

# HCIE-Security 备考指南

## 虚拟网关（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 虚拟网关 (SVN) 需要掌握的知识点.....	1
虚拟网关简介.....	1
虚拟网关原理描述.....	2
虚拟网关应用场景.....	5
创建虚拟网关.....	7
配置虚拟网关管理员.....	9
配置虚拟网关级策略.....	10
配置 DNS.....	14
配置 SSL.....	14
登录 SSL VPN 网关.....	15
SSL 在线用户监控信息.....	19
HCIE-Security 模拟面试问题及面试建议 .....	20

## HCIE-Security 虚拟网关 (SVN) 需要掌握的知识点

- 掌握 SSL VPN 虚拟网关原理及配置

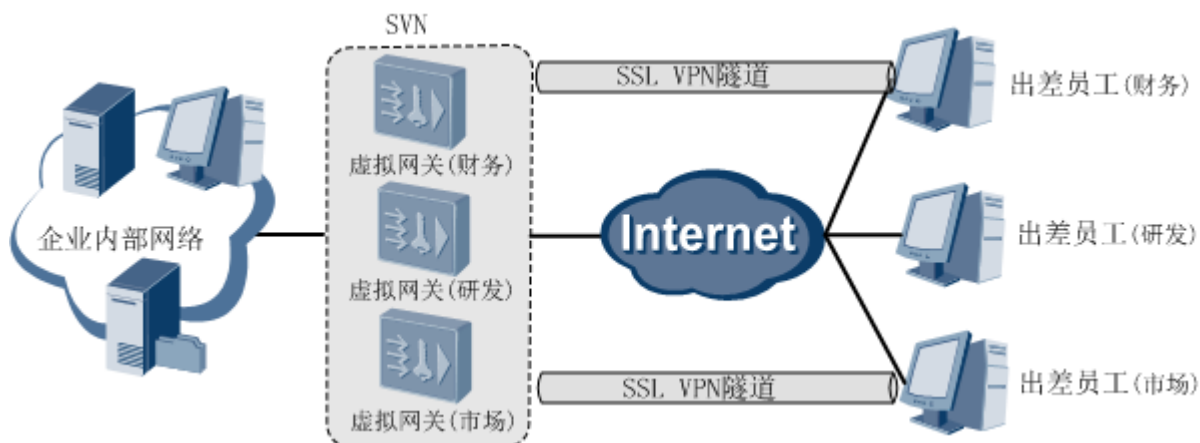
### 虚拟网关简介

介绍虚拟网关及其相关概念的定义。

SVN 作为一个网关设备可以向终端用户提供 SSL VPN 业务。一台 SVN 网关无法对其所代理的资源以及其下用户做到差异化管理。为解决该问题，一个可行方法就是将一台 SVN 网关从逻辑上划分成多台虚拟的 SVN 网关，这些虚拟的 SVN 网关可以对外独立的提供 SSL VPN 业务，从而使业务的管理更加清晰和简单。虚拟的 SVN 网关简称为虚拟网关。虚拟网关是企业将内部资源向远程用户开放的窗口，远程用户需要登录到虚拟网关后才可访问企业的内网资源。

如图1，远程出差用户都可以通过与 SVN 的虚拟网关建立隧道来安全地访问指定的内网资源。一个虚拟网关可以有其独立的资源和用户，并可以控制用户访问内网资源的权限。

图 1 虚拟网关示意图



其中虚拟网关是 SVN 上提供 SSL VPN 功能的模块，客户端是指 SSL VPN 用户使用的终端设备。客户端与虚拟网关间传输的数据都通过 SSL 协议加密。



**说明：**

为了突出表现虚拟网关，图中省略了防火墙等设备。

## 虚拟网关原理描述

介绍虚拟网关、局域网隔离的原理。

### 虚拟网关

SVN 作为一个物理实体，可以通过虚拟技术分割为多个逻辑上相互独立的 SSL VPN 网关，以提供给多个企业或者一个企业的多个部门使用。每个虚拟网关的配置和服务相互独立，虚拟网关按照 IP 地址和域名的分配方式分为两种：

- 独占型

独占型虚拟网关可以配置多个 IP 地址，且独占一个域名。该虚拟网关的用户共用这些 IP 地址，即该虚拟网关下的用户可以通过其中任何一个 IP 地址访问该虚拟网关。桌面云和负载均衡网关只支持独占型虚拟网关。

