AG 10.3.0

用户手册

北京华耀科技有限公司

二零二五年

版权声明

本手册所涉及的案例均是当前情况，华耀有权利随时更改，恕不提前通知。对于本手册内容，包括但不限于隐含的商业性能和特定用途适应性说明，华耀不承担任何责任。

如因本手册的描述造成设备性能、使用和按键操作问题，进而引发相关事故并造成损失的，华耀不承担任何责任。

警告：未经华耀许可，任何人不得对华耀 AG 设备进行任何改动，否则将无权继续使用该设备。

商标声明

本手册中所涉及的产品名称仅作识别之用。手册中涉及的其他公司的注册商标或版权属各商标注册人所有，恕不逐一列明。

合格声明

华耀自主声明华耀 AG 系列产品符合 FCC 规范第 15 部分的规定。操作本设备需要满足以下条件：（1）本设备不会产生有害干扰，（2）本设备必须能够接受收到的所有干扰，包括可能导致意外操作的干扰。

关于华耀

北京华耀科技有限公司（简称：华耀）于 2003 年创建于北京，是优秀的网络功能平台解决方案提供商，也是应用交付解决方案、移动应用接入（SSL VPN）解决方案的全球领导者。华耀现有员工 150 余人，其中研发团队近百人，总部位于北京。并在北京、上海、广州、杭州、深圳等全国多地设有销售及技术支持部门，负责销售及客户支持工作。

华耀一贯秉持为用户打造敏捷灵活与安全性能兼顾的网络环境的理念。作为多年的应用交付解决方案全球领导者，华耀确保应用性能、高可靠性和安全性的同时，将应用推送到终端用户。通过华耀产品，用户可以使用任何设备、从任何地点访问云环境或企业数据中心的应用、桌面或服务。从 Web 站点、到电子商务、到企业应用、再到云服务，华耀解决方案提供了卓越的终端用户体验和可靠的安全性，全力保障企业的运营效率。

联系华耀

请通过以下方式联系华耀：

- 官方网站：https://www.arraynetworks.com.cn/
- 电子信箱：support@arraynetworks.com.cn
- 地址：北京市海淀区建枫路（南延）6 号西三旗金隅科技园 2 号楼信安大厦
- 邮编：100096
- 电话：010-68025518、400-6007878
- 电话联系时间：周一至周五早 9 点至晚 6 点

目录

第1章 引言

1.1 编写目的

本手册详细介绍了安全接入网关的系统各模块的功能原理，以及如何通过 CLI 命令配置具体功能，指导用户正确使用该系统。

1.2 适用对象

本手册适用对象为售前、产品实施及技术支持人员、网络管理员、以及测试人员等，假定具备以下概念知识：

- 网络拓扑
- 网络地址、路由和 DNS
- TCP/IP、SSL、HTTP/HTTPS

第2章 产品简介

2.1 简介

AG 设备是基于 SSL 的 VPN 平台，为应用提供快速、安全和可扩展的远程接入。AG 设备通过 SSL 加速提升访问速度，通过 AAA 和用户策略确保访问安全性，为 Web、邮件、文件和本地应用服务器提供了接入方法，通过华耀虚拟站点和 HA 技术确保了可扩展性。通过将这些功能特性集成到一台的设备，华耀 AG 为受信的员工、客户和全世界的合作伙伴交付安全的内网接入。在保护内部网络安全的同时，让用户可以轻松地使用基于 Web 的应用程序和常见的传统应用程序。

重要的 AG 概念如下：

SSL 加密：华耀 AG 设备支持使用 SSLv3/TLSv1/TLSv1.2/DTLS 协议对传输的数据进行加密。基于 ArrayOS 和 SSL 硬件架构，AG 提供了业界最好的 SSL 性能。此外，AG 可以完全支持与 PKI 和 CA 服务器集成。

虚拟站点：是一个可管理和可配置的单元，包括客户端安全连接、用户访问控制、企业资源和用户与资源之间的映射关系。华耀 AG 可以支持最多 256 个虚拟站点。

AAA：为网络中进行的所有事务提供身份验证和授权。该功能帮助管理员严格控制用户对内容的访问，并提供准确的审计日志。华耀 AG 使用一个或多个可用的 AAA 服务器来验证试图访问该网络的最终用户的身份。可以支持的 AAA 服务器包括 LocalDB、LDAP、RADIUS、客户机证书、SMS、SAML 和 FIDM。一旦最终用户通过身份验证，华耀 AG 将向最终用户呈现带有授权资源列表的 Web 门户页面。

用户策略：AG 的用户策略包括用户角色、访问控制列表和用户会话管理。用户角色可以根据已认证的用户的资格（例如登录时间、用户名、组名、源 IP 地址和选择的 AAA 方法）为其授权资源，从而实现精确的、细粒度的和灵活的资源分配。访问控制列表控制哪些用户、组或角色可以访问特定的资源。当用户通过虚拟站点访问内容时，这些 ACL 规则将应用于用户。会话管理用于控制所有的在线用户。

访问方法-网络访问：它是华耀 AG 提供的通用网络访问解决方案，广泛用于为内部网络资源提供安全的远程访问，允许移动用户、远程办公人员、合作伙伴和客户访问部署在安全的内部网络中的应用程序。该功能的设计最大限度地保护了公司网络的安全性。

2.2 快速启动 AG

快速启动 AG 的步骤如下：

1. 完成 AG 设备的初始网络设置。例如，将 port1 的接口 IP 地址设置为 10.10.0.2，并将默认网关设置为 10.10.0.1。有关更多信息，请参考 3.1.3 系统初始化设置。
2. 创建虚拟站点。例如，配置一个虚拟站点，其站点 IP 地址为 10.10.0.2，端口为 443，并为该虚拟站点导入一个有效的证书。有关更多信息，请参考第 4 章虚拟站点。
3. 配置 AAA。例如，使用 LocalDB 作为 AAA 服务器，为员工和管理人员添加 LocalDB 帐户，并将他们分别添加到员工和经理组中。更多信息，请参考第 5 章 AAA。
4. 配置接入方法。更多信息，请参考第 8 章接入方法。
5. 配置用户策略。例如，定义员工和管理人员两个角色，并确保员工组中的员工获得员工角色，经理组中的管理人员则获得管理人员角色。将资源 OA 门户分配给员工角色，并将资源 OA 门户和 ERP 服务器分配给管理人员角色。更多信息，请参考第 7 章用户策略。
6. 在防火墙上为远程访问服务添加 IP 映射规则：2.0.0.1:443 到 10.10.0.2:443。

第3章 系统与网络设置

3.1 概述

本节将介绍 AG 设备的初始连接，基本设置和配置。下文将介绍快速配置步骤。

3.1.1 连接 AG 设备

用户可以通过如下方式连接 AG 设备：

- 控制台
- SSH（Secure Shell）
- WebUI

注意：在连接 AG 设备前，用户已经通过按设备前面板上的电源按钮启动 AG 设备。

3.1.1.1 控制台连接

如果选择使用控制台连接，用户需要将 Console 线连接到 AG 设备的 Console 接口上，然后将控制台终端设置如下：

表3–1 控制台设置

设置项	取值
终端仿真类型	VT 100
波特率	9600
数据位	8
奇偶校验	无
停止位	1
流控	无

使用默认的用户名“array”和密码“admin”建立与 AG 设备的控制台连接。建立控制台连接后，用户将进入 AGCLI 的 User 模式。执行“**enable**”命令并按 Enter 键（如果 Enable 模式的密码未发生变化）进入 AG CLI 的 Enable 模式。然后执行“**config terminal**”命令进入 AG CLI 的 Config 模式。当看到 AG 提示符“AN (config)#”，用户可以开始配置流程。关于可用的 CLI 命令行，请参见命令行用户手册。

如果用户希望通过 SSH 或 WebUI 方式远程访问 AG 设备，推荐用户先通过控制台连接完成系统的初始化配置。详细信息，请参见 3.1.3 系统初始化设置小节。

3.1.1.2 SSH 连接

在完成系统初始化配置后，用户可以通过 SSH 远程连接 AG 设备。

注意：Windows、MacOS 或者 Unix 下的 SSH 软件，可以从 http://www.openssh.com 网站获得。

要建立 SSH 连接，执行以下步骤（以使用默认的用户名“admin”和密码“admin”为例）：

1. 在工作站上运行 SSH 程序，并执行如下命令：

```
>> ssh "array'@10.10.0.2"
```

10.10.0.2 是为 AG 设备管理接口配置的 IP 地址。

2. 按提示输入密码。

```
>> ssh "array@10.10.0.2"

>> array@10.10.0.2's password:
```

建立 SSH 连接后，用户将进入 CLI 的 User 模式。当用户进入 CLI 的 Config 模式后，可以开始修改配置。关于如何进入 CLI 的 Config 模式，请参见 3.1.1.1 控制台连接小节。

3.1.1.3 WebUI 连接

本节介绍通过 WebUI 与设备建立连接的方法。WebUI 提供直观、友好的图形化接口，用于对设备进行配置和管理，达到与命令行配置同样的配置效果，大大方便了用户的使用和操作。

WebUI 功能具有以下优点：

- 通过快速响应来改善用户体验；
- 将设备的功能和性能最大化；
- 实现更简便的系统配置和管理；
- 通过 HTTPS 协议提供安全接入。

注意：WebUI 功能默认是禁用的。如果想通过 WebUI 对设备进行配置和管理，请首先参见 3.1.3 系统初始化设置小节。

要与设备建立 WebUI 连接，用户需要在 Web 浏览器中打开 WebUI 的 URL 地址。WebUI 的 URL 地址的格式为：https://<management_IP>:<WebUI_port>。

（management_IP 表示为 AG 管理接口配置的 IP 地址，WebUI_port 默认值为 8888，用户可以执行“**webui port**”命令修改 WebUI 端口。）

访问 WebUI 的示例：

```
https://10.10.0.2:8888
```

然后按 Enter 键。登录页面将会弹出，提醒用户输入用户名和密码。默认的用户名和密码分别是 **admin** 和 **admin**。

WebUI 支持主流的浏览器，例如 Chrome（推荐）、Firefox 和 Internet Explorer （11 或更高版本）。浏览器分辨率应设置为 1024×786 或更高。

3.1.1.4 WebUI SSL 设置

3.1.1.4.1 SSL 客户端认证配置

在 SSL 通信中，如果对客户端身份没有认证的必要，SSL 协商流程通常只对服务器身份进行认证，即执行 SSL 单向认证。在某些对客户端身份有严苛要求的场景中，SSL 协商流程需要同时对客户端身份和服务器身份进行认证，即需要执行 SSL 双向认证。

设备支持 WebUI SSL 客户端认证功能，来满足特定应用场景中对于 SSL 双向认证的需求。同时，设备还支持 WebUI SSL 客户端认证强制模式。启用强制模式后，WebUI 客户端必须通过客户端身份认证后才能与 WebUI 建立 SSL 连接。否则，WebUI 访问将失败。如果只开启客户端认证而不开启强制认证模式，客户端不提供证书，但管理员仍然能访问 WebUI。

- **CLI 配置示例**

要启用 WebUI SSL 客户端认证功能，执行以下步骤：

1. 为 WebUI 导入证书链文件。

```
AN(config)#webui ssl import certificate ftp://10.8.6.20/cert/chain.pem
```

2. 导入客户端 CA 证书。

```
AN(config)#webui ssl import clientca ftp://10.8.6.20/cert/webui.pem
```

3. 启用 WebUI SSL 客户端认证功能。

```
AN(config)#webui ssl settings clientauth enable
```

4. 启用 WebUI SSL 客户端认证强制模式。

```
AN(config)# webui ssl settings authmandatory enable
```

3.1.1.4.2 SSL 协议版本和密码套件设置

设备还支持修改 WebUI（SSL 服务器）支持的 SSL 协议版本和密码套件。

1. 执行以下命令修改 WebUI 支持的 SSL 协议版本：

```
AN(config)#webui ssl settings protocol TLSv11:TLSv12
```

2. 执行以下命令修改 WebUI 支持的 SSL 密码套件：

```
AN(config)#webui ssl settings protocol
“ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:AES128-GCM-SHA256:AES256-GCM-SHA384:DES-CBC3-SHA”
```

3.1.2 LED 信息

设备前面板上有三个 LED 指示灯：黄色、绿色和蓝色。下面对每个 LED 指示灯的含义及功能做出说明。

表3–2 前面板 LED 指示灯说明

LED 颜色	LED 名称	功能描述
蓝色	电源（Power）	指示电源工作状态和设备的启动状态（关闭/打开）。
绿色	运行（Run）	ArrayOS 系统启动后，此灯开始亮起，用来指示 CPU 的使用率。CPU 的使用率越高，闪烁速率越快。
黄色	故障（Fault）	正常情况下该 LED 灯保持熄灭状态。当该 LED 灯亮起时，表明设备有可能出现了以下问题： • CPU 风扇停止工作。 • CPU 过热（CPU 过热温度为 85℃）。 • 系统过热（1U 设备系统过热温度为 75℃，2U 设备系统过热温度为 85℃）。 • 冗余电源出现故障（如果该设备支持冗余电源）。
	**注意：**当设备的黄色故障 LED 指示灯亮起时，请联系华耀客户支持，并可以通过查看设备的日志来检查设备出现的问题。	

3.1.3 系统初始化设置

在设备的初始化配置前，用户首先需要使用网线将前面板上的管理接口与管理网络连接起来，然后与设备建立控制台连接。要完成初始化配置，执行如下步骤：

1. 为管理接口分配 IP 地址和掩码，例如：

```
AN(config)#ip address port1 10.10.0.2 255.255.255.0
```

该 IP 地址将作为远程管理接入的管理 IP 地址，例如 WebUI 或 SSH 接入。

2. 为设备配置默认路由，例如：

```
AN(config)#ip route default 10.10.0.1
```

3. 启用 WebUI 功能。

```
AN(config)#webui on
```

4. 执行如下命令保存配置：

```
AN(config)#write memory all
```

在完成任何配置修改后请记得保存配置。否则，系统重启后，未保存的配置修改将会丢失。

3.1.4 CLI 介绍

CLI 允许管理员通过控制台终端和 SSH 连接使用命令行对设备的主要功能进行配置和控制。

3.1.4.1 CLI 使用说明

设备的软件设计提升了与设备交互的友好性，例如自动补齐。自动补齐是一种非常直观易用的方式，允许用户仅输入 CLI 命令的第一个或前几个字母，设备就能补齐 CLI 命令。下表列举了 CLI 支持的快捷方式。

表3–3 CLI 快捷方式

CLI 快捷方式	操作
Ctrl+a	将光标移动到行的开头。
Ctrl+e	将光标移动到行的结尾。
Ctrl+f	将光标向前移动一个字符。
Ctrl+b	将光标向后移动一个字符。
Esc+f	将光标向前移动一个单词。
Esc+b	将光标向后移动一个单词。
Ctrl+d	删除光标对应的字符。
Ctrl+k	删除光标处到行尾的内容。
Ctrl+u	删除输入的行。

设备的 CLI 命令行遵守下表中的格式约定：

表3–4 命令行格式约定

格式	约定
Bold	命令行主体采用加粗字体表示。
Italic	命令行参数采用斜体表示。

< >	表示用“< >”括起来的参数在配置时是必选的。
[ ]	表示用“[ ]”括起来的参数在配置时是可选的。
{x|y|…}	表示从两个或多个选项中至少选取一个。
[x|y|…]	表示从两个或多个选项中选取一个或者不选。

注意：当参数取值为字符串时，推荐将参数取值置于双引号中，以确保设备能够正确执行命令。

示例：

ip address <*ip_address*> {*netmask*|*prefix*}

3.1.4.2 访问控制级别

3.1.4.2.1 全局访问控制级别

设备的命令行接口为全局提供三个级别（模式）的访问控制，对需要登录系统并进行特定配置操作的管理员进行权限管理。每个模式分别用不同的命令行提示符来表示，其组成形式分别为：“设备的主机名称”+“>”或“#”或“(config)#”。

- **User 模式**

User 模式是最低的访问级别。处于该级别的管理员只能使用一些基本的操作和非关键的设备功能。在命令行接口中，User 模式提示符的表现形式为“AN>”。

- **Enable 模式**

处于该级别的管理员可以使用大量的查看类命令，例如“**show version**”命令。管理员可以执行 User 模式和 Enable 模式下的命令。要想进入 Enable 级别，管理员需要在 User 模式下执行“**enable**”命令，并输入正确的 Enable 模式密码。默认的 Enable 模式密码为空。

管理员成功进入 Enable 模式后，CLI 命令行提示符从“AN>”变为“AN#”。

- **Config 模式**

Config 模式是最高的访问级别。处于该级别的管理员可以修改设备的各项配置。要想进入 Config 级别，管理员需要在 Enable 级别下执行“**config terminal**”命令。管理员进入 Config 模式后，CLI 命令行提示符从“AN#”变为“AN(config)#”。

同一时刻只能有一个管理员处于 Config 模式。如果当前另一个管理员处于 Config 模式，可以执行“**config terminal force**”命令强制进入 Config 模式。

注意：

- 在 ArrayOS 中，可以创建管理员账户，并为其分配两类访问权限：Enable 和

Config。只有拥有 Config 访问权限的管理员账户才能访问 Config 模式。

- 在任何模式下，用户可以输入“?”查看当前模式下可用的 CLI 命令。
- 本文档中所有的 CLI 配置示例的前提是用户已经成功登录 CLI 并进入所需的访问模式。

3.1.4.2.2 虚拟站点访问控制级别

设备的命令行接口为虚拟站点提供两个级别（模式）的访问控制，对需要登录系统并进行特定配置操作的管理员进行权限管理。每个模式分别用不同的命令行提示符来表示，其组成形式分别为：“虚拟站点名称”+ “$”或“(config)$”。

- **Enable 模式**

处于该级别的管理员可以使用大量的查看类命令，例如“**show version**”命令。光标将显示虚拟站点的预配置名称，后面跟随“$”。管理员成功进入 Enable 模式后，CLI 命令行提示符将变成“虚拟站点名称”+“$”。

```
demo_portal$
```

- **Config 模式**

Config 模式是最高的访问级别。处于该级别的管理员可以修改虚拟站点的各项配置。两个管理员不可以同时处于 Config 级别（无论是在全局还是在虚拟站点视图中）。为了获得对设备的特定虚拟站点的完整配置权限，管理员必须执行以下命令：

```
demo_portal$config terminal
```

输入此命令后，CLI 提示符将更改为：

```
demo_portal(config)$
```

注意：全局管理员具有使用所有虚拟站点和全局配置功能的权限。

3.1.4.3 全局和虚拟站点切换

设备允许管理员通过以下命令在全局模式和虚拟站点模式之间切换：

switch <*global*|*virtual_site_name*> *[enable|config]*

例如，管理员可以通过执行以下命令从全局模式切换到 demo_portal 虚拟站点模式（例如，一个名为“demo_portal”的虚拟站点）：

```
AN#switch demo_portal
```

输入此命令后，CLI 提示符将更改为：

```
demo_portal$
```

要切换回全局模式，管理员可以执行以下命令：

```
demo_portal$switch global
```

输入此命令后，CLI 提示符将更改为：

```
AN#
```

默认情况下，当在全局模式和虚拟站点模式之间切换时，管理员权限级别（例如，Enable 级别或 Config 级别）将保持不变。但是，如果在切换过程中指定了“enable|config”参数，则将相应地切换管理员权限级别。

例如，管理员执行以下命令：

```
AN#switch demo_portal config
```

输入此命令后，CLI 提示符将更改为：

```
demo_portal(config)$
```

3.2 通用系统和网络设置

3.2.1 系统时间

3.2.1.1 系统时间手动设置

系统允许管理员为设备设置系统日期、时间和时区。该功能主要应用于网络中没有 NTP（Network Time Protocol，网络时间协议）服务器的场景。

- **CLI 配置示例**

1. 设置系统日期为 2021 年 3 月 3 日。

```
AN(config)#system date 21 3 3
```

2. 设置系统时间为上午 **14 05 40**。

```
AN(config)#system time 14 05 40
```

3. 查看系统时间和日期。

```
AN#show date

Wed Mar 03 14:05:46 GMT (+0000) 2021
```

4. 使用“**system timezone**”命令设置时区。

   a. 选择大陆。

b. 选择国家。

c. 选择时区。

5. 查看系统时区。

```
AN#show system timezone

system timezone "CST"
```

3.2.1.2 NTP

NTP 功能能够让设备与配置的 NTP 服务器同步系统时间。

要使用 NTP 功能，用户首先需要配置至少 1 个 NTP 服务器。当启用 NTP 功能时，设备将作为 NTP 客户端，按照大约 15 分钟的间隔自动与配置的 NTP 服务器同步系统时间。系统允许配置最多 6 个 NTP 服务器。系统支持 IPv4 和 IPv6 NTP 服务器。

如果用户配置了多个 NTP 服务器，设备将根据从每个 NTP 服务器返回的响应报文中的时间信息计算往返延时，然后跟延时最小的 NTP 服务器同步系统时间。

注意：

- 在启用 NTP 时间同步器以后，请不要再手动设置设备的系统时间。
- 部署在海光平台上的设备不支持指定“index”参数。

➢ **CLI 配置示例**

1. 配置 NTP 服务器。

```
AN(config)#ntp server 192.168.1.100 4
```

2. 启用 NTP 功能。

```
AN(config)#ntp on 0
```

用户可以执行“**show ntp**”命令查看当前的 NTP 配置，以及设备与 NTP 服务器的时间分差和关联。

```
AN1(config)#show ntp
ntp server 172.16.85.12 4
ntp server 172.16.85.60 4
ntp on 0
time since restart:        20
time since reset:          20
packets received:          2
packets processed:         1
current version:           1
previous version:          0
```

```
declined:                  0
access denied:             0
bad length or format:      0
bad authentication:        0
rate exceeded:             0

     remote                local          st poll reach   delay     offset      disp
==============================================================================
=172.16.85.12      172.16.85.80     16     64      0 0.00000   0.000000 3.99217
*172.16.85.60      172.16.85.80      3     64      1 0.00189   0.000050 2.81735
```

以下解释了输出信息中的内容：

表3–5 “show ntp”输出信息

输出信息	含义
Time since restart	上次系统重启后运行的时间，以小时为单位。
Time since reset	统计信息重置和系统统计监控文件更新之后运行的时间。这个信息是专门为繁忙服务器而收集的，例如操作系统为 NIST、USNO 的服务器，并能为它们早期探测到 clogging 攻击。
Packets received	收到的数据报的总数。
Packets processed	上一个数据报发出之后收到的响应包数目。
Current version	与当前 NTP 版本兼容的数据报的数目。
Previous version	与之前 NTP 版本兼容的数据报的数目。
Bad version	与任何一个 NTP 版本都不兼容的数据报的数目。
Declined	因主机上已经存在 NTP 程序而拒绝日期设置请求的次数。
Access denied	由于某种原因被拒绝访问的数据报的数目。
Bad length or format	具有无效长度、格式或者端口号的数据报的数目。
Bad authentication	未通过验证的数据报的数目。
Rate exceeded	由于速率限制而被丢弃的数目包。

3.2.2 主机名

设备的默认主机名为 AN。系统允许用户修改设备的主机名。

- **CLI 配置示例**

执行“**hostname**”命令修改设备的主机名。

```
AN(config)#hostname my_ag
my_ag(config)#
```

3.3 DNS 配置

3.3.1 DNS 简介

域名解析是将文件或网络位置名称转换为管理员用于维护网络安全和可访问性的相应网络地址的功能。DNS 系统自动将名称转换为 IP 地址。设备尝试通过以下顺序来应答正向和反向域名查找：

1. 本地 DNS 缓存
2. DNS 域名服务器

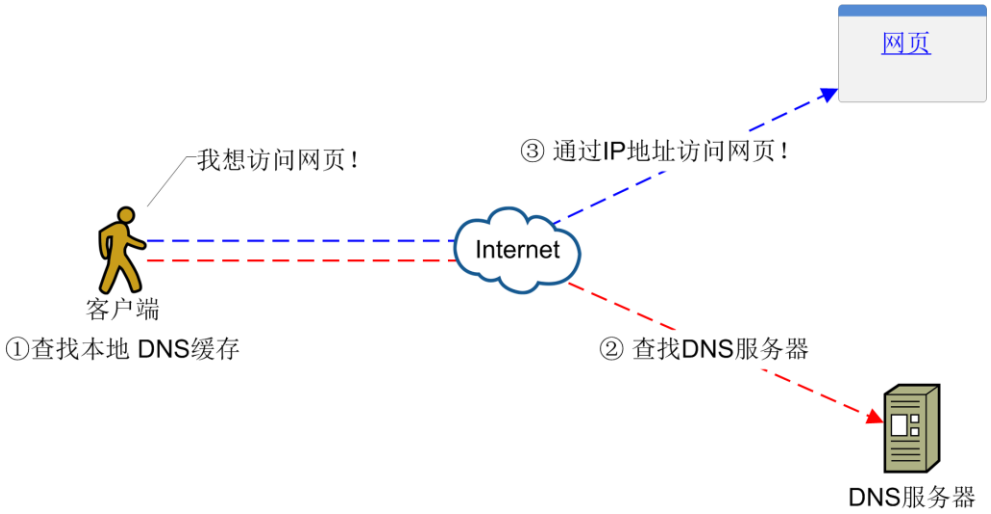

图3–1 DNS 查询过程

3.3.2 DNS 域名服务器

系统提供本地 DNS 域名服务器。如果包含目标域名和相关 IP 地址的缓存条目不存在，客户端将向本地 DNS 服务器发送请求。

系统允许为设备配置最多 3 个 DNS 域名服务器。系统只支持 IPv4 DNS 域名服务器。

- **CLI 配置示例**

1. 添加一个域名服务器。

```
AN(config)#ip nameserver 10.3.0.10
```

3.3.3 DNS 缓存

系统支持 DNS 缓存（DNS Cache）功能。当启用 DNS 缓存功能后，设备收到一个 DNS 服务发送回来的 A 记录或 AAAA 记录响应，就会将它缓存下来。然后，

当设备再次收到访问这条 A 记录或 AAAA 记录的客户请求时，设备会直接将缓存中的 A 记录或 AAAA 记录发送给客户端。如果缓存中没有相关记录，设备就会将 DNS 请求转发给后台服务器，并将后台服务器返回的结果保存至缓存，以待下一次的 DNS 请求。

系统还允许管理员手动定义静态 DNS 记录。系统可以根据这些静态 DNS 记录响应 DNS 查找请求。

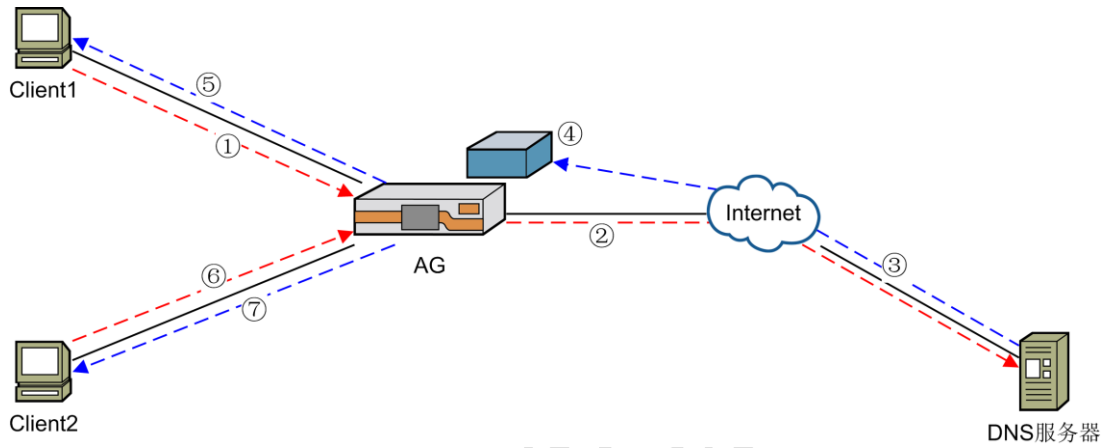

图3–2 DNS 缓存

如上图所示，Client1 和 Client2 正在请求相同的 Web 服务。

1. Client1 首先向设备发送 Web 服务的 DNS 请求。
2. 如果设备上不存在相关的静态记录和缓存记录，则设备将向已定义的 DNS 服务器发送 DNS 请求。
3. DNS 服务器响应请求。
4. 设备缓存 DNS 响应。
5. 设备向 Client1 发送 DNS 响应。
6. 然后，Client2 发送相同域名的 DNS 请求。
7. 设备将缓存的记录发送给 Client2。

➢ **CLI 配置示例**

1. 启用 DNS 缓存。

```
AN(config)#dns cache on
```

2. 配置 DNS 缓存的失效时间。

```
AN(config)#dns cache expire 1 36000
```

3. 建立 DNS 缓存主机。

```
AN(config)#dns cache host "sting" 10.1.61.200
```

4. 添加静态 DNS 资源记录。

```
AN(config)#ip host test.com.cn 20.4.5.6
```

第4章 虚拟站点

4.1 简介

VPN 代理服务器通常用来为用户提供虚拟服务，包括客户安全连接、用户访问控制和后端资源管理。当客户需要使用不同的安全连接策略，提供不同的访问控制方法或实现不同的资源管理方式时，他们就需要购买更多的 VPN 代理服务器。为帮助用户提升可扩展性和成本效益，引入了“虚拟站点”的概念。

虚拟站点是一个可供管理员自行配置和管理的资源站点，用于提供如客户安全连接、用户访问控制和后端资源管理等多种类型的服务。

当需要为特定的用户和群组提供不同的服务时，客户不再需要为每个用户和群组单独购买 VPN 代理服务器，而只需在设备上创建多个独立的虚拟站点即可，因而实现了服务可扩展性和成本效益的提升。

设备目前只支持独占型虚拟站点。最多支持 255 个虚拟站点。

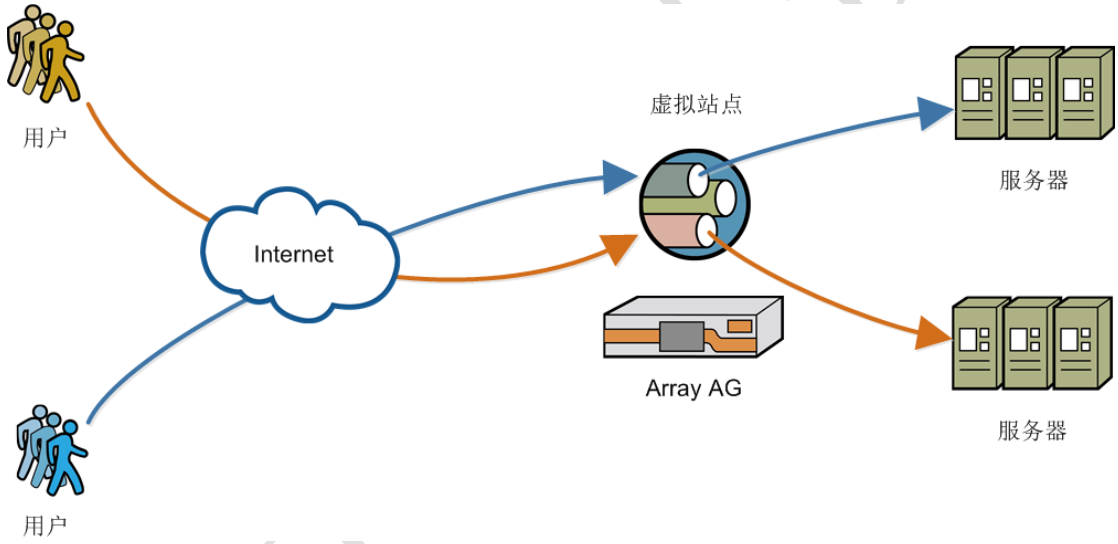

图4–1 虚拟站点

- **CLI 配置示例**

1. 添加一个虚拟站点。

```
vs(config)#virtual site name vs "vs" "exclusive"
```

2. 为虚拟站点添加 IP 地址。

```
vs(config)#virtual site ip vs 172.16.88.67 33
```

3. 为虚拟站点添加域名。

```
vs(config)#virtual site domain vs "vs.com.cn"
```

第5章 AAA

设备支持对登录的用户进行认证，这是将内网资源授权给用户的先决条件。启用 AAA 认证功能后，收到客户端请求时，认证服务器将检查用户的凭据。如果凭据有效，用户将被授权成功登录，否则将被拒绝登录。

5.1 认证

进行 AAA 认证前，首先需要定义一个认证服务器。

5.2 认证服务器

5.2.1 LocalDB

支持使用 LocalDB（本地数据库）进行认证。在 LocalDB 认证中，如果输入的用户名和密码匹配了在设备上为虚拟站点在本地数据库中配置的条目，终端用户就通过 LocalDB 认证。

➢ **认证模式**

AG 支持三种 LocalDB 认证模式：

- 静态密码：表示用户登录虚拟站点时只需要输入静态密码。
- 动态密码：表示用户登录虚拟站点时只需要输入动态密码。
- 双重模式：表示用户登录虚拟站点时需要输入静态和动态密码。

当为 LocalDB 认证启用动态密码时，用户需要在手机上安装 iSecSP 应用。安装后，用户需要填写服务器信息（虚拟站点 IP 和端口号）和用户凭证（用户名和静态密码）在 iSecSP 上获取动态密码。然后在客户端或 Web 门户的登录页面上输入用户名和动态密码登录虚拟站点。

当为 LocalDB 认证启用动态密码和静态密码时，用户应输入用户名和自定义的密码（由静态密码和动态密码组成）。

此外，AG 还支持设置动态密码的刷新间隔。

➢ **动态码绑定**

AG 还支持动态码重复绑定功能。启用该功能后，在一台移动客户端登录 iSecSP 应用后，用户仍可以使用同一个 LocalDB 账号在另一台移动客户端登录 iSecSP 应用。用户的旧的注册凭据将会被新的注册凭据替代。

➢ **LocalDB 服务器、账户和组**

AG 仅支持为一个虚拟站点配置一个 LocalDB 服务器。在 AG 设备上，一个虚拟站点的 LocalDB 服务器与其他虚拟站点的 LocalDB 服务器共享存储空间。

每个 LocalDB 账户可以与多个 LocalDB 组关联。

此外，管理员可以更新已有的 LocalDB 账户的名称和密码。

➢ **CLI 配置示例**

1. 定义 LocalDB 服务器。

```
vs(config)#aaa server name localdb vs localdb
```

2. 创建一个 LocalDB 账户。

```
vs(config)#localdb account test test "test account"
```

3. 创建一个 LocalDB 组。

```
vs(config)#localdb group group1 "group1" 23
```

4. 将一个已有 LocalDB 账户与一个已有 LocalDB 组关联。

```
vs(config)#localdb member group1 test
```

5.2.1.1 LocalDB 账户密码设置

系统支持为 LocalDB 账户密码配置如下检查：

- 最小密码长度检查
- 大写字符检查
- 小写字符检查
- 特殊字符检查
- 非字母数字字符检查
- 特殊字符最小数量检查
- 用户名和密码重复性检查
- 新密码和老密码一致性检查

5.2.1.2 LocalDB 账户密码过期

系统支持为 LocalDB 账户配置过期时间。管理员可以为指定的 LocalDB 账户设置密码过期时间和下次登录时强制密码更新。账户密码过期后，用户下次通过客户端登录时，客户端会自动跳转至修改密码页面。

5.2.1.3 LocalDB 账户锁定

系统支持对所有或者指定的 LocalDB 账户进行自动空闲锁定和自动登录失败锁定。

管理员可以对指定的 LocalDB 账户在指定时间内进行手动锁定或解锁一个已上锁的 LocalDB 账户。

5.2.1.4 LocalDB 账户有效期

系统支持为 LocalDB 账户配置账户有效期，当用户的账户到达有效期后将会被永久锁定，管理员可以通过命令“**localdb lockout unlock** *[account_name]*”为用户解锁。

5.2.2 LDAP（包括 AD）

AG 支持使用 LDAP 进行认证和授权。AAA 模块支持 LDAP v3 协议的所有 LDAP 服务器，包括 OpenLDAP 和活动目录（Active Directory，AD）。

一个虚拟站点支持配置 32 个 LDAP 服务器。考虑到冗余性，每个服务器可以有三个主机。如果使用多个 LDAP 服务器，将使用主机轮询（Round Robin，rr）负载均衡来进一步提高性能。

通过在每个主机上使用 SSL/TLS 协议，LDAP 服务器可以被配置用来进行认证和授权。

5.2.3 RADIUS

AG 支持使用 RADIUS 进行认证和授权。

一个虚拟站点最多支持配置 32 台 RADIUS 服务器。考虑到冗余性，每台服务器可以有 3 个主机。如果使用多台 RADIUS 主机，将使用主机轮询（Round Robin，rr）负载均衡来进一步提高性能。

RADIUS 请求是非阻塞的。将会为所有 RADIUS 请求定义超时时间。

5.2.4 客户端证书

AG 可以验证由受信任的证书授权中心（Certificate Authority，CA）签发的证书。AG 支持三种类型的客户端证书认证：

- 匿名（Anonymous）：匿名认证只需要客户端证书。
- 非挑战（NoChallenge）：非挑战认证需要认证服务器上有客户端证书和用户账户。

- 挑战（Challenge）：挑战认证需要客户端证书、用户账户和用户账户的密码。

对于匿名类型，管理员不需要使用其他认证服务器，由 SSL 模块进行证书验证检查证书是否由受信任的 CA 证书签发。对于非挑战或挑战类型，管理员必须配置一个 LocalDB 或 LDAP 服务器作为认证服务器来验证客户端证书。

对于客户端证书授权，管理员需要使用 LocalDB、LDAP 或外部组作为认证服务器，证书将通过它来授权。外部组授权基于用户证书的特定字段区分用户（例如，字段值相同的用户被视为同一组并被授予相同的许可）。

证书认证/授权的基本工作流程如下：

1. SSL 基于受信 CA 验证客户端证书。
2. SSL 从证书中提取相应字段。
3. SSL 将字段值发给 AAA 服务器。
4. AAA 使用 LDAP 服务器或 LocalDB 进行认证。
5. AAA 使用 LDAP 服务器、LocalDB 或外部组进行授权。

5.2.5 SMS

短消息服务（Short Message Service，SMS）认证可以与常规认证服务器（如 LocalDB、LDAP、RADIUS 证书或 HTTP AAA 服务器）一起使用进行两步认证。

当使用两步认证时，AG 首先使用常规认证服务器认证并获取用户的手机号码或者邮箱。然后 AG 使用通过命令“**aaa server sms import**”导入的 SMS 认证模板构建 SMS 认证请求并将其发送给 SMS 认证服务器进行认证。当从 SMS 服务器接收的 SMS 验证响应与通过“**aaa server sms result**”命令配置的规则匹配时，AG 会返回要求用户输入验证码的 SMS 验证页面。如果用户输入正确的验证码，他将成功通过两步认证流程。对于 SMS 模板的细节，请参见命令行手册的“**aaa server sms import**”命令。

5.2.5.1 验证码

系统允许用户通过移动手机号码和邮箱获取验证码。系统会根据配置选择通过手机号码或邮箱向用户发送验证码。如果两种方式都配置，则会通过两种方式发送验证码。手机号码和邮箱可以通过以下方式获取：

- LocalDB
- LDAP 服务器
- RADIUS 服务器
- Certificate 服务器（仅用于手机号码）

- HTTP AAA 服务器

注意：由于不同 SMS 认证服务器接口规范不同，如果管理员为单个用户配置了多个手机号码，SMS 认证可能会失败。建议管理员只为用户配置一个手机号码。

用户有三次输入验证码的机会。如果用户三次输入都为错误密码，系统将会跳回用户登录界面。AG 发送的验证码的有效期可通过命令“**aaa server sms expiretime**”指定。用户最多可以点击三次 SMS 认证页面的“Resend”按钮给手机重新发送验证码。

5.2.5.2 配置示例

➢ **通过手机发送验证码**

为 SMS 服务器配置主机、短消息内容和 SMS 认证响应过滤器规则。

```
vs(config)#aaa server sms host "sms" "dysmsapi.cs.com" 443 "CUSTOM" "anonymous"
"XXXXXYW5vbnltb3Vz" "" "" "conn_reuse" "tls"
vs(config)#aaa server sms result "sms" <reg_condi>
vs(config)#aaa server sms message "sms" <message> 0
```

➢ **通过邮箱发送验证码**

为 SMS 服务器配置邮箱、邮件主题和内容。

```
vs(config)#aaa server sms email from "sms" "admin@AN.dom"
vs(config)#aaa server sms email subject "sms" "邮件主题"
vs(config)#aaa server sms email content "sms" "你好<USER>，这是本次的注册码：<OTP>，
请在 5 分钟内使用。
```

➢ **配置验证码过期时间、长度和类型**

```
vs(config)#aaa server sms verificationcode "sms" 8 "num"
vs(config)$aaa server sms expiretime "sms" 300
```

5.2.6 HTTP

AG 支持使用客户已有的 HTTP AAA 服务器进行认证和授权。

当 HTTP AAA 服务器用于认证时：

1. 收到 HTTP 认证登录请求时，AG 首先根据变量解析规则（通过命令“**aaa server http variant request name**”和“**aaa server http variant request profile**”配置）解析 HTTP 认证登录请求中的自定义用户变量（如果存在）。然后 AG 使用 HTTP 认证登录模板（通过命令“**aaa server http login template**”配置），将模板中的动态数据替代为待认证用户的数据来构建 HTTP 认证登

录授权请求，并发送构建的 HTTP 认证登录请求给 HTTP AAA 服务器进行认证。

2. 收到 HTTP 响应后，AG 将 HTTP 响应匹配 HTTP 响应过滤器的正则表达式（通过命令“**aaa server http result**”配置）。

   a. 如果 HTTP 响应数据包匹配配置的 HTTP 响应过滤器，用户将通过认证，否则，将显示包含错误信息的（通过命令“**aaa server http result**”配置）错误页面。

   b. 如果 HTTP 响应数据包不能匹配配置的 HTTP 响应过滤器且要求更多信息，包含挑战信息（通过命令“**aaa server http login challengemessage**”配置）的登录挑战页面将显示用于认证挑战。在这种情况下，AG 使用挑战模板（通过命令“**aaa server http challenge template**”和“**aaa server http challenge require**”指定）构建 HTTP 挑战请求并发送构建的 HTTP 挑战请求给 HTTP AAA 服务器。

   c. 如果需要进一步挑战，包含挑战信息（通过命令“**aaa server http challenge challengemessage**”配置）的挑战页面将会显示用于再次认证挑战。挑战的流程与登录挑战流程一样。如果用户通过挑战认证，系统将进行授权。否则，将显示包含错误信息（通过命令“**aaa server http result**”配置）的错误页面。

对于 HTTP 认证登录和挑战模板的细节，请参见命令行手册的“**aaa server http login template**”和“**aaa server http challenge template**”命令。

当 HTTP AAA 服务器用于授权时，AG 使用 HTTP 响应过滤器从 HTTP（授权）响应数据包中获取用户信息，例如用户名和组名。获取的用户名将会现在门户欢迎页面上替代用于登录的用户名。获取的组名可能会用于进一步的用户授权。如果没有获取到认证用户的组名，将会使用默认组（通过命令“**aaa server http defaultgroup**”配置）用于进一步授权。

AG 支持最多配置 3 台 HTTP AAA 服务器和为 HTTP AAA 服务器配置 3 台 HTTP 主机。

注意：使用 HTTPS 协议的 HTTP 主机不支持 SSL 双向认证。

5.2.6.1 高级 HTTP 认证

为了加强设备的认证授权，系统在已有 HTTP 认证的基础上，为 HTTP 认证过程增加了 Pre-Login（登录前）和 Post-Login（登录后）过程。

1. Pre-Login（登录前）：系统将检查登录前环境。Pre-Login 过程通过 HTTP 认证方式的 Challenge 过程支持与客户端多次交互以检查客户端环境。由于

与服务器可能有连续访问，所以 Challenge 可能有自动挑战，无需客户端参与。如果配置了单包授权，也在此过程中进行认证。此步骤为必须步骤。

2. 登录中：使用上一步获取的登录方法进行认证。

3. Post-Login（登录后）：该过程用于客户端信息备案。此步骤非必须的步骤。

在高级 HTTP 认证场景中，系统支持了二维码、短信认证和第三方软件认证类型的 HTTP 认证服务器。

5.2.6.2 HTTP OAuth 认证

为了简化管理员的配置步骤，针对几种常见的认证场景企业微信、钉钉和 Welink，系统提供了 HTTP OAuth 认证方式，管理员仅需在 WebUI 上填写一些必要的参数，即可轻松完成相关认证场景的创建。

5.2.6.2.1 配置示例

- **企业微信**

1. 获取企业微信认证相关参数企业 ID、应用 ID 和密钥。

2. 在 WebUI 的虚拟站点模式下，选择 **AAA 设置>AAA 服务器管理>AAA 服务器**。点击**添加**，在弹出的**新建 HTTP 服务器**页面中，设置**类型**为 **HTTP/OAuth 类型**，**OAuth 类型**设置为**企业微信**，然后填写企业微信认证的相关参数创建基于 HTTP OAuth 认证的企业微信认证服务器。

