UNIS NGIPS 8000[T1000-CN-G][T1000-E]

系列入侵防御系统

典型配置举例

紫光恒越技术有限公司
www.unisyue.com

资料版本：5W101-20210610

前 言

本手册详细介绍了此产品常用功能的典型方案和具体配置步骤。

前言部分包含如下内容：

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1. 命令行格式约定

格　式	意　义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | … }	表示从多个选项中仅选取一个。
[x | y | …]	表示从多个选项中选取一个或者不选。
{ x | y | … }*	表示从多个选项中至少选取一个。
[x | y | …]*	表示从多个选项中选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1～n次。
#	由“#”号开始的行表示为注释行。

2. 图形界面格式约定

格　式	意　义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[ ]	带方括号“[ ]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
说明	对操作内容的描述进行必要的补充和说明。
窍门	配置、操作、或使用设备的技巧、小窍门。

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其它运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。
	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 端口编号示例约定

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

产品配套资料

本产品的配套资料包括如下部分：

大类	资料名称	内容介绍
硬件描述硬件描述与安装与安装	安全兼容性手册	列出产品的兼容性声明，并对兼容性和安全的细节进行说明
	快速入门	指导您对设备进行初始安装、配置，通常针对最常用的情况，减少您的检索时间
	安装指导	帮助您详细了解设备硬件规格和安装方法，指导您对设备进行安装
业务配置	配置指导	帮助您掌握设备软件功能的配置方法及配置步骤
	命令参考	详细介绍设备的命令，相当于命令字典，方便您查阅各个命令的功能
	典型配置举例	帮助您了解产品的典型应用和推荐配置，从组网需求、组网图、配置步骤几方面进行介绍
运行维护	版本说明书	帮助您了解产品版本的相关信息（包括：版本配套说明、兼容性说明、特性变更说明、技术支持信息）及软件升级方法

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：info@unisyue.com

感谢您的反馈，让我们做得更好！

目录

1 简介

本文档介绍设备的行为审计配置举例，包括 HTTP 类行为审计、邮件类行为审计、即时通讯类行为审计、网络基础协议类行为审计、娱乐股票类行为审计和网络应用其它应用行为审计。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解行为审计特性。

3 使用限制

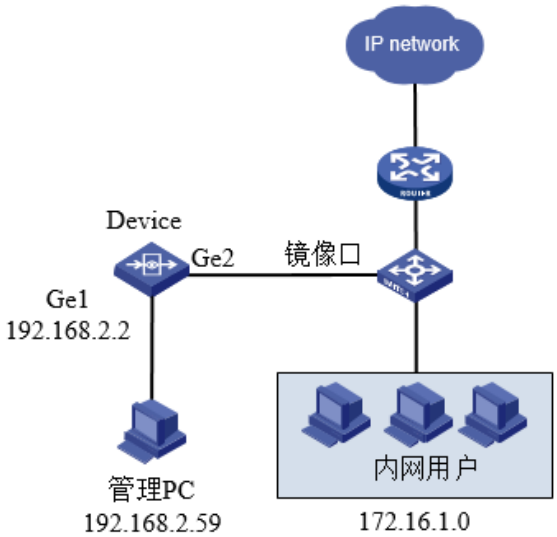
设备对于采用私有算法进行加密的应用，无法审计其内容，例如无法审计 QQ 聊天内容。

4 审计策略配置举例

4.1 组网需求

如图 1 所示，某公司使用设备以旁挂方式部署于核心设备旁边，将用户上网的流量通过端口镜像的方式镜像至设备的旁路接口，对用户上网行为进行分析与审计。旁路模式不修改网络结构，不关心网络细节，关机也不掉线，不会影响企业内部网络，部署简单。

图1 审计功能配置组网图



4.2 配置思路

- 配置设备接口地址。
- 配置设备旁路部署。
- 配置审计策略。

4.3 使用版本

本举例是在 E6201 版本上进行配置和验证的。

4.4 配置注意事项

- 一般情况下，目前应用都是应用行为进行审计，如果是 HTTPS 访问的应用，则需要优先配置 HTTPS 解密策略，优先进行解密才能进一步进行审计。
- 旁路部署模式下，不支持 HTTPS 解密策略。
- 审计策略匹配是由上至下进行匹配，策略匹配到之后将不会往下继续匹配。

4.5 配置步骤

4.5.1 配置设备

1. 配置网络接口

如图 2 所示，进入“网络配置>接口配置>物理接口”，点击 ge1<编辑>按钮，配置 ge1 的 IP 地址为 192.168.2.2/24。

图2 配置接口地址

(2) 配置部署方式

如图 3 所示，进入“网络配置>基础网络>部署方式”，配置勾选 ge2 口启用。

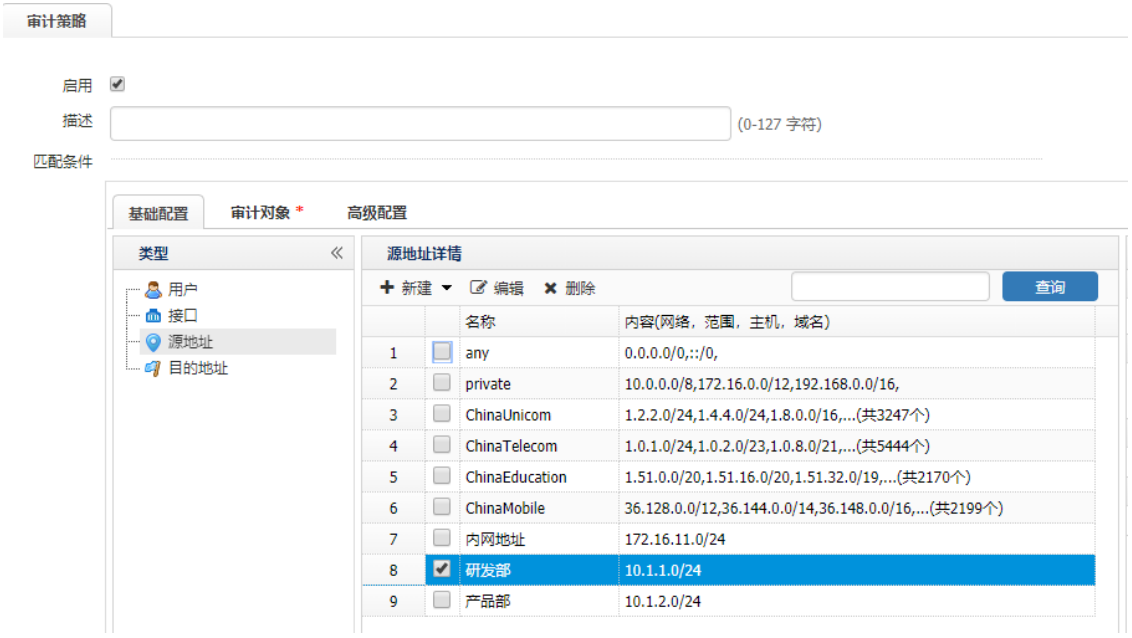
图3 配置部署方式

2. 配置审计策略

(1) 配置研发部审计策略

如图 4 所示，进入“策略配置>审计策略”，点击<新建>，“源地址”配置为研发部，然后点击“审计对象”页面。

图4 配置研发部审计策略



如下图所示，进入“策略配置>审计策略”，点击<新建>配置审计策略，然后点击“审计对象”页面，审计对象选择全部（审计用户上网行为并记录日志），最后单击“提交”提交配置。

图5 配置所有审计对象

如图 6 所示，创建成功的产品部审计策略配置如下。

图6 审计策略配置成功

4.6 验证配置

内网用户进行上网操作，选择“数据中心>日志中心>审计日志”，选择需要查看的日志类型，可以查看到相应的审计日志。如图 7 所示。

图7 产品部 IM 聊天软件日志


访问网站日志

查询 重置 导出 **查询结果:** 在 2020-09-06 约 14578 条日志记录中，从 1 - 14578 搜索出相关结果 14578 条

	用户	用户mac	URL分类	网页标题	URL	级别	时间	操作
1		00:ac:20:08:02:07	IP站点	Vulnerability: Brute Force :: Damn Vu		告警	2020-09-06 13:42:31	详细
2		00:ac:20:08:02:44	IP站点	Vulnerability: Brute Force :: Damn Vu		告警	2020-09-06 13:42:28	详细
3		00:ac:20:03:02:15	IP站点	Vulnerability: Brute Force :: Damn Vu		告警	2020-09-06 13:42:15	详细
4		00:00:b5:11:73:f2	IP站点	Vulnerability: Brute Force :: Damn Vu		告警	2020-09-06 13:42:13	详细
5		00:ac:20:08:02:52	IP站点	Vulnerability: Brute Force :: Damn Vu		告警	2020-09-06 13:42:13	详细
6		00:ac:20:03:02:60	IP站点	Vulnerability: Brute Force :: Damn Vu		告警	2020-09-06 13:42:11	详细
7		00:00:b5:11:73:fe	IP站点	Vulnerability: Brute Force :: Damn Vu		告警	2020-09-06 13:42:09	详细

目录

1 简介

本文档介绍设备的用户认证配置举例，包括本地用户 Web 认证、Radius 联动 Web 认证和 LDAP 联动 Web 认证。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解用户认证特性。

3 使用限制

设备的 E6201 版本仅支持与 AD 域服务器联动认证，与 openldap 服务器联动仅支持用户同步不支持认证，在配置使用时请使用 AD 域服务器联动认证。

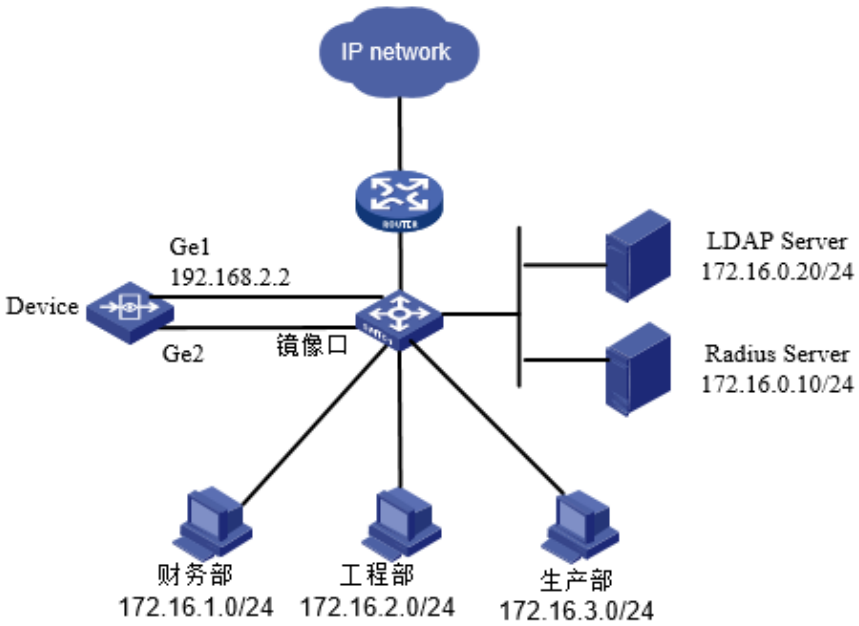
4 用户认证配置举例

4.1 组网需求

如图 1 所示，某公司；财务部、工程部和生产部实行用户认证上网，其网段分别是 172.16.1.0/24、172.16.2.0/24 和 172.16.3.0/24。内网 Radius 服务器的地址为 172.16.0.10/24、LDAP 服务器的地址为 172.16.0.20/24。使用设备以旁挂方式部署于核心设备旁边，将用户上网的流量通过端口镜像的方式镜像至设备的旁路接口，在设备上配置用户认证功能。具体要求如下：

- 财务部进行 Web 认证上网，用户名和密码存储在设备的本地。
- 工程部进行 Web 认证上网，用户名和密码存储在 Radius 服务器上。
- 生产部进行 Web 认证上网，用户名和密码存储在 LDAP 服务器上。
- 财务部、工程部和生产部的每个 Web 认证用户需要支持两个终端同时并发登录，要求用户成功登录后跳转到 http://www.baidu.com。

图1 用户认证功能配置组网图



4.2 配置思路

- 基本网络配置。
- 开启旁路认证。
- 配置 Radius 和 LDAP 服务器对象，设备上的相关参数配置需要和服务器保持一致。
- 配置地址对象。
- 配置本地认证用户，RADIUS 和 LDAP 认证用户直接在相应的服务器创建即可。
- 配置用户认证策略。

4.3 使用版本

本举例是在 E6201 版本上进行配置和验证的。

4.4 配置注意事项

- 设备的配置 Web 认证时，允许用户的 TCP 三次握手报文、DNS 报文以及 ICMP 报文通过，当检测到用户 HTTP 报文时拦截并弹出认证页面。所以，在使用 Web 认证功能时，需要保证终端可以进行正常的 HTTP 访问。
- 如果需要实现访问某些资源时免 Web 认证，请在对应用户策略的目的地址对象中配置排除地址，将需要免认证访问的目的 IP 地址排除即可。
- 旁路部署时，认证策略和控制策略的源接口以及目的接口必须配置接收镜像流量的旁路部署接口或者是 any。

- 旁路认证务必保证旁路设备到上网 PC 可达，否则功能无法使用。
- 旁路认证只对于 HTTP 流量生效。

4.5 配置步骤

4.5.1 配置设备

1. 配置基础网络

(1) 配置网络接口

如图 2 所示，进入“网络配置>接口配置>物理接口”，点击 ge1<编辑>按钮，配置 ge1 的 IP 地址为 192.168.2.2/24。

图2 配置接口地址

(2) 配置静态路由

进入“网络配置 > 路由管理 > 静态路由”，进入 IPv4 静态路由页面，点击“新建”配置静态路由，最后点击“提交”提交配置，如下图所示。

图3 配置静态路由

(3) 配置部署方式

如图 4 所示，进入“网络配置>基础网络>部署方式”，配置勾选 ge2 口启用。

图4 配置部署方式

2. 配置旁路认证

如图 5 所示，进入“网络配置>基础网络>部署方式>高级配置”，开启旁路认证。

图5 配置旁路认证和旁路阻断

3. 添加服务器

(1) 配置工程部 Radius 服务器

如图 6 所示，进入“用户管理>认证管理>认证服务器”，点击<新建>，选择 Radius 服务器，配置“服务器地址”为 172.16.0.10，“服务器密码”和“端口”需要和 Radius 服务器保持一致，点击<提交>。

图6 添加工程部 radius 服务器

(2) 配置生产部 LDAP 服务器

如图 7 所示，进入“用户管理>认证管理>认证服务器>”，点击<新建>选择 LDAP 服务器，配置“服务器地址”为 172.16.0.20，“端口”和“通用名标识”和“Base DN”需要和 LDAP 服务器保持一致，点击<提交>。

图7 添加生产部 LDAP 服务器

4. 配置 Web 认证用户

(1) 配置市场部本地认证用户

如图 8 所示，进入“用户管理>用户组织结构”，点击“新建>用户”，配置用户名称为“user1”，配置和确认密码后，点击<提交>。

图8 配置市场部本地认证用户

(2) 配置工程部 Radius 认证用户

设备本地不需要创建 Radius 认证用户，直接在 Radius 服务器上创建即可。

(3) 配置生产部 LDAP 认证用户

设备本地不需要创建 LDAP 认证用户，直接在 LDAP 服务器上创建即可。

如图 9 所示，添加完成的认证用户对象配置如下。

图9 Web 认证用户对象配置完成

5. 配置用户认证地址对象

(1) 配置财务部地址对象

如图 10 所示，进入“策略配置>对象管理>地址对象>地址对象”，点击<新建>，命名为“财务部地址对象”，“地址项目”选为子网地址，配置地址为 172.16.1.0/24，点击<提交>。

图10 配置财务部地址对象

(2) 配置工程部地址对象

如图 11 所示，进入“策略配置>对象管理>地址对象>地址对象”，点击<新建>，命名为“工程部地址对象”，“地址项目”选为子网地址，配置地址为 172.16.2.0/24，点击<提交>。

图11 配置工程部地址对象

(3) 配置生产部地址对象

如图 12 所示，进入“策略配置>对象管理>地址对象>地址对象”，点击<新建>，命名为“生产部地址对象”，“地址项目”选为子网地址，配置地址为 172.16.3.0/24，点击<提交>。

图12 配置生产部地址对象

如图 13所示，创建完成的地址对象配置如下。

图13 用户认证地址对象配置完成

6. 配置 Web 认证参数

如图 14所示，进入“用户管理>认证管理>认证方式>本地 WEB 认证”，勾选“允许重复登录”，配置“允许登录数”为 2，配置重定向 URL 为 https://www.baidu.com，点击<提交>。

图14 配置 Web 认证

7. 配置控制策略

如图 15 所示，进入“策略配置>控制策略”，将默认规则修改为允许。

图15 配置控制策略

8. 配置用户认证策略

(1) 配置财务部用户认证策略

如图 16 所示，进入“用户管理>认证管理>认证策略”，点击<新建>，源地址配置为“财务部地址对象”，认证方式选择“本地 WEB 认证”，其它选项保持默认，点击<提交>。

图16 配置财务部用户认证策略

(2) 配置工程部用户策略

如图 17 所示，进入“用户管理>认证管理>认证策略”，点击<新建>，源地址配置为“工程部地址对象”，认证方式选择“本地 WEB 认证”，其它选项保持默认，点击<提交>。

图17 配置工程部用户认证策略

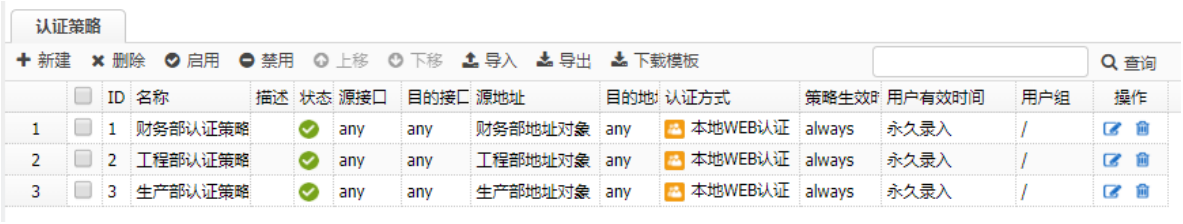
(3) 配置生产部用户认证策略

如图 18 所示，进入“用户管理>认证管理>认证策略”，点击<新建>，源地址配置为“生产部地址对象”，认证方式选择“本地 WEB 认证”，其它选项保持默认，点击<提交>。

图18 配置生产部用户认证策略

如图 19 所示，添加完成的用户策略配置如下。

图19 用户策略配置完成



9. 启用第三方认证

如图 20、图 21 所示，进入“用户管理>认证管理>高级选项>全局配置”，当与 Radius 服务器认证对接时，启用 Radius 方式，当与 LDAP 服务器认证对接时，启用 LDAP 服务器。

