配置站点到站点VPN请建立隧道在RV系列路由器和ASA 5500系列可适应安全工具之间

目标

安全是重要保护事务的知识产权，虽然同样保证企业连续性和提供能力致以公司工作场所对任何时候需要的员工，对公司资源的任何地方访问。

VPN安全问题解决方案变为重要对中小企业公司。VPN是在一个公共网络结构内被修建的私有网络，例如全球互联网。VPN扩大在地理独立的办公地点之间的一私有网络。因为他们是私有网络的必要组成部分与所有功能的它使主机计算机发送和接收在间公共网络的数据。VPN强化一个分布式组织的安全，进行它容易为了员工能工作从不同的站点，无需减弱网络。使用VPN的动机是需求"虚拟化"组织的通信的某个部分和通信经济。

有不同的VPN拓扑：星型网、点对点和全网状。此聪明的提示包括站点到站点(点对点)VPN，提供基于互联网的基础设施传播网络资源到远程办公室、家庭办公室和业务伙伴站点。使用IP安全协议，站点之间的所有流量加密，并且网络功能例如路由、服务质量(QoS)和组播支持集成。

Cisco RV系列路由器提供稳健和容易地被管理的VPN解决方案对成本意识的小型企业公司。平衡与生产率的安全的Cisco ASA 5500系列自适应安全设备帮助组织。它与全面的下一代网络安全服务结合业界最高的部署的状态检测防火墙，包括：可见性和应用程序粒状控制和简单应用程序、Web安全、入侵防御系统(IPS)，高度安全远程访问和其他。
此短的指南描述设计的示例构件的站点至站点IPSec VPN在RV系列路由器和ASA 5500系列可适应安全工具之间并且提供配置示例。

可适用的设备

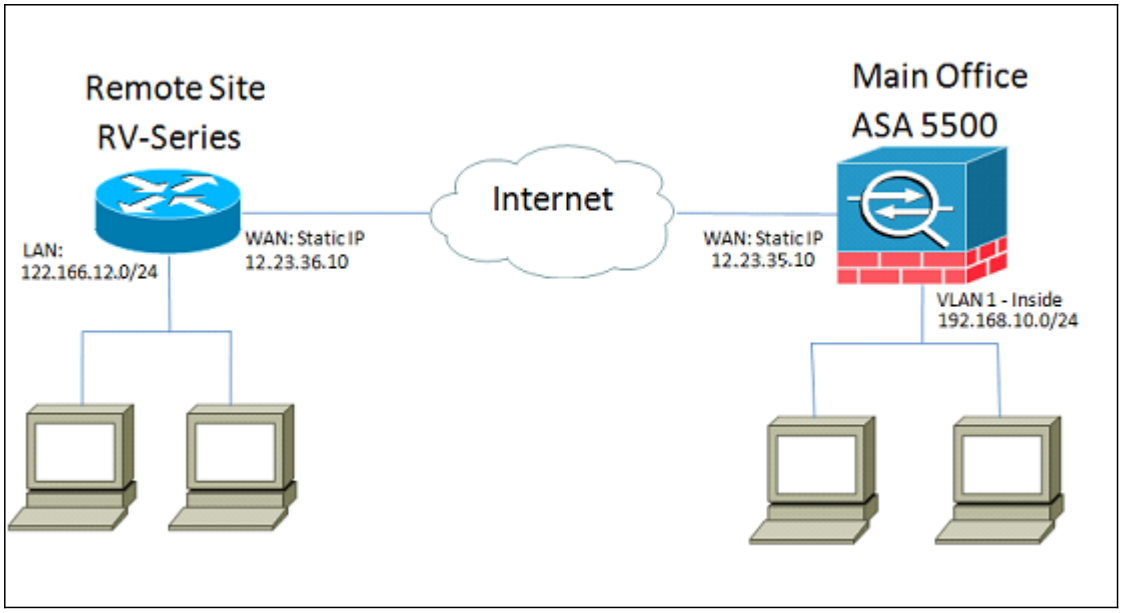
- Cisco RV0xx系列VPN路由器
- Cisco ASA 5500 系列自适应安全设备

软件版本

- 4.2.2.08 [Cisco RV0xx Series VPN Routers]

预配置

使用RV系列路由器(远程站点)和ASA 5500 (总部)，以下镜像显示站点到站点VPN通道的示例实施。



使用此配置在122.166.12.x远程站点网络的一台主机和在VLAN总部能与彼此安全地联络的1at的一台主机。

主要特点

Internet 密钥交换 (IKE)

Internet Key Exchange (IKE)是用于的协议设置安全关联(SA)在IPSec协议套件。在Oakley协议和互联网安全协会和密钥管理协议(ISAKMP)的IKE修造，和使用迪菲–赫尔曼密钥交换设置一共享会话机密，加密密钥派生。必须手工维护每对等体的一个安全策略。

Internet协议安全性(IPSec)

IPsec使用口令安全服务保护在网络协议(IP)网络的通信。IPSec技术支持网络级别对等点身份验证、数据来源验证、数据完整性、数据机密性(加密)和重播保护。IPSec介入许多组件技术和加密方法。 IPSec的操作可以被分解为五个主要步骤：
步骤1."关注数据流"开始IPSec进程-流量视为触发的，当在IPSec对等体配置的IPSec安全策略开始IKE进程时。
步骤2. IKE相位1 -在此相位期间， IKE验证IPSec对等体并且协商IKE SAS，设置协商的IPSec SAS一条安全信道在第2阶段。
步骤3. IKE第2阶段- IKE协商SA IPSec参数并且设置匹配在对等体的IPSec SAS。
步骤4.数据传输-数据转接在根据IPSec参数的在SA数据库存储的IPSec对等体和密钥之间。
步骤5. IPSec隧道终端- IPSec SAS终止通过删除或由定时。

