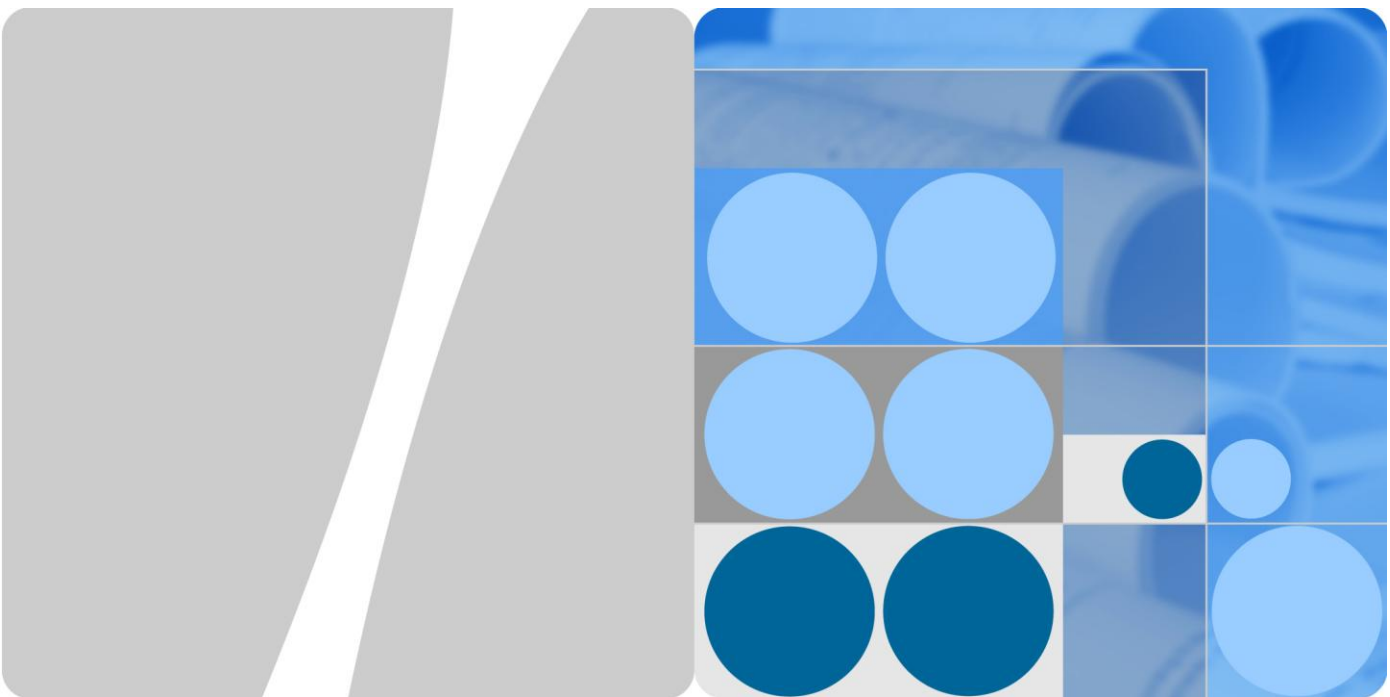




eSpace UC SVN 配置案例

文档版本 01
发布日期 2012-07-05

华为技术有限公司



版权所有 © 华为技术有限公司 2008-2012。 保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： <http://www.huawei.com>

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

目 录

1 配置场景	1
1.1 配置目标.....	1
1.2 场景组网.....	2
1.3 参数规划.....	2
2 配置流程	4
3 配置前准备	5
3.1 建立物理连接	5
3.2 配置 IP 地址	6
3.3 导入系统 License	7
4 配置过程	9
4.1 登录 Web 网管	9
4.2 创建虚拟网关	10
4.3 配置网络扩展信息	12
4.4 配置 VPNDDB 用户	13
4.5 配置 DNS 和域名（可选）	14
4.6 保存配置	15
5 配置关键点	16
6 结果验证	17