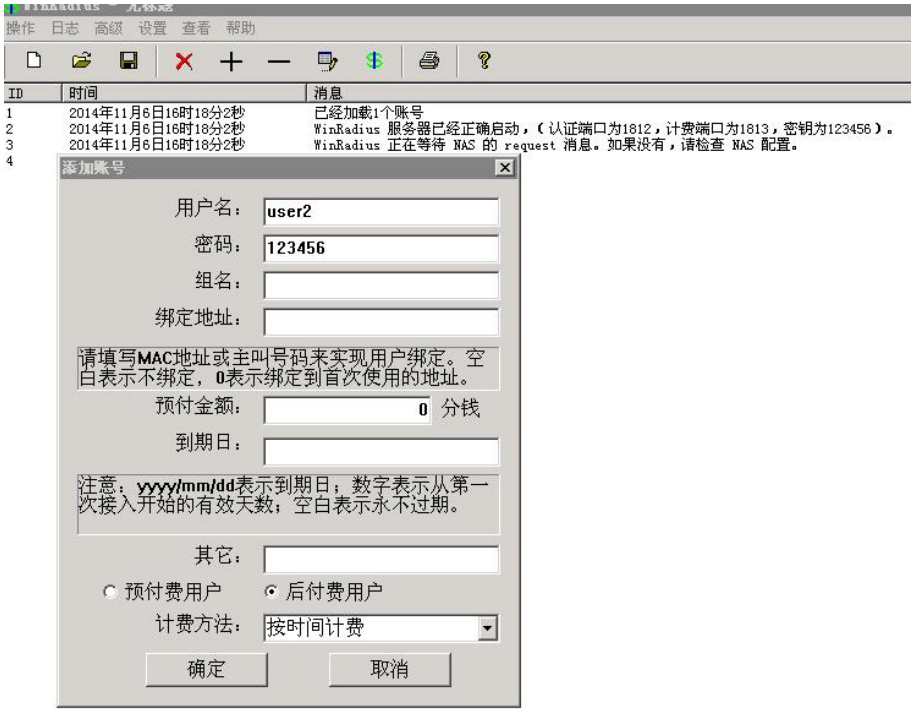
图20 启用第三方认证 Radius

图21 启用第三方认证 LDAP

10. 配置 Radius 服务器

如图 22 所示，以 WinRadius 为例搭建 Radius 服务器，点击<操作>，配置用户名为 user2，密码为 123456，点击<确定>。

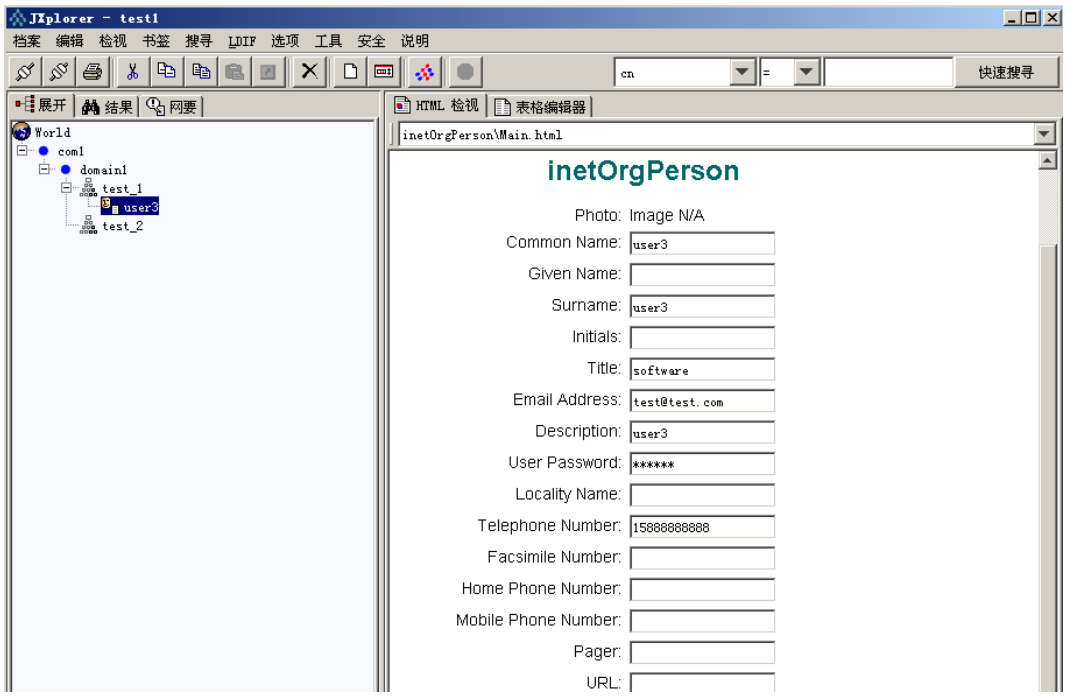
图22 配置 Radius 服务器



11. 配置 LDAP 服务器

如图 23 所示，在 LDAP 服务器上配置 Common Name 和 Sumname 为 user3，User Password 为 123456。

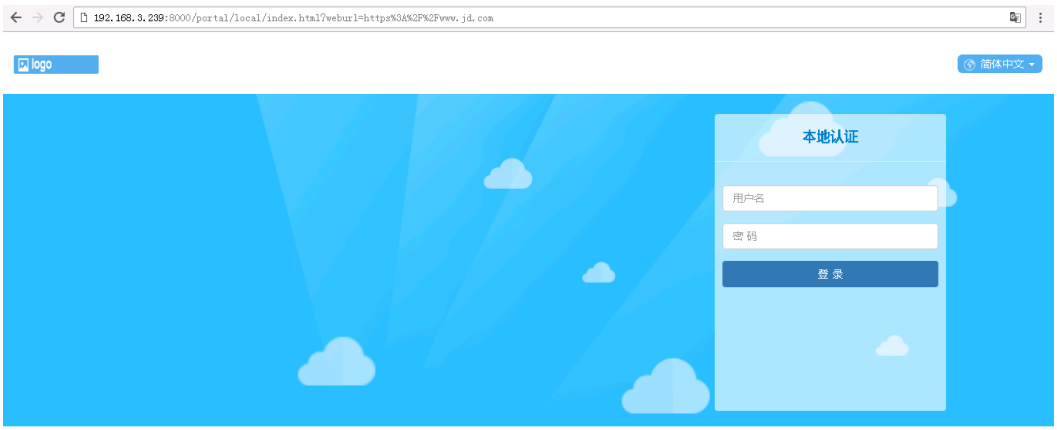
图23 配置 LDAP 服务器



4.6 验证配置

如图 24 所示，在每个网段使用终端进行 HTTP 访问，弹出如下本地 Web 认证页面，填写用户名和密码进行认证。

图24 本地 Web 认证页面



如图 25 所示，财务部（172.16.1.0/24）本地用户 user1 测试认证成功。

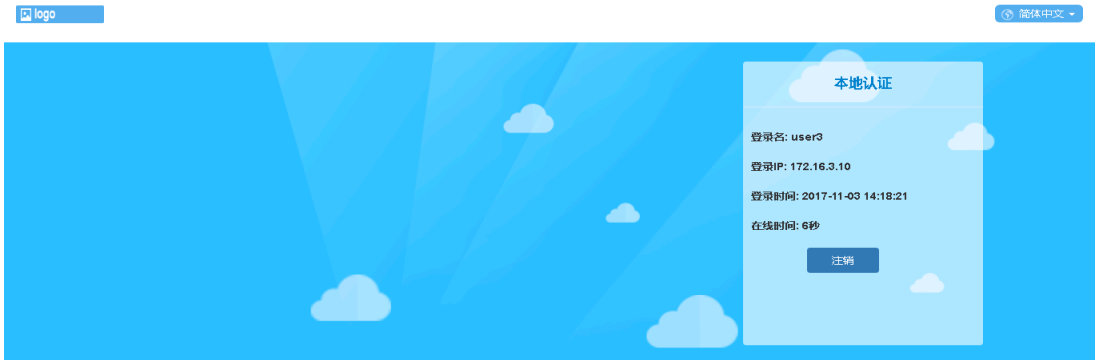
图25 财务部本地 Web 认证成功

如图 26 所示，工程部（172.16.2.0/24）Radius 联动用户 user2 测试认证成功。

图26 Radius 联动用户 Web 认证成功

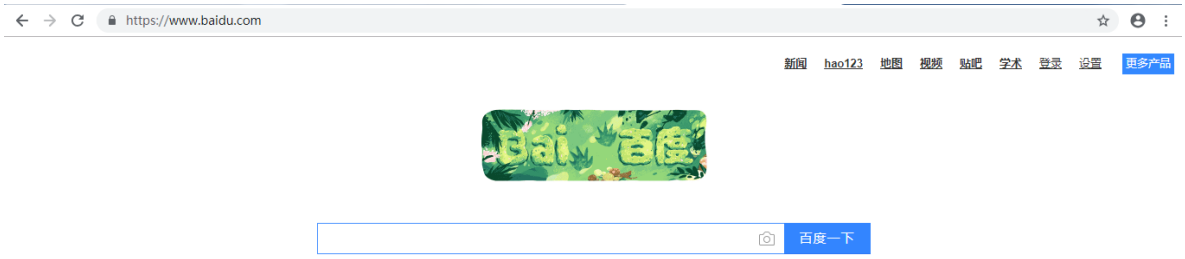
如图 27 所示，生产部（172.16.3.0/24）LDAP 联动用户 user3 测试认证成功。

图27 LDAP 联动用户 Web 认证成功



如图 28 所示，用户 Web 认证通过后跳转到配置的 https://www.baidu.com。

图28 Web 认证通过后重定向到 www.baidu.com



目 录

1 简介

本文档介绍设备用户同步配置举例，用户同步包含 LDAP 同步、ARP 扫描、SNMP 同步。同步成功录入设备的用户支持策略调用、QOS 控制、策略路由等模块的引用控制。本文档主要针对用户同步中的 LDAP 同步和 SNMP 同步进行典型配置举例介绍。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解用户同步特性。

针对 SNMP 同步在配置前，需要做如下准备：

- 交换机上已开启 SNMP 代理功能。
- 设备的与交换机网络可达。

3 使用限制

- LDAP 同步条目 128。
- SNMP 同步条目 64。
- Arp 扫描条目 64。
- LDAP 仅支持简单模式的联动认证，不支持匿名和通用模式的联动认证。
- LDAP 服务器用户名长度大于 63 字符后无法录入。
- LDAP 服务器同步目前支持 389 明文传输，不支持 636 密文传输（不能与加密服务器交互，无法进行身份验证）。
- 只支持 Windows AD 域用户同步，不支持匿名同步用户。只支持 OpenLdap 服务器用户同步，不支持 OpenLdap 认证（OpenLdap 同步的用户没有 dn 属性无法参与认证）。
- AD 服务器上用户名超长(大于 63 字符)，含有异常字符（汉字数字字母以及@._-()[]|以外的特殊字符）可以同步，不能录入到本地用户结构，同步过程中会依次在本地用户结构添加用户、用户组，本地满规格时无法录入，同步规格和本地用户规格相同。
- LDAP BaseDN 如果写根 OU 的话，同步 LDAP 服务器的时候会把根 OU 下的所有子 OU 以及用户全部同步下来。
- 多个用户同步条目存在时，同步任务为串行，上面同步条目同步完成后在进行下面同步条目的同步。
- LDAP 同步周期起始时间（0-23），间隔时间（1-24），例如起始时间 8，间隔 2，代表该同步条目每天 8 点开始同步，每隔 2 小时同步一次，晚上 12 点结束当天的同步任务。
- AD 域用户更新密码后，使用同步的 LDAP 认证时，新旧密码都可以认证。在 server 2008 级别的 AD 下，旧密码生存期为 5 分钟，在 server 2003 级别的 AD 下，旧密码生存期为 60 分钟。

这个 5 分钟就是为了防止 AD 同步延时问题，防止 DC 数量比较多时，用户登录所在的站点内还没有成功的更新到密码的修改的情况。这样，即使新密码没有生效，旧密码依然可用。

测试 2003 的服务器，旧密码有效期为 60 分钟，自测 60 分钟后密码失效，此为 AD 域服务器的保护机制，不修改。

- 手动创建用户组、用户创建为本地用户，和 LDAP 服务器上组、用户名称一样，点 LDAP 同步，这个用户没法用 LDAP 认证，LDAP 同步当存在重名用户时，只移动用户，不覆盖。
- LDAP 组里第一个 LDAP 服务器密码不对，用户在第二个服务器，此时用户认证浏览器无响应，目前不能处理跨域的 LDAP 组认证，需要保障 LDAP 组下地址可达，服务器密码正确。
- arp 扫描只支持扫描设备同网段用户。
- 新建 SNMP 同步条目的 MAC 地址是与设备相连的交换机的地址。
- 设备的配置的团体名需要跟交换机上的团体名一致，团体字中不能包含中文。
- 开启 SNMP 同步及 IP-MAC 绑定后，交换机下的新用户 IP-MAC 如果不能及时学习到，数据直接放通，在线用户列表中的 MAC 会显示成三层交换机的 MAC。
- 在配置多个交换机时扫描开始后串行逐个扫描，待所有交换机扫描完毕后等待配置的更新时间后再开始下一轮扫描。
- 对于每次扫描结果如何处理：如果旧表中有对应 MAC，则更新老化时间，如果没有，则新增。对于旧表中有但没有新学习到的 MAC，等老化后删除。
- SNMP 同步分两步：

  1. SNMP 协议跟交换机交互报文，来学习 IP-MAC 条目，并将 IP-MAC 条目存到文件中（网络好时报文交互快，学的也快）。

  2.从文件中读 IP-MAC，进行新旧对比并更新老化时间。
- 正常情况下，开启 SNMP 同步功能后启动老化定时器，30 分钟执行一次老化，然后更新定时器的时间进行下一次老化，如果条目达到 59000 条，触发定时器快速老化（记录本次快速老化的时间），然后刷新定时器为 30 分钟；当再次达到 59000 条时，判断当前时间-上次快速老化时间小于 10 分钟，什么都不做；否则触发定时器快速老化（记录本次快速老化的时间），然后刷新定时器为 30 分钟。
- 快速老化机制：

  1.IP-MAC 表达到 59000 条时触发快速老化，将已经老化的 IP-MAC 全清掉，规格满直接丢新的条目。

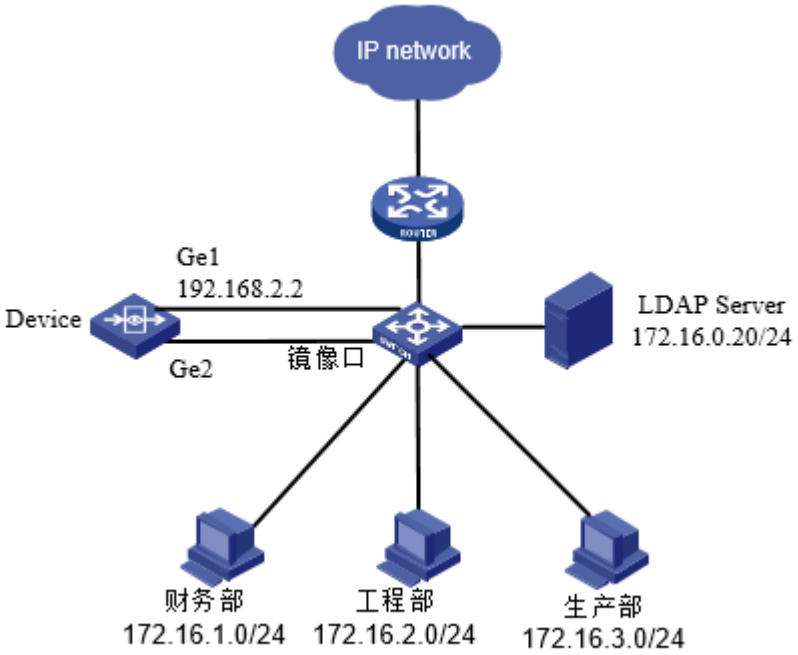
  2.两次快速老化的时间间隔是 10 分钟。

4 用户同步配置举例

4.1 组网需求

如图 1 所示，某公司的财务部、工程部员工实行固定设备使用静态绑定 IP/MAC 的方式上网，生产部员工使用 LDAP 服务器配置的用户账号认证上网，其网段分别是 172.16.1.0/24、172.16.2.0/24 和 172.16.3.0/24，LDAP 服务器的地址为 172.16.0.20/24。工程部 SNMP 服务器地址为 172.16.0.10/24。使用设备以旁挂方式部署于核心设备旁边，将用户上网的流量通过端口镜像的方式镜像至设备的旁路接口，在设备上配置用户同步。

图1 用户同步功能配置组网图



4.2 配置思路

(1) 按照组网图组网
(2) 配置旁路认证
(3) 添加 LDAP 服务器
(4) 配置用户组
(5) 配置用户同步任务
(6) 配置用户认证地址对象
(7) 配置 WEB 认证参数
(8) 配置控制策略
(9) 全局配置启用第三方 LDAP 服务器
(10) 配置用户策略

4.3 使用版本

本举例是在 E6201 版本上进行配置和验证的。

4.4 配置步骤

4.4.1 配置设备

1. 配置旁路认证

如图 2 所示，进入“网络配置>基础网络>部署方式>高级配置”，开启旁路认证。

图2 配置旁路认证和旁路阻断

2. 添加 LDAP 服务器

通过菜单“用户管理>认证管理>认证服务器”，点击<新建>LDAP 服务器。进入如图 3 所示的页面。

图3 LDAP 服务器配置

3. 配置用户组

通过菜单“用户管理>用户组织结构”，单击选择“新建>用户组”，配置财务部和工程部用户组，如图 4、图 5 所示。

图4 财务部用户组配置

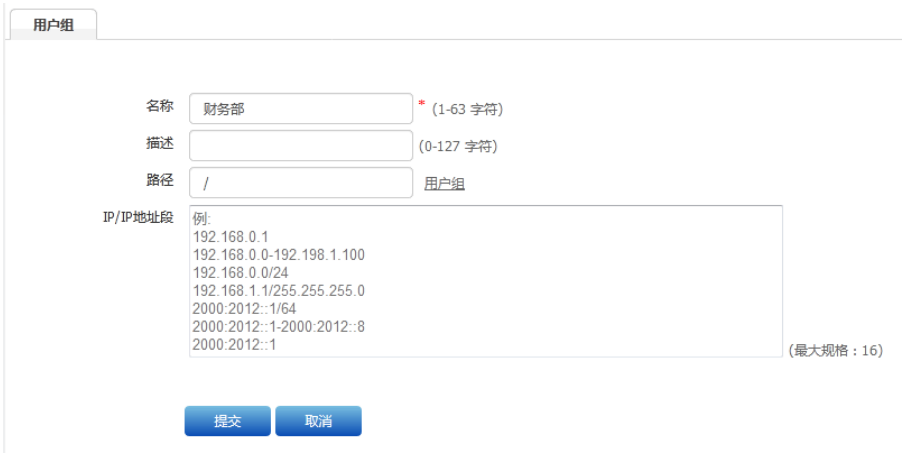


图5 工程部用户组配置

4. 配置用户同步认证

(1) 配置 LDAP 同步

通过菜单“用户管理>用户同步”，单击选择“新建>LDAP 同步”，进入 LDAP 同步配置页面。配置 LDAP 同步任务名称，选择 LDAP 服务器，选择开启同步周期并配置同步周期（每天的某个整点），或者选择关闭周期同步，如图 6 所示。

图6 配置生产部 LDAP 同步

(2) 配置 SNMP 同步

通过菜单“用户管理>用户同步”，单击选择“新建>SNMP 同步”，进入 SNMP 配置页面。配置 SNMP 同步任务名称，IP 地址和 MAC 地址配置为 SNMP server 的 IP 地址和 MAC 地址，配置团体名和 SNMP 的版本号，选择开启周期同步并配置同步周期或者关闭周期同步（只在配置成功后同步一次），选择开启自动录入并配置同步结果的录入用户组，或者关闭自动录入由后期用户手动添加。如图 7 所示。

图7 配置工程部 SNMP 同步

(3) 配置 ARP 扫描

通过菜单“用户管理>用户同步”，单击选择“新建>ARP 扫描”，进入 ARP 扫描配置页面。配置“扫描网段”为财务部网段，选择配置是否开启周期同步，是否开启自动录入并选择录入用户的组织结构的用户组。如图 8 所示。

图8 配置财务部 ARP 扫描

5. 配置用户认证地址对象

通过菜单“策略配置 > 对象管理 > 地址对象”，单击“新建>地址对象”，配置生产部地址对象。如图 9 所示。

图9 地址对象配置

6. 配置 Web 认证参数

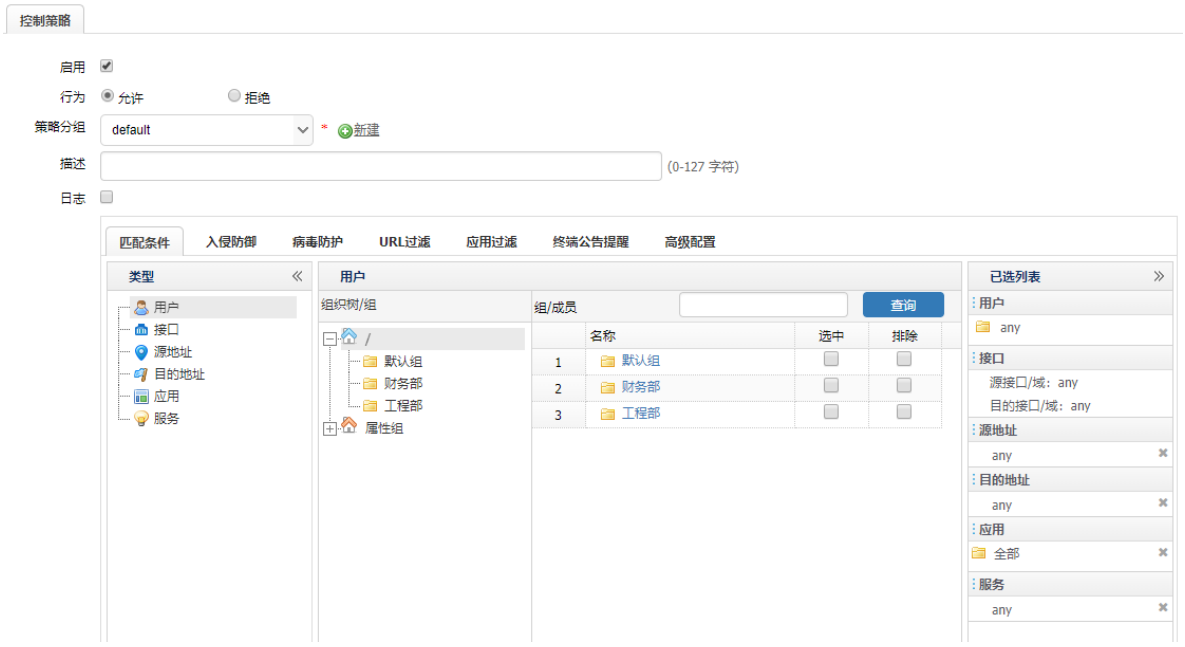
通过菜单“用户管理>认证管理>认证方式 > 本地 WEB 认证”，勾选“允许重复登录”，配置“允许登录数”为无限制，单击<提交>。如图 10 所示。

