NetScreen 概念与范例

ScreenOS 参考指南

第 8 卷：用户认证

ScreenOS 5.1.0

编号 093-1373-000-SC

修订本 B

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with NetScreen's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Consult the dealer or an experienced radio/TV technician for help.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device.

Disclaimer

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR NETSCREEN REPRESENTATIVE FOR A COPY.

目录

前言

第 8 卷，“用户认证”介绍 ScreenOS 中认证不同类型用户的方法。本卷介绍了用户认证、可存储用户配置文件的两个位置 (内部数据库和外部认证服务器)，然后提供了配置认证、IKE、Xauth 及 L2TP 用户和用户组的诸多示例。其中还涵盖了用户认证的其它一些方面，如更改登录标题、创建多类型用户 (如 IKE/XAuth 用户) 及在应用认证的策略中使用组表达式。

约定

本文档包含几种类型的约定，以下各节将对其加以介绍：

CLI 约定

当出现命令行界面 (CLI) 命令的语法时，使用以下约定：

- 在中括号 [ ] 中的任何内容都是可选的。
- 在大括号 { } 中的任何内容都是必需的。
- 如果选项不止一个，则使用管道 (|) 分隔每个选项。例如，

  ```
  set interface { ethernet1 | ethernet2 | ethernet3 } manage
  ```

  意味着 “设置 ethernet1、 ethernet2 或 ethernet3 接口的管理选项”。
- 变量以*斜体*方式出现。例如：

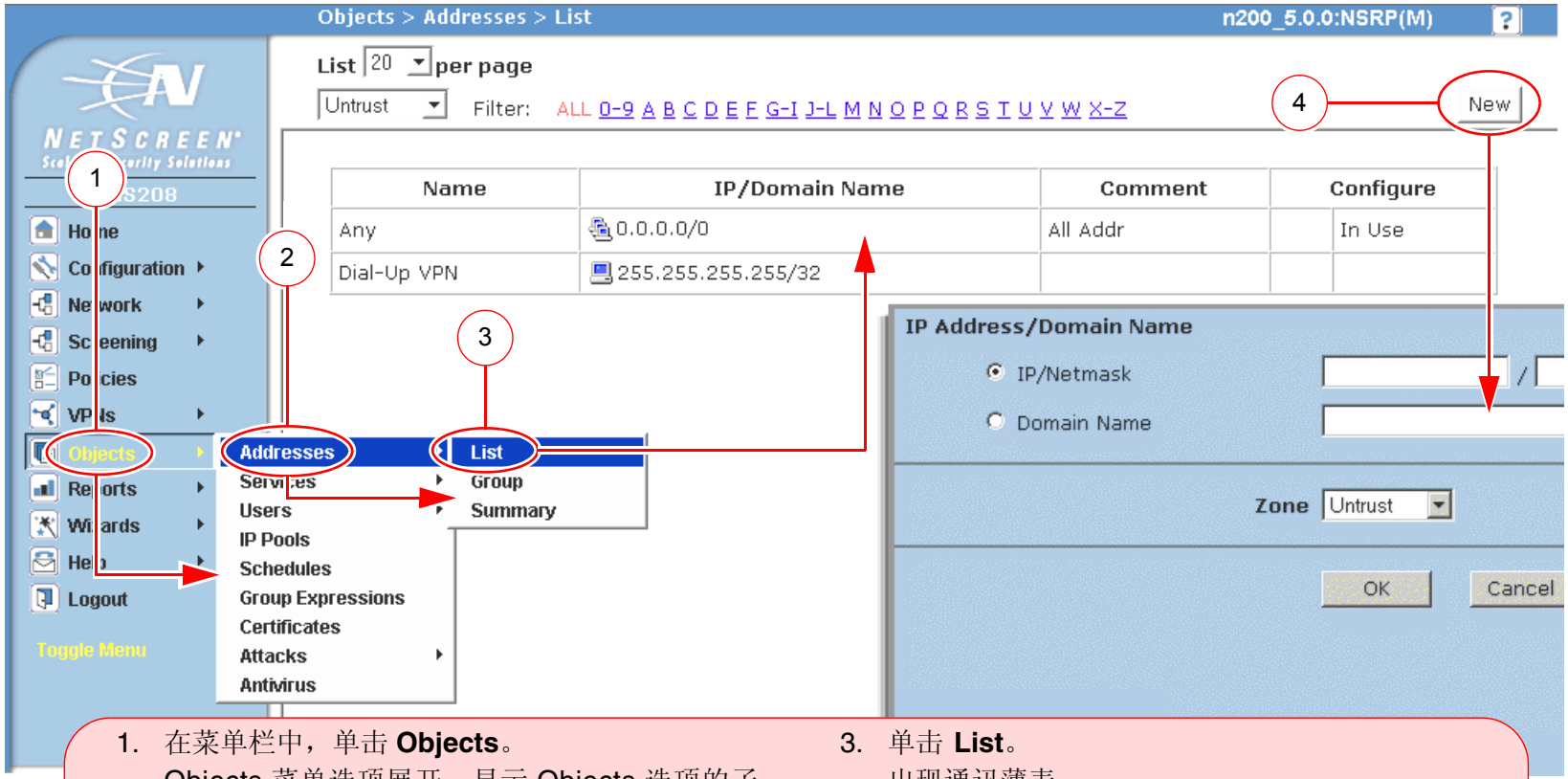
  ```
  set admin user name password
  ```

当 CLI 命令在句子的上下文中出现时，应为**粗体** (除了始终为*斜体*的变量之外)。例如：“使用 **get system** 命令显示 NetScreen 设备的序列号”。

注意：*当键入关键字时，只需键入足够的字母就可以唯一地标识单词。例如，要输入命令* ***set admin user joe j12fmt54****，键入* ***set adm u joe j12fmt54*** *就足够了。尽管输入命令时可以使用此捷径，但本文所述的所有命令都以完整的方式提供。*

WebUI 约定

贯穿本书的全部篇章，用一个 V 形符号 (>) 来指示在 WebUI 中导航，其方法是单击菜单选项和链接。例如，指向地址配置对话框的路径显示为 **Objects > Addresses > List > New**。此导航序列如下所示。



1. 在菜单栏中，单击 **Objects**。
   Objects 菜单选项展开，显示 Objects 选项的子菜单。
2. (Applet 菜单) 将鼠标光标悬停在 **Addresses** 上。
   (DHTML 菜单) 单击 **Addresses**。
   Addresses 选项展开，显示 Addresses 选项的子菜单。
3. 单击 **List**。
   出现通讯薄表。
4. 单击 **New** 链接。
   出现新地址配置对话框。

如要用 WebUI 执行任务，必须首先导航到相应的对话框，然后可在该对话框中定义对象和设置参数。每个任务的指令集划分为两部分：导航路径和配置详细信息。例如，下列指令集包含指向地址配置对话框的路径和要配置的设置：

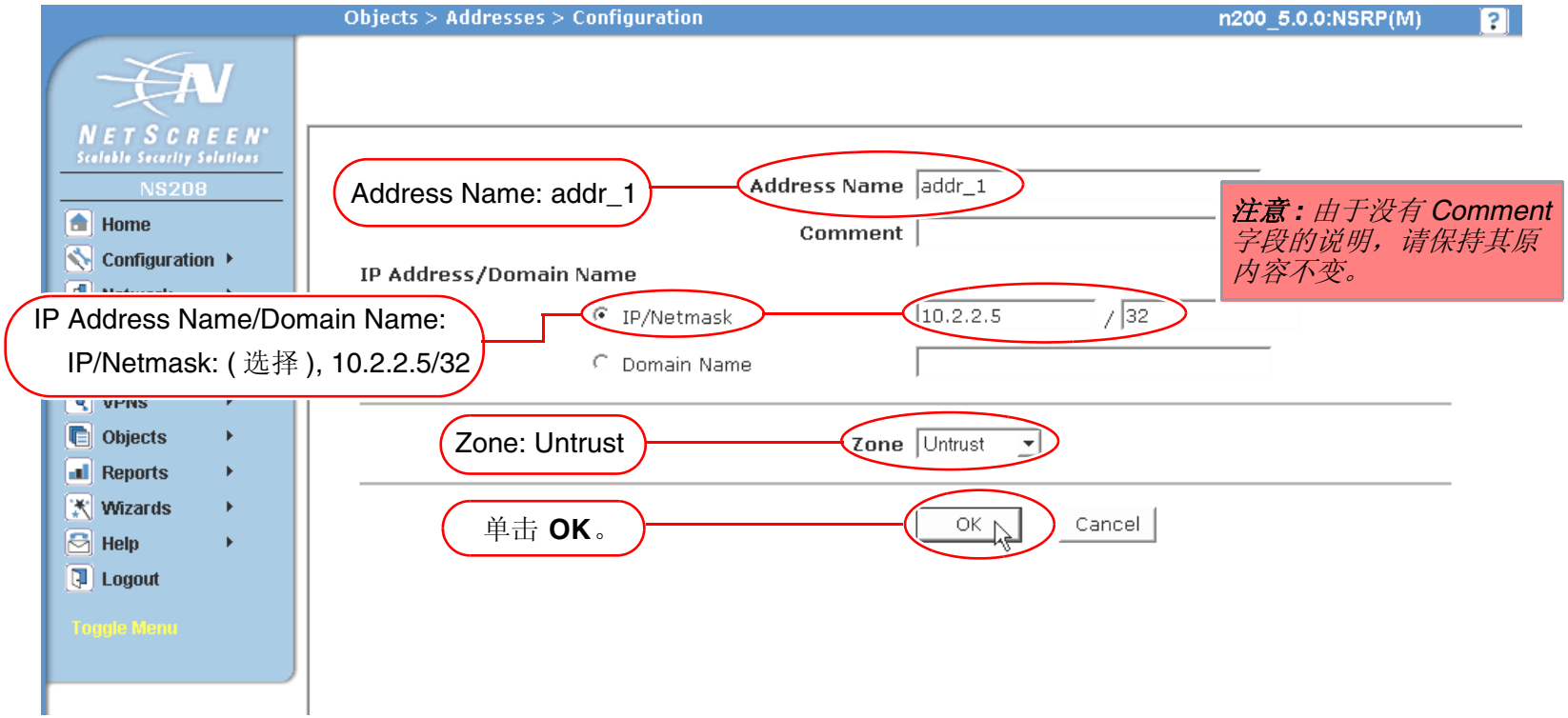
Objects > Addresses > List > New: 输入以下内容，然后单击 **OK**:

Address Name: addr_1

IP Address/Domain Name:

IP/Netmask: (选择), 10.2.2.5/32

Zone: Untrust

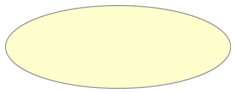


插图约定

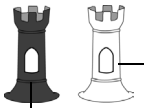
下列图形构成了贯穿本书的插图所用的基本图像集：

通用 NetScreen 设备

虚拟路由选择域



安全区段



安全区段接口

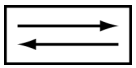
白色 = 受保护区段接口
（例如：Trust 区段）

黑色 = 区段外接口
（例如：Untrust 区段）

通道接口

VPN 通道

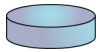
路由器图标



交换机图标

包含单个子网的局域网 (LAN)
（例如：10.1.1.0/24）

互联网



动态 IP (DIP) 池

台式计算机

便携式计算机

通用网络设备
（例如：NAT 服务器，
接入集中器）

服务器

命名约定和字符类型

关于 ScreenOS 配置中定义的对象 (如地址、 admin 用户、 auth 服务器、 IKE 网关、虚拟系统、 VPN 通道和区段) 的名称， ScreenOS 采用下列约定。

- 如果名称字符串包含一个或多个空格，则必须将该整个名称字符串用双引号 (") 括起来；例如，**set address trust "local LAN" 10.1.1.0/24**。
- NetScreen 会删除一组双引号内文本的前导或结尾空格，例如，**" local LAN "** 将变为 **"local LAN"**。
- NetScreen 将多个连续的空格视为单个空格。
- 尽管许多 CLI 关键字不区分大小写，但名称字符串是区分大小写的。例如，**"local LAN"** 不同于 **"local lan"**。

ScreenOS 支持以下字符类型 :

- 单字节字符集 (SBCS) 和多字节字符集 (MBCS)。SBCS 的例子是 ASCII、欧洲语和希伯莱语。MBCS (也称为双字节字符集， DBCS) 的例子是中文、韩文和日文。

  注意 : *控制台连接只支持 SBCS。WebUI 对 SBCS 和 MBCS 都支持，取决于 Web 浏览器所支持的字符集。*

- 从 32 (十六进制 0x20) 到 255 (0xff) 的 ASCII 字符，双引号 (") 除外，该字符有特殊的意义，它用作包含空格的名称字符串的开始或结尾指示符。

JUNIPER NETWORKS NETSCREEN 文档

要获取任何 Juniper Networks NetScreen 产品的技术文档，请访问 www.juniper.net/techpubs/。

要获取技术支持，请使用 http://www.juniper.net/support/ 下的 Case Manager 链接打开支持个例，还可拨打电话 1-888-314-JTAC (美国国内) 或 1-408-745-9500 (美国以外的地区)。

如果在以下内容中发现任何错误或遗漏，请用下面的电子邮件地址与我们联系：

techpubs-comments@juniper.net

1

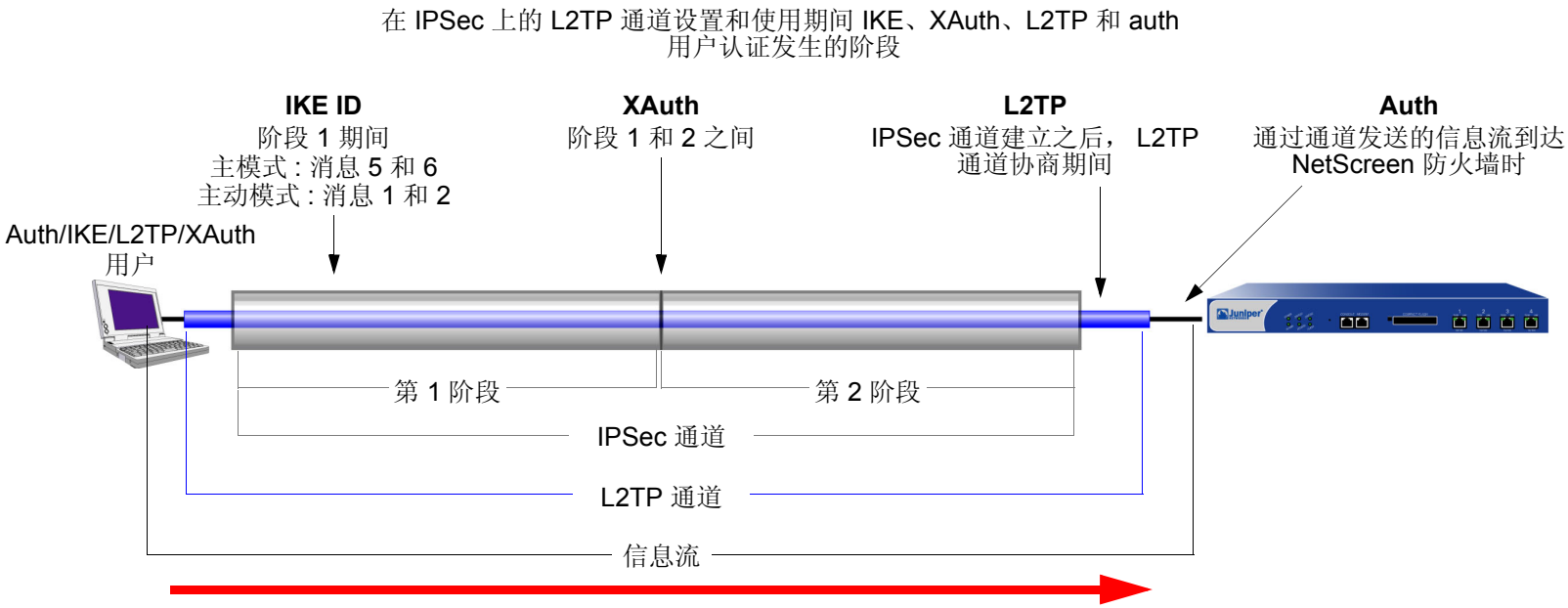
认证

对可用于不同类型网络用户的不同认证类型进行简介后，本章将简要介绍 admin 用户认证。然后，将提供有关组合不同用户类型、组表达式的使用及如何定制 HTTP、 FTP、 L2TP、 Telnet 和 XAuth 登录提示时出现的标题的信息。本章包括以下部分：

用户认证类型

以下章节介绍可以创建的不同类型的用户和用户组，以及配置策略、 IKE 网关和 L2TP 通道时如何使用它们：

NetScreen 设备在连接过程的不同阶段对不同类型的用户进行认证。有关在创建 IPSec 上的 L2TP VPN 通道期间 IKE、 XAuth、 L2TP 和 Auth 用户认证技术运行的时间，请参阅下图：



注意：因为 XAuth 和 L2TP 都提供用户认证和地址分配，故通常它们不同时使用。此处将两者同时显示，只为说明 VPN 通道创建期间各认证类型发生的时间。

ADMIN 用户

Admin 用户是 NetScreen 设备的管理员。共有五种 admin 用户：

- 根 admin
- 根级读 / 写 admin
- 根级只读 admin
- Vsys admin
- Vsys 只读 admin

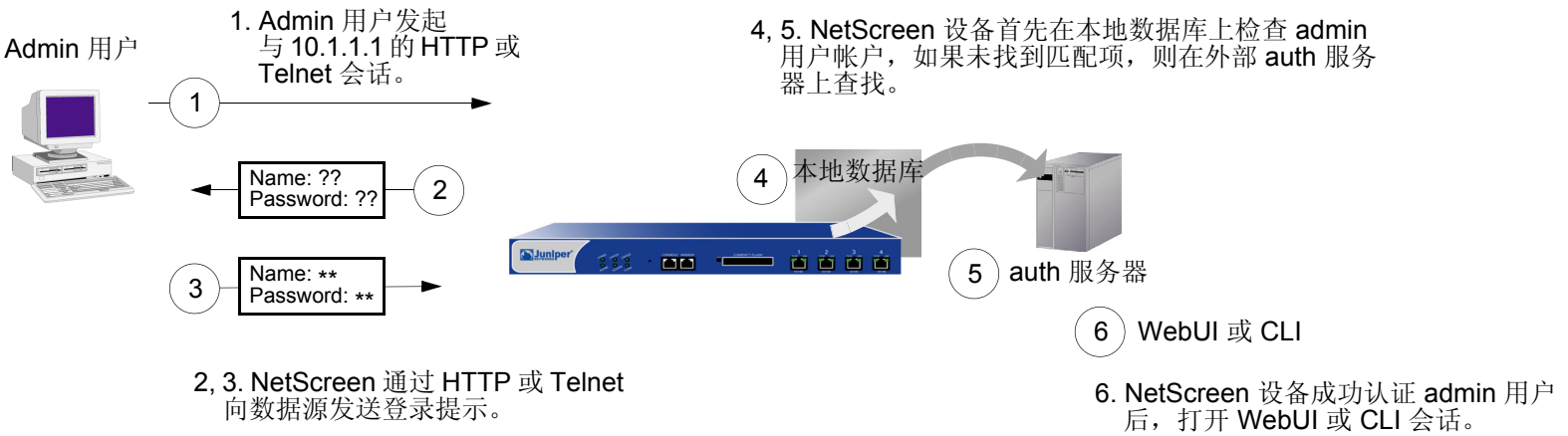
> ***注意：****有关各类型 admin 用户权限的信息，以及创建、修改和删除 admin 用户的范例，请参阅第* ***3*** *-****1*** *页上的“管理”。*

尽管 NetScreen 设备根用户的配置文件必须存储在本地数据库中，但可将具有读 / 写和只读权限的 vsys 用户和根级 admin 用户存储在本地数据库或外部 auth 服务器中。

如果将 admin 用户帐户存储在外部 RADIUS auth 服务器上，并在 auth 服务器上加载 NetScreen 词典文件 (请参阅第 25 页上的“NetScreen 词典文件”)，则可选举查询服务器上定义的 admin 权限。此外，您也可以指定某权限级别，以全局方式应用于该 auth 服务器上存储的所有 admin 用户。可指定读 / 写或只读权限。如果将 admin 用户存储在外部 SecurID 或 LDAP auth 服务器或者未加载 NetScreen 词典文件的 RADIUS 服务器上，则不能在 auth 服务器上定义它们的权限属性。因此，必须在 NetScreen 设备上为它们指定权限级别。