- 共享型

多个共享型虚拟网关共享同一个 IP 地址，具有相同的父域名，通过子域名来区分各虚拟网关。客户只能通过域名访问共享型虚拟网关。



#### 说明：

当企业可提供的公网 IP 地址有限的时候，可选用共享型虚拟网关。

### SSL 协议

当客户端向 SVN 发送请求时需建立 SSL 连接。[图 1](#)所示的是 SSL 协议的握手过程。

**图 1** SSL 协议握手过程

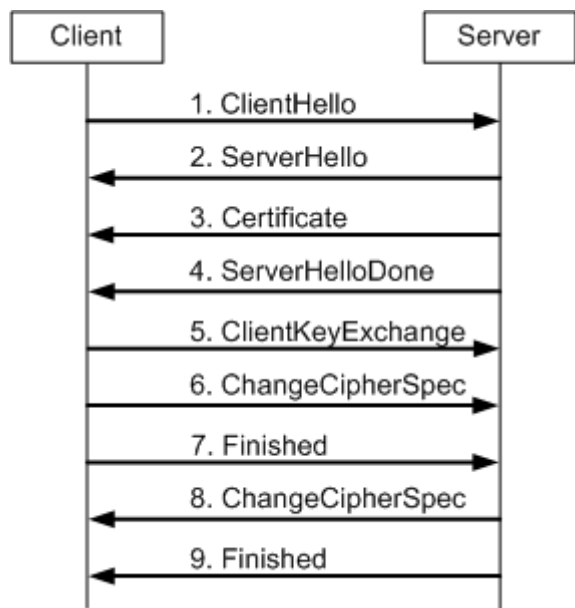


图 1 中各消息的传送步骤是：

1. 客户端向服务器发送 **ClientHello** 消息。此消息包含了客户端支持的所有 SSL 版本，加密算法列表。这些加密算法列表以优先级排序，优先级最高的加密算法列表同时也是客户端推荐的服务器使用的加密算法列表。
2. 服务器向客户端发送 **ServerHello** 消息。该消息包含了服务器从客户端选择确定的 SSL 版本、支持加密算法的套件和一个随机值。
3. 服务器通过 **Certificate** 消息向客户端发送自己的证书，使客户端确认通信对端的身份。服务器发送自己的证书时，包含自己的公钥和用自己的私钥进行的数字签名。客户端利用服务器证书对应的根证书来验证证书的真实性，用包含在证书里的公钥来检验签名，确定服务器的身份，然后用服务器的公钥加密信息，也就是说，从这一步以后，数据就是受到加密保护的了的。
4. 服务器向客户端发送一条空消息 **ServerHelloDone**，表明服务器已经发送完了在此阶段要发送的全部信息。
5. 客户端向服务器端发送消息 **ClientKeyExchange**，用公钥进行加密。在 SSL 实现中，只有在利用证书对对端进行身份验证时使用公钥加密。在实际数据传输中，使用的是效率更高的共享密钥加密方式，并用服务器证书包含的公钥对这部分信息进行加密保护。
6. 客户端向服务器端发送消息 **ChangeCipherSpec**，使用刚协商好的加密方式进行加密。
7. 客户端向服务器端发送消息 **Finished**，使用新的加密参数进行加密，并告诉服务器端信息发送完毕。另外确认没有任何消息被攻击者篡改过。
8. 服务器向客户端发送消息 **ChangeCipherSpec**，使用刚协商好的加密方式进行加密。

9. 服务器端向客户端发送消息 Finished，告诉客户端信息发送完毕。

## 局域网隔离

在创建虚拟网关时，如果需要本虚拟网关和其他虚拟网关所在的局域网相互独立，可开启局域网隔离功能。

如图2所示，企业A和企业B共用一台设备SVN，其实现局域网隔离的过程如下：

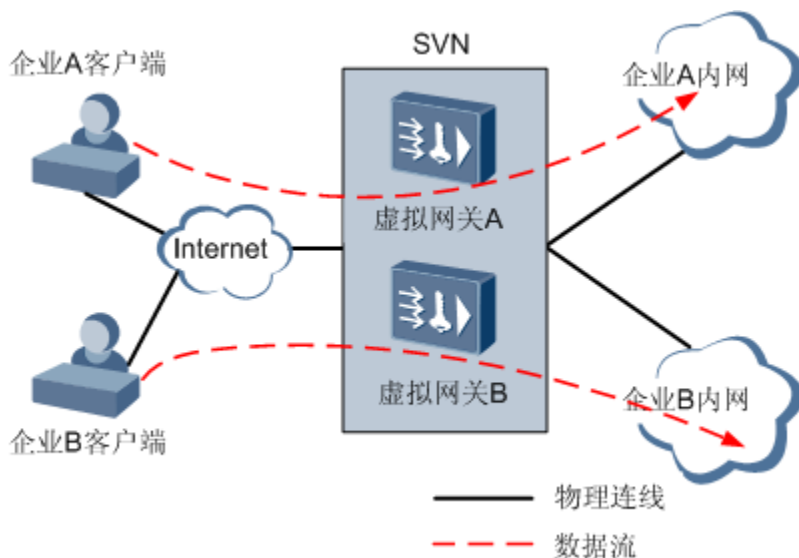
1. 在SVN上为企业A和企业B分别创建两个虚拟网关A、B，且均开启局域网隔离功能。

每个虚拟网关都拥有独立的路由转发表，当虚拟网关下的用户访问其下的内网资源时，用户的访问流量将按照该虚拟网关对应的路由表进行转发。

2. 当企业A用户访问A公司内网时，首先向SVN发送请求，请求报文按照虚拟网关A对应的路由表进行转发。同理，企业B用户访问B公司内网时，按照虚拟网关B对应的路由表进行转发。
3. 接着由SVN将企业A的报文发送至企业A内网，将企业B的报文发送至企业B内网。
4. 最后由各企业内网服务器发出响应，响应报文依然走各自虚拟网关对应的路由。