图10 配置 Web 认证

7. 配置安全策略

通过菜单“策略配置>控制策略”，单击<新建>配置控制策略。如图 11 所示。配置用户组财务部、工程部和生产部（LDAP 同步下来的用户组）允许访问外网。

图11 控制策略配置



8. 全局配置启用第三方认证选择 LDAP 服务器

在导航栏中选择“用户管理>认证管理>高级选项”，进入全局配置页面，启用第三方认证，选择 LDAP 服务器，如图 12 所示。

图12 全局模式启用第三方 Ldap 配置

9. 配置用户策略

通过菜单进入“用户管理>认证管理>认证策略”，单击<新建>，源地址配置为“生产部地址对象”，认证方式配置为“Web 认证”，其它选项保持默认，单击<提交>。如图 13 所示。

图13 用户策略配置

4.5 验证配置

(1) 进入“用户管理>用户组织结构”，查看“财务部”用户组。财务部 ARP 同步成功后，财务部固定设备的用户全部自动录入，用户静态绑定对应的 IP，固定设备直接可以上网。如图 14 所示。

图14 财务部 ARP 同步用户

(2) 进入“用户管理>用户组织结构”，查看“工程部”用户组。工程部 SNMP 同步成功后，生产部固定设备的用户全部自动录入，用户静态绑定对应的 IP/MAC，固定设备直接可以上网。如图 15 所示。

图15 工程部 SNMP 同步用户

(3) 进入“用户管理>用户组织结构”，查看“生产部”用户组。从 LDAP 成功同步了生产部的用户，同步了用户组“生产部”以及用户组的直属用户 user1，user2，user3。如图 16 所示。

图16 生产部 LDAP 同步用户

(4) 在生产部网段（172.16.3.0/24）使用 PC 终端进行 HTTP 访问，弹出本地 Web 认证页面，使用 LDAP 联动用户 user3（此用户在 LDAP 服务器上真实存在且已经通过 LDAP 同步功能录入到了设备本地用户组）认证成功，认证成功后可以正常访问外网。如图 17 所示。

图17 生产部 LDAP 用户认证页面

目 录

1 简介

本文档介绍设备的短信认证功能配置举例，在配置前，先了解如下定义：

- 短信网关：与设备对接，给认证终端指定手机号下发授权验证码的设备，目前支持对接的短信网关厂商包括：亿美软通、凌凯、一信通、佳诺、阿里云、梦网科技、移动云 MAS。

本文档以亿美软通短信网关厂商对接进行举例说明。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

在配置前，需要做如下准备：

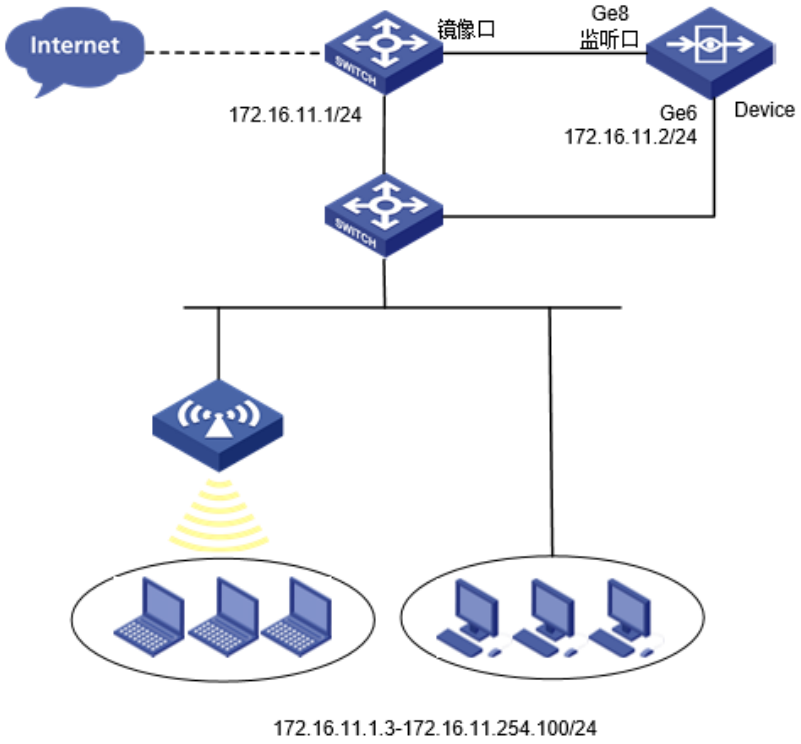
- 客户已经在对应的短信网关厂商进行了注册（如亿美软通）。
- 本文档假设您已了短信认证特性。

3 短信认证功能配置举例

3.1 组网需求

如图 1 所示，某公司内网办公网段 IP 地址 172.16.11.0/24，使用设备以旁挂方式部署于核心设备旁边，将用户上网的流量通过端口镜像的方式镜像至设备的旁路接口，设备上开启短信认证功能，用户通过短信认证后才能上网。

图1 短信认证配置举例组网图



3.2 配置思路

- 配置设备接口地址。
- 配置设备旁路部署。
- 配置设备旁路认证。
- 注册短信网关厂商，获取授权。
- 配置短信认证功能。

3.3 使用版本

本举例是在 E6201 版本上进行配置和验证的。

3.4 配置步骤

(1) 配置接口地址

如图 2 所示，进入“网络配置>接口配置>物理接口”，点击 ge6<编辑>按钮，配置 ge6 的 IP 地址为 172.16.11.2/24。

图2 配置接口地址

(2) 配置部署方式

如图 3 所示，进入“网络配置>基础网络>部署方式”，配置勾选 ge8 口启用。

图3 配置部署方式

(3)　配置旁路认证和阻断

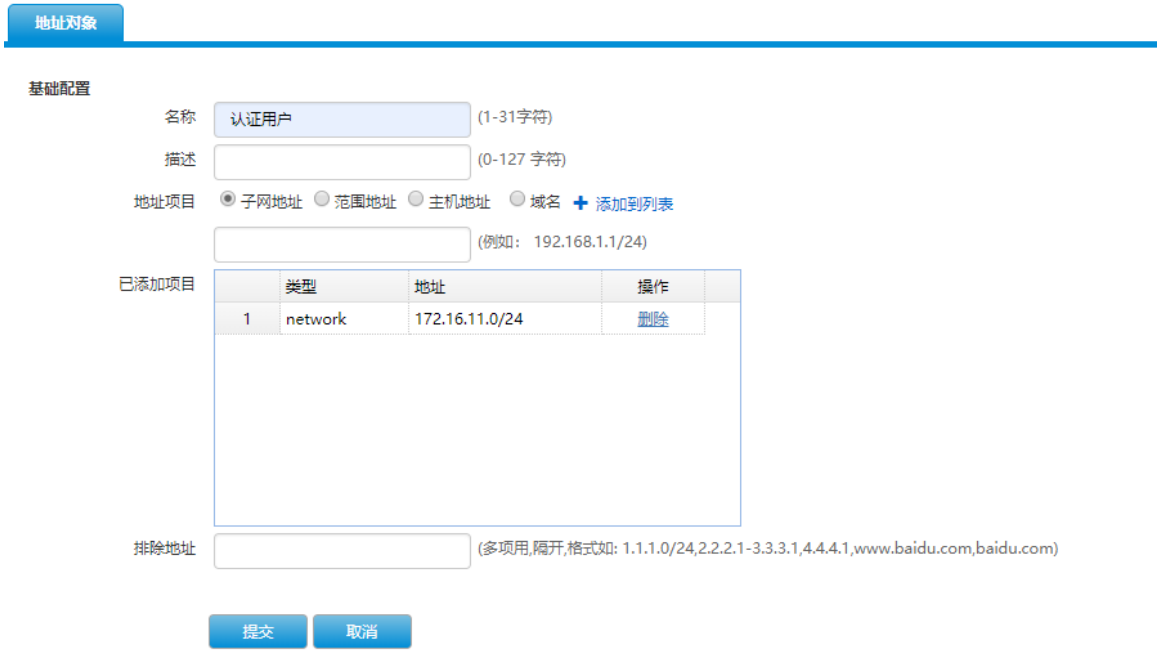
如图 4 所示，进入“网络配置>基础网络>部署方式>高级配置”，配置旁路认证和旁路阻断。

图4 配置旁路认证和旁路阻断

(4)　配置短信认证地址对象

如图 5 所示，进入“策略配置>对象管理>地址对象>地址对象”，点击<新建>按钮创建认证用户地址对象，设置地址为 172.16.11.0/24，点击<提交>。

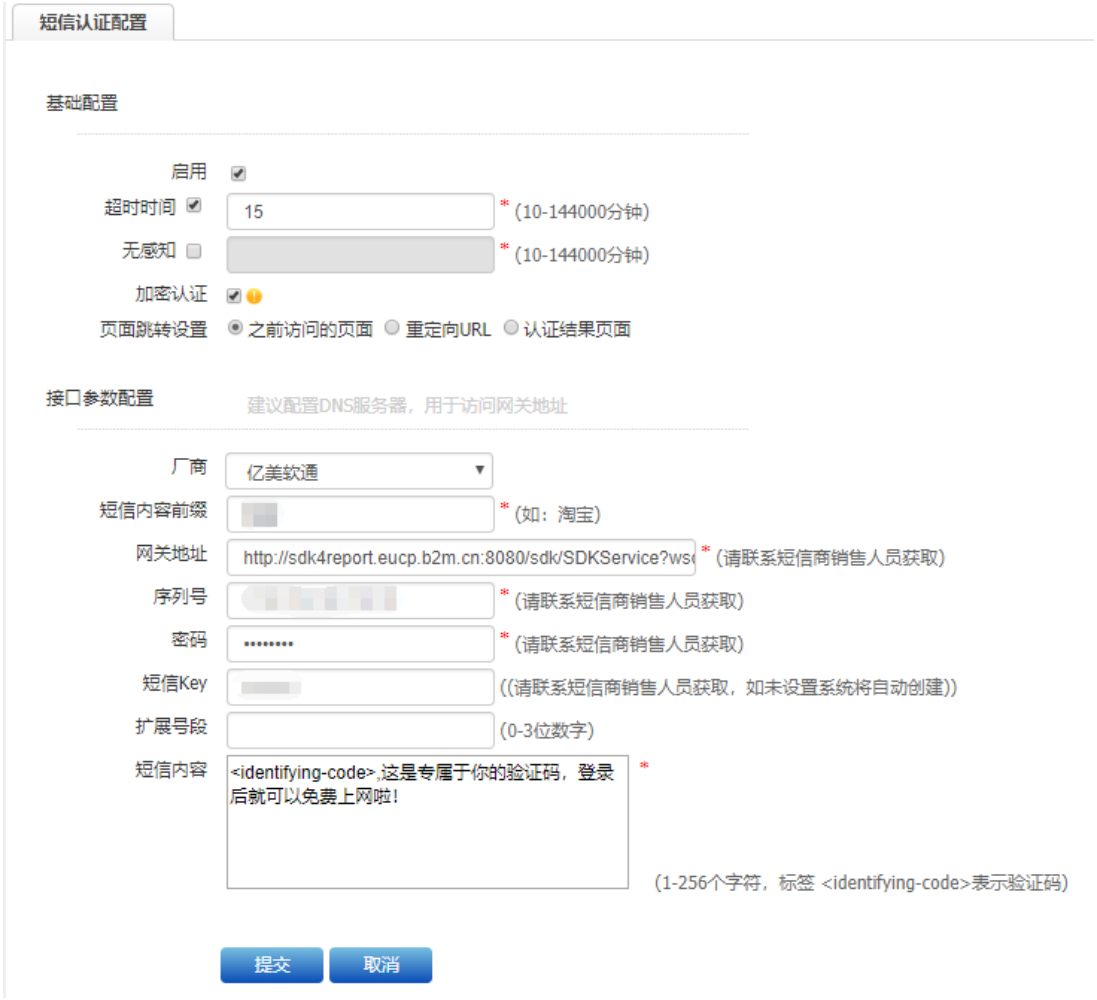
图5 配置短信认证地址对象



(5)　配置短信认证参数

如图 6 所示，进入“用户管理 > 认证管理 > 认证方式 > 短信认证”页面，配置短信认证参数。

图6 短信认证配置



(6) 配置短信认证策略

如图 7 所示，进入“用户管理 > 认证管理 > 认证策略”页面，选择新建认证策略，源接口选择内网口 ge2，源地址选择“认证用户”，认证方式使用“短信认证”，提交策略。

图7 认证策略页面

(7) 配置用户识别范围

如图 8 所示，进入“用户管理>认证管理>高级选项>全局配置”页面，识别范围选择“认证用户”，其它配置默认，提交配置。

图8 用户识别范围

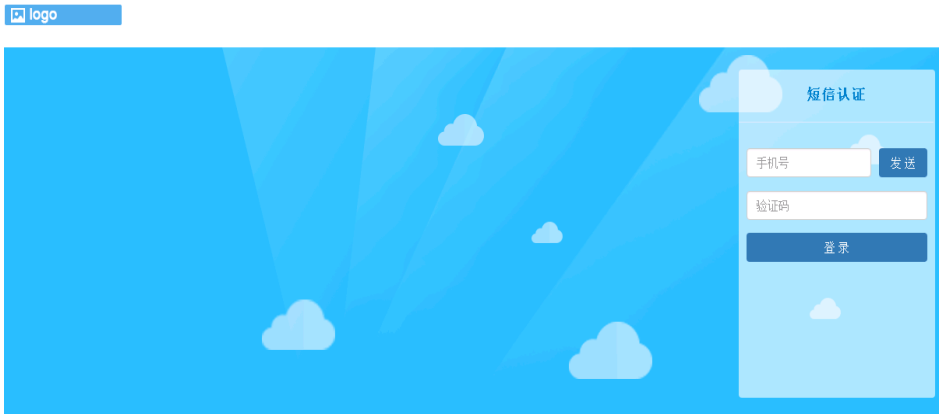
3.5 配置注意事项

- FW 设备需要开启 DHCP 功能，地址池范围为 172.16.11.3/24~172.16.11.254/24。
- 设备在旁路部署时，用户认证策略和控制策略的源接口以及目的接口必须配置接收镜像流量的旁路部署接口或者是 any。
- 旁路认证务必保证旁路设备到上网 PC 可达，否则功能无法使用。
- 认证用户网段必须在用户识别范围中，否则会导致不能正常认证。

3.6 验证配置

如图 9 所示，终端访问网页上网时，浏览器弹出 portal 页面。

图9　认证 portal 页面

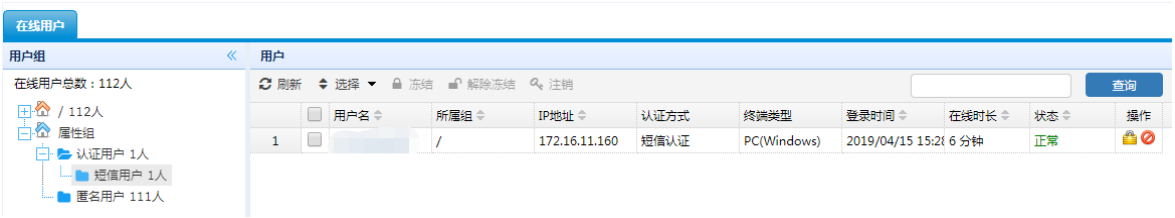


如图 10 所示，输入手机号，点击<发送>获取验证码，待手机获取到短信网关发送的验证码后，输入正确的验证码，点击登录即可完成认证。

图10 短信认证

如图 11 所示，在“数据中心>系统监控>在线用户”管理中查看该用户已认证成功。

图11 在线用户



目 录

1 简介

本文档介绍设备的 APP 认证功能配置举例，在配置前，先了解如下定义：

- APP 认证：主要应用在金融、连锁商超等用户场景，与设备联动，因为这些客户场景（如金融网点，连锁商超）有专门的办公 APP 应用，办公人员本身已经拥有合法的 APP 实名账号，为了对这一类用户实现实名认证以及上网行为管控,传统的解决方案是需要在设备侧重新创建一份认证账号用于认证上网。对于客户或网络管理员而言，需要同时维护设备和 APP 两套用户认证账号，非常不方便。为了解决这一问题，设备可以直接通过指定的规则分析和监听 APP 应用登录报文中的账号并进行提取，然后将提取到的账号直接作为合法认证用户的身份标识，将用户加入在线用户列表，并可选择将监听到的账号录入到设备本地，以用于后续基于实名账号的上网行为管控，以此来实现设备认证和 APP 应用的联动。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

在配置前，需要做如下准备：

- 客户已经拥有自己的 APP 客户端程序，且 APP 登录账号交互为明文方式。
- 本文档假设您已了解 APP 认证特性。

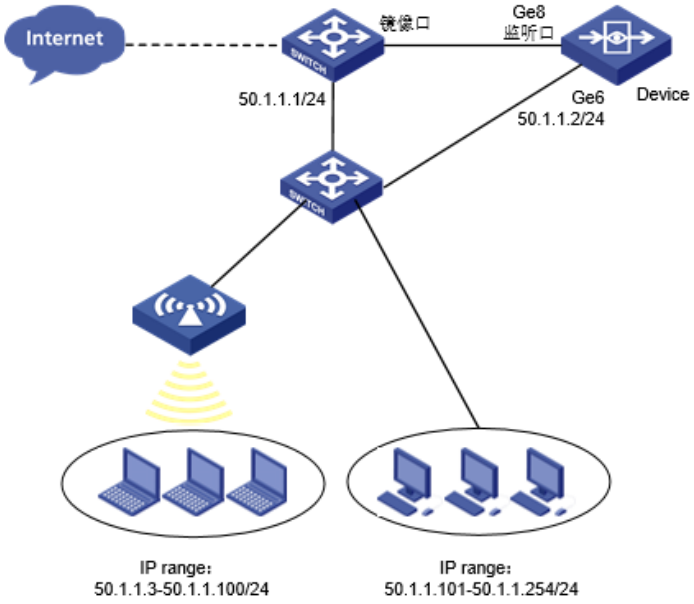
3 APP 认证功能配置举例

3.1 组网需求

如图 1 所示，某连锁商超内网办公网段的 IP 地址为 50.4.1.0/24，使用设备以旁挂方式部署于核心设备旁边，将用户上网的流量通过端口镜像的方式镜像至设备的旁路接口，在设备上配置 APP 认证功能。

- 需要对商超内登录 APP 的办公人员进行实名认证，要求设备侧在线用户能实名显示哪些办公人员在线。
- 当有新办公人员的移动终端加入商超连网时可以通过设备的推送页面直接下载 APP 应用。

图1 APP 认证组网图



3.2 配置思路

- 根据组网图组网
- 配置旁路认证
- 获取 APP 账号规则和服务器地址
- 配置 APP 认证参数
- 配置 APP 用户组
- 配置地址对象
- 配置 APP 认证策略

