HCIE-Security 备考指南

用户和认证

HCIE 只是一个开始….

HCIE 仅是一个证书…懂得做人和处事比证书和技能更重要…

希望大家顺利通过 HCIE，取得更好的职业发展！

目 录

HCIE-Security 用户和认证需要掌握的知识点

- 列举防火墙支持的用户类别和认证方法
- 描述防火墙上用户认证的流程
- 描述防火墙上用户单点登陆的原理
- 配置防火墙上网用户本地认证
- 配置防火墙上网用户单点登陆

用户与认证简介

介绍用户与认证的定义和目的。

用户

用户指的是访问网络资源的主体，表示“谁”在进行访问，是网络访问行为的重要标识。NGFW 上的用户包括上网用户和接入用户两种形式：

- 上网用户

  内部网络中访问网络资源的主体，如企业总部的内部员工。上网用户可以直接通过 NGFW 访问网络资源。

- 接入用户

  外部网络中访问网络资源的主体，如企业的分支机构员工和出差员工。接入用户需要先通过 SSL VPN、L2TP VPN、IPSec VPN 或 PPPoE 方式接入到 NGFW，然后才能访问企业总部的网络资源。

认证

NGFW 通过认证来验证访问者的身份，NGFW 对访问者进行认证的方式包括：

- 本地认证

  访问者将标识其身份的用户名和密码发送给 NGFW，NGFW 上存储了密码，验证过程在 NGFW 上进行，该方式称为本地认证。

- 服务器认证

访问者将标识其身份的用户名和密码发送给 NGFW，NGFW 上没有存储密码，NGFW 将用户名和密码发送至第三方认证服务器，验证过程在认证服务器上进行，该方式称为服务器认证。

- 单点登录

  访问者将标识其身份的用户名和密码发送给第三方认证服务器，认证通过后，第三方认证服务器将访问者的身份信息发送给 NGFW。NGFW 记录访问者的身份信息，该方式称为单点登录（Single Sign-On）。

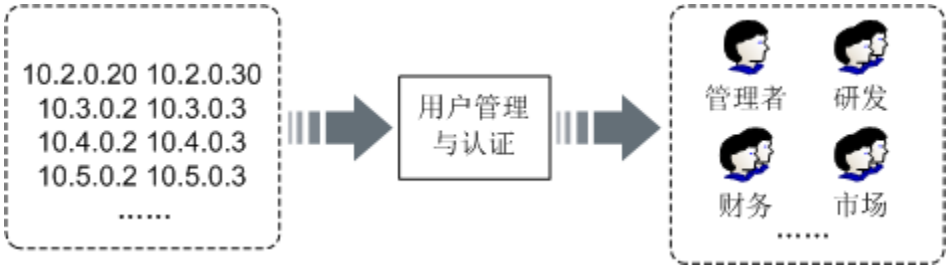
对于上网用户，访问网络资源时 NGFW 会对其进行认证。对于接入用户，接入 NGFW 时 NGFW 会对其进行认证；访问网络资源时，NGFW 还可以根据需要来对其进行二次认证。

目的

如图 1 所示，在 NGFW 上部署用户管理与认证，将网络流量的 IP 地址识别为用户，为网络行为控制和网络权限分配提供了基于用户的管理维度，实现精细化的管理：

- 基于用户进行策略的可视化制定，提高策略的易用性。
- 基于用户进行威胁、流量的报表查看和统计分析，实现对用户网络访问行为的追踪审计。
- 解决了 IP 地址动态变化带来的策略控制问题，即以不变的用户应对变化的 IP 地址。

图 1 将 IP 地址识别为用户



用户/组

用户是网络访问的主体，是 NGFW 进行网络行为控制和网络权限分配的基本单元。

用户属性

用户的主要属性及其说明如表 1 所示。

表 1 用户属性	
属性	**说明**
登录名	用户的账号，即用户进行认证时使用的名称。
显示名	用户在 NGFW 上显示的名称，仅作为区分用户的标识。 通常情况下，在日志、报表的用户字段中，用户会以“登录名（显示名）”的格式出现。
描述	用户的描述信息，便于管理员对该用户进行识别和维护。
所属组	用户所在的父组，一个用户最多可以属于三个父组。
密码	用户的密码。 使用本地认证时，必须在 NGFW 上配置用户的密码；使用服务器认证时，用户的密码在第三方认证服务器上配置，无需在 NGFW 上配置。
账号过期时间	账号的有效期，过期之后该账号无法使用。
允许多人同时使用该账号登录	是否允许多人同时使用该用户的登录名登录，即允许该登录名同时在多台计算机上登录。
IP/MAC 绑定	将用户与 IP/MAC 绑定，限制该用户只能在特定的 IP/MAC 地址上登录。

树形组织结构

用户按树形结构组织，用户隶属于组（部门）。管理员可以根据企业的组织结构来创建部门和用户。这种方式易于管理员查询、定位，是常用的用户组织方式。

树形组织结构如图 1 所示，树形组织结构的顶级节点是“认证域”，也可以看作是根组，认证域下级可以是用户组、用户。

default 认证域是设备缺省存在的认证域，相当于/default 根组。通常情况下，在缺省的 default 认证域下规划组织结构即可，如果有不同用户使用不同认证方式、与服务器上域名对应等需求时才需要规划新的认证域。

如果有规划新的认证域需求，NGFW 提供如下两种方式规划用户组织结构：

- **每个认证域拥有独立的用户帐号**

  每个认证域是一个独立的树形组织结构，类似于 AD/LDAP 等认证服务器上的域结构。各认证域的用户账号独立，不同认证域的账号允许重名。

- **所有认证域共享 default 认证域的用户帐号**

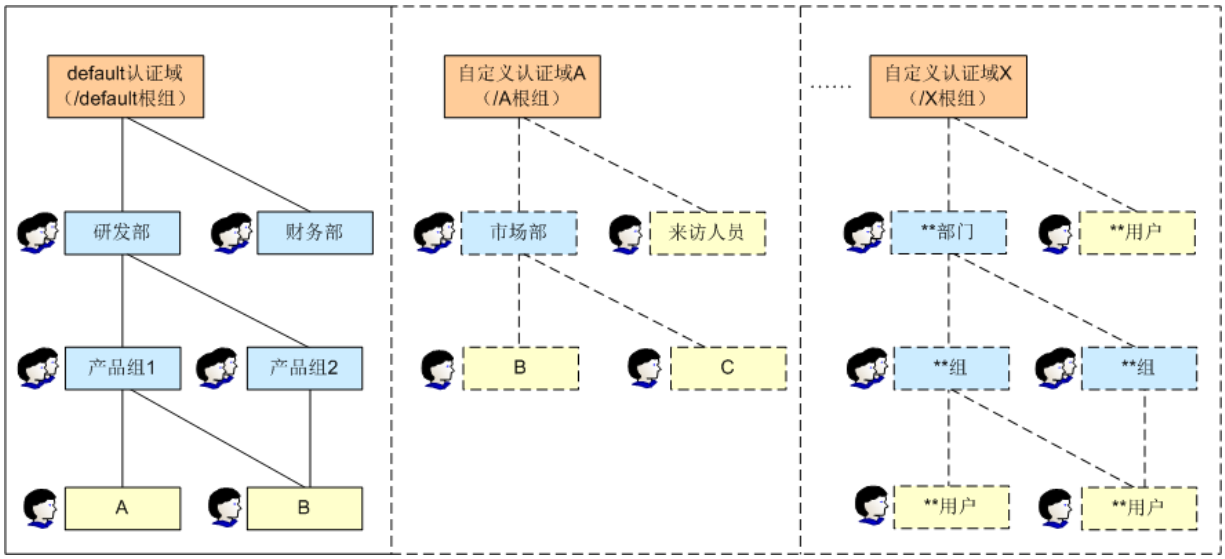
只有 default 认证域一个树形组织结构，其他认证域与 default 认证域共享账号。此时新建认证域的作用在于决定哪些用户使用哪种认证方式，不作为用户组织结构的顶级节点。

说明：

建议按第一种方式规划用户组织结构，与服务器组织结构对应。第二种方式主要用于，同一个用户账号有使用不同认证方式或认证服务器需求的特殊情况。选择哪种部署方式由认证域下的配置决定。

。用户属于哪个认证域是由用户登录时用户名中携带的“@”后的字符串来决定的，如“user1@bj”属于“bj”认证域，“user2”属于 default 认证域。如果用户名中没有携带“@”，则属于缺省的 default 认证域。

图 1 用户/组的树形组织结构示意图



规划树形组织结构时必须遵循如下规定：

- default 认证域是设备默认自带的认证域，不能被删除，且名称不能被修改。
- 设备最多支持 20 层用户结构，包括认证域和用户，即认证域和用户之间最多允许存在 18 层组。
- 每个组可以包括多个用户和组，但每个组只能属于一个父组。
- 一个用户最多可以属于三个父组。
- 组名允许重名，但所在组织结构的全路径必须确保唯一性。
- 用户和组都可以被策略所引用，如果组被策略引用，则组下的用户继承其父组和所有上级节点的策略。

用户/组的来源

在 NGFW 上创建用户和组时，可以使用以下方式：

说明：

对用户进行权限控制需要在策略中引用用户或用户组，因此即使采用服务器认证方式的用户也需要在 NGFW 存在对应的用户组或用户，至少要存在用户组。

- 手动创建

  管理员手动创建用户和组，并配置用户属性。例如，管理员可根据企业的组织架构创建组，然后在各组下创建用户信息。

  如果没有部署第三方认证服务器或者部署的第三方认证服务器不支持向 NGFW 导入用户信息的功能，请使用该方式来创建用户。

- 从 CSV 文件导入

  将用户信息按照指定格式写入 CSV 文件中，再将 CSV 文件导入到 NGFW 中，或者将之前从 NGFW 上导出的 CSV 文件再次导入，批量创建用户和组。

  如果没有部署第三方认证服务器或者部署的第三方认证服务器不支持向 NGFW 导入用户信息的功能，请使用该方式来创建用户。与手动创建方式相比，可以简化配置。

- 从服务器导入

  如果实际环境中已经部署了身份验证机制，并且用户信息都存放在第三方认证服务器上，则可以通过执行服务器导入策略，将第三方认证服务器上用户和组的信息导入到 NGFW 上。

  目前 NGFW 只支持从 AD、LDAP 和 TSM 服务器导入用户和组。对于其他服务器，请使用手动创建、CSV 文件导入或设备自动发现并创建的方式。

- 设备自动发现并创建

  NGFW 可以自动发现新用户并将新用户添加到指定的组中，后续管理员可以调整其所属组。新用户指的是通过了认证但是在 NGFW 上不存在的用户，例如在第三方认证服务器上新创建了用户信息，但没有导入到 NGFW 中，用户可以通过认证但 NGFW 上并没有存储该用户的信息。

在线用户

用户访问网络资源前，首先需要经过 NGFW 的认证，目的是识别这个用户当前在使用哪个 IP 地址。对于通过认证的用户，NGFW 还会检查用户的属性（用户状态、账号过期时间、IP/MAC 地址绑定、是否允许多人同时使用该账号登录），只有认证和用户属性检查都通过的用户，该用户才能上线，称为在线用户。

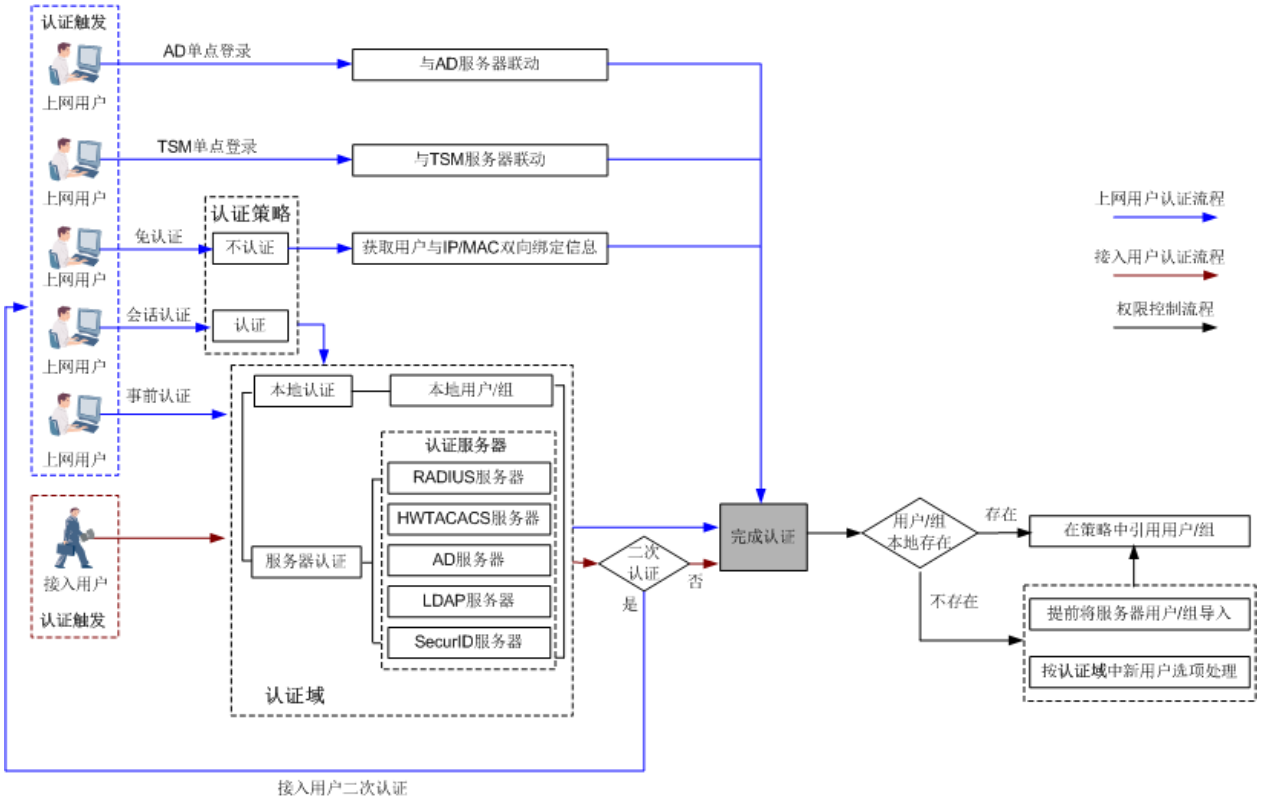
NGFW 上的在线用户表记录了用户和该用户当前所使用的地址的对应关系，对用户实施策略，也就是对该用户对应的 IP 地址实施策略。

用户认证总体流程

了解整体的认证流程，有助于后续配置。

NGFW 上的认证过程由多个环节组成，各个环节的处理存在先后顺序。根据不同的部署方式和网络环境，NGFW 提供了多种用户认证方案供管理员选择，如图 1 所示。

图 1 认证流程示意图



认证触发

介绍上网用户和接入用户触发认证的方式。

上网用户触发认证的方式

上网用户触发认证的方式包括：

- **AD 单点登录**

  在 AD 环境中，访问者通常希望经过 AD 服务器的认证后，就会自动通过 NGFW 的认证，然后可以访问所有的网络资源。此种情况下，访问者可以使用 AD 单点登录的方式来触发 NGFW 上的认证。

  AD 单点登录时，NGFW 提供如下两种方式获取用户认证通过的消息：

  说明：

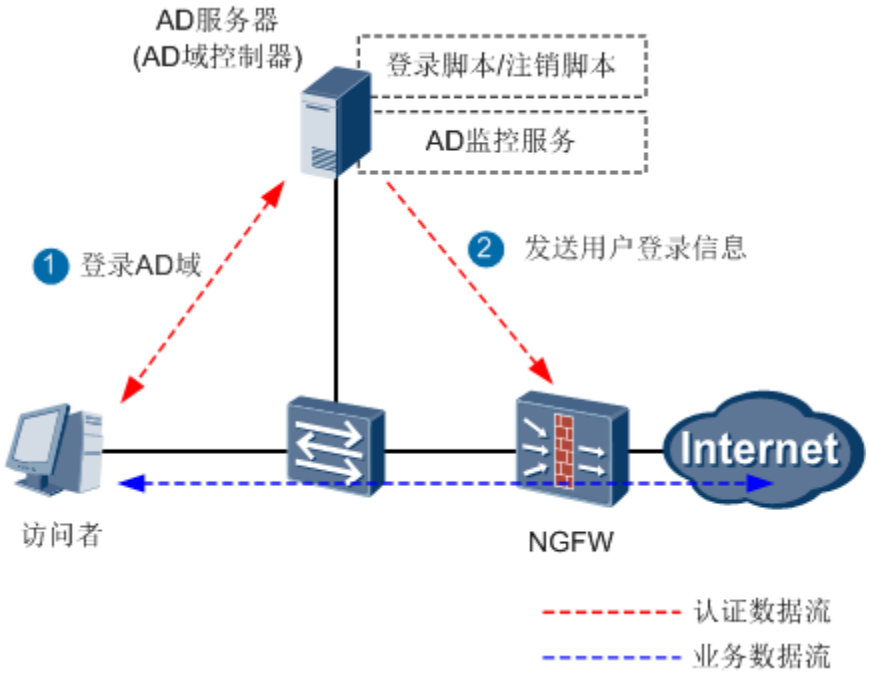
  如果 NGFW 部署在访问者和 AD 服务器之间，则需要在 NGFW 上配置认证策略时，不对访问者与 AD 服务器之间的认证报文进行认证，同时在安全策略中保证这类报文可以正常通过 NGFW。

  方式一：插件方式

  插件方式下，管理员需要在 AD 服务器（AD 域控制器）上部署 AD 单点登录服务，设置登录脚本和注销脚本，同时在 NGFW 上配置 AD 单点登录参数，接收 AD 服务器发送的用户登录/注销消息。

  如图 1 所示，以登录过程为例进行说明。访问者首先登录到 AD 域中，然后由 AD 单点登录服务将登录信息发送给 NGFW。

  图 1 AD 单点登录示意图（插件方式）



访问者注销时，AD 服务器执行 AD 服务器上的注销脚本，将注销信息发送至 AD 单点登录服务，然后由 AD 单点登录服务将注销信息发送给 NGFW，完成注销过程。

方式二：免插件方式

说明：

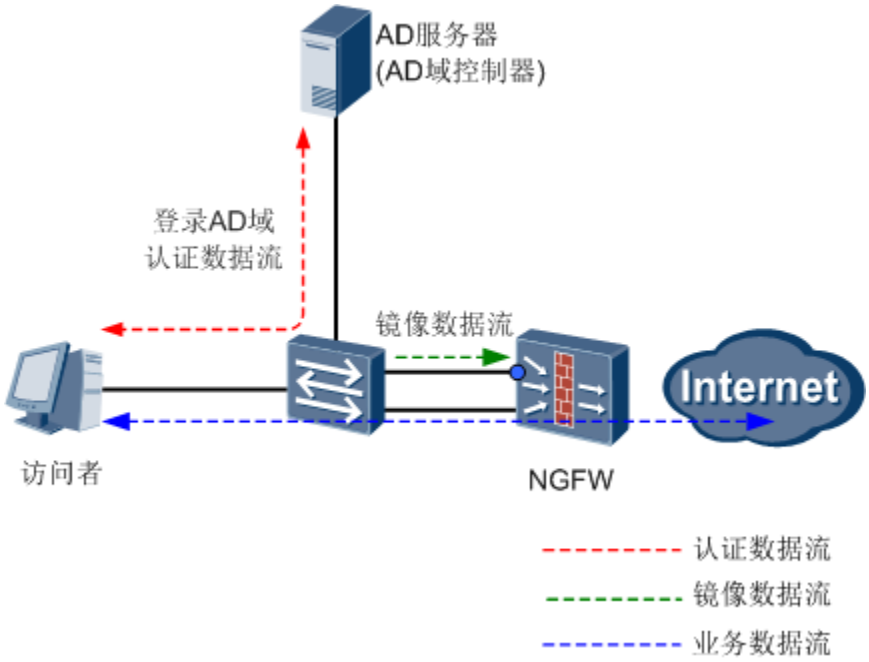
免插件方式下，NGFW 无法获取用户的注销消息，因此用户只能根据在线用户超时时间下线。

NGFW 需要使用独立的二层接口接收镜像认证报文，该接口不能与其他业务口共用。

免插件方式下，无需在 AD 服务器上安装程序。NGFW 通过监控访问者登录 AD 服务器（AD 域控制器）的认证报文获取认证结果，如果认证成功将用户和 IP 对应关系添加到在线用户表。

当 NGFW 部署在访问者和 AD 服务器之间时，NGFW 可以直接获取认证报文；如果认证报文未经过 NGFW（如图 2 所示），则需要将 AD 服务器发给访问者的认证结果报文镜像到 NGFW。

图 2 AD 单点登录示意图（免插件方式）



- **TSM 单点登录**

在 TSM 环境中，访问者通常希望经过 TSM 服务器的认证后，就会自动通过 NGFW 的认证，然后可以访问所有的网络资源。此种情况下，访问者可以使用 TSM 单点登录的方式来触发 NGFW 上的认证。

为了实现 TSM 单点登录，管理员需要在 TSM 服务器（TSM 控制器）上配置与 NGFW 的通信参数，确保 TSM 服务器可以将用户的登录信息发送至 NGFW。同时在 NGFW 上配置 TSM 服务器以及 TSM 单点登录参数，接收 TSM 控制器发送的用户登录/注销消息。

说明：

如果 NGFW 部署在访问者和 TSM 服务器之间，则需要在 NGFW 上配置认证策略时，不对访问者与 TSM 服务器之间的认证报文进行认证，同时在安全策略中保证这类报文可以正常通过 NGFW。

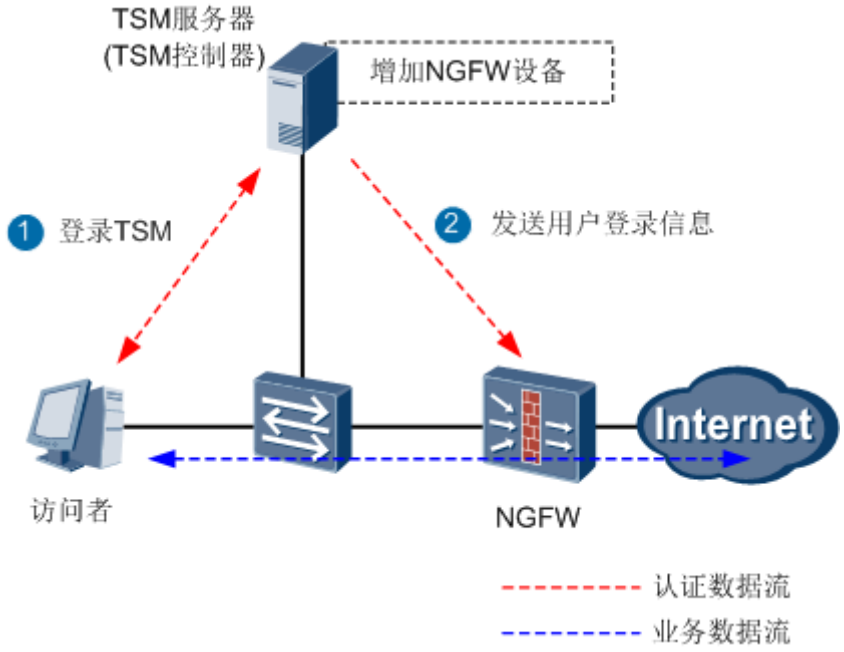
NGFW 支持与多个 TSM 服务器通信，此处以一台 TSM 服务器为例进行描述。

TSM 单点登录提供以下两种触发方式：

方式一：访问者主动触发 TSM 单点登录

如图 3 所示，以登录过程为例进行说明。访问者访问业务之前首先通过 TSM 客户端或 Portal 认证页面登录到 TSM 中，然后由 TSM 服务器将登录信息（包括访问者使用的用户名和 IP 地址）发送给 NGFW。

图 3 访问者主动触发 TSM 单点登录示意图

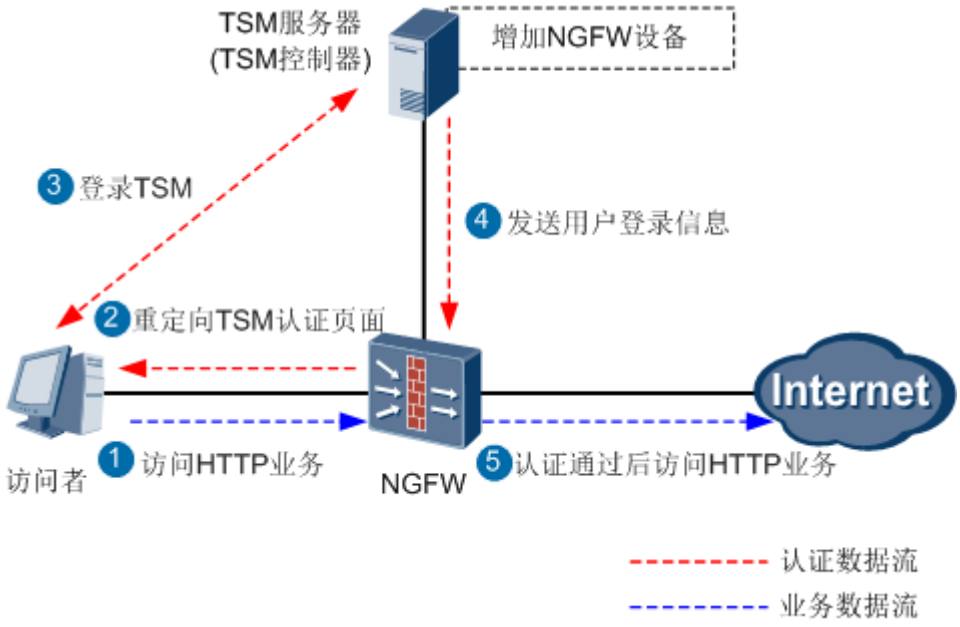


访问者注销时，TSM 服务器将注销信息发送给 NGFW，完成注销过程。

方式二：访问者访问 HTTP 业务触发 TSM 单点登录

如图 4 所示，NGFW 收到访问者的第一条目的端口为 80 的 HTTP 业务访问数据流时，将 HTTP 请求重定向到 TSM 的 Portal 认证页面，触发 TSM 对访问者进行身份认证。认证通过后，TSM 服务器将登录信息（包括访问者使用的用户名和 IP 地址）发送给 NGFW，然后访问者就可以访问 HTTP 业务以及其他业务。

