在RV320和RV325 VPN路由器系列的网关到网关的虚拟专用网络(VPN)配置

客观

VPN用于通过什么形成非常安全连接两个终端，在公共或共有的互联网，被呼叫VPN隧道。网关到网关的VPN连接特别地允许两路由器彼此安全地接通和逻辑上看来的一端的一个客户端是同一个远程网络的一部分在另一端的。在互联网和资源更加容易地和安全地将共享的此enable (event)数据。必须执行配置在能将设立的成功的网关到网关的VPN连接的连接的两边。此条款的目的将指导您与网关到网关的VPN连接的配置在RV32x VPN路由器系列的。

可适用的设备

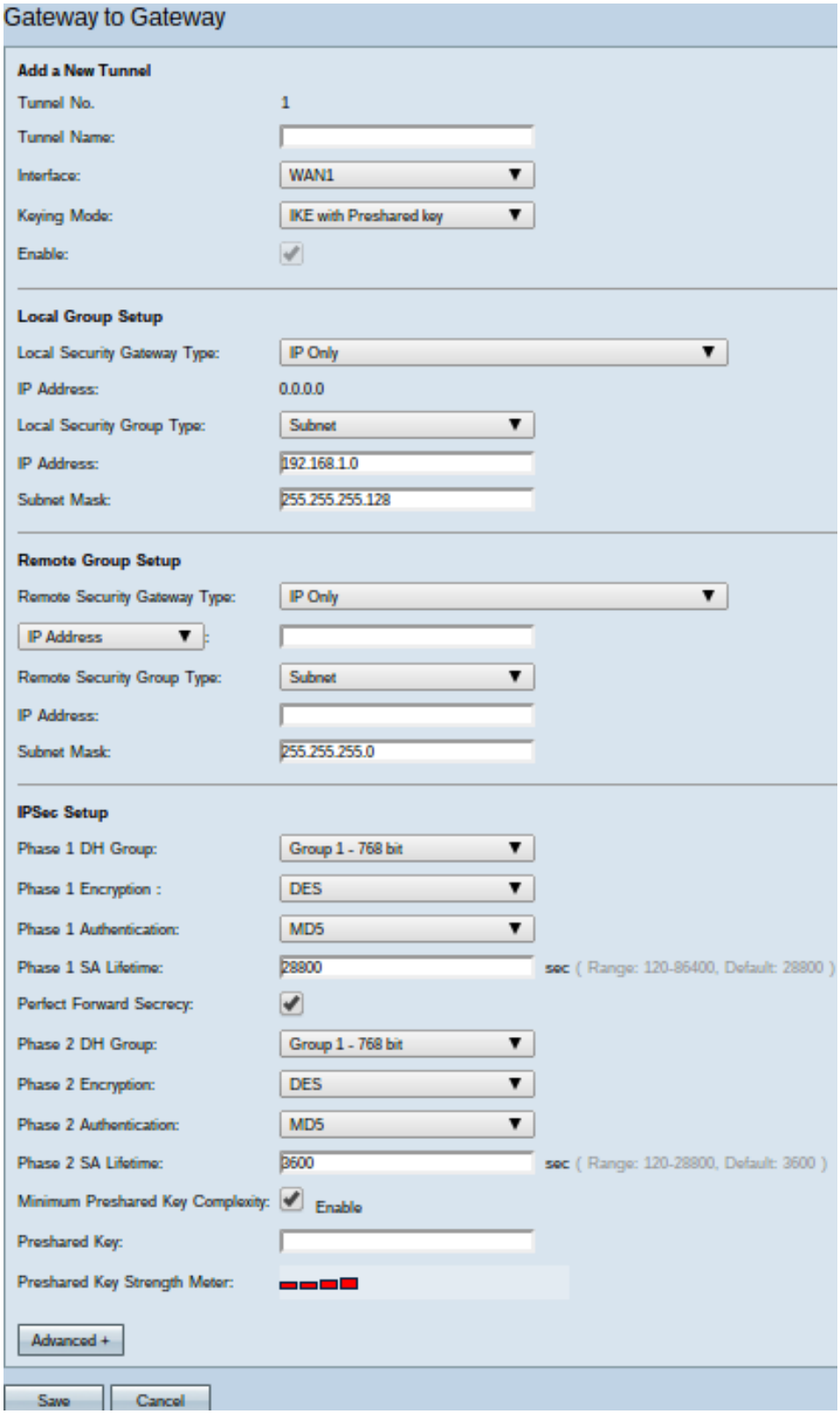
- RV320双倍广域网VPN路由器
- RV325千兆位双重广域网VPN路由器

软件版本

- v1.1.0.09

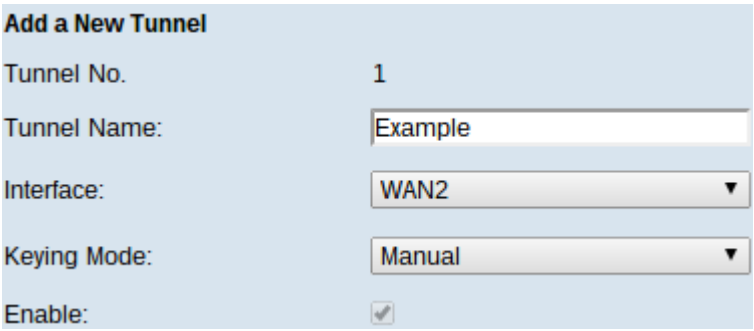
网关到网关

步骤1.登陆到Web配置工具并且选择**VPN >网关到网关**。*网关到网关的*页打开：



为了VPN连接能适当地工作，互联网协议安全(IPSec)值在连接的两边必须是相同的。连接的两边必须属于到不同的是区域网(LAN)和其中至少一的路由器可识别的由静态IP地址或一个动态DNS主机名-。