3.3 使用版本

本举例是在 E6201 版本上进行配置和验证的。

3.4 配置步骤

(1) 根据组网图组网。

请参考“旁路认证和阻断配置举例”的相关配置步骤。

(2) 配置旁路认证

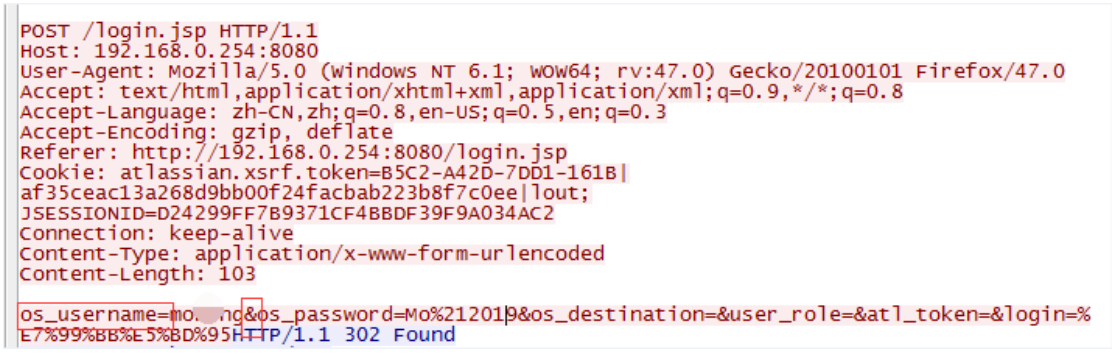
如图 2 所示，进入“网络配置>基础网络>部署方式>高级配置”，开启旁路认证。

图2 配置旁路认证和旁路阻断

(3) 获取 APP 账号规则和服务器地址

如下图所示，使用办公人员终端登录 APP，整个过程使用抓包获取 APP 账号登录的报文，过滤 HTTP 登录报文，查找用户名字段所在位置。

图3 抓包获取 APP 账号登录的报文



得到服务器地址：192.168.0.254

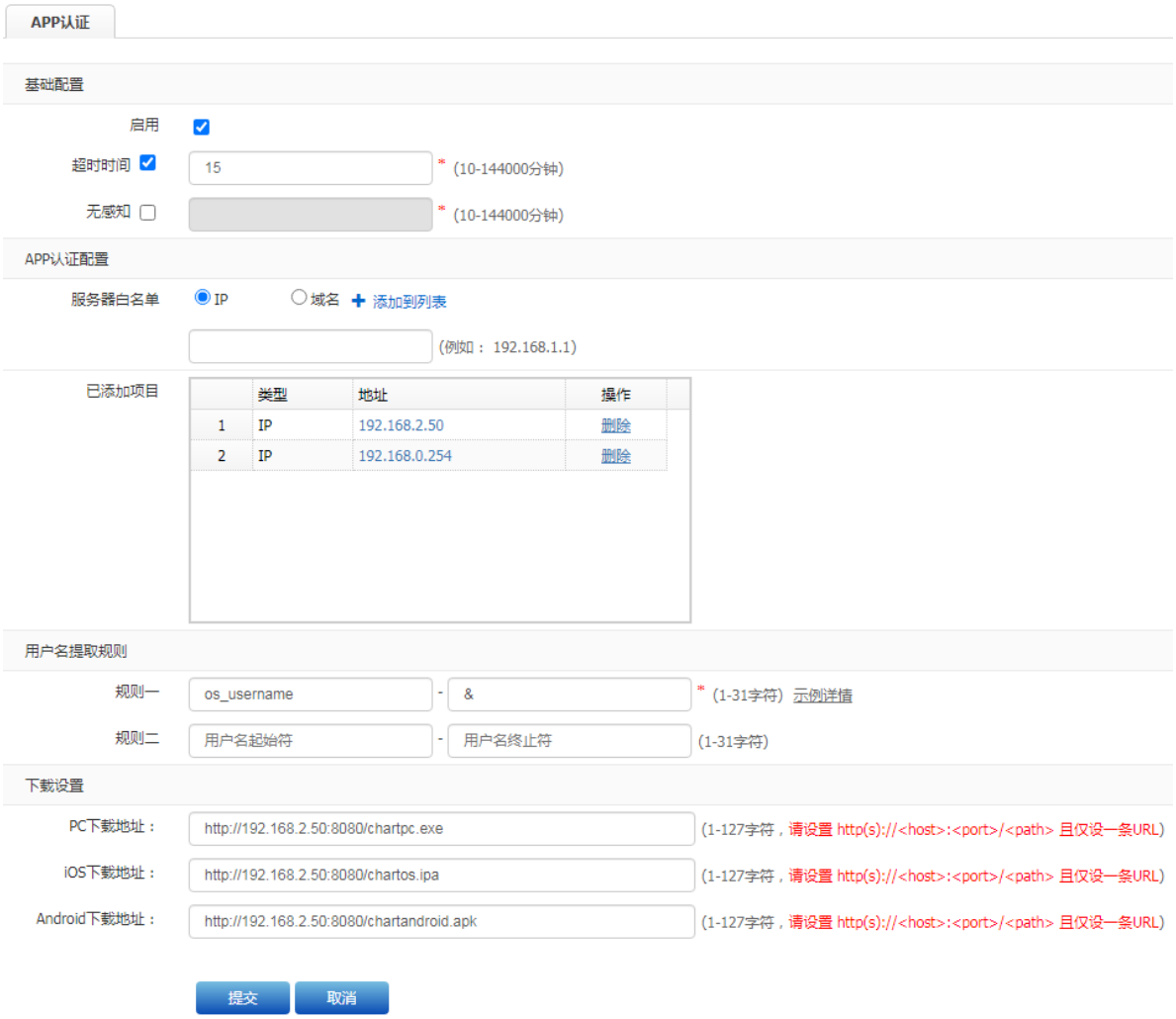
得到用户起始字符：os_username= 结束字符：&

同时网络内指定的APP下载服务器地址为：192.168.2.50，各客户端软件均放在此HTTP服务器上。

(4) 配置 APP 认证参数

如图 4 所示，进入“用户管理>认证管理>认证方式>APP 认证”，配置 APP 认证参数，点击<提交>。

图4 配置 APP 认证参数



(5) 配置 APP 用户组

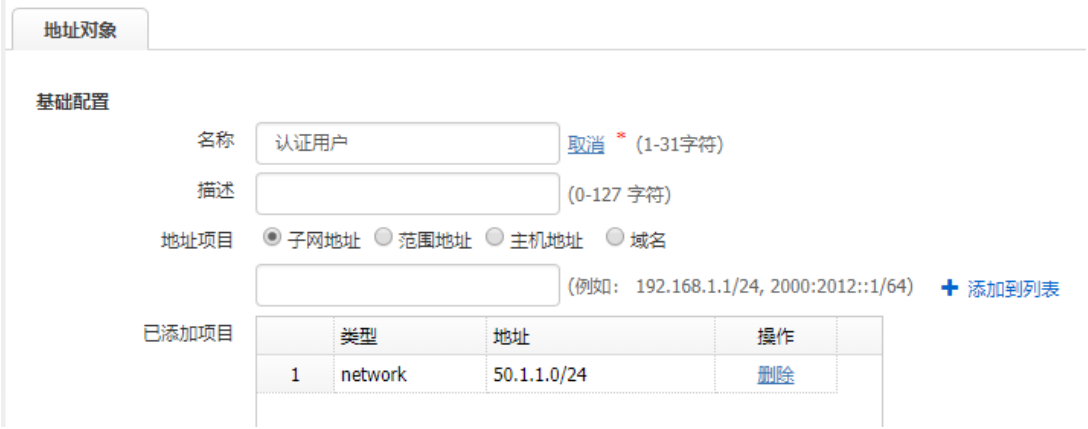
如下图所示，进入“用户管理 > 用户组织结构 ”页面，点击<新建>选择”组”，配置完成后提交。

图5 配置 APP 用户组

(6) 配置地址对象

如下图所示，进入“策略管理 > 对象管理>地址对象”页面，点击<新建>，配置完成后提交。

图6 配置地址对象



(7) 配置 APP 认证策略

如图 7 所示，进入“用户管理 > 认证管理 > 认证策略”页面，选择新建认证策略，源接口选择内网口 ge3，源地址选择“认证用户”，认证方式使用“APP 认证”，提交策略。

图7 配置 APP 认证策略

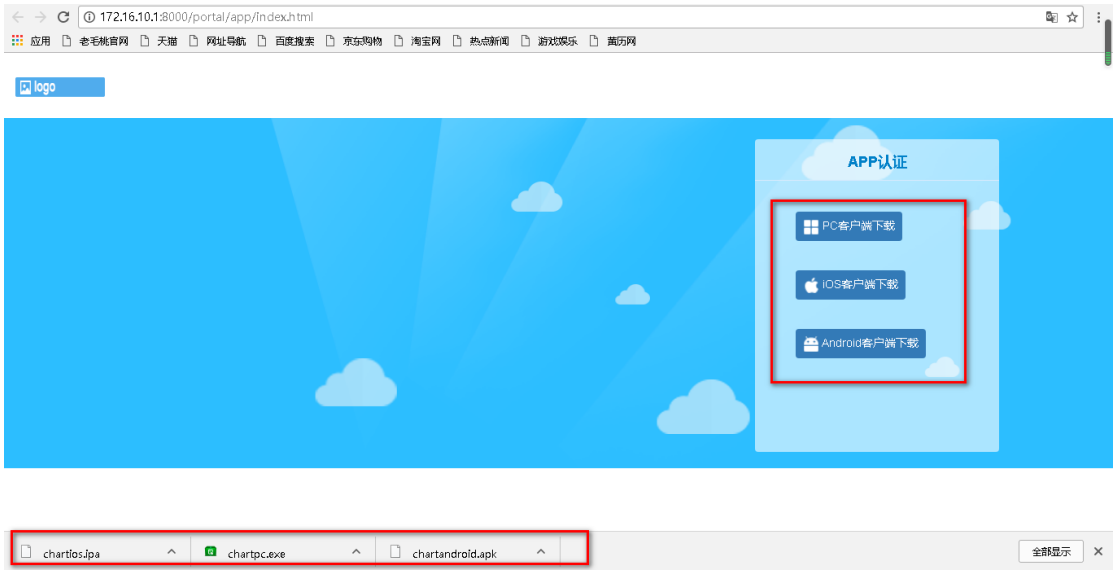
3.5 配置注意事项

- APP 认证参数配置中必须将 HTTP 服务器地址和 APP 认证服务器地址放通。
- 认证用户网段必须在用户识别范围中，否则会导致不能正常认证。
- APP 下载链接为 HTTP 时，放通 APP 服务器的流量只能通过配置 IP 实现，不能配置域名，报文交互中域名被加密了提取不到对应的域名。
- APP 认证不支持 HTTP 加密应用中的用户名提取。
- APP 账号登录支持 GET 和 POST 两种方式，POST 登录方式如举例所示，用户名需要在 HTTP POST 表单中，GET 登录方式用户名需要在 GET 头部字段中如：GET/login.html?account=test0&mac=48-a1-95-57-6e-93&ipaddr=172.16.11.170 HTTP/1.1
- APP 账号监控不支持结果检验，账号登录失败，或账号不存在的情况下，也能监控到用户输入的账号正常上线。

3.6 验证配置

如图 8 所示，用户在认证之前访问网络会弹出认证页面，点击认证页面上的下载按钮，可以直接下载对应的 APP 应用程序。

图8 认证 portal 页面



如下图所示，用户打开 APP 应用登录账号，会直接在设备侧认证成功，并加入在线用户列表

图9 在线用户

如下图所示，登录成功的用户会被录入到设备本地用户组织结构对应的用户组中。

图10 用户组织结构

目 录

1 简介

本文档介绍设备的 IC 卡认证功能配置举例，在配置前，先了解如下定义：

- IC 卡：IC 卡是集成电路卡，IC 卡芯片具有写入数据和存储数据的能力，可对 IC 卡存储器中的内容进行判定。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

在配置前，需要做如下准备：

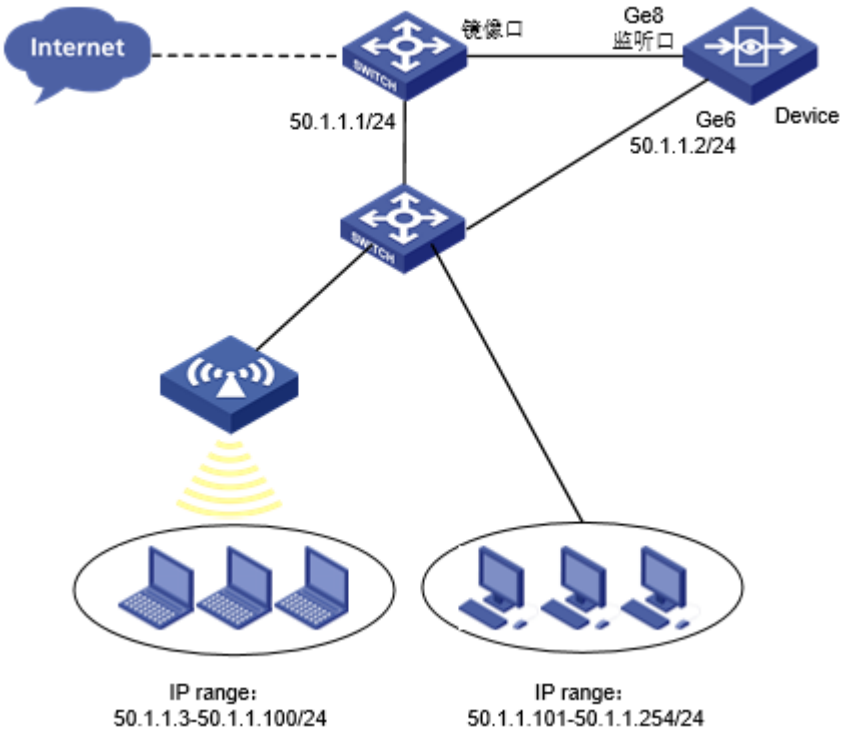
- 本文档假设您已了解 IC 卡认证特性。

3 IC 卡认证功能配置举例

3.1 组网需求

如图 1 所示，某公司内网用户网段 IP 地址为 50.1.1.0/24，使用设备以旁挂方式部署于核心设备旁边，将用户上网的流量通过端口镜像的方式镜像至设备的旁路接口，设备上开启 IC 卡认证功能，用户通过 IC 卡认证后才能上网。

图1 IC 卡认证路由模式组网图



3.2 配置思路

- 配置基本网络。
- 配置旁路认证。
- 配置 IC 卡认证功能。

3.3 使用版本

本举例是在 E6201 版本上进行配置和验证的。

3.4 配置步骤

3.4.1 配置设备

1. 基础网络配置

根据组网图组网，请参考“旁路认证和阻断配置举例”的相关配置步骤。

2. 配置旁路认证

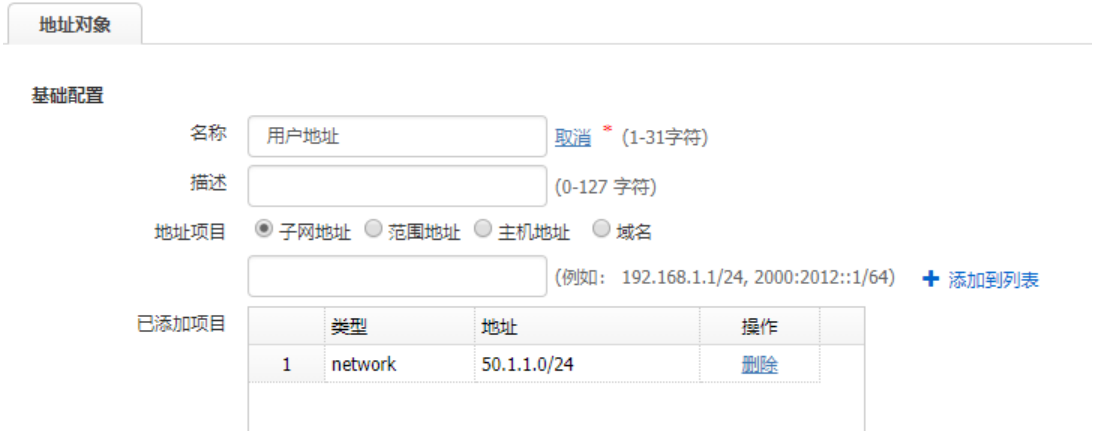
如图 2 所示，进入“网络配置>基础网络>部署方式>高级配置”，开启旁路认证。

图2 配置旁路认证和旁路阻断

3. 配置对象

如图 3 所示，进入“策略配置>对象管理>地址对象>地址对象”页面，点击<新建>按钮创建用户地址对象，地址为 172.16.1.0/24，点击<提交>。

图3 配置用户地址对象



4. 配置 IC 卡认证策略

如图 4 所示，进入“用户管理 > 认证管理 > 认证策略”页面，选择新建认证策略，源接口选择内网口 ge2，源地址选择“用户地址”，认证方式使用“IC 卡认证”，提交策略。

图4 IC 卡认证策略页面

5. 配置用户识别范围

如图 5 所示，进入“用户管理>认证管理>高级选项”页面，识别范围选择“用户地址”，其它配置默认，提交配置。

图5 用户识别范围

3.4.2 PC 端卡机配置

如图 6 所示，修改卡机软件配置文件 InternetManager.exe.config。

参数“host”的取值配置为 172.16.1.1（设备的地址）；

参数“ReaderPort”的取值配置为 100；

参数“IsYZH”的取值配置为 0。

图6 卡机软件配置

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

    <supportedRuntime version="v2.0.50727"/></startup>
  <appSettings>
    <!--<add key="host" value="http://localhost:1593/"/>-->
    <add key="host" value="https://192.168.1.240/"/>
    <add key="cardhost" value="http://192.168.1.109:8077/"/>
    <add key="ListenTimeSpan" value="5000"/>
    <add key="ReqTimeout" value="3500"/>
    <add key="KeepTimeSpan" value="30000"/>
    <add key="ReaderPort" value="5"/>
    <add key="cardNo" value="123456"/>
    <add key="IsYZH" value="1"/>
    <add key="IsTask" value="1"/>
    <!--<add key="host" value="http://116.196.93.178:1593/"/>-->
    <!--<add key="host" value="http://192.168.1.194:1593/"/>-->
  </appSettings>