图 4 HTTP 业务触发 TSM 单点登录示意图



访问者注销时，TSM 服务器将注销信息发送给 NGFW，完成注销过程。

- **免认证**

对于企业的高级管理者，他们希望可以简化操作过程，不输入用户名和密码就可以完成认证并访问网络资源，同时对安全要求又更加严格。此种情况下，这类访问者可以使用免认证的方式来触发 NGFW 上的认证。

NGFW 通过识别 IP/MAC 和用户的双向绑定关系，确定访问者的身份。进行免认证的访问者只能使用特定的 IP/MAC 地址来访问网络资源。

- **会话认证**

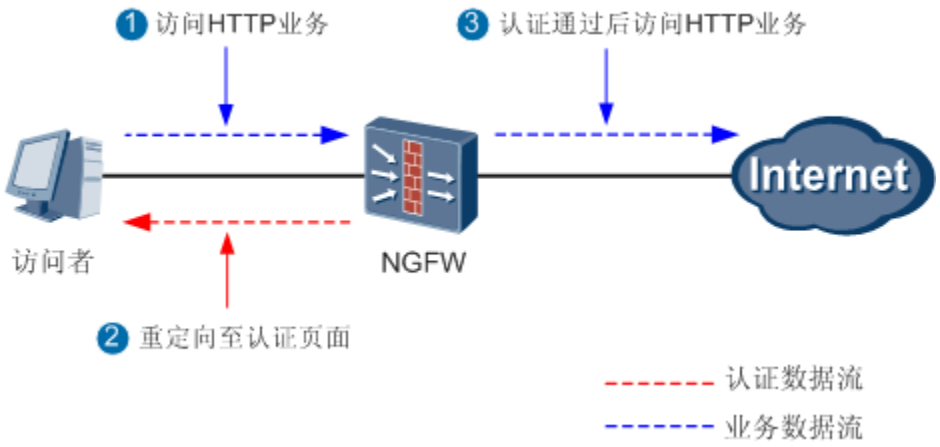
如果实际网络环境中访问者只使用单一的 HTTP 业务访问网络资源，建议使用会话认证方式来触发 NGFW 上的认证。会话认证是指访问者不主动进行身份认证，先进行 HTTP 业务访问，在访问过程中进行认证。认证通过后，再进行业务访问。目前 NGFW 只支持向目的端口为 80 的 HTTP 方式业务访问推送认证页面，其余业务报文包括通过端口映射（port-mapping）功能识别出的 HTTP 报文，均会被 NGFW 丢弃。

注意：

用户使用 URL 地址来进行 HTTP 业务访问时，首先需要与 DNS 服务器交互 DNS 业务报文来解析 URL 地址。如果用户与 DNS 服务器交互的 DNS 业务报文经过 NGFW 转发，则需要管理员在 NGFW 上配置安全策略，允许 DNS 业务报文通过。

如图 5 所示，当 NGFW 收到访问者的第一条目的端口为 80 的 HTTP 业务访问数据流时，将 HTTP 请求重定向到认证页面，触发访问者身份认证。认证通过后，就可以访问 HTTP 业务以及其他业务。

图 5 会话认证示意图

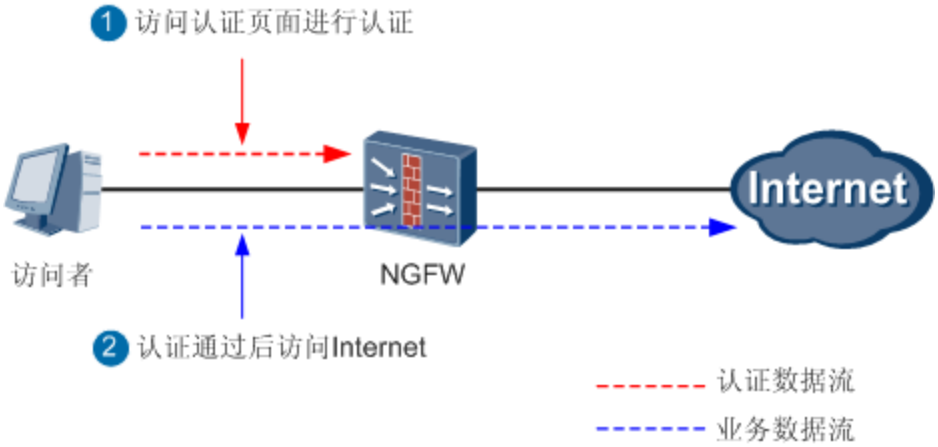


- **事前认证**

如果实际网络环境中访问者需要通过多种业务形式访问网络资源，可以使用事前认证方式来触发 NGFW 上的认证。事前认证是指访问者在访问网络资源之前，先主动进行身份认证，认证通过后，再访问网络资源。

如图 6 所示，访问者主动向 NGFW 提供的认证页面发起认证请求。NGFW 收到认证请求后，对其进行身份认证。认证通过后，就可以访问 Internet。

图 6 事前认证示意图



接入用户触发认证的方式

接入用户触发认证的方式由接入方式决定，包括 SSL VPN、L2TP VPN、IPSec VPN 和 PPPoE：

- **SSL VPN 接入用户**

  访问者登录 SSL VPN 模块提供的认证页面来触发认证过程，认证完成后，SSL VPN 接入用户可以使用网络扩展业务访问总部的网络资源。

- **L2TP VPN 接入用户**

  对于 LAC 自主拨号方式，在接入阶段，分支机构的 LAC 通过拨号方式触发认证过程，与 LNS 建立 L2TP VPN 隧道。在访问资源阶段，分支机构中的访问者可以使用事前认证、会话认证等方式触发认证过程，认证完成后，L2TP VPN 接入用户可以访问总部的网络资源。

  对于 NAS-Initiated/Client-Initiated 方式，在接入阶段，访问者通过拨号方式触发认证过程，与 LNS 建立 L2TP VPN 隧道。在访问资源阶段，分支机构中的访问者可以直接访问总部的网络资源；也可以使用事前认证、会话认证等方式触发二次认证，通过二次认证后，访问总部的网络资源。

- **IPSec VPN 接入用户**

分支机构与总部建立 IPSec VPN 隧道后，分支机构中的访问者可以使用事前认证、会话认证等方式触发认证过程，认证完成后，IPSec VPN 接入用户可以访问总部的网络资源。

- **PPPoE 接入用户**

  在接入阶段，访问者通过拨号方式触发认证过程，与 NGFW 建立 PPPoE 连接。在访问资源阶段，访问者可以直接访问网络资源；也可以使用事前认证、会话认证等方式触发二次认证，通过二次认证后，访问网络资源。

认证策略

上网用户使用免认证或会话认证方式触发认证过程、以及已经接入 NGFW 的接入用户使用会话认证方式触发认证过程时，必须经过认证策略的处理。

认证策略的作用是选出需要进行免认证或会话认证的数据流，对免认证的数据流，NGFW 根据用户与 IP/MAC 地址的绑定关系来识别用户；对会话认证的数据流，NGFW 会推送认证页面。认证策略对单点登录或事前认证方式不起作用。

组成信息

认证策略是多个认证策略规则的集合，认证策略决定是否对一条流量进行认证。

认证策略规则由条件和动作组成，条件指的是 NGFW 匹配报文的依据，包括：

- 源安全区域
- 目的安全区域
- 源地址/地区
- 目的地址/地区

动作指的是 NGFW 对匹配到的数据流采取的处理方式，包括：

- 不认证

  对符合条件的数据流不进行认证，主要应用于以下情况：

- 对于企业的高级管理者来说，一方面他们希望省略认证过程；另一方面，他们可以访问机密数据，对安全要求又更加严格。为此，管理员可将这类用户与 IP/MAC 地址双向绑定，不对这类数据流进行认证，但是要求其只能使用指定的 IP 或者 MAC 地址访问网络资源。NGFW 通过用户与 IP/MAC 地址的绑定关系来识别该数据流所属的用户。
- 在 AD/TSM 单点登录的场景中，如果待认证的访问者与认证服务器之间交互的数据流经过 NGFW，则要求不对这类数据流进行认证。

- 认证

  对符合条件的数据流进行认证。

说明：

以下流量即使匹配了认证策略也不会触发认证：

- 访问设备或设备发起的流量
- DHCP、BGP、OSPF、LDP 报文
- 触发认证的一条 HTTP 业务数据流对应的 DNS 报文不受认证策略控制，用户认证通过上线后的 DNS 报文受认证策略控制

匹配顺序

NGFW 匹配报文时总是在多条认证策略规则之间进行，从上往下进行匹配，如图 1 所示。当数据流的属性和某条规则的所有条件匹配时，认为匹配该条规则成功，就不会再匹配后续的规则。如果所有规则都没有匹配到，则按照缺省认证策略进行处理。

图 1 认证策略匹配顺序

NGFW 上存在一条缺省的认证策略，所有匹配条件均为任意（any），动作为不认证。

认证域

认证域是认证流程中的重要环节，认证域上的配置决定了对用户的认证方式以及用户的组织结构。

概述

对于不同认证方式的用户，认证域的作用不尽相同：

- 本地认证/服务器认证用户：决定用户认证时采用本地认证方式还是服务器认证方式，如果是服务器认证方式还包含了使用哪个认证服务器。
- 单点登录用户：单点登录用户的认证过程 NGFW 不参与，只是从认证服务器接收用户登录/注销消息，所以认证域中的认证方式配置对单点登录用户不起作用。但是在与用户域名（dc 字段）同名的认证域中配置的新用户选项对单点登录用户生效。

NGFW 通过识别用户名中包含的认证域，将所有待认证的用户“分流”到对应的认证域中，根据认证域上的配置来对用户进行认证。

用户属于哪个认证域是由用户名中携带的“@”后的字符串来决定的。如“user1@bj”属于“bj”认证域，“user2@hz”属于“hz”认证域。如果用户名中没有携带“@”，则属于缺省的 default 认证域。

规划认证域时，管理员可以使用新创建的认证域，也可以使用缺省的 default 认证域。如果使用新创建的认证域，用户登录时需要输入“登录名@认证域名”；如果使用缺省的 default 认证域，则用户登录时只需要输入登录名，便于记忆。

接入控制

认证域可以对不同的用户进行接入控制：

- 允许对用户做基于策略的控制

  针对上网用户进行基于安全策略、策略路由、带宽策略的控制。

- 允许 VPN 接入

  针对接入用户的控制。

  此外，还可以根据实际情况来选择是否配置认证域是否允许对用户做基于策略的控制。如果认证域同时允许对用户做基于策略的控制，接入用户接入 NGFW 后，可以直接访问网络资源，无需进行二次认证。如果认证域只允许 VPN 接入，则接入用户接入 NGFW 后，在访问网络资源时还需要进行二次认证，此时还需要为这些用户创建一个接入控制方式为“允许对用户做基于策略的控制”的认证域。

认证方式和认证服务器

认证域决定了认证时采用本地认证方式还是服务器认证方式：

- 采用本地认证方式时，由 NGFW 来完成用户名和密码的验证过程，无需配置认证服务器。
- 采用服务器认证方式时，需要在 NGFW 上配置相应的认证服务器，然后由第三方认证服务器来完成用户名和密码的验证过程。

地址池

对于使用 L2TP VPN 以及 PPPoE 方式接入到 NGFW 的接入用户，NGFW 会使用认证域中配置的地址池为其分配地址，然后这类接入用户即可以使用该地址来访问网络资源。

对于接入控制为“允许对用户做基于策略的控制”的认证域，不需要配置地址池。

新用户选项

新用户指的是通过了服务器认证或单点登录，但是在 NGFW 上不存在的用户。例如，在 AD 服务器上为新员工创建了相应的用户名和密码，但没有在 NGFW 中同步创建。这些用户可以通过认证，但是 NGFW 中并没有存储这些用户。

NGFW 根据新用户选项来决定对新用户的处理方式，包括：

- 不允许新用户登录

  不允许添加新用户到 NGFW 的本地用户组中。即不管该用户是否通过了认证服务器的认证，NGFW 都不允许新用户登录。

- 添加到指定的用户组中

  新用户认证通过后允许自动添加到 NGFW 上指定的本地用户组中。新用户添加到指定组后，就可以拥有该组的权限。

  该方式可以看做是一种向 NGFW 中添加用户的方式，可以作为手动创建方式和服务器导入方式的补充。

- 仅作为临时用户，不添加到本地用户列表中

新用户认证通过后只能作为临时用户，不添加到 NGFW 的本地用户组中，但可以临时拥有 NGFW 上某个组的权限。

临时用户只在一次登录中有效，用户下线或 NGFW 重启后该用户的信息就会消失，下次登录时仍然被识别为新用户。

认证服务器

介绍认证时常用的服务器，包括 RADIUS 服务器、HWTACACS 服务器、LDAP 服务器、AD 服务器、SecurID 服务器和 TSM 服务器。

了解各类服务器的基本概念和实现原理，将会有助于管理员在 NGFW 上正确配置服务器对接参数，确保 NGFW 和服务器正常通信。

本节对服务器以及 NGFW 与服务器通信时所使用协议进行简要介绍，详细的内容请参见服务器自带的文档。

RADIUS 服务器

NGFW 与 RADIUS 服务器之间使用 RADIUS 协议通信，RADIUS 协议使用 UDP 协议作为传输协议，具有良好的实时性；同时也支持重传机制和备用服务器机制，从而具有较好的可靠性。NGFW 与 RADIUS 服务器之间使用共享密钥对传输的报文进行加密，具有较好的安全性。

RADIUS 协议的实现比较简单，适用于大用户量时服务器端的多线程结构。

HWTACACS 服务器

NGFW 与 HWTACACS 服务器之间使用 HWTACACS 协议通信，HWTACACS 协议是在 TACACS 基础上进行了功能增强的一种安全协议，主要用于用户的认证、授权和计费。

与 RADIUS 协议相比，HWTACACS 协议具有更加可靠的传输和加密特性，更加适合于安全控制。HWTACACS 协议与 RADIUS 协议的主要区别如表 1 所示。

表 1 HWTACACS 协议与 RADIUS 协议的比较

HWTACACS	RADIUS
使用 TCP 协议，网络传输更可靠	使用 UDP 协议
除了标准的 HWTACACS 报文头，对报文主体全部进行	只是对认证报文中的密码字段进行加密

表 1 HWTACACS 协议与 RADIUS 协议的比较	
HWTACACS	**RADIUS**
加密	
认证与授权分离	认证与授权一起处理
适于进行安全控制	适于进行计费
支持对配置命令进行授权	不支持对配置命令进行授权

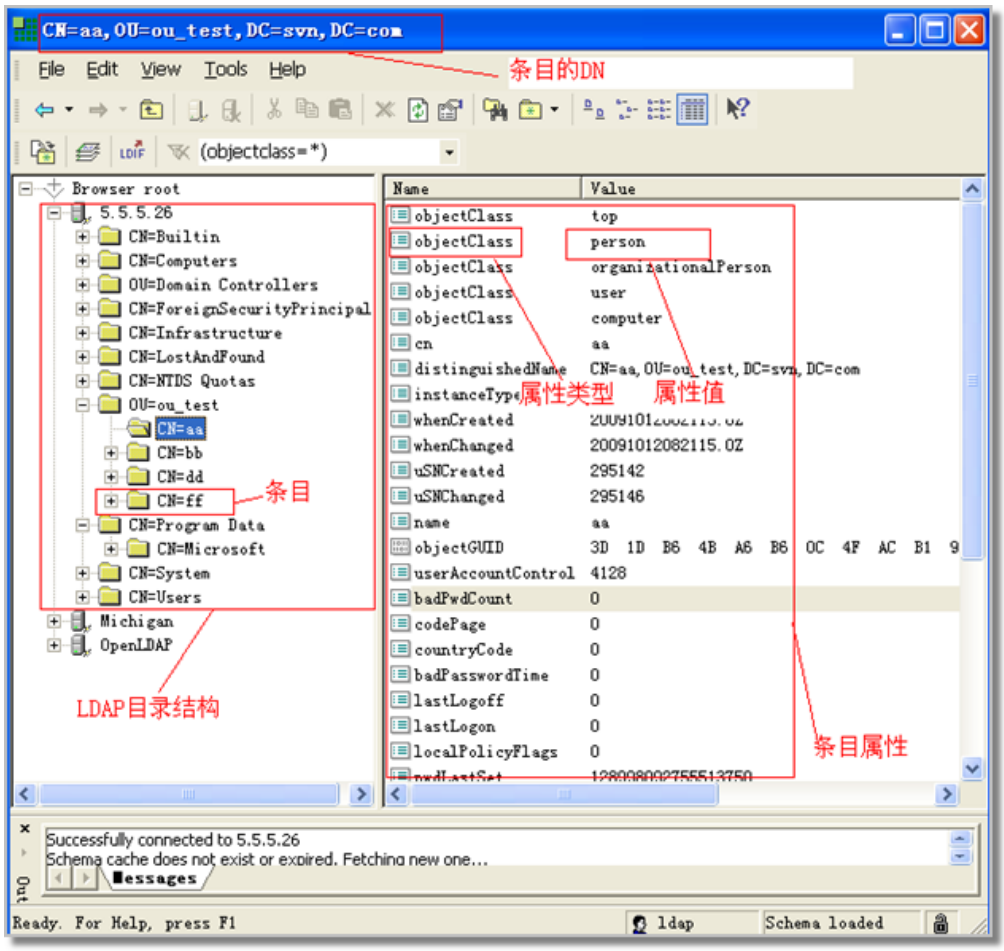
LDAP 服务器

LDAP 是轻量级目录访问协议的简称，是一种基于 TCP/IP 的访问在线目录服务的协议。LDAP 协议的典型应用是用来保存系统的用户信息，用于用户登录时的认证和授权。LDAP 的目录服务功能建立在 Client/Server 的基础之上，所有的目录信息存储在 LDAP 服务器上。

目录是一组具有类似属性、以一定逻辑和层次组合的信息。LDAP 协议中目录是按照树型结构组织，目录由条目（Entry）组成，条目是具有区别名 DN（Distinguished Name）的属性（Attribute）集合。属性由类型（Type）和多个值（Values）组成。LDAP 目录树的最顶部就是根，根的区别名称为“Base DN”。

如图 1 所示，通过 LDAP Client 来查看 LDAP 协议的目录结构。LDAP 服务器所管辖域 svn.com 中存在组织单元“ou_test”，其中包括 aa、bb、dd 和 ff 条目，则条目“aa”的 Base DN 为：“CN=aa,OU=ou_test,dc=svn,dc=com”。

图 1 LDAP 目录结构



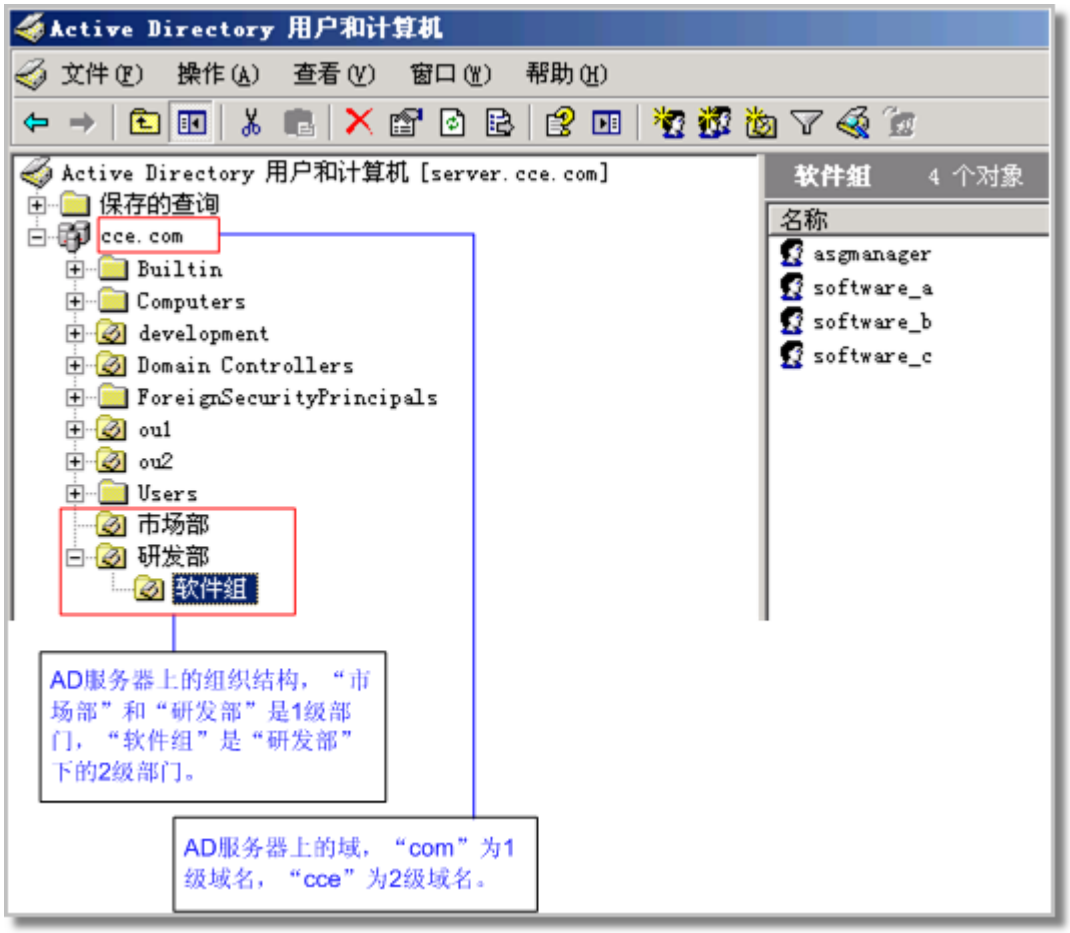
AD 服务器

AD 是 Windows Server 域环境中提供目录服务的组件，可以将活动目录理解为目录服务在微软平台的一种实现方式。

活动目录将登录身份验证以及目录对象的访问控制集成在一起，管理员可以管理分散在网络各处的目录数据和组织单位，经过授权的网络用户可以访问网络任意位置的资源。

如图 2 所示，AD 服务器所管辖域 cce.com 中包括“研发部”和“市场部”两个部门，则“研发部”的 Base DN 为：“OU=研发部,DC=cce,DC=com”。

图 2 AD 目录结构



SecurID 服务器

SecurID 服务器通过双因素认证能够有效的管理用户认证，用户登录时需要输入用户名及密码，密码由静态 PIN 码和动态 Token 序列号组成：

- 静态 PIN 码在 SecurID 服务器上进行设置，由管理员提供给用户。
- 动态 Token 序列号由令牌生成，这些动态 Token 序列号每隔一定的时间变化一次。

静态 PIN 码和动态 Token 序列号任一出现错误，用户无法登录成功。因为需要两个因素，所以 SecurID 认证方式能提供更加安全的身份认证机制。

NGFW 与 SecurID 服务器之间使用共享密钥对传输的报文进行加密，具有较好的安全性。

TSM 服务器

TSM 是华为公司开发的终端安全管理软件，基于 TSM 代理提供安全接入控制、终端安全管理、补丁管理、终端用户的行为管理、软件分发、资产管理六大功能。

TSM 服务器以树状结构呈现企业整个部门的组织结构，一个部门对应于企业中的一个部门，一个部门包括若干个终端用户。

NGFW 从 TSM 服务器导入部门和终端用户信息，同时支持对通过 TSM 服务器身份认证的用户实施单点登录认证方式，使其不用进行二次身份认证。

应用场景——上网用户访问网络资源

介绍上网用户访问网络资源时，如何实施用户管理与认证机制。

NGFW 作为企业的出口网关，内部网络中的访问者通过 NGFW 访问资源服务器或 Internet 时，为了实现基于用户的访问行为控制，需要在 NGFW 上完成如下任务：

