在Cisco RV320千兆双WAN VPN路由器和Cisco 500系列集成服务适配器之间配置站点到站点VPN隧道

目标

虚拟专用网络(VPN)是广泛用于将远程网络连接到主专用网络的技术，通过公共线路以加密信道的形式模拟专用链路。远程网络可以连接到专用主网络，就像它作为专用主网络的一部分存在一样，而不会引起安全问题，因为两阶段协商会以只有VPN终端知道如何解密的方式加密VPN流量。
本简短指南提供了在Cisco 500系列集成多业务适配器和Cisco RV系列路由器之间构建站点到站点IPsec VPN隧道的示例设计。

适用设备

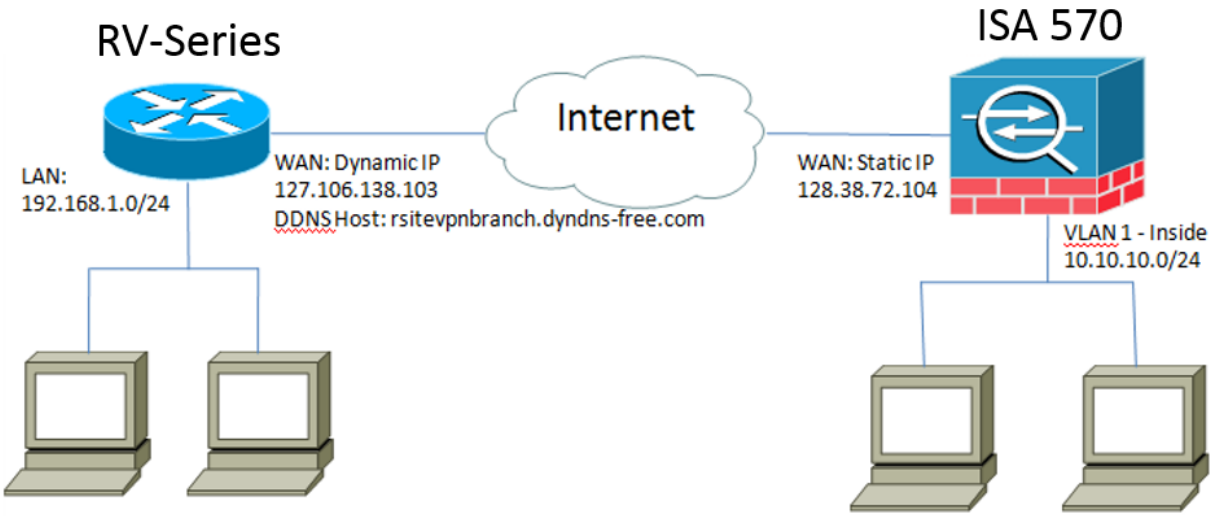
·思科RV系列路由器(RV320)
·思科500系列集成多业务适配器(ISA570)

软件版本

·4.2.2.08 [Cisco RV0xx系列VPN路由器]

预配置

网络图
以下显示站点到站点VPN拓扑。



在远程办公室的Cisco RV系列路由器与总部的Cisco 500系列ISA之间配置并建立站点到站点IPsec VPN隧道。

通过此配置，远程办公室LAN 192.168.1.0/24中的主机和总部LAN 10.10.10.0/24中的主机可以通过VPN安全地相互通信。

核心概念

Internet 密钥交换 (IKE)

互联网密钥交换(IKE)是用于在IPsec协议簇中设置安全关联(SA)的协议。IKE以Oakley协议、Internet安全关联和密钥管理协议(ISAKMP)为基础构建，并使用Diffie-Hellman密钥交换来设置共享会话密钥，从中派生加密密钥。

Internet 安全关联和密钥管理协议 (ISAKMP)

Internet安全关联和密钥管理协议(ISAKMP)用于协商两个VPN终端之间的VPN隧道。它定义了身份验证、通信和密钥生成的过程，并由IKE协议用于交换加密密钥和建立安全连接。