  <system.net>
    <settings>
      <httpWebRequest useUnsafeHeaderParsing="true"/>
    </settings>
  </system.net>
</configuration>
```

3.5 配置注意事项

- IC 卡只支持深圳市德卡科技有限公司的 D8 型号卡机。
- IC 卡卡机只支持 win10 系统。
- 认证用户网段必须在用户识别范围中，否则会导致不能正常认证。

3.6 验证配置

如图 7 所示，终端访问网页上网时，浏览器弹出 portal 页面。

图7 认证 portal 页面

如图 8 所示，PC 进行刷卡认证后，可以正常上网，查看设备在线用户，可以看到在线用户信息。

图8 在线用户


在线用户
用户组
在线用户总数: 42人
/ 41人
属性组
认证用户 1人
ic_card 1人
匿名用户 41人
用户
刷新
选择
冻结
解除冻结
注销
查询
用户名
所属组
IP地址
认证方式
终端类型
登录时间
在线时长
状态
操作
1
1414964851
ic_card
172.16.1.2
ic-card
正在识别
2020/12/02 15:51
5 秒
正常

目录

1 简介

本文档介绍设备的用户 POP3 认证配置举例，在配置前，先了解如下定义：

POP3 认证：是指用户在使网络服务时，可以在认证页面中输入内网或外网邮箱服务器中的邮箱账号和密码进行认证，从而使认证用户接入使用网络。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解用户 POP3 认证特性。

3 使用限制

- 如果配置 SSL 加密方式认证对应需要修改 POP3 服务器的端口和勾选 SSL 选项
- 配置 POP3 服务器的地址时不支持配置域名地址。
- 在配置 POP3 服务器中的服务器端口要和实际的服务器端口对应，否则无法进行认证。

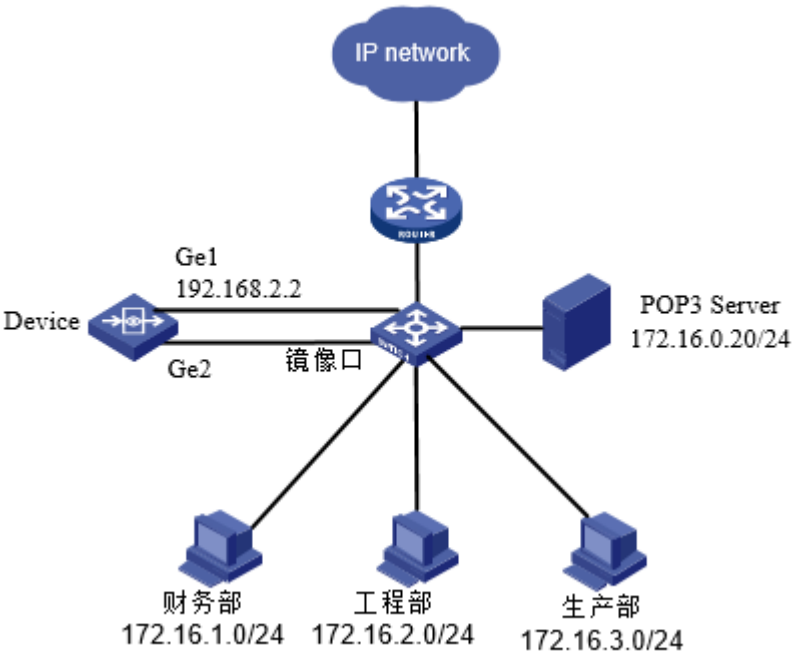
4 配置举例

4.1 组网需求

如图 1 所示，某公司内网搭建 POP3 服务器，用户名全部存放在 POP3 服务器上，要求内网用户使用 POP3 服务器上的用户进行认证。使用设备以旁挂方式部署于交换机旁边，将用户上网的流量通过端口镜像的方式镜像至设备的旁路接口，不影响企业内部网络结构。具体要求如下：

- 内网用户进行 POP3 认证上网，用户名和密码存储在 POP3 服务器上。

图1 POP3 认证功能配置组网图



4.2 配置思路

- 基本网络配置。
- 配置旁路认证。
- 配置 POP3 服务器对象，设备上的相关参数配置需要和服务器保持一致。
- 配置地址对象；
- 配置控制策略允许上网；
- 配置到网关的默认路由；
- 在认证方式中 POP3 认证页面引用 POP3 服务器；
- 配置用户策略触发认证。

4.3 使用版本

本举例是在 E6201 版本上进行配置和验证的。

4.4 配置注意事项

- 设备的配置 POP3 认证时，允许用户的 TCP 三次握手报文通过，当检测到用户 HTTP 报文时拦截并弹出认证页面。所以，在使用 Web 认证功能时，需要保证终端可以进行正常的 HTTP 访问。

- 如果需要实现访问某些资源时免 POP3 认证，请在对应用户策略的目的地址对象中配置排除地址，将需要免认证访问的 IP 地址排除。目前仅支持排除 IP 地址，不支持排除域名。

4.5 配置步骤

4.5.1 配置设备

1. 配置基础网络

按照组网图组网，请参考“用户认证功能典型配置举例”的相关配置步骤。

2. 配置旁路认证

如图 2 所示，进入“网络配置>基础网络>部署方式>高级配置”，开启旁路认证。

图2 配置旁路认证和旁路阻断

3. 添加服务器

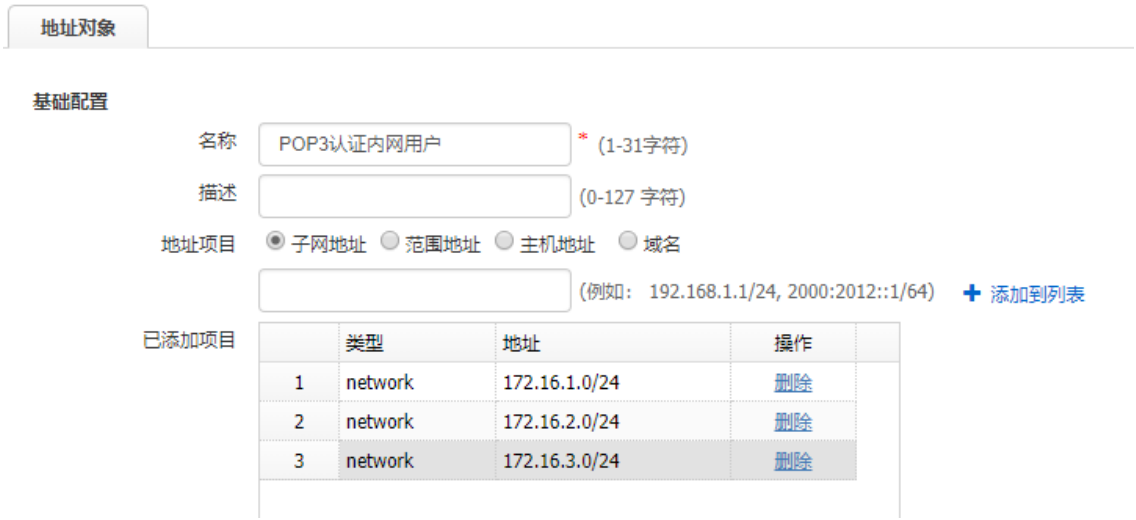
通过菜单“用户管理>认证管理>认证服务器”，点击<新建>选择 POP3 服务器，配置“服务器地址”为 10.0.1.31，“端口”需要和 POP3 服务器保持一致，点击<提交>。进入如图 3 所示的页面。

图3 添加 POP3 服务器

4. 配置地址对象

通过菜单“策略配置>对象管理 > 地址对象”，点击<新建>地址对象，配置内网用户和无线 wifi 地址对象。如图 4 所示。

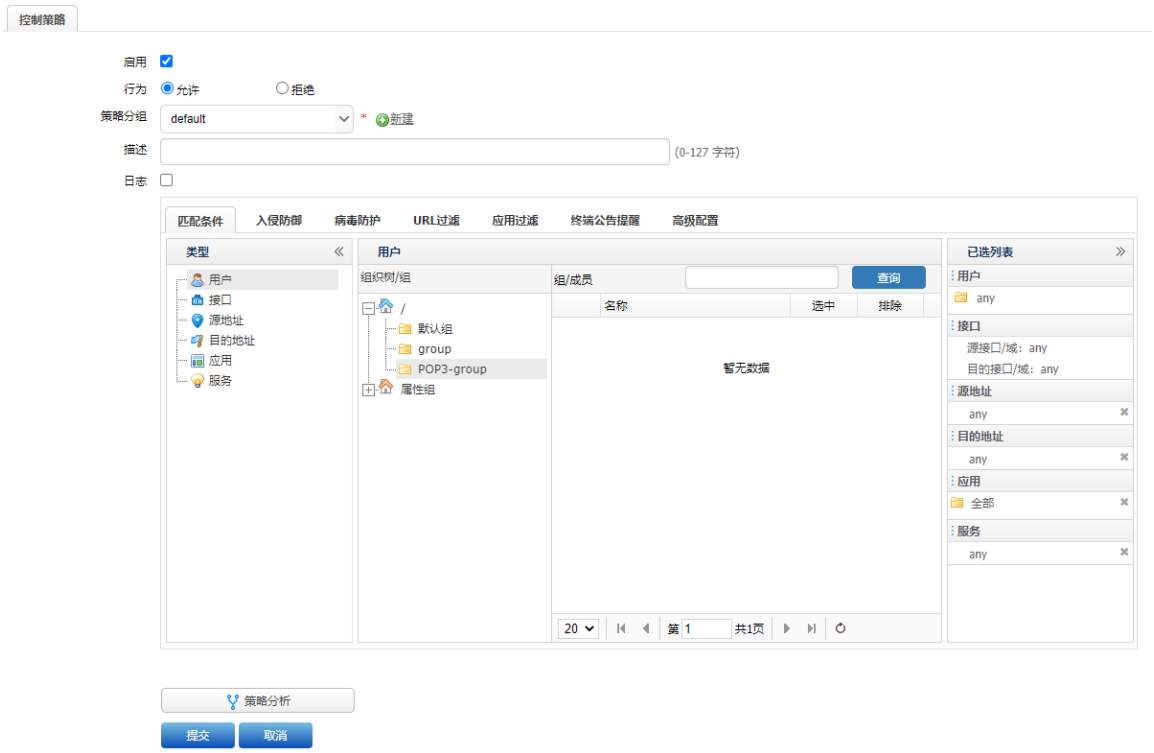
图4 添加内网用户地址对象



5. 配置控制策略

通过菜单“策略配置>控制策略”，点击<新建>控制策略，进入如图 5 所示的页面。

图5 控制策略配置



6. 配置 POP3 认证

在导航栏中选择“用户管理>认证管理>认证方式>POP3 认证”，进入 POP3 认证配置页面，认证服务器选择刚才配置的 POP3 服务器，如下图所示。

图6 POP3 认证配置页面

7. 配置静态路由

配置设备为路由模式，在导航栏中选择“网络配置>路由管理>静态路由”，点击新建，配置到网关的默认路由，如下图所示。

图7 静态路由配置页面

8. 配置用户认证策略

通过菜单进入“用户管理>认证管理>认证策略”，点击<新建>，源地址配置为“POP3 认证内网用户”，相关认证方式配置为“POP3 认证”，点击<提交>。如图 8 所示。

图8 配置用户认证策略

4.6 验证配置

内网用户使用 POP3 用户认证。如图 9 所示，内网终端进行 HTTP 访问，弹出如下 POP3 认证页面，使用 POP3 服务器上用户名、密码进行认证。

图9 内网用户使用 POP3 用户认证成功

如图 10 所示，设备在线用户 POP3 用户认证。

图10 用户 POP3 认证成功

目 录

1 简介

本文档介绍设备上钉钉认证功能的配置举例。

在配置前，先了解如下几个定义：

- 钉钉：由阿里巴巴官方推出的一款专为企业量身打造的统一办公通讯平台 https://oa.dingtalk.com/register_new.htm?source=2905&regType=person&noNewFlow=1&lwfrom=20171202020091367000000911
- AppID：在钉钉开放平台 https://open-dev.dingtalk.com 设置扫码登录应用授权，钉钉服务器自动生成的个人钉钉的唯一标识

AppSecret：钉钉服务器自动生成的应用秘钥。

- 企业 ID：从钉钉认证服务器获取的 enterpriseid（企业 id）唯一标识。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

在配置前，需要做如下准备：

- 客户已经注册钉钉。
- 本文档假设您已了解钉钉认证特性。

3 钉钉认证配置步骤

3.1 使用版本

本举例是在 E6201 版本上进行配置和验证的。

3.2 钉钉开发平台配置

(1) 登录钉钉开放平台：https://open-dev.dingtalk.com/#/index，首页显示企业 ID，如下图所示。

图3-1 登录钉钉开放平台

(2) 在导航栏选择“应用开发>登录”，单击<创建扫码登录应用授权>按钮，弹出“创建扫码登录应用授权”页面，如下图所示。

授权 logo 地址配置为 https://img.alicdn.com/tfs/TB1ylubM6DpK1RjSZFrXXa78VXa-144-144.png

回调域名填写设备的地址，如果域名为 http 方式，端口为 8000。配置完成后点击“确定”提交。

图3-2 创建扫码登录应用授权页面

(3) 配置完成之后，在页面点击已创建的应用图标，打开创建的应用即可获取到 appid 和 appsecret 字段。如下图所示。

图3-3 查看应用授权

(4) 选择“应用开发>H5 微应用>创建应用”，创建企业内部应用。应用类型选择“小程序”，输入应用名称、应用描述，上传应用图标后，点击“确定创建”按钮。

图3-4 创建企业内部应用

(5) 企业内部应用创建完成后，在 H5 微应用页面，可以查看到该应用的 AgentId、AppKey、AppSecret 字段。

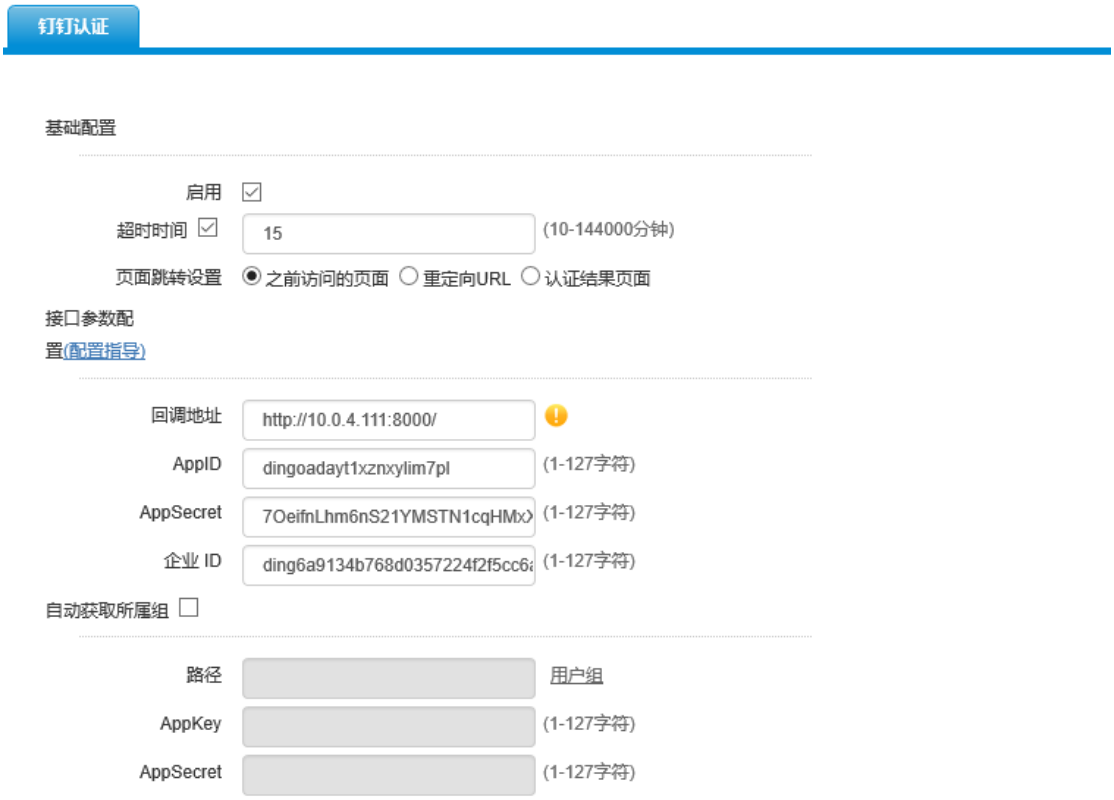
图3-5 查看企业内部应用

3.3 配置设备

3.3.1 配置钉钉认证

进入“用户管理>认证管理>认证方式>钉钉认证”页面，配置钉钉认证。

图3-6 钉钉认证配置页面



说明

- 回调地址为设备管理地址，且配置必须和钉钉服务器配置一致。
- AppID、AppSecret、企业 ID、Appkey 均配置为与钉钉服务器配置一致。
- 自动获取所属组默认关闭。开启自动获取所属组时，会将认证用户路径自动获取并在“监控统计->在线用户->属性组->认证用户”中显示；同时可以手动配置认证用户的所属路径。

3.3.2 配置 DNS 服务器

进入“网络管理->DNS 服务->DNS 服务器”后配置 DNS 服务器，点击“提交”。

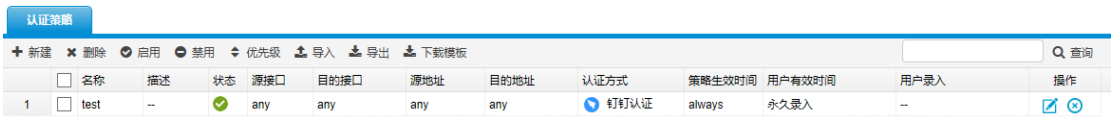
图3-7 DNS 服务器配置页面

3.3.3 配置认证策略

进入“用户管理->认证策略”页面，点击新建配置钉钉认证策略。如下图所示

图3-8 认证策略配置页面

配置完成截图如下：

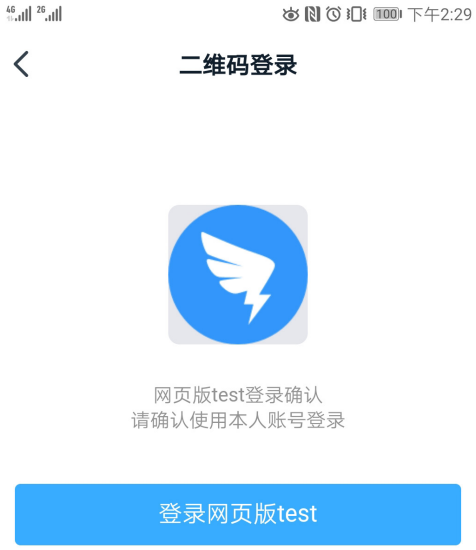


4 验证配置

4.1 PC端使用钉钉认证进行上网

(1) 开启认证策略，PC 输入浏览网页时，浏览器弹出 portal 页面。

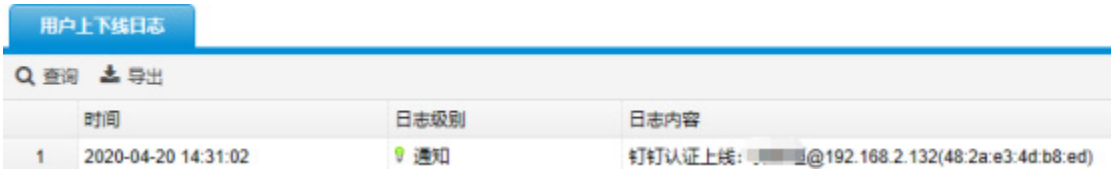
(2) 弹出 portal 页面，使用移动端钉钉扫描二维码。



(3) 点击“登录网页版 test”，完成钉钉认证。

4.2 在线用户查看

(1) 进入“数据中心>终端日志>用户上下线日志”查看钉钉认证日志。



(2) 进入“监控统计>在线用户”，查看已认证成功用户。

5 钉钉认证功能使用限制及注意事项

- 用户超时的时间范围为：10-144000 分钟，默认 15 分钟。
- 回调地址需要配置设备的管理 ip 地址+指定端口。例：设备的管理 ip 为 192.168.4.33 则回调地址为 http://192.168.4.33:8000 或 https://192.168.4.33:8001 另外，需注意钉钉服务器上回调地址需要与设备上配置的回调地址保持一致。