- 存储用户信息，使用户可以被安全策略、策略路由、带宽策略以及审计策略所引用。
- 对访问者进行认证，验证访问者的身份，同时获取用户与 IP 地址的对应关系。

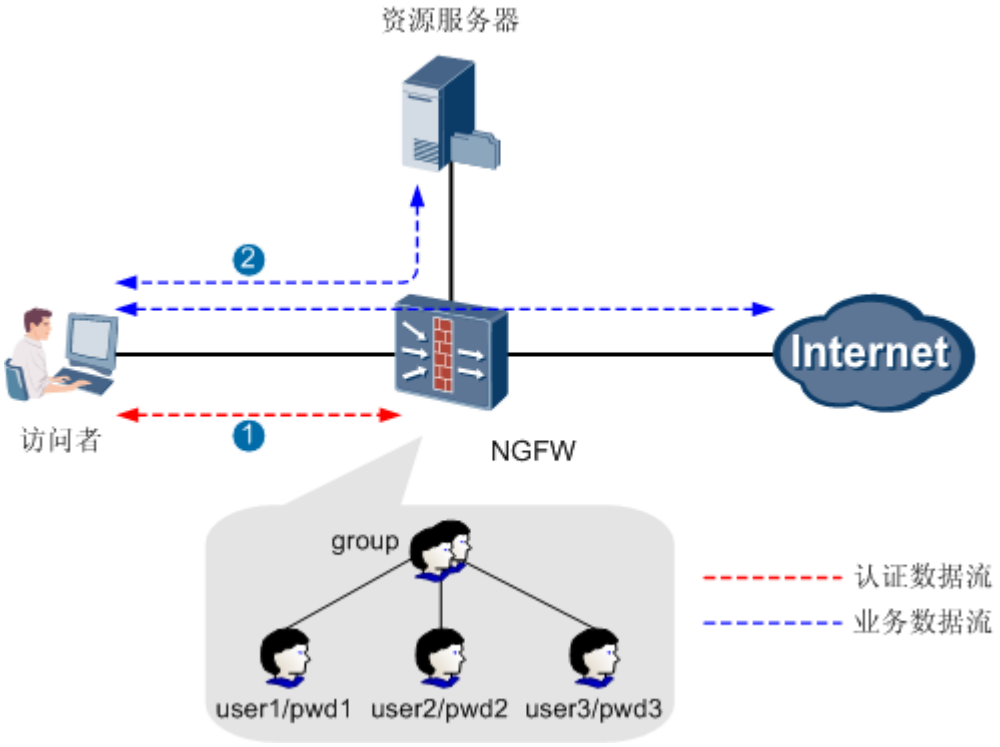
在不同的网络环境下，针对这两个任务也有不同的实现方式，下面分情况介绍。

本地认证

管理员依据企业的组织结构，在 NGFW 上创建相应的用户/组，并设置用户的密码。认证时，由 NGFW 来验证访问者使用的用户和密码，对访问者进行认证。

如图 1 所示，NGFW 上存储了用户/组和密码等信息。内部网络中的访问者在访问网络资源之前，必须先通过 NGFW 的认证。认证成功后，NGFW 记录访问者使用的用户和 IP 地址之间的对应关系。访问者访问网络资源时，NGFW 上基于此用户或用户所属组的策略决定了访问者的权限和行为。

图 1 本地认证时用户管理和认证方式示意图



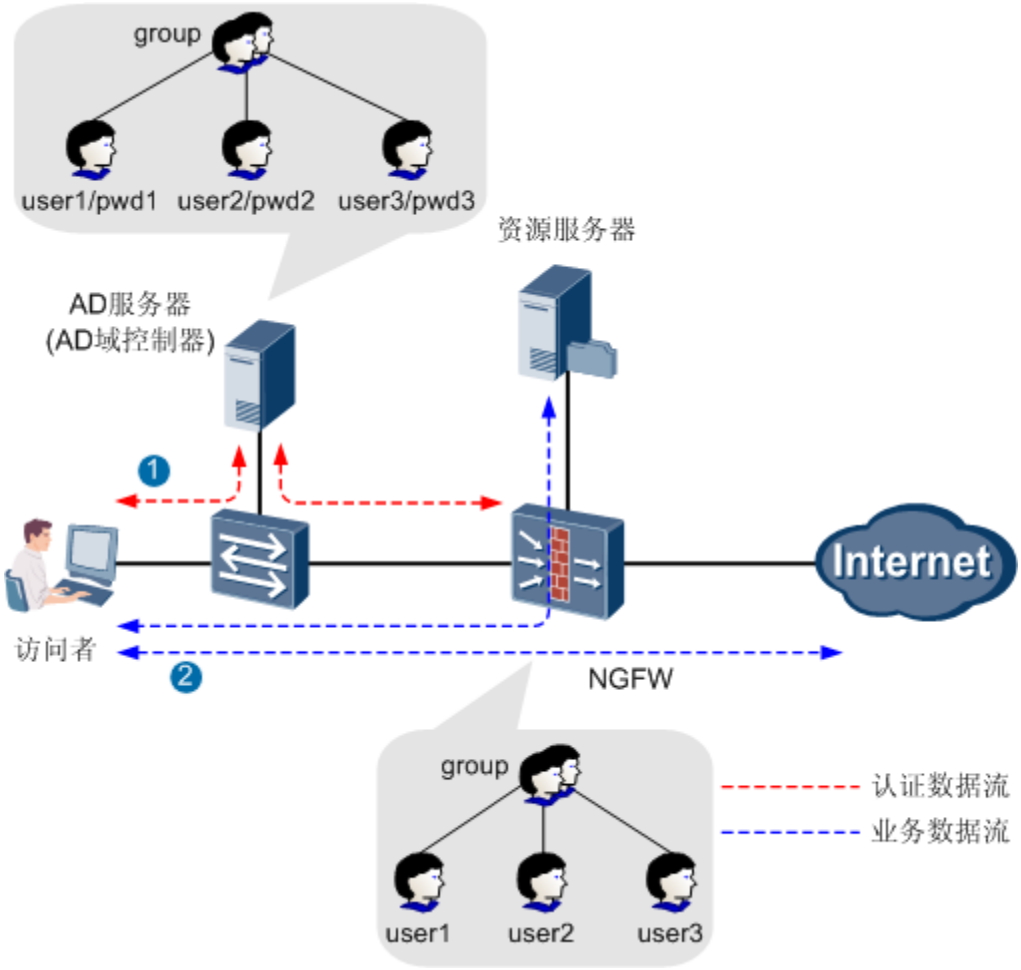
AD 单点登录

企业已经部署了 AD（Active Directory）身份验证机制，AD 服务器上存储了用户/组和密码等信息。管理员可以将 AD 服务器上的组织结构和账号信息导入到 NGFW。对于 AD 服务器上新创建的用户信息，还可以按照一定的时间间隔定时导入。以便后续管理员可以在 NGFW 上通过策略来控制不同用户/组对网络的访问行为。

认证时，由 AD 服务器对访问者进行认证，并将认证信息发送至 NGFW，使 NGFW 能够获取用户与 IP 地址的对应关系。访问者通过 AD 服务器的认证后，就可以直接访问网络资源，无需再由 NGFW 进行认证，这种认证方式也称为“AD 单点登录”。

如图 2 所示，AD 服务器上存储了用户/组和密码等信息，NGFW 上可以存储用户/组信息以及组织结构关系。内部网络中的访问者使用 AD 域账号和密码进行认证，认证通过后，AD 服务器将域账号和 IP 地址发送至 NGFW，NGFW 记录访问者使用的用户和 IP 地址之间的对应关系。访问者访问网络资源时，NGFW 上基于此用户或用户所属组的策略决定了访问者的权限和行为。

图 2 AD 单点登录时用户管理和认证方式示意图



说明：

此处以 AD 服务器位于访问者所在的网络为例进行说明，如果 AD 服务器位于资源服务器所在的网络，则需要在 NGFW 上配置认证策略时，不对访问者与 AD 服务器之间的认证报文进行认证，同时在安全策略中保证这类报文可以正常通过 NGFW。

TSM 单点登录

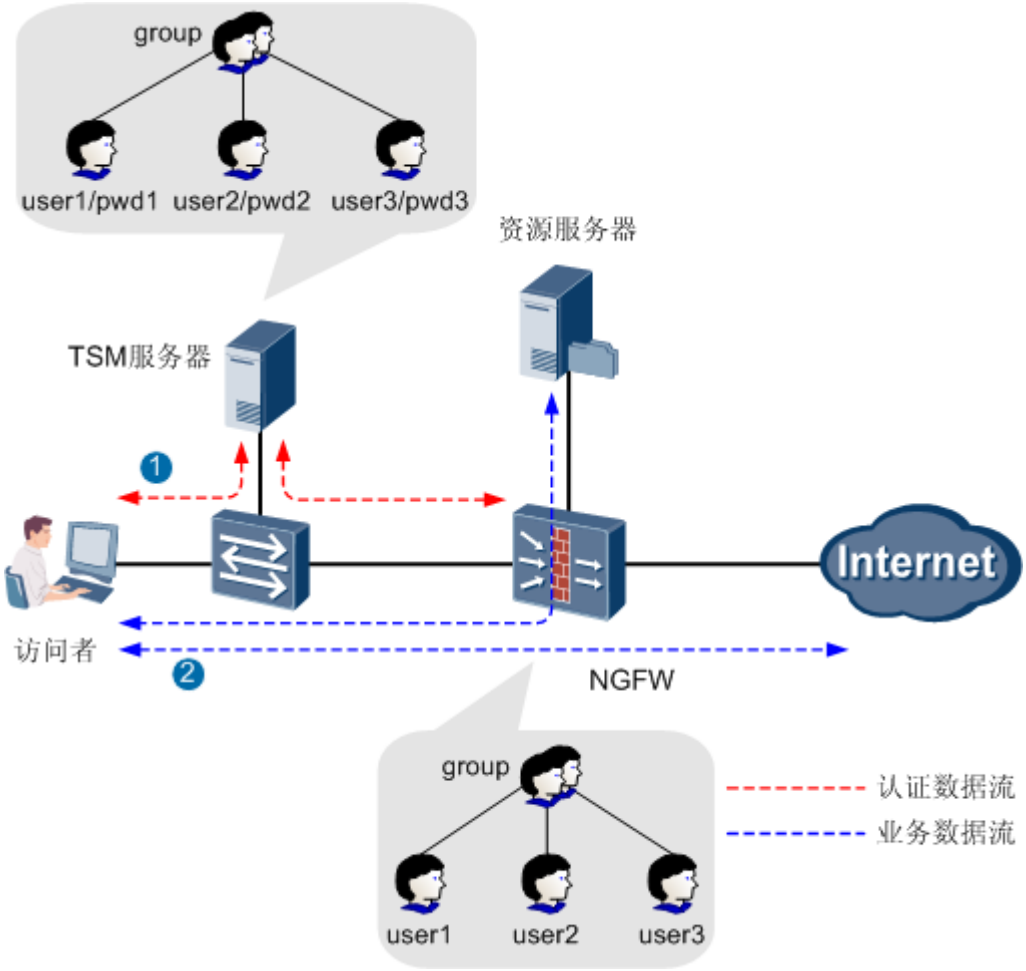
企业已经部署了 TSM（Terminal Security Management）身份验证机制，TSM 服务器上存储了用户/组和密码等信息。管理员可以将 TSM 服务器上的组织结构和账号信息导入到 NGFW，以便后续管理员可以在 NGFW 上通过策略来控制不同用户/组对网络的访问行为。

认证时，由 TSM 服务器对访问者进行认证，并将认证信息发送至 NGFW，使 NGFW 能够获取用户与 IP 地址的对应关系。访问者通过 TSM 服务器的认证后，就可以直接访问网络资源，无需再由 NGFW 进行认证，这种认证方式也称为“TSM 单点登录”。

如图 3 所示，TSM 服务器上存储了用户/组和密码等信息，NGFW 上可以存储用户/组信息。内部网络中的访问者使用 TSM 账号和密码进行认证，认证通过后，TSM 服务器将账号和 IP 地址发送至 NGFW，NGFW 记录访问者使用

的用户和 IP 地址之间的对应关系。访问者访问网络资源时，NGFW 上基于此用户或用户所属组的策略决定了访问者的权限和行为。

图 3 TSM 单点登录时用户管理和认证方式示意图



说明：

此处以 TSM 服务器位于访问者所在的网络为例进行说明，如果 TSM 服务器位于资源服务器所在的网络，则需要在 NGFW 上配置认证策略时，不对访问者与 TSM 服务器之间的认证报文进行认证，同时在安全策略中保证这类报文可以正常通过 NGFW。

服务器认证

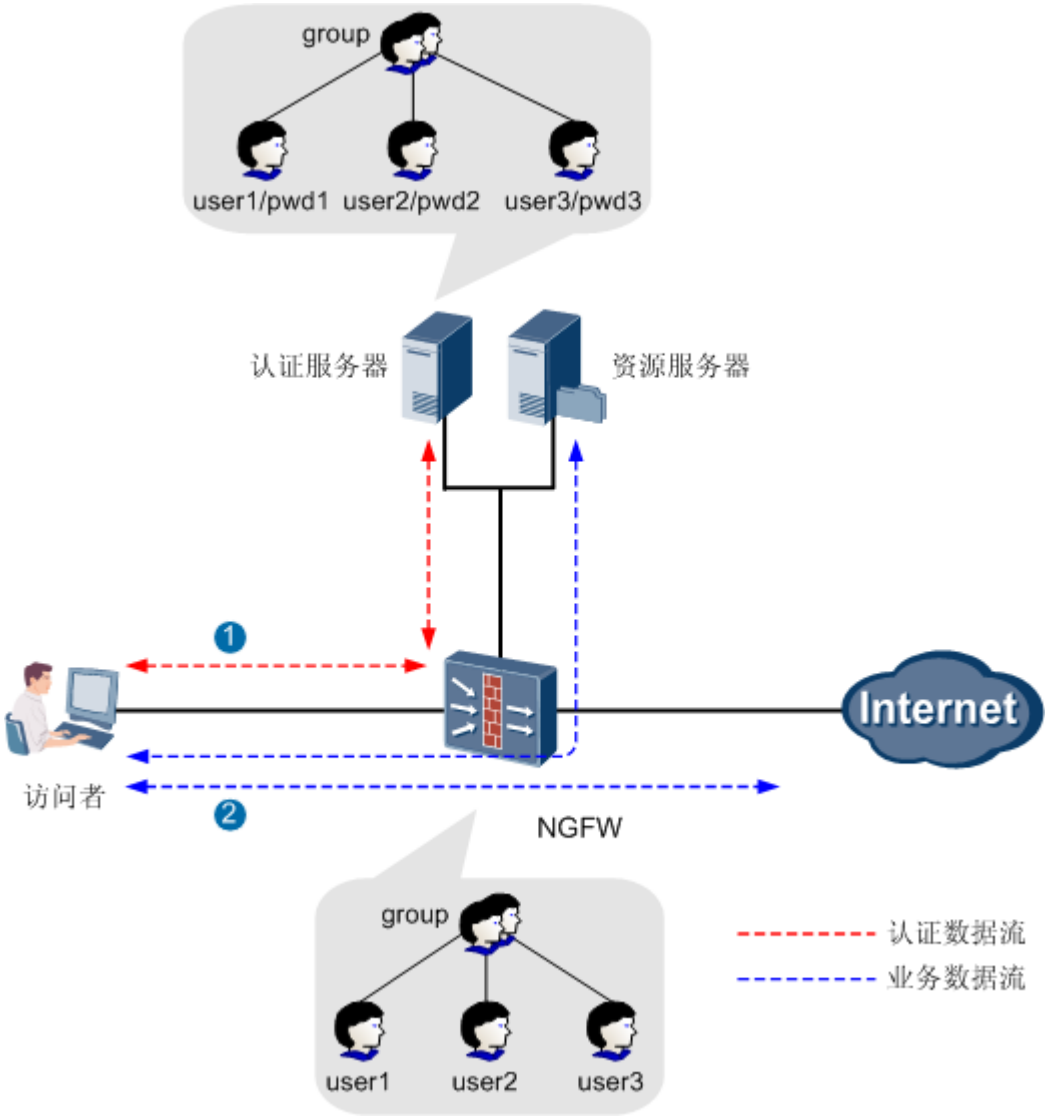
企业已经部署了 RADIUS（Remote Authentication Dial In User Service）、HWTACACS（HuaWei Terminal Access Controller Access Control System）、AD、LDAP（Lightweight Directory Access Protocol）或 SecurID 认证服务器，并在认证服务器上存储了用户/组和密码等信息。对于 RADIUS、HWTACACS 或 SecurID 服务器，管理员需要根据现有的组织结构，在 NGFW 上手动创建或者使用文件批量导入相应的用户/组。对于 AD

或 LDAP 服务器，管理员可以将 AD 或 LDAP 服务器中的用户信息导入到 NGFW 上，以便后续管理员可以在 NGFW 上通过策略来控制不同用户/组对网络的访问行为。

认证时，NGFW 作为认证服务器的代理客户端，将用户名和密码发送给认证服务器进行认证。

如图 4 所示，认证服务器上存储了用户/组和密码等信息，NGFW 上可以存储用户/组信息。内部网络中的访问者在访问网络资源之前，必须先通过认证服务器的认证。认证成功后，NGFW 会记录访问者使用的用户和 IP 地址之间的对应关系。访问者访问网络资源时，NGFW 上基于此用户或用户所属组的策略决定了访问者的权限和行为。

图 4 服务器认证时用户管理和认证方式示意图



说明：

此处以认证服务器位于资源服务器所在的网络为例进行说明，描述同样适用于认证服务器位于访问者所在网络的情况。

应用场景——接入用户使用 SSL VPN 接入设备后访问网络资源

介绍接入用户使用 SSL VPN 接入 NGFW 并访问网络资源时，如何实施用户管理与认证机制。

NGFW 作为企业的 VPN 接入网关，接入用户使用 SSL VPN 接入 NGFW 并访问网络资源时，整体过程可以分为接入（建立隧道）和访问资源两个阶段：

- 接入阶段

  在接入阶段，访问者登录 SSL VPN 认证页面，NGFW 对访问者进行身份验证，建立 SSL VPN 隧道。

- 访问资源阶段

  接入后，访问者可以使用 Web 代理或网络扩展业务来访问网络资源。其中 Web 代理业务是由 NGFW 中转来访问网络资源，无法基于用户来进行控制，本节只针对网络扩展业务进行介绍。

为了保证访问者正常接入，以及对访问者使用网络扩展业务访问资源时进行控制，需要在 NGFW 上完成如下任务：

- 存储用户信息，使用户也可以被安全策略、策略路由、带宽策略以及审计策略所引用。另外，配置 SSL VPN 功能时也要引用用户。
- 在接入阶段，对访问者进行认证，防止非授权的访问者接入。在访问资源阶段，对于使用网络扩展业务的访问者，获取其用户与 IP 地址的对应关系。

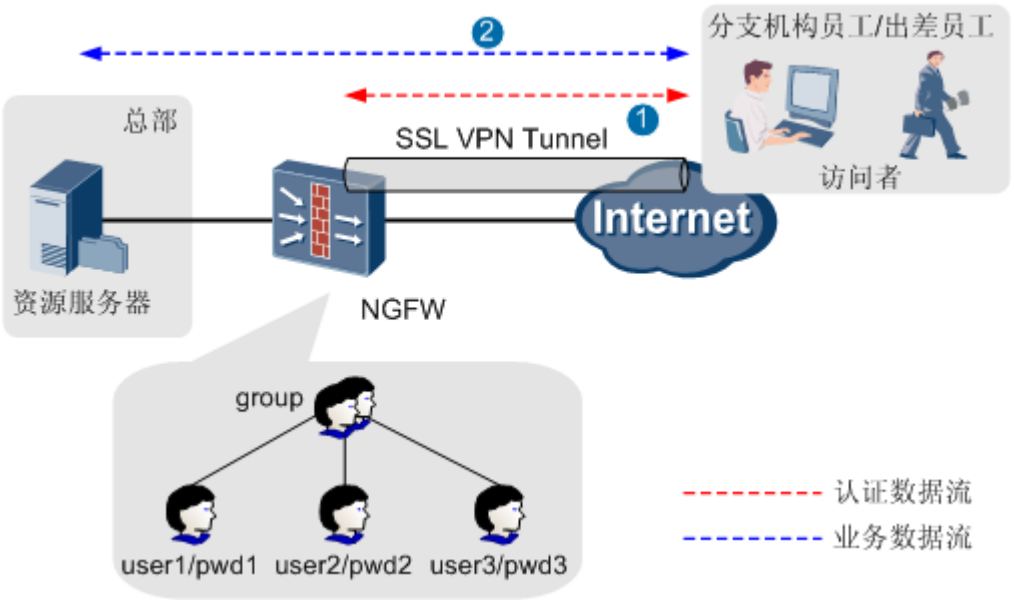
说明：

为了便于描述，下面以本地认证为例来进行说明，即 NGFW 上已经创建了相应的用户/组，并设置了用户的密码，由 NGFW 来完成验证密码的过程。下文的描述同样适用于服务器认证的情况，不同之处在于服务器认证是由认证服务器来完成验证密码的过程。

如图 1 所示，分支机构员工或出差员工接入时，必须先通过 NGFW 的认证。认证成功后，对于使用网络扩展业务的访问者，NGFW 会为其分配私网 IP 地址，同时会记录访问者使用的用户和私网 IP 地址之间的对应关系。

在访问资源阶段，由于 NGFW 已经记录了访问者使用的用户和私网 IP 地址的对应关系，NGFW 上基于此用户或用户所属组的策略决定了访问者的权限和行为，在这一阶段无需对访问者进行二次认证。

图 1 接入用户使用 SSL VPN 网络扩展功能访问网络资源时用户管理和认证方式示意图



应用场景——接入用户使用 L2TP VPN 接入设备后访问网络资源

介绍接入用户使用 L2TP VPN 接入 NGFW 并访问网络资源时，如何实施用户管理与认证机制。

说明：

本节的描述也适用于接入用户使用 L2TP over IPSec VPN 接入 NGFW 并访问网络资源的场景。

NGFW 作为企业的 VPN 接入网关，接入用户使用 L2TP VPN 接入 NGFW 并访问网络资源时，整体过程可以分为接入（建立隧道）和访问资源两个阶段：

- 接入阶段

  在接入阶段，NGFW 对访问者进行身份验证，建立 L2TP VPN 隧道。

- 访问资源阶段

  接入后，访问者可以访问企业总部的网络资源。

为了保证访问者正常接入，以及访问资源时对其进行控制，需要在 NGFW 上完成如下任务：

- 存储用户信息，使用户也可以被安全策略、策略路由、带宽策略以及审计策略所引用。另外，配置 L2TP VPN 功能时也要引用用户。

- 在接入阶段，对访问者进行认证，防止非授权的访问者接入。在访问资源阶段，是否对访问者进行二次认证，与实际网络环境中对安全管理和权限控制的需求有关，需要综合考虑各方面的因素。

下面根据建立 L2TP 隧道的不同方式来分情况介绍。

说明：

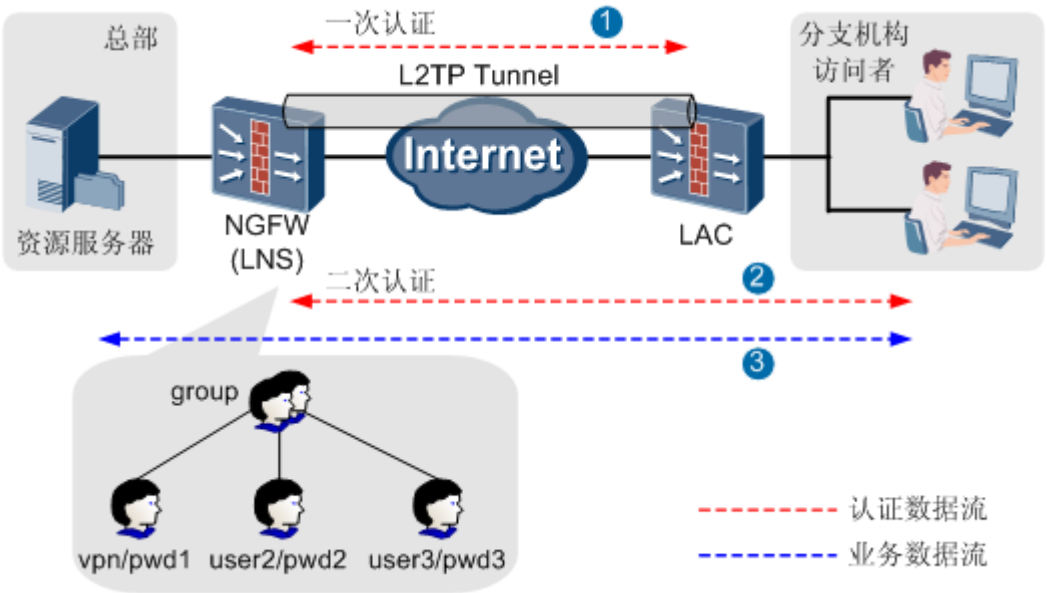
为了便于描述，下面以本地认证为例来进行说明，即 NGFW 上已经创建了相应的用户/组，并设置了用户的密码，由 NGFW 来完成验证密码的过程。下文的描述同样适用于服务器认证的情况，不同之处在于服务器认证是由认证服务器来完成验证密码的过程。

LAC 自主拨号方式

如图 1 所示，分支机构通过 LAC 自主拨号方式与总部建立 L2TP VPN 隧道。在接入阶段，NGFW（LNS）对 LAC 进行认证。隧道一旦建立，分支机构中的访问者可以直接访问总部的网络资源。

由于在接入阶段 LAC 使用的用户仅用于标识 LAC 的身份，NGFW 无法使用该用户来标识分支机构中的访问者，因此在访问资源阶段，NGFW 必须对分支机构中的访问者再次进行认证。认证成功后，NGFW 记录访问者使用的用户和 IP 地址之间的对应关系。分支机构中的访问者访问总部网络资源时，NGFW 上基于此用户或用户所属组的策略决定了访问者的权限和行为。