互联网协议安全(IPsec)

IP安全协议(IPsec)是一种协议簇，用于通过验证和加密数据流的每个IP数据包来保护IP通信。IPsec还包括用于在会话开始时在代理之间建立相互身份验证的协议以及在会话期间使用的加密密钥的协商。 IPsec可用于保护主机、网关或网络对之间的数据流。

设计提示

VPN拓扑 — 点对点VPN拓扑意味着在主站点和远程站点之间配置了安全的IPsec隧道。企业通常需要多站点拓扑中的多个远程站点，并实施中心辐射型VPN拓扑或全网状VPN拓扑。中心辐射型VPN拓扑意味着远程站点不需要与其他远程站点通信，并且每个远程站点只与主站点建立一个安全的IPsec隧道。全网状VPN拓扑意味着远程站点需要与其他远程站点通信，并且每个远程站点与主站点和所有其他远程站点建立一个安全的IPsec隧道。
VPN Authentication - IKE协议用于在建立VPN隧道时对VPN对等体进行身份验证。IKE身份验证方法多种多样，而预共享密钥是最方便的方法。思科建议应用强预共享密钥。
VPN加密 — 为确保通过VPN传输的数据的机密性，加密算法用于加密IP数据包的负载。DES、3DES和AES是三种常见的加密标准。与DES和3DES相比，AES被认为是最安全的。思科强烈建议应用AES-128位或更高加密（例如AES-192和AES-256）。 但是，更强大的加密算法需要路由器提供更多的处理资源。
动态WAN IP寻址和动态域名服务(DDNS) — 需要在两个公有IP地址之间建立VPN隧道。如果WAN路由器从Internet服务提供商(ISP)接收静态IP地址，则可以直接使用静态公有IP地址实施VPN隧道。但是，大多数小型企业使用经济高效的宽带Internet服务（如DSL或电缆），并从ISP接收动态IP地址。在这种情况下，动态域名服务(DDNS)可用于将动态IP地址映射到完全限定域名(FQDN)。
LAN IP编址 — 每个站点的专用LAN IP网络地址应不重叠。应始终更改每个远程站点的默认LAN IP网络地址。

配置提示

预配置核对表
步骤1.在RV320与其DSL或电缆调制解调器之间连接以太网电缆，在ISA570与其DSL或电缆调制解调器之间连接以太网电缆。
步骤2.打开RV320，然后将内部PC、服务器和其他IP设备连接到RV320的LAN端口。
步骤3.打开ISA570，然后将内部PC、服务器和其他IP设备连接到ISA570的LAN端口。
步骤4.确保在不同子网上的每个站点配置网络IP地址。在本例中，远程办公室LAN使用192.168.1.0，而主办公室LAN使用10.10.10.0。