添加新通道



•隧道没有—显示被创建的当前隧道。路由器支持100条隧道。

步骤1.输入一个名字对于VPN隧道在隧道名字段。它不必须匹配名字使用在隧道的另一端。

Step 2.从接口下拉列表请选择广域网络(广域网)端口使用隧道。

•WAN1 —路由器的专用的WAN端口。

•WAN2 —路由器的WAN2/DMZ端口。在下拉菜单只显示，如果被配置了作为广域网而不是解除军事管制区域(DMZ)端口。

•USB1 —路由器的USB1端口。如果有3G/4G/LTE USB Dongle附有端口，只工作。

•USB2 —路由器的USB2端口。如果有3G/4G/LTE USB Dongle附有端口，只工作。

第 3 步：从密钥模式下拉列表请选择隧道安全使用。

•手工—此选项手工让您配置键而不是协商键与VPN连接的另一边。

•IKE用预共用的键—选择此选项对enable (event)设置VPN隧道的一个安全关联的互联网密钥交换协议(IKE)。IKE使用一个预共用的键验证远端对等体。

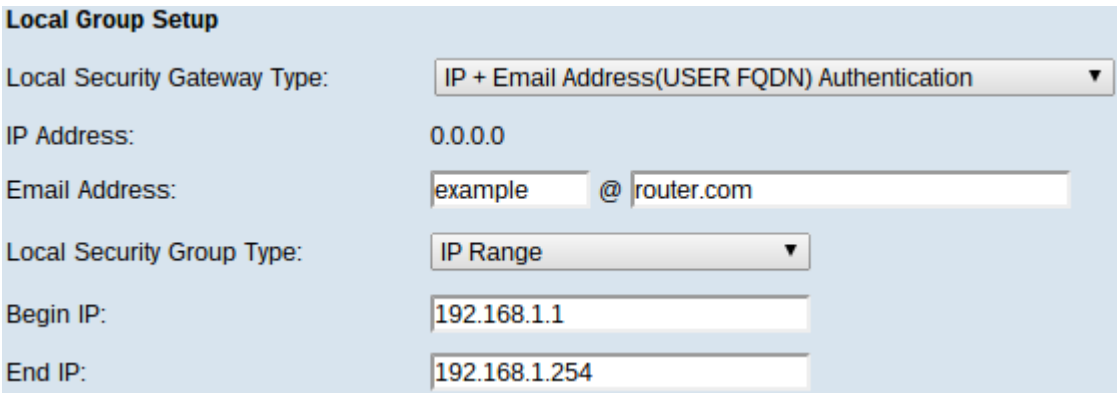
•与认证的IKE —选择此选项对enable (event)与提供一个更加安全的方式自动地生成和交换预共用的隧道的键设立验证和安全通信的认证的Internet Key Exchange (IKE)协议。

第 4 步：检查Enable复选框对enable (event) VPN隧道。默认情况下它是启用的。

本地组设置

这些设置应该匹配路由器的“远程组建立”设置在另一端VPN隧道的。

Note:如果Manual或IKE用预共用的键从密钥模式下拉列表被挑选从第3步Add新通道开始从Step1并且跳到第2步到第4.步。如果与认证的IKE选择了请跳过Step1。



第 1 步：从本地安全网关请键入下拉列表选择方法识别路由器设立VPN隧道。

•仅IP —对隧道的访问通过仅静态广域网IP是可能的。如果仅路由器有任何静态广域网IP，您能选择此选项。静态广域网IP地址是自动生成的字段。

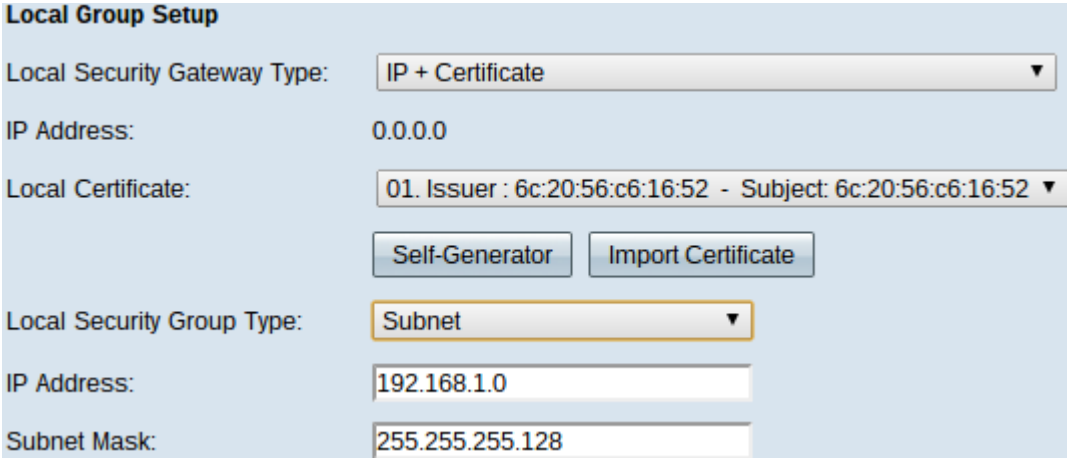
•IP+对隧道的域名(FQDN)验证访问通过静态IP地址和一个注册的域是可能的。如果选择此选项，请输入注册的域的名字在域名字段。静态广域网IP地址是自动生成的字段。

•IP+电子邮件地址。(用户FQDN)对隧道的验证访问通过静态IP地址和电子邮件地址是可能的。如果选择此选项，请输入电子邮件地址在电子邮件地址字段。静态广域网IP地址是自动生成的字段。