如果在 NetScreen 设备上设置：	且 RADIUS 服务器已加载 NetScreen 词典文件，则：	且 SecurID、 LDAP 或 RADIUS 服务器未加载 NetScreen 词典文件，则：
从 RADIUS 服务器获取权限	指定适当权限	根级或 vsys 级 admin 登录失败
为外部 admin 指定读 / 写权限	指定根级或 vsys 级读 / 写权限	指定根级读 / 写权限 Vsys admin 登录失败
为外部 admin 指定只读权限	指定根级或 vsys 级只读权限	指定根级只读权限 Vsys admin 登录失败

admin 认证过程如下图所示：



多类型用户

可将 auth、 IKE、 L2TP、 XAuth 用户组合在一起，创建下列组合并存储在本地数据库上：

- Auth/IKE 用户
- Auth/L2TP 用户
- Auth/IKE/L2TP 用户
- IKE/L2TP 用户
- Auth/XAuth 用户
- Auth/IKE/XAuth 用户
- IKE/XAuth 用户
- L2TP/XAuth 用户
- IKE/L2TP/XAuth 用户
- Auth/IKE/L2TP/XAuth 用户

尽管在本地数据库上定义多类型用户帐户时，可以创建上述所有组合，但在创建之前仍须考虑以下事项：

- 将 IKE 用户类型与其它任何用户类型组合后，会限制其扩展潜能。必须将 IKE 用户帐户存储在本地数据库上。如果创建 auth/IKE、 IKE/L2TP 和 IKE/XAuth 用户帐户，而后用户数超出本地数据库容量时，就无法将这些帐户重新置于外部 auth 服务器中。如果将 IKE 用户帐户与其它类型帐户分离，必要时可以灵活地将非 IKE 用户帐户移动到外部 auth 服务器中。
- L2TP 和 XAuth 提供相同的服务：远程用户认证以及 IP、DNS 服务器与 WINS 服务器地址分配。建议不要对 IPSec 上的 L2TP 通道同时使用 L2TP 和 XAuth。不仅因为这两种协议的作用相同，而且在 “阶段 2” IKE 协商完成、 L2TP 协商开始后， L2TP 地址分配将会覆盖 XAuth 地址分配。
- 如果将 auth/L2TP 或 auth/XAuth 组合在一起，在本地数据库上创建多类型用户帐户，则两种类型用户登录时必须使用相同的用户名和密码。

  尽管创建一个多类型用户帐户较之将用户类型分为两个单独帐户操作起来更为方便，但后者却可以为您带来更高的安全性。例如，可将 auth 用户帐户存储在外部 auth 服务器上，将 XAuth 用户帐户存储在本地数据库上。然后，可以为每个帐户指定不同的登录用户名和密码，并在 IKE 网关配置中引用 XAuth 用户，而在策略配置中引用 auth 用户。拨号 VPN 用户必须经过两次认证，认证时可以使用两个完全不同的用户名和密码。

组表达式

组表达式是可以在策略中用来使认证要求实现条件化的语句。组表达式可以将用户、用户组或其它组表达式作为认证的可选条件 (“a” OR “b”) 或者作为认证的必需条件 (“a” AND “b”) 组合起来，也可以将某个用户、用户组或另一组表达式排除在外 (NOT “c”)。

注意：*虽然您在 NetScreen 设备上定义组表达式 (并存储在本地数据库上)，但组表达式中引用的用户和用户组必须存储在外部 RADIUS 服务器上。 RADIUS 服务器允许一个用户属于多个用户组。但本地数据库不允许这样。*

组表达式使用三个运算符 OR、 AND 和 NOT。表达式中用 OR、 AND 和 NOT 关联起来的对象可以是一个 auth 用户、 auth 用户组或先前定义的组表达式。

用户

OR – 如果策略的认证指定用户为 “a” OR “b”，用户是其中之一时， NetScreen 设备会对其进行认证。

AND – 组表达式中使用 AND 运算符时，要求两个表达式对象中至少有一个是用户组或组表达式。(要求某个用户为用户 “a” AND 用户 “b” 是不符合逻辑的。) 如果策略的认证要求用户为 “a” AND 组 “b” 中的成员，则只有当满足这两个条件时， NetScreen 设备才会认证该用户。

NOT – 如果策略的认证指定用户为除用户 “c” 外的任何其它用户 (NOT “c”)，则只要用户不是 “c”，NetScreen 设备就会认证他 / 她。

用户组

OR – 如果策略的认证指定该用户属于组 “a” OR 组 “b”，则只要他 / 她属于任何一组，NetScreen 设备即会认证该用户。

AND – 如果策略的认证要求用户属于组 “a” AND 组 “b”，则只有当用户同时属于两个组时， NetScreen 设备才会认证他 / 她。

NOT – 如果策略的认证指定用户属于除组 “c” 外的任意组 (NOT “c”)，则当用户不属于此组时， NetScreen 设备会认证他 / 她。

组表达式

OR – 如果策略的认证指定用户符合组表达式 “a” OR 组表达式 “b” 的描述，则只有当其中某一组表达式适用于该用户时， NetScreen 设备才会认证他 / 她。

AND – 如果策略的认证指定用户符合组表达式 “a” AND 组表达式 “b” 的描述，则只有当两个表达式都适用于该用户时， NetScreen 设备才会认证他 / 她。

NOT – 如果策略的认证指定用户应不符合组表达式 “c” 的描述 (NOT “c”)，则只有当该用户不符合此组表达式时， NetScreen 设备才会认证他 / 她。

范例 : 组表达式 (AND)

在本例中，将创建一个代表 “sales AND marketing” 的组表达式 “s+m”。您先前已在名为 “radius1” 的外部 RADIUS auth 服务器上创建了 auth 用户组 “sales” 和 “marketing”，并在其中添加了用户。(有关如何配置外部 RADIUS auth 服务器的范例，请参阅第 32 页上的 “范例 : RADIUS Auth 服务器”。) 然后，在区段内部策略[1] 中使用该组表达式，策略中的认证部分要求用户必须是这两个用户组的成员，才能访问名为 “project1” 的服务器 (10.1.1.70) 上的机密内容。

WebUI

1. 地址

   Objects > Addresses > List > New: 输入以下内容，然后单击 **OK**:

   Address Name: project1

   IP Address/Domain Name:

   IP/Netmask: (选择), 10.1.1.70/32

   Zone: Trust

2. 组表达式

   Objects > Group Expressions > New: 输入以下内容，然后单击 **OK**:

   Group Expression: s+m

   AND: (选择), sales AND marketing

1. 要使区段内部策略正常工作，源地址和目标地址必须位于不同的子网中，这些子网通过绑定到同一区段的接口连接到 NetScreen 设备。除可在两个地址间转发信息流的 NetScreen 设备外，不能有任何其它路由设备。有关区段内部策略的详细信息，请参阅第 **2** -293 页上的 “策略”。

3. 策略

Policies > (From: Trust, To: Trust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), project1

Service: ANY

Action: Permit

Position at Top: (选择)

> Advanced: 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页：

Authentication: (选择)

Auth Server: (选择)

Use: radius1

Group Expression: (选择), External Group Expression - s+m

CLI

1. 地址

```
set address trust project1 10.1.1.70/32
```

2. 组表达式

```
set group-expression s+m sales and marketing
```

3. 策略

```
set policy top from trust to trust any project1 any permit auth server radius1
    group-expression s+m
save
```

范例 : 组表达式 (OR)

在本例中，将创建一个代表 “amy OR basil” 的组表达式 “a/b”。您先前已在名为 “radius1” 的外部 RADIUS auth 服务器上创建了 auth 用户帐户 “amy” 和 “basil”。(有关如何配置外部 RADIUS auth 服务器的范例，请参阅 第 32 页上的 “范例 : RADIUS Auth 服务器”。) 然后在从 Trust 区段到 DMZ 的策略中使用该组表达式。策略的认证部分要求用户必须为 amy 或 basil，才能访问 210.1.1.70 处名为 “web1” 的 Web 服务器。

WebUI

1. 地址

   Objects > Addresses > List > New: 输入以下内容，然后单击 **OK**:

   Address Name: web1

   IP Address/Domain Name

   IP/Netmask: (选择), 210.1.1.70/32

   Zone: DMZ

2. 组表达式

   Objects > Group Expressions > New: 输入以下内容，然后单击 **OK**:

   Group Expression: a/b

   OR: (选择), amy OR basil

3. 策略

Policies > (From: Trust, To: DMZ) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), web1

Service: ANY

Action: Permit

Position at Top: (选择)

> Advanced: 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页：

Authentication: (选择)

Auth Server: (选择)

Use: radius1

Group Expression: (选择), External Group Expression - a/b

CLI

1. 地址

```
set address trust project1 210.1.1.70/32
```

2. 组表达式

```
set group-expression a/b amy or basil
```

3. 策略

```
set policy top from trust to dmz any web1 any permit auth server radius1
    group-expression a/b
save
```

范例 : 组表达式 (NOT)

在本例中，将创建一个代表 “NOT temp” 的组表达式 “-temp”。您先前已在名为 “radius1” 的外部 RADIUS auth 服务器上创建本地 auth 用户组 “temp”。 (有关如何配置外部 RADIUS auth 服务器的范例，请参阅第 32 页上的 “范例 : RADIUS Auth 服务器”。) 然后，在从 Trust 区段到 Untrust 区段的策略中使用该组表达式，该策略允许除临时合同工以外的所有专职雇员访问互联网。策略的认证部分要求认证 Trust 区段中除 “temp” 中的用户以外的所有人员，拒绝 “temp” 中的用户访问 Untrust 区段。

WebUI

1. 组表达式

   Objects > Group Expressions > New: 输入以下内容，然后单击 **OK**:

   Group Expression: -temp

   OR: (选择), NOT temp

2. 策略

   Policies > (From: Trust, To: Untrust) New: 输入以下内容，然后单击 **OK**:

   Source Address:

   Address Book Entry: (选择), Any

   Destination Address:

   Address Book Entry: (选择), Any

   Service: HTTP

   Action: Permit

   Position at Top: (选择)

   > Advanced: 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页 :

   Authentication: (选择)

   Auth Server: (选择)

   Use: Local

   Group Expression: (选择), External Group Expression - -temp

CLI

1. 组表达式

```
set group-expression -temp not temp
```

2. 策略

```
set policy top from trust to untrust any any any permit auth server radius1
    group-expression -temp
save
```

标题自定义

标题是指在以下类型登录期间在屏幕的下列位置出现的消息：

- Admin 用户连接以登录到 NetScreen 设备时，在 Telnet 或控制台显示器的顶部显示[2]
- Auth 用户成功登录到 WebAuth 地址后，在 Web 浏览器屏幕的顶部显示
- 对于 Auth 用户，在 Telnet、 FTP 或 HTTP 的登录提示、成功消息和失败消息上显示

除控制台登录标题外，所有标题都具有缺省消息。您可以自定义出现在标题上的消息，使其更适合使用 NetScreen 设备的网络环境。

范例：自定义 WebAuth 标题

在本例中，将更改出现在 Web 浏览器中的消息，用以指示 Auth 用户通过 WebAuth 成功登录后已成功通过认证。新消息为 “Authentication approved”。

WebUI

Configuration > Banners > WebAuth: 在 Success Banner 字段中，键入 **Authentication approved**，然后单击 **Apply**。

CLI

```
set webauth banner success “Authentication approved”
save
```

2. 可在 Telnet 或控制台标题下面加入其它标题行。虽然 Telnet 标题可不同于控制台标题，但 Telnet 和控制台登录显示的第二个标题行相同。要创建二级标题，请输入以下命令：**set admin auth banner secondary** *string*。

2

认证服务器

本章研究不同类型的认证服务器 — 内置于各 NetScreen 设备中的本地数据库以及外部 RADIUS、SecurID 和 LDAP 认证服务器。本章包括以下部分：

认证服务器类型

可对 NetScreen 设备进行配置，以便使用本地数据库或者一个或多个外部认证服务器验证以下类型用户的身份：

- Auth 用户
- IKE 用户
- L2TP 用户
- XAuth 用户
- Admin 用户

> ***注意：****IKE 用户帐户必须存储在本地数据库上。RADIUS 是唯一支持 L2TP 和 XAuth 远程设置指派和管理权限指派的外部服务器。*

除其本地数据库外，NetScreen 设备还支持外部 RADIUS、SecurID 和 LDAP 服务器。可使用各种类型的认证服务器对 auth 用户、L2TP 用户、XAuth 用户和 admin 用户进行认证。此外，NetScreen 还支持 WebAuth，这是面向 auth 用户的一种可选认证方案。[有关 WebAuth 的范例，请参阅第 70 页上的 “范例：仅 WebAuth + SSL (外部用户组)”。] 所有包含 auth 用户帐户类型的 auth 服务器都可以作为缺省的 WebAuth auth 服务器。下表对服务器与用户类型及认证功能之间的对应支持关系加以总结：

服务器类型	支持的用户类型和功能									
	Auth 用户	IKE 用户	L2TP 用户		XAuth 用户		Admin 用户		用户组	组表达式
			Auth	远程设置	Auth	远程设置	Auth	权限		
Local	✓	✓	✓	✓	✓	✓	✓	✓	✓	
RADIUS	✓		✓	✓	✓	✓	✓	✓	✓	✓
SecurID	✓		✓		✓		✓			
LDAP	✓		✓		✓		✓			

在大多数 NetScreen 设备上，可对每个系统 — 根系统和虚拟系统 — 以任意组合形式最多使用 10 个主认证服务器。这一数字包括本地数据库，但不包括备份认证服务器。一个 RADIUS 或 LDAP 服务器支持两个备份服务器，一个 SecurID 服务器支持一个备份服务器；例如，您可使用本数据库和 9 个不同的主 RADIUS 服务器，每个 RADIUS 服务器分配有两个备份服务器。

多个认证服务器同时运行

各连接请求的颜色与认证检查的匹配颜色相关：

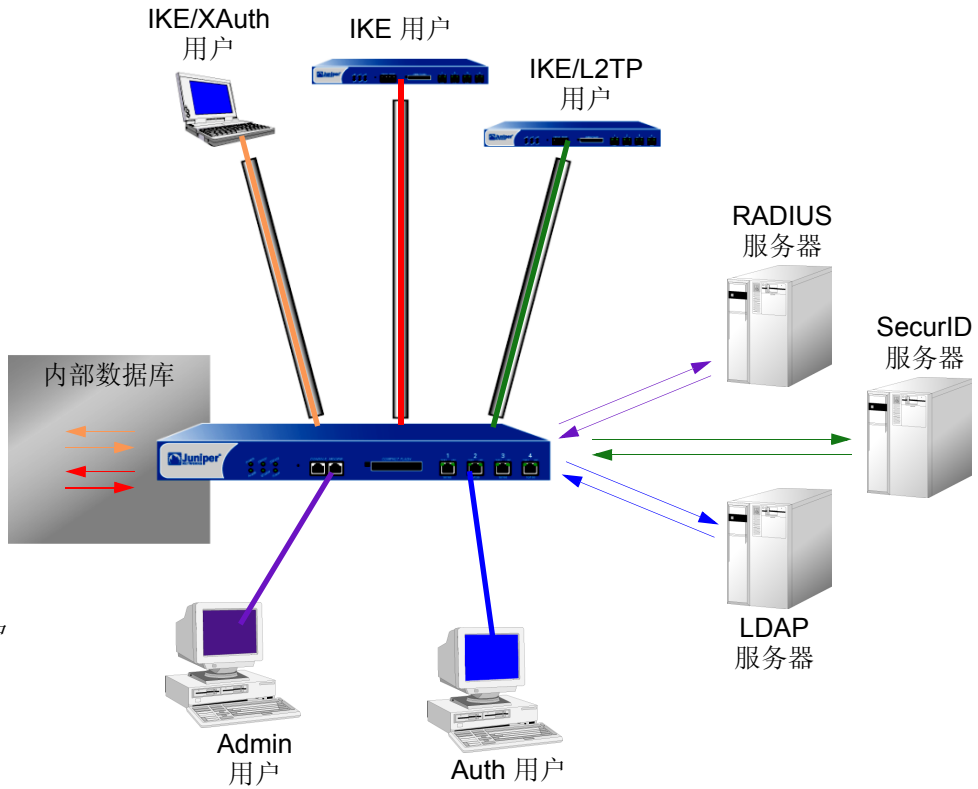
IKE/XAuth 用户 (橙色) –> 本地数据库

IKE 用户 (红色) –> 本地数据库

IKE/L2TP 用户 (绿色) –> SecurID 服务器

Admin 用户 (紫色) –> RADIUS 服务器

Auth 用户 (蓝色) –> LDAP 服务器

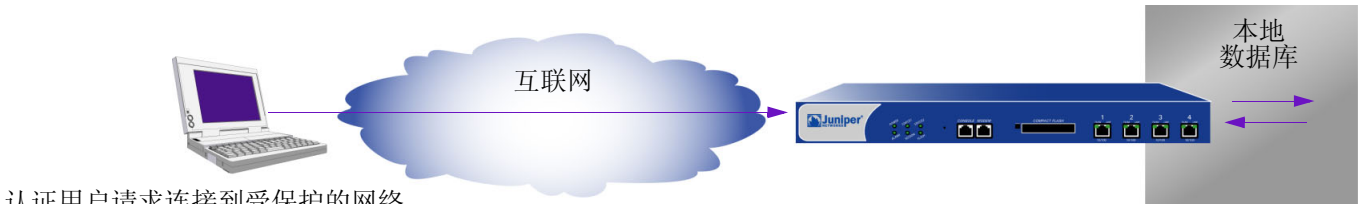


注意：*可使用一个认证服务器完成多种类型的用户认证。例如，RADIUS 服务器可同时存储 admin、auth、L2TP 和 XAuth 用户。*

以下部分进一步详细研究本地数据库以及各种认证服务器。

本地数据库

所有 NetScreen 设备都支持使用内置用户数据库进行认证。在 NetScreen 设备上定义用户时， NetScreen 设备将用户名和密码输入到其本地数据库中。



认证用户请求连接到受保护的网络。

NetScreen 设备在批准连接请求之前，会查阅其内部数据库，对认证用户进行身份认证。

支持的用户类型和功能

本地数据库支持以下类型的用户和认证功能：

- Auth 用户
- IKE 用户
- L2TP 用户
- XAuth 用户
- Admin 用户
- Admin 权限
- WebAuth
- 用户组
- 组表达式*

* 在 NetScreen 设备上定义组表达式，但用户和用户组必须存储在外部 RADIUS auth 服务器上。有关组表达式的详细信息，请参阅第 6 页上的 “组表达式”。

对于所有类型的认证而言，本地数据库是缺省的认证服务器 (auth 服务器)。有关如何通过 WebUI 和 CLI 向本地数据库添加用户和用户组的说明，请参阅第 41 页上的 “认证用户”和第 75 页上的 “IKE、 XAuth 和 L2TP 用户”。

范例：本地数据库超时

在缺省情况下， admin 和 auth 用户的本地数据库认证超时时限为 10 分钟。在本例中，将 admin 用户的此项设置更改为永不超时，而将 auth 用户的此项设置更改为 30 分钟后超时。

WebUI

Configuration > Admin > Management: 清除 Enable Web Management Idle Timeout 复选框，然后单击 **Apply**。

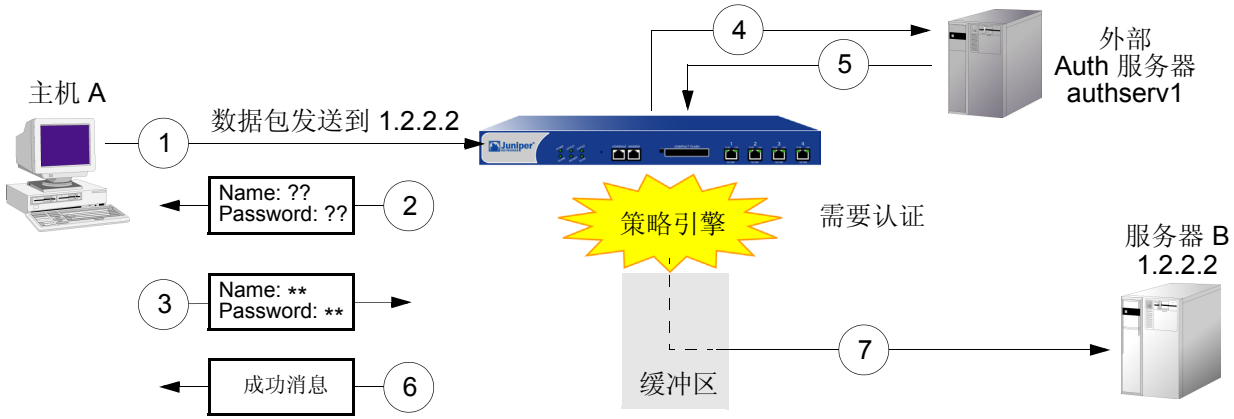
Configuration > Auth > Servers > Edit (对于 Local): 在 Timeout 字段中输入 **30**，然后单击 **Apply**。

