AG 安全接入网关
产品白皮书

北京信安世纪科技股份有限公司
2024 年 4 月

知识产权声明

注意

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

北京信安世纪科技股份有限公司

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
网　　址：http://www.infosec.com.cn
电　　话：86-10-68025518
传　　真：86-10-68025519
电子邮箱：support@infosec.com.cn

目录

1. 前言

1.1 背景

随着互联网数字化经济发展，企业内部网络与 Internet 互联，彻底改变了传统的业务处理模式。企业利用 Internet，加速业务处理流程并实现随时随地的业务响应。使得跨地区的不同企业或者不同部门之间通过公网互联成为可能，为企业节省了大量的通信费用。

但与此同时，也带来了巨大的安全威胁：企业的高敏感数字资产一旦被泄露，将会带来难以估计的损失，如何保证企业内部的数据通过公网传输的安全性和保密性？如何管理网络中的各个节点？成为首要问题。

在企业网络建设中，除了建设物理设备隔离的业务网络之外，衍生出了更具性价比的解决方案——使用 VPN（Virtual Private Network 虚拟专用网）技术，通过虚拟的加密隧道与企业内部网络互联，而公共网络上的用户无法穿透虚拟通道访问企业内网业务系统，构建安全的业务网络。

1.2 参考标准

GM/T 0002-2012 《SM4 分组密码算法》
GM/T 0003-2012 《SM2 椭圆曲线公钥密码算法》
GM/T 0004-2012 《SM3 密码杂凑算法》
GM/T 0005-2012 《随机性检测规范》
GM/T 0009-2012 《SM2 密码算法使用规范》
GM/T 0010-2012 《SM2 密码算法加密签名消息语法规范》
GM/T 0015-2012 《基于 SM2 密码算法的数字证书格式规范》
GM-T 0016-2012 《智能 IC 卡及智能密码钥匙密码应用接口规范》
GM/T 0018-2012 《密码设备应用接口规范》
GM/T 0022-2014 《IPSec VPN 技术规范》
GM/T 0023-2014 《IPSec VPN 网关产品规范》
GM/T 0024-2014 《SSL VPN 技术规范》
GM/T 0025-2014 《SSL VPN 网关产品规范》
GM/T 0026-2014 《安全认证网关产品规范》
GM/T 0028-2014 《密码模块安全技术要求》
GB/T 20518-2018 《信息安全技术公钥基础设施数字证书格式》
GB/T 25064-2010《信息安全技术 公钥基础设施 电子签名格式规范》

1.3 术语和缩略语

表 1 术语

名词	解释
数字签名	采用 PKI 技术，先对原文信息进行摘要（Hash），然后通过私钥进行签名处理，生成签名信息，签名信息只有私钥才能产生，签名过程不可逆，通过数字签名，可以保证明文数据的完整性和不可抵赖性。
数据完整性	表明数据没有遭受以非授权方式所作的篡改或破坏。
不可抵赖性	是指对行为的确认，确定行为必须是某人或某机构所为，不能否认，数字签名通过非对称密码技术和 PKI 管理体制保证不可抵赖。
轻量级目录访问协议	LDAP，即 Lightweight Directory Access Protocol 的缩写，是一种较为简单的轻量级目录访问协议。随着互联网成为网络的主流，LDAP 也成为一个具备目录的大部分服务的协议。
X.509 证书标准	国际电话与电报咨询委员会(CCITT)规定的一种行业标准。在这个标准中提供了一个数字证书的标准格式，规定数字证书必须包含的一些信息：如版本号、序列号、签名算法、有效期限等。
国密算法	国家密码管理局基于 ECC 椭圆曲线加密算法开发的新一代中国自主控制的加密算法，是目前国家密码管理局在商业密码领域强制实施的标准。
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。信安世纪 AG 可以支持最多 256 个虚拟站点。
Web 门户	当用户使用浏览器访问虚拟站点时，用户可以看到的所有 Web 页面统称为“Web 门户”。AG 为客户提供一组默认的门户页面。为了满足客户的特殊需求，AG 支持通过自定义虚拟门户页面或门户主题来定制虚拟门户的外观。
USB Key	一种智能存储设备，内置密码运算芯片，用于存放数字证书和数字证书对应的私钥。可进行数字签名和签名验证的运算。可插在电脑的 USB 接口中使用。

表 2 缩略语

缩略语	英文	中文
CA	Certificate Authority	数字证书中心。作为权威的第三方负责发放数字证书
RA	Register Authority	审核注册中心

CRL	Certificate Revoke List	证书吊销列表
LDAP	Lightweight Directory Access Protocol	轻量级目录访问协议
OCSP	Online Certificate Status Protocol	在线证书状态协议
PKI	Public Key Infrastructure	公钥基础设施
SM1	商密 1 算法	国密算法中的一种对称算法
SM2	商密 2 算法	国密算法中非对称算法的简称
SM3	商密 3 算法	国密算法中的散列算法（Hash）
SM4	商密 4 算法	国密算法中的一种对称算法，替代 SM1 算法
RSA	RSA(Rivest-Shamir-Adleman)	一种非对称加密算法
ECC	Elliptic Curve Cryptography	椭圆曲线算法
SHA	Secure Hash Algorithm	安全散列算法
SSO	Single Sign-On	单点登录
SSL	Secure Socket Layer	安全套接层协议层。它是网景（Netscape）公司提出的基于 WEB 应用的安全协议
B/S	Browser/Server	浏览器/服务器模式，客户端是浏览器
C/S	Client/Server	客户机和服务器结构，客户端需要安装专用的客户端软件

2. 产品介绍

2.1 产品简介

AG 安全接入网关是一款基于 IPSec 和 SSL 技术实现远程接入、跨区域组网的综合安全 VPN 平台。产品支持 SSL 加速、IPSec 组网、虚拟站点、单点登录等功能，适用于远程办公、移动办公、多分支机构组网等场景，在保护内部网络安全的同时，为员工、合作伙伴和企业客户提供安全、便捷的网络接入。

AG 可以为企业应用提供以下安全支撑服务：

- 支持用户名口令、数字证书、硬件 ID、生物特征码等多因素认证方式；
- 支持基于用户角色的动态访问控制机制；
- 提供 URL 级别的 Web 应用资源细粒度权限控制；
- 提供端到端高强度的链路加密；

- 支持 IPSec 组网，可创建国密 VPN 隧道；
- 支持多种方式的轻量级单点登录服务；
- 对用户访问行为进行全方位监控、追踪和审计。

该产品基于开放的标准开发，具备良好的兼容性和可扩展性，支持与企业各类应用系统集成，实现无边界化的全量级解决方案。

2.2 国产化支持

支持的国产 CPU：海光、飞腾、龙芯、兆芯等。

支持的国产操作系统：统信 UOS、银河麒麟等。

支持的国密浏览器：iSecSP 内置国密浏览器、红莲花国密浏览器、奇安信可信浏览器、360 国密浏览器等。

2.3 产品架构

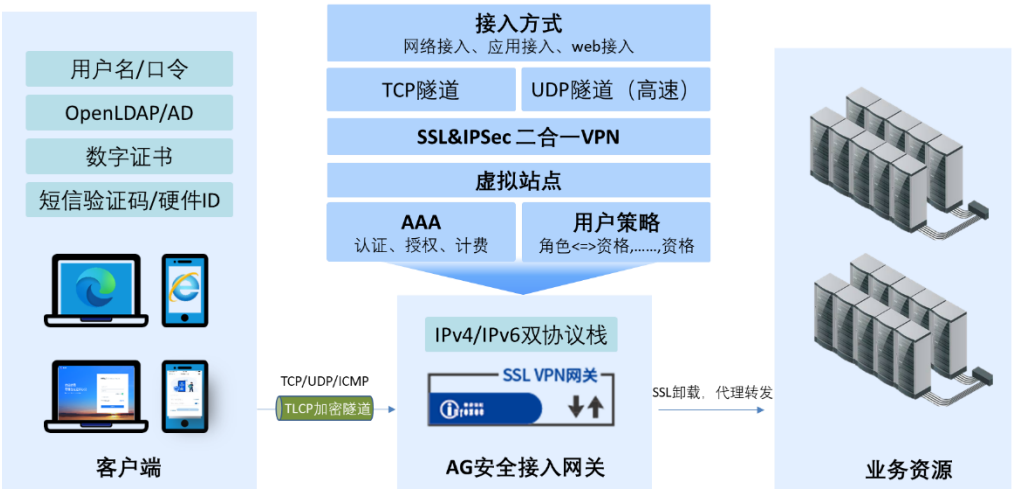


图 1 产品功能示意图

AG 安全接入网关支持 SSL、IPSec 两种 VPN，在 SSL VPN 接入场景下，由客户端、服务端两部分组成，客户端 iSecSP 安全代理客户端负责发起 SSL 连接请求，AG 负责处理请求并创建国密 VPN 隧道，并进行身份认证、授权、访问控制等；在 IPSec VPN 组网场景下，可将不同地理位置的分支机构网络通过 IPSec VPN 连接起来，保护数据在传输过程中的安全性和隐私性，实现安全的跨网络通信。

2.4 主要功能

表 3 主要功能

功能名称	功能说明
身份鉴别	
数字证书	AG 可以验证由受信任的证书授权中心（CA）签发的证书。支持三种类型的客户端证书认证： ➢ 匿名认证：仅需客户端证书； ➢ 非挑战认证：需要认证服务器上有客户端证书和用户账户； ➢ 挑战认证：需要客户端证书、用户账户和用户账户的密码。
设备认证	支持硬件 ID 认证、全平台设备证书认证（对接信安世纪 MAuth 移动安全认证系统），提供安全的可信设备身份鉴别服务。支持用户自注册证书和管理员代注册证书两种模式。
无密码生物识别	移动终端设备上支持无密码生物识别，如：指纹、人脸、手势。当检测到终端属于可信设备或（并）处于可信环境中时，可采用无密码生物识别快速登录，便捷高效，规避密码安全风险，不易伪造和假冒。
扫码登录	应用协同签名技术，实现客户端扫码登录。通过在 PC 端显示二维码，Mobile 可快速扫码登录，无需记忆密码，减少隐私泄露，提升用户使用体验。
本地数据库	支持三种 LocalDB 认证模式： ➢ 静态密码：用户登录虚拟站点时只需要输入静态密码； ➢ 动态密码：用户登录虚拟站点时只需要输入动态密码； ➢ 双重模式：用户登录虚拟站点时需要输入静态和动态密码。
OAuth 认证	支持使用第三方 OAuth 服务器进行用户认证，如微信、企业微信等快捷登录。
SMS 认证	短消息服务（SMS）认证可以与常规认证服务器（如 LocalDB、LDAP、RADIUS 等）结合使用进行二次认证，易用性好，安全性更高。
LDAP/RADIUS 认证	支持使用 LDAP、RADIUS 进行认证和授权。支持 LDAP v3 协议的所有 LDAP 服务器，包括 OpenLDAP 和活动目录（AD）。如果使用多个 LDAP/RADIUS 服务器，支持使用主机轮询负载均衡来进一步提高认证性能，保障用户登录安全。

MFA	支持以上多种认证方式组合的多因素认证。如：数字证书+短信验证码、数字证书+用户名口令、用户名口令+动态密码等。
动态身份认证	可通过 iSecSP 完成客户端环境检测，评估安全等级，针对不同安全级别的用户，动态分配身份鉴别方式。
授权与访问控制	
基于角色授权	根据特定的资格（如登录时间、用户名、组名、源 IP 和 AAA 认证方法）授予已认证的用户相应的角色，使其可以访问相应资源，以此来实现精准灵活的资源分配。
细粒度访问控制	可规定用户、用户组或角色有权访问的指定资源，并对不同类型的资源提供不同粒度的访问控制： ➢ 对于 WEB 应用，支持 URL 级别的访问控制； ➢ 对于非 web 应用，支持对网络类型的资源进行访问控制，如 IP/TCP/UDP/ICMP 等。
动态访问控制	配合信安世纪 NetAuth 零信任统一身份认证管理系统，实现在用户访问期间，基于客户端安全状况，动态调整该用户的授权资源和访问权限。
应用发布	
7 层代理	7 层代理的技术，通过最新版语法解析器对 Web 应用源代码（如 HTML、JS）进行精准的分析改写，保证内网服务不暴露在互联网的基础上实现基于 Web 的 B/S 应用的访问代理。
4 层代理	4 层代理技术，无需安装和启用虚拟网卡，即可实现所有支持 Web 的 B/S 应用的代理访问，提升解决方案的适配性和易用性。
3 层代理	3 层代理技术可劫持特定的网络流量： ➢ 支持发布基于 TCP/UDP 的 B/S、C/S 结构的业务系统资源； ➢ 支持发布三层域名资源，解决 Web 服务器具有浮动 IP 地址的服务器，给管理员和终端用户带来很多不便。 ➢ 支持发布使用动态端口的应用协议，如 FTP、TFTP、Oracle、SQL Server 等。
远程桌面应用	➢ 支持远程桌面的发布和访问管理； ➢ 远程桌面的单点登录，用户登录 AG 后，无需 2 次登录即可直接访问远程桌面应用。

双栈网络支持	➢ 支持 IPv4、IPv6 双栈，可同时访问 IPv4 和 IPv6 资源； ➢ 支持 IPv4、IPv6 互访。即当请求地址为 IPv6 时，既可以访问 IPv6 资源也可以访问 IPv4 资源；当请求地址为 IPv4 时，既可以访问 IPv6 资源也可以访问 IPv4 资源。
轻量级单点登录	
Basic/NTLM 认证	用户登录后，可通过 Basic 认证或 NTML 认证进行单点登录。
SAML 认证	基于 SAML 2.0 标准实现。在 SAML 框架下实现 SAML IDP 和 SP。可以在登录一次的情况下，访问多个不同的系统服务，系统安全性更高，用户体验更好。
OAuth 认证	支持 OAuth2.0 协议进行单点登录访问后台系统和资源。
CAS 认证	支持 CAS 协议进行单点登录并访问后台系统和资源。
单点代填	支持以下单点代填： ➢ 实现 PC 端 WEB、APP 资源的用户信息代填； ➢ 实现对登录页面图片进行识别并代填登录。
Kubernetes 认证	系统支持用户登录 AG 之后，通过 Kubernetes 身份认证协议进行单点登录。
POST 单点登录	➢ 支持 SSO POST，支持 FORM 表单方式的单点登录代填，支持静态参数代填，如用户名、密码； ➢ 支持 PortalTheme SSO，支持 ajax POST 方式提交登录信息，支持动态参数代填，如 Cookie 信息等； ➢ 支持密码加密，可将用户原始密码加密发送给后台服务器，加密算法支持 SM3、MD5、SHA1、SHA256 等。
安全策略中心	
Mini 策略中心	AG 单体即可实现零信任 Mini 策略中心能力，当用户/设备/环境触发预置条件时，会立即执行对应的处置策略。支持以下处置策略： ➢ 提升认证等级，支持多因素认证； ➢ 动态权限，灵活处置； ➢ 拒绝访问，阻断风险。
IPSec VPN	

IPSec 安全协议	支持 IKE/AH/ESP/PFS 等标准 IPSec 协议。 ➢ AH 认证头协议：对 IP 报文进行数据源认证、完整性校验，可保证传输的数据来源可信和数据不被篡改，但不提供加密功能。AH 协议在每个数据包的标准 IP 报文头后面添加一个 AH 报头，AH 协议对报文的完整性校验的范围是整个 IP 报文； ➢ ESP 封装安全载荷协议：除了对 IP 报文进行数据源认证和完整性校验，还能做数据加密。ESP 协议在每个数据包的标准 IP 报文头后面添加一个 ESP 报头，在数据包后方加 ESP 报尾，可对 IP 数据包中 ESP 报头之后与 ESP 报尾之间的数据进行加密。ESP 协议在传输模式下的数据完整性校验不包含 IP 头。
IPSec 参数协商	两个对等体间要想通过 IPSec VPN 通信，首先要建立 IPSec SA。在进行 IPSec SA 建立时对等体间要进行 IPSec SA 参数协商，两端参数相同时才会建立成功。 支持两种参数协商方式：手动指定生成、IKE 协商生成两种方式，IKE 协商模式支持 IKEv1、IKEv1.1、IKEv2。
IKE 协商模式	在 IKE 第一阶段有两种协商模式可建立 IKE SA，分为主模式和野蛮模式，这两个模式的主要区别在于进行 IKE 协商的时候所采用的协商方式不同： ➢ 主模式：主模式在 IKE 协商时交换信息为 6 条。占用较多的交换资源和时间，但是对身份信息的交换进行了加密，安全性比野蛮模式高，适用于两端设备的公网 IP 是固定 IP 的场景； ➢ 野蛮模式：野蛮模式交换信息为 3 个。占用资源少，协商速度快，适用于公网 IP 是动态的或存在 NAT 设备的场景，缺点是以明文方式传输身份交换信息。
IKE 认证方式	支持 PSK 预共享密钥认证、国密双证、RSA 数字证书认证。
IPSec 封装模式	支持使用两种封装模式：传输模式和隧道模式。 ➢ 在传输模式下，IPSec 协议对 IP 报文的载荷部分进行加密和认证，而报文头部分保持不变； ➢ 在隧道模式下，整个 IP 报文都被封装在一个新的 IP 报文中，并对新的报文进行加密和认证，安全性更高。
IPSec 加密方式	支持 SM4、DES、3DES、AES 等标准加密算法。
IPSec 验证方式	支持 SM2、MD5、SHA1、SHA256、SHA384 等校验算法。

高级功能	➢ 在 IPSec VPN 配置完成后，隧道创建模式支持三种，主动创建、被动创建、流量触发； ➢ IPSec 链路探测：当对端设备出现问题后，无需等待 IPSec 隧道超时后（1 小时）才中断隧道，可通过链路探测功能主动发起消息，探测对端设备状态。支持 DPD 探测、Track 探测； ➢ 动态隧道：当遇到一端有固定公网 IP 但对端没有时，无法使用静态隧道方式建立。此时应用动态隧道配置可不指定对端 IP,即可接收来自非特定 IP 的协商请求，此模式也适用于多分支机构接入总部的场景中，无需总部创建大量 IPSec VPN 对等体，减少配置量。
WireGuard VPN	
集中认证授权	● 数据面、控制面分离。AG 作为控制中心负责访问用户的认证授权，iSecSP 与 WireGuard 网关建立 WireGuard UDP 隧道，转发用户的访问流量； ● 管理 WireGuard 网关，帮助 iSecSP 和 WireGuard 网关交换建立 WireGuard 隧道的必要信息。
性能优化	采用 WireGuard 协议创建 UDP 加密隧道，可有效提升单用户访问速度，降低延迟： ➢ 在内网千兆有线网络环境下，上传和下载速率较传统连接方式提升超 60%； ➢ 在移动 4G 热点网络下，上传速率提升超 120%，下载速率提升超 70%； ➢ 在华为云外网移动带宽环境下，下载速率较传统连接方式提升 331%。
灵活部署	● 软件形态，部署环境更灵活，方便扩容； ● iSecSP 建立 WireGuard 隧道之后，可从可连接列表中选取其它的 WireGuard 网关建立隧道。
AG 集中监控与管理	
集中监控	AG 设备的集中监控，可监测 AG 的在线时长、空闲时间、认证方式等。
集中管理	➢ 支持远程运维。管理员无需到达设备现场逐台操作，AG 支持与 AG 安全接入网关设备联动，实现反向管理 AG； ➢ 管理员可远程升级、重启，减轻运维成本； ➢ 支持上传 AG 新版本供设备新版本自动检索。在无人值守的状态下启用此功能，AG 可自动下载新版本升级； ➢ 可随时下载 AG 设备日志。

一键巡检	可单独选择巡检设备也支持纳管设备全部巡检，将会收集以下信息，支持导出巡检结果： ➢ AG 纳管的基本设备信息，包含 AG 名称、型号、版本、内存磁盘使用率等； ➢ VPN 状态（账户、虚拟站点 IP、网络吞吐、在线状态（如果不在线，记录下线时间）等）。
日志审计与监控	
日志服务器	为了能够存储所有历史系统日志，以备管理员进行系统故障排除，产品支持将指定级别的系统日志消息发送并存储在远程日志服务器上，可同时支持 6 个不同的远程日志服务器。
标准化日志格式	日志格式符合 Syslog 标准，支持多种日志类型，且每种类型日志的表项都符合 WELF（国际通行的防火墙日志规范格式）标准。
精细化日志类型	AG 设备支持以下日志记录类型： ➢ 用户访问日志：记录认证和会话、Web 访问、TCP 应用、门户登录和注销以及 HTTP 请求和响应等； ➢ 管理日志：记录通过 CLI 或 WebUI 对 AG 设备进行配置的操作信息。 通过上述日志的记录，可以实现对用户（包括管理员）的所有访问、操作行为的监控和审计。
SNMP	支持 SNMP v1、v2 和 v3 版本，维护并提供自有 SNMP MIB 供管理员对设备进行监控和管理。
Email 告警	可调用 Email 告警，通过设置触发条件将告警信息发送至指定邮箱，提升告警管理能力。
页面定制	
定制化页面	➢ 支持对登录页面、登出页面、门户资源页面、challenge 挑战页面、更改密码页面和错误页面的部分定制； ➢ 支持整页定制功能，包括更改页面样式、图片、文字等，可以满足不同用户定制需求。
国产化支持	
主流国产化系统	支持银河麒麟、统信 UOS、鸿蒙等国产操作系统环境。

国密改造	
国密标准	系统全面支持国密标准，配合零信任客户端 iSecSP 或国密浏览器，可以完成对应用无感知的国密整改，符合等保、合规需求。
其他	
内外网自动探测	支持自动探测接入终端所处的网络位置，根据网络位置提供不同的策略。
内网流量旁路	提供内网流量旁路功能：当用户处于内网位置且经过认证授权后，访问流量可不经过网关代理，直达服务提供者，有效减轻设备的网络负载。
用户自主改密	为了满足客户端产品易用性及安全性，支持自助密码修改功能： ➢ 用户登录时如果忘记登录密码，可通过自定义验证方式修改密码； ➢ 用户登录后可自主修改登录密码； ➢ 用户登录后可强制用户修改登录密码； ➢ 闲时锁定。