图 1 LAC 自主拨号方式的 L2TP VPN 场景中接入用户访问网络资源时用户管理和认证方式示意图

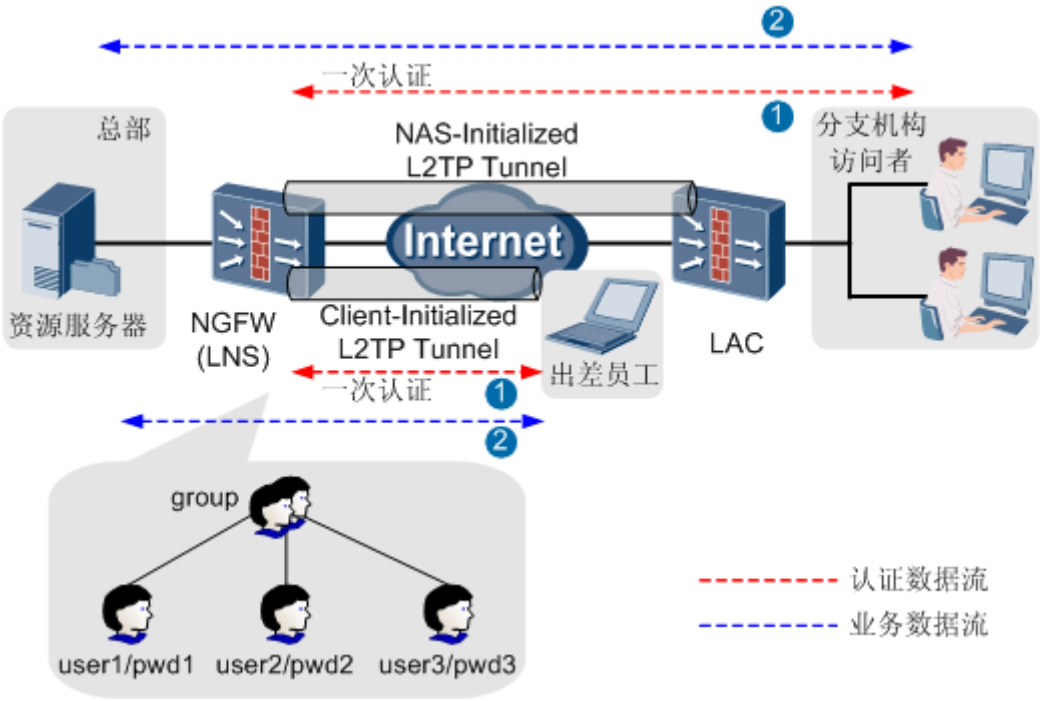


NAS-Initiated/Client-Initiated 方式

如图 2 所示，分支机构通过 NAS-Initiated 方式与总部建立 L2TP 隧道，出差员工通过 Client-Initiated 方式与总部建立 L2TP 隧道。在接入阶段，这两种方式都是使用用户名和密码通过拨号方式来触发 L2TP 隧道的建立。L2TP 隧道建立过程中，NGFW（LNS）会为访问者分配私网 IP 地址，同时会记录访问者使用的用户和私网 IP 地址之间的对应关系。

在访问资源阶段，NGFW 可以直接根据接入阶段记录的用户来控制访问者的权限和行为，不需要对访问者进行二次认证。

图 2 NAS-Initiated/Client-Initiated 方式的 L2TP VPN 场景中接入用户访问网络资源时用户管理和认证方式示意图



如果需要进一步对访问者实施安全管理和权限控制，也可以在访问资源阶段对访问者进行二次认证，NGFW 根据访问者在二次认证中使用的用户来控制访问者的权限和行为。

应用场景——接入用户使用 IPSec VPN 接入设备后访问网络资源

介绍接入用户使用 IPSec VPN 接入 NGFW 并访问网络资源时，如何实施用户管理与认证机制。

说明：

本节的描述也适用于接入用户使用 GRE VPN 接入 NGFW 并访问网络资源的场景。

NGFW 作为企业的 VPN 接入网关，接入用户使用 IPSec VPN 接入 NGFW 并访问网络资源时，整体过程可以分为接入（建立隧道）和访问资源两个阶段：

- 接入阶段

  在接入阶段，两台 NGFW 协商建立 IPSec VPN 隧道，在协商的过程中会进行隧道验证，在这一阶段不涉及用户的内容。

- 访问资源阶段

  接入后，访问者可以访问企业总部的网络资源。

为了实现基于用户的访问行为控制，需要在 NGFW 上完成如下任务：

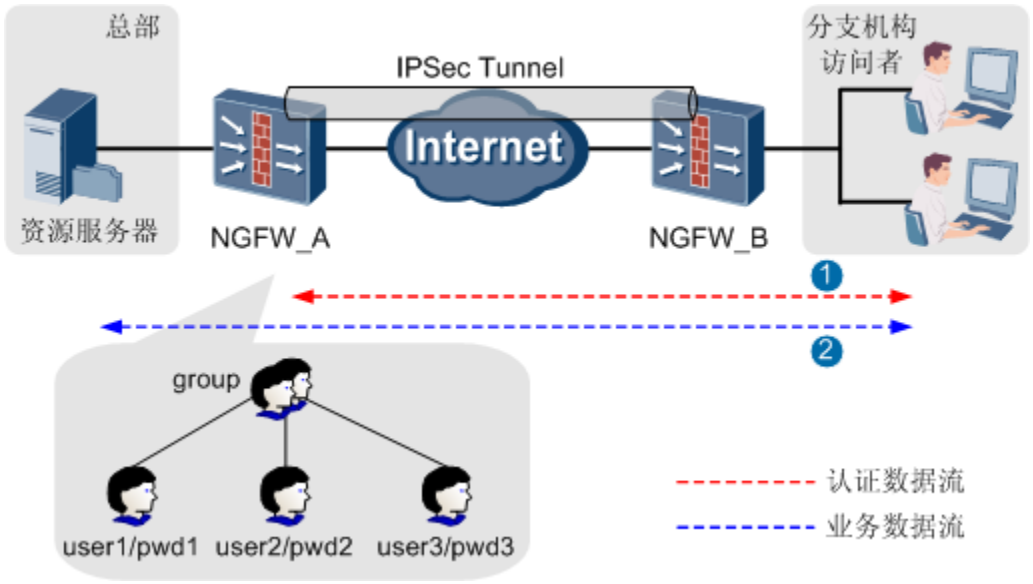
- 存储用户信息，使用户可以被安全策略、策略路由、带宽策略以及审计策略所引用。
- 在访问资源阶段，对访问者进行认证，获取用户与 IP 地址的对应关系。

说明：

为了便于描述，下面以本地认证为例来进行说明，即 NGFW 上已经创建了相应的用户/组，并设置了用户的密码，由 NGFW 来完成验证密码的过程。下文的描述同样适用于服务器认证的情况，不同之处在于服务器认证是由认证服务器来完成验证密码的过程。

如图 1 所示，分支机构与总部建立 IPSec VPN 隧道。隧道成功建立后，分支机构中的访问者在访问企业总部的网络资源之前，必须先通过 NGFW 的认证。认证成功后，NGFW 记录访问者使用的用户和 IP 地址之间的对应关系。分支机构中的访问者访问总部网络资源时，NGFW 上基于此用户或用户所属组的策略决定了访问者的权限和行为。

图 1 接入用户使用 IPSec VPN 访问网络资源时用户管理和认证方式示意图



应用场景——接入用户使用 PPPoE 接入设备后访问网络资源

介绍接入用户使用 PPPoE 接入 NGFW 并访问网络资源时，如何实施用户管理与认证机制。

NGFW 作为企业的接入网关，接入用户使用 PPPoE 接入 NGFW 并访问网络资源时，整体过程可以分为接入和访问资源两个阶段：

- 接入阶段

  在接入阶段，NGFW 对访问者进行身份验证，建立 PPPoE 连接。

- 访问资源阶段

  接入后，访问者可以访问网络资源。

为了实现基于用户的访问行为控制，需要在 NGFW 上完成如下任务：

- 存储用户信息，使用户也可以被安全策略、策略路由、带宽策略以及审计策略所引用。另外，配置 PPPoE 功能时也要引用用户。
- 在接入阶段，对访问者进行认证，防止非授权的访问者接入。在访问资源阶段，是否对访问者进行二次认证，与实际网络环境中对安全管理和权限控制的需求有关，需要综合考虑各方面的因素。

说明：

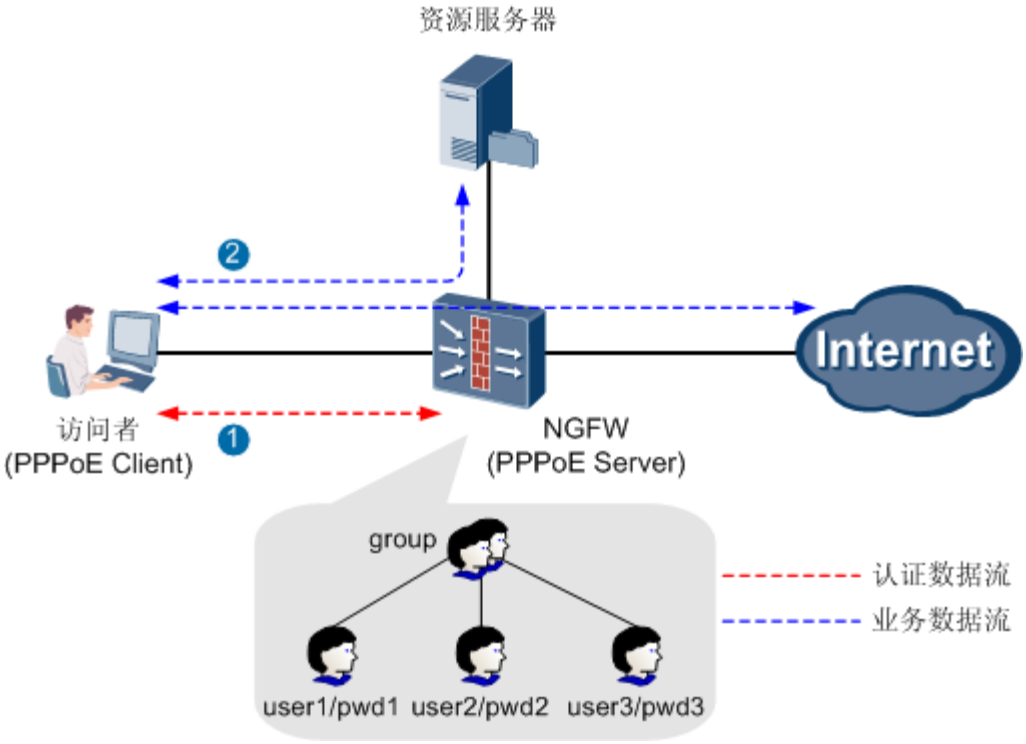
为了便于描述，下面以本地认证为例来进行说明，即 NGFW 上已经创建了相应的用户/组，并设置了用户的密码，

由 NGFW 来完成验证密码的过程。下文的描述同样适用于服务器认证的情况，不同之处在于服务器认证是由认证服务器来完成验证密码的过程。

如图 1 所示，NGFW 作为 PPPoE Server，访问者作为 PPPoE Client。在接入阶段，访问者使用用户名和密码通过拨号方式来触发 PPPoE 协商。PPPoE 连接建立过程中，NGFW 会为访问者分配私网 IP 地址，同时会记录访问者使用的用户和私网 IP 地址之间的对应关系。

在访问资源阶段，NGFW 可以直接根据接入阶段记录的用户来控制访问者的权限和行为，不需要对访问者进行二次认证。

图 1 接入用户使用 PPPoE 访问网络资源时用户管理和认证方式示意图



如果需要进一步对访问者实施安全管理和权限控制，也可以在访问资源阶段对访问者进行二次认证，NGFW 根据访问者在二次认证中使用的用户来控制访问者的权限和行为。

使用限制和注意事项

配置用户与认证之前请先阅读使用限制和注意事项。

配置用户与认证前，请注意以下事项：

- 如果内部网络中有多个主机的网络数据是经过源地址转换（源 NAT）为同一个 IP 地址后才到达 NGFW，则 NGFW 只能根据地址转换后的 IP 来进行认证，将多个主机视作同一个用户。

- 如果网络中使用 DHCP 方式动态分配 IP 地址，则需要在 DHCP 服务器上为配置了 IP/MAC 双向绑定的用户分配固定的 IP 地址。
- 当用户和 NGFW 之间存在三层设备时，如果该用户是 MAC 地址双向绑定免认证用户，由于三层设备转发报文时会改变 MAC 地址，该用户将登录失败；如果该用户是 MAC 地址绑定用户，但采用了单点登录方式进行认证，此时，MAC 地址绑定属性不生效，用户使用其他 MAC 地址仍可登录。
- 如果网络中存在长连接业务，该长连接业务对应的用户老化时，会话也会老化，将会导致长连接业务中断。为了解决该问题，可以在配置认证策略时将长连接业务配置为不认证。
- 只能在根系统中配置重定向认证方式和认证页面，所有虚拟系统共用根系统的配置。
- 虚拟系统下不支持单点登录功能。
- 非 default 认证域的用户登录时必须以“用户名@认证域”的形式输入用户名（单点登录除外，单点登录输入形式由原始认证系统决定）。
- 对于规划不同认证域用户账号独立的场景，用户组织结构是多个以“认证域”为顶级节点的树形组织结构，注意以下几点：
  - 执行引用非 default 认证域下的用户的命令行时，必须携带“@认证域名”，例如 user1@test 表示 test 认证域下的 user1。
  - 用户的创建、移动、服务器导入都是基于某一个认证域的，不能跨域进行。

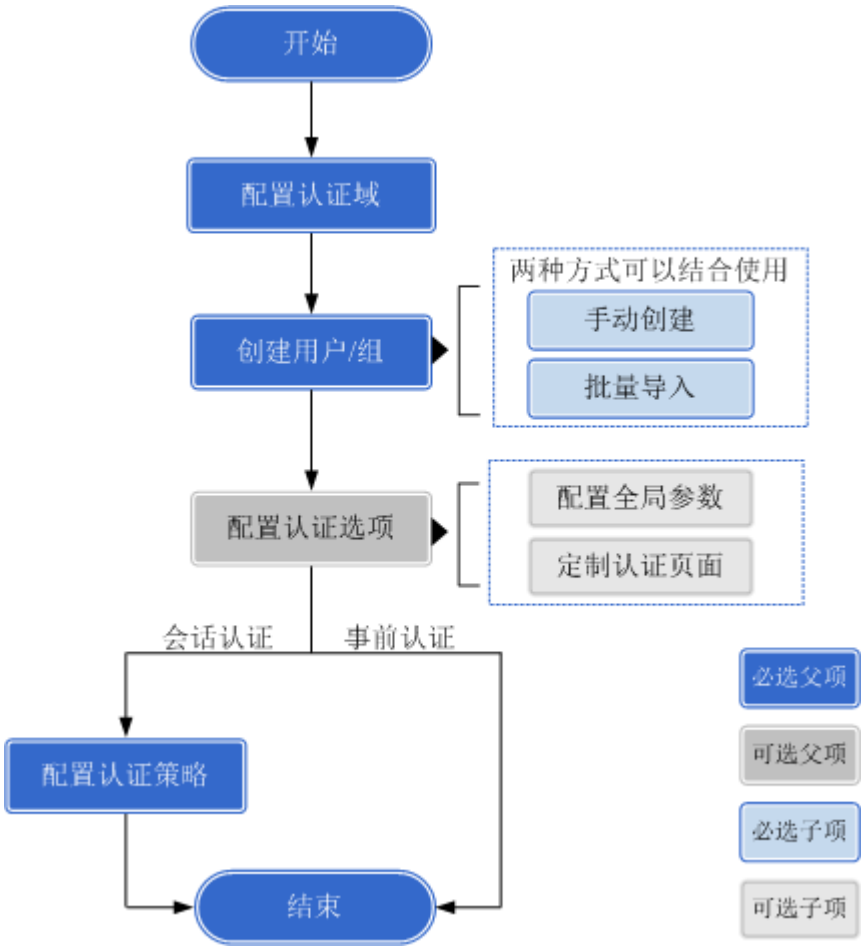
配置流程

了解用户与认证的配置流程，有助于您根据需要选择阅读后续的内容。

本地认证配置流程

使用本地认证方式时，需要在 NGFW 上创建用户/组并设置密码，然后根据触发认证的方式来选择配置认证策略。本地认证的配置流程如图 1 所示。

图 1 本地认证配置流程

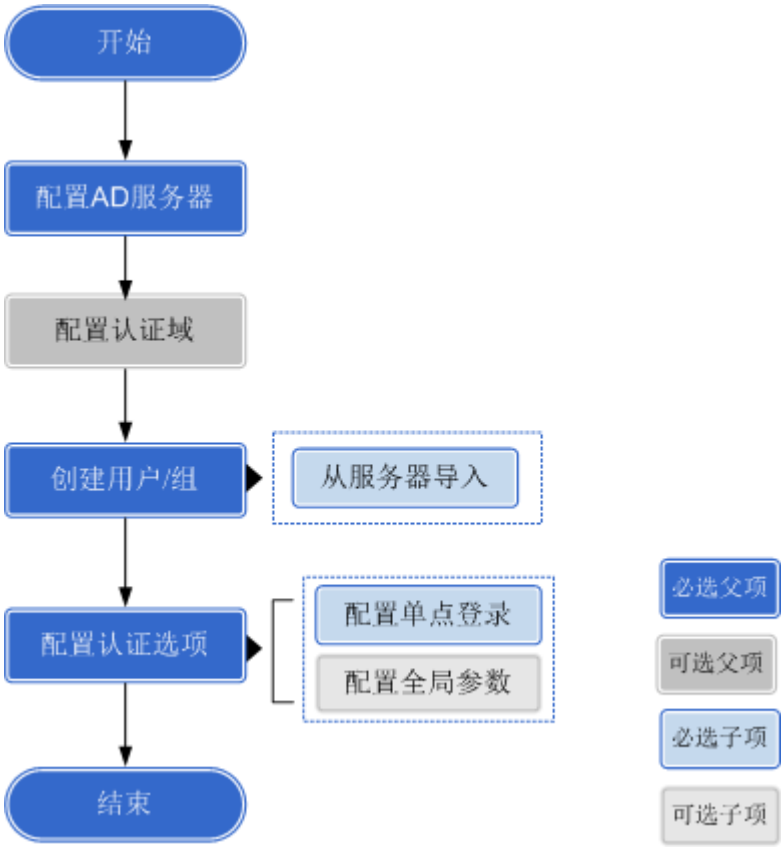


AD 单点登录配置流程

使用 AD 单点登录方式时，需要将 AD 服务器上的用户/组信息导入到 NGFW 上，然后配置认证选项中的 AD 单点登录。AD 单点登录配置流程如图 2 所示。

单点登录的认证过程不需要认证域参与，但是因为对用户进行权限控制需要本地存在用户或用户组，所以需要将 AD 服务器上的用户或用户组导入到 NGFW 的某个认证域下。NGFW 仅支持将 AD 服务器用户或用户组导入到与服务器同名的认证域或 default 认证域（所有认证域共享 default 认证域的用户帐号的情形）下，并且需要在与用户域名（dc 字段）同名的认证域下配置新用户选项。

图 2 AD 单点登录配置流程



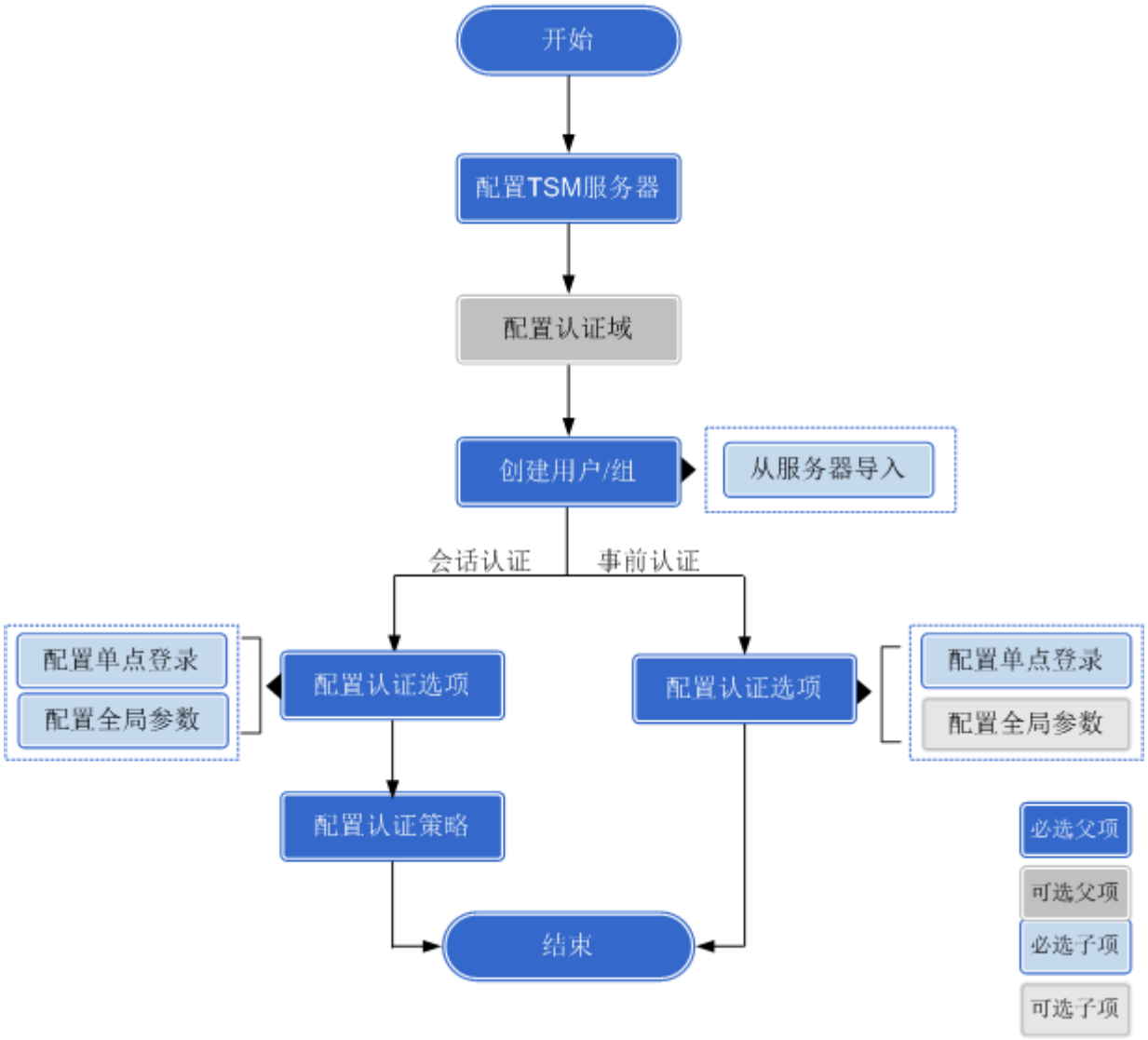
TSM 单点登录配置流程

使用 TSM 单点登录方式时，需要将 TSM 服务器上的用户/组信息导入到 NGFW 上，然后配置认证选项中的 TSM 单点登录。TSM 单点登录配置流程如图 3 所示。

单点登录的认证过程不需要认证域参与，但是因为对用户进行权限控制需要本地存在用户或用户组，所以需要将服务器上的用户或用户组导入到 NGFW 的某个认证域下。NGFW 仅支持将 TSM 服务器用户或用户组导入到 default 认证域，并且需要在 default 认证域下配置新用户选项。

TSM 单点登录有事前认证和会话认证两种触发方式。事前认证需要用户主动访问 TSM 的 Portal 认证页面进行登录，登录成功才可以访问业务；会话认证用户可以直接访问 HTTP 业务，NGFW 将 HTTP 请求重定向到 TSM 的 Portal 认证页面，用户登录成功后继续访问业务。会话认证需要在“全局参数”中配置用户登录 URL 为 TSM 的 Portal 认证页面地址，并配置认证策略触发会话认证。

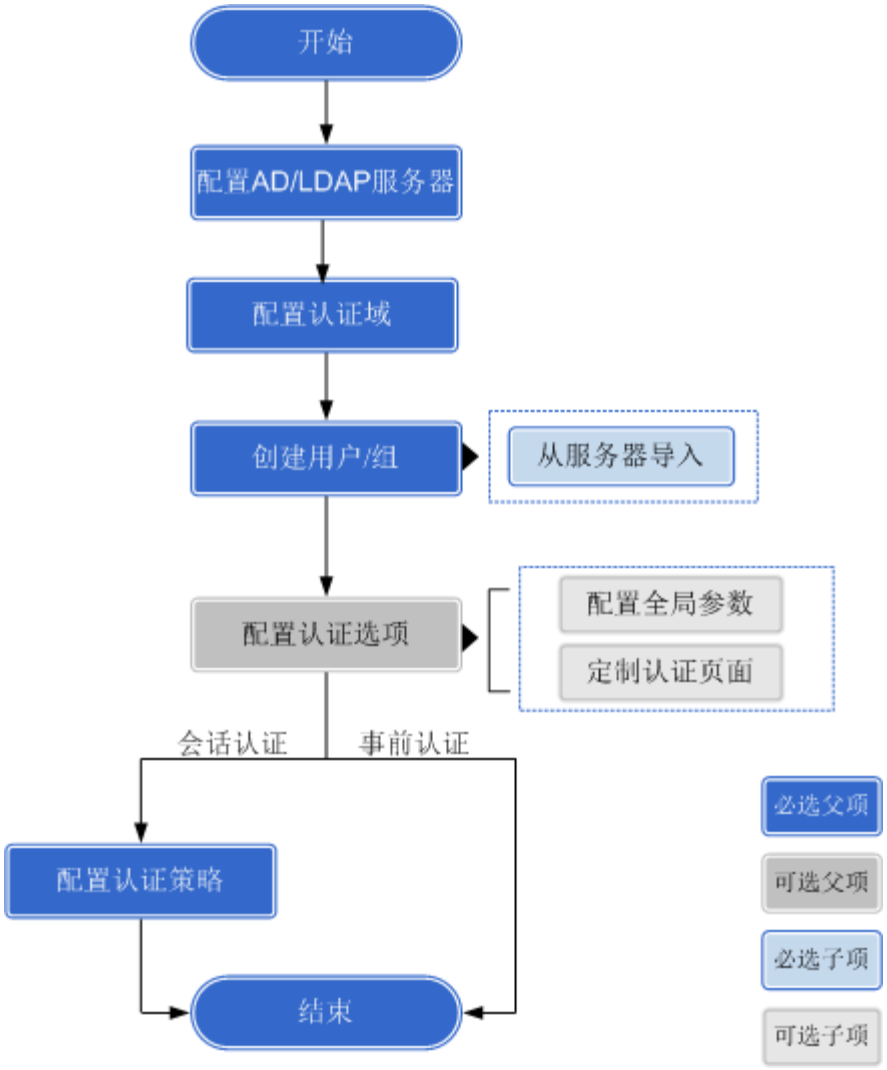
图 3 TSM 单点登录配置流程



AD/LDAP 服务器认证配置流程

使用 AD/LDAP 服务器认证方式时，需要将 AD/LDAP 服务器上的用户或用户组信息导入到 NGFW 上，然后根据触发认证的方式来选择配置认证策略。AD/LDAP 服务器认证配置流程如图 4 所示。