•对隧道的动态IP+域名(FQDN)验证访问通过一个动态IP地址和一个注册的域是可能的。如果选择此选项，请输入注册的域的名字在域名字段。

•动态IP+电子邮件地址。(用户FQDN)对隧道的验证访问通过一个动态IP地址和电子邮件地址是可能的。如果选择此选项，请输入电子邮件地址在电子邮件地址字段。

Note:在本地组建立区域的以下更改更改，当与与认证的IKE一起使用。



本地安全网关类型下拉列表变得uneditable并且显示IP+认证。这是能使用隧道的LAN资源。IP Address字段显示设备的广域网IP地址。它不是编辑可能的用户。

步骤2.从本地认证下拉列表选择认证。证书在VPN连接提供强力身份验证安全。

第3.步(可选)点击自**生成器**按钮显示*证书生成器*窗口配置和生成证书。

第4.步(可选)点击**进口证明书**按钮显示*我的认证*窗口查看和配置证书。

第 5 步：从本地安全组请键入下拉列表选择下列之一：

•IP地址—此选项让您指定能使用此VPN隧道的一个设备。您只需要在IP Address字段输入设备的IP地址。

•子网—选择此选项允许属于相同子网使用VPN隧道的所有设备。您在子网掩码字段需要输入网络IP地址在IP Address字段和其各自子网掩码。

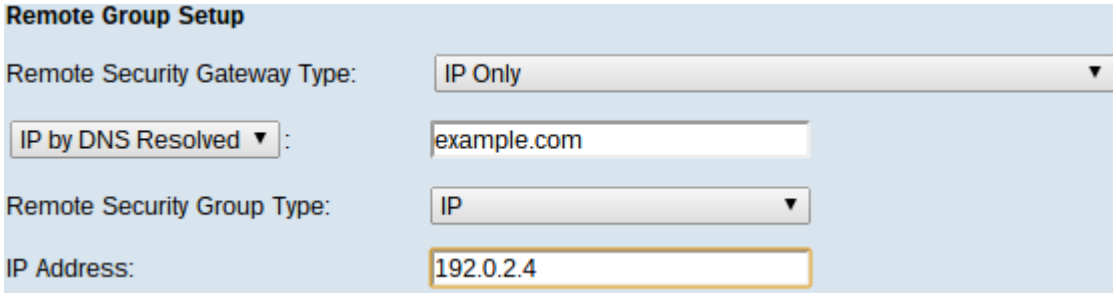
•IP范围—选择此选项指定能使用VPN隧道设备的范围。您在开始IP字段需要输入第一个IP地址和设备的范围的最后IP地址和结束IP字段。

远程组建立

这些设置应该匹配路由器的“本地组设置的”设置在另一端VPN隧道的。

Note:如果Manual或IKE用预共用的键从密钥模式下拉列表被挑选从第3步Add新通道开始从

Step1并且跳到第2步到第5.步。或者，如果与认证的IKE选择了请跳过Step1。



第 1 步：从远程安全网关请键入下拉列表，选择方法识别另一个路由器设立VPN隧道。

•仅IP —对隧道的访问通过仅静态广域网IP是可能的。如果认识远程路由器的IP地址请直接地在远程安全网关类型字段之下选择在下拉列表的IP地址并且输入地址。由被解决的DNS选择IP是否在IP不认识IP地址，然而认识域名并且输入路由器的域名由DNS被解决的字段。

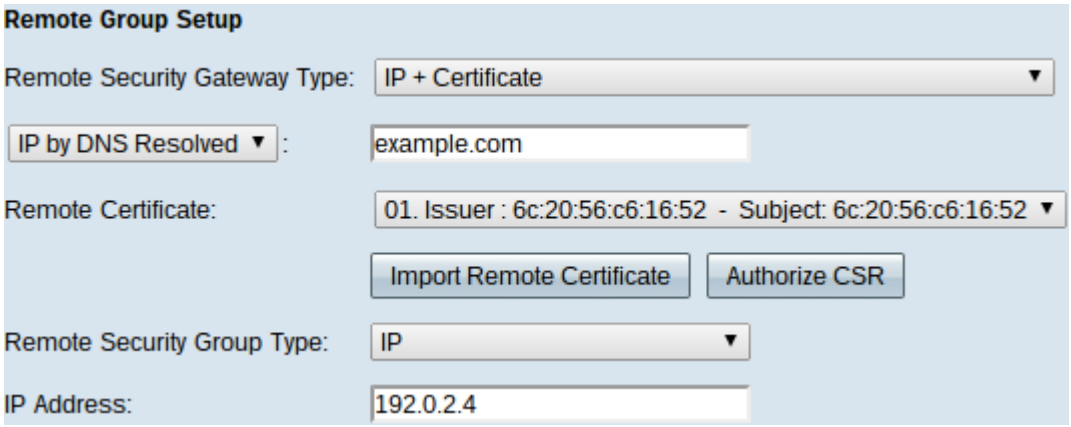
•IP+对隧道的域名(FQDN)验证访问通过静态IP地址和路由器的一个注册的域是可能的。如果认识远程路由器的IP地址请直接地在远程安全网关类型字段之下选择在下拉列表的IP地址并且输入地址。由被解决的DNS选择IP是否在IP不认识IP地址，然而认识域名并且输入路由器的域名由DNS被解决的字段。如果选择此选项，请输入注册的域的名字在域名字段。

•IP+电子邮件地址。(用户FQDN)对隧道的验证访问通过静态IP地址和电子邮件地址是可能的。如果认识远程路由器的IP地址请直接地在远程安全网关类型字段之下选择在下拉列表的IP地址并且输入地址。由被解决的DNS选择IP是否在IP不认识IP地址，然而认识域名并且输入路由器的域名由DNS被解决的字段。输入电子邮件地址在电子邮件地址字段。