ISAKMP

互联网安全协会和密钥管理协议(ISAKMP)用于协商在两个终端之间的通道。 定义了验证、通信和密钥生成的步骤和IKE协议使用它交换加密密钥和建立安全连接。

设计提示

VPN拓扑—使用站点到站点VPN，一个被巩固的IPSec隧道配置在每个站点和其他站点之间。多站点拓扑通常实现，当站点到站点VPN全网状建立隧道(即每个站点有已建隧道到其他站点)。如果通信不是需要的在远程办公室之间，集中星型VPN拓扑用于减少VPN通道数量(即每个站点仅设立一个VPN通道到总部)。

广域网IP寻址和DDNS — VPN通道需要设立在两个公共IP地址之间。如果WAN路由器收到从互联网服务提供商的静态IP地址，直接地使用静态公共IP地址， VPN通道可以实现。然而，多数小型企业使用有效宽带网络服务例如DSL或有线调制解调器，并且收到从他们的ISP的动态IP地址。在这类情况下， DDNS可以用于映射动态IP地址到完全合格的域名(FQDN)。
LAN IP寻址—每个站点专用LAN IP网络地址不应该有交叠。应该总是更改在每个远程站点的默认LAN IP网络地址。
VPN验证—，当设立VPN通道时， IKE协议用于验证VPN对等体。多种IKE验证方法存在，并且预先共享密钥是最方便的方法。Cisco推荐应用一强预先共享密钥。
VPN加密—要保证在VPN传输的数据的机密性，加密算法用于加密IP信息包有效负载。DES,3DES和AES是三普通的加密标准。AES被认为安全的多数，当与DES和3DES比较。Cisco强烈建议应用AES-128位或更高的加密(例如， AES-192和AES-256)。然而，越强要求的加密算法，处理资源。

配置提示

预配置清单

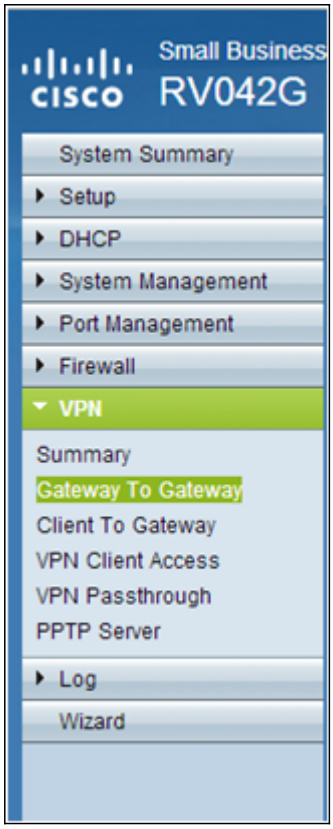
步骤1.确保ASA和RV路由器两个连接到互联网网关(ISP路由器或调制解调器)。
步骤2.启动Cisco RV路由器然后连接内部PCs、服务器和其他IP设备到LAN交换机或RV路由器的交换机端口。
第 3 步：为在ASA后的网络执行同样。步骤4.确保LAN IP网络地址在每个站点配置并且是冷漠子网。在本例中，总部LAN使用远程站点LAN使用122.166.12.0/24的192.168.10.0/24,and。
步骤4.确保本地PC，并且服务器能通信彼此和用路由器。

识别WAN连接

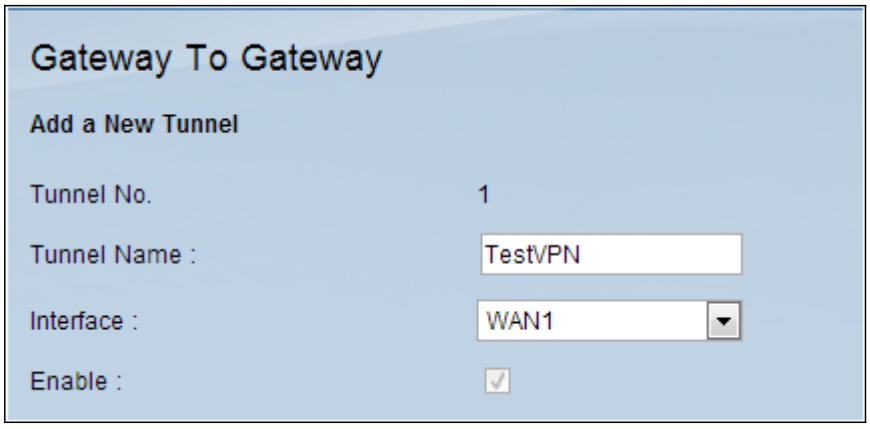
您将需要知道您的ISP是否实施一个动态IP地址或是否接收静态IP。通常ISP将给动态IP，但是您将需要确认此完成配置。