这样，不同的虚拟网关与内网的交互就可以走不同的路由，收发报文互不干扰，从而实现局域网隔离。

图2 局域网隔离实现原理图



## 虚拟网关应用场景

介绍虚拟网关和局域网隔离的应用场景。

SVN 作为一个物理实体，可以通过虚拟技术分割为多个逻辑上的 SSL VPN 网关，即虚拟网关。虚拟网关之间互相独立，每个虚拟网关可以独立配置自身的业务、用户信息，实现精细化的管理和部署。



### 说明：

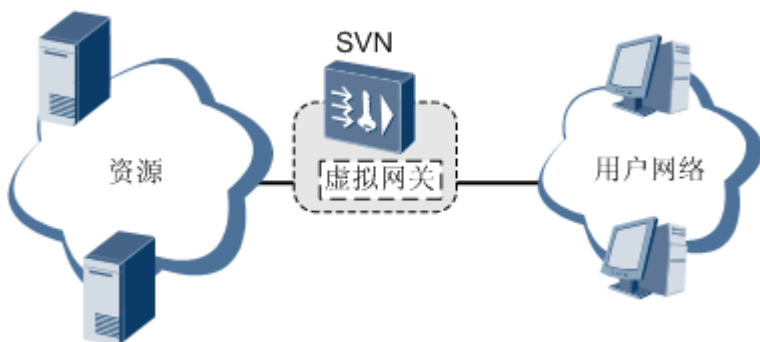
SVN 支持的虚拟网关数受 License 控制，SVN 默认支持的虚拟网关数为 1 个。用户购买虚拟网关 license 后，可用的虚拟网关规格总数等于 License 支持的虚拟网关数加 1，1 代表缺省的虚拟网关。

为了突出表现虚拟网关，图中均省略了防火墙、路由器等设备。

### 单虚拟网关

单虚拟网关的典型组网如图 1 所示，SVN 设备上只配置一个虚拟网关。所有用户均访问该虚拟网关提供的服务。用户可以从 Internet 远程接入，也可以从公司内网接入。

图 1 单虚拟网关组网图

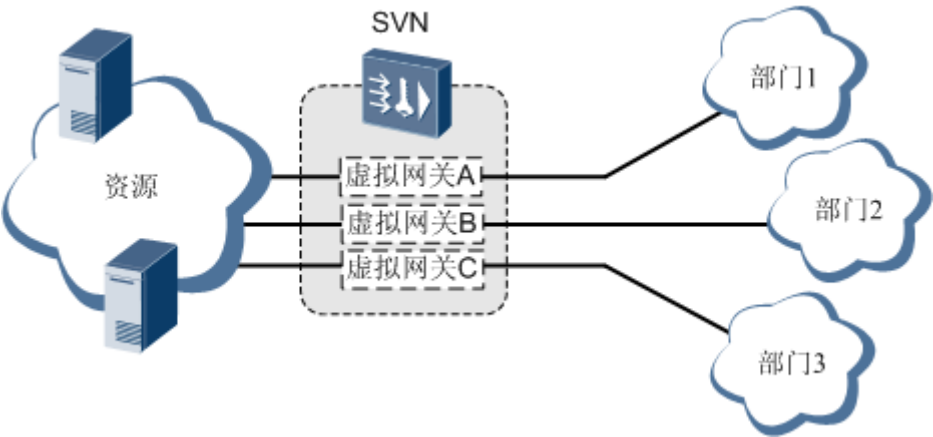


### 多虚拟网关

多虚拟网关是指在 SVN 设备上部署多个虚拟网关，通常用于企业中多个部门需要独立部署的场景。例如各部门的员工能够访问的资源和服务各不相同，有不同的访问控制规则。在这种情况下，为每个部门分配一个虚拟网关，每个虚拟网关都是独立可管理的，可以配置各自的用户、资源和策略，形成独立的运营。

多虚拟网关的典型组网如图 2 所示，其中虚拟网关 A 给部门 1 提供服务；虚拟网关 B 给部门 2 提供服务；虚拟网关 C 给部门 3 提供服务。

图 2 多虚拟网关组网图



说明：

多虚拟网关实现了业务上的独立（不同的虚拟网关提供不同的服务），没有完成物理网络的独立。例如图 2 所示的网络中，不同部门之间的 IP 地址不能冲突。

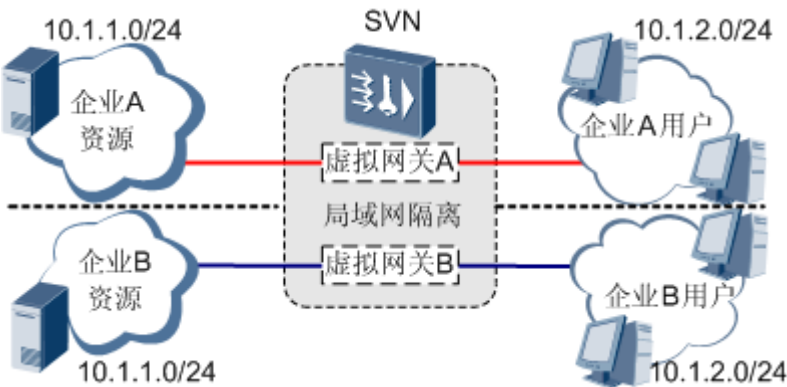
### 局域网隔离网关

局域网隔离是多虚拟网关的一种特殊应用，解决了物理网络隔离（IP 地址复用）的问题。传统的多虚拟网关不能解决该问题，需要借助局域网隔离功能。

局域网隔离将一台 SVN 从逻辑上划分为多个虚拟网关。与普通多虚拟网关不同，局域网隔离的虚拟网关更加独立，每个虚拟网关维护自己的转发信息（例如接口 IP 地址、路由等）。这样就可以实现不同的虚拟网关有自己的转发路径，解决了 IP 地址复用的问题。