•对隧道的动态IP+域名(FQDN)验证访问通过一个动态IP地址和一个注册的域是可能的。如果选择此选项，请输入注册的域的名字在域名字段。

•动态IP+电子邮件地址。(用户FQDN)对隧道的验证访问通过一个动态IP地址和电子邮件地址是可能的。如果选择此选项，请输入电子邮件地址在电子邮件地址字段。
Note:如果两路由器有动态IP地址不选择两个网关的动态IP+电子邮件地址。

Note:在远程组建立地区的以下更改更改，当与与认证的IKE一起使用。



远程安全网关类型下拉列表变得uneditable并且显示IP+认证。这是能使用隧道的LAN资源。

Step 2.如果认识远程路由器的IP地址请直接地在远程安全网关类型字段之下选择在下拉列表的IP地址并且输入地址。由被解决的DNS选择IP是否在IP不认识IP地址，然而认识域名并且输入远程路由器的域名由DNS被解决的字段

步骤3.从远程认证下拉列表选择认证。证书在VPN连接提供强力身份验证安全。

第4.步(可选)点击**导入远程认证**按钮导入新证书。

第5.步(可选)点击**核准CSR**按钮识别与一个数字式的署名请求的认证。

第6.步。从本地安全组请键入下拉列表选择下列之一：

•IP地址—此选项让您指定能使用此VPN隧道的一个设备。您只需要在IP Address字段输入设备的IP地址。

•子网—选择此选项允许属于相同子网使用VPN隧道的所有设备。您在子网掩码字段需要输入网络IP地址在IP Address字段和其各自子网掩码。

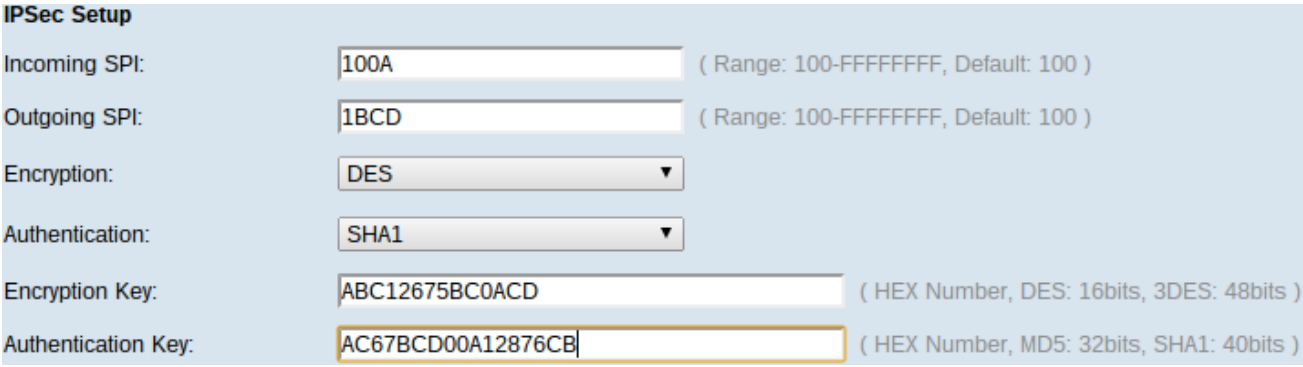
•IP范围—选择此选项指定能使用VPN隧道设备的范围。您需要输入第一个IP地址和设备的范围的最后IP地址。在开始IP字段和末端IP字段。

IPSec设置

对于加密适当地设置在VPN隧道之间的二末端他们必须两个有确切同样设置。IPSec在这种情况下创建在两个设备之间的一个安全的认证。它在两个阶段内如此执行。

IPSec为手工的密钥模式设置

仅可用，如果Manual从从第3步的密钥模式下拉列表被挑选Add新通道。这是生成一个新的安全密钥的一个自定义安全模式单独和对以键的不是协商。使用在排除故障和小的静态环境期间，是最佳的。



步骤1.输入流入安全参数索引(SPI)的唯一十六进制值在流入SPI字段。SPI是一起确定流入信息包的保护的输入的封装安全有效载荷(ESP)协议报头。您能从100进入到FFFFFFFF。