配置RV042G在远程办公室

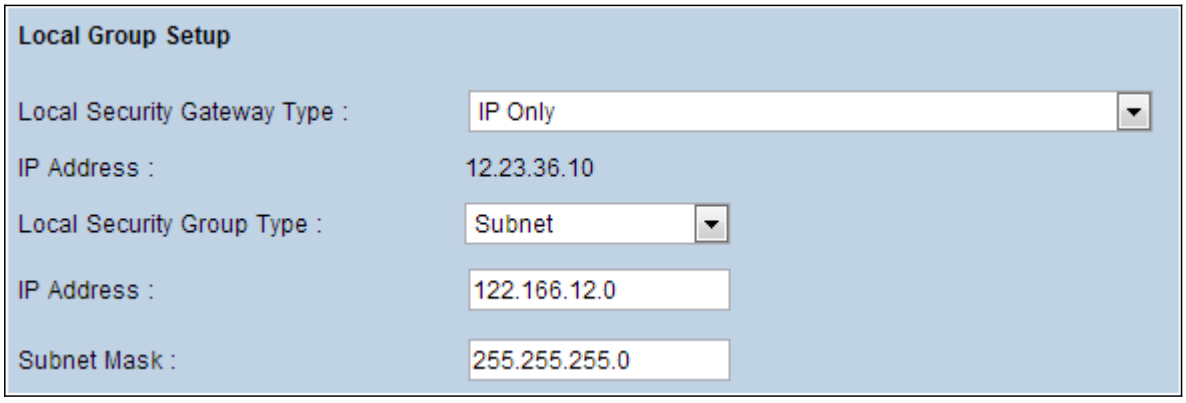
步骤1.登陆对Web UI并且去**VPN >网关到网关的**部分。因为我们添加一LAN-to-LAN连接，终端将是每网络网关。



步骤2.配置本地和远程终点路由器的
a)配置通道名称从您可能已经配置的所有其他通道识别它。

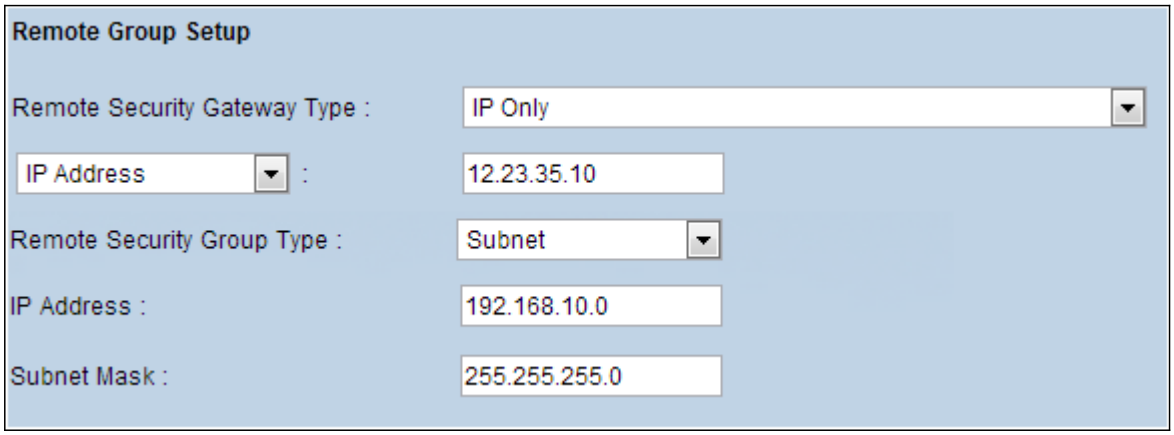


b) 本地组设置配置在VPN通道将允许的本地主机。确保您有正确子网和掩码您要在通道允许的网络的。



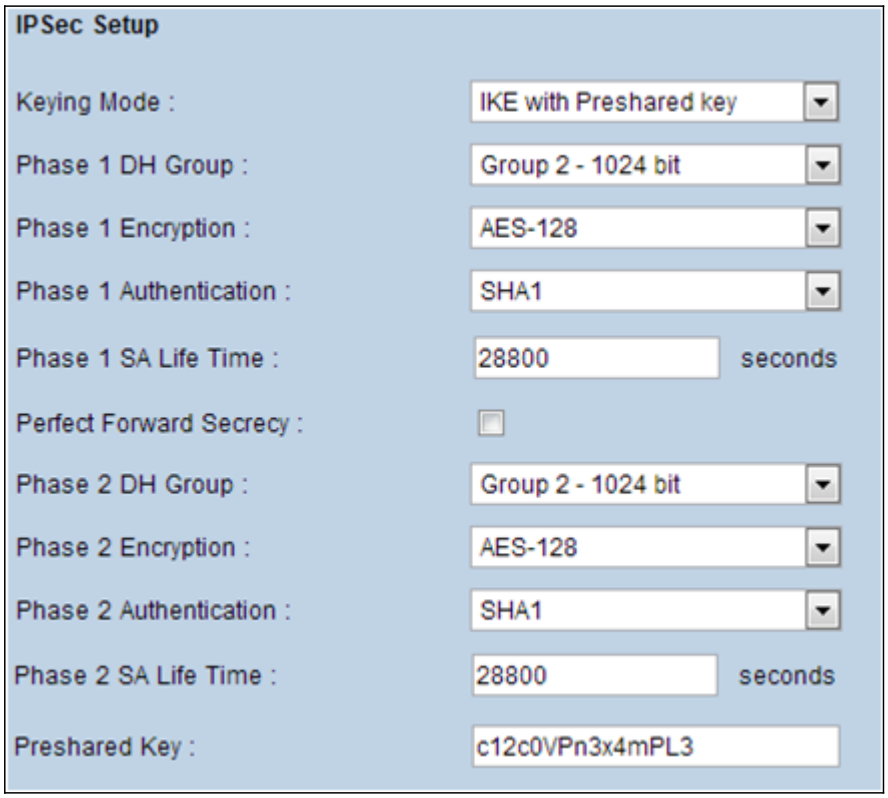
C) 远程组建立配置远程终点和网络流量路由器的能寻找。 进入远程网关的静态IP在网关IP地

