之间建立的是 SSL VPN 隧道。在该方案中，用户可以使用 IE 浏览器或独立的网络扩展客户端（客户端名称：Huawei AnyOffice VPN）来登录虚拟网关。如果用户使用 IE 浏览器访问虚拟网关时，浏览器还需要安装 ActiveX 控件，该控件在用户访问 SVN 虚拟网关时，由虚拟网关推送给用户，用户只要安装运行即可。独立的网络扩展客户端可以从 SVN 的管理员处获取或是通过 IE 浏览器成功登录虚拟网关后点击客户端下载链接进行在线下载。

IE 浏览器获取方便且无需进行配置，普及率高。独立的网络扩展客户端需要稍作配置，但使用也较为简便，可以作为 SSL 网络扩展的一种辅助接入手段。

图 1 SSL 网络扩展组网图



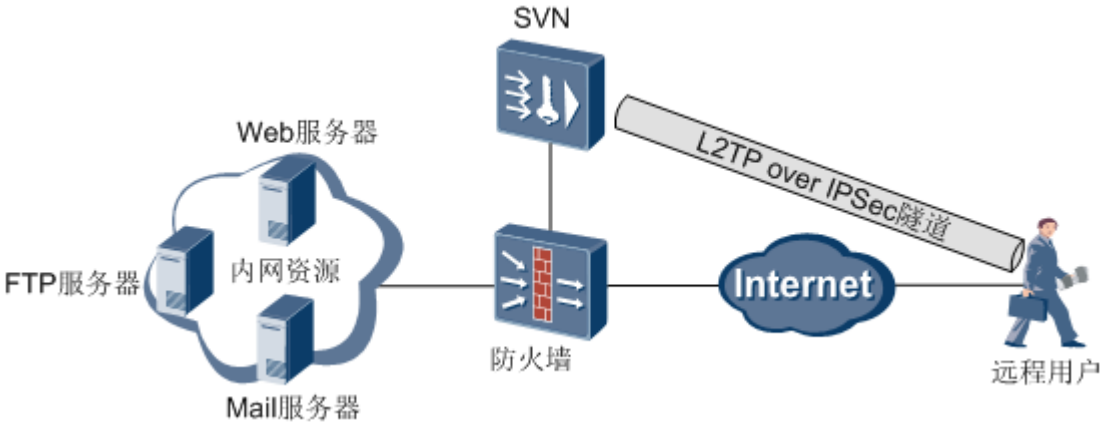
L2TP over IPSec 网络扩展

图 2 所示是 L2TP over IPSec 网络扩展的实现方案，远程用户和 SVN 虚拟网关之间建立的是 L2TP over IPSec 隧道。在该方案中，用户可以使用设备（便携机、智能手机、PAD）自带的 L2TP 客户端或独立的 VPN Client 软件来登录 SVN 虚拟网关。现有的 Windows、IOS、Android 等操作系统大多自带有 L2TP 客户端软件，用户只需要做简单配置即可使用。独立的 VPN Client 软件需要从 SVN 的管理员处获取。

说明：

- 单独使用 L2TP 也可以实现远程用户访问企业内网资源的需求，但由于 L2TP 自身不具备加密功能，因此安全性较低，不建议使用。为了提高安全性，在本方案中通常会将 L2TP 和 IPSec 配合使用，即上述的 L2TP over IPSec 网络扩展。
- 目前 SVN 还不支持智能手机使用 SSL 网络扩展功能，此场景下只能使用 L2TP over IPSec 网络扩展功能。

图 2 SSL 网络扩展组网图



SSL 网络扩展方案和 L2TP over IPSec 网络扩展方案都可以满足远程用户访问企业内网资源的需求，实际采用哪一种方案，这取决于用户终端所使用的操作系统以及浏览器类型，详细支持情况请参见规格。远程用户可以根据其终端的支持情况，选择一种简单、方便的接入方式。

业务应用

SVN 配置了网络扩展功能以后，远程用户访问企业内网资源的过程如下：

- 使用 IE 浏览器

  1. 远程用户在 IE 浏览器地址栏中输入 SVN 虚拟网关的访问地址。
  2. 出现虚拟网关登录界面后，输入用户名和密码。
  3. 登录成功的远程用户可以在虚拟网关的资源页面看到“网络扩展”页签，单击网络扩展下的“启动”，如图 3 所示。