1 配置场景

关于本章

介绍 SVN 配置基于的场景。

1.1 配置目标

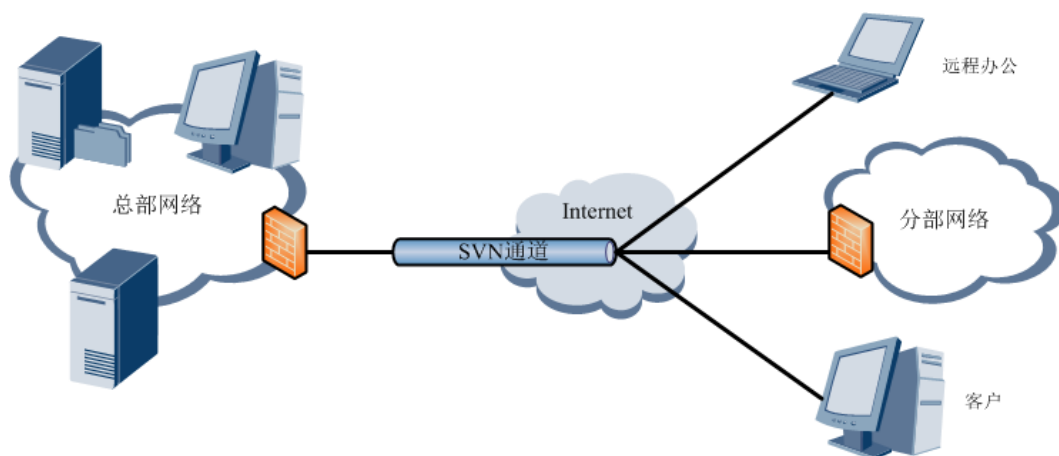
1.2 场景组网

1.3 参数规划

1.1 配置目标

利用 Internet 公网资源在企业分部、企业总部和内外网用户之间建立一个安全加密的、完整性保护的数据传输通道，如图 1-1 所示。

图1-1 SVN 数据传输通道



通过识别传输协议类型对网络数据进行 SSL 或者 UDP 隧道封装，为用户认证提供了安全加密传输，并实现通信数据在复杂网络环境下的传输。

1.2 场景组网

SVN 一般部署在网络出入口防火墙或者交换机之后，位于防火墙/交换机与内网服务器之间。

SVN 可以单臂挂接在出入口防火墙或者交换机上，如图 1-2 所示，也可以双臂挂接在防火墙和交换机之间，如图 1-3 所示。

图1-2 SVN 单臂模式应用组网图

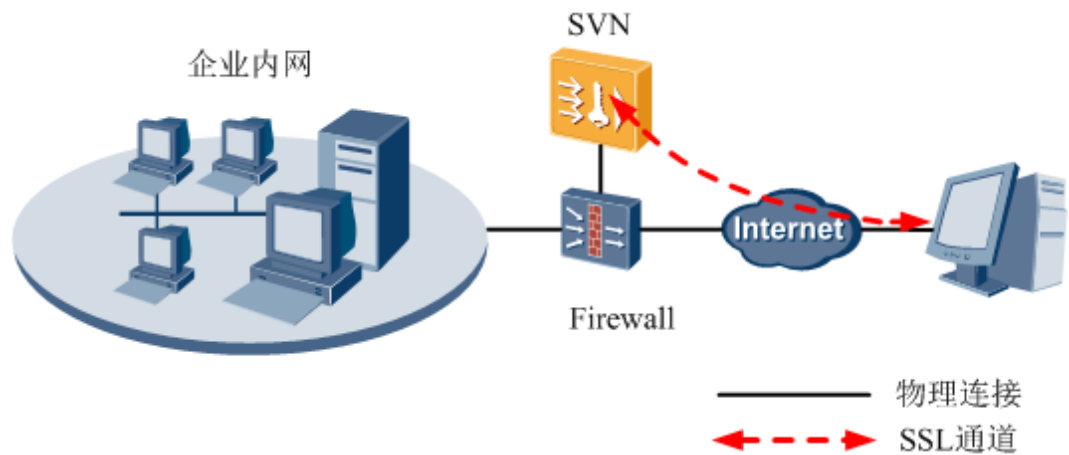
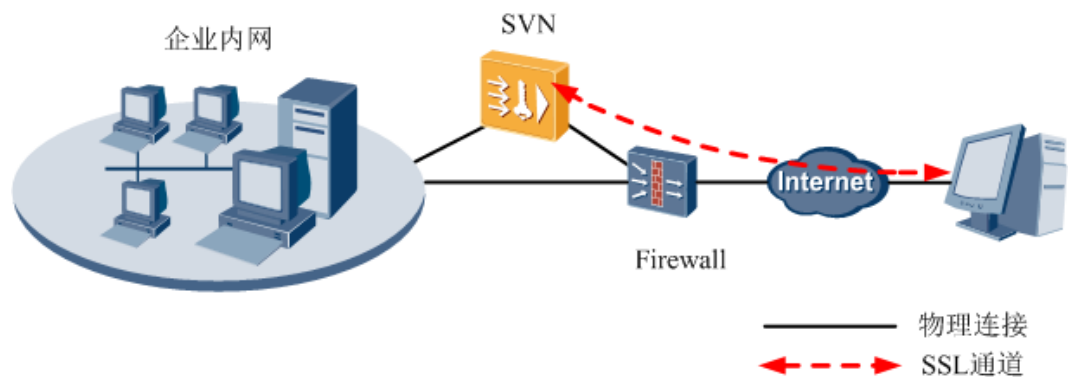