址字段建立连接。 然后请输入在从远程站点(总部LAN)的VPN允许的子网。



步骤3.配置隧道设置。
a)您将要配置最佳的结果的一预先共享密钥。
阶段1和第2阶段是不同的相位验证，阶段1创建最初的通道并且开始协商，并且第2阶段确定加密密钥协商并且保护数据传输，一旦通道设立。
b) DH组将对应于ASA的crypto isakmp policy组，您在下一部分将看到。 在ASA默认是第2组，并且ASA代码新版本要求至少DH组2。 折衷是它是一个更高的位和，因此采取更多CPU时间。
c)阶段1加密定义了使用的加密算法。 在RV系列的默认是DES，但是在ASA的默认将是3DES。 然而，这些是更旧的标准并且不是高效在当前实施。 AES加密是安全更加快速等等的，并且Cisco推荐至少AES-128 (或完全AES)最好的结果的。
d)阶段1验证验证信息包完整性。 选项是SHA-1和MD5，并且二者之一应该工作，当他们导致相同的结果。
第2阶段配置遵从规则和阶段1一样。 当配置IPSec设置时，请记住在ASA的设置在RV042G将必须匹配那些。 如果有任何差异，设备不能协商加密密钥，并且连接将发生故障。

Note:确保在导航保存设置远离此页前!



配置ASA 5500在总部(CLI)

Note:确保您使用“write mem”命令经常避免丢失配置。首先，这是我们在ASA配置的接口。 你的也许有所不同，因此请确保相应地修改配置。

```
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.10.1 255.255.255.0
!
interface Vlan10
 nameif outside
 security-level 0
 ip address 12.23.35.10 255.255.255.0
```

步骤1.配置加密管理(ISAKMP)
第一步设置ISAKMP策略，是什么用于协商通道的加密。 此配置应该是相同的在两个终端。 这是您将配置加密设置匹配从RV配置的地方阶段1。

```
ASA5505(config)# crypto isakmp policy 1
ASA5505(config-isakmp-policy)# authentication pre-share
ASA5505(config-isakmp-policy)# encryption aes
ASA5505(config-isakmp-policy)# hash sha
ASA5505(config-isakmp-policy)# group 2
ASA5505(config-isakmp-policy)# lifetime 28800
ASA5505(config-isakmp-policy)# exit
ASA5505(config)#
```

步骤2.流量选择
这是相同的象RV042G的本地和远程安全组。 在ASA我们使用得access-list (s)定义什么网络在VPN视为“关注数据流”承认。
首先，请配置远程站点和本地站点的网络对象：

```
object network insidenet
 subnet 192.168.10.0 255.255.255.0
object network rsite
 subnet 122.166.12.0 255.255.255.0
```

然后请配置access-list使用这些对象：

```
access-list vpn extended permit ip object insidenet object rsite
```

或者，您能使用子网，但是在更加大的实施使用对象和对象组是更加容易的。
步骤3. IPSec隧道配置(第2阶段验证)
此处我们将配置“转换设置的”和隧道组，将设置Phase-2验证。 如果跟Phase-1设置Phase-2不同，您将有一不同的转换集。 此处ESP aes定义了加密和esp-sha-hmac定义了哈希。 隧道群命令配置连接特定的隧道信息，类似预先共享密钥。 请使用远端对等体的公有IP作为组名。

```
ASA5505(config)# crypto ipsec transform-set asarv esp-aes esp-sha-hmac
ASA5505(config)# tunnel-group 12.23.36.10 type ipsec-l2l
ASA5505(config)# tunnel-group 12.23.36.10 ipsec-attributes
ASA5505(config-tunnel-ipsec)# pre-shared-key c12c0VPn3x4mPL3
ASA5505(config-tunnel-ipsec)# exit
ASA5505(config)#
```

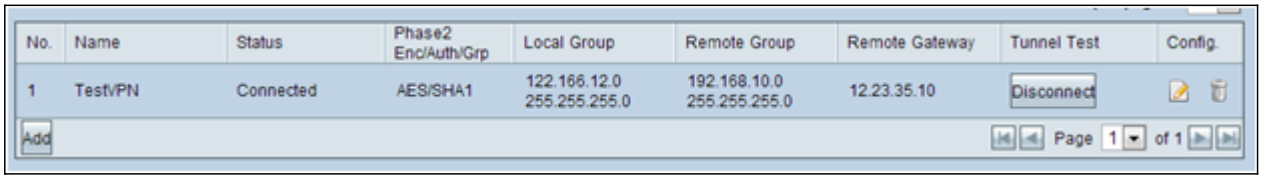
步骤4.加密映射配置
现在我们需要运用Phase-1和Phase-2配置到将允许ASA设立VPN和发送正确流量的“加密映射”。 认为此作为配合VPN的片段。

```
ASA5505(config)# crypto map asarv 1 match address vpn
ASA5505(config)# crypto map asarv 1 set peer 12.23.36.10
ASA5505(config)# crypto map asarv 1 set transform-set asarv
ASA5505(config)# crypto map asarv interface outside
ASA5505(config)#
```

步骤5.验证VPN状态
最后，请检查终端验证VPN连接启用和工作。 连接独自地不会出来，您将需要通过流量，因此ASA能检测它和尝试建立连接。在ASA请使用命令“显示crypto isakmpsa”显示状态。