局域网隔离组网图如图 3 所示，企业 A 和企业 B 规划的 IP 地址重叠，通过启用局域网隔离后，企业 A 和企业 B 的网络互不干扰，各自的报文走各自虚拟网关的路由。

图 3 局域网隔离组网图





## 创建虚拟网关

介绍新建、修改、查询、删除虚拟网关的方法。在使用 SSL VPN 业务之前，必须先创建虚拟网关。

创建虚拟网关的时候，请确认是否需要启用局域网隔离，一旦虚拟网关创建成功后，无法取消或新建局域网隔离。




### 说明：

创建虚拟网关只是配置 SSL VPN 业务的第一个步骤，要使用 SSL VPN 业务还需要对虚拟网关做进一步配置，如配置虚拟网关的管理员、定制虚拟网关页面、配置虚拟网关下的资源等等。进入虚拟网关的配置界面有两个入口：

- 在虚拟网关列表中选择要配置的虚拟网关，单击其后的**详细配置**。
- 在 Web 配置界面右上角的虚拟网关下拉列表中，选择要配置的虚拟网关。

- 选择“系统 > 虚拟网关管理”。
- 单击“新建”，依次输入或选择各项参数。


参数	说明
名称	虚拟网关名称。“root”和“public”是系统使用的关键字，不能作为虚拟网关名称。
类型	<p>虚拟网关分为：</p> <ul style="list-style-type: none"> <li><b>独占型</b> 独占型虚拟网关独占 IP 地址和域名。用户可以通过域名或者 IP 地址访问独占型虚拟网关。</li> <li><b>共享型</b> 多个共享型虚拟网关共享同一个 IP 地址，用户只能通过域名访问共享型虚拟网关。共享型虚拟网关的域名有以下两种区分方式： <ul style="list-style-type: none"> <li>父域名相同，通过子域名进行区分。如共享型虚拟网关 aaa 的域名为 <code>www.example.com/aaa</code>；共享型虚拟网关 bbb 的域名为 <code>www.example.com/bbb</code>。</li> <li>域名的第一个节点不同，后面节点都相同。如共享型虚拟网关 a 的域名为 <code>a.example.com</code>；共享型虚拟网关 b 的域名为 <code>b.example.com</code>。</li> </ul> </li> </ul> <p>当网络 IP 地址紧张时，建议使用共享型虚拟网关，减少 IP 地址占用数量。 当设备作为桌面云代理设备的网关时，请设置为“独占型”。</p>
HTTP 重定向	<p>HTTP 重定向是指将 HTTP 方式的用户请求以 HTTPS 的方式重定向到虚拟网关首页。例如：虚拟网关的首页为 <code>https://10.10.1.22</code>，域名为 <code>www.example.com</code>，启用 HTTP 重定向服务后，用户输入 <code>10.10.1.22</code>、<code>www.example.com</code>、<code>http://10.10.1.22</code> 或 <code>http://www.example.com</code> 均会以 HTTPS 方式重定向到虚拟网关的首页。</p> <p>启用 HTTP 重定向功能后，会占用 HTTP 的 80 端口，因此虚拟网关 IP 地址不能与管理 SVN 网关接口的 IP 地址相同。</p>

