SecPath 系列防火墙 IPSec 典型配置举例

关键词：**IKE、IPSec**

摘　要：本章首先介绍了 **IKE** 和 **IPSec** 的基本概念，随后说明了防火墙的配置方法，最后给出两种典型应用的举例。

缩略语：

缩略语	英文全名	中文解释
IKE	Internet Key Exchange	因特网密钥交换
IPsec	IP Security	IP 网络安全协议

目 录

1 特性简介

IPsec（IP Security）协议族是 IETF 制定的一系列协议，它为 IP 数据报提供了高质量的、可互操作的、基于密码学的安全性。特定的通信方之间在 IP 层通过加密与数据源验证等方式，来保证数据报在网络上传输时的私有性、完整性、真实性和防重放。

IPsec 通过 AH（Authentication Header，认证头）和 ESP（Encapsulating Security Payload，封装安全载荷）这两个安全协议来实现上述目标，并且还可以通过 IKE（Internet Key Exchange，因特网密钥交换协议）为 IPsec 提供自动协商交换密钥、建立和维护安全联盟的服务，以简化 IPsec 的使用和管理。

1.1 IPSec 基本概念

1.1.1 SA

IPSec 在两个端点之间提供安全通信，端点被称为 IPSec 对等体。

SA（Security Association，安全联盟）是 IPSec 的基础，也是 IPSec 的本质。SA 是通信对等体间对某些要素的约定，例如，使用哪种协议（AH、ESP 还是两者结合使用）、协议的封装模式（传输模式和隧道模式）、加密算法（DES、3DES 和 AES）、特定流中保护数据的共享密钥以及密钥的生存周期等。SA 可以通过 IKE 自动协商建立。

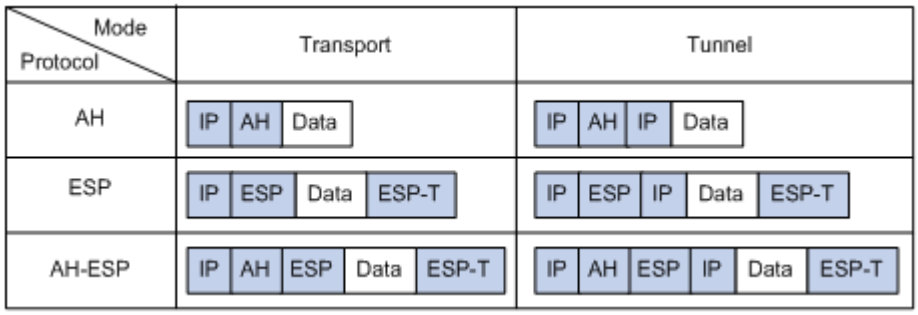
1.1.2 封装模式

IPSec 有如下两种工作模式：

- 隧道（Tunnel）模式：用户的整个 IP 数据包被用来计算 AH 或 ESP 头，AH 或 ESP 头以及 ESP 加密的用户数据被封装在一个新的 IP 数据包中。通常，隧道模式应用在两个安全网关之间的通讯。
- 传输（Transport）模式：只是传输层数据被用来计算 AH 或 ESP 头，AH 或 ESP 头以及 ESP 加密的用户数据被放置在原 IP 包头后面。通常，传输模式应用在两台主机之间的通讯，或一台主机和一个安全网关之间的通讯。

不同的安全协议在Tunnel和Transport模式下的数据封装形式如 图 1 所示，data为传输层数据。

图1 安全协议数据封装格式



认证算法与加密算法

(1) 认证算法

认证算法的实现主要是通过杂凑函数。杂凑函数是一种能够接受任意长的消息输入，并产生固定长度输出的算法，该输出称为消息摘要。IPSec 对等体计算摘要，如果两个摘要是相同的，则表示报文是完整未经篡改的。IPSec 使用两种认证算法：

- MD5：MD5 通过输入任意长度的消息，产生 128bit 的消息摘要。
- SHA-1：SHA-1 通过输入长度小于 2 的 64 次方 bit 的消息，产生 160bit 的消息摘要。

MD5 算法的计算速度比 SHA-1 算法快，而 SHA-1 算法的安全强度比 MD5 算法高。

(2) 加密算法

加密算法实现主要通过对称密钥系统，它使用相同的密钥对数据进行加密和解密。目前设备的 IPSec 实现三种加密算法：

- DES（Data Encryption Standard）：使用 56bit 的密钥对一个 64bit 的明文块进行加密。
- 3DES（Triple DES）：使用三个 56bit 的 DES 密钥（共 168bit 密钥）对明文进行加密。
- AES（Advanced Encryption Standard）：使用 128bit、192bit 或 256bit 密钥长度的 AES 算法对明文进行加密。

这三个加密算法的安全性由高到低依次是：AES、3DES、DES。安全性高的加密算法实现机制复杂，运算速度慢。对于普通的安全要求，DES 算法就可以满足需要。

2 应用场合

IPsec 作为一种 VPN 技术，其最显著的特点就是可以为载荷数据提供加密以及数据源验证服务，保护数据的机密性和完整性。同时通过 IKE 可以对密钥进行定时更新维护，增强系统的安全性。鉴于这些特点，IPsec 被广泛应用于传输敏感数据的 VPN 网络中。

3 配置指南

3.1 配置概述

目前，设备支持使用 IPSec 安全策略建立 IPSec 安全隧道。这种方式下，由 ACL（Access Control List，访问控制列表）来指定要保护的数据流范围，通过配置安全策略并将安全策略绑定在实际的物理接口上来完成 IPsec 的配置。这种方式可以利用 ACL 的丰富配置功能，结合实际的组网环境灵活制定 IPsec 安全策略。其基本配置思路如下：

(1) 通过配置 ACL，用于匹配需要保护的数据流。

(2) 通过配置安全提议，指定安全协议、认证算法和加密算法、封装模式等。

(3) 通过配置安全策略，将要保护的数据流和安全提议进行关联（即定义对何种数据流实施何种保护），并指定 SA 的协商方式、对等体 IP 地址（即保护路径的起/终点）、所需要的密钥和 SA 的生存周期等。

