Clavister VMware VSG系列

入门指南

Clavister AB
Sj gatan 6J
SE-89160 rnsk ldsvik
SWEDEN

电话：+46-660-299200
传真：+46-660-12250

www.clavister.com

出版方 2011-09-30

Clavister VMware VSG系列
入门指南

出版方 2011-09-30

版权声明

免责声明

本文档中所包含的信息可以不进行通知的情况下进行更改。Clavister对其中的内容不进行保证，并特别地，不承诺对出于任何其它特定目的的使用承担责任。Clavister保留其对此文件的修改权利，而不承担向任何人进行内容更改的通知的义务与责任。

有限责任条款

在任何情况下，Clavister或其供应商都不为任何方面的损失（如利润的损失、软件恢复、工作停止、已存数据的丢失或任何其它商业损坏或损失）负责，无论这些损失是由于应用程序所导致还是对Clavister产品的不正确使用或设备故障所引起，即使Clavister已被通知有这些损坏的可能性。此外，Clavister在任何情况下都不对第三方针对客户的损失或损坏负责。Clavister在任何情况下都不对自最终用户处收到的总量之外的损坏负责。

目录

插图清单

前言

目标读者

本指南的目标读者为那些希望在VMware hypervisor之上运行CorePlus网络操作系统的管理人员。本指南指导用户完成从安装CorePlus到启动该软件，其中还包括网络连接和CorePlus的初始配置。在VMware上的CorePlus的产品名称为Clavister 虚拟安全网关 （VSG）系列。

文本结构

本指南被分为章和节。具有编号的节被显示在本文档开始部分中的目录中。

文本链接

一个“参见某节”链接提供了主文本，可以点击这些链接，以直接把读者引导到链接所指向的参考处。例如 第 3.5 节 “对设置进行排错” 。

Web链接

本文档中所包含的Web链接为可点击的。例如， http://www.clavister.com .

对主文本的注释

需要读者特别注意的文本部分，由页面左侧的图标表示，其后是一小段斜体文字。这是下面此类文本部分的类型：

注意
这个图标提示了一些简短的信息，这些信息是前面文本的附加内容，可以认为一些内容需要被强调或一些内容不明显，或者没有在前面的文本中清楚地陈述。

提示
该图标用于提示一些不太关键的信息，对于理解特定情况是有用的，但不是必读内容。

小心
这个图标表示读者应该留心，并采取必要行动，如果不注意，就有可能出现不良好的结果。

重要
这是必要点，读者应该认真阅读并理解。

警告
对于读者来说这是必要内容，如果采取或没有采取特定的行动就会导致严重问题的出现，读者对此必须提高警惕。

商标

本文档中特定的名称为其各自的所有者的商标。

CorePlus 是 Clavister AB 的商标。

Windows、Windows XP、Windows Vista 和 Windows 7 为Microsoft美国公司和/或其它国家公司的注册商标或商标。

VMware 为VMware, Inc.美国公司和/或其它国家公司的注册商标。

第 1 章 概述

CorePlus与VMware

通过使用VMware产品套件，就有可能在一台单独的计算机上运行多台、虚拟的Clavister安全网关，每台虚拟的Clavister安全网关都运行自己的CorePlus，互不影响。这种技术被称为 虚拟化，并且每台虚拟的Clavister安全网关可以被认为是运行在自己的 虚拟机器 中的一台 VMware主机上。这是Clavister 虚拟安全网关 （VSG）产品系列的基础。

CorePlus不仅可以运行在基于VMware的自己的虚拟机器上，用于管理CorePlus的管理工作站也可以运行于相同的VMware之上。这个工作站可以运行InControl、Web界面或使用安全壳客户端的CLI控制台。

参阅VMware的文档

本指南描述了在VMware
x86硬件上安装CorePlus时所涉及的步骤，以及涵盖了许多运行在VMware虚拟环境中的CorePlus可能遇到的问题。

本向导的目的是处理运行在VMware上的CorePlus的特定问题，并且，如无必要，不详细介绍VMware本身的安装，或者仅与VMware相关的问题。纯粹的VMware问题还是VMware自己解释得最好，要得到这些最全面的文档，请访问http://www.vmware.com。

支持的VMware服务器

CorePlus可以运行在下面的适用于x86硬件的VMware产品上：

- VMware Server（经典服务器）。
- VMware ESXi Server。

CorePlus用于这些服务器的安装文件可以从Clavister网站
下载。这些文件同样也可以从VMware虚拟硬件的网站上进行下载，具体地
https://www.clavister.com址为 http://www.vmware.com/appliances。

第 2 章 CorePlus的安装

如在 第 1 章 概述 中所述，用于VMware的安装文件可以从Clavister Customer Web下载，或者从VMware虚拟硬件的网站上下载。

CorePlus在VMware服务器上的安装

在“经典”服务器和ESX上安装CorePlus的步骤为：

1. 解压缩Clavister分发包。
2. 在VMware中，点击 文件 > 打开 ，再从已解压的包中打开文件 Other.vmx 。
3. 启动虚拟机器。
4. 在你被问到 “你要创建一个唯一的标识符吗”的时候，点击 创建 选项。

CorePlus在ESXi服务器上的安装

在ESXi服务器上安装CorePlus的步骤为：

1. 解压缩Clavister分发包。
2. 在VMware infrastructure客户端上，点击 文件 > 虚拟硬件 > 导入 并从已解压的包中导入 .ovf 文件。
3. 现在，通过适当的设置来完成设置向导的运行。所选择的虚拟接口将与被定义于CorePlus中的缺省接口进行匹配。您可以在以后添加额外的接口，如果许可证允许，这些接口也可以被使用。
4. 4 在向导完成之后，就可以为ESXi虚拟机器加电了。