步骤2.输入SPI的唯一十六进制值在流出的SPI字段。SPI是一起确定流出的信息包的保护的输入的ESP报头。您能从100进入到FFFFFFFF。

Note:流入和流出的SPI应该互相匹配在两端为了设立隧道。

步骤3.从加密下拉列表选择适当的加密方法。推荐的加密是3DES。VPN隧道需要使用同一个加密方法两个其末端。

•DES — DES (数据加密标准)是老56位，更加向后兼容，不那么的加密方法安全，虽然中断容易的。

•3DES — 3DES (三重数据加密标准)是168位，增加密钥大小的简单的加密方法通过加密提供更多安全然后DES的数据为三次。

步骤4.从认证下拉列表选择适当的认证方法。推荐的认证是SHA1。VPN隧道需要使用同一个

认证方法两个其末端。

•MD5 — MD5 (提供防护给数据免受恶意攻击由校验和计算的消息摘要Algorithm-5)represents 32位十六进制散列函数。

•SHA1 — SHA1 (安全散列算法版本1)是比MD5安全的160-bit散列函数。

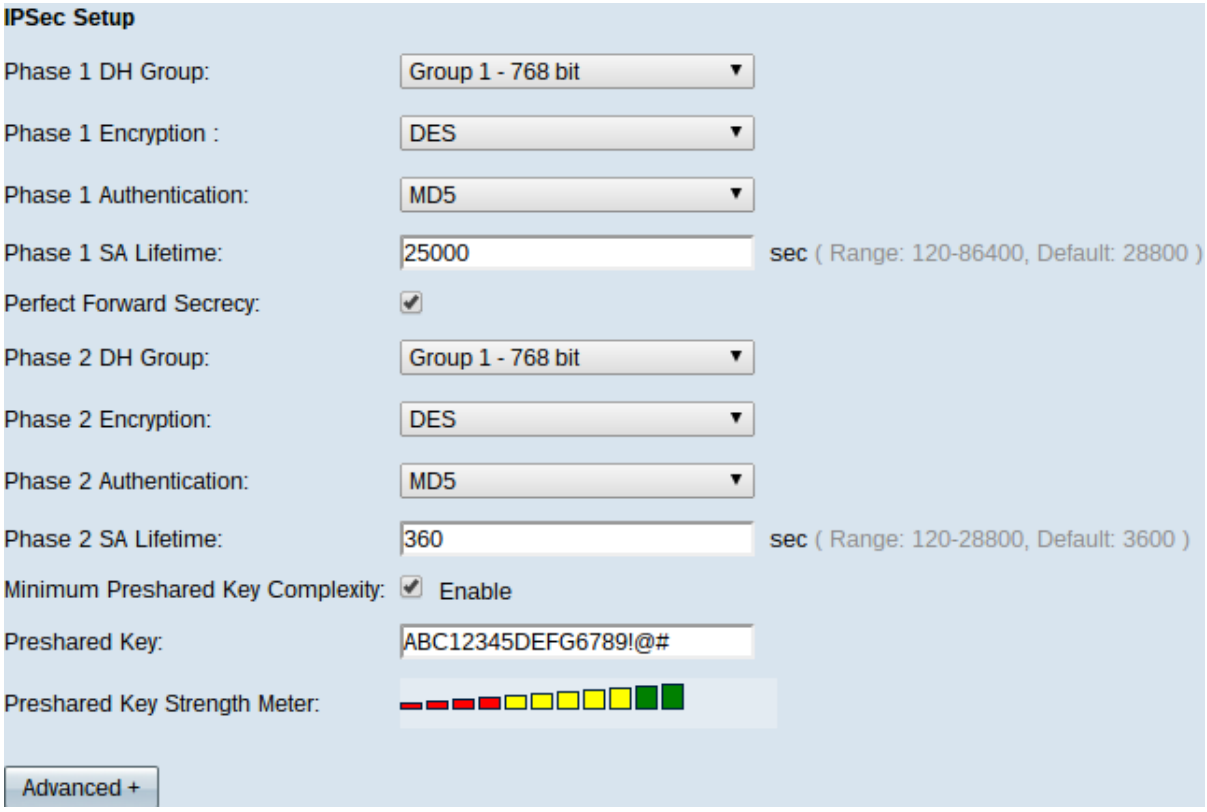
步骤5.输入键加密和解码在加密密钥领域的数据。如果选择DES作为在第3步的加密方法，请输入一个16个位十六进制值。如果选择3DES作为在第3步的加密方法，请输入一个40个位十六进制值。

步骤6.输入预共享密钥验证在认证密钥领域的数据流。如果选择MD5作为在第4步的认证方法，请输入一个32个位十六进制值。如果选择SHA作为在第4步的认证方法，请输入一个40个位十六进制值。VPN隧道需要使用同一个预共用的键两个其末端。

步骤7.点击**"Save"**保存设置。

IPSec为IKE设置用预共用的键

仅可用，如果IKE用预共用的键从从第3步的密钥模式下拉列表被挑选Add新通道。



步骤1.从阶段1 DH组下拉列表选择适当的阶段1 DH组。阶段1用于设立在隧道之间的二末端的单工，逻辑安全关联(SA)支持安全验证通信。Diffie-Hellman (DH)是在阶段1连接时用于共享密钥验证通信的密码学密钥交换协议。

•Group1 - 768位—表示最高强度的键和最安全的认证组。它需要更多时刻计算IKE键。更喜欢网络的速度是否高。

•第2组-第1024组位—表示更加高强度的键和更加安全的认证组。它需要一些时间计算IKE键。

•Group5 - 1536位—表示最低的力量键和最不安全的认证组。它需要较少时刻计算IKE键。更喜欢网络的速度是否是低的。

步骤2.选择适当的阶段1加密加密从阶段1加密下拉列表的键。AES-128、AES-192或者AES-256是推荐的。VPN隧道需要使用同一个加密方法两个其末端。

•DES —数据加密标准(DES)是56位，不是非常在今天世界的安全的加密方法的老加密方法。

•3DES —三重数据加密标准(3DES)是168-bit，增加密钥大小的简单的加密方法通过加密比DES提供更多安全的数据为三次。

•AES-128 —高级加密标准(AES)是128-bit变换纯文本成密码文本through10循环重复的加密方法。

•AES-192 —是192-bit变换纯文本成密码文本通过12循环重复的加密方法。

•AES-256 —是变换纯文本成密码文本通过14循环重复的256-bit加密方法。

步骤3.从阶段1认证下拉列表选择适当的认证方法。VPN隧道需要使用同一个认证方法两个其末端。SHA1是推荐的。

•MD5 —提供防护给数据免受恶意攻击由校验和计算的消息摘要Algorithm-5 (MD5)表示32个位十六进制散列函数。

•SHA1 —比MD5安全的160-bit散列函数。

步骤4.以秒钟输入时间VPN隧道在SA阶段1生活时间字段保持活动。

第 5 步：检查优秀的转发保密性复选框提供更多防护给键。如果任何键减弱，此选项准许生成新密钥。加密的数据通过减弱的键只减弱。因此它提供更加安全并且验证通信，当获取其他键键虽则减弱。这是推荐的行为作为它提供更多安全。