参数	说明
	如果不启用 HTTP 重定向，则用户无法通过 HTTP 方式访问虚拟网关。
链路备份	<p>链路备份功能是否启用：</p> <ul style="list-style-type: none"> <li>• 启用 客户端可以从 SVN 网关的多条链路中动态选择响应速度最快的链路接入。</li> <li>• 禁用 客户端不能从 SVN 网关的多条链路中动态选择响应速度最快的链路接入。</li> </ul> <p>一个虚拟网关最多配置 3 个 IP 地址。用户通过某一 IP 地址登录虚拟网关时，客户端根据该虚拟网关所有 IP 地址的响应速度，挑选响应最快的 IP 地址，并重定向到该 IP 地址访问虚拟网关。</p>
全局负载均衡加速	在桌面云中需要启用负载均衡加速功能。开启本功能后，还要配置外部 IP 作为负载均衡网关的 IP 地址，远程用户使用此 IP 地址来访问负载均衡网关。
局域网隔离	<p>本虚拟网关和其他虚拟网关对应的局域网相互独立的场景下，需要配置此功能。</p> <p>开启局域网隔离功能后，还需要将 SVN 连接不同内网的接口与其虚拟网关进行绑定，并配置到不同虚拟网关内网的路由。</p> <p>如果不开启此功能，虚拟网关所代理的内网资源 IP 地址不能重叠。</p>
IP 地址	<p>虚拟网关 IP 地址。用户可通过输入此地址来访问虚拟网关。</p> <p>在双机热备组网时，请手工配置 VRRP 地址作为虚拟网关的 IP 地址；其他情况下，请选择接口的某个 IP 地址作为虚拟网关的 IP 地址。如果新建虚拟网关时选择的接口已经被其他虚拟网关所使用，则系统会提示“IP 地址已经被占用”，此时更换一个未被使用的接口即可。</p> <p>在 DNS 负载均衡场景下才需要配置外部 IP。在“外部 IP”中输入虚拟网关 IP 地址对应的 NAT 后的公网 IP 地址。</p> <p>独占型虚拟网关可通过单击  来添加多个 IP 地址，最多可以配置 3 个 IP 地址。独占型虚拟网关的用户可以通过该虚拟网关的任一 IP 地址访问虚拟网关。</p> <p><b>说明：</b> 删除、修改 IP 地址将使虚拟网关下使用此地址登录的全部用户下线。</p>
负载均衡网关 IP 地址	<p>用户可通过输入此地址来访问负载均衡网关。</p> <p>该 IP 地址必须是某个接口上的 IP 地址，即客户端通过该接口连接负载均衡网关。</p> <p>该参数仅在桌面云代理中需要配置。</p> <p>当设备作为负载均衡网关时，需要同时开启“HTTP 重定向”。</p>
安全云网关 IP 地址	<p>用户可通过输入此地址来访问安全云网关。</p> <p>该 IP 地址必须是某个接口上的 IP 地址，即客户端通过该接口连接安全云网关。</p> <p>该参数仅在桌面云代理中需要配置。</p>
虚拟网关域名	<p>用户可通过输入此域名来访问虚拟网关。</p> <p>必须为合法域名，且外网中必须要有一台 DNS 服务器，能够将其域名解析为对应的 IP 地址。</p> <p>配置示例：<a href="http://www.example.com">www.example.com</a>（独占型）、<a href="http://vt1.company.com">vt1.company.com</a>（共享型）、<a href="http://www.example.com/aa">www.example.com/aa</a>（共享型）。</p> <p>独占型虚拟网关中，“虚拟网关域名”为选填。共享型虚拟网关中，“虚拟网关域名”为必填。</p>

参数	说明
安全云网关域名	用户可通过输入此域名来访问安全云网关。 必须为合法域名，且外网中必须要有一台实服务器，能够将其域名解析为对应的 IP 地址。
最大 SSL VPN 在线用户数	本虚拟网关允许同时接入的 SSL VPN 用户数。 SSL VPN 在线用户是指通过 SSL VPN 与虚拟网关建立连接的用户。
最大云接入在线用户数	本虚拟网关允许同时接入的云用户数。
最大用户数	本虚拟网关允许配置的最大用户数。 新建虚拟网关的最大用户数不大于系统剩余可用的用户数。
最大资源数	本虚拟网关允许配置的最大资源数。 新建虚拟网关的最大资源数不大于系统剩余可用的资源数。

3. 单击“确定”。

### 其他操作

- 修改虚拟网关：单击待修改的虚拟网关对应的  可修改参数。其中“名称”、“类型”和“创建时间”不可更改。删除、修改 IP 地址将使虚拟网关下使用此地址登录的全部用户下线。
- 查询虚拟网关：在菜单栏的下拉列表中选择“所有类型”、“独占”或“共享”，并输入对应的独占型虚拟网关名称或共享型虚拟网关名称。
- 删除虚拟网关：选中待删除的虚拟网关名前面的复选框，单击“删除”。删除虚拟网关后，原有的虚拟网关业务会断开，请注意。

## 配置虚拟网关管理员

虚拟网关管理员只可以管理其所属的虚拟网关。系统初始没有虚拟网关管理员账号。

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“系统 > 虚拟网关管理员 > 虚拟网关管理员”。
3. 单击“新建”，依次输入各项参数，配置虚拟网关管理员的基本信息。

参数	说明
管理员账号	虚拟网关管理员账号名。 此“管理员账号”即为虚拟网关管理员在 Web 登录页面中输入的管理员账号。 <b>说明：</b> 系统对虚拟网关管理员账号名的格式有要求，格式必须是“账号名@虚拟网关名”。

参数	说明
密码	虚拟网关管理员账号密码。 此密码即为虚拟网关管理员在 Web 登录页面中输入的密码。
确认密码	重新输入虚拟网关管理员账号密码。
管理员姓名	虚拟网关管理员的真实姓名。
联系电话	虚拟网关管理员的联系电话。
Email	虚拟网关管理员的 Email 邮箱地址。
角色	<p>虚拟网关管理员对虚拟网关的管理权限与其自身所扮演的角色相关。系统缺省提供了以下 3 种角色，并对这三种角色赋予了各自的缺省权限，此权限不可更改。</p> <ul style="list-style-type: none"> <li>系统管理员：系统管理员对其管理的虚拟网关有查看、配置权限，并可以为该虚拟网关创建新的管理员。</li> <li>配置管理员：配置管理员对其管理的虚拟网关有查看、配置权限，无法为该虚拟网关创建新的管理员。</li> <li>配置管理员（只读）：只读配置管理员只对其管理的虚拟网关有查看权限。</li> </ul> <p>不同的角色可以具体可以访问哪些资源，需要进入“虚拟网关管理员角色”节点，单击该角色后对应的进行查看。</p> <p>除了上述的 3 个缺省角色，系统还支持用户根据需要自定义角色。例如，用户可以自定义一个角色“abc”，并指定该角色只具有查看虚拟网关下“面板”资源这个权限。在随后新建虚拟网关管理员时，如果该虚拟网关管理员被赋予了“abc”这个角色，即表示该管理员登录虚拟网关后，只能看到虚拟网关下“面板”这个资源。</p> <p>进入“虚拟网关管理员角色”，单击“新建”即可以创建一个新角色。在“虚拟网关管理员角色”界面右上角的查询输入框中输入角色名称，可以查找指定角色。此查询功能为精确匹配，即要求输入的角色名称与角色的实际名称完全保持一致。</p>
信任主机	<p>指定可登录设备的主机 IP 地址范围，格式为：IP 地址/掩码。例如 10.1.1.1/24 或 10.1.1.1/255.255.255.0。</p> <p>可通过右边的按钮增加信任主机的范围，最多可配置 10 个。</p>