图1-3 SVN 双臂模式应用组网图



1.3 参数规划

SVN 配置的相关参数如表 1-1 所示。

表1-1 SVN 配置相关参数

配置参数	IP 地址	子网掩码	网关地址
SVN 外网 IP 地址	11.11.11.1	255.255.255.0	11.11.11.1
SVN 内网 IP 地址	192.162.1.5	255.255.255.0	192.162.1.1
Web 网管 IP 地址	192.162.1.5	255.255.255.0	192.162.1.1
虚拟 IP 地址池	192.162.1.10~192.162.1.250	255.255.255.0	192.162.1.1
虚拟网关 IP 地址	11.11.11.1	255.255.255.0	-

2 配置流程

以 SVN3000 为例，介绍 SVN 的配置过程。配置流程如[图 2-1](#) 所示。

图2-1 SVN 配置流程



3 配置前准备

关于本章

3.1 建立物理连接

SVN3000 提供了一个 EIA/TIA-232 异步串行配置口（Console），通过这个接口用户可完成对 SVN3000 的配置。

3.2 配置 IP 地址

配置 IP 地址并启用 Web 网管后，才能登录 Web 网管进行 SVN 的配置操作。

3.3 导入系统 License

未导入系统 License 的情况下，默认只能有两个虚拟网关和 10 个用户，建议在使用 Web 网管功能前，先导入系统 License。

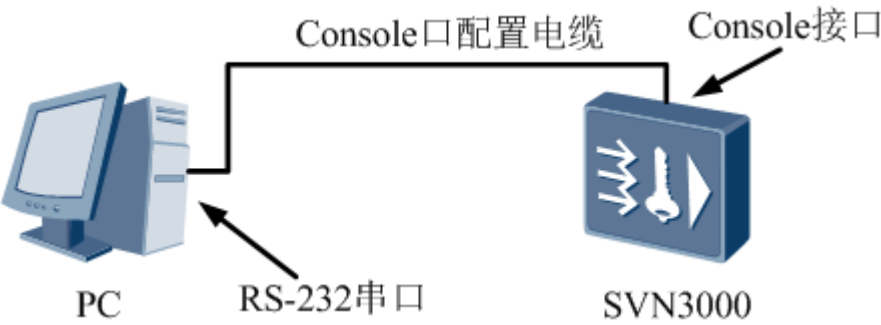
3.1 建立物理连接

SVN3000 提供了一个 EIA/TIA-232 异步串行配置口（Console），通过这个接口用户可完成对 SVN3000 的配置。

操作步骤

- 步骤 1 使用配置口电缆将 PC 的 RS-232 串口和 SVN3000 的 Console 接口相连，如[图 3-1](#)所示。

图3-1 Console 口连接



步骤 2 通过 PC 超级终端工具连接 SVN3000。

参数设置如表 3-1 所示。

表3-1 配置终端参数（以 Windows xp 超级终端为例）

参数项	参数值	参考路径
每秒位数	9600	-
数据位	8	-
奇偶校验	无	-
停止位	1	-
数据流控制	无	-
终端仿真	VT100	在“超级终端窗口”，单击“文件 > 属性 > 设置”
用户名和密码	admin/Admin@123	-