CLI

```
set admin auth timeout 0
set auth-server Local timeout 30
save
```

外部 AUTH 服务器

一台 NetScreen 设备可与存储用户帐户的一个或多个外部认证服务器或 “auth 服务器” 相连。 NetScreen 设备在接收到要求进行认证验证的连接请求后，会请求策略、 L2TP 通道配置或 IKE 网关配置中所指定的 auth 外部服务器进行认证检查。然后， NetScreen 充当用户请求认证与 auth 服务器批准认证之间的中继器。成功的外部 auth 服务器认证检查的过程如下：

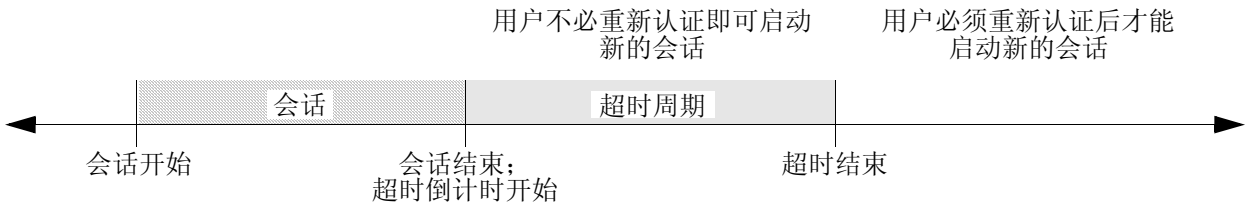


1. 主机 A 将 FTP、 HTTP 或 Telnet TCP SYN 数据包发送到 1.2.2.2。
2. NetScreen 设备截取数据包、记录其相应策略、要求从 authserv1 获得认证、将数据包放入缓冲区，并提示用户输入用户名和密码。
3. 用户以用户名和密码回复。
4. NetScreen 设备将登录信息转发到 authserv1。
5. Authserv1 将成功通知发送回 NetScreen 设备。
6. NetScreen 设备通知 auth 用户登录成功。
7. 然后， NetScreen 设备将数据包从其缓冲区转发到其目的地 1.2.2.2。

Auth 服务器对象属性

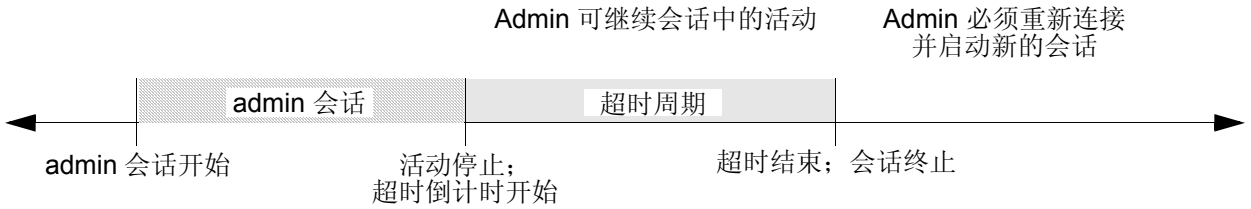
NetScreen 设备将每个 auth 服务器视为可在策略、 IKE 网关和 L2TP 通道中引用的一个对象。以下属性定义并唯一标识 auth 服务器对象 :

- 对象名 : 名称字符串，如 “authserv1” (唯一的预定义 auth 服务器为 “Local”。)
- ID 号 : 可手动设置 ID 号，也可让 NetScreen 设备自动对其进行设置。如果设置 ID 号，则必须选择未使用的号码。
- 类型 : RADIUS、 SecurID、 LDAP。
- 服务器名称 : 服务器的 IP 地址或域名。
- 备份服务器 1: 主备份服务器的 IP 地址或域名。
- 备份服务器 2: (RADIUS 和 LDAP) 辅助备份服务器的 IP 地址或域名。
- 帐户类型 : 以下一种或多种用户类型 : Auth、 L2TP、 XAuth ； 或仅 Admin。
- 超时值 : 对于不同的用户 (auth 用户或 admin 用户)，超时值具有不同的意义。
  - Auth 用户 : 第一个认证会话完成后开始超时倒计时。如果用户在倒计时达到超时临界值前发起新的会话，则不必重新认证，超时倒计时功能会自动重置。缺省超时值为 10 分钟，最大值为 255 分钟。也可将超时值设置为 0，此时认证周期将永远不会超时。



注意 : *用户认证超时与会话空闲超时不同。如果在预定的时间长度内，某会话中未发生任何活动，NetScreen 设备会自动将该会话从其会话表中移除。*

– Admin 用户：如果空闲时间长度达到超时临界值， NetScreen 设备将终止 admin 会话。要继续管理 NetScreen 设备， admin 必须重新连接到该设备并重新认证。缺省超时值为 10 分钟，最大值为 1000 分钟。也可将超时值设置为 0，此时 admin 会话将永远不会超时。



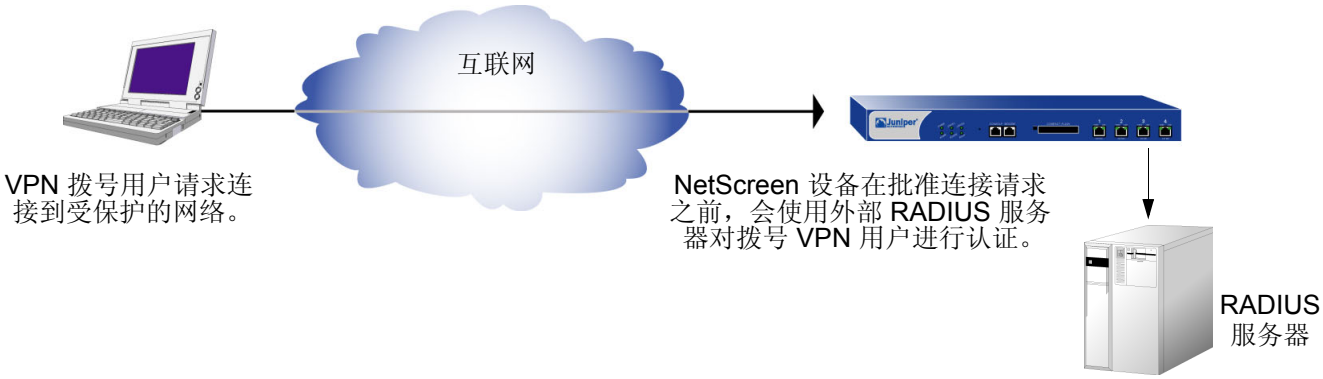
除上述适用于所有 auth 服务器对象的属性外，每个服务器还具有一些自己专有的属性。这些内容将在后续的 RADIUS、 SecurID 和 LDAP auth 服务器属性部分中加以说明。

AUTH 服务器类型

除内部数据库外， NetScreen 设备还支持三种类型的外部 auth 服务器 : RADIUS、 SecurID 和 LDAP。

RADIUS

远程认证拨号的用户服务 (RADIUS) 是一个用于认证服务器的协议，它最多可支持几万个用户。



RADIUS 客户端 (即 NetScreen 设备) 通过客户端与服务器之间的一系列通信对用户进行认证。通常，RADIUS 会要求登录人员输入其用户名和密码。然后，它将这些值与其数据库中的对应值比较，用户通过认证后，客户端即允许其访问相应的网络服务。

要针对 RADIUS 配置 NetScreen 设备，必须指定 RADIUS 服务器的 IP 地址并定义共享机密 — 与 RADIUS 服务器上的定义相同。共享机密是一个密码， RADIUS 服务器用它来生成密钥，以便对 NetScreen 和 RADIUS 设备之间的信息流进行加密。

RADIUS Auth 服务器对象属性

除第 21 页上的 “Auth 服务器对象属性”中列出的通用 auth 服务器属性外， RADIUS 服务器还使用以下属性 :

- **Shared Secret:** NetScreen 设备与 RADIUS 服务器之间共享的机密 (密码)。设备利用此机密将其向 RADIUS 服务器发送的用户密码进行加密。
- **RADIUS Port:** RADIUS 服务器上的端口号， NetScreen 设备向此处发送认证请求。缺省端口号为 1645。
- **RADIUS Retry Timeout:** 先前的请求未引发响应时，向 RADIUS 服务器发送另外的认证请求之前，NetScreen 设备等待的时间间隔 (单位为秒)。缺省值为三秒。

支持的用户类型和功能

RADIUS 服务器支持以下类型的用户和认证功能 :

- Auth 用户
- L2TP 用户 (认证和远程设置)
- XAuth 用户 (认证和远程设置)
- Admin 用户 (认证和权限指派)
- 用户组

RADIUS 服务器可支持本地数据库所支持的所有用户类型和功能 (除 IKE 用户之外)。在三种类型的外部 auth 服务器中， RADIUS 是目前唯一能支持如此众多对象的服务器。为了使 RADIUS 服务器能够支持管理权限、用户组及远程 L2TP 和 XAuth IP 地址[1]、 DNS 和 WINS 服务器地址分配等 NetScreen 专用属性，必须在 RADIUS 服务器上加载定义上述属性的 NetScreen 词典文件。

1. NetScreen 使用标准 RADIUS 属性进行 IP 地址分配。如果只想用 RADIUS 进行 IP 地址分配，则不必加载 NetScreen 供应商专用属性 (VSA)。

NetScreen 词典文件

词典文件用于定义可加载到 RADIUS 服务器上的供应商专用属性 (VSA)。定义上述 VSA 的值后， NetScreen 可以在用户登录 NetScreen 设备时查询这些属性。 NetScreen VSA 包括管理权限、用户组及远程 L2TP 和 XAuth IP 地址、DNS 和 WINS 服务器地址分配。 NetScreen 词典文件共有两个，一个用于 Cisco RADIUS 服务器，另一个用于 Funk Software RADIUS 服务器。如果使用 Microsoft RADIUS 服务器，则不会有任何词典文件。必须如 *Bi-Directional NetScreen Remote VPN using xAuth and Firewall Authentication with Microsoft Internet Authentication Service (IAS)* 中所述对其进行配置，该文件可从以下网址下载 : http://ns200-support.netscreen.com/knowbase/root/public/ns10382.pdf。

每个 NetScreen 词典文件都包含以下具体信息 :

- **Vendor ID:** NetScreen 供应商 ID (VID ； 也称 “IETF 编号”) 为 3224。 VID 用于识别特殊属性的具体供应商。某些类型的 RADIUS 服务器要求为每个属性条目输入 VID，而其它类型则只要求输入一次，然后即可全局应用。有关详细信息，请参阅 RADIUS 服务器文档。
- **Attribute Name:** 属性名用于描述各 NetScreen 专用属性，例如 NS-Admin-Privilege、 NS-User-Group、NS-Primary-DNS-Server 等等。
- **Attribute Number:** 属性编号用于识别各供应商专用属性。 NetScreen 专用属性编号分为两个范围 :
  - NetScreen ScreenOS: 1 – 199
  - NetScreen-Global PRO: 200 以上

  例如，用户组的 ScreenOS 属性编号为 3。用户组的 NetScreen-Global PRO 属性编号为 200。
- **Attribute Type:** 属性类型用于确定属性数据 (或 “值”) 的显示形式 — 字符串、 IP 地址或整数。

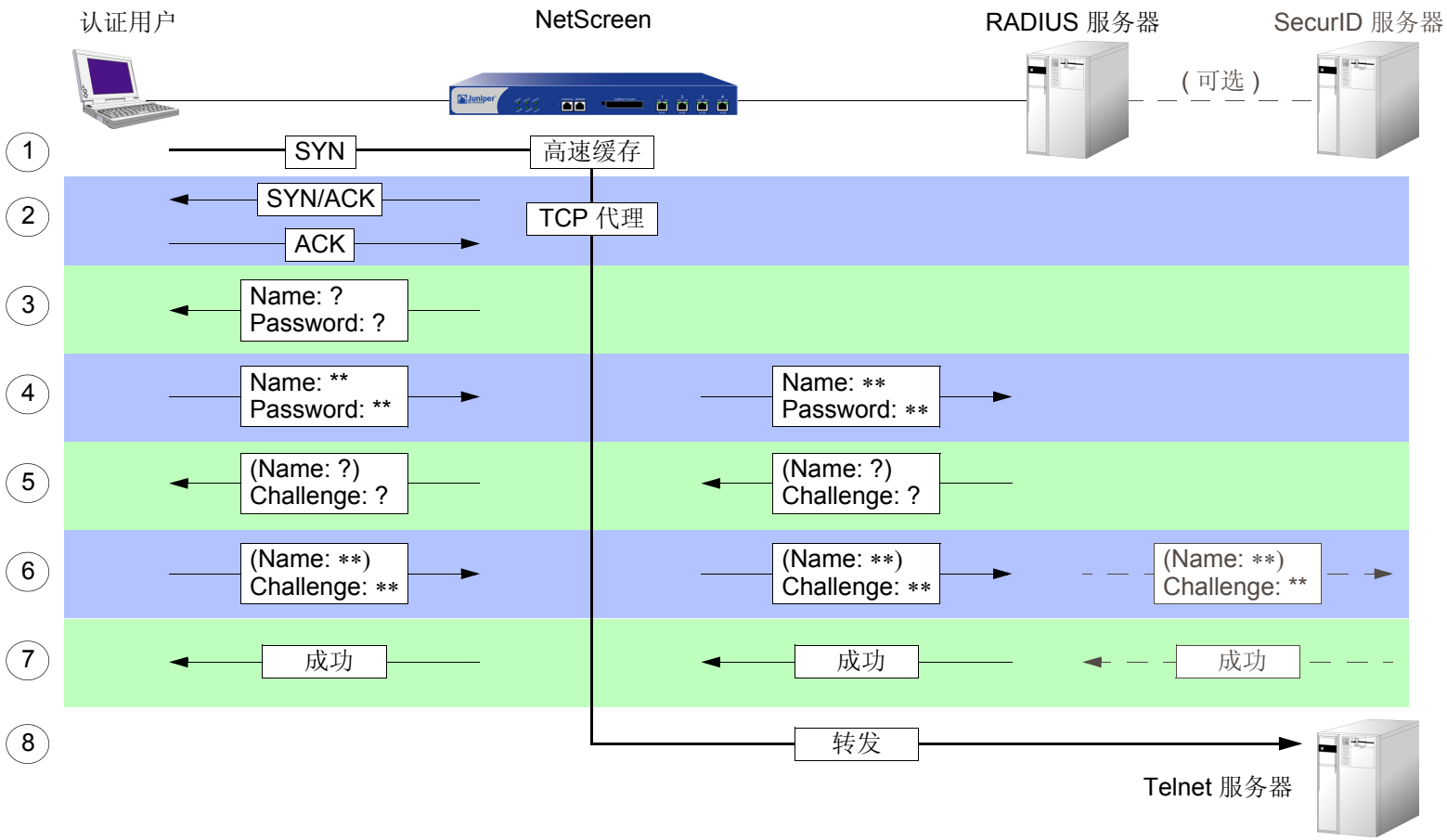
向 RADIUS 服务器加载 NetScreen 词典文件时，服务器会自动接收上述信息。要输入新数据，必须以属性类型所指定的形式手动输入所需值。例如，为读写 admin 输入如下条目 :

VID	属性名	属性编号	属性类型	值
3224	NS-Admin-Privileges	1	data=int4 (即整数)	2 (2 = 全部权限)

要下载词典文件，请转到 http://www.juniper.net/customers/csc/research/netscreen_kb/downloads/dictionary/funk_radius.zip 或 http://www.juniper.net/customers/csc/research/netscreen_kb/downloads/dictionary/cisco_radius.zip，进行登录，然后将文件保存到本地驱动器。

RADIUS 访问质询

现在，当认证用户尝试通过 Telnet 登录时， NetScreen 设备可以处理外部 RADIUS 服务器的 “访问质询”数据包。批准用户名和密码后，“访问质询”向登录过程提供附加条件。在认证用户响应登录提示、输入正确的用户名和密码后， RADIUS 服务器向 NetScreen 设备发送 “访问质询”，然后 NetScreen 设备将其转发给用户。用户回应后，NetScreen 设备向 RADIUS 服务器发送含有用户响应的新的 “访问请求”。如果用户响应正确，则认证过程成功结束。请考虑认证用户希望 telnet 到服务器的下列方案：



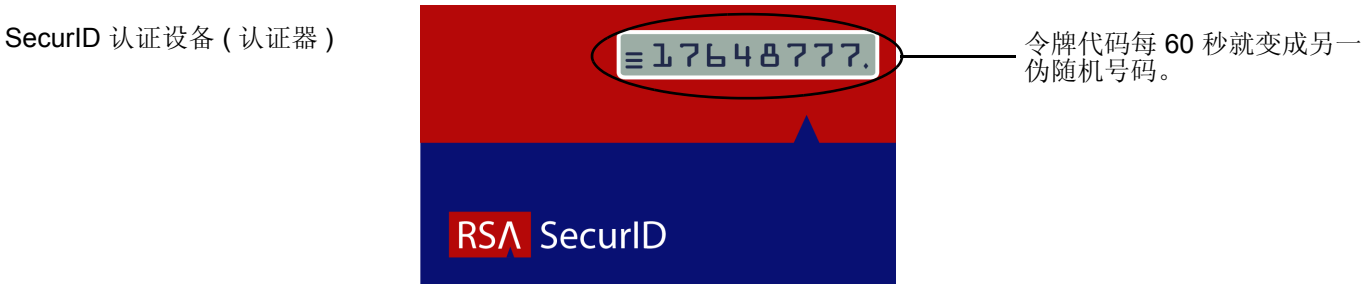
1. 认证用户发送 SYN 数据包，以启动 Telnet 会话与 Telnet 服务器的 TCP 连接。
2. NetScreen 设备截取该数据包、检查其策略列表、确定该会话是否需要用户认证。NetScreen 设备缓存 SYN 数据包并代理与该用户的 TCP 三方握手。
3. NetScreen 设备提示用户输入用户名和密码进行登录。
4. 认证用户输入用户名和密码并发送给 NetScreen 设备。然后， NetScreen 设备将含有登录信息的 “访问请求” 发送到 RADIUS 服务器。
5. 如果信息正确，则 RADIUS 服务器向 NetScreen 设备发送具有 “回复消息” 属性的 “访问质询”，提示用户对质询提供响应。 (“访问质询” 可以有选择地提示认证用户再次提供用户名。第二个用户名可以与第一个相同，也可以不同。) 然后， NetScreen 设备向该用户发送另一条包括 “回复消息” 属性的登录提示。
6. 认证用户输入质询响应 (或者用户名) 并发送给 NetScreen 设备。然后， NetScreen 设备将含有用户 “访问响应” 的第二个 “访问请求” 发送到 RADIUS 服务器。

   如果 RADIUS 服务器需要通过另一台 auth 服务器对 “访问响应” 进行认证 (例如，如果 SecurID 服务器必须对令牌代码进行认证)，则 RADIUS 服务器向其它 auth 服务器发送 “访问请求”。
7. 如果 RADIUS 服务器将 “访问响应” 转发给另一台 auth 服务器，并且该服务器发送 “访问接受”，或者如果 RADIUS 服务器本身批准 “访问响应”，则 RADIUS 服务器向 NetScreen 设备发送 “访问接受” 消息。然后， NetScreen 设备通知认证用户登录成功。
8. NetScreen 设备将初始 SYN 数据包转发到其初始目的地 : Telnet 服务器。

***注意：** 在本版发行时， NetScreen 并不支持具有 L2TP 的 “访问质询”。*

SecurID

SecurID 结合两种因素来创建动态变化的密码，而不使用固定密码。 SecurID 具有一个信用卡大小的设备，称为认证器，它拥有一个用于显示随机生成的数字字符串的 LCD 窗口，这种数字字符串称为令牌代码，每分钟变化一次。用户还拥有个人识别号码 (PIN)。用户登录时，需要输入用户名、其 PIN 以及当前令牌代码。



认证器执行只有 RSA 了解的算法，创建 LCD 窗口中出现的值。被认证的用户输入其 PIN 及卡上的号码时，执行相同算法的 ACE 服务器将接收到的值与其数据库中的值进行比较。如果它们匹配，则认证成功。