2.5 支持的算法

产品适用国际算法、国密算法多种算法场景，提供基于 SM2、SM3、SM4 商用密码算法实现的通信加密能力，并提供国际密码算法 ECC、RSA、AES、3DES 等，充分保障数据传输过程中的机密性和完整性。

产品支持算法明细如下：

信安世纪 AG 设备全面支持国产密码算法以及主流商业加密算法，具体如下：

1） SM1

2） SM2

3） SM3

4） SM4

5） ECDHE-SM4-SM3

6） ECC-SM4-SM3

7） ECDHE-SM4-GCM-SM3

8） ECDHE-SM4-CBC-SM3

9） ECC-SM4-GCM-SM3

10）ECC-SM4-CBC-SM3

11）RSA_SM4_CBC_SHA256

12）RSA_SM4_GCM_SHA256

13）RSA-SM4-CBC-SM3

14）RSA-SM4-CBC-SM3

其中 SM4 算法支持 CBC、ECB 和 GCM 模式，密钥长度 128bits；SM2 密钥长度可达到 256bits。

支持国际算法为（共计 112 种）：

1） RSA

2） ECDHE

3） DH

4） DSA

5） ECDSA

6） x25519

7） x448

8） ed25519

9） ed448

10）Kyber

11）secp256r1

12）secp384r1

13）secp521r1

14）MD2

15）MD3

16）MD4

17）MD5

18）SHA1

19）SHA3

20）SHA224

21）SHA256

22）SHA384

23）SHA512

24）DES

25）3-DES

26）AES

27）RC4

28）Camellia

29）SEED

30）ChaCha20

31）RC4-MD5

32）RC4-SHA

33）DES-CBC-SHA

34）DES-CBC3-SHA

35）EXP-RC4-MD5

36）EXP-DES-CBC-SHA

37）AES128-SHA

38）AES256-SHA

39）AES128-SHA256

40）AES256-SHA256

41）AES128-GCM-SHA256

42）AES256-GCM-SHA384

43）ECDHE-RSA-AES128-SHA

44）ECDHE-RSA-AES256-SHA

45）ECDHE-ECDSA-AES128-SHA

46) ECDHE-ECDSA-AES256-SHA

47) ECDHE-RSA-AES128-SHA256

48) ECDHE-RSA-AES256-SHA384

49) ECDHE-RSA-AE S128-GCM-SHA256

50) ECDHE-RSA-AE S256-GCM-SHA384

51) ECDHE-ECDSA-AES128-SHA256

52) ECDHE-ECDSA-AES256-SHA384

53) ECDHE-ECDSA- AES128-GCM-SHA256

54) ECDHE-ECDSA-AES256-GCM-SHA384

55) TLS-AES128-GCM-SHA256

56) TLS-AES256-GCM-SHA384

57) TLS_RSA_WITH_CAMELLIA_128_CBC_SHA

58) TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA

59) TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA

60) TLS_RSA_WITH_CAMELLIA_256_CBC_SHA

61) TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA

62) TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA

63) TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256

64) TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA256

65) TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256

66) TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256

67) TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA256

68) TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256

69) TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256

70) TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384

71) TLS_ECDH_ECDSA_WITH_CAMELLIA_128_CBC_SHA256

72) TLS_ECDH_ECDSA_WITH_CAMELLIA_256_CBC_SHA384

73) TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256

74) TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384

75) TLS_ECDH_RSA_WITH_CAMELLIA_128_CBC_SHA256

76) TLS_ECDH_RSA_WITH_CAMELLIA_256_CBC_SHA384

77) TLS_RSA_WITH_CAMELLIA_128_GCM_SHA256

78) TLS_RSA_WITH_CAMELLIA_256_GCM_SHA384

79) TLS_DHE_RSA_WITH_CAMELLIA_128_GCM_SHA256

80) TLS_DHE_RSA_WITH_CAMELLIA_256_GCM_SHA384

81) TLS_DH_RSA_WITH_CAMELLIA_128_GCM_SHA256

82) TLS_DH_RSA_WITH_CAMELLIA_256_GCM_SHA384

83) TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_GCM_SHA256

84) TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_GCM_SHA384

85) TLS_ECDH_ECDSA_WITH_CAMELLIA_128_GCM_SHA256

86) TLS_ECDH_ECDSA_WITH_CAMELLIA_256_GCM_SHA384

87) TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256

88) TLS_ECDHE_RSA_WITH_CAMELLIA_256_GCM_SHA384

89) TLS_ECDH_RSA_WITH_CAMELLIA_128_GCM_SHA256

90) TLS_ECDH_RSA_WITH_CAMELLIA_256_GCM_SHA384

91) ecdsa_secp256r1_sha256

92) ecdsa_secp384r1_sha384

93) ecdsa_secp521r1_sha512

94) rsa_pss_rsae_sha256

95) rsa_pss_rsae_sha384

96) rsa_pss_rsae_sha512

97) rsa_pss_pss_sha256

98) rsa_pss_pss_sha384

99) rsa_pss_pss_sha512

100) secp256r1

101) secp384r1

102） secp521r1

103） sha256ECDSA

104） sha256RSA

105） sha384ECDSA

106） sha384RSA

107） sha512ECDSA

108） sha512RSA

109） sha224ECDSA

110） sha224RSA

111） sha1ECDSA

112） sha1RSA

AG 产品支持国密算法 14 种，支持国际算法 112 种,其中：SM2、RSA、ECDHE、DH、DSA、ECDSA、x25519、x448、ed25519、ed448、Kyber 、secp256r1、secp384r1, secp521r1 等公钥算法，RSA 密钥长度可达到 4096bits； 支持 SM3、MD2、MD3、MD4、MD5、SHA1、SHA3、SHA224、SHA256、SHA384、SHA512 等 HASH 算法；支持 SM4、DES、3-DES、AES、RC4 、Camellia，SEED，ChaCha20 等对称密钥加密算法，其中 SM4 算法支持 CBC、ECB 和 GCM 模式，密钥长度 128bits；支持 SM2 非对称算法，密钥长度可达到 256bits。

2.6 IPv6 证明

由于 IPv4 地址耗尽，如何从 IPv4 网络向 IPv6 网络过渡成为许多互联网服务提供商面临的一大挑战。

AG 设备提供 IPv6 支持，以帮助企业和组织进行 IPv4 到 IPv6 的转换。AG 支持 IPv4/IPv6 双协议栈，IPv4 资源可以交付给 IPv6 用户。

本章将概述主要系统模块的 IPv6 支持状态，如一般设置和网络、角色、访问方法、HA、系统监控和管理工具。关于 IPv6 支持的细节，请参考 AG IPv6 支持矩阵。

2.6.1 一般设置和网络

系统提供以下 IPv6 支持：

- 可以为系统接口配置 IPv6 地址。

- 支持 IPv6 静态和动态路由表。
- 支持 IPv6 NTP 服务器。
- 支持 NDP 协议。

2.6.2 虚拟站点

虚拟站点的 IP 地址可以是 IPv6 地址。请注意，IPv6 虚拟站点 IP 必须与配置了 IPv6 地址的系统接口相关联。

2.6.3 角色

可以将 IPv6 源 IP 配置为角色限定条件。

2.6.4 访问方法

2.6.4.1 Web 访问

IPv6 用户可以访问 IPv4（QuickLink）和 IPv6 Web 资源。

- 对于 QuickLink Web 资源，AG 支持 IPv4 over IPv6，这意味着客户端和 AG 设备使用 IPv6 地址进行网络连接，而后台服务器使用 IPv4 地址。
- 对于 IPv6 Web 资源，客户端、AG 设备和后台服务器都使用 IPv6 地址。

2.6.4.2 网络访问

IPv6 用户可以通过 AG 设备建立 L3VPN 隧道来访问内部 IPv4 和 IPv6 网络。也就是说，客户端和 AG 设备使用 IPv6 地址进行网络连接，而客户端可以使用内部 IPv4 或 IPv6 地址。

2.6.5 HA

HA 特性支持 IPv6，可以为 HA 单元配置 IPv6 地址。请注意，一个 HA 域中的所有 HA 单元必须都是 IPv4 地址，或者所有都是 IPv6 地址，不能是两者的混合。

2.6.5.1 系统监控

日志

支持 IPv6 远程 syslog 主机。

SNMP

支持 IPv6 SNMP 陷阱主机。

2.6.5.2 管理工具

系统提供以下 IPv6 支持：

- ping6
- traceroute6
- nslookup
- WebUI IPv6 访问
- SSH IPv6 访问

3. 特性

3.1 自适应多因素认证

提供数字证书认证、协同签名、动态密码认证、设备认证、人脸识别、指纹识别、手势识别、扫码登录、SMS 等丰富的身份认证方式，支持多种认证方式组合的多因素认证机制。同时，还可配合零信任客户端（iSecSP）和零信任控制中心（NetAuth）对终端物理环境变化感知、网络环境威胁检测、用户操作行为的安全等级评估，提供不同安全等级的身份认证方式，完成对接入设备和接入主体的身份鉴别。

3.1.1 LocalDB

AG 支持使用 LocalDB（本地数据库）进行认证和授权。在 LocalDB 认证中，如果输入的用户名和密码匹配了在 AG 上为虚拟站点在本地数据库中配置的条目，终端用户就可以登录虚拟站点。在授权时，AG 会获取认证用户的组名，用于进一步的用户授权。如果 AG 没有获取认证用户的组名，将会使用默认组（通过命令

“aaa server localdb defaultgroup”配置）。

认证模式

AG 支持三种 LocalDB 认证模式：

静态密码：表示用户要登录虚拟站点只需要输入静态密码。

动态密码：表示用户要登录虚拟站点只需要输入动态密码。

双重模式：表示用户要登录虚拟站点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 MotionProOTP 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）并通过手机登录虚拟站点。然后在 PC 上的 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）。

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，且 LocalDB 服务器的名称和虚拟站点的名称一致。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。

AG 上的本地数据库可容纳 500,000 个 LocalDB 账户和 50,000 个 LocalDB 组。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 账户和 LocalDB 组的名称和密码。

LocalDB 账户密码设置

AG 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

数值字符检查

非字母数字字符检查

包含的特殊字符的最小数量检查

用户名和密码重复性检查

新密码和老密码一致性检查

此外，管理员可以为指定的 LocalDB 账号设置密码过期时间和下次登录时密码强制过期。

LocalDB 锁定

AG 支持对所有 LocalDB 账户进行自动空闲锁定和自动登录失败锁定。

此外，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。

LocalDB 备份和恢复

AG 支持备份虚拟站点的本地数据库和从指定的 LocalDB 备份中恢复本地数据库。

此外，AG 支持自动保存 LocalDB 设置。

LocalDB 导出和导入

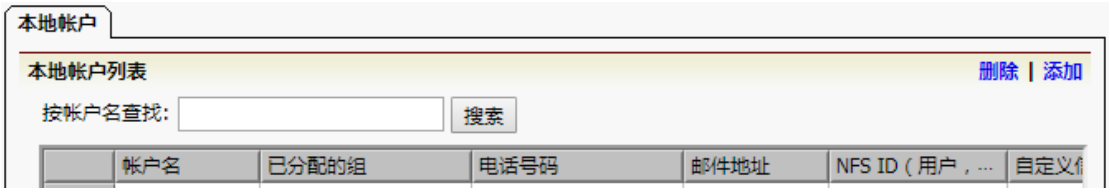
AG 支持将 LocalDB 数据库中的帐户，组或成员关系导出到系统上的配置文件中，并支持从系统配置文件中将包含帐户，组或成员关系的文件导入 LocalDB。

配置示例

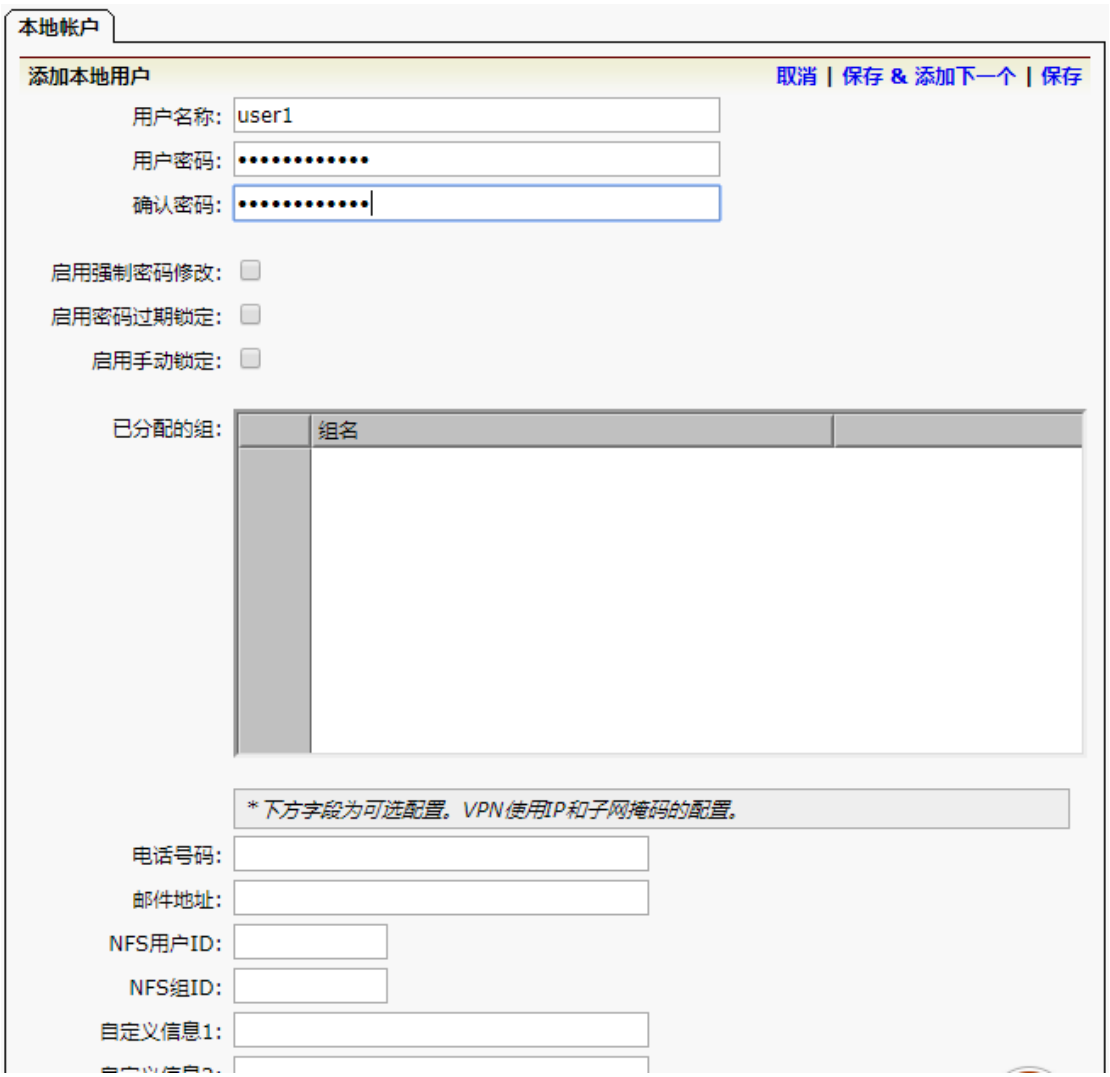
在启用 LocalDB 作为虚拟站点的 AAA 服务器前，管理员需要在 LocalDB 中添加本地账户和本地组。

添加本地账户

在虚拟站点模式下，选择本地数据库>本地账户>本地账户，在本地账户列表区域点击添加操作链接。



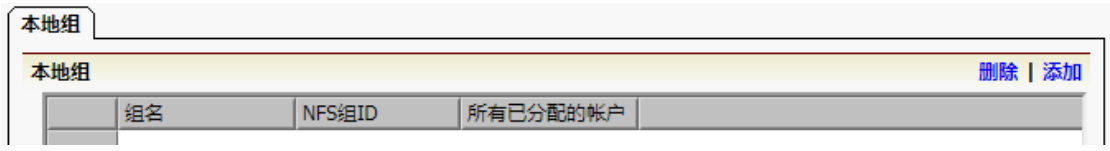
在添加本地用户区域，指定用户名称、用户密码和确认密码，视情况选择其他可选框和参数，并点击保存操作链接。



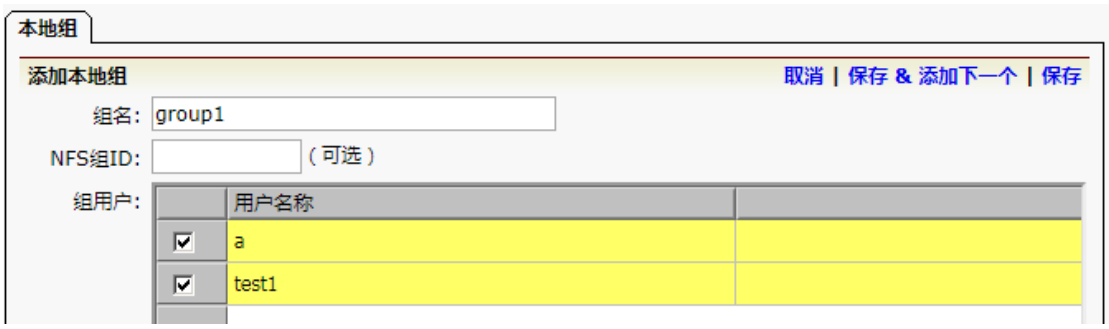
添加本地账户

添加本地组

在虚拟站点模式下，选择本地数据库>本地组>本地组，在本地组区域点击添加链接。



在添加本地组区域，指定参数组名，选择要添加到本地组的本地账户的复选框，并点击保存操作链接。



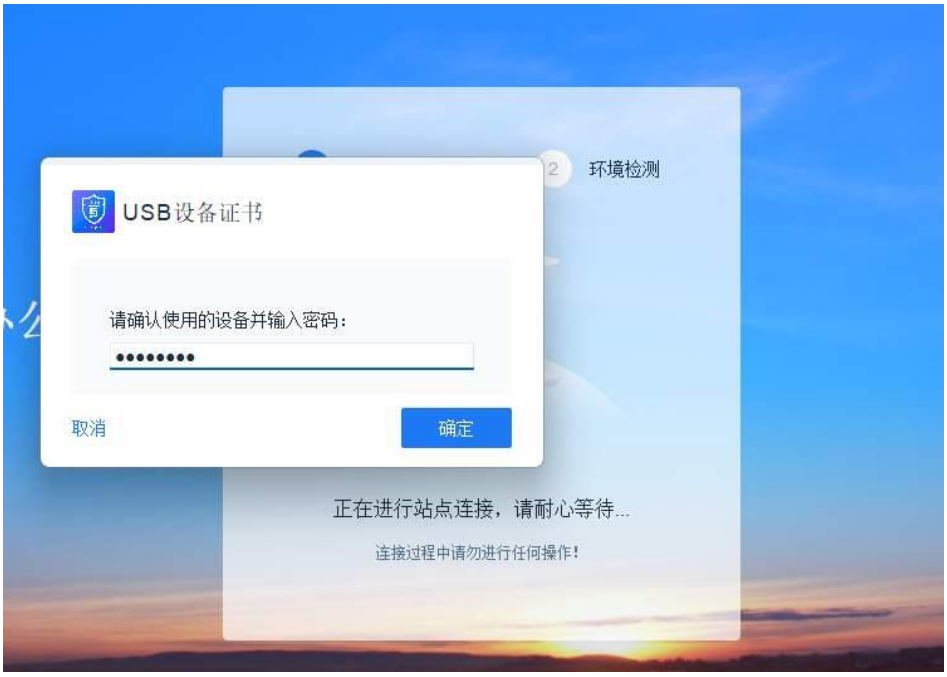
启用 LocalDB 服务器

在虚拟站点模式下，选择站点配置>AAA>服务器>本地数据库，选择复选框启用本地数据库服务器和 LocalDB 认证时用户名不区分大小写，并在本地数据库服务器配置区域指定参数默认组名并在右上角点击应用修改按钮保存配置。

3.1.2 USB KEY

客户登录 VPN 客户端，首先输入站点。

连接站点时，插入 USB KE，并填写 pin 码



成功登陆业务系统

3.1.3 短信认证

短消息服务（Short Message Service，SMS）认证可以单独使用或与常规认证服务器（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。然后 AG 代替用户将 SMS 认证请求发给 SMS 认证服务器并返回 SMS 认证页面，要求用户输入验证码。输入正确的验证码后，用户将成功通过两步认证流程。

AG 支持以下类型的 SMS 认证方式：

CMPP2：表示 CMPPv2.0 协议。

CMPP3：表示 CMPPv3.0 协议。

EM：表示 EM 专有协议。

CUSTOM：表示自定义协议。

自定义 SMS 认证不同于其他 SMS 认证协议，AG 使用通过命令“aaa server sms custom import request”导入的自定义 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 custom 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，他将成功通过自定义 SMS 认证流程。

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。

用户的移动手机号码可以通过以下方式获取：

LocalDB

LDAP 服务器

RADIUS 服务器

Certificate 服务器

HTTP AAA 服务器

配置示例

在虚拟站点模式下，选择站点配置>AAA>服务器>SMS，在服务器列表区域指定参数服务器名和描述并点击添加按钮添加 SMS 服务器。

双击服务器列表区域的服务器条目，在显示窗口的 SMS 服务器高级配置区域，指定 SMS 服务器的基本参数并按需指定 SMS 服务器的高级参数。

3.1.4 硬件特征码

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 生成注册工具。

硬件 ID 授权基于客户端的硬件 ID 值准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。当用户通过认证和授权后，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、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 用户或组能够使用的客户端的限制条件。

硬件 ID 授权可以与 LocalDB 以及其他第三方授权服务器集成（例如 LDAP 和

RADIUS）。请注意，外部组需要映射到 LocalDB 组才能使用该功能。

硬件 ID 同步

系统支持硬件 ID 同步。为用户账户配置的处于“批准”状态的硬件 ID 规则可以被同步到硬件 ID 同步主机（即外部账户管理平台）。AG 设备支持自动和手动同步硬件 ID。