(4) 最后在设备接口上应用安全策略即完成了 IPSec 的配置。

IPSec配置的推荐步骤如 表 1 所示。

表1 IPSec 配置步骤

步骤	配置任务	说明
1	3.2 配置ACL	必选 ACL 是用来实现流识别功能的。网络设备为了过滤报文，需要配置一系列的匹配条件对报文进行分类，当设备的端口接收到报文后，即根据当前端口上应用的 ACL 规则对报文进行分析、识别之后，根据预先设定的策略对报文进行不同的处理 提示 ACL 在“防火墙 > ACL”中配置，本章中只介绍在配置 IPSec 所引用的 ACL 时需要注意的事项
2	3.3 配置IKE	必选 IKE 为 IPSec 提供了自动协商交换密钥、建立 SA 的服务，能够简化 IPSec 的使用和管理，大大简化 IPSec 的配置和维护工作
3	3.4 IPSec安全提议	必选 安全提议用于保存 IPSec 需要使用的特定安全协议、加密/认证算法以及封装模式，为 IPSec 协商 SA 提供各种安全参数 提示 若已存在的 IPSec 安全提议的配置发生了修改，则对已协商成功的 SA，新修改的安全提议并不起作用，即 SA 仍然使用原来的 IPSec 安全提议，只有新协商的 SA 将使用新的 IPSec 安全提议
4	3.5 配置安全策略模板	安全策略中需要引用安全策略模板组时必选 名称相同 的所有安全策略模板称为一个安全策略模板组。其中，序号越小的安全策略模板，优先级越高。在配置安全策略时，可以直接引用安全策略模板组来创建安全策略
5	3.6 配置安全策略	必选 Web 界面采用 IKE 方式来配置安全策略，在配置时可以直接设置策略中的参数，也可以通过引用已创建的安全策略模板组来配置 名称相同的所有安全策略称为一个安全策略组。其中，序号越小的安全策略，优先级越高 提示 不能用应用安全策略模板的安全策略来发起安全联盟的协商，但可以响应协商。在协商过程中进行策略匹配时，策略模板中定义的参数必须相符，而策略模板中没有定义的参数由发起方来决定，响应方接受发起方的建议
6	3.7 应用安全策略组	必选 在要加密的数据流和要解密的数据流所在接口（逻辑的或物理的）上应用一个安全策略组
7	5.4.1 查看IPSec安全联盟	可选 查看所有 IPSec 安全联盟的概要信息，通过查看显示信息验证配置的效果
8	5.4.2 查看报文统计	可选 查看 IPSec 处理报文的统计信息，通过查看 IPSec 的运行情况验证配置的效果

3.2 配置 ACL

IPsec 通过配置 ACL（Access Control List，访问控制列表）来定义需要过滤的数据流。在 IPsec 的应用中，ACL 规则中的 **permit** 关键字表示与之匹配的流量需要被 IPsec 保护，而规则中的 **deny** 关键字则表示与之匹配的那些流量不需要保护。配置 ACL，需要在“防火墙 > ACL”菜单中做如下配置：

(1) 创建访问控制列表。

(2) 配置相应的匹配规则（rule）。

说明

仅对确实需要 IPSec 保护的数据流配置“允许”规则，否则，一旦指定范围上入方向收到的某流量本来应该不被 IPSec 保护的，那么该流量就会被丢弃，这会造成一些本不需要 IPSec 处理的流量丢失，影响正常的业务流传输。

3.3 配置 IKE

需要通过 IKE 方式来建立 SA，所以在介绍 IPSec 的配置步骤前，先介绍 IKE 的配置方法。

3.3.1 配置 IKE 全局参数

在导航栏中选择“VPN > IKE > 全局设置”，进入IKE全局设置的页面，如 图 2 所示。

图2 全局设置

IKE全局参数的详细配置如 表 2 所示。

表2 IKE 全局参数的详细配置

配置项	说明
IKE 本端名称	设置本端安全网关的名称 当 IKE 协商的发起端使用安全网关名称进行协商时，本端需要设置该参数，发起端会发送自己的“IKE 本端名称”给对端来标识自己的身份，而对端使用“对端网关名称”参数来认证发起端，故此时“对端网关名称”应与发起端上的“IKE 本端名称”保持一致 缺省情况下，使用设备名作为 IKE 本端名称

配置项	说明
NAT Keepalive 报文时间间隔	设置 ISAKMP SA 向对端发送 NAT Keepalive 报文的时间间隔 由于在 NAT 网关上的 NAT 映射会话有一定存活时间，因此一旦安全隧道建立后如果长时间没有报文穿越，NAT 会话表项会被删除，这样将导致在 NAT 外侧的隧道无法继续传输数据。为防止 NAT 表项老化，ISAKMP SA 以一定的时间间隔向对端发送 NAT Keepalive 报文，以维持 NAT 会话的存活

3.3.2 配置 IKE 安全提议

在导航栏中选择“VPN > IKE > 安全提议”，进入IKE安全提议的显示页面，如 图 3 所示。单击<新建>按钮，进入新建IKE安全提议的配置页面，如 图 4 所示。

图3 安全提议

说明

在日常使用时通常省略 IKE 安全提议的设置，直接使用缺省提议 default 即可完成协商。

图4 新建 IKE 安全提议

新建IKE安全提议的详细配置如 表 3 所示。

表3 新建 IKE 安全提议的详细配置

配置项	说明
IKE 安全提议号	设置 IKE 安全提议的序号 该序号同时表示该 IKE 安全提议的优先级，数值越小，优先级越高，即在进行 IKE 协商的时候，会从序号最小的 IKE 安全提议进行匹配
认证方法	设置 IKE 安全提议所采用的认证方法 ● Preshared Key：采用预共享密钥的认证方法 ● RSA Signature：采用 RSA 数字签名的认证方法
认证算法	设置 IKE 安全提议所采用的认证算法 ● SHA1：采用 HMAC-SHA1 认证算法 ● MD5：采用 HMAC-MD5 认证算法
加密算法	设置 IKE 安全提议所采用的加密算法 ● DES-CBC：采用 CBC 模式的 DES 算法，采用 56 bits 的密钥进行加密 ● 3DES-CBC：采用 CBC 模式的 3DES 算法，采用 168 bits 的密钥进行加密 ● AES-128：采用 CBC 模式的 AES 算法，采用 128 bits 的密钥进行加密 ● AES-192：采用 CBC 模式的 AES 算法，采用 192 bits 的密钥进行加密 ● AES-256：采用 CBC 模式的 AES 算法，采用 256 bits 的密钥进行加密
DH 组	设置 IKE 阶段 1 密钥协商时所采用的 DH 密钥交换参数 ● Group1：采用 768-bit 的 Diffie-Hellman 组 ● Group2：采用 1024-bit 的 Diffie-Hellman 组 ● Group5：采用 1536-bit 的 Diffie-Hellman 组 ● Group14：采用 2048-bit 的 Diffie-Hellman 组
SA 生存周期	设置 IKE 安全提议的 ISAKMP SA 生存周期 在设定的生存周期超时前，会提前协商另一个 SA 来替换旧的 SA。在新的 SA 还没有协商完之前，依然使用旧的 SA；在新的 SA 建立后，将立即使用新的 SA，而旧的 SA 在生存周期超时后，被自动清除 提示 如果 SA 生存周期超时，ISAKMP SA 将自动更新。因为 IKE 协商需要进行 DH 计算，在低端设备上需要经过较长的时间，为使 ISAKMP SA 的更新不影响安全通信，建议设置 SA 生存周期大于 10 分钟

3.3.3 配置 IKE 对等体

在导航栏中选择“VPN > IKE > 对等体”，进入IKE对等体的显示页面，如 图 5 所示。单击<新建>按钮，进入新建IKE对等体的配置页面，如 图 6 所示。