- AppID、AppSecret、企业 ID、Appkey 均需要与钉钉服务器配置一致。
- 同一时间只能支持对接一台服务器（即只能配置一组对接参数）。
- 暂不支持混合认证。
- 暂不支持已认证用户无感知。

目录

1 简介

端口镜像（port Mirroring）功能是网络设备上常用的功能，将一个或多个端口的数据流量复制到某一个指定端口来实现对网络的监控。在不影响源端口正常吞吐流量的情况下，可以通过镜像端口对网络的流量进行监控分析。

端口镜像功能是对网络流量监控的一个有效的安全手段，对监控流量进行分析和安全性的检查，同时也能及时的在网络发生故障时进行准确的定位。端口镜像功能简单地说就是将被监控流量镜像到监控端口，以便对被监控流量进行故障定位、流量分析、流量备份等，监控端口一般直接与监控主机等相连。端口镜像功能能够将进出网络的所有数据包，供安装了监控软件的管理服务器抓取数据。而企业出于信息安全、保护公司机密的需要，也迫切需要网络中有一个端口能提供这种实时监控功能。在企业中用端口镜像功能，可以很好的对企业内部的网络数据进行监控管理，在网络出现故障的时候，可以做到很好地故障定位。

本模块功能具有如下功能点：

- 支持纯物理接口的端口镜像。
- 支持入流量镜像/出流量镜像/双向流量镜像。
- 支持纯端口镜像，不支持 ACL 镜像。
- 支持一个接口流量镜像到一个或多个监控接口。
- 支持多个接口流量镜像到一个或多个监控接口。
- 支持配置的最大端口镜像规则数量为 8 条。
- 支持保护功能，当设备 packet buffer 数量使用率超过 3/4 时不再进行流量镜像。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解端口镜像特性。

3 使用限制

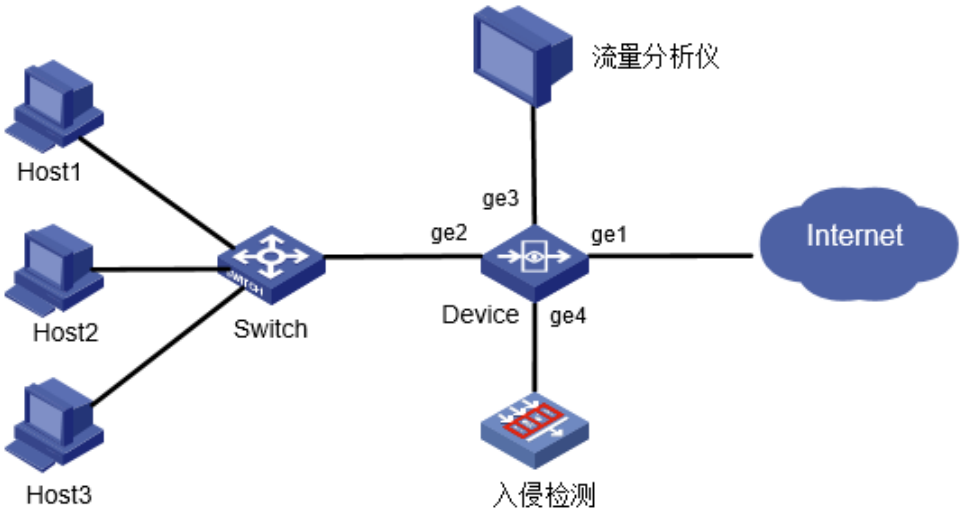
- 接口已经作为镜像规则源接口时不可再配置为其它规则的监控接口。
- 接口已经作为镜像规则监控接口时不可再配置为其它规则的源接口。
- 源接口和监控接口不能是同一个物理接口，要么配置为源接口，要么配置为监控接口，不能同时配置。
- 管理口以及旁路接口不可配置为监控接口。
- 在线业务口不可配置为监控接口（在线业务口即为现网在跑正常业务的物理接口）。
- 端口镜像规则数量规格为 8 条。

4 配置举例

4.1 组网需求

如图 1 所示用户有两台监控分析设备，功能不同，一台是专用流量分析仪，另一台是 IDS 设备。用户希望能对设备上去往和来自 Internet 的流量同时进行流量综合分析和入侵检测。

图1 组网图



4.2 配置思路

按照组网图组网。

(1) 登录 Web 网管。

(2) 新建端口镜像规则，将设备连接 Internet 接口流量镜像到设备与流量分析仪所连接口。

(3) 新建端口镜像规则，将设备连接 Internet 接口流量镜像到设备与 IDS 设备所连接口。

4.3 使用版本

本举例是在 E6201 版本上进行配置和验证的。

4.4 配置步骤

1. 新建端口镜像规则，将设备连接 Internet 接口流量镜像到设备与流量分析仪所连接口

如图 2 所示，进入“网络配置>基础网络>端口镜像”，新建端口镜像规则 port-mirror1，源端口为 ge1，监控接口为 ge3，规则类型为双向流量，点击<提交>按钮。

图2 新建端口镜像规则 port-mirror1

2. 新建端口镜像规则，将设备连接 Internet 接口流量镜像到设备与 IDS 设备所连接口

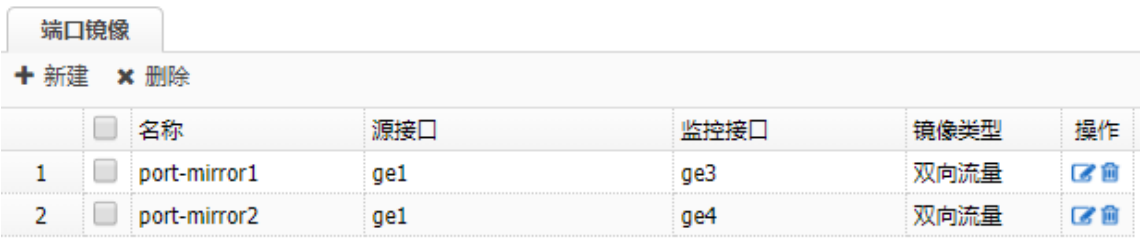
如图 3 所示，进入“网络配置>基础网络>端口镜像”，新建端口镜像规则 port-mirror2,源端口为 ge1，监控接口为 ge4，规则类型为双向流量，点击<提交>按钮。

图3 新建端口镜像规则 port-mirror2

3. 配置完成后效果图

如图 4 所示，配置完成后效果如下图。

图4 端口镜像配置效果图



4.5 验证配置

(1) 在设备查看接口流量大小，如下图所示，ge3、ge4 接口发送的流量大小等于 ge1 接口接收和发送流量之和。

图5 验证图

	名称	链路状态	属性	工作速率	双工模式	IP地址	IPv6地址	接收速率	发送速率	接收总包数	接收总字节数	发送总包数	发送总字节数	MAC地址
3	ge1	up	-	1000	full	211.136.100.1/24		529.60 Mbps	21.82 Mbps	3653944	5324240611	3645742	219321696	00:01:7a:c4:ca:a7
4	ge2	up	-	1000	full	172.16.1.1/24		21.82 Mbps	529.60 Mbps	3646255	219352476	3654205	5324283897	00:01:7a:c4:ca:a8
5	ge3	up	-	1000	full			0 bps	551.42 Mbps	0	0	7299757	5543613396	00:01:7a:c4:ca:a9
6	ge4	up	-	1000	full			0 bps	551.42 Mbps	0	0	7299794	5543644696	00:01:7a:c4:ca:aa

(2) 用户在两台监控分析设备上可以同时收到去往和来自 Internet 的流量，镜像功能生效。这样，用户就可以对去往和来自 Internet 的流量分别进行综合分析和入侵检测了。

目 录

1 简介

本文档介绍设备的旁路认证和阻断功能配置举例，设备上配置旁路认证和阻断功能之后，针对用户识别范围内的用户会进行旁路认证或者旁路阻断，对于没有认证的用户发送 http 302 报文重定向，防火墙控制策略为拒绝时，对匹配上安全策略的 TCP 报文发送 reset 报文，阻止用户访问网络。

开启旁路认证后需要配置用户认证策略，开启旁路阻断后需要配置控制策略。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

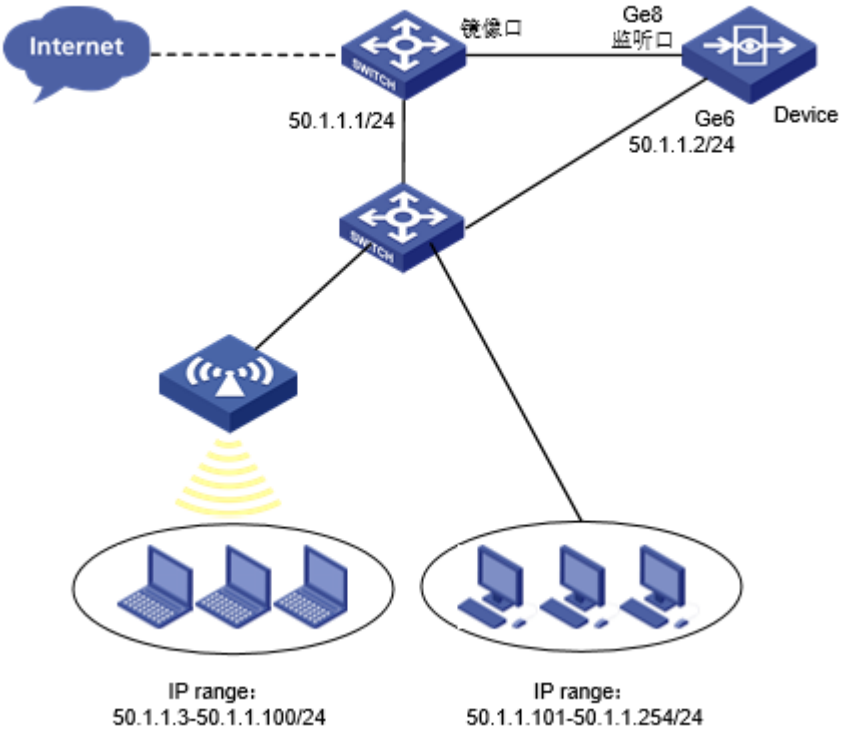
本文档假设您已了解旁路认证和阻断的特性。

3 旁路认证和阻断配置举例

3.1.1 组网需求

如图 1 所示，某企业对内网用户 50.1.1.3-100/24 工作时间都将进行用户认证和内网用户 50.1.1.101-254/24 工作时间都进行行为控制，不提供任何 NAT，DHCP 或者 DNS 服务。部署在交换机旁边，通过镜像的方式，仅仅提供认证和阻断的功能。旁路模式不修改网络结构，不关心网络细节，关机也不掉线，不会影响企业内部网络。

图1 旁路认证和阻断组网



3.1.2 配置思路

- 配置设备接口地址。
- 配置设备旁路部署。
- 配置设备旁路认证。
- 配置设备旁路阻断。
- 配置用户识别范围。
- 配置用户认证策略。
- 配置控制策略。

3.1.3 使用版本

本举例是在 E6201 版本上进行配置和验证的。

3.1.4 配置步骤

(1) 配置接口地址

如图 2 所示，进入“网络配置>接口配置>物理接口”，点击 ge6<编辑>按钮，配置 ge6 的 IP 地址为 50.1.1.2/24。

图2 配置接口地址

	接口名称	描述	IP地址	IPv6地址	MAC地址	工作模式	双工模式	速率(Mbps)	连接状态	启用状态	操作
1	ge0				00:21:45:c8:15:c0	route	full	1000	down		
2	ge1				00:21:45:c8:15:c1	route	full	1000	down		
3	ge2				00:21:45:c8:15:c2	route	full	1000	down		
4	ge3				00:21:45:c8:15:c3	route	full	1000	down		
5	ge4				00:21:45:c8:15:c4	route	full	1000	down		
6	ge5				00:21:45:c8:15:c5	route	full	1000	down		
7	ge6		50.1.1.2/24		00:21:45:c8:15:c6	route	full	1000	up		
8	ge7				00:21:45:c8:15:c7	route	full	1000	down		
9	ge8				00:21:45:c8:15:c8	listen	full	1000	up		
10	ge9				00:21:45:c8:15:c9	route	full	1000	down		

(2) 配置部署方式

如图 3 所示，进入“网络配置>基础网络>部署方式”，配置勾选 ge8 口启用。

图3 配置部署方式

(3) 配置旁路认证和阻断

如图 4 所示，进入“网络配置>基础网络>部署方式>高级配置”，配置旁路认证和旁路阻断。

图4 配置旁路认证和旁路阻断

(4) 配置内网用户地址对象

如图 5 所示，进入“策略配置>对象管理>地址对象>地址对象”，点击<新建>按钮创建内用户地址对象 50.1.1.0/24、50.1.1.3 和 50.1.1.101，点击<提交>。

图5 配置内网用户地址对象

(5) 配置用户识别范围

如图 6 所示，进入“用户管理>认证管理>高级选项>全局配置”页面，识别范围选择“50.1.1.0”，其它配置默认，提交配置。

图6 用户识别范围

(6) 配置用户认证策略

如图 7 所示，进入“用户管理>认证管理>认证策略”，新建一条认证方式为本地认证的认证策略，源地址选择 50.1.1.3，其它配置默认，<提交>策略。

图7 配置用户认证策略

(7)　配置控制策略

如图 8 所示，进入“策略配置>控制策略”，源地址选择 50.1.1.101，行为选择拒绝，其它配置默认，<提交>策略。

图8 配置控制策略

3.1.5 配置注意事项

- 用户认证策略和控制策略的源接口以及目的接口必须配置接收镜像流量的旁路部署接口或者是 any。
- 旁路认证和阻断务必保证旁路设备到上网 PC 可达，否则功能无法使用。
- 旁路阻断只针对于 TCP 报文生效，对于 UDP、ICMP 等报文无法进行阻断。

3.1.6 验证配置

如图 9 所示，内网用户（50.1.1.3）访问外网需要进行本地认证，本地认证成功后，访问外网成功。

图9 内网用户需要进行本地认证

如图 10 所示，内网用户（50.1.1.101）访问外网资源会被阻断。

图10 内网用户访问外网阻断

4 配置文件