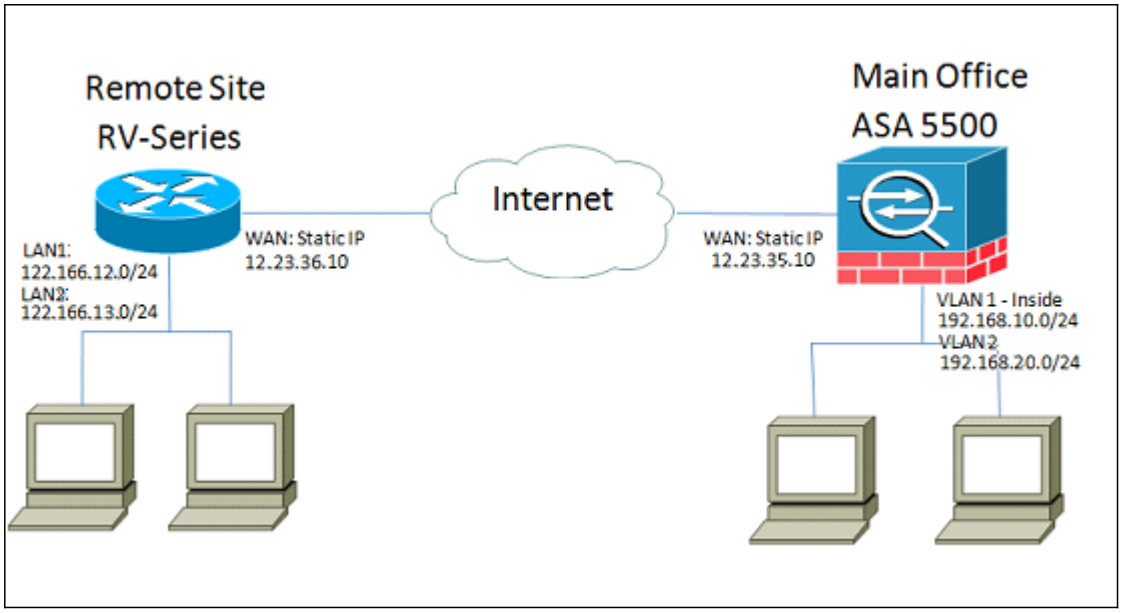
```
ASA5505(config)# show crypto isakmp sa

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 12.23.36.10
    Type    : L2L             Role    : responder
    Rekey   : no              State   : MM_ACTIVE
ASA5505(config)#
```

在RV42G去**VPN >汇总页**并且检查状态。



备选方案：在网络的多个子网

请勿恐慌。这能似乎类似一压倒多数地复杂进程，当您建立网络时，但是您已经完成了上面硬部分。(除非您的子网方案是广泛的)，配置多个子网的VPN要求某更多的配置，但是很少另外的复杂性。我们使用了为此部分使用2的示例在每个站点分支子网。更新网络拓扑是非常类似的：



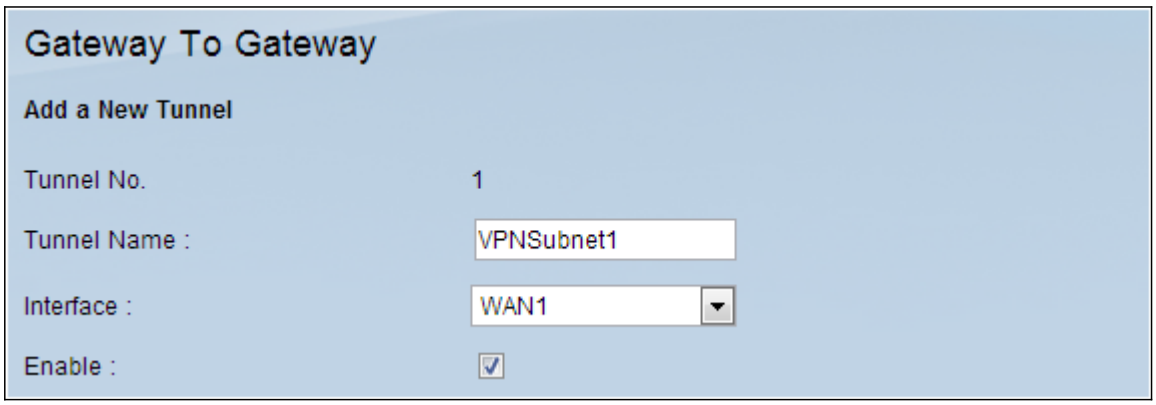
配置RV042G

类似前面，我们首先将配置RV042G。RV042G不能配置在单个通道的多个子网，因此我们将需要添加新的子网的其它条目。此部分只将包括多个子网的VPN配置，没有他们的任何另外的设置配置。

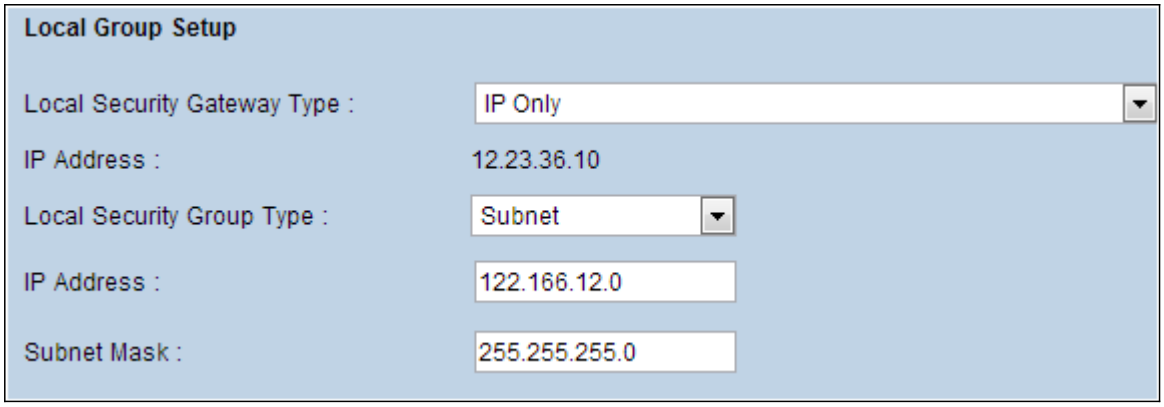
步骤1.配置第一个通道

我们将使用相同的配置每个通道至于单个子网示例的。 和前面，您通过去对**VPN >网关到网关**和添加新通道配置此，或者，如果使用一个现有隧道去**VPN >汇总页，**并且编辑存在的一个。