图5 对等体

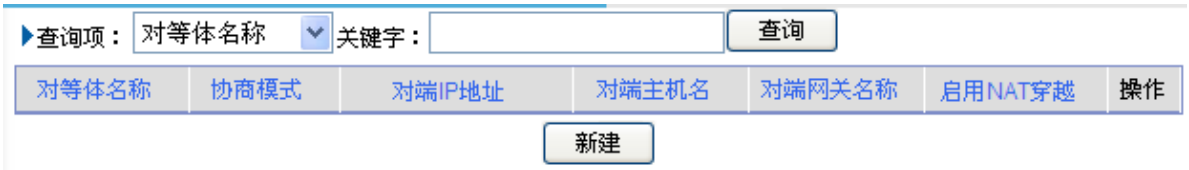
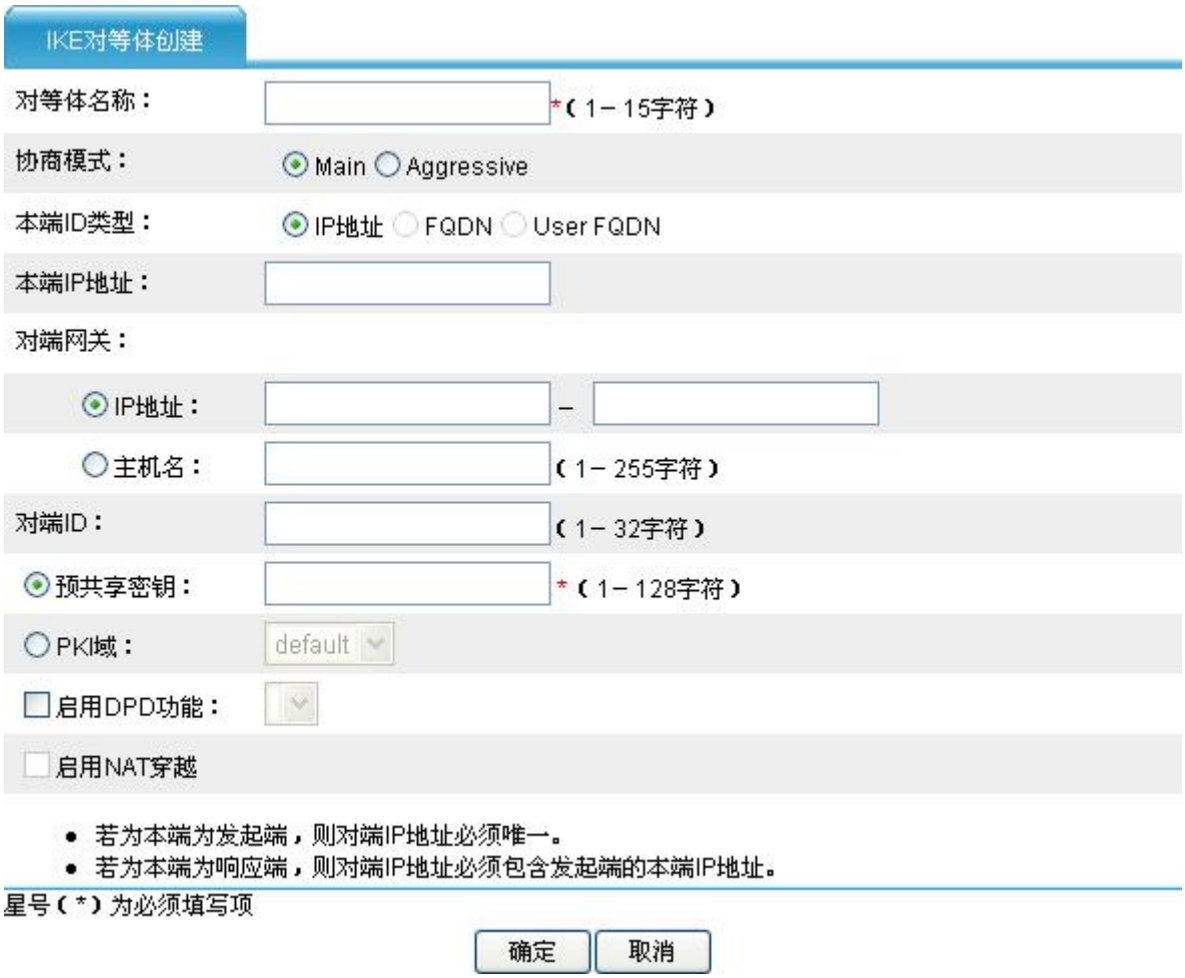


图6 新建 IKE 对等体



新建IKE对等体的详细配置如 表 4 所示。

表4 新建 IKE 对等体的详细配置

配置项	说明
对等体名称	设置 IKE 对等体的名称
协商模式	设置 IKE 第一阶段的协商模式为 Main 或 Aggressive 提示 ● 当安全隧道一端的 IP 地址为自动获取时，必须将协商模式配置为“Aggressive”。这种情况下，只要建立安全联盟时使用的用户名和密码正确，就可以建立安全联盟 ● IKE 对等体中配置的协商模式表示本端作为发起方时所使用的协商模式，响应方将自动适配发起方的协商模式
本端 ID 类型	设置 IKE 第一阶段的协商过程中使用的本端 ID 的类型 ● IP 地址：表示选择 IP 地址作为 IKE 协商过程中使用的 ID ● 网关名称：表示选择网关名称作为 IKE 协商过程中使用的 ID 提示 当协商模式为“Main”时，只能使用 IP 地址类型的身份进行 IKE 协商，建立安全联盟

配置项		说明
本端 IP 地址		设置 IKE 协商时的本端安全网关的 IP 地址 缺省情况下，本端 IP 地址使用应用安全策略的接口的主地址。只有当用户需要指定特殊的本端网关地址时才需要设置此配置项 提示 一般情况下本端 IP 地址不需要配置，只有当用户需要指定特殊的本端网关地址时（如指定 loopback 接口地址）才需要配置。而发起方的对端网关名字或对端网关 IP 地址需要配置，它们用于发起方在协商过程中寻找对端
对端网关	IP 地址	设置 IPSec 隧道对端安全网关的地址，可以是 IP 地址或主机名 ● 对端网关的 IP 地址可以是一个 IP 地址，也可以是一个 IP 地址范围。若本端为 IKE 协商的发起端，则此配置项所配的 IP 地址必须唯一，且与响应端的“本端 IP 地址”保持一致；若本端为 IKE 协商的响应端，则此配置项所配的 IP 地址必须包含发起端的“本端 IP 地址” ● 对端网关的主机名是 IPsec 对端在网络中的唯一标识，可被 DNS 服务器解析为 IP 地址。采用主机名方式时，本端可以作为 IKE 协商的发起端
	主机名	
对端 ID		设置 IKE 协商时，对端的安全网关名称 当 IKE 协商的发起端配置了本端 ID 类型为“网关名称”时，发起端会发送自己的“IKE 本端名称”给对端来标识自己的身份，而对端使用“对端 ID”来认证发起端，故此时“对端 ID”应与发起端上的“IKE 本端名称”保持一致
预共享密钥		根据 IKE 安全提议中设置的认证方法选择二者中的一个配置 ● 若认证方法设置为“Preshared Key”，则这里选择“预共享密钥”，即设置 IKE 协商采用预共享密钥认证时，所使用的预共享密钥 ● 若认证方法”置为“RSA Signature”，则这里选择“PKI 域”，即设置 IKE 协商采用数字签名认证时，证书所属的 PKI 域
PKI 域		
启用 DPD 功能		设置为 IKE 对等体应用一个 IKE DPD
启用 NAT 穿越		设置 IPSec/IKE 的 NAT 穿越功能 在 IPSec/IKE 组建的 VPN 隧道中，若存在 NAT 安全网关设备，则必须配置 IPSec/IKE 的 NAT 穿越功能 主模式下的 IKE 不支持 NAT 穿越功能，即当协商模式选择“Main”时，此项不可配 提示 为了节省 IP 地址空间，ISP 经常会在公网中加入 NAT 网关，以便于将私有 IP 地址分配给用户。此时可能会导致 IPSec/IKE 隧道的两端一端为公网地址，另一端为私网地址。所以，为保证隧道能够正常协商建立，公网和私网两端都要配置 nat 穿越。