NetScreen 设备和 RSA SecurID ACE 服务器之间的关系与 NetScreen 设备和 RADIUS 服务器之间的关系相似。即，NetScreen 设备充当客户端，将认证请求转发到外部服务器申请批准，并在用户和服务器之间传递登录信息。SecurID 与 RADIUS 的不同之处在于用户 “密码”中包括不断变化的令牌代码。

SecurID Auth 服务器对象属性

除第 21 页上的 “Auth 服务器对象属性”中列出的通用 auth 服务器属性外， SecurID 服务器还使用以下属性 :

- **Authentication Port:** SecurID ACE 服务器上的端口号， NetScreen 设备向此处发送认证请求。缺省端口号为 5500。
- **Encryption Type:** 用于对 NetScreen 设备与 SecurID ACE 服务器之间的通信进行加密的算法 — SDI 或 DES。
- **Client Retries:** 放弃尝试之前，SecurID 客户端 (即 NetScreen 设备) 尝试建立与 SecurID ACE 服务器的通信的次数。
- **Client Timeout:** 两次认证重试操作之间 NetScreen 设备等待的时间长度 (秒)。
- **Use Duress:** 禁止或允许使用不同 PIN 号码的选项。如果启用此选项，用户输入先前确定的强迫 PIN 号码时，NetScreen 设备会向 SecurID ACE 服务器发送一个信号，指示用户正在违背自己的意愿进行登录；即处于强迫之下。 SecurID ACE 服务器会允许访问一次，之后，它会拒绝该用户的所有其它登录尝试，直至他 / 她与 SecurID 管理员联系。只有 SecurID ACE 服务器支持此选项时，才可使用强迫模式。

支持的用户类型和功能

SecurID ACE 服务器支持以下类型的用户和认证功能 :

- Auth 用户
- L2TP 用户 (用户认证； L2TP 用户从 NetScreen 设备接收缺省 L2TP 设置)
- XAuth 用户 (用户认证；不支持远程设置指派)
- Admin 用户 (用户认证； admin 用户接收只读的缺省权限指派)

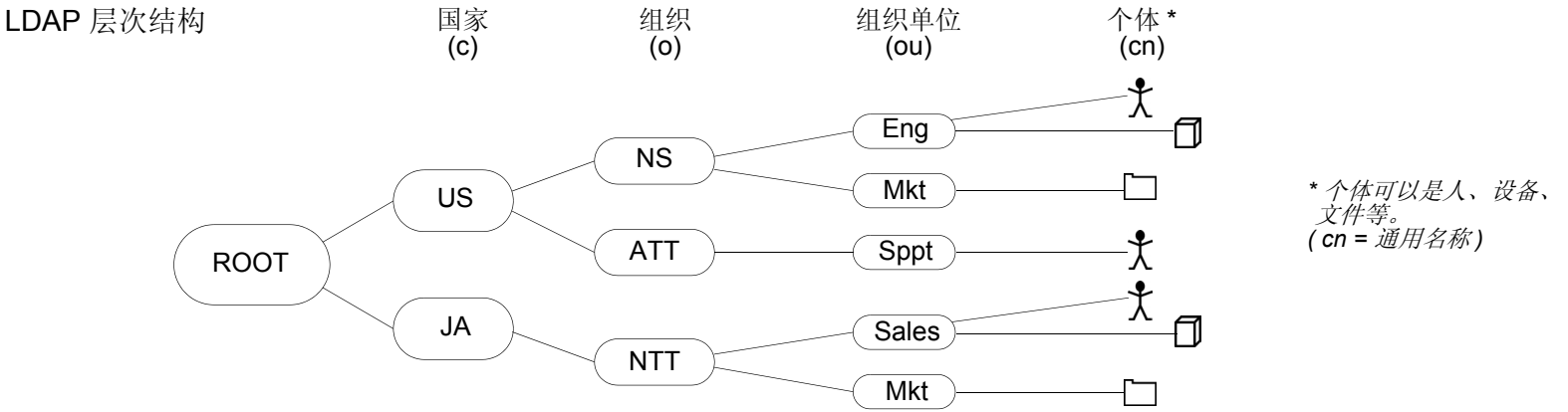
目前，尽管可使用 SecurID 服务器存储 L2TP、 XAuth 和 admin 用户帐户进行认证，但 SecurID ACE 服务器仍不能指派 L2TP 或 XAuth 远程设置或 NetScreen 管理权限。此外，与 SecurID 配套使用时， NetScreen 不支持用户组。

LDAP

轻量目录访问协议 (LDAP) 是密歇根大学在 1996 年开发出来的目录服务器标准。 LDAP 是一个用于以类似分支树的层次结构组织并访问信息的协议。其用途包括两部分：

- 确定资源位置，如网络上的组织、个体和文件等
- 帮助认证用户尝试连接由目录服务器控制的网络

LDAP 的基本结构分支至上而下依次为国家、组织、组织单位、个体。其中间还可包含其它分支层，如 “州” 和 “县” 等。下图为 LDAP 分支组织结构的一个范例。



***注意：** 有关 LDAP 的信息，请参阅* RFC-1777, “Lightweight Directory Access Protocol”。

可对 NetScreen 设备进行配置，以便链接到 “轻量目录访问协议” (LDAP) 服务器。此服务器使用 LDAP 分层式语法来唯一识别每位用户。

LDAP Auth 服务器对象属性

除第 21 页上的 “Auth 服务器对象属性”中列出的通用 auth 服务器属性外， LDAP 服务器还使用以下属性 :

- **LDAP Server Port:** LDAP 服务器上的端口号， NetScreen 设备向此处发送认证请求。缺省端口号为 389。

  注意 : 如果更改 NetScreen 设备上的 LDAP 端口号，同时也应在 LDAP 服务器上进行更改。

- **Common Name Identifier:** LDAP 服务器用来识别在 LDAP 服务器中输入的个体的标识符。例如，“uid” 表示 “用户 ID”，“cn” 表示 “通用名称”。
- **Distinguished Name (dn):** LDAP 服务器在使用通用名称标识符搜索具体条目前使用的路径。 (例如 c=us;o=juniper，其中 “c” 代表 “国家”，“o” 代表 “组织”。)

支持的用户类型和功能

LDAP 服务器支持以下类型的用户和认证功能 :

- Auth 用户
- L2TP 用户 (用户认证； L2TP 用户从 NetScreen 设备接收缺省 L2TP 设置)
- XAuth 用户 (用户认证；不支持远程设置指派)
- Admin 用户 (用户认证； admin 用户接收只读的缺省权限指派)

目前，尽管可使用 LDAP 服务器存储 L2TP、XAuth 和 admin 用户帐户进行认证，但 LDAP 服务器仍不能指派 L2TP 或 XAuth 远程设置或 NetScreen 管理权限。此外，与 LDAP 配套使用时， NetScreen 不支持用户组。

定义 AUTH 服务器对象

要在策略、IKE 网关和 L2TP 通道中引用外部认证服务器 (auth 服务器)，必须首先定义 auth 服务器对象。以下示例说明如何为 RADIUS 服务器、 SecurID 服务器和 LDAP 服务器定义 auth 服务器对象。

范例 : RADIUS Auth 服务器

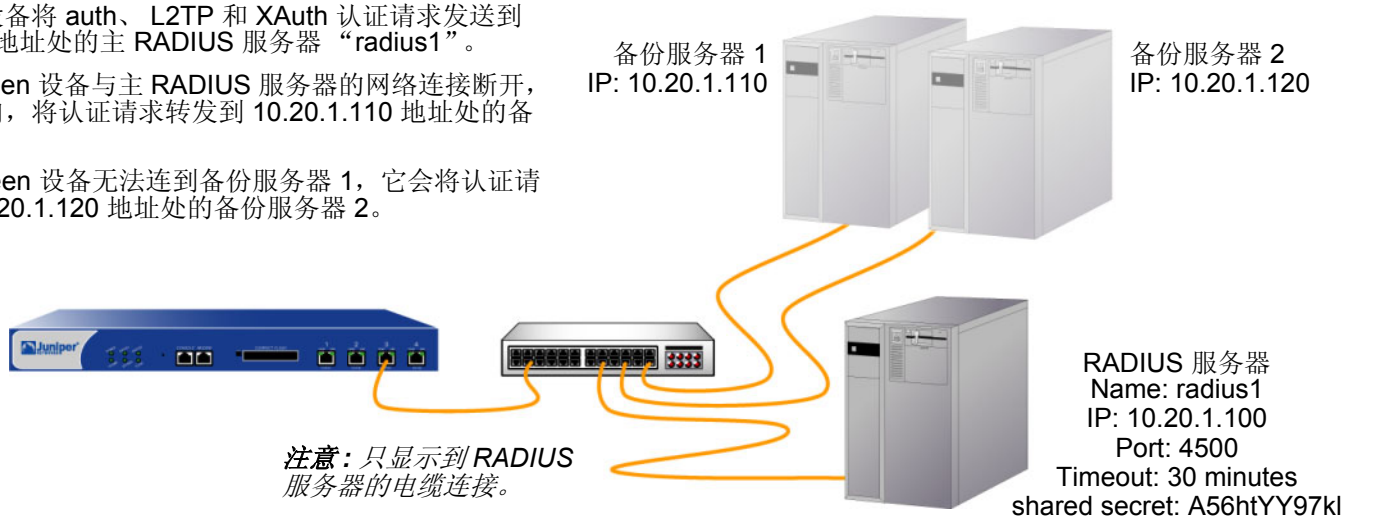
在下例中，将为 RADIUS 服务器定义 auth 服务器对象。将其用户帐户类型指定为 auth、 L2TP 和 XAuth。将 RADIUS 服务器命名为 “radius1”，并接受 NetScreen 设备自动指派的 ID 号。输入其 IP 地址 10.20.1.100 ；将其端口号由缺省值 (1645) 更改为 4500。将其共享机密定义为 “A56htYY97kl”。将认证超时值由缺省值 (10 分钟) 更改为 30 分钟，并将 RADIUS 重试超时值由 3 秒更改为 4 秒。同时将两个备份服务器的 IP 地址分别指定为 10.20.1.110 和 10.20.1.120。

此外，还要将 NetScreen 词典文件加载到 RADIUS 服务器上，使其能支持下列供应商专用属性 (VSA) 的查询 : 用户组、管理权限、远程 L2TP 和 XAuth 设置。

NetScreen 设备将 auth、 L2TP 和 XAuth 认证请求发送到 10.20.1.100 地址处的主 RADIUS 服务器 “radius1”。

如果 NetScreen 设备与主 RADIUS 服务器的网络连接断开，它会重新定向，将认证请求转发到 10.20.1.110 地址处的备份服务器 1。

如果 NetScreen 设备无法连到备份服务器 1，它会将认证请求转发到 10.20.1.120 地址处的备份服务器 2。



WebUI

Configuration > Auth > Servers > New: 输入以下内容，然后单击 **OK**:

Name: radius1

IP/Domain Name: 10.20.1.100

Backup1: 10.20.1.110

Backup2: 10.20.1.120

Timeout: 30

Account Type: Auth、 L2TP、 XAuth

RADIUS: (选择)

RADIUS Port: 4500

Retry Timeout: 4 (seconds)

Shared Secret: A56htYY97kl

将 NetScreen 词典文件加载到 RADIUS 服务器上。

***注意：**有关 NetScreen 词典文件的详细信息，请参阅第 25 页上的 “NetScreen 词典文件”。有关如何将词典文件加载到 RADIUS 服务器的说明，请参阅具体服务器的文档。*

CLI

```
set auth-server radius1 type radius
set auth-server radius1 account-type auth l2tp xauth[2]
set auth-server radius1 server-name 10.20.1.100
set auth-server radius1 backup1 10.20.1.110
set auth-server radius1 backup2 10.20.1.120
set auth-server radius1 timeout 30
set auth-server radius1 radius port 4500[3]
set auth-server radius1 radius timeout 4
set auth-server radius1 radius secret A56htYY97kl
save
```

将 NetScreen 词典文件加载到 RADIUS 服务器上。

***注意：**有关 NetScreen 词典文件的详细信息，请参阅第 25 页上的 “NetScreen 词典文件”。有关如何将词典文件加载到 RADIUS 服务器的说明，请参阅具体服务器的文档。*

2. 帐户类型的输入顺序非常重要。例如，如果首先键入 **set auth-server radius1 account-type l2tp**，则随后只能选择 **xauth**；不能在 **l2tp** 后键入 **auth**。正确顺序非常容易记住，因为它是按字母顺序排列的。
3. 更改端口号有助于防止可能有针对缺省 RADIUS 端口号 (1645) 展开的攻击。

范例 : SecurID Auth 服务器

在下例中，将为 SecurID ACE 服务器配置 auth 服务器对象。将其用户帐户类型指定为 admin。将服务器命名为“securid1”，并接受 NetScreen 设备自动指派的 ID 号。输入主服务器的 IP 地址 10.20.2.100，及备份服务器的 IP 地址 : 10.20.2.110。将其端口号由缺省值 (5500) 更改为 15000。 NetScreen 设备和 SecurID ACE 服务器使用 DES 加密法保护认证信息。允许重试三次，客户端超时值为 10 秒[4]。将空闲超时值由缺省值 (10 分钟) 更改为 60 分钟[5]。禁用 **Use Duress** 设置。

NetScreen 设备将 admin 认证请求发送到 10.20.2.100 地址处的主 SecurID 服务器 “securid1”。

如果 NetScreen 设备与主 SecurID 服务器的网络连接断开，它会重新定向，将认证请求转发到 10.20.2.110 地址处的备份服务器 1。

注意 : *NetScreen 针对 SecurID 只支持一个备份服务器。*

4. 客户端超时值是指两次认证重试操作之间 SecurID 客户端 (即 NetScreen 设备) 等待的时间长度 (秒)。
5. 空闲超时值是指 NetScreen 设备在自动终止非活动 admin 会话前等待的空闲时间长度 (分钟)。(有关应用于 admin 用户和其它用户类型的超时值比较信息，请参阅第 21 页上的 “Auth 服务器对象属性”。)

WebUI

Configuration > Auth > Servers > New: 输入以下内容，然后单击 **OK**:

Name: securid1

IP/Domain Name: 10.20.2.100

Backup1: 10.20.2.110

Timeout: 60

Account Type: Admin

SecurID: (选择)

Client Retries: 3

Client Timeout: 10 seconds

Authentication Port: 15000

Encryption Type: DES

User Duress: No

CLI

```
set auth-server securid1 type securid
set auth-server securid1 server-name 10.20.2.100
set auth-server securid1 backup1 10.20.2.110
set auth-server securid1 timeout 60
set auth-server securid1 account-type admin
set auth-server securid1 securid retries 3
set auth-server securid1 securid timeout 10
set auth-server securid1 securid auth-port 15000
set auth-server securid1 securid encr 1
set auth-server securid1 securid duress 0
save
```

范例 : LDAP Auth 服务器

在下例中，将为 LDAP 服务器配置 auth 服务器对象。将用户帐户类型指定为 auth。将 LDAP 服务器命名为“ldap1”，并接受 NetScreen 设备自动指派的 ID 号。输入其 IP 地址 10.20.3.100 ；将其端口号由缺省值 (389) 更改为 19830。将超时值由缺省值 (10 分钟) 更改为 40 分钟。同时将两个备份服务器的 IP 地址分别指定为 10.20.3.110 和 10.20.3.120。 LDAP 通用名称标识符为 cn， Distinguished Name (识别名称) 为 c=us;o=juniper;ou=marketing。

NetScreen 设备将认证请求从 auth 用户发送到 10.20.3.100 地址处的主 LDAP 服务器 “ldap1”。

如果 NetScreen 设备与主 LDAP 服务器的网络连接断开，它会重新定向，将认证请求转发到 10.20.3.110 地址处的备份服务器 1。

如果 NetScreen 设备无法连到备份服务器 1，它会将认证请求转发到 10.20.3.120 地址处的备份服务器 2。

WebUI

Configuration > Auth > Servers > New: 输入以下内容，然后单击 **OK**:

Name: ldap1

IP/Domain Name: 10.20.3.100

Backup1: 10.20.3.110

Backup2: 10.20.3.120

Timeout: 40

Account Type: Auth

LDAP: (选择)

LDAP Port: 4500

Common Name Identifier: cn

Distinguished Name (dn): c=us;o=juniper;ou=marketing

CLI

```
set auth-server ldap1 type ldap
set auth-server ldap1 account-type auth
set auth-server ldap1 server-name 10.20.3.100
set auth-server ldap1 backup1 10.20.3.110
set auth-server ldap1 backup2 10.20.3.120
set auth-server ldap1 timeout 40
set auth-server ldap1 ldap port 15000
set auth-server ldap1 ldap cn cn
set auth-server ldap1 ldap dn c=us;o=juniper;ou=marketing
save
```

定义缺省 AUTH 服务器

在缺省情况下，本地数据库是所有用户类型的缺省 auth 服务器。您可针对下列一种或多种用户类型，指定外部 auth 服务器作为缺省 auth 服务器 :

- Admin
- Auth
- L2TP
- XAuth

这样，在策略、 L2TP 通道、或 IKE 网关中配置认证时，如果希望对具体用户类型使用缺省 auth 服务器，则不必在每个配置中都指定 auth 服务器。 NetScreen 设备会引用先前已指定为缺省服务器的相应 auth 服务器。

范例 : 更改缺省 Auth 服务器

在本例中，将使用先前范例中创建的 RADIUS、 SecurID 和 LDAP auth 服务器对象 :

- radius1 (第 32 页上的 “范例 : RADIUS Auth 服务器”)
- securid1 (第 35 页上的 “范例 : SecurID Auth 服务器”)
- ldap1 (第 37 页上的 “范例 : LDAP Auth 服务器”)

然后，指定本地数据库、 radius1、 securid1 和 ldap1 作为下列用户类型的缺省服务器 :

- Local: XAuth 用户的缺省 auth 服务器[6]
- radius1: L2TP 用户的缺省 auth 服务器
- securid1: admin 用户的缺省 auth 服务器
- ldap1: auth 用户的缺省 auth 服务器

6. 在缺省情况下，本地数据库是所有用户类型的缺省 auth 服务器。因此，除非先前已为 XAuth 用户指定外部 auth 服务器作为缺省服务器，否则不必进行此配置。

WebUI

VPNs > AutoKey Advanced > XAuth Settings: 从 Default Authentication Server 下拉列表中选择 **Local**，然后单击 **Apply**[7]。

VPNs > L2TP > Default Settings: 从 Default Authentication Server 下拉列表中选择 **radius1**，然后单击 Apply。

Configuration > Admin > Administrators: 从 Admin Auth Server 下拉列表中选择 **Local/securid1**，然后单击 **Apply**。

Configuration > Auth > Firewall: 从 Default Auth Server 下拉列表中选择 **ldap1**，然后单击 **Apply**。

CLI

```
set xauth default auth server Local[7]
set l2tp default auth server radius1
set admin auth server securid1
set auth default auth server ldap1
save
```

7. 在缺省情况下，本地数据库是所有用户类型的缺省 auth 服务器。因此，除非先前已为 XAuth 用户指定外部 auth 服务器作为缺省服务器，否则不必进行此配置。

3

认证用户

认证用户 (或 “auth 用户”) 指启动通过防火墙的连接时必须提供用户名和密码进行认证的网络用户。可将 auth 用户帐户存储在本地数据库或外部 RADIUS、 SecurID 或 LDAP 服务器上。