```
!
!
interface ge6
 ip address 50.1.1.2/24
 allow access https
 allow access http
 allow access ping
 allow access ssh
 allow access telnet
 allow access center-monitor
!
interface ge7
!
interface ge8
!
interface ge9
 deploy-mode listen enable
policy any any 50.1.1.101 any any any any always any deny 1
policy default-action permit
policy white-list enable
!
!policy-decrypt
!
```

policy listen block enable

!

user-policy listen authentication enable

user-policy https-portal enable

user-policy any any 50.1.1.3 any always local-webauth enable test no-record forever

目 录

1 简介

本文档介绍设备的全局白名单功能配置举例，设备上配置全局白名单功能之后，针对配置白名单的用户网络基础转发会匹配，应用识别会匹配，其它策略模块流程将都不会匹配，直接放通处理。

全局白名单配置支持 IP 地址和 MAC 地址两种格式。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

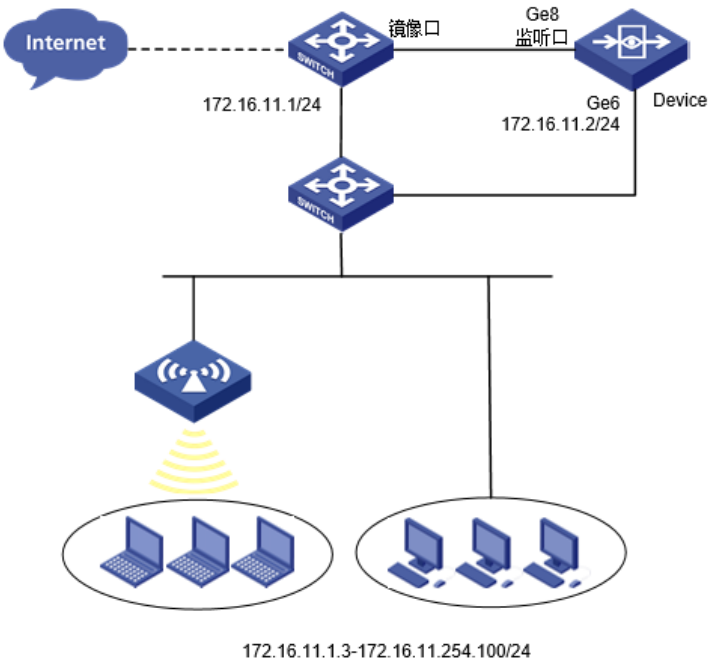
本文档假设您已了解全局白名单特性。

3 全局白名单配置举例

3.1 组网需求

如图 1 所示，某企业对内网用户 172.16.11.0/24 在工作时间进行审计并控制登录即时通讯软件，但是对该内网用户中 172.16.11.3 地址不需要进行审计和控制，通过全局白名单实现该需求。

图1 全局白名单组网



3.2 配置思路

- 配置网络接口。
- 配置旁路部署、旁路阻断。
- 配置内网用户地址对象。
- 配置时间对象。
- 配置用户识别范围。
- 配置审计策略。
- 配置控制策略。
- 配置全局白名单。

3.3 使用版本

本举例是在 E6201 版本上进行配置和验证的。

3.4 配置步骤

(1) 配置接口地址

如图 2 所示，进入“网络配置>接口配置>物理接口”，点击 ge6<编辑>按钮，配置 ge6 的 IP 地址为 172.16.11.2/24。

图2 配置接口地址

(2) 配置部署方式

如图 3 所示，进入“网络配置>基础网络>部署方式”，配置勾选 ge8 口启用。

图3 配置部署方式

(3)　配置旁路认证和阻断

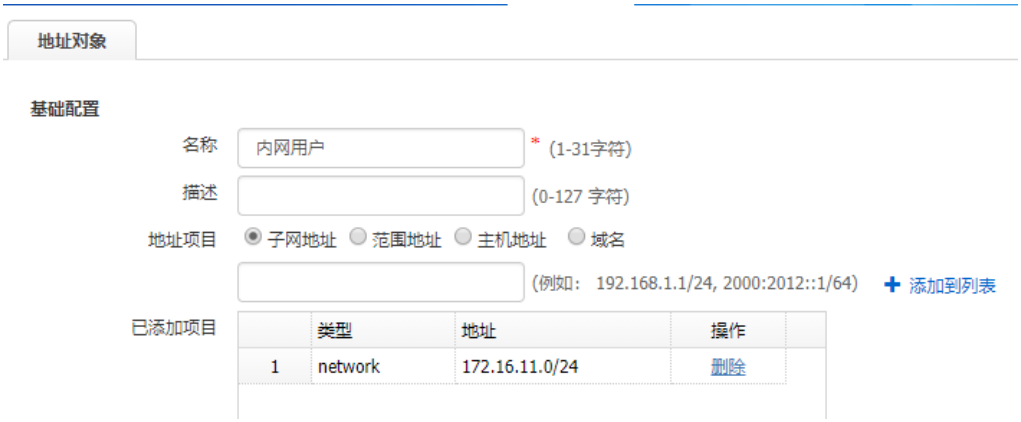
如图 4 所示，进入“网络配置>基础网络>部署方式>高级配置”，配置旁路阻断。

图4 配置旁路阻断

(4)　配置内网用户地址对象

如(4)图 5 所示，进入“策略配置>对象管理>地址对象>地址对象”，点击<新建>按钮创建内网用户地址对象 172.16.11.0/24，点击<提交>。

图5 配置内网用户地址对象



(5)　配置用户识别范围

如(5)图 6 所示，进入“用户管理>认证管理>高级选项>全局配置”页面，识别范围选择“内网用户”，其它配置默认，提交配置。

图6 用户识别范围

(6) 配置审计策略

如图 7 所示，进入“策略配置>审计策略”，源地址选择内网用户，审计对象配置所有，时间选择工作时间，其它配置默认，<提交>策略。

图7 配置审计策略

(7) 配置控制策略

如图 8 所示，进入“策略配置>控制策略”，源地址选择内网用户，应用控制策略配置一条应用选择即时通讯类动作配置拒绝，日志级别配置通知，时间选择工作时间，其它配置默认，<提交>策略。

图8 配置控制策略

(8) 配置全局白名单

如图 9 所示，进入“策略配置>全局白名单”，点击<新建>配置一条地址 172.16.11.3 的全局白名单策略。

图9 配置全局白名单

3.4.2 配置注意事项

- 配置的全局白名单地址必须在用户识别范围中，且全局白名单地址只匹配会话中源 IP 和源 MAC。

3.4.3 验证配置

如图 10 所示，分别使用白名单用户（172.16.11.3）和非白名单用户（172.16.11.11）工作时间访问外网，白名单用户访问外网没有相关上网行为审计日志，非白名单用户访问外网有相关上网行为审计日志。

图10 非白名单用户访问外网审计日志

如图 11 所示， 白名单用户工作时间分别登录 QQ 和微信即时通讯聊天软件，只有白名单用户能登录，无相关日志；非白名单用户无法登录，有相应的应用控制阻断日志。

图11 非白名单用户登录即时聊天软件被阻断日志

应用控制日志

查询 重置 导出 **查询结果:** 在 2019-03-26 约 69 条日志记录中，从 1 - 69 搜索出相关结果 69 条

	用户	用户mac	应用分类	应用	策略类型	处理动作	终端类型	级别	时间
1	10.1.1.11	64:9a:be:8b:85:44	即时通讯	微信_登录	应用控制	阻断	移动终端	通知	2019-03-26
2	10.1.1.11	64:9a:be:8b:85:44	即时通讯	QQ(移动端)_登	应用控制	阻断	移动终端	通知	2019-03-26
3	10.1.1.11	64:9a:be:8b:85:44	即时通讯	微信_登录	应用控制	阻断	移动终端	通知	2019-03-26
4	10.1.1.11	64:9a:be:8b:85:44	即时通讯	微信_登录	应用控制	阻断	移动终端	通知	2019-03-26
5	10.1.1.11	64:9a:be:8b:85:44	即时通讯	微信_登录	应用控制	阻断	移动终端	通知	2019-03-26
6	10.1.1.11	64:9a:be:8b:85:44	即时通讯	微信_登录	应用控制	阻断	移动终端	通知	2019-03-26
7	10.1.1.11	64:9a:be:8b:85:44	即时通讯	微信_登录	应用控制	阻断	移动终端	通知	2019-03-26
8	10.1.1.11	64:9a:be:8b:85:44	即时通讯	微信_登录	应用控制	阻断	移动终端	通知	2019-03-26
9	10.1.1.11	64:9a:be:8b:85:44	即时通讯	微信_登录	应用控制	阻断	移动终端	通知	2019-03-26
10	10.1.1.11	64:9a:be:8b:85:44	即时通讯	QQ(移动端)_登	应用控制	阻断	移动终端	通知	2019-03-26
11	10.1.1.11	64:9a:be:8b:85:44	即时通讯	QQ(移动端)_登	应用控制	阻断	移动终端	通知	2019-03-26

目录

1 简介

本文档介绍设备的入侵防御功能配置举例。随着互联网的飞速发展，网络环境也变得越来越复杂，恶意攻击、木马、蠕虫病毒等混合威胁不断增大，单一的防护措施已经无能为力，企业需要对网络进行多层、深层的防护来有效保证其网络安全，而入侵防御系统则是提供深层防护体系的保障。

入侵防御涉及以下概念：

- 规则模板：规则模板是一个或多个规则的集合，规则模板分为预定义规则模板、派生规则模板和自定义规则模板。

  预定义规则模板由系统自动创建，其中包含的规则以及每条规则的配置（阻断、抓包等）也都由系统预先设定，规则不允许增加或删除，每条规则的配置也不允许修改。预定义规则模板包括以下四个：

  - ALL：包含全部规则
  - Webserver：Web 规则模板
  - Windows：包含 Windows 系统漏洞规则
  - Unix-like：包含 Unix、Linux 系统漏洞规则

  派生规则模板由预定义规则模板派生而来，其中包含的规则与对应的预定义规则模板相同，也是不允许增加或删除，但是可以修改每条规则的配置。派生规则模板由用户根据需要手动派生创建，派生规则模板不可以再派生。

  自定义规则模板完全由用户自己定义创建，其中包含的规则以及配置都可以随意修改。
- 规则：规则除了包含有检测攻击的特征之外，还有规则严重程度、规则状态、日志、阻断、隔离、抓包，CVE、CNNVD、操作系统、发布年份、厂商，操作。一条规则可以属于多个规则模板。

  入侵防御安全引擎提供自定义规则功能，通过对进入设备报文的协议类型，协议字段，字段内容形成匹配条件，并通过逻辑与、逻辑或形成多条件匹配的方式实现入侵防御。安全管理员可以使用自定义规则功能，自己写签名进行防护。自定义规则检测是基于流检测的，支持多种协议字段，其中包括 IP、UDP、TCP、FTP、HTTP、ICMP、POP3、SMTP 协议。对于字符串字段，可支持正则和非正则匹配的方式。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解入侵防御特性。

3 使用限制及注意事项

- 由于部分特征需要修改检测深度才行识别，可以通过配置 max-ips-detect 4096 命令，提升检测深度，注：此命令只适合测试使用，实际使用开启此命令，会导致性能大幅度下降。

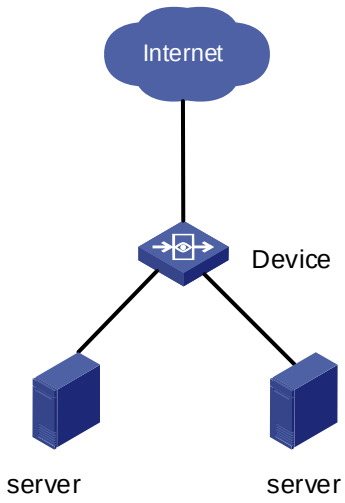
- 设备同时配置有日志聚合和告警规则时，告警规则优先，即：匹配命中告警规则的报文产生的日志不聚合。
- IPS 自定义规则最多可配置 32 条，每条自定义规则最多可包含 8 个协议字段，每个协议字段最多可包含 8 个协议匹配条件。
- IPS 规则如果配置了阻断，命中该规则后会丢弃当前报文。如果是 TCP 协议，阻断会发 rst；如果是 UDP 协议，阻断直接丢弃报文。阻断只是阻断当前连接或会话。
- IPS 规则如果配置了隔离，命中该规则后会将报文的源地址加入加黑名单（时间可配置），加黑名单以后，该地址用户后续的报文都会阻断。
- IPS 的防逃避功能只能通过命令行开启，Web 页面不支持配置，此功能开启后对性能影响比较大，不建议开启，仅在特殊场景下使用。
- 因为目前仅支持木马后门、蠕虫病毒、挖矿、webshell、木马外联五类攻击，因为这五类攻击是攻击渗透成功之后做的向外传输数据的动作，一般有这种流量基本确定内网已有主机被攻陷，所以能断定被攻击成功，其它种类攻击目前暂不支持判断，入侵日志中的成功标志为否。

4 配置举例

4.1 组网需求

如图 1 所示，服务器通过 Internet 提供 Web 和 FTP 服务，在设备上启用入侵防御功能来保护 Web 和 FTP 服务器。同时通过自定义规则来禁止使用除 210 以外的端口访问 FTP 服务器，且不允许上传文件和新建目录，为了减少日志量，按照规则进行日志聚合。

图1 入侵防御功能配置组网图



4.2 配置思路

- 配置模板，决定需要对哪些规则做检测，并决定检测到攻击之后的日志和动作，可以使用系统预定义的模板，也可以自定义新的模板。

- 配置控制策略，在控制策略中配置入侵防御，引用已经配置的模板，对命中控制策略的流量做入侵防御相关的检测。

4.3 使用版本

本举例是在 E6201 版本上进行配置和验证的。

4.4 配置注意事项

- 入侵防御策略匹配是由上至下进行匹配，策略匹配到之后将不会往下继续匹配。
- 是否启用防护模式，只有启用防护模式且模板下的规则或协议异常检查配置为阻断，匹配到策略后才会阻断流量。

4.5 配置步骤

4.5.1 配置自定义入侵防御规则

进入“策略配置>安全设置>入侵防御>规则库”，进入 IPS 自定义规则配置页面，禁止使用除 210 以外的端口访问 FTP 服务器，且不允许上传文件和新建目录。

图2 配置自定义入侵防御规则

4.5.2 配置入侵防御模板

进入“策略设置>安全设置>入侵防御>模板”，进入入侵防御配置页面，新建模板并添加规则，如下图所示。

图3 新建入侵防御模板

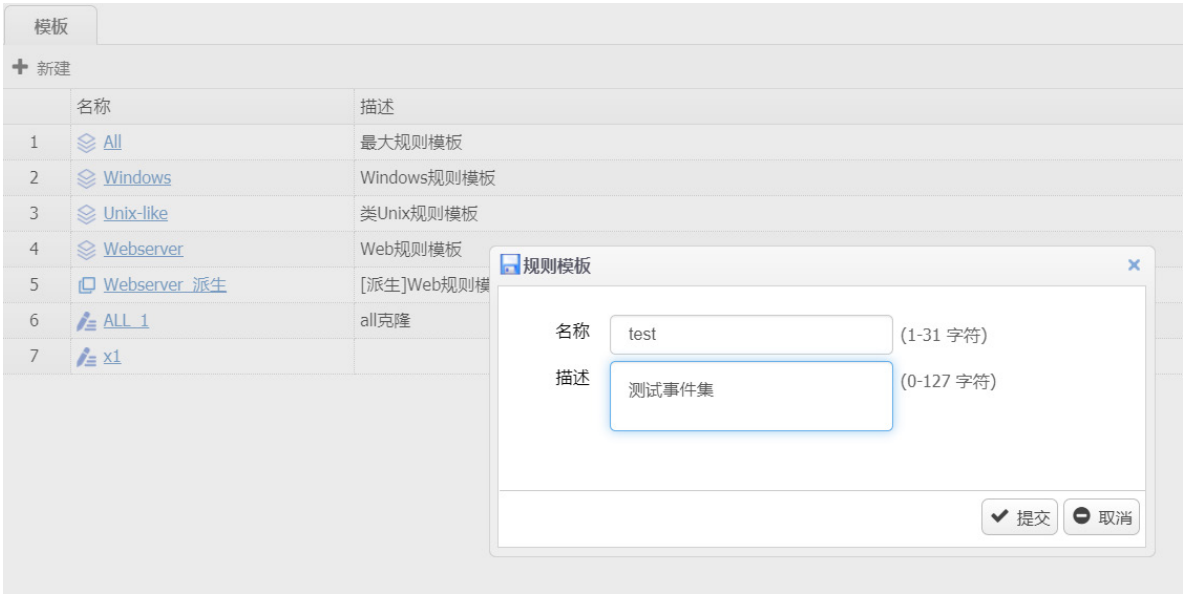
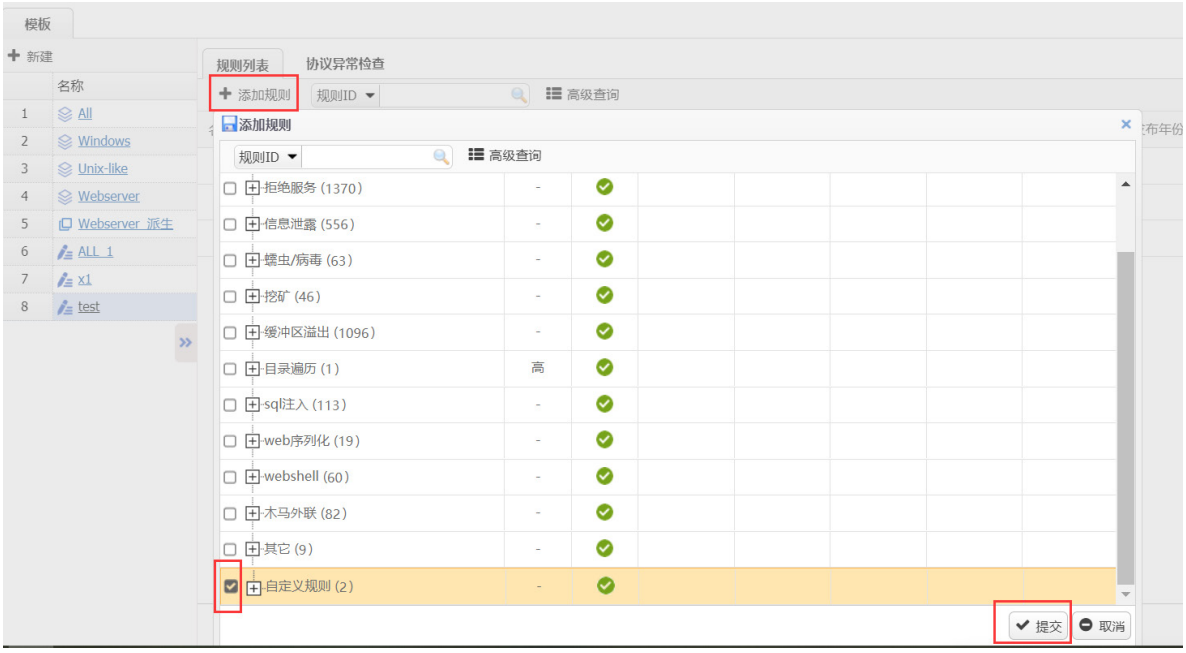


图4 添加规则



4.5.3 配置控制策略

进入“策略配置>策略配置>控制策略”，进入控制策略页面，如图 5 所示，新建策略，在入侵防御子菜单中启用功能并选择模板“test”，完成后点击提交。

图5 配置控制策略

4.5.4 配置日志聚合

进入“数据中心>日志中心>安全日志>入侵日志”，进入日志聚合配置页面，如 4.5.3 图 5 所示，选择聚合方式点击提交。

图6 配置日志聚合

4.6 验证配置

4.6.1 默认入侵防御功能验证

使用测试 PC 进行攻击操作。在“数据中心>日志中心>安全日志>入侵日志”中可看到相应攻击日志信息，如图 7 所示。

图7 入侵日志

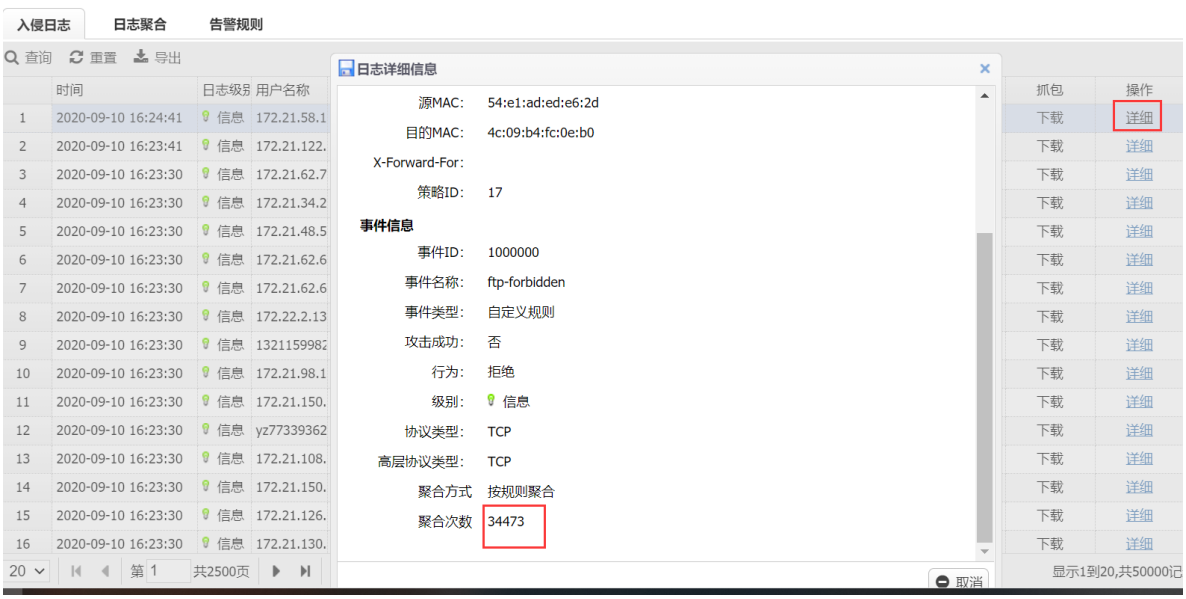
4.6.2 自定义入侵防御功能验证

配置完成自定义 IPS 规则后，用户只能使用 210 端口访问 FTP 服务器，可以下载文件，但是无法上传和创建目录。否则无法登录服务器，并记录相应日志信息。使用测试 PC 进行 FTP 服务器登录操作，在“数据中心>日志中心>安全日志>入侵日志”中可看到相应日志信息，如图 8 所示。

图8 入侵检测日志

在“数据中心>日志中心>安全日志>入侵日志”中可看到相应日志信息，如图 8 所示。

图9 入侵检测日志聚合



目 录

1 简介

本文档介绍设备的病毒防护配置举例，设备可以针对内外网入口处，进行实时的病毒扫描，将外来病毒隔离在内网之外，实现工作站被动防御病毒之外的主动病毒防护，我们可以在诸如 HTTP、FTP、IMAP、POP3、SMTP 等应用协议时进行文件扫描。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解病毒防护特性。

3 使用限制

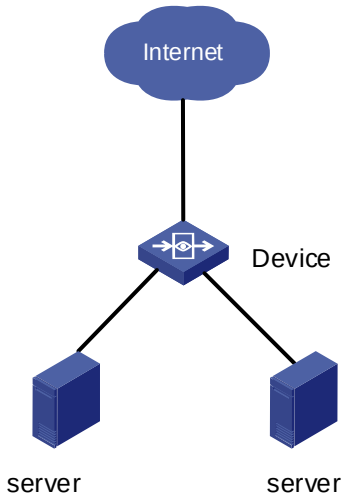
- 压缩包最大解压层数为 20 层。
- 病毒文件大小小于 2M。
- 不支持 rar 文件格式解压。

4 病毒防护配置举例

4.1 组网需求

如图 1 所示，某公司内网存在两台服务器，测试设备可以针对内外网入口处进行实时病毒扫描，实现服务器主动病毒防护功能，模拟测试服务器通过 FTP 进行下载带有病毒文件操作或局域网内上传带有病毒文件操作。

图1 病毒防护测试组网图



4.2 配置思路

- 配置防病毒设定，设置病毒文件扫描类型
- 配置安全策略，启用病毒防护功能

4.3 使用版本

本举例是在 E6201 版本上进行配置和验证的。

4.4 配置步骤

1. 配置防病毒设定，设置病毒文件扫描类型

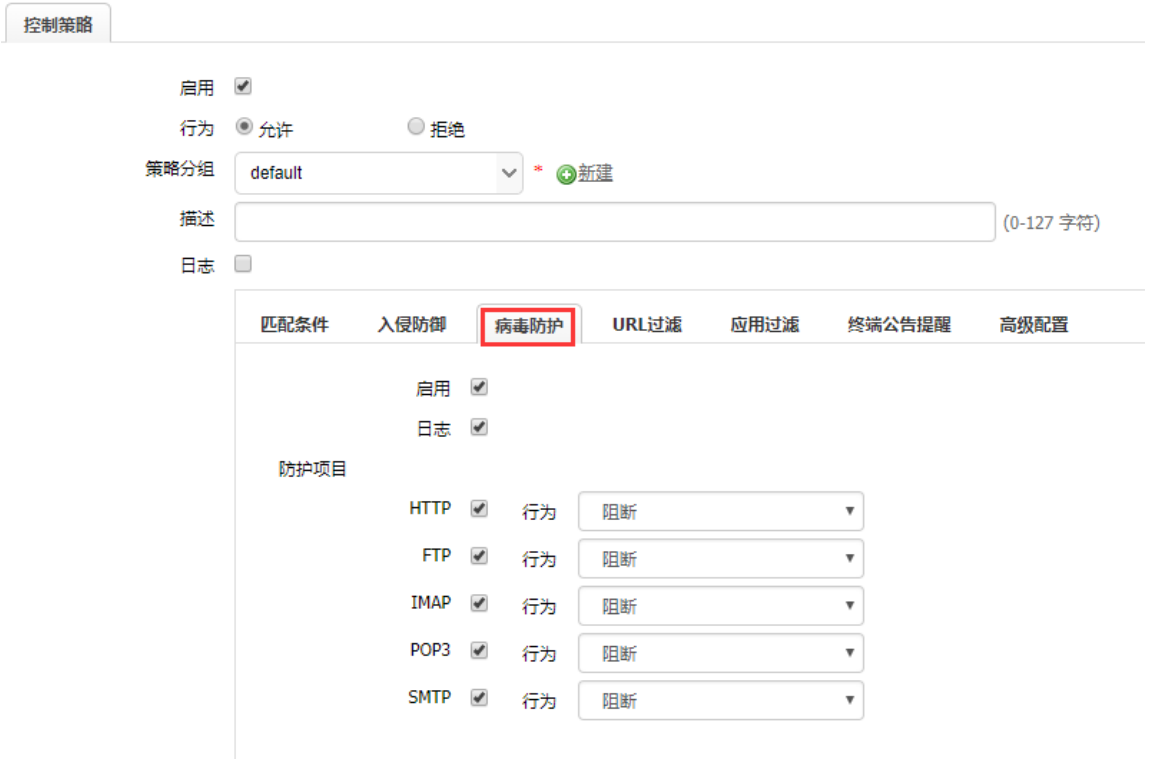
如图 2 所示，进入“策略配置 > 安全设备 > 病毒防护 > 防病毒设定”，勾选<启用解压>，选择最大解压层数，选择扫描文件类型或勾选<扫描所有文件>。

图2 配置防病毒设定

2. 配置安全策略，启用病毒防护功能

如图 3 所示，进入“策略配置>控制策略”，进入控制策略页面，新建策略，病毒防护子菜单中启用功能并选择防护项，完成后点击提交。

图3 配置安全策略



4.5 验证配置

(1) 验证病毒防护功能

在导航栏中选择“数据中心>日志中心>安全日志>病毒防护日志”，进入病毒防护日志页面，可以查看到病毒防护日志信息。

图4 病毒防护日志查看

4.6 配置注意事项

- 及时升级最新规则库。
- 防护策略开启并引用。
- 匹配策略 IP 端口的流量通过病毒防护系统转发。

目录

1 简介

暴力破解是指攻击者通过穷举的方法登录相应服务从而获得可以登录的用户名密码对。用户可配置防暴力破解功能，通过检测出流量中的暴力破解行为并进行阻断。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解防暴力破解特性。

3 使用限制

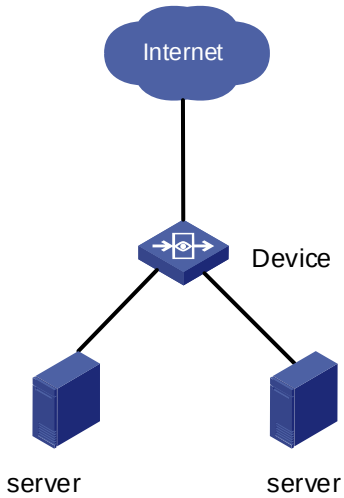
- 管理员可以设定最大登录重试次数默认为 5 次。
- 如果某账户连续输入错误的口令次数超过最大登录重试次数，系统将锁定该账户。为了防止攻击者通过不断尝试，故意造成的 DOS 攻击，设备在一定时间后会自动解锁，在不影响正常使用的同时，尽可能的降低攻击风险。

4 配置举例

4.1 组网需求

如图 1 所示，服务器通过 Internet 提供 FTP 服务，在设备上启用防暴力破解功能来监测攻击行为，当攻击次数达到阈值触发防暴力破解记录攻击事件。同时实施相应措施保护 FTP 服务器。

图1 防暴力破解功能配置组网图



4.2 配置思路

- 配置服务类型，在防暴力破解配置页面选择监测的服务。
- 配置检测时长，选择防暴力破解的检测周期。
- 配置阈值，达到阈值触发防暴力破解记录攻击事件。阈值范围为 3-1000。
- 配置响应行为，是否将攻击者加入黑名单，阻断攻击行为。

4.3 使用版本

本举例是在 E6201 版本上进行配置和验证的。

4.4 配置注意事项

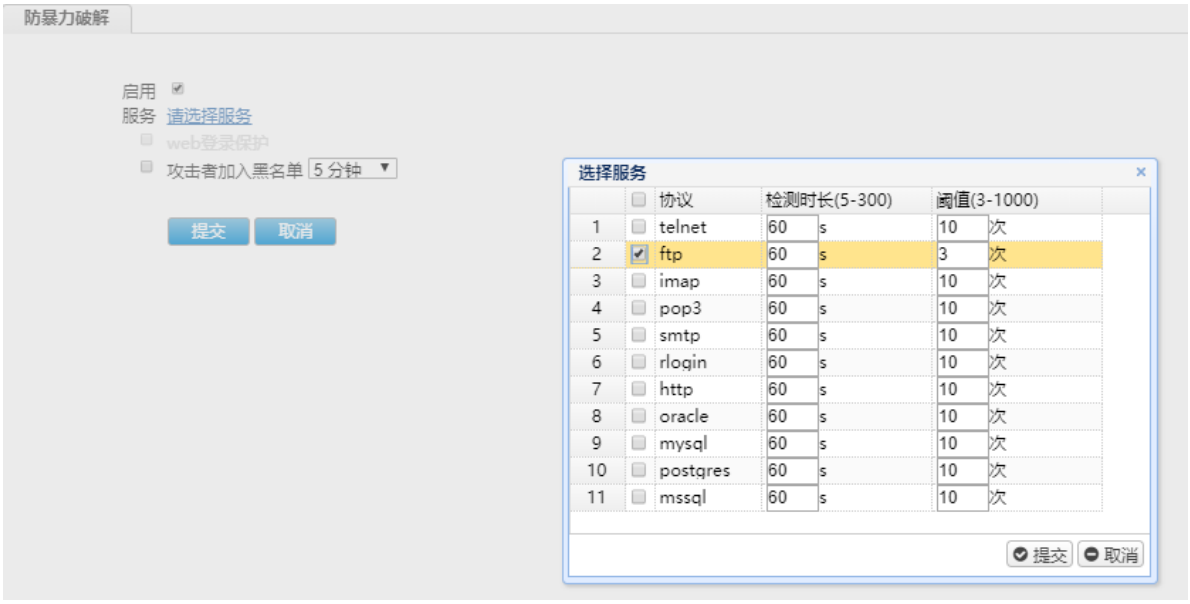
- 防暴力破解功能支持的服务类型包括 ftp、telnet、smtp、http、imap、mssql、mysql、oracle、pop3、postgres。
- 各个服务单独配置暴力破解检测时长和阈值。
- 系统支持配置是否把攻击者加入黑名单。本例分别在两种情况下进行。

4.5 配置步骤

4.5.1 启用防暴力破解功能

进入“安全设置>安全防护>防暴力破解”，进入防暴力破解配置页面，如图 2 所示。设置启用防暴力破解功能，选择服务类型为 FTP，检查次数 3。提交配置。

图2 配置防暴力破解