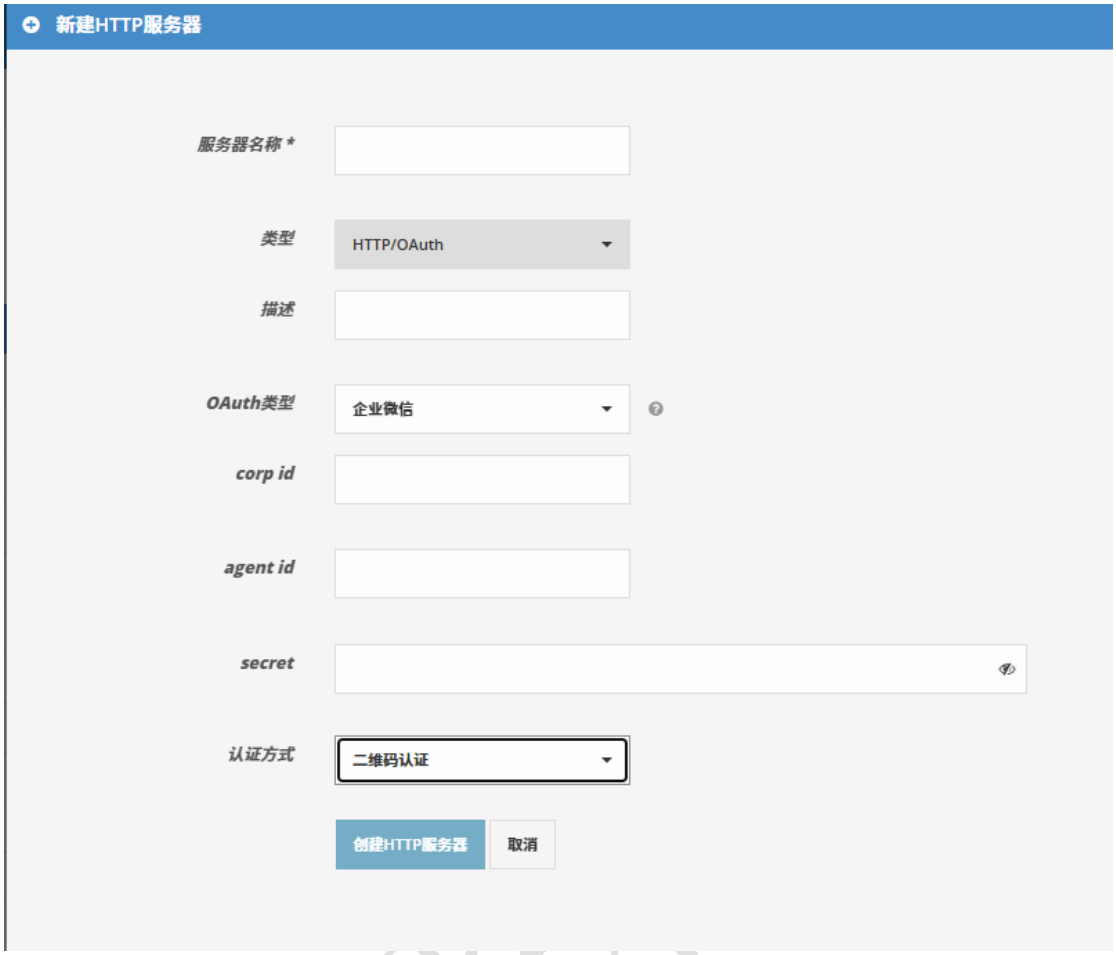

图5–1 创建基于 HTTP OAuth 认证的企业微信认证服务器

➢ **钉钉**

1. 获取钉钉认证相关参数 Client ID 和 Client Secret。
2. 在 WebUI 的虚拟站点模式下，选择 **AAA 设置>AAA 服务器管理>AAA 服务器**。点击**添加**，在弹出的**新建 HTTP 服务器**页面中，设置**类型**为 **HTTP/OAuth 类型**，**OAuth 类型**设置为**钉钉**，然后填写钉钉认证的相关参数创建基于 HTTP OAuth 认证的钉钉认证服务器。

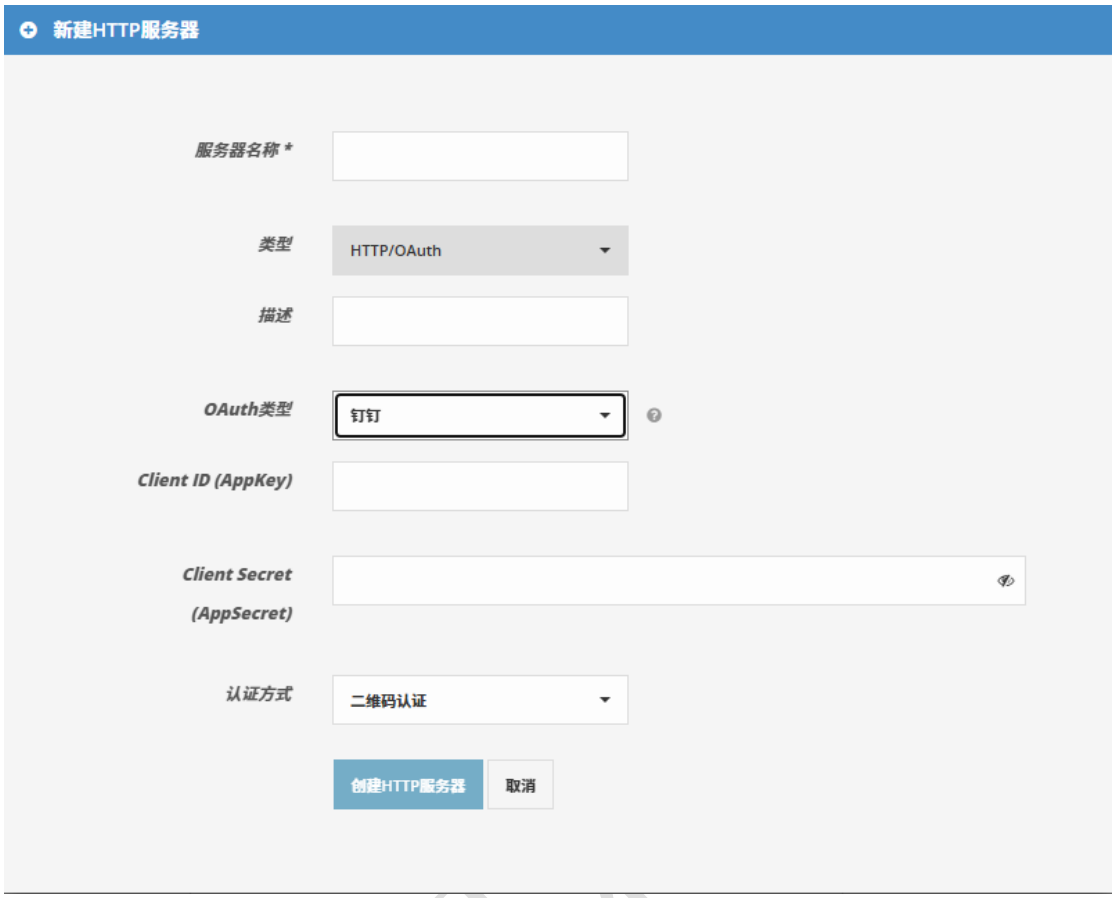

图5–2 创建基于 HTTP OAuth 认证的钉钉认证服务器

- **Welink**

1. 获取 Welink 认证相关参数 Client ID 和 Client Secret。
2. 在 WebUI 的虚拟站点模式下，选择 **AAA 设置>AAA 服务器管理>AAA 服务器**。点击**添加**，在弹出的**新建 HTTP 服务器**页面中，设置**类型**为 **HTTP/OAuth 类型**，**OAuth 类型**设置为 **welink**，然后填写企 Welink 认证的相关参数创建基于 HTTP OAuth 认证的 Welink 认证服务器。

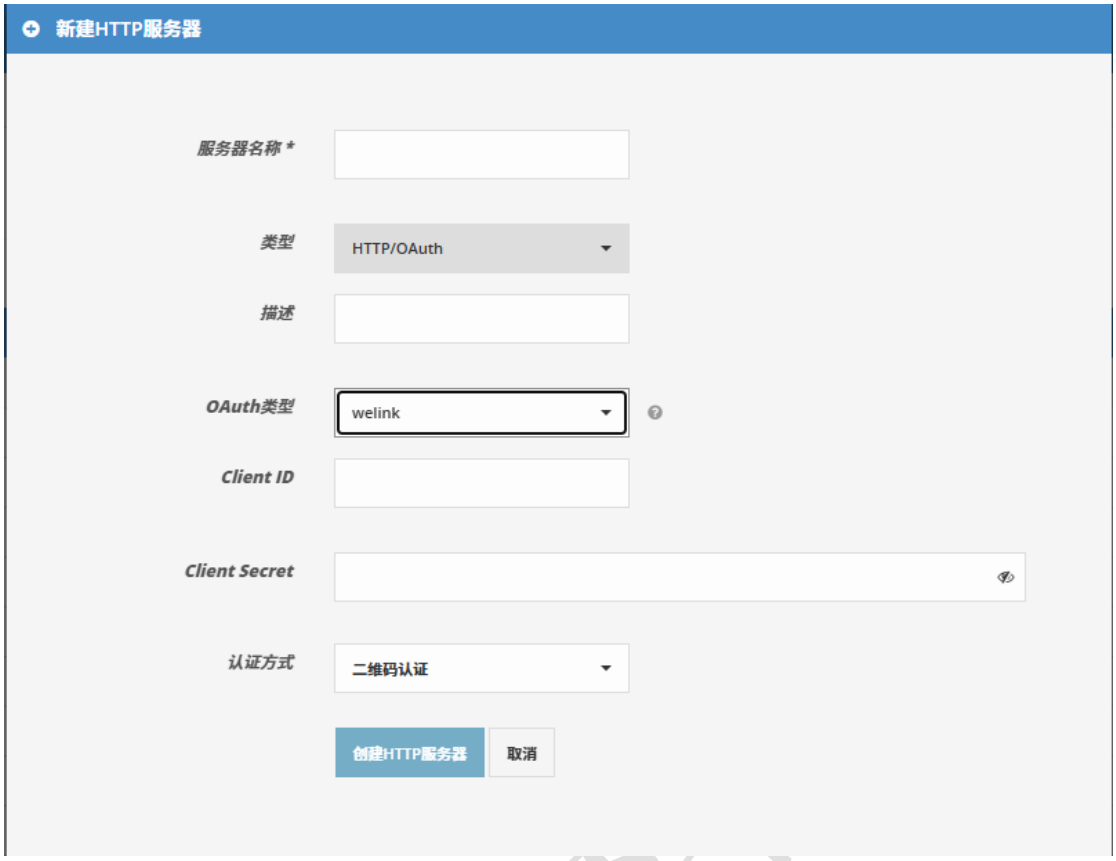

图5–3 创建基于 HTTP OAuth 认证的 Welink 认证服务器

5.2.7 硬件 ID

硬件 ID 是唯一可以标识访问虚拟站点的客户端的硬件字符串。硬件 ID 值可以在登录过程中通过 ActiveX 或 Java applet 组件自动搜集，也可以由管理员手动通过专门的硬件 ID 生成工具注册。

硬件 ID 授权基于客户端的硬件 ID 值允许或拒绝用户使用特定客户端访问虚拟站点。为了使 LocalDB 组的硬件 ID 授权生效，管理员必须启用全局硬件 ID 授权并为 LocalDB 组启用硬件 ID 授权。默认情况下，全局硬件 ID 授权和单个 LocalDB 组的硬件 ID 授权都是禁用的。

当为 LocalDB 组启用硬件 ID 授权后，自动搜集选项也应被启用以便搜集该组用户的客户端硬件 ID 值。只有通过审批的客户端才可以访问虚拟站点。当用户通过 AAA 认证和授权后，硬件 ID 授权请求将被发送给管理员审批，客户端的状态为“待定的”。当为组启用聚集选项后，管理员可以配置硬件 ID 规则授权该组的所有用户使用该客户端访问虚拟站点。当为组禁用聚集选项后，管理员可以配置硬件 ID 规则授权该组中的指定用户使用该客户端访问虚拟站点。搜集的硬件 ID 值可以匹配三种模式的硬件 ID 规则：

- “mac_any”：当任一客户端的 MAC 地址命中硬件 ID 规则中的 MAC 地址时，系统将匹配该硬件 ID 规则。
- “mac_all”：当所有客户端的 MAC 地址命中硬件 ID 规则中的 MAC 地址且客户端 MAC 地址的数量等于规则中 MAC 地址的数量时，系统将匹配该规则。
- “machineid”：当客户端的 MachineID 命中硬件 ID 规则中的 MachineID 时，系统将匹配硬件 ID 规则。MachineID 是客户端的 MAC 地址、CPU ID 和 OS ID 的组合。

为减轻管理员负担，硬件 ID 授权支持为 LocalDB 组提供自动审批选项，即虚拟站点可以自动将组中用户使用的客户端的状态设置为“批准”。

另外，管理员可以设置 LocalDB 用户或组能够自动批准的限制条件。

5.3 SAML

SAML 定义了一种基于 XML 的框架，在该框架内，各个实体之间创建并交换认证、授权和属性信息。在设备上，SAML 认证基于 SAML 2.0（Security Assertion Markup Language，安全断言标记语言）标准实现。在 SAML 框架下主要有主体（Subject）、IdP（Identity Provider，身份提供者）和 SP（Service Provider，服务提供者）三个实体。

注意：IdP 和 SP 的时区和日期、时间设置必须相同（至少在分钟级别）。

5.3.1 元数据

元数据文件定义了实体之间如何共享必要的配置信息。在开始使用 SAML 进行认证前，SP 和 IdP 需分别导入对方的元数据文件。当元数据文件有更新时，管理员必须为实体导入新的元数据文件。元数据文件主要包含以下信息：

- 实体的标识 ID
- 实体的证书，用于签名和加密
- SSO、SLO（Single Logout，单点注销）、ACS（Assertion Consumer Service，断言消费服务）等服务的 URL 地址和协议绑定类型。协议绑定类型定义了 SAML 消息在 SP 和 IdP 之间传输时使用的传输层协议。在设备上，SLO 服务支持 HTTP Redirect 和 HTTP POST 协议绑定类型，ACS 服务支持 HTTP POST 和 HTTP Artifact 协议绑定类型。
  - HTTP Redirect：利用 HTTP 重定向消息（即 302 响应）传输 SAML 消息。
  - HTTP POST：利用 Base64 编码的 HTML 内容传输 SAML 消息。

- HTTP Artifact：利用 HTML 内容或 URL 查询字符串传输 SAML 消息的索引。

- 联系人、属性要求等其他信息

5.3.2 SSO 流程

在基于 SAML 的 SSO 认证方式中，设备作为 SP 服务器，利用 IdP 服务器提供的用户身份信息进行用户认证，双方之间通过基于 SAML 标准交换信息。下图显示了基于 SAML 的 SSO 的基本流程：

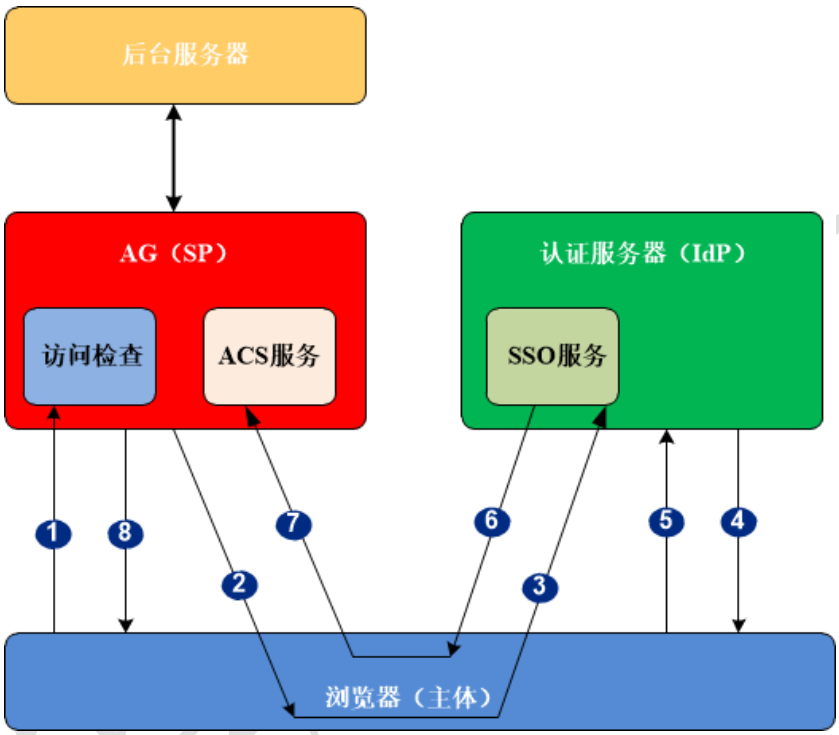

图5–4 SSO 流程

1. 客户端通过浏览器访问 SP，请求获取后台服务上的资源。

3. SP 创建一个 SAML 认证请求，重定向客户端到 IdP 服务器请求认证，请求里会指定 ACS 模块支持的协议绑定类型（通过“**aaa samlsp sp acs**”命令配置）。

4. 客户端将 SAML 认证请求发给 IdP。

5. IdP 向客户端返回认证页面，要求客户端输入登录凭据。

6. 客户端输入登录凭据。

7. IdP 验证登录凭据后返回一个 SAML 响应给客户端，其中包含关于该用户的身份断言，例如“This user is John Doe, he has an email address of john.doe@example.com, and he was authenticated into this system using a password mechanism.”。

8. 客户端浏览器将 SAML 响应发送给 SP（ACS 模块）。

9. SP 从 SAML 响应中提取出用户名（通过“**aaa samlsp idp attributes**”命令配置），确定客户端已经经过认证，返回资源给客户端。

基于以上流程的认证后，如果客户端后续访问其他资源，设备会基于已有的认证会话直接返回资源，无需客户端再次输入密码。

5.3.3 SLO 流程

通过 SAML SSO，一个终端用户可以通过一个认证环境访问多个站点，这样一个用户会在所有站点上都拥有登录会话。相比之下，SLO 的作用是回退所有这些会话的 SAML SSO 流程，将该用户在所有已登录站点上的登录会话同时注销。例如，一个终端用户通过一个 IdP 同时登录了多个 SP 站点，当该用户从其中一个 SP 站点注销时，所有其他站点上的登录也将同时被注销。

下图显示了基于 SAML 的 SLO 的基本流程：

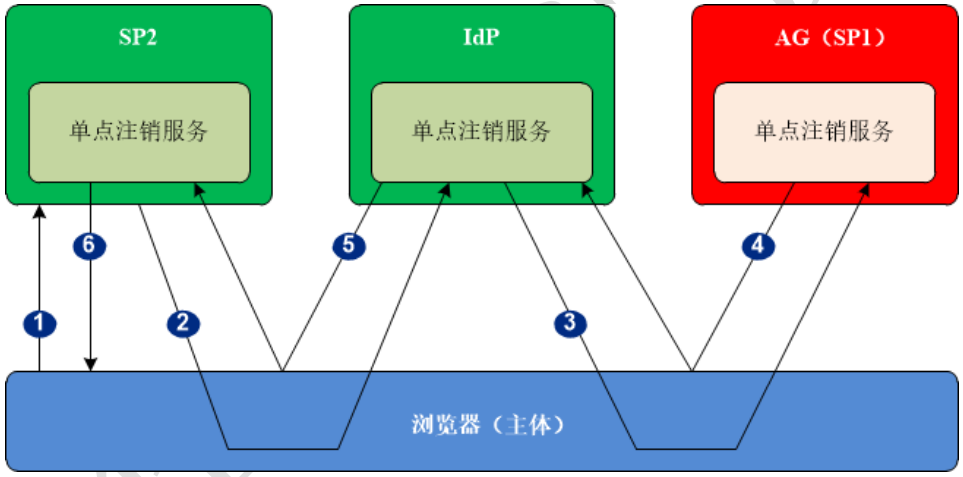

图5–5 SSO 基本流程

1. 客户端在 SP2 上发起注销请求。

10. SP2 创建 SAML 注销请求，重定向客户端到 IdP 请求注销。

11. IdP 创建 SAML 注销请求，根据 SP1 元数据文件定义的协议绑定类型将请求通过客户端的浏览器发送给 SP1 的 SLO 模块。

12. SP1 创建 SAML 注销响应，通过浏览器告知 IdP 客户端的登录会话已注销

13. IdP 通过客户端浏览器回复注销响应给 SP2，告知 SP2 客户端已经在其他 SP 上注销。

14. SP2 回复注销响应给客户端，客户端从 SP2 注销。

注意：

- 系统不支持为“shared”和“alias”虚拟站点启用 SAML 功能。
- SAML 功能不能与其他认证方法一起工作，且不支持多因素认证。
- 目前，AG 只支持终端用户直接访问 IdP。如果终端用户通过 AG 访问 IdP，SAML 认证将会失败。

5.4 FIdM

联合身份管理（Federated Identity Management，FIdM），也叫身份联合，是一种跨多个安全域联合用户的方案，每个域有自己的身份管理系统。当两个域联合时，用户可以到一个域认证，然后不用再进行重新登录就可以访问其他域的资源。

FIdM 系统的示例包括 OpenID、OAuth 和 SAML。目前，AG 仅支持 SAML FIdM 系统。

默认情况下，虚拟站点的 FIdM 方案为禁用。

5.4.1 SAML FIdM

SAML FIdM 可以让虚拟站点成为 SAML IdP，为其他 SAML SP 提供认证和授权。默认情况下，为虚拟站点禁用该功能。启用了 FIdM 方案后，系统将自动启动该功能。

要使用 SAML FIdM，管理员需要为虚拟站点（作为 SAML IdP）配置 SAML SP 作为提供认证和授权服务的对象。

5.5 AAA 方法

AAA 方法指定用于认证的 AAA 服务器。

5.5.1 多因素认证

为了对用户实施严格的安全检查并确保虚拟站点拥有更高级别的安全性，AG 允许管理员为单个 AAA 方法配置多个认证服务器以支持多因素认证（共同的用户名和多个密码）。用户只有在通过所有认证服务器的认证后才能成功登录虚拟站点。

一个 AAA 方法最多允许配置 3 个认证服务器。这三个认证服务器可以是相同类型，也可以是不同类型。

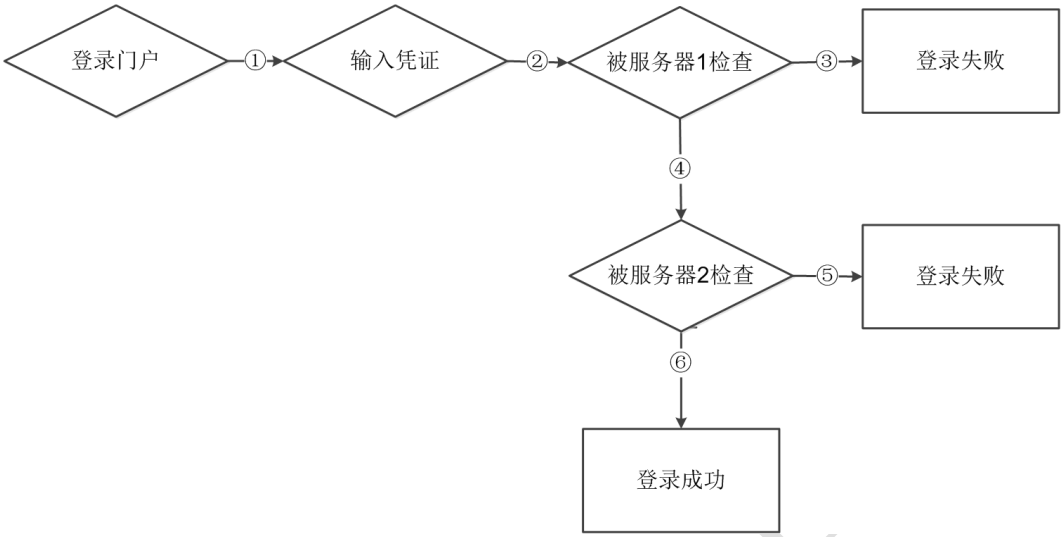

图5–6 多因素认证

上图显示了多因素认证的工作流程（两个认证服务器）：

1. 用户到达需要凭证的虚拟站点的 Web 门户。
15. 认证服务器 1 检查为这台服务器输入的用户凭据。
16. 如果凭证被服务器 1 拒绝，登录失败。
17. 如果凭证被服务器 1 接受，认证服务器 2（例如，具有次高优先级的认证服务器）检查为这台服务器输入的用户凭证。
18. 如果凭证不正确，AG 提示用户再次输入凭证。
19. 如果凭证正确，AG 为用户显示成功登录页面。

5.5.2 授权

在授权过程中，AG 将从授权服务器获取授权数据，例如组信息、外部访问控制列表（ACL）、外部子网/Netpool。

这些授权数据将进一步用于资源分配和访问控制。更多信息，请参见 7.1 用户角色和 7.2 访问控制列表。

5.5.3 修改密码

管理员可以通过为指定的 AAA 方法配置修改账户密码的认证方法的方式在登录虚拟站点前直接修改账户密码。配置该功能后，用户通过手机验证码或其他的自定义的验证方式进行身份验证，如果用户通过了验证方式，便可以对账户密码进行修改。目前仅支持为 LocalDB 类型的用户配置修改账户密码的认证方法。

5.5.3.1 配置示例

➢ **配置步骤**

1. 配置一个 LocalDB 账户。

```
Demo(config)$aaa server name localdb local
Demo(config)$aaa method server localdbf local local
Demo(config)$localdb account a a
```

2. 配置 HTTP 认证。

```
Demo(config)$aaa server name http http1
Demo(config)$aaa server http host http1 192.168.83.71 80
Demo(config)$aaa server http variant request name "http1" "<an_tc>" "tc=<an_tc>&"
Demo(config)$aaa server http variant request profile "http1" "deviceid=<an_tc>&"
Demo(config)$aaa server http result http1 "200"
Demo(config)$aaa method server httpf http1 http1
```

3. 将 HTTP 认证方法配置为 LocalDB 认证方法的修改密码的认证方法。

```
Demo(config)$aaa method changepass localdbf httpf
```

➢ **配置验证**

1. 通过浏览器打开登录虚拟站点的页面，如下图所示。可以看到认证方法“httpf”被隐藏，只有“localdbf”认证方法。

图5–7 浏览器登录虚拟站点

2. 点击上图中的“忘记密码？”，将会跳转到“httpf”认证页面。

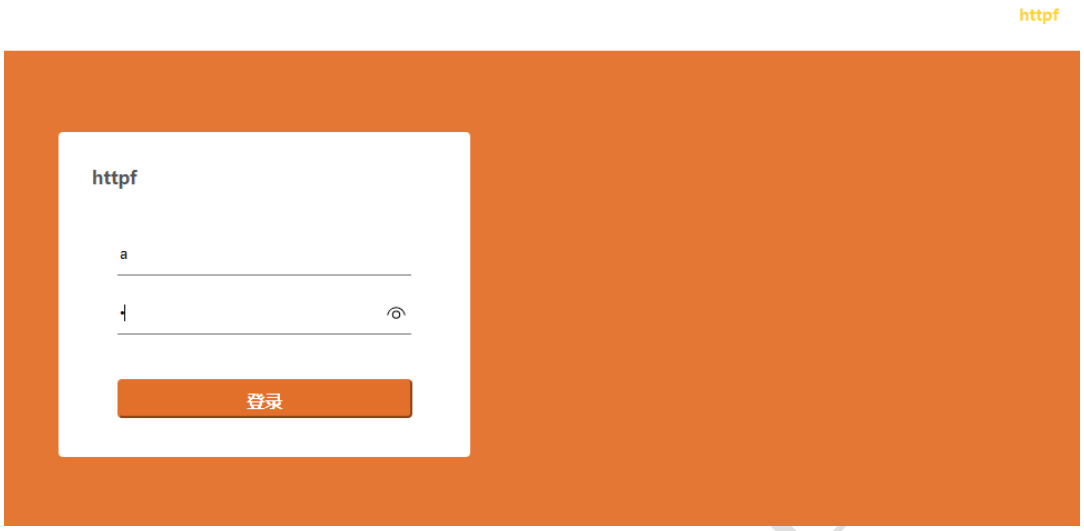

图5–8 HTTP 认证页面

3. 当输入用户名密码通过“httpf”认证页面后将会跳转到修改密码页面。

图5–9 修改密码页面

20. 输入两次新密码后，点击修改密码，将会跳转到最初的认证页面，此时用户可以使用修改后的新密码进行认证登录。

图5－10 初始认证页面

5.6 启用 AAA 功能

完成全部配置后，可以启用 AAA 功能。

- **CLI 配置示例**

启用 AAA 功能。

```
vs(config)#aaa on
```

第6章 旁路认证

AG 支持旁路认证模式。在该模式下，AG 作为旁路认证网关进行部署，当用户需要通过自有的认证平台访问后台资源时，认证平台将 HTTP/HTTPS 请求报文发送给 AG，AG 解析报文并进行处理，并将认证结果返回认证平台。认证完成后，AG 不再进行后续的数据处理。

AG 支持证书认证、静态认证和联合认证三种认证方式。其中，联合认证即同时进行证书认证和静态口令认证。

下面是一种典型的旁路认证部署方式。

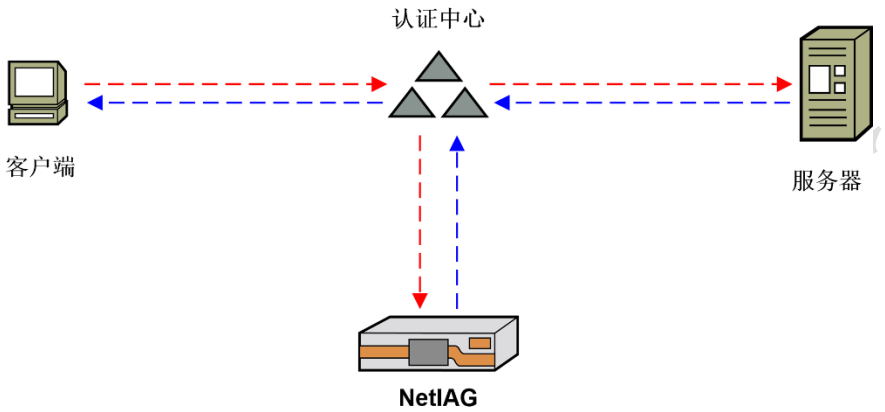

图6–1 旁路认证

6.1 静态认证

AG 将请求中的用户凭据与本地的配置文件进行匹配。如果使用静态认证，需要配置 AAA 认证服务器及 AAA 方法。系统支持的静态认证包括 LocalDB、RADIUS、LDAP/AD、HTTP 认证等。不支持多步认证。出于安全考虑，使用静态认证应该使用 HTTPS 协议。

静态认证流程如下：

1. 客户端向服务器访问后台资源。
2. 服务器使用身份认证请求报文发送给服务器。身份认证请求报文格式见 6.1.1。
3. AG 验证身份认证请求并返回身份认证响应报文。身份认证响应报文格式见 6.1.2。

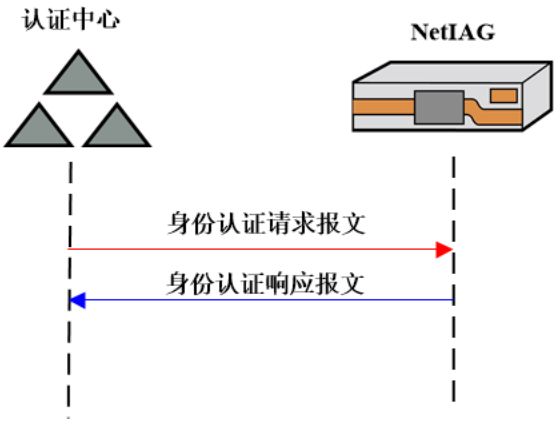

图6–2 静态认证

下面介绍报文的格式。

6.1.1 身份认证请求报文

```
<?xml version="1.0" encoding="UTF-8"?>
<message>
    <head>
        <version>1.0</version>
        <serviceType>authenService</serviceType>
    </head>
    <body>
        <appId>T1</appId>
        <authen>
        <authCredential authMode="password">
        <uname>t</uname>
        <pwd>t</pwd>
        </authCredential>
        </authen>
    </body>
</message>
```

version：报文版本信息。

serviceType：表示请求服务的类型。分别为 OriginalService 和 authenService。OriginalService 表示请求随机数，authenService 表示认证。

authCredential：表示静态密码认证方法，authMode 需要设为“password”。

uname：用户名。

pwd：密码，为明文。

6.1.2 身份认证响应报文

```
<?xml version="1.0" encoding="utf-8"?>
<message>
    <head>
        <version>1.0</version>
        <serviceType>AuthenService</serviceType>
        <messageState>true</messageState>
    </head>
    <body>
        <authResultSet allFailed="false">
        <authResult authMode="password" success="true"/>
        </authResultSet>
    </body>
</message>
```

version：报文版本信息。

serviceType：表示请求服务的类型。分别为 OriginalService 和 authenService。OriginalService 表示请求随机数，authenService 表示认证。

authResultSet allFailed：是否所有认证请求都失败。“true”所有认证请求都失败，“false”至少有一种认证请求成功。

authResult：认证结果项。

authMode：认证的方式。包括“cert”和“password”，分别表示证书认证方式和静态口令认证方式。

success：认证结果。“true”表示当前认证方式成功。“false”表示认证失败。

6.2 证书认证

使用证书认证前，需要先将认证中心的根证书导入 AG。

证书认证流程如下：

1. 客户端向服务器访问后台资源。
2. 服务器向 AG 发送随机数请求报文。
3. AG 生成随机数并将随机数响应报文返回给服务器。
4. 服务器使用随机数生成身份认证请求报文发送给服务器。
5. AG 验证身份认证请求并返回身份认证响应报文。

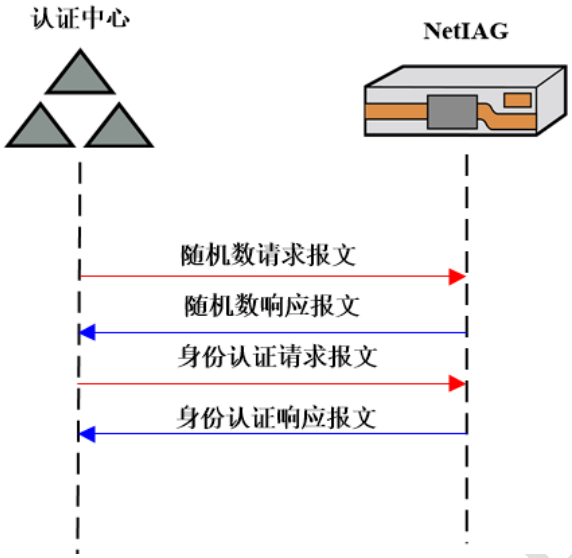

图6–3 证书认证

下面介绍四种报文的格式。

6.2.1 随机数请求报文

随机数请求报文格式如下：

```
<?xml version="1.0" encoding="UTF-8"?>
<message>
    <head>
        <version>1.0</version>
        <serviceType>OriginalService</serviceType>
    </head>
    <body>
        <appId>T1</appId>
    </body>
</message>
```

version：报文版本信息。

serviceType：表示请求服务的类型。分别为 OriginalService 和 authenService。OriginalService 表示请求随机数，authenService 表示认证。

appId：表示注册的服务名称。使用旁路认证服务前须在 AG 上预先注册，如果没注册过，则不予注册。

6.2.2 随机数响应报文

随机数响应报文格式如下：

```
<?xml version="1.0" encoding="utf-8"?>
```

```
<message>
    <head>
        <version>1.0</version>
        <serviceType>OriginalService</serviceType>
        <messageState>true</messageState>
    </head>
    <body>
        <original>icC7s5nwLf</original>
    </body>
</message>
```

version：报文版本信息。

serviceType：表示请求服务的类型。分别为 OriginalService 和 authenService。OriginalService 表示请求随机数，authenService 表示认证。

messageState：表示报文处理是否正常，“true”代表报文处理正常，“false”代表报文处理异常。在报文处理正常的情况下，报文请求服务成功或失败通过 messageCode 和 messageDesc 标识。

original：生成的随机数，由 10 位的数字和字母组合而成。

6.2.3 身份认证请求报文

```
<?xml version="1.0" encoding="UTF-8"?>
<message>
    <head>
        <version>1.0</version>
        <serviceType>authenService</serviceType>
    </head>
    <body>
        <appId>T1</appId>
        <authen>
        <authCredential authMode="cert">
        <detach>MIIDLgYJKoZIhvcNAQcCoIIDHzCCAxsCAQExDjAMBggqgRzPVQGDEQ
UAMAsGCSqGSIb3DQEHAaCCAjkwggI1MIIB2qADAgECAgYA0Bk5JsAwDAYIKoEcz1UBg
3UFADBDMQswCQYDVQQGEwJjbjEQMA4GA1UECgwHaW5mb3NlYzEPMA0GA1UECw
wGc3lzdGVtMREwDwYDVQQDDAhjYTYyX3NtMjAeFw0yMDA1MTkwNjI1MzBaFw0yMz
AyMTMwNjI1MzBaMDgxCzAJBgNVBAYTAkNOMQswCQYDVQQKDAJkZDEMMAoGA1
UECwwDZGQxMQ4wDAYDVQQDDAVxcXFxcTBZMBMGByqGSM49AgEGCCqBHM9VAY
ItA0IABFGVtisUMl3QooUJ/Hrpgd7Eklw99hX80PYolcdH21gzb+lUeSOREnobAiBMx1zKH/jeJ
42l7QalQTNlHeuiT8ijgcIwgb8wHwYDVR0jBBgwFoAU0HzHHs//lXfy/1yIRG2kk05QD5owCQ
YDVR0TBAIwADBiBgNVHR8EWzBZMFegVaBTpFEwTzEPMA0GA1UEAwwGY3JsMzA5M
QwwCgYDVQQLDANjcmwxDzANBgNVBAsMBnN5c3RlbTEQMA4GA1UECgwHaW5mb3N
```

```
lYzELMAkGA1UEBhMCY24wDgYDVR0PAQH/BAQDAgbAMB0GA1UdDgQWBBTJdtR+vp
emqoALxqr9Z0QTK+CVHDAMBggqgRzPVQGDdQUAA0cAMEQCICcmkTloeg82CKawt91y
10jmu/vUi+TtArDTCNt/GhFkAiBl0Q71IKY1/FXbvKFCPW20sKX2AM8crTFW3HT9h3dbKD
GBuzCBuAIBATBNMEMxCzAJBgNVBAYTAmNuMRAwDgYDVQQKDAdpbmZvc2VjMQ8
wDQYDVQQLDAZzeXN0ZW0xETAPBgNVBAMMCGNhNjJfc20yAgYA0Bk5JsAwDAYIKoE
cz1UBgxEFADANBgkqgRzPVQGCLQMFAARHMEUCIQDjpyZxSOfzwRI9414nb2n3Q8QC2Z
gSuAfUO+3EdenlvwIgALiyBYmf5eOxql/lzsKQTJgQnb+CZXBCMVFXpYSgJ20=</detach>
        <original>icC7s5nwLf</original>
        </authCredential>
        </authen>
        <attributes attributeType="portion">
        <attr name="X509Certificate.SubjectDN"></attr>
        </attributes>
    </body>
</message>
```

version：报文版本信息。

serviceType：表示请求服务的类型。分别为 OriginalService 和 authenService。OriginalService 表示请求随机数，authenService 表示认证。

appId：表示注册的服务名称。使用旁路认证服务前须在 AG 上预先注册，如果没注册过，则不予应答。

authCredential：表示证书认证方法，authMode 需要设为“cert”。以 Base64 方式呈现。分为<detach>和<attach>两种方式。Detach 方式的认证请求包中不包含随机数，所以需要与<original>字段配合使用将认证原文提交给网关。<attach>方式包含随机数，不需要设置<original>字段

original：生成的随机数，可以使用明文，也可以使用 Base64 编码。

attributes：用户属性请求列表，表示应用系统需要请求的用户属性。这些属性来自于用户的身份证书，可根据需要向网关请求用户的所有属性、指定属性或不请求属性。

attributeType：用户属性请求类型。分为“all”、“portion”或者“none”。“all”表示请求所有属性信息；“portion”表示只请求列表中指定的属性信息；“none”表示不请求任何属性信息。

attr name：指定要请求的某项用户属性信息。例如：X509Certificate.SubjectDN 表示请求的是用户身份证书中的主题（证书 DN）信息。其中 name 表示所请求属性的名称，可为中文。目前支持的取值如下：

- X509Certificate.NotBefore：证书开始生效时间。
- X509Certificate.NotAfter：证书结束生效时间。
- X509Certificate.SubjectDN：证书主题。

- X509Certificate.SerialNumber：证书序列号。
- X509Certificate.IssuerDN：证书颁发者 DN。

6.2.4 身份认证响应报文

```
<?xml version="1.0" encoding="utf-8"?>
<message>
    <head>
        <version>1.0</version>
        <serviceType>AuthenService</serviceType>
        <messageState>true</messageState>
    </head>
    <body>
        <authResultSet allFailed="false">
        <authResult authMode="cert" success="true"/>
        </authResultSet>
        <attributes>
            <attr name="X509Certificate.SubjectDN"> C =CN, O = dd, OU = dd1, CN =
qqqqq</attr>
        </attributes>
    </body>
</message>
```

version：报文版本信息。

serviceType：表示请求服务的类型。分别为 OriginalService 和 authenService。OriginalService 表示请求随机数，authenService 表示认证。

messageState：表示报文处理是否正常，“true”代表报文处理正常，“false”代表报文处理异常。在报文处理正常的情况下，报文请求服务成功或失败通过 messageCode 和 messageDesc 标识。

authResultSet allFailed：是否所有认证请求都失败。“true”所有认证请求都失败，“false”至少有一种认证请求成功。

authResult：认证结果项。

authMode：认证的方式。包括“cert”和“password”，各表示证书认证方式和口令认证方式。

success：认证结果。“true”表示当前认证方式成功。“false”表示认证失败。并出现 **authMessageCode 和 authMessageDesc** 做错误提示。**authMessageCode** 为认证错误代码。**authMessageDesc** 为认证错误描述。

attributes：用户属性列表。

attr：每个表示属性的定义。

name：所请求属性的名称，与请求报文中相同。

6.3 配置示例

6.3.1 前提条件

1. 假设已配置了虚拟站点。
2. 如果要使用 HTTPS 协议发送认证请求，需要先启用 SSL 功能。
3. 如果使用静态口令认证，需要配置 AAA 认证服务器及 AAA 方法。

6.3.2 配置步骤

1. 导入受信任的 CA 证书。如果使用静态口令认证，不需要进行该配置。

```
vs1(config)$ssl import rootca
-----BEGIN CERTIFICATE-----
MIIBsDCCAVSgAwIBAgIGAOCLTsvGMAwGCCqBHM9VAYN1BQAwLDELMAkGA1UEBh
MCY24xDTALBgNVBAoMBGluZm8xDjAMBgNVBAMMBXNtMmNhMB4XDTE1MTAzMD
A2MzEzOVoXDTI1MTAzMDA2MzEzOVowLDELMAkGA1UEBhMCY24xDTALBgNVBAoM
BGluZm8xDjAMBgNVBAMMBXNtMmNhMFkwEwYHKoZIzj0CAQYIKoEcz1UBgi0DQgAE
06Og74VLlxRhNp7YAsLc85gxxl1MvwlZZKL/3IssMy8NovgIcNUpDe7Bdaie4/yIqYWVv1SYK
YcOtgdAAXJUvKNgMF4wHwYDVR0jBBgwFoAUBP8AQRdSMrSmwBEm+sExR19YHXcw
DwYDVR0TAQH/BAUwAwEB/zALBgNVHQ8EBAMCAQYwHQYDVR0OBBYEFAT/AEEX
UjK0psARJvrBMUdfWB13MAwGCCqBHM9VAYN1BQADSAAwRQIgQRrmZ9VuBnEUUhF
NdvNNWcfk61tOTtLqD5TovXEk53oCIQCdoL1eABzY0r/uaS9bwb0SncIJ+jhrXB5VQ7/ORu5jq
Q==
-----END CERTIFICATE-----
…
```

2. 启用联合身份认证功能。

```
vs1(config)$aaa federation enable
```

3. 启用旁路认证功能。

```
vs1(config)$aaa federation restful enable
```

4. 注册要访问的应用。

```
vs1(config)$aaa federation restful register "testApp1" "123456"
vs1(config)$aaa federation restful register "testApp2" "abcd"
```

5. （可选）设置证书认证的随机数超时时间。如果使用静态口令认证，不需要进行该配置。

```
vs1(config)$aaa federation restful random timeout 300
```

6. （可选）设置静态口令认证使用的认证方法。如果使用证书认证，不需要进行该配置。

```
vs1(config)$aaa federation restful password method "radius"
```