     图 3 采用 IE 浏览器访问虚拟网关

     启动网络扩展业务以后，远程用户就相当于接入了企业总部的内网，可以和内网用户一样访问所有内网的 IP 资源。

- 使用独立客户端（包括 Huawei AnyOffice VPN 客户端、自带 L2TP 客户端、VPN Client 客户端）

  1. 远程用户在所持终端上安装独立网络扩展客户端。

部分操作系统通常是自带 L2TP 客户端，因此该客户端无需安装。

2. 配置网络扩展客户端，如配置虚拟网关的 IP 地址。

3. 在独立网络客户端的登录页面输入登录虚拟网关的用户名和密码。图 4 所示为 Huawei AnyOffice VPN 客户端连接虚拟网关界面。

图 4 采用 HUAWEI AnyOffice VPN 独立客户端访问虚拟网关

登录成功后，远程用户就相当于接入了企业总部的内网，可以和内网用户一样访问所有内网的 IP 资源。

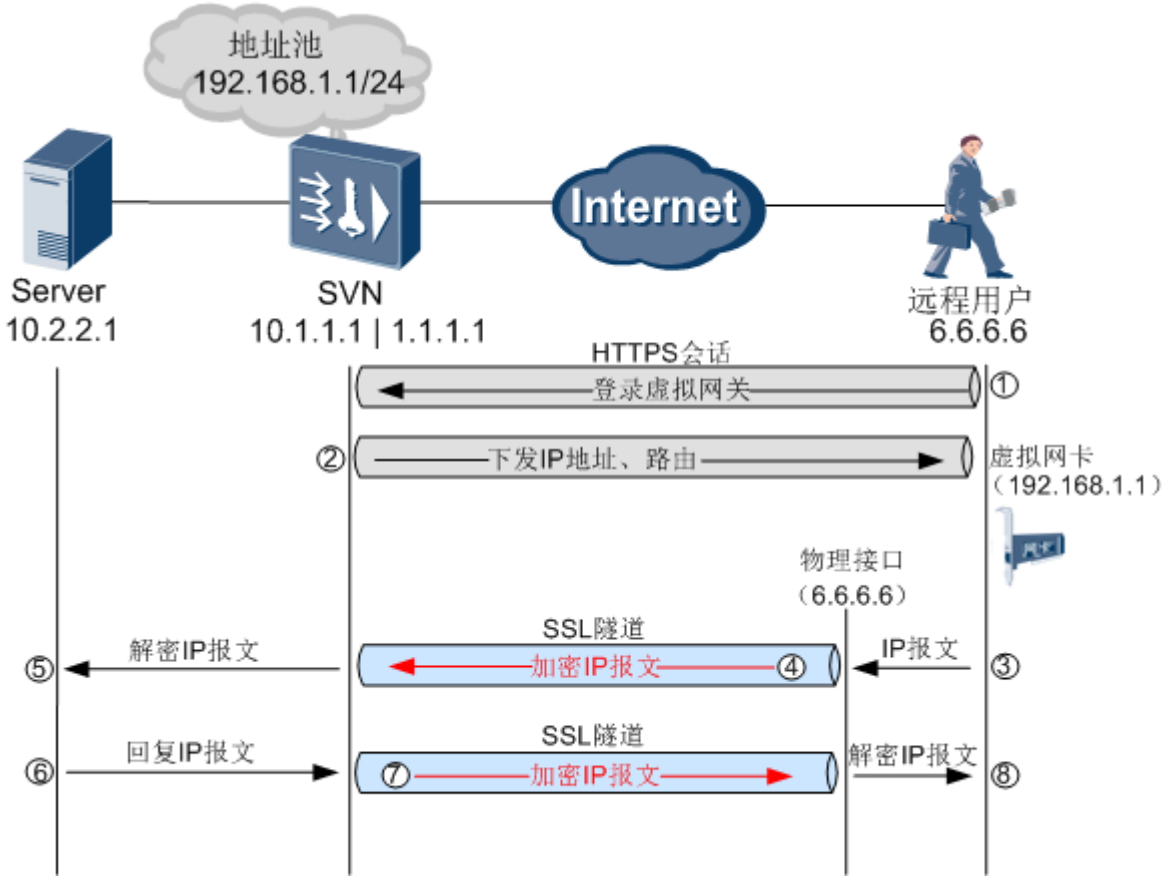
SSL 网络扩展

SVN 通过网络扩展业务，在虚拟网关与远程用户之间建立安全的 SSL VPN 隧道，将用户连接到企业内网，实现对企业 IP 业务的全面访问。

SSL 网络扩展业务交互流程

远程用户使用 SSL 网络扩展功能访问内网资源时，其内部交互过程如图 1 所示。

图 1 SSL 网络扩展业务交互流程



1. 远程用户通过 IE 浏览器登录虚拟网关，建立 HTTPS 会话。

2. 远程用户在虚拟网关上启动网络扩展功能。

   远程用户使用 IE 浏览器或 Huawei AnyOffice VPN 客户端时，系统会自动生成一个虚拟网卡。启动网络扩展功能以后，虚拟网关将向该虚拟网卡分配 IP 地址，该地址作为远程用户与企业内网之间通信之用。同时，SVN 会根据网络扩展业务中的配置，向远程用户下发不同的路由信息，该路由会影响到远程用户访问本地局域网、Internet、企业内网资源的范围。