----结束

3.2 配置 IP 地址

配置 IP 地址并启用 Web 网管后，才能登录 Web 网管进行 SVN 的配置操作。

操作步骤

步骤 1 执行 **system-view** 命令，进入系统视图。

步骤 2 执行 **interface GigabitEthernet interface-number** 命令，进入以太网接口视图。

interface-number 代表接口，如 0/0 和 0/1。



说明

在 SVN5300 中，相应的接口为 0/0/0 和 0/0/1。

步骤 3 执行 **ip address ip address net-mask** 命令，配置接口的 IP 地址。

ip address 代表 IP 地址，*ip address net-mask* 代表子网掩码。

步骤 4 执行 **quit** 命令，退回系统视图。

步骤 5 执行 **web-manager ip address ip-address[port port-number]** 命令，绑定 IP 地址和 Web 网管。

port-number 代表端口号。

----结束

任务示例

以规划参数为例进行配置。

1. 执行 **interface GigabitEthernet 0/0** 命令，进入以太网接口 0 视图。
2. 执行 **ip address 11.11.11.1 255.255.255.0** 命令，配置接口外网 IP 地址。
3. 执行 **interface GigabitEthernet 0/1** 命令，进入以太网接口 1 视图。
4. 执行 **ip address 192.162.1.5 255.255.255.0** 命令，配置接口内网 IP 地址。
5. 执行 **quit** 命令，退回系统视图。
6. 执行 **web-manager ip address 192.162.1.5** 命令，绑定 Web 网管的 IP 地址为内网 IP 地址。



说明

- SVN3000 可以同时提供最多 2 个接口地址作为 Web 网管地址。
- Web 网管默认端口号为 443，如果绑定 Web 网管和 IP 地址时设置的端口号为 443 以外的端口号，那么在下次登录 Web 网管输入 IP 地址时，请在 IP 地址后面加上“端口号”，如“https://x.x.x.x:port”，否则将不能登录 Web 网管。

绑定 Web 网管的 IP 地址后，您可以通过此 IP 地址访问 Web 网管。



注意

请确保防火墙上已开放 SVN3000 的相关端口，通常为 443 端口。

3.3 导入系统 License

未导入系统 License 的情况下，默认只能有两个虚拟网关和 10 个用户，建议在使用 Web 网管功能前，先导入系统 License。

下载系统 License

步骤 1 把要导入的系统 License 文件放到 FTP 服务器上。

步骤 2 使用超级终端工具登录 SVN3000。

步骤 3 执行 **ftp host-ip** 命令，进入 FTP 客户端视图。

host-ip 为 FTP 服务器的 IP 地址。

步骤 4 输入 FTP 服务器的用户名和密码。

步骤 5 执行 **dir** 命令，查看当前 FTP 服务器的目录。

步骤 6 执行 **get source-file-name [filepath]** 命令，用 FTP 下载系统 License 文件到 SVN3000 上。

source-file-name 为系统 License 文件的名称，*filepath* 为系统 License 文件在 SVN3000 上规划的存放路径。

----结束

激活系统 License



更新 license 时，如果新 license 中的虚拟网关数和并发用户数比原配置的小，则导入新 license 后，原配置中超出原有 license 限额部分不会被加载，这些多余的虚拟网关将无法查看和使用。因此在导入新 license 之前，请先检查虚拟网关数和并发用户数，保证所有虚拟网关的并发用户数之和以及虚拟网关数分别小于新 license 的并发用户数和虚拟网关数。

步骤 1 执行 **license file filename** 命令，激活系统 License。

步骤 2 执行 **reboot** 命令，重新启动设备。

----结束

4 配置过程

关于本章

- 4.1 登录 Web 网管
- 4.2 创建虚拟网关
- 4.3 配置网络扩展信息
- 4.4 配置 VPNDDB 用户
- 4.5 配置 DNS 和域名（可选）
- 4.6 保存配置