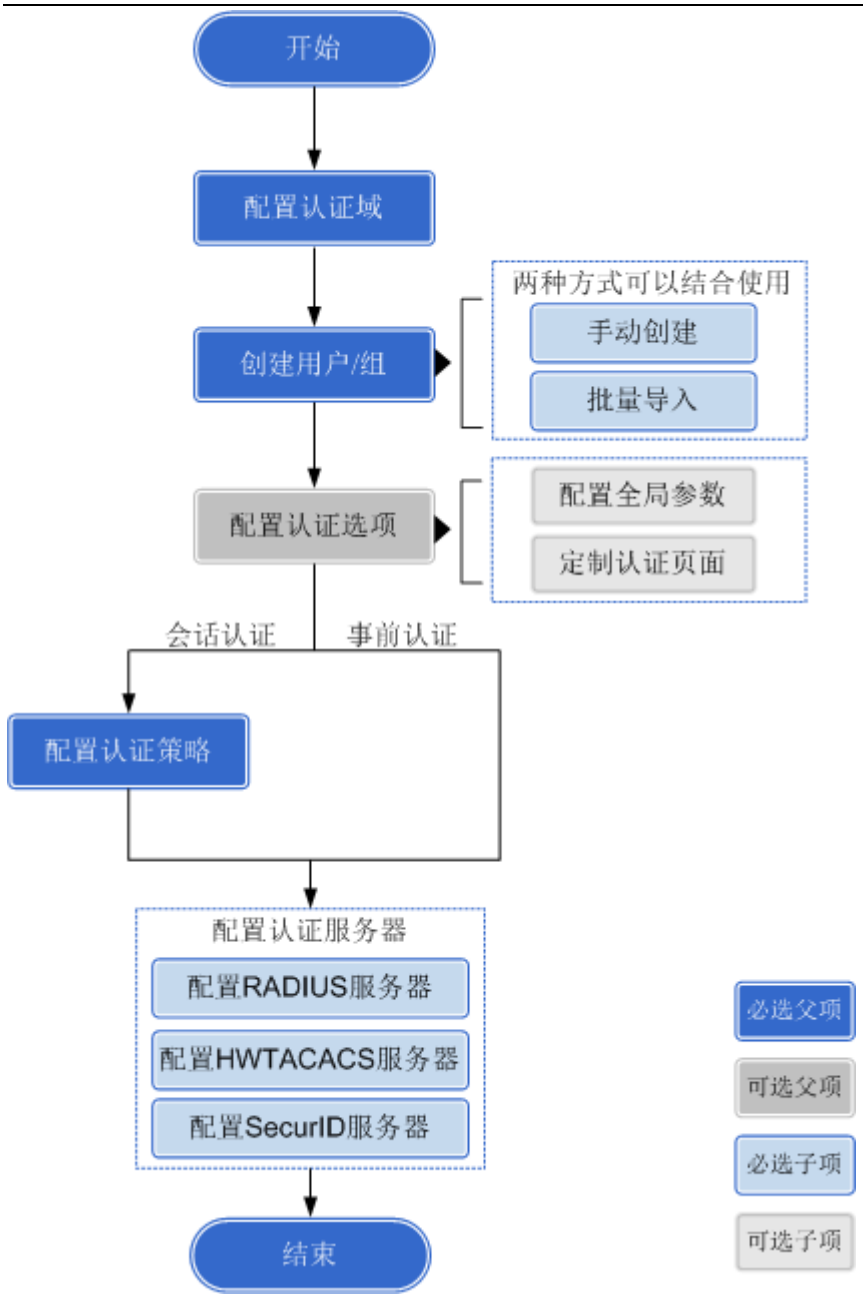
图 4 AD/LDAP 服务器认证配置流程



RADIUS/HWTACACS/SecurID 服务器认证配置流程

使用 RADIUS/HWTACACS/SecurID 服务器认证方式时，需要在 NGFW 上创建用户/组，与服务器上存储的用户信息保持一致，然后根据触发认证的方式来选择配置认证策略。RADIUS/HWTACACS/SecurID 服务器认证配置流程如图 5 所示。

图 5 RADIUS/HWTACACS/SecurID 服务器认证配置流程



配置认证域

通过配置认证域，可以规划用户组织结构并针对不同类型的用户实施不同的认证方式。

背景信息

对于不同认证方式的用户，认证域的作用不尽相同：

- 本地认证/服务器认证用户：决定用户认证时采用本地认证方式还是服务器认证方式，如果是服务器认证方式还包含了使用哪个认证服务器。

- 单点登录用户：单点登录用户的认证过程 NGFW 不参与，只是从认证服务器接收用户登录/注销消息，所以认证域中的认证方式配置对单点登录用户不起作用。但是在与用户域名（dc 字段）同名的认证域中新用户选项的配置对单点登录用户生效。

用户属于哪个认证域是由用户名中携带的“@”后的字符串来决定的。如“user1@bj”属于“bj”认证域，“user2@hz”属于“hz”认证域。如果用户名中没有携带“@”，则属于缺省的 default 认证域。

规划认证域时，管理员可以使用新创建的认证域，也可以使用缺省的 default 认证域。如果使用新创建的认证域，用户登录时需要输入“登录名@认证域名”，且“登录名@认证域名”的总长度不能长于 63 个字符；如果使用缺省的 default 认证域，则用户登录时只需要输入登录名，便于记忆。

通常情况下 default 认证域即可满足需要，以下情况可能需要规划新的认证域：

- 不同的用户采用不同的认证方式或使用不同的认证服务器，此时需要将用户规划到不同的认证域下。
- 如果服务器上存在域的概念，且多个域间的用户还可能重名，此时可以在 NGFW 上创建与服务器上域名同名的认证域以对应服务器上的组织结构。

操作步骤

1. 选择“对象 > 用户 > 认证域”。
2. 单击“新建”。
3. 配置认证域的名称、描述、认证用户/组、接入控制和认证服务器。

参数	说明
名称	输入认证域的名称。
描述	输入认证域的描述信息。 为方便识别认证域的用途，建议输入的描述信息应具有一定的意义。
接入控制	选择认证域的接入控制方式。 • “允许 VPN 接入”表示该认证域可以对接入用户进行认证。 • “允许对用户做基于策略的控制”表示该认证域可以对上网用户进行认证。
关联用户组	选择认证下用户的组织结构。 • 认证域同名组：创建认证域的同时在用户组织结构上将新增与认证域同名的根组，然后在此根组下继续规划用户/组。此选项用于每个认证域的用户账号独立的情况。 • default 组：不产生与认证域同名的根组，新认证域直接使用 default 组的组织结构。如需规划新的用户/组直接在 default 组下规划。

参数	说明
认证服务器	选择认证服务器的类型。 选中该参数，表示使用第三方服务器认证方式；不选中该参数，表示使用本地认证方式。 可以选择已经存在的认证服务器，或者创建认证服务器。

4. 配置认证域的 IP 地址池。

只有认证域的“接入控制”为“允许 VPN 接入”时才需要配置 IP 地址池。

a. 单击“新建”。

b. 配置 IP 地址池的参数。

参数	说明
IP 地址池号	输入 IP 地址池的编号。
起始 IP 地址	输入 IP 地址池的起始地址。
结束 IP 地址	输入 IP 地址池的结束地址。 如果没有输入结束地址，表示 IP 地址池的起始 IP 地址和结束 IP 地址是一样的。

c. 单击“确定”。

5. 配置认证域的新用户认证选项。

对于通过了服务器认证或单点登录，但是在 NGFW 上不存的用户，其权限受新用户选项控制。

说明：

NGFW 上用户的名称中不能包含斜线（/）、逗号（,）、双引号（"）、问号（?）、“@”。如果新用户的名称中包含斜线（/）、逗号（,）、双引号（"）、问号（?）、“@”，则无法添加到 NGFW 的临时组或本地组。

如果认证域关联认证域同名组，首次创建认证域时，认证域下不存在用户组，因此只能将新用户直接添加到域下。如需将新用户加入其他组，请在创建认证域后创建新的用户组并修改认证域的配置。

TSM 单点登录用户属于 default 认证域，因此 TSM 单点登录的新用户选项必须在 default 认证域下配置。

参数	说明
不允许新用户登录	选择该项后，不管认证服务器是否认证通过，NGFW 都不允许新用户登录。
添加到指定的用户组中	选择该项后，新用户认证通过后允许自动添加到指定的组中，并使用该组上网权限。有以下两种配置方式： • 添加到本地已有户组：单击“选择组”后的“选择”选择用户组。

参数	说明
	• 将用户在服务器上的组织结构导入本地（仅限 LDAP、AD、TSM 服务器）：选中“若采用 LDAP、AD 认证或 TSM 单点登录，自动导入服务器上的用户到本地的组织结构中，此时配置的用户组不起作用”，并选择服务器导入策略。NGFW 将根据服务器导入策略自动将用户组织结构导入到本地。 **说明：** 仅 default 认证域支持 TSM 服务器导入策略，供 TSM 单点登录新用户使用。
仅作为临时用户，不添加到本地用户列表中	选择该项后，新用户认证通过后只能作为临时用户，不添加到本地用户列表，但可以享有指定本地用户组的上网权限。 单击“使用该组权限”后的“选择”选择用户组。 另外对于 default 认证域的 TSM 单点登录新用户，还支持优先使用用户在 TSM 服务器上的用户组进行策略管理。选中“优先使用服务器上的用户组进行策略管理”，并选择 TSM 服务器导入策略。选择的导入策略用于获取用户在服务器上的组织结构，如果服务器上的组织结构在本地存在则使用服务器上用户组的上网权限，如果不存在则使用在“使用该组权限”中指定的本地用户组的上网权限。 **说明：** 仅 default 认证域支持“优先使用服务器上的用户组进行策略管理”，且仅支持选择 TSM 服务器导入策略。

6. 单击“确定”。

手动创建用户/组

在 NGFW 上手动创建用户/组，并配置其属性。

背景信息

NGFW 上的用户和组是企业组织结构的体现，在 NGFW 上存储用户和组的主要目的是供策略所引用，实现基于用户的访问控制和权限管理。

说明：

用户的创建、移动、导出都是基于某一个认证域的，不能跨域进行。

创建用户和组时必须遵循如下规定：

- NGFW 上默认存在 default 认证域，可以在其下级创建用户/组，如果需要规划其他认证域的组织结构请先配置认证域。

- 设备最多支持 20 层用户结构，包括认证域和用户，即认证域和用户之间最多允许存在 18 层组。
- 每个组可以包括多个用户和组，但每个组只能属于一个父组。
- 一个用户最多可以属于三个父组。
- 用户和组都可以被策略所引用，如果组被策略引用，则组下的用户继承其父组和所有上级节点的策略。

操作步骤

- 创建组。

  1. 选择“对象 > 用户 > 用户/组”。
  2. 选中需要创建组的认证域，缺省只有 default 认证域。
  3. 在“成员管理”中，单击“新建”，选择“新建组”。
  4. 配置组的参数。

参数	说明
名称	输入组的名称。 组允许重名，但组所在组织结构的全路径必须确保唯一性。例如，/default/research/group1 和/default/marketing/group1 是两个不同的组。
描述	输入组的描述信息。 合理填写描述信息有助于管理员正确理解组的功能，便于查找和维护。
所属组	输入组所属的父组。 单击“选择”，在“组织结构”中选择所属的父组，然后单击“确定”。 每个组只能属于一个父组。

  5. 单击“确定”。

     配置完成后，在“组织结构”中可以查看到新创建的组，在新创建的组所属父组的“成员管理”中可以查看到其信息。

- 创建用户。

  创建用户的方式包括“新建用户”和“批量新建用户”，“新建用户”是指一次只创建一个用户；“批量新建用户”是指一次创建多个用户，创建的多个用户只有登录名不同，其他属性都相同。与“新建用户”不同的是，“批量新建用户”时不能配置显示名和 IP/MAC 地址双向绑定。

  当待创建的多个用户的大部分属性基本相同时，请通过“批量新建用户”完成多个用户共有属性的配置，然后再修改每个用户的特有属性，这样可以减少管理员重复配置的工作量。

1. 选择“对象 > 用户 > 用户/组”。
2. 选中需要创建用户的认证域，缺省只有 default 认证域。

   非 default 域用户登录时必须输入“登录名@认证域名”，例如 test 认证域的用户 user1 登录时需要输入 user1@test。

3. 在“成员管理”中，单击“新建”，选择“新建用户”或者“批量新建用户”。
4. 配置用户的参数。

参数	说明
登录名	输入用户的登录名，即用户进行认证时使用的名称。 同一认证域下的登录名（账号）不允许重名。
显示名	输入用户的显示名。 显示名仅作为区分用户的标识，用户不能使用显示名发起认证请求。为方便记忆和管理，建议采用直观的名字（如员工的真实姓名）作为显示名，不同的用户允许使用相同的显示名。 批量新建用户时不能设置此参数。
描述	输入用户的描述信息。 合理填写描述信息有助于管理员识别用户，便于查找和维护。
所属组	输入用户所属的父组。 单击“选择”，在“组织结构”中选择新建用户所属的父组，单击“确定”。 一个用户最多可以属于三个父组。
认证类型	选择用户的认证类型。 • “本地认证”表示由 NGFW 来认证用户，这种情况下需要在 NGFW 上配置用户的密码。 • “服务器认证”表示由认证服务器来认证用户，这种情况下不需要在 NGFW 上配置用户的密码。
密码	输入用户的密码。 该参数只在“认证类型”为“本地认证”时需要配置。
确认密码	再次输入用户的密码。 该参数只在“认证类型”为“本地认证”时需要配置。
用户属性	
账号过期时间	• 选中“永不过期”，表示账号永远不会过期。 • 选中“在此时间之后过期”，表示账号将在指定的时间之后过期。该时间不能早于 NGFW 当前的系统时间。 账号过期后无法再使用，但是对于已经在线的用户，NGFW 不强制其下线。 账号过期后，如果想将其恢复为有效状态，可以通过延长过期时间或设置为永不过期来实现。
允许多人同时使用该账号登录	不选中该参数，表示同一时刻仅允许账号在一台计算机（IP 地址）上登录。

参数	说明
	如果 NGFW 检测到账号已经在线，则提示账号在其他 IP 上登录，在当前 IP 上登录失败。
IP/MAC 绑定方式	选择用户与 IP/MAC 地址的绑定方式，用来限制用户只能使用特定的 IP/MAC 地址登录。 • “不绑定”表示用户与 IP/MAC 地址不绑定，只要匹配认证策略的计算机（IP 地址）都能使用该账号登录。 • “单向绑定”表示用户只能使用指定的 IP/MAC 地址登录，但同时允许其他用户也使用该 IP/MAC 地址登录。 • “双向绑定”表示用户只能使用指定的 IP/MAC 地址登录，并且其他双向绑定用户不能使用该 IP/MAC 地址登录。 批量新建用户时不能设置“双向绑定”参数。 **说明：** 目前 NGFW 不支持配置用户与 IPv6 地址绑定。
IP/MAC 地址	输入与用户绑定的 IP 地址、MAC 地址或 IP/MAC 地址对。 该参数只在“IP/MAC 绑定方式”为“单向绑定”或“双向绑定”时需要配置。 一个用户最多绑定三个条目。

5. 单击“确定”。

配置完成后，在新创建用户所属父组的“成员管理”中可以查看到该用户的信息。

后续处理

组和用户创建完成后，可以使用如下操作进行调整：

- **添加已有用户**

将已经存在的用户添加到现有的组中。一个用户最多可以被加入到三个父组中，如果某用户加入的父组已达到上限，则该用户无法再加入新父组。

1. 选择“对象 > 用户 > 用户/组”。
2. 在“组织结构”中单击待添加已有用户的组，然后在“成员管理”中，单击“新建”，选择“添加已有用户”。
3. 在“组织结构”中选中已经存在的用户，该用户将会出现在“已选用户”中。
4. 单击“确定”。

- **批量修改**

对于属性相同的多个用户，可以使用批量修改功能修改这些用户的属性，减少重复配置的工作量。批量修改功能只能修改用户的属性，不能用来修改组的属性。

1. 选择“对象 > 用户 > 用户/组”。
2. 在“组织结构”中单击用户所在的组，然后在“成员管理”中，选中所有待修改的用户，单击“批量修改”。
3. 在“批量修改用户”中，选中待修改的属性，然后进行修改。
4. 单击“确定”。

- **移动**

如果组或用户的父组发生变更，可以使用移动功能将用户或组移动到其他组中，以此来调整组织结构。

此外，通过调整“组成员”中的“组路径”，也可以实现移动组的目的。

1. 选择“对象 > 用户 > 用户/组”。
2. 在“组织结构”中单击待移动组或用户所在的组，然后在“成员管理”中，选中所有待移动的组或用户，单击“移动”。
3. 在“组织结构”中，选中目的组，单击“确定”。

   移动时，目的组只能选择一个。

- **激活/去激活**

用户创建完成后，缺省情况下为激活状态。如果需要暂时取消其访问网络资源的权限，在不删除用户的前提下，可以通过设置用户状态为去激活来实现。如果将已经在线的用户的状态设置为去激活，则该在线用户将被强制下线。

1. 选择“对象 > 用户 > 用户/组”。
2. 在“组织结构”中单击待激活/去激活用户所在的组，然后在“成员管理”中，选中待激活用户或取消选中待去激活用户对应的复选框。
3. 单击“确定”。

- **导出**

导出用户/组是指将用户信息以 CSV 文件的格式导出到 NGFW 之外的存储介质上。管理员可以将用户/组导出到 CSV 文件中作为备份，后续也可以将导出的 CSV 文件再导入到设备中，实现批量创建用户/组的需求。如何导入 CSV 文件，请参见手动批量导入用户/组。

说明：

当 NGFW 的 CF 卡剩余空间小于 4MB 时，不允许将用户信息导出到 CSV 文件中。

1. 选择“对象 > 用户 > 用户/组”。
2. 在“组织结构”中单击待导出用户所属的父组或单击待导出的组，然后在“成员管理”中单击“导出”。

   当某个组下没有用户时，此组不支持单独导出。

3. 将以当前组的名称命名的 CSV 文件保存到 NGFW 之外的存储介质（如管理员的 PC）上。

用户信息导出到 CSV 文件中后，密码以密文形式存放。

手动批量导入用户/组

将包含用户/组信息的 CSV 文件导入到 NGFW，批量创建用户/组。

前提条件

导入 CSV 文件前，请先准备指定格式的 CSV 文件。CSV 文件来源有以下途径：

- 使用之前从本 NGFW 或其他 NGFW 上导出的 CSV 文件。如何导出 CSV 文件，请参见手动创建用户/组中的后续处理。
- 从“对象 > 用户 > 用户导入 > 本地导入”中或者“对象 > 用户 > 用户/组 > 成员管理 > 导入”中下载 CSV 文件模板，请仔细阅读 CSV 文件模板中批注文字，然后将用户信息按照格式要求填写到 CSV 文件模板中，如图 1 所示。

说明：

登录名中不能包含斜线（/）、逗号（,）、双引号（"）、问号（?）、“@”，所属组路径中不能包含逗号（,）、双引号（"）、问号（?）。

使用本地认证时，登录名和本地密码为必选项；使用服务器认证时，登录名为必选项。

“所属组路径”的第一级为认证域，例如/default/research 代表 default 认证域下的 research 组。如果需要导入用户到其他认证域下请首先配置认证域。

图 1 CSV 文件格式示意图

登录名	显示名	所属组路径	用户描述	本地密码	绑定地址	绑定模式	是否允许多人同时上网	帐号是否启动	帐号过期时间
user_001	张三	/default/research		password			N	Y	
user_002	李四	/default/marketing		password1			N	Y	

背景信息

NGFW 支持通过导入 CSV 文件的方式批量创建用户/组，在“对象 > 用户 > 用户导入 > 本地导入”中或者“对象 > 用户 > 用户/组 > 成员管理 > 导入”中都可以进行导入操作。在“对象 > 用户 > 用户/组 > 成员管理 > 导入”中，导入操作和当前组没有关系，在任意组的下执行导入操作，效果均相同。

批量导入用户/组时必须遵循如下规定：

- CSV 文件的名称必须以“.csv”作为后缀。
- 在导入过程中，如果当前用户数达到最大限制，则导入中止，但不影响已导入的用户；如果 CSV 文件中某个用户的属性不合法，则从该用户开始的所有用户都无法导入，但不影响已导入的用户。
- CSV 文件导入成功后，用户/组的信息只是导入到内存中，NGFW 重启后数据将丢失，请及时保存配置。
- 在双机热备组网环境下，通过 CSV 文件导入的用户不会从主用设备备份到备用设备，需要分别在主用和备用设备上执行导入操作。

操作步骤

1. 选择“对象 > 用户 > 用户导入 > 本地导入”。

   此处以“对象 > 用户 > 用户导入 > 本地导入”中的导入操作为例进行介绍，内容同样适用于“对象 > 用户 > 用户/组 > 成员管理 > 导入”中的导入操作。

2. 配置导入的参数。

参数	说明
用户导入文件	单击“浏览”，选择已经编辑好的 CSV 文件，单击“打开”，完成 CSV 文件的选择。
自动创建用户组	如果选中复选框，当 CSV 文件中某用户所属组不存在时，NGFW 会自动创建

参数	说明
	该组；如果不选中复选框，当 CSV 文件中某用户所属组不存在时，用户导入失败。
当前用户存在时，覆盖本地用户记录	当用户已经存在时，如果选中复选框，导入时 NGFW 会采用覆盖的方式更新此用户的属性；如果不选中复选框，导入时 NGFW 会跳过此用户。

3. 单击“开始导入”。

   导入完成后，在“组织结构”中可以查看到导入的组，在组的“成员管理”中可以查看到其子组和成员的信息。

从服务器导入用户/组

如果网络中已经部署了 AD、LDAP 或 TSM 服务器，可以将服务器上用户/组的信息导入到 NGFW 上，减少手动创建的工作量。

前提条件

从服务器导入用户/组之前，需要完成以下任务：

- 配置 AD、LDAP 或 TSM 服务器，具体配置方法请参见配置 AD 服务器、配置 LDAP 服务器或配置 TSM 服务器。
- 查看 AD、LDAP 或 TSM 服务器上用户的组织结构信息，确定导入位置和过滤参数。

背景信息

NGFW 支持从 AD、LDAP 和 TSM 服务器导入用户。其中，LDAP 服务器支持 AD 和 Open LDAP 两种类型。

从服务器导入用户/组时必须遵循如下规定：

- 从服务器导入用户到 NGFW，只能导入用户的账号和组织结构，不能导入用户的其他属性。
- 在双机热备组网环境下，从服务器导入的用户不会从主用设备备份到备用设备，需要分别在主用和备用设备上执行导入操作。
- 导入操作只能增加、覆盖用户，不能删除用户。如果在服务器上已经删除了某个用户，那么需要管理员手动在 NGFW 上删除该用户。

注意：

对于 AD/LDAP 服务器导入，NGFW 只支持将服务器用户导入到与服务器上用户域名同名的认证域或 default 认证域（所有认证域共享 default 认证域的用户帐号的情形）下。服务器上的用户域名由 dc 字段决定，例如“dc=cce,dc=com”表示域名是 cce.com 的用户。

如果导入 AD/LDAP 服务器上多个域的用户，建议在 NGFW 上配置多个对应的认证域（关联认证域同名根组）、多个 AD/LDAP 服务器（IP 地址相同、Base DN 不同）、多条服务器导入策略。例如导入“dc=cce1,dc=com ”和“dc=cce2,dc=com ”两个域下的用户，则配置两个名字分别为 cce1.com 和 cce2.com 的认证域、两个 Base DN 分别为“dc=cce1,dc=com”和“dc=cce2,dc=com”的认证服务器、两条服务器导入策略分别导入这两个域的用户。

NGFW 上用户的名称中不能包含斜线（/）、逗号（,）、双引号（"）、问号（?）、“@”，如果服务器上用户的名称中包含上述字符，则该用户不会导入到 NGFW。用户组的名称中不能包含逗号（,）、双引号（"）、问号（?），如果服务器上用户组的名称中包含上述字符以及斜线（/），该组及其所有子节点都不会导入到 NGFW。但 NGFW 与 TSM 服务器对接中，对@字符有特殊处理，即如果 TSM 服务器上的用户的名称中包含@字符，NGFW 将去掉@的内容。例如 abc@test，则该用户导入到 NGFW 后为 abc。