   - 全路由模式

     当网络扩展中“客户端路由方式”选择的是“全路由模式”时，表示远程用户启用网络扩展功能以后，只能访问企业内网资源，不能访问 Internet 和本地局域网。在该模式下，远程用户从虚拟网关获取到的路由下一跳，全部指向自身虚拟网卡，即所有流量都会经过虚拟网卡封装后发往 SVN 虚拟网关。

   - 分离模式

     当网络扩展中“客户端路由方式”选择的是“分离模式”时，表示远程用户只能访问企业内网资源和本地局域网资源，但不能访问 Internet 资源。

- 手工模式

  当网络扩展中“客户端路由方式”选择的是“手工模式”时，表示远程用户在访问企业内网资源时，只能访问指定的资源（具体资源要在 SVN 虚拟网关中配置），访问本地局域网和 Internet 不受网络扩展功能影响。远程用户只能访问指定的企业内网资源是因为 SVN 虚拟网关会根据配置向远程用户下发到该资源的路由信息。对于未经配置的内网资源，由于用户本地不会生成到该资源的路由，因此无法访问。手工模式下的优点在于远程用户访问本地局域网和 Internet 不会受网络扩展的影响；其不足的地方在于需要逐个配置用户所要访问的企业内网资源，配置会比较繁琐。