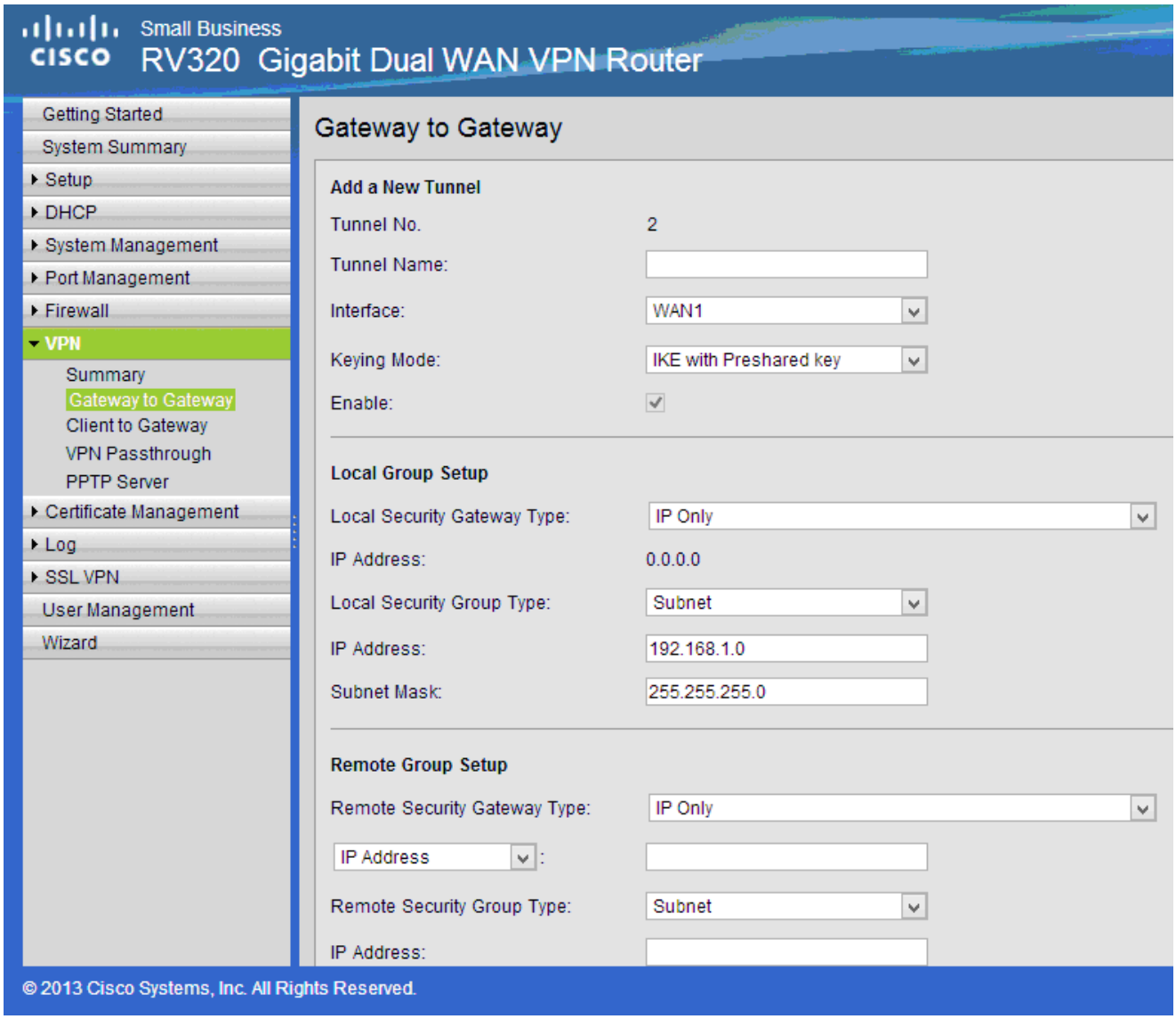
步骤5.确保本地PC能够连接到各自的路由器，以及与同一LAN中的其他PC连接。

识别WAN连接

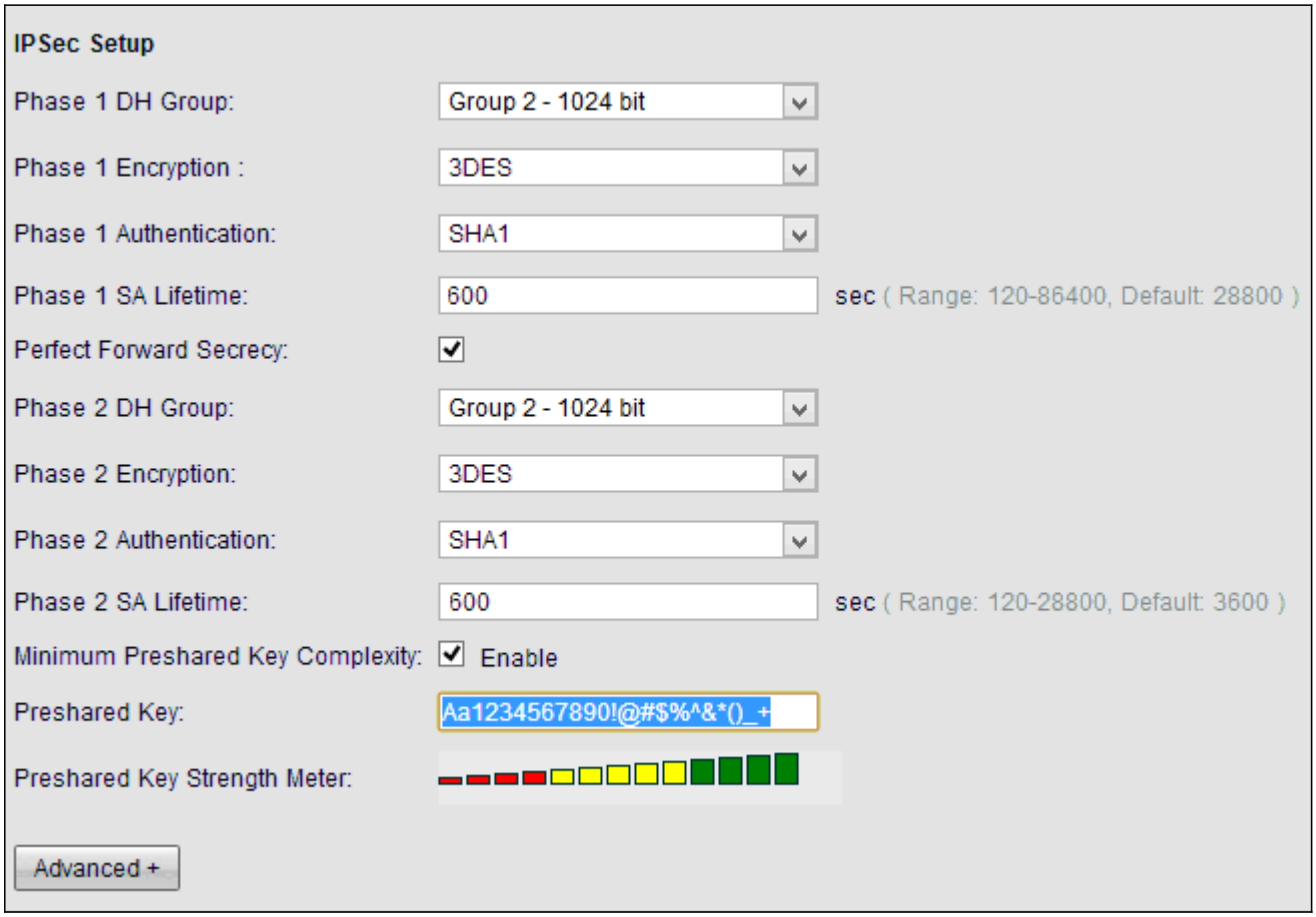
您需要知道ISP是提供动态IP地址还是静态IP地址。ISP通常提供动态IP地址，但您应在完成站点到站点VPN隧道配置之前确认这一点。

在远程办公室为RV320配置站点到站点IPsec VPN隧道

步骤1.转到**VPN > Gateway-to-Gateway**（参见图片）
a) 输入隧道名称，例如RemoteOffice。
b) 将接口设置为WAN1。
c) 使用预共享密钥将密钥模式设置为IKE。
d) 输入本地IP地址和远程IP地址。
下图显示RV320千兆双WAN VPN路由器网关到网关页面：