7. （可选）如果需要通过 HTTP 协议发送认证请求，需要启用 80 端口监听。执行以下命令后，AG 会对该虚拟站点对应的所有 IP 地址的 80 端口进行监听。

```
vs1(config)$aaa federation restful http start
```

第7章 用户策略

7.1 用户角色

设备根据用户特定的资格（如登录时间、用户名、组名、源 IP 和 AAA 认证方法）授予已认证用户相应的角色，使其可以访问相应资源，以此来实现精准灵活的资源分配。

要访问虚拟站点中的任何资源，用户必须获得至少一个角色。否则，设备将强迫用户登出虚拟站点并要求用户重新登录虚拟站点。用户在获得一个或多个角色之后，将被授权访问和角色相关的所有资源。

7.1.1 用户角色、资格和条件

用户只有在满足一个特定资格中的一个或多个条件时才能获得一个用户角色。设备允许管理员为一个角色定义多个资格，也允许为一个资格定义多个条件。用户只有在满足一个资格中的所有条件时才能满足该角色条件，同时只有在满足任意角色资格时才能获得一个角色。

资格条件可以描述以下用户特征：

- 登录年份
- 登录月份
- 登录日期
- 登录时间
- 登录日期
- 登录星期
- 用户名
- 组名
- 源 IP 地址
- AAA 认证方法

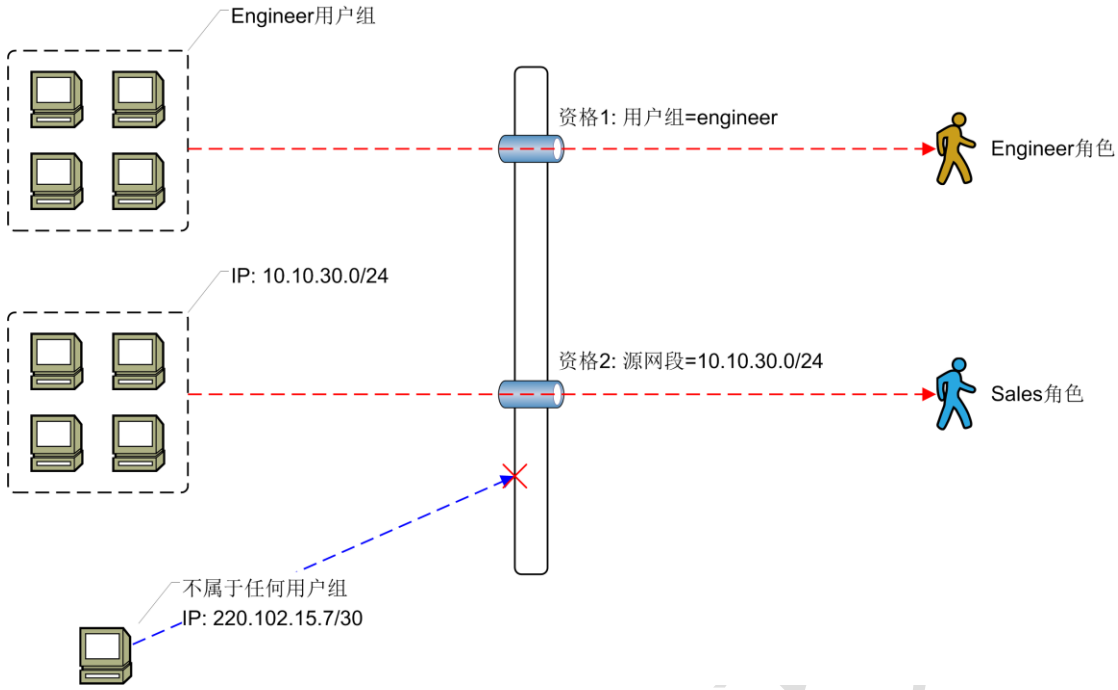

图7–1 角色、资格和条件

上图展示了在授权大量登录用户时，用户角色资格授予的整个过程。该案例中设计两种资格，每个资格包含一个条件：

- 资格 1 的条件：用户组为“engineer”
- 资格 2 的条件：源网络为“10.10.30.0/24”

按照上图所示，访问结果如下：

- 来自“Engineer 用户组”的用户符合资格 1 的条件“group = engineer”，因此这些用户获得了“Engineer”角色。
- 来自网段“10.10.30.0/24”的用户符合资格 2 的条件“network = 10.10.30.0/24”，因此这些用户获得了“Sales”角色。
- 用户如果既不符合资格 1 的条件又不符合资格 2 的条件，将无法获得任何角色，因此无法通过设备访问任何资源。

注意：

- 管理员可以为一个资格定义多个条件，这些条件之间的逻辑关系为“AND”。管理员可以为一个角色绑定多个资格，这些资格之间的逻辑关系为“OR”。
- 管理员可以定义一种不包含任何条件的全匹配资格。定义为这种类型资格的角色可以被分配给任何已认证的用户。

➢ **CLI 配置示例**

1. 定义一个用户角色。

```
vs(config)#role name role1 "role1" 3
```

2. 为指定的用户角色添加一个角色资格。

```
vs(config)#role qualification role1 qual1 "qual1"
```

3. 为指定的用户角色和资格添加关联条件。

```
vs(config)#role condition role1 qual1 " LOGINDAY IS 1"
```

7.2 访问控制列表

访问控制列表（ACL）可以规定哪些用户、用户组或者角色可以访问指定的资源。当用户通过虚拟站点访问资源时，这些 ACL 规则将应用于用户。目前，ACL 只支持对网络（IP/TCP/UDP/ICMP）类型的资源进行访问权限控制。更多关于这类资源的信息，请参考章节第 8 章接入方法。

ACL 规则可以配置在用户、用户角色或是用户组上。当用户访问虚拟站点时，配置在与该用户相关的用户、角色和用户组上的所有 ACL 规则都会生效。所有的 ACL 规则会以从高到低的优先级排序并储存在用户会话中。

经过身份认证后，ACL 与用户会话相关联且不能在会话中断前修改或更新。因此，如果管理员对一个已经登录（处于会话有效期）的用户修改 ACL 规则，这些修改只有在用户登出再重新登录（开始新会话）时才会生效。

如果用户会话未匹配虚拟站点的任何 ACL 规则，用户将能通过该虚拟站点不受限制地访问所有 VPN 类型的资源。如果用户会话匹配了虚拟站点的一条或多条 ACL 规则，且这些 ACL 规则应用到了某种类型 VPN 的部分或全部资源，那么在没有 ACL 规则明令允许访问的前提下，设备将拒绝用户访问该类型的资源。

7.2.1 ACL 资源

目前，系统只支持网络类型的 ACL 资源。网络资源是一种三层或四层的资源，如“udp://10.1.1.1:25”、“tcp://10.1.1.0/24:25, 1080, 2200”或“10.10.1.1/24”。

资源组是一种可以包含一个或多个同类型资源的对象。一条 ACL 规则可以允许或拒绝一种角色、一个用户或一个用户组访问指定的资源组。

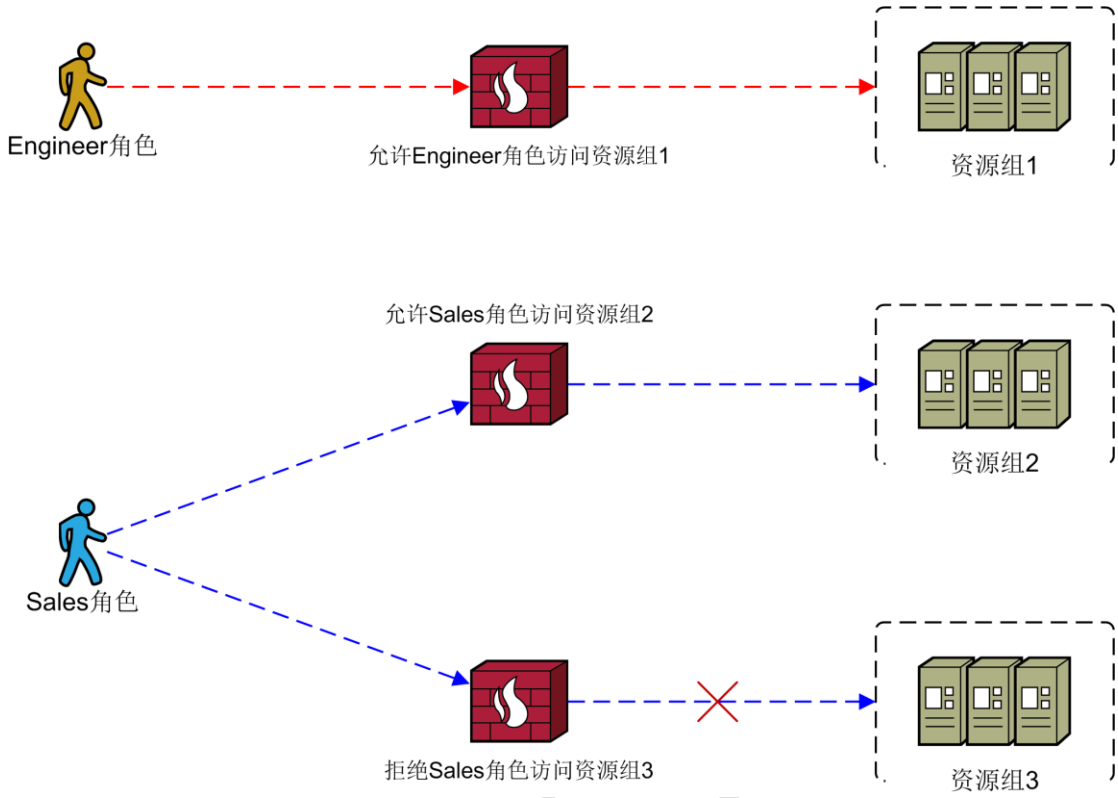

图7–2 ACL 规则

- **CLI 配置示例**

1. 添加一个“network”类型的资源组。

```
vs(config)#acl resourcegroup network network networkresource
```

2. 为 ACL 资源组添加一个资源。

```
vs(config)#acl resource network "10.10.10.0/24"
```

3. 定义一条 ACL 规则。

```
vs(config)#acl rule user1 network deny 90 U
```

7.3 用户会话管理

会话管理为设备提供了一种控制设备使用的方式。客户端和设备之间的会话记录了一些重要的用户信息，如用户名、角色名、会话类型、L3 所需的 IP 或是连接参数等。

设备允许管理员监控、终止、重用和限制用户会话。

7.3.1 会话统计

通过会话管理，可按照先前创建的顺序列出活动会话。并且，管理员可以执行“**show session active**”命令来查看以下会话统计：

表7–1 会话统计

统计信息	描述
用户名	本次会话的用户名。
会话 ID	会话 ID。如果会话重用被开启，一些统计记录可能会有相同的会话 ID。
会话时间	自会话被创建后会话的剩余时间。
最后活跃时间	自用户上一次操作后会话的剩余时间。

如果需要查看活动会话关联的客户端 IP、Netpool 或 VPN 资源，管理员可以执行“**show session policy**”命令：

表7–2 会话统计

统计信息	描述
客户端 IP	分配给 SSL VPN 客户端的动态 IPv4 地址。
Netpool 名称	分配给 SSL VPN 客户端 Netpool。
VPN 资源类型	分配给 SSL VPN 客户端的 VPN 资源的类型
VPN 资源	分配给 SSL VPN 客户端的 VPN 资源。

- **CLI 配置示例**

显示匹配指定过滤条件的活动会话。

```
vs(config)$show session active all

User Name                Session ID     Age          Last Active
u1                       31760CF2       00:59:20     00:00:28
```

显示匹配指定过滤条件的活动会话关联的客户端 IP。

```
vs(config)$show session policy all i
User Name                Session ID     Client IP
u1                       31760D13       10.0.0.227/24
```

```
u35                      31760D16       10.0.1.201/24
```

7.3.2 会话超时

管理员可以单独管理已认证和未认证会话的超时时间。

对于已认证的会话，管理员可以通过两种方式使它们超时：

- 空闲超时：当会话的空闲时间到达上限，会话将超时（通过“**session timeout idle**”命令配置）。
- 生存期超时：当会话的生存时间到达上限，会话将超时（通过“**session timeout lifetime**”命令配置）。

注意：如果管理员同时设置了两种类型的超时时间，系统将基于最先到达的超时时间终止已认证的会话。

管理员也可以使用“**session kill**”命令手动终止会话。

➢ **配置示例**

1. 设置会话空闲超时。

```
vs(config)$session timeout idle 1000
```

2. 设置会话生存周期超时。

```
vs(config)$session timeout lifetime 1000
```

3. 终止指定的活动会话。

```
vs(config)$session kill "user=u1"
```

7.3.3 会话重用

当为一个虚拟站点启用会话重用功能后，通过同一用户名登录该虚拟站点的用户将共享同一个会话。如果一个用户终止了会话，所有其他用户需要重新登录，以继续维持连接。此功能针对每个虚拟站点单独生效。

当会话重用功能禁用之后，不同客户端的用户将使用自己独立的会话。

当 AAA 功能禁用后，系统将为每一个试图访问 AG 的最终用户生成“guest”会话。在这种情况下，必须关闭会话重用功能。

会话重用功能可以通过启用 AAA 功能和为虚拟站点启用会话重用功能来开启。

注意：会话重用功能只能在全局模式下进行设置。

➢ **CLI 配置示例**

1. 启用会话复用功能。

```
AN(config)$virtual site session reuse on
```

2. 启用 AAA 功能。

```
vs(config)$aaa on
```

7.3.4 会话限制

站点会话限制维持虚拟站点的活跃会话数。如果用户试图登录并且活跃且非过期的会话数小于允许的上限，那么就可以创建新会话，同时虚拟站点会话计数器的数值将会增加。匿名会话不计入其内。

用户会话限制允许管理员限制每个用户同时使用的会话数。如果用户会话数到达上限，用户将不能创建新的会话。

- **CLI 配置示例**

设置最大并发会话数量。

```
vs(config)$virtual site session limit vs 1000
```

设置单个用户的最大会话数量。

```
vs(config)$session maxperuser 1000
```

第8章 接入方法

系统支持两种类型的接入方法：Web 接入和网络接入。Web 接入适用于浏览 HTTP/HTTPS 资源的 Web 应用，网络接入适用于所有 IP 应用。Web 接入不要求任何客户端软件或浏览器插件，然而对于网络接入，第一次部署时需要安装客户端软件（SSL VPN 客户端）。网络接入支持两种类型的启动方式：Web 启动和独立启动。此外，系统提供了 API（Application Programming Interface，应用程序编程接口）调用 SSL VPN 客户端。

8.1 Web 接入

Web 接入功能提供了一种无客户端的、无缝的安全接入方式。Web 接入允许用户只需点击门户页面的链接即可访问内网资源，非常便捷高效。同时 Web 接入功能可以通过映射、改写等方式，隐藏内网资源的 URL，为内网应用提供了安全保护。

本节主要从以下几个方面介绍：

- Web 资源：门户页面直接展示供用户访问的 Web 资源。
- Web 策略：将指定客户端请求映射到指定后台资源。
- 网页改写：对后台服务器的请求、响应的包头或者报文主体进行改写。
- SSO：用户在登录门户之后可以直接访问后台应用而无需再次进行认证。

8.1.1 Web 资源

系统支持两种方式配置 Web 资源：

- 直接创建：直接创建 Web 资源（通过命令“**resource name**”）。此类资源将直接显示在门户页面上。
- 后台映射：将客户端请求映射到后台资源（通过命令“**server resource**”）。此类资源需要结合 Web 策略才能访问。

8.1.2 Web 策略

Web 策略可以将指定客户端请求映射到指定后台资源。当客户端请求中的 URL 匹配 Web 策略中配置的 URL 时，设备将请求转发到对应的后台 Web 服务器上。

此外，系统也支持将 Web 策略与直接创建的 Web 资源搭配使用。用户点击门户页面的 Web 资源链接将会访问对应的 URL，命中 Web 策略，之后设备将请求转发到指定的后台 Web 服务器上。

➢ **配置示例**

1. 创建一个虚拟站点。

```
demo(config)#virtual site name vs "vs" "exclusive"
demo(config)#virtual site ip vs 1.1.1.1 443
```

2. 配置一个 LocalDB 账户并配置角色、角色资格。

```
vs(config)#aaa server name localdb localdb localdb
vs(config)#aaa method server localf localdb
vs(config)#no localdb passwdqc all
vs(config)#localdb account test test
vs(config)#localdb group group1 "group1" 23
vs(config)#localdb member group1 test
vs(config)#aaa on
vs(config)#role name role1
vs(config)#role qualification role1 q1
```

3. 配置 Web 资源。

➢ **方式一**

1. 配置一个后台 Web 资源并配置 Web 策略。

```
vs(config)#server resource "server1" "http" "10.3.0.70" 80
vs(config)#server policy "/aaa" "server1" "" "public" virtual
```

用户第一次访问“https://1.1.1.1:443/aaa”时，需要输入账号密码登录虚拟站点，之后再次访问“https://1.1.1.1:443/aaa”时，将会命中设备上配置的 Web 策略，之后设备将请求转发到后台服务器（http://10.3.0.70/aaa）。

➢ **方式二**

2. 创建 Web 资源。

```
vs(config)#resource name web web1
vs(config)#resource web url web1 "https://1.1.1.1:443/aaa" "" 0 1
vs(config)#resource assign torole web web1 role1
```

注意：采用 Web 策略和直接创建的 Web 资源配合使用的方式时，通过命令“**resource web url**”为门户页面上的 Web 资源配置 URL 时，参数“rewrite_url”和“rewrite_response”的取值必须分别为“0”和“1”。

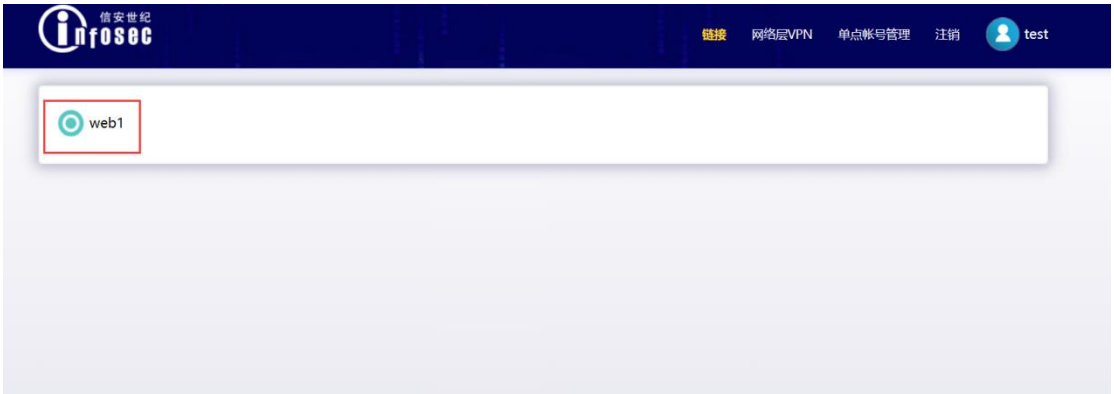

图8–1 虚拟站点上显示的资源

此时用户只需点击虚拟站点上的 Web 资源链接（web1）即可访问后台 Web 服务器。

8.1.3 网页改写

网页改写功能通过仅将一个域名或 IP 地址暴露到公网来隐藏内部网络架构。网页改写功能支持对客户端请求和响应的头部字段以及响应页面内容进行改写，从而隐藏后台服务器 URL 地址、文件名称、路径等信息来保障后台服务器的安全。具体如下：

- 支持对如下 HTTP 请求、响应的头部字段进行改写：Location、Origin、Referer、Content-Length、Cookie、Host、Range、If-Range。
- 支持改写 HTML 中所有带有 URL 属性的标签。
- 支持改写 JavaScript、Cascading Style Sheets（CSS）、HTTP Cookie 等内容。
- 支持改写 HTML/JavaScript 内容中嵌入的链接。
- 支持不同的传输场景（例如：分段透传）。
- 通过配置浏览器 localStorage 对象改写规则、中括号变量改写规则等能够使系统支持对不同的内容进行改写。

注意：

- 由于非标准的 Web 编程、新技术或其他原因，网页改写功能可能无法处理某些情况。因此，在部署前，请先使用网页改写测试应用。
- 对于 URL 中不带主机名的请求，系统通过 Referer 转发处理。当收到的客户端请求中无主机名时，例如 https://192.168.1.1/test.html，系统会从请求头部字段中的 Referer 字段信息重新组建一个 URL 地址重定向到客户端，这样客户端就会重新发起带有主机名的请求。例如，如果收到“https://192.168.1.1/js/1.js”的请求，设备将使用当前请求头部字段中的 Referer 中的主机地址来进行转发。假设 Referer 字段的值为：https://<vsite>/prx/000/http/1.1.1.1/path1/1.html，当收到“https://192.168.1.1/js/1.js”这样的请求时，会组建一个 URL

https://192.168.1.1/prx/000/http/1.1.1.1/js/1.js 进行重定向。

- 网页改写功能不支持的 Web 内容包括：
  1. 大于 5M 的文件。
  2. 浏览器插件(比如 ActiveX)中的代码。
  3. ES6 及以上语法标准的脚本。
  4. 由于使用嵌入的 Java 小程序、Flash 或 ActiveX 元素的 Web 应用不是通过 HTTP 与后台服务器通信，所以它们必须通过端口 433（HTTPS）或 80（HTTP）路由。
  5. 网页改写功能不能改写内嵌在 PDF 或 Microsoft Office 文件（包括 Word、Excel、PowerPoint 等）中的 URL。因此，推荐在这类文档中使用相对 URL。

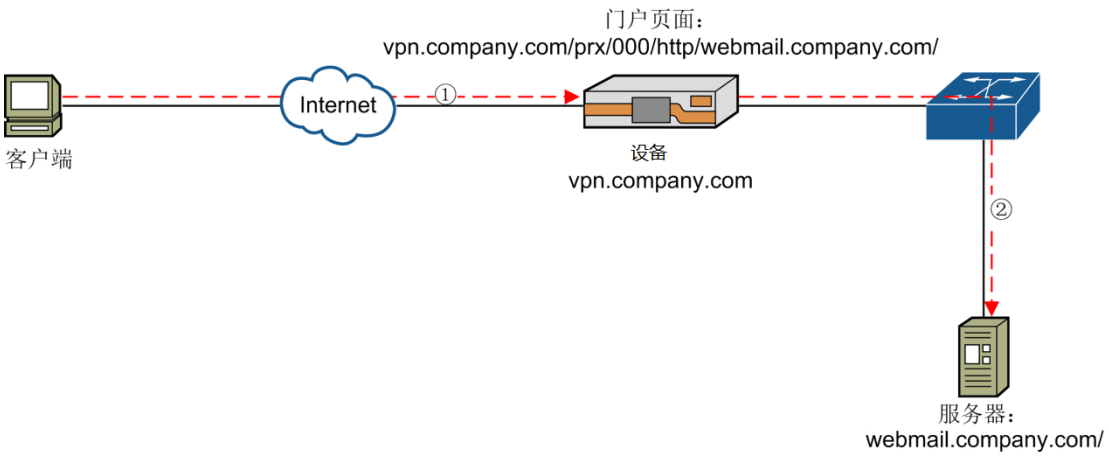

图8–2 网页改写部署

在上图场景中，用户访问虚拟门户 vpn.company.com 上的资源时，设备将自动把链接 http://webmail.company.com 改写为 https://vpn.company.com/prx/000/http/webmail.company.com。新的链接指向设备因而 Internet 中的用户请求将被发送到设备，再被转发到真实的 webmail 服务器。

网页改写使用如下格式将内部 URL 转换为外部 URL：

https://<virtual_portal>/prx/000/<scheme>/<internal_URL>

- <virtual_portal>是虚拟门户的全限定域名（Fully Qualified Domain Name，FQDN）；
- <scheme>为“http”或“https”；
- <internal_URL>为原始 URL（主机和路径）。

例如，“http://server.company.com/”将被转换为“https://sp.company.com/prx/000/http/server.company.com/”。

8.1.3.1 基本设置

8.1.3.1.1 相对 URL 改写

系统支持对服务器响应的相对 URL 进行改写，如果不启用该功能，系统将不会对相对 URL 进行改写。例如：“./1.jpg”将会被改写为“/prx/000/http(s)/xxxxx/1.jpg”。

- **配置示例**

1. 启用相对 URL 改写。

```
vs(config)$rewrite relative
```

8.1.3.1.2 URL 隐藏

出于安全考虑，URL 隐藏功能用于向客户端隐藏内网架构。URL 隐藏功能是在网页改写对 URL 进行标准改写后，再对 URL 使用预设置的算法进行改写以隐藏协议、文件名和文件类型。

要启用 URL 隐藏功能，必须启用改写相对 URL 的功能。

例如，URL“http://www.sina.com.cn”被隐藏为“https://virtualsite_domain_name/prx/00/54xr/3TAk11slMsAnwnr_/”。

- **配置示例**

1. 启用 URL 隐藏功能。

```
vs(config)$rewrite urlmask "filename" "dynamic"
```

8.1.3.2 自定义改写

系统支持自定义改写功能。配置一条自定义改写规则后，如果响应中的报文主体匹配了指定的 URL 字符串，系统将对该报文进行自定义改写。

系统还允许管理员自定义数据脱敏规则，用于对用户的敏感信息进行脱敏。

- **配置示例**

1. 启用自定义改写功能。

```
vs(config)$rewrite custom on
```

2. 配置自定义改写规则。

```
vs(config)$ rewrite custom rules 1 pre "http://1.1.1.1/test" "$$abc$$fixed$$def$$"
```

系统将在网页改写功能对“http://1.1.1.1/test”返回的响应改写前进行改写，将响应页面内容中的“abc”替换为“def”。

21. 配置默认电话号码的屏蔽规则。

```
vs(config)$rewrite custom rules 1 pre "http://1.1.1.1/test" "$$<phone>$$"
```

系统将在网页改写功能对“http://1.1.1.1/test”返回的响应改写前进行脱敏，将响应页面内容中匹配到的电话号中间四位改为“*”。如“17705637791”将被改写为“177****7791”。

22. 配置指定正则表达式的电话号码的屏蔽规则。

```
vs(config)$rewrite custom rules 1 pre "http://1.1.1.1/test"
"$$1111111111$$mask$$<phone>$$"
```

系统将在网页改写功能对“http://1.1.1.1/test”返回的响应改写前进行脱敏，将响应页面内容中的“11111111111”中间四位改为“*”，而其它正常格式的电话号码不会被匹配到。

23. 配置电话号进行“sha256”加密。

```
vs(config)$rewrite custom rules 1 pre "http://1.1.1.1/test" "$$<phone>$$sha256$$$$"
```

系统将在网页改写功能对“http://1.1.1.1/test”返回的响应改写前进行脱敏，响应页面内容中匹配到的电话号码进行“sha256”加密。

8.1.3.3 高级设置

8.1.3.3.1 分段透传

HTTP 头部 Range 字段用于请求服务器返回指定部分内容，常用于文件的断点续传以及视频文件的播放。成功响应后，后台服务器将返回带有 Content-Range 头部字段的响应，Content-Range 头部字段的内容包含数据格式、数据索引起始位置及数据大小。

设备支持对指定 URL 的 Range 字段范围的内容进行透传。

- **配置示例**

1. 启用分段透传功能。

```
vs(config)$http range “http://1.1.1.1/test”
```

8.1.3.3.2 中括号变量改写

系统将对中括号内的变量进行改写。一般情况当系统检测到中括号内为字符串，能够正常进行改写；当中括号内的参数为变量时，需要启用中括号变量改写功能，系统才会对中括号内的变量进行改写，如果配置了中括号变量自定义改写规则，则系统会优先按照中括号变量自定义改写规则的配置判断是否对指定的 URL 进行中括号变量改写，以及如何进行改写。

- **配置示例**

1. 启用中括号变量改写功能。

```
vs(config)$rewrite bracket on
```

2. 配置中括号变量自定义改写规则。

```
vs(config)$rewrite bracket rules 1 off "http://1.1.1.1/test" "i"
```

按照上面的配置，系统将对指定的 URL“http://1.1.1.1/test”禁用中括号变量改写功能，对其他的 URL 启用中括号变量改写功能。

8.1.3.3.3 响应不压缩

HTTP 请求头部的 Accept-Encoding 字段是用于告诉服务端客户端支持哪些编码方式，系统支持在请求头的 Accept-Encoding 字段插入 identity 发送给后台 Web 服务器，让后台服务器返回不压缩的页面内容。但如果后台服务器只支持压缩，则该功能无效。

- **配置示例**

1. 启用响应不压缩功能。

```
vs(config)$rewrite identity on
```

8.1.3.3.4 GZIP 压缩

系统支持后台服务器发送 GZIP 格式的应答报文。能对其进行解压，然后将内容进行改写，再将改写后的内容进行压缩并返回给客户端浏览器。服务器应答报文头部的格式如下：Content-Encoding: gzip。

8.1.3.3.5 Javascript 属性不改写

系统支持在对 Javascript 脚本进行改写的时候，对其中的某些属性不改写，并且支持在同一 URL 中配置多个不改写的属性，用“|”分隔符隔开。

- **配置示例**

1. 配置 Javascript 属性不改写规则。

```
vs(config)$rewrite maskattr rules 1 "http://1.1.1.1/test" "href|url"
```

按照上面的配置，系统将对“http://1.1.1.1/test”返回的响应中 Javascript 代码中的“href”属性和“url”属性的内容不改写。

8.1.3.3.6 浏览器 localStorage 对象改写

localStorage 是 HTML5 中引入的一个特性，该特性主要是用来作为本地存储，解决 cookie 存储空间不足的问题。系统支持对浏览器 localStorage 对象进行改写，通过配置浏览器 localStorage 对象改写规则，系统将改写与规则匹配的 URL 响应报文中的 localStorage 的内容。

- **配置示例**

2. 配置浏览器 localStorage 对象改写规则。

```
vs(config)$rewrite storage rules 1 "http://1.1.1.1/test" "i"
```

按照上面的配置，系统将对“http://1.1.1.1/test”返回响应中的 localStorage 的内容进行改写，并且不区分大小写。

8.1.4 HTTP 设置

系统支持设备与后台 Web 服务器之间的连接复用功能。通过该功能可以避免每次 HTTP 连接都进行 TCP 握手，从而节省开销。启用该功能后，系统在与后台服务器进行一组 TCP 三次握手后发送 HTTP 请求，当后台服务器响应后并不会进行四次 TCP 挥手，而是继续保持该 TCP 连接，复用该 TCP 连接进行下一次 HTTP 请求。

- **配置示例**

1. 通过全局命令启用设备与后台服务器的连接复用功能。

```
Demo(config)$http serverconnreuse on
```

2. 通过全局命令设置连接复用功能的最大请求数。

```
Demo(config)$http serverconnreuse maxreq 100
```

按照上面的配置，当复用的连接数达到 100 时，系统将会断开与后台服务器的 TCP 连接，下次发起 HTTP 请求时需要重新进行 TCP 三次握手。

3. 通过全局命令设置连接复用功能保持的最大时长。

```
Demo(config)$http serverconnreuse timeout 100
```

按照上面的配置，当复用的连接时间达到 100 秒时，系统将会断开与后台服务器的 TCP 连接。

8.2 VPN 接入

VPN（Virtual Private Network，虚拟专用网）功能提供了一种接入方法，使得用户可以随时随地访问内网和企业应用，就像这些应用位于内部局域网一样，这样不仅可以提升生产力而且也保证了安全和兼容性。

当 VPN 功能启用后，设备将作为一台 VPN 服务器提供网络接入服务。另一方面，最终用户使用 SSL VPN 客户端与 VPN 服务器建立 VPN 隧道。SSL VPN 客户端以独立的应用安装在最终用户的客户端平台上。

VPN 功能支持三种运行模式：

- 网络模式：该模式下，最终用户和设备间将建立一条三层 SSL VPN 隧道。系统将为 SSL VPN 客户端分配一个内网 IP 地址。最终用户通过该内网 IP 访问部分或整个内网，可访问的资源由网络类型的 VPN 资源配置决定。
- 应用模式：该模式下，最终用户和设备间将建立一条四层 SSL VPN 隧道。只有授权的 TCP 应用的流量会通过四层 SSL VPN 隧道。授权的 TCP 应用将被配置为应用类型的 VPN 资源。
- 双重模式：该模式下，三层和四层 SSL VPN 隧道都将建立。SSL VPN 客户端将先尝试使用四层 SSL VPN 隧道传输数据。如果失败，将使用三层 SSL VPN 隧道。

8.2.1 网络模式和应用模式

8.2.1.1 网络模式

网络模式即三层 VPN 隧道。网络接入模式的工作流程如下图所示：

网络接入模式 VPN 的工作流程如下：

1. 用户使用预装的 SSL VPN 客户端启用 VPN 功能。
2. SSL VPN 客户端与设备建立 L3VPN 隧道并被分配一个内网 IP 地址。该用户将被分配网络类型的 VPN 资源。
3. 去往内网的用户流量在穿过 L3VPN 隧道时将被加密。
4. 如果用户断开 L3VPN 隧道，SSL VPN 客户端将终止与设备的 L3VPN 隧道。

由于 IP 流量通过隧道到达网络，所以基于 IP 的应用，包括使用动态端口的 TCP 和 UDP 协议或 ICMP 协议的应用，都以透明方式工作。

8.2.1.2 应用模式

应用模式即四层 VPN 隧道。应用模式实现了一个本地代理，可以拦截由客户端应用发起的 VPN 连接，使数据通过一个安全的 SSL 连接穿过隧道，然后将数据代理到既定的后台资源。

下图所示为应用模式 VPN 的工作流程。

应用模式 VPN 的工作流程如下：

1. 用户通过预装的 SSL VPN 客户端启用 VPN 功能。
2. SSL VPN 客户端与本地代理建立 L4VPN 隧道。用户将被分配应用类型的 VPN 资源。
3. 用户打开一个特定的应用并访问后台应用服务器。

4. SSL VPN 客户端作为本地代理拦截去往后台应用服务器的流量并通过 L4VPN 隧道将流量发往设备。
5. 设备打开与后台应用服务器的连接并传输数据。
6. 如果用户从 L4VPN 隧道断开，SSL VPN 客户端将终结与设备之间的 L4VPN 隧道。

SSL VPN 客户端监听运行在客户设备上的已授权应用的 TCP 流量，加密数据包并通过高加密强度的四层 SSL VPN 隧道转发到设备。设备解密数据包并转发到适合的后台服务器。

四层 VPN 隧道目前支持 DesktopDirect 和 Webapp 应用。

8.2.1.3 隧道类型

系统支持两种类型的 VPN 隧道：TCP 隧道和 UDP 隧道。默认情况下，当用户连接 VPN 时，将建立 TCP 隧道。

UDP 隧道是高速隧道，是除了 TCP 隧道外系统支持的另一种隧道。高速隧道适用于要求实时传输并可以容忍丢包和无序接收的应用，例如 VoIP。

当启用 UDP 高速隧道后，系统将建立一条高速 UDP 隧道。通过 UDP 高速隧道的流量默认为密文。

当为最终用户同时建立了 TCP 和高速隧道时，SSL VPN 客户端将根据配置的分派规则分派 VPN 数据（VPN 和 UDP 数据）。

系统支持四种分派规则：

- 0：表示所有的 VPN 数据都将通过 TCP 隧道。
- 1：表示 TCP 数据将通过 TCP 隧道，UDP 数据将通过高速隧道。
- 2：表示 TCP 数据将通过高速隧道，UDP 数据将通过 TCP 隧道。
- 3：表示所有 VPN 数据都将通过高速隧道。

注意：请注意目前只有 Windows 平台的 SSL VPN 客户端支持高速隧道。运行在其他平台的 SSL VPN 客户端，即便启用了高速隧道，其与虚拟站点间仍然只建立 TCP 隧道。

8.2.1.4 隧道模式

L3VPN 隧道支持两种隧道模式：分裂隧道和全隧道。

➢ **分裂隧道**

在分裂隧道模式下，只有到特定目的地的流量会被加密并通过 SSL VPN 隧道发送到设备，然后再发送到安全的内网，所有其他的流量正常通过路由传输。在分裂隧道模式下，只要客户端的 IP 地址与其它网段的 IP 地址不冲突，客户端就可以访问本地的资源或网络。下图所示的为分裂隧道模式。

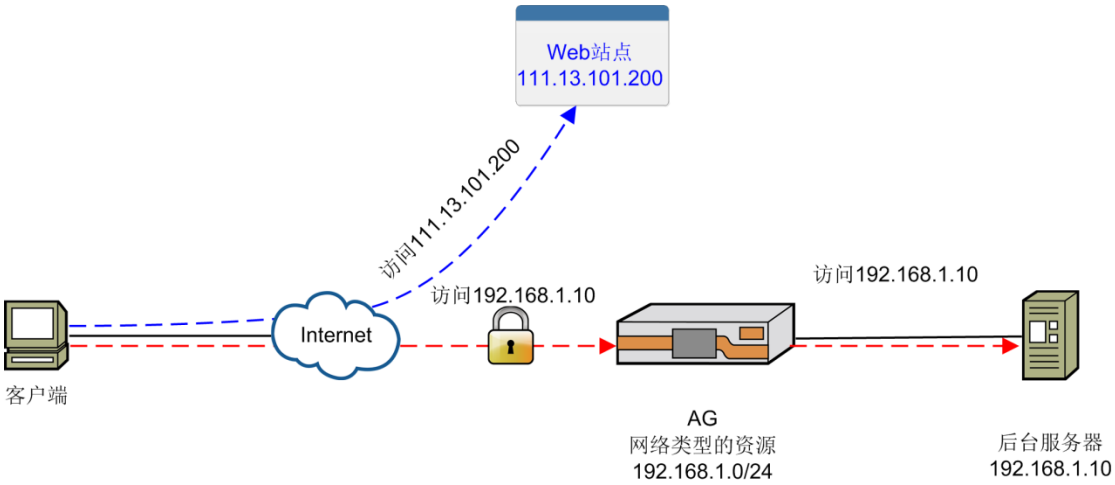

图8–3 分裂隧道

在上图中：

- 到后台服务器 192.168.1.10 的流量将通过 SSL VPN 隧道发送到设备。
- 到 Web 站点 111.13.101.200 的流量不会通过设备。

➢ **全隧道**

在全隧道模式下，所有流量（无论目的地为哪里）都将通过隧道。也就是说，即使流量不是去往安全的内部网络，也会通过隧道；然而如果企业的网络策略不允许访问某些目的地址，用户就不能通过 SSL VPN 隧道访问这些资源。请注意在全隧道模式下，客户端不能访问本地网络，只有 AG 上添加的服务器名称可以被查询到。如果客户端断开 VPN，客户端上原有的 DNS/WINS 将被存储。

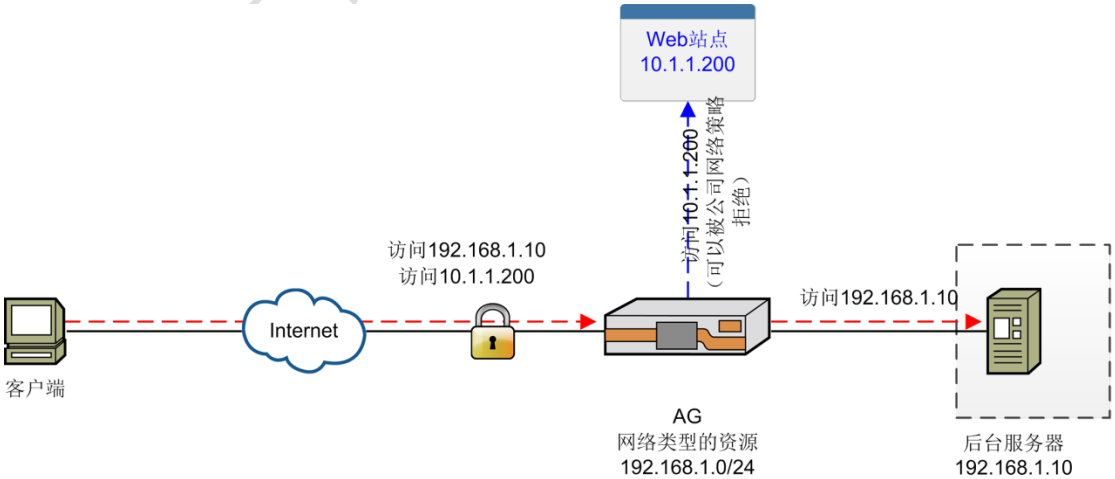

图8–4 全隧道

在上图中：

- 所有流量都将从 SSL VPN 隧道通过设备。
- 对于内部资源的请求，将被发到内网。
- 对于 Internet 资源的请求，将通过设备发到对应的 Internet 服务器。

注意：

- 要建立全隧道 VPN，可以将 VPN 资源组配置为“0.0.0.0/0.0.0.0:0-65535”使得所有流量都经过 VPN 隧道。对于 VPN 资源组的细节，请参见 8.2.4VPN 资源。
- 要建立分裂 VPN 隧道，可以将部分网络资源配置为 VPN 资源组，例如“10.10.10.0/255.255.255.0:0-65535”使得只有在这个 IP 段（10.10.10.0 和 10.10.10.255 之间）的流量会经过 VPN 隧道。

8.2.2 SSL VPN 客户端

目前与设备适配的 SSL VPN 客户端，包括 Windows、MacOS、Linux、安卓和 iOS。

SSL VPN 客户端可以以两种方式启动：

- Web 启动
- 独立启动

注意：

- 在最终用户 PC 上安装 iSecSP 客户端，需要管理员权限。安装完 iSecSP VPN 客户端后，不再需要管理员权限。
- 安装在最终用户 PC 上的防火墙软件可能会阻止 iSecSP 客户端的安装。因此在安装前，请暂时关闭防火墙软件。

8.2.2.1 Web 启动

使用 Web 启动方式时，终端用户使用 Web 浏览器登录虚拟站点并从网络层 VPN 页面启动 Web 启动的客户端建立 SSL VPN 隧道。

8.2.2.2 独立启动的客户端

独立启动的客户端即 iSecSP 客户端。终端用户在 iSecSP 客户端上指定站点地址即可登录虚拟站点，并建立 SSL VPN 隧道。

iSecSP 客户端仅一次安装即可同时支持 Web 启动和独立启动。

8.2.3 Netpool

Netpool 为 SSL VPN 客户端定义了网络连通性参数集以用来建立与设备的 VPN 隧道。

Netpool 可以与用户和组关联。

一般情况下，Netpool 包括如下设置：

- 客户端 IP 分配
- 路由
- DNS
- NAT
- VPN 流量日志

➢ **CLI 配置示例**

定义一个 Netpool，并将其关联到用户或者组。

```
vs(config)#vpn netpool name netpool1
vs(config)#vpn netpool assign touser netpool1 testuser
vs(config)# vpn netpool assign togroup netpool1 testgroup
```

8.2.3.1 客户端 IP 分配

当用户建立 3 层 SSL VPN 隧道时，系统从分配的 Netpool 为 SSL VPN 客户端分配一个内网 IP 地址。SSL VPN 隧道断开时，SSL VPN 客户端将释放该内网 IP 地址。

只有网络接入模式要求设置客户端 IP 分配。

8.2.3.1.1 接口模式或路由模式

对于 Netpool 分配的内网 IP 地址，AG 支持两种分配模式：接口模式（分配的 IP 地址是与物理接口绑定的 IP 地址）和路由模式（分配的 IP 地址是虚拟 IP 地址）。

➢ **接口模式**

如果 AG 在网络中的物理接口包含了待分配的 IP 地址，那么应该为这个接口配置该 IP 地址。

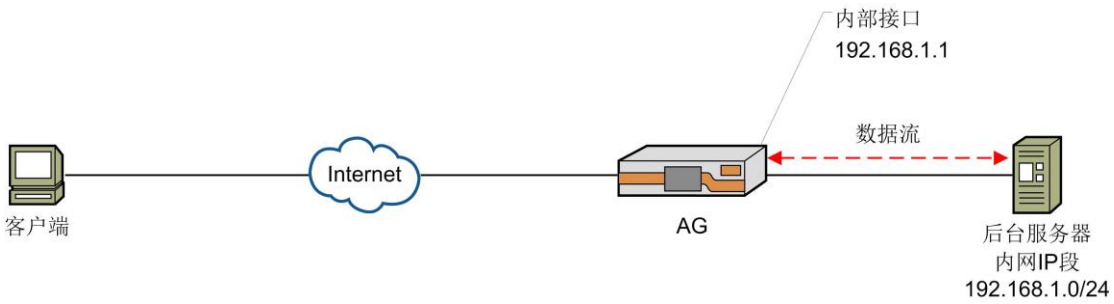

图8–5 接口模式

工作流程如下：

- 用户启用 SSL VPN 客户端并与设备建立 SSL VPN 隧道。
- 设备分配内网 IP 地址（192.168.1.1）给 SSL VPN 客户端。这样用户就可以使用该 IP 地址访问在网段 192.168.1.0/24 的资源。