SVN 虚拟网关向远程用户分配 IP、下发路由以后，还会在远程用户与虚拟网关之间建立一个新的 SSL 隧道，专门用来传输远程用户与企业内网之间的流量。

3. 远程用户向企业内网的 Server 发送 IP 报文。

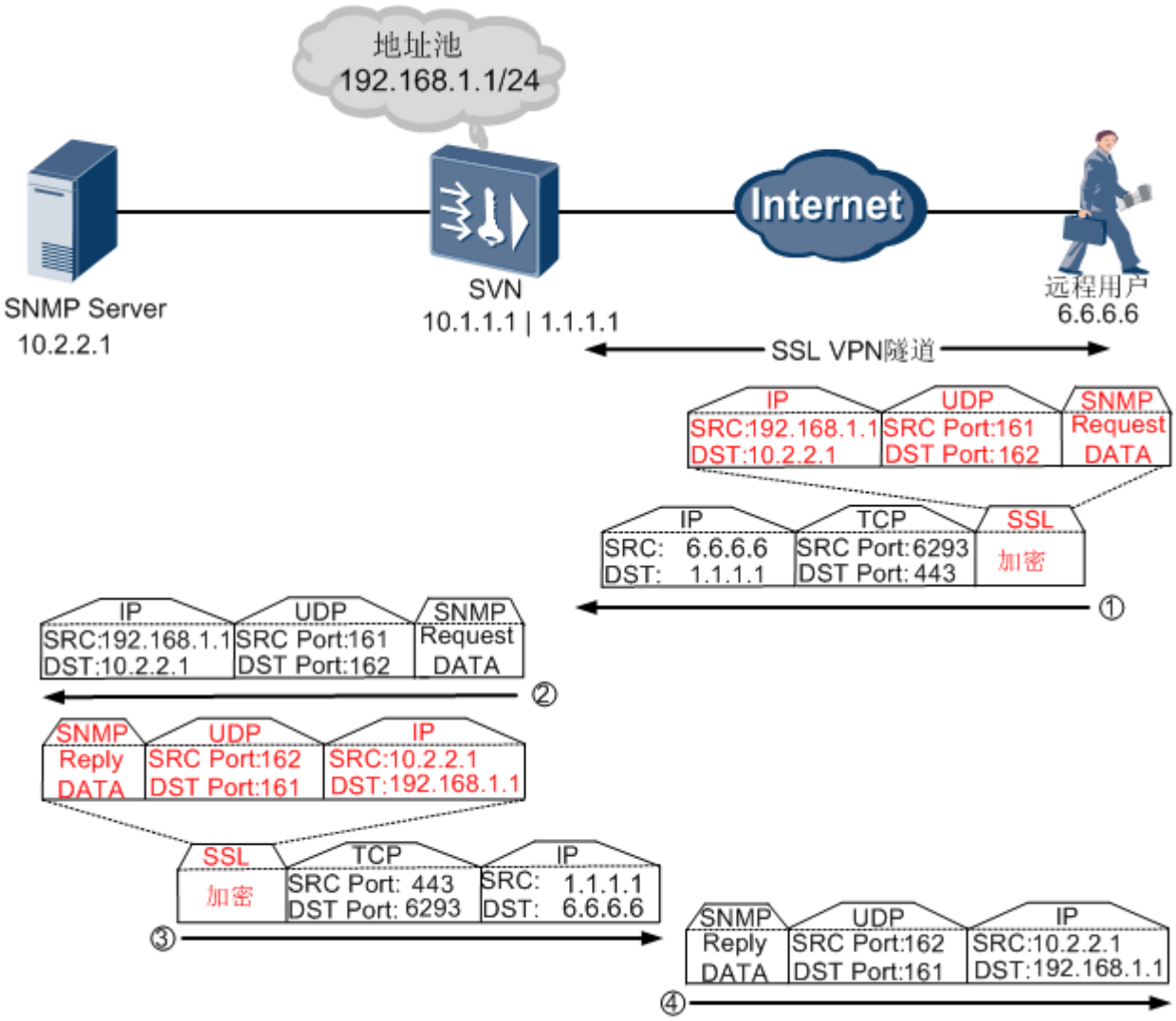
   该 IP 报文首先流向虚拟网卡，经过虚拟网卡后再进入 SSL 隧道。

4. 进入 SSL 隧道的 IP 报文被加密保护，并送往虚拟网关。
5. 虚拟网关解密远程用户发来的 IP 报文，并将解密后的 IP 报文发送给企业内网 Server。
6. 企业内网 Server 回复远程用户的资源请求，回复报文到达虚拟网关后，经过虚拟网关进入 SSL 隧道。
7. 进入 SSL 隧道的 IP 报文被加密保护，并送往远程用户。
8. 远程用户解密虚拟网关发来的 IP 报文。

SSL 网络扩展报文封装过程

图 1 所示是 SSL 网络扩展业务的报文封装过程。从图中可以看出，远程用户与企业内网（SNMP Server）之间通信的源地址（SRC：192.168.1.1）就是它虚拟网卡的 IP 地址。期间的报文交互经过往复的加解密之后安全到达通信双方。远程用户访问 SNMP Server 时，源端口是 161，目的端口是 162，传输协议使用的是 UDP。