步骤6.从第2阶段DH组下拉列表选择适当的第2阶段DH组。阶段1用于设立在隧道之间的二末端的单工，逻辑安全关联(SA)支持安全验证通信。DH是在阶段1连接时用于共享密钥验证通信的一个加密密钥交换协议。

•Group1 - 768位—表示最高强度的键和最安全的认证组。它需要更多时刻计算IKE键。更喜欢网络的速度是否高。

•第2组-第1024组位—表示更加高强度的键和更加安全的认证组。 它需要一些时间计算IKE键。

•Group5 - 1536位—表示最低的力量键和最不安全的认证组。它需要较少时刻计算IKE键。更喜欢网络的速度是否是低的。

Note:因为任何新密钥没有生成，您不需要配置第2阶段DH组，如果不选定在第5.步的优秀的转发保密性。

步骤7.选择适当的第2阶段加密加密从第2阶段加密下拉列表的键。AES-128、AES-192或者AES-256是推荐的。VPN隧道需要使用同一个加密方法两个其末端。

•DES — DES是56位，不是非常在今天世界的安全的加密方法的老加密方法。

•3DES — 3DES是168-bit，增加密钥大小的简单的加密方法通过加密比DES提供更多安全的数据为三次。

•AES-128 — AES是128-bit变换纯文本成密码文本through10循环重复的加密方法。

•AES-192 —是192-bit变换纯文本成密码文本通过12循环重复的加密方法。

•AES-256 —是变换纯文本成密码文本通过14循环重复的256-bit加密方法。

步骤8.从第2阶段认证下拉列表选择适当的认证方法。VPN隧道需要使用同一个认证方法两个其末端。

•MD5 — MD5表示32个提供防护给数据免受恶意攻击由校验和计算的位十六进制散列函数。

•SHA1 —安全散列算法版本1 (SHA1)是比MD5安全的160位散列数据功能。

•零位—没有使用认证方法。

步骤9.以秒钟输入时间VPN隧道在SA第2阶段生活时间字段保持活动。

第10.步。如果希望到enable (event)预共用的键的，力量公尺请检查最低的预共用的关键复杂性复选框。

步骤11.输入以前被共享在预共用的关键字段的IKE对等体之间的键。30十六进制和字符可以使用作为一个预共用的键。VPN隧道需要使用同一个预共用的键两个其末端。

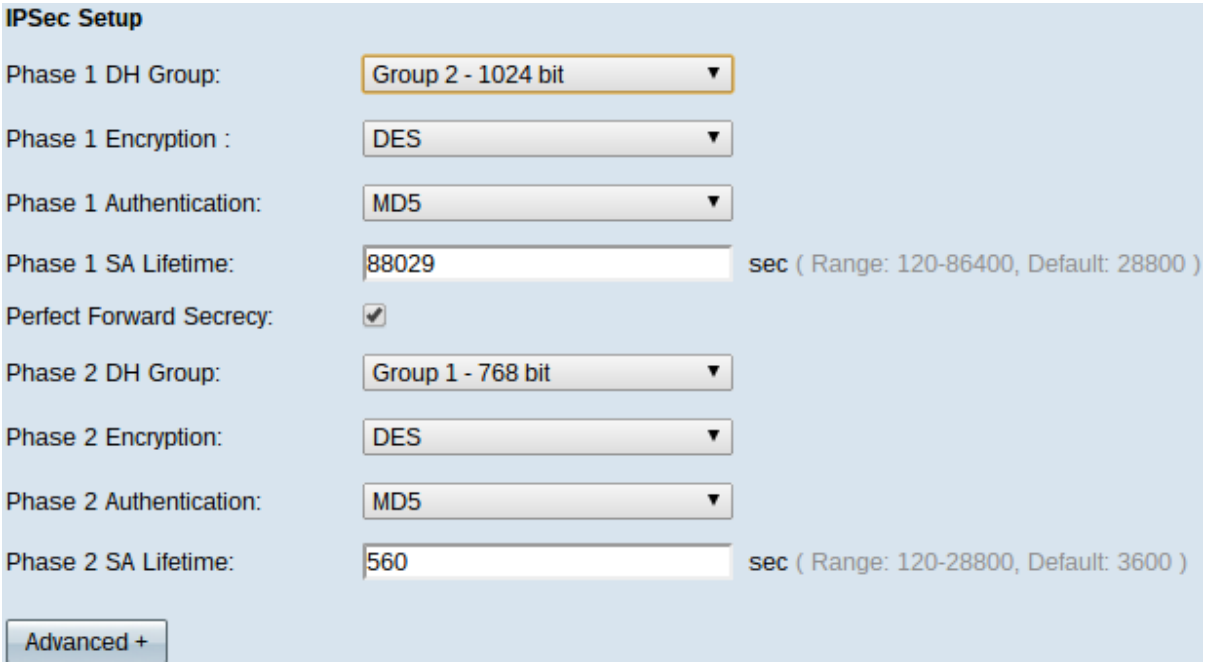
Note:强烈建议频繁地更换在IKE对等体之间的预共用的键，因此VPN保持安全。

预共用的密钥强度公尺通过对有色人种的歧视显示预共用的键的力量。红色指示弱的力量，黄色指示可接受的力量和绿色指示严格的力量。

步骤12。点击**“Save”**保存设置。

IPSec为与认证的IKE设置

仅可用，如果与认证的IKE从从第3步的密钥模式下拉列表被挑选Add新通道。



步骤1.从阶段1 DH组下拉列表选择适当的阶段1 DH组。阶段1用于设立单工，逻辑SA (安全关联)在隧道之间的二末端支持安全验证通信。DH是在阶段1连接时用于共享密钥验证通信的一个加密密钥交换协议。