操作步骤

1. 选择“对象 > 用户 > 用户导入 > 服务器导入”。
2. 单击“新建”。
3. 配置 AD、LDAP 或 TSM 服务器导入策略的参数。

参数	说明
名称	输入服务器导入策略的名称。 新创建的服务器导入策略的名称不能与已存在的服务器导入策略的名称相同。
服务器类型	选择服务器的类型。 • “AD”表示 AD 服务器。 • “LDAP”表示 LDAP 服务器。 • “TSM”表示 TSM 服务器。
服务器名称	选择服务器的名称，或者选择“新建”来创建服务器。 此处的服务器定义了 NGFW 与 AD、LDAP 或 TSM 服务器之间通信的参数。
服务器路径	输入从服务器上导入用户/组信息的起始位置，或者单击“选择”，连接到服务器上选择导入用户/组信息的起始位置。必须选择了“服务器名称”后，才能配置该参数。 导入位置由服务器上的域名和用户组名组成。格式为：ou=N 级用户组,……,ou=2 级用户组,ou=1 级用户组,dc=N 级域名,……,dc=2 级域名,dc=1 级

参数	说明
	域名。
导入类型	选择从服务器上导入用户/组的类型，包括： • 导入用户和用户组到本地 表示同时将服务器上的用户和组织结构导入 NGFW。 当 NGFW 需要对服务器中的全部或者大部分用户进行管理，并且按照组织结构配置策略，建议采用这种方式。 • 仅导入用户到本地 表示只将服务器上的用户导入 NGFW，忽略组织结构，导入的所有用户在 NGFW 上都属于同一部门。 当 NGFW 不使用服务器上的组织结构，而是在 NGFW 重新构建组织结构时，建议采用这种方式。 • 仅导入用户组结构到本地 表示只将服务器上的组织结构作为部门导入 NGFW，不导入用户。 当服务器上的用户量太大，而 NGFW 又只管理部分用户时，为避免导入大量无效用户，建议采用这种方式。
导入到用户组	选择导入的用户/组在 NGFW 上的位置。 可以在文本框中直接手工输入，也可以单击“选择”，选择组。 对于 AD/LDAP 导入，该组只能是与服务器上用户域名同名的认证域或 default 认证域（所有认证域共享 default 认证域的用户帐号的情形）下的组。对于 TSM 导入只能是 default 认证域。 **说明：** 对于 TSM 服务器用户导入，不支持将相邻层级用户组同名的用户组织结构导入到 NGFW 上与服务器同名的组下，否则会导致用户层级错误。例如：用户 user1 在 TSM 服务器上的组织结构为/group/group/user1，将 user1 的组织结构导入到 NGFW 的/default/group 组，结果 user1 被导入到/default/group，而不是/default/group/group。
服务器自动同步	选中复选框，表示 NGFW 根据设置的时间间隔，定时从服务器上导入用户/组信息。
当前用户存在时，覆盖本地用户记录	选中复选框，如果 NGFW 已经存在同名用户，则从服务器上导入的用户将覆盖 NGFW 上已经存在的用户，用户的信息以新导入的数据为准。 不选中复选框，如果 NGFW 已经存在同名用户，则跳过该用户，接着导入下一个用户。 **说明：** 只有从第三方认证服务器导入的用户（不区分服务器类型，同时包括通过新用户方式导入的用户）才会互相覆盖，管理员手动创建或者从 CSV 文件导入的用户不会被覆盖。
过滤参数	
用户	输入过滤条件，用来筛选用户，过滤条件使用正则表达式表示。 由于 OU 下除了用户还有很多其他信息，这些信息对 NGFW 来说是没有用的，不需要导入。在执行导入操作时，AD 或 LDAP 服务器会根据该过滤条件搜索满足条件的用户信息，发送给 NGFW。

参数	说明
	该参数仅对于 AD 或 LDAP 类型的服务器生效，建议使用默认值。
用户组	输入过滤条件，用来筛选组，过滤条件使用正则表达式表示。 由于 OU 下除了组还有很多其他信息，这些信息对 NGFW 来说是没有用的，不需要导入。在执行导入操作时，AD 或 LDAP 服务器会根据该过滤条件搜索满足条件的组信息，发送给 NGFW。 该参数仅对于 AD 或 LDAP 类型的服务器生效，建议使用默认值。
用户属性	选择 AD 或 LDAP 服务器中用户的哪个属性作为 NGFW 中用户的登录名。 “sAMAccountName”是 AD 服务器中用户的属性，表示用户的登录名；“cn”是 LDAP 服务器中用户的属性，表示用户的登录名。 该参数仅对于 AD 或 LDAP 类型的服务器生效，建议使用默认值。

4. 单击“确定”。

后续处理

服务器导入策略创建完成后，管理员执行立即导入操作，就能将服务器上的用户/组信息导入 NGFW。如果在服务器导入策略中配置了“服务器自动同步”，NGFW 将按照配置的时间间隔定时从服务器上导入用户/组信息。

配置全局参数

介绍全局参数的配置方法。

背景信息

全局参数的配置包括：

- 设置用户密码的强度、用户首次登录必须修改密码以及密码过期的设置
- 定义用户认证后的跳转页面
- 定义认证界面使用的协议和端口
- 定义用户登录错误次数限制、达到限制次数后的锁定时间以及用户在线超时时间

操作步骤

1. 选择“对象 > 用户 > 认证选项 > 全局配置”。
2. 配置全局的参数。

参数	说明
密码选项设置	
密码强度设置	该配置只适用于用户通过认证页面来修改密码的情况。
首次登录必须修改密码	选中复选框，表示用户在首次登录时必须修改密码。 不选中复选框，表示用户在首次登录时不需要修改密码。 该配置只适用于认证方式为本地认证或者 AD/LDAP 服务器认证的场景。
密码过期设置	• 永不过期 表示密码永远都不过期。 • 过期时间设置 表示密码在指定的时间后过期。同时还可以设置在密码过期前提醒用户的时间，当用户在密码过期提醒时间之内登录后，将会跳转到密码过期提示页面，设备会提示用户需要修改密码。
Portal 认证设置	
启用认证用户登录 URL	设置用户访问 HTTP 业务（80 端口）时重定向的认证页面 URL。如果不指定该参数 NGFW 会以接收到用户 HTTP 请求的接口地址作为认证页面的地址向用户推送内置认证页面，如果指定该参数则使用自定义的 URL 作为认证页面地址。 必须存在用户可访问的提供认证页面的 Portal 服务器，并且 Portal 服务器可以与 NGFW 配合完成认证过程。 例如 TSM 单点登录场景，如果未指定自定义 URL，用户使用 TSM 系统的 Portal 认证页面进行事前认证；如果指定自定义 URL 为 TSM 的 Portal 认证页面，则用户可以直接访问 HTTP 业务，然后 NGFW 向用户推送 TSM 的 Portal 认证页面进行认证，此时注意需要配置认证策略触发会话认证。
其他设置	
认证通过后跳转设置	设置用户认证通过后，在浏览器中显示的页面。该功能对自定义 Portal 认证无效。 • 不跳转 不跳转，浏览器中显示认证页面。用户访问页面时还需要重新使用浏览器来打开。 • 跳转到最近使用的 Web 页面 跳转到最近请求的页面，即用户触发认证时所访问的页面。 • 跳转到自定义 URL 页面 跳转到管理员设置的自定义页面。
认证端口	输入用户进行认证时，设备推送认证界面时使用的端口。
用户登录错误次数限制	输入用户认证失败次数的阈值，当用户连续认证失败次数达到阈值后，该用户将被锁定。 用户连续认证失败次数与 IP 地址无关，即使不同 IP 地址认证失败，次数也会进行累加。例如，配置用户连续认证失败 3 次后锁定用户，如果在三台不同 IP 地址的 PC 连续使用同一用户进行认证一次，均认证失败，则用户总认证失败次数达到 3 次，该用户被锁定。 该配置仅对采用本地认证方式的用户生效。

参数	说明
用户锁定时间	输入用户被锁定的时间。该锁定时间不受系统时间改变和夏令时调整的影响，在锁定时间内，设备不允许被锁定用户进行认证。 该配置仅对采用本地认证方式的用户生效。
在线用户超时时间	输入在线用户的超时时间。 用户认证通过后，在线用户监控表中将产生对应的在线用户监控表项。由于在线用户监控表的存储空间有限，为了防止在线用户监控表项占满存储空间，导致新的用户无法上线，需要为监控表中的在线用户设置合理的超时时间。如果某用户在超时时间内没有发起业务流量，则该用户对应的在线用户监控表项将被删除。当该用户下次再发起业务访问时，需要重新进行认证。 修改在线用户超时时间对已在线用户不生效。

3. 单击“应用”。

配置单点登录

介绍 AD 单点登录和 TSM 单点登录的配置方法。

AD 单点登录（插件方式）

背景信息

插件方式下，管理员需要在 AD 域控制器和 NGFW 上完成如下配置：

- AD 域控制器

  在 AD 域控制器上部署 AD 单点登录服务，接收用户发送的登录/注销消息，然后将消息发送给 NGFW。

  在 AD 域控制器上设置登录脚本和注销脚本，并通过组策略下发，要求用户登录和注销时分别执行登录和注销脚本，将登录/注销信息发送至 AD 域控制器。

- NGFW

  在 NGFW 上配置 AD 单点登录参数，接收 AD 单点登录服务发送的用户登录/注销消息。

说明：

如果 NGFW 部署在用户和 AD 域控制器之间，用户的认证报文经过 NGFW。为实现单点登录功能，配置认证策略时对于该数据流不进行认证。另外，认证报文还需要通过安全策略的安全检查，即管理员需要在 NGFW 上配置

如下安全策略：

- 源安全区域：用户 PC 所在的安全区域。
- 目的安全区域：AD 服务器所在的安全区域。
- 目的地址：AD 服务器的 IP 地址。
- 动作：允许。

当用户通过 AD 域控制器的认证后，如果该用户信息在 NGFW 上存在，则 NGFW 仍会对该用户属性（用户状态、账号过期时间、IP 地址绑定、是否允许多人同时使用该账号登录）进行检查。只有用户属性检查通过的用户，才能访问网络。例如，某用户被管理员冻结，在冻结期内，该用户即使通过了 AD 域控制器认证，也不能访问网络。

AD 单点登录不支持用户名包含$的用户上线。

操作步骤

- 配置 AD 域控制器。
  1. 从 NGFW 的“对象 > 用户 > 认证选项 > 单点登录”中下载 AD 服务器单点登录程序并解压缩。然后在 AD 域控制器上安装 ADSSO_Setup.exe，配置 AD 单点登录服务的运行参数。
  2. 在 AD 域控制器上配置组策略，设置登录（Logon.exe）和注销（Logoff.exe）脚本，然后添加 ReportLogin.exe 脚本文件，并配置脚本参数。ReportLogin.exe 脚本文件请从 ADSSO_Setup.exe 的安装路径下 Script 文件夹中获取。详细的配置请参见举例：上网用户+AD 单点登录（插件方式）。
- 配置 NGFW。
  1. 选择“对象 > 用户 > 认证选项 > 单点登录”，选中“AD 单点登录”。
  2. 选择获取登录信息方式为“通过执行安装到 AD 服务器的程序”。
  3. 配置 NGFW 与 AD 域控制器通讯时报文加密的共享密钥。

     共享密钥必须与在 AD 域控制器上安装 ADSSO_Setup.exe 时配置的“设备共享密钥”保持一致。
  4. 单击“应用”。

AD 单点登录（免插件方式）

背景信息

免插件方式下，无需在 AD 服务器上安装程序。NGFW 通过监控访问者登录 AD 服务器（AD 域控制器）的认证报文获取认证结果，如果认证成功将用户和 IP 对应关系添加到在线用户表。

说明：

免插件方式下，NGFW 无法获取用户的注销消息，因此用户只能根据在线用户超时时间下线。

如果 NGFW 部署在用户和 AD 域控制器之间，用户的认证报文经过 NGFW。为实现单点登录功能，配置认证策略时对于该数据流不进行认证。另外，认证报文还需要通过安全策略的安全检查，即管理员需要在 NGFW 上配置如下安全策略：

- 源安全区域：用户 PC 所在的安全区域。
- 目的安全区域：AD 服务器所在的安全区域。
- 目的地址：AD 服务器的 IP 地址。
- 动作：允许。

当用户通过 AD 域控制器的认证后，如果该用户信息在 NGFW 上存在，则 NGFW 仍会对该用户属性（用户状态、账号过期时间、IP 地址绑定、是否允许多人同时使用该账号登录）进行检查。只有用户属性检查通过的用户，才能访问网络。例如，某用户被管理员冻结，在冻结期内，该用户即使通过了 AD 域控制器认证，也不能访问网络。

AD 单点登录不支持用户名包含$的用户上线。

操作步骤

1. 选择“对象 > 用户 > 认证选项 > 单点登录”，选中“AD 单点登录”。
2. 选择获取登录信息方式为“通过监控 AD 服务器登录域的 IP/端口”。
3. **可选：**当用户访问 AD 服务器的认证报文未经过 NGFW 时，选择“将认证报文镜像到防火墙”并指定镜像接口。

   镜像接口必须使用独立的二层接口且不能与其他业务口共用。“镜像接口”下拉列表中只显示二层接口，如果不存在二层接口需要到“网络 > 接口”中将某个三层接口切换为交换模式作为镜像接口。

4. 指定需要监控的 AD 服务器的 IP 地址和认证报文端口。

   端口需要与 AD 服务器保持一致，一般情况下 AD 服务器使用 UDP 88 端口发送 AD 认证结果报文。因此该参数一般配置为“*ip-address*:88”。

5. 单击“应用”。

TSM 单点登录

背景信息

为了实现 TSM（Policy Center）单点登录，管理员需要在 NGFW 和 TSM 控制器（即安全控制器）上完成如下配置：

- TSM 控制器

  在 TSM 控制器配置与 NGFW 的通信参数，将用户登录/注销消息发送给 NGFW。

- NGFW

  在 NGFW 上配置 TSM 服务器以及 TSM 单点登录参数，接收 TSM 控制器发送的用户登录/注销消息。

说明：

如果 NGFW 部署在用户和 TSM 控制器之间，用户的认证报文经过 NGFW。为实现单点登录功能，配置认证策略时对于该数据流不进行认证。另外，认证报文还需要通过安全策略的安全检查，即管理员需要在 NGFW 上配置如下安全策略：

- 源安全区域：用户 PC 所在的安全区域。
- 目的安全区域：TSM 控制器所在的安全区域。
- 目的地址：TSM 控制器的 IP 地址。
- 动作：允许。

当用户通过 TSM 的认证后，如果该用户信息在 NGFW 上存在，则 NGFW 仍会对该用户属性（用户状态、账号过期时间、IP 地址绑定、是否允许多人同时使用该账号登录）进行检查。只有用户属性检查通过的用户，才能访问网络。例如，某用户被管理员冻结，在冻结期内，该用户即使通过了 TSM 认证，也不能访问网络。

操作步骤

- 配置 TSM 控制器。

  此处以 Policy Center V100R003C00 版本为例进行介绍，不同版本界面可能会不同，请参考 Policy Center 版本对应的产品文档。

1. 选择“系统配置 > 服务器配置 > 上网行为管理设备配置”。
2. 单击“增加”。
3. 配置 NGFW 的参数。

参数	说明
IP 地址	输入 TSM 控制器发送用户登录/注销消息的目的 IP 地址。
端口	输入 TSM 控制器发送用户登录/注销消息的目的端口。
接入密码	输入 TSM 控制器与 NGFW 通讯时报文加密的密码。
终端 IP 地址列表	输入需要进行上网行为管理的终端用户 IP 地址或网段。TSM 控制器只会发送属于该列表的用户登录/注销消息给 NGFW。
描述	输入 TSM 控制器上对 NGFW 的描述信息。

4. 单击“确定”。

- 配置 NGFW。

1. 配置 TSM 服务器。

   具体配置请参见配置 TSM 服务器，其中“共享密钥”必须与 TSM 控制器上设置的密码一致。

2. 选择“对象 > 用户 > 认证选项 > 单点登录”，选中“TSM 单点登录”。
3. 配置 TSM 单点登录参数。
   - TSM 身份认证通过后允许用户上网：身份已经被 TSM 识别出来，但未通过安全检查的用户就可以上网。
   - TSM 安全检查通过后允许用户上网：不仅身份已经被 TSM 识别出来，还通过安全检查的用户才可以上网。
4. 单击“应用”。

定制认证页面

介绍认证页面的定制方法。

背景信息

认证页面可以根据实际情况，设置 Logo 图片、背景图片、欢迎语或求助语，满足个性化的页面定制需求。

操作步骤

1. 选择“对象 > 用户 > 认证选项 > 页面定制”。
2. 配置页面定制的参数。

   在配置的过程中，管理员可以单击“预览”来查看显示效果。

参数	说明
Logo	单击“浏览”，选择 Logo 图形文件，单击“上传”。
背景	单击“浏览”，选择背景图形文件，单击“上传”。
欢迎语	输入认证页面的欢迎语。
用户求助	输入认证页面的求助语。

3. 单击“应用”。

配置认证策略

上网用户或已经接入 NGFW 的接入用户使用会话认证方式触发认证过程时，必须经过认证策略的处理。

背景信息

认证策略是多条认证策略规则的集合，NGFW 匹配报文时总是在多条规则之间进行，从上往下进行匹配。当报文的属性和某条规则的所有条件匹配时，认为匹配该条规则成功，就不会再匹配后续的规则。如果所有规则都没有匹配到，则按照缺省认证策略进行处理。

NGFW 上存在一条缺省的认证策略，所有匹配条件均为任意（any），动作为不认证。

操作步骤

1. 选择“策略 > 认证策略”。
2. 单击“新建”。
3. 配置认证策略的名称和描述信息。

参数	说明
名称	输入认证策略的名称。 输入的名称不能与已经存在的认证策略名称相同。

参数	说明
描述	输入认证策略的描述信息。 为方便识别认证策略的用途，建议输入的描述信息应具有一定的意义。

4. 配置认证策略的匹配条件。

各个匹配条件之间是“与”的关系，报文的属性与各个条件必须全部匹配，才认为该报文匹配这条规则。而同一个匹配条件中的多个信息之间是“或”的关系，报文的属性只要匹配了其中的一个信息，就认为报文的属性匹配了这个条件。

配置多条认证策略规则时，请先配置条件精确的规则，再配置条件宽泛的规则，即保证条件精确的规则位于条件宽泛的规则之上。

参数	说明
源安全区域	配置认证策略的源安全区域。
目的安全区域	配置认证策略的目的安全区域。
源地址/地区	配置认证策略的源地址，可以手动输入地址或者从下拉列表中选择已有的地址对象。 源地址包括如下两类： • 地址和地址组：管理员可以指定一个单独的 IP/MAC 地址或者一个连续的 IP 网段，还可以通过地址组来划定不连续的或者是不方便通过掩码指定的连续的 IP 地址范围、MAC 地址集合。具体请参见地址和地址组。 • 地区和地区组：管理员可以通过指定地区或地址地区组，将某些地区的 IP 地址作为策略的匹配条件。具体参见地区和地区组。 下拉列表中的地址对象包含如下几类： • 图标代表地址。 • 图标代表地址组。 • 或国旗图标代表地区，先显示自定义地区再显示预定义地区。地区相当于以地区为单位的 IP 地址集合。 • 图标代表地区组。 **说明：** 当使用 MAC 地址作为策略匹配条件时，需注意： • 如果 NGFW 与内网之间直连或通过二层交换机相连，可以直接以 MAC 地址作为匹配条件。 • 如果 NGFW 与内网之间通过三层网络设备相连，首先需要配置 NGFW 的跨三层 MAC 识别功能，再以 MAC 地址作为匹配条件。有关跨三层 MAC 识别功能的介绍，请参见跨三层 MAC 识别。
目的地址/地区	配置认证策略的目的地址，可以手动输入地址或者从下拉列表中选择已有的地址对象。下拉列表中的地址对象类型与源地址相同。

5. 配置认证策略的动作。

参数	说明
认证动作	选择认证策略的认证动作。

6. 单击“确定”。

配置 RADIUS 服务器

第三方认证服务器为 RADIUS 时，请配置 RADIUS 服务器。

背景信息

在使用 RADIUS 服务器对用户进行服务器认证的场景中，NGFW 作为 RADIUS 服务器的代理客户端，将用户名和密码发送给 RADIUS 服务器进行认证。为了保证 NGFW 和 RADIUS 服务器之间正常通信，需要在 NGFW 上配置与 RADIUS 服务器通信时使用的一系列参数。

操作步骤

1. 选择“对象 > 认证服务器 > RADIUS”。
2. 单击“新建”。
3. 配置 RADIUS 服务器的参数。

说明：

在 NGFW 上配置的参数必须与 RADIUS 服务器上的参数保持一致。

参数	说明
名称	输入 RADIUS 服务器的名称。 新创建的 RADIUS 服务器的名称不能与已存在的 RADIUS 服务器名称相同。
共享密钥	输入 NGFW 与 RADIUS 服务器通信时使用的共享密钥。 NGFW 与 RADIUS 服务器使用该密钥对传输的报文进行加密。
认证主服务器 IP/端口	输入提供认证服务的主用 RADIUS 服务器的 IP 地址和端口号。 一般情况下，RADIUS 服务器提供认证服务时使用的端口号为 1812。
认证从服务器 IP/端口	输入提供认证服务的备用 RADIUS 服务器的 IP 地址和端口号。 NGFW 会优先使用主用 RADIUS 服务器，当主用 RADIUS 服务器不可达时，才会使用备用 RADIUS 服务器。
计费主服务器 IP/端口	输入提供计费服务的主用 RADIUS 服务器的 IP 地址和端口号。 一般情况下，RADIUS 服务器提供计费服务时使用的端口号为 1813。

参数	说明
计费从服务器 IP/端口	输入提供计费服务的备用 RADIUS 服务器的 IP 地址和端口号。 NGFW 会优先使用主用 RADIUS 服务器，当主用 RADIUS 服务器不可达时，才会使用备用 RADIUS 服务器。
高级选项	
重传次数	选择 NGFW 发送请求报文的重传次数。 NGFW 向 RADIUS 服务器发出请求报文后，如果在“应答超时时间”内未得到 RADIUS 服务器发回的应答，NGFW 需重传请求报文。重传次数超该值后，NGFW 认为 RADIUS 服务器已不能正常工作。
单位	选择 RADIUS 服务器计费时的流量单位。 • Byte：以字节作为流量的单位。 • KB：以千字节作为流量的单位。 • MB：以兆（Mega）字节作为流量的单位。 • GB：以吉（Giga）字节作为流量的单位。
应答超时时间	选择 NGFW 等待 RADIUS 服务器应答的超时时间。 为判断某个 RADIUS 服务器是否失效，NGFW 会向 RADIUS 服务器周期性地发送请求报文，如果在该时间内未得到 RADIUS 服务器发回的应答，需重传请求报文。
服务器类型	选择 RADIUS 服务器使用的协议版本。 • 标准：表示标准的 RADIUS 协议。 • Portal：表示 Portal RADIUS 协议（也称为 RADIUS+，V1.1）。
NAS-Port 端口类型	选择 RADIUS 服务器的 NAS 端口类型。 • 旧：端口形式为槽位号（12 位）+端口号（8 位）+VLAN ID（12 位）。 • 新：端口形式为槽位号（8 位）+子槽位号（4 位）+端口号（8 位）+VLAN ID（12 位）。
NAS-Port-Id 端口类型	选择 RADIUS 服务器的 NAS 端口 ID 形式。 • 旧：对于以太网接入用户，NAS 端口 ID 形式为端口号（两个字符）＋子槽号（两个字节）＋卡号（三个字节）＋VLANID（9 个字符）；对于 ADSL 接入用户，NAS 端口 ID 形式为：端口号（两个字符）＋子槽号（两个字节）＋卡号（三个字节）＋VPI（8 个字符）＋VCI（16 个字符），字节数不够的，在前面补零。 • 新：对于以太网接入用户，NAS 端口 ID 形式为“slot＝XX；subslot＝XX；port＝XXX；VLANID＝XXXX；”，其中，slot 取值范围是 0～15，subslot 取值范围是 0～15，port 取值范围是 0～255，VLANID 取值范围是 0～4095；对于 ADSL 接入用户，NAS 端口 ID 形式为“slot＝XX；subslot＝X；port＝X；VPI＝XXX；VCI＝XXXXX；”其中，slot 取值范围是 0～15，subslot 取值范围是 0～9，port 取值范围是 0～9，VPI 取值范围是 0～255，VCI 取值范围是 0～65535。
用户名格式	选中复选框，表示 NGFW 发送给 RADIUS 服务器的用户名中包含认证域的名称；不选中复选框，表示 NGFW 发送给 RADIUS 服务器的用户名中不包含认证域的名称。

参数	说明
	用户名通常采用“纯用户名@认证域名”的格式。如果 RADIUS 服务器不接受携带认证域的用户名，可以配置将用户名中的认证域去除后再发送给 RADIUS 服务器。

4. 单击“检测”，在弹出的窗口中单击“确认”，然后输入测试账号及密码。单击“开始检测”，检测 RADIUS 服务器的连通性。

说明：

用于测试服务器连通性的用户名和密码可以为任意值，不需要与服务器端保持一致。

检测结果及其处理建议如下表所示。

输出信息	处理建议
服务器检测成功。	正常运行信息，无需处理。
服务器检测失败，请检查配置。	服务器检测失败，请检查 NGFW 上配置的 RADIUS 服务器参数是否正确。
服务器连接失败。	服务器连接失败，请检查 NGFW 与 RADIUS 服务器的物理连通是否正常、路由是否可达、NGFW 上设置的 RADIUS 服务器的 IP 地址和端口是否正确。
正在检测另外一个服务器，请稍等。	NGFW 正在检测另外一个 RADIUS 服务器的连通性，请稍后再试，确保同一时间 NGFW 只与一个 RADIUS 服务器进行连通性测试。