3.4 IPSec 安全提议

在导航栏中选择“VPN > IPSec > 安全提议”，进入 IPSec 安全提议的配置显示页面。

Web 网管提供了两种 IPSec 安全提议的配置方式，在向导页面进行选择即可进入对应方式的配置页面。

- 套件方式：如 图 7 所示，用户可以直接在设备提供的加密套件中选择一种，方便用户的操作。详细配置如 表 5 所示。

图7 新建 IPSec 安全提议（套件方式）

表5 新建 IPSec 安全提议的详细配置（套件方式）

配置项	说明
安全提议名称	设置要新建的 IPSec 安全提议的名称
加密套件	设置安全提议采用的报文封装、安全协议及对应的认证/加密算法的套件 可选的加密套件有以下几种，其中“Tunnel”表示报文封装模式为隧道模式，其余参数的含义将在下面分别进行介绍： ● Tunnel-ESP-DES-MD5：采用 ESP 协议，ESP 加密算法为 DES，ESP 认证算法为 MD5 ● Tunnel-ESP-3DES-MD5：采用 ESP 协议，ESP 加密算法为 3DES，ESP 认证算法为 MD5 ● Tunnel-AH-MD5-ESP-DES：先用 ESP 协议对报文进行保护，再用 AH 协议进行保护，AH 认证算法为 MD5，ESP 加密算法为 DES，不进行 ESP 认证 ● Tunnel-AH-MD5-ESP-3DES：先用 ESP 协议对报文进行保护，再用 AH 协议进行保护，AH 认证算法为 MD5，ESP 加密算法为 3DES，不进行 ESP 认证

- 定制方式：如 图 8 所示，用户可以根据自己的需要配置安全提议的参数。详细配置如 表 6 所示。

图8 新建 IPSec 安全提议（定制方式）

表6 新建 IPSec 安全提议的详细配置（定制方式）

配置项	说明
安全提议名称	设置要新建的 IPSec 安全提议的名称
报文封装模式	设置安全协议对 IP 报文的封装模式 ● Tunnel：表示采用隧道模式 ● Transport：表示采用传输模式
安全协议	设置安全提议采用的安全协议 ● AH：表示采用 AH 协议 ● ESP：表示采用 ESP 协议 ● AH-ESP：表示先用 ESP 协议对报文进行保护，再用 AH 协议进行保护
AH 认证算法	当安全协议选择 AH 或 AH-ESP 时，设置 AH 协议采用的认证算法 可选的认证算法有 MD5 和 SHA1（表示 SHA-1 算法）
ESP 认证算法	当安全协议选择 ESP 或 AH-ESP 时，设置 ESP 协议采用的认证算法 可选的认证算法有 MD5 和 SHA1（表示 SHA-1 算法），选择空表示不进行 ESP 认证 提示 ESP 认证算法和 ESP 加密算法不能同时设置为空
ESP 加密算法	当安全协议选择 ESP 或 AH-ESP 时，设置 ESP 协议采用的加密算法 ● DES：表示采用 DES 算法，采用 56bits 的密钥进行加密 ● 3DES：表示采用 3DES 算法，采用 168bits 的密钥进行加密 ● AES128：表示采用 AES 算法，采用 128bits 的密钥进行加密 ● AES192：表示采用 AES 算法，采用 192bits 的密钥进行加密 ● AES256：表示采用 AES 算法，采用 256bits 的密钥进行加密 ● 选择空表示不进行 ESP 加密 提示 ● 对于保密及安全性要求非常高的地方，采用 3DES 算法可以满足需要，但 3DES 加密速度比较慢；对于普通的安全要求，DES 算法就可以满足需要 ● ESP 认证算法和 ESP 加密算法不能同时设置为空

3.5 配置安全策略模板

在导航栏中选择“VPN > IPSec > 模板配置”，进入安全策略模板的显示页面，如 图 9 所示。单击<新建>按钮，进入新建安全策略模板的配置页面，如 图 10 所示。

图9 模板配置

图10 新建安全策略模板

新建安全策略模板的详细配置如 表 7 所示。

表7 新建安全策略模板的详细配置

配置项	说明
模板名称	设置要新建安全策略模板的名称
模板序号	设置安全策略模板的序号 在一个安全策略模板组中，序号越小的安全策略模板，优先级越高
IKE 对等体	设置安全策略模板所引用的 IKE 对等体名称 可选的 IKE 对等体需先在“VPN > IKE > 对等体”中创建
IPSec 安全提议	设置安全策略模板所引用的 IPSec 安全提议名称，最多可以引用 6 个 IKE 协商将在安全隧道的两端搜索能够完全匹配的 IPSec 安全提议，如果找不到，则 SA 不能建立，需要被保护的报文将被丢弃

配置项		说明
PFS		设置使用此安全策略发起协商时是否使用 PFS（Perfect Forward Secrecy，完善的前向安全）特性，并指定采用的 Diffie-Hellman 组： ● DH Group1：表示采用 768-bit Diffie-Hellman 组 ● DH Group2：表示采用 1024-bit Diffie-Hellman 组 ● DH Group5：表示采用 1536-bit Diffie-Hellman 组 ● DH Group14：表示采用 2048-bit Diffie-Hellman 组 提示 ● DH Group14、DH Group5、DH Group2、DH Group1 的安全性和需要的计算时间依次递减 ● IPSec 在使用配置了 PFS 的安全策略发起一个协商时，在阶段 2 的协商中进行一次附加的密钥交换以提高通讯的安全性 ● 本端和对端指定的 Diffie-Hellman 组必须一致，否则协商会失败
ACL		设置安全策略模板所引用的 ACL 指定的 ACL 必须已经存在，且至少要包含一条规则 可支持保护 VPN 实例间的数据流
SA 生存周期	基于时间	设置安全策略的 SA 生存周期，可以选择基于时间和基于流量 提示 IKE 为 IPSec 协商建立安全联盟时，采用本地配置的生存周期和对端提议的生存周期中较小的一个
	基于流量	

3.6 配置安全策略

在导航栏中选择“VPN > IPSec > 策略”，进入安全策略的显示页面，如 图 11 所示。单击<新建>按钮，进入新建安全策略的配置页面，如 图 12 所示。

图11 策略

图12 新建安全策略

新建安全策略的详细配置如 表 8 所示。

表8 新建安全策略的详细配置

配置项	说明
策略名称	设置要新建安全策略的名称
策略序号	设置安全策略的序号 在一个安全策略组中，序号越小的安全策略，优先级越高
策略模板	设置安全策略所引用的安全策略模板组 提示 若选择了某个安全策略模板组，则后面的配置项（除了“聚合方式”）都不可配
IKE 对等体	设置安全策略所引用的 IKE 对等体名称 可选的 IKE 对等体需先在“VPN > IKE > 对等体”中创建
IPSec 安全提议	设置安全策略所引用的 IPSec 安全提议名称，最多可以引用 6 个 IKE 协商将在安全隧道的两端搜索能够完全匹配的 IPSec 安全提议，如果找不到，则 SA 不能建立，需要被保护的报文将被丢弃