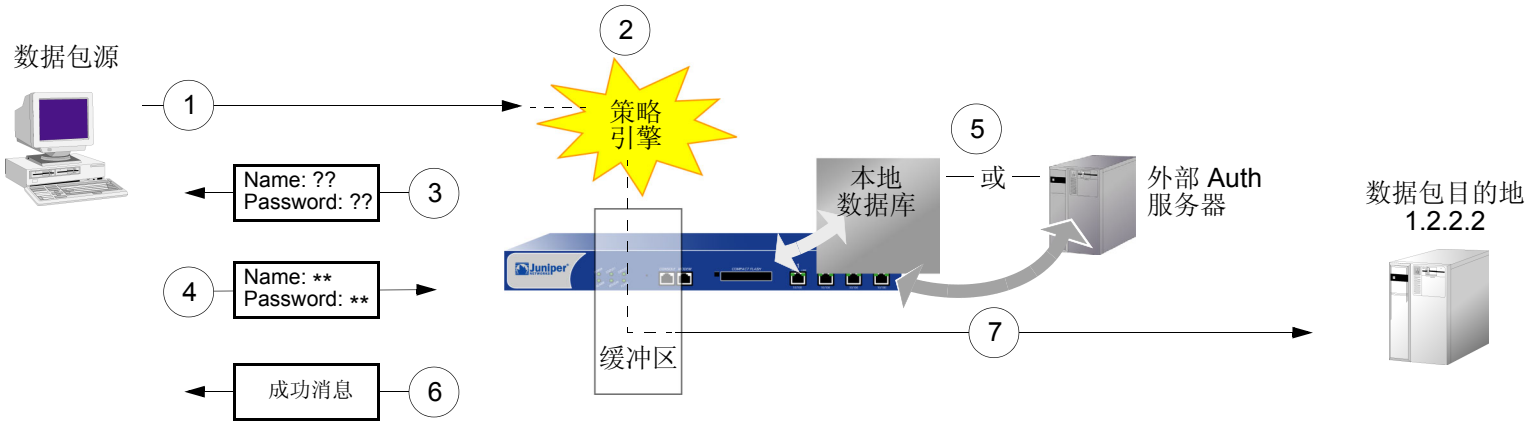
可将多个 auth 用户帐户集合到一起组成 auth 用户组，用户组可以存储在本地数据库或 RADIUS 服务器上。单个 auth 用户帐户最多可以存在于本地数据库或 RADIUS 服务器上的四个用户组中。如果在 RADIUS 服务器上创建外部用户组，也必须在 NetScreen 设备上创建一个相同 (但空白) 的用户组。例如，如果在名为 “rs1” 的 RADIUS 服务器上定义一个名为 “au_grp1” 的 auth 用户组，并在组中添加 10 个成员，则在 NetScreen 设备上必须也定义一个名为 “au_grp1” 的 auth 用户组，将其标识为外部用户组，但不在其中添加成员。如果在策略中引用外部 auth 用户组 “au_grp1” 和 auth 服务器 “rs1”，则当与该策略匹配的信息流引发认证检查时， NetScreen 设备可以正确查询指定的 RADIUS 服务器。

在策略中引用 AUTH 用户

定义 auth 用户后，可创建一个要求用户通过两种认证方案之一进行认证的策略。第一种方案在与要求认证的策略匹配的 FTP、 HTTP 或 Telnet 信息流到达 NetScreen 设备时，对用户进行认证。在第二种方案中，用户在发送应用要求用户认证的策略的信息流 (任何类型，不局限于 FTP、 HTTP 或 Telnet) 之前进行认证。

运行时认证

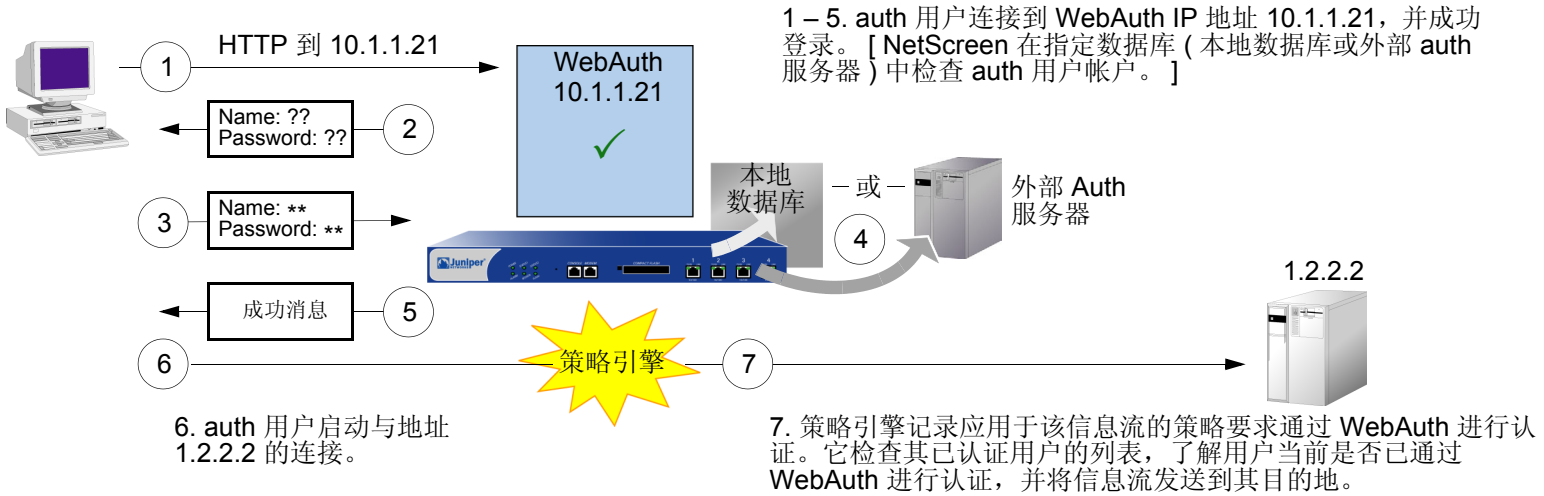
用户尝试发起 (应用要求进行认证的策略的) HTTP、FTP 或 Telnet 连接请求时， NetScreen 设备会截取该请求，并提示用户输入名称和密码 (请参阅第 **2**-306 页上的 “用户认证”)。在批准请求之前， NetScreen 设备会将用户名和密码与本地数据库或外部 auth 服务器上的用户名和密码进行比较，以确认其有效性。



1. auth 用户将 FTP、 HTTP 或 Telnet 数据包发送到 1.2.2.2。
2. NetScreen 设备截取数据包，记录其策略要求从本地数据库或 auth 服务器获得认证，并将数据包放入缓冲区。
3. NetScreen 设备提示用户通过 FTP、 HTTP 或 Telnet 输入登录信息。
4. 用户以用户名和密码回复。
5. NetScreen 设备在其本地数据库上检查 auth 用户帐户，或将登录信息发送到策略中指定的外部 auth 服务器。
6. 找到有效匹配项 (或从外部 auth 服务器接收到有效匹配的通告) 后， NetScreen 设备会通知用户登录成功。
7. NetScreen 设备将数据包从其缓冲区转发到其目的地 1.2.2.2。

策略前检查认证 (WebAuth)

将信息流发送到预定目的地之前， auth 用户发起与此 IP 地址的 HTTP 会话 (将 WebAuth 功能交由 NetScreen 设备托管)，并对自己进行认证。 NetScreen 设备对用户进行认证后，用户可根据要求通过 WebAuth 进行认证的策略的许可，将信息流发送至目的地。



有关 WebAuth 的一些详细说明 :

- 可保留本地数据库作为缺省 WebAuth auth 服务器，也可为之选择外部 auth 服务器。 WebAuth auth 服务器的主要要求是 auth 服务器必须具有 auth 用户帐户类型。
- WebAuth 地址必须与要用来托管该地址的接口处于相同的子网内。例如，如果希望 auth 用户通过 ethernet3 (IP 地址为 1.1.1.1/24) 与 WebAuth 相连，则可将 WebAuth 的 IP 地址指定在 1.1.1.0/24 子网内。
- 可将 WebAuth 地址设置在与任意物理接口、子接口或虚拟安全接口 (VSI) 相同的子网内。 (有关不同类型接口的信息，请参阅第 **2**-51 页上的 “接口”。)
- 如果要在 “透明”模式中使用 WebAuth，可将 WebAuth 地址设置在与 VLAN1 IP 地址相同的子网内。

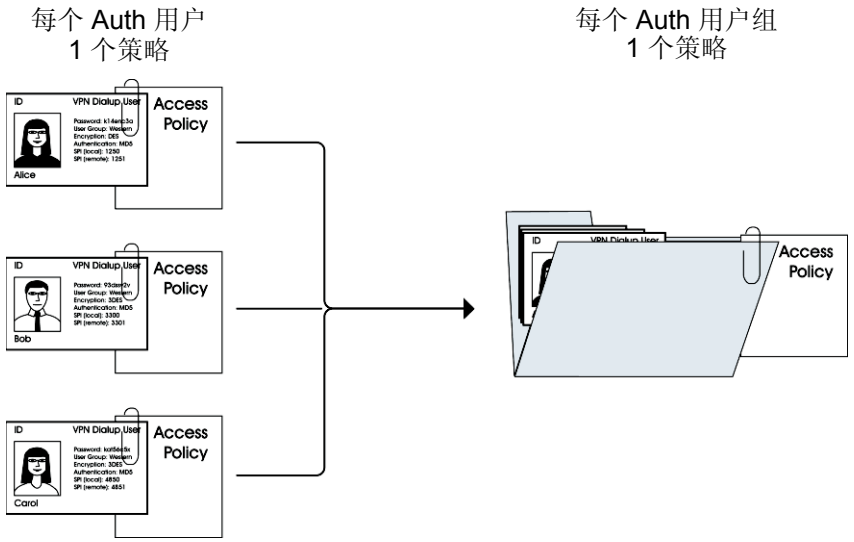
- 可将 WebAuth 地址设置于多个接口上。
- 如果在同一安全区段绑定多个接口，则可将 WebAuth 地址设置于某个接口的子网中，来自同一区段但使用不同接口的信息流仍可到达该处。
- 注意 : NetScreen 设备对特定源 IP 地址的用户进行认证，随后允许来自同一地址其他任何用户的信息流 (在需要通过 WebAuth 进行认证的策略中指定)。如果用户从 NAT 设备 (可将所有初始源地址更改为单个转换后的地址) 后面发出信息流，则实际情况可能就是这样。
- 可指示设备仅接受 WebAuth 会话的 SSL (HTTPS) 连接。

在策略中引用 AUTH 用户组

要管理多个 auth 用户，可创建 auth 用户组，并将其存储在本地 NetScreen 设备或外部 RADIUS 服务器上。

注意：*如果将用户存储到 RADIUS 服务器上的组中，则必须在 NetScreen 设备上创建空白的外部用户组，其名称与在 RADIUS 服务器上创建的用户组名称一致。*

您可将用户集合成组，使对此组实施的任何更改应用于组的所有成员，而不必分别管理每个用户。一个 auth 用户最多可以成为本地数据库或 RADIUS 服务器上的四个用户组的成员。属于多个组的 auth 用户只需提供一次用户名和密码，即可获准访问为该用户所属的每个组定义的资源。



范例：运行时认证 (本地用户)

在本例中，将定义一个名为 louis 的本地 auth 用户，其密码为 iDa84rNk，在 Trust 区段通讯簿中的地址名为“host1”。然后配置两个外向策略：一个拒绝所有出站信息流，另一个来自 host1，要求 louis 进行认证。(Louis 必须从 host1 启动所有出站信息流。) NetScreen 设备会拒绝来自其它所有地址的出站访问请求以及来自 “host1” 的未经认证信息流。

WebUI

1. 本地 Auth 用户和地址

Objects > Users > Local > New: 输入以下内容，然后单击 **OK**:

User Name: louis

Status: Enable

Authentication User: (选择)

User Password: iDa84rNk

Confirm Password: iDa84rNk

Objects > Addresses > List > New: 输入以下内容，然后单击 **OK**:

Address Name: host1

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.4/32

Zone: Trust

2. 策略

Policies > (From: Trust, To: Untrust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: ANY

Action: Deny

Policies > (From: Trust, To: Untrust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), host1

Destination Address:

Address Book Entry: (选择), Any

Service: ANY

Action: Permit

Position at Top: (选择)

> Advanced**:** 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页 :

Authentication: (选择)

Auth Server: (选择)

Use: Local

User: (选择), Local Auth User - louis

CLI

1. 本地用户和地址

```
set user louis password iDa84rNk[1]
set address trust host1 10.1.1.4/32
```

2. 策略

```
set policy from trust to untrust any any any deny
set policy top from trust to untrust host1 any any permit auth user louis
save
```

1. 在缺省情况下，要为之指定密码的用户被归类为 auth 用户。

范例：运行时认证 (本地用户组)

在本例中，将定义一个名为 auth_grp1 的本地用户组。将先前创建的 auth 用户 louis 和 lara 添加到该组中[2]。然后配置一个引用 auth_grp1 的策略。此策略为 auth_grp1 提供 FTP-GET 和 FTP-PUT 权限，令其以 Trust 区段中“auth_grp1”地址名 (IP 地址 10.1.8.0/24) 访问 DMZ 区段中名为 “ftp1” (IP 地址 1.2.2.3/32) 的 FTP 服务器。

WebUI

1. 本地用户组和成员

Objects > Users > Local Groups > New: 在 Group Name 字段中输入 **auth_grp1**，执行以下操作，然后单击 **OK**:

选择 **louis**，并使用 **<<** 按钮将其从 Available Members 栏移动到 Group Members 栏中。

选择 **lara**，并使用 **<<** 按钮将其从 Available Members 栏移动到 Group Members 栏中。

2. 地址

Objects > Addresses > List > New: 输入以下内容，然后单击 **OK**:

Address Name: auth_grp1

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.8.0/24

Zone: Trust

2. 在本地数据库中创建用户组时，在向组中添加用户之前，用户组的用户类型不会定义。而添加用户后，用户组会获得与添加于其中的用户相同的类型。通过添加 auth、 IKE、 L2TP 和 XAuth 用户类型可创建多类型用户组。不能将 Admin 用户与其它任意用户类型组合。

Objects > Addresses > List > New: 输入以下内容，然后单击 **OK**:

Address Name: ftp1

IP Address/Domain Name:

IP/Netmask: (选择), 1.2.2.3/32

Zone: DMZ

3. 策略

Policies > (From: Trust; To: DMZ) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), auth_grp1

Destination Address:

Address Book Entry: (选择), ftp1

Service: FTP

Action: Permit

Position at Top: (选择)

> Advanced: 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页 :

Authentication: (选择)

Auth Server: (选择)

Use: Local

User Group: (选择), Local Auth Group - auth_grp1

CLI

1. 本地用户组和成员

```
set user-group auth_grp1 location local
set user-group auth_grp1 user louis
set user-group auth_grp1 user lara
```

2. 地址

```
set address trust auth_grp1 10.1.8.0/24
set address dmz ftp1 1.2.2.3/32
```

3. 策略

```
set policy top from trust to dmz auth_grp1 ftp1 ftp permit auth user-group
    auth_grp1
save
```

范例 : 运行时认证 (外部用户)

在本例中，将定义名为 “x_srv1” 的外部 LDAP auth 服务器，其属性如下 :

- Account type: auth
- IP address: 10.1.1.100
- Backup1 IP address: 10.1.1.110
- Backup2 IP address: 10.1.1.120
- Authentication timeout: 60 minutes
- LDAP port number: 14500
- Common name identifier: cn
- Distinguished name: c=us;o=netscreen

以密码 eTcS114u 将 auth 用户 “euclid” 加载到外部 auth 服务器上。然后，为外部用户 euclid 配置要求在 auth 服务器 x_srv1 上进行认证的外向策略。

WebUI

1. Auth 服务器

Configuration > Auth > Servers > New: 输入以下内容，然后单击 **OK**:

Name: x_srv1

IP/Domain Name: 10.1.1.100

Backup1: 10.1.1.110

Backup2: 10.1.1.120

Timeout: 60

Account Type: Auth

LDAP: (选择)

LDAP Port: 14500

Common Name Identifier: cn

Distinguished Name (dn): c=us;o=netscreen

2. 外部用户

在外部 LDAP auth 服务器 x_serv1 上定义 auth 用户 “euclid”，密码为 eTcS114u。

3. 地址

Objects > Addresses > List > New: 输入以下内容，然后单击 **OK**:

Address Name: euc_host

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.20/32

Zone: Trust

4. 策略

Policies > (From: Trust, To: Untrust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: ANY

Action: Permit

Position at Top: (选择)

> Advanced: 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页：

Authentication: (选择)

Auth Server: (选择)

Use: x_srv1

User: (选择), External User

External User: euclid

CLI

1. Auth 服务器

```
set auth-server x_srv1
set auth-server x_srv1 type ldap
set auth-server x_srv1 account-type auth
set auth-server x_srv1 server-name 10.1.1.100
set auth-server lx_srv1 backup1 10.1.1.110
set auth-server x_srv1 backup2 10.1.1.120
set auth-server x_srv1 timeout 60
set auth-server x_srv1 ldap port 14500
set auth-server x_srv1 ldap cn cn
set auth-server x_srv1 ldap dn c=us;o=netscreen
```

2. 外部用户

在外部 LDAP auth 服务器 x_serv1 上定义 auth 用户 “euclid”，密码为 eTcS114u。

3. 地址

```
set address trust euc_host 10.1.1.20/32
```

4. 策略

```
set policy top from trust to untrust euc_host any any auth server x_srv1 user
    euclid
save
```

范例：运行时认证 (外部用户组)

在本例中，将配置名为 “radius1” 的外部 RADIUS auth 服务器[3]，定义名为 “auth_grp2” 的外部 auth 用户组。在下列两个位置定义外部 auth 用户组 auth_grp2:

1. 外部 RADIUS auth 服务器 “radius1”
2. NetScreen 设备

只在 RADIUS 服务器上将 auth 用户加入 auth 用户组 “auth_grp2” 中，而将 NetScreen 设备上的组保留为空白。此组中的成员是要求独占访问 IP 地址 10.1.1.80 处服务器的会计师。为该服务器创建一个通讯簿条目，并将地址命名为 “midas”。然后配置一个区段内部策略，只允许经认证的信息流从 auth_grp2 流向 midas，这两者均位于 Trust 区段中。 (有关区段内部策略的详细信息，请参阅第 **2**-293 页上的 “策略”。)

RADIUS 服务器

1. 将 NetScreen 词典文件加载到 RADIUS 服务器上[4]。

   ***注意：**有关 NetScreen 词典文件的信息，请参阅第 25 页上的 “NetScreen 词典文件”。有关将词典文件加载到 RADIUS 服务器的说明，请参阅 RADIUS 服务器文档。*

2. 在 RADIUS 服务器上定义 auth 用户帐户后，使用 NetScreen 用户组 VSA 创建用户组 “auth_grp2”，并将其应用于要添加到该组中的 auth 用户帐户。

3. RADIUS auth 服务器的配置与第 32 页上的 “范例 : RADIUS Auth 服务器”中大致相同，但本例中仅指定 “auth” 作为用户帐户类型。
4. 如果使用 Microsoft IAS RADIUS 服务器，则没有词典文件要加载。而应在服务器上定义正确的供应商专用属性 (VSA)。

WebUI

1. Auth 服务器

   Configuration > Auth > Servers > New: 输入以下内容，然后单击 **OK**:

   Name: radius1

   IP/Domain Name: 10.20.1.100

   Backup1: 10.20.1.110

   Backup2: 10.20.1.120

   Timeout: 30

   Account Type: Auth

   RADIUS: (选择)

   RADIUS Port: 4500

   Shared Secret: A56htYY97kl

2. 外部用户组

   Objects > Users > External Groups> New: 输入以下内容，然后单击 **OK**:

   Group Name: auth_grp2

   Group Type: Auth

3. 地址

   Objects > Addresses > List > New: 输入以下内容，然后单击 **OK**:

   Address Name: midas

   IP Address/Domain Name:

   IP/Netmask: (选择), 10.1.1.80/32

   Zone: Trust

4. 策略

Policies > (From: Trust， To: Trust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), midas

Service: ANY

Action: Permit

Position at Top: (选择)

> Advanced: 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页：

Authentication: (选择)

Auth Server: (选择)

Use: radius1

User Group: (选择), External Auth Group - auth_grp2

CLI

1. Auth 服务器

```
set auth-server radius1 type radius
set auth-server radius1 account-type auth
set auth-server radius1 server-name 10.20.1.100
set auth-server radius1 backup1 10.20.1.110
set auth-server radius1 backup2 10.20.1.120
set auth-server radius1 timeout 30
set auth-server radius1 radius port 4500
set auth-server radius1 radius secret A56htYY97kl
```

2. 外部用户组

```
set user-group auth_grp2 location external
set user-group auth_grp2 type auth
```

3. 地址

```
set address trust midas 10.1.1.80/32
```

4. 策略

```
set policy top from trust to trust any midas any permit auth server radius1
    user-group auth_grp2
save
```

范例：多个组中的本地 Auth 用户

在本例中，将定义一个名为 Mary 的本地 auth 用户。 Mary 是一名销售经理，需要访问下列两台服务器：销售人员 (sales_reps 组) 使用的服务器 A 和经理 (sales_mgrs 组) 使用的服务器 B。要提供对这两台服务器的访问权限，需要将 Mary 添加到这两个用户组中。然后创建两个策略 — 每组一个策略。

注意：*本例并不说明其他组成员的配置。*

WebUI

1. 本地用户

   Objects > Users > Local > New: 输入以下内容，然后单击 **OK**:

   User Name: mary

   Status: Enable

   Authentication User: (选择)

   User Password: iFa8rBd

   Confirm Password: iFa8rBd

2. 本地用户组和成员

   Objects > Users > Local Groups > New: 在 Group Name 字段中输入 **sales_mgrs**，执行以下操作，然后单击 **OK**:

   选择 **mary**，并使用 **<<** 按钮将其从 Available Members 栏移动到 Group Members 栏中。

   Objects > Users > Local Groups > New: 在 Group Name 字段中输入 **sales_reps**，执行以下操作，然后单击 **OK**:

   选择 **mary**，并使用 **<<** 按钮将其从 Available Members 栏移动到 Group Members 栏中。

3. 地址

Objects > Addresses > List > New: 输入以下内容，然后单击 **OK**:

Address Name: sales

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.8.0/24

Zone: Trust

Objects > Addresses > List > New: 输入以下内容，然后单击 **OK**:

Address Name: server_a

IP Address/Domain Name:

IP/Netmask: (选择), 1.1.1.5/32

Zone: Untrust

Objects > Addresses > List > New: 输入以下内容，然后单击 **OK**:

Address Name: server_b

IP Address/Domain Name:

IP/Netmask: (选择), 1.1.1.6/32

Zone: Untrust

4. 策略

Policies > (From: Trust; To: Untrust)> New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), sales

Destination Address:

Address Book Entry: (选择), server_a

Service: FTP

Action: Permit

Position at Top: (选择)

> Advanced: 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页：

Authentication: (选择)

Auth Server: (选择)

Use: Local

User Group: (选择), Local Auth Group - sales_reps

Policies > (From: Trust; To: Untrust)> New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), sales

Destination Address:

Address Book Entry: (选择), server_b

Service: FTP

Action: Permit

Position at Top: (选择)

> Advanced: 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页：

Authentication: (选择)

Auth Server: (选择)

Use: Local

User Group: (选择), Local Auth Group - sales_mgrs

CLI

1. 本地用户

```
set user mary password iFa8rBd
```

2. 本地用户组和成员

```
set user-group sales_mgrs location local
set user-group sales_mgrs user mary
set user-group sales_reps location local
set user-group sales_reps user mary
```

3. 地址

```
set address trust sales 10.1.8.0/24
set address untrust server_a 1.1.1.5/32
set address untrust server_b 1.1.1.6/32
```

4. 策略

```
set policy top from trust to untrust sales server_a ftp permit auth user-group
    sales_reps
set policy top from trust to untrust sales server_b ftp permit auth user-group
    sales_mgrs
save
```

范例 : WebAuth (本地用户组)

本例中，在启动流向互联网的出站信息流之前，要求用户通过 WebAuth 方式进行预认证。在 NetScreen 设备上的本地数据库中创建名为 “auth_grp3” 的用户组。然后，为 Trust 区段中的每个人创建 auth 用户帐户，并将他们添加到 “auth_grp3” 中。

Trust 区段接口使用 ethernet1，其 IP 地址为 10.1.1.1/24。指定 10.1.1.50 作为 WebAuth IP 地址，并保留本地数据库作为缺省的 WebAuth 服务器。因此，用户在启动流向互联网的信息流之前，必须首先以 HTTP 方式连接到 10.1.1.50，并以用户名和密码登录。然后， NetScreen 设备将该用户名和密码与其数据库中的内容进行比较，以批准或拒绝认证请求。如果它批准该请求，被认证的用户将有 30 分钟的时间启动流向互联网的信息流。终止该启动会话后，在 NetScreen 设备要求用户重新认证之前，用户又有 30 分钟的时间启动另一会话。

WebUI

1. WebAuth

Configuration > Auth > WebAuth: 从 WebAuth Server 下拉列表中选择 **Local**，然后单击 **Apply**。

Network > Interfaces > Edit (对于 ethernet1): 选择 **WebAuth**，在 WebAuth IP 字段中输入 **10.1.1.50**。

Configuration > Auth > Servers > Edit (对于 Local): 在 Timeout 字段中输入 **30**，然后单击 **Apply**。

2. 用户组

Objects > Users > Local Groups > New: 在 Group Name 字段中输入 **auth_grp3**，执行以下操作，然后单击 **OK**:

选择 ***user name***，并使用 **<<** 按钮将该用户从 Available Members 栏移动到 Group Members 栏中。

重复选择过程，添加 auth 用户，直到该组完成为止。

3. 策略

Policies > (From: Trust, To: Untrust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: ANY

Action: Permit

> Advanced: 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页 :

Authentication: (选择)

WebAuth: (选择)

User Group: (选择), Local Auth Group - auth_grp3

CLI

1. WebAuth

```
set webauth server Local
set interface ethernet1 webauth-ip 10.1.1.50
set interface ethernet1 webauth
set auth-server Local timeout 30
```

2. 用户组

```
set user-group auth_grp3 location local
```

> ***注意：*** *NetScreen 设备根据添加于组中的成员类型来确定本地用户组的类型。要使 auth_grp3 成为 auth 用户组，应在组中添加一个 auth 用户。*

使用以下命令将 auth 用户添加到刚刚创建的用户组中：

```
set user-group auth_grp3 user name_str
```

3. 策略

```
set policy top from trust to untrust any any any permit webauth user-group
    auth_grp3
save
```

范例 : WebAuth (外部用户组)

WebAuth 是一种用于在用户启动通过防火墙的信息流之前进行预认证的方法。在本例中，将创建一个要求对所有外向信息流通过 WebAuth 方法进行认证的策略。

在 RADIUS 服务器 “radius1” 和 NetScreen 设备上创建名为 “auth_grp4” 的 auth 用户组。在 RADIUS 服务器上，为 Trust 区段中的每个人创建用户帐户，并将他们添加到 “auth_grp4” 中。

注意 : *此处使用的 RADIUS 服务器设置与第 32 页上的 “范例 : RADIUS Auth 服务器”中大致相同，但本例中仅指定 “auth” 作为用户帐户类型。*

Trust 区段接口使用 ethernet1，其 IP 地址为 10.1.1.1/24。指定 10.1.1.50 作为 WebAuth IP 地址，并使用外部 RADIUS auth 服务器 “radius1” 作为缺省的 WebAuth 服务器。因此，用户在启动流向互联网的信息流之前，必须首先以 HTTP 方式连接到 10.1.1.50，并以用户名和密码登录。然后， NetScreen 设备在 “radius1” 和尝试登录的用户之间中继所有 WebAuth 用户认证请求及响应。

RADIUS 服务器

1. 将 NetScreen 词典文件加载到 RADIUS 服务器上。

   注意 : *有关 NetScreen 词典文件的信息，请参阅第 25 页上的 “NetScreen 词典文件”。有关将词典文件加载到 RADIUS 服务器的说明，请参阅 RADIUS 服务器文档。*

2. 在 auth 服务器 “radius1” 上输入用户组 “auth_grp4”，然后在其中加入 auth 用户帐户。

WebUI

1. Auth 服务器

   Configuration > Auth > Servers > New: 输入以下内容，然后单击 **OK**:

   Name: radius1

   IP/Domain Name: 10.20.1.100

   Backup1: 10.20.1.110

   Backup2: 10.20.1.120

   Timeout: 30

   Account Type: Auth

   RADIUS: (选择)

   RADIUS Port: 4500

   Shared Secret: A56htYY97k

2. WebAuth

   Configuration > Auth > WebAuth: 从 WebAuth Server 下拉列表中选择 **radius1**，然后单击 **Apply**。

   Network > Interfaces > Edit (对于 ethernet1): 选择 **WebAuth**，在 WebAuth IP 字段中输入 **10.10.1.50**，然后单击 **OK**。

3. 用户组

   Objects > Users > External Groups> New: 输入以下内容，然后单击 **OK**:

   Group Name: auth_grp4

   Group Type: Auth

4. 策略

Policies > (From: Trust, To: Untrust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: ANY

Action: Permit

> Advanced: 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页 :

Authentication: (选择)

WebAuth: (选择)

User Group: (选择), External Auth Group - auth_grp4

CLI

1. Auth 服务器

```
set auth-server radius1 type radius
set auth-server radius1 account-type auth
set auth-server radius1 server-name 10.20.1.100
set auth-server radius1 backup1 10.20.1.110
set auth-server radius1 backup2 10.20.1.120
set auth-server radius1 timeout 30
set auth-server radius1 radius port 4500
set auth-server radius1 radius secret A56htYY97kl
```

2. WebAuth

```
set webauth server radius1
set interface ethernet1 webauth-ip 10.1.1.50
set interface ethernet1 webauth
```

3. 用户组

```
set user-group auth_grp4 location external
set user-group auth_grp4 type auth
```

4. 策略

```
set policy top from trust to untrust any any any permit webauth user-group
    auth_grp4
save
```

范例：仅 WebAuth + SSL (外部用户组)

在本例中，将 WebAuth 与 “安全套接字层” (SSL) 技术组合，来保护用户登录时发送的用户名和密码。 WebAuth 利用保护流向 NetScreen 设备的管理信息流的证书来通过 WebUI 实现管理。(有关 SSL 的详细信息，请参阅第 **3**-7 页上的 “安全套接字层”。)

使用外部 auth 服务器的 WebAuth 加 SSL 的配置包括以下步骤：

- 定义外部 RADIUS auth 服务器 “radius1”，在 RADIUS 服务器和 NetScreen 设备上创建名为 “auth_grp5” 的 auth 用户组。在 RADIUS 服务器上，为 Untrust 区段中的所有 auth 用户创建用户帐户，并将其添加到 “auth_grp5” 中。

  注意：*此处使用的 RADIUS 服务器设置与第 32 页上的 “范例：RADIUS Auth 服务器”中大致相同，但本例中仅指定 “auth” 作为用户帐户类型。*

- Untrust 区段接口使用 ethernet3，IP 地址为 1.1.1.1/24。将 1.1.1.50 指定为 WebAuth IP 地址，指示设备对 WebAuth 认证请求只接受 SSL 连接，并将外部 RADIUS auth 服务器 “radius1” 定义为缺省 WebAuth 服务器。
- 指定以下 SSL 设置：
  - 先前加载到 NetScreen 设备上的证书的 IDX 号 (本例中为 1)[5]
  - DES_SHA-1 密码
  - SSL 端口号 2020
- 然后，配置一个要求对从 Untrust 区段到 Trust 区段的所有信息流通过 WebAuth + SSL 方法进行认证的内向策略。

因此，用户在启动流向互联网的信息流之前，必须首先以 HTTP 方式连接到 https://1.1.1.50:2020，并以用户名和密码登录。然后， NetScreen 设备在 “radius1” 和尝试登录的用户之间中继所有 WebAuth 用户认证请求及响应。

5. 有关如何获取数字证书并将其加载到 NetScreen 设备的信息，请参阅第 **5**-23 页上的 “公开密钥密码术”。

RADIUS 服务器

1. 将 NetScreen 词典文件加载到 RADIUS 服务器上。

   ***注意：**有关 NetScreen 词典文件的信息，请参阅第 25 页上的 “NetScreen 词典文件”。有关将词典文件加载到 RADIUS 服务器的说明，请参阅 RADIUS 服务器文档。*

2. 在 auth 服务器 “radius1” 上输入用户组 “auth_grp5”，然后在其中加入 auth 用户帐户。

WebUI

1. Auth 服务器

Configuration > Auth > Servers > New: 输入以下内容，然后单击 **OK**:

Name: radius1

IP/Domain Name: 10.20.1.100

Backup1: 10.20.1.110

Backup2: 10.20.1.120

Timeout: 30

Account Type: Auth

RADIUS: (选择)

RADIUS Port: 4500

Shared Secret: A56htYY97k

2. WebAuth

Configuration > Auth > WebAuth: 从 WebAuth Server 下拉列表中选择 **radius1**，然后单击 **Apply**。

Network > Interfaces > Edit (对于 ethernet3): 输入以下内容，然后单击 **OK**:

WebAuth: (选择)

IP: 1.1.1.50

SSL Only: (选择)

3. SSL

Configuration > Admin > Management: 输入以下内容，然后单击 **OK**:

HTTPS (SSL) Port: 2020

Certificate: (选择先前加载的证书)

Cipher: DES_SHA-1

4. 用户组

Objects > Users > External Groups> New: 输入以下内容，然后单击 **OK**:

Group Name: auth_grp5

Group Type: Auth

5. 策略

Policies > (From: Untrust, To: Trust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: ANY

Action: Permit

> Advanced: 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页：

Authentication: (选择)

WebAuth: (选择)

User Group: (选择), External Auth Group - auth_grp5

CLI

1. Auth 服务器

```
set auth-server radius1 type radius
set auth-server radius1 account-type auth
set auth-server radius1 server-name 10.20.1.100
set auth-server radius1 backup1 10.20.1.110
set auth-server radius1 backup2 10.20.1.120
set auth-server radius1 timeout 30
set auth-server radius1 radius port 4500
set auth-server radius1 radius secret A56htYY97kl
```

将 NetScreen 词典文件加载到 RADIUS 服务器上。

注意：*有关 NetScreen 词典文件的信息，请参阅第 25 页上的 “NetScreen 词典文件”。有关将词典文件加载到 RADIUS 服务器的说明，请参阅 RADIUS 服务器文档。*

2. WebAuth

```
set webauth server radius1
set interface ethernet3 webauth-ip 1.1.1.50
set interface ethernet3 webauth ssl-only
```

3. SSL

```
set ssl port 2020
set ssl cert 1
set ssl encrypt des sha-1
set ssl enable
```

4. 用户组

```
set user-group auth_grp5 location external
set user-group auth_grp5 type auth
```

5. 策略

```
set policy top from untrust to trust any any any permit webauth user-group
    auth_grp5
save
```

4

IKE、 XAuth 和 L2TP 用户

本章介绍与通道协议有关的三种类型的用户 — “互联网密钥交换” (IKE) 用户、 XAuth 用户和 “第 2 层传输协议” (L2TP) 用户：

注意：*有关 IKE 和 L2TP 的更多概念性信息和配置示例，请参阅第 5 卷，“VPN”。*

IKE 用户和用户组

IKE 用户是具有动态分配 IP 地址的远程 VPN 用户。用户 (实际上是用户的设备) 在 “阶段 1” 与 NetScreen 设备协商期间，通过发送证书或 IKE ID 及预共享密钥，来对自身进行认证。

IKE ID 可以是电子邮件地址、IP 地址、域名或 ASN1-DN 字符串[1]。如果某 IKE 用户发送以下两项之一， NetScreen 设备将认证此 IKE 用户 :

- **证书**，其中 Distinguished name (DN) (识别名称) 字段或 SubAltName 字段中的一个或多个值与 NetScreen 设备上配置的用户 IKE ID 相同
- **预共享密钥**和 **IKE ID**， NetScreen 设备可从接收的 IKE ID 及其上存储的预共享密钥种子值成功生成相同的预共享密钥

在 “自动密钥” IKE 网关配置中引用 IKE 用户或用户组。将需要相同网关和通道配置的 IKE 用户集合到一个组后，只需定义一个引用该组的网关 (和一个引用该网关的 VPN 通道)，而不必为每个 IKE 用户定义一个网关和通道。

为每个主机创建独立的用户帐户常常是不可能的。在这种情况下，可创建只具有一个成员的 IKE 用户组，称为组 IKE ID 用户。该用户的 IKE ID 包含一组必须出现在拨号 IKE 用户的 IKE ID 定义中的值。如果远程拨号 IKE 用户的 IKE ID 与组 IKE ID 用户的 IKE ID 相匹配， NetScreen 将认证该远程用户。有关详细信息，请参阅第 **5** -270 页上的 “组 IKE ID”。

注意 : *IKE 用户和 IKE 用户组帐户只能存储在本地数据库上。*

1. 使用 “抽象语法表示法” 版本 1 的一个 IKE ID 示例，识别名称 (ASN1-DN) 格式为 : CN=joe,OU=it,O=netscreen,L=sunnyvale,ST=ca,C=us,E=joe@ns.com。

范例 : 定义 IKE 用户

在本例中，将定义四个 IKE 用户， Amy、 Basil、 Clara 和 Desmond，每个用户具有不同的 IKE ID 类型。

- Amy – 电子邮件地址 (用户完全合格的域名或 U-FQDN): amy@ns.com
- Basil – IP 地址 : 3.3.1.1
- Clara – 完全合格的域名 (FQDN): www.netscreen.com
- Desmond – ASN1-DN 字符串 : CN=des,OU=art,O=netscreen,L=sunnyvale,ST=ca,C=us,E=des@ns.com

WebUI

Objects > Users > Local > New: 输入以下内容，然后单击 **OK**:

User Name: Amy

Status: Enable

IKE User: (选择)

Simple Identity: (选择)

IKE ID Type: AUTO

IKE Identity: amy@ns.com

Objects > Users > Local > New: 输入以下内容，然后单击 **OK**:

User Name: Basil

Status: Enable

IKE User: (选择)

Simple Identity: (选择)

IKE ID Type: AUTO

IKE Identity: 3.3.1.1

Objects > Users > Local > New: 输入以下内容，然后单击 **OK**:

User Name: Clara

Status: Enable

IKE User: (选择)

Simple Identity: (选择)

IKE ID Type: AUTO

IKE Identity: www.netscreen.com

Objects > Users > Local > New: 输入以下内容，然后单击 **OK**:

User Name: Desmond

Status: Enable

IKE User: (选择)

Use Distinguished Name for ID: (选择)

CN: des

OU: art

Organization: netscreen

Location: sunnyvale

State: ca

Country: us

E-mail: des@ns.com

CLI

```
set user Amy ike-id u-fqdn amy@ns.com
set user Basil ike-id ip 3.3.1.1
set user Clara ike-id fqdn www.netscreen.com
set user Desmond ike-id wildcard
    CN=des,OU=art,O=netscreen,L=sunnyvale,ST=ca,C=us,E=des@ns.com
save
```

范例 : 创建 IKE 用户组

在本例中，将创建一个名为 ike_grp1 的用户组。向其中添加 IKE 用户 Amy 时，它即成为 IKE 用户组。然后添加上例第 77 页上的 “范例 : 定义 IKE 用户”中定义的其它三个 IKE 用户。

WebUI

Objects > Users > Local Groups > New: 在 Group Name 字段中输入 **ike_grp1**，执行以下操作，然后单击 **OK**:

选择 **Amy**，并使用 **<<** 按钮将其从 Available Members 栏移动到 Group Members 栏中。

选择 **Basil**，并使用 **<<** 按钮将其从 Available Members 栏移动到 Group Members 栏中。

选择 **Clara**，并使用 **<<** 按钮将其从 Available Members 栏移动到 Group Members 栏中。

选择 **Desmond**，并使用 **<<** 按钮将其从 Available Members 栏移动到 Group Members 栏中。

CLI

```
set user-group ike_grp1 location local
set user-group ike_grp1 user amy
set user-group ike_grp1 user basil
set user-group ike_grp1 user clara
set user-group ike_grp1 user desmond
save
```

在网关中引用 IKE 用户

定义 IKE 用户或 IKE 用户组后，当远程 IKE 网关是拨号用户或拨号用户组时，可在 IKE 网关配置中引用它。

以下为在网关配置中引用 IKE 用户的范例 :

- 第 **5**-231 页上的 “范例 : 基于策略的拨号 VPN，自动密钥 IKE”
- 第 **5**-276 页上的 “范例 : 组 IKE ID (证书)”
- 第 **5**-285 页上的 “范例 : 组 IKE ID (预共享密钥)”

XAuth 用户和用户组

XAuth 协议包括两个部分 : 远程 VPN 用户认证 (用户名加密码) 以及 TCP/IP 地址分配 (IP 地址、网络掩码[2]、 DNS 服务器与 WINS 服务器分配)。 NetScreen 支持其中一项或两项同时应用。

XAuth 用户或用户组是指通过 “自动密钥 IKE” VPN 通道连接到 NetScreen 设备时对自身进行认证的一个或多个远程用户，也可接受来自 NetScreen 设备的 TCP/IP 设置。 IKE 用户认证实际是对 VPN 网关或客户端的认证，而 XAuth 用户的认证则是对个体自身的认证。 XAuth 用户必须输入只有自己应该知道的信息 — 用户名和密码。