4. 单击“确定”。

## 配置虚拟网关级策略

管理员通过配置虚拟网关级策略，可以控制远程用户访问虚拟网关或企业内网资源的权限。

远程用户访问虚拟网关以及虚拟网关下代理的内网资源时，虚拟网关缺省情况下并未对该访问做控制。然而有时需要灵活控制用户的访问权限，实现用户的差异化管理，则可以通过配置虚拟网关级策略来实现此目的。

### 虚拟网关源 IP

通过用户的源 IP 地址来控制用户访问虚拟网关的权限。当用户访问虚拟网关时，如果用户的源 IP 地址命中了该策略（例如策略动作为限制），则用户访问虚拟网关失败。此方式下用户看不到虚拟网关的登录页面。

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“系统 > 虚拟网关级策略 > 策略默认行为”。
3. 勾选“虚拟网关源 IP”中的“限制”，并单击“应用”。
4. 选择“系统 > 虚拟网关级策略 > 虚拟网关源 IP 型策略”。
5. 单击“新建”，配置限制策略。

参数	说明
IP	需要控制访问权限的用户 IP 地址。
行为	策略的行为。 <ul style="list-style-type: none"> <li>• 允许：允许命中该策略的用户访问虚拟网关。</li> <li>• 限制：禁止命中该策略的用户访问虚拟网关。</li> </ul>

6. 单击“确定”。

## 用户源 IP

通过用户的源 IP 地址来控制用户访问虚拟网关的权限。当用户访问虚拟网关时，如果用户的源 IP 地址命中了该策略（例如策略动作为限制），则用户登录虚拟网关失败。此方式下用户虽然可以访问虚拟网关的登录页面，但在输入登录账号和密码后，系统会提示登录失败。

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“系统 > 虚拟网关级策略 > 策略默认行为”。
3. 勾选“用户源 IP”中的“限制”，并单击“应用”。
4. 选择“SSL VPN > 用户 > 访问控制组管理”。
5. 单击“新建”，配置访问控制策略。

参数	说明
访问控制策略组	
名称	访问控制组名称。一个访问控制组下，可以配置多条控制策略。
描述	访问控制策略组的描述信息。
访问控制策略（策略列表下单击“新建”）	
策略类型	选择源 IP 类型。
IP 类型	勾选“任意 IP”表示针对所有 IP；不勾选“任意 IP”则需要指定具体的 IP 地址/地址段。
IP 地址/IP 段	需要控制访问权限的用户 IP 地址或地址段。

- 单击“确定”。

## 用户目的 IP

通过用户的目的 IP 地址来控制用户访问虚拟网关下代理的内网资源。如果用户的目的地址命中了该策略（例如策略动作为限制），则成功登录虚拟网关以后，该用户所要访问的内网资源（用户访问的目的地址即内网资源服务器对应的 IP 地址）在虚拟网关的资源列表中无法看到，即限制访问。

- 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。
- 选择“系统 > 虚拟网关级策略 > 策略默认行为”。
- 勾选“用户目的 IP”中的“限制”，并单击“应用”。
- 选择“SSL VPN > 用户 > 访问控制组管理”。
- 单击“新建”，配置访问控制策略。

参数	说明
访问控制策略组	
名称	访问控制组名称。一个访问控制组下，可以配置多条控制策略。
描述	访问控制策略组的描述信息。
访问控制策略（策略列表下单击“新建”）	
策略类型	选择目的 IP 类型。
IP 类型	勾选“任意 IP”表示针对所有 IP；不勾选“任意 IP”则需要指定具体的 IP 地址/地址段。
IP 地址/IP 段	需要控制访问权限的用户 IP 地址或地址段。
协议类型	用户访问资源时所使用的协议类型。
端口类型	勾选“任意端口”表示针对所有端口；不勾选“任意端口”则需要指定具体的端口/端口段。
端口/端口段	用户访问内网服务器的端口/端口段。

- 单击“确定”。

## 用户 URL

通过用户所要访问的 URL 资源名称控制用户访问虚拟网关下代理的内网资源。如果用户所要访问的 URL 命中了该策略（例如策略动作为限制），则成功登录虚拟网关以后，该用户所要访问的 URL 在资源列表中无法看到，即限制访问。

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“系统 > 虚拟网关级策略 > 策略默认行为”。
3. 勾选“用户 URL”中的“限制”，并单击“应用”。
4. 选择“SSL VPN > 用户 > 访问控制组管理”。
5. 单击“新建”，配置访问控制策略。

