

# 站点IKEv2 VPN通道的动态站点在两ASA配置示例之间

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[网络图](#)

[配置](#)

[解决方案1 -使用DefaultL2LGroup](#)

[静态ASA配置](#)

[动态ASA](#)

[解决方案2 -创建一用户定义的隧道群](#)

[静态ASA配置](#)

[动态ASA配置](#)

[验证](#)

[在静态ASA](#)

[在动态ASA](#)

[故障排除](#)

## 简介

本文描述如何配置在两可适应安全工具(ASA)之间的一个站点到站点互联网密钥交换版本2 (IKEv2) VPN通道一个ASA有一个动态IP地址的地方，并且其他有一个静态IP地址。

## [先决条件](#)

### [要求](#)

本文档没有任何特定的要求。

### [使用的组件](#)

本文档中的信息基于以下软件和硬件版本：

- ASA版本5505

- ASA版本9.1(5)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

## 背景信息

有两种方式此配置可以设置：

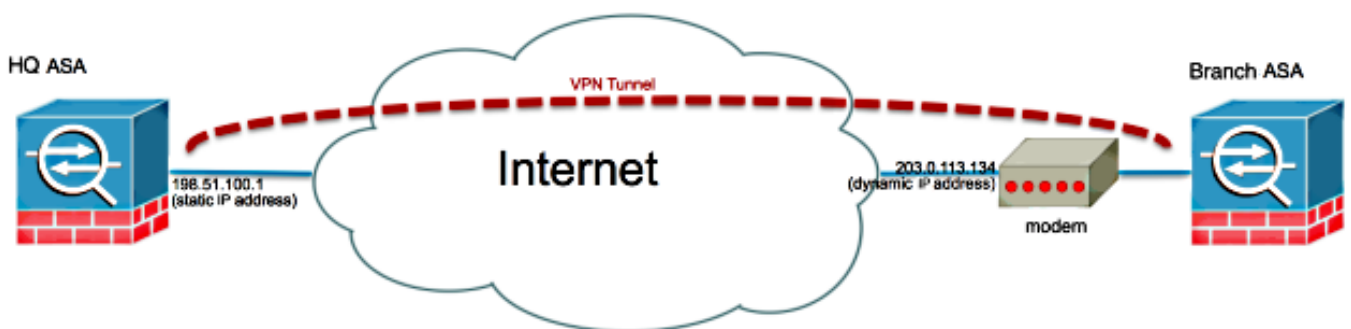
- 使用DefaultL2LGroup隧道组
- 使用一个已命名隧道组

两个方案之间的最大的配置差别是远程ASA使用的互联网安全协会和密钥管理协议(ISAKMP) ID。当DefaultL2LGroup在静态ASA时使用，对等体的ISAKMP ID必须是地址。然而，如果使用一个已命名隧道组使用此命令，对等体的ISAKMP ID必须是相同的隧道组组名：

```
crypto isakmp identity key-id <tunnel-group_name>
```