VMware的控制台

在CorePlus启动的时候，VMware将显示一个控制台，这个控制台和正常情况下，通过RS-232端口连接到物理的Clavister安全网关的控制台是相同的。

这个控制台所显示的CorePlus的输出与非虚拟的Clavister安全网关上所显示的完全相同。它将显示初始的启动序列，而且启动过程可以在需要时通过按键被中断，从而进入到引导菜单。在启动完成之后，VMware控制台可以被用来发布CLI命令，以更进一步地配置CorePlus。

改变焦点到VMwre控制台

如果点击了控制台窗口，VMware将保持焦点在这个窗口上。通过使用 Ctrl-Alt 组合键可以释放焦点。

缺省的虚拟以太网接口

标准的CorePlus安装提供了一个虚拟以太网接口的编号。这个编号类似于E1000 NICs这样的形式，并且可以通过VMware的 桥接 选项来连接到一个物理的以太网接口，或者通过自定义 选项来连接到同一台主机上的另一台虚拟机器上。

CorePlus为虚拟接口分配以下的缺省的名称：

- 接口名称： Ifn。例如，第一个接口的名称为 If1。
- IP地址对象： Ifn_ip。例如，第一个地址对象为 If1_ip。

- 网络掩码IP对象： Ifn_net。例如，第一个网络掩码就是 If1_net。

连接到虚拟的Clavister安全网关

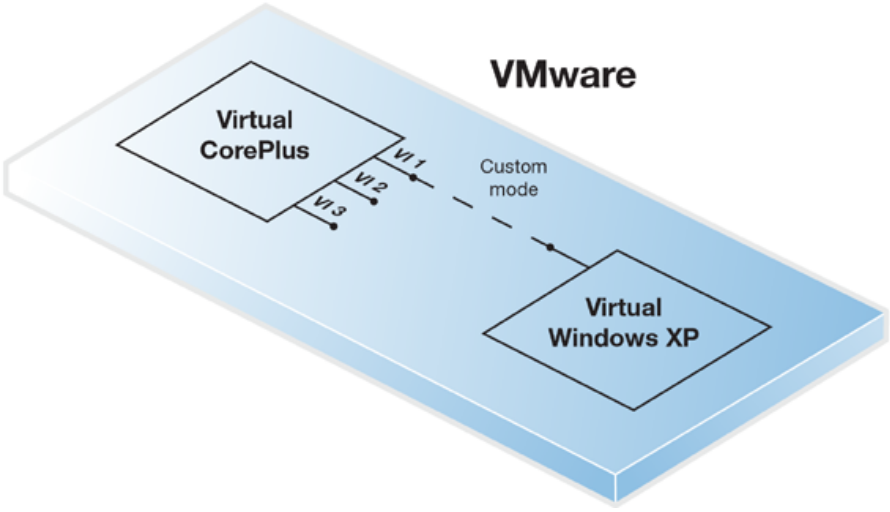
第一个虚拟的以太网接口， If1，将被CorePlus分配一个 192.168.1.1 的IP地址。这是CorePlus缺省的管理接口，并且可以通过一个web浏览器（使用CorePlus的Web界面）来连接这个地址，或者通过SSH客户端（使用CorePlus的CLI）来连接这个地址，就如同在非VMware上一样。

运行web浏览器或SSH客户端的工作站可以为以下一种：

- 运行在同一台VMware主机上的虚拟工作站。

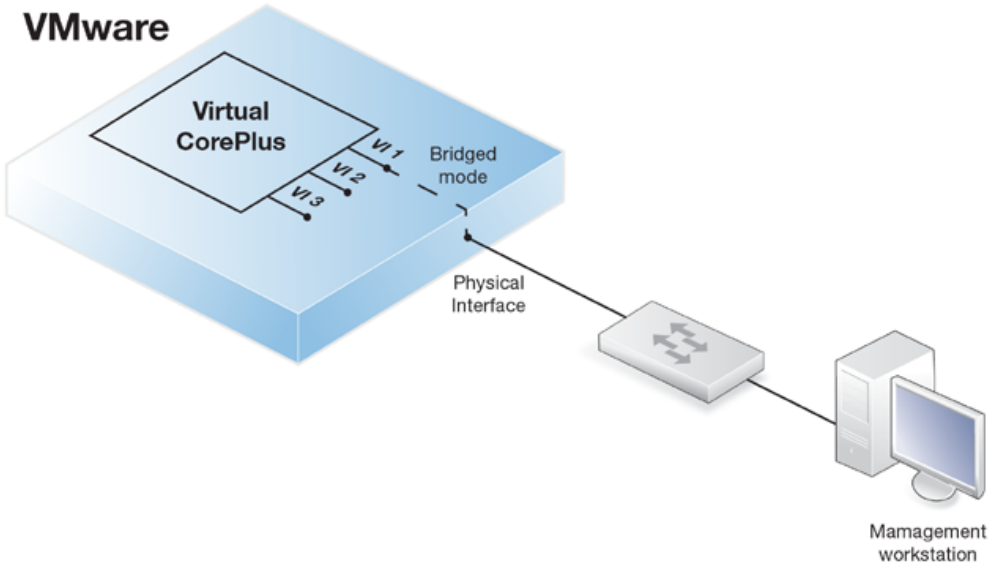
  在这种情况下，VMware的自定义（不是桥接）选项可以被用于连接这个虚拟的以太网接口，通过虚拟工作站上后个虚拟的以太网接口。这台虚拟的工作站可以为，例如，一个Windows XP，如下所示。

  要使该选项生效，VMware必须被配置好，以使CorePlus和工作站上的虚拟以太网接口处于同一个虚拟的网络中。



- 一台物理上互不相干的工作站计算机。

  在这种情况下，VMware的 桥接模式应该被用于连接虚拟以太网接口到物理接口。接下来，就要在物理接口和另一个分离的工作站计算机的物理接口之间建立连接。



在以上的两个例子中，真实的或虚拟的工作站PC需要把自己已建立了连接的以太网接口配置为和CorePlus的接口在同一个网络中的IP地址。一旦完成了配置，管理工作站就可以和Clavister安全网关进行通信了，这时就可以进行初始的CorePlus的设置了，和在非虚拟的安全网关上的操作完全相同。这将在下一章 第 3 章 配置CorePlus 中进行描述。