配置项		说明
PFS		设置使用此安全策略发起协商时是否使用 PFS（Perfect Forward Secrecy，完善的前向安全）特性，并指定采用的 Diffie-Hellman 组： ● DH Group1：表示采用 768-bit Diffie-Hellman 组 ● DH Group2：表示采用 1024-bit Diffie-Hellman 组 ● DH Group5：表示采用 1536-bit Diffie-Hellman 组 ● DH Group14：表示采用 2048-bit Diffie-Hellman 组 提示 ● DH Group14、DH Group5、DH Group2、DH Group1 的安全性和需要的计算时间依次递减 ● IPSec 在使用配置了 PFS 的安全策略发起一个协商时，在阶段 2 的协商中进行一次附加的密钥交换以提高通讯的安全性 ● 本端和对端指定的 Diffie-Hellman 组必须一致，否则协商会失败
ACL		设置安全策略所引用的 ACL 指定的 ACL 必须已经存在，且至少要包含一条规则 可支持保护 VPN 实例间的数据流
聚合方式		设置安全策略的数据流保护方式为聚合方式，如果不选中该项，则安全策略的数据流保护方式为标准方式 该项的配置只在指定了安全策略所引用的 ACL 时才有效 提示 对于聚合方式和标准方式都支持的设备，要求两端的配置必须一致，即两端要么同时配置聚合方式，要么同时配置标准方式
SA 生存周期	基于时间	设置安全策略的 SA 生存周期，可以选择基于时间和基于流量 提示 IKE 为 IPSec 协商建立安全联盟时，采用本地配置的生存周期和对端提议的生存周期中较小的一个
	基于流量	

3.7 应用安全策略组

在导航栏中选择“VPN > IPSec > 应用”，进入接口应用安全策略情况的显示页面，如 图 13 所示。找到要应用安全策略组的接口，单击其对应的操作列中的图标，进入IPSec应用设置页面，如 图 14 所示。

图13 应用

图14 IPSec 应用设置

应用安全策略组的详细配置如 表 9 所示。

表9 应用安全策略组的详细配置

配置项	说明
接口名称	显示要应用安全策略组的接口名称
策略名称	设置应用的安全策略组的名称

说明

一个接口下只能引用一个安全策略组。如果在引用新的安全策略前，接口上已经配置了安全策略，需删除原来的安全策略才能配置新的安全策略。

4 配置举例一：基本应用

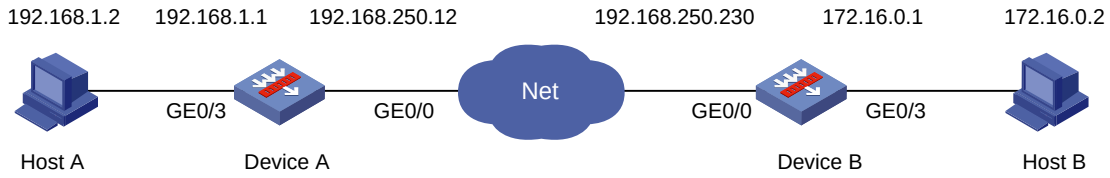
4.1 组网需求

说明

本配置举例中，采用的设备为 UTM 设备。该典型配置适合 Secpath F5000-A5、Secpath F1000E、Secpath UTM 200-A/200-M/200-S 防火墙

- 如 图 15 所示，在Device A和Device B之间建立一个安全隧道，对Host A所在的子网（192.168.1.0/24）与Host B所在的子网（172.16.0.0/24）之间的数据流进行安全保护。
- 安全协议采用 ESP 协议，认证算法采用 MD5，加密算法采用 DES。

图15 IPSec 配置组网图



4.2 使用版本

Secpath F1000E：V300R001B01 R3166 系列版本、V300R001B01 F3166 系列版本

Secpath F5000-A5：V300R002B01 R3206 系列版本

Secpath UTM 200-A/200-M/200-S 防火墙：V500R001B01 R5116 系列版本

4.3 配置步骤

1. 配置 Device A

步骤1 配置各接口的 IP 地址和所属安全域。（略）

步骤2 配置 ACL 3101，定义由子网 192.168.1.0/24 去子网 172.16.0.0/24 的数据流。

- 在导航栏中选择“防火墙 > ACL”，单击<新建>按钮，进行如下配置。

图16 新建 ACL 3101

- 输入访问控制列表 ID 为“3101”。
- 选择匹配规则为“用户配置”。
- 单击<确定>按钮完成操作。
- 在 ACL 的列表中找到访问控制列表 ID 为“3101”的 ACL，单击对应的图标，进入 ACL 3101 的规则显示页面，单击<新建>按钮，进行如下配置。

图17 配置允许由子网 192.168.1.0/24 去子网 172.16.0.0/24 数据流的规则

- 选择操作为“允许”。
- 选中“源 IP 地址”前的复选框，输入源 IP 地址为“192.168.1.0”，输入源地址通配符为“0.0.0.255”。
- 选中“目的 IP 地址”前的复选框，输入目的 IP 地址为“172.16.0.0”，输入目的地址通配符为“0.0.0.255”。
- 单击<确定>按钮完成操作。

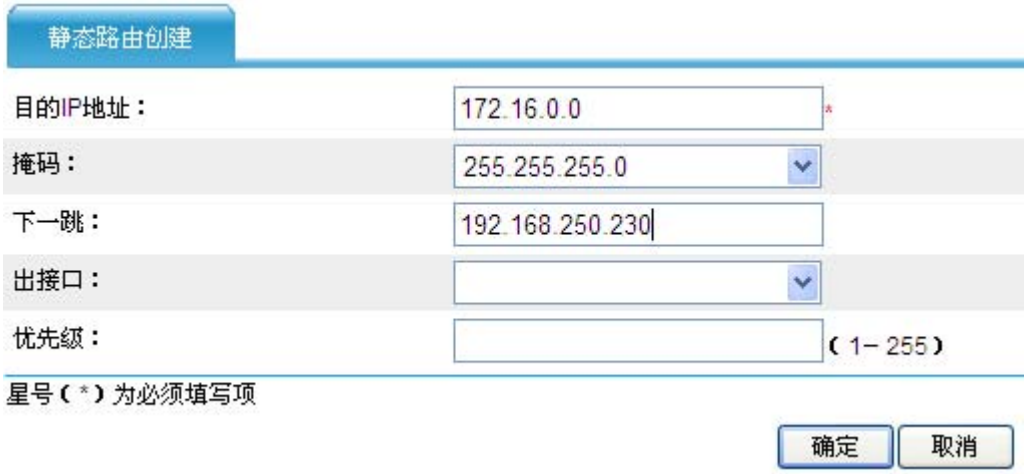
说明

- 如果在应用 IPSec 的出口上配置了对内网地址的 NAT 转换，如该例中的 GE0/0 上配置了对该内部地址 192.168.1.0/24 网段的 NAT 转换，则从子网 192.168.1.0/24 子网发出的流量会先进行 NAT 转换，则无法匹配 IPSec 保护的数据流，无法触发 IPSec 隧道的建立。这种情况下可以在 NAT 转换时用到的 ACL 中增加规则。
- 如在 GE0/0 口上配置了对 ACL 3901 的 NAT 转换。ACL 3901 原来只有规则 5， 允许源为 192.168.1.0/24 的子网。现在增加规则 1，则由子网 192.168.1.0/24 去子网 172.16.0.0/24 数据流不会匹配 ACL 3901。