➢ **路由模式**

如果分配的 IP 地址位于虚拟网络上，用户需要在网关上配置一条路由保证来自后台服务器的流量可以被发送到设备。

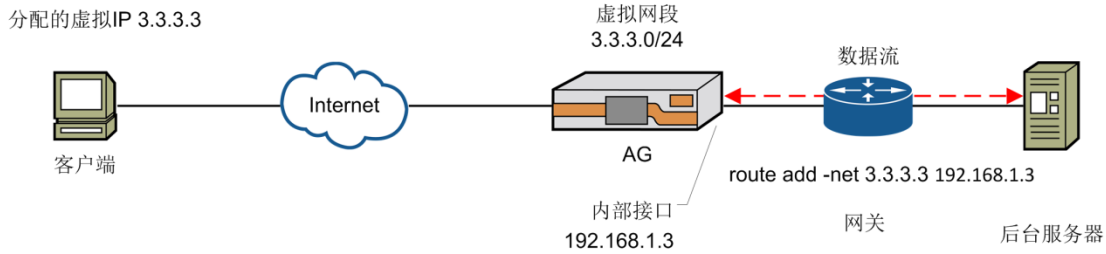

图8–6 路由模式

工作流程如下：

- 用户启用 SSL VPN 客户端并与设备建立 SSL VPN 隧道。
- 设备分配虚拟 IP（3.3.3.3）给 SSL VPN 客户端。接着在 3.3.3.3 网段的用户访问内网后台服务器。
- 当流量从内网后台服务器返回时，将被路由到设备。

注意：

- 为了避免 IP 冲突，管理员应该保证 AG 分配的 IP 地址不会分配给内网中的其他主机。

- 当配置网络模式时，管理员不应该使用保留地址 1.1.1.1 和 2.2.2.2。

8.2.3.1.2 IP 分配方法

目前，AG 支持动态分配 IP 地址。

可以为一个 Netpool 配置多个动态 IP 范围。当为用户分配一个已配置动态 IP 范围的 Netpool 时，系统将从动态 IP 范围中挑选一个 IP 地址。

Netpool 之间的动态 IP 范围不能重叠，也不能与 LocalDB 服务器中的用户的静态 IP 地址重叠。

注意：请保证所有配置的 VPN 资源对为 Netpool 配置的所有的动态 IP 范围来说都是路由可达的。

➢ **CLI 配置示例**

为指定的 Netpool 分配动态 IP 范围。

```
vs(config)#vpn netpool iprange dynamic netpool1 2.3.6.5 2.3.6.9
```

8.2.3.2 路由

管理员可以使用该功能引导指定的 Netpool 的 VPN 隧道流量。收到数据包后，AG 将根据下面规则引导流量：

- 如果为 Netpool 配置了路由网关（通过命令“**vpn netpool route gateway** *<netpool> <gateway>*”），收到的数据文将一直被发送到该路由网关。
- 如果没有为 Netpool 配置路由网关，收到的数据包将根据全局路由表发送。

请注意该功能只适用于网络模式的 VPN。

➢ **CLI 配置示例**

1. 为指定的 Netpool 配置路由网关。

```
vs(config)#vpn netpool route gateway netpool1 172.16.83.1
```

8.2.3.3 DNS

VPN 连接后，当用户访问由主机名指定的资源时，SSL VPN 客户端可以使用以下两种类型的 DNS 服务器。

- Netpool DNS 服务器：包含 Hostmap 和 DNS 域名服务器。
- 本地 DNS 服务器：表示在安装了 SSL VPN 客户端的 PC 上配置的本地 DNS 服务器。

8.2.3.3.1 常规 DNS 解析

为 Netpool 配置 DNS 服务器后，在 VPN 连接时，由 SSL VPN 客户端执行的常规 DNS 解析流程如下：

1. SSL VPN 客户端首先尝试使用 Netpool DNS 服务器执行 DNS 解析。收到 DNS 请求时，SSL VPN 客户端先将 DNS 请求与 DNS Hostmap 中的 IPv4 DNS 记录进行匹配，如果失败，将收到的 DNS 请求发送给 DNS 域名服务器进行解析。
2. 如果 Netpoo DNS 服务器解析失败，SSL VPN 客户端将接着尝试使用本地 DNS 服务器执行 DNS 解析。

管理员可以根据网络环境为 Netpool DNS 服务器或本地 DNS 服务器配置超时时间。对于往返时延（Round-Trip Time，RTT）非常大的 3G/WIFI 网络，应相应增加 DNS 超时时间。此外，用户可以自己在 SSL VPN 客户端上设置超时时间。

- **CLI 配置示例**

1. 为指定 Netpool 中的主机名添加 IPv4 DNS 记录。

```
vs(config)#vpn netpool dns hostmap netpool1 test.com.cn 172.16.88.34
```

2. 为指定的 Netpool 配置域名服务器。

```
vs(config)#vpn netpool dns nameserver netpool1 172.16.88.5
```

3. 为指定的 Netpool 设置本地 DNS 服务器的超时时间。

```
vs(config)#vpn netpool dns timeout local netpool1 2000
```

4. 为指定的 Netpool 设置 Netpool DNS 服务器的超时时间。

```
vs(config)#vpn netpool dns timeout virtual netpool1 2000
```

5. 为指定的 Netpool 设置 Windows DNS 服务器的超时时间。

```
vs(config)#vpn netpool dns timeout windows netpool1 1000
```

8.2.3.3.2 DNS 过滤

AG 为管理员提供了 DNS 过滤规则，可以为分配了指定 Netpool 的最终用户定制 DNS 解析流程。当 VPN 连接建立时，DNS 过滤规则将与 Netpool 一起被分配给最终用户。当最终用户访问由域名指代的资源时，SSL VPN 客户端将根据 DNS 过滤规则执行 DNS 解析流程。

AG 支持两种类型的 DNS 过滤规则：

- 虚拟 DNS 过滤规则：配置虚拟 DNS 过滤规则后，如果待解析的域名匹配该过滤规则，SSL VPN 客户端将只使用 Netpool DNS 服务器进行 DNS 解析。如果不匹配，SSL VPN 客户端将执行常规 DNS 解析流程（flag=0）或者根据

虚拟 DNS 过滤规则的设置只使用本地 DNS 服务器（flag=1）进行 DNS 解析。关于“flag”参数的细节，请参见命令行手册。

- 本地 DNS 过滤规则：配置本地 DNS 过滤规则后，如果待解析的域名匹配该过滤规则，SSL VPN 客户端将只使用本地 DNS 服务器进行 DNS 解析。如果不匹配，SSL VPN 客户端将执行常规 DNS 解析流程（flag=0）或者根据本地 DNS 过滤规则的设置只使用 Netpool DNS 服务器（flag=1）进行 DNS 解析。

如果没有配置虚拟或本地 DNS 过滤规则，SSL VPN 客户端将执行常规 DNS 解析流程。

当同时配置了虚拟和本地 DNS 过滤规则时：

- 如果域名匹配了虚拟 DNS 过滤规则，该虚拟 DNS 过滤规则将生效。
- 如果域名不匹配任何虚拟 DNS 过滤规则但是匹配本地 DNS 过滤规则，本地 DNS 过滤规则将生效。
- 如果域名不匹配任何虚拟或本地 DNS 过滤规则，但存在 flag=1 的虚拟 DNS 过滤规则，该虚拟 DNS 过滤规则将生效。
- 如果域名不匹配任何虚拟或本地 DNS 过滤规则，但存在 flag=0 的虚拟 DNS 过滤规则，SSL VPN 客户端将执行常规 DNS 解析流程。

➢ **CLI 配置示例**

1. 为指定的 Netpool 配置虚拟 DNS 过滤规则。

```
vs(config)#vpn netpool dns filter virtual pool "a.b.com" 0
```

2. 为指定的 Netpool 配置本地 DNS 过滤规则。

```
vs(config)#vpn netpool dns filter local pool "a.b.com" 0
```

8.2.3.4 NAT

系统允许管理员为 Netpool 启用 NAT 功能，可以为 Netpool 启用全局模式和虚拟站点模式下的 NAT 配置。默认情况下，该功能是禁用的。

➢ **CLI 配置示例**

为指定的 Netpool 启用 VPN Netpool NAT 功能。

```
vs(config)#vpn netpool nat netpool1 "useglobal"
```

8.2.3.5 保持活动间隔

系统支持为 Netpool 配置客户端保持活动间隔。在指定间隔期间，对于不活动的或没有连接的 VPN 隧道，SSL VPN 客户端将向设备发送“keepalive”数据包来保持隧道的激活状态。

➢ **CLI 配置示例**

为指定的 Netpool 配置客户端保持活动间隔。

```
vs(config)#vpn netpool keepalive netpool1 5
```

8.2.3.6 VPN 流量日志

系统允许管理员为 Netpool 启用或禁用 VPN 流量日志功能。

➢ **CLI 配置示例**

为指定的 Netpool 启用 VPN 流量日志功能。

```
vs(config)#vpn netpool trafficlog netpool1
```

8.2.4 VPN 资源

VPN 资源定义了何种类型网络可以通过 SSL VPN 隧道访问。需要为最终用户分配 VPN 资源以便 VPN 功能正常工作。

VPN 隧道是根据 VPN 资源的需求建立的。也就是说，当为最终用户分配了网络模式的 VPN 资源后，在 VPN 启动时将建立三层 SSL VPN 隧道。

目前系统只支持网络类型的 VPN 资源。VPN 资源需要加入到 VPN 资源组。VPN 资源组可以与用户或组关联。

8.2.4.1 网络模式的 VPN 资源

对于网络模式，应该使用命令“**vpn resource groupitem network**”配置网络类型的 VPN 资源。对于分裂隧道，可以根据需求配置一个或多个的网络类型的资源。

此外，管理员可以将网络类型的 VPN 资源添加到排除列表中。通过这种方式，当最终用户访问与这些网络类型的 VPN 资源匹配的资源时，流量不会通过三层 SSL VPN 隧道。

➢ **CLI 配置示例**

1. 定义一个 VPN 资源组。

```
vs(config)#vpn resource group resourcegroup1
```

2. 为指定的 VPN 资源组添加一个网络资源条目。

```
vs(config)#vpn resource groupitem network resourcegroup1 1 "172.16.0.1-172.16.3.255:0-65535" 1
```

3. 为指定的 VPN 资源组添加网络资源条目到排除列表中。

```
vs(config)#vpn resource groupexcludeditem network "resourcegroup1" 2
"172.16.0.1-172.16.3.255: 0-65535" 1
```

4. 将指定的 VPN 资源组与指定的用户账号关联。

```
vs(config)#vpn resource assign touser resourcegroup1 user1
```

5. 将指定的 VPN 资源组与指定的用户组关联。

```
vs(config)#vpn resource assign togroup resourcegroup1 group1
```

8.2.4.2 应用模式的 VPN 资源

系统支持的应用模式的 VPN 资源包括 Webapp 资源和 DesktopDirect 资源。管理员可以将应用模式的 VPN 资源添加到指定的资源组。

管理员还可以将应用模式的 VPN 资源关联到指定的用户、用户组和角色。

8.2.5 Site2Site VPN

8.2.5.1 概述

对于有多个分支机构或既有私有云又有物理网络的企业，最关心的是如何安全地桥接他们的网络。Site2Site VPN 功能可以帮助企业建立一个 Spoke-Hub-Spoke 虚拟私有网络（Site2Site VPN），该网络由 Hub 子网和 Spoke 子网组成。在各个 Spoke 和 Hub 间建立单独安全的 Site2Site VPN 隧道后，在远端站点（Spoke）和中心网络（Hub）的员工就可以安全地互访对方的网络。

在 Site2Site VPN 中，设备作为 Hub（VPN 服务器），AG-E 作为 Spoke。当 Site2Site VPN 在 Spoke 上启动后，将在 Spoke 和 Hub 间建立 Site2Site VPN 隧道，并且将为 Spoke 分配一个隧道 IP。通过 Site2Site VPN 隧道，该 Spoke 子网中的客户端可以安全地访问 Hub 子网，且 Hub 子网中的客户端也可以安全地访问 Spoke 子网。

Site2Site VPN 适用于以下场景：

- Spoke-to-Hub 访问：在 Spoke 子网的客户端可以访问 Hub 子网中的资源。
- Hub-to-Spoke 访问：在 Hub 子网中的客户端可以访问 Spoke 子网中的资源。
- Spoke-to-Spoke 访问：在 Spoke 子网的客户端可以访问另一个 Spoke 子网中的资源。Spoke-to-Spoke 访问可以是单向也可以是双向的。

注意：

- Site2Stie VPN 功能支持 TCP 和 Speed 隧道。
- Site2Stie VPN 功能支持 ACL。

- Site2Stie VPN 功能支持 TCP、UDP 和 ICMP 应用。
- 对于 Spoke-to-Spoke 访问，流量先从 Spoke 发到 Hub，然后从 Hub 发到对端 Spoke。因而，要支持 Spoke-to-Spoke 访问，应该使用命令“**vpn client isolate off**”禁用客户端流量隔离功能。
- 在 Hub 设备上同时配置 L3VPN 与 Spoke 资源时：

  1. 当使用命令“**vpn client isolate on**”为 L3VPN 和 Site2Site VPN 启用客户端流量隔离功能时，客户端连接虚拟站点的 L3VPN 用户将无法访问 Spoke 子网的资源，Spoke 子网下的设备也无法访问其他 Spoke 子网下的资源；

  2. 当使用命令“**vpn client isolate off**”为 L3VPN 和 Site2Site VPN 禁用客户端流量隔离功能时，客户端连接虚拟站点的 L3VPN 用户将能够正常访问 Spoke 子网的资源。

8.2.5.2 配置示例

本节以 Spoke-to-Hub 访问场景为例。关于如何安装 Site2Site VPN 客户端，及配置其他场景下的 Site2Site VPN 功能，请参见 Site2Site VPN 配置指南。

注意：如果 Spoke 子网和 Hub 子网有 IP 冲突，需要为 Spoke 子网或 Hub 子网配置虚拟子网。通过这种方式，虚拟子网将加入到 Site2Site VPN 中代替真正的 Spoke 子网或 Hub 子网。Spoke 子网或 Hub 子网与虚拟子网之间的映射会被 Spoke 用来将数据包中的 Spoke 子网 IP 或 Hub 子网 IP 转换为虚拟子网 IP。注意只有 IP 的网络部分会被转换，主机部分保持不变。

8.2.5.2.1 无 IP 冲突的 Spoke-to-Hub 访问

➢ **配置场景**

Spoke 子网“10.8.1.0/24”和 Hub 子网“172.16.1.0/24”没有 IP 冲突。

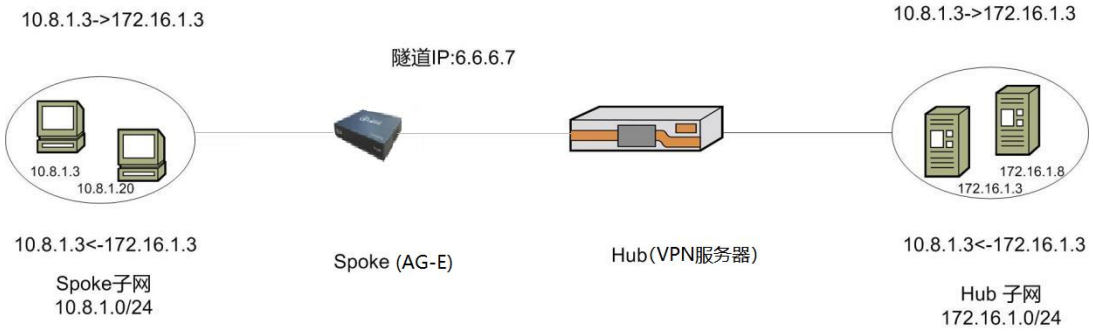

图8–7 无 IP 冲突的 Spoke-to-Hub 访问

➢ **配置目标**

Spoke 子网“10.8.1.0/24”要访问 Hub 子网“172.16.1.0/24”。当 Spoke 子网访问 Hub 子网“192.168.2.0”时，流程如下：

1. 当收到来自于 Spoke 子网的请求（目的 IP 为 172.16.1.3）时，且请求的目的 IP 匹配 Spoke 拥有的 VPN 网络资源（通过命令“vpn resource groupitem network”配置），Spoke 将请求通过 Site2Site VPN 隧道（分配的隧道 IP 为 6.6.6.7）转发给 Hub。
2. Hub 将收到的请求转发到 Hub 子网。
3. Hub 子网将响应返回给 Hub，Hub 通过命令“site2site spoke resource”的配置判断响应属于 Spoke 子网，将响应通过 Site2Site VPN 隧道转发。
4. 最后，Spoke 根据数据包中的目的 IP 将响应返回给 Spoke 子网。

➢ **配置示例**

1. 创建一个虚拟站点。

```
demo(config)#virtual site name vs "vs" "exclusive"
demo(config)#virtual site ip vs 1.1.1.1 443
```

2. 配置一个 LocalDB 账户，配置角色、角色资格。

```
vs(config)#aaa server name localdb localdb localdb
vs(config)#aaa method server localf localdb
vs(config)#no localdb passwdqc all
vs(config)#localdb account test test
vs(config)#localdb group group1 "group1" 23
vs(config)#localdb member group1 test
vs(config)#aaa on
vs(config)#role name role1
vs(config)#role qualification role1 q1
```

3. 配置 VPN 资源组与网络池。

```
vs(config)#vpn resource group g1
vs(config)#vpn resource groupitem network g1 1 "172.16.1.3"
vs(config)#vpn resource assign torole g1 role1
vs(config)#vpn netpool name pool1
vs(config)#vpn netpool iprange dynamic pool1 6.6.6.7 6.6.6.7
vs(config)#vpn netpool assign torole pool1 role1
```

4. 配置 Spoke 属性与 Spoke 资源。

```
vs(config)#site2site spoke name spoke1 test
vs(config)#site2site spoke resource spoke1 "10.8.1.0" "24"
```

5. 启用 Site2Site VPN 功能。

```
vs(config)#site2site on
```

6. 配置好 Spoke 后，在 Spoke 上连接 Hub。

图8–8 使用 Spoke（AG-E）连接 Hub

8.2.5.2.2 有 IP 冲突的 Spoke-to-Hub 访问

➢ **配置场景**

Spoke 子网的本地子网“192.168.2.0/24”和 Hub 子网“192.168.2.0/24”有 IP 冲突。

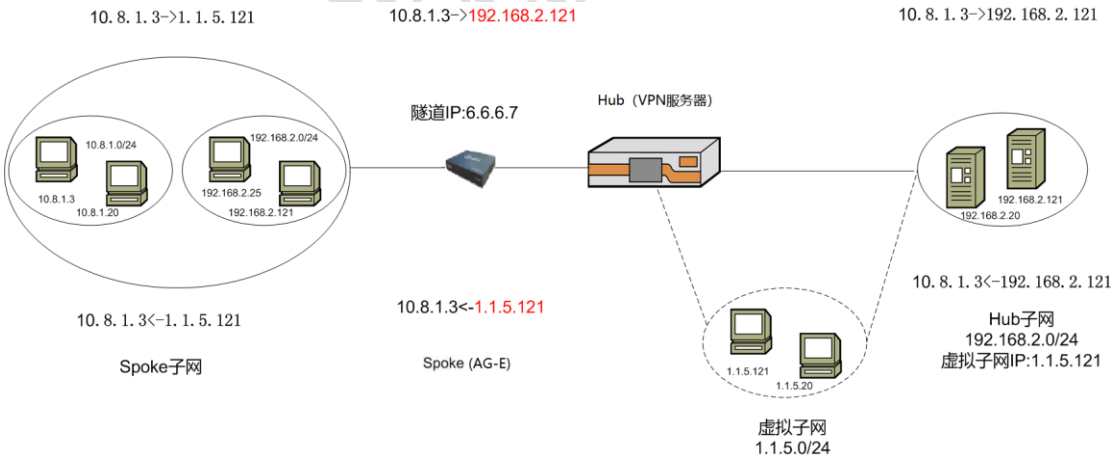

图8–9 有 IP 冲突的 Spoke-to-Hub 访问

➢ **配置目标**

Spoke 子网“10.8.1.0/24”要访问 Hub 子网“192.168.2.0”和本地子网“192.168.2.0”。当 Spoke 子网访问 Hub 子网“192.168.2.0”时，流程如下：

1. 当收到来自于 Spoke 子网的访问请求（目的 IP 为 1.1.5.121）时，且请求的目的 IP 匹配 Spoke 拥有的 VPN 网络资源（通过命令“**vpn resource groupitem network**”配置）Spoke 将客户端目的 IP（1.1.5.121）转换为 Hub 子网中的服务器 IP（192.168.2.121）。
2. Spoke 通过 Site2Site VPN 隧道转发请求（源 IP：10.8.1.3，目的 IP：192.168.2.121）给 Hub。
3. Hub 根据路由配置将收到的请求转发给 Hub 子网。
4. 当收到 Hub 的响应时，Spoke 将响应中的源 IP（192.168.2.121）转换为 Hub 子网配置的虚拟子网 IP（1.1.5.121）。
5. Spoke 根据路由配置将响应转发到 Spoke 子网。

➢ **配置示例**

该场景的配置步骤仅在步骤 3 与步骤 4 与“无 IP 冲突的 Spoke-to-Hub 访问”不同。

1. 创建一个虚拟站点。

```
demo(config)#virtual site name vs "vs" "exclusive"
demo(config)#virtual site ip vs 1.1.1.1 443
```

2. 配置一个 LocalDB 账户，配置角色、角色资格。

```
vs(config)#aaa server name localdb localdb localdb
vs(config)#aaa method server localf localdb
vs(config)#no localdb passwdqc all
vs(config)#localdb account test test
vs(config)#localdb group group1 "group1" 23
vs(config)#localdb member group1 test
vs(config)#aaa on
vs(config)#role name role1
vs(config)#role qualification role1 q1
```

3. 配置 VPN 资源组与网络池。

```
vs(config)#vpn resource group g1
vs(config)#vpn resource groupitem network g1 1 "172.16.1.3"
vs(config)#vpn resource assign torole g1 role1
vs(config)#vpn netpool name pool1
vs(config)#vpn netpool iprange dynamic pool1 6.6.6.7 6.6.6.7
vs(config)#vpn netpool assign torole pool1 role1
```

4. 配置 Spoke 属性与 Spoke 资源。

```
vs(config)#site2site spoke name spoke1 test
```

```
vs(config)#site2site spoke resource spoke1 "10.8.1.0" "24"
```

5. 配置 Hub 资源。

```
vs(config)#site2site hub resource "192.168.2.0" "24" "1.1.5.0" "24"
```

6. 将 Hub 的虚拟子网 IP 配置为 VPN 网络资源。

```
vs(config)#vpn resource groupitem network g1 1 "1.1.5.121"
```

7. 启用 Site2Site VPN 功能。

```
vs(config)#site2site on
```

8.3 TAP VPN

8.3.1 概述

TAP（Trust Access Proxy，可信安全访问代理服务器）VPN 可以在保证安全的前提下，在 5G+网络中，进一步提升单用户的 VPN 访问速度体验。与传统的 SSL VPN 相比，TAP VPN 具有如下优势：

- 任何访问主体（人/设备、应用），都必须经过身份认证和授权，才能访问资源。
- 用户可以根据需要选择最佳 VPN 接入点。
- 控制通道和数据通道的分离。SSL VPN 隧道作为控制通道，TAP 隧道作为数据通道。
- TAP VPN 可以在保证安全的前提下，在 5G+络中，进一步提升单用户的 VPN 访问速度体验。

TAP VPN 包含以下概念：

- TAP 网关：TAP 网关通过 TAP 代理与 VPN 服务器通信获得建立隧道需要的相关信息。TAP 代理用于管理已注册的 TAP 网关，并为 iSecSP 客户端提供创建 TAP 隧道需的必要信息。系统内置本地 TAP 网关。此外，系统也支持通过在 Linux 服务器安装 TAP 代理或部署镜像的方式部署远端 TAP 网关。
- VPN 服务器（AG 设备）：VPN 服务器会同时与 iSecSP 客户端和 TAP 网关通信。VPN 服务器与 iSecSP 客户端通信接收用户登录、创建和断开隧道的客户端请求，和 TAP 代理通信从而管理 TAP 网关。
- iSecSP 客户端：代理用户与 VPN 服务器建立断开隧道。支持三种隧道：SSL VPN TCP 隧道、SSL VPN UDP 隧道、TAP VPN UDP 隧道。

TAP VPN 隧道建立的详细交互流程如下：

24. iSecSP 客户端向 VPN 服务器发送请求进行登录授权。
25. iSecSP 客户端向 VPN 服务器获取包括 TAP 网关列表在内的相关信息。
26. iSecSP 客户端会向 VPN 服务器请求建立 SSL VPN 隧道的相关信息。
27. VPN 服务器返回 VPN 接入信息(包括客户端 IP、DNS 地址、授权子网等)，与 iSecSP 客户端建立 SSL VPN 隧道（控制通道）。
28. iSecSP 客户端产生一次性秘钥对，并将公钥及其他信息发送给 VPN 服务器，并通知 VPN 服务器待连的指定 TAP 网关。
29. VPN 服务器向指定的 TAP 网关发送 iSecSP 客户端的相关信息（包括用户的公钥等），并通知 iSecSP 客户端建立 TAP VPN 隧道（数据通道）。
30. iSecSP 客户端断开 TAP VPN 隧道，并向 VPN 服务器发送断开 TAP VPN 隧道的请求。
31. VPN 服务器通知指定的 TAP 网关删除相应的 iSecSP 客户端信息，从而断开相应的 TAP VPN 隧道。

8.3.2 TAP 网关

系统支持配置最多 10 个 TAP 网关，但同一个 TAP 网关只允许对应一台 VPN 服务器。如果一个虚拟站点配置了多个 TAP 网关，VPN 服务器会将多个 TAP 网关发送给 iSecSP 客户端，iSecSP 客户端可以根据需要进行选择。

8.3.3 内外网角色

系统支持通过角色判断 iSecSP 客户端所处的网络环境：内网或者外网。如果 iSecSP 客户端处于内网，则 iSecSP 客户端会获取到内网角色，并优先获得内网的 TAP 网关地址，如果未获取到内网 TAP 网关地址，则获取 TAP 网关外网地址；如果 iSecSP 客户端处于外网，则 iSecSP 客户端会获得外网角色，获取到 TAP 网关外网地址。

注意：当 iSecSP 客户端获取到内网 TAP 网关地址时，如果想要内网 iSecSP 客户端建立 TAP VPN 隧道，需要设置内网用户在认证登录时强制建立 VPN 隧道（通过命令“role intranet”中设置参数“force_tunnel”为 1）。

8.3.4 TAP 网关保活

VPN 服务器通过向 TAP 网关发送 Keep-alive 心跳包监控 TAP 网关的状态。

8.3.5 安全通信机制

TAP 网关和 VPN 服务器通过预设的挑战码的方式，结合 IP/Port 校验的机制来保证 TAP 代理和 AG 代理之间的认证，确保通信双方的实体是可信赖的；同时通过 HTTPS 的安全加密机制保证通信通道的安全。

8.3.6 配置示例

8.3.6.1 基础配置

与 L3VPN 隧道相同，需要配置 AAA 方法、角色授权以及角色拥有的 Netpool 和 VPN 资源。例如通过 TAP VPN 访问后台服务网段 3.0.0.0/24。

```
vs(config)#aaa server name localdb "ldb" "ldb"
vs(config)#aaa method server "localdb" "ldb" "ldb" "localdb" "" ""
vs(config)#aaa on
vs(config)#role name "r" "" 1 1
vs(config)#role qualification "r" "q" ""
vs(config)#vpn on
vs(config)#vpn client policy "l3vpn"
vs(config)#vpn netpool name "np"
vs(config)#vpn netpool iprange dynamic "np" 3.0.0.100 3.0.0.200
vs(config)#vpn netpool assign torole "np" "r"
vs(config)#vpn resource group "rg"
vs(config)#vpn resource groupitem network "rg" 1 "3.0.0.0/255.255.255.0:0-65535" 1 0
vs(config)#vpn resource assign torole "rg" "r"
```

8.3.6.2 本地 TAP 网关场景

完成基础配置后，对于本地 TAP 网关场景，需要进行如下配置。

图8–10 本地 TAP 网关拓扑

为本地 TAP 网关设置 UDP 服务端口。

```
global(config)#system tune tap localport 51820
```

本地 TAP 网关只需修改服务端口，所有虚拟站点共用此服务器。本地 TAP 网关暂不支持 NAT。

配置一个 TAP 网关。

```
vs(config)#tap name "localtap" ""
```

配置 TAP 网关和 VPN 服务器通信的挑战码。

```
vs(config)#tap challenge "localtap" "XXXXXXXXXUzCkXRkQGM2S6NmURrNNh2ZZ"
```

配置 TAP 网关的服务地址。

```
vs(config)#tap address service "localtap" "1.0.0.2" 51820
```

配置 TAP 网关的管理地址。本地 TAP 网关的管理 IP 必须是 127.0.0.1。

```
vs(config)#tap address management "localtap" "127.0.0.1" 54321
```

配置 TAP 网关角色。

```
vs(config)#role name "r" "" 1 1
vs(config)#role qualification "r" "q" ""
```

将 TAP 网关关联到指定的角色。

```
vs(config)#tap assign torole "localtap" "r"
```

8.3.6.3 远端 TAP 网关场景

完成基础配置后，对于远端 TAP 网关场景，需要进行如下配置。

8.3.6.3.1 TAP 代理配置

下面分别介绍不启用和启用 NAT 情况下 TAP 代理的配置。

- **未启用 NAT**

这种模式下，需要调整后台网络的路由设置。

```
#####wg server interface
wg_if = ens256
wg_dhcp = 0

####AG server address
ag_ip = 2.0.0.1
challenge = XXXXXXXXXUzCkXRkQGM2S6NmURrNNh2ZZ

####WG info, used to communicate with the MP client
wg_virtual_net =
```

```
wg_address = 1.0.0.2/32
wg_port = 8443
wg_dns = 8.8.8.8
wg_mtu = 1460

####WG Agent info, used to communicate with the AG server
wga_if = ens33
wga_address = 2.0.0.2:54321

syslog_address = 0
```

- **启用 NAT**

```
#####wg server interface
wg_if = ens256
wg_dhcp = 0

####AG server address
ag_ip = 2.0.0.1
challenge = XXXXXXXXXUzCkXRkQGM2S6NmURrNNh2ZZ

####WG info, used to communicate with the MP client
wg_virtual_net = 3.0.0.0/24
wg_address = 1.0.0.2/32
wg_port = 8443
wg_dns = 8.8.8.8
wg_mtu = 1460

####WG Agent info, used to communicate with the AG server
wga_if = ens33
wga_address = 2.0.0.2:54321

syslog_address = 0
```

8.3.6.3.2 有公网 IP 的远端 TAP 网关

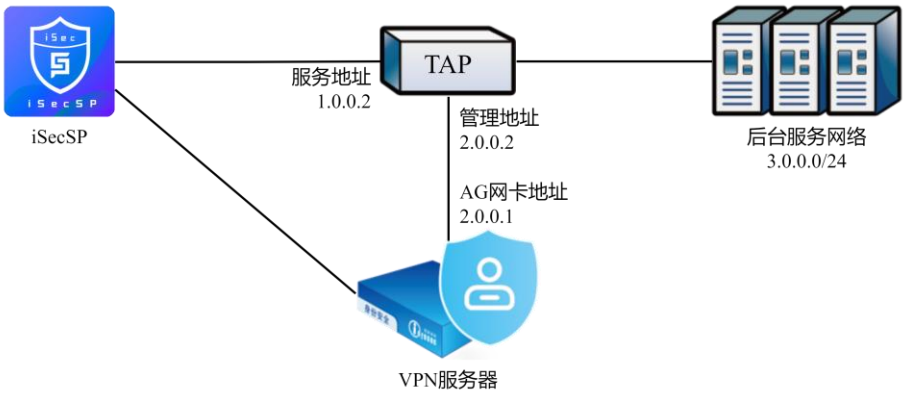

图8－11 有公网 IP 的远端 TAP 网关拓扑

配置一个 TAP 网关。

```
vs(config)#tap name "tap" ""
```

配置 TAP 网关和 VPN 服务器通信的挑战码。

```
vs(config)#tap challenge "tap" "XXXXXXXXXUzCkXRkQGM2S6NmURrNNh2ZZ"
```

配置 TAP 网关的服务地址。

```
vs(config)#tap address service "tap" "1.0.0.2" 8443
```

配置 TAP 网关的管理地址。

```
vs(config)#tap address management "tap" "2.0.0.2" 54321
```

将 TAP 网关关联到指定的角色。

```
vs(config)#tap assign torole "tap" "r"
```

8.3.6.3.3 无公网 IP 的远端 TAP 网关

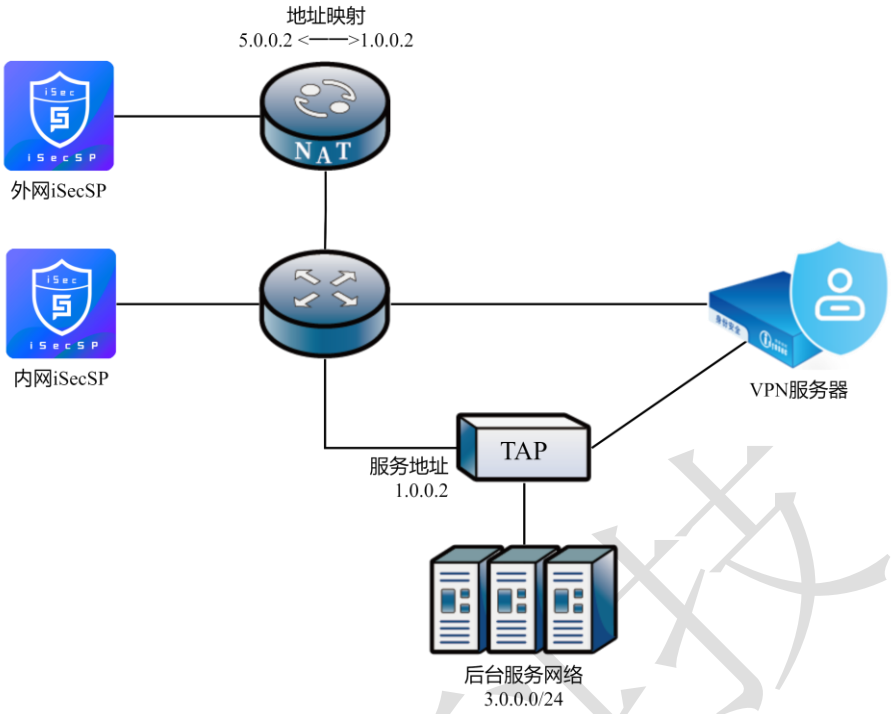

图8–12 无公网 IP 的远端 TAP 网关拓扑

TAP 网关部署在内网中，可同时支持内网 iSecSP 客户端通过内网 IP 访问 TAP 服务地址，外网 iSecSP 客户端通过 NAT 映射的外网 IP 访问 TAP 服务地址。

➢ **配置步骤**

配置一个 TAP 网关。

```
vs(config)#tap name "tap" ""
```

配置 TAP 网关和 VPN 服务器通信的挑战码。

```
vs(config)#tap challenge "tap" "XXXXXXXXXUzCkXRkQGM2S6NmURrNNh2ZZ"
```

配置 TAP 网关映射到外网的服务地址和 TAP 网关的内网服务地址。

```
vs(config)#tap address service "tap" "5.0.0.2" 8443 0
vs(config)#tap address service "tap" "1.0.0.2" 8443 1
```

配置 TAP 网关的管理地址。

```
vs(config)#tap address management "tap" "2.0.0.2" 54321
```

配置 TAP 网关角色。内网客户端获得拥有内网权限的角色“inr”，因此将通过内网地址 1.0.0.2:8443 访问 TAP 网关。外网客户端没有获得任何拥有内网权限的角色，因此将通过外网地址 5.0.0.2:8443 访问 TAP 网关。

```
vs(config)#role name "inr" "" 1 1
```

```
vs(config)#role qualification "inr" "inq" ""
vs(config)#role condition "inr" "inq" "SRCIP IS 1.0.0.0/24"
vs(config)#role intranet "inr" 1

vs(config)#role name "r" "" 1 1
vs(config)#role qualification "r" "q" ""
```

将 TAP 网关关联到指定的角色。

```
vs(config)#tap assign torole "tap" "inr"
vs(config)#tap assign torole "tap" "r"
```

8.4 IPSec VPN

8.4.1 概述

IPSec 是一种网络安全协议，用于保护 IP 通信的机密性、完整性和身份验证,它是一种广泛应用于企业网络和远程访问等场景中的成熟安全协议。通过配置 IPSec VPN 功能能够实现多台设备之间的互相访问。

IPSec VPN 具有如下优势：

- 加密数据传输：IPSec VPN 使用加密算法对数据进行加密，确保数据在传输过程中的安全性，所以即使在通过公共网络传输时，数据也不会被未经授权的人员读取或篡改。
- 认证身份：IPSec VPN 使用身份认证机制来验证用户或设备的身份，能够防止未经授权的用户访问私有网络资源，确保只有经过身份验证的用户才能建立 VPN 连接。
- 数据完整性：IPSec VPN 使用完整性检查机制来确保数据在传输过程中没有被篡改或损坏，能够防止恶意攻击者对数据进行篡改或插入恶意代码。
- 灵活性：IPSec VPN 可以在不同的网络设备上实现，包括路由器、防火墙和安全网关等，使 IPSec VPN 能够适用于各种网络环境和设备。
- 兼容性：IPSec VPN 是一种标准化的协议，被广泛支持和采用，使 IPSec VPN 能够与各种厂商和操作系统的设备进行互操作，提供了更大的灵活性和选择性。

8.4.2 部署场景

IPSec VPN 支持 Site2Site 一对一组网、Site2Site 一对多组网场景，以及 Client2Site 场景。

8.4.2.1 Site2Site 一对一

图8–13 Site2Site 一对一

在上图中，设备 1 与设备 2 之间通过 IPsec 建立 VPN 连接，从而实现 PC1 与 PC2 的互访。

8.4.2.2 Site2Site 一对多

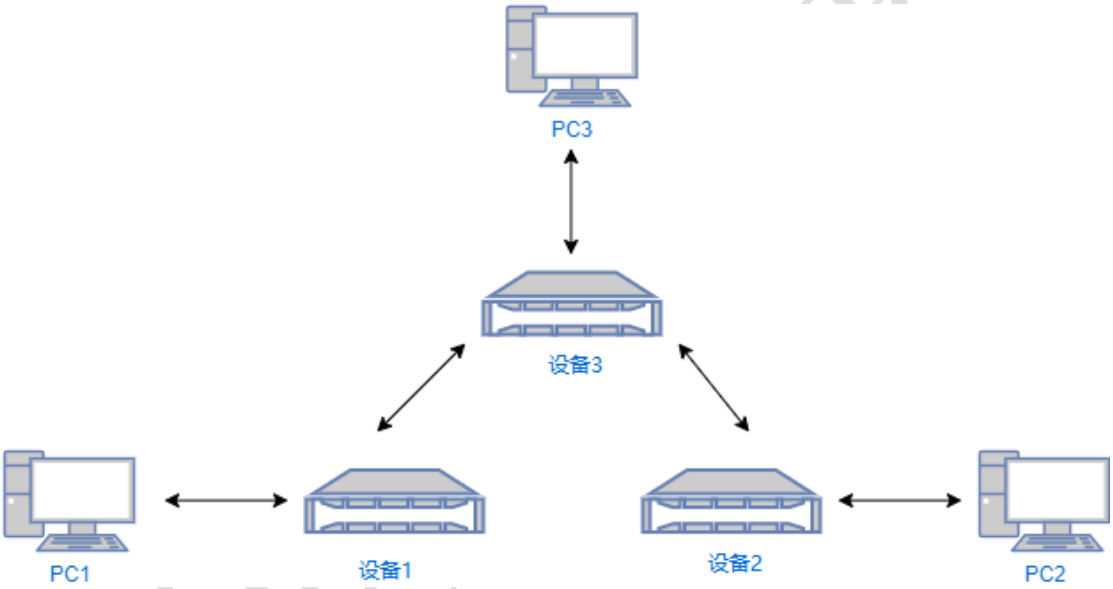

图8–14 Site2Site 一对多

在上图中，设备 1 与设备 2 分别与设备 3 通过 IPsec 建立 VPN 连接，能够实现 PC1 与 PC3、PC2 与 PC3 的互联。

注意：设备 3 暂不支持对设备 1 与设备 2 间的数据做中继。

8.4.2.3 Client2Site

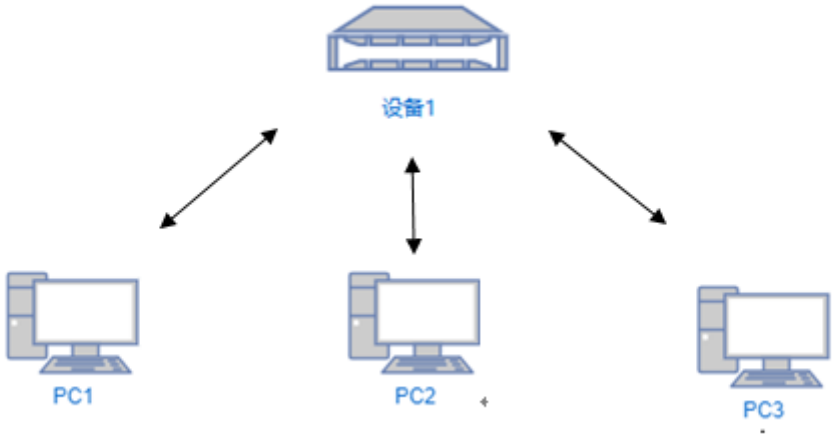

图8–15 Client2Site

在上图中，每个 PC 设备与设备 1 通过 IPsec 建立 VPN 连接，实现安全传输。

8.4.3 配置示例

8.4.3.1 Site2Site

8.4.3.1.1 配置场景

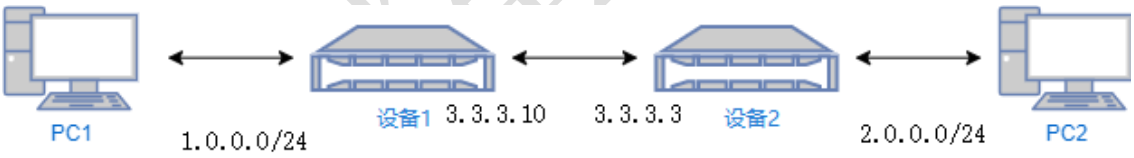

图8–16 配置场景

设备 1 与设备 2 建立 IPSec VPN 连接后，PC1 与 PC2 能够互访。

8.4.3.1.2 前置条件

- 已完成虚拟站点基础配置。
- 已完成 AAA 配置。
- 已完成用户策略配置。

8.4.3.1.3 配置步骤

➢ **设备 1**

```
vs1(config)$ipsec site2site on
```

```
vs1(config)$ipsec site2site local name "ipsec1"
vs1(config)$ipsec site2site local version "ipsec1" "2"
vs1(config)$ipsec site2site local addr "ipsec1" "3.3.3.10"
vs1(config)$ipsec site2site local auth "ipsec1" "psk"
vs1(config)$ipsec site2site local psk "ipsec1" "ipseckey"
vs1(config)$ipsec site2site local ikesa aggressive "ipsec1" 0
vs1(config)$ipsec site2site local ikesa algorithm "ipsec1" "sm4cbc129-sm3-sm2"
vs1(config)$ipsec site2site local ikesa lifetime "ipsec1" 86400
vs1(config)$ipsec site2site local ipsecsa life "ipsec1" 36000
vs1(config)$ipsec site2site local ipsecsa algorithm "ipsec1" "sm4cbc127-sm3-sm2"
vs1(config)$ipsec site2site local ipsecsa forceudp "ipsec1" "off"
vs1(config)$ipsec site2site local id "ipsec1" "3.3.3.10"
vs1(config)$ipsec site2site local subnet "ipsec1" "1.0.0.0/24"

vs1(config)$ipsec site2site remote name "ipsec2"
vs1(config)$ipsec site2site remote addr "ipsec2" "3.3.3.3"
vs1(config)$ipsec site2site remote connect "ipsec2" "active"
vs1(config)$ipsec site2site remote margintime "ipsec2" 540
vs1(config)$ipsec site2site remote id "ipsec2" "3.3.3.3"
vs1(config)$ipsec site2site remote dpd "ipsec2" "clear" 30 150
vs1(config)$ipsec site2site remote subnet "ipsec2" "2.0.0.0/24"

vs1(config)$ipsec site2site tunnel link "ipsec1" "ipsec2" "on"
```