图 2 SSL 网络扩展报文封装过程



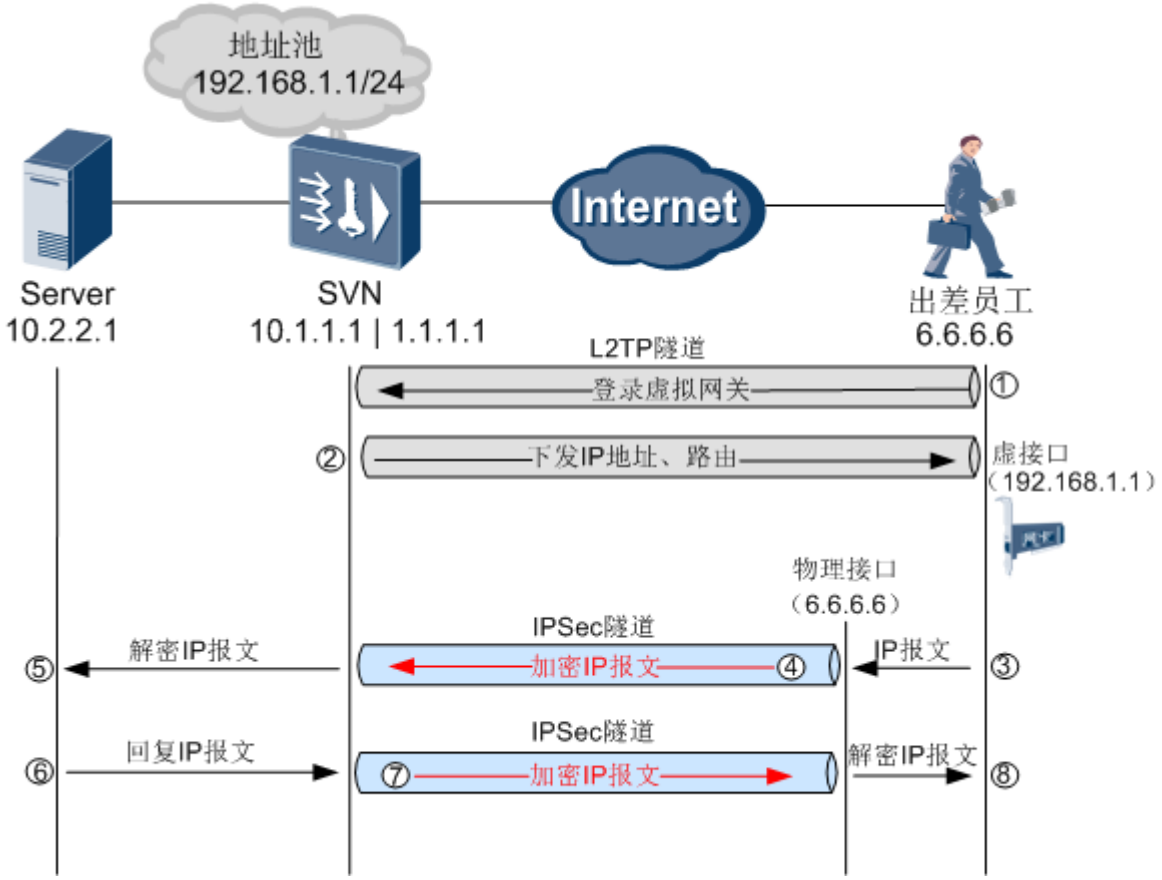
L2TP over IPSec 网络扩展

SVN 通过网络扩展业务，在虚拟网关与远程用户之间建立安全的 L2TP over IPSec 隧道，将用户连接到企业内网，实现对企业 IP 业务的全面访问。

L2TP over IPSec 网络扩展业务交互过程

L2TP over IPSec 网络扩展业务的内部交互过程如图 1 所示。

图 1 L2TP over IPSec 网络扩展业务交互流程



1. 远程用户采用 L2TP 自带客户端或 VPN Client 登录虚拟网关。

   登录成功后，远程用户会自动启用网络扩展功能。

2. 虚拟网关向远程用户分配私网 IP 地址，并下发路由信息。

   在 L2TP over IPSec 网络扩展方案中，远程用户安装网络扩展客户端以后，会在本地生成一个虚接口（其作用类似于 SSL VPN 网络扩展方案中的虚拟网卡），虚接口的 IP 地址就是虚拟网关向远程用户分配的 IP 地址。缺省情况下，远程用户获取到虚拟网关分配的私网地址以后，就只能访问企业内网的资源，不能访问本地局域网和 Internet。如果用户想在使用网络扩展业务的同时，还要访问本地局域网和 Internet，则需要在网络客户端中进行单独配置。这个路由控制方式和 SSL VPN 网络扩展的路由控制方式有所不同，SSL VPN 网络扩展中的路由是由虚拟网关上的配置决定，而 L2TP over IPSec 网络扩展中的路由是由独立客户端上的配置决定。

3. 远程用户向企业内网的 Server 发送 IP 报文。

   该 IP 报文首先流向虚接口，经过虚接口后再进入 IPSec 隧道。

4. 进入 IPSec 隧道的 IP 报文被加密保护，并送往虚拟网关。

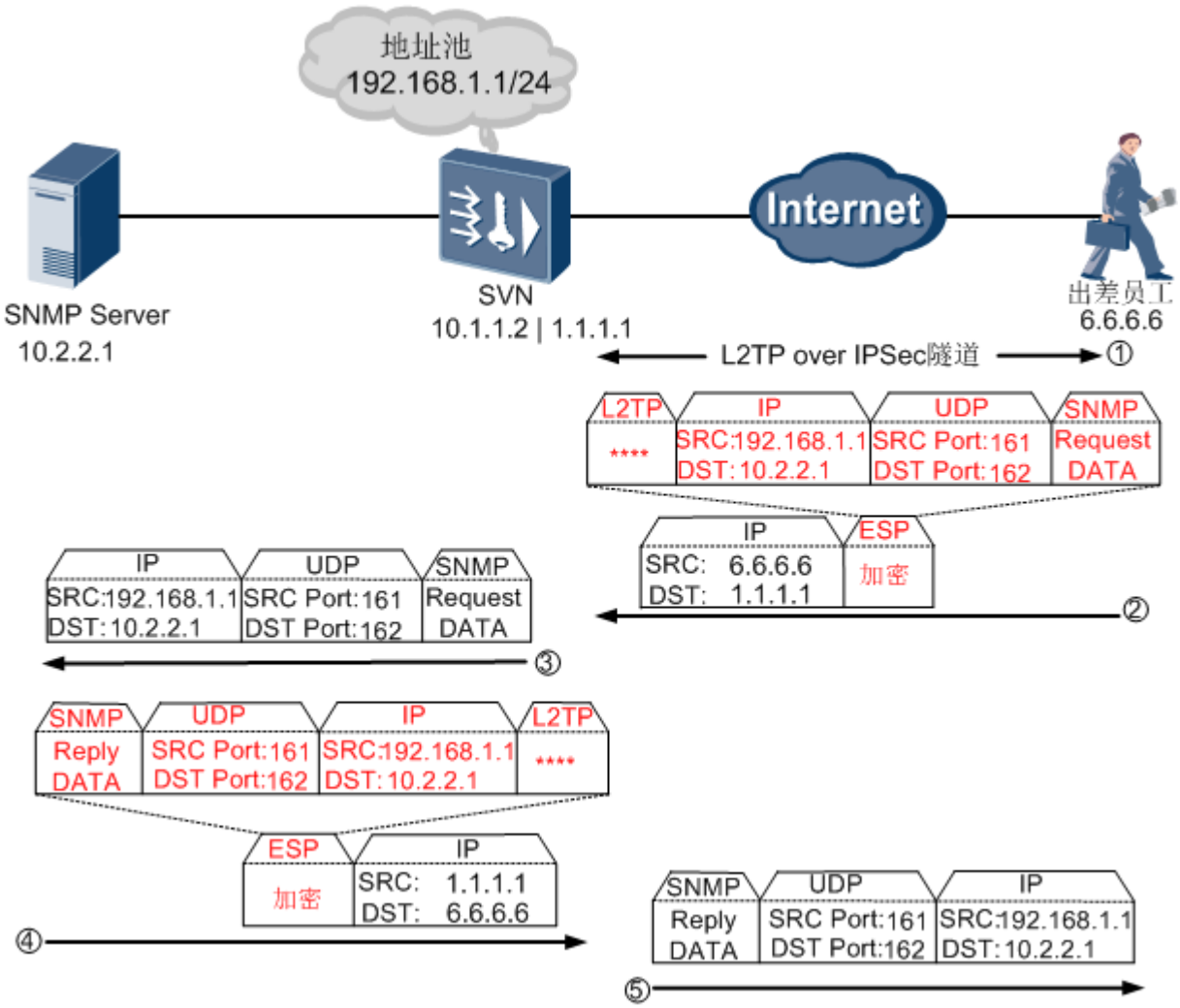
5. 虚拟网关解密远程用户发来的 IP 报文，并将解密后的 IP 报文发送给企业内网 Server。
6. 企业内网 Server 回复远程用户的资源请求，回复报文到达虚拟网关后，经过虚拟网关进入 IPSec 隧道。
7. 进入 IPSec 隧道的 IP 报文被加密保护，并送往远程用户。
8. 远程用户解密虚拟网关发来的 IP 报文。