自动：如果启用自动硬件 ID 同步功能，为用户配置的硬件 ID 规则将被实时地同步到硬件 ID 同步主机。如果为用户配置的硬件 ID 规则的状态从“批准”变为“待定”或“拒绝”，或删除了一条为用户配置的硬件 ID 规则，为用户配置的相应的硬件 ID 规则将从硬件 ID 同步主机删除。

手动：管理员也可以手动同步为指定用户配置的硬件 ID 规则。推荐只在硬件 ID 同步主机重新配置或从长时间停机状态恢复时才使用手动硬件 ID 同步。

要使用硬件 ID 同步功能，必须使用命令“localdb hardwareid sync host”配置同步主机，并使用命令“localdb hardwareid sync req”配置 HTTP 请求模板。

基于电子邮件的硬件 ID 自注册

系统支持基于电子邮件的硬件 ID 自注册功能。为组启用该功能后，当用户尝试登录虚拟站点请求硬件 ID 授权且未被任何硬件 ID 规则批准时，系统将向组中用户的电子邮件地址发送自注册的电子邮件。这个电子邮件有一个系统生成的随机 URL，用户可以在随机 URL 超时前点击它注册硬件 ID。如果随机 URL 超时后，用户可以在自注册电子邮件重发间隔到达后尝试重新登录虚拟站点，此时系统将向用户重新发送自注册电子邮件。用户成功注册硬件 ID 后，系统将为用户自动批准硬件 ID。

系统允许管理员在自注册电子邮件中设置随机 URL 的超时时间和重新发送自注册电子邮件的间隔。

要使用该功能，管理员需要配置系统电子邮件服务器或外部 SMTP 电子邮件服务器，并配置在 LocalDB 或 LDAP 授权服务器上获取用户的电子邮件地址的位置。

配置示例

配置硬件 ID 授权

在虚拟站点模式下，选择本地数据库>登录授权>硬件 ID>基本设置，。

在基本设置区域，按照需要指定参数启用 AAA 硬件 ID、硬件 ID 授权启动模式、自动选择可用启动模式、通知邮件接收地址、硬件 ID 限制（针对单个用户）和硬件 ID 用户限制（针对单个设备）和硬件 ID 类型。

在硬件 ID 授权（组设置）区域，选择组条目的激活复选框，然后根据需要指定参数 ID 类型、自动收集、自动审批、聚集和硬件 ID 限制。

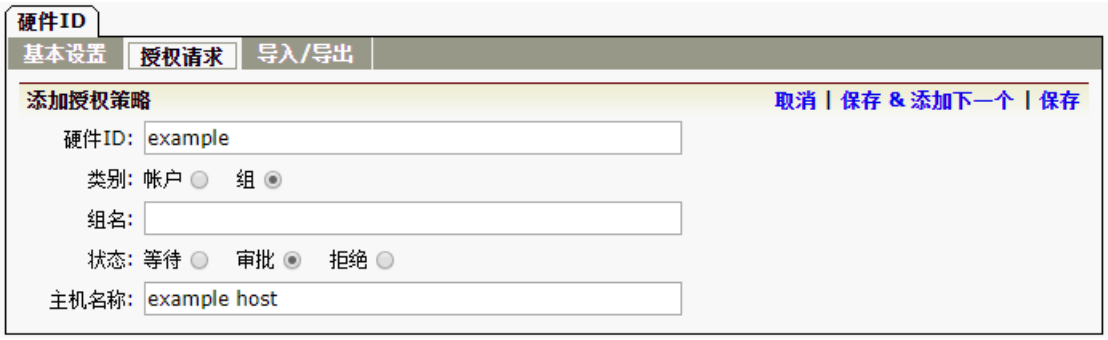
下载硬件 ID 生成工具

在硬件 ID 生成工具区域点击其中一个下载操作链接为运行指定 OS 的 PC 下载硬件 ID 生成工具。

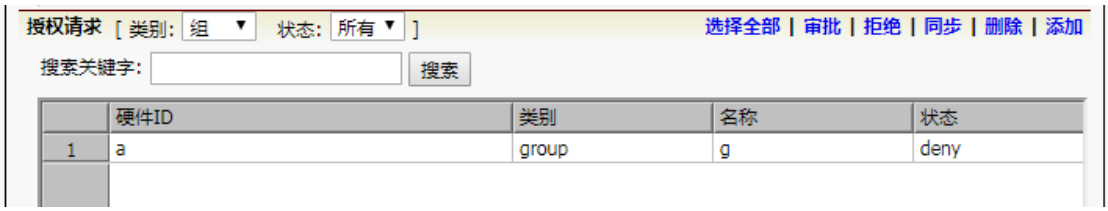
配置硬件 ID 规则

在虚拟站点模式下，选择本地数据库>登录授权>硬件 ID>授权请求。在授权请求区域，选择添加操作链接添加一个授权请求。

在添加授权策略配置窗口中，指定参数硬件 ID、类别、用户名称/组名、状态和主机名称。



从下拉列表指定类别和状态并指定参数搜索关键字来过滤硬件 ID 授权请求。

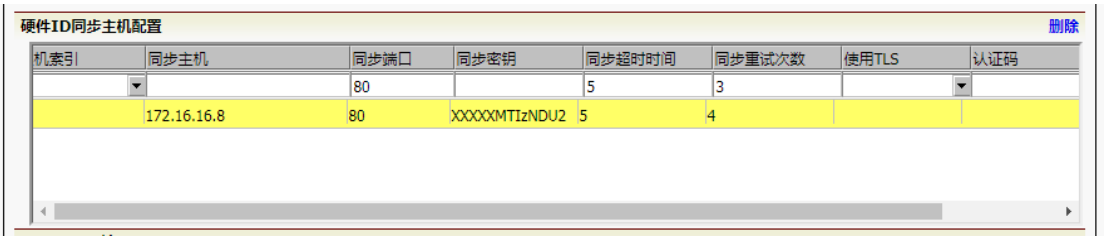


选择一个请求条目，然后选择审批或拒绝操作链接更新请求状态。

配置硬件 ID 同步

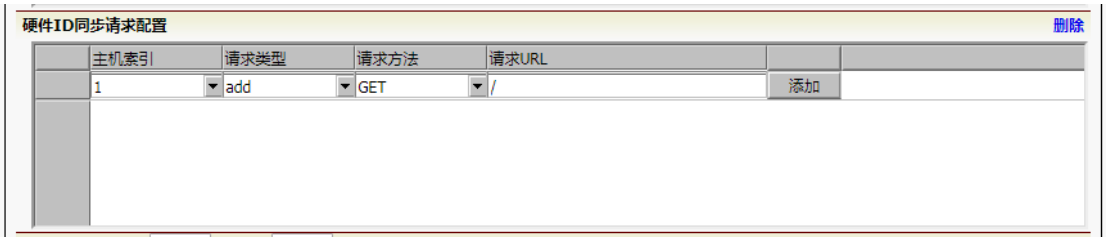
配置硬件 ID 同步主机

在虚拟站点模式下，选择本地数据库>登录授权>硬件 ID>授权请求。在硬件 ID 同步主机配置区域，指定参数主机索引、同步主机、同步端口、同步密钥、同步超时时间、同步重试次数、使用 TLS 和认证码，并点击添加操作按钮。



配置硬件 ID 同步请求模板

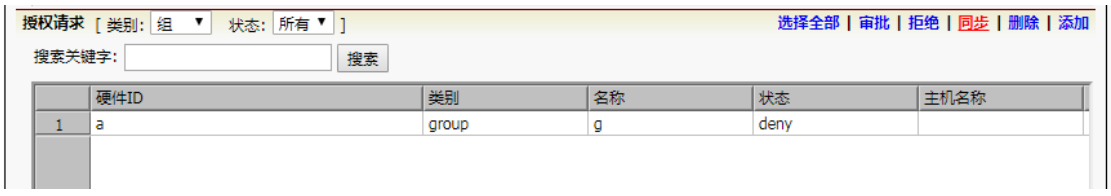
在硬件 ID 同步请求配置区域，指定参数主机索引、请求类型、请求方法和请求 URL 并点击添加按钮。



启用硬件 ID 同步

要自动同步硬件 ID 规则，在硬件 ID 同步配置区域，选择启动自动同步复选框并点击应用修改按钮。

管理员也可以在授权请求区域点击同步操作链接手动同步选择的硬件 ID 规则，。



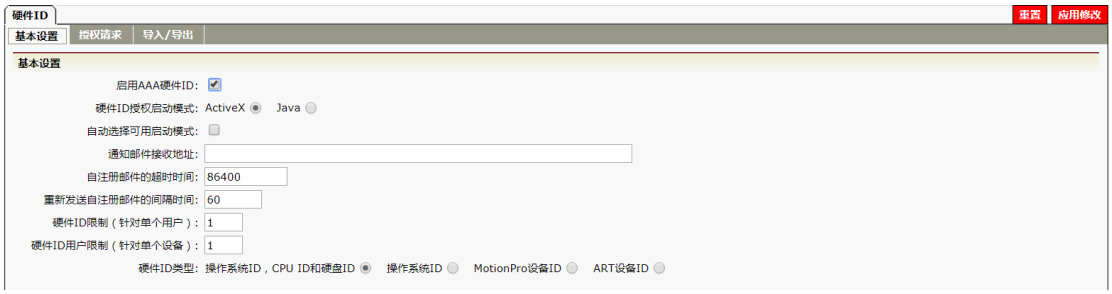
配置基于电子邮件的硬件 ID 自注册

配置获取电子邮件的属性

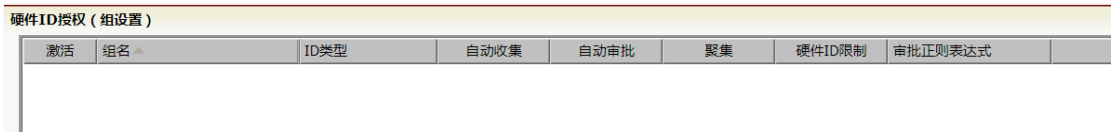
在虚拟站点模式下，选择站点配置>AAA>服务器>LDAP。在服务器列表区域，双击服务器条目为 LDAP 服务器添加更多的高级配置。在高级 LDAP 服务器配置区域，指定参数获取用户邮件地址的属性。

配置硬件 ID 设置

在虚拟站点模式下，选择本地数据库>登录授权>硬件 ID>基本设置。在基本设置区域，指定参数自注册邮件的超时时间和重新发送自注册邮件的间隔时间。



在硬件 ID 授权（组设置）区域，设置审批正则表达式参数为“email”。



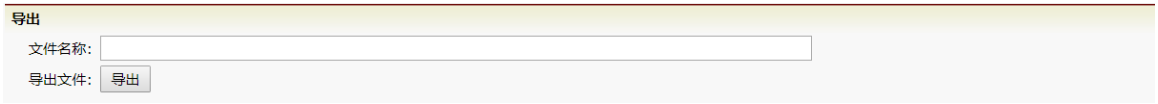
配置硬件 ID 导入/导出

配置硬件 ID 导入

在虚拟站点模式下，选择本地数据库>登录授权>硬件 ID>导入/导出。在导入区域，指定参数文件路径和选项，并点击导入按钮。

配置硬件 ID 导出

在导出区域，指定参数文件名称，并点击导出按钮。



3.1.5 动态令牌

客户在登录时输入动态口令，可登录业务系统。

3.1.6 LDAP 认证

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三个 LDAP 服务器。考虑到冗余性，每个服务器可以有三个主机。

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。

组映射

组映射是另一种控制用户和组访问内网资源的方法。该特性使 AG 可以从外部 LDAP/RADIUS 服务器获取组信息并映射组信息到本地 AG 组。外部组中的用户

可以像被映射的本地组一样获得授权。

对于每个虚拟站点，管理员可以酌情配置一个本地默认组。如果外部认证服务器和 AG 间的组映射不完全（例如外部组名未映射到任何 LocalDB 组），AG 将映射这些外部组到本地默认组。如果未配置本地默认组，这些未被映射的外部组的登录将被拒绝。

LDAP 密码修改

LDAP 密码修改功能允许 LDAP 用户通过虚拟门户修改密码并显示密码过期警告信息来友好地通知 LDAP 用户其密码即将过期。

该功能允许在虚拟门户的欢迎页面一直显示“LDAP 密码修改”链接，或是在当密码过期警告消息开始出现时在门户页面上显示“LDAP 密码修改”链接。通过点击“LDAP 密码修改”链接，用户可以在显示的密码更改页面中更改指定 LDAP 服务器上的密码。如果 LDAP 密码过期，用户将在 LDAP 认证过程中被重定向到密码修改页面。

该功能将在欢迎页面上显示密码过期警告信息，用于通知 LDAP 用户密码的剩余有效时间。该密码过期警告机制可以帮助 LDAP 用户及时修改密码以避免登录失败，从而提升了用户体验。

在使用 LDAP 密码修改功能之前，请确保：

在相关的 LDAP 服务器上，配置了 LDAP 密码的有效期。

对于 OpenLDAP 服务器，配置了外部默认策略。

对于 Windows AD 服务器，系统时间必须和 AG 设备的系统时间一致。

在 AG 设备上，已将相关的 Windows AD 服务器配置为使用端口 636 并通过 TLS 协议访问。

LDAP 浏览器

LDAP 浏览器功能可以帮助管理员够轻松地从 LDAP 主机搜索用户名和组并将其添加到用户角色条件。

此外，该功能支持 LDAP 自动搜索和电子邮件通知，能够按照指定频率自动搜索用户名和组，并通过电子邮件通知搜索结果。

要启用 LDAP 自动搜索和电子邮件通知，管理员需要定义一个 LDAP 自动搜索配置文件，用于配置 LDAP 主机、搜索属性、搜索过滤器和搜索频率、要通知的电子邮件地址和电子邮件主题。

LDAP 自动搜索配置文件启用后，系统将在每天、每周或每月指定的时间在指定的 LDAP 主机上进行搜索。如果搜索结果自上次搜索后有变化，将通过邮件通知管理员搜索结果的变化。此外，管理员还可以手动执行配置文件来立即进行搜索。

LDAP 自动搜索和邮件通知也为角色资格提供了捷径，允许管理员可以很容易地将搜索结果中的用户名和组添加到角色条件。

配置示例

添加 LDAP 服务器

在虚拟站点模式下，选择站点配置>AAA>服务器>LDAP，指定参数服务器名和描述并在服务器列表区域点击添加按钮。

在服务器列表区域，双击服务器条目为 LDAP 服务器添加更多的配置。

在显示的 LDAP 服务器配置窗口，点击添加 LDAP 服务器操作链接为 LDAP 服务器添加一个主机。

3.1.7 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 3 台 RADIUS 服务器。考虑到冗余性，每台服务器可以有 3 个主机。

RADIUS 请求是非阻塞的。将会为所有 RADIUS 请求定义超时时间。

配置示例

添加 RADIUS 服务器

在虚拟站点模式下，选择站点配置>AAA>服务器>RADIUS，指定参数服务器名和描述，并在服务器列表区域点击添加按钮。

在服务器列表区域，双击服务器条目为 RADIUS 服务器添加更多的高级配置。在显示窗口的 RADIUS 服务器配置区域，点击添加 RADIUS 服务器操作链接为 RADIUS 服务器添加一台主机。

在添加 RADIUS 服务器区域，指定参数服务器 IP 地址、服务器端口、密码、超时时间、冗余顺序、重试次数和审计端口，并点击保存操作链接。

重复以上步骤为 RADIUS 服务器添加至多 3 台主机。

在 RADIUS 服务器高级配置区域，指定参数 RADIUS NASIP，RADIUS 属性组，RADIUS 属性默认组、RADIUS 属性客户端 IP、RADIUS 属性客户端 IP 掩码和其他需要的参数，并点击右上角的应用修改按钮保存配置。

在添加 LDAP 服务器区域，指定参数服务器 IP 地址、服务器端口、用户名、用户密码、基本字符串、超时时间和冗余顺序，按需选择使用 SSL/TLS 复选框，并点击保存操作链接。

重复之前的配置为 LDAP 服务器添加最多 3 台主机。

在高级 LDAP 服务器配置区域，指定参数搜索过滤规则、组属性字段、默认组和带绑定认证，按需指定其他参数，并在右上角点击应用修改按钮保存配置。

配置组映射

在虚拟站点模式下，选择站点配置>AAA>组映射，指定参数外部组和内部组并在组列表区域点击添加按钮。

添加组映射条目

配置 LDAP 密码修改

配置密码过期警告

在高级 LDAP 服务器配置窗口中，指定参数密码过期提醒和密码策略 DN（仅限于 OpenLDAP 服务器）并点击应用修改按钮。

在 Web 门户上启用 LDAP 密码修改

在虚拟站点模式下，在站点配置>门户>基本设置>基本设置的基本设置区域，选择启用 LDAP 密码修改复选框，并按需选择仅密码过期提醒时复选框。

配置 LDAP 浏览器

LDAP 浏览器允许管理员从 LDAP 服务器添加用户名或者组作为角色条件。

从现有的 LDAP 主机添加用户名

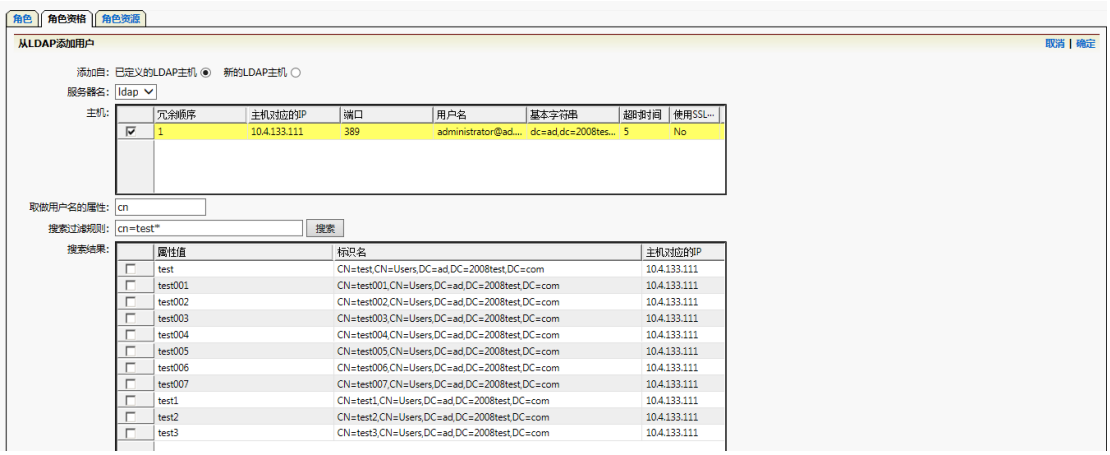
在虚拟站点模式下，选择用户策略>角色>角色资格，并点击添加按钮。

在添加角色资格配置窗口中，从下拉列表中选择已定义的角色名称，输入资格名称和描述（可选）。然后，指定条件类型为用户名，从 LDAP 添加按钮会出现在内容文本框的右侧。

点击从 LDAP 添加按钮后，从 LDAP 添加用户配置窗口将会出现。选择添加自已定义的 LDAP 主机单选按钮，可用的 LDAP 主机将会显示。

从主机表中选择一台 LDAP 主机，指定取做用户名的属性和搜索过滤规则文本框（搜索过滤规则的内容需要遵循 LDAP 搜索规则），然后点击搜索按钮。

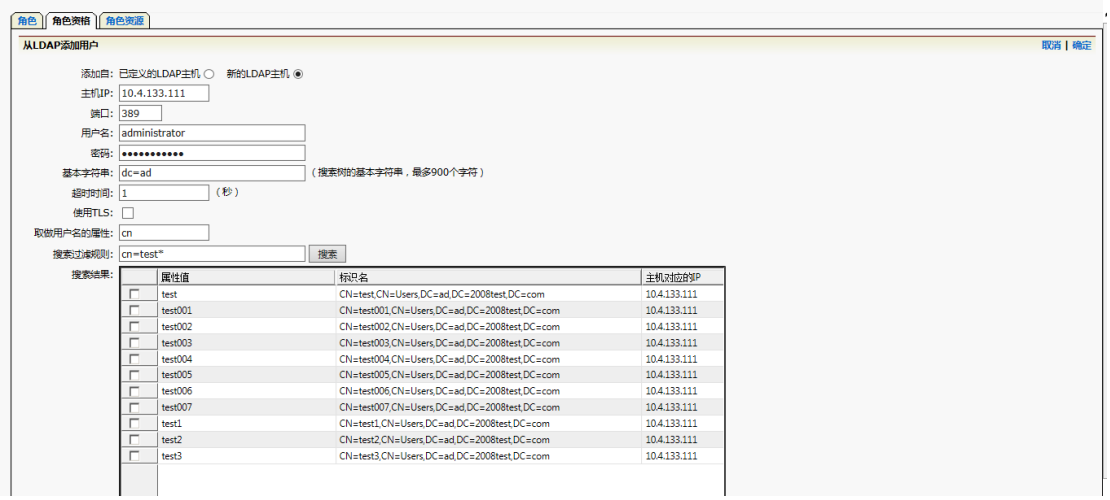
在点击搜索按钮后，将会返回搜索结果。



在搜索结果中选择记录，并点击右上角的确定按钮添加用户名。一次最多可以选择 10 个条目。

从新的 LDAP 主机添加用户名

要从新 LDAP 主机添加用户名，请在从 LDAP 添加用户配置窗口中选择添加自新的 LDAP 主机单选按钮，指定主机 IP、端口、用户名、密码、基本字符串、超时时间、取做用户名的属性和搜索过滤规则，并点击搜索按钮。搜索结果将会显示在下表中。



在搜索结果中选择记录，并在右上角点击确定按钮。一次至多可以选择 10 个条目。

从 LDAP 主机添加组

在添加角色资格配置窗口中，从下拉列表中选择已定义的角色名称，输入资格名称和描述（可选）。然后，指定条件类型为组名，从 LDAP 添加按钮会出现在内容文本框的右侧。