4.1 登录 Web 网管

步骤 1 运行网络浏览器，在地址栏输入 SVN3000 Web 网管的 IP 地址，例如“https://192.162.1.5:443”，按“Enter”键。

系统进入 Web 网管登录界面。

步骤 2 输入用户名和密码，登录 SVN3000。

系统进入 Web 网管主页，如图 4-1 所示。

图4-1 Web 网管主页



说明

为安全起见，管理员首次登录后，请在“系统管理 > 管理员帐号管理”中修改密码，并创建新的系统管理员来管理 SVN3000。

----结束

4.2 创建虚拟网关

步骤 1 在“系统管理”导航树上单击“虚拟网关管理”。

系统进入网关配置页面。



说明

SVN5300 的虚拟网关配置路径为“SSL 虚拟网关 > 虚拟网关”。

步骤 2 单击虚拟网关列表右下方的“添加”。

系统进入“添加虚拟网关”页面。

步骤 3 填写相关配置信息，如图 4-2 所示。

图4-2 添加虚拟网关

虚拟网关管理 >> 添加虚拟网关

虚拟网关名	test	* 字母、数字或下划线，1~15个字符
虚拟网关类型	独占	
IP地址	11 . 11 . 11 . 1	* 添加IP地址
虚拟网关域名		示例: www.company.com(独占型), vt1.company.com(共享型), www.company.com/aa(共享型)
HTTP重定向	☒	启用HTTP重定向服务
最大并发用户数	20	* 1~1980, 默认为1 (系统限额:2000, 当前剩余可用并发用户数:1980)
最大用户数	20	* 1~29980, 默认为1 (系统限额:30000, 当前剩余可用用户数:29980)
最大管理员数	20	* 1~1260, 默认为1 (系统限额:1280, 当前剩余可用管理员数:1260)
最大资源数	20	* 1~102380, 默认为1 (系统限额:102400, 当前剩余可用资源数:102380)

- 在“虚拟网关名”中输入虚拟网关名称。
- 在“虚拟网关类型”中选择虚拟网关的类型。
虚拟网关类型有两种：独占型和共享型。
 - 独占型：虚拟网关独占一个 IP 地址和域名。
 - 共享型：多个虚拟网关共享一个 IP 地址，具有相同的父域名，通过子域名来区分各虚拟网关。
- 在“IP 地址”中输入虚拟网关的 IP 地址。
虚拟网关的 IP 地址必须已经在接口或者子接口上进行配置。
- 在“虚拟网关域名”中输入虚拟网关的域名。
独占型虚拟网关中，此项为选填，共享型虚拟网关中，此项为必填。
- 请按照实际需求，在“最大并发用户数”、“最大用户数”、“最大管理员数”和“最大资源数”填入相关参数。

步骤 4 单击“提交”。



说明

配置完成后，可以通过在网络浏览器中输入“https://虚拟网关 IP 地址”来访问虚拟网关。

----结束

4.3 配置网络扩展信息

SSL VPN 的网络扩展允许客户端通过获取内网虚拟 IP 地址从而允许用户访问内网资源。使用户的 PC 如同工作在企业内网一样，快速、安全地访问企业内网的所有资源，并保证客户端和网关之间的通信采用 SSL 安全协议。通过配置，管理员可以控制客户端在访问内网资源时能否同时访问其他非内网的资源，如 Internet 资源。

步骤 1 在“虚拟网关列表”中新创建的虚拟网关导航树上单击“网络扩展”。

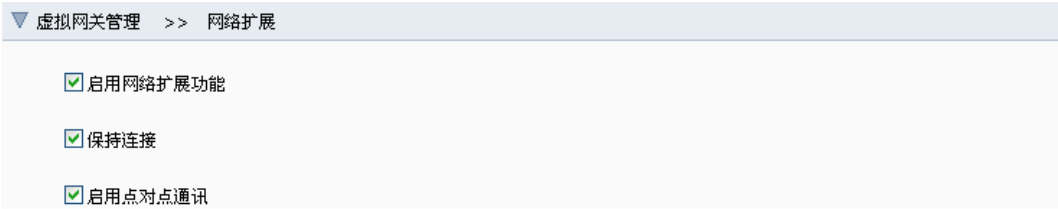
系统显示“网络扩展”页面。



SVN5300 的网络扩展配置路径为“资源管理 > 网络扩展 > SSL 网络扩展”。

步骤 2 在“网络扩展”区域框中，选中“启用网络扩展功能”、“保持连接”和“启用点对点通讯”，如图 4-3 所示。

图4-3 网络扩展



步骤 3 在“网络扩展 >> 客户端 IP 分配方式”区域框中，选择“IP 地址池方式”，添加规划的网段，如图 4-4 所示。

图4-4 客户端 IP 分配方式



步骤 4 在“网络扩展 >> 客户端路由方式”区域框中，选择“手动方式”，添加规划的网段，配置允许外网访问内网的地址范围，如图 4-5 所示。

图4-5 客户端路由方式

网络扩展 >> 客户端路由方式

☐	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。
☐	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	用户可以访问远端企业内网特定网段的资源，对其它Internet和本地局域网的访问不受影响。网段冲突时优先访问远端企业内网。
▼ IP网段		子网掩码
0	192 . 162 . 1 . 0	255 . 255 . 255 . 0
		添加网段

步骤 5 单击“提交”。

----结束

4.4 配置 VPNDB 用户

- 步骤 1 在“虚拟网关列表”导航树上单击“”，展开新创建的虚拟网关。
- 步骤 2 单击“认证授权配置”，选择“认证授权方式”页签。
- 步骤 3 单击各优先级对应的“”，在“选择认证方式”和“选择授权方式”中选择“VPNDB”，如图 4-6 所示。