发送 VPN 信息流时，NetScreen-Remote 客户端可使用接收的 TCP/IP 设置创建一个虚拟适配器[3]，而对于非 VPN 信息流则使用 ISP 或网络管理员提供的 TCP/IP 网络适配器设置。通过为远程用户分配已知的 IP 地址，可在 NetScreen 设备上定义通过特定通道接口到达此地址的路由。然后， NetScreen 设备可以确保返回路由通过 VPN 通道而非缺省网关，到达远程用户的 IP 地址。地址分配还允许下游防火墙在创建策略时引用这些地址。您可控制 IP 地址与具有 XAuth 生存期设置的单个 XAuth 用户相关联的时间长度。

2. 分配的网络掩码始终为 255.255.255.255，并且不能修改。

3. 虚拟适配器是 TCP/IP 设置 (IP 地址、 DNS 服务器地址、 WINS 服务器地址)，它由 NetScreen 设备在 VPN 通道连接期间分配给远程用户。只有 NetScreen-Remote 客户端才支持虚拟适配器功能。 NetScreen 平台不支持此功能。

ScreenOS 支持 XAuth 的以下方面 :

- 本地 XAuth 用户和外部 XAuth 用户的认证
- 本地 XAuth 用户组和外部 XAuth 用户组的认证 (如果存储在 RADIUS auth 服务器上)
- 从 IP 地址池为本地 XAuth 用户和 RADIUS auth 服务器上存储的外部 XAuth 用户分配 IP、 DNS 服务器和 WINS 服务器地址

  要配置 NetScreen 设备，使之使用外部 RADIUS 服务器上存储的缺省 XAuth 设置，请执行以下任一操作 :

  – WebUI: 在 VPNs > AutoKey Advanced > XAuth Settings 页面上，选择 **Query Client Settings on Default Server**。
  – CLI: 输入 **set xauth default auth server** *name_str* **query-config** 命令。

  NetScreen 设备还可使用外部 RADIUS 服务器上存储的网关专用 XAuth 设置。配置具体的 IKE 网关时，请执行以下操作之一 :

  – WebUI: 在 VPNs > AutoKey Advanced > Gateway > New > Advanced 页面上，从 External Authentication 下拉列表中选择 RADIUS 服务器的名称，然后选择 **Query Remote Setting**。
  – CLI: 输入 **set ike gateway** *name_str* **xauth server** *name_str* **query-config** 命令。
- 仅认证不分配地址、仅分配地址不认证 (**set ike gateway** *name_str* **xauth bypass-auth**) 及同时进行认证和地址分配。

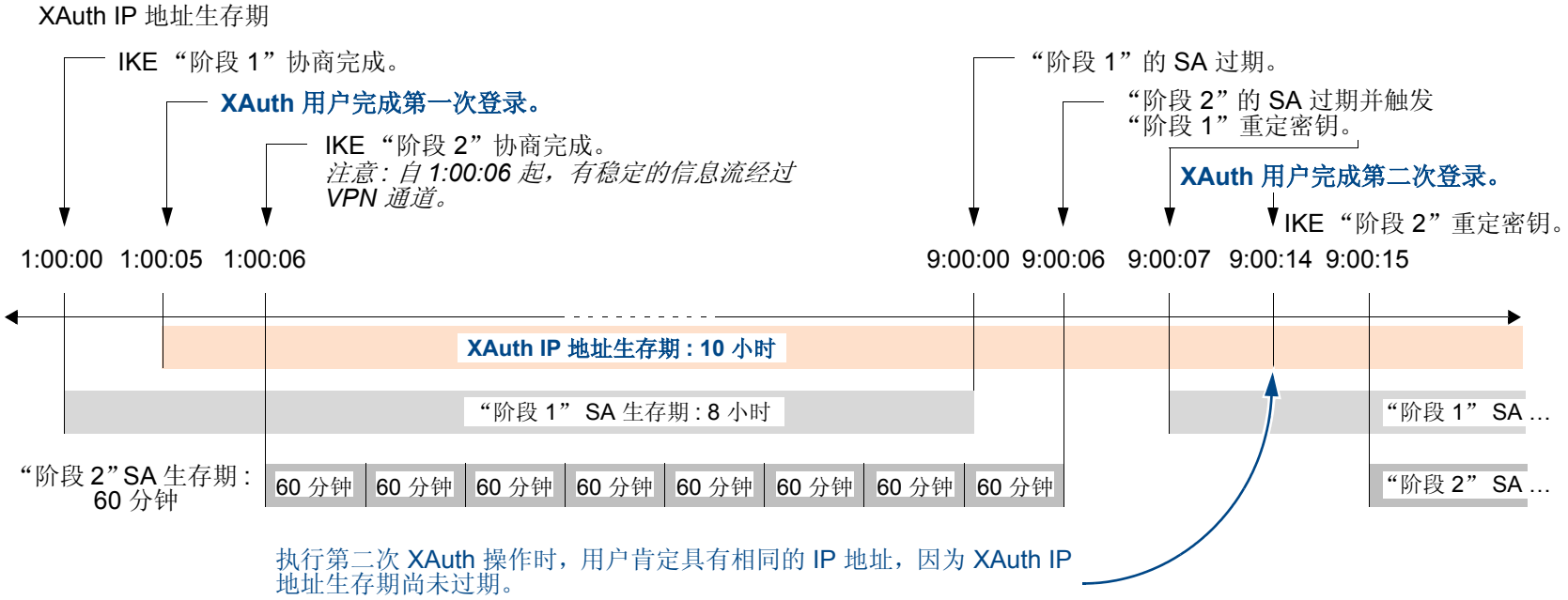
IKE 协商中的 XAuth 用户

NetScreen 支持 XAuth 版本 6 (v6)。为确保 “阶段 1” IKE 协商中的双方都支持 XAuth v6，它们在前两个 “阶段 1” 消息中都向对方发送以下供应商 ID: 0x09002689DFD6B712。此供应商 ID 号在 XAuth 互联网草案 draft-beaulieu-ike-xauth-02.txt 中指定。

“阶段 1” 协商完成后，NetScreen 设备向远程站点的 XAuth 用户发送登录提示。如果 XAuth 用户使用正确的用户名和密码成功登录，则 NetScreen 设备将为该用户分配 IP 地址、32 位网络掩码、DNS 服务器地址和 WINS 服务器地址，双方继续进行 “阶段 2” 协商。

XAuth 用户有 60 秒时间完成登录过程。如果第一次登录尝试失败，则 XAuth 用户还可进行四次尝试，每次尝试都有 60 秒时间。如果用户连续 5 次尝试均失败，则 NetScreen 设备停止提供登录提示，并切断会话。

至少，XAuth 分配的 IP 地址在指定的 XAuth 地址生存期期间属于某用户。IP 地址属于 XAuth 用户的时间可能更长，具体取决于 “阶段 1” 和 “阶段 2” 安全联盟 (SA) 重定密钥的时间。下例说明 “阶段 1” 和 “阶段 2” 重定密钥操作与 XAuth IP 地址生存期的关系。



1. “阶段 1” SA 生存期设置为 8 小时，第一个 8 小时后过期。
2. “阶段 2” SA 生存期设置为 60 分钟。由于当 XAuth 用户输入用户名和密码时，在初始 IKE 协商期间有 5 秒的延迟，所以 “阶段 1” 协商完成后，第 8 个 “阶段 2” SA 过期 8 小时 6 秒 (XAuth 登录 5 秒 + “阶段 2” 协商 1 秒)。
3. 由于有活动的 VPN 信息流，所以第 8 个 “阶段 2” SA 的到期引起 6 秒前到期的 “阶段 1” SA 重定密钥，即发生 “阶段 1” IKE 协商 (或 “重新协商”)。

4. “阶段 1” IKE 重新协商完成后， NetScreen 设备提示 XAuth 用户再次登录。

***注意：**要避免初始登录后重复进行其它登录，请用 CLI 命令为 VPN 通道配置除 0 之外的空闲时间：**set vpn** name **gateway** name **idletime** number (单位为分钟)。如果 “阶段 1” IKE 重新协商完成时有 VPN 活动，则 NetScreen 设备不会提示 XAuth 用户再次登录。利用此选项，用户可以毫无中断地下载大文件、传输或接收流动媒体、参与网络会议。*

5. 由于 XAuth 地址生存期 (10 小时) 超过了 “阶段 1” SA 生存期，所以用户保持相同的 IP 地址 — 尽管下一个 “阶段 1” 重定密钥后，用户可能得到一个不同的地址。

   如果 XAuth 地址生存期比 “阶段 1” SA 生存期短，则 NetScreen 设备会为用户分配另一个 IP 地址，它可能与先前分配的地址[4] 相同，也可能不同。

***注意：**要更改地址生存期，请执行以下操作之一：*

- (WebUI) VPNs > AutoKey Advanced > XAuth Settings: 在 Reserve Private IP for XAuth User 字段中输入数值 (分钟)，然后单击 **Apply**。
- (CLI) set xauth lifetime number

  要有效禁用地址生存期功能，请输入允许的最小值 1。

4. 如果必须为某个用户始终分配相同的 IP 地址，则可在用户配置中指定地址。然后， NetScreen 设备会分配此地址，而不是从 IP 池中随机分配一个地址。请注意，这样的地址不能在 IP 池中，否则，它可能会被分配给其他用户，而在需要时无法使用。

范例 : XAuth 认证 (本地用户)

在本例中，将在本地数据库上定义名为 x1、密码为 aGgb80L0ws 的 XAuth 用户。

然后，在远程 IKE 网关配置中对 IP 2.2.2.2 处的对等方引用该用户。将远程网关命名为 “gw1”，为 “阶段 1” 协商指定 “主” 模式和提议 pre-g2-3des-sha，并使用预共享密钥 “netscreen1”。将 VPN 通道命名为 “vpn1”，为 “阶段 2” 协商指定 “兼容” 组的提议。选择 Untrust 区段接口 ethernet3 作为出接口。

WebUI

1. XAuth 用户

Objects > Users > Local > New: 输入以下内容，然后单击 **OK**:

User Name: x1

Status: Enable

XAuth User: (选择)

User Password: iDa84rNk

Confirm Password: iDa84rNk

2. VPN

VPNs > AutoKey Advanced > Gateway > New: 输入以下内容，然后单击 **OK**:

Gateway Name: gw1

Security Level: Custom

Remote Gateway Type:

Static IP Address: (选择), Address/Hostname: 2.2.2.2

Preshared Key: netscreen1

Outgoing Interface: ethernet3

> Advanced: 输入以下高级设置，然后单击 **Return**，返回基本 Gateway 配置页 :

Security Level: Custom: (选择)

Phase 1 Proposal: pre-g2-3des-sha

Mode (Initiator): Main (ID Protection)

XAuth Server: (选择)

Local Authentication: (选择)

User: (选择), x1

VPNs > AutoKey IKE > New: 输入以下内容，然后单击 **OK**:

VPN Name: vpn1

Security Level: Compatible

Remote Gateway Tunnel: gw1

CLI

1. XAuth 用户

```
set user x1 password aGgb80L0ws
set user x1 type xauth
unset user x1 type auth
```
[5]

2. VPN

```
set ike gate gw1 ip 2.2.2.2 main outgoing-interface ethernet3 preshare
    netscreen1 proposal pre-g2-3des-sha
set ike gateway gw1 xauth server Local user x1
set vpn vpn1 gateway gw1 sec-level compatible
save
```

5. CLI 命令 **set user** *name_str* **password** *pswd_str* 将创建一个 auth 用户。要创建仅为 XAuth 类型的用户，必须将该用户定义为 XAuth 用户 (**set user** *name_str* type **xauth**)，然后删除 auth 用户定义 (**unset user** *name_str* **type auth**)。

范例 : XAuth 认证 (本地用户组)

本例中，将在本地数据库上创建一个名为 xa-grp1 的用户组，并添加在上例第 85 页上的 “范例 : XAuth 认证 (本地用户)”中创建的 XAuth 用户 “x1”。将该用户添加到组中时，它会自动成为 XAuth 用户组。

然后，在远程 IKE 网关配置中对 IP 2.2.2.2 处的对等方引用该组。将远程网关命名为 “gw2”，为 “阶段 1” 协商指定 “主模式” 和提议 pre-g2-3des-sha，并使用预共享密钥 “netscreen2”。将 VPN 通道命名为 “vpn2”，为 “阶段 2” 协商指定 “兼容” 组的提议。选择 Untrust 区段接口 ethernet3 作为出接口。

WebUI

1. XAuth 用户组

   Objects > Users > Local Groups > New: 在 Group Name 字段中输入 **xa-grp1**，执行以下操作，然后单击 **OK**:

   选择 **x1**，并使用 **<<** 按钮将其从 Available Members 栏移动到 Group Members 栏中。

2. VPN

   VPNs > AutoKey Advanced > Gateway > New: 输入以下内容，然后单击 **OK**:

   Gateway Name: gw2

   Security Level: Custom

   Remote Gateway Type:

   Static IP Address: (选择), Address/Hostname: 2.2.2.2

   Preshared Key: netscreen2

   Outgoing Interface: ethernet3

> Advanced: 输入以下高级设置，然后单击 **Return**，返回基本 Gateway 配置页 :

Phase 1 Proposal: pre-g2-3des-sha

Mode (Initiator): Main (ID Protection)

XAuth Server: (选择)

Local Authentication: (选择)

User Group: (选择), xa-grp1

VPNs > AutoKey IKE > New: 输入以下内容，然后单击 **OK**:

VPN Name: vpn2

Security Level: Compatible

Remote Gateway Tunnel:

Predefined: (选择), gw2

CLI

1. XAuth 用户组

```
set user-group xa-grp1 location local
set user-group xa-grp1 user x1
```

2. VPN

```
set ike gate gw2 ip 2.2.2.2 main outgoing-interface ethernet3 preshare
    netscreen2 proposal pre-g2-3des-sha
set ike gateway gw2 xauth server Local user-group xa-grp1
set vpn vpn2 gateway gw2 sec-level compatible
save
```

范例 : XAuth 认证 (外部用户)

在本例中，将引用先前加载到外部 SecurID auth 服务器上的 XAuth 用户，用户名为 “xa-1”，密码为 iNWw10bd01。本例使用的 SecurID auth 服务器配置与第 35 页上的 “范例 : SecurID Auth 服务器”中定义的大致相同，但此处将帐户类型定义为 XAuth。

将远程 IKE 网关配置中的 XAuth 用户 xa-1 引用到 IP 2.2.2.2 处的对等方。将远程网关命名为 “gw3”，为 “阶段 1” 协商指定 “主模式” 和提议 pre-g2-3des-sha，并使用预共享密钥 “netscreen3”。将 VPN 通道命名为 “vpn3”，为 “阶段 2” 协商指定提议 g2-esp-3des-sha。选择 Untrust 区段接口 ethernet3 作为出接口。

WebUI

1. 外部 SecurID Auth 服务器

   Configuration > Auth > Servers > New: 输入以下内容，然后单击 **OK**:

   Name: securid1

   IP/Domain Name: 10.20.2.100

   Backup1: 10.20.2.110

   Timeout: 60

   Account Type: XAuth

   SecurID: (选择)

   Client Retries: 3

   Client Timeout: 10 seconds

   Authentication Port: 15000

   Encryption Type: DES

   User Duress: No

2. XAuth 用户

在外部 SecurID auth 服务器 securid1 上定义密码为 iNWw10bd01 的 auth 用户 “xa-1”。

3. VPN

VPNs > AutoKey Advanced > Gateway > New: 输入以下内容，然后单击 **OK**:

Gateway Name: gw3

Security Level: Custom

Remote Gateway Type:

Static IP Address: (选择), Address/Hostname: 2.2.2.2

Preshared Key: netscreen3

Outgoing Interface: ethernet3

> Advanced: 输入以下高级设置，然后单击 **Return**，返回基本 Gateway 配置页 :

Phase 1 Proposal: pre-g2-3des-sha

Mode (Initiator): Main (ID Protection)

XAuth Server: (选择)

External Authentication: (选择), securid1

User: (选择)

Name: xa-1

VPNs > AutoKey IKE > New: 输入以下内容，然后单击 **OK**:

VPN Name: vpn3

Security Level: Compatible

Remote Gateway Tunnel:

Predefined: (选择), gw3

CLI

1. 外部 SecurID Auth 服务器

```
set auth-server securid1 type securid
set auth-server securid1 server-name 10.20.2.100
set auth-server securid1 backup1 10.20.2.110
set auth-server securid1 timeout 60
set auth-server securid1 account-type xauth
set auth-server securid1 securid retries 3
set auth-server securid1 securid timeout 10
set auth-server securid1 securid auth-port 15000
set auth-server securid1 securid encr 1
set auth-server securid1 securid duress 0
```

2. XAuth 用户

在外部 SecurID auth 服务器 securid1 上定义密码为 iNWw10bd01 的 auth 用户 “xa-1”。

3. VPN

```
set ike gate gw3 ip 2.2.2.2 main outgoing-interface ethernet3 preshare
    netscreen3 proposal pre-g2-3des-sha
set ike gateway gw3 xauth server securid1 user xa-1
set vpn vpn3 gateway gw3 sec-level compatible
save
```

范例 : XAuth 认证 (外部用户组)

在本例中，将配置名为 “radius1”[6] 的外部 RADIUS auth 服务器，定义名为 “xa-grp2” 的外部 auth 用户组。在下列两个位置定义外部 XAuth 用户组 xa-grp2:

1. 外部 RADIUS auth 服务器 “radius1”
2. NetScreen 设备

只在 RADIUS 服务器上将 XAuth 用户加入 XAuth 用户组 “xa-grp2” 中，而将 NetScreen 设备上的组保留为空白。该组中的成员为远程站点处的分销商，需要访问企业 LAN 中的 FTP 服务器。在 Untrust 区段通讯簿中，为远程站点添加一个条目， IP 地址 10.2.2.0/24、名称为 “reseller1”。也可在 Trust 区段通讯簿中，为 IP 地址 10.1.1.5/32 的 FTP 服务器 “rsl-srv1” 输入一个地址。

配置到 2.2.2.2 的 VPN 通道，以便对用户组 xa-grp2 中的 XAuth 用户进行认证。将远程网关命名为 “gw4”，为 “阶段 1” 协商指定 “主模式” 和提议 pre-g2-3des-sha，并使用预共享密钥 “netscreen4”。将 VPN 通道命名为 “vpn4”，为 “阶段 2” 协商指定 “兼容” 组的提议。选择 Untrust 区段接口 ethernet3 作为出接口。

最后，创建一个策略，允许 FTP 信息流从 Untrust 区段中的 reseller1 通过 vpn4 流向 Trust 区段中的 rsl-svr1。

RADIUS 服务器

1. 将 NetScreen 词典文件加载到 RADIUS 服务器上。

   注意 : *有关 NetScreen 词典文件的信息，请参阅第 25 页上的 “NetScreen 词典文件”。有关将词典文件加载到 RADIUS 服务器的说明，请参阅 RADIUS 服务器文档。*

2. 在外部 auth 服务器 “radius1” 上输入 auth 用户组 “xa-grp2”，然后在其中加入 XAuth 用户帐户。

6. RADIUS auth 服务器的配置与第 32 页上的 “范例 : RADIUS Auth 服务器”中大致相同，但本例中仅指定 “xauth” 作为用户帐户类型。

WebUI

1. Auth 服务器

   Configuration > Auth > Servers > New: 输入以下内容，然后单击 **OK**:

   Name: radius1

   IP/Domain Name: 10.20.1.100

   Backup1: 10.20.1.110

   Backup2: 10.20.1.120

   Timeout: 30

   Account Type: XAuth

   RADIUS: (选择)

   RADIUS Port: 4500

   Shared Secret: A56htYY97kl

2. 外部用户组

   Objects > Users > External Groups> New: 输入以下内容，然后单击 **OK**:

   Group Name: xa-grp2

   Group Type: XAuth

3. 地址

   Objects > Addresses > List > New: 输入以下内容，然后单击 **OK**:

   Address Name: reseller1

   IP Address/Domain Name:

   IP/Netmask: (选择), 10.2.2.0/24

   Zone: Untrust

Objects > Addresses > List > New: 输入以下内容，然后单击 **OK**:

Address Name: rsl-svr1

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.5/32

Zone: Trust

4. VPN

VPNs > AutoKey Advanced > Gateway > New: 输入以下内容，然后单击 **OK**:

Gateway Name: gw4

Security Level: Custom

Remote Gateway Type:

Static IP Address: (选择), Address/Hostname: 2.2.2.2

Preshared Key: netscreen4

Outgoing Interface: ethernet3

> Advanced: 输入以下高级设置，然后单击 **Return**，返回基本 Gateway 配置页 :

Phase 1 Proposal: pre-g2-3des-sha

Mode (Initiator): Main (ID Protection)

XAuth Server: (选择)

External Authentication: (选择), securid1

User Group: (选择)