添加组和添加用户名唯一的区别是取做组名的属性是从高级 LDAP 服务器配置中的 LDAP 属性组获取。

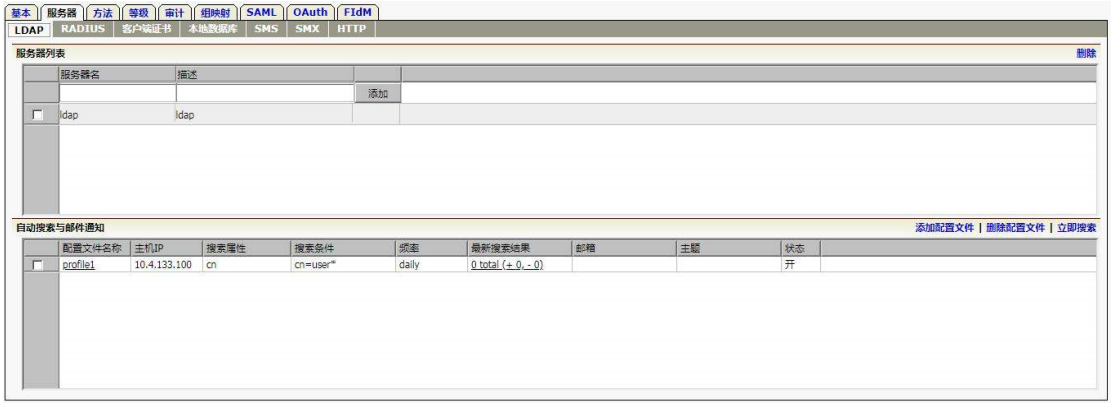
配置 LDAP 自动搜索配置文件

在虚拟站点模式下，选择站点配置>AAA>服务器>LDAP，并在自动搜索与邮件通知区域点击添加配置文件操作链接。

在添加搜索配置文件配置窗口中，选择启用搜索与通知复选框，指定参数配置文件名称、搜索自、服务器名称、主机、搜索属性、搜索条件、搜索于、邮箱和主题，并点击保存操作链接。

要将 LDAP 自动搜索配置文件关联到一个新 LDAP 主机，也需要指定参数主机 IP、端口、用户名、密码、基本字符串和使用 TLS。

要查看指定配置文件的最新搜索结果，在自动搜索与邮件通知表上点击配置文件条目的最新搜索结果单元。在搜索结果及检测变化窗口中，最新的搜索结果和检测到的改变将会显示。



要将用户名和组名添加到指定的角色资格，在快捷方式到角色资格区域点击展开操作链接，指定所需参数。

3.1.8 CA（数字证书认证）

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账户。

挑战（Challenge）：挑战认证需要客户端证书和密码。

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。

如果启用了 SSL 证书认证（在虚拟站点模式下站点配置>SSL/DTLS 证书>SSL 设置>客户端验证的路径选择激活客户端认证复选框），当用户访问虚拟站点时，

选择客户端证书的消息框将会在门户登录页面之前显示。否则，选择客户端证书的消息框将在使用客户端证书认证的 AAA 方法被选择时显示。

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：

SSL 基于受信 CA 验证客户端证书。

SSL 从证书中提取相应字段。

SSL 将字段值发给 AAA 服务器。

AAA 使用 LDAP 服务器或 LocalDB 进行认证。

AAA 使用 LDAP 服务器、LocalDB 或外部组进行授权。

配置示例

在虚拟站点模式下，选择站点配置>AAA>服务器>客户端证书，在

证书服务器配置区域点击添加证书服务器按钮。

在添加证书服务器区域，指定参数服务器名和显示名称，根据实际需求选择认证和授权复选框，如果预定义的 AAA 服务器被选用做客户端证书认证和授权，请指定其它必要参数。

3.1.9 OAuth 认证

描述

OAuth 2.0 为 Web 应用、桌面应用、移动电话和家居设备提供了特定的授权流程。

OAuth 2.0 架构包含以下概念：

用户：指资源拥有者。

用户代理：指用户的浏览器或手机应用。

资源服务器：指主管用户资源的服务器。它可以与 OAuth 服务器集成，也可以是一台独立的服务器。

OAuth 服务器：指为用户提供认证和授权的授权服务器。

OAuth 客户端：指被用户授权可以使用其存储在服务器的资源的客户端。

AG 支持使用一个第三方 OAuth 服务器进行用户认证。当 OAuth 认证启用后，在 AG 设备上将为虚拟站点启用一个 OAuth 客户端。

当终端用户访问虚拟站点并选择使用第三方 OAuth 服务器（例如 Google，WeChat 或企业 WeChat）认证时，OAuth 客户端将重定向终端用户使用 OAuth 服

务器认证并从 OAuth 服务器获取授权。当 OAuth 客户端获取授权许可（授权码）时，它从 OAuth 服务器请求访问令牌。通过访问令牌，OAuth 客户端可以从资源服务器获取用户信息和资源，例如用户名和头像图片。获取的用户名将用于进一步的授权，头像图片将被用做欢迎页面上用户头像。

当 OAuth 客户端成功获取访问令牌后，虚拟站点将通过用户 OAuth 认证。

OAuth 认证工作流程的细节为：

终端用户使用用户代理访问虚拟站点，并选择使用第三方 OAuth 服务器登录。请注意，Google 和 WeChat 仅支持浏览器形式的用户代理，企业 WeChat 支持浏览器和手机应用。

OAuth 客户端（集成在 AG 上）返回一个 302 响应（包括客户端标识符、请求范围和重定向 URL）将用户代理重定向到 OAuth 服务器。

用户代理发送授权请求给 OAuth 服务器。

OAuth 服务器验证授权请求，并将带有登录表格的登录页面或二维码（QR Code）返回给用户进行身份验证。

当通过浏览器使用 WeChat 或企业 WeChat OAuth 服务器进行身份验证时，用户需要输入正确的用户凭证或扫描二维码；当通过手机应用使用企业 WeChat OAuth 服务器进行身份验证时，用户应在企业 WeChat 的工作台页面上选择所需的应用程序，然后单击登录按钮。有关企业 WeChat 手机应用配置的更多详细信息，请参阅配置指南。

如果用户通过认证，OAuth 服务器将检查用户是否将访问权限授权给了 OAuth 客户端。

用户给 OAuth 客户端授予访问权限。

OAuth 服务器返回带有授权码的 302 响应。

用户代理发送授权码给 OAuth 客户端。

OAuth 客户端发送带有授权码的访问令牌请求给 OAuth 服务器。

OAuth 服务器认证 OAuth 客户端并返回携带已发布访问令牌的访问令牌响应。

OAuth 客户端使用访问令牌向资源服务器请求用户信息。

资源服务器返回用户信息（例如用户 ID、邮箱账户、昵称和头像图片）给 OAuth 客户端。

当前，AG 支持使用 Google、WeChat 或企业 WeChat OAuth 服务器进行 OAuth 认证。

如 OAuth 2.0 框架所要求，OAuth 客户端向 OAuth 服务器进行自我身份认证。为达到该目的，管理员需要注册 OAuth 客户端来获取客户端 ID 和密钥并在 OAuth 服务器的服务提供者的研发平台上注册重定向 URL。对于 Google OAuth 服

务器，重定向URL格式必须为“https://<virtual_site_domain_name>/prx/000/http/localhost/oauth_code”。对于WeChat或企业WeChat OAuth服务器，重定向URL必须为虚拟站点域名。关于如何注册OAuth客户端和重定向URL的信息，请联系OAuth服务器的服务供应商。

高级设置

OAuth认证后用户注册

通过OAuth认证后用户注册功能，OAuth认证功能允许将获取的OAuth用户名与AAA服务器上保存的已有公司账号绑定。

当启用OAuth认证后用户注册功能后，OAuth用户需要在通过OAuth认证后在系统上进行注册。在用户注册过程中，用户需要使用“aaa method register”命令指定的AAA方法到认证服务器进行认证。认证通过后，系统将获取的OAuth用户ID（UID）与注册的用户名绑定。注册的用户名将代替获取的OAuth用户名用于后续的授权并显示在欢迎页面上。

当禁用OAuth认证后用户注册功能后，获取的OAuth用户名（用于Google OAuth服务器的邮箱账号或用于WeChat OAuth服务器的昵称）将用于授权。因而，授权服务器与同一AAA方法中的OAuth服务器应该有与获取的OAuth用户名一样的账号。否则，授权会失败。在OAuth用户通过授权后，OAuth用户名将显示在欢迎页面上。

使用邮箱账号前缀作为用户名

当配置了Google OAuth服务器且禁用了OAuth认证后用户注册功能，邮箱账号将被作为授权的OAuth用户名。

通过使用邮箱账号前缀为用户名选项，OAuth认证功能允许使用邮箱账号前缀作为用户名。例如，如果启用该选项且获取的邮箱账号名为“test@gmail.com”，只有“test”会被作为用户名用于后续授权。

OAuth认证后授权过滤

OAuth认证功能允许配置OAuth认证后授权过滤，用于确保只有有效的公司用户可以在OAuth认证后通过授权。只有当OAuth用户名（用于Google OAuth服务器的邮箱账号或用于WeChat OAuth服务器的昵称）匹配OAuth认证后授权过滤时，系统才对用户进行授权。

例如，当OAuth认证后授权过滤配置为“@infosec.com.cn”时，如果获取的OAuth用户名为“test@infosec.com.cn”，系统将对用户进行授权。

使用WeChat服务账号发布虚拟站点资源

当使用WeChat OAuth服务器时，OAuth认证功能允许使用WeChat服务器账号向终端用户发布虚拟站点资源。

当使用WeChat服务器账号时，管理员需要在WeChat官方账户管理平台上注册重定向URL（与研发平台上注册的同样的虚拟站点域名）并获取应用ID和服

务号应用密钥。

此外，管理员需要设置获取的应用 ID 和服务号的应用密码并设置认证服务号的 URL。

配置示例

前提条件

假设已获取到客户端 ID 和密钥、注册的重定向 URL，管理员如果使用了 WeChat OAuth 服务器，那么还需获取应用 ID 和 WeChat 服务号的应用密钥。如果使用了企业 WeChat OAuth 服务器，那么管理员还需要获取企业 ID、应用代理 ID 和企业密钥。

配置指导

要对虚拟站点应用 OAuth 认证，管理员需要完成以下操作：

启用 OAuth 认证来为虚拟站点启用 OAuth 客户端。

定义一个 OAuth 服务器并为 OAuth 客户端设置参数来与 OAuth 服务器通信。这些参数包括：

浏览器的登录 URL：指定 OAuth 服务器登录页面的 URL。

手机应用的登录 URL：指定 OAuth 服务器登录页面的 URL。（只适用于企业 WeChat）

浏览器的响应重定向 URL：指定 OAuth 服务器将重定向响应的 URL。取值必须与注册的 OAuth 服务器的服务提供者的重定向 URL 相同。

手机应用的响应重定向 URL：指定 OAuth 服务器将重定向响应的 URL。取值必须与注册的 OAuth 服务器的服务提供者的重定向 URL 相同。（只适用于企业 WeChat）

获取访问令牌的 URL：指定 OAuth 客户端从 OAuth 服务器获取访问令牌的 URL。

获取用户资源的 URL：指定 OAuth 客户端从资源服务器获取用户信息的 URL。

获取 JWK 集合的 URL：指定 OAuth 客户端获取 JWK 集合的 URL。

注册的客户端 ID：指定注册的 OAuth 客户端 ID。

注册的客户端密钥：指定注册的 OAuth 客户端密钥。

OAuth 认证后注册：指定是否在 OAuth 认证后启用用户注册。

使用邮箱账号前缀作为用户名：指定是否使用邮箱账号前缀作为用户名。

OAuth 认证后授权过滤：指定用于后续授权过滤的正则表达式。

认证服务号的 URL：指定认证服务号的 URL。（只适用于 WeChat OAuth 认证）

服务号的应用 ID：指定注册的服务号的应用 ID。（只适用于 WeChat OAuth

认证）

服务号的应用密钥：指定注册的服务号的应用密钥。（只适用于 WeChat OAuth 认证）

定义一个 HTTP 类型的 AAA 服务器表示 OAuth 客户端，添加 HTTP 请求模板并配置 HTTP 响应过滤规则。

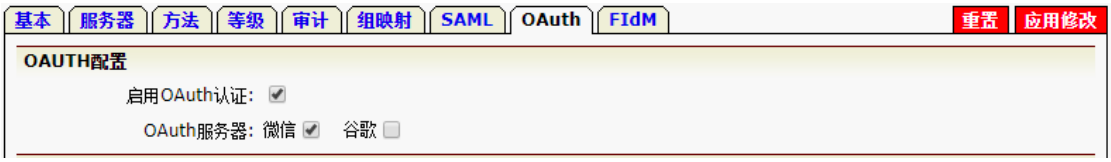
通过将 HTTP 类型的 AAA 服务器设置为认证服务器，以及将另一个 AAA 服务器设置为授权服务器，来配置一个 AAA 方法。

通过将授权服务器设置为 None 来配置另一个 AAA 方法，并配置该 AAA 方法用于 OAuth 认证后用户注册。

为虚拟站点导入并激活 H5VPN 门户主题。

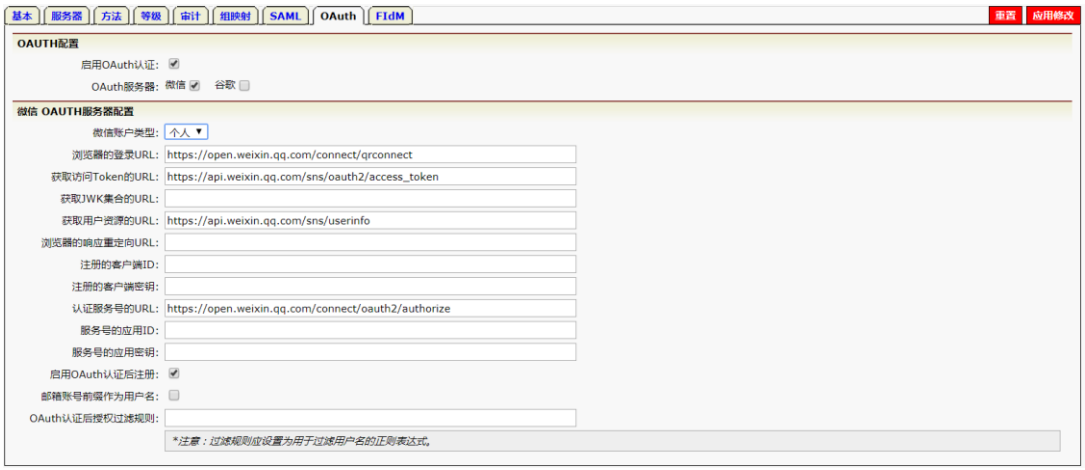
配置步骤

选择站点配置>AAA>OAuth，在 OAuth 配置区域选择启用 OAuth 认证复选框，为参数 OAuth 服务器选择 WeChat 或 Google 复选框，并点击应用修改按钮。



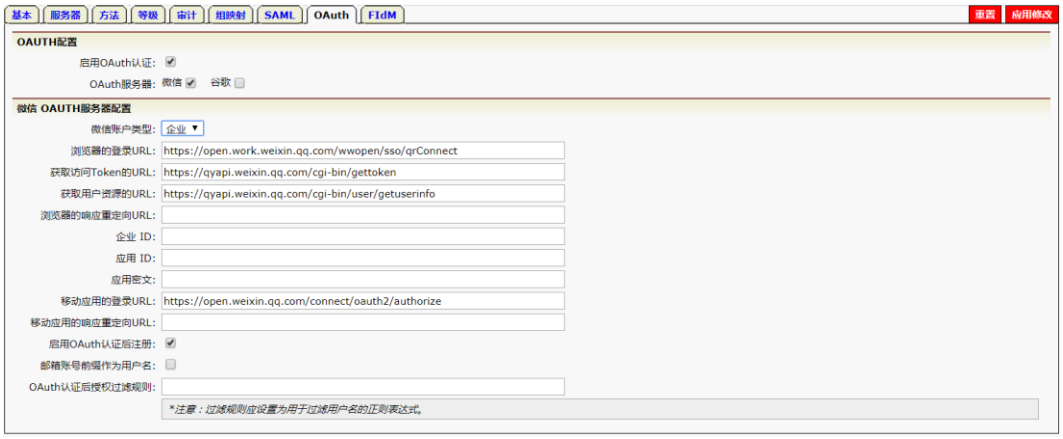
如果为参数 OAuth 服务器选择了 WeChat 复选框，在 WeChat OAuth 服务器配置区域：

对于使用 WeChat OAuth 服务器的认证，设置参数微信账号类型为个人，指定参数浏览器的登录 URL、获取访问 Token 的 URL、获取 JWK 集合的 URL、获取用户资源的 URL、浏览器的响应重定向的 URL、注册的客户端 ID、注册的客户端密钥、认证服务号的 URL、服务号的应用 ID、服务号的应用密钥、启用 OAuth 认证后注册、邮箱账号前缀作为用户名和 OAuth 认证后授权过滤规则，并点击应用修改按钮。

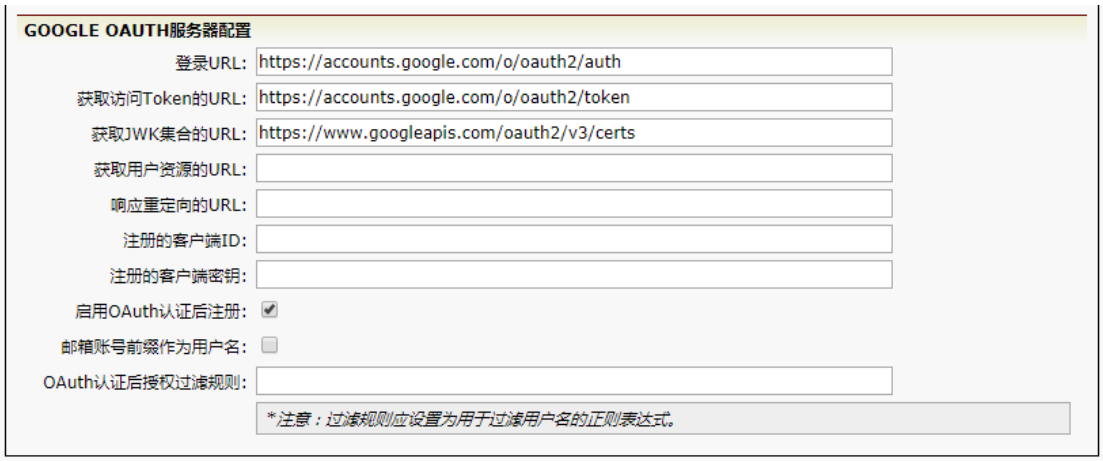


对于使用企业 WeChat OAuth 服务器的认证，设置参数微信账号类型为企业，指定参数浏览器的登录 URL、获取访问 Token 的 URL、获取 JWK 集合的 URL、获

取用户资源的 URL、浏览器的响应重定向的 URL、企业 ID、应用 ID、应用密文、移动应用的登录 URL、移动应用的响应重定向 URL、启用 OAuth 认证后注册、邮箱账号前缀作为用户名和 OAuth 认证后授权过滤规则，并点击应用修改按钮。



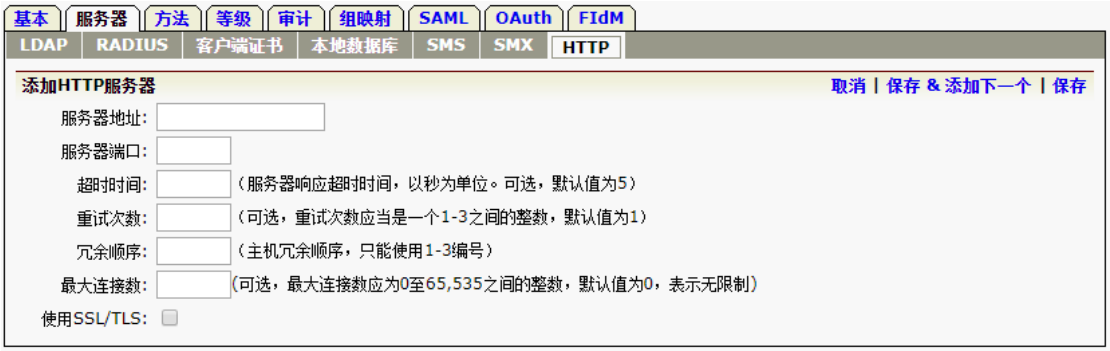
如果为参数 OAuth 服务器选择了 Google 复选框，在 Google OAuth 服务器配置区域，指定参数登录 URL、获取访问 Token 的 URL、获取 JWK 集合的 URL、获取用户资源的 URL、响应重定向的 URL、注册的客户端 ID、注册的客户端密钥、启用 OAuth 认证后注册、邮箱账号前缀作为用户名和 OAuth 认证后授权过滤规则，并点击应用修改按钮。



选择站点配置>AAA>服务器>HTTP，在服务器列表区域指定参数服务器名并点击添加操作链接。

双击新加的条目。在弹出窗口的 HTTP 服务器配置，点击添加 HTTP 服务器操作链接。

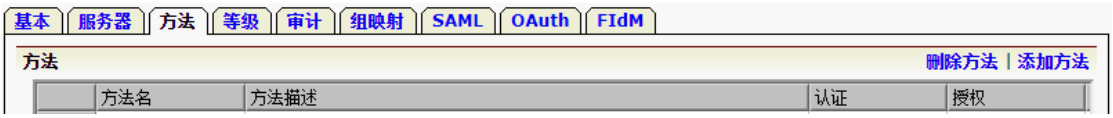
在弹出的添加 HTTP 服务器窗口中，分别设置参数服务器地址和服务器端口为“localhost”和“54322”并点击保存操作链接。