说明

SVN5300 的认证授权配置路径为“认证授权 > 认证授权方式 > 认证授权方式”。

图4-6 认证授权方式

认证授权配置 >> 认证授权方式

☐ 需要用户提供证书

优先级	选择认证方式	选择授权方式	操作
1	VPNDB	VPNDB	
2			
3			

☒ 允许一个账号在多处同时登录

各账号的默认最大在线数: 参数范围：1~10

提交

- 步骤 4 单击“提交”，使配置生效。
- 步骤 5 单击导航树上的“VPNDB”，选择“用户管理”页签。

步骤 6 单击“添加”。

进入 VPND 用户配置页面，填入相关用户信息，选择虚拟 IP 地址池，如图 4-7 所示。

 说明

SVN5300 的用户配置路径为“用户和用户组 > 用户管理 > VPND 用户”。

图4-7 用户配置页面

用户管理

组管理

密码设置

▼ VPND配置 >> 用户管理 >> 添加用户

用户名	user1	* 示例: test、test@test, 1~63个字符, 一个汉字占6个字符
密码		* 1~31个字符, 不能含有空格
确认密码		*
UID		只允许为空或数字(0~65535), 输入为空表示65534
GID		只允许为空或数字(0~65535), 输入为空表示65534
虚拟IP地址		指定用户使用网络扩展业务时分配的虚拟IP地址
虚拟IP地址池	192.162.1.10-192.162.1.250	指定用户的网络扩展虚拟IP地址池
备注		

▼ VPND配置 >> 用户管理 >> 所属组信息

待选组列表

用户所属组列表

>>

All >>

<<

All <<

提交

步骤 7 单击“提交”，添加一个用户。

 说明

批量添加用户的方法请参见《Quidway SVN3000 产品文档》中的“配置本地用户”章节。

----结束

4.5 配置 DNS 和域名（可选）

步骤 1 在 Web 网管主页，单击“虚拟网关列表”。

打开虚拟网关列表。

步骤 2 单击新创建的虚拟网关前的“”。

展开虚拟网关管理导航树。

步骤 3 在导航树上单击“网络配置”。

进入 DNS 配置页面，如图 4-8 所示。

 说明

SVN5300 的 DNS 配置路径在新创建虚拟网关的“虚拟网关系统 > DNS > DNS”。

图4-8 配置 DNS 和域名

▼ 网络配置 >> 配置DNS服务器

服务器类型	服务器地址	操作
首选DNS服务器		 
备选DNS服务器 1		 
备选DNS服务器 2		 

服务器类型	服务器域名	操作
DNS domain	示例: huawei.com	 

请根据实际场景填写 DNS 的 IP 地址和域名参数。

----结束

4.6 保存配置

步骤 1 在“系统管理”导航树上单击“设备维护”。

步骤 2 单击“保存”，保持配置。

----结束

5 配置关键点

- 在防火墙上开放 SVN3000 所使用的端口给外网用户访问，通常是 443 端口。（如果用户希望可以在外网对 SVN3000 进行管理的话则同时需要开放 Web 网管绑定的端口）。
- SVN3000 设备已经在内网交换机或路由器上添加路由以便 SVN3000 的内网口可以与内网服务器相通。

6 结果验证

在外网通过 SVN 客户端软件或集成了 SSL VPN 隧道接入能力的客户端软件登录内网应用服务器，登录并通信成功，则代表 SVN 配置成功。

以 eSpace Desktop 为例进行验证。

步骤 1 启动 eSpace Desktop，如图 6-1 所示。

图6-1 eSpace 登录界面



步骤 2 单击“设置”。

在“登录服务器”中选择“公司外网”，选中“SVN”，如图 6-2 所示。

图6-2 eSpace 外网登录



用户登录

信息助理 沟通专家

帐号登录

UC帐号: 00199883 删除帐号

密码: *****

☒ 记住密码 ☐ 自动登录 状态: 在线

设置

登录服务器: 公司外网 ☒ SVN

服务器IP地址: 192.162.1.2 端口: 8011

SVN帐号: user1 密码: *****

SVN地址: 11.11.11.1

登录

步骤3 输入 eServer 服务器的 IP 地址、SVN 帐号密码、SVN 服务器外网 IP 地址。

步骤4 输入 UC 帐号和密码，单击“登录”。

如果登录成功，并能成功通信，则代表 SVN 配置正确。

----结束