RADIUS 服务器连通性检测成功后，请单击“取消”。

5. 单击“确定”。

配置 TSM 服务器

TSM 单点登录场景中，需要配置 TSM 服务器。

背景信息

在 TSM 单点登录的场景中，为了将 TSM 服务器上的用户信息导入到 NGFW，需要在 NGFW 上配置与 TSM 服务器通信时使用的一系列参数。

操作步骤

1. 选择“对象 > 认证服务器 > TSM”。

2. 单击“新建”。

3. 配置 TSM 服务器的参数。

说明：

在 NGFW 上配置的参数必须与 TSM 服务器上的参数保持一致。

参数	说明
服务器名称	输入 TSM 服务器的名称。
TSM 控制器 IP 地址	输入 TSM 控制器的 IP 地址。 最多能够配置 20 个 IP 地址，NGFW 会按照配置顺序从上到下连接直到成功为止。
服务器端口	输入提供认证服务的 TSM 服务器的端口号。
加密算法	指定 NGFW 与 TSM 服务器通信时采用 3DES 或 AES128 算法对传输的报文进行加密。 **说明：** 不同 TSM（Policy Center）版本，支持的加密方式可能不一致。配置前，请确认对应的 TSM 版本是否支持该加密方式，确保两端配置的加密方式一致。
共享密钥	输入 NGFW 与 TSM 服务器通信时使用的共享密钥。 NGFW 与 TSM 服务器使用该共享密钥对传输的报文进行加密。

4. 单击“检测”，在弹出的窗口中单击“确定”，测试 NGFW 与 TSM 服务器的连通性。

监控

管理员可以查看到已经通过认证的在线用户，并进行强制注销、全部强制注销、冻结和解冻操作。

查看在线用户

如果需要了解当前已经通过认证的所有用户，可以查看在线用户功能。

1. 选择“对象 > 用户 > 在线用户”。

2. 定位待查看的在线用户。

   管理员可以使用以下方式定位待查看的在线用户。

   - 在“组织结构”中单击待查看用户所属的组，属于该组的所有在线用户将会出现在“在线用户列表”中。

- 使用简单查询或高级查询功能查找待查看的用户，查找结果将会出现在“在线用户列表”中。

3. 在“在线用户列表”中查看在线用户的信息。

参数	说明
登录名(显示名)	在线用户的登录名（显示名），其中“（显示名）”仅在该用户存在显示名时出现。 例如，“t0001（tom）”，其中“t0001”表示用户的登录名，“tom”表示用户的显示名。
所属组	在线用户所属的组。
IP 地址	在线用户登录时所用的 IP 地址。
认证方式	在线用户的认证方式，可能的取值为： • 不认证 • 本地认证 • AD 服务器认证 • LDAP 服务器认证 • HWTACACS 服务器认证 • RADIUS 服务器认证 • SecurID 服务器认证 • 单点登录
接入方式	在线用户的接入方式，可能的取值为： • 本地 • PPP • SSL VPN • IPSec VPN
登录时间/冻结时间	在线用户的登录时间或冻结时间，其中冻结时间以红色字体表示。
在线时长/解冻剩余时间	在线用户的在线时长或被冻结用户的解冻剩余时间，其中解冻剩余时间以红色字体表示。
流量(KB)	在线用户的总流量。单击该列标题，可进行用户流量排序，支持升序和降序。

强制注销在线用户

在线用户被强制注销后，如果需要再次访问网络资源，则必须重新进行认证。

当同一个用户使用多个 IP 地址登录时，如果强制注销其中使用某个指定 IP 地址登录的用户，则使用其他 IP 地址登录的用户不受影响。

1. 选择“对象 > 用户 > 在线用户”。

2. 定位待注销的在线用户。

管理员可以使用以下方式定位待注销的在线用户。

- 在“组织结构”中单击待注销用户所属的组，属于该组的所有在线用户将会出现在“在线用户列表”中。
- 使用简单查询或高级查询功能查找待注销的用户，查找结果将会出现在“在线用户列表”中。

3. 在“在线用户列表”中选中所有待注销的用户，单击“强制注销”。

如果操作成功，已经被注销的用户将不会出现在“在线用户列表”中。

强制注销全部在线用户

强制注销在线用户操作只能注销指定的在线用户，如果需要注销所有的在线用户，可以使用强制注销全部在线用户功能。

1. 选择“对象 > 用户 > 在线用户”。
2. 在“在线用户列表”中单击“全部强制注销”。

如果操作成功，所有在线用户将不会出现在“在线用户列表”中。

冻结在线用户

如果需要临时取消某个在线用户访问网络资源的权限，可以使用冻结在线用户功能。

1. 选择“对象 > 用户 > 在线用户”。
2. 定位待冻结的在线用户。

管理员可以使用以下方式定位待冻结的在线用户。

- 在“组织结构”中单击待冻结用户所属的组，属于该组的所有在线用户将会出现在“在线用户列表”中。
- 使用简单查询或高级查询功能查找待冻结的用户，查找结果将会出现在“在线用户列表”中。

3. 在“在线用户列表”中选中所有待冻结的用户，单击“冻结”。
4. 输入冻结时间，单击“确定”。

如果操作成功，已经被冻结的在线用户对应的“登录时间/冻结时间”将以红色字体显示冻结及被冻结时间。

在线用户被冻结后，不能访问网络资源，不能自行注销，也不能重新发起用户认证申请。等待冻结时间到期或者被管理员解冻后，如果该在线用户的在线超时时间未到期，则可以继续访问网络资源，否则需要重新认证通过后才能访问网络资源。

解冻在线用户

如果需要重新开放已经被冻结的用户访问网络资源的权限，可以使用解冻在线用户功能。

1. 选择“对象 > 用户 > 在线用户”。
2. 定位待解冻的在线用户。

   管理员可以使用以下方式定位待解冻的在线用户。

   - 在“组织结构”中单击待解冻用户所属的组，属于该组的所有在线用户将会出现在“在线用户列表”中。
   - 使用简单查询或高级查询功能查找待解冻的用户，查找结果将会出现在“在线用户列表”中。
3. 在“在线用户列表”中选中所有待解冻的用户，单击“解冻”。

   如果操作成功，已经被解冻的在线用户对应的“登录时间/冻结时间”不会出现红色字体显示冻结及被冻结时间。

在线用户被管理员解冻后，如果该在线用户的在线超时时间未到期，则可以继续访问网络资源，否则需要重新认证通过后才能访问网络资源。

举例：上网用户+本地认证

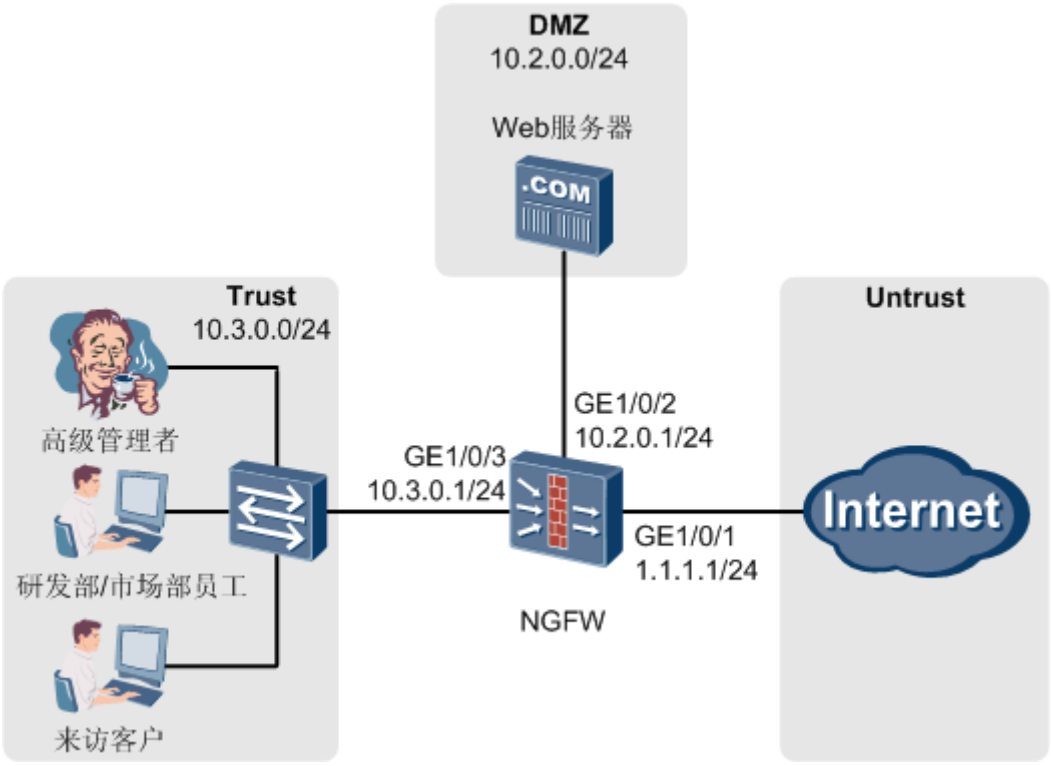
介绍了 NGFW 作为企业的出口网关时，对上网用户进行管理和认证的举例。

组网需求

如图 1 所示，某企业在网络边界处部署了 NGFW 作为出口网关，连接内部网络与 Internet。

企业内部网络中的访问者角色包括高级管理者、研发部员工、市场部员工和来访客户。其中，高级管理者使用固定的 IP 地址 10.3.0.2；研发部员工、市场部员工和来访客户动态获取 IP 地址。

图 1 上网用户+本地认证组网图



企业的网络管理员希望利用 NGFW 提供的用户管理与认证机制，将内部网络中的 IP 地址识别为用户，为实现基于用户的网络行为控制和网络权限分配提供基础。具体需求如下：

- 在 NGFW 上存储用户和部门的信息，体现公司的组织结构，供策略引用。
- 对于高级管理者，为了提高其办公效率，要求省略认证过程。同时为了保证安全，将该用户与 IP 地址和 MAC 地址双向绑定，要求其只能使用指定的 IP 和 MAC 地址访问网络资源。
- 研发部员工和市场部员工访问网络资源之前必须通过 NGFW 的认证。
- 对于来访客户，访问网络资源之前必须通过 NGFW 的认证，并且只能使用特定的用户 Guest 来进行认证。
- 访问者使用会话认证的方式来触发认证过程，即访问者使用 IE 浏览器访问某个 Web 页面，NGFW 会将 IE 浏览器重定向到认证页面。认证通过后，IE 浏览器的界面会自动跳转到先前访问的 Web 页面。

配置思路

说明：

本举例只介绍配置用户与认证相关的内容。

1. 创建组和用户，同时设置用户的密码。针对高级管理者，还需要配置用户与 IP/MAC 双向绑定。
2. 创建认证策略，配置匹配条件和认证动作。其中，对于高级管理者不进行认证；对于研发部员工、市场部员工和来访客户进行认证。
3. 配置 default 认证域，认证域中包括研发部员工、市场部员工和来访客户，并将接入控制设置为“允许对用户做基于策略的控制”。
4. 配置安全策略，允许访问者访问认证页面。如果用户与 DNS 服务器交互的 DNS 业务报文经过 NGFW 转发，还需要配置安全策略，允许 DNS 业务报文通过。

数据规划

项目	数据	说明
高级管理者	**组** • 组名：manager • 所属组：/default **用户** • 登录名：user_0001 • 显示名：高级管理者 A • 所属组：/default/manager • 认证类型：服务器认证 • 不允许多人同时使用该账号登录 • IP/MAC 绑定方式：双向绑定 • IP/MAC 地址：10.3.0.2/aaaa-bbbb-cccc • 账号过期时间：永不过期	将高级管理者规划到“manager”组中，并配置用户与 IP/MAC 双向绑定。“认证类型”选择“服务器认证”，是因为高级管理者的密码不需要设置，NGFW 通过用户与 IP/MAC 双向绑定管理来对高级管理者进行认证。 此处只给出了一个用户的创建过程作为示例，请根据实际情况创建多个用户。
研发部员工	**组** • 组名：research • 所属组：/default **用户** • 登录名：user_0002 • 显示名：研发部员工 B • 所属组：/default/research • 认证类型：本地认证 • 密码/确认密码：Admin@123 • 不允许多人同时使用该账号登录 • IP/MAC 绑定方式：不绑定	将研发部员工规划到“research”组中。 此处只给出了一个用户的创建过程作为示例，请根据实际情况创建多个用户。

项目	数据	说明
	• 账号过期时间：永不过期	
市场部员工	**组** • 组名：marketing • 所属组：/default **用户** • 登录名：user_0003 • 显示名：市场部员工 C • 所属组：/default/marketing • 认证类型：本地认证 • 密码/确认密码：Admin@123 • 不允许多人同时使用该账号登录 • IP/MAC 绑定方式：不绑定 • 账号过期时间：永不过期	将市场部员工规划到“marketing”组中。 此处只给出了一个用户的创建过程作为示例，请根据实际情况创建多个用户。
来访客户	**组** 组名：/default **用户** • 登录名：guest • 显示名：来访客户 • 所属组：/default • 认证类型：本地认证 • 密码/确认密码：Admin@123 • 允许多人同时使用该账号登录 • IP/MAC 绑定方式：不绑定 • 账号过期时间：永不过期	所有来访客户都使用“guest”用户来进行认证，该用户允许多人同时登录。
高级管理者的认证策略	• 名称：policy_auth_01 • 源安全区域：Trust • 目的安全区域：any • 源地址/地区：10.3.0.2/32 • 目的地址/地区：any • 认证动作：不认证	对匹配条件的高级管理者不进行认证，NGFW 通过用户与 IP/MAC 的绑定关系即可识别出用户。 高级管理者无需输入用户和密码就可以访问网络资源，不会影响体验。
研发部员工、市场部员工和来访客户的认证策略	• 名称：policy_auth_02 • 源安全区域：Trust • 目的安全区域：any • 目的地址/地区：any • 认证动作：认证	对匹配条件的研发部员工、市场部员工和来访客户进行认证。 研发部员工、市场部员工和来访客户必须通过 NGFW 的认证后才能访问网络资源。
认证域	• 名称：default	使用缺省的 default 认证域来进行认证，研发部员工、市场部员工和来访客户在认证时

项目	数据	说明
	• 接入控制：允许对用户做基于策略的控制	输入的用户名无需携带认证域，便于记忆。
安全策略	• 名称：policy_sec_1 • 源安全区域：trust • 目的安全区域：local • 动作：允许	配置安全策略，允许访问者访问认证页面。
	• 名称：policy_sec_2 • 源安全区域：trust • 目的安全区域：untrust • 服务：dns • 动作：允许	配置安全策略，允许 DNS 业务报文通过。

操作步骤

1. 创建高级管理者对应的组和用户。

   a. 选择“对象 > 用户 > 用户/组”。

   b. 选中“default”认证域。

   c. 在“成员管理”中，单击“新建”，选择“新建组”，按如下参数配置。

组名	manager
所属组	/default

   d. 单击“确定”。

   e. 在“成员管理”中，单击“新建”，选择“新建用户”，按如下参数配置。

f. 单击“确定”。

2. 创建研发部员工对应的组和用户。

a. 选择“对象 > 用户 > 用户/组”。

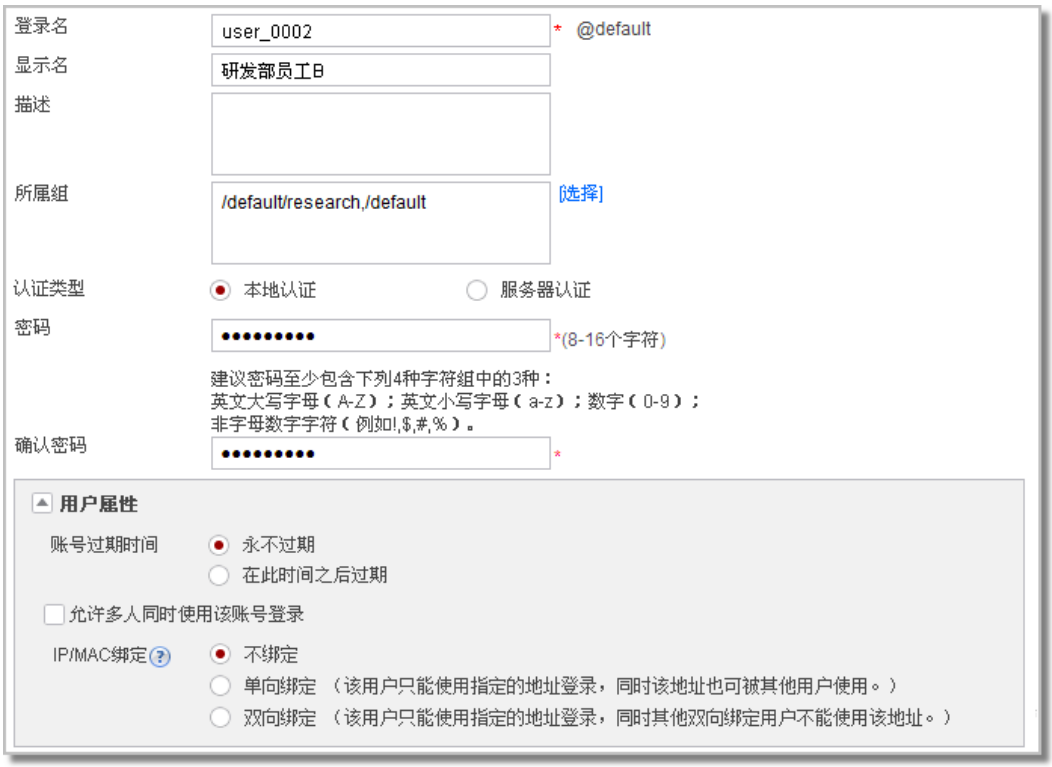
b. 选中“default”认证域。

c. 在“成员管理”中，单击“新建”，选择“新建组”，按如下参数配置。

组名	research
所属组	/default

d. 单击“确定”。

e. 在“成员管理”中，单击“新建”，选择“新建用户”，按如下参数配置。



f. 单击“确定”。

3. 创建市场部员工对应的组和用户。

a. 选择“对象 > 用户 > 用户/组”。

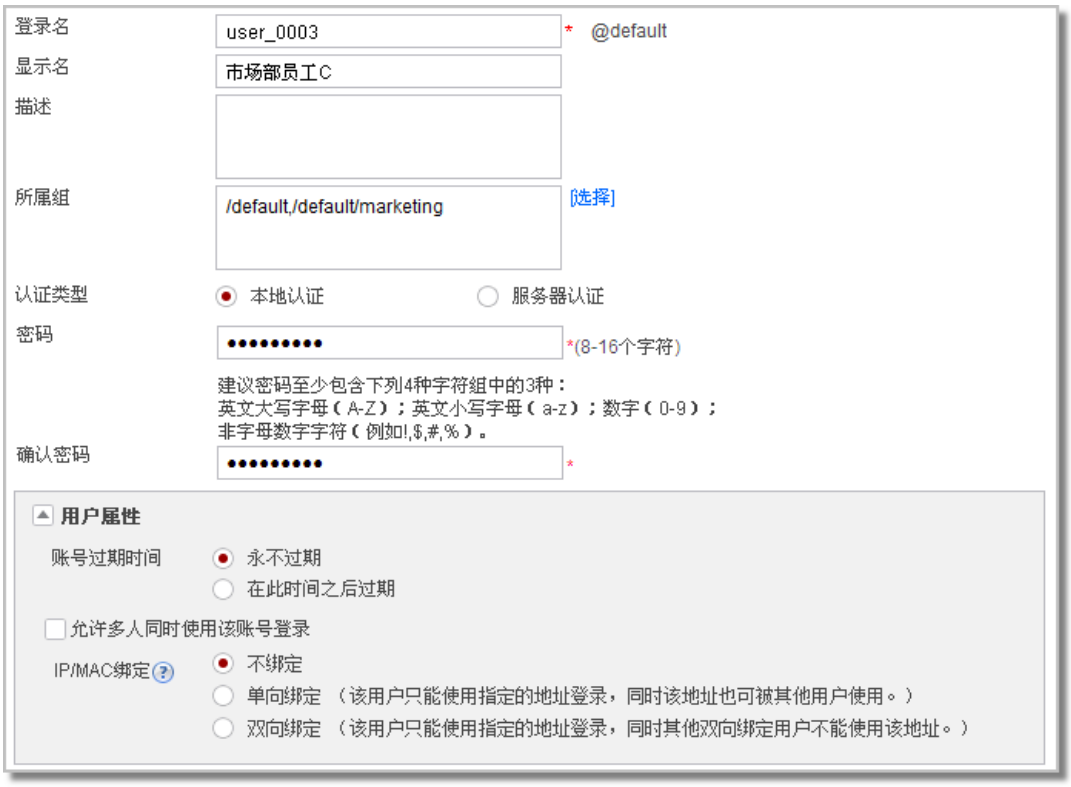
b. 选中“default”认证域。

c. 在“成员管理”中，单击“新建”，选择“新建组”，按如下参数配置。

组名	marketing
所属组	/default

d. 单击“确定”。

e. 在“成员管理”中，单击“新建”，选择“新建用户”，按如下参数配置。



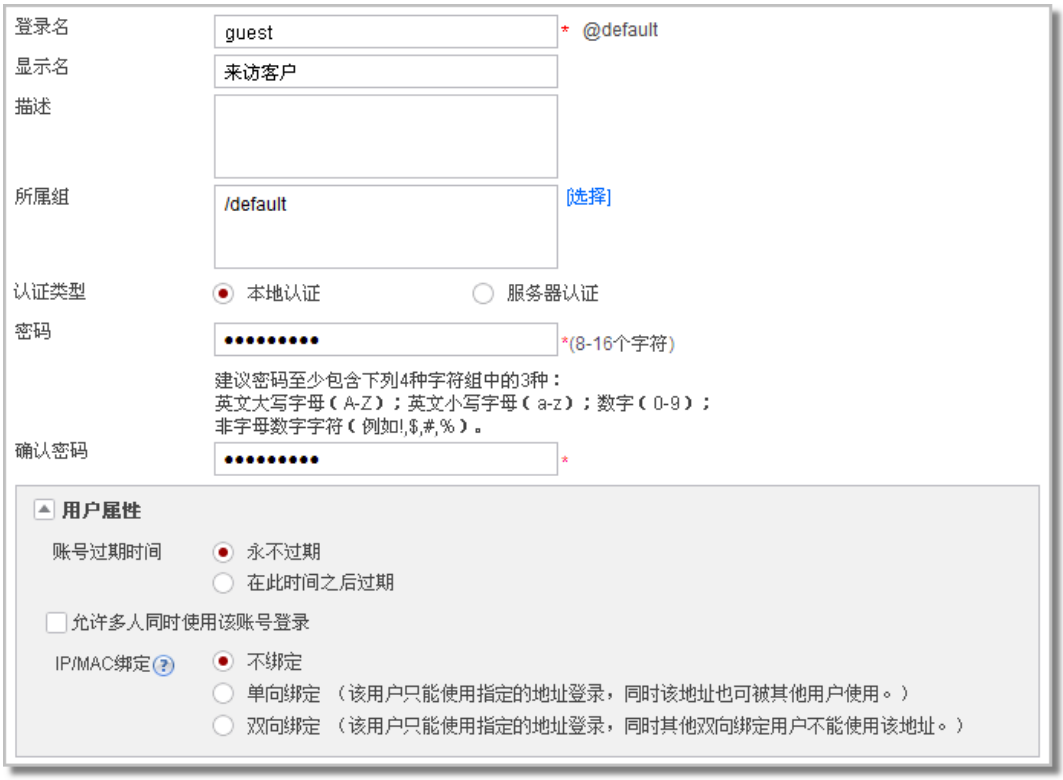
f. 单击“确定”。

4. 创建来访客户对应的用户。

a. 选择“对象 > 用户 > 用户/组”。

b. 选中“default”认证域。

c. 在“成员管理”中，单击“新建”，选择“新建用户”，按如下参数配置。



d. 单击“确定”。

5. 配置认证选项。

a. 选择“对象 > 用户 > 认证选项”。

b. 在“全局配置”中，按如下参数配置。

认证通过后跳转设置	跳转到最近使用的 Web 页面

c. 单击“应用”。

6. 配置认证策略。

a. 选择“策略 > 认证策略”。

b. 单击“新建”，按如下参数配置。

名称	policy_auth_01
源安全区域	trust
目的安全区域	any
源地址/地区	10.3.0.2/32
目的地址/地区	any
认证动作	不认证

c. 单击“确定”。

d. 单击“新建”，按如下参数配置。

名称	policy_auth_02
源安全区域	trust
目的安全区域	any
源地址/地区	any
目的地址/地区	any
认证动作	认证

e. 单击“确定”。

7. 配置认证域。

a. 选择“对象 > 用户 > 认证域”。

b. 单击“default”，按如下参数配置。

接入控制	选中“允许对用户做基于策略的控制”
认证服务器	NONE

c. 单击“确定”。

8. 配置安全策略。

a. 选择“策略 > 安全策略 > 安全策略”。

b. 单击“新建”，按如下参数配置。

名称	policy_sec_1
源安全区域	trust
目的安全区域	local
动作	允许

c. 单击“确定”。

d. 单击“新建”，按如下参数配置。

名称	policy_sec_2
源安全区域	trust
目的安全区域	untrust
服务	dns
动作	允许

e. 单击“确定”。

9. 完成上述配置后，管理员在配置针对业务的安全策略、策略路由、带宽策略以及审计策略时可以引用用户/组。

结果验证

- 在 NGFW 上的“对象 > 用户 > 用户/组”中可以查看到用户/组的信息。
- 高级管理者 A 无需进行认证就可以访问网络资源，其他用户即使获取到了高级管理者 A 的用户名，也无法使用 IP 地址不是 10.3.0.2 并且 MAC 地址不是 aaaa-bbbb-cccc 的 PC 访问网络资源。
- 研发部员工 B 使用 IE 浏览器访问 www.example.org，将会重定向至认证页面，输入用户名 user_0002 和密码 Admin@123 进行认证。通过认证后，IE 浏览器的界面会自动跳转到 www.example.org 页面。
- 市场部员工 C 使用 IE 浏览器访问 www.example.org，将会重定向至认证页面，输入用户名 user_0003 和密码 Admin@123 进行认证。通过认证后，IE 浏览器的界面会自动跳转到 www.example.org 页面。
- 来访客户使用 IE 浏览器访问 www.example.org，将会重定向至认证页面，输入用户名 guest 和密码 Admin@123 进行认证。通过认证后，IE 浏览器的界面会自动跳转到 www.example.org 页面。
- 在 NGFW 上的“对象 > 用户 > 在线用户”中可以查看到在线用户的信息。