参数	说明
访问控制策略组	
名称	访问控制组名称。一个访问控制组下，可以配置多条控制策略。
描述	访问控制策略组的描述信息。
访问控制策略（策略列表下单击“新建”）	
策略类型	选择 URL 类型。
URL 类型	勾选“任意 URL”表示针对所有 URL；不勾选“任意 URL”则需要指定具体的 URL。
URL	需要控制访问的 URL。
协议类型	用户访问资源时所使用的协议类型。
端口类型	勾选“任意端口”表示针对所有端口；不勾选“任意端口”则需要指定具体的端口/端口段。
端口/端口段	用户访问内网服务器的端口/端口段。

6. 单击“确定”。

## 策略匹配顺序

根据策略类型进行匹配，匹配顺序为：

1. 虚拟网关源 IP 型。
2. 用户源 IP 型。
3. 用户目的 IP 型/用户 URL 型。

针对每种类型的策略，其内部的匹配顺序如下：

1. 虚拟网关源 IP 型。

如果配置了多条虚拟网关源 IP 策略，则采取最长匹配原则，即掩码长的策略优先。如果没有匹配到自定义的虚拟网关源 IP 策略，则最后匹配缺省的虚拟网关源 IP 策略。



2. 用户源 IP 型、用户目的 IP 型、用户 URL 型的策略匹配规则较为复杂，具体请参见[用户授权](#)。

## 配置 DNS

配置 DNS 服务器后，用户可以通过域名访问虚拟网关的业务。配置 DNS 服务器的域名可以让用户无需输入域名后缀就能访问内网服务器。

当内网域名资源对应的 IP 地址发生变化时，网关侧的 DNS 缓存由于需要一定的时间才能老化，不能及时更新域名和 IP 地址的对应关系，用户通过域名形式访问内网资源会导致访问失败，此时需要在网关侧清空 DNS 缓存。

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“系统 > DNS”。
3. 依次输入或选择各项参数。

参数	说明
首选 DNS 服务器	首选 DNS 服务器的 IP 地址。
备选 DNS 服务器 1	当首选 DNS 服务器失效后，使用的备选 DNS 服务器地址。
备选 DNS 服务器 2	当首选 DNS 服务器和备选 DNS 服务器 1 都失效后，使用的备选 DNS 服务器。
服务器域名	配置 DNS 服务器的域名可以让用户无需输入域名后缀就能访问内网服务器。 域名只能由字母、数字和连字符组成。如果域名格式为 x.x.x，“.”之间的字符串长度不能超过 63 个字符，连字符不能为字符串的第一个字符或最后一个字符。最后一个“.”后的字符串必须至少包含一个字符。 例如：假设虚拟网关管理员配置服务器域名为 example.com，当用户要访问 URL 是 http://oa.example.com，只需要输入 oa 即可访问该 URL。 当 SVN 设备进行域名访问时，本配置无效。

4. 单击“应用”。

## 配置 SSL

配置设备使用 SSL 协议的版本、加密套件、会话超时时间和生命周期。可选配置，可直接使用默认值。

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“系统 > SSL 配置”。
3. 依次输入或选择各项参数。



参数	说明
SSL 版本	设备支持的 SSL 版本。客户端必须支持这些版本才能接入虚拟网关。
加密套件	<p>加密套件用来对客户端发给虚拟网关的数据进行加密。</p> <p><b>说明：</b> rc4-sha, rc4-md5 和 des-cbc-sha 算法安全性较弱，建议使用 aes256-sha 等其他安全性较强的算法。</p> <p>如果客户端使用的操作系统为 Windows XP，则设备需要支持 des-cbc3-sha 或 des-cbc-sha 算法，否则客户端将无法登录到虚拟网关。</p> <p>客户端和虚拟网关在数据通信前，需要协商加密套件，其过程如下：</p> <ol style="list-style-type: none"> <li>客户端首先向虚拟网关发送加密套件提议。 例如客户端建议虚拟网关后续使用“256-bit AES encryption with RSA and a SHA MAC”加密套件对数据进行加密。</li> <li>虚拟网关查找自己所有的加密套件，然后将结果告知客户端。 如果此时虚拟网关存在“256-bit AES encryption with RSA and a SHA MAC”加密套件，则接受客户端的这个提议。如果虚拟网关上不存在该加密套件，加密套件协商失败。</li> </ol> <p>加密套件是加密算法和 HASH 算法的组合。加密算法的区别如下：</p> <ul style="list-style-type: none"> <li>RC4 的算法原理基于数据流段 (stream)，速度相对于其他加密算法较快。但是 RC4 需要与认证算法 RSA 一起使用来确保安全，即一般以加密套件的形式使用，而不单独使用。</li> <li>AES、DES、3DES 的算法原理基于数据块 (block)，一般可以单独使用，也可以结合认证算法一起使用。</li> <li>3DES 的密钥长度是 DES 的三倍，相对于 DES 不易被破解。</li> <li>AES 是一种较新的加密算法，比 DES 和 3DES 更安全。</li> <li>RSA 是非对称加密算法，一般用于密钥交换或身份验证。</li> </ul> <p>设备支持的 HASH 算法包括 SHA-1 和 MD5：</p> <ul style="list-style-type: none"> <li>MD5 算法使用 128 位的密钥，MD5 算法的计算速度比 SHA-1 算法快。</li> <li>SHA-1 算法使用 160 位的密钥，SHA-1 算法的安全强度比 MD5 算法高。</li> </ul>
会话超时时间	<p>会话超时时间亦称老化时间，指在没有流量通过的情况下，断开用户连接的时间。当达到会话超时时间时，客户端和服务端要重新互相认证。</p> <p>如果允许用户使用一个账号在多处同时登录虚拟网关，建议“会话超时时间”保留默认值。</p>
生命周期无限制	不限制生命周期。用户登录虚拟网关后，会一直处于连接状态，不会自动断开。
生命周期	<p>当用户的连接时间达到生命周期值时，虚拟网关会自动断开。如果用户想继续访问虚拟网关，需要重新登录虚拟网关。</p> <p>选中“生命周期无限制”后，“生命周期”不可配。</p>
SSL 压缩	对 SSL 会话进行压缩能够提高数据的传输效率。