生成唯一的 设备ID

由Clavister提供的随时都可以运行的VMware虚拟机器总是具有相同的 设备ID，这会在通过InControl管理客户端来管理的时候带来问题。通过CLI命令可以显示当前的ID：

```
Device:/> show Device

        Property  Value                                Remarks
 ----------------  -----------------------------------  ---------
            Name:  Device
   ConfigVersion:  21                                   Read-only
      ConfigUser:  admin                                Read-only
   ConfigSession:  WebUI                                Read-only
        ConfigIP:  192.168.1.2                          Read-only
      ConfigDate:  2009-02-30 15:25:56                  Read-only
        DeviceID:  22b685f1-72e0-4124-b2a9-4c3d82834ae3 Read-only
         HWModel:  SOFTWARE                             Read-only
 RegistrationKey:  <empty>                              Read-only
  ProductionDate:  <empty>                              Read-only
        HWSerial:  <empty>                              Read-only
        Comments:  <empty>
```

要为一台虚拟安全网关生成一个唯一的 设备ID ，就需要进入安全网关的引导菜单，并选择恢复到基本配置 菜单，这将生成一个新的ID。很明显，这样的操作只能在新的安全网关刚被创建的时候就进行，否则其上已有的配置会全部丢失。

多台虚拟的Clavister安全网关的设置

在一台VMware主机上同时有多台虚拟机器在运行CorePlus的时候，用于管理的虚拟以太网接口的IP地址必须是每台设备一个，不能与其它的设备管理用的虚拟接口的IP地址相同，这样才可以实现Web界面管理或者SSH客户端管理。

要改变管理接口的IP地址，推荐的方法是使用CorePlus的控制台，控制台在CorePlus启动后由VMware显示。改变管理接口的IP地址具体的CLI命令如下：

1. 设置缺省的管理接口的IP地址 If1_ip。在这个例子中，它将被设为 10.0.0.1：

```
Device:/> set Address IP4Address If1_ip Address=10.0.0.1
```

2. 接下来，设置此接口的网络地址。该对象的名称为If1_net。

```
Device:/> set Address IP4Address If1_net Address=10.0.0.0/24
```

3. 进行检查。通过如下所示的命令，显示用于HTTP访问的当前的管理规则：

```
Device:/> show RemoteManagement RemoteMgmtHTTP
```

在这些步骤之后，应该发布一个 activate 和一个 commit 命令以部署更改。

相同的步骤也可以在Web界面上进行，但一旦改变被提交，管理员就必须在30秒钟之内登录到CorePlus，否则所做的更改就会被撤销，并且CorePlus将会因滚到前一次的配置。

生成唯一的 设备ID

由Clavister提供的随时都可以运行的VMware虚拟机器总是具有相同的 设备ID，这会在通过InControl管理客户端来管理的时候带来问题。通过CLI命令可以显示当前的ID：

```
Device:/> show Device

        Property  Value                                Remarks
 ----------------  -----------------------------------  ---------
            Name:  Device
   ConfigVersion:  21                                   Read-only
      ConfigUser:  admin                                Read-only
   ConfigSession:  WebUI                                Read-only
        ConfigIP:  192.168.1.2                          Read-only
      ConfigDate:  2009-02-30 15:25:56                  Read-only
        DeviceID:  22b685f1-72e0-4124-b2a9-4c3d82834ae3  Read-only
         HWModel:  SOFTWARE                             Read-only
 RegistrationKey:  <empty>                              Read-only
  ProductionDate:  <empty>                              Read-only
        HWSerial:  <empty>                              Read-only
        Comments:  <empty>
```

要为一台虚拟安全网关生成一个唯一的 设备ID ，就需要进入安全网关的引导菜单，并选择恢复到基本配置
菜单，这将生成一个新的ID。很明显，这样的操作只能在新的安全网关刚被创建的时候就进行，否则其上已有的配置会全部丢失。

第 3 章 配置CorePlus

3.1. 管理工作站的连接

缺省的管理接口

在首次启动之后，CorePlus将扫描可用的以太网接口，并使其找到的第一个接口成为进行管理访问的接口，并为它分配 192.168.1.1 作为它的内部IP地址。

对于VMware的安装来说，这个用于管理的接口就是 If1 。

可选的CorePlus配置方法

CorePlus的初始的软件的配置也可以通过以下几种方法之一来进行：

- 通过web浏览器进行配置。

  一个在一台独立的计算机（也叫 管理工作站）上运行的web浏览器可以被用于访问CorePlus的 Web界面。 这为CorePlus的管理提供了一个直观的图形界面。在首次访问这个界面的时候， 设置向导就会自动运行，以引导新用户完成关键的设置步骤。如果管理人员希望直接通过Web界面来进行手动的设置，这个向导也可以被关闭。

  因为这个向导简化了初始的配置，因此推荐使用这个向导，更多细节在 第 3.2 节 “Web界面和向导设置”中介绍。

- 通过终端控制台使用CLI命令进行配置。

  设置过程也可以通过使用控制台CLI命令来完成，通过控制台CLI命令进行设置的详细内容在 第 3.4 节 中进行描述。CLI允许一步一步地控制设置，并且应该由完全懂得CLI和设置步骤的管 “CLI设置”理人员来实施。

  CLI访问可以为远程、跨越网络到达CorePlus的访问，使用与访问Web界面相似的连接方式。另外，CLI访问还可以直接通过VMware的控制台窗口来实现。

网络连接设置

为了设置以使用Web界面或使用远程的CLI，我们必须首先把一台工作站通过网络连接到CorePlus。工作站的连接在前面的 第 2 章 CorePlus的安装 中已经进行了描述。