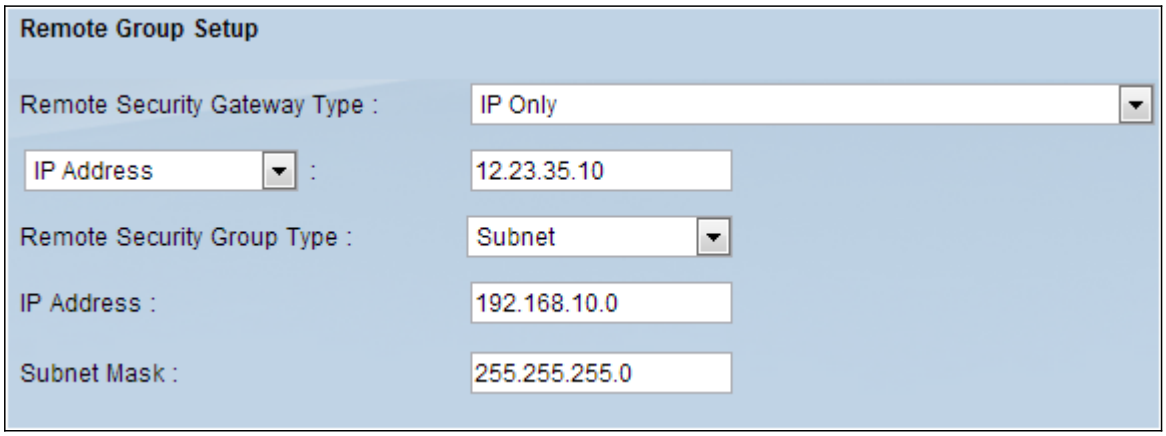
a)，因为我们将有超过一更改是的名称更加说明性的，请配置通道名称，但是更改。



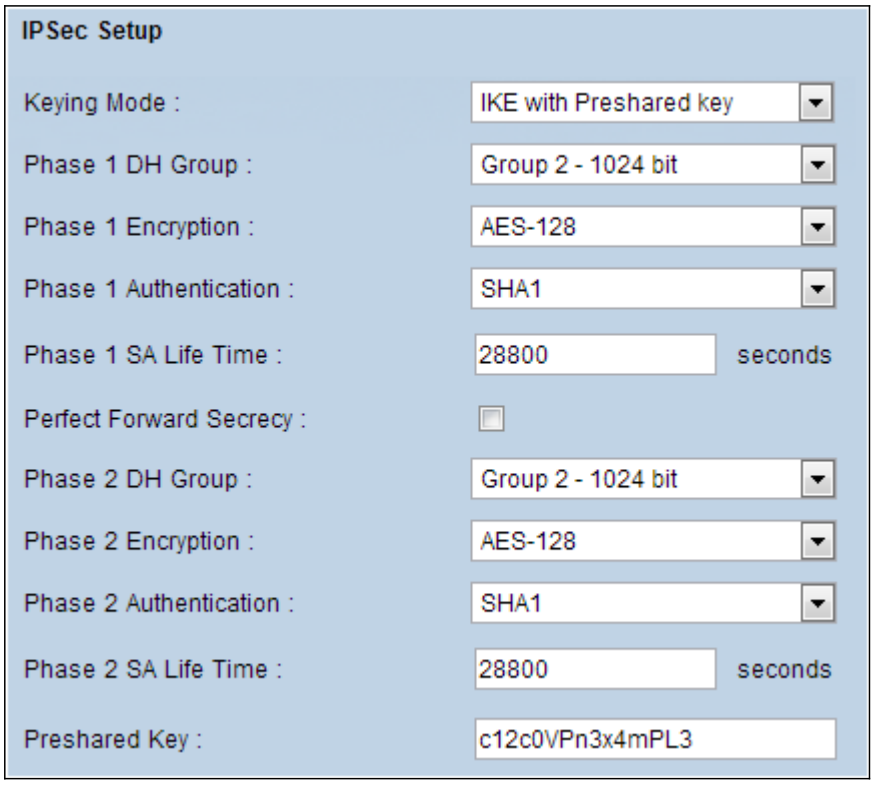
b)其次我们将配置本地组，同以前一样。 为需要访问一子网的只配置此。 我们将有122.166.12.x的一个通道条目和另一个122.166.13.x子网的。