- **设备 2**

```
vs2(config)$ipsec site2site on

vs2(config)$ipsec site2site local name "ipsec2"
vs2(config)$ipsec site2site local version "ipsec2" "2"
vs2(config)$ipsec site2site local addr "ipsec2" "3.3.3.3"
vs2(config)$ipsec site2site local auth "ipsec2" "psk"
vs2(config)$ipsec site2site local psk "ipsec2" "ipseckey"
vs2(config)$ipsec site2site local ikesa aggressive "ipsec2" 0
vs2(config)$ipsec site2site local ikesa algorithm "ipsec2" "sm4cbc129-sm3-sm2"
vs2(config)$ipsec site2site local ikesa lifetime "ipsec2" 86400
vs2(config)$ipsec site2site local ipsecsa life "ipsec2" 36000
vs2(config)$ipsec site2site local ipsecsa algorithm "ipsec2" "sm4cbc127-sm3-sm2"
vs2(config)$ipsec site2site local ipsecsa forceudp "ipsec2" "off"
vs2(config)$ipsec site2site local id "ipsec2" "3.3.3.3"
vs2(config)$ipsec site2site local subnet "ipsec2" "2.0.0.0/24"
```

```
vs2(config)$ipsec site2site remote name "ipsec1"
vs2(config)$ipsec site2site remote addr "ipsec1" "3.3.3.10"
vs2(config)$ipsec site2site remote connect "ipsec1" "active"
vs2(config)$ipsec site2site remote margintime "ipsec1" 540
vs2(config)$ipsec site2site remote id "ipsec1" "3.3.3.10"
vs2(config)$ipsec site2site remote dpd "ipsec1" "clear" 30 150
vs2(config)$ipsec site2site remote subnet "ipsec1" "1.0.0.0/24"

vs2(config)$ipsec site2site tunnel link "ipsec2" "ipsec1" "on"
```

8.4.3.2 Client2Site

8.4.3.2.1 前置条件

- 已完成虚拟站点基础配置。
- 已完成 AAA 配置。
- 已完成用户策略配置。

8.4.3.2.2 配置步骤

```
vs(config)$ ipsec client2site on
vs(config)$ ipsec client2site ikesa algorithm "sm4cbc129-sm3-sm2"
vs(config)$ ipsec client2site ipsecsa algorithm "aes128-sha256"
```

第9章 资源管理

9.1 资源简介

根据资源类型的不同，设备的资源类型可以分为 Web 和 APP 两种。Web 是网页类型的资源。App 资源可以是本地可执行文件（.exe）、脚本（.bat、.sh）或快捷方式（.lnk）等。

资源可以分配给不同的角色。一个资源可以绑定多个角色，一个角色也可以绑定多个资源。

用户登录 Web 门户后，门户页面将展示用户所属角色的资源。用户点击资源链接，就可以访问相应的资源。

9.2 客户端单点登录

客户端单点登录（Single Sign On，SSO）功能允许用户登记资源的用户名密码就可以通过本地应用程序访问内网资源而无需再次输入资源服务器的用户名和密码。

Web 资源的单点登录（SSO）支持以下两种：

- IE 代填登录：当用户在门户页面点击 Web 资源时，AG 将启动 IE，通过 HTML 的标签属性定位登录界面，并代替用户将用户名和密码填入登录框，接着自动点击提交按钮进行登录操作。只适用于 IE 浏览器。
- 图形识别登录：当用户在门户页面点击 Web 资源时，系统通过智能匹配配置的样本图片并通过配置的横纵坐标来定位相应的点击位置，以及输入的内容，从而代替用户在程序登录界面填入用户名和密码并点击登录按钮。适用于所有浏览器。
- 前端 SSO：当配置好 Web 资源以及 HTTP POST SSO 规则时，系统通过 HTTP POST SSO 规则代替用户填入用户名和密码并点击登录按钮。

APP 资源的 SSO 支持以下几种：

- exe：当用户在门户页面上点击链接，系统将根据管理员配置的参数启用并执行目标程序，并代替用户在填入用户名和密码。
- winlogin：当用户在门户页面上点击链接时，系统可以通过窗口标题捕捉登录窗口，再通过地址找到输入框和按钮，代替用户填入用户名和密码，并且自动点击登录按钮进行登录。
- windetect：当用户登录门户页面后，系统将监控这类程序。此时如果用户打开了目标程序，系统将通过和 winlogin 相同的方式，代替用户在 App 登录页面填入用户名和密码，并且点击提交按钮。

- tablogin：对于无法使用 winlogin 的程序，可以使用 tablogin 的方式。当用户在门户页面上点击链接时，系统将打开目标程序，通过窗口标题捕捉登录窗口，再通过模拟按下 tab 按键切换焦点，代替用户在 app 登录页面填入用户名和密码，并且点击提交按钮。

注意：

- 目前只支持在 Windows 系统中使用 SSO 功能。
- 使用 SSO 功能需要用户安装组件 iSecSP 客户端。
- SSO 功能不支持多因素认证。

9.3 服务端单点登录

服务端单点登录功能允许用户在登录门户之后可以直接访问后台应用而无需再次进行认证。在启用服务端 SSO 功能后，当最终用户在登录门户网站后访问后台应用时，设备会将登录凭证发送至后台应用服务器。

管理员可以为 Web 应用启用服务端 SSO 功能。

服务端 SSO 功能支持以下认证方式：

- NT LAN Manager (NTLM)&HTTP basic：当最终用户使用这两种认证方式中的任意一种访问 Web 应用时，后台 Web 服务器将会返回 HTTP 401 错误给设备，这会触发针对该 Web 应用的 SSO 操作。
- SSO Post：对于使用其它认证方式（非 NTLM 和 HTTP Basic）的 Web 应用，如果要让 SSO 功能生效，管理员需要为这些 Web 应用配置 SSO Post 规则。
- 欢迎页面 SSO：此外，系统还支持欢迎页面 SSO 功能。该功能需要定制门户主题。该功能通过定制的门户主题将提交登录凭据的动作集成在用户的访问动作中，并且将凭据通过欢迎页面返回给客户端。

9.3.1 NTLM 认证 SSO

NTLM 使用 Challenge/Response（挑战/应答）机制进行身份认证。

当收到来自后台 Web 服务器的 HTTP 401 响应报文并请求 NTLM 认证时，设备将代替用户发送 challenge 报文给后台 Web 服务器以通过身份验证。

9.3.2 HTTP 基本认证 SSO

HTTP 基本认证只通过验证登录信息（用户名和密码）来验证用户身份。

当收到来自后台 Web 服务器的 HTTP 401 响应报文并请求 HTTP 基本认证时，设备使用缓存的门户登录凭证并将头部包含 Basic 标识和加密凭证的 HTTP 请求

发送给后台 Web 服务器。因此，最终用户无需在登录后台 Web 服务器时再次输入用户名和密码。

9.3.3 SSO Post

对于使用其他认证方式（非 NTML 和 HTTP Basic）的 Web 应用，如果要让 SSO 功能生效，管理员需要为这些 Web 应用配置 SSO Post 规则。为 Web 应用配置的 SSO Post 规则决定了在何处以及如何将应用登录凭证发送到后台 Web 服务器。

以下两种情况将会命中 HTTP POST SSO 规则：

- 当 302 HTTP 重定向响应报文中的重定向 URL 匹配上已配置的 SSO Post 规则时，设备将会基于 HTTP 格式构建 Post 请求报文来执行 SSO 操作。
- 当最终用户登录的 Web 应用的 URL 匹配 SSO Post 规则时，也会触发 SSO 操作。

只有当 Web 应用使用上述提到的认证方式且会话尚未结束时，SSO 功能才能正常工作。

根据构建 HTTP 形式的 Post 请求的实体，SSO Post 可以分成：

- 后端 SSO Post

后端 SSO Post 允许设备代替用户将基于 HTTP 表单构建且包含应用登录凭证的 Post 请求发送给后台 Web 服务器。后端 SSO Post 只有在 Web 应用的 SSO 功能启用的情况下才能正常工作。

- 前端 SSO Post

当客户访问 Web 资源且管理员已从门户为这些资源启用了前端 SSO Post 时，设备会将包含 HTTP 表单和（由设备生成的）前端代码的 HTTP 响应报文返回给客户端。前端 SSO Post 允许客户端执行前端代码并自动构建和发送基于 HTTP 表单创建的 Post 请求。

只有前端 SSO Post 可以在会话重用功能时依旧正常工作。而且，前端 SSO Post 可以在会话周期内始终保持有效。

前端 SSO Post 只有在 Web 应用的 SSO 功能启用的情况下才能正常工作。

注意：

- 如果请求的 Web URL 是一个直接链接，客户端会将 Post 请求直接发送到后台服务器。
- 如果请求的 Web URL 不是直接链接，客户端会先将 Post 请求发送给设备，然后设备再将请求转发给后台 Web 服务器。

9.3.3.1 SSO Post 密码加密

出于安全考虑，在用户输入用户名和密码登录虚拟站点后，通过 SSO Post 发送请求到后台服务器时，支持对请求中的用户密码进行加密（通过命令“**sso post**”中的参数“enc_type”指定）。

9.3.3.2 SSO Post 模板

如果使用 SSO Post 模板方式发送 SSO Post 请求时，当设备匹配到 HTTP POST SSO 规则时，不再按照 HTTP POST SSO 规则中的参数“username_field”、“username_field”、“post_host”、“post_url”、“other_post_fields”和“other_header_fields”的配置构建 SSO Post 请求，而是按照模板文件中的格式（包括 HTTP 头部及包体）构建 SSO Post 请求并发送给后台服务器。

通过 SSO Post 模板方式执行 SSO 操作，需要导入 SSO POST 模板，并在 HTTP POST SSO 规则中配置通过 SSO POST 模板方式发送 SSO POST 请求。

SSO POST 模板示例如下：

```
POST /api/v1/login/ HTTP/1.1
Host: vpn.test.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 99

j_uname=<ANU>&j_pass=<ANP>&type=VPN&Param1=801&rptFlag=7&lang=EN
```

在上面的示例中，支持的动态字段（动态字段将被实际值动态替换）如下：

- <ANU>：替换为当前登录设备的用户名。
- <ANP>：替换为当前登录设备的密码，替换时根据 HTTP POST SSO 规则中规定的密码加密方式进行计算并替换。
- <ANC_XXX>：替换为客户端发给设备的请求中的 Cookie 中的 XXX 字段（key）的值。例如，SSO 请求中有一条这样的 Cookie: JSESSID=aBcd1234。则模板中的这样的字符串将会进行如下替换：“JSESSID=<ANC_JSESSID>”替换为“JSESSID=aBcd1234”。如果模板中的动态标记找不到应被替换的值，则用空字符串进行替换。例如，模板中使用了<ANC_JSESSID>，但是没有在 Cookie 中找到 JSESSID 这个名称对应的 key，则该标记用空字符串来替换。

假设登录设备的用户名是“zhangsan”，密码是“123456”，匹配到 HTTP POST SSO 规则中的密码加密方式是 md5，则用户通过该模板进行单点登录时，后台服务器将收到如下格式的 POST 报文：

```
POST /api/v1/login/ HTTP/1.1
Host: vpn.test.com
```

```
Content-Type: application/x-www-form-urlencoded
Content-Length: 94

j_uname=zhangsan&j_pass=e10adc3949ba59abbe56e057f20f883e&type=VPN&Param1=801&rptFlag=7&lang=EN
```

json 格式模板内容示例：

```
POST /api/v1/login/ HTTP/1.1
Host: 10.10.1.2
Content-Type: application/json; charset=UTF-8
Content-Length: 99

{"username":"<ANU>","password":"<ANP>","authmode":"0","redir_url":"/index.cgi"}
```

9.3.3.3 代填 SSO

在某些场景下，SSO Post 模板可能无法成功完成单点登录，管理员可以通过配置代填 SSO 的方式解决该问题。

SSO Post 方式进行的代填 SSO 通过配置自定义改写规则来实现代填操作。当设备接收到客户端发给后台服务器的 POST 请求时，代填 SSO 功能代替用户将用户名和密码填在相应的登录输入框内，并自动触发提交按钮实现登录。具体流程为：代填 SSO 功能通过 JavaScript 代码将表示用户名和密码的特定字符串赋值给相应的变量（FORM 表单中的用户名和密码字段，或者 ajax POST 数据中的用户名和密码字段），然后通过 JS 代码自动触发提交按钮的操作。

代填 SSO 功能需要管理员为要进行代填用户名和密码的 Web 资源配置 SSO Post 规则并配置自定义改写规则。

注意：

- 目前不支持带有验证码的单点登录；
- 仅支持以下几种加密算法：“MD5”、“md5”、“SHA1”、“sha1”、“SHA256”、“sha256”、“SHA384”、“sha384”或者“base64”；
- 暂不支持对用户名的加密算法。

➢ **配置示例**

1. 配置 Web 资源。

```
vs(config)$resource name "web" "quicklink_post" "quicklink_post"
vs(config)$resource name "web" "wrm_post" "wrm_post"
vs(config)$resource web url "quicklink_post" "http://1.1.1.1/bug" "" 0 1 0
vs(config)$resource web url "wrm_post" "http://abc.com.cn/bug/" "" 1 1 0
vs(config)$resource assign torole "web" "quicklink_post" "r" 1
```

```
vs(config)$resource assign torole "web" "wrm_post" "r" 1
```

2. 配置后台 Web 资源与转发策略。

```
vs(config)$server resource "quicklink_post" "http" "abc.com.cn" 80
vs(config)$server policy "/bug" "quicklink_post" "" "private" ""
```

3. 配置 HTTP POST SSO 规则。

```
vs(config)$sso post "abc.com.cn" "/bug/index.cgi" "abc" "123" "" "/bug/index.cgi"
"GoAheadAndLogin=Log+in" "" "disable" "" "" "1"
```

4. 启用 SSO 功能。

```
vs(config)$sso on
```

5. 配置自定义改写规则。

```
vs(config)$rewrite custom rules 2 pre "http://abc.com.cn/bug/" "s/body onload=../body
onload=\x22var
f1=document.getElementById(\x27mini_login_top\x27);f1.login.value=\x27<ANU>\x27;f1.pa
ssword.value=\x27<ANP>\x27;f1.submit();\x22/" ""
vs(config)$rewrite custom on
```

在上面的示例中：

- <ANU>：表示将使用登录设备的用户名来进行替换；
- <ANP>：表示将使用登录设备的密码进行替换，在 HTTP POST SSO 规则中定义密码的加密方式。

9.3.4 欢迎页面 SSO

除以上的单点登录方式外，系统还支持欢迎页面 SSO 功能。该功能需要定制门户主题。当用户访问需要经过认证授权的七层资源时，通过定制的门户主题，设备将提交登录凭据的动作集成在用户的访问动作中，并且将凭据（用户名和密码）通过欢迎页面返回给客户端，并支持对返回客户端的密码进行编码。关于如何获取定制的门户主题，请联系技术支持。

9.3.5 配置示例

1. 启用 SSO 功能。

```
v1(config)$sso on
```

2. 配置一条 HTTP POST SSO 规则。

```
v1(config)$sso post “10.3.0.70” “/bugzilla/” “Bugzilla_login” “Bugzilla_password” “”
“bugzilla/index.cgi” “GoAheadAndLogIn=Log+in” “” “disable”
```

3. 启用通过欢迎页面返回用户名和密码给客户端的功能。

```
v1(config)$sso portaltheme on
```

4. （可选）设置返回密码时的编码方式为 sha256。

```
v1(config)$sso portaltheme passencode sha256
```

第10章 零信任

零信任安全架构的核心原则是“从不信任，始终验证”，用于应对网络安全边界日趋复杂以及安全边界防护越发困难的问题。零信任主要解决传统的企业网边界安全架构存在的如下问题：

- 防护对象层面：只关注网络层面的防护，忽略以数据为中心的防护。
- 防护基础层面：只关注防护边界。在防护区域内部，防护不足。
- 防护理念层面：使用静态策略以及一次认证，缺少对访问者的持续评估。

AG 基于零信任安全架构提出的要求，实现了如下功能：

- 控制通道和数据通道分离：控制通道和数据通道的分离，使得企业内网资源对外不可见，并使网络架构更加灵活。AG 设备作为控制中心，控制安全代理隧道的建立。访问策略代理作为数据中心，接收并处理业务流量。
- 内网服务隐身：企业内网用户也需要通过设备的认证和授权，才能访问相关资源。内网服务隐身功能可以防患内部攻击，使得系统的安全性更好。
- 动态授权：根据用户环境的变化情况，系统主动地对用户进行持续的动态认证和持续的动态授权，提升了系统的安全性。
- 单包授权：外网用户只有通过敲门报文的身份校验，才能访问企业内网资源。由于所有业务端口对外不可见，本技术实现了端口的隐身。

10.1 内网服务隐身

对于传统的数据中心，访问的认证和授权过程一般只针对外部用户，而内部网络用户一般被认为是安全可信的。这种防护策略存在极大的安全隐患，如果攻击者突破边界，就可以在进行横向渗透，去攻击其他内部网络。

内网服务隐身功能要求内网客户端在访问敏感服务时，也必须先通过设备进行认证和授权。通过认证和授权后，设备会发送访问策略给访问策略代理，访问控制代理会建立允许转发规则，这时客户端才可以访问授权的资源。

10.1.1 基本概念

内网服务隐身功能由如下部分构成：

- 策略中心：存储访问策略代理基本信息，资源所在的访问策略代理，用于生成认证和授权的访问策略。
- 访问控制中心（AP Center）：存储访问策略代理的基本信息，用于与访问策略代理通信。

- 访问策略代理（AP Agent）：通过防火墙过滤访问流量，从而控制三层资源的访问。

访问策略代理有两种部署方式：

  - 一种方式是部署在待保护的资源服务器上，该服务器上需安装防火墙 iptables，且操作系统与设备相同。
  - 一种方式是部署在通往待保护的后台服务器的必经路由上，在该路由段部署本公司应用交付系统。这种方式下，应用交付系统操作系统需与设备相同，且其后可以部署多台待保护的资源服务器。

9.1.2 转发规则

转发规则被访问策略代理用来控制是否允许客户端请求访问后台服务器上的资源。转发规则分为静态转发规则和动态转发规则。动态转发规则是用户登录设备过程中依据资源配置动态生成的规则，并且只有允许规则；静态转发规则是由管理员手动配置的规则，分为允许规则和拒绝规则。

系统支持为转发规则设置优先级。同一访问策略代理的动态转发规则具有相同的优先级。对于 iptables 方式部署的访问策略代理，将按转发规则的优先级从高到低的顺序匹配客户端请求。对于部署在本公司应用交付系统上的访问策略代理，将忽略规则优先级，按照拒绝规则高于允许规则的顺序匹配客户端请求。

对于 iptables 方式部署的访问策略代理，需要在设备上预先为其配置全拒绝规则、允许 AG 设备访问访问策略代理的规则和其他需要的规则。对于部署在本公司应用交付系统上的访问策略代理，需要配置允许 AG 设备访问访问策略代理的规则和其他需要的规则。

9.1.2.1 获取方式

访问策略代理获取转发规则分为两种方式：

- 访问控制中心主动下发转发规则给访问策略代理。
- 访问策略代理主动向访问控制中心获取转发规则。访问策略代理会在两种情况下向访问控制中心主动获取转发规则：
  - 访问策略代理启动时。
  - 访问策略代理与访问控制中心通信中断且超过保活超时时间重新恢复通信后。

10.1.2 工作流程

在设备上配置完内网服务隐身功能后，其工作流程细节如下：

1. 客户端向设备发起登录请求，请求访问某资源。
1. 设备收到请求后，设备对客户端进行认证授权，系统根据授权后客户端获得的角色判断客户端属于内网还是外网，并据此为客户端分配 VPN 配置。
2. 设备的策略中心根据待访问资源的信息（三层资源信息、资源所在访问策略代理、以及客户端访问资源时的源 IP）生成相应的访问策略，并告知相应的访问控制中心。访问控制中心处理后向资源所在访问策略代理发送相关信息。
3. 访问策略代理收到访问策略后，在本地防火墙墙上建立相应的转发规则，并向设备返回响应。
4. 设备向客户端返回 L3VPN 隧道建立的结果，其中携带了相应的 VPN 配置。
5. 成功建立 L3VPN 隧道后，对于内网客户端，后续访问流量将不再经过设备，而是直接发往 AP Agent，并由 AP Agent 转发到后台服务器。对于外网客户端，流量仍按原有流程进行转发。

9.1.3 配置示例

1. 创建一个访问策略代理（AP Agent）。

```
vs(config)#ap agent name apname ""
```

2. 为 AP Agent 添加 IP 地址和端口号。

```
vs(config)#ap agent address apname "192.168.0.1" "567"
```

3. 为 AP Agent 关联一个网络资源条目。

```
vs(config)#ap agent resource vpnnetwork apname rg1 1
```

4. 为 AP Agent 设置访问控制中心（AP Center）向 AP Agent 发送保活报文的时间间隔。

```
vs(config)#ap agent timeoutinterval apname 5
```

5. 为 AP Agent 设置最大保活超时次数。

```
vs(config)#ap agent timeoutmaxtime apname 5
```

6. 为 AP Agent 导入证书。

```
vs(config)#ap agent rootca apname ftp://root:t@192.168.81.199/rel_ag_10_0_4/ca.crt
```

7. 为 AP Center 导入证书。

```
vs(config)#ap center certificate ftp://root:t@192.168.81.199/rel_ag_10_0_4/test1.crt
```

8. 为 AP Center 导入密钥。

```
vs(config)#ap center key ftp://root:t@192.168.81.199/rel_ag_10_0_4/center.key
```

9. 设置访问策略中心的日志级别。

```
vs(config)#ap center loglevel "error"
```

10. 为 AP Agent 创建一条静态转发规则。

```
vs(config)#ap agent rule static "apname" 111 "permit" "tcp"
"10.10.14.210/255.255.255.255:0-65535" "10.10.14.212/255.255.255.255:0-65535"
```

11. 为 AP Agent 的静态转发规则配置优先级。

```
vs(config)#ap agent rule priority static apname 111 1000
```

12. 为 AP Agent 的动态转发规则配置优先级。

```
vs(config)#ap agent rule priority dynamic apname 500
```

10.2 单包授权

本节主要介绍单包授权功能及其配置示例。

10.2.1 概述

单包授权（Single Packet Authorization，SPA）是零信任软件定义边界（Software Defined Perimeter，SDP）架构中一种授权方案。

启用单包授权功能后，系统将对外关闭所有业务接口。用户在建立连接前，需要发送一个 UDP 端口敲门报文进行身份校验。

单包授权功能在未进行单包授权前不允许用户接入 IP/TCP 协议栈，实现端口隐藏和服务隐身，有效地过滤非法访问，规避攻击者的探测，同时也缓解了拒绝服务攻击。

10.2.2 工作原理

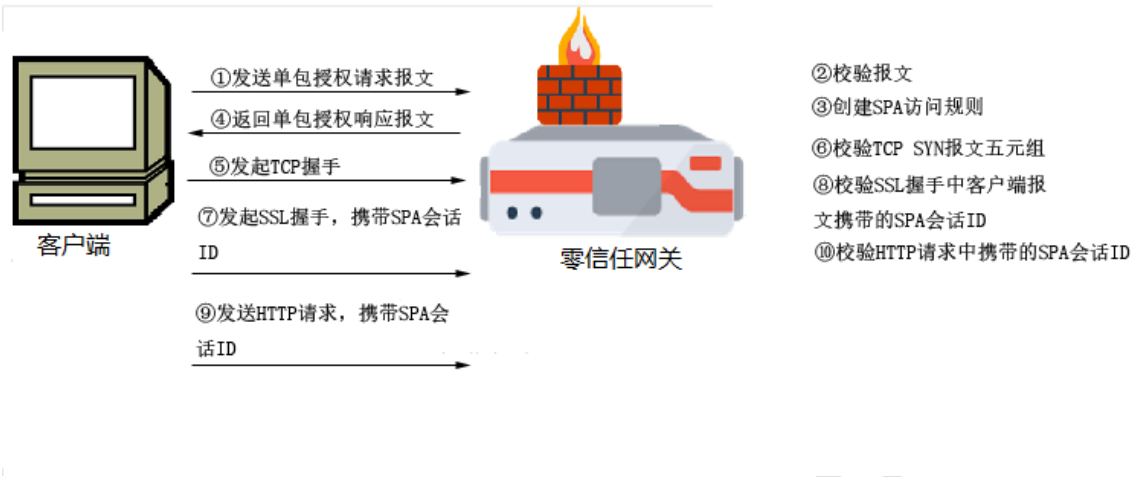

图10–1 单包授权数据流

设备上单包授权过程如下：

1. 客户端发送单包授权请求报文给 AG 设备的敲门端口，请求报文中主要包含了用户名、设备 ID、时间戳、和敲门五元组信息（源 IP、源端口、目的 IP、目的端口和协议）。
2. 如果配置了 SPA 用户，收到请求报文后，AG 将首先通过 SPA 用户认证方式（用户名和密码）对用户进行认证。如果未配置 SPA 用户或者 SPA 用户认证失败，AG 将采用指定认证方法进行 SPA 外部认证（通过 AAA）。
3. 如果敲门失败，客户端将直接连接虚拟站点。如果敲门成功，AG 设备将创建 SPA 会话，并在 SPA 会话中记录请求报文中的五元组信息（源 IP、目标 IP、源端口、服务端口和协议），即创建 SPA 访问规则。
4. AG 设备返回单包授权响应报文给客户端。客户端收到单包授权响应后，会生成 SPA 会话 ID。
5. 如果启用了 TCP、SSL 和 HTTP 校验：
   a. 对于后续的 TCP 请求，设备将客户端发送 TCP SYN 包中的五元组信息与设备上保存的 SPA 会话中的五元组信息进行对比，如果一致，则认为是合法的 TCP 连接，否则设备将会丢弃该报文，无法建立 TCP 连接。
   b. 对于后续的 HTTP 和 SSL 请求，将在发送 HTTP 和 SSL 请求时携带 SPA 会话 ID。如果携带的 SPA 会话 ID 和 SPA 会话中保存的信息一致，访问通过。

   如果未启用，访问将直接被放行。
6. TCP、HTTP 和 SSL 校验通过后，客户端访问服务端口，并建立连接。

注意：

- 单包授权功能对虚拟站点单独配置，相互独立。
- 客户端要使用 iSecSP 客户端或内嵌相应的 SDK。
- AG 的敲门端口由管理员配置，只接收 UDP 报文。
- AG 设备为用户开放的服务端口到期后，用户新建连接需要再次进行单包授权，已建立的连接可以继续使用。
- 单包授权请求报文对数据进行了加密，需要在客户端和 AG 上设置相同的共享密钥。

10.2.3 SPA 白名单

系统支持 SPA 白名单功能。管理员将客户端的 IP 地址或 IP 网段添加到 SPA 白名单后，用户登录时，系统不在 HTTP 和 SSL 层对该用户进行校验，也不校验 SPA 会话，直接允许该用户登录。

10.2.4 配置示例

10.2.4.1 配置前提

1. 管理员已完成了虚拟站点的配置。
1. 用户已为客户端配置了共享密钥。

10.2.4.2 配置步骤

1. 为虚拟站点启用单包授权功能。

```
vs(config)$spa on 60021
```

2. 为虚拟站点设置允许客户端在单包敲门成功后访问业务端口的时长（例如 60 秒）。

```
vs(config)$spa duration 60
```

3. 配置 SPA 认证方式。下面两种认证方式至少需要配置一种。

   SPA 用户认证。为虚拟站点添加 SPA 用户账号。

```
vs(config)$spa user u1 password1
```

   SPA 外部认证。为虚拟站点添加 SPA 外部认证所使用的 AAA 方法。

```
vs(config)$spa authmethod m1
```

4. 为虚拟站点配置共享密钥。

```
vs(config)$spa secret abcxxxyzclick1
```

5. （可选）启用校验 SSL 请求中的 SPA 会话 ID 的功能。

```
vs(config)$spa sessioncheck ssl on
```

6. （可选）启用校验 HTTP 请求中的 SPA 会话 ID 的功能。

```
vs(config)$spa sessioncheck http on
```

7. （可选）启用用户名校验功能。

```
vs(config)$spa sessioncheck username on
```

8. （可选）配置 SPA 白名单

```
vs(config)$spa whitelist "192.168.1.100"
```

9. 查看虚拟站点的 SPA 访问控制列表。

```
vs(config)$show spa accesslist all
```

10.3 动态授权

在实际应用场景中，用户的环境和管理员配置可能经常会发生变化。另外，用户在访问高敏资源时，也可能需要权限的临时提升，以满足安全需求。出于此原因，系统支持了动态授权功能。动态授权功能通过切换访问模式实现了不同场景下的动态授权。

10.3.1 访问模式切换

由于不同的角色具有不同的 ACL 列表、Netpool 和 VPN 资源，将不同的角色关联到访问模式后，不同的访问模式就具有不同的访问权限。访问模式切换允许用户在访问过程中主动切换访问模式来进行角色过滤，从而达到动态切换的目的，不需要重新登录就可以获得新的访问权限。

访问模式切换的流程如下：

1. 客户端向设备发送认证请求，认证请求中将携带用户凭据（用户名、密码以及其他认证因素）
2. 设备将认证请求转发给指定的认证服务器。
3. 认证服务器返回认证响应。如果认证成功，设备将筛选符合该登录用户身份的角色列表，并根据角色列表生成 ACL 列表等参数。如果管理员配置了访问模式，设备还将生成符合此登录用户的访问模式列表。
4. 设备将认证响应返回客户端。客户端基于服务器提供的响应，与设备建立 SSL 隧道。客户端认证成功后，默认选择优先级最高的访问模式为当前模式。

5. 访问过程中，如果用户需要切换访问模式，用户可以在客户端点击相应的菜单向设备发送切换命令。
6. 设备收到客户端发送的切换命令后，将执行切换动作，重建资源列表（包括 Netpool、VPN 资源以及 ACL）。如果配置发生变化，还需要根据配置决定是否重建 L3VPN 隧道。
7. 设备向客户端发送切换响应。如果切换成功，切换状态。如果切换失败，设备将提示用户。

10.3.2 再认证授权

对于已经登录的用户，如果需要切换到其他访问模式，而该访问模式需要更高级别的认证，系统支持运行时的再认证。如果当前所在访问模式所需的再认证方法与希望切换的目标访问模式的再认证方法相同，则不需要再次认证。

10.4 可信设备证书认证

系统支持可信设备证书认证。客户端在登录 AG 前，需要先向 AG 申请可信设备证书。收到可信设备证书申请请求后，AG 将请求透传至安全认证服务器，安全认证服务器验证通过，则返回可信设备证书。可信设备证书申请成功后，用户需要将该证书安装到客户端上。后续客户端访问内网资源时，需要提供该证书用于 SSL 双向认证和用户证书信息的校验。

10.4.1 证书和 HTTP 联合认证

在用户采用证书认证登录 AG 时，AG 将提取收到的请求中的客户端证书相关信息，并插入到用户身份认证请求中，透传到用于联合认证的 HTTP 服务器进行联合认证。为了使用证书和 HTTP 联合认证功能，管理员需要通过命令“**aaa server certificate authenticate server**”指定联合认证的认证服务器。

第11章 策略中心

11.1 概述

策略中心是一个用户安全管理中心。策略中心对用户环境进行实时检查，在用户环境满足特定的触发条件时，将会匹配预先配置的规则，决定对用户的处置策略，并根据策略返回相应的安全认证方法。认证成功后即可建立 VPN 隧道。在用户环境发生变化时，策略中心将基于当前环境重新向用户返回新的认证结果，实现动态认证授权。

策略中心的工作流程如下图所示：

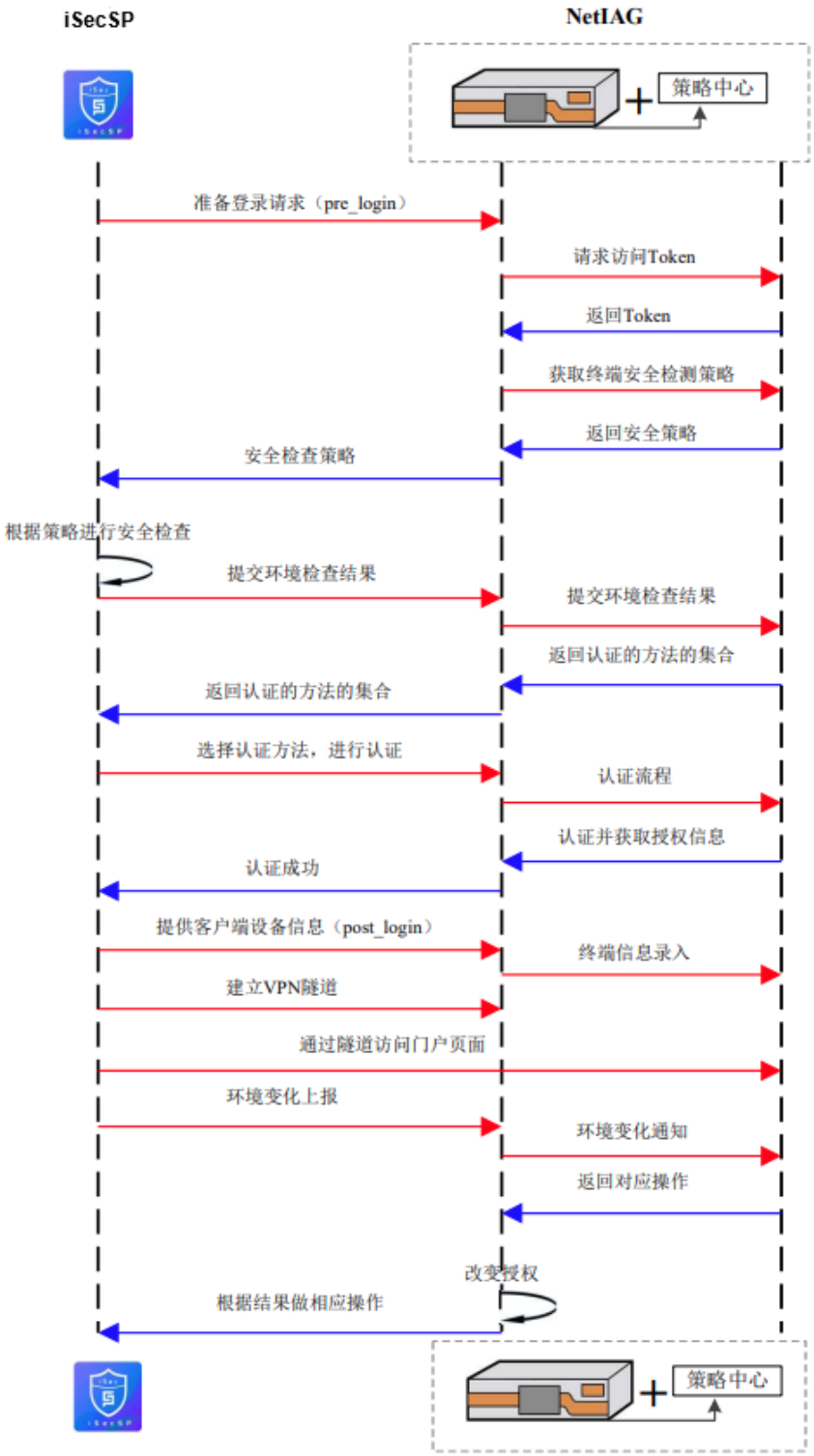

图11–1 工作流程

上述交互流程的详细说明如下：

1. 用户通过 iSecSP 客户端向 AG 发送登录请求（Pre-Login 过程如有也在这一步）。
2. iSecSP 客户端向策略中心请求访问令牌。
3. 策略中心向 iSecSP 返回访问令牌。
4. iSecSP 客户端向策略中心请求获取终端安全检测策略。
5. 策略中心返回安全策略。
6. iSecSP 客户端获取安全策略，并根据策略进行安全检查。
7. iSecSP 客户端向策略中心提交安全检查结果。
8. 策略中心根据安全检查结果，匹配规则，并返回认证方法。
9. iSecSP 客户端选择认证方法进行认证。
10. 用户认证后，策略中心会返回与用户相匹配的组，获取授权信息。
11. 提供客户端设备信息（Post-log 过程）。
12. 建立 VPN 隧道，通过隧道访问门户页面。
13. 用户环境变化，上传环境变化结果。
14. 策略中心根据环境变化结果，返回对应操作。

在上面的步骤中，1 到 8 步是 Pre-Login 过程。

11.2 基本元素

策略中心包含以下基本元素：

- 条件
- 规则
- 处置策略
- 认证方法

11.2.1 条件

条件指策略中心生效前提的条件。条件之间的关系可以为“与”、“或”或“自定义”。

条件由因素和运算符组成。因素是条件中用于判断的因子。因素分为预定义因素和自定义因素。自定义因素包括 IP 地址和认证方法两种类型。预定义因素也称安全策略因素。包括：

- 基础检查项：iSecSP 客户端会进行 IP 检测、登录账号检测、MAC 地址检测、操作系统版本检测、热点是否启用检测等项目。
- 危险端口：iSecSP 客户端会根据配置检查是否存在危险端口。支持 Windows、Linux 和 MAC 系统。
- 系统补丁：iSecSP 客户端会根据配置检查是否存在相应的系统补丁。
- 安全软件：iSecSP 客户端会根据配置检查是否开启相应的软件。
- 软件黑红名单：iSecSP 客户端会根据配置的黑名单或红名单检查软件是否启用或者安装。
- 注册表黑红名单：iSecSP 客户端会根据配置检查指定路径下的注册表是否包含对应的键值对。
- 录屏软件：iSecSP 客户端会根据配置检查是否开启录屏软件进程。

注意：不同操作系统的检测项存在一些差异。

11.2.2 规则

策略中心采用基于规则进行响应的机制。当用户的环境条件匹配指定的规则时，系统会根据预先配置的规则进行处理。

一个规则可以由单个或多个条件触发。规则具有优先级，取值越大，优先级越高。如果匹配了多条规则，系统按照优先级从大到小进行匹配。

系统通过规则组管理多条规则。一个规则可以关联多个规则组。

注意：认证仅匹配最高优先级，授权支持优先级从大到小匹配。

11.2.3 处置策略

处置策略指匹配指定规则后，系统采取的处理方式。处置策略执行时机包括三种：认证时执行，授权时执行和环境变化时执行。

处置策略包括：

- 认证等级：从一到十级，用户登录时提供高于认证等级的认证方法。
- 拒绝访问：拒绝指定用户访问。
- 动态授权：基于用户当前环境动态授权。包括两种情况
  - 角色授权时，基于用户拥有的角色对用户的角色进行增减。

- 环境变化时，基于用户当前的角色列表对用户的角色进行增减。

- 重新认证：用户环境变化后，重新登录时按照原来的认证等级再次认证。

11.2.4 认证方法

系统预置了六种认证方法：支持静态密码、动态密码、证书认证、LDAP 认证、扫码登录和设备证书认证。每个认证方法都有认证等级。认证等级包括十个级别，认证等级越高，对终端的安全要求越高。系统为用户返回的认证方法为大于等于为用户设定的级别的认证方法。

11.3 配置示例

➢ **配置环境**

在虚拟站点模式下，选择**零信任部署>策略评估中心**，在**策略评估中心**区域点击**一键部署**按钮，即可为策略中心设置所需的 AAA 配置。如下图所示：

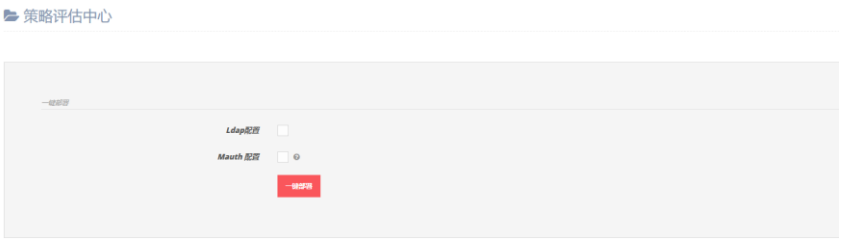

图11－2 一键部署

注意：一键部署功能仅能配置策略中心所需环境，具体设置需手动配置。

➢ **配置因素**

在虚拟站点模式下，选择**策略评估中心>因素管理>因素管理**，在**因素管理**区域点击**添加**按钮添加因素。如下图所示：

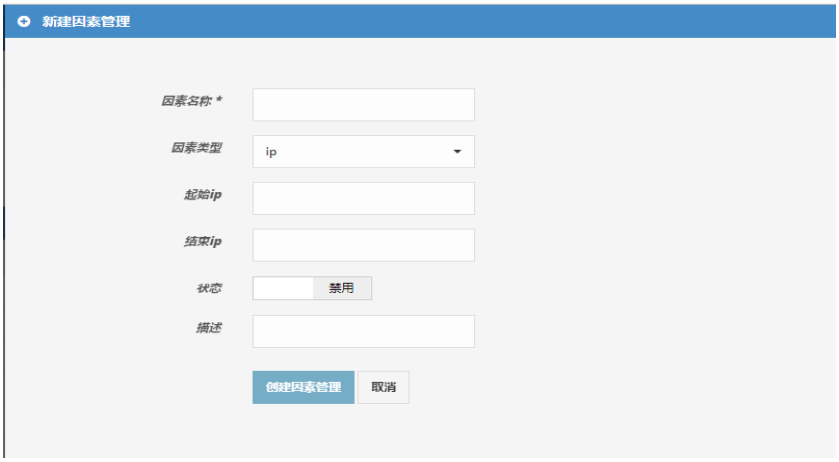

图11–3 因素管理

- **配置规则**

在虚拟站点模式下，选择**策略评估中心>规则管理>规则管理**，在**规则管理**区域点击**添加**，并设置相关参数。如下图所示：

图11–4 规则管理

- **配置规则组**

在虚拟站点模式下，选择**策略评估中心>规则组管理>规则组管理**，在**规则组管理**区域，点击**添加**，对规则组进行管理。如下图所示：

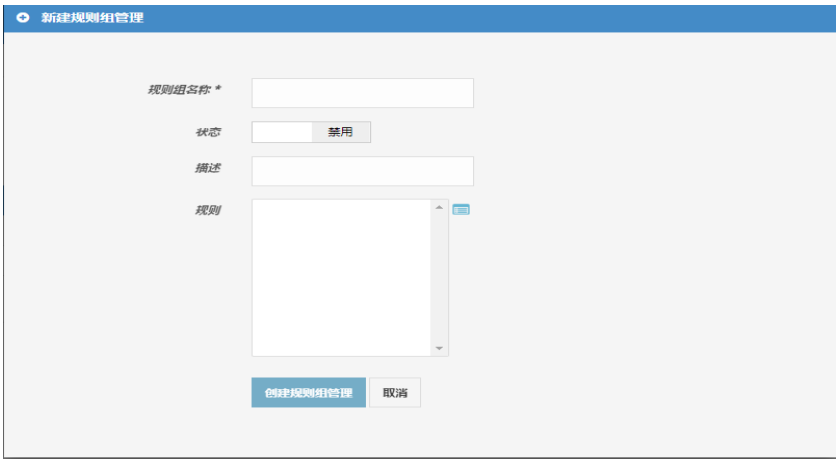

图11–5 规则组管理

- **配置终端安全策略**

在虚拟站点模式下，选择**策略评估中心>终端安全策略**。在导航栏选择相应的策略并点击，跳转后点击**添加**，即可配置相关策略。如下图所示：

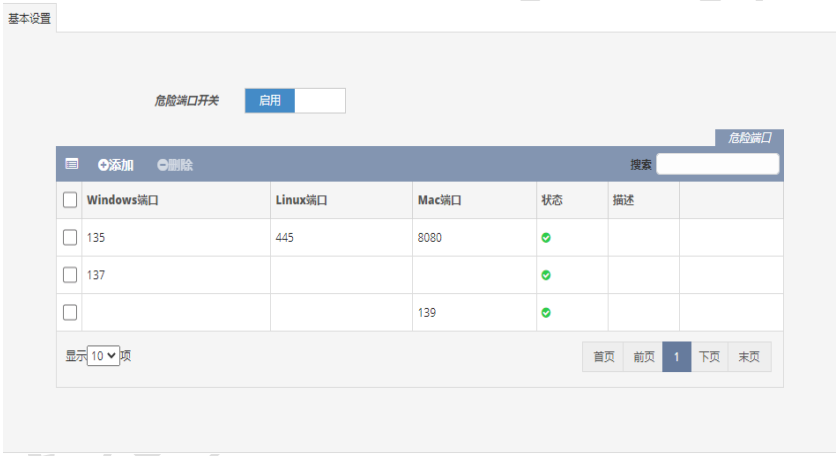

图11–6 终端安全策略

- **配置认证方法**

在虚拟站点模式下，选择**策略评估中心>认证方法>认证方法**。可以启用或禁用验证码状态，并可以选择指定的认证方法修改认证等级和状态。如下图所示：

图11–7 认证方法

第12章 终端安全策略

12.1 沙箱

沙箱技术将个人工作空间和沙箱工作空间进行隔离，为沙箱内运行的应用提供了一个独立安全的工作环境，其中的数据及文件受到安全策略（比如网络隔离、文件隔离等）的保护。同时，沙箱中的所有改动都不会影响操作系统。

沙箱目前支持两个版本 v1 和 v2（通过命令“**vpn client windows sandbox version**”或者命令“**vpn client android sandbox version**”设置）。

Windows 沙箱 v1 和 v2 支持的功能如下表所示。

表12–1 Windows 沙箱 v1 和 v2 功能对比

功能列表	沙箱 v1 版本	沙箱 v2 版本
沙箱 VPN	Y	Y
屏幕水印	Y	Y
网络隔离	Y	Y
阅后即焚	Y	Y
打印机重定向	Y	Y
剪贴板重定向	Y	Y
安全角标	Y	Y
文件隔离	Y	Y
防录屏	N	Y
防截屏	N	Y
在沙箱中启用本地应用	N	Y
窗口染色	N	Y
内置应用	N	Y