使用VMware进行管理的接口为 If1 ，这个接口应该被连接到管理工作站所处的的网络（或者一个通过一台或多台路由器可达的网络）中。典型情况下，这种连接是通过网络中的交换机或hub来建立的，使用常规的直通以太网张线缆。如果要连接到公共互联网，设备的接口之一就应该被连接到您的ISP，这将在下面谈到，即设置向导中的 WAN 接口。

工作站的接口设置

数据流可以在工作上特定的网络接口和Clavister安全网关接口之间流动，因为它们位于相同的IP网络中。这意味着工作站接口必须首先被配置为下面的静态IP地址：

- IP地址：192.168.1.30
- 子网掩码：255.255.255.0
- 缺省网关：192.168.1.1

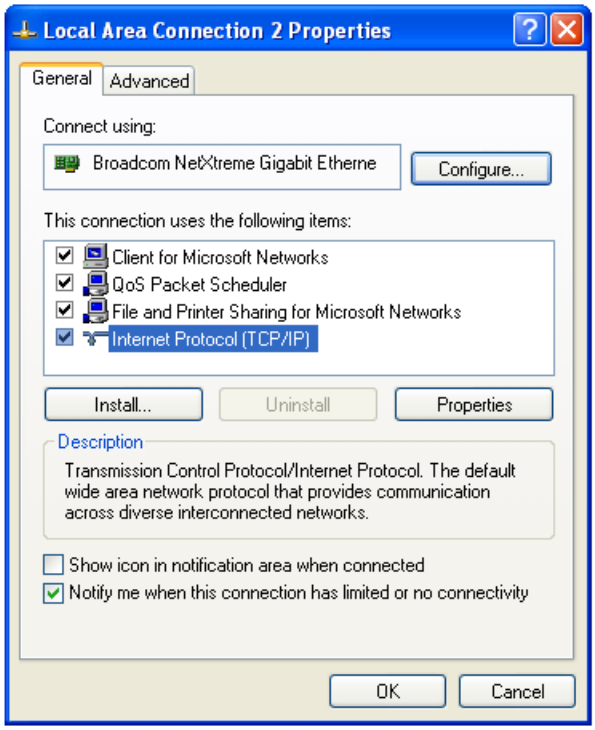
提示

所分配的IP地址 192.168.1.30 可以是 192.168.1.0/24 网络中的另一个地址，但不可以是 192.168.1.1 ，这是被CorePlus使用的地址。

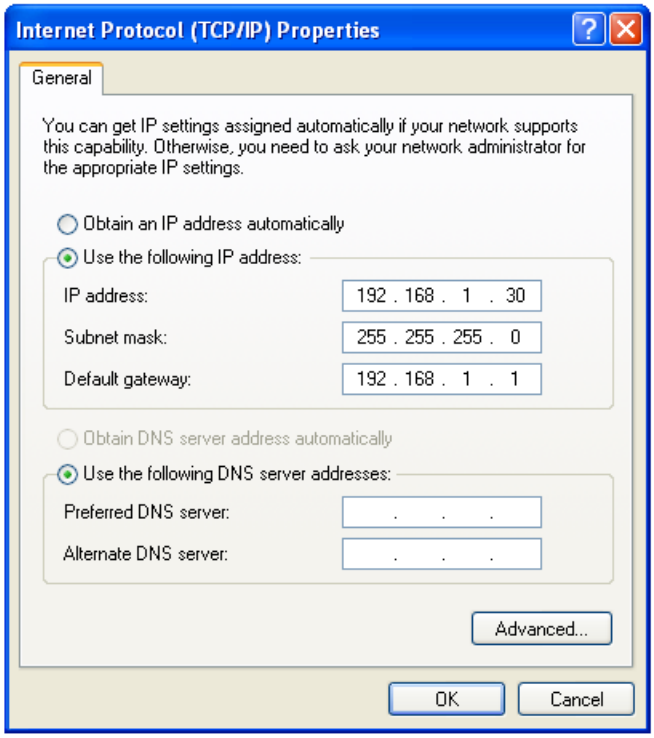
要进入一台运行着Windows XP的PC的设置界面，您需要通过下面的步骤：

- 点击 开始 按钮。
- 右击 网上邻居 并选择 属性 。

- 在所选的以太网接口上右击并选择 属性 。
- 选择 互联网协议（TCP/IP） 并点击 属性 。



- 输入上面所给定的IP地址并点击 确定 按钮。



其它操作系统平台上的IP设置

下面的附录描述了如何为运行其它操作系统平台的工作站设置IP地址：

- 附录 A，Vista的IP设置 .
- 附录 B，Windows 7的IP设置 .
- 附录 C，Apple Mac的IP设置 .

3.2. Web界面和向导设置

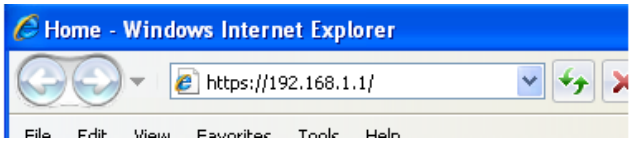
本章描述首次通过一个web浏览器访问CorePlus时的设置。这种用于访问的用户界面被称为Web界面（通常也被称为WebUI）。