L2TP over IPSec 网络扩展报文封装过程

图 2 所示是 L2TP over IPSec 网络扩展报文封装过程。远程用户将访问内网的报文先进行 L2TP 封装，然后再通过 IPSec（ESP 是 IPSec 中的一种加密算法）封装加密并送往 SVN。SVN 虚拟网关将解密远程用户访问 SNMP Server 的报文，并将解密后的报文转发给 SNMP Server。对于 SNMP Server 回复给远程用户的报文，SVN 会对该报文进行加密封装后，再发给远程用户，远程用户获得该报文后再解密即可。

L2TP over IPSec 网络扩展业务和 SSL VPN 网络扩展业务的交互过程和报文封装过程相似，所不同的是 SSL VPN 采用的是 SSL 隧道对数据进行加密，L2TP over IPSec 是采用 IPSec 隧道对数据进行加密。

图 2 L2TP over IPSec 网络扩展报文封装过程



配置 SSL 网络扩展

介绍 SSL 网络扩展的配置方法。

配置 SSL 网络扩展基本功能，包括以下几个步骤：

1. 启用 SSL 网络扩展功能。

   只有启用 SSL 网络扩展功能后，用户才能使用 SSL 网络扩展业务。

2. 配置客户端（即远程用户）地址分配方式。
3. 配置客户端路由生成方式。
4. 配置用户虚拟 IP 处理方式和日志连接记录方式。
5. 新建虚拟网关下的用户。

该用户就是访问企业内网资源的远程用户。

6. 配置用户访问内网资源的权限。

   角色是权限的集合，通过为用户分配角色，使其具有访问不同资源的权限。例如用户 A 的角色名称是 role，角色 role 的权限是可以访问 *http://www.svn/resource.html* 这条资源。则将用户 A 的角色配置为 role 以后，该用户就可以访问此资源。

7. 配置虚拟网关的安全策略。

配置 SSL 网络扩展

1. 启用网络扩展功能。

   a. 创建虚拟网关，并进入虚拟网关配置界面。详细步骤略，具体配置请参见创建虚拟网关。

   b. 选择“SSL VPN > 资源 > 网络扩展”。

   c. 在“SSL 网络扩展”页签中，启用“网络扩展功能”。

表 1 启用网络扩展功能参数说明	
参数	**说明**
网络扩展功能	启用虚拟网关的网络扩展功能。 只有启用网络扩展功能后，“保持连接”、“点对点通讯”后的“启用”复选框才可选。
保持连接	启用保持连接功能后，客户端会定时向虚拟网关发送报文，确保客户端和虚拟网关的网络扩展连接不会因为 SSL 会话超时而断开。
点对点通讯	启用点对点通讯功能后，同一虚拟网关的用户可以互相通讯，如同在一个局域网内部。 **说明：** 启用网络扩展的点对点通讯功能后，如果客户端路由方式采用手动模式，请将虚拟 IP 地址池包含在手动模式的 IP 网段中。

2. 配置客户端地址分配方式。

表 2 客户端地址分配方式参数说明	
参数	**说明**
DHCP 方式	使用 DHCP 方式为客户端分配 IP 地址。选择此项时，需指定 DHCP 服务器的 IP 地址。 **说明：** 在配置 DHCP 服务器可分配的 IP 地址时，该 IP 地址不能为虚拟网关 IP 地址或设备接口的 IP 地址，以免客户端地址分配失败，导致网络扩展业务无法正常使用。 在多虚拟网关的组网中，DHCP 服务器分配的 IP 地址不能和网络扩展地址池中的地址冲突。