4.5.2 配置攻击者加入黑名单

进入“安全设置>安全防护>防暴力破解”，进入防暴力破解配置页面，如图 3 所示，设置攻击者加入黑名单时长，提交配置。

图3 配置 IPv4 策略

4.6 验证配置

使用测试 PC 进行 FTP 爆破测试。

(1) 未配置攻击者加入黑名单情况下进行 FTP 爆破测试

在导航栏中选择“数据中心>日志中心>安全日志>防暴力破解日志”，进入防暴力破解日志页面，可以查看到防暴力破解日志信息。如图 4 所示。

图4 防暴力破解日志

防暴力破解日志

查询 导出

	时间	源地址	归属地	目的地址	服务	防御动作
1	2020-01-02 16:22:23	192.168.20.50	局域网	192.168.1.116	ftp	加入黑名单
2	2020-01-02 16:19:07	192.168.20.50	局域网	192.168.1.116	ftp	忽略
3	2020-01-02 16:18:57	192.168.20.50	局域网	192.168.1.116	ftp	忽略
4	2020-01-02 16:18:57	192.168.20.50	局域网	192.168.1.116	ftp	忽略
5	2020-01-02 16:18:57	192.168.20.50	局域网	192.168.1.116	ftp	忽略
6	2020-01-02 16:18:57	192.168.20.50	局域网	192.168.1.116	ftp	忽略
7	2020-01-02 16:18:57	192.168.20.50	局域网	192.168.1.116	ftp	忽略
8	2020-01-02 16:18:57	192.168.20.50	局域网	192.168.1.116	ftp	忽略
9	2020-01-02 16:18:57	192.168.20.50	局域网	192.168.1.116	ftp	忽略
10	2020-01-02 16:18:57	192.168.20.50	局域网	192.168.1.116	ftp	忽略
11	2020-01-02 16:18:57	192.168.20.50	局域网	192.168.1.116	ftp	忽略
12	2020-01-02 16:18:57	192.168.20.50	局域网	192.168.1.116	ftp	忽略

(2) 配置攻击者加入黑名单下情况进行 FTP 爆破测试

在导航栏中选择“数据中心>系统监控>黑名单记录”，进入黑名单页面，可以查看到防暴力破解加入黑名单信息。如图 5 所示。

图5 黑名单记录

黑名单 黑名单记录

查询

	源IP	生命周期	生效时间	添加方式
1	192.168.20.50	5分0秒	2020-01-02 16:22:23	防暴力破解

目 录

1 简介

对于密码明文传输的服务，从登录报文中提取出密码并判断出密码强度，若为弱密码则产生日志但不阻断登录。支持的服务包括 ftp、imap、pop3、smtp、telnet。用户可以配置开启或者关闭弱密码检测功能，目标服务，弱密码密码强度。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解弱密码防护特性。

3 使用限制

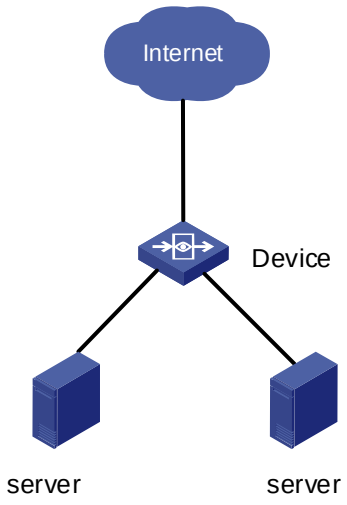
无。

4 配置举例

4.1 组网需求

如图 1 所示，某公司内网存在两台服务器，测试设备可以针对内外网进行弱密码防护日志记录，实现弱密码防护功能，测试服务器通过 FTP 对另一台服务器进行弱密码登录。

图1 弱密码防护测试组网图



4.2 配置思路

- 配置弱密码防护功能
- 配置默认规则库与自定义弱密码

4.3 使用版本

本举例是在 E6201 版本上进行配置和验证的。

4.4 配置步骤

1. 弱密码防护配置

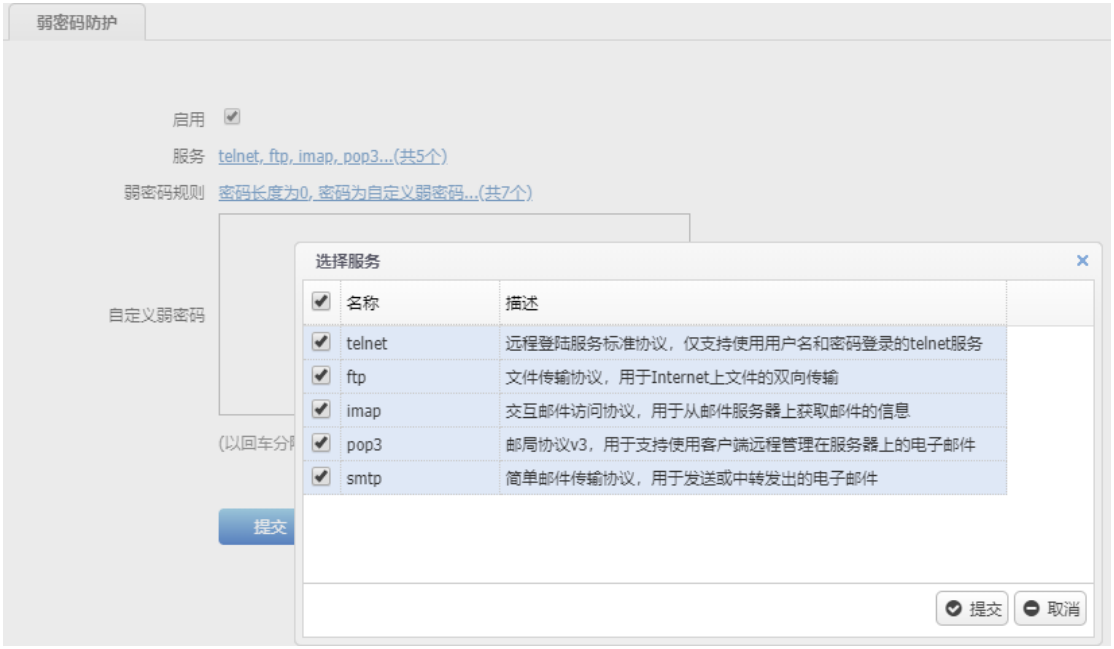
如图 2 所示，在导航栏中选择“策略配置>安全设置>安全防护>弱密码防护”，进入弱密码防护的配置界面，勾选启用。

图2 开启弱密码防护设定

2. 防护服务类型选择

如图 3 所示，点击“选择服务”弹框出现服务配置页面，选择弱密码防护服务。

图3 配置弱密码防护服务



4.5 验证配置

(1) 验证弱密码防护功能

如图 4 所示，在导航栏中选择“数据中心>日志中心>安全日志>弱密码防护日志”，进入弱密码防护日志页面，可以查看到弱密码防护日志信息。

图4 弱密码防护验证

	时间	源地址	服务器地址	服务	用户名称	弱密码类型
1	2020-01-02 15:40:58	192.168.2.50	192.168.1.116	ftp	admin	密码长度小于等于8 且为字典序
2	2020-01-02 15:40:58	192.168.2.50	192.168.1.116	ftp	admin	密码长度小于等于8 且为字典序

目 录

1 简介

ND 协议是 IPv6 协议中的一个关键协议，但是，由于 ND 协议并未提供认证机制，导致网络中的节点不可信，也使攻击者有机可乘，可针对 ND 协议发起一系列攻击。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

3 使用限制

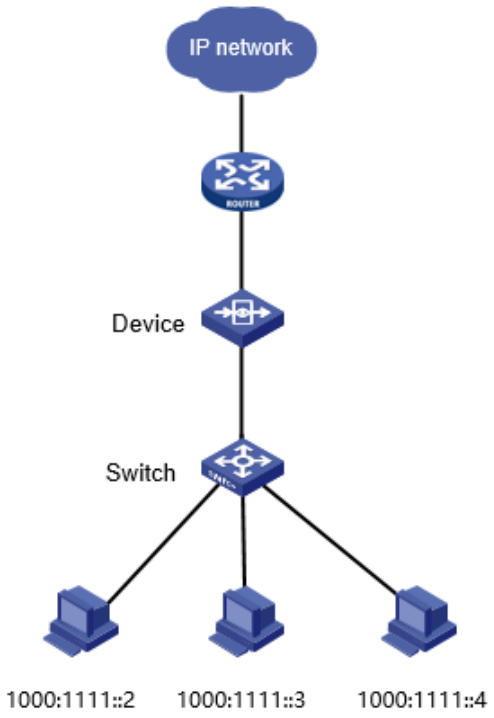
必须保证设备间通信数据经过设备转发。

4 配置举例

4.1 组网需求

如图 1 所示，公司内网有多台服务器设备，防止服务器被局域网内 PC 进行 ND 欺骗造成服务器无法正常访问。

图1 ND 防护典型组网图



4.2 配置思路

(1) 开启防 ND 欺骗功能。

(2) 开启防止 ND Flood 攻击。

4.3 使用版本

本举例是在 E6201 版本上进行配置和验证的。

4.4 配置步骤

(1) 开启防 ND 欺骗

如图 2 所示，进入“策略配置>安全设置>安全防护>ARP/ND 攻击防护>防 ND 欺骗”；关闭 ND 学习，开启 ND 反向查询，设置每 MAC 地址 IP 数检查，开启接口主动保护，点击<提交>按钮提交配置。

图2 启用防 ND 欺骗

(2) 配置 IP-MAC 绑定

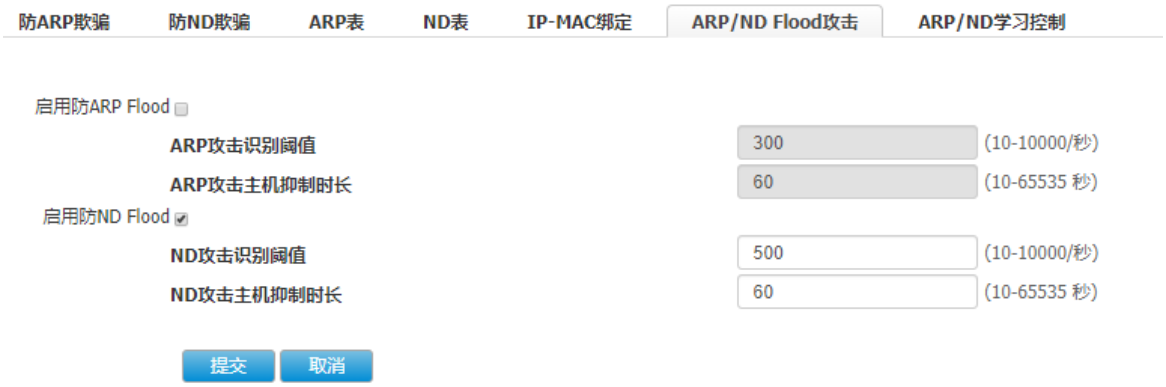
如图 3 所示，进入“策略配置>安全设置>安全防护>ARP/ND 攻击防护>IP-MAC 绑定”；绑定被保护服务器的 IPMAC 地址，勾选唯一性，点击<提交>按钮提交配置。

图3 配置 IP-MAC 绑定

(3) 配置 ARP/ND Flood 攻击

如图 4 所示，进入“策略配置>安全设置>安全防护>ARP/ND 攻击防护>ARP/ND Flood 攻击”；设置阈值和抑制时长，点击<提交>按钮提交配置。

图4 配置 ND Flood 攻击防护



4.5 验证配置

如图 5 所示，进入>“数据中心>安全日志>安全防护日志”，进入安全防护日志显示页面。

图5 防 ND 欺骗日志

安全防护日志

查询 重置 导出

		日志级别	源MAC	源IP	归属地	目的IP	协议	威胁名称	威胁类型	攻击次数	接口	开始时间
1521	9 11:37:24	警告	00:50:56:b8:0c:75	b001:1111:2222:3333:4444:5555:6666:124b:0	未知	ff02::1:ff66:aaa1:0	ICMP	permac-ipcount-che	nd-attack	1000	mgt3	2019-12-09 11:37:13
1522	9 11:37:14	警告	00:50:56:b8:0c:75	b001:1111:2222:3333:4444:5555:6666:124b:0	未知	ff02::1:ff66:aaa1:0	ICMP	permac-ipcount-che	nd-attack	213	mgt3	2019-12-09 11:37:11
1523	9 10:27:23	警告	00:50:56:b8:0c:75	b001:1111:2222:3333:4444:5555:6666:156f:0	未知	ff02::1:ff66:aaa1:0	ICMP	nd-flood	nd-attack	828	mgt3	2019-12-09 10:27:14
1524	9 10:27:13	警告	00:50:56:b8:0c:75	b001:1111:2222:3333:4444:5555:6666:1b62:0	未知	ff02::1:ff66:aaa1:0	ICMP	nd-flood	nd-attack	582	mgt3	2019-12-09 10:27:02
1525	9 10:27:03	警告	00:50:56:b8:0c:75	b001:1111:2222:3333:4444:5555:6666:191c:0	未知	ff02::1:ff66:aaa1:0	ICMP	nd-flood	nd-attack	2294	mgt3	2019-12-09 10:26:52
1526	9 10:26:53	警告	00:50:56:b8:0c:75	b001:1111:2222:3333:4444:5555:6666:209b:0	未知	ff02::1:ff66:aaa1:0	ICMP	nd-flood	nd-attack	3339	mgt3	2019-12-09 10:26:42
1527	9 10:26:43	警告	00:50:56:b8:0c:75	b001:1111:2222:3333:4444:5555:6666:135e:0	未知	ff02::1:ff66:aaa1:0	ICMP	permac-ipcount-che	nd-attack	288	mgt3	2019-12-09 10:26:41
1528	9 10:26:43	警告	00:50:56:b8:0c:75	b001:1111:2222:3333:4444:5555:6666:1390:0	未知	ff02::1:ff66:aaa1:0	ICMP	nd-flood	nd-attack	50	mgt3	2019-12-09 10:26:42
1529	9 10:21:52	警告	00:50:56:b8:0c:75	b001:1111:2222:3333:4444:5555:6666:1236:0	未知	ff02::1:ff66:aaa1:0	ICMP	nd-flood	nd-attack	5429	mgt3	2019-12-09 10:21:41

目录

1 简介

随着网络信息化的发展，越来越多的企业利用 WEB 应用系统提供客户服务，进行产品推广、市场宣传、培训服务、远程服务协作甚至网上交易。WEB2.0 的发展更是加强了用户和 WEB 服务之间的交互性，但是各种安全问题也随之而来。WEB 应用数据被窃取、网页被篡改，甚至 WEB 站点成为传播木马的傀儡，给更多访问者造成危害，带来损失；也对政府、公司形象造成严重的破坏。目前 WAF 设备产品是用户用来保护 WEB 应用的首要选择。为了能够给客户提供一套更完全的安全解决方案，Web 应用防护作为一个功能模块，整体上基于当前的平台设计实现，增加 WEB 应用防护策略，匹配条件是源地址、目的地址（WEB 服务器地址）和端口，同时在策略下配置各个防护功能（精确访问控制、规则防护、防盗链、CSRF 攻击防护、CC 攻击防护、网页防篡改、应用隐藏），当报文匹配策略时，就会逐一进行防护功能的处理，并执行相应的动作。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 WEB 防护特性。

3 使用限制

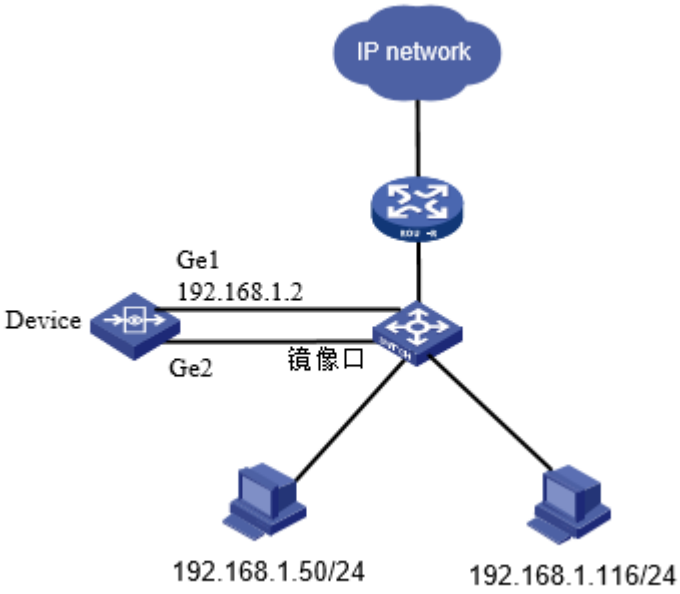
WEB 防护的优先级是精确访问控制、规则防护、防盗链、CSRF 攻击防护、CC 攻击防护、网页防篡改、应用隐藏，在未阻断情况下依次防护。

4 WEB 防护配置举例

4.1 组网需求

如图 1 所示，设备以旁路的方式部署在网络的关键节点上，将用户上网的流量通过端口镜像的方式镜像至设备的旁路接口，公司内网中存在主机 192.168.1.50/24 和 192.168.1.116/24 两台主机，在设备上启用 WEB 防护功能，增加 WEB 应用防护策略，以此来实现主机访问网络的安全防护。

图1 WEB 防护功能配置组网图



4.2 配置思路

- 新建防护策略
- 配置规则防护
- 配置防盗链
- 配置 CSRF
- 配置 CC 攻击防护
- 配置网页防篡改
- 配置应用隐藏

4.3 使用版本

本举例是在 E6201 版本上进行配置和验证的。

4.4 配置注意事项

- WEB 防护功能包含精确访问控制、规则防护、防盗链、CSRF 攻击防护、CC 攻击防护、网页防篡改、应用隐藏 7 个模块，每个模块都需配置相应策略。
- 根据严重程度的不同，日志分为以下几个级别：紧急、告警、严重、错误、警告、通知、信息。
- 规则防护日志对应下面 web 防护策略中的规则防护；精确访问控制、规则防护、防盗链、CSRF 攻击防护、CC 攻击防护、网页防篡改、应用隐藏等功能模块产生的日志记录在高级防护日志中。
- 及时升级最新规则库。

- 防护策略开启并引用。
- 匹配策略 IP 端口的流量通过 WEB 防护系统转发。

4.5 配置步骤

4.5.1 配置 WEB 防护策略

进入“策略配置>安全设置>WEB 防护>防护策略”，点击“新建”进入 WEB 防护策略配置页面，完成后点击提交，如图 2 所示。

图2 配置 WEB 防护策略

4.5.2 配置规则防护

在 WEB 防护策略配置页面选择规则防护子菜单，启用规则防护，选择防护等级，完成后点击提交。如图 3 所示。

图3 配置规则防护

4.5.3 配置防盗链

在 WEB 防护策略配置页面选择防盗链子菜单，勾选启用，选择防护范围，完成后点击提交。如图 4 所示。

图4 配置防盗链

4.5.4 配置 CSRF

在 WEB 防护策略配置页面选择 CSRF 攻击防护子菜单，勾选启用，新建防护的 url，完成后点击提交。如图 5、图 6 所示。

图5 配置 CSRF

图6 配置 CSRF 防护规则

4.5.5 配置 CC 防护

在 WEB 防护策略配置页面选择 CC 攻击防护子菜单，勾选启用，选择防护范围，访问次数，处理动作。如图 7 所示，

图7 配置 CC 防护

4.5.6 配置网页防篡改

在 WEB 防护策略配置页面选择网页防篡改子菜单，勾选启用，填写防护 url，处理动作。如图 8 所示。

图8 配置网页防篡改

4.5.7 配置应用隐藏

在 WEB 防护策略配置页面选择应用隐藏子菜单，勾选启用，选择防护类型。如图 9 所示，

图9 配置应用隐藏

4.6 验证配置

使用测试 PC 进行攻击测试。

在导航栏中选择“数据中心>日志中心>安全日志>WEB 防护日志”，进入 WEB 防护日志页面，可以查看到 WEB 防护日志规则防护信息。如图 10 所示。

图10 WEB 规则防护日志

在导航栏中选择“数据中心>日志中心>安全日志>WEB 防护日志”，点击进入高级防护日志页面，可以查看到 WEB 防护高级防护信息。如图 11 所示

图11 WEB 高级防护日志

规则防护日志 高级防护日志

查询 导出

	时间	日志级别	源地址	归属地	请求方法	请求URL	事件类型	事件描述	处理动作	操作
1	2020-01-03 15:19:34	信息	192.168.20.116	局域网		http://42.236.98.110/hquery	应用隐藏	server字段被隐藏	允许	详细
2	2020-01-03 15:14:55	信息	192.168.20.116	局域网		http://tile-service.weather.m	应用隐藏	server字段被隐藏	允许	详细
3	2020-01-03 15:04:15	信息	192.168.20.116	局域网		http://ctldl.windowsupdate.c	应用隐藏	server字段被隐藏	允许	详细
4	2020-01-03 15:03:15	信息	192.168.20.116	局域网		http://mscrl.microsoft.com/p	应用隐藏	server字段被隐藏	允许	详细
5	2020-01-03 15:02:27	信息	192.168.20.116	局域网		http://ctldl.windowsupdate.c	应用隐藏	server字段被隐藏	允许	详细
6	2020-01-03 14:59:17	信息	1.1.187.114	泰国		http://AmOJuCGO/ZmhQOG	应用隐藏	server字段被隐藏	允许	详细
7	2020-01-03 14:59:14	信息	1.1.187.114	泰国		http://AmOJuCGO/ZmhQOG	应用隐藏	server字段被隐藏	允许	详细
8	2020-01-03 14:59:10	信息	1.1.231.174	泰国		http://NxAYWab/video.flv	应用隐藏	server字段被隐藏	允许	详细
9	2020-01-03 14:59:07	信息	1.1.100.164	日本		http://TpyJVDBFRPxXhORyR	应用隐藏	server字段被隐藏	允许	详细
10	2020-01-03 14:59:04	信息	1.1.166.40	泰国		http://172.16.1.2/~jxia/poc.p	应用隐藏	server字段被隐藏	允许	详细
11	2020-01-03 14:59:00	信息	1.1.166.40	泰国		http://172.16.1.2/~jxia/poc.h	应用隐藏	server字段被隐藏	允许	详细
12	2020-01-03 14:58:57	信息	1.1.255.230	泰国		http://172.16.1.11/~swarelis,	应用隐藏	server字段被隐藏	允许	详细