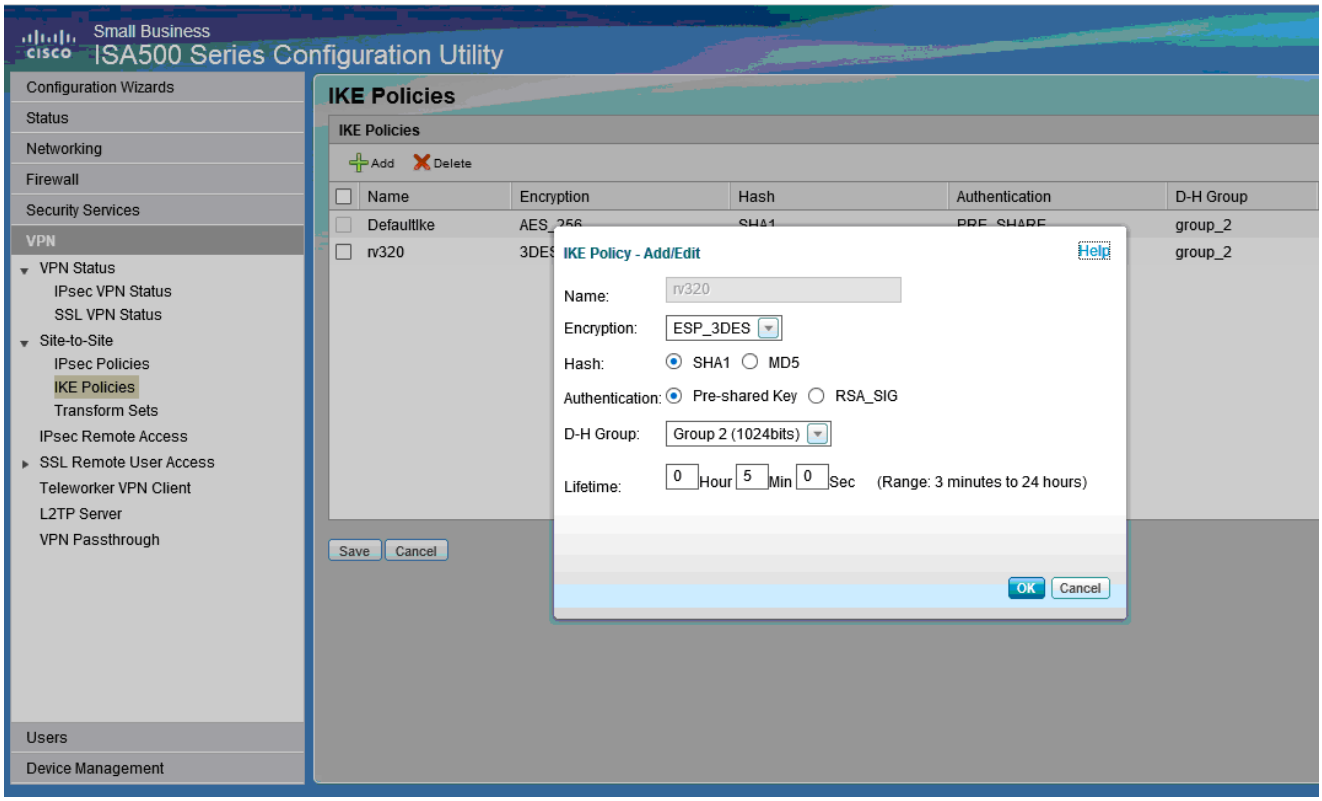
步骤2.设置IPSec隧道设置（参见图片）
a) 将*Encryption*设置为3DES。
b) 将*Authentication*设置为SHA1。
c) 查查完*全向前保密*。
d) 设置预*共享密*钥（两台路由器上需要相同）。
以下显示IPSec设置（第1和第2阶段）：