注意

本章中的许多屏幕快照都是从原始图像中删除了空白区域的，以增加可读性。然而，这些图片中的信息性的内容还是被保留了下来。

通过浏览 https://192.168.1.1来进行连接

在一个web浏览器的地址栏中，输入 https://192.168.1.1 ，如下所示。



检查代理服务器并关闭弹出窗口阻止。

确保web浏览器没有配置代理服务器。

浏览器里的所有弹出窗口阻止设置都应该被临时关闭，以允许设置向导可以正确运行。

如果CorePlus没有响应，并且原因不清楚，请参阅 第 3.5 节 “对设置进行排错”中的帮助列表。

CorePlus的自签名的证书

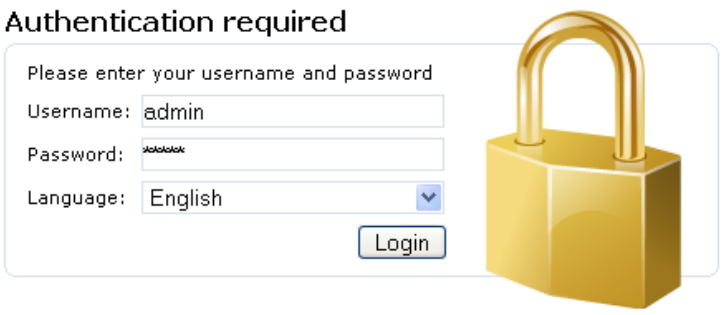
在对一个 https:// 请求进行响应的时候，CorePlus将发送一个自签名的证书，这个证书一开始不会被识别，因此就有必要告诉浏览器要接受这个证书，并在以后的过程中也一直接受它。不同的浏览器处理这个问题的的方法会稍有不同。在Microsoft Internet Explrer中，将会在浏览器窗口中显示下面的错误消息。

要继续，就要告诉IE必须接受这个证书，具体做法是点击如下图所示的出现在浏览器窗口中的按钮附近的链接。

在FireFox中，这个过程被称为 添加一个安全性例外。

登录对话框

接下来，CorePlus将作为一个web服务器来进行响应，并显示初始的登录对话框页面，如下图所示。



Web界面的语言选项是可选的，位于此对话框的底部。如果CorePlus支持浏览器的默认语言设置中的语言集，那么页面的语言就是浏览器的默认语言设置中指定的语言。

登入及设置向导

现在以 admin 和 admin 作为用户名和密码登入。Web界面将显示出来，并且CorePlus的设置向导就会自动运行。首次的向导对话框为欢迎页，如下图所示。

取消向导

在任何时候，设置向导都可以在最后的 激活 页面显示之前被取消。在Web界面工具栏里选择 设置向导 选项又可以再次运行该向导。一旦任何配置更改已发生，并且已经激活，无论是通过设置向导、Web界面还是CLI，设置向导都不会再次被运行，因为CorePlus已经不是出厂状态了。

向导认为Internet访问将会被配置

向导认为Internet访问将被配置。如果不需要配置Internet访问，例如，Clavister CorePlus安全网关被用于 透明模式 ，部署于两个内部网络之间。在这种情况下，最好是通过一般的Web页面来实现，或者通过CLI来完成配置，而不是使用向导。

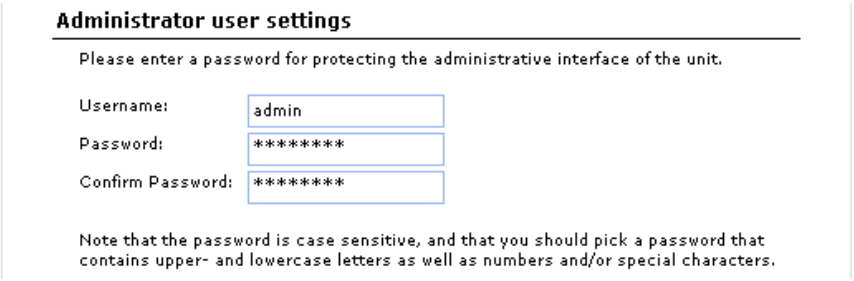
使用向导的优势

向导使得设置过程更为简单，因为它可以自动决定需要配置什么，与此相比，在Web界面中一步步的进行配置显得相对复杂了些。它也能够提醒您执行一些重要的任务，如设置日期和时间以及配置日志服务器。

向导中欢迎页面出现之后的后续步骤如下。

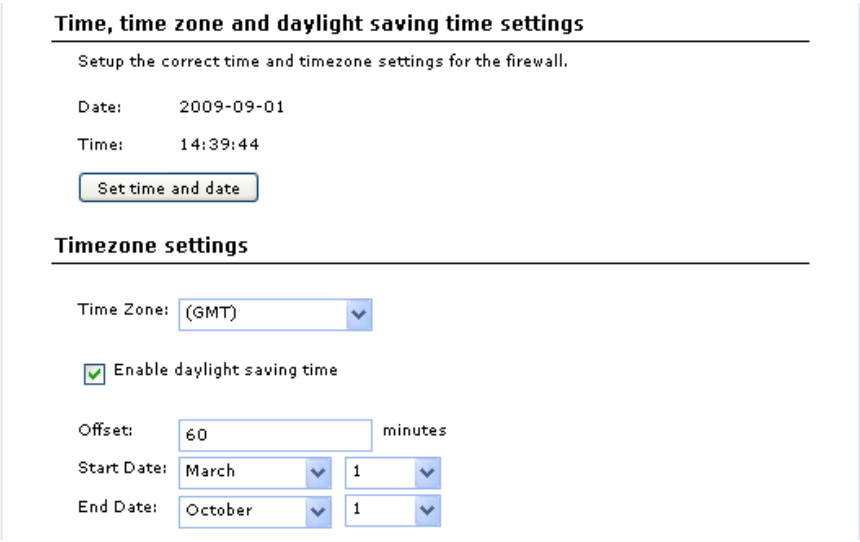
向导步骤1：输入新的用户名和口令

您将被提醒以输入一个新的管理员用户名和口令，如下图所示。推荐完成这一步，并记住新的用户名和口令（如果忘记，可以通过恢复到出厂设置来恢复初始的 admin / admin 的组合）。口令应该足够复杂，以免被轻易猜出。