配置脚本

```
#
 sysname NGFW
#
 user-manage redirect
#
interface GigabitEthernet1/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/2
 ip address 10.2.0.1 255.255.255.0
#
interface GigabitEthernet1/0/3
 ip address 10.3.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GigabitEthernet1/0/3
#
firewall zone untrust
```

```
 set priority 5
 add interface GigabitEthernet1/0/1
#
firewall zone dmz
 set priority 50
 add interface GigabitEthernet1/0/2
#
aaa
 #
 domain default
  service-type internetaccess
 #
#
security-policy
  rule name policy_sec_1
    source-zone trust
    destination-zone local
    action permit
  rule name policy_sec_2
    source-zone trust
    destination-zone untrust
    service dns
    action permit
#
auth-policy
  rule name policy_auth_01
    source-zone trust
    source-address 10.3.0.2 32
    action no-auth
  rule name policy_auth_02
    source-zone trust
    action auth
#
return
```

举例：上网用户+TSM 单点登录（事前认证）

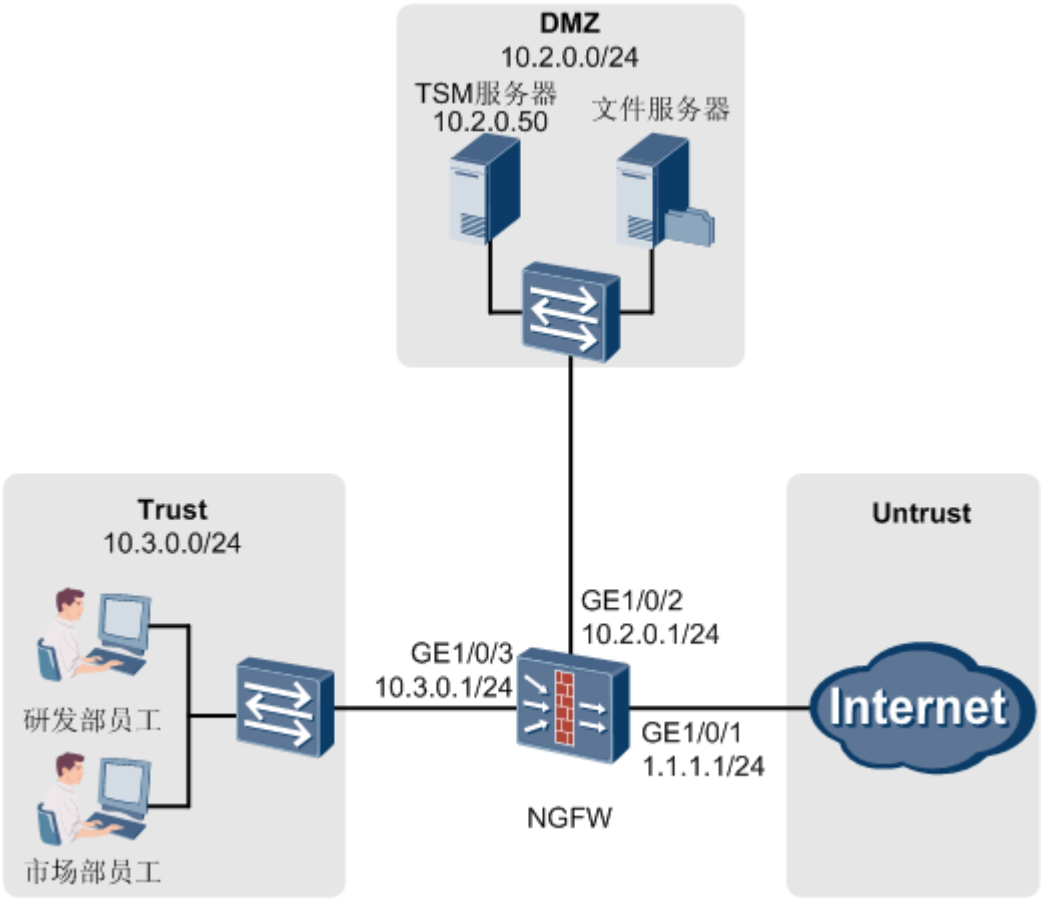
介绍了 NGFW 作为企业的出口网关时，配合 TSM 服务器（即 Policy Center）对上网用户进行管理和认证的举例。事前认证需要用户主动访问 TSM 的 Portal 认证页面进行登录，登录成功才可以访问业务。

组网需求

如图 1 所示，某企业在网络边界处部署了 NGFW 作为出口网关，连接内部网络与 Internet。具体情况如下：

- 内部网络中已经部署了 TSM 身份验证机制，TSM 服务器上存储了用户和组的信息。
- 内部网络中的访问者角色包括研发部员工和市场部员工。

图 1 上网用户+TSM 单点登录组网图



企业的网络管理员希望利用 NGFW 提供的用户管理与认证机制，将内部网络中的 IP 地址识别为用户，为实现基于用户的网络行为控制和网络权限分配提供基础。具体需求如下：

- 在 NGFW 上存储用户和部门的信息，体现公司的组织结构，供策略引用。
- 研发部员工和市场部员工使用 TSM 帐号和密码认证通过后，无需再进行认证就可以访问网络资源。研发部员工和市场部员工的身份标识就是其 TSM 认证时使用的用户名。
- 对于新入职的员工，可能已经在 TSM 服务器上创建了用户信息，但是没有在 NGFW 上存储该用户。对于这类用户，通过认证后将其作为临时用户使用某指定组的权限。

配置思路

说明：

本举例只介绍配置用户与认证相关的内容。

1. 在 TSM 服务器上添加 NGFW，并在 NGFW 上配置 TSM 服务器，使 NGFW 能与 TSM 服务器进行通信。
2. 在 NGFW 上配置服务器导入策略，将 TSM 服务器上的用户信息导入到 NGFW。
3. 在 NGFW 上配置 TSM 单点登录参数。
4. 配置认证域中的新用户选项，新用户通过认证后，使用 newuser 组的权限访问网络资源。
5. 为避免在工作时间段内（此处假定工作时间为 8 小时）因在线用户超时时间频繁到期而导致频繁重新到 TSM 服务器认证的现象，需要配置在线用户超时时间为 480 分钟。
6. 由于 NGFW 部署在用户和 TSM 服务器之间，用户的认证报文经过 NGFW。为实现单点登录功能，需要配置认证策略，对目的地址为 TSM 服务器的报文不进行认证处理；同时配置安全策略，确保 NGFW 和 TSM 服务器之间能正常通信。

数据规划

项目	数据	说明
TSM 服务器	• 名称：auth_server_tsm • TSM 控制器 IP 地址：10.2.0.50 • 服务器端口：8080 • 加密算法：AES128 • 共享密钥：Admin@123	在 NGFW 上配置 TSM 服务器，即 NGFW 与 TSM 服务器通信时使用的一系列参数。 此处设置的参数必须与 TSM 服务器的参数保持一致。
服务器导入策略	• 名称：policy_import • 服务器类型：TSM • 服务器名称：auth_server_tsm • 导入类型：导入用户和用户组到本地 • 导入到用户组：/default • 服务器自动同步：120 分钟 • 当前用户存在时，覆盖本地用户记录	从 TSM 服务器上将用户导入到 NGFW 中。
新用户所属组	• 组名：newuser • 所属组：/default	新用户通过认证后，作为临时用户使用 newuser 组的权限访问网络资源。

项目	数据	说明
TSM 单点登录	• TSM 单点登录：启用 • TSM 身份认证通过后允许用户上网	在 NGFW 上配置单点登录参数，接收 TSM 服务器发送的用户登录/注销信息。

操作步骤

1. 配置安全策略，确保用户、TSM 服务器和 NGFW 之间通信正常。

   a. 配置用户所在安全区域 Trust 到 TSM 服务器所在安全区域 DMZ 的安全策略，用于用户到 TSM 服务器进行认证。

      1. 选择“策略 > 安全策略 > 安全策略”。

      2. 单击“新建”，按如下参数配置。

名称	sec_policy_tsm
源安全区域	trust
目的安全区域	dmz
源地址/地区	10.3.0.0/24
目的地址/地区	10.2.0.50/32
动作	允许

      3. 单击“确定”。

   b. 配置 TSM 服务器所在安全区域 DMZ 到 Local 域的安全策略，用于 TSM 服务器与 NGFW 的交互。

      1. 单击“新建”，按如下参数配置。

名称	local_policy_tsm_1
源安全区域	local
目的安全区域	dmz
动作	允许

      2. 单击“确定”。

      3. 单击“新建”，按如下参数配置。

名称	local_policy_tsm_2
源安全区域	dmz
目的安全区域	local

动作	允许

4. 单击“确定”。

2. 在 TSM 服务器上添加 NGFW。

说明：

此处以 Policy Center V100R003C00 版本为例进行介绍，不同版本界面可能会不同，请参考 Policy Center 版本对应的产品文档。

a. 选择“系统配置 > 服务器配置 > 上网行为管理设备配置”。

b. 单击“增加”，按如下参数配置。

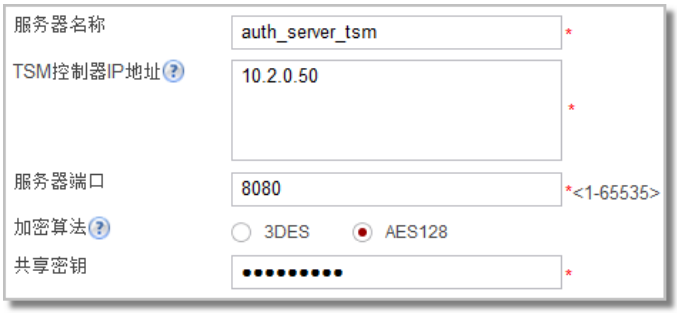
c. 单击“确定”。

3. 在 NGFW 上配置 TSM 服务器。

a. 选择“对象 > 认证服务器 > TSM”。

b. 单击“新建”，按如下参数配置。

此处设置的参数必须与 TSM 服务器上的参数保持一致。



c. 单击“确定”。

4. 在 NGFW 上配置服务器导入策略。

   a. 选择“对象 > 用户 > 用户导入 > 服务器导入”。

   b. 单击“新建”，按如下参数配置。

   c. 单击“确定”。

   d. 单击“policy_import”对应的，在弹出的确认对话框中，单击“是”，立即执行该导入策略，将 TSM 服务器上的用户信息导入 NGFW。

5. 在 NGFW 上创建新用户所属的组。

   a. 选择“对象 > 用户 > 用户/组”。

   b. 选中“default”。

   c. 在“成员管理”中，单击“新建”，选择“新建组”，按如下参数配置。

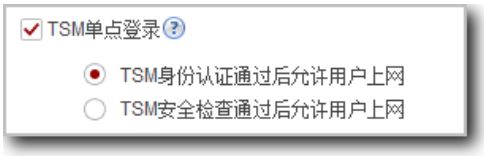
组名	newuser
所属组	/default

   d. 单击“确定”。

6. 在 NGFW 上配置单点登录参数。

   a. 选择“对象 > 用户 > 认证选项 > 单点登录”。

   b. 按如下参数配置。



   c. 单击“应用”。

7. 配置认证域中的新用户选项。

a. 选择“对象 > 用户 > 认证域”。

b. 修改 default 认证域，按如下参数配置。

8. 配置在线用户超时时间为 480 分钟。

a. 选择“对象 > 用户 > 认证选项 > 全局配置”。

b. 在“在线用户超时时间”中输入“480”。

c. 单击“应用”。

9. 配置认证策略，使用户认证报文能经过 NGFW 到达 TSM 服务器。

a. 选择“策略 > 认证策略”。

b. 单击“新建”，按如下参数配置。

c. 单击“确定”。

10. 完成上述配置后，管理员在配置安全策略、策略路由、带宽策略以及审计策略时引用用户/组。

结果验证

- 在 NGFW 上的“对象 > 用户 > 用户/组”中可以查看到用户/组的信息。
- 研发部员工使用 TSM 账号和密码登录成功后，就可以访问网络资源。
- 市场部员工使用 TSM 账号和密码登录成功后，就可以访问网络资源。
- 在 NGFW 上的“对象 > 用户 > 在线用户”中可以查看到在线用户的信息。

配置脚本

```
#
 sysname NGFW
#
 user-manage online-user aging-time 480
 user-manage single-sign-on tsm enable
#
tsm-server template auth_server_tsm
 tsm-server encryption-mode aes128 shared-key %$%$|5<h@/062'gA|%:9CO.2/JA8%$%$
 tsm-server ip-address 10.2.0.50
#
security-policy
 rule name sec_policy_tsm
  source-zone trust
  destination-zone dmz
  source-address 10.3.0.0 24
  destination-address 10.2.0.50 32
  action permit
 rule name local_policy_tsm_1
  source-zone local
  destination-zone dmz
  action permit
 rule name local_policy_tsm_2
  source-zone dmz
  destination-zone trust
  action permit
#
auth-policy
 rule name auth_policy_tsm
  source-zone trust
```

```
  destination-zone dmz
  source-address 10.3.0.0 24
  destination-address 10.2.0.50 32
  action no-auth
#
interface GigabitEthernet1/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/2
 ip address 10.2.0.1 255.255.255.0
#
interface GigabitEthernet1/0/3
 ip address 10.3.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GigabitEthernet1/0/3
#
firewall zone untrust
 set priority 5
 add interface GigabitEthernet1/0/1
#
firewall zone dmz
 set priority 50
 add interface GigabitEthernet1/0/2
#
 user-manage import-policy policy_import from tsm
 server template auth_server_tsm
 server basedn tsm
 destination-group /default
 import-type all
 import-override enable
 time-interval 120
#
domain default
 service-type internetaccess
 new-user add-temporary group /default/newuser
#
return
```

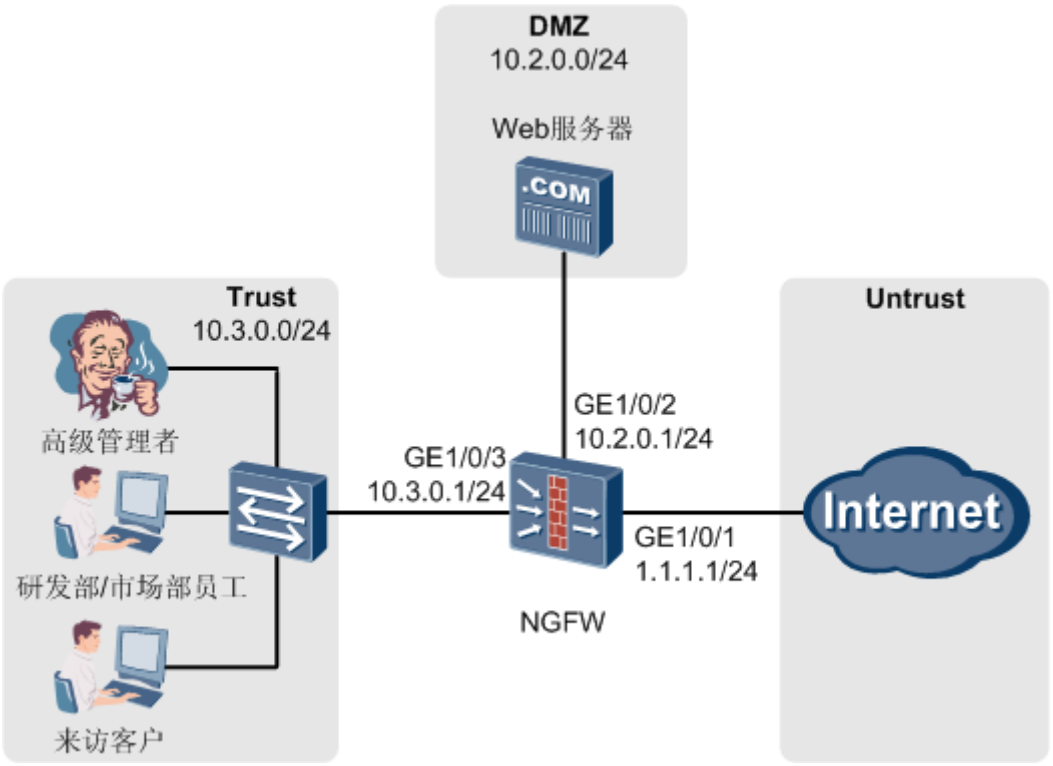
处理故障——使用免认证方式的双向绑定用户不能访问网络资源

介绍使用免认证方式的双向绑定用户不能访问网络资源时的故障处理诊断过程。

现象描述

如图 1 所示，某企业在网络边界处部署了 NGFW 作为网关，连接内部网络与 Internet。管理员在 NGFW 上配置了用户管理和认证机制，将高级管理者的用户与 IP/MAC 地址双向绑定，高级管理者不需要进行认证就可以访问网络资源。

图 1 使用免认证方式的双向绑定用户不能访问网络资源组网图



实际使用中，发现高级管理者无法使用浏览器访问 Internet 上的网站。

定位思路

选择“对象 > 用户 > 在线用户”，在“在线用户列表”中以高级管理者的登录名为条件，查询是否存在高级管理者的用户表项。根据查询结果可以缩小可能原因的范围，请分别按以下情况逐一排查可能原因：

- 不存在高级管理者的用户表项。
- 存在高级管理者的用户表项。

处理步骤

不存在高级管理者的用户表项。

可能原因及相应的处理步骤如下：

1. 认证策略中的匹配条件配置有误。

   选择“策略 > 认证策略”，以高级管理者的源地址或所属的安全区域为条件查询是否匹配了认证策略，检查认证策略的匹配条件是否正确，确保认证策略能否匹配到高级管理者发出的流量。

2. 认证策略中的认证动作配置有误。

   选择“策略 > 认证策略”，查看匹配高级管理者的认证策略中的认证动作是否正确，认证动作应该为“不认证”。

3. 高级管理者没有使用指定 IP/MAC 地址的 PC。

   查看高级管理者当前使用 PC 的 IP 地址和 MAC 地址，确保当前的 IP 地址和 MAC 地址就是与高级管理者的用户绑定的 IP 和 MAC 地址。

4. 在线用户已经达到最大值。

   选择“对象 > 用户 > 在线用户”，查看在线用户的数量。

存在高级管理者的用户表项。

可能原因及相应的处理步骤如下：

5. 高级管理者的用户已经被冻结。

   选择“对象 > 用户 > 在线用户”，查看被冻结的用户。如果高级管理者的用户已经被冻结，使用“解冻”功能取消冻结。

6. 安全策略配置有误。

   选择“监控 > 策略命中日志”，以高级管理者的用户名或源地址为查询条件，查询命中的安全策略。然后检查安全策略及其配置文件是否将高级管理者发出的流量阻断。

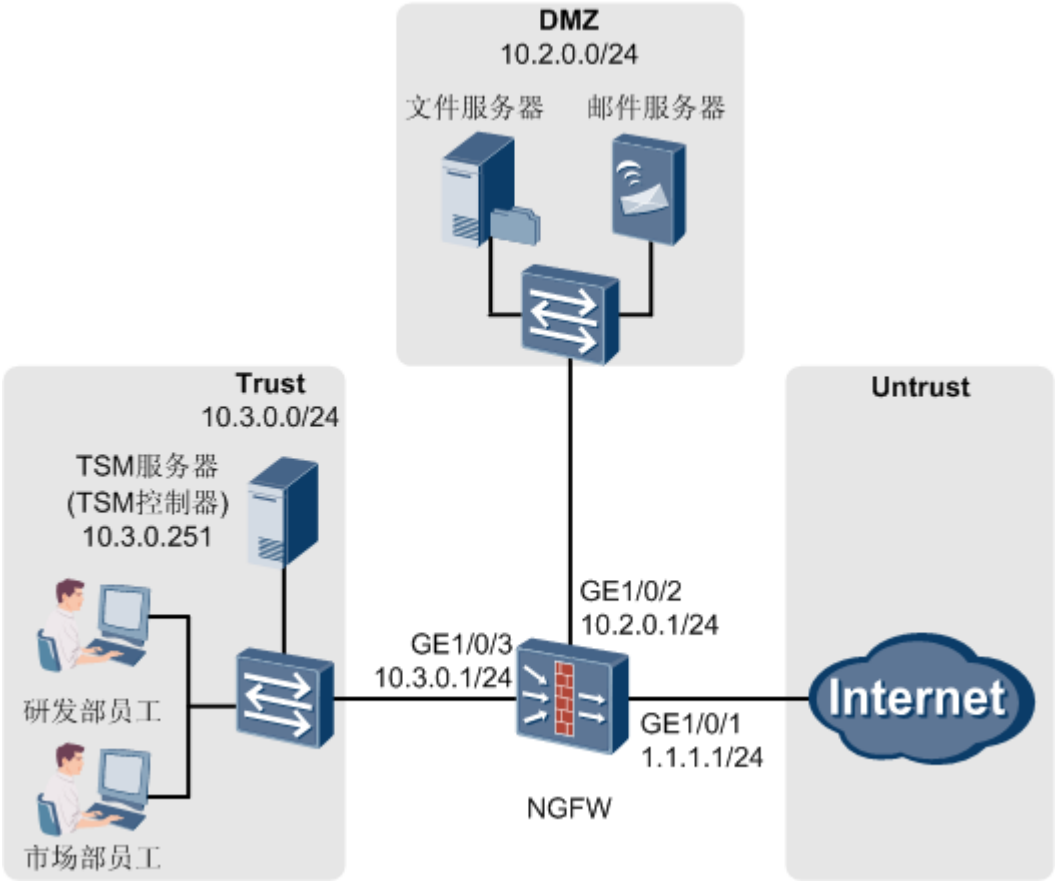
处理故障——使用 TSM 单点登录方式进行认证的用户不能访问网络资源

介绍使用 TSM 单点登录方式进行认证的用户不能访问网络资源时的故障处理诊断过程。

现象描述

如图 1 所示，某企业在网络边界处部署了 NGFW 作为网关，连接内部网络与 Internet。内部网络中已经部署了 TSM 身份验证机制，管理员在 NGFW 上配置了用户管理和认证机制，使用 TSM 单点登录方式对内部网络用户进行认证。

图 1 使用 TSM 单点登录方式进行认证的用户不能访问网络资源组网图



实际使用中，发现研发部员工和市场部员工可以正常登录到 TSM，但是无法使用浏览器访问 Internet 上的网站。

定位思路

选择“对象 > 用户 > 在线用户”，在“在线用户列表”中以研发部员工或市场部员工的登录名为条件，查询是否存在研发部员工和市场部员工的用户表项。根据查询结果可以缩小可能原因的范围，请分别按以下情况逐一排查可能原因：

- 不存在研发部员工和市场部员工的用户表项。
- 存在研发部员工和市场部员工的用户表项。

处理步骤

不存在研发部员工和市场部员工的用户表项。

可能原因及相应的处理步骤如下：

1. TSM 控制器的设置有误。

   检查 TSM 控制器的配置，TSM 控制器上设置的参数应该与 NGFW 上设置的参数保持一致。

2. 在线用户已经达到最大值。

   选择“对象 > 用户 > 在线用户”，查看在线用户的数量。

存在研发部员工和市场部员工的用户表项。

可能原因及相应的处理步骤如下：

3. 研发部员工和市场部员工的用户已经被冻结。

   选择“对象 > 用户 > 在线用户”，查看被冻结的用户。如果研发部员工和市场部员工的用户已经被冻结，使用“解冻”功能取消冻结。

4. 研发部员工和市场部员工属于新用户，被加入到指定的组中，该组的权限设置有误。

   选择“对象 > 用户 > 认证域”，查看新用户选项加入的用户组。然后以该组为查询条件，查询所有引用了该组的安全策略，检查安全策略及其配置文件是否将研发部员工和市场部员工发出的流量阻断。

5. 安全策略配置有误。

   选择“监控 > 策略命中日志”，以研发部员工和市场部员工的用户名或源地址为查询条件，查询命中的安全策略。然后检查安全策略及其配置文件是否将研发部员工和市场部员工发出的流量阻断。

HCIE-Security 模拟面试问题及面试建议

1. 防火墙有哪些用户认证方式？
2. RADIUS 和 HWTACACS 有什么区别？

每一章的 FAQ 都是面试考官喜欢追问的地方^_^
每一章的故障排除也是哦……