使用静态ASA的已命名隧道组优点是，当使用时DefaultL2LGroup，在远程动态ASA的配置，包括预先共享密钥，必须是相同的，并且不允许与策略设置的粒度。

## 网络图



## 配置

此部分根据哪解决方案描述在每个ASA的配置您决定使用。

### 解决方案1 -使用DefaultL2LGroup

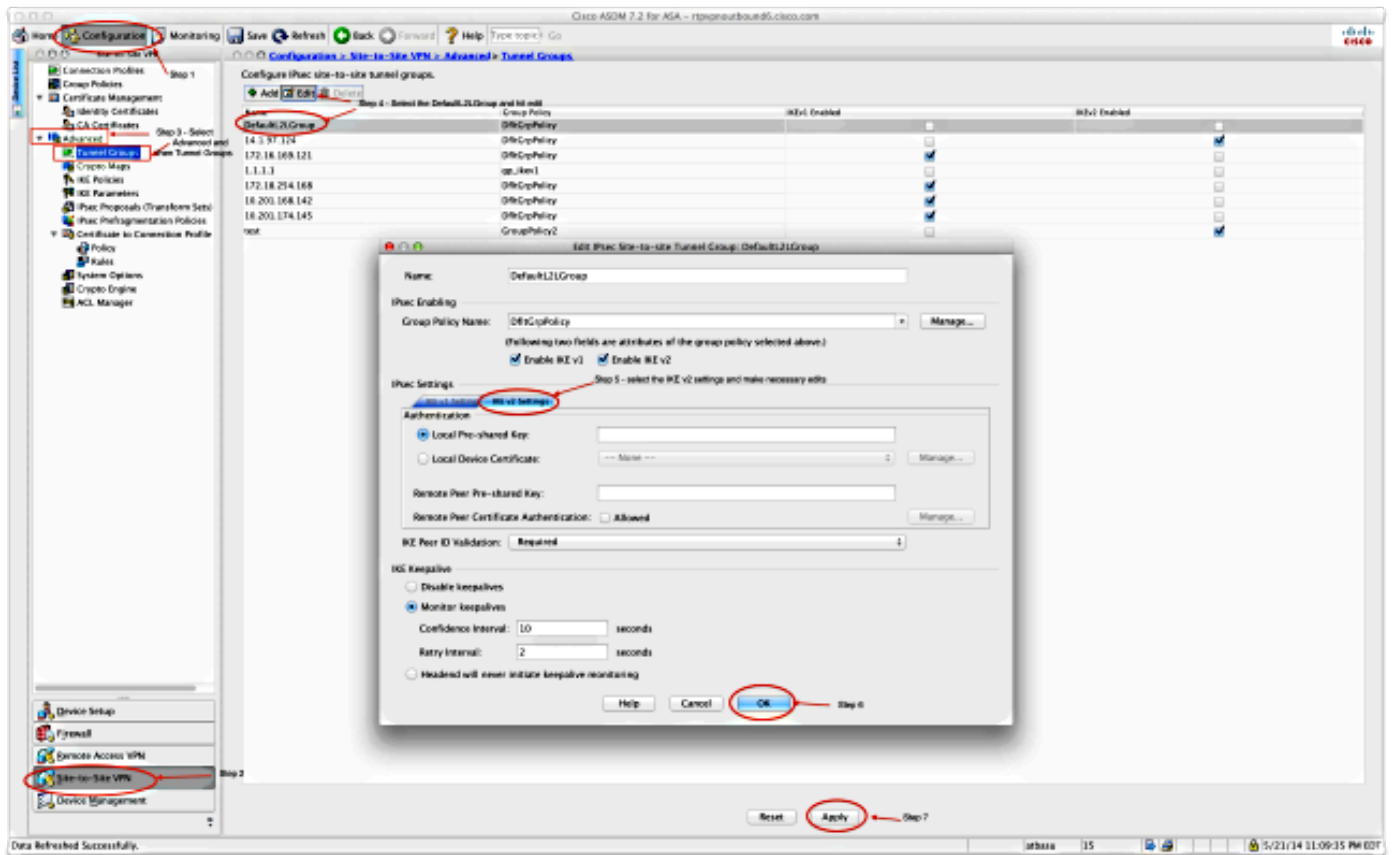
这是简单方法配置在两ASA之间的LAN对LAN (L2L)通道，当一个ASA动态地时得到其地址。DefaultL2L组是ASA的一个预先配置的隧道组，并且不明确地匹配任何特定的隧道组的所有连接在此连接落。因为动态ASA没有常数预先了确定IP地址，它含义admin不能配置Statis ASA为了允许在一个特定隧道组的连接。在这种情况下，DefaultL2L组可以使用为了允许动态连接。