c)现在请配置远程站点，再使用步骤和上述一样。



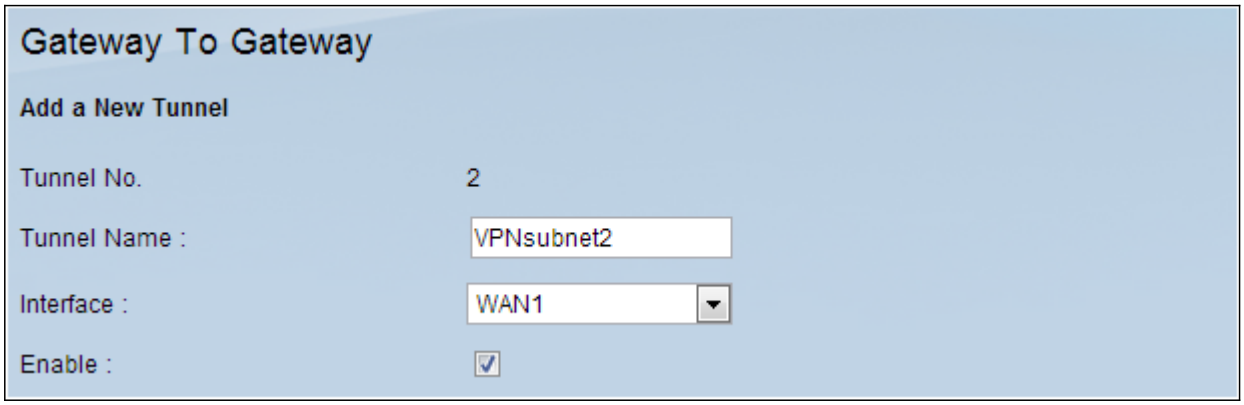
d)最后，请配置加密设置。 请切记这些设置，因为您将希望他们是同样在我们配置的两个通道。