准备 HTTP 请求模板文件并通过在导入 HTTP 请求模板区域点击导入操作链接导入。

在 HTTP 服务器高级配置区域，指定参数正则表达式、用户名属性、头像 URL 属性、用户 ID 属性和错误信息属性，并点击应用修改按钮。

选择站点配置>AAA>方法，并在方法区域点击添加方法按钮。



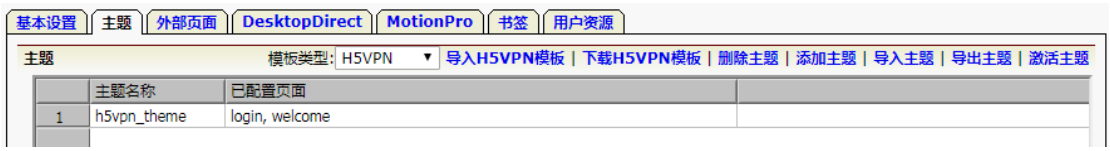
在弹出的添加方法配置区域，指定参数方法名，将认证参数设置成为 OAuth 认证配置的 HTTP 服务器，将授权参数设置为另一台 AAA 服务器，并点击保存&添加下一个操作链接。

在弹出的添加方法配置区域，指定方法名参数，为配置的 AAA 服务器设置认证参数，例如 LocalDB 服务器，设置授权参数为 NONE，并点击保存操作链接。

点击方法页签，设置参数用于设备、MotionProOTP 或用户注册的 AAA 方法，并点击应用修改按钮以保存配置。

选择站点配置>门户>主题，设置目标类型为 H5VPN，并在主题区域点击导入 H5VPN 模板操作链接。

选择导入的 H5VPN 主题，并点击激活主题操作链接进行激活。



3.1.10 SMX

安全矩阵（SECUREMATRIX，SMX）是一个高度安全和无令牌的认证方法，结它将模式和图像组合在一起形成一次性密码。在需要认证时，SMX 服务器随机产生一个唯一的矩阵并发送给用户终端。矩阵表格每次登录都会改变，但是模式不

变。用户只需要在他们选择的叠加模式中按照预先选择和注册的顺序输入数字。

注意：SECUREMATRIX®认证方法的专利拥有权归属于日本的 CSE Secure Systems 公司。

AG 只支持使用 SMX 进行认证。

一个虚拟站点最多支持配置 3 台 SMX 服务器。考虑到冗余性，每台服务器最多可以有两台主机：一台主用主机和一台备用主机。主用主机是必须配置，备用主机为可选。只有当用户未通过主用主机认证或主用主机不可用时，才会使用备用主机。

为了使得 SMX 主机可以用于认证，必须为 AG 导入 SMX 主机的证书文件。可以通过 AG WebUI 使用下面任意一种方法将证书文件导入 AG：

从 SMX 主机导入：需要指定登录 SMX 主机的凭证。

从本地主机导入：需要在本地主机上指定证书文件的路径。

从远程主机导入：需要指定登录远程主机的凭证和远程主机上证书文件的路径。

配置示例

在虚拟站点模式下，选择站点配置>AAA>服务器>SMX，在服务器列表区域指定参数服务器名和描述，并点击添加按钮添加一台 SMX 服务器。

在服务器列表区域双击该服务器条目，在显示窗口的 SMX 服务器高级配置区域，为 SMX 服务器添加主用和备用主机。

3.1.11 HTTP AAA 服务器认证

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：

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“portal custom variant name”和“portal custom variant 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。

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）。

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。

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。

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。

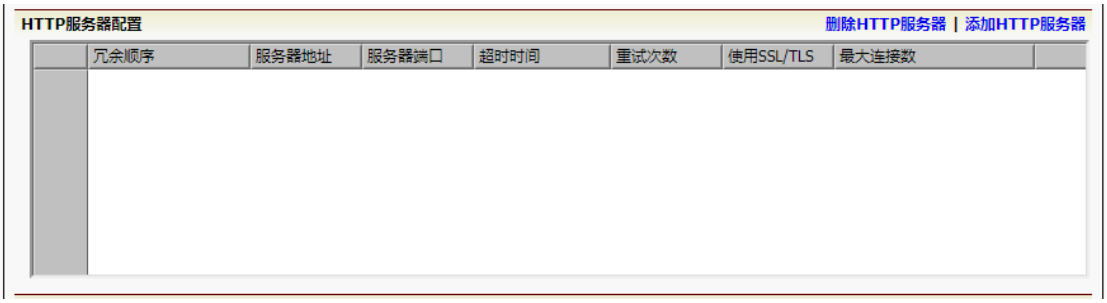
当 HTTP AAA 服务器用于授权时，AG 使用 HTTP 响应过滤器从 HTTP（授权）响应数据包中获取用户信息，例如用户名和组名。获取的用户名将会现在门户欢迎页面上替代用于登录的用户名。获取的组名可能会用于进一步的用户授权。如果没有获取到认证用户的组名，将会使用默认组（通过命令“aaa server http defaultgroup”配置）用于进一步授权。

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。

配置示例

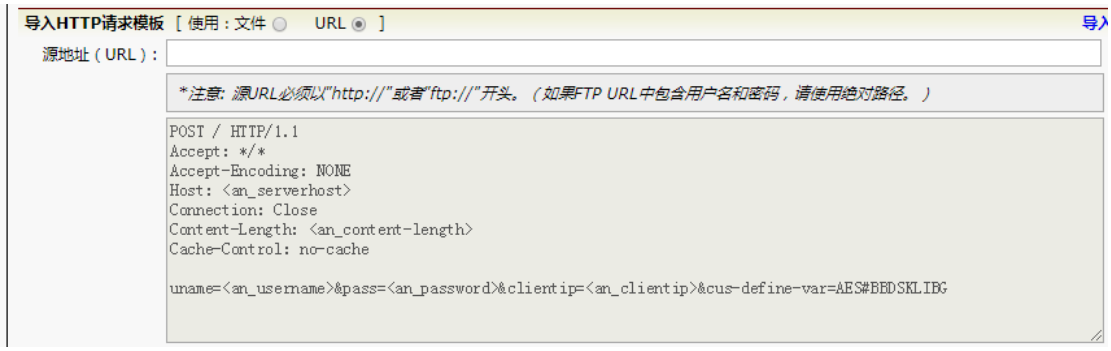
在虚拟站点模式下，选择站点配置>AAA>服务器>HTTP，在服务器列表区域指定参数服务器名和描述并点击添加按钮添加一个 HTTP 服务器。

在服务器列表区域双击该服务器条目。在 HTTP 服务器配置区域，点击添加 HTTP 服务器操作链接。



根据需要指定 HTTP 服务器的参数。

在导入 HTTP 请求模板区域，点击导入导入 HTTP 认证请求模板。



在 HTTP 服务器高级配置区域，根据需要指定 HTTP 服务器的高级参数。

3.1.12 SAML

SAML（Security Assertion Markup Language，安全声明标记语言）是一种基于 XML 的开放标准数据格式，用于交换数据。

在 SAML 架构中，两个主要实体为：

身份提供者（Identity Provider，IdP）：对用户的信息进行声明的实体。IdP 声明的信息与认证、属性和授权有关。

服务提供者（Service Provider，SP）：为用户提供资源并依靠 IdP 的声明信息进行认证和授权的实体。当启用 SAML 功能时，AG 相当于 SAML SP。

当为虚拟站点启用 SAML 功能后，虚拟站点将只使用 SAML 进行认证和授权，并忽略 AAA 功能的其他认证和授权配置，例如 LocalDB 和 LDAP。当禁用 SAML 功能后，虚拟站点将使用 AAA 功能的认证和授权配置。

一个虚拟站点最多可配置 3 个 IdP，但是一个 SP 最多只能启用一个 IdP。在为 SP 启用 IdP 前，需要将 IdP 的元数据导入 SP 并使用命令“aaa saml idp attributes”指定用于从 IdP 返回的 SAML 声明响应用于获取用户身份信息的属性。

SSO（Single Sign-On，单点登录）

SAML SSO 的工作流程如下：

当 SAML 功能启用后，终端用户使用浏览器访问 AG（SP）提供的后台资源

AG 构建一个 SAML 认证请求并指示浏览器根据 IdP 元数据中要求的绑定类型发送 SAML 认证请求。

检查用户凭据后，IdP 生成一个包含声明信息的 SAML 响应并基于 SP 元数据中要求的绑定类型将响应返回给 SP。

AG 提取并验证 SAML 响应中的声明信息，以此决定用户是否通过 SAML 认证。

AG 使用命令“aaa saml idp attributes”中指定的属性从 SAML 响应中提取用户身份信息，例如用户名、组名、外部 ACL 规则和 Netpool，以用于进一步授权。

当用户访问其他由 AG 保护的后台资源时，用户不需要再次提供用户凭据，如果在已有的用户会话中资源已授权给终端用户，AG 将提供这些资源的访问。

SLO（Single LogOut，单点退出）

当启用 SAML 功能后，AG 也支持 SAML SLO。也就是说，如果终端用户登录 AG 和其他 SP 并由（使用 SAML SSO 的）相同 IdP 进行身份验证，那么当他们从一个 SP 退出时，他们也会从其他 SP 退出。

SAML SLO 的工作流程如下：

当收到一台 SP（非 AG）的 SAML 退出请求时，IdP 构建一个 SAML 退出请求并使用 SP 元数据中要求的绑定类型将它发送到 AG 上的 SLO 服务。

收到 SAML 退出请求后，AG 移除终端用户的会话并通知 IdP。

然后发送 SAML 退出响应给 SP，用于通知所有相关 SP 的退出进程状态

反过来，当从 AG 退出时，终端用户也会从其他 SP 退出。

元数据

为了建立 IdP 和 SP 间的信任关系，管理员需要交换 IdP 和 SP 的元数据。即管理员需要将 IdP 的元数据导入到 SP（AG）并将 SP 的元数据导入到 IdP。而且，导入到其他实体的元数据应为最新状态。

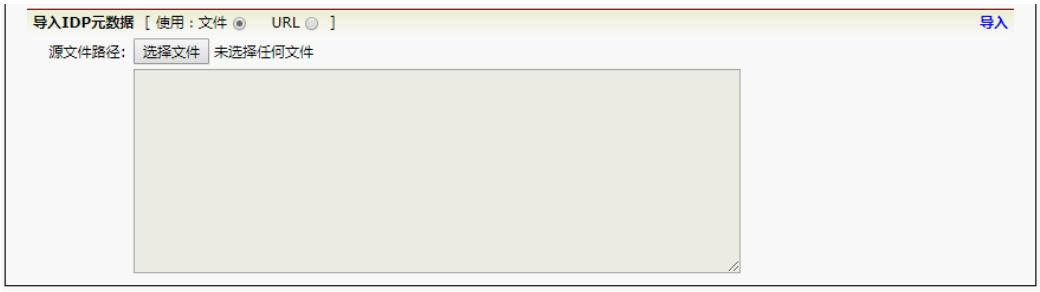
IdP 的元数据指定了 IdP 的配置和要求，例如为 IdP 的 SSO 服务指定 SAML 认证请求的绑定类型。

SP 的元数据指定服务器提供者的配置和要求，例如为 SP 上的 ACS（Assertion Consumer Service，声明消费者服务）指定 SAML 响应的绑定类型以及为 SP 上的 SLO 要求的 SAML 退出请求指定绑定类型。ACS 要求的 SAML 响应的绑定类型可以通过“aaa saml sp acs”命令配置。SLO 要求的 SAML 退出请求的绑定类型可以通过“aaa saml sp slo”命令配置。

配置示例

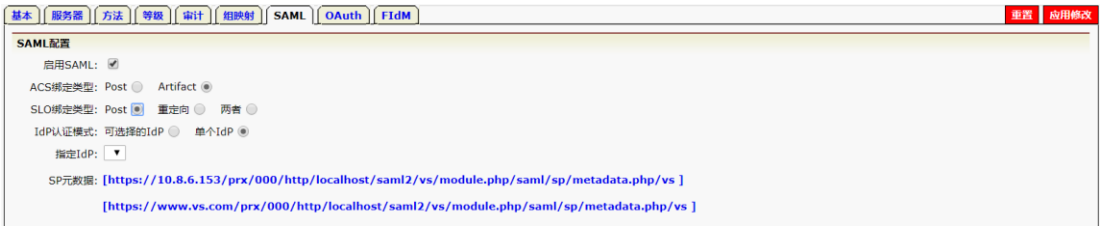
在虚拟站点模式下，选择站点配置>AAA> SAML。点击增加 IDP。在 IdP 配置区域指定参数并在 IDP 属性区域指定参数用户名称、组名称、外部 ACL、Netpool、用户密码和角色。

在导入 IDP 元数据区域，指定参数源文件路径并点击导入将 IdP 的元数据文件导入 SP。



在 SAML 配置区域，指定参数 IdP 认证模式为单个 IdP 并选择一个 IdP。

在 SAML 配置区域，选择启用 SAML 复选框并指定参数 ACS 绑定类型和 SLO 绑定类型。

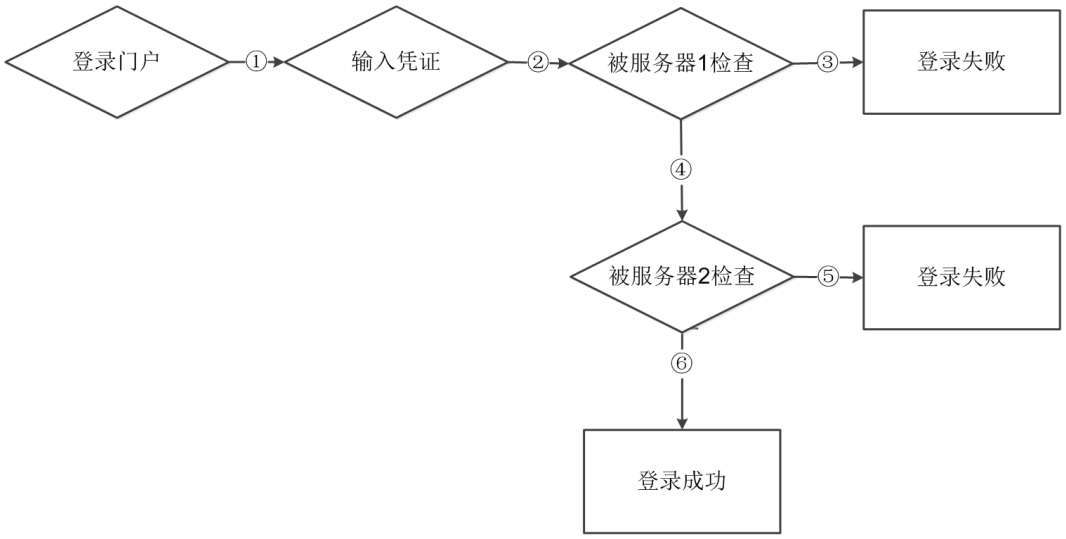


点击 SP 元数据的任一 URL 下载 SP 的元数据文件并导入到 IdP。

3.1.13 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。



上图显示了多因素认证的工作流程（两个认证服务器）：

用户到达需要凭证的虚拟站点的 Web 门户。

认证服务器 1 检查为这台服务器输入的用户凭据。

如果凭证被服务器 1 拒绝，登录失败。

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。

如果凭证不正确，AG 提示用户再次输入凭证。

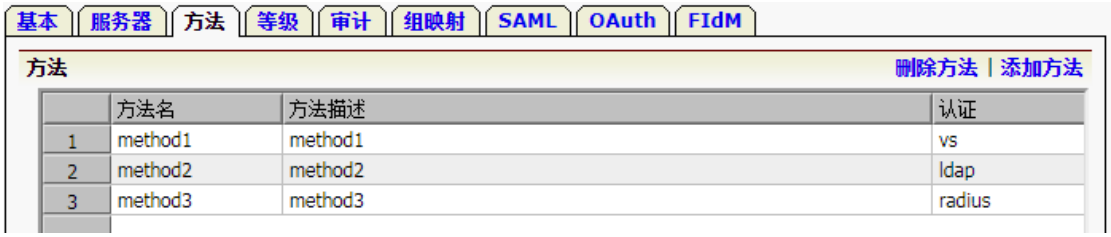
如果凭证正确，AG 为用户显示成功登录页面。

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。

配置示例

在虚拟站点模式下，选择站点配置>AAA>方法，并在方法区域点击添加方法按钮。



在添加方法配置区域，指定参数方法名和方法描述，为认证选择特定的 AAA 服务器，并为授权选择特定的 AAA 服务器，点击保存操作链接。

3.1.14 FIdM 认证

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。

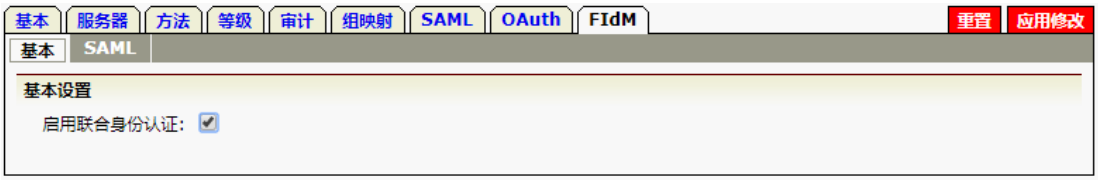
SAML FIdM 认证

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。

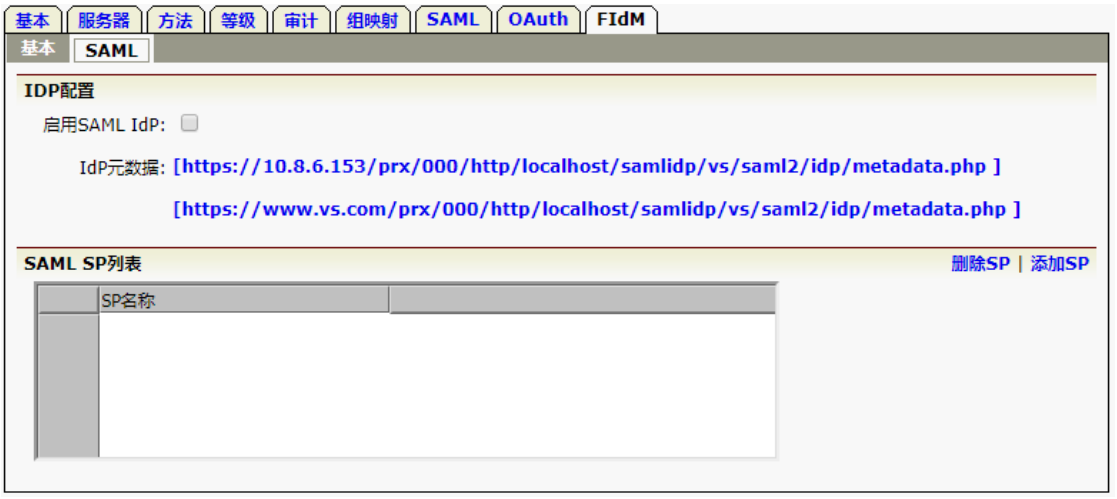
要使用 SAML FIdM，管理员需要为虚拟站点（作为 SAML IdP）配置 SAML SP 作为提供认证和授权服务的对象。

配置示例

在虚拟站点模式下，选择站点配置>AAA>FIdM>基本，在基本设置区域选择启用联合身份认证复选框，并点击应用修改按钮。

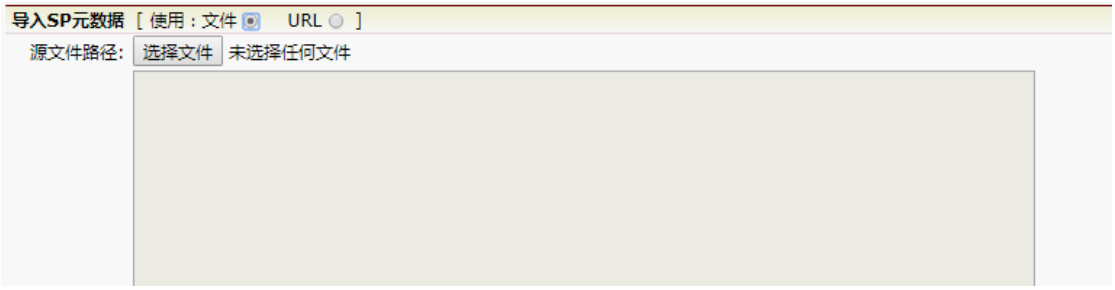


点击 SAML 页签，并在 SAML SP 列表区域点击添加 SP 操作链接。



在 SAML SP 配置区域，指定参数 SP 名称并点击应用修改按钮。

在导入 SP 元数据区域，指定使用为文件，点击选择文件按钮定位本地元数据文件，并点击导入操作链接。或者，也可以指定使用为 URL，指定参数源地址（URL）并点击导入操作链接。



3.1.15 用户角色

AG 设备根据特定的资格（如登录时间、用户名、组名、源 IP 和 AAA 认证方法）授予已认证的用户相应的角色，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，AG 设备将迫使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。用户登录虚拟站点后，AG 设备支持在 Web 门户中显示可访问授权资源（通常为网页和文件共享资源）的相关链接。

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。AG 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

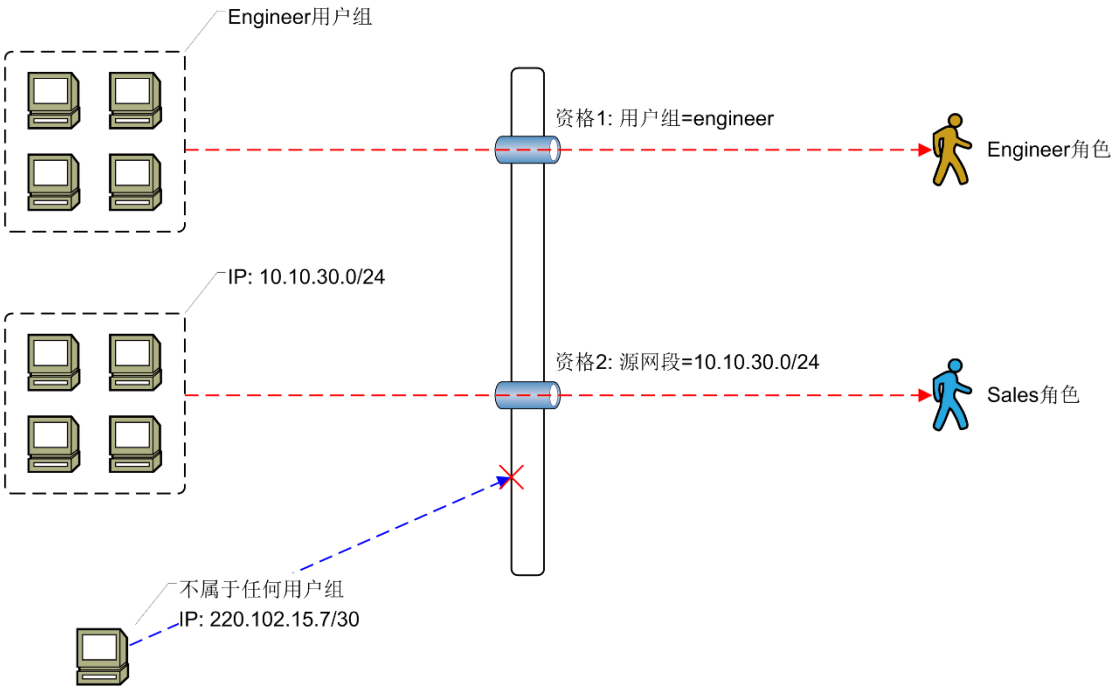
登录星期

用户名

组名

源 IP 地址

AAA 认证方法



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 Group”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“Sale”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，因此无法访问 AG 设备的任何资源。