•Group1 - 768位—表示最高强度的键和最安全的认证组。但是它需要更多时刻计算IKE键。

更喜欢网络的速度是否高。

•第2组-第1024组位—表示更加高强度的键和更加安全的认证组。但是它需要一些时间计算IKE键。

•Group5 - 1536位—表示最低的力量键和最不安全的认证组。它需要较少时刻计算IKE键。更喜欢网络的速度是否是低的。

步骤2.选择适当的阶段1加密加密从阶段1加密下拉列表的键。AES-128、AES-192或者AES-256是推荐的。VPN隧道需要使用同一个加密方法两个其末端。

•DES — DES是56位，不是非常在今天世界的安全的加密方法的老加密方法。

•3DES — 3DES是168-bit，增加密钥大小的简单的加密方法通过加密比DES提供更多安全的数据为三次。

•AES-128 — AES是128-bit变换纯文本成密码文本through10循环重复的加密方法。

•AES-192 —是192-bit变换纯文本成密码文本通过12循环重复的加密方法。

•AES-256 —是变换纯文本成密码文本通过14循环重复的256-bit加密方法。

步骤3.从阶段1认证下拉列表选择适当的认证方法。VPN隧道需要使用同一个认证方法两个其末端。SHA1是推荐的。

•MD5 — MD5表示32个提供防护给数据免受恶意攻击由校验和计算的位十六进制散列函数。

•SHA1 —比MD5安全的160-bit散列函数。

步骤4.以秒钟输入时间VPN隧道在SA阶段1生活时间字段保持活动。

第 5 步：检查优秀的转发保密性复选框提供更多防护给键。如果任何键减弱，此选项准许生成新密钥。加密的数据通过减弱的键只减弱。因此它提供更加安全和验证的通信，当获取其他键，当另一个键减弱时。这是推荐的行为作为它提供更多安全。

步骤6.从第2阶段DH组下拉列表选择适当的第2阶段DH组。阶段1用于设立在隧道之间的二末端的单工，逻辑SA支持安全验证通信。DH是在阶段1连接时用于共享密钥验证通信的一个加密密钥交换协议。

•Group1 - 768位—表示最高强度的键和最安全的认证组。但是它需要更多时刻计算IKE键。更喜欢网络的速度是否高。

•第2组-第1024组位—表示更加高强度的键和更加安全的认证组。但是它需要一些时间计算IKE键。

•Group5 - 1536位—表示最低的力量键和最不安全的认证组。它需要较少时刻计算IKE键。更喜欢网络的速度是否是低的。

Note:因为任何新密钥没有生成，您不需要配置第2阶段DH组，如果不了选定在第5.步的优秀的转发保密性。

步骤7.选择适当的第2阶段加密加密从第2阶段加密下拉列表的键。AES-128、AES-192或者AES-256是推荐的。VPN隧道需要使用同一个加密方法两个其末端。