**提示：** 使用此方法，下侧是所有对等体将有同一预先共享密钥，因为仅一预先共享密钥可以每隧道群定义，并且所有对等体将联络对同一DefaultL2LGroup隧道群。

## 静态ASA配置

```
crypto isakmp identity key-id <tunnel-group_name>
```

在可适应安全设备管理器(ASDM)，您能配置DefaultL2LGroup如显示此处：



## 动态ASA

```
crypto isakmp identity key-id <tunnel-group_name>
```

在ASDM，您能使用标准的向导为了设置适当的连接配置文件或您能添加新连接和遵从标准程序。

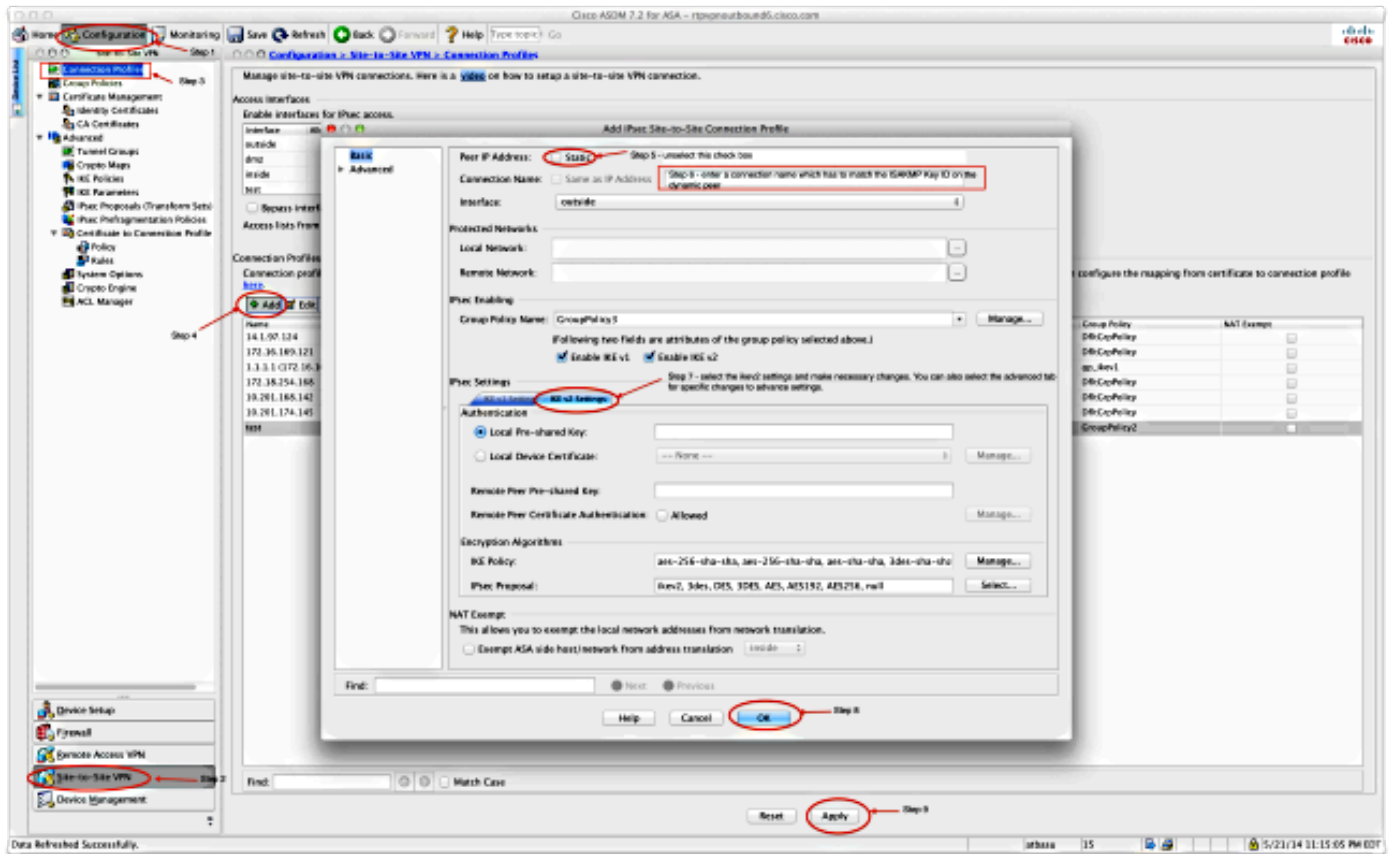
## 解决方案2 -创建用户定义的隧道群

此方法要求slightly更多配置，但是允许更多粒度。每对等体能有其自己的独立的政策和预先共享密钥。在这里更改在动态对等体的ISAKMP ID重要的，以便它使用一名称而不是IP地址。这允许静态ASA匹配流入ISAKMP初始化请求对正确的隧道组和使用正确的策略。