4. 单击“应用”。

## 登录 SSL VPN 网关

介绍在 SSL VPN 配置完成后，用户如何登录 SSL VPN 网关，使用 SSL VPN 业务。

## 操作步骤

1. 从 SVN 的管理员处获取用户登录信息。

根据 SSL VPN 的用户认证方式不同，获取的用户登录信息和进行的操作不同：

- 本地认证、服务器认证：获取用户名和密码。
- 证书匿名认证：获取并安装客户端证书。
- 证书挑战认证：获取客户端证书和密码，安装客户端证书。

2. 在电脑的浏览器中输入 **https://网关地址:端口**或 **https://域名**后，单击回车键。

### 说明：

如果用户 PC 运行的是 64 位的 Windows 7 操作系统，则要求使用 32 位的 IE 浏览器访问虚拟网关。因为兼容性的问题，使用 64 位的 IE 浏览器会导致访问虚拟网关失败。

3. 在弹出的安全警报中选择“是”，进入 SSL VPN 网关登录界面。

如果用户希望消除安全警报，操作步骤如下：

- a. 在 SSL VPN 网关登录界面单击“点此下载证书”，下载 CA 证书。
  - b. 在本地电脑上安装证书。安装证书的方法请单击“如何安装证书”查看。
4. 在 SSL VPN 网关登录界面输入用户信息后，单击“登录”。

根据 SSL VPN 的用户认证方式不同，需要输入和选择的信息不同，具体如下所示：

- **图 1** 用户认证、服务器认证



- 图 2 证书匿名认证



- 图 3 证书挑战认证



5. 在 SSL VPN 网关界面上使用各种 SSL VPN 业务。

如[图 4](#)所示，SSL VPN 网关界面显示用户可以使用的 SSL VPN 业务。

 说明：

不同用户能够使用的 SSL VPN 业务不同，[图 4](#) 仅供参考。

图 4 SSL VPN 业务



SSL VPN 业务的使用方法如下：

- Web 代理

单击“Web 代理”下的资源名称，例如单击“ERP”。

- 网络扩展提供了 Web 和客户端软件两种使用方式：
  - 登录虚拟网关后，单击网络扩展页签下的“启动”，将自动安装虚拟网卡获取虚拟 IP 地址，如下图所示。



- 单击右上角的“用户选项”，通过下载网络扩展客户端软件，使用网络扩展业务。



**说明：**

网络扩展客户端软件需在未登录虚拟网关的情况下使用。网络扩展客户端界面中的“地址”即为虚拟网关地址。

## SSL 在线用户监控信息

介绍如何查看 SSL 在线用户信息。

### 查看在线用户列表

- 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。
- 选择“监控 > 在线用户监控 > SSL 在线用户监控信息”，在“SSL 在线用户监控列表”区域框中，查看在线用户信息。

参数	说明
用户	单击用户前对应的复选框，可选中该用户。
用户类型	登录用户的类型。
域名	用户所属的域。
登录 IP	用户上线时所使用的 IP 地址。
用户上线时间	用户成功登录虚拟网关的时间。
获取的虚拟 IP 地址	登录用户获取到的虚拟 IP 地址。 对于访问网络扩展业务的用户，此处显示用户被分配的虚拟 IP 地址。
上行流量 (MB)	用户访问虚拟网关时，发送给虚拟网关的报文流量。
下行流量 (MB)	用户访问虚拟网关时，虚拟网关发送给用户的报文流量。
认证方式	虚拟网关对此用户采用的认证方式。

### 相关操作

除了查看 SSL 在线用户以外，虚拟网关管理员还可以对 SSL 在线用户进行排序或是断开某个在线用户访问虚拟网关的连接。

- SSL 在线用户排序

在“用户排序：”后的下拉框中选择排序条件。

HCIE-Security 备考指南 虚拟网关 (SVN)

参数	说明
在线时间	根据用户上线时间的先后顺序进行排序。
上行流量	根据上行流量的大小进行排序。
下行流量	根据下行流量的大小进行排序。

- 断开 SSL 在线用户

在虚拟网关列表中，勾选一个或多个表项最左侧的复选框，单击“切断”，表示断开已选中的这些 SSL 在线用户。如果想断开所有 SSL 在线用户，单击“切断所有用户”即可。

## HCIE-Security 模拟面试问题及面试建议

1. 虚拟网关的作用和原理是什么？