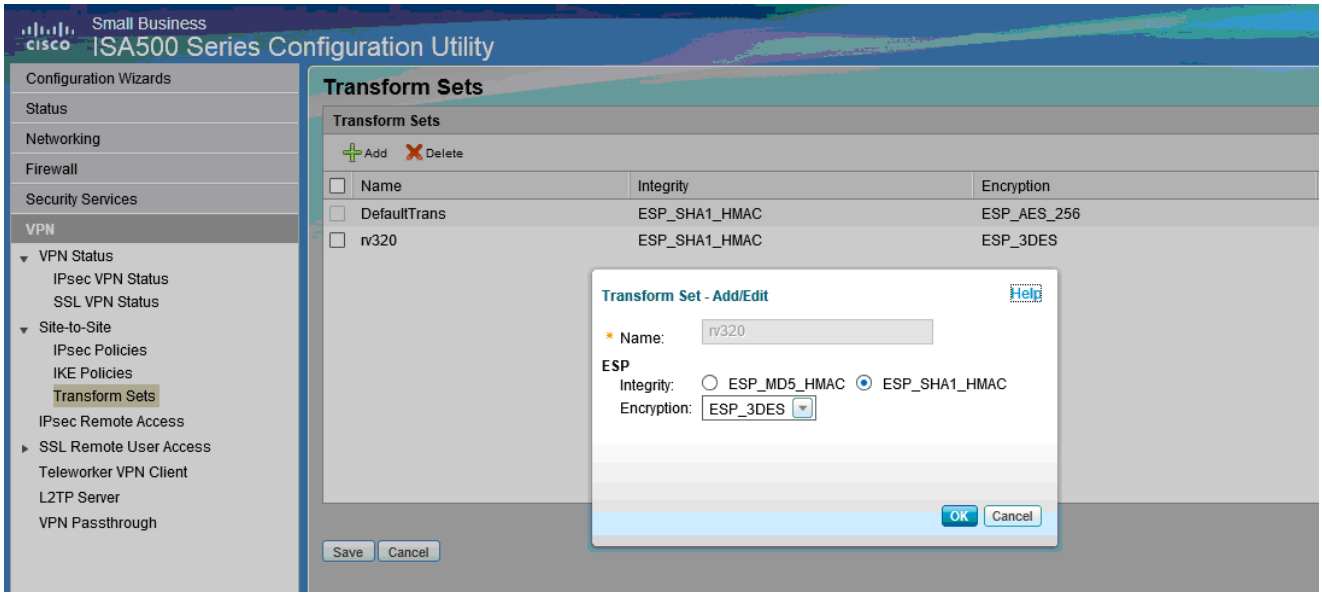
注意：请记住，站点到站点IPsec VPN隧道两端的IPsec隧道设置必须匹配。如果RV320的IPsec隧道设置和ISA570之间存在任何差异，则两台设备将无法协商加密密钥并无法连接。
步骤3.单击**Save**完成配置。

在总部为ISA570配置站点到站点IPsec VPN隧道

步骤1.转到**VPN > IKE**策略（参见图片）
a) 将*Encryption*设置为ESP_3DES。
b) 将*Hash*设置为SHA1。
c) 将*Authentication*设置为Pre-shared Key。
d) 将*D-H组*设置为组2（1024位）。
下图显示IKE策略：