## 静态ASA配置

```
crypto isakmp identity key-id <tunnel-group_name>
```

默认情况下在ASDM，连接配置文件名称是IP地址。因此，当您创建它时，您必须更改它为了给予它名称如屏幕画面所显示此处：



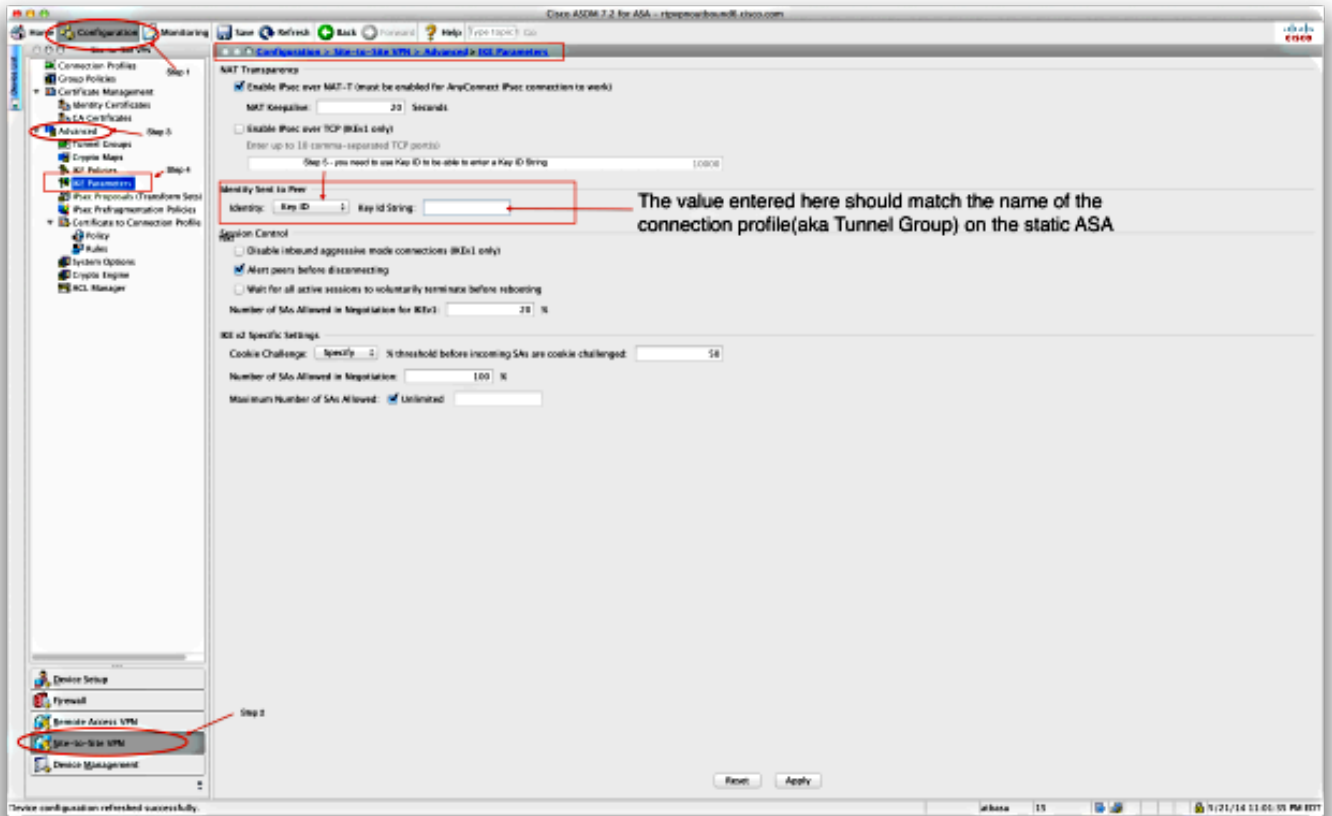
## 动态ASA配置

动态ASA是几乎配置在两解决方案的同一个方式增加一命令如显示此处：

```
crypto isakmp identity key-id DynamicSite2Site1
```

默认情况下如描述以前，ASA使用VPN通道被映射对作为ISAKMP key-id接口的IP地址。在此种情况，在动态ASA的key-id是相同的象隧道群的名称静态ASA的。因此在每动态对等体，key-id不同的，并且一对应的隧道群在与正确的名称的静态ASA必须创建。

如此屏幕画面所显示，在ASDM，这可以配置：



## 验证

使用本部分可确认配置能否正常运行。

## 在静态ASA

这是显示crypto sa IKEv2 det命令的结果：

```
crypto isakmp identity key-id DynamicSite2Site1
```

这是结果show crypto ipsec sa命令：

```
crypto isakmp identity key-id DynamicSite2Site1
```

## 在动态ASA

这是detail命令显示crypto的IKEv2 sa的结果：

```
crypto isakmp identity key-id DynamicSite2Site1
```

这是结果show crypto ipsec sa命令：

```
crypto isakmp identity key-id DynamicSite2Site1
```

[命令输出解释程序工具](#) ( [仅限注册用户](#) ) 支持某些 show 命令。请使用Output Interpreter Tool为了查看show命令输出分析。

## 故障排除

本部分提供了可用于对配置进行故障排除的信息。

[命令输出解释程序工具](#) ( [仅限注册用户](#) ) 支持某些 **show** 命令。请使用Output Interpreter Tool为了查看show命令输出分析。

**注意：**使用 **debug** 命令之前，请参阅[有关 Debug 命令的重要信息](#)。

- deb crypto IKEv2数据包
- 内部的deb crypto IKEv2