角色资源

可为角色分配以下类型的资源：

WRM

QuickLink

IPv6 网页

Netpool

VPN 资源组

通用互联网文件系统（CIFS）

要为角色分配资源，管理员需要将角色和资源进行关联。

WRM、QuickLink 和 IPv6 网页角色资源都属于 Web 角色资源。当用户获得的角色关联了 IPv4 或 IPv6 网页角色资源时，Web 门户上将会显示这些 Web 资源的访问链接。用户可以通过点击链接来访问这些 Web 资源。

Netpool 角色资源将角色与 VPN Netpool 资源绑定在一起，该资源包含用于 VPN 网络访问的配置（如 IP 范围）。

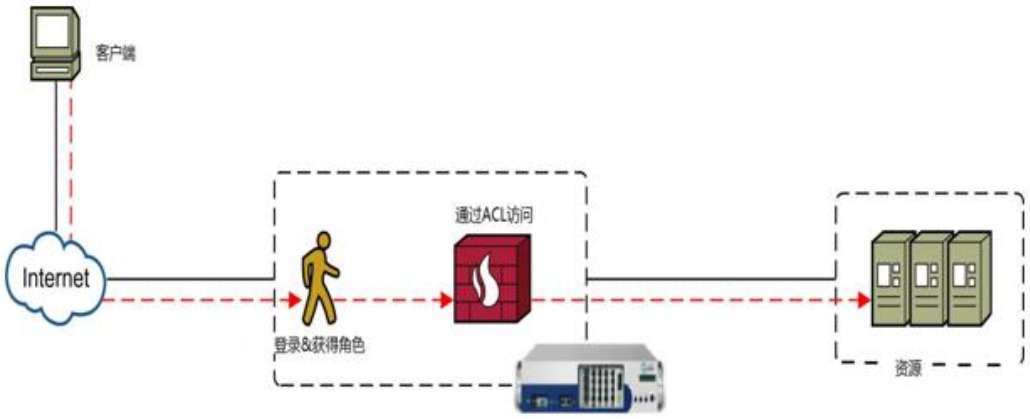
VPN 资源组将角色与 VPN 资源组绑定在一起，VPN 资源组包含应用型和网络型 VPN 资源列表。

当用户同时获得 Netpool 角色资源和 VPN 资源组访问权限时，Web 门户将会显示一个连接 VPN 的按钮。点击按钮后，用户和 AG 设备间的 VPN 通信隧道将会建立。在客户端与 VPN 资源组指示的目的地址之间传输的数据将会被 VPN 隧道加密。

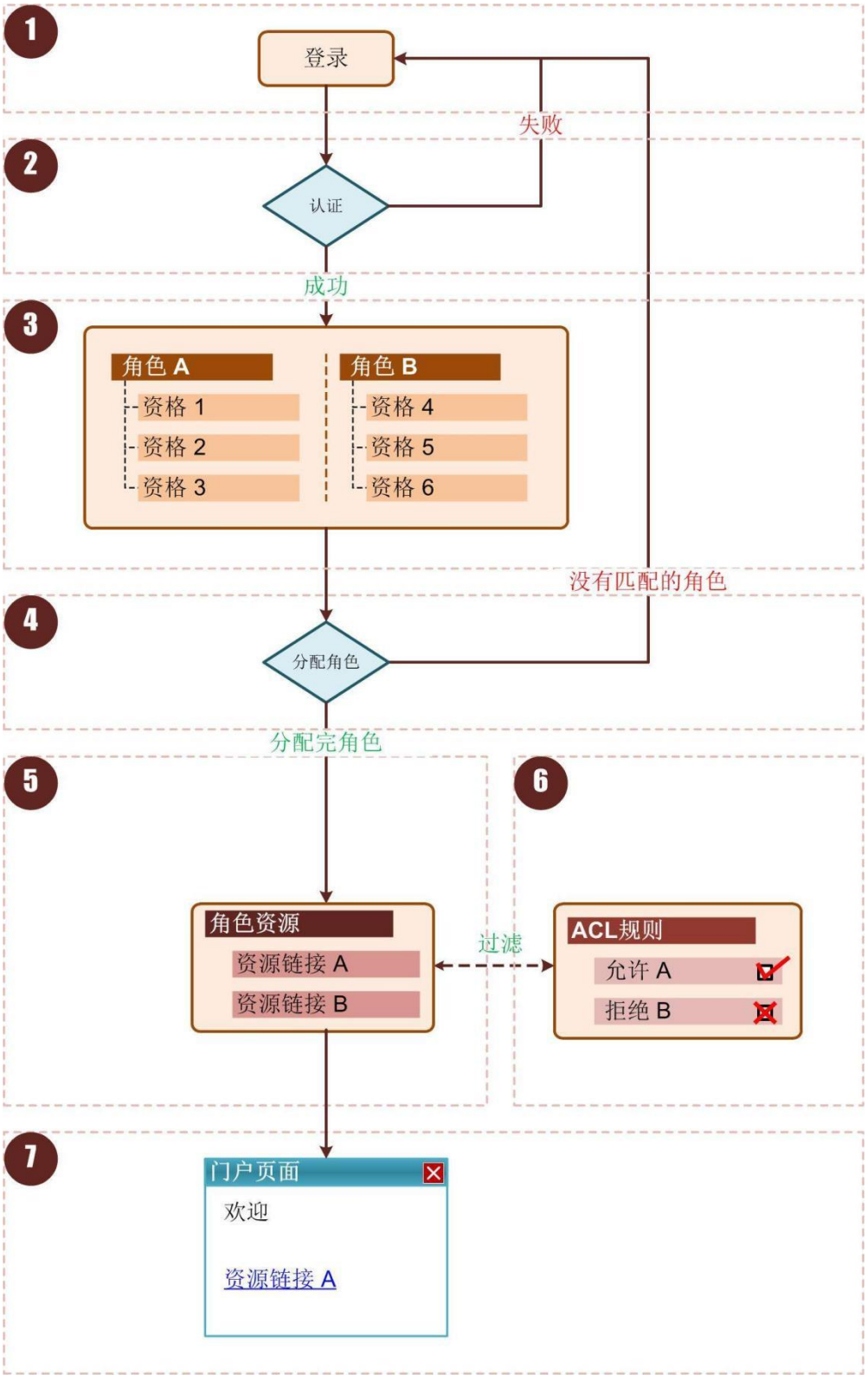
CIFS 资源将角色与运行 CIFS 协议的后端主机共享文件夹绑定在一起。点击该链接时，该角色用户可以查看共享文件夹下的所有文件。角色对于该共享文件夹的操作权限取决于后端主机上设置的共享文件夹权限。

系统为 WRM、QuickLink 和 CIFS 类型的角色资源提供了一个“自动生成 ACL 允许配置”选项。当添加 WRM、QuickLink 和 CIFS 角色资源时启用了该选项，系统会自动生成一个 ACL 资源，并将 ACL 资源添加到一个自动生成的资源组，最后生成一个优先级为 200 的 ACL 允许规则。对于 WRM 和 QuickLink 类型的角色资源，自动生成的资源组名称为“auto_web_resgroup_for_<role_name>”。对于 CIFS 类型的角色资源，自动生成的资源组名称为“auto_fileshare_resgroup_for_<role_name>”。自动生成的 ACL 允许规则配置无法手动删除，而只有通过删除指定的角色资源才能将其删除。

下图展示了角色资源的工作流程。



用户角色的工作流程



上图展示了用户角色的工作流程：

最终用户登录到虚拟站点的 Web 门户。

用户名和密码被发送到 AAA 服务器进行认证。如果身份认证失败，最终用户将被要求重新登录。如果认证成功，AG 设备将会为通过身份认证的用户分配一个角色。

AG 设备中已经预先定义了几个角色，每个角色中定义了若干资格。

要获取一个角色，用户信息必须至少匹配为角色定义的其中一个资格。如果用户信息无法匹配任何资格，用户将会看到登录错误提示信息，并重新回到登录页面。

获得角色之后，用户将被授权访问与角色相关的资源。在该示例中，角色关联了两个 Web 资源：资源链接 A 和资源链接 B。

AG 设备会进一步使用 ACL 规则过滤已授权的资源。根据配置的 ACL 规则，用户可以访问资源链接 A，而无法访问资源链接 B。因此，只有资源链接 A 被授权给此用户访问。

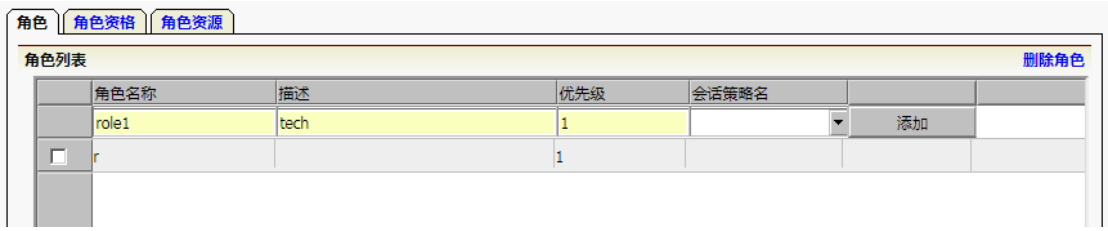
最后，资源链接 A 会显示在 Web 门户上，以供最终用户访问。

配置示例

角色设定

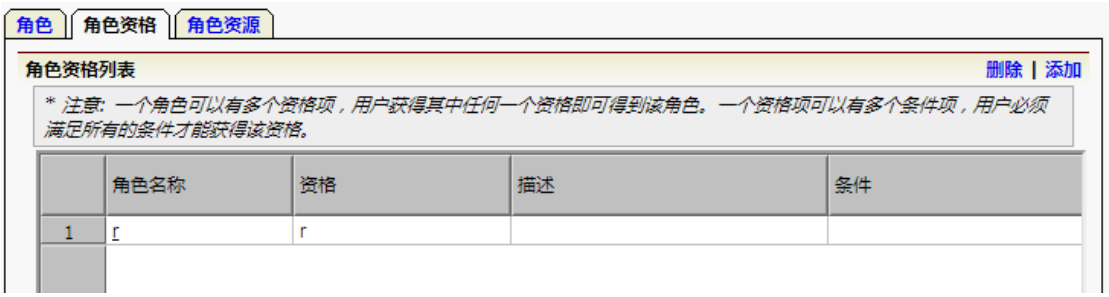
添加一个角色

在虚拟站点模式下，选择用户策略>角色>角色，输入角色名称和描述（可选）中，然后点击添加按钮。



添加一个角色资格

在虚拟站点模式下，选择用户策略>角色>角色资格，点击添加按钮。



在添加角色资格窗口，从下拉菜单中选择已创建的角色名称，输入资格名称，描述（可选），并在条件中指定类型、操作和内容。

添加一个角色资格

例如，可以在角色条件中将登录时间指定为工作时间。

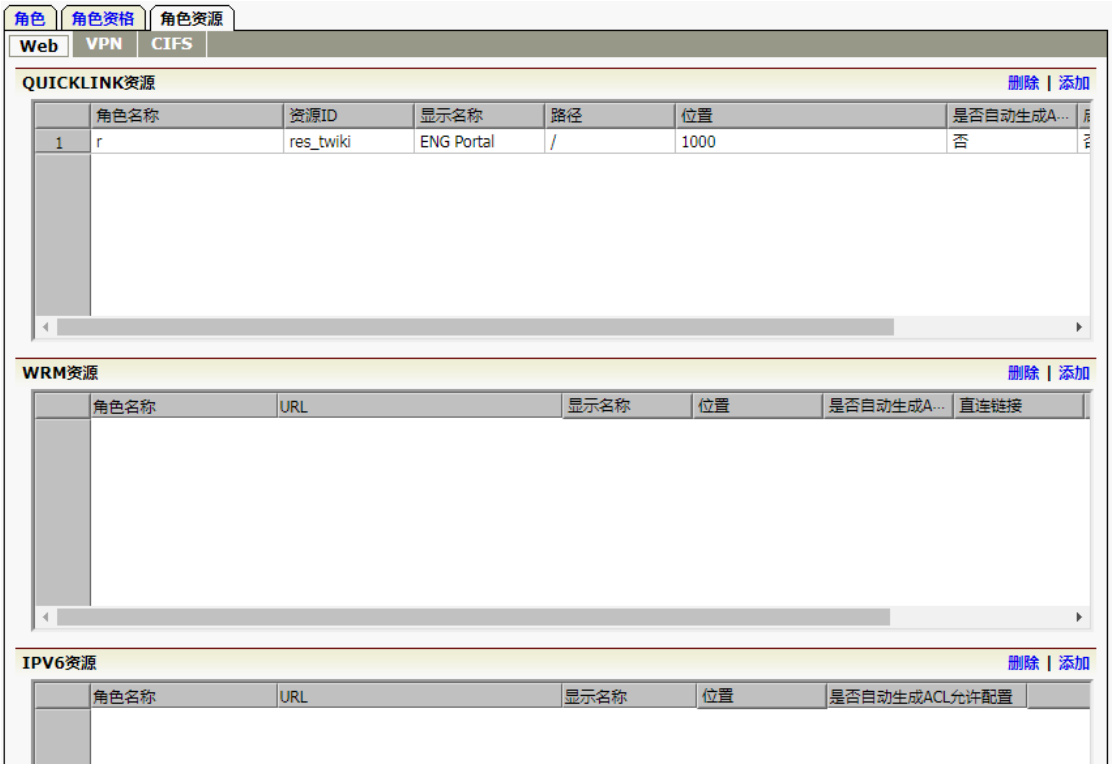
点击添加按钮，角色条件添加成功。

在添加角色资格区域定义完所有参数后，请点击右上角的保存按钮。

角色资源

添加 QuickLink 类型的角色资源

在虚拟站点模式下，选择用户策略>角色>角色资源>Web，在 QuickLink 资源区域点击添加按钮来为角色分配 QuickLink 资源。



在添加 QuickLink 资源窗口，在角色名称下拉菜单中选择已定义的角色，在资源 ID 下拉菜单中选择一个已定义的 QuickLink 策略，指定参数显示名称、路径、位置，按需勾选是否自动生成 ACL 允许配置，启用前端 SSO 和设备 ID 字段选项框，最后点击保存按钮将 QuickLink 资源分配给角色。

添加 WRM 类型的角色资源

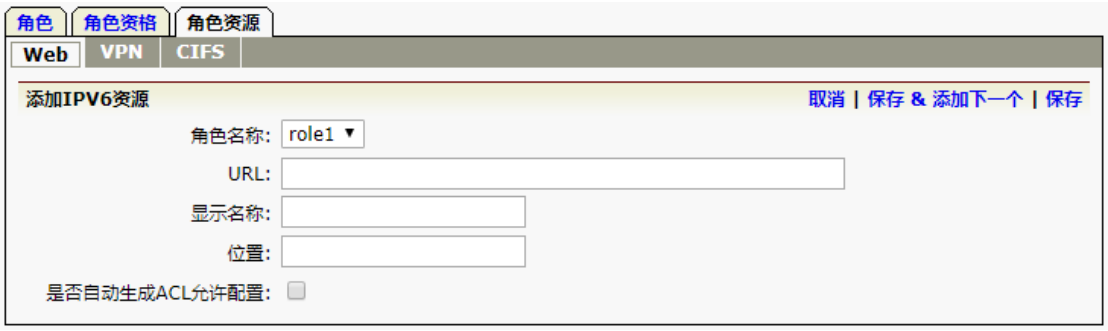
在虚拟站点模式下，选择用户策略>角色>角色资源>Web，在 WRM 资源区域点击添加按钮来为角色分配 WRM 资源。

在添加 WRM 资源窗口，在角色名称下拉菜单中选择已定义的角色，指定参数 URL、显示名称、位置，按需勾选是否自动生成 ACL 允许配置、直连链接、启用前端 SSO 和设备 ID 字段选项框，最后点击保存按钮将 WRM 资源分配给角色，。

添加 IPv6 Web 类型的角色资源

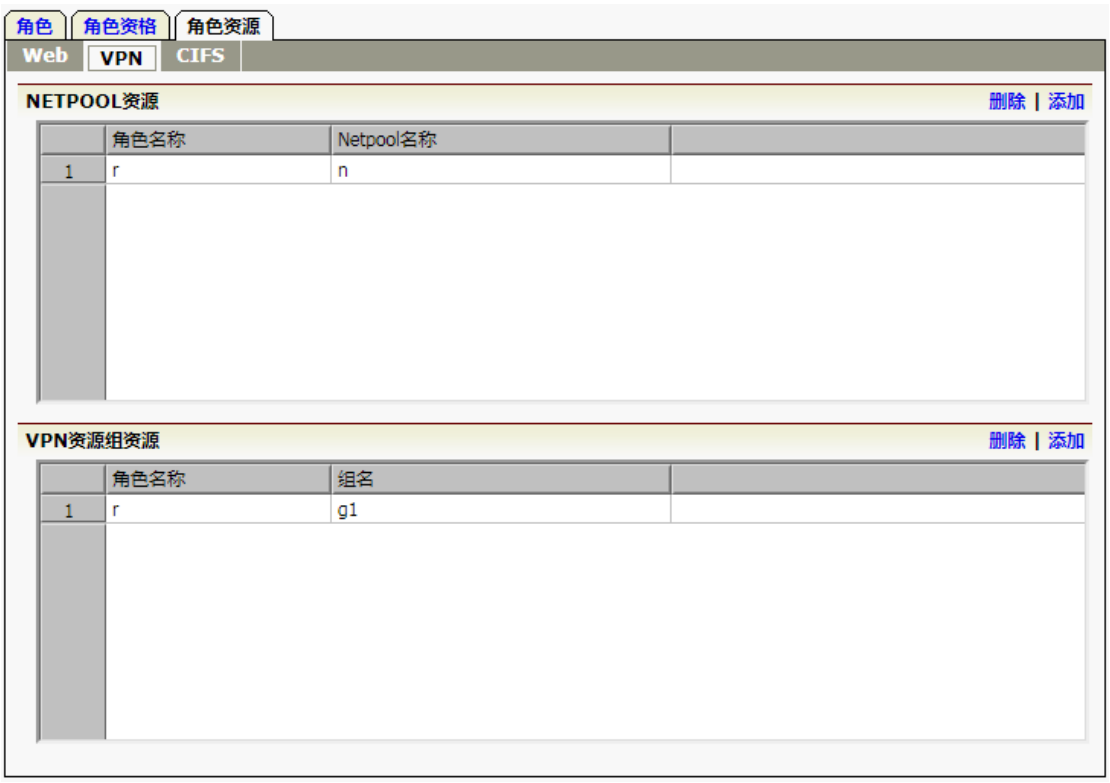
在虚拟站点模式下，选择用户策略>角色>角色资源>Web，在 IPv6 资源区域点击添加按钮来为角色分配 IPv6 资源。

在添加 IPv6 资源窗口，在角色名称下拉菜单中选择已定义的角色，指定参数 URL、显示名称、位置，按需勾选是否自动生成 ACL 允许配置选项框，最后点击保存按钮将 IPv6 资源分配给角色。

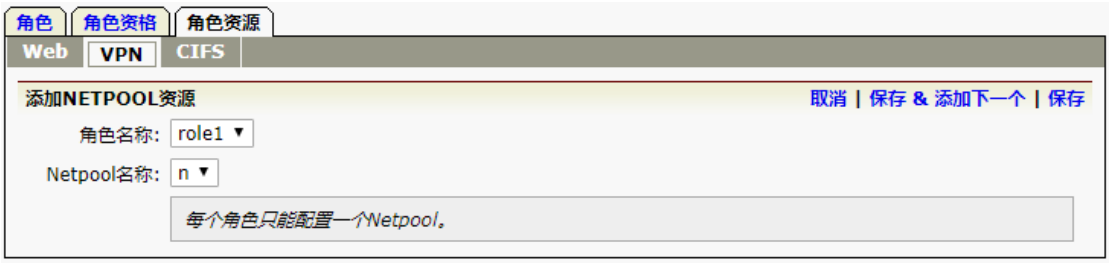


添加 VPN 类型的角色资源

在虚拟站点模式下，选择用户策略>角色>角色资源>VPN，在 Netpool 资源区域点击添加按钮来为角色分配 Netpool 资源。

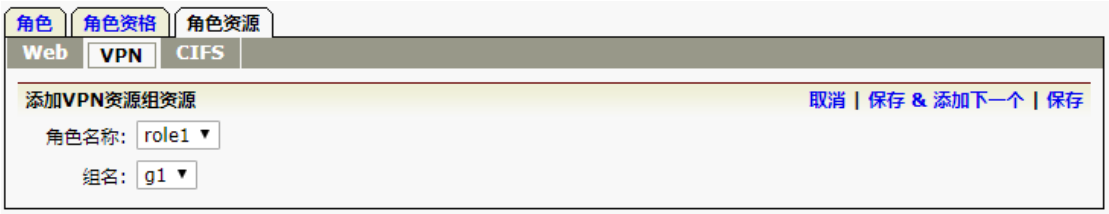


在添加 Netpool 资源窗口，在角色名称和 Netpool 名称下拉菜单中选择已定义的角色名称和 Netpool 名称，最后点击保存按钮将 Netpool 分配给角色。