表 2 客户端地址分配方式参数说明

参数	说明
外部获取方式	表示用户的 IP 地址由第三方服务器来分配，此时第三方服务器上需要配置虚拟 IP 地址字段。 例如用户认证是由 Radius 服务器来认证，并且用户地址也是由 Raidus 服务器来分配，则此时地址分配方式就选择“外部获取方式”。
IP 地址池方式	使用地址池方式分配客户端 IP 地址。 当“客户端 IP 分配方式”为“IP 地址池方式”时，需在“IP 地址池列表”中创建地址池，步骤如下： a. 在“IP 地址池列表”中，单击“新建”。 b. 依次输入 IP 地址池的地址范围和子网掩码。 c. 单击“确定”。 重复以上步骤，完成所有地址池的配置。 **注意：** • 选择 IP 地址池方式时，请至少指定一个 IP 地址池。SVN 网络地址池不能包含内网已经分配的 IP 地址。 • 在配置虚拟 IP 地址池时，虚拟 IP 地址池范围内的 IP 地址不能为虚拟网关或接口的 IP 地址，以免客户端地址分配失败，导致网络扩展业务无法正常使用 • 在配置虚拟 IP 地址池时，如果用户使用的操作系统为 Windows XP 及之前版本 Windows 操作系统，请不要使用包含 192.168.x.255 的地址，以免启用网络扩展失败。 • 网络扩展功能支持为指定用户分配固定 IP 地址的情况，即用户与 IP 地址存在绑定关系，该绑定关系是在创建用户时进行配置。在用户和 IP 地址池绑定的情况下可以删除地址池，删除 IP 地址池后，该用户从现有的所有地址池中获取虚拟 IP 地址。

3. 配置客户端路由生成方式。

表 3 客户端路由生成方式参数说明

参数	说明
分离模式	用户可以访问远端企业内网和本地局域网，不能访问 Internet。 **说明：** 设置客户端路由方式为分离模式时，如果客户端的本地网卡有默认网关，则这个默认网关将失效，由虚拟网卡的默认网关替代。
全路由模式	用户只允许访问远端企业内网，不能访问 Internet 和本地局域网。
手动模式	通过手动设置，用户可以访问远端企业内网特定网段的资源，对 Internet 和本地局域网的访问不受影响。当网段冲突时优先访问远端企业内网。 当“客户端路由方式”为“手动模式”时，需在“IP 网段列表”中配置允许用户访问的内网网段，步骤如下： . 在“IP 网段列表”中，单击“新建”。 a. 依次输入允许用户访问的内网 IP 网段和子网掩码。 b. 单击“确定”。 重复以上步骤，完成所有网段的配置。

4. 配置用户虚拟 IP 处理方式和日志连接记录方式。

虚拟网关下配置远程用户时，可以指定远程用户与 IP 地址的使用关系。例如，可以通过配置使远程用户 admin 固定使用 IP 地址池 10.1.1.1～10.1.1.100 中的 10.1.1.1 这个地址。而在某些情况下，用户可能需要对地址池进行修改，例如删除 10.1.1.1～10.1.1.100 这个地址池，重新建立 10.2.2.1～10.2.2.100 地址池，此时远程用户 admin 就面临地址如何分配的问题。通过此处配置，可以指定该类用户在地址池发生变更时的地址分配方式。

表 4 客户端路由生成方式参数说明

参数	说明
用户虚拟 IP 处理方式（绑定虚拟 IP 的用户）	
清除不在新地址范围内的用户虚拟 IP	表示清除不在地址池中的用户。
清除所有用户虚拟 IP	清空所有用户与虚拟 IP 地址的绑定关系。
保留所有用户虚拟 IP	保留所有用户与虚拟 IP 地址的绑定关系。
连接日志记录方式	
不记录连接日志	设置客户端与内网服务器建立 TCP 连接时不记录日志。 启用网络扩展后，每次客户端通过网络扩展与内网服务器建立 TCP 连接时，网关侧都会记录一条连接日志。如果 TCP 连接很频繁时，会在网关侧生成很多的日志信息，这样会影响其他日志信息的查看。如果您不想关注网络扩展日志信息，请选择“不记录连接日志”。
记录连接日志	设置客户端与内网服务器建立 TCP 连接时记录日志。

配置完用户虚拟 IP 处理方式和日志连接记录方式后，单击“应用”。

5. 新建虚拟网关下的用户。

. 选择“SSL VPN > 用户 > 用户组”。

a. 在“成员管理”页签中，单击“新建”，选择“新建用户”。

参数	说明
登录名	远程用户登录虚拟网关时的名称。
密码	远程用户登录虚拟网关时的密码。
确认密码	重新输入远程用户登录虚拟网关时的密码。

b. 单击“确定”。

6. 配置用户访问内网 Web 资源的权限。

. 选择“SSL VPN > 角色授权”。

a. 单击“新建”，配置角色所具有资源访问权限。

参数	说明
角色	角色名称。
业务启用	启用该用户的业务功能。例如用户要使用“网络扩展”业务，则需要勾选“网络扩展”后的启用。
资源授权列表	单击“选择”，配置该角色所能访问的资源。