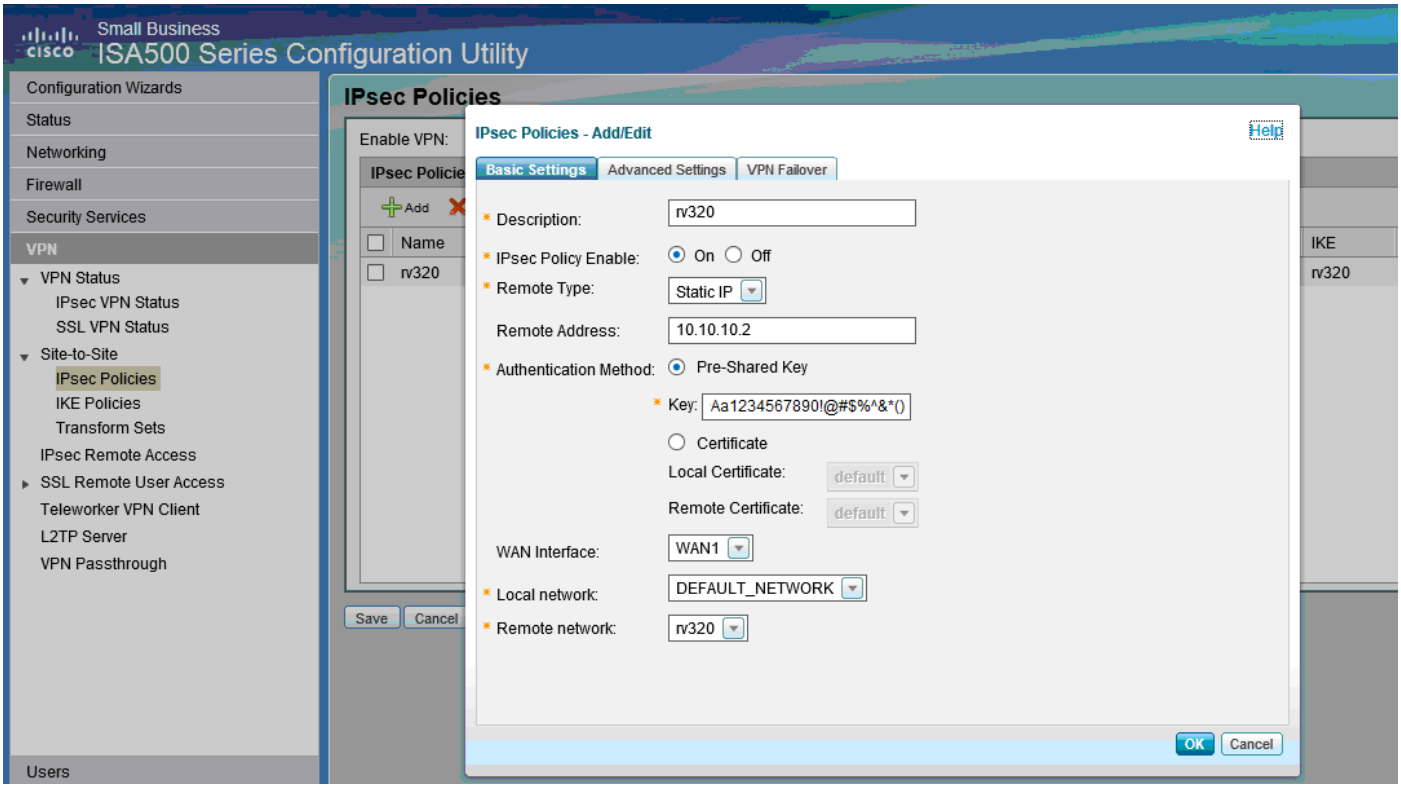
步骤2.转到**VPN > IKE转换集**（参见图片）
a) 将*Integrity*设置为ESP_SHA1_HMAC。
b) 将*Encryption*设置为ESP_DES。
以下显示IKE转换集：