向导步骤2：设置时间和日期

CorePlus的许多功能都依赖于准确的日期和时间，因此，准确设置下图所示的输入域就显得尤其重要。

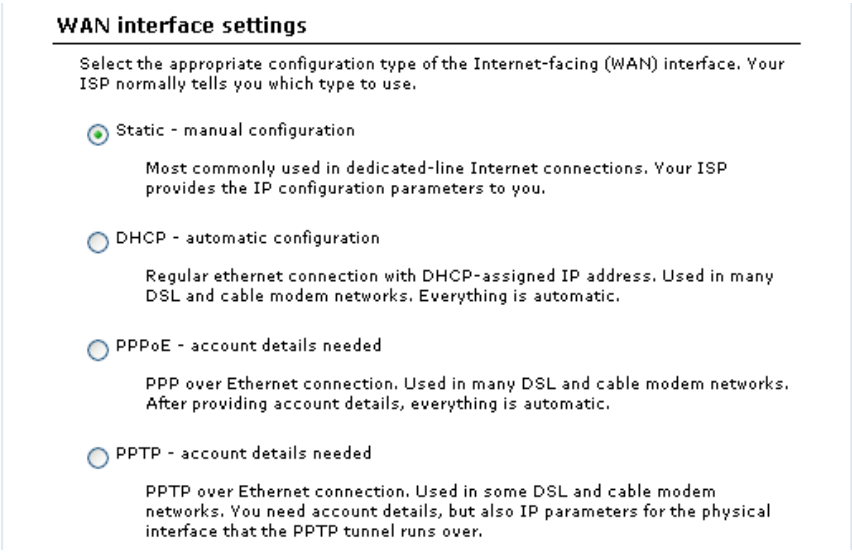


向导步骤3：选择WAN接口 WAN 接口

Next, you will be asked for the WAN interface that will be used to connect to your ISP for Internet access.

向导步骤4：选择 WAN 接口的设置

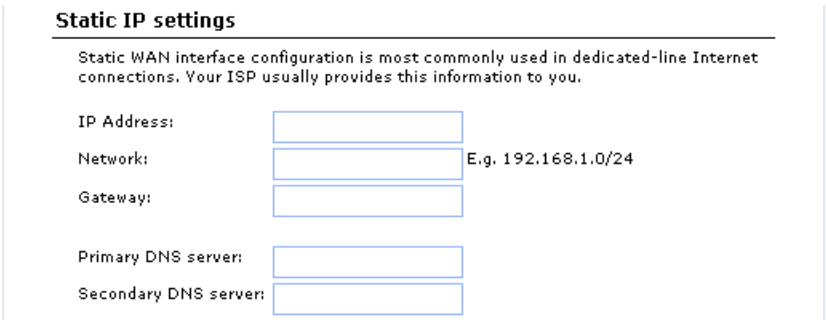
这一步将选择WAN到Internet的连接方式。既可以 手动设置 ， DHCP ， PPPoE 或 PPTP 来连接，如下图所示。



这四个不同的连接选项在下面的子节 4A 到 4D中进行讨论。

- 4A. 静态 - 手动配置

  ISP提供的信息应该被输入到下一步的向导界面中。所有输入域都需要被输入，除过备份DNS服务器 输入域。

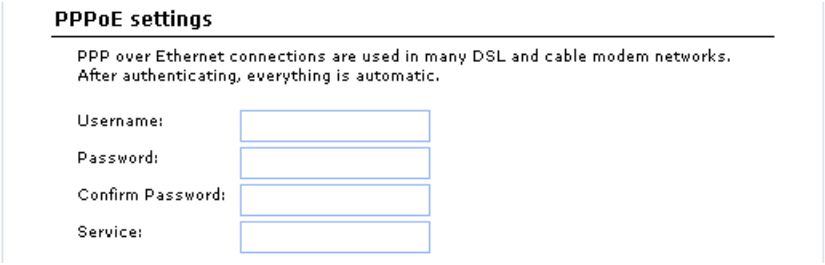


- 4B. DHCP - 自动配置

  如果选择此选项，则意味着所有必需的IP地址都要从ISP的DHCP服务器获得。此选项无需更多配置，因此它没有更进一步的向导界面。

- 4C. PPPoE设置

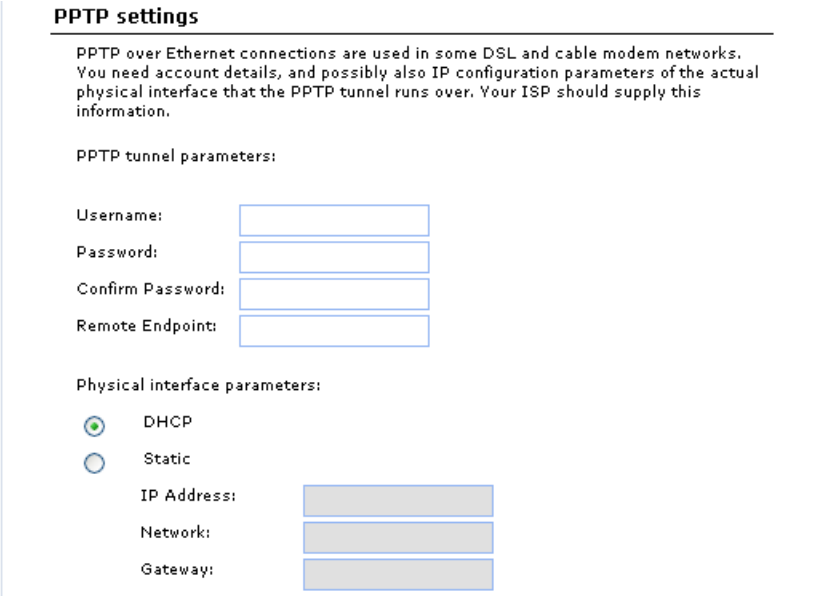
  由ISP提供、用于PPPoE连接的用户名和口令在这里输入。服务域应该留空，除非ISP为提供了一个服务名称。



  在建立了PPPoE的连接后，DNS将会被自动设置。

- 4D. PPTP设置

由ISP提供、用于PPTP连接的用户名和口令应该在这里被输入。如果要ISP同时也使用DHCP，那么此项就应该被选择，否则，请选择下面的 静态 ，并输入由ISP提供的静态IP地址。