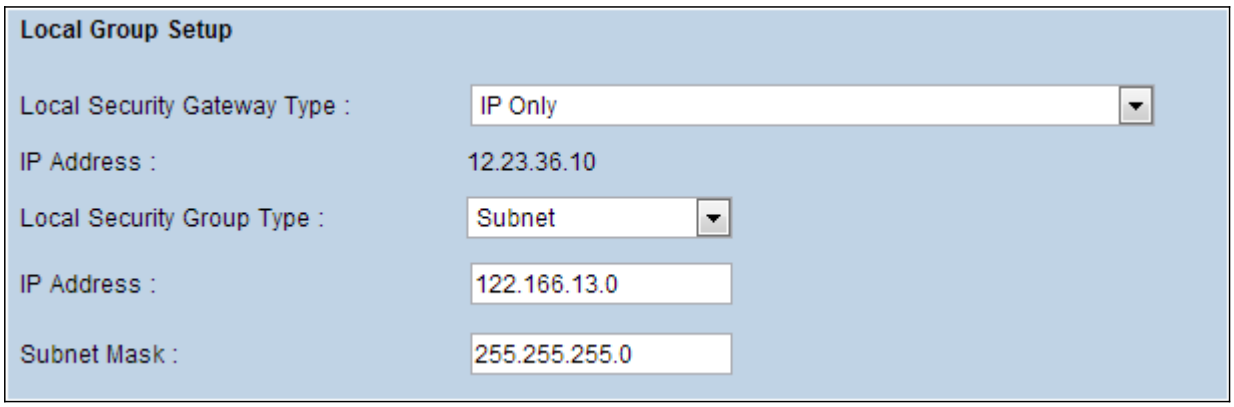
步骤2.配置第二个通道

即然子网1为VPN通道配置，我们需要去对**VPN >网关到网关**和添加第二个通道。 此第二个条目将配置同第一个一样，但是与从每个站点的二级子网。

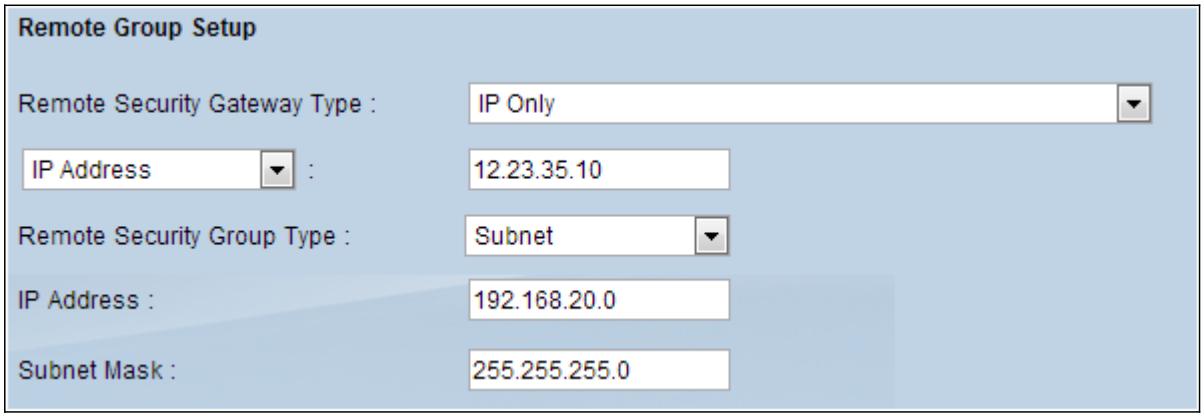
a)确保命名它区分的某事，因此您知道哪连接它是。



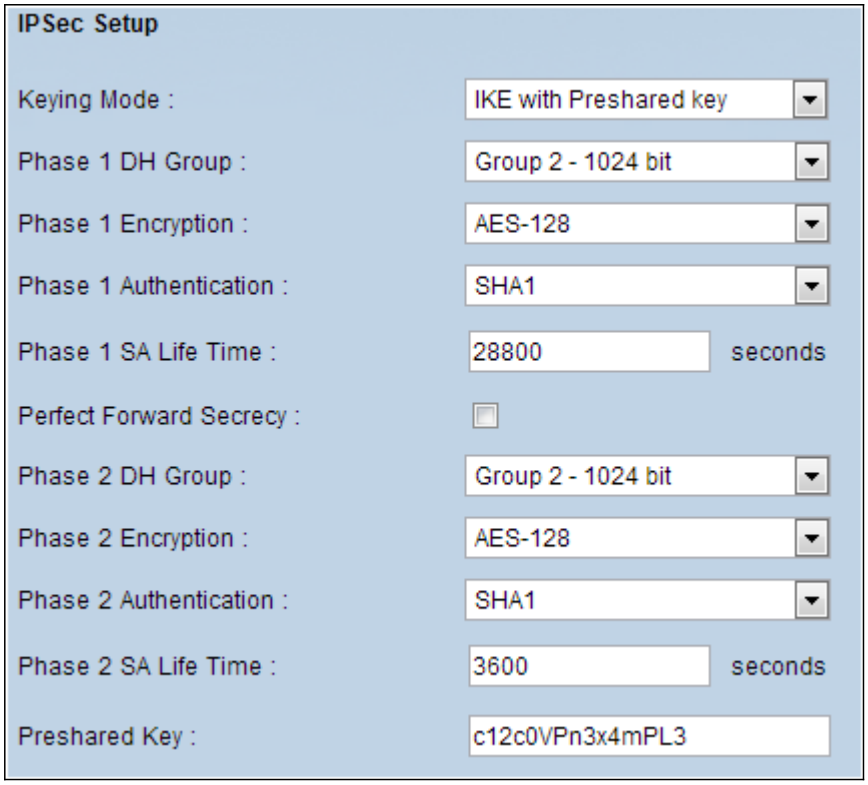
b)请使用第二子网作为“本地安全”组。



C) 并且请使用第二个远程子网作为“远程安全”组。



d)配置阶段1和2的加密同一样第一个通道的。



配置ASA

现在我们将修改在ASA的配置。 此配置难以置信地简单。 您能使用相同的配置如上所述，当使用完会一样的加密设置，与仅次要变化。 我们需要标记另外的流量作为“触发的”防火墙的能发送它在VPN。 因为我们使用access-list为了识别关注数据流，我们需要执行的所有是修改此访问列表。
第 1 步： 要开始时，请删除旧有access-list，因此我们能修改在ASA的对象。 请使用命令的no表删除在CLI的配置。
第二步： 一旦ACL删除，我们希望创建介入的新的子网的新的对象(假设您在设置已经未执行此那些子网)。 我们也要使他们更加说明性。
基于下面我们的VLAN配置：

```
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.10.1 255.255.255.0
!
interface Vlan2
 nameif engineering
 security-level 100
 ip address 192.168.20.1 255.255.255.0
!
interface Vlan10
 nameif outside
 security-level 0
 ip address 12.23.35.10 255.255.255.0
!
```

我们需要主要内部网络(192.168.10.x)和工程网络的(192.168.20.x)一个对象组。 配置网络对象类似如此：

```
ASA5505(config)# show run object
object network ASAvlan1
 subnet 192.168.10.0 255.255.255.0
object network ASAvlan2
 subnet 192.168.20.0 255.255.255.0
object network RVvlan1
 subnet 122.166.12.0 255.255.255.0
object network RVvlan2
 subnet 122.166.13.0 255.255.255.0
```

步骤3.即然相关网络对象配置，我们能配置access-list标记适当的流量。 您要确保您有两网络的一个访问列表条目在ASA后到两个远程子网。 最终结果如下所示:。

```
ASA5505(config)# show run access-list
access-list vpn extended permit ip object ASAvlan1 object RVvlan1
access-list vpn extended permit ip object ASAvlan1 object RVvlan2
access-list vpn extended permit ip object ASAvlan2 object RVvlan1
access-list vpn extended permit ip object ASAvlan2 object RVvlan2
```

第 4 步： 现在，因为我们删除旧有access-list，我们需要重新应用它到加密映射使用命令和以前一样：

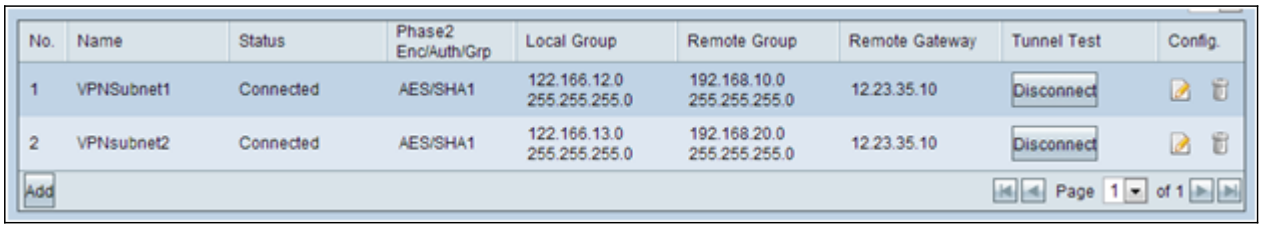
```
ASA5505(config)# crypto map asarv 1 match address vpn
```

验证连接

并且好了!您的通道应该当前是可操作的。首次连接并且检查状态使用“显示crypto isakmpsa” on命令ASA。

```
ASA5505(config)# show crypto isakmp sa

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 12.23.36.10
    Type    : L2L             Role    : responder
    Rekey   : no              State   : MM_ACTIVE
ASA5505(config)#
```

在RV系列状态在将显示VPN >汇总页。



No.	Name	Status	Phase2 Enc/Auth/Grp	Local Group	Remote Group	Remote Gateway	Tunnel Test	Config.
1	VPNSubnet1	Connected	AES/SHA1	122.166.12.0 255.255.255.0	192.168.10.0 255.255.255.0	12.23.35.10	Disconnect	
2	VPNsubnet2	Connected	AES/SHA1	122.166.13.0 255.255.255.0	192.168.20.0 255.255.255.0	12.23.35.10	Disconnect	

Add Page 1 of 1

查看与此条款涉及的视频...

[点击此处查看从Cisco的其他技术谈话]