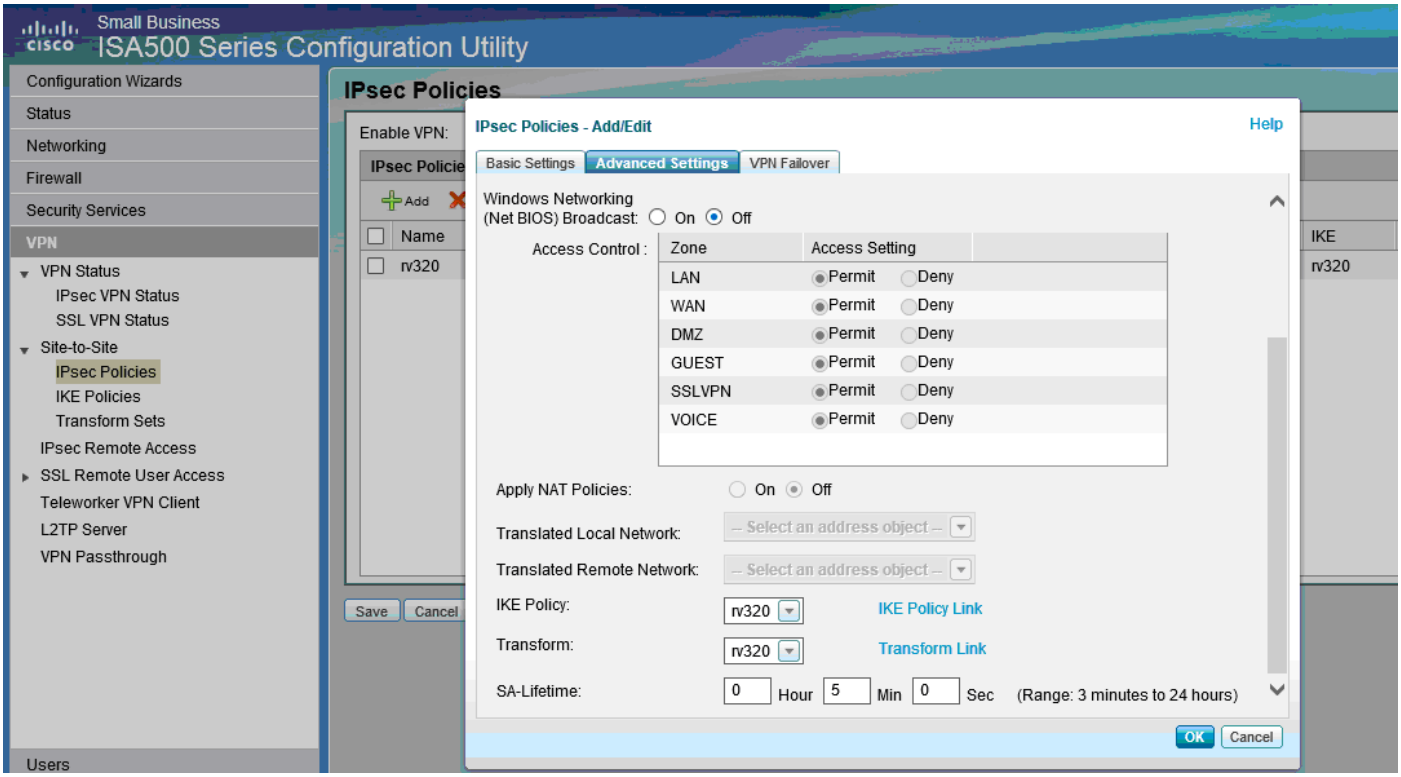
步骤3.转到VPN > **IPsec Policies > Add > Basic Settings**（参见图片）

a) 输入 *Description*，如RV320。
b) 将IPsec *Policy Enable*设置为On。
c) 将 *Remote Type（远程类型）设置为Static IP*。
d) 输入 *远程地址*。
e) 将 *Authentication Method*（身份验证方法）设置为Pre-Shared Key。
f) 将 *WAN接口*设置为WAN1。
g) 将本 *地网络*设置为DEFAULT_NETWORK。

h.) 将 *Remote Network*设置为RV320。
下图显示IPsec策略基本设置：



步骤4.转到VPN > **IPsec Policies > Add > Advanced Settings**（参见图片）
a) 分别 *将IKE策略* *和IKE转*换集设置为步骤1和步骤2中创建的。
b) 将 *SA-Lifetime*设置为0小时5分0秒。
c) Click **OK**.
以下显示IPsec策略高级设置：



步骤5.连接站点到站点IPsec VPN隧道（参见图片）

a) 将 *Enable VPN* 设置为On。
b) 单击“ **Connect (连接)** ”按钮。
下图显示连接按钮：