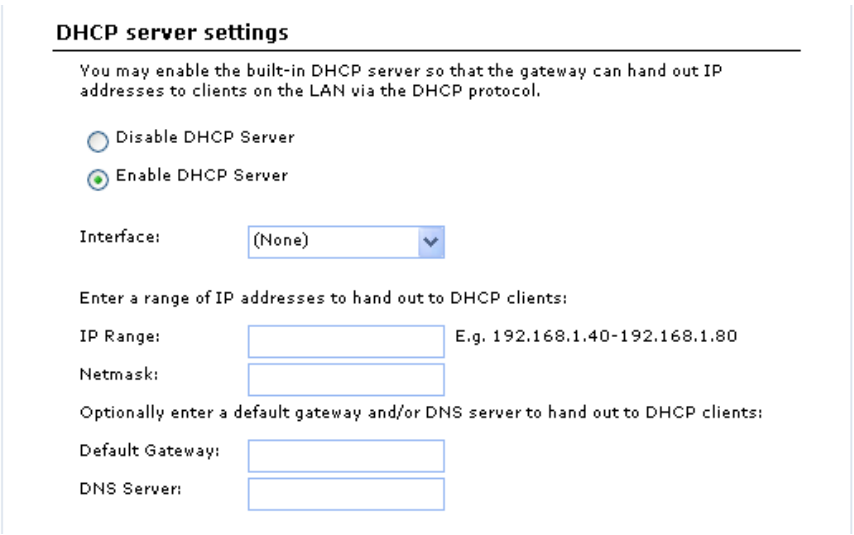


在建立了PPTP连接之后，DNS将会被自动设置。

向导步骤5：DHCP服务器设置

如果Clavister安全网关需要作为一台DHCP服务器，在这一步里就可以启用此功能，这需要在向导中指定特定的接口，或者在以后进行配置。

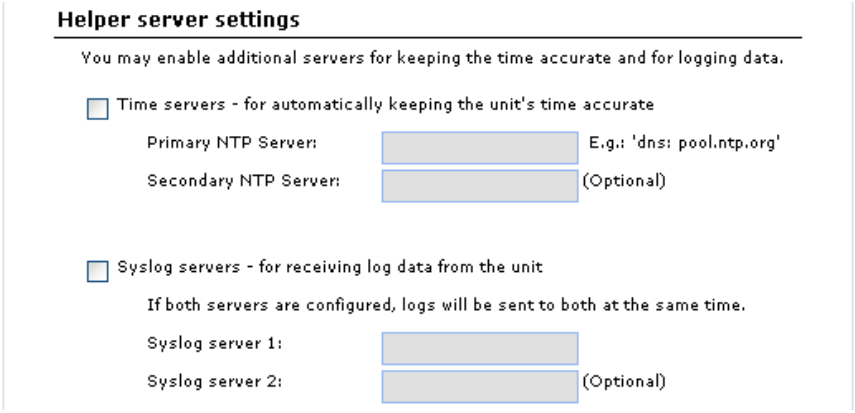
要对DHCP客户端进行分发的IP地址范围必须以 nn.nn.nn.nn - nn.nn.nn.nn的形式来指定。例如，可以指定 192.168.1.50 - 192.168.1.150 这样的内部IP地址范围。



向导步骤6：帮助服务器设置

服

务器可以保持系统日期和时间的精确性。Syslog服务器可以被用来接收和存储由CorePlus所发出的日志消息。

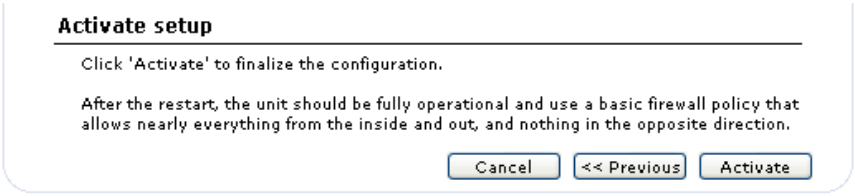


缺省网关，推荐指定为 192.168.1.1 ，同时，所指定的DNS服务器应该为您的ISP所提供的DNS。

在指定一个主机名而不是一个IP地址来作为一个服务器的时候，主机名应该以字符串 dns:作为前缀。例如，主机名 host1.company.com 应该被以 dns:host1.company.com的形式输入。

向导步骤7：激活设置

最后的步骤就是激活您所做的配置，只需点击 Activate 按钮就可完成。在此步骤之后，Web界面就会返回到它正常的外观形式，管理人员就可以继续对系统进行配置了。



再次运行配置向导

一旦向导被成功结束，并且配置已被激活，它就不能再次运行。这一情况的例外就是，如果Clavister安全网关被恢复了出厂配置，在这种情况下，设备就会认为自己是第一次运行，因此配置向导就会再次运行。

上传许可证

无论向导是否在运行，Web界面此刻都可以被用于上传一个可用的许可证到Clavister安全网关。如果没有许可证，CorePlus将运行在 演示模式 下，这意味着它将在正常运行两个小时之后停止工作（重新启动系统将允许CorePlus再运行两个小时）。上传许可证的步骤在 第 4 章 许可证 中进行讨论。

3.3. 手动Web界面配置

本节描述CorePlus的初始化配置，通过直接的Web界面来执行，而无需使用设置向导。不同的配置通过一系列相互独立的步骤来完成，这可以使得管理人员能够更直接地控制配置过程。即使使用了向导，这一节也是值得阅读的，因为本节是对使用Web界面来配置CorePlus的各个关键方面的很好的介绍。

以太网接口

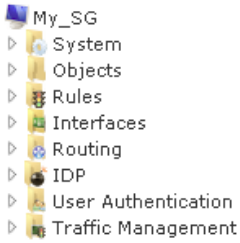
到达Clavister安全网关的外部网络的物理连接是建立在不同的种类的 以太网接口之上的，这取决于所提供的硬件平台。在VMware中，这些接口都是由hypervisor所提供的。在第一次运行的时候，CorePlus扫描这些接口，并判断哪些可用，并为它们分配各自的接口名称。扫描过程中第一个被检测到的接口将成为初始的缺省管理接口，并且这种分配方式虚拟接口不可提在事先被改变。