步骤3 配置到 Host B 的静态路由。

- 在导航栏中选择“网络管理 > 路由管理 > 静态路由”，单击<新建>按钮，进行如下配置，如下图所示。

图18 配置到 Host B 的静态路由

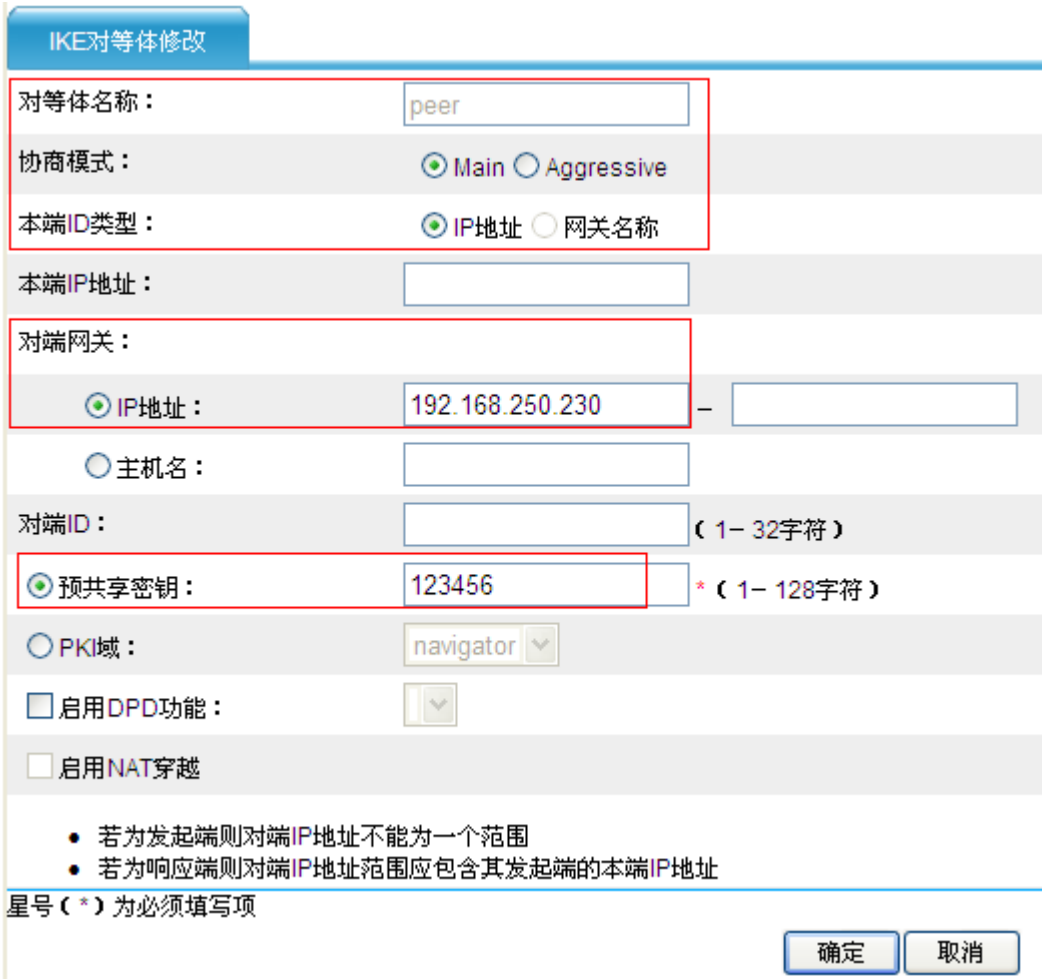


- 输入目的 IP 地址为“172.16.0.0”。
- 选择掩码为“255.255.255.0”。
- 输入下一跳为“192.168.250.230”
- 单击<确定>按钮完成操作。

步骤4 配置名为 peer 的 IKE 对等体。

- 在导航栏中选择“VPN > IKE > 对等体”，单击<新建>按钮，进行如下配置。

图19 配置 IKE 对等体



- 输入对等体名称为“peer”。
- 协商模式为默认的“Main”。
- 输入对端网关 IP 地址为“192.168.250.230”。
- 选中“预共享密钥”前的单选按钮，输入预共享密钥为“123456”。
- 单击<确定>按钮完成操作

步骤5 IKE 的安全提议采用默认值。

步骤6 配置名为 proposal 的 IPSec 安全提议，报文封装形式采用 Tunnel 模式，安全协议采用 ESP 协议，认证算法采用 MD5，加密算法采用 DES。

- 在导航栏中选择“VPN > IPSec > 安全提议”，单击<新建>按钮。
- 在安全提议配置向导页面选择“定制方式”，进行如下配置。

图20 配置名为 proposal 的 IPSec 安全提议

- 输入安全提议名称为“proposal”。
- 选择报文封装模式为“Tunnel”。
- 选择安全协议为“ESP”。
- 选择 ESP 认证算法为“MD5”。
- 选择 ESP 加密算法为“DES”。
- 单击<确定>按钮完成操作。

步骤7 配置名为 policy 的 IPSec 安全策略。

- 在导航栏中选择“VPN > IPSec > 策略”，单击<新建>按钮，进行如下配置。

图21 配置 IPSec 安全策略

- 输入策略名称为“policy”。
- 输入策略序号为“1”。
- 选择 IKE 对等体为“peer”。
- 选中名为“proposal”的 IPSec 安全提议，单击“<<”按钮。
- 输入 ACL 为“3101”。
- 单击<确定>按钮完成操作。

步骤8 在接口 GigabitEthernet0/0 上应用 IPSec 安全策略 map1。

- 在导航栏中选择“VPN > IPSec > 应用”，单击接口“GigabitEthernet0/0”对应的图标，进行如下配置。

图22 在接口 GigabitEthernet0/0 上应用 IPSec 安全策略

- 选择策略名称为“policy”。
- 单击<确定>按钮完成操作。

2. 配置 Device B

步骤1 配置各接口的 IP 地址和所属安全域。（略）

步骤2 配置 ACL 3101，定义由子网 172.16.0.0/24 去子网 192.168.1.0/24 的数据流。

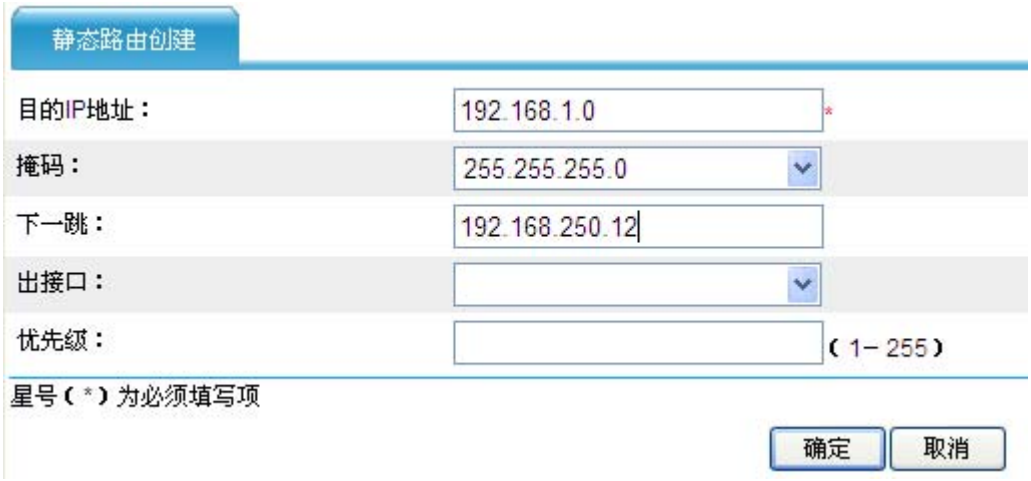
- 在导航栏中选择“防火墙 > ACL”，单击<新建>按钮。
- 输入访问控制列表 ID 为“3101”。
- 选择匹配规则为“用户配置”。
- 单击<确定>按钮完成操作。
- 在 ACL 的列表中找到访问控制列表 ID 为“3101”的 ACL，单击对应的图标，进入 ACL 3101 的规则显示页面，在该页面单击<新建>按钮。配置规则如下