7. 配置虚拟网关的安全策略。

. 配置安全策略，允许用户登录 SVN 虚拟网关。

1. 在界面右上角的“虚拟网关”中选择 root，进入 root 配置界面。

2. 选择“策略”“安全策略”，单击“新建”，配置安全策略。

参数	说明
源安全区域	选择远程用户所在的安全区域。
目的安全区域	选择“local”。
服务	选择“https”。
动作	选择“允许”。

3. 单击“确定”。

a. 配置安全策略，允许用户访问企业内网资源。

1. 选择“策略”“安全策略”，单击“新建”，配置安全策略。

参数	说明
源地址/地区	可分配 IP 地址池范围。
目的地址	可访问内网网段。
用户	允许访问此内网资源的用户或用户组。
动作	选择“允许”。

2. 单击“确定”。

配置 L2TP over IPSec 网络扩展

介绍 L2TP over IPSec 网络扩展的配置方法。

说明：

单纯使用 L2TP 方式也可以接入企业内网，但由于 L2TP 本身不具备加密功能，所以需要依赖 IPSec 来加密保护，因此推荐使用 L2TP over IPSec 网络扩展方式。

配置 L2TP over IPSec 网络扩展基本功能，包括以下几个步骤：

1. 配置 L2TP 网络扩展。

   在该方式下，有关 L2TP 的配置 SVN 会自动生成，只需要为远程用户创建地址池即可。

2. 配置 IPSec 隧道。

3. 新建虚拟网关下的用户。

   该用户就是远程访问企业内网资源的用户。

4. 配置用户访问内网资源的权限。

   角色是权限的集合，通过为用户分配角色，使其具有访问不同资源的权限。例如用户 A 的角色名称是 role，角色 role 的权限是可以访问 *http://www.svn/resource.html* 这条资源。则将用户 A 的角色配置为 role 以后，该用户就可以访问此资源。

5. 配置虚拟网关的安全策略。

配置 L2TP over IPSec 网络扩展

1. 为远程用户创建地址池。

   a. 创建虚拟网关，并进入虚拟网关配置界面。详细步骤略，具体配置请参见创建虚拟网关。

   b. 选择“SSL VPN > 资源 > 网络扩展”。

   c. 选择“L2TP 网络扩展”页签，配置为远程用户分配 IP 地址的地址池。

表 1 启用网络扩展功能参数说明

参数	说明
起始 IP 地址	为用户分配的地址池的起始 IP 地址。
结束 IP 地址	为用户分配的地址池的结束 IP 地址。不输入结束地址时，表示地址池的起始 IP 地址和结束 IP 地址是一样的。

d. 单击“应用”。

2. 配置 IPSec 隧道。

单击“应用并设置 IPSec”进行 IPSec 的参数配置。IPSec 的配置请参见配置 IPSec。

3. 新建虚拟网关下的用户。

a. 选择“SSL VPN > 用户 > 用户组”。

b. 在“成员管理”页签中，单击“新建”，选择“新建用户”。

参数	说明
登录名	远程用户登录虚拟网关时的名称。
密码	远程用户登录虚拟网关时的密码。
确认密码	重新输入远程用户登录虚拟网关时的密码。

c. 单击“确定”。

4. 配置用户访问内网 Web 资源的权限。

a. 选择“SSL VPN > 角色授权”。

b. 单击“新建”，配置角色所具有资源访问权限。

参数	说明
角色	角色名称。
业务启用	启用该用户的业务功能。例如用户要使用“网络扩展”业务，则需要勾选“网络扩展”后的启用。
资源授权列表	单击“选择”，配置该角色所能访问的资源。

5. 配置虚拟网关的安全策略。

a. 配置安全策略，允许用户登录 SVN 虚拟网关。

1. 在界面右上角的“虚拟网关”中选择 root，进入 root 配置界面。

2. 选择“策略”“安全策略”，单击“新建”，配置安全策略。

参数	说明
源安全域	选择远程用户所在的安全域
目的安全域名	选择“local”。
动作	选择“允许”。

3. 单击“确定”。

b. 配置安全策略，允许用户访问企业内网资源。

1. 选择“策略”“安全策略”，单击“新建”，配置安全策略。

参数	说明
源地址/地区	远程用户分配 IP 地址池范围。
目的地址	可访问内网网段。
用户	允许访问此内网资源的用户或用户组。
动作	选择“允许”。

2. 单击“确定”。

HCIE-Security 模拟面试问题及面试建议

1. 分别解释 SSL VPN 的 4 种应用，画图解释。