CorePlus的所有接口在逻辑上对于CorePlus来说都是相等的，并且，尽管其物理性能可能极其不同，接口总是管理接口。假设常
规的VMware总共具有3个虚
拟接口，另外两个虚拟接口

接口将被用于连
接到一个受保护
的、本地的网络
If2和If3。在这一节里，我们将假设If2接口将被用于连接到公共互联网，同时，If3。

导航树

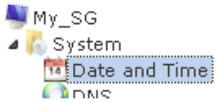
Web界面以树状结构显示了CorePlus中的各个不同组成部分，这个树状视图位于浏览器窗口中的左侧面板中。



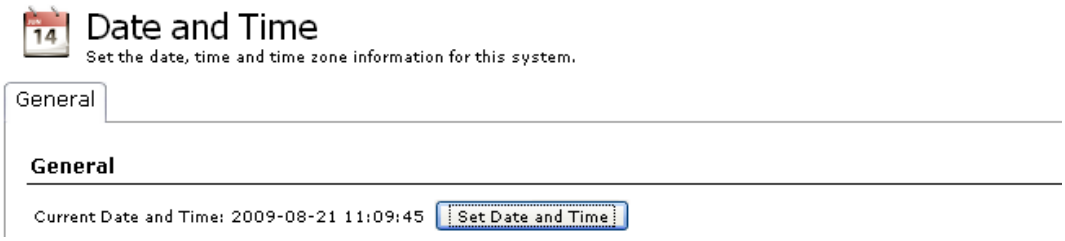
通过点击导航树的各个不同部分，我们就可以展开它的节点以查看并配置不同的属性，如 设置、对象 和 规则 ，这样就可以对CorePlus进行配置。下面我们将讨论一个改变配置的简单例子。

设置日期和时间

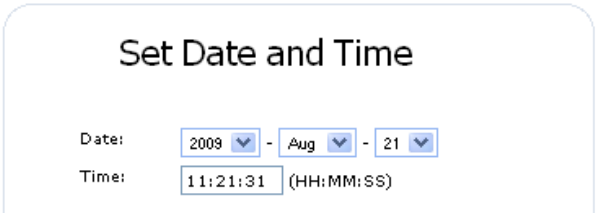
CorePlus的许多功能都依赖于准确的日期和时间，因此日期和时间的设置就显得相当重要。即使运行在VMware上的时候，每一台虚拟的安全网关也都保持着各自的日期和时间，因此要注意对每一台安全网关都要进行准确的日期和时间的设置。要进行此操作，请在导航对中打开 系统 节点。



如果我们此刻点击 Date and Time 节点，当前的日期和时间属性设置界面就会出现在Web界面的中部。



通过点击 设置日期和时间 按钮，就可以显示一个对话框，在这个对话框中您可以设置精确的时间。



（NTP）服务器也可以可选性地被配置，用来维护精确的系统日期和时间，同时，这也要求安全网关能够访问公共互联网。强烈推荐启用该选项，因为它可以确保日期和时间的网络时间协议精确度。一个典型的NTP设置如下图所示。

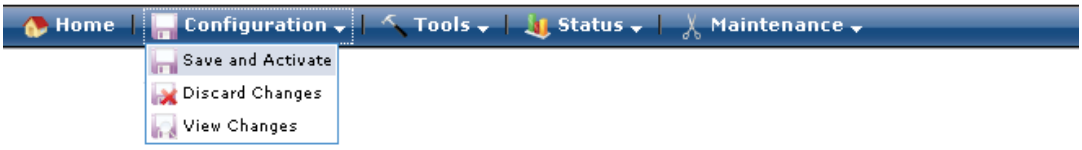
注意：时间服务器的URL需要以“dns:”作为其前缀

作为其前缀
在CorePlus中指定一个时间服务器的URL的时候，所使用的URL必须以“dns:。

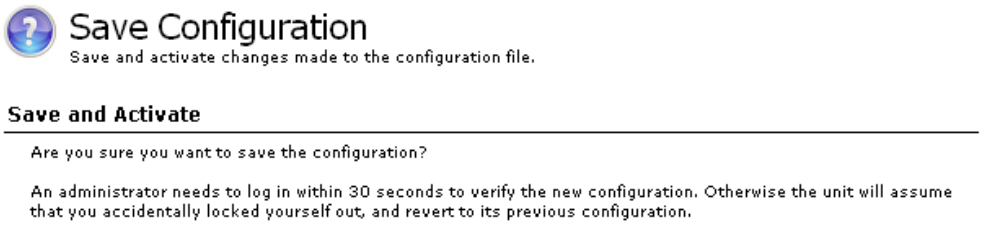
来保存这个值，然后就可以进行CorePlus配置步骤中的后续步骤了。虽然被改变的值，如同这个时间服务器的URL一样，已经被CorePlus保存了，但他们不会立刻被应用，直到所有被保存的配置成为当前配置，并进行了配置的激活。我们将在下一步中看到如何进行这样的操作一旦这个值被正确设置，我们就可以点击确定。

激活配置的更改

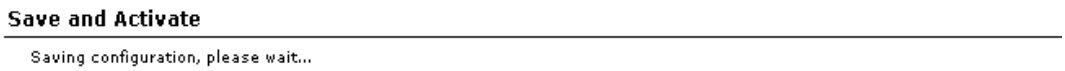
要激活CorePlus中的任何配置变化，我们都需要在 配置 菜单中选择 保存并激活（该过程有时也被称为 部署 一个配置）选项。



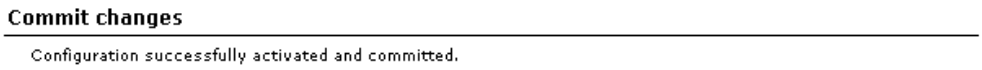
此时，将