DNS 隔离	N	Y

安卓沙箱 v1 和 v2 支持的功能如下所示。

表12–2 安卓沙箱 v1 和 v2 功能对比

功能列表	沙箱 v1 版本	沙箱 v2 版本
沙箱 VPN	Y	Y
沙箱内安装应用	Y	Y
网络隔离	Y	Y
文件隔离	Y	Y
水印	N	Y
阅后即焚	N	Y
防录屏	N	Y
防截屏	N	Y
内置应用	N	Y

12.1.2 沙箱 v1

12.1.2.1 Windows 沙箱

Windows 沙箱采用 Windows 系统内置沙箱，提供了轻型桌面环境，可以安全地在隔离状态下运行应用程序。安装在 Windows 沙箱环境下的软件保持“沙箱”状态，并且与主机分开运行。

12.1.2.1.1 Windows 沙箱客户端

Windows 沙箱支持的功能如下：

- 阅后即焚

启用阅后即焚功能后，用户断开 iSecSP 客户端与虚拟站点的连接后，沙箱将自动关闭。

- 打印机重定向

启用打印机重定向功能后，沙箱能够使用 Windows 的打印机。该功能默认是禁用的。

- 剪贴板重定向

启用剪贴板重定向功能后，用户能够将沙箱内的文字、文件或文件夹复制粘贴到沙箱外，也能将沙箱外的文字、文件或文件夹复制粘贴到沙箱内。该功能默认是禁用的。

- 安全角标

启用安全角标功能后，带沙箱属性的资源将会在 iSecSP 客户端上显示为带盾牌的资源。该功能默认是禁用的。

- 水印

水印功能允许在沙箱内显示主机名、IP 地址、MAC 地址、电话号码。此外水印功能允许用户配置水印的倾斜角度、透明度、字体颜色等。该功能默认是禁用的。

- 沙箱 VPN

沙箱 VPN 功能支持在沙箱内建立 VPN 隧道，沙箱资源将只能通过沙箱 VPN 访问。

- 网络隔离

网络隔离功能基于沙箱隧道模式将沙箱内外资源隔离，使得用户只能在沙箱内访问沙箱资源，在沙箱外访问非沙箱资源。

- 屏幕水印

沙箱启用后，整个屏幕都会显示水印。

12.1.2.1.2 工作流程

Windows 沙箱工作流程如下：

1. 用户安装支持 Windows 沙箱功能的 iSecSP 客户端，之后 Windows 客户端将自动安装 Windows 沙箱。
2. 为 NetIAG 的虚拟站点启用沙箱功能。
3. 使用 iSecSP 客户端连接虚拟站点，建立沙箱 VPN。此时 Windows 客户端将自动启动 Windows 沙箱，并在沙箱中打开浏览器。如果用户未安装 Windows 沙箱 VPN 客户端 iSecSPSandBox，Windows 客户端将提示用户在沙箱内下载安装 iSecSPSandBox。
4. 成功建立沙箱 VPN 后，点击 iSecSP 客户端上的沙箱资源（显示为带盾牌的资源），该资源将会在沙箱内打开；点击其他非沙箱资源，资源将会在沙箱外打开。

关于如何获取支持 Windows 沙箱功能的 iSecSP 客户端，请联系客户支持。

12.1.2.1.3 网络隔离

Windows 沙箱提供了网络隔离功能。网络隔离功能基于沙箱内外的 VPN 隧道分离，支持多种隧道模式。具体如下：

- 沙箱外 L3VPN 和 L4VPN 隧道

该模式适用于所有资源都通过沙箱外 VPN 隧道访问的场景。

在该模式下，所有资源都在沙箱外建立 VPN 隧道，在 NetIAG 上配置不带沙箱属性的 L3VPN 资源和不带沙箱属性的 L4VPN 资源，沙箱内无需任何操作。

- 沙箱外 L3VPN 隧道，沙箱内 L4VPN 隧道

该模式适用于所有 L3VPN 资源都通过沙箱外隧道访问，所有 L4VPN 资源都通过沙箱内隧道访问的场景。

在该模式下，需要在 NetIAG 上配置不带沙箱属性的 L3VPN 资源和带沙箱属性的 L4VPN 资源，沙箱内需安装 iSecSPSandBox。

- 沙箱外 L3VPN 隧道，沙箱内 L4VPN 隧道+沙箱外 L4VPN 隧道

该模式适用于所有 L3VPN 资源都通过沙箱外隧道访问，部分 L4VPN 资源通过沙箱内隧道，部分 L4VPN 资源通过沙箱外隧道访问的场景。

在该模式下，需要在 NetIAG 上配置不带沙箱属性的 L3VPN 资源、带沙箱属性的 L4VPN 资源以及不带沙箱属性的 L4VPN 资源，沙箱内需安装 iSecSPSandBox。

- 沙箱内 L3VPN 隧道，沙箱内 L4VPN 隧道

该模式适用于所有资源都通过沙箱内 VPN 隧道访问的场景。

在该模式下，所有资源都在沙箱内建立 VPN 隧道，在 NetIAG 上配置带沙箱属性的 L3VPN 资源和带沙箱属性的 L4VPN 资源，沙箱内需安装 iSecSPSandBox。

- 沙箱内 L3VPN 隧道，沙箱外 L4VPN 隧道

该模式适用于所有 L3VPN 资源都通过沙箱内隧道访问，所有 L4VPN 资源都通过沙箱外隧道访问的场景。

在该模式下，需要在 NetIAG 上配置带沙箱属性的 L3VPN 资源和不带沙箱属性的 L4VPN 资源，沙箱内需安装 iSecSPSandBox。

- 沙箱内 L3VPN 隧道，沙箱内 L4VPN 隧道+沙箱外 L4VPN 隧道

该模式适用于所有 L3VPN 资源都通过沙箱内隧道访问，部分 L4VPN 资源通过沙箱内隧道，部分 L4VPN 资源通过沙箱外隧道访问的场景。

在该模式下，需要在 NetIAG 上配置带沙箱属性的 L3VPN 资源、带沙箱属性的 L4VPN 资源以及不带沙箱属性的 L4VPN 资源，沙箱内需安装 iSecSPSandBox。

注意：L3VPN 隧道只能全部都建立在沙箱内或者沙箱外。当配置了带沙箱属性的 L3VPN 资源，不带沙箱属性的 L3VPN 资源将会全部失效。

12.1.2.1.4 配置示例

➢ **配置要求**

配置带沙箱属性的 L3VPN 资源（192.168.83.12）和 L4VPN 资源（webapp1），使得用户只能通过沙箱访问该资源。

➢ **配置步骤**

1. 配置 AAA 服务器与 AAA 方法。

```
vs(config)$aaa server name localdb localdb
vs(config)$aaa method server localdbf localdb localdb
```

2. 添加 LocalDB 用户、密码、LocalDB 用户组、角色(角色资格)。

```
vs(config)$localdb account a "123,Abc."
vs(config)$localdb group group1
vs(config)$local member group1 a
vs(config)$role name role1
vs(config)$role qualification role1 q1
```

3. 配置 VPN 资源组、网络池。

```
vs(config)$vpn resource group g1
vs(config)$vpn resource groupitem network g1 1 "192.168.83.12" 1 1
vs(config)$vpn resource assign torole g1 role1
vs(config)$vpn netpool name POOL
vs(config)$vpn netpool iprange dynamic POOL 192.168.83.11 192.168.83.13
vs(config)$vpn netpool assign torole POOL role1
```

4. 添加沙箱属性的 VPN 资源。

```
vs(config)$vpn resource webapp webapp1 "http(l4vpn)://www.baidu.com" "" "" 1
vs(config)$vpn resource groupitem webapp g1 webapp1
```

5. 启用沙箱功能。

```
vs(config)$vpn client sandbox on
```

12.1.2.2 安卓沙箱

12.1.2.2.1 安卓沙箱客户端

安卓沙箱支持功能如下：

- 安装应用

安卓沙箱支持通过本地应用程序列表安装应用，本地应用程序列表只支持 QQ 浏览器。

- 网络隔离

网络隔离功能基于沙箱隧道模式将沙箱内外资源隔离，使得用户只能在沙箱内访问沙箱资源，在沙箱外访问非沙箱资源。

- 文件隔离

文件隔离功能将沙箱内文件全部与外部个人工作空间隔离，个人工作空间不能访问沙箱内空间。

12.1.3 沙箱 v2

12.1.3.1 Windows 沙箱

Windows 沙箱 v2 基于操作系统虚拟化技术在 Windows 系统上创建一个虚拟环境。应用可以在虚拟环境内运行，从而隔离和保护真实的用户环境。

Windows 沙箱 v2 启动后，用户在沙箱环境中运行的浏览器或其他程序的运行痕迹可以及时删除。通过 Windows 沙箱 v2，用户还可以恢复收藏夹、主页、注册表等，并及时清除沙箱环境中下载的文件。

12.1.3.1.1 Windows 沙箱客户端

Windows 沙箱 v2 支持 Windows 沙箱 v1 的所有功能。此外，Windows 沙箱 v2 还增加了以下功能。

- DNS 隔离

沙箱外的 DNS 请求根据沙箱外的 DNS 规则解析，沙箱内的 DNS 请求根据沙箱内的 DNS 规则解析。

- 网络隔离

带沙箱属性的 L3VPN 资源只能在沙箱内访问，不带沙箱属性 L3VPN 资源在沙箱内外都可以访问。

- 阅后即焚

Windows 沙箱 v2 对阅后即焚功能进行了增强。

用户首次登录配置了 Windows 沙箱 v2 的虚拟站点，访问沙箱资源时，iSecSP 客户端会在 Windows 系统中为用户建立沙箱目录（C:\Sandbox\demo\a1）。这里 demo 为 Windows 系统的登录账号名称，a1 为登录虚拟站点的账号名称。

启用阅后即焚功能后，用户断开 iSecSP 与虚拟站点的连接后，系统将立即删除已认证用户的沙箱目录。

禁用阅后即焚功能后，用户断开 iSecSP 与虚拟站点的连接后，为已认证用户建立的沙箱目录不会被删除，并且下次用户登录虚拟站点时会自动加载。

- 在沙箱中启用本地应用

Windows 沙箱 v2 支持将本地应用在沙箱中启用。支持三种启用方式：右键菜单、开始菜单和路径打开。

- 窗口染色

系统会为用户通过沙箱打开的应用在窗口边框上进行染色，以此区分普通应用与沙箱应用。对于沙箱应用，在禁用阅后即焚功能后，窗口边框的颜色为黄色；在启用阅后即焚功能后，窗口边框的颜色为红色。

- 防录屏

防录屏功能用于控制是否允许沙箱用户进行录屏。启用防录屏功能后，用户在沙箱内外都无法录屏。该功能默认是禁用的。

- 防截屏

防截屏功能用于控制是否允许沙箱用户进行截屏。启用防截屏功能后，用户在沙箱内外都无法截屏。该功能默认是禁用的。

- 内置应用

Windows 沙箱支持内置应用。在创建内置应用时用户可以通过设置命令“**vpn client windows sandbox application**”中参数“permission”来决定是否支持在沙箱内外显示并运行该应用，具体参见命令行手册。

- 屏幕水印

沙箱启用后，整个屏幕都会显示水印。

12.1.3.1.2 工作流程

Windows 沙箱工作流程如下：

1. iSecSP 客户端默认不安装沙箱，需要管理员手动设置 OEM.ini 文件中的参数 SandBoxInstall=2，再双击 iSecSPSetup.exe 按照指示安装 Windows 沙箱 v2。
2. 为虚拟站点启用沙箱功能。
3. 使用 iSecSP 客户端连接虚拟站点，建立沙箱 VPN。
4. 成功建立沙箱 VPN 后，将在 Windows 客户端整个屏幕显示沙箱水印。

5. 点击 iSecSP 客户端上的沙箱资源（显示为带盾牌的资源），该资源将会在沙箱内打开，在沙箱内打开的资源的窗口边框将被染色；点击其他非沙箱资源，资源将会在沙箱外打开。

关于如何获取支持 Windows 沙箱功能的 iSecSP 客户端，请联系客户支持。

12.1.3.2 安卓沙箱

沙箱 v2 在沙箱 v1 的基础上还支持的功能如下：

- 阅后即焚

启用阅后即焚功能后，用户断开 iSecSP 客户端与虚拟站点的连接后，沙箱将自动关闭，同时会清除沙箱内浏览过的数据。

- 水印

水印功能允许在沙箱内显示主机名、IP 地址、MAC 地址、电话号码。此外水印功能允许用户配置水印的自定义信息、透明度、字体颜色、字体大小等。该功能默认是禁用的。

- 防录屏

防录屏功能用于控制是否允许沙箱用户进行录屏。启用防录屏功能后，用户在沙箱内无法录屏，此时打开沙箱内资源，沙箱内的录屏画面为黑屏。该功能默认是禁用的。

- 防截屏

防截屏功能用于控制是否允许沙箱用户进行截屏。启用防截屏功能后，用户在沙箱内无法截屏。该功能默认是禁用的。

- 内置应用

安卓沙箱支持内置应用，在创建内置应用时用户可以通过设置命令“**vpn client android sandbox application**”中参数“permission”来决定是否支持在沙箱内外显示并运行该应用，具体参见命令行手册。

- 剪切板隔离

启用剪切板隔离后，在沙箱内复制内容，不能粘贴到沙箱外，在沙箱外复制内容，也不能粘贴到沙箱内。禁用该功能后，沙箱内文字可以粘贴到沙箱外，反之亦然。

12.2 Web 水印

Web 水印支持为 Web 资源添加水印，用于防录屏、截屏。配置 Web 水印后，当用户成功访问 Web 资源后，后续访问与该 Web 资源相关的所有页面，系统都会为其添加水印。Web 水印只适用于 Web 资源所在 Web 页面，并不会覆盖整个屏

幕。导入的 Web 水印始终置于屏幕最顶层，但不会影响相关页面中其他元素的使用。

Web 水印支持通过 WebUI 和 CLI 两种方式导入。对于 CLI 方式，管理员可以通过导入一个 Web 水印模板（参见命令“**watermark template**”）配置 Web 水印。对于 Web 方式，参见配置示例。

注意：

- 以下情况不会显示 Web 水印：
  - 在 URL 栏输入内容为图片文件的地址，页面显示为一个图片时；
  - 在 URL 栏输入内容为 JS/CSS 文件地址时，页面显示为 JS/CSS 源代码时；
  - 在 URL 栏输入 txt 等设备不会改写的文本文件地址，页面显示为文本文件内容时；
  - 设备自身未获取到会话的页面，如登录页面、注销页面和 SMS 页面等。
- 如果配置了不改写特定页面的功能，则 Web 水印功能对该页面不会生效。

12.2.1 配置示例

12.2.1.1 WebUI 配置示例

关于如何在 WebUI 上配置 Web 水印，支持手动配置和通过模板导入两种方式。

12.2.1.1.1 手动配置 Web 水印

在 WebUI 上虚拟站点模式下，选择**策略中心>终端安全策略>Web 水印设置>PC 端/移动端**手动设置 Web 水印。支持设置水印样式包括：

- 字体类型（font-family）：支持常用的字体类型，例如“Arial”、“宋体”、“黑体”等。
- 字体大小：无单位（使用默认单位），取值为 5 到 72。
- 透明度：取值为 0（完全透明）到 255（完全不透明）。
- 字体颜色：RGB 值，分别为 0 到 255 之间的数。
- 字体倾斜度：-180 到 180，正数为顺时针度数，负数为逆时针度数。
- 字符间距：无单位（使用默认单位），取值为 0 到 10。
- 行间距：无单位（使用默认单位），取值为 10 到 60。
- 支持自定义水印内容，支持静态内容与动态内容：

- 静态内容：输入的内容即显示的内容；
- 动态内容：动态获取用户的信息，包括用户名、组信息、角色信息、用户的手机号码、用户 email、用户的 IP 地址/MAC 地址、用户的主机名、User-Agent 和时间戳。不同的用户获取到的用户信息不同，显示的水印不同。

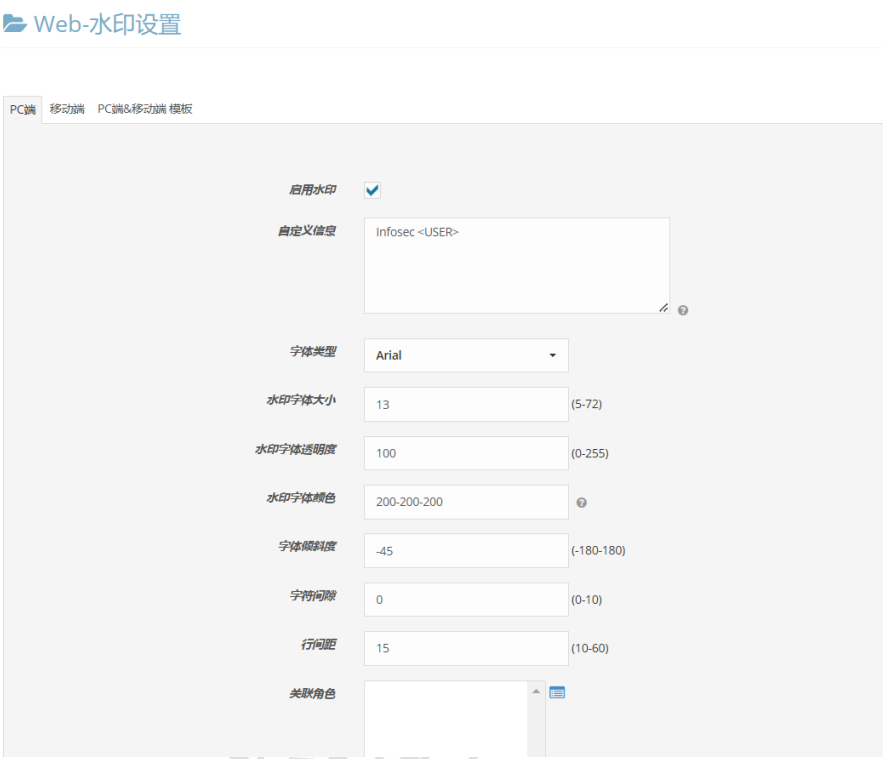

图12–1 Web 水印设置

配置完成 Web 水印的样式与内容后，关联已有的角色，勾选启用水印，即可使用 Web 水印功能。

12.2.1.1.2 导入 Web 水印模板

在 WebUI 上虚拟站点模式下，选择**策略中心>终端安全策略>Web 水印设置> PC&移动端模板**。

图12–2 导入 Web 水印模板或者重置 Web 水印模板

点击参数**导入 PC&移动端模板**右侧的**导入**按钮后，管理员可以通过本地文件或者 URL 地址的方式导入 Web 水印模板。

图12–3 通过本地文件或者 URL 导入 Web 水印模板

一个 Web 水印模板的格式如下：

```
{
    "PC": {
        "status": "on",
         "content": ["demo", "<USER> <PHONE>"],
         "role": "role1,role2",
         "style": {
                "angle": -45,
                "opacity": 0.4,
                "colorR": 200,
                "colorG": 200,
                "colorB": 200,
                "font-size": 15
          }
    },
    "Mobile": {
         "status": "off",
         "content": ["<USER>demo <PHONE>"],
         "style": {
                "angle": 45,
                "opacity": 0.8,
                "colorR": 240,
                "colorG": 200,
                "colorB": 200,
                "font-size": 12
```

```
            }
        }
}
```

水印模板中对象与属性的含义如下：

- PC：表示用于 Windows/MacOS 的水印配置。
- status：表示水印的开关，取值只能是 on 或 off，不能为空。
- content：表示要显示的水印内容。支持动态标记，支持多行文本，多行文本每一行都需要置于双引号内，并且用逗号隔开，例如："content": ["demo", "<USER> <PHONE>"]。最大长度是 100 字节，每一行最大长度不超过 64 字节，不能为空。另外该字段支持动态内容。关于如何配置动态内容，详见 ØWeb 水印动态内容。
- role：表示水印模板关联的角色，支持同时关联多个角色；
- style：表示水印的样式，子属性包括 angle、opacity、colorR、colorG、colorB、font-family、font-size、letter-spacing 以及 line-spacing。该参数取值可以为空，且该属性的某些子属性也可以为空，取值为空时将使用默认配置的样式添加水印；
- angle：表示倾斜角度，正数表示顺时针，负数表示逆时针，取值为数字-180 到 180；
- opacity：表示水印的透明度，取值为数字 0 到 255，0 表示完全透明，255 表示完全不透明，默认值为 100；
- colorR：表示水印文本的 RGB 中 R 的颜色值，取值为数字 0 到 255；
- colorG：表示水印文本的 RGB 中 G 的颜色值，取值为数字 0 到 255；
- colorB：表示水印文本的 RGB 中 B 的颜色值，取值为数字 0 到 255；
- font-family：表示字体的家族，取值为字符串；
- font-size：表示字体大小，取值为数字 5 到 72；
- letter-spacing：表示字符间距，取值为数字 0 到 10；
- line-spacing：表示多行文本时的行间距，取值为数字 10 到 60。
- Mobile：表示用于移动端的水印。

注意：上面示例中属性 PC 或 Mobile、status 和 content 为必选属性，其中 PC 和 Mobile 属性至少需要有一个。其他属性为可选属性。不设置的属性系统将会设置默认值。

➢ Web 水印动态内容

Web 水印的动态内容支持通过模板导入，也支持通过 WebUI 手动配置。系统支持的动态属性如下：

- <PHONE>：表示用户的手机号码；当用户有多个号码时，最终取值为第一个手机号码；手机号码支持屏蔽指定位置及数量的数字，被屏蔽的数据用“*”代替；支持只显示后 4 位数字，例如：<PHONE(4,4,1)>，表示手机号码从第 4 位开始屏蔽，共屏蔽 4 位，最后的 1 表示显示被屏蔽的数字位置，用“*”代替，12345678900 将显示为 123****8900；<PHONE(1,7,0)>表示从第 1 位开始屏蔽 7 位，并且这 7 个数字都不显示（即只显示手机号码后 4 位），12345678900 将显示为 8900。
- <USER>：表示用户登录设备使用的用户名。
- <GROUP>：表示用户关联的用户组，通过命令“localdb member”将用户与用户组关联；当用户关联多个用户组时，将显示所有用户组，用分隔符隔开。
- <USERDESC>：表示用户的描述字段的内容。
- <EMAIL>：表示用户的邮箱。
- <ROLE>：表示用户关联的角色，如果用户登录条件满足角色资格中包含的所有角色条件，则获得该角色资格，用户将与该角色关联；当用户关联多个角色时，将显示所有角色，用分隔符隔开。
- <TIME>：表示用户登录的日期，显示的格式为 2023/9/18 10:47:59。
- <UA>：表示 User Agent 信息中的操作系统信息及浏览器信息，从 User Agent 字段值中获取，例如：Windows NT 10.0。
- <IP>：表示用户分配到的 IP 地址（启用 L3VPN）或者用户与 AG 建立连接的 IP 地址（未启用 L3VPN）。
- <MAC>：表示用户登录虚拟站点使用的 MAC 地址。
- <HOSTNAME>：表示用户登录虚拟站点使用的主机名称。

注意：用户需要创建 SSL VPN 隧道，系统才可以动态获取属性<IP>、<MAC>和<HOSTNAME>。

12.2.1.2 CLI 配置示例

假设 Web 水印模板的名称为 1.json，在虚拟站点下执行下面命令将为虚拟站点导入一个 Web 水印模板。

```
v2(config)$watermark template "http://1.1.1.1/1.json"
```

第13章 Web 门户

13.1 虚拟门户

一个虚拟站点的虚拟门户允许用户通过统一的入口远程获取日常工作所需的各种资源。用户在获取访问权限之前，设备通过检查用户凭证（如用户名和密码）验证其身份。然后，根据分配给用户的权限/角色，设备授权用户访问文件、应用程序和其它子网上的目标。正因如此，所有的资源访问均经过设备仔细严格的控制和审查。虚拟门户的外观也可以由管理员自定义。

13.1.1 了解虚拟门户

虚拟门户为访问内部网络内容的远程用户提供了一个统一界面。每个虚拟门户均与一个 FQDN（全限定域名）相关联，并可以监听多个 IP 地址或端口（默认为 443）。本质上来说，设备允许管理员通过向公共网络仅披露 若干 IP 和域名来隐藏内部网络结构。同时，这种方法允许管理员有效地控制和记录用户在浏览门户时的活动。虚拟门户被设计成可独立配置，以便每个虚拟门户都拥有自定义界面（登录页面和欢迎页面）、SSL 设置、AAA 设置和访问方法等。

虚拟门户具备可配置多个用户角色的独特功能，因此在向不同类型用户显示内部资源方面体现出更高的灵活性。例如，一家公司可以配置员工角色，允许访问网站、文件和自有应用资源；也可能配置合作伙伴角色，只允许访问网络资源。

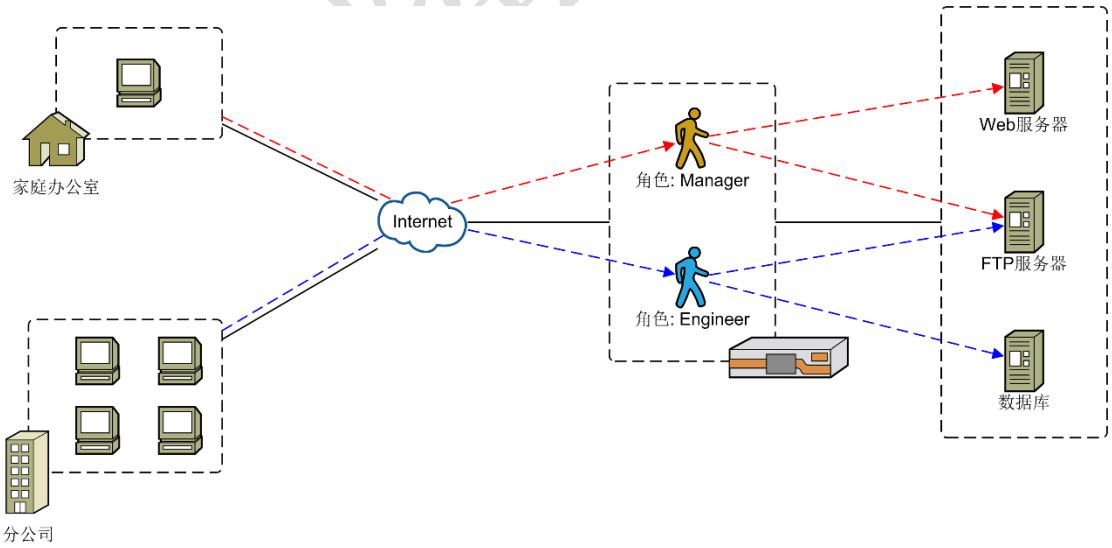

图13–1 虚拟门户

13.1.2 定义虚拟门户外观

管理员可以将虚拟门户外观配置成与公司现有的品牌方案相匹配的风格。具备统一外观的网站，可以被最终用户立即识别，实现了完美的无缝集成。

13.1.2.1 默认门户

在设备上，默认的门户主题可以应用到独占站点和别名站点。默认的门户主题定义了以下门户页面的整体外观：

- RADIUS Challenge 响应页面
- 登录页面
- 注销页面
- SMS 认证页面
- 欢迎页面
- 修改用户 LocalDB 密码的页面

13.2 门户主题

门户主题功能允许管理员自定义所有显示给最终用户的门户页面外观（例如登录页面、注销页面、RADIUS Challenge 页面等）。通过门户主题功能，管理员可以：

- 将默认的门户页面导入 AG，而无需在设计上花费太多时间。
- 根据需要定制符合需求的门户页面，并导入到 AG。

门户主题包包括多个对象，对象中的每一个文件称为资源。对象中的资源包括 HTML 页面、CSS 文件、JavaScript 文件和图片等。一个对象包括多个资源。

如需创建一个自定义门户主题包（ZIP 文件），所有的自定义门户页面应分别储存在以下文件夹中：

表13–1 门户主题包中的文件夹

文件夹	描述
challenge	RADIUS 认证使用的挑战页面。
login	登陆页面。
logout	登出页面。
welcome	欢迎页面。
custom	与任何默认页面类型无关的对象，其它对象可以访问其中的资源。可以通过该对象定制页面，或是存放公用资源以供其它对象访问。
sms	短信认证页面。

管理员可以通过访问“/prx/000/http/localh/<文件名称>”获取 JavaScript 文件。下表列出了每个 JavaScript 文件的更多相关信息：

文件名称：an_login.js

此文件用来定义登录页面上的显示信息。

表13–2 门户主题 JavaScript 文件

变量		含义	
_AN_str_title_login		登录页面标题。	
_AN_str_help		帮助字符串。如果用户使用英语作为门户网站语言，该值将是“Help”。	
_AN_str_username		用户名字段的标签。	
_AN_str_password		密码字段的标签。	
_AN_str_login		登录操作链接的标签。	
_AN_str_errormsg_login		登录失败的错误消息。	
_AN_str_h5_vpn_pls		未安装 iSecSP 客户端。	
_AN_str_h5_vpn_install		VPN 安装提示。	
_AN_str_h5_vpn_download		VPN 下载提示。	
_AN_vsite_name		虚拟站点的名称	
_AN_str_info_login		选择登录方式	
_AN_str_info_method		登录方式	
_AN_msg_id		错误码信息	
_AN_dyncode_interval		动态码刷新时间间隔	
_AN_hardwareid_on		是否启用 Hardware ID 授权功能。	
_AN_dyncode_interval		动态码刷新频率。	
AN_aaa_method]	name	认证方法名。	
	method_disp	方法的显示名称。	
	authserver	认证服务器的名称。	
	authtype	身份验证类型：LocalDB/LDAP/RADIUS/CERT。	
	server_disp	显示的认证服务器名称。	
	url	samlsp 认证跳转地址。	
	cert_id_type	使用证书认证时，如何显示用户名文本框。取值可以为“showid”和“getid”。	
	cert_id_value	当 cert_id_type 设置为 showid 时，该参数表示用户名。否则，参数取值为 0。	
	authaction	身份验证操作类型（证书匿名、证书 Challenge 等）	
	multiauth	启用或禁用多因素认证。	
	multistep	除基本的验证步骤外，另外所需的验证步骤数。	
	[multisteps]	含义：多重验证步骤的结构。	
		取值	含义
		authserver	认证服务器的名称。
		authtype	身份验证类型：LocalDB/LDAP/RADIUS/CERT。

		action	是否需要密码。
		server_disp	认证服务器说明。

文件名：an_welcome.js

此文件包含可以用于定义可分配给用户的资源的对象。这些资源包括网络链接、文件分享链接、VPN 资源和 DesktopDirect 资源等。

表13–3 门户主题 JavaScript 文件

变量	含义
_AN_str_weblinks	门户链接显示区域的标题，如网络链接等。
_AN_enable_vpn	是否启用 SSL VPN • 0：禁用 • 1：启用
_AN_str_networkresource	SSL/Mobile VPN 显示区域的标题。
_AN_str_startvpn	启用 SSL/Mobile VPN 的操作链接标签。
_AN_needlogoutlink	是否显示注销链接： • true：显示 • false：不显示
_AN_user	用户名。
_AN_str_logout	显示在注销链接上的字符串。
_AN_str_pagetitle	显示在欢迎页面上的标题。
_AN_str_msg_welcome	用于欢迎用户的消息语。
_AN_str_title_welcome	欢迎页面的标签页标题。
_AN_logout_url	登出 URL。
_AN_str_h5_vpn_disconn	断开 VPN 提示。
_AN_str_h5_vpn_pls	安装 VPN 客户端说明。
_AN_str_h5_vpn_install	安装说明。
_AN_str_h5_vpn_download	下载说明。
_AN_str_h5_vpn_reload	刷新。
_AN_str_h5_vpn_detecting	检测中。
_AN_str_h5_vpn_disconnect	断开。
_AN_str_h5_vpn1	关闭失败。
_AN_str_h5_vpn2	正在连接…
_AN_str_h5_vpn3	已经连接。
_AN_str_h5_vpn4	正在断开连接…
_AN_str_h5_vpn5	正在重连…
_AN_str_h5_vpn6	连接失败。
_AN_str_h5_vpn7	已断开连接。
_AN_str_h5_vpn_if	如果无法启动 VPN，请安装 iSecSP。

文件名：文件名：an_logout.js

此文件用于定义登出页面显示信息

表13–4 门户主题 JavaScript 文件

变量	含义
_AN_str_title_logout	注销页面的标题。
_AN_str_bye	表示 Goodbye 消息的字符串。
_AN_str_info	表示用户已注销的提示信息。
_AN_str_hint	提示用户应如何操作的信息。
_AN_str-close	提示用户关闭窗口的弹出窗口的字符串。

文件名：an_challenge.js

此文件用于定义 RADIUS challenge 页面显示信息。

表13–5 门户主题 JavaScript 文件

变量	含义
_AN_str_title_challenge	Challenge 页面标题。
_AN_str_signin	登录操作链接的标签。
_AN_str_cancel	取消操作链接的标签。
_AN_str_password	密码字段的标签。
_AN_str_info_chal	Challenge 页面的信息。
_AN_str_errmsg_char	Challenge 页面的错误信息。

文件名：an_sms.js

此文件用于定义短信认证页面显示信息。

表13–6 门户主题 JavaScript 文件

变量	含义
_AN_str_title_otp	短信认证页面的标题。
_AN_str_otp_result	验证码检查或重新发送的结果。
_AN_str_otp_message	短信认证页面显示的消息。
_AN_str_resend	重新发送操作链接的标签。
_AN_str_submit	提交操作链接的标签。
_AN_str_cancel	取消操作链接的标签。
_AN_str_vcode	输入验证码的文本框的名称。
_AN_str_otp_resend	是否允许用户重新发送验证码。

第14章 高可用性（HA）

14.1 概述

随着网络应用的不断深入和发展，用户对网络和网络设备可靠性的要求越来越高。在网络规划设计时，为提高网络的可靠性，一般需要对关键节点的网络设备进行冗余备份。本章将介绍设备引入的高可用性（High Availability，HA）功能，该功能不仅可以解决单点故障问题，并且提供了更多的可靠性保证策略。

HA 功能允许两台或者多台设备持续不断地交互各自的状态信息，并保持各台设备上的配置信息同步更新。当一台设备发生故障时，其它可用设备将会自动接管该节点处理的应用服务，从而保证了应用服务的高可用性。

HA 功能的部署方式非常灵活。除了两台设备的 Active/Active 和 Active/Standby 部署场景外，HA 还支持多台设备互为备份的部署场景。

14.2 基本概念

14.2.1 HA 域和节点

HA 域是由一组提供 HA 功能的设备组成。HA 域中的设备通常称为节点。一个 HA 域支持配置多达 32 个节点。

14.2.2 浮动 IP 分组

通常来说，节点上的主备切换是通过浮动 IP 切换来实现。相同的浮动 IP 可以定义在多个节点上，但在同一时刻，只有一个节点上的浮动 IP 为 Active 状态。

为了保证切换的一致性和灵活性，在 HA 技术中，浮动 IP 的切换是按照分组进行的，即每个浮动 IP 必须加入浮动 IP 分组中才能实现状态切换。同一个分组中的所有浮动 IP 在同一时刻保持相同状态，也称为浮动 IP 分组状态。

浮动 IP 分组的状态是由分组优先级、切换模式和分组相关的健康检查结果决定的。在正确地配置了浮动 IP 分组后，HA 模块将根据配置的健康检查条件对分组的运行环境进行检查。根据检查结果，分组可以有以下两类状态：

- Active/Standby：分组通过了所关联的所有健康检查，表明分组处于可以提供服务的状态。此时，分组状态为“Active”或“Standby”。如果分组状态为“Active”，该节点将获得该分组中所有的浮动 IP 地址，并提供服务。如果分组状态为“Standby”，该节点将提供服务备份，在发生切换时，接管服务。
- Init：初始化状态。分组没有通过所关联的任意一个健康检查，分组状态为“Init”。当分组处于“Init”状态时，表明节点无法提供分组对应的服务，即使在它节点上该分组的状态发生了切换，也无法接管服务。

注意：当分组处于“Init”状态时，需要检查分组配置或者健康检查的结果，使分组状态切换为“Active/Standby”，以提供服务或服务备份。

一个节点上可以配置多个浮动 IP 分组，各个分组的状态相互独立。如果需要同时切换节点上的所有分组，需采用“Unit_Failover”切换方式（参见“14.4 失效切换规则”小节）。

浮动 IP 地址通过“**ha group fip**”和“**ha group fiprange**”命令配置。如需详细信息，请参见《AG 命令行使用手册》。

14.2.3 分组切换模式

HA 支持两种分组切换模式：非抢占（non-preempt）模式和抢占（preempt）模式。

当一个浮动 IP 分组被启用在多个节点上时：

- 在非抢占模式下：只有发生了失效切换，本节点上的分组状态才会发生切换。
- 在抢占模式下：如果本节点上设置的分组优先级高于所有对端节点上分组优先级，那么强制将本节点上的分组状态设置为“Active”。如果在此之前在某对端节点上的分组状态为“Active”，那么该状态将会被强制修改为“Standby”。

14.2.4 HA 部署场景

HA 功能提供多种部署场景。除了支持常见的两台设备的 Active/Active 和 Active/Standby 部署场景外，还支持多台设备互为备份的部署场景。

- Active/Active 部署场景是指 HA 域只包含两个节点，每个节点上都有“Active”状态的浮动 IP 分组，同时对端节点上“Active”状态的浮动 IP 分组在本节点上的状态为“Standby”。
- Active/Standby 部署场景是指 HA 域只包含两个节点，所有浮动 IP 分组的状态在一个节点上为“Active”，在另一个节点上为“Standby”。
- 多台设备互为备份的部署场景：多台设备用来提供服务和服务备份。其中，N+1 为最常见的部署场景。即 HA 域包含 N+1 个节点，在其中 N 个节点上，浮动 IP 分组的状态都为“Active”，在另外一个节点上，浮动 IP 分组的状态都为“Standby”。

14.3 可靠通信链路

HA 域中的节点可以通过多种通信链路交互各自的状态信息，从而确保通信的高可靠性。HA 节点可以通过以下三种链路进行通信：

- 主链路（Primary Link）

- 备用链路（Secondary Link）

主链路和备用链路都是通过普通网线将两个节点连接起来，因此统称为网络链路。每两个节点之间有且只有一条主链路，可以有 1~31 条备用链路。默认情况下，系统启用网络链路。

在节点加入 HA 域后，节点之间将会自动建立起主链路连接。主链路主要提供如下功能：

- 发送心跳包：本节点通过主链路向所有对端节点发送心跳包，用于探测其它节点的运行状况。
- 用于运行时配置同步：在运行时配置同步模式（runtime synconfig）下，如果本节点的相关的白名单配置发生变化时，本节点通过主链路将白名单的配置变化同步到对端节点。本节点黑名单的配置发生变化时，黑名单的配置变化不会同步到对端节点。

备用链路只能用来向对端节点发送心跳包，是可选配置。使用时需要手动在本地和对端 HA 节点上都进行备用链路配置。需要注意的是，在两个 HA 节点之间建立一条备用链路，需要分别在两个节点上配置一个 ID 相同的备用链路。

例如，两个 HA 节点“u1”和“u2”的备用链路的 IP 地址分别为 192.168.1.1 和 192.168.1.2，如果为两个 HA 节点创建一条备用链路，分别在每个 HA 节点上做如下配置：

```
AN(config)#ha link network secondary u1 1 192.168.1.1 65521
AN(config)#ha link network secondary u2 1 192.168.1.2 65521
```

这样，HA 节点“u1”和“u2”之间就建立了 ID 为“1”的备用链路。

下表介绍了两种通信链路的相同点和差异点。

表14–1 HA 通信链路的异同对比

项目		主链路	备用链路
不同点	连接方式	通过普通网线直连或者通过网络连接。	
	链路配置	在本地 HA 节点和对端 HA 节点都加入 HA 域后，HA 将在两个节点之间自动建立起主链路连接。	需要手动在本地和对端 HA 节点上都进行备用链路配置。
	应用场景	应用于所有部署场景。	
	登录 HA 域的方式	配置本地和对端节点的 IP 地址。 • 启用 HA 功能。	不涉及。
相同点		• 两种链路都可以用来发送心跳包。HA 节点通过发送心跳包交换各自的健康检查状况和分组状态信息等。 • 在 Active/Active 和 Active/Standby 部署场景下，两种链路可以互为备份。	

	• 如果两种链路都失效，则表明对端设备发生故障。

14.4 失效切换规则

在 HA 域中，HA 模块会对系统状态和网络状况进行健康检查。当健康检查的结果表明节点出现故障并满足定义的分组切换条件时，要进行切换操作。通常需要重新选出最高优先级的可用节点，并将该节点上的浮动 IP 分组的状态强制修改为“Active”。为了实现该目的，HA 提供失效切换规则来控制分组状态的切换。

失效切换规则是由切换条件和切换动作组成。其中，切换条件指系统的某个软硬件的监控状态。常见的切换条件有网络接口状态、CPU 使用率等。而切换动作则是指切换条件发生时，系统执行的动作。HA 提供三种切换动作，每种动作的含义如下：

- **Group_Failover**：对指定的浮动 IP 分组执行状态切换动作。该切换动作的含义是：按照健康状况和分组优先级选择新节点，并将其上的浮动 IP 分组为“Active”状态，并接管服务。
- **Unit_Failover**：对节点上所有的浮动 IP 分组执行状态切换动作。
- **Reboot**：对节点上所有的浮动 IP 分组执行状态切换动作后，再执行重启设备操作。

HA 支持以下健康检查类型：

➢ **预定义健康检查：**

HA 预定义了基本的网络连通性检查，即 PORT_1~PORT_32，用于检查网络接口故障和节点之间网络中断等异常情况。默认情况下，当网络接口出现故障时，系统会执行 Group_Failover 切换，管理员可以根据需要修改预定义健康检查关联的失效切换动作。

注意：

- 只有 Bond 接口中所有接口的网线连接不正常时，Bond 接口上的 IP 所在的浮动 IP 分组才会执行“Group_Failover”动作。
- 对于 HA 域中为同一浮动 IP 分组提供失效切换支持的各节点，需要为该浮动 IP 分组配置相同的失效规则,包括切换规则中健康检查条件的名称。
- 对于 HA 域中为“Unit_Failover”提供失效切换支持的各节点，需要为“Unit_Failover”配置相同的失效规则，包括切换规则中健康检查条件的名称。

➢ **系统健康检查：**

HA 功能可以复用系统健康检查作为失效切换条件。管理员可以自定义以下系统健康检查条件用于 HA 节点的失效切换：

硬件类：

- CPU 过热健康检查条件
- SSL 加速卡健康检查条件

软件类：

- CPU 使用率健康检查条件

网络环境类：

- 网关健康检查条件

在一些复杂的应用环境中，管理员需要定义一些更加复杂的失效切换规则。例如：在 Bond 接口环境中，只有所有网络端口的网线连接不正常，才执行切换动作。实际应用却要求在任意一个端口网线连接不正常，就执行切换动作。为了支持这些复杂应用，HA 功能支持配置健康检查条件组（vcondition）。vcondition 可以嵌套多个子健康检查条件，子条件之间逻辑关系可以指定为“AND”或者“OR”。对于上述例子的问题，可以通过定义多个网络端口的健康检查条件，并使用“OR”关系把它们组合成一个 vcondition，然后把 vcondition 关联切换动作。

➢ **自定义健康检查脚本：**

设备支持通过 SCP 或 TFTP 服务器导入自定义的健康检查脚本。自定义的健康检查脚本需通过签名认证后才生效，如需使用该功能，请联系华耀公司技术支持获取脚本。

14.5 配置同步

HA 功能提供配置同步功能，简化了节点上的配置，并确保域中所有节点上配置信息的一致性。目前，HA 功能只支持运行时配置同步（runtime synconfig）。

14.5.1 运行时配置同步

运行时配置同步是指在 HA 功能运行的过程中，管理员在一个节点上增删或者修改相关的命令配置时，该节点能够将变化的配置信息自动同步到域中其它节点。这样能够确保 HA 域中所有节点上的配置信息相同。

注意：只有在本节点和对端节点上都启用了运行时配置同步方式，节点才会把本地配置变化同步到对端节点。

14.6 连接同步（SSF）

HA 使用连接同步（Stateful Session Failover, SSF）来同步单元间的会话信息。

每个浮动 IP 组处理的会话信息将实时同步，从组状态为“Active”的单元到组状态为“备份”的其他单元。这样，当发生组故障转移时，一个“备份”单元可以

接管由这个组处理的现有会话。但是，客户需要重新建立与新单元上这个组的连接。新单元将重用会话信息，因此客户机不需要再次通过登录、身份认证、授权和其他进程。

SSF 同步的会话信息包括：

- 用户名
- 虚拟站点名称
- 角色名称
- AAA 方法名称

14.6.1 SPA 同步

SPA 同步是在连接同步（SSF）功能的基础上增加了 SPA 访问规则信息的同步。

该功能只要在 SSF 功能启用后才能生效。启用 SSF 功能后，当主备切换发生时，备机不需要重新敲门生成 SPA 访问规则。

14.7 HA 日志

HA 提供日志功能。默认情况下，系统禁用该功能。如果启用了 HA 功能，则日志功能同时被启用；如果禁用了 HA 功能，则日志功能同时被禁用。

设备支持八个 HA 日志级别：emerg、alert、crit、err、warning、notice、info 和 debug。管理员可以设置 HA 日志的级别。一旦设定了日志级别，低于这个级别的 HA 日志消息将被忽略，即系统不记录这些日志。默认的 HA 日志级别为 info。