高级ACL3101

规则ID	操作	描述
0	permit	ip source 172.16.0.0 0.0.0.255 destination 192.168.1.0 0.0.0.255

步骤3 配置到 Host A 的静态路由。

在导航栏中选择“网络管理 > 路由管理 > 静态路由”，单击<新建>按钮。配置如下。



步骤4 配置名为 peer 的 IKE 对等体。

- 在导航栏中选择“VPN > IKE > 对等体”，单击<新建>按钮。

- 输入对等体名称为“peer”。
- 选择协商模式为“Main”。
- 输入对端网关 IP 地址为“192.168.250.12”。
- 选中“预共享密钥”前的单选按钮，输入预共享密钥为“123456”。

- 单击<确定>按钮完成操作

步骤5 IKE 的安全提议采用默认值。

步骤6 配置名为 proposal 的 IPSec 安全提议。

- 在导航栏中选择“VPN > IPSec > 安全提议”，单击<新建>按钮。
- 在安全提议配置向导页面选择“定制方式”，进行如下配置。

图23 配置名为 proposal 的 IPSec 安全提议

- 输入安全提议名称为“proposal”。
- 选择报文封装模式为“Tunnel”。
- 选择安全协议为“ESP”。
- 选择 ESP 认证算法为“MD5”。
- 选择 ESP 加密算法为“DES”。
- 单击<确定>按钮完成操作。

步骤7 配置名为 policy 的 IPSec 安全策略。

- 在导航栏中选择“VPN > IPSec > 策略”，单击<新建>按钮，进行如下配置。

图24 配置 IPSec 安全策略

- 输入策略名称为“policy”。
- 输入策略序号为“1”。
- 选择 IKE 对等体为“peer”。
- 选中名为“proposal”的 IPSec 安全提议，单击“<<”按钮。
- 输入 ACL 为“3101”。
- 单击<确定>按钮完成操作。

步骤8 在接口 GigabitEthernet0/0 上应用 IPSec 安全策略 policy。

- 在导航栏中选择“VPN > IPSec > 应用”，单击接口“GigabitEthernet0/0”对应的图标。
- 选择策略名称为“policy”。
- 单击<确定>按钮完成操作。

4.4 配置结果验证

完成上述配置后，Device A 和 Device B 之间如果有子网 192.168.1.0/24 与子网 172.16.0.0/24 之间的报文通过，将触发 IKE 进行协商建立 SA。IKE 协商成功并创建了 SA 后，子网 192.168.1.0/24 与子网 172.16.0.0/24 之间的数据流将被加密传输。

4.4.1 查看 IPSec 安全联盟

在导航栏中选择“VPN > IPSec > 安全联盟”，进入 IPSec 安全联盟概要信息的显示页面。

本端IP地址	对端IP地址	SPI	安全协议	认证算法	加密算法
192.168.250.12	192.168.250.230	1105559047	ESP	HMAC-MD5-96	DES
192.168.250.230	192.168.250.12	4067445650	ESP	HMAC-MD5-96	DES

4.4.2 查看报文统计

在导航栏中选择“VPN > IPSec > 报文统计”，进入报文统计信息的显示页面。

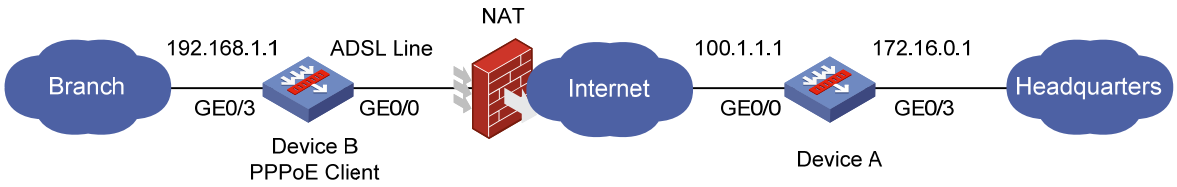
统计项	统计值
受安全保护的输入/输出数据包	4/4
受安全保护的输入/输出字节数	336/336
被设备丢弃了的受安全保护的输入/输出数据包	0/0
因为内存不足而被丢弃的数据包数目	0
因为找不到安全联盟而被丢弃的数据包的数目	0
因为队列满而被丢弃的数据包的数目	0
因为认证失败而被丢弃的数据包的数目	0
因为数据包长度不正确而被丢弃的数据包数目	0
重放的数据包数目	0
因为数据包过长而被丢弃的数据包的数目	0
因为安全联盟不正确而被丢弃的数据包的数目	0

5 配置举例二：与 NAT 结合

5.1 组网需求

本例将 IPsec 和 ADSL 相结合，是目前实际中广泛应用的典型案例。

- Device B 通过 ADSL 卡直接连接公网的 DSLAM 接入端，作为 PPPoE 的 Client 端。Device B 从 ISP 动态获得的 IP 地址为私网地址，故 Device A、Device B 都需要配置 NAT 穿越。
- 总公司局域网通过 Device A 接入到因特网。
- 为了保证信息安全采用 IPsec/IKE 方式创建安全隧道。



5.2 配置说明

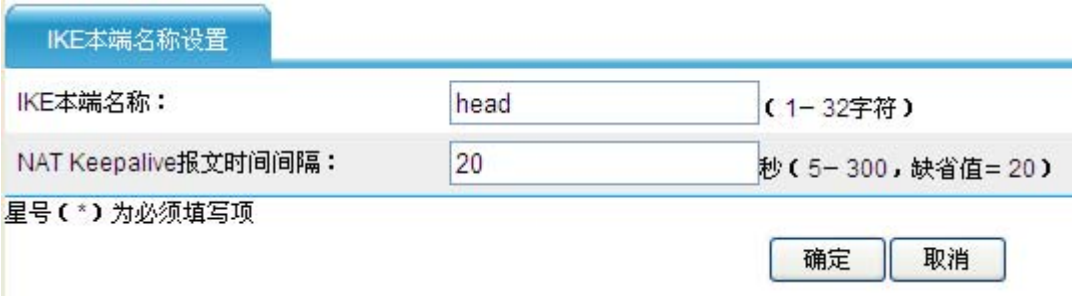
因为分支的 IP 地址为自动获取，必须将 IKE 的协商模式配置为“Aggressive”。IKE 协商采用“网关名称”，且配置“NAT 穿越”。