Name: xa-grp2

VPNs > AutoKey IKE > New: 输入以下内容，然后单击 **OK**:

VPN Name: vpn4

Security Level: Compatible

Remote Gateway:

Predefined: (选择), gw4

5. 策略

Policies > (From: Untrust, To: Trust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), reseller1

Destination Address:

Address Book Entry: (选择), rsl-svr1

Service: FTP-Get

Action: 通道

Tunnel VPN: vpn4

Modify matching bidirectional VPN policy: (清除)

Position at Top: (选择)

CLI

1. Auth 服务器

```
set auth-server radius1 type radius
set auth-server radius1 account-type xauth
set auth-server radius1 server-name 10.20.1.100
set auth-server radius1 backup1 10.20.1.110
set auth-server radius1 backup2 10.20.1.120
set auth-server radius1 timeout 30
set auth-server radius1 radius port 4500
set auth-server radius1 radius secret A56htYY97kl
```

2. 外部用户组

```
set user-group xa-grp2 location external
set user-group xa-grp2 type xauth
```

3. 地址

```
set address untrust reseller1 10.2.2.0/24
set address trust rsl-svr1 10.1.1.5/32
```

4. VPN

```
set ike gate gw4 ip 2.2.2.2 main outgoing-interface ethernet3 preshare
    netscreen4 proposal pre-g2-3des-sha
set ike gateway gw4 xauth server radius1 user-group xa-grp2
set vpn vpn4 gateway gw4 sec-level compatible
```

5. 策略

```
set policy top from untrust to trust reseller1 rsl-svr1 ftp-get tunnel vpn vpn4
save
```

范例 : XAuth 认证和地址分配 (本地用户组)

在本例中，为本地数据库上存储的 IKE/XAuth 用户组建立认证和 IP、 DNS 服务器及 WINS 服务器 IP 地址分配[7]。IKE/XAuth 用户以拨号 VPN 连接方式尝试连接 NetScreen 设备时， NetScreen 设备会在 “阶段 1” 协商期间使用 IKE ID 和 RSA 证书对用户 (即客户端设备) 进行认证。然后， NetScreen 设备使用用户名和密码对 XAuth 用户 (即使用设备的个体) 进行认证，并在 “阶段 1” 和 “阶段 2” 协商之间分配 IP、 DNS 服务器和 WINS 服务器 IP 地址。

创建本地用户组 ixa-grp1。然后定义两个名为 “ixa-u1” (密码 : ccF1m84s) 和 “ixa-u2” (密码 : C113g1tw) 的用户，并将其添加到组中，从而将组类型定义为 IKE/XAuth。 (本例中将不向组中另外添加其它 IKE/XAuth 用户。)

创建名为 xa-pool1 的 DIP 池，地址范围从 10.2.2.1 到 10.2.2.100。 NetScreen 设备为 XAuth 用户分配 IP 地址时，即从此地址池中提取地址。

注意 : *DIP 池与 XAuth 用户发送信息流的目标区段必须具有不同的地址空间，以避免出现路由选择问题和地址分配重复。*

配置以下 XAuth 缺省设置 :

- 将 XAUTH 地址超时设置为 480 分钟。
- 选择本地数据库作为缺省 auth 服务器。
- 启用 CHAP (质询握手认证协议)， NetScreen 设备根据此协议向远程客户端发送一个质询 (加密密钥)，该客户端用户使用此密钥对其登录名和密码进行加密。
- 选择 xa-pool1 作为缺省 DIP 池。
- 将主、辅 DNS 服务器 IP 地址分别定义为 10.1.1.150 和 10.1.1.151。
- 将主、辅 WINS 服务器 IP 地址分别定义为 10.1.1.160 和 10.1.1.161。

引用用户组 ixa-grp1 并使用缺省 XAuth auth 服务器设置，配置名为 “ixa-gw1” 的 IKE 网关。然后，配置名为 “ixa-tun1” 的 VPN 通道和允许信息流通过 VPN 通道 ixa-tun1 从 ixa-grp1 流向 Trust 区段 (IP 地址为 10.1.1.0/24) 的策略。

7. 也可使用外部 RADIUS auth 服务器对 XAuth 用户进行认证和地址分配。但外部 SecurID 或 LDAP auth 服务器只能用于 XAuth 认证 (不能进行地址分配)。对于 IKE 用户认证，只能使用本地数据库。

WebUI

1. IKE/XAuth 用户和用户组

Objects > Users > Local > New: 输入以下内容，然后单击 **OK**:

User Name: ixa-u1

Status: Enable

IKE User: (选择)

Simple Identity: (选择)

IKE ID Type: AUTO

IKE Identity: u1@ns.com

XAuth User: (选择)

User Password: ccF1m84s

Confirm Password: ccF1m84s

Objects > Users > Local > New: 输入以下内容，然后单击 **OK**:

User Name: ixa-u2

Status: Enable

IKE User: (选择)

Simple Identity: (选择)

IKE ID Type: AUTO

IKE Identity: u2@ns.com

XAuth User: (选择)

User Password: C113g1tw

Confirm Password: C113g1tw

Objects > Users > Local Groups > New: 在 Group Name 字段中输入 **ixa-grp1**，执行以下操作，然后单击 **OK**:

选择 **ixa-u1**，并使用 **<<** 按钮将其从 Available Members 栏移动到 Group Members 栏中。

选择 **ixa-u2**，并使用 **<<** 按钮将其从 Available Members 栏移动到 Group Members 栏中。

2. IP 池

Objects > IP Pools > New: 输入以下内容，然后单击 **OK**:

IP Pool Name: xa-pool1

Start IP: 10.2.2.1

End IP: 10.2.2.100

3. 缺省 XAuth Auth 服务器

VPNs > AutoKey Advanced > XAuth Settings: 输入以下内容，然后单击 **Apply**:

Reserve Private IP for XAuth User: 480 Minutes

Default Authentication Server: Local

Query Client Settings on Default Server: (清除)

CHAP: (选择)

IP Pool Name: xa-pool1

DNS Primary Server IP: 10.1.1.150

DNS Secondary Server IP: 10.1.1.151

WINS Primary Server IP: 10.1.1.160

WINS Secondary Server IP: 10.1.1.161

4. 地址

Objects > Addresses > List > New: 输入以下内容，然后单击 **OK**:

Address Name: Trust_zone
IP Address/Domain Name:
IP/Netmask: (选择), 10.1.1.0/24
Zone: Trust

5. VPN

VPNs > AutoKey Advanced > Gateway > New: 输入以下内容，然后单击 **OK**:

Gateway Name: ixa-gw1
Security Level: Custom
Remote Gateway Type:
Dialup User Group: (选择)
Group: ixa-grp1
> Advanced: 输入以下高级设置，然后单击 **Return**，返回基本 Gateway 配置页 :
Phase 1 Proposal: rsa-g2-3des-sha
Mode (Initiator): Aggressive
Outgoing Interface: ethernet3
XAuth Server: (选择)
Use Default: (选择)
User Group: (选择), ixa-grp1

VPNs > AutoKey IKE > New: 输入以下内容，然后单击 **OK**:

VPN Name: ixa-vpn1

Security Level: Compatible

Remote Gateway:

Predefined: (选择), ixa-gw1

6. 策略

Policies > (From: Untrust; To: Trust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Dial-Up VPN

Destination Address:

Address Book Entry: (选择), Trust_zone

Service: ANY

Action: Tunnel

Tunnel VPN: ixa-vpn1

Modify matching bidirectional VPN policy: (清除)

Position at Top: (选择)

CLI

1. IKE/XAuth 用户和用户组

```
set user-group ixa-grp1 location local
set user ixa-u1 type ike xauth
set user ixa-u1 ike-id u-fqdn u1@ns.com
set user ixa-u1 password ccF1m84s
unset user ixa-u1 type auth
set user ixa-u2 type ike xauth
set user ixa-u2 ike-id u-fqdn u2@ns.com
set user ixa-u2 password C113g1tw
unset user ixa-u2 type auth
```

2. IP 池

```
set ippool xa-pool1 10.2.2.1 10.2.2.100
```

3. 缺省 XAuth Auth 服务器

```
set xauth lifetime 480
set xauth default auth server Local chap
set xauth default ippool xa-pool1
set xauth default dns1 10.1.1.150
set xauth default dns2 10.1.1.151
set xauth default wins1 10.1.1.160
set xauth default wins2 10.1.1.161
```

4. 地址

```
set address trust Trust_zone 10.1.1.0/24
```

5. VPN

```
set ike gateway ixa-gw1 dialup ixa-grp1 aggressive outgoing-interface ethernet3
    proposal rsa-g2-3des-sha
set ike gateway ixa-gw1 xauth server Local user-group ixa-grp1
set vpn ixa-vpn1 gateway ixa-gw1 sec-level compatible
```

6. 策略

```
set policy top from untrust to trust "Dial-Up VPN" Trust_zone any tunnel vpn
    ixa-vpn1
save
```

XAuth 客户端

XAuth 客户端是一个远程用户或设备，它通过“自动密钥 IKE” VPN 通道与 XAuth 服务器相连。 NetScreen 设备可以作为 XAuth 客户端，响应远程 XAuth 服务器的认证请求。“阶段 1”协商完成后，远程 XAuth 服务器向 NetScreen 设备发送登录提示。如果作为 XAuth 客户端的 NetScreen 设备使用正确的用户名和密码成功登录，则“阶段 2”协商开始。

要将 NetScreen 设备配置为 XAuth 客户端，必须指定下列内容 :

- IKE 网关名
- XAuth 用户名和密码

可以配置以下类型的 XAuth 认证 :

- Any — 允许 “质询握手认证协议” (CHAP) 或 “密码认证协议” (PAP)
- CHAP — 只允许 CHAP

范例 : NetScreen 设备作为 XAuth 客户端

在本例中，首先配置 IP 地址为 2.2.2.2 的远程 IKE 网关 *gw1*。指定标准安全级别，并使用预共享密钥 *netscreen1*。然后，为用户名为 *beluga9*、密码为 *1234567* 的 IKE 网关配置 XAuth 客户端。还需要对该客户端进行 CHAP 认证。

WebUI

VPN > AutoKey Advanced > Gateway > New: 输入以下内容，然后单击 **OK**:

Gateway Name: gw1

Security Level: Standard (选择)

Remote Gateway Type:

Static IP Address: (选择), Address/Hostname: 2.2.2.2

Preshared Key: netscreen1

Outgoing Interface: Untrust

> Advanced: 输入以下高级设置，然后单击 **Return**，返回基本 Gateway 配置页 :

XAuth Client: (选择)

User Name: beluga9

Password: 1234567

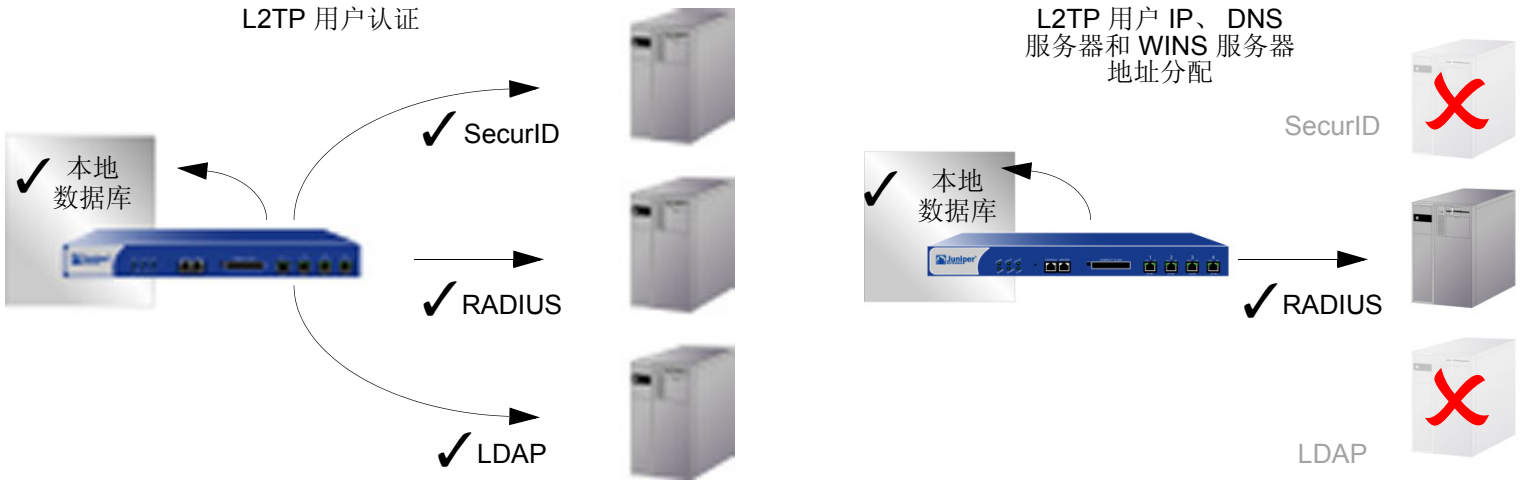
Allowed Authentication Type: (选择), CHAP Only

CLI

```
set ike gateway gw1 ip 2.2.2.2 Main outgoing-interface untrust preshare
    netscreen1 sec-level standard
set ike gateway gw1 xauth client chap username beluga1 password 1234567
save
```

L2TP 用户和用户组

“第 2 层通道协议” (L2TP) 提供一种认证远程用户和分配 IP、 DNS 服务器与 WINS 服务器地址的方法。可对 NetScreen 设备进行配置，以便使用本地数据库或外部 auth 服务器认证 L2TP 用户。要对 IP、DNS 服务器及 WINS 服务器地址进行分配，可相应配置 NetScreen 设备，以使用本地数据库或 RADIUS 服务器 (加载 NetScreen 词典文件 — 请参阅第 25 页上的 “NetScreen 词典文件”)。



甚至可使用 auth 服务器的组合，不同服务器分别对应 L2TP 两个方面之一。例如，可使用 SecurID 服务器对 L2TP 用户进行认证，但从本地数据库进行地址分配。下例说明如何应用两个 auth 服务器分别处理 L2TP 的两方面需求。有关其它范例以及 L2TP 的详细说明，请参阅第 **5**-301 页上的 “L2TP”。

范例：本地和外部 L2TP Auth 服务器

在本例中，将设置外部 SecurID auth 服务器对 L2TP 用户进行认证，并使用本地数据库为 L2TP 用户分配 IP、 DNS 服务器和 WINS 服务器地址。

外部 SecurID auth 服务器为 securid1。 Auth 服务器的配置与第 35 页上的 “范例：SecurID Auth 服务器”中基本相同，只是此处帐户类型为 L2TP。 SecurID auth 服务器参数如下：

- Name: securid1
- IP Address: 10.20.2.100
- Backup1 IP Address: 10.20.2.110
- Port: 15000
- Encryption: DES
- Client Retries: 3
- Client Timeout: 10 seconds
- Idle Timeout: 60 minutes
- Account Type: L2TP

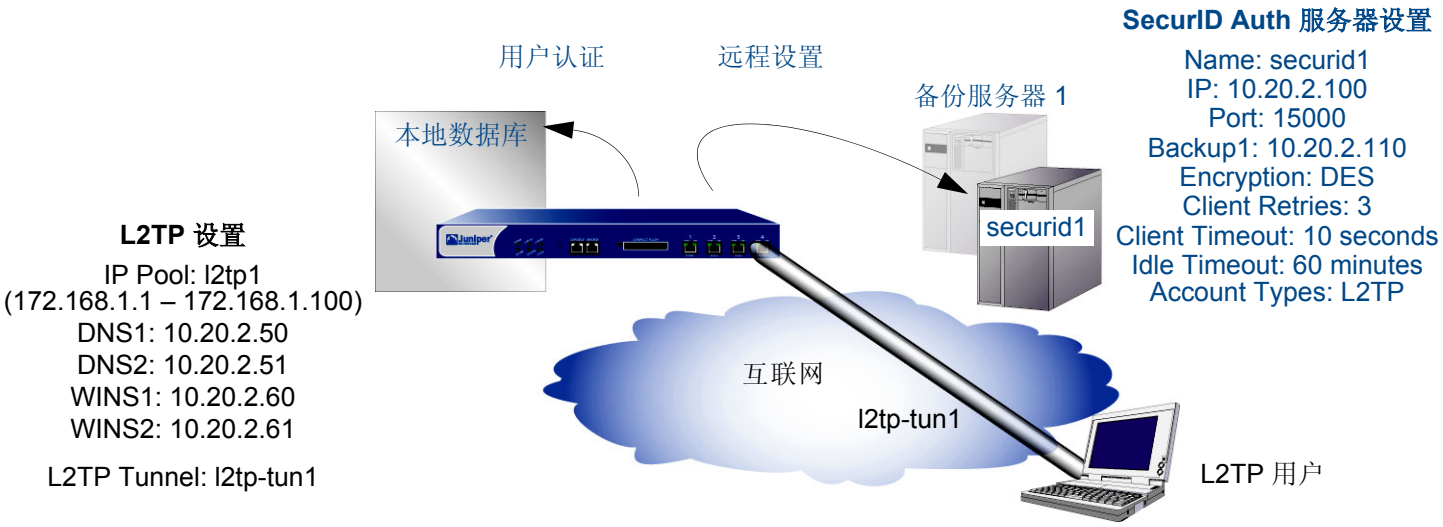
L2TP 缺省设置如下：

- IP Pool: l2tp1 (172.168.1.1 – 172.168.1.100)
- DNS Primary Server IP: 10.20.2.50
- DNS Secondary Server IP: 10.20.2.51
- PPP Authentication: CHAP
- WINS Primary Server IP: 10.20.2.60
- WINS Secondary Server IP: 10.20.2.61

以上述设置对 NetScreen 设备进行配置后，创建名为 “l2tp-tun1” 的 L2TP 通道，它引用 securid1 进行认证，并使用缺省设置进行地址分配。

此外，还必须如上所示设置 SecurID 服务器，并在其中加入 L2TP 用户。

***注意：** 一个只有 L2TP 的配置并不安全。为了增加 L2TP 通道的安全性，建议将其与 IPSec 通道 (必须处于 Transport 模式) 结合使用，如第 **5**-320 页上的 “范例：配置 IPSec 上的 L2TP” 中所示。*



WebUI

1. Auth 服务器

Configuration > Auth > Servers > New: 输入以下内容，然后单击 **OK**:

Name: securid1
IP/Domain Name: 10.20.2.100
Backup1: 10.20.2.110
Timeout: 60
Account Type: L2TP
SecurID: (选择)
Client Retries: 3
Client Timeout: 10 seconds
Authentication Port: 15000
Encryption Type: DES
Use Duress: No

2. IP 池

Objects > IP Pools > New: 输入以下内容，然后单击 **OK**:

IP Pool Name: l2tp1

Start IP: 172.168.1.1

End IP: 172.168.1.100

3. L2TP 缺省设置

VPNs > L2TP > Default Settings: 输入以下内容，然后单击 **Apply**:

Default Authentication Server: Local

IP Pool Name: l2tp1

PPP Authentication: CHAP

DNS Primary Server IP: 10.20.2.50

DNS Secondary Server IP: 10.20.2.51

WINS Primary Server IP: 10.20.2.60

WINS Secondary Server IP: 10.20.2.61

4. L2TP 通道

VPNs > L2TP > Tunnel > New: 输入以下内容，然后单击 **OK**:

Name: l2tp-tun1

Use Custom Settings: (选择)

Authentication Server: securid1

Query Remote Settings: (清除)

Dialup User: (选择), Allow Any

CLI

1. Auth 服务器

```
set auth-server securid1 type securid
set auth-server securid1 server-name 10.20.2.100
set auth-server securid1 backup1 10.20.2.110
set auth-server securid1 timeout 60
set auth-server securid1 account-type l2tp
set auth-server securid1 securid retries 3
set auth-server securid1 securid timeout 10
set auth-server securid1 securid auth-port 15000
set auth-server securid1 securid encr 1
set auth-server securid1 securid duress 0
```

2. IP 池

```
set ippool l2tp1 172.168.1.1 172.168.1.100
```

3. L2TP 缺省设置

```
set l2tp default auth server Local
set l2tp default ippool l2tp1
set l2tp default ppp-auth chap
set l2tp dns1 10.20.2.50
set l2tp dns1 10.20.2.51
set l2tp wins1 10.20.2.60
set l2tp wins2 10.20.2.61
```

4. L2TP 通道

```
set l2tp l2tp-tun1
set l2tp l2tp-tun1 auth server securid1
save
```

索引

M

N

R

S

V

W

X

Y

Z