•DES — DES是56位，不是非常在今天世界的安全的加密方法的老加密方法。

•3DES — 3DES是168-bit，增加密钥大小的简单的加密方法通过加密比DES提供更多安全的数据为三次。

•AES-128 — AES是128-bit变换纯文本成密码文本through10循环重复的加密方法。

•AES-192 —是192-bit变换纯文本成密码文本通过12循环重复的加密方法。

•AES-256 —是变换纯文本成密码文本通过14循环重复的256-bit加密方法。

步骤8.从第2阶段认证下拉列表选择适当的认证方法。VPN隧道需要使用同一个认证方法两个其末端。

•MD5 — MD5表示32个提供防护给数据免受恶意攻击由校验和计算的位十六进制散列函数。

•SHA1 — SHA1是比MD5安全的160位散列数据功能。

•零位—没有使用认证方法。

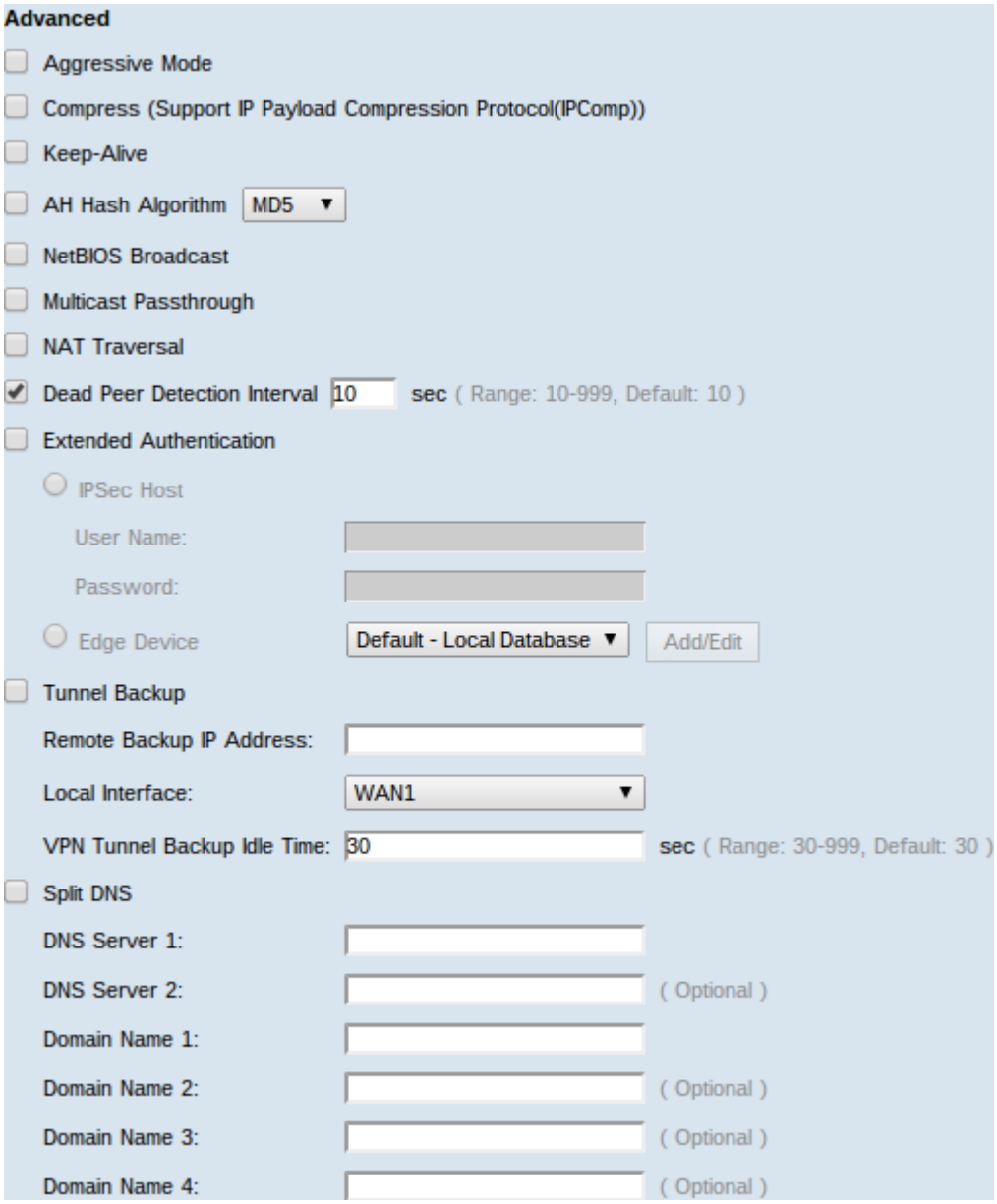
步骤9.以秒钟输入时间VPN隧道在SA第2阶段生活时间字段保持活动。

步骤10.点击**"Save"**保存设置。

(IKE与认证和IKE的可选的) IPSec预先的设置用预共用的键

如果与认证的IKE或IKE用Presahred键从从第3步的密钥模式下拉列表被挑选Add新通道，预先的选项是可用的。同样设置为密钥模式的两个类型是可用的。

步骤1.点击**Advanced+**按钮显示预先的IPSec选项。



Step 2.如果您的网络速度是低的，请检查积极模式复选框。它在SA连接时交换隧道的端点的ID在明文的，需要较少时刻交换，但是巩固。

第 3 步：检查压缩(支持IP有效负载压缩协议(IPComp))复选框，如果要压缩IP数据包的大小。IPComp是用于压缩IP数据包的大小的IP压缩协议，如果网络速度是低的，并且用户要迅速传输数据，不用任何损失通过低速网络。

步骤4.Check keep-alive复选框，如果总是想要VPN隧道的连接保持活动。如果任何连接变得非激活，它帮助立即重建连接。

第 5 步：请检查AH Hash算法复选框，如果想要对认证验证报头(AH)。AH提供认证给数据起始点，数据完整性通过校验和，并且保护是延长的到IP头。隧道应该有两个的同样算法其边。

- MD5 — MD5表示128个提供防护给数据免受恶意攻击由校验和计算的位十六进制散列函数。
- SHA1 — SHA1是比MD5安全的160位散列数据功能。

第6.步。如果要通过VPN隧道，允许不可路由的数据流请检查NetBIOS广播。默认值被不选定。NetBIOS用于通过一些软件应用发现网络资源类似打印机，计算机在网络的等和Windows功能类似网络邻居。

第 7 步：如果您的VPN路由器是在NAT网关后，请检查机箱对enable (event) NAT横越。网络地址转换(NAT) enable (event)用户以公开访问互联网资源的专用LAN地址通过使用一个可路由IP地址作为源地址。然而，对于Inbound数据流， NAT网关没有转换公共IP地址自动方法对在专用LAN的一个特定目的地。此问题防止成功的IPSec交换。NAT横越设置此返程转换。在隧道的两端必须使用同一个设置。

第8.步。检查对端死机检测间隔通过Hello检查VPN隧道或ACK的充满活力以定期方式。如果检查此复选框，请以您希望hello消息的秒钟输入期限或间隔。

第9.步。检查扩展认证使用IPSec主机用户名和密码验证VPN客户端或使用被找到的数据库在用户管理方面。这必须是在两个设备的enable (event)它的能工作。点击**IPSec主机**单选按钮使用IPSec主机和用户名和输入用户名和密码在用户名名称字段和密码字段。或者请点击**边界设备**单选按钮使用数据库。从边界设备下拉列表选择期望数据库。

第10.步。检查隧道备份的复选框对enable (event)隧道备份。当对端死机检测间隔被检查时，此功能是可用的。功能enable (event)重建VPN隧道的设备通过一个代替广域网接口或IP地址。

- 远程备份IP地址—远端对等体的选择IP。输入它或为在此字段的远程网关已经设置的广域网IP。
- 本地接口—用于的广域网接口重建连接。从下拉列表选择所需的接口。
- 如果主要的隧道没有被连接， VPN什么时候建立隧道备份空闲定期选择的时期的使用备份的隧道。以秒钟送进它。

第11.步。检查分割DNS复选框到enable (event)分割DNS。此功能准许发送DNS请求到根据指定的域名的一个被定义的DNS服务器。输入DNS服务器名在DNS Server1和DNS Server2字段并且输入域名在域名#字段。

步骤12。点击**“Save”**完成配置设备。