5.3 配置步骤

1. 配置中心设备 DeviceA

步骤1 配置各接口的 IP 地址和所属安全域。（略）

步骤2 配置 IKE 本端名称为 head。



步骤3 配置名为 gate 的 IKE 对等体。

- 在导航栏中选择“VPN > IKE > 对等体”，单击<新建>按钮。
- 输入对等体名称为“gate”。
- 选择协商模式为“Aggressive”。
- 选择本端 ID 类型为“网关名称”。
- 输入“对端 ID”为 branch。
- 选中“预共享密钥”前的单选按钮，输入预共享密钥为“123456”。
- 勾选“启用 NAT 穿越”前的单选框。
- 单击<确定>按钮完成操作。

步骤4 配置名为 proposal 的 IPSec 安全提议。

- 在导航栏中选择“VPN > IPSec > 安全提议”，单击<新建>按钮。
- 在安全提议配置向导页面选择“定制方式”。
- 配置名为 proposal 的安全提议，算法均采用默认配置，如下图。

图25 配置名为 proposal 的 IPSec 安全提议

步骤5 配置名为 template 的 IPSec 安全策略模板。

- 输入模板序号为“1”。
- 选择 IKE 对等体为“gate”。
- 选中名为“proposal”的 IPSec 安全提议，单击“<<”按钮。
- 单击<确定>按钮完成操作。

步骤6 配置名为 policy_nat 的 IPSec 安全策略。

- 在导航栏中选择“VPN > IPSec > 策略”，单击<新建>按钮，进行如下配置。

步骤7 在接口 GigabitEthernet0/0 上应用 IPSec 安全策略 policy_nat。

2. 配置分支设备 DeviceB

步骤1 配置各接口的 IP 地址和所属安全域。（略）

步骤2 配置 ACL 3101，定义由子网 192.168.1.0/24 去子网 172.16.0.0/24 的数据流。

说明

- 如果在应用 IPSec 的出口上配置了对内网地址的 NAT 转换，如该例中的 GE0/0 上配置了对该内部地址 192.168.1.0/24 网段的 NAT 转换，则从子网 192.168.1.0/24 子网发出的流量会先进行 NAT 转换，则无法匹配 IPSec 保护的数据流，无法触发 IPSec 隧道的建立。这种情况下可以在 NAT 转换时用到的 ACL 中增加规则。
- 如在 GE0/0 口上配置了对 ACL 3901 的 NAT 转换。ACL 3901 原来只有规则 5， 允许源为 192.168.1.0/24 的子网。现在增加规则 1，则由子网 192.168.1.0/24 去子网 172.16.0.0/24 数据流不会匹配 ACL 3901。

步骤3 配置 IKE 本端名称为 branch。

步骤4 配置名为 gate 的 IKE 对等体。

- 在导航栏中选择“VPN > IKE > 对等体”，单击<新建>按钮。
- 输入对等体名称为“gate”。
- 选择协商模式为“Aggressive”。
- 选择本端 ID 类型为“网关名称”。
- 设置对端网关 IP 地址为 100.1.1.1。 //分支上要指定中心的 IP 地址
- 输入“对端 ID”为 head。
- 选中“预共享密钥”前的单选按钮，输入预共享密钥为“123456”。
- 勾选“启用 NAT 穿越”前的单选框。
- 单击<确定>按钮完成操作。

步骤5 配置名为 proposal 的 IPSec 安全提议。

- 在导航栏中选择“VPN > IPSec > 安全提议”，单击<新建>按钮。
- 在安全提议配置向导页面选择“定制方式”。
- 配置名为 proposal 的安全提议，算法均采用默认配置，如下图。

图26 配置名为 proposal 的 IPSec 安全提议

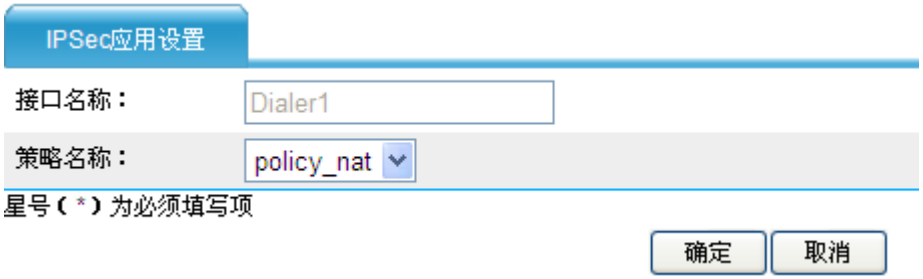
步骤6 配置名为 policy_nat 的 IPSec 安全策略。

- 在导航栏中选择“VPN > IPSec > 策略”，单击<新建>按钮，进行如下配置。

图27 配置 IPSec 安全策略

- 输入策略名称为“policy_nat”。
- 输入策略序号为“1”。
- 选择 IKE 对等体为“gate”。
- 选中名为“proposal”的 IPSec 安全提议，单击“<<”按钮。
- 输入 ACL 为“3101”。
- 单击<确定>按钮完成操作。

步骤7 在接口 Dialer1 上应用 IPSec 安全策略 policy_nat。



5.4 配置验证结果

从分支的主机 192.168.1.2 访问中心的内部地址 172.16.1.2，触发 IPSec 隧道建立。

5.4.1 查看 IPSec 安全联盟

在导航栏中选择“VPN > IPSec > 安全联盟”，进入 IPSec 安全联盟概要信息的显示页面。

本端IP地址 查询 | 高级查询

本端IP地址	对端IP地址	SPI	安全协议	认证算法	加密算法	操作
100.1.1.1	140.0.0.7	2342415508	ESP	HMAC-MD5-96	DES	

5.4.2 查看报文统计

在导航栏中选择“VPN > IPSec > 报文统计”，进入报文统计信息的显示页面。

统计项	统计值
受安全保护的输入/输出数据包	18109/25970
受安全保护的输入/输出字节数	9174824/31471120
被设备丢弃了的受安全保护的输入/输出数据包	0/1
因为内存不足而被丢弃的数据包数目	0
因为找不到安全联盟而被丢弃的数据包的数目	1
因为队列满而被丢弃的数据包的数目	0
因为认证失败而被丢弃的数据包的数目	0
因为数据包长度不正确而被丢弃的数据包数目	0
重放的数据包数目	0
因为数据包过长而被丢弃的数据包的数目	0
因为安全联盟不正确而被丢弃的数据包的数目	0

刷新 全部清零

6 注意事项

配置 IPSec 时需要注意如下事项：

(1) 通常情况下，由于 IKE 协议采用 UDP 的 500 端口进行通信，IPSec 的 AH 和 ESP 协议分别使用 51 或 50 号协议来工作，因此为保障 IKE 和 IPSec 的正常运行，需要确保应用了 IKE 和 IPSec 配置的接口上没有禁止掉属于以上端口和协议的流量。

(2) 若在接口上同时使能 IPSec 和 QoS，同一个 IPSec 安全联盟的数据流如果被 QoS 分类进入不同队列，会导致部分报文发送乱序。由于 IPSec 具有防重放功能，IPSec 入方向上对于防重放窗口之外的报文会进行丢弃，从而导致丢包现象。因此当 IPSec 与 QoS 结合使用时，必须保证 IPSec 分类与 QoS 分类规则配置保持一致。IPSec 的分类规则完全由引用的 ACL 规则确定。

7 相关资料

7.1 相关协议和标准

- RFC2401：Security Architecture for the Internet Protocol
- RFC2402：IP Authentication Header
- RFC2406：IP Encapsulating Security Payload

7.2 其它相关资料

《Web 配置手册 IPSec》

《SecPath 操作手册-VPN》