HA 内部信息计入 HA 日志，浮动 IP 分组和节点变化将被计入系统日志。

14.8 配置示例

HA 功能可以部署在以下典型场景中：

- 场景 1：Active/Standby
- 场景 2：Active/Active
- 场景 3：N+1

下列章节将分别介绍三种典型场景的配置示例。

14.8.1 场景 1：Active/Standby

14.8.1.1 配置目标

Active/Standby 部署场景可以用来实现如下配置目标：

- HA 域包含两个 HA 节点，每个节点上都启用同一个浮动 IP 分组。
- 浮动 IP 分组中包含两个应用服务的 VIP 地址。
- 节点 1 提供应用服务，节点 2 提供备份。

实现如上配置目标的网络拓扑图如下图所示。

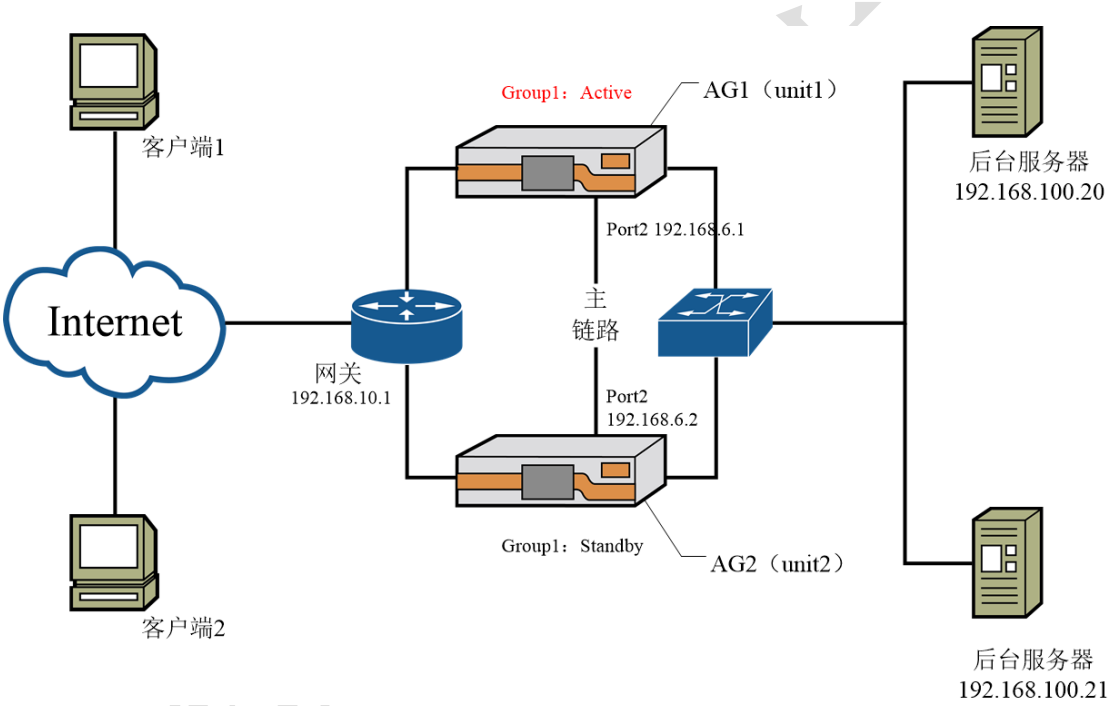

图14–1 Active/Standby 部署场景

14.8.1.2 配置示例

➢ **AG1 上的配置：**

1. 执行如下命令添加 HA 节点和链路配置：

```
AN(config)#ha unit "unit1" 1 192.168.6.1 65521
AN(config)#ha unit "unit2" 2 192.168.6.2 65521
AN(config)#synconfig peer "unit1" 192.168.6.1
AN(config)#synconfig peer "unit2" 192.168.6.2
AN(config)#ha link network on
```

2. 执行如下命令添加浮动 IP 分组配置：

```
AN(config)#ha group id 1
AN(config)#ha group fip 1 192.168.10.2 port1
AN(config)#ha group fip 1 192.168.10.3 port1
AN(config)#ha group fip 1 192.168.100.2 port3
AN(config)#ha group fip 1 192.168.100.3 port3
AN(config)#ha group priority unit1 1 10
AN(config)#ha group priority unit2 1 5
AN(config)#ha group preempt on 1
AN(config)#ha group enable 1
```

3. （可选）执行如下命令添加健康检查条件。下面以网关和 CPU 使用率的健康检查配置为例。

```
AN(config)#monitor network gateway unit1 192.168.10.1 GATEWAY_1 1000 3 3
AN(config)#monitor network gateway unit2 192.168.10.1 GATEWAY_1 1000 3 3
AN(config)#monitor system cpu utilization 90 5000 3 3
AN(config)#monitor vcondition name vcondition1 VCONDITION_1 AND
AN(config)#monitor vcondition member vcondition1 GATEWAY_1
AN(config)#monitor vcondition member vcondition1 CPU_UTIL
```

4. （可选）执行如下命令添加失效切换规则：

```
AN(config)#ha decision rule vcondition1 Group_Failover 1
```

5. （可选）执行如下命令启用 SSF 功能：

```
AN(config)#ha ssf on
```

6. （可选）执行如下命令设置配置同步模式：

```
AN(config)#ha synconfig runtime on
```

7. （可选）执行如下命令启用 HA 日志功能：

```
AN(config)#ha log on
```

8. 执行如下命令启用 HA 功能并保存 HA 的相关配置到内存中：

```
AN(config)#ha on
AN(config)#write memory
```

- **AG2 上的配置：**

在 Active/Standby 场景中，推荐使用主链路从对端节点同步相关配置信息。配置步骤应与 AG1 上的配置相同。

14.8.2 场景 2：Active/Active

14.8.2.1 配置目标

Active/Active 部署场景可以用来实现如下配置目标：

- HA 域包含两个 HA 节点，提供两个浮动 IP 分组。
- 每个浮动 IP 分组中包含一个应用服务的 VIP 地址。
- 节点 1 提供分组 1 的应用服务，节点 2 提供分组 2 的应用服务。节点 1 和节点 2 相互提供备份。

实现如上配置目标的网络拓扑图如下图所示。

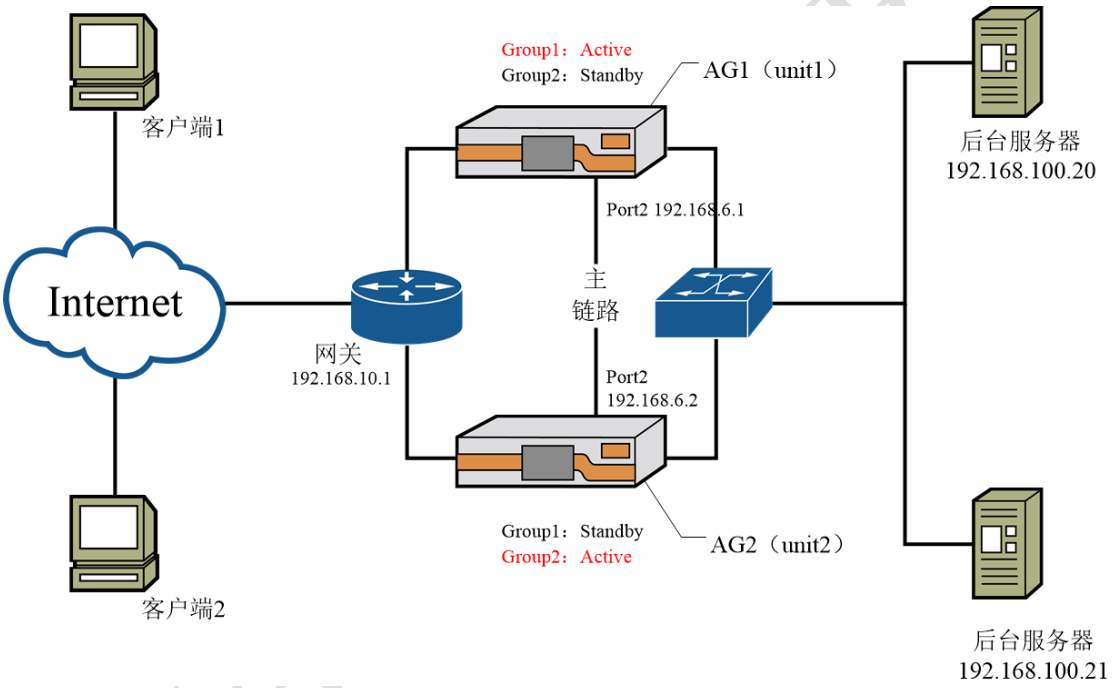

图14–2 Active/Active 部署场景

14.8.2.2 配置示例

➢ **AG1 上的配置：**

1. 执行如下命令添加 HA 节点和链路配置：

```
AN(config)#ha unit "unit1" 1 192.168.6.1 65521
AN(config)#ha unit "unit2" 2 192.168.6.2 65521
AN(config)#synconfig peer "unit1" 192.168.6.1
AN(config)#synconfig peer "unit2" 192.168.6.2
AN(config)#ha link network on
```

2. 执行如下命令添加浮动 IP 分组配置：

```
AN(config)#ha group id 1
AN(config)#ha group fip 1 192.168.10.2 port1
AN(config)#ha group fip 1 192.168.100.2 port3
AN(config)#ha group priority unit1 1 10
AN(config)#ha group priority unit2 1 5
AN(config)#ha group preempt on 1
AN(config)#ha group enable 1

AN(config)#ha group id 2
AN(config)#ha group fip 2 192.168.10.3 port1
AN(config)#ha group fip 2 192.168.100.3 port3
AN(config)#ha group priority unit1 2 5
AN(config)#ha group priority unit2 2 10
AN(config)#ha group preempt on 2
AN(config)#ha group enable 2
```

3. （可选）执行如下命令添加健康检查条件。下面以网关和 CPU 使用率的健康检查配置为例。

```
AN(config)#monitor network gateway unit1 192.168.10.1 GATEWAY_1 1000 3 3
AN(config)#monitor network gateway unit2 192.168.10.1 GATEWAY_1 1000 3 3
AN(config)#monitor system cpu utilization 90 5000 3 3
AN(config)#monitor vcondition name vcondition1 VCONDITION_1 AND
AN(config)#monitor vcondition member vcondition1 GATEWAY_1
AN(config)#monitor vcondition member vcondition1 CPU_UTIL
```

4. （可选）执行如下命令添加失效切换规则：

```
AN(config)#ha decision rule vcondition1 Unit_Failover
```

5. （可选）执行如下命令启用 SSF 功能：

```
AN(config)#ha ssf on
```

6. （可选）执行如下命令设置配置同步模式：

```
AN(config)#ha synconfig runtime on
```

7. （可选）执行如下命令启用 HA 日志功能：

```
AN(config)#ha log on
```

8. 执行如下命令启用 HA 功能并保存 HA 的相关配置到内存中：

```
AN(config)#ha on
AN(config)#write memory
```

➢ **AG2 上的配置：**

在 Active/Active 场景中，推荐使用主链路从对端节点同步相关配置信息。配置步骤应与 AG1 上的配置相同。

14.8.3 场景 3：N+1

在 N+1 部署场景中，HA 域包含 N+1 个节点，在其中 N 个节点上，浮动 IP 分组的状态都为“Active”，在另外一个节点上，所有浮动 IP 分组的状态都为“Standby”。本节将介绍“3+1”部署场景的配置目标和配置示例。

14.8.3.1 配置目标

“3+1”部署场景可以用来实现如下配置目标：

- HA 域包含四个节点，提供三个浮动 IP 分组。
- 每个浮动 IP 分组中包含一个虚拟服务的 VIP 地址。
- 节点 1~3 分别提供分组 1~3 的虚拟服务，节点 4 为节点 1~3 提供备份。

实现如上配置目标的网络拓扑图如下图所示。

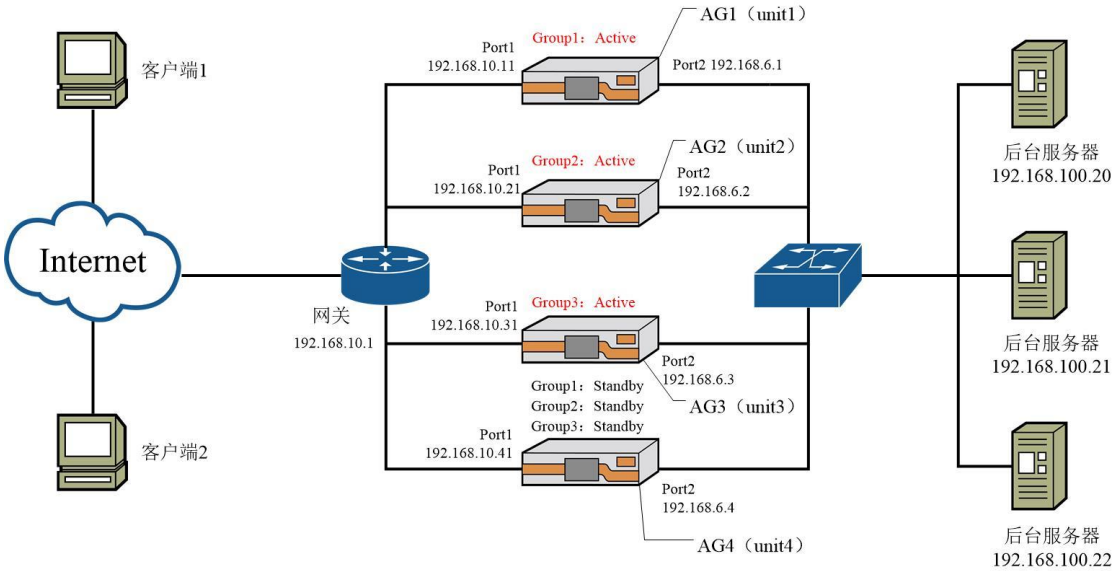

图14–3 N+1 部署场景

14.8.3.2 配置示例

➢ **AG1 上的配置：**

1. 执行如下命令添加 HA 节点和链路配置：

```
AN(config)#ha unit "unit1" 1 192.168.6.1 65521
```

```
AN(config)#ha unit "unit2" 2 192.168.6.2 65521
AN(config)#ha unit "unit3" 3 192.168.6.3 65521
AN(config)#ha unit "unit4" 4 192.168.6.4 65521
AN(config)#synconfig peer "unit1" 192.168.6.1
AN(config)#synconfig peer "unit2" 192.168.6.2
AN(config)#synconfig peer "unit3" 192.168.6.3
AN(config)#synconfig peer "unit4" 192.168.6.4
AN(config)#ha link network secondary unit1 1 192.168.10.11
AN(config)#ha link network secondary unit2 1 192.168.10.21
AN(config)#ha link network secondary unit3 1 192.168.10.31
AN(config)#ha link network secondary unit4 1 192.168.10.41
AN(config)#ha link network on
```

2. 执行如下命令添加浮动 IP 分组配置：

```
AN(config)#ha group id 1
AN(config)#ha group fip 1 192.168.10.2 port1
AN(config)#ha group fip 1 192.168.100.2 port3
AN(config)#ha group priority unit1 1 200
AN(config)#ha group priority unit2 1 100
AN(config)#ha group priority unit3 1 50
AN(config)#ha group priority unit4 1 150
AN(config)#ha group preempt on 1
AN(config)#ha group enable 1

AN(config)#ha group id 2
AN(config)#ha group fip 2 192.168.10.3 port1
AN(config)#ha group fip 2 192.168.100.3 port3
AN(config)#ha group priority unit1 2 50
AN(config)#ha group priority unit2 2 200
AN(config)#ha group priority unit3 2 100
AN(config)#ha group priority unit4 2 150
AN(config)#ha group preempt on 2
AN(config)#ha group enable 2

AN(config)#ha group id 3
AN(config)#ha group fip 3 192.168.10.4 port1
AN(config)#ha group fip 3 192.168.100.4 port3
AN(config)#ha group priority unit1 3 100
AN(config)#ha group priority unit2 3 50
AN(config)#ha group priority unit3 3 200
AN(config)#ha group priority unit4 3 150
AN(config)#ha group preempt on 3
```

```
AN(config)#ha group enable 3
```

3. （可选）执行如下命令添加健康检查条件。下面以网关和 CPU 使用率的健康检查配置为例。

```
AN(config)#monitor network gateway unit1 192.168.10.1 GATEWAY_1 1000 3 3
AN(config)#monitor network gateway unit2 192.168.10.1 GATEWAY_1 1000 3 3
AN(config)#monitor network gateway unit3 192.168.10.1 GATEWAY_1 1000 3 3
AN(config)#monitor network gateway unit4 192.168.10.1 GATEWAY_1 1000 3 3
AN(config)#monitor system cpu utilization 90 5000 3 3
AN(config)#monitor vcondition name vcondition1 VCONDITION_1 AND
AN(config)#monitor vcondition member vcondition1 GATEWAY_1
AN(config)#monitor vcondition member vcondition1 CPU_UTIL
```

4. （可选）执行如下命令添加失效切换规则：

```
AN(config)#ha decision rule vcondition1 Unit_Failover
```

5. （可选）执行如下命令设置配置同步模式：

```
AN(config)#ha synconfig runtime on
```

6. （可选）执行如下命令启用 HA 日志功能。

```
AN(config)#ha log on
```

7. 执行如下命令启用 HA 功能并保存 HA 相关配置到内存中：

```
AN(config)#ha on
AN(config)#write memory
```

- **AG2、AG3 和 AG4 上的配置：**

AG2、AG3 和 AG4 上的配置步骤应与 AG1 相同。

第15章 SSL 加速

15.1 概述

设备支持 SSL（Secure Sockets Layer，安全套接字层）加速，来改善我们客户端通讯的安全性。SSL 加速对安全数据进行解密，将解密后的信息传递到后台服务器。

15.2 SSL 加速的原理

SSL 最主要的作用是为 Web 流量提供安全访问机制。安全的含义包括保密性、信息完整性和安全认证。SSL 使用密码、数字签名和证书来保证这些元素的安全。

15.2.1 加密算法

SSL 使用加密算法保障重要信息的安全。设备可以使敏感数据在通过公共网络时，能够以较高的安全性到达目的地。数据的加密算法有两种类型：对称加密和非对称加密。

- 对称加密算法中，加密与解密使用相同的密钥，密钥由通信双方约定。密钥的传递可能被第三方截获，在实际应用中，常使用非对称加密算法来将对称密钥加密后再传递。常见的对称加密算法包括 DES、AES 等等。
- 非对称加密也称为公钥加密算法，该算法使用一对密钥，公钥和私钥。其中公钥是公开的，私钥只由一方持有，通过公钥加密的数据只能通过私钥解密。设备支持的非对称加密算法有 RSA、ECC 和 SM2 算法。

➢ **RSA 加密算法**

RSA 是最常用的非对称加密算法，其安全性的提高依赖于密钥长度的增加。随着密钥长度的逐步增加，RSA 加密算法的计算速度逐渐减慢。

➢ **ECC 加密算法**

与 RSA 算法相比，ECC 算法能够以较短的密钥长度实现与 RSA 算法同等的安全性。

➢ **SM2 加密算法**

SM2 加密算法是由中国国家商用密码局发布的基于椭圆曲线的公钥密码算法。自 SM2v1.1 版本开始，SM2 引入了双证书系统，SSL 服务器需具备两个证书：签名证书和加密证书。相应的密钥对为签名密钥对和加密密钥对。

- 签名密钥对和签名证书
- 签名证书用于 SSL 握手过程中的身份验证。

在服务器证书验证环节，服务器会在 Server Certificate 消息中携带这两种 SM2 证书，在 Server Key Exchange 消息中使用自己的签名密钥对里的私钥做数字签名，客户端会使用服务器的签名密钥对里的公钥验证签名，确认服务器的身份。

如果服务器需要验证客户端证书，客户端在 Client Certificate 消息中会携带这两种 SM2 证书，并在随后的 Client Certificate Verify 消息中使用自己的签名密钥对的私钥做数字签名，服务器会使用客户端的签名密钥对里的公钥验证签名，确认客户端的身份。

- 加密密钥对和加密证书

加密证书用于生成预主密钥。

在 ECC 密钥交换方式下，客户端在生成预主密钥后，会使用服务器的加密密钥对的公钥加密预主密钥，然后通过 Client Key Exchange 消息将预主密钥发送给服务器。服务器会用加密密钥对里的私钥进行解密，获取预主密钥的明文。

在 ECDHE 密钥交换方式下，在客户端发送 Client Key Exchange 消息给服务器后，双方会各自生成预主密钥。

15.2.2 数字签名

数字签名通过不可逆的签名算法计算得出。通过验证数字签名，可以判断信息发送方或签名者的身份，以及数据在传输过程中是否发生过篡改。SSL 虚拟站点支持在 SSL 握手过程中协商 RSA 签名算法和 ECDSA 签名算法，以及验证 RSA 和 ECDSA 签名证书。

在 ECDHE（Ephemeral Elliptic Curve Diffie-Hellman）方式的密钥交换环节，服务器会通过 Server Key Exchange 消息向客户端传送临时公钥信息，该信息里会附带一个数字签名。客户端会通过验证签名判断公钥是否完整、可靠。

在客户端证书验证环节，客户端会通过 Certificate Verify 消息向服务器发送一个数字签名，目的是让服务器验证客户端身份。服务器会用客户端证书里的公钥来验证签名。

SSL 虚拟站点支持的 RSA 和 ECDSA 签名算法如下表所示。

表15–1 签名算法

类型	SSL 虚拟站点
RSA 签名算法	SHA1RSA SHA224RSA SHA256RSA SHA384RSA SHA512RSA
ECDSA 签名算法	SHA1ECDSA SHA224ECDSA

	SHA256ECDSA SHA384ECDSA SHA512ECDSA

15.2.3 数字证书

证书包含了用于识别用户或设备的信息，这些数字文件可以证明一个公共密钥同个人或企业安全的绑定在一起。数字签名允许核实一个特定公共密钥的细节。证书有助于防止有人用虚假的密钥冒充服务器密钥。SSL 证书使用 X.509 标准来验证身份，X.509 标准证书包含了有关单位的信息，包括公共密钥和名字。一些权威的证书机构来保障证书的有效性。下面列出了 X.509 证书所包含的内容。

表15–2 X.509 证书所包含内容

名称	含义
Version	证书版本号，不同版本的证书格式不同。
Serial Number	证书序列号，具有唯一性，区别于该机构发布的其他证书。如果一个证书被撤销，其序号将被加入 CRL（Certificate Revocation List，证书撤销列表）中。
Issuer	证书发布机构，一般是权威的证书认证中心（Certificate Authority，CA）。
Valid from	证书的有效起始日期
Valid to	证书的有效截止日期
Subject	证书标识的个人或企业
Public key	证书持有者的公钥
Signature algorithm	用于生成数字签名的签名算法。
Thumbprint, Thumprint algorithm	指纹以及指纹算法，指纹是根据指纹算法计算出的整个证书的哈希值，然后通过 CA 的私钥加密后得到的。

设备支持两种数字证书：RSA、ECC 和 SM2 证书。

数字证书由 CA 签发，个人或企业需要通过发送证书签名请求（Certificate Signing Request，CSR）从 CA 获取证书后导入和激活证书。设备支持为虚拟站点生成 RSA、ECC 和 SM2 类型的 CSR。

➢ **生成 CSR**

- 如果需要申请 RSA 证书，可以使用“**ssl csr**”命令生成 RSA CSR。
- 如果需要申请 ECC 证书，可以使用“**ssl ecc csr**”命令生成 ECC CSR。

CA 会通过邮件回复需要申请的证书。获得证书后，需要通过命令导入证书。

- 如果需要申请 SM2 证书，可以使用“**ssl sm2 csr**”命令生成 SM2 CSR。

➢ **导入证书**

- RSA 和 ECC 证书通过“**ssl import certificate**”命令导入。
- 对于 SM2 证书申请， CA 会签发一个签名证书、一个加密证书和一个加密私钥，加密私钥有明文和数字信封（加密）两种形式。签名证书通过“**ssl sm2 import signcertificate**”命令导入，加密证书通过“**ssl sm2 import enccertificate**”命令导入，明文的加密私钥通过“**ssl sm2 import enckey**”命令导入，数字信封通过“**ssl sm2 import encevp**”命令导入。在导入数字信封前，必须先导入签名私钥。

➢ **激活证书**

RSA、ECC 和 SM2 证书都通过“**ssl activate certificate**”命令激活，在激活证书时，可以一次激活所有类型的证书或仅激活指定类型的证书。

- 如果 SSL 主机关联了一个或多个域名，那么可以为该主机的每个域各导入三个 RSA 证书和三个 ECC 证书，每个域可以各激活一个 RSA 证书和一个 ECC 证书。
- 如果 SSL 主机不关联任何域名，每个主机可以导入三个 RSA 证书、三个 ECC 证书和三对 SM2，同时激活一个 RSA 证书、一个 ECC 证书和一对 SM2 证书。

15.2.3.1 客户端证书认证

客户端证书认证是指客户端依据服务器的要求（Client Certificate Request）向服务器发送自己的证书，用于证明客户端的身份。设备支持通过证书分析器（华耀公司专利技术）来快速验证 X.509 证书。

当设备作为代理服务器（SSL 虚拟站点）时，启用客户端认证的 SSL 虚拟站点会向客户端发送证书请求消息，要求客户端提供证书进行认证。

15.3 SSL 加速配置

15.3.1 配置示例

➢ **为新建的 SSL 虚拟站点导入私钥和证书**

以下步骤以为虚拟站点申请、导入和激活 RSA 私钥和证书为例。

1. 执行“**ssl csr**”命令生成一个 RSA CSR（如果需要申请 ECC 证书，执行“**ssl ecc csr**”命令。如果需要申请 SM2 证书，执行“**ssl sm2 csr**”命令）。

```
AN(config)#ssl csr
```

Generating keys for "www.example.com"....please wait

We will now gather some required information about your SSL virtual site.

This information will be encoded into your certificate.
TWO-character country code for your organization (eg. US) :US
State or province []:CA
location or local city []:San Jose
Organization Name :Example.com
Organizational Unit :Example.com
Organizational Unit []:
Organizational Unit []:
Do you want to use the virtual site name "www.example.com"
as the Common Name? (recommended) [Y/N]: Y
email address of administrator []:admin@example.com
Do you want to add Subject Alternative Names? (recommended) [Y/N] N
-----BEGIN CERTIFICATE REQUEST-----
MIIC6jCCAdICAQAwgZUxCzAJBgNVBAYTAlVTMQswCQYDVQQIDAJDQTERMA8GA1U
EBwwIU2FuIEpvc2UxFDASBgNVBAoMC0V4YW1wbGUuY29tMRQwEgYDVQQLDAtFeGF
tcGxlLmNvbTEYMBYGA1UEAwwPd3d3LmV4YW1wbGUuY29tMSAwHgYJKoZIhvcNAQkB
FhFhZG1pbkBleGFtcGxlLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggE
BAKfPzHgGQA2DKh7kkzSKczUO9RkMRvrMX+MssKiVwGUpwUZ3B0YlW5gqUQ0ieYqNQ
bYr4s7G+d+zHe7NtsyUADMJwgDKK4pQaiBuxVWzQtqQqIGEZc4NqIaltJzOpzZSMqY0SvbQ
3MJqrvVgZpdObeedW5SRVjn8zyebr2j/re4tTIJpm+lj9FiFf/yVHsJdXjJrOONYfsAcaI9c8a5BLqe
PavZEvzh3p+eiCwjGflv8n48O8ub+PIGU1W230gkfRdG5D6e1yWlXFdceveunuOlfuoL2yBgHu
yxxgu+RkQd6ZqV6eACLbv47OTMr9MUGuW6TuQ0TI+T24lY8DBn/TxcCAwEAAaAPMA0G
CSqGSIb3DQEJDjEAMA0GCSqGSIb3DQEBCwUAA4IBAQCRl4Mao7hBqsqH/+kU8IQK7aq
wdujSDj5KxO5rKkSutslaqfsIbpr85nGKFqxrBxpy0lFs6NegztSV0dCc/Dt3iVaAqLEgeVmdFA9Z
bcpwHecQmeg1D200GmpsU3T2xiqM0mDc7jmRywWenCJkRWmO3EWeO9N5mbbeoOUs4Kel
KvVayMe2k9YvArSmOa3NHzyTQ1Zhqc80Q6Jg7mSw6B9et0JpKIim+3Hw12ULOdhIDijLOa8
GiDdhuL4J5FBDW0wY8Jl+YKeW7r8GDldENP1bdvWDdDkI0zHhVuwPDOuAcwWj23gT7jLo
wcNYRNIVW5RGrXHjlfb9UXKqMboJmpp+
-----END CERTIFICATE REQUEST-----

Do you want the private key to be exportable [Yes/(No)]:Yes
Enter passphrase for the private key:

Confirm passphrase for the private key:

Warning: RSA certificate chain is incomplete for www.example.com. Please add interca or rootca certificate.

除了生成 RSA CSR 外，该命令同时也为 SSL 虚拟站点创建了一个 RSA 密钥对和测试证书。测试证书只能用于测试目的，如果希望利用该测试证书进行测试或演示，可以直接启用该 SSL 虚拟站点：

```
AN(config)#ssl start
```

此时，管理员可以使用网页浏览器安全地连接到该网站。

2. 转发证书签发请求到认证中心。

从“**ssl csr**”命令的输出中，复制从“-----BEGIN CERTIFICATE REQUEST-----”到“-----END CERTIFICATE REQUEST-----”的内容，转发给 CA，CA 会回复一封包含数字证书的电子邮件。以下显示的是一个证书样例。

```
-----BEGIN CERTIFICATE-----
MIICnjCANgcANgEUMA0GCSqGSIb3DQEBBAUAMIG5MQswCQYDVQQGEwJVUzETMB
EGA1UECBMKQ2FsaWZvcm5pYTERMA8GA1UEBxMIU2FuIEpvc2UxHDAaBgNVBAoTE0
NsaWNrQXJyYXkgTmV0d29ya3MxFDASBgNVBAsTC0RldmVsb3BtZW50MSMwIQYDVQ
QDExpkZXZlbG9wbWVudC5jbGlja2FycmF5LmNvbTEpMCcGCSqGSIb3DQEJARYaZGV2Z
WxvcG1lbnRAY2xpY2thcnJheS5jb20wHhcNMDIwMjEzMTgwMTI5WhcNMDMwMjA4MTgw
MTI5WjB0MQswCQYDVQQGEwJVUzEMMAoGA1UECBMDRE9EMQwwCgYDVQQHEw
NET08xCzAJBgNVBAoTAkRPMQswCQYDVQQLEwJETzETMBEGA1UEAxMKMTAuMTIu
MC4xNDEaMBgGCSqGSIb3DQEJARYLbWhAZGtkay5jb20wgZ8wDQYJKoZIhvcNAQEBBQ
ADgY0AMIGJAoGBAMx4r+ae4kTZggtyU047OsKUyqCt+V1MHgTPTpVxdtxYhSTSOZwYIX
gRqBEdJvs2/ua1XZRzLOCTa58VI/8I3derAPqz79WpBRsxD25rCT1rzmalfkTea3V8jHJYP6Yin
DTWKFKztxeUclkzukzPUZO6M0fI5ToXNuLEe+IwvOkfAgMBAAEwDQYJKoZIhvcNAQEEB
QADgYEAodV5O0LKUr/O0BbxOnwmyP/DkLj4bpe9XxQO6B4psDey/+xBHs6tgGKuy8spbcJ4
pQc+5KLydK1ZYcTkbxJq41K4RHM11OClXVjm3xRhqKQnjzNboExIvkZsKIBbfLkBrM1eBnE
aiYWXmsYGfxPkwdhKlQCLQgN+G3IKu2cRQLU=
-----END CERTIFICATE-----
```

注意：进行 SSL 配置时请务必谨慎操作。在导入从认证中心获得的证书之前，请一定不要删除 SSL 虚拟站点。如果清除了 SSL 信息，则只能再次发送证书签发请求到认证中心以获得另一个证书。不过，大多数认证中心允许有 30 天的试用期以便于获得另一个证书，超过了这个期限，就必须购买另一个证书。

3. 使用“**ssl import certificate**”命令为 SSL 虚拟站点导入收到的证书。

```
AN(config)#ssl import certificate 1

You may overwrite an existing certificate.
Type YES to continue, NO to abort: YES
Enter the certificate file in PEM format,
  use "..." on a single line, without quotes
  to terminate import
-----BEGIN CERTIFICATE-----
```

```
MIICnjCANgcANgEUMA0GCSqGSIb3DQEBBAUAMIG5MQswCQYDVQQGEwJVUzETMB
EGA1UECBMKQ2FsaWZvcm5pYTERMA8GA1UEBxMIU2FuIEpvc2UxHDAaBgNVBAoTE0
NsaWNrQXJyYXkgTmV0d29ya3MxFDASBgNVBAsTC0RldmVsb3BtZW50MSMwIQYDVQ
QDExpkZXZlbG9wbWVudC5jbGlja2FycmF5LmNvbTEpMCcGCSqGSIb3DQEJARYaZGV2Z
WxvcG1lbnRAY2xpY2thcnJheS5jb20wHhcNMDIwMjEzMTgwMTI5WhcNMDMwMjA4MTgw
MTI5WjB0MQswCQYDVQQGEwJVUzEMMAoGA1UECBMDRE9EMQwwCgYDVQQHEw
NET08xCzAJBgNVBAoTAkRPMQswCQYDVQQLEwJETzETMBEGA1UEAxMKMTAuMTIu
MC4xNDEaMBgGCSqGSIb3DQEJARYLbWhAZGtkay5jb20wgZ8wDQYJKoZIhvcNAQEBBQ
ADgY0AMIGJAoGBAMx4r+ae4kTZggtyU047OsKUyqCt+V1MHgTPTpVxdtxYhSTSOZwYIX
gRqBEdJvs2/ua1XZRzLOCTa58VI/8I3derAPqz79WpBRsxD25rCT1rzmalfkTea3V8jHJYP6Yin
DTWKFKztxeUclkzukzPUZO6M0fI5ToXNuLEe+IwvOkfAgMBAAEwDQYJKoZIhvcNAQEEB
QADgYEAodV5O0LKUr/O0BbxOnwmyP/DkLj4bpe9XxQO6B4psDey/+xBHs6tgGKuy8spbcJ4
pQc+5KLydK1ZYcTkbxJq41K4RHM11OClXVjm3xRhqKQnjzNboExIvkZsKIBbfLkBrM1eBnE
aiYWXmsYGfxPkwdhKlQCLQgN+G3IKu2cRQLU=
-----END CERTIFICATE-----
```

也可以从远程 TFTP 服务器导入证书。使用这种方法时，需要指定 TFTP 服务器的 IP 地址和证书文件的名称：

```
AN(config)#ssl import certificate 1 10.10.13.82 example.crt
You may overwrite an existing certificate.
Type YES to continue, NO to abort: YES
```

注意：

如果已经存在可以使用的密钥和证书文件（无需通过 CSR 申请证书），可以使用“**ssl import key**”命令和“**ssl import certificate**”命令为 SSL 虚拟站点直接导入密钥和证书，导入时既可以使用手动粘贴文件内容的方法，也可以通过远程 TFTP 服务器导入，但有两点需要注意：

- 必须先导入密钥然后再导入证书。
- 非 PEM 格式的密钥和证书，必须通过 TFTP 方式导入。

4. 使用“**ssl activate certificate**”命令激活证书。

```
AN(config)#ssl activate certificate 1
```

注意：在激活证书时，系统会检查证书链。如果根证书和中级证书在全局受信 CA 文件或中级 CA 文件中无法找到，系统将会打印一条警告信息提示证书链不完整。可以分别使用命令“**ssl import rootca**”和“**ssl import interca**”来导入根证书和中级证书。

5. 启用 SSL 虚拟站点。

```
AN(config)#ssl start
```

至此已经完成了 SSL 加速配置，客户端可以通过 HTTPS 正常访问。

➢ **从 IIS 网页服务器中导入证书和密钥**

IIS

如果使用的是 Microsoft IIS 服务器，设备允许通过 TFTP 机制从 IIS4/5 中导入证书。IIS 在同一个.PFX 格式的证书中存储 SSL 密钥和证书。先将该文件放到 TFTP 服务器的根目录下，以<vhostname>.crt 命名，然后使用“**ssl import certificate**”命令将证书导入到设备中。本命令需要输入 TFTP 服务器的 IP 地址做为参数。

```
AN(config)#ssl import certificate 1 10.10.0.3
```

该命令将下载名为<host_name>.crt 的证书，在我们的例子中是从 TFTP 服务器 10.10.0.3 上下载 www.example.com.crt。

成功导入证书后，可以使用“**ssl activate certificate**”命令启动这个证书。

```
SJ-Box1(config)#ssl activate certificate 1
```

从 TFTP 服务器上成功导入密钥和证书后，可以使用“**ssl start**”启动 SSL 子系统。

```
AN(config)#ssl start
```

15.3.1.1 SSL 虚拟站点的高级配置

1. 禁用 SSL 虚拟站点。

```
AN(config)#ssl stop
```

如果更改 SSL 虚拟站点的配置，必须先禁用该站点。

2. 为 SSL 虚拟站点配置密码套件。

```
AN(config)#ssl settings ciphersuite "DES-CBC3-SHA"
```

下表列出了不同协议版本的 SSL 虚拟站点对 RSA、ECC（ECDHE-ECDSA..）和 SM2 密码套件的支持情况。“Y”表示支持，“N”表示不支持。

表15–3 不同协议版本的 SSL 虚拟站点对 RSA、ECC 和 SM2 密码套件的支持情况

密码套件	位数	SSL 协议			
		SSLv3.0	TLSv1	TLSv1.2	SM2v1.1
AES256-GCM-SHA384	256	N	N	Y	N
AES128-GCM-SHA256	128	N	N	Y	N
AES256-SHA256	256	N	N	Y	N
AES256-SHA	256	Y	Y	Y	N
AES128-SHA256	128	N	N	Y	N
AES128-SHA	128	Y	Y	Y	N

DES-CBC3-SHA	192	Y	Y	Y	N
DES-CBC-SHA	64	Y	Y	N	N
RC4-SHA	128	Y	Y	Y	N
RC4-MD5	128	Y	Y	Y	N
EXP-DES-CBC-SHA	40	Y	N	N	N
EXP-RC4-MD5	40	Y	N	N	N
ECDHE-RSA-AES256-GCM-SHA384	256	N	N	Y	N
ECDHE-RSA-AES128-GCM-SHA256	128	N	N	Y	N
ECDHE-RSA-AES256-SHA384	256	N	N	Y	N
ECDHE-RSA-AES256-SHA	256	Y	Y	Y	N
ECDHE-RSA-AES128-SHA256	128	N	N	Y	N
ECDHE-RSA-AES128-SHA	128	Y	Y	Y	N
ECDHE-ECDSA-AES256-GCM-SHA384	256	N	N	Y	N
ECDHE-ECDSA-AES128-GCM-SHA256	128	N	N	Y	N
ECDHE-ECDSA-AES256-SHA384	256	N	N	Y	N
ECDHE-ECDSA-AES256-SHA	256	Y	Y	Y	N
ECDHE-ECDSA-AES128-SHA256	128	N	N	Y	N
ECDHE-ECDSA-AES128-SHA	128	Y	Y	Y	N
ECDHE-SM4-SM3	128	N	N	N	Y
ECC-SM4-SM3	128	N	N	N	Y

如果要为一个 SSL 虚拟站点配置多个密码套件，需要在各密码套件之间以冒号“:”分隔。

3. 为 SSL 虚拟站点配置协议版本。

```
AN(config)#ssl settings protocol "SSLv3:TLSv1:TLSv12"
```

4. 可以设置为 SSLv3、TLSv1、TLSv12 或 SM2v11，或者同时设置其中的几个或者全部。

注意：“TLSv12”代表 TLSv1.2 协议，SM2v11 代表 SM2v1.1 协议

5. 为 SSL 虚拟站点配置会话复用功能。

```
AN(config)#ssl settings reuse
```

该功能默认是启用的，可以使用命令“**no ssl settings reuse**”关闭该功能。

6. 为 SSL 虚拟站点配置客户端认证。

设备支持基于 SSL 的客户端认证。如果启用该功能，在客户端可以连接到 SSL 虚拟站点之前，设备要求每个客户端提供 SSL 证书。

此外，SSL 虚拟站点还可以根据配置的证书过滤规则（使用“**ssl settings certfilter**”命令）检查客户端证书。如果客户端证书没有通过证书校验，SSL 虚拟站点将拒绝客户端访问。

```
AN(config)#ssl settings clientauth
```

注意：如果为 SSL 虚拟站点启用了 SSL 客户端认证功能，则必须提供一个受信 CA 证书，使用它对客户端证书进行校验。

```
AN(config)#ssl import rootca
```

该命令将提示用户粘贴一个 PEM 格式的受信 CA 证书。可以为 SSL 虚拟站点配置多个受信 CA。

一个 SSL 虚拟站点最多支持三条 certfilter 配置，配置之间为逻辑“或”关系。如果客户端证书匹配不到任何一条 certfilter 配置，SSL 虚拟站点将拒绝客户端访问。

例如：

```
AN(config)#ssl settings certfilter
"subject:/C=CN/O=Enterprise/OU=QA/emailAddress=admin@infossec.com.cn"
"issuer:/C=CN/"
```

在本例中，只有当客户端证书同时满足以下两个条件，才能通过校验：

- “subject”字段中，“C”为“CN”，“O”为“Enterprise”，“OU”为“QA”，“emailAddress”为 admin@arraynetworks.com.cn。
- “issuer”字段中，“C”为“CN”。

否则，客户端证书不能通过证书校验。

设备支持两种客户端认证方式：强制的和非强制的。客户端认证模式默认是强制的。在非强制模式下，当服务器发送一个证书请求到客户端时，如果客户没有匹配的证书，或者点“Cancel”取消时，服务器将会允许客户连接到限制性的网络资源，而不是放弃这个 SSL 连接。

7. 为 SSL 虚拟站点配置 CRL。

CRL（即证书撤销列表），可以通过 HTTP、FTP 或 LDAP 定期从 CRL 分发点获取 CRL 文件，CRL 分发点最多可以配置 10 条。

示例：在一个 HTTP 网页服务器上保存有 CRL 文件（list.crl），希望每隔 1 分钟获取该文件。配置命令如下：

```
AN(config)#ssl settings crl offline cdp1 "http://www.crldp.com/list.crl" 1
```

这样设备每隔 1 分钟会从 www.crldp.com 上下载 CRL 文件 list.crl。

也可以从 FTP 网站上下载 CRL 文件：

```
AN(config)#ssl settings crl offline cdp1 "ftp://ftp.crldp.com/list.crl" 1
```

也支持从 LDAP 网站上下载 CRL 文件：

```
AN(config)#ssl settings crl offline cdp1
"ldap://ldap.crldp.com/cn=bjhy,dc=enterprise,dc=com" 1
```

8. 为 SSL 虚拟站点配置 OCSP 在线检测证书有效性。

设备支持 OCSP（在线证书状态协议）。可以在一个 OCSP 服务器上线上校验证书。

示例：配置一个 OCSP 服务器（ocsp.crldp.com:8888）在线校验证书：

```
AN(config)#ssl settings ocsp "http:// ocsp.crldp.com:8888"
```

注意：OCSP 具有最高的优先级。本命令配置后，将仅通过该 OCSP 服务器对证书校验。

9. 为不具有强加密支持的客户端配置复位向。

设备提供复位向弱客户端（没有使用强加密的客户端）到另一个 URL 的功能。指定可以接受的最弱强度，任何使用比此更弱的加密算法的客户端将被复位向到另一个 URL。

比如，希望将密钥长度小于 168 位的客户端复位向到另一个不同的网站 www.example2.com。

配置命令如下：

```
AN(config)#ssl settings minimum 168 "http://www.example2.com"
```

10. 启用并查看 SSL 配置。

启动 SSL 虚拟站点：

```
AN(config)#ssl start
```

查看当前 SSL 设置：

```
AN(config)#show ssl setting
```

第16章 防火墙

16.1 概述

本节将主要介绍防火墙（WebWall）的原理、高级功能、工作流程和配置方法。

通过设备的防火墙，网络管理员可以建立允许或拒绝规则来过滤各种通过网络的数据报，设备的防火墙支持对基于 IPv4 或 IPv6 地址的 TCP、UDP 和 ICMP 协议数据包的过滤。系统默认为每个接口禁用防火墙功能。