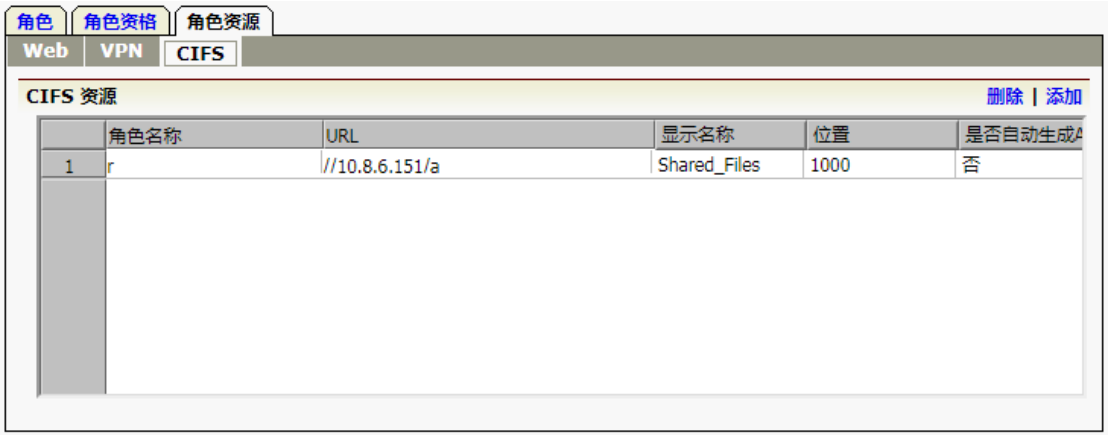
为确保 VPN 资源能正常工作，需要将 VPN 资源组分配给角色。在虚拟站点模式下，选择用户策略>角色>角色资源>VPN，在 VPN 资源组资源区域点击添加按钮来为角色分配 VPN 资源组。所示。

在添加 VPN 资源组资源窗口，在角色名称和组名下拉菜单中选择已定义的角色名称和组名，最后点击保存按钮将 VPN 资源组分配给角色。



添加 CIFS 类型的角色资源

在虚拟站点模式下，选择用户策略>角色>角色资源>CIFS，在 CIFS 资源区域点击添加按钮来为角色分配 CIFS 资源。



在添加 CIFS 资源窗口，在角色名称下拉菜单中选择已定义的角色，指定参数 URL、显示名、位置，按需勾选是否自动生成 ACL 允许配置选项框，最后点击保存按钮将 CIFS 资源分配给角色。

3.1.16 访问控制列表

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，可以针对被访问资源的 IP 地址、端口、提供的服务、URL 地址等进行权限控制。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。ACL 支持对三种类型的资源进行访问权限控制：Web 应用（HTTP/HTTPS）、网络资源（IP/TCP/UDP/ICMP）和 CIFS（文件共享）资源。

ACL 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 都会生效。所有的 ACL 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，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。

如果用户会话与指定虚拟站点关联的 ACL 没有任何匹配项，用户将能通过该虚拟站点不受限制地访问所有 Web、文件共享和 VPN 类型的资源。如果用户会话与指定虚拟站点关联的 ACL 有一项或多项匹配，且这些 ACL 应用到了某种类型（Web、文件共享或 VPN）的部分或全部资源，那么在没有 ACL 指定允许访问的前提下，AG 设备将拒绝用户访问该类型的资源。

ACL 资源

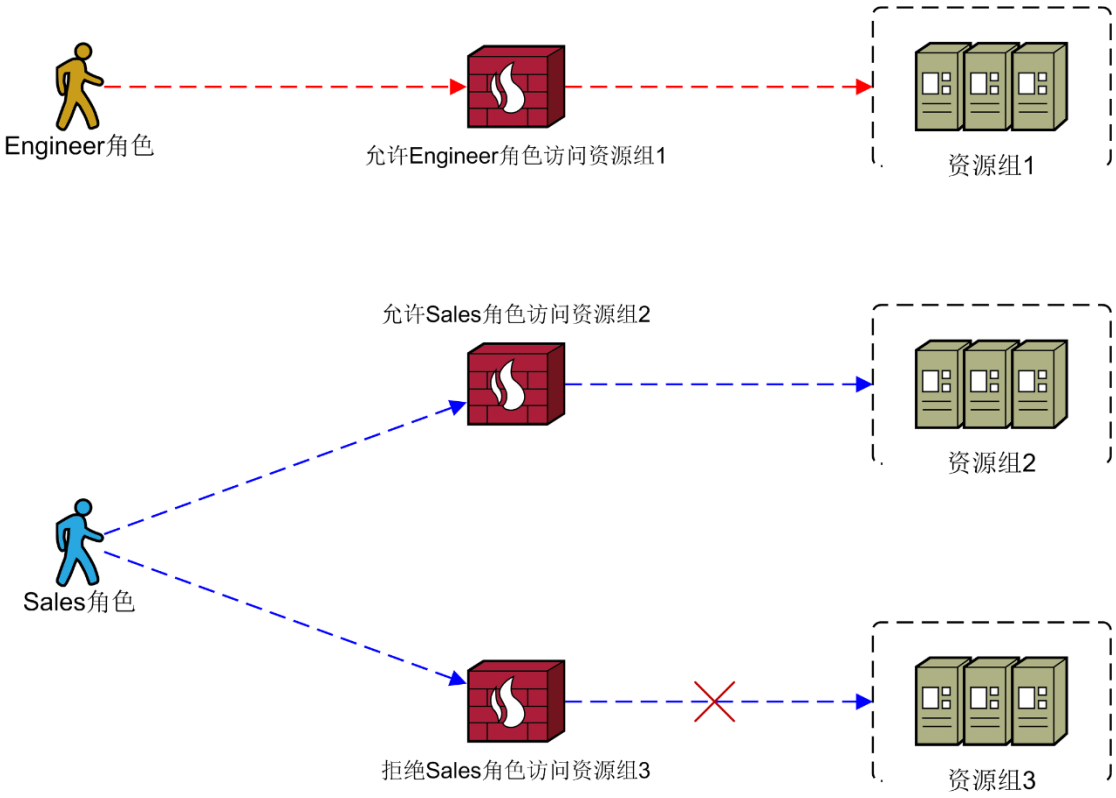
管理员可以定义三种类型的 ACL 资源:Web 资源、网络资源和文件共享资源。

Web 资源是一种七层资源，如“http://*.domain.com/public/*”或“https://www.domain.com:443/*”。

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”。

文件共享资源是一种 CIFS（DFS）资源，如“\\10.3.0.255\test”和“\\Intranet\Employees*”。

资源组是一种可以包含一个或多个同类型资源的对象。一个 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。



外部 ACL

AG 设备也支持储存在 LDAP 或 RADIUS 服务器上的外部 ACL。外部 ACL 将会检查用户是否可以访问请求的资源，优先级高于配置在 AG 设备的 ACL。当没有匹配任何外部 ACL 时，AG 才会使用配置在设备上的 ACL。

AG 设备支持两种类型的外部 ACL。

第一种类型的 ACL 应用于 Web 和文件共享流量，其格式为：

<priority> <scheme>:<host><path> [AND <virtual_site_id>] {PERMIT|DENY}

下表描述了每个字段的含义：

字段	含义
priority	该字段指定 ACL 的优先级，取值越小，优先级越高。当请求匹配多个 ACL 时，由优先级最高的 ACL 来决定是否允许或拒绝该请求。
scheme	该字段的取值只能是“http”或“file”。 “http”表示该 ACL 应用于 Web 请求(包括 HTTP 和 HTTPS)。 “file”表示该 ACL 应用于文件共享请求（CIFS)。
host	该字段指定后端 Web 或 CIFS 服务器的 IP 地址或是服务器名称。支持在主机名称前使用通配符（*）来匹配一个或多个字符。
path	该字段指定后端 Web 或 CIFS 服务器的请求的 Web 路径或文件共享路径。路径名称必须包含至少一个正斜杠（/)。如果请求路径以 ACL 中的“path”字段值开始，则请求路径匹配该 ACL。
virtual_site_id	该字段指定该 ACL 关联的虚拟站点名称。取值“ALL”表示该 ACL 关联所有的虚拟站点。
PERMIT|DENY	该字段指定是否允许或拒绝访问后端 Web 和 CIFS 服务器的 Web 和 CIFS 请求。

第二种类型的 ACL 应用于 VPN 流量，其格式为：

<priority> ip <protocol>:<host_ip>[/<netmask>][:port] [AND <virtual_site_id>] {PERMIT|DENY}

下表描述了每个字段的含义：

字段	含义
priority	该字段指定 ACL 的优先级，取值越小，优先级越高。当请求匹配多个 ACL 时，由优先级最高的 ACL 来决定是否允许或拒绝该请求。

字段	含义
ip	该字段中的“ip”为固定值。
protocol	该字段取值必须为： “tcp”：表示 ACL 应用于使用 TCP 协议的 VPN 流量。 “udp”：表示 ACL 应用于使用 UDP 协议的 VPN 流量。 “icmp”：表示 ACL 应用于使用 ICMP 协议的 VPN 流量。 “*”：表示 ACL 应用于使用任何协议的 VPN 流量，如 TCP、UDP、ICMP 和其它基于 IP 的流量。
host_ip	该字段指定 ACL 所应用的主机或网络的 IP 地址，取值必须为 IPv4 地址。
netmask	该字段指定 ACL 所应用的主机或网络的掩码，取值可以为点分 IP 或是一个整数，如果取值为整数，必须范围为 0 至 32。如果没有指定该字段，默认使用“255.255.255.255”。
port	该字段 ACL 所应用的端口，取值可以为一个端口值或一个端口段，如 60-70。如果不指定该字段，ACL 将应用于所有端口。
virtual_site_id	该字段指定该 ACL 关联的虚拟站点名称。取值“ALL”表示该 ACL 关联所有的虚拟站点。
PERMIT|DENY	该字段指定是否允许或拒绝发送至指定主机或网络的 VPN 报文。

动态 ACL

动态 ACL 功能允许 AG 设备接收由客户端生成的动态 ACL。当有请求访问一个虚拟站点时，AG 设备首先使用外部 ACL 进行匹配。如果请求没有匹配任何外部 ACL，系统会使用配置在设备上的 ACL。如果请求仍然没有匹配配置在设备上的 ACL，系统会使用动态 ACL 进行匹配。

匹配的动态 ACL 将会一直生效至会话结束。当用户登出虚拟站点后，会话中的动态 ACL 将会被清除。

该功能默认为禁用，表示 AG 设备不会将请求与动态 ACL 进行匹配。

配置示例

配置 ACL 规则

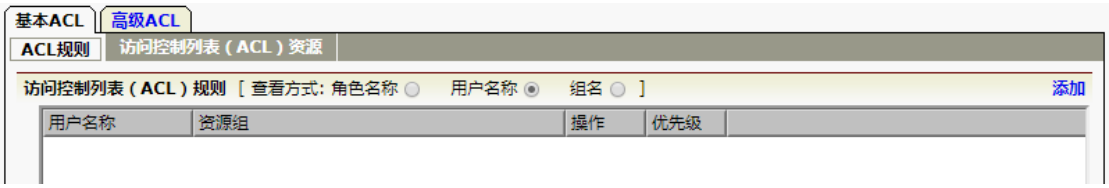
为角色添加 ACL 规则

在虚拟站点模式下。选择用户策略>访问控制列表>基本 ACL>ACL 规则，在访问控制列表（ACL）规则区域点击添加来添加一条 ACL 规则。

在显示的添加访问控制列表（ACL）规则窗口，在 ACL 对象中选择角色名称单选按钮，在角色名称下拉菜单中选择角色名称，在操作选项中选择允许或拒绝，再指定优先级数值。要定义一个新的资源组，请指定参数资源组、描述、资源类型、资源列表，再点击保存按钮。

为用户添加 ACL 规则

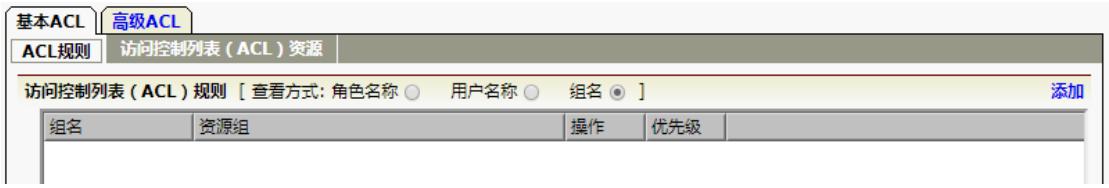
在虚拟站点模式下。选择用户策略>访问控制列表>基本 ACL>ACL 规则，在访问控制列表（ACL）规则区域点击添加来添加一条 ACL 规则。



在显示的添加访问控制列表（ACL）规则窗口，在 ACL 对象中选择用户名称单选按钮，指定参数用户名称，在操作选项中选择允许或拒绝，再参数优先级。要定义一个新的资源组，指定参数资源组、描述、资源类型、资源列表，再点击保存按钮。

为用户组添加 ACL 规则

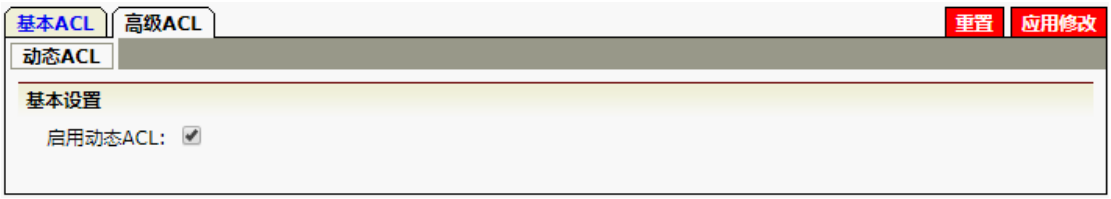
在虚拟站点模式下。选择用户策略>访问控制列表>基本 ACL>ACL 规则，在访问控制列表（ACL）规则区域点击添加来添加一条 ACL 规则。



在显示的添加访问控制列表（ACL）规则窗口，在 ACL 对象中选择组名单选按钮，指定组名参数，在操作选项中选择允许或拒绝，再指定参数优先级。要定义一个新的资源组，指定参数资源组、描述、资源类型、资源列表，再点击保存按钮。

启用动态 ACL

在虚拟站点模式下。选择用户策略>访问控制列表>高级 ACL>动态 ACL，在基本设置区域勾选启用动态 ACL，并点击应用修改按钮。



3.1.17 Kerberos 认证 SSO

Kerberos 认证需要用户从密钥分发中心（Key Distribution Center，KDC）获取服务票证来访问 Web 应用。Kerberos 认证系统包括以下部分：

密钥分发中心（KDC）：KDC 是一台已取得客户端和服务器信任的，用于分发 Kerberos 认证票证的第三方服务器。它由认证服务器(Authentication Server，AS）和票证发放服务（Ticket Granting Service，TGS）两部分组成。

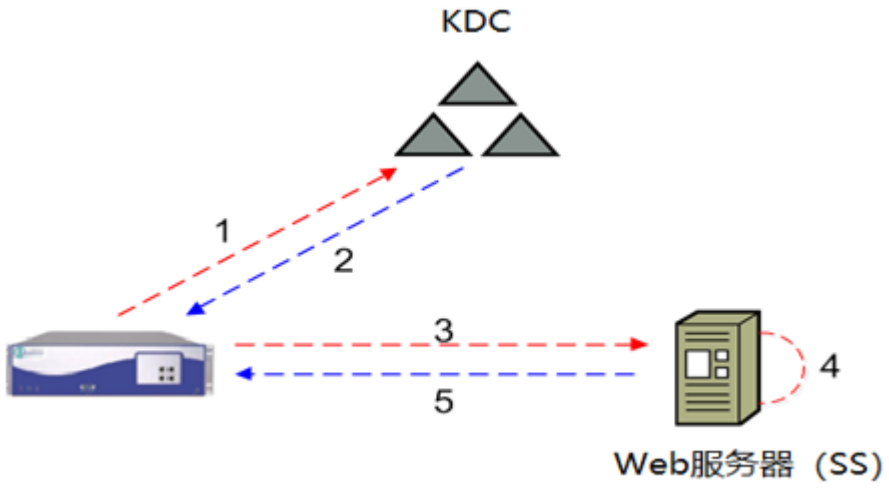
提供服务的服务器（SS）：SS 是一台客户要访问的 Web 服务器。

域：域是指一个由域控制器（DC）管理的网络，域控制器和同域中的主机共享相同的服务数据目录。Web 服务器和 KDC 必须在同一个域中。

Kerberos 单点认证

当 AG 设备收到来自后台 Web 服务器的 HTTP 401 响应报文并请求 Kerberos

认证时，Kerberos 单点认证操作将被触发，AG 将代替最终用户启动 Kerberos 认证流程。



如上图所示，Kerberos SSO 流程如下：

AG 发送票证请求消息给 KDC。

KDC 回复包含“客户-服务器”票证的消息。

AG 向 Web 服务器发送包含“客户-服务器”票证的 HTTP 请求。

Web 服务器对票证进行验证。

Web 服务器回复 HTTP 响应给 AG，AG 再将该相应转发给最终用户。

关于 Kerberos 认证流程的详细信息，请参考 Kerberos 相关的 RFC 协议文档。

3.1.18 NTLM 认证 SSO

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

当 AG 设备收到来自后台 Web 服务器的 HTTP 401 响应报文并请求 NTLM 认证时，AG 将代替最终用户发送 challenge 报文给后台 Web 服务器，验证通过后用户将不再需要单独向后台 Web 服务器发送 challenge 报文来验证身份。

3.1.19 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 AG 设备收到来自后台 Web 服务器的 HTTP 401 响应报文并请求 HTTP 基本认证时，AG 使用缓存的门户登录凭证并将头部包含 Basic 标识和 base64 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。

3.1.20 SSO Post

对于使用其它认证方式并返回 HTTP 302 重定向报文给 AG 设备的 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。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，AG 将会基于 HTTP 格式构建 post 请求报文来执行 SSO 操作。

此外，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

前端 SSO post

前端 SSO post 在 Web 应用的 SSO 功能被禁用的情况下依旧可以工作；后端 SSO 只有在 Web 应用的 SSO 功能启用的情况下才能正常工作。

后端 SSO post

后端 SSO post 允许 AG 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。

前端 SSO Post

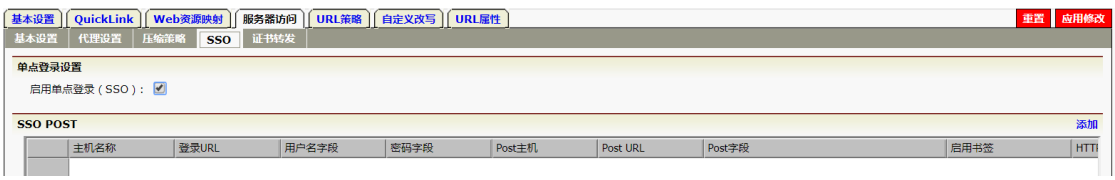
当客户访问 Web 资源（WRM 或 QuickLink）且管理员已从门户为这些资源启用了前端 SSO post 时，AG 会将包含 HTTP 表单和（由 AG 生成的）JavaScript 代码的 HTTP 响应报文返回给客户端。前端 SSO post 允许客户端执行 JavaScript 代码并自动构建和发送基于 HTTP 表单创建的 post 请求。

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。

配置示例

启用 SSO 功能

为 Web 应用启用 SSO 功能，请进入虚拟站点模式，选择访问方法>Web 访问>服务器访问>SSO，在单点登录设置区域勾选启用单点登录（SSO），然后点击保存配置。



Kerberos 认证 SSO

添加域

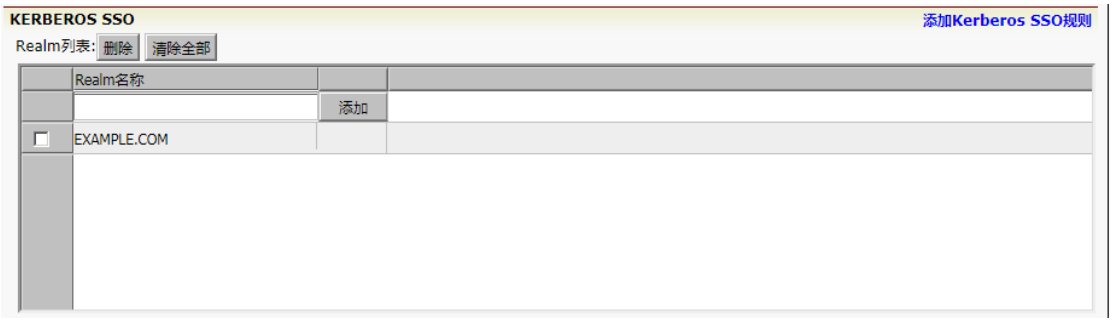
在 Kerberos SSO 区域，输入域名称，点击添加操作链接。

为域添加 KDC

双击已添加的域，在 KDC 列表中指定主机名/IP 地址和端口，然后点击添加操作链接。

添加 Kerberos SSO 规则

在 Kerberos SSO 区域，点击添加 Kerberos SSO 规则。



在添加 Kerberos SSO 规则区域，输入主机名称和 Realm 名称，然后点击保存。

后端 SSO Post

要配置后端 SSO post，请先启用 SSO 功能，再添加一个 SSO post 规则。

要添加 SSO post 规则，选择访问方法>Web 访问>服务器访问>SSO，在 SSO Post 区域点击添加。

在添加 SSO Post 编辑窗口，按需指定参数，然后点击保存操作链接。

前端 SSO Post

要配置前端 SSO post，请先添加一个 SSO Post 规则，然后为指定资源启用前端 SSO post。

为 WRM 资源启用前端 SSO Post

在虚拟站点模式下，选择用户策略>角色>角色资源>Web，在 WRM 资源区域点击添加，然后在添加 WRM 资源区域勾选启用前端 SSO。

为 DirectLink 资源启用前端 SSO Post

在虚拟站点模式下，选择用户策略>角色>角色资源>Web，在 WRM 资源区域点击添加，然后在添加 WRM 资源区域勾选直接链接和启用前端 SSO。

为 QuickLink 资源启用前端 SSO Post

在虚拟站点模式下，选择用户策略>角色>角色资源>Web，在 QuickLink 资源区域点击添加，然后在添加 QuickLink 资源区域勾选启用前端 SSO。

3.2 端到端链路加密

支持用户终端到网关的端到端通信链路加密。产品采用 TLCP 国家标准协议（即国密 SSL 协议），提供基于 SM2、SM3、SM4 商用密码算法实现的通信加密能力，并提供国际密码算法 ECC、RSA、AES、3DES 等，充分保障数据传输过程中的机密性和完整性。

为了释放服务器的解密能力，节省对硬件资源的消耗，AG 对内实现 SSL 卸载功能，业务服务可以不用修改也能满足外网安全需要，以零改造的方式减轻服务加解密资源压力。

3.3 细粒度访问控制

多样化权限设计，可以为不同的用户或者用户组定制不同安全策略和使用权限。提供基于角色/用户/组的权限策略引擎，对用户的 Web、文件、网络和应用接入权限进行控制。

3.4 安全的应用发布

根据不同的用户业务场景需求，支持通过 7 层、4 层和 3 层的技术发布企业服务，仅允许授权用户可见及访问。

- 7 层方案满足所有 B/S 架构的服务应用发布需求；
- 4 层方案满足远程桌面等应用的发布以及 C/S、B/S 应用的加速访问；
- 3 层方案可以满足所有基于 TCP/UDP/ICMP 协议的应用安全访问。

3.5 灵活的部署方式

根据不同用户场景需求，AG 安全接入网关同时支持串行部署（业务流量经过网关）和旁路部署，最大化业务应用场景。用户可根据自身网络环境，实现影响最小，帮助最大的放置方式。

3.6 多样化接入模式

- **在定制化虚拟门户上接入**

安全接入网关内置一个可定制化的应用发布虚拟站点门户，用户登录门户系统后可以查看当前有权限访问的应用列表，通过点击相应的应用名称就可以打开业务系统。这种访问流程为：

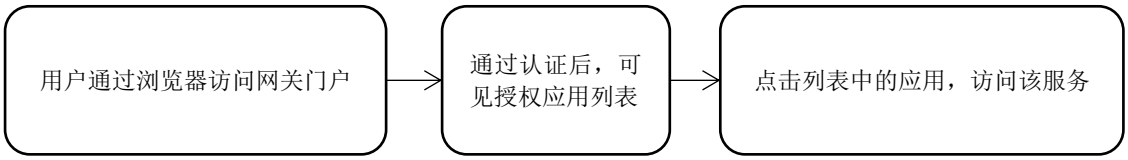


图 2

- **在用户现有业务门户上接入**

用户业务系统中已有集中的应用门户，且不希望应用安全接入网关后改变原有的用户访问习惯，这是较大型用户场景中经常会遇到的情况。支持“网关地址+应用标识”的发布方式，可以按此格式将应用地址发布到用户门户中去，不改变原有的用户访问方式和使用习惯。流程如下：

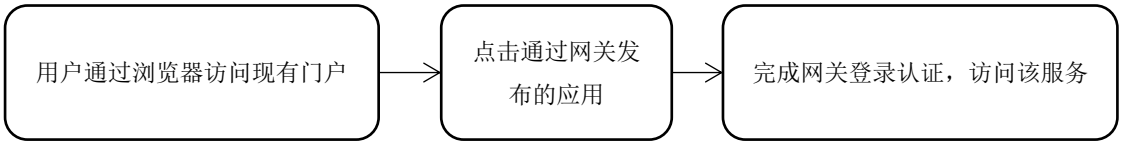


图 3

- **通过 iSecSP 客户端接入**

用户使用 iSecSP 客户端登录网关虚拟站点后，客户端呈现该用户被权限访问的应用列表，通过点击相应的应用名称就可以访问对应业务应用系统。

3.7 强大的单点登录

网关系统支持用户只需要通过一次强身份认证，就可以免登录访问授权范围内的所有系统应用，帮助企业打通各个业务系统之间的身份信息孤岛，提高了登录的流程效率；同时对用户账户的生命周期统一管理，极大降低运营维护成本，使整体系统兼具安全性与易用性，大幅提升用户体验。

- 通过支持 SAML2.0、OAuth 等通用认证授权协议框架的支持，无缝对接微信、企业微信、Azure 等身份认证系统；
- 通过集成 CNG-SSO，大幅提升 windows 平台非 Web 应用的单点登录解决方案能力。

3.8 完善的监控审计

在业务监控方面，可以完整地记录用户的认证和业务访问过程，并可按日期、用户、应用、IP 等信息对日志进行查询。支持将标准化格式日志信息发送到日志服务器，供审计监控平台进行用户行为建模，对用户访问行为进行监控，回溯。

在系统硬件资源使用率的实时监控方面，可通过图形界面方式动态实时监测系统 CPU 资源、存储空间、系统内存的使用情况以及各网络接口的网络流量监测，形成简捷的集中式、自动化管理系统。

3.9 连续性应急管理

信安世纪业务连续性应急许可（contingency licenses）帮助企业在不中断服务的同时，应对类似疫情期间并发用户突增的远程接入扩容需求。

3.10 领先的性能保障

- 采用自建协议栈，提升系统处理速率，保障系统安全性；
- 产品做到了业内领先的大吞吐量和高并发，满足海量用户的客户需求；
- 引入的高可用性（High Availability，HA）功能模块，允许两台或者多台设备持续同步各自的状态和配置信息，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。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。

4. 典型场景

4.1 主路模式访问：iSecSP 发布应用资源

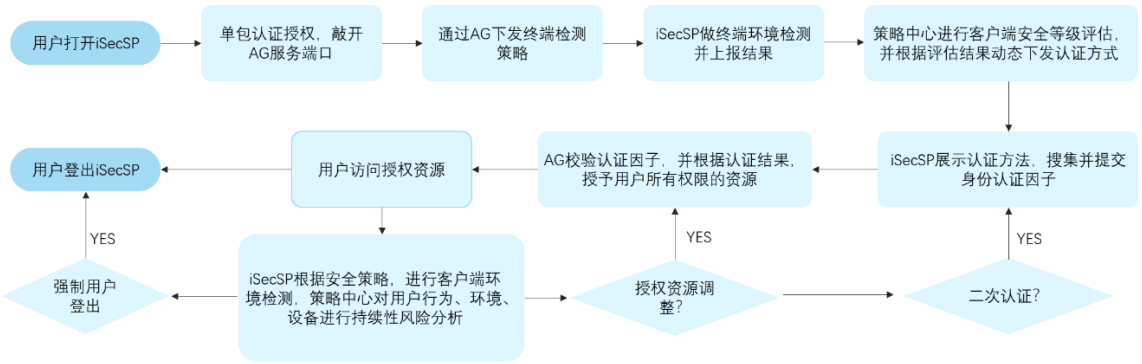


图 4

1. 用户打开 iSecSP，进行单包敲门。
2. 通过单包认证，完成对访问终端的认证和授权，AG 网关允许该终端的后续访问。
3. 策略中心通过 AG 网关下发终端安全检测的策略到 iSecSP。
4. iSecSP 执行各项终端安全检测，并通过 AG 网关上报各项检测结果到安全策略中心。
5. 策略中心通过对 iSecSP 上报的安全扫描结果，综合该账号的历史访问记录评估，根据评估的安全等级给出不同安全等级对应的认证方法。
6. iSecSP 展示此次访问需要的认证方法：用户名/密码，证书，多因素身份认证等，并搜集和提交用户的认证因子。
7. AG 根据用户提交的认证因子，认证用户身份并授权此次认证结果的可访问应用资源。
8. 用户访问授权的应用资源。
   - 8.1 用户访问授权应用资源期间，iSecSP 持续进行终端安全环境检测并上报检测结果。
   - 8.2 安全策略中心通过 AG 网关持续对用户的访问行为进行监控分析。
   - 8.3 综合以上安全评估结果，对用户访问行为进行干预。
9. 用户登出，结束此次访问。

4.2 主路模式访问：浏览器门户发布应用资源

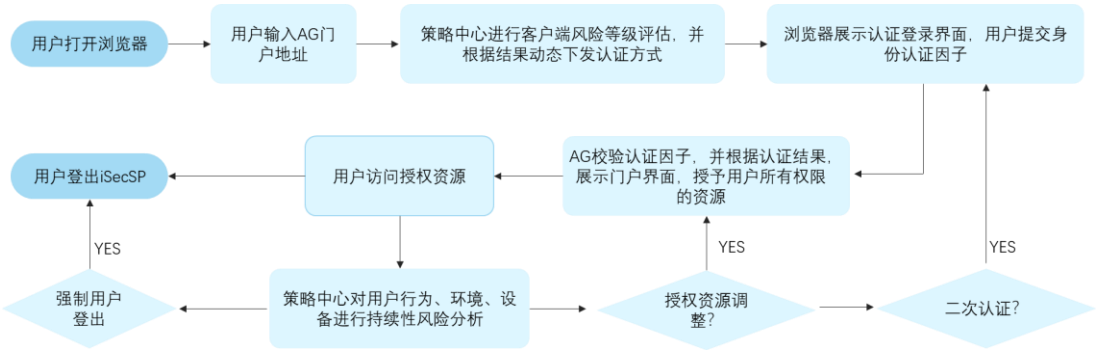


图 5

1. 用户打开浏览器，访问 AG 网关地址。
2. 策略中心根据评估的安全等级给出不同安全等级对应的认证方法。
3. 通过 AG 网关下发登录认证页面。
4. 浏览器展示此次访问需要的认证方法：用户名/密码，证书，多因素身份认证等，并搜集和提交用户的认证因子。
5. AG 根据用户提交的认证因子，认证用户身份并授权此次认证结果的可访问应用资源。
6. 用户访问授权的应用资源。
   6.1 策略中心通过 AG 网关持续对用户的访问行为进行监控分析。
   6.2 综合以上安全评估结果，对用户访问行为进行干预。
7. 用户登出，结束此次访问。

4.3 旁路模式访问

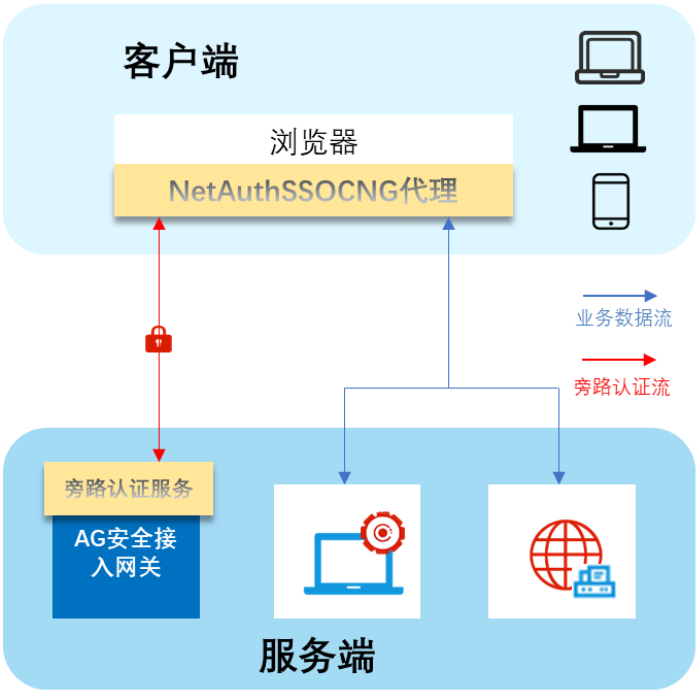


图 6

访问流程如下：

1. 用户启动客户端浏览器，访问应用系统；
2. NetAuthCNGSSO 截获请求，连接网关检查用户是否已经认证，如果未认证，走认证流程；
3. NetAuthCNGSSO 请求网关生成随机数；
4. NetAuthCNGSSO 通过证书签名服务对随机数进行签名；
5. NetAuthCNGSSO 将签名结果送往安全接入网关；
6. 安全接入网关验证该签名，并根据验证结果给出认证确认；
7. 当认证网关返回认证成功后，NetAuthCNGSSO 放行该应用系统访问；
8. 用户正常访问应用系统。

4.4 旁路模式访问（SAML IDP）

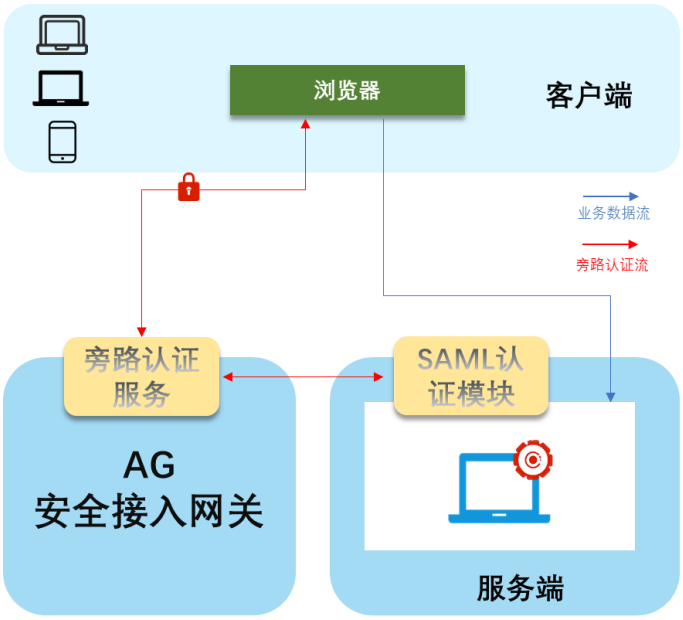


图 7

访问流程如下：

1. 用户启动客户端浏览器，访问应用系统；
2. 应用系统的 SAML 认证模块截获请求，连接安全接入网关检查用户是否已经认证，如果未认证，浏览器通过 SAML 协议将请求重定向到安全接入网关；
3. 安全接入网关根据配置规则走认证流程，如证书认证，扫码，指纹，多因素认证；
4. 认证成功后，携带认证 token，重定向到应用业务系统；
5. 服务端 SAML 认证模块校验 token，放行应用访问。

4.5 IPSec & SSL VPN 综合应用场景

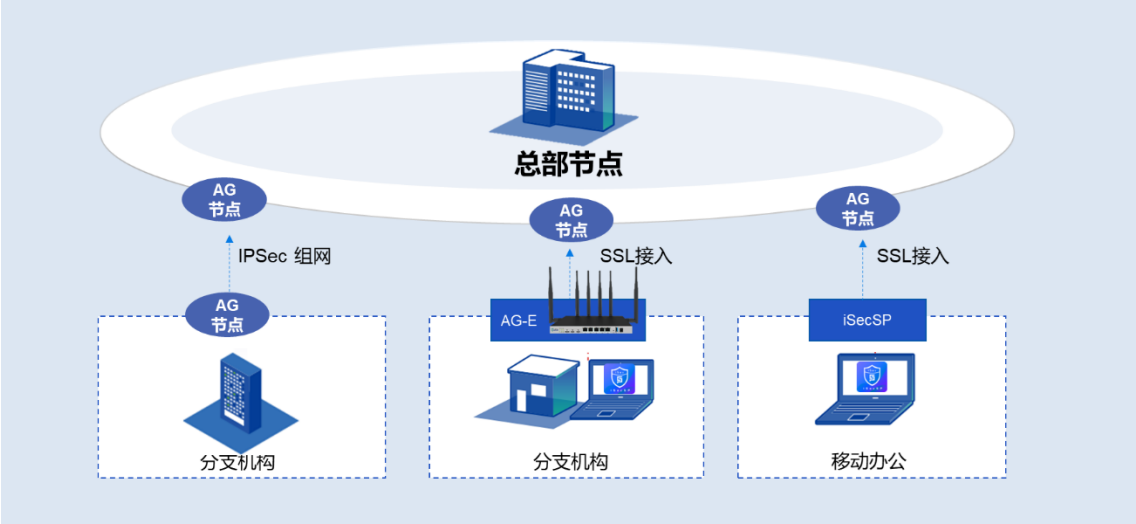


图 8

场景描述如下：

在总部、大型分支机构部署 AG 安全接入网关，在小型分支机构、办事处部署 AG 边缘安全网关，远程接入办公用户在移动设备上安装 iSecSP。在此场景下，既满足 IPSec VPN 组网，又满足 SSL VPN 接入办公，形成 VPN 综合安全应用场景。

1. 总部、大型分支机构之间通过 AG 创建 IPSec 国密 VPN 隧道，形成一张大的局域网，实现内网互通，内部办公人员可授权访问总部业务资源。
2. 小型分支机构、办事处通过 AG 与总部 AG 节点创建 SSL 国密隧道，内部办公人员可通过 WIFI、有线接入总部网络。
3. 远程移动办公人员可通过 iSecSP 接入就近的 AG 节点，访问内部办公资源。

5. 部署方式

5.1 单臂部署模式

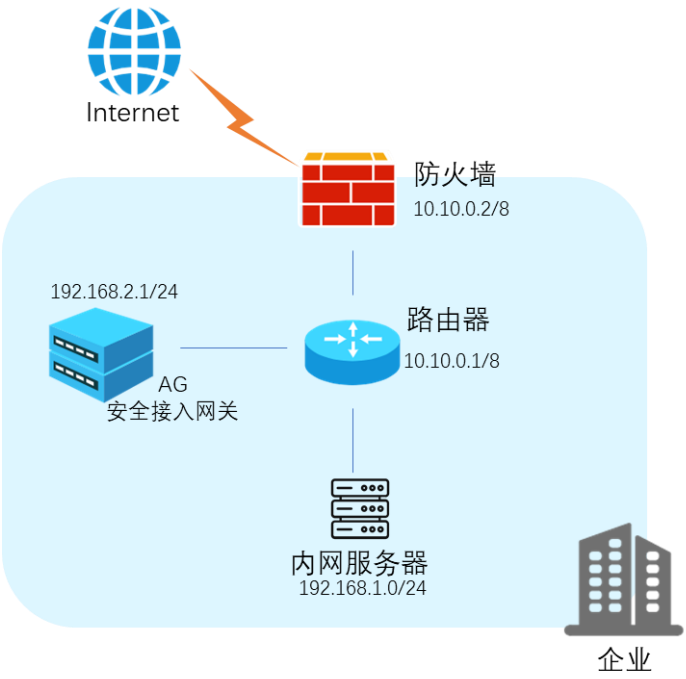


图 9

单臂部署仅使用了 AG 上的一个接口。在使用部署方式时，加密和未加密的流量通过同一个网络传输。因此，强烈建议将 AG 设备部署在防火墙后方。

5.2 双臂部署模式

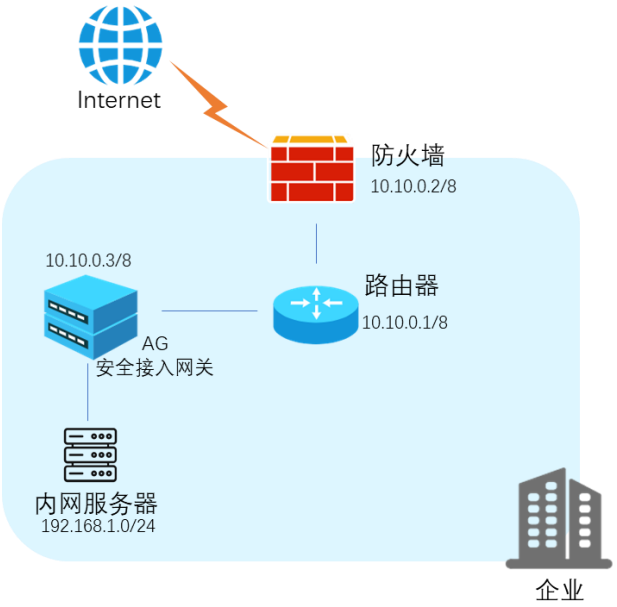


图 10

双臂部署使用 AG 设备的两个接口来分别处理所有入站和出站的流量。在该场景中，一个接口连接到 Internet（或其他一些出站设备，例如网关路由器、防火墙等），另一个接口连接到安全的内部网络。这是 AG 设备最常见的网络部署。

6. 产品规格

表 4 产品规格

产品型号	AG-1000 系列	AG-1200C-DA 系列 （海光 CPU、银河麒麟操作系统）
设备形态	1U	2U
加密吞吐（国密）	≥3Gbps	≥5Gbps
加密吞吐（国际）	≥20Gbps	≥15Gbps
并发用户数	128000	128000
网络端口	4 个千兆电口、4 个万兆光口，默认配备多模光纤模块	6 个千兆电口、4 个千兆光口、4 个万兆光口
电源	双电源	双电源
最大功率	400-600W	350W

7. 产品资质

- 商用密码产品认证证书
- 计算机信息系统安全专用产品销售许可证
- 计算机软件著作权登记证书
- 信息技术产品安全测试证书
- IPv6 Ready Logo 认证证书
- 海光 CPU 生态兼容认证证书
- 麒麟软件兼容性认证证书
- 龙芯中科产品兼容互认证书
- ……

8. 客户案例

- 中国移动集团
- 中国联合网络通信有限公司
- 浙江移动
- 上海移动
- 交通银行股份有限公司
- 平安银行股份有限公司
- 国信证券股份有限公司
- 齐鲁证券有限公司
- 安邦保险集团股份有限公司
- 中国太平保险集团有限责任公司
- 中国石油化工集团公司
- 中国石油化工股份有限公司北京化工研究院
- 神华国华（北京）电力研究院有限公司
- 国家电网公司客户服务中心
- 深圳烟草工业有限责任公司
- 国家食品药品监督管理局
- 华为技术有限公司
- 长城汽车股份有限公司
- 北汽集团
- 广汽集团
- 郑州宇通客车股份有限公司
- 奇瑞汽车股份有限公司
- 宝钢集团
- 新奥燃气集团
- 德邦物流
- 顺丰速运有限公司
- 苏宁电器集团

- 中国免税品（集团）有限责任公司
- 青岛双星轮胎工业有限公司
- 中粮置地管理有限公司
- 金地（集团）股份有限公司
- 鞍钢集团
- 徐州工程机械集团有限公司
- ……