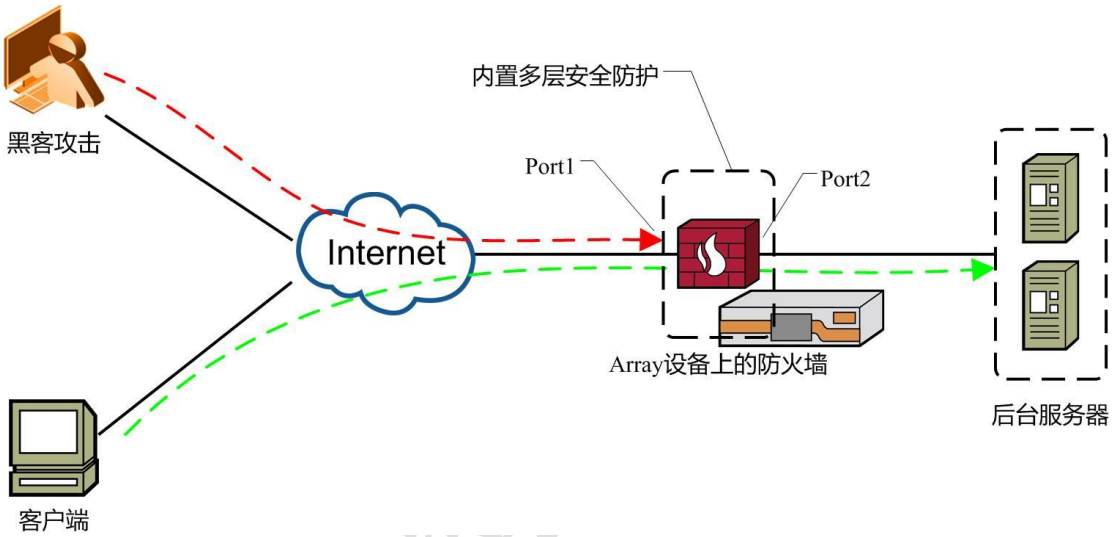

图16–1 防火墙

防火墙功能利用设备的快速规则引擎严格控制着访问者的身份识别和访问权限。该功能确保了设备运行了 1000 个以上的 ACL 规则时，不会有超过 1%的性能损失。

要使用防火墙功能，管理员首先应创建允许和拒绝的访问规则，再将访问规则关联到接口，最后再为接口启用防火墙功能。

16.2 防火墙配置

16.2.1 配置场景

在设备上配置防火墙功能，确保防火墙能够按照以下规则处理管理流量和业务流量：

- 允许 IP 地址为 10.10.10.30 的客户端通过 22 端口来配置和管理设备（通过 SSH 访问）

- 允许 IP 地址为 10.10.10.30 的客户端通过 8888 端口配置和管理设备（通过 WebUI 访问）。
- 允许除 IP 地址为 10.10.10.30 以外的所有客户端通过 80 端口访问虚拟 IP 地址 10.10.0.10。
- 允许所有内网客户端 Ping 设备的 Port2 接口 IP 地址 192.168.10.1。

该配置举例所基于的网络拓扑请参见下图。

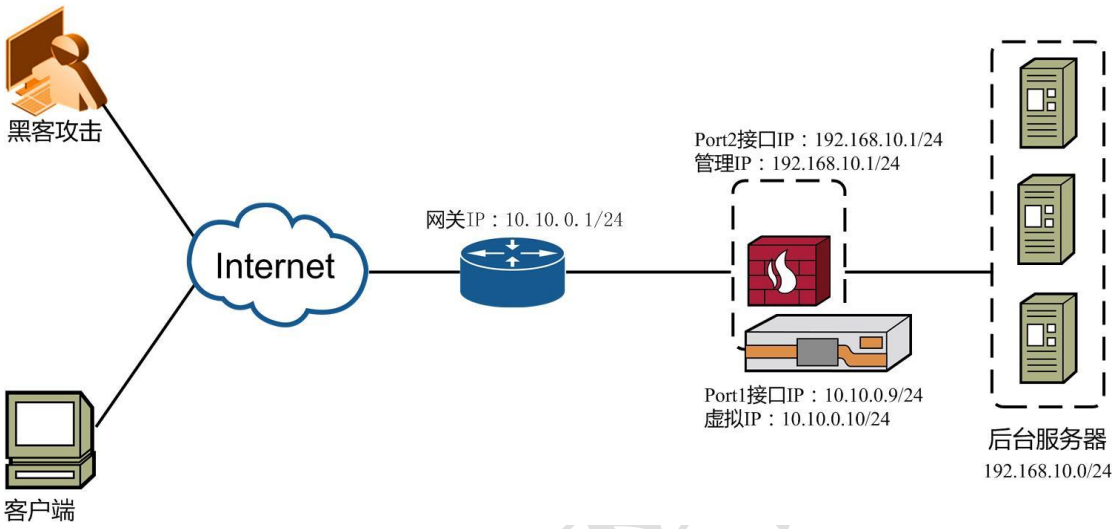

图16－2 防火墙配置

16.2.2 配置步骤

➢ **配置 ACL 访问规则**

1. 配置允许 IP 地址为 10.10.10.30 的客户端通过 22 端口来配置和管理设备（通过 SSH 访问）

```
AN(config)#accesslist permit tcp 10.10.10.30 255.255.255.255 0 192.168.10.1 255.255.255.255 22 100
```

2. 配置允许 IP 地址为 10.10.10.30 的客户端通过 8888 端口配置和管理设备（通过 WebUI 访问）。

```
AN(config)#accesslist permit tcp 10.10.10.30 255.255.255.255 0 192.168.10.1 255.255.255.255 8888 100
```

3. 配置允许除 IP 地址为 10.10.10.30 以外的所有客户端通过 80 端口访问虚拟 IP 地址 10.10.0.10。

```
AN(config)#accesslist permit tcp 0.0.0.0 0.0.0.0 0 10.10. 0.10 255.255.255.255 80 150
AN(config)#accesslist deny tcp 10.10.10.30 255.255.255.255 0 10.10. 0.10 255.255.255.255 80 150
```

4. 配置允许所有的内网客户端 Ping 设备的 Port2 接口 IP 地址 192.168.10.1。

```
AN(config)#accesslist permit icmp echorequest 192.168.10.0 255.255.255.0 192.168.10.1 255.255.255.255 50
AN(config)#accesslist permit icmp echoreply 192.168.10.1 255.255.255.255 192.168.10.0 255.255.255.0 50
```

➢ **关联访问规则到接口**

1. 将不同类型的访问规则（访问规则标识为 50）关联到指定的接口。

```
AN(config)#accessgroup 50 port2
```

2. 将用于管理 IP 地址的访问规则（访问规则标识为 100）关联到指定的接口。

```
AN(config)#accessgroup 100 port2
```

3. 将与虚拟 IP 地址相关的访问规则（访问规则标识为 150）关联到指定的接口。

```
AN(config)#accessgroup 150 port1
```

➢ **为接口启用防火墙**

执行下面的命令启用防火墙。

```
AN(config)#webwall port2 on
AN(config)#webwall port1 on
```

启用防火墙之前，需注意：

- 如果配置了域名解析服务器，并且需要在 DNS 流量通过的接口上打开防火墙，需要配置相应的访问规则以允许访问 53 端口的流量通过。

在启用防火墙后，如果需要调整防火墙配置，请注意正在使用中的 SSH 或 WebUI 访问会话可能由于配置失误而被中断。

➢ **配置验证**

配置完成后，可以使用下列命令来检查配置的结果。

```
AN(config)#show accesslist
accesslist permit tcp 10.10.10.30 255.255.255.255 0 192.168.10.1 255.255.255.255 22 100
accesslist permit tcp 10.10.10.30 255.255.255.255 0 192.168.10.1 255.255.255.255 8888 100
accesslist permit tcp 0.0.0.0 0.0.0.0 0 10.10. 0.10 255.255.255.255 80 150
accesslist deny tcp 10.10.10.30 255.255.255.255 0 10.10. 0.10 255.255.255.255 80 150
accesslist permit icmp echorequest 192.168.10.0 255.255.255.255 192.168.10.1 255.255.255.255 50
accesslist permit icmp echoreply 192.168.10.1 255.255.255.255 192.168.10.0 255.255.255.0 50
AN(config)#show accessgroup
accessgroup 50 port2
```

```
accessgroup 100 port2
accessgroup 150 port1
```

如果访问规则过于复杂，可以简化配置。如果关联了多条访问规则，可以尝试每次关联一个访问规则来判断是哪个访问规则引起的问题。也可以禁用防火墙功能，来定位问题。

使用“**show webwall**”命令可以查看哪些接口上开启了防火墙功能，例如：

```
AN(config)#show webwall
webwall "port2" on 0
webwall "port3" on 0
```

使用“**show interface**”命令可以查看包过滤功能的丢包状况，在下面的示例中，packet drop (not permit): 0 表示通过默认的拒绝包过滤规则丢弃的报文数量；packet drop (deny): 0 表示通过自定义的拒绝包过滤规则丢弃的报文数量。

```
AN(config)#show interface
port2(port2): flags=2008842<BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether 00:25:90:39:97:f1
        media: autoselect
        status: no carrier
        webwall status: ON
        Hardware is i82574l
        Input queue: 0/4096 (size/max)
                total: 0 packets, good: 0 packets, 0 bytes
                broadcasts: 0, multicasts: 0
                0 64 bytes, 0 65-127 bytes,0 128-255 bytes
                0 255-511 bytes,0 512-1023 bytes,0 1024-1522 bytes
                0 input errors
                0 runts, 0 giants, 0 Jabbers, 0 CRCs
                0 Flow Control, 0 Fragments, 0 Receive errors
                0 Driver dropped, 0 Frame, 0 Lengths, 0 No Buffers
                0 overruns, Carrier extension errors: 0
        Output queue: 0/4096 (size/max)
                total: 0 packets, good:    0 packets, 0 bytes
                broadcasts: 0, multicasts: 0
                0 64 bytes, 0 65-127 bytes,0 128-255 bytes
                0 255-511 bytes,0 512-1023 bytes,0 1024-1522 bytes
                0 output errors
                0 Collisions, 0 Late collisions, 0 Deferred
                0 Single Collisions, 0 Multiple Collisions, 0 Excessive collisions
        0 lost carrier, 0 WDT reset
        packet drop (not permit): 0
                tcp 0           udp 0           icmp 0          ah 0            esp 0
```

packet drop (deny): 0

tcp 0 *udp 0* *icmp 0* *ah 0* *esp 0*

5 minute input rate 0 bits/sec, 0 packets/sec

5 minute output rate 0 bits/sec, 0 packets/sec

第17章 日志

17.1 概述

本章将介绍设备的日志（Logging）功能。

设备的日志记录机制遵从 Syslog 的原则。日志子系统负责记录系统错误信息和代理（Proxy）服务中的 HTTP 访问信息。Syslog 是 Unix 平台中的一个通用程序，在 Windows 平台也存在 Syslog 的应用。在 Unix 平台上使用 Syslogd 命令来启动 Syslog 功能，Syslog 监听 UDP514 端口，负责接收并存储本机和非本地的日志信息。设备现在已经支持向三个非本地日志服务器传送日志信息。

17.2 日志原理

17.2.1 Syslog 机制

Syslog 是一种可以将警告和通知信息在网络上传送的协议。

Syslog 日志有八种日志信息的安全级别：紧急（emerg）、报警（alert）、关键（crit）、错误（err）、警告（warning）、提示（notice）、信息（info）和测试（debug），并且支持从 LOCAL0 到 LOCAL7 的八个设备。用户可以使用日志信息查看管理工具来查看内部信息、选择传输协议、设置 syslog 的源、目的端口，设置设备的警告等级等等。

17.2.2 RFC 5424 Syslog

RFC5424 定义了 Syslog 的标准格式。设备支持 RFC 5424 syslog 功能。当启用 RFC 5424 syslog 功能后，系统将会生成 RFC 5424 标准格式的系统日志。RFC 5424 标准日志格式为“<PRI>VER TIMESTAMP HOSTNAME APPNAME PROCID MSGID STRUCTURED-DATA MSG-CONTENT”。（暂不支持 PROCID 和 STRUCTURED-DATA 字段，这两个字段默认显示为“-”。）默认情况下，系统禁用 RFC 5424 syslog 功能。只有执行“**log on**”和“**log rfc5424 on**”命令后，RFC 5424 syslog 功能才能生效。

注意：只有当客户端和 Web 服务器之间完成一次正常的 HTTP 通信之后，设备才会记录一条 HTTP 访问日志。

17.2.3 日志过滤

日志过滤通过匹配过滤字符串把日志过滤到不同的日志服务器。其中，过滤字符串是在命令“**log filter**”中定义的。

通过 ArrayOS 中的日志过滤功能，管理员可以只收集感兴趣的日志信息，而不用收集所有的日志信息。例如，“www.site1.com”的管理员可能只需要“www.site1.com”的 HTTP 访问日志。如果知道这些日志中都包含一个关键词串“site1.com”，管理员可以定义一个日志过滤器，该过滤器可以过滤出所有与该字符串匹配的日志。从而管理员就能获得只包含他所需要日志的日志文件。

如果一个 Syslog 日志主机上配置了多个日志过滤器，只要与其中任意一个过滤字符串匹配的日志都会被过滤到该 Syslog 日志主机。

17.2.4 本地 Syslog 主机

系统允许管理员在设备上启用一个本地 syslog 主机，用于接收和存储系统日志消息。本地 syslog 主机默认设置为禁用。

启用了本地 syslog 主机后，本地 syslog 主机开始在 IP 地址 127.0.0.1 和 UDP 端口 515 上接收系统发送的系统日志。本地 syslog 主机可以为每个日志级别存储最多 50,000 条系统日志。在本地 syslog 主机上存储的系统日志可以通过 WebUI 查看和导出。

要启用本地 syslog 主机，管理员可以 CLI 里执行“**log localhost on**”命令。

17.3 配置示例

1. 启用设备的日志功能。

设备的日志功能默认是关闭的。

```
AN(config)#log on
```

2. 启用设备的 RFC 5424 syslog 功能。

```
AN(config)#log rfc5424 on
```

3. 设置用户接受日志信息的远程主机。

命令“**log host**”用于配置日志服务器来接收系统所产生的日志信息。日志服务器的 IP 地址应该使用 dotted IP 格式来配置，日志服务器的端口是可选的，默认端口是 514。Syslog 所使用的传输层协议可采用 UDP 和 TCP，默认使用 UDP。

```
AN(config)#log host 10.2.37.1 514 udp1
```

4. 为主机配置日志过滤。

日志主机上最多可以配置三条日志过滤条目，并且过滤条目不能配置在 ID 为 0 的日志主机上。在下列命令运行后，只有符合过滤字符串的日志可以到达日志主机。

```
AN(config)#log filter 1 1 "index"
```

5. 调整日志记录的级别。

设置某一日志记录的级别后，那些低于该级别的日志信息将会被系统忽略。默认的日志记录的级别为信息（info）。

```
AN(config)#log level err
```

6. 自定义日志的设备。

命令“**log facility**”用于修改记录 Syslog 的自定义设备。系统为用户自定义设备预留从 LOCAL0 到 LOCAL7 一共八个设备。系统默认的设备为 LOCAL0。

```
AN(config)#log facility LOCAL0
```

7. 生成测试信息。

命令“**log test**”用于以 emerg 的日志级别生成一条测试日志信息。

```
AN(config)#log test
```

8. 查看和调整日志信息和配置。

命令“**show log buff** *{forward|backward} [match_str]*”用于查看日志缓冲区的日志信息，参数“backward”和“forward”分别用于查看最近产生的日志和最先产生的日志信息。

```
AN(config)#show log buffer backward
start of buffer
<128>1 2012-07-17T06:35:26Z AN - - 100021002 - test message
```

命令“**clear log buffer**”用于清空日志缓冲区的日志信息。

```
AN(config)#clear log buffer
```

第18章 系统管理

18.1 管理工具

18.1.1 概述

本章将介绍如何使用设备的管理工具，包括如何下载新的 ArrayOS 软件，如何重启设备，如何将现有配置恢复到一个已保存的配置以及如何恢复到出厂预设状态等内容。

本章介绍的这些配置将关系到您的设备的运行情况及它与外部网络的关联。在 Web 接口上点击“管理工具”目录，您在那里可以找到一系列子目录允许您更改管理员口令、配置同步以及定义重启策略等。另外，您也可以通过命令行来设置这些功能。

18.1.2 管理工具配置

18.1.2.1 配置示例

18.1.2.1.1 配置系统维护

使用“**quit**”命令，您可以退出命令行模式。如果您想终止设备的所有网络交互，可以使用“**system shutdown**”命令。

```
AN(config)#system shutdown
```

运行该命令后，设备会显示一条警告信息，并询问您是否真的要关闭设备。输入“YES”回车，设备就开始关闭。在 60 秒后，使用者可以关闭设备了。

有时更改系统功能配置后，您可能需要重新启动设备。使用“**system reboot**”命令即可重启设备。

```
AN(config)#system reboot
```

18.1.2.1.2 配置文件维护

如果您想测试一些新的配置项，但又不想覆盖现有的配置，系统为您提供了配置文件的维护命令。通常，您可以使用“**write memory**”命令将运行配置保存到磁盘上。您还可以使用“**config file**”命令将现有的配置保存到指定的文件中。您还可以通过 TFTP 方式来导入或导出配置。

当您使用“**write memory**”命令时，请记住，设备重新启动后将会装载该命令所保存的配置。如果您更改配置项后想清除当前正在运行的配置，请使用“**clear config**”命令。

```
AN(config)#clear config all
```

现在设备已恢复到出厂的默认设置了。

在任何时候，如果您想导入以前保存的配置，您首先需要如上文所述的那样清除当前的运行配置。清除完成后，您可以导入新的配置。设备为您提供了三个可以保存配置的地方。

- “memory”：当设备重启时会加载该文件作为当前配置。
- “file”：可以保存各种不同的配置到磁盘文件上。
- “net”：可以保存配置文件到网络上的其它远程路径。

下面是保存和加载配置文件的三类命令。

```
AN(config)#write net tftp 10.10.0.3 default_config
```

如果想将配置文件重新导入并覆盖正在运行的配置文件，需要运行以下命令。

```
AN(config)#config memory
AN(config)#config file new_lb
AN(config)#config net tftp 10.10.0.3 default_config
```

如果您想查看某个特定的配置文件（将内容显示到屏幕），请在“**show config file**”命令后增加文件名：

```
AN(config)#show config file new_lb
```

当设备运行时加载一个已保存的配置时，请注意，保存的配置项是被合并到当前运行的配置项中。因此，您通常需要首先清除设备上某些相应的配置，然后再导入新的配置。例如，当前已经定义了五个后台服务器，然后执行“**config net tftp 10.10.0.3 default_config**”命令，如果将导入的配置文件中也定义了五个相同名称的后台服务器，那么您将得到一个错误提示，因为后台服务器名称不能重复。

18.1.2.1.3 软件升级程序

如果想查看当前 ArrayOS 的软件版本，请使用“**show version**”命令。

如果您想升级到新的版本，请使用以下步骤。

首先，请联系华耀客户支持获得软件和文档库的访问权。请联系您的华耀客户支持或发送 Email 到 support@arraynetworks.com.cn。

当您收到口令或者华耀客户支持的确认后，您就可以进行升级了，您可以首先从华耀公司的网站上下载软件包。您可以把下载的软件包放到本地的 Web 服务器或匿名的 FTP 服务器上。

建议您使用串口终端来进行 ArrayOS 升级。当您连接到终端后，您可以使用“**system update**”命令来更新。当前更新支持 HTTP 和 FTP 两种方式。两种方式的命令行相同，只是 URL 不同。

注意：如果您使用域名方式，如：system-update http://s5.sj.example.com 时，请确保设备上正确的配置了域名解析，您可以使用“**ip nameserver**”命令为“s5”主机定义域名解析服务器或者使用“**ip host**”命令为“s5”主机定义本地解析，否则您再下载映象时将收到一个错误信息。

接下来系统将关闭所有的负载均衡特性开始下载升级软件包，并进行确认，确认软件包来自华耀公司后开始安装。如果映象档有任何问题，将停止升级并在屏幕上给出错误提示，反之，您会获得升级成功的提示信息，并且设备将重新启动。重新启动后，您可以使用“**show version**”命令确认升级结果。

软件许可

设备的一些功能受到软件许可密钥的控制。如果您需要这些功能，请与华耀客户支持联系：support@arraynetworks.com.cn 来获得新的软件许可密钥。

18.1.2.1.4 XML RPC

XML 远程过程调用协议（Remote Procedure Call，RPC）功能通过给设备发送基于 HTTP 的请求或文件来工作。该方法允许传输多个参数到远端设备并将结果通过一个响应返回。通过该方法，大量复杂的配置仅通过一个操作就能传输，极大简化了配置过程。管理员可以使用管理接口 IP（仅支持 IPv4）通过 XML-RPC 访问设备。

如下图所示，客户端发送了一个 HTTP POST 请求到设备，XML-RPC 信息相当于这个 HTTP 请求的主体部分，包含了需要运行的命令和参数。设备对 XML-RPC 信息进行译码并提取相关的命令予以执行。最后，将执行的结果以 XML 代码的形式返回给客户端。

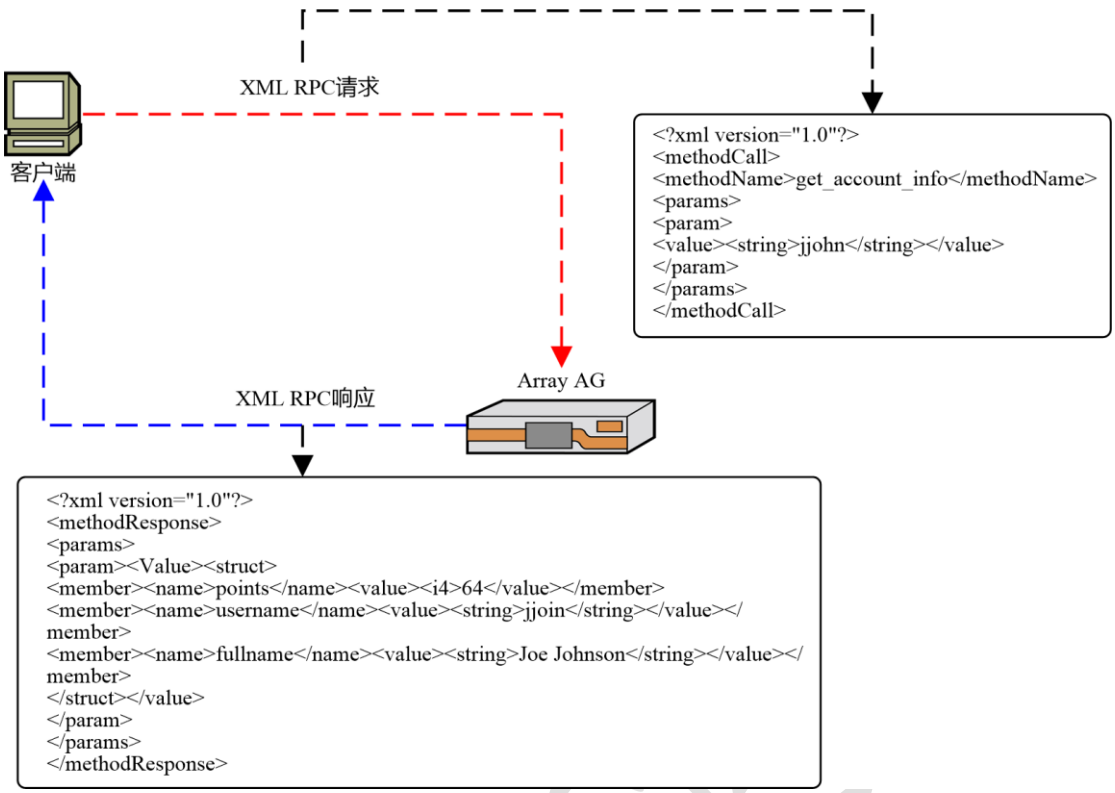

图18–1 XML RPC 工作机制

为了使用 XML-RPC 功能，需要使用如下格式的 XML 文件包含要在设备上执行的命令：

```
<?xml version="1.0" ?>
<methodCall>
<methodName>arrayos_cli_config</methodName>
<params>
<param>
<value>
<struct>
<member>
<name>enable_passwd</name>
<value>
<string>PASSWD</string>
</value>
</member>
<name>num</name>
<value>
<int>2</int>
</value>
</member>
<member>
<name>cli_string0</name>
```

```
<value>
<string>show version</string>
</value>
</member>
<member>
<name>cli_string1</name>
<value>
<string>vpn off</string>
</value>
</member>
</struct>
</value>
</param>
</params>
</methodCall>
```

下面是该文件的关键限制条件和要求：

“arrayos_cli_config”、“enable_passwd”、“username”、“password”、“num”和“cli_string”为固定值不能修改。

斜体样式的文本可以根据需要修改。上述斜体加粗样式的文本仅为示例。

- arrayos_cli_config：指定用于调用 CLI 命令的方法。关于该方法和支持的 XML-RPC 方法，请参见图 18‑5 附录 II。
- enable_passwd：“<string>*PASSWD*</string>”包含 enable 密码。（*PASSWD* 应该使用真正的 enable 密码代替；如果未使用命令“**passwd enable**”配置 enable 密码，请使用“<string/>”而非“<string> </string>”。）
- num：可选。该参数指定管理员需要设备执行的 CLI 命令的数量。在格式<int>X</int>输入值，其中 X 应该用要执行的 CLI 命令的真实数量值代替。如果未指定该参数，只有 cli_string0 指定的命令可被执行。
- cli_string0：指定索引为 0 的 CLI 命令。
- cli_stringN：指定索引为 N 的 CLI 命令。（N=X-1）
- （如果 num 为 4，cli_string 的后缀应为 0、1、2 和 3：cli_string0、cli_string1、cli_string2 和 cli_string3。）
- **show version** 和 **vpn off**：指定真实的 CLI 命令。可以被修改为 XML-RPC 支持的任何 CLI 命令。

我们可以使用下列命令来配置 XML RPC 功能。

1. 开启 XML RPC。

```
AN1(config)#xml on https
```

2. 配置 XML RPC 所监听的端口号。

```
AN1(config)#xml port 9999
```

18.1.2.1.5 远程管理

设备支持使用者使用 Telnet 和 SSH 协议连接到其他设备上进行远程管理工作，协助使用者远程排查其他设备上的问题和故障。

在设备上运行命令“**telnet** *"host port""*”来使用 Telnet 功能，如下所示：

```
AN#telnet “‘172.16.2.182 -4’”
Trying 172.16.2.182...
Connected to 172.16.2.182 -4.
Escape character is '^]'.
Trying SRA secure login:
User (root): admin
Password:
[ SRA accepts you ].....succeed
```

在设备上运行命令“**ssh remote** *“user@hostname”*”来使用 SSH 功能，如下所示：

```
AN#ssh remote "root@172.16.85.240"
root@172.16.85.240's password:
Linux libh-server1 2.6.32-22-generic #33-Ubuntu SMP Wed Apr 28 13:27:30 UTC 2010 i686
GNU/Linux

Welcome to Ylmf_OS!
 * Information:    http://www.ylmf.com/

0 packages can be updated.
0 updates are security updates.

Last login: Wed Apr 20 00:39:35 2011 from 10.3.46.1
```

18.2 SNMP

简单网络管理协议（Simple Network Management Protocol，SNMP）框架包括如下三部分：

- 网络管理系统（Network Management System，NMS）：NMS 是控制和监控使用 SNMP 协议的网络主机活动的系统。
- SNMP 代理：SNMP 代理是被管理设备中的软件模块，用于维护设备数据并在需要时上报这些数据给管理设备。

- 管理信息库（Management Information Base，MIB）：MIB 是用于管理信息的虚拟信息存储区域，包括 SNMP 代理的被管理的对象。

系统支持 SNMP 功能。当 SNMP 功能启用后，SNMP 代理将在系统中启用。华耀提供了一个专有的 MIB 文件，包含了设备的被管理对象。每个被管理对象都有唯一的对象标识符（Object ID，OID）。关于设备支持的 SNMP OID 的更多信息，请参见命令行使用手册中的 SNMP OID 列表。

SNMP 代理支持的 SNMP 版本有 v1、v2c 和 v3。目前 SNMP 代理可以提供如下功能：

- 响应来自于 NMS 的 SNMP GET 请求
- 给 NMS 发送 SNMP Trap 消息
- 系统支持 IPv4 NMS 和 IPv6 NMS。

18.2.1 SNMP 请求

下图展示了 SNMP GET 请求的流程。

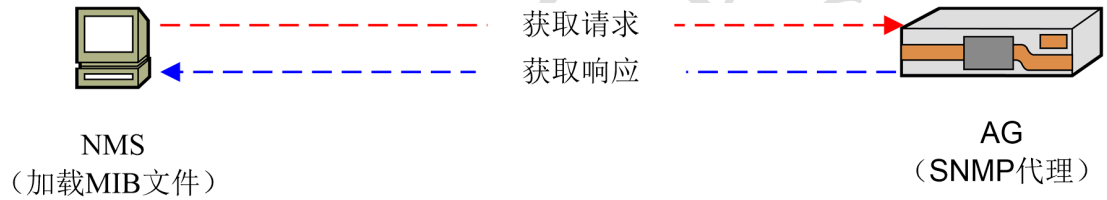

图18–2 SNMP GET 请求

将设备的 MIB 文件导入到 NMS 并正确设置 SNMP 参数后，NMS 用户可以发起 SNMP GET 请求获取 MIB 文件中的 OID 值。然后，设备上的 SNMP 代理将通过发送 SNMP GET 响应返回查询的 OID 值。

当使用 SNMP v3 时，SNMP 代理可以支持基于用户的安全模型（User-Based Security Model，USM）和基于视图的访问控制模型（View-Based Access Control Model，VACM）。USM 可以为 SNMP 消息提供用户认证和私密性；VACM 可以提供基于 IP 的 SNMP 访问控制。在使用 SNMP v3 时可以使用这两个安全模型。

- 使用 USM 时，SNMP 代理只响应来自于使用 SNMP v3 用户账户的 NMS 发送的 SNMP GET 请求。因而，要使用 USM，需要在系统中为 NMS 创建 SNMP v3 用户账户。最多可以创建 16 个 SNMP v3 用户账户。
- 使用 VACM 时，只有当 SNMP GET 请求的源 IP 地址匹配任意一条配置的允许 SNMP 访问控制规则时，SNMP 代理才会响应该 SNMP GET 请求。因而，要使用 VACM，需要启用基于 IP 的 SNMP 访问控制功能并配置允许 SNMP 访问控制规则。

18.2.2 SNMP Trap

下图展示了 SNMP Trap 的流程。

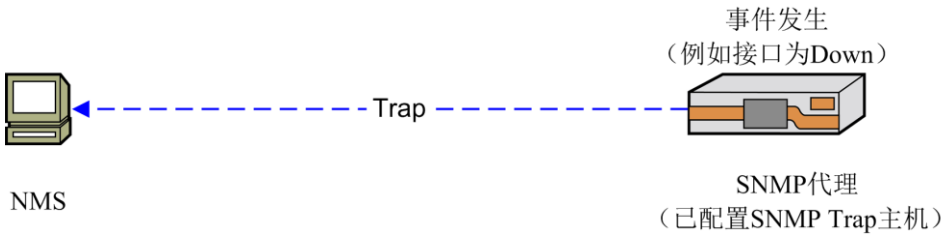

图18–3 SNMP Trap

当满足以下任意条件时，SNMP 代理将发送 SNMP Trap 到 NMS：

- 接口状态为 down 或 up 时
- 有错误（error）或更高级别的系统日志生成时
- 许可证将在 15 天内过期时
- 系统启动时
- 系统关闭时

为了让 NMS 能接收 SNMP 代理的 SNMP Trap，需要在设备上将 NMS 配置为 SNMP Trap 主机。最多可以配置 10 个 SNMP Trap 主机。

注意：NMS 不会给 SNMP 代理重新发送响应，SNMP 代理也不会给 NMS 重新发送 SNMP Trap。因而，请确保使用命令“**snmp host**”配置的 SNMP Trap 主机是可达的。

18.2.3 配置示例

18.2.3.1 配置 SNMP 代理

➢ **CLI 配置示例**

1. 为 SNMP 代理设置 Community 字符串，例如：

```
AN(config)#snmp community privatepassword
```

2. （可选）设置 SNMP 代理的联系方式。

```
AN(config)#snmp contact admin
```

3. （可选）设置 SNMP 代理的物理位置。

```
AN(config)#snmp location Beijing
```

4. （可选）配置 SNMP 访问控制，例如：

```
AN(config)#snmp ipcontrol on
AN(config)#snmp ippermit 192.168.0.0 255.255.0.0
```

5. 在设备上启用 SNMP 代理，例如启用支持 SNMP v3 的 SNMP 代理:

```
AN(config)#snmp on v3
```

6. 要启用支持 SNMP v1 和 SNMP v2c 的 SNMP 代理，执行命令“**snmp on default**”。

7. 配置一个 SNMP v3 用户。

```
AN(config)#snmp v3user test test authNopriv
```

18.2.3.2 配置 SNMP Traps

➢ **CLI 配置示例**

- （可选）配置 SNMP Trap 主机，例如：

```
AN(config)#snmp host 11.1.1.20 3 "ryan" "14" "1234567855" authNopriv
```

- （可选）启用 SNMP Trap 服务，例如：

```
AN(config)#snmp enable traps
```

18.3 管理员设置和权限管理

18.3.1 WebUI 双因素认证登录

身份认证涉及三方面要素，即需记忆的身份认证内容（如密码）、认证设备（如 USB Key）和本身特征（如指纹）。由于传统的帐号密码登录方式只涉及单一的认证要素，存在被盗或泄漏的风险。为增强 WebUI 客户端登录的安全性，系统支持 WebUI 双因素认证，以此来提升设备安全访问的强度。

目前，系统已支持使用第三方 USB Key 设备作为认证设备来实现双因素认证。要为特定用户启用 WebUI 双因素认证功能，管理员必须在 USB Key 设备中导入证书，并将证书与用户账号进行绑定，最后再为此用户启用 WebUI 双因素认证功能。下次登录设备 WebUI 时，该用户必须输入帐号密码和 USB Key 的 PIN 码向认证服务器请求身份认证信息才能登录设备。

注意：

- 该功能目前支持龙脉 USB Key 设备。

- 系统目前支持使用 SM2 算法加密的公钥证书。

➢ **启用 USB Key 认证的配置流程**

1. 安装 USB Key 管理工具并导入证书。

   在使用 USB Key 访问设备前，管理员需要安装相应的 USB Key 管理工具（认证客户端软件 GM3000）。管理员需要通过该管理工具导入证书，修改初始 PIN 码。

2. 安装 WebUI 插件。

   打开 WebUI 登录界面，根据提示安装认证插件。该插件用于实现浏览器和 USB Key 管理工具的交互。安装该插件后，将能在 WebUI 中查看导入 USB Key 设备的证书。

3. 绑定证书与用户。

   安装完 WebUI 插件后，在**系统>用户管理>系统管理员>WebUI 双因素认证**页面点击**绑定证书**。在弹出的**绑定证书**窗口，选择证书，然后点击**绑定证书**。

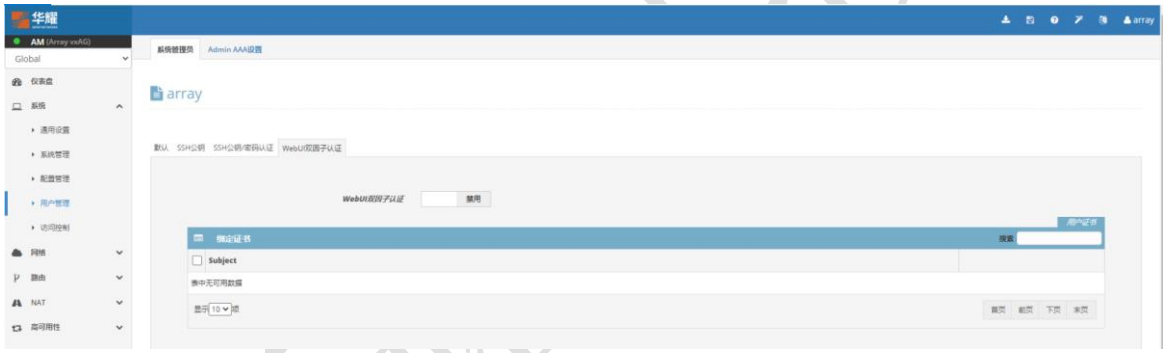

图18–4 绑定证书

4. 启用 WebUI 双因素认证功能。

   在**系统>用户管理>系统管理员>WebUI 双因素认证**页面（见上图）将 **WebUI 双因素认证**滑块置为**启用**。启用该功能后，指定用户在下次登录 WebUI 时，将必须使用 USB Key 通过双因素认证身份信息。选择 USB Key 登录模式，登录界面将变成如下状态：

图18－5 登录界面

注意：如果是 UOS 系统用户，需要在浏览器中完成以下配置：

- 在浏览器中导入 rootca 证书。
- 启用 TSL1.0 和 TSL1.1。

➢ 用户通过 USB Key 访问 WebUI 流程

完成上述配置并启用双因素认证后，用户访问 WebUI 流程如下：

1. 启动 USB Key 管理工具。
2. 将 USB Key 插入要访问 WebUI 的本地设备。
3. 打开 WebUI 登录界面，输入用户帐号密码和 USB Key 的 PIN 码，确认登录。

附录I 缩略语

缩写	全称	中文
AAA	Authentication, Authorization & Accounting	验证、授权和统计
ACL	Access Control List	访问控制列表
API	Application Programming Interface	应用程序编程接口
ARP	Address Resolution Protocol	地址解析协议
ASCII	American Standard Code for Information Interchange	美国信息交换标准码
ASN.1	Abstract Syntax Notation One	抽象语法标记
ATCP	Array TCP	华耀 TCP
CA	Certificate Authority	认证中心
CDN	Content Distribution Network	内容分发网络
CDP	CRL Distribution Point	CRL 分发点
CGI	Common Gateway Interface	公共网关接口
CLI	Command Line Interface	命令行接口
CNAME	Canonical Name	别名
CPS	Connections Per Second	每秒连接数
CPU	Central Processing Unit	中央处理器
CRC	Cyclic Redundancy Check	循环冗余校验
CRL	Certificate Revocation List	证书撤销列表
CRS	Core Rule Set	核心规则集
CSR	Certificate Signing Request	证书签发请求
DMZ	DeMilitarized Zone	隔离区
DNS	Domain Name System	域名服务系统
DoS	Denial Of Service	拒绝服务攻击
DPS	Dynamic Proximity System	动态邻接系统
FIFO	First-In First-Out	先入先出(法)
FTP	File Transfer Protocol	文件传输协议
FTPS	FTP over SSL	安全文件传输协议
GMT	Greenwich Mean Time	格林威治标准时间
GRE	Generic Routing Encapsulation	通用路由封装
HA	High Availability	高可用性
HC	Health Check	健康检查
HTML	HyperText Markup Language	超文本标记语言
HTTP	HyperText Transfer Protocol	超文本传输协议
HTTPS	HyperText Transfer Protocol over Secure Sockets Layer	安全超文本传输协议
ICMP	Internet Control Message Protocol	因特网控制报文协议
ICMPv6	Internet Control Message Protocol version 6	因特网控制报文协议第六版
IEEE	Institute of Electrical and Electronics Engineers	美国电气和电子工程师学会

IETF	Internet Engineering Task Force	因特网工程任务组
IIS	Internet Information Server	因特网信息服务器
IMS	Information Management System	信息管理系统
IP	Internet Protocol	因特网协议
ISP	Internet Service Provider	因特网服务供货商
LACP	Link Aggregation Control Protocol	链路汇聚控制协议
LAN	Local Area Network	局域网
LDAP	Lightweight Directory Access Protocol	轻量级目录访问协议
LED	Light Emitting Diode	发光二极管显示器
Local DNS	Local Domain Name System	本地域名服务
MAC	Media Access Control	媒体访问控制
MIB	Management Information Base	管理信息库
MIME	Multipurpose Internet Mail Extensions	多用途因特网邮件扩展
MNET	Multi-Netting	多地址端口
MTU	Maximum Transmission Unit	最大传输单元
NAT	Network Address Translation	网络地址转换
NDP	Neighbor Discovery Protocol	邻居发现协议
NIC	Network Interface Card	网络适配器
NMS	Network Management Station	网络管理站
NTP	Network Time Protocol	网络时间协议
NUMA	Non-uniform Memory Access	非一致性内存访问
OCSP	Online Certificate Status Protocol	在线证书状态协议
OID	Object Identifier	对象标识符
OSI	Open System Interconnection	开放式系统互连模型
OSPF	Open Shortest Path First	开放式最短路径优先协议
OSPFv2	Open Shortest Path First version 2	开放式最短路径优先协议第二版
OSPFv3	Open Shortest Path First version 3	开放式最短路径优先协议第三版
OWA	Outlook Web Access	基于微软 Hosted Exchange 技术的托管邮局的一项 Web 访问功能
PCI	Peripheral Component Interface	外围组件接口
PEM	Privacy Enhanced Mail	增强保密的邮件
PHY	Physical Layer	物理层
PKI	Public Key Infrastructure	公钥基础架构
PLR	Packet Loss Rate	丢包率
POP3	Post Office Protocol - Version 3	邮局协议-版本 3
PPP	Point-to-Point Protocol	点到点协议
PPTP	Point-to-Point Tunneling Protocol	点到点隧道协议
PST	Pacific Standard Time	太平洋标准时间
QoS	Quality of Service	服务质量
RADIUS	Remote Authentication Dial-In User Service	远程用户拨入认证系统

RAM	Random Access Memory	随机存取内存
RDP	Remote Desktop Protocol	远程桌面协议
RFC	Request For Comments	请求注解
RHI	Route Health Injection	路由健康注入
RIPv2	Routing Information Protocol version 2	路由选择信息协议第二版
RPS	Requests Per Second	每秒请求数
RTS	Return to Sender	原链路返回
RTSP	Real Time Streaming Protocol	实时流媒体协议
RTT	Round Trip Time	往返时间
SCP	Session Control Protocol	会话控制协议
SIP	Session Initiation Protocol	会话初始化协定
SMTP	Simple Mail Transfer Protocol	简单邮件传输协议
SOAP	Simple Object Access Protocol	简单对象访问协议
SQL	Structured Query Language	结构化查询语言
SSF	Stateful Session Failover	链接同步
SSH	Secure Shell Protocol	安全外壳协议
SSL	Secure Sockets Layer	安全套接字层
SSLv3	Secure Sockets Layer version 3	安全套接字层第三版
SSO	Single Sign On	单点登录
TACACS	Terminal Access Controller Access Control System	终端访问控制器访问控制系统
TCI	Tag Control Information	标记控制信息
TCL	Tools Command Language	工具命令语言
TCP	Transmission Control Protocol	传输控制协议
TCPS	TCP with SSL	安全 TCP
TELNET	Terminal Emulation Protocol in a TCP/IP Environment	TCP/IP 终端模拟协议
TFTP	Trivial File Transfer Protocol	简单文件传输协议
TLS	Transport Layer Security Protocol	传输层安全协议
TPID	Tag Protocol Identifier	标签协议标识
TTL	Time to Live	生存时间
UDP	User Datagram Protocol	用户数据报协议
URL	Uniform Resource Locator	统一资源定位符
VCID	Virtual Cluster ID	虚拟集群标识
VIP	Virtual IP	虚拟 IP 地址
VLAN	Virtual Local Area Network	虚拟局域网
VOD	Video On Demand	视频点播
VoIP	Voice over Internet Protocol	基于 IP 的语音传输
VRRP	Virtual Router Redundancy Protocol	虚拟路由冗余协议
WebUI	Web User Interface	Web 用户接口
WELF	WebTrends Enhanced Log Format	国际通行的防火墙日志规范格式
XSS	Cross Site Scripting	跨站脚本攻击

附录II XML RPC 方法

一般 XML RPC 方法				
方法名称	命令行	{参数名称，参数类型}	可选参数	注意事项
arrayos_cli_enable	所有 Enable 模式下的命令	{num,int}, {cli_string0,string}, {cli_string1,string}, {cli_string2,string}, {cli_string3, string} ……	num	如果没有设置参数“num”值，那么其默认值为 1，则必须配置“cli_string0”。CLI 命令的名称必须从“cli_string0”到“cli_string{n-1}”结束。如果中间的CLI命令丢失，XML RPC 系统将忽略这个问题，并且不会报错。
arrayos_cli_config	所有 Config 模式下的命令			
arrayos_cli_config_with_input	所有 Config 模式下的命令	{cli_string, string}, {num, int}, {input_string0, string}, {input_string1, string} ...	num, input_string0, input_string1, ...	如果要调用交互式 CLI 命令（例如输入“YES”来继续执行命令），则必须使用该方法。本方法一次只能执行一条 CLI 命令。如果没有设置参数“num”则其默认值为 1。参数“input_string”从“input_string0”开始到“input_string(num-1)”，如果中间丢失“input_string(n)”，则其默认值为空。如果 CLI 要求在此处必须输入一个有效的值，那么此次调用可能挂起或返回错误。本方法一次只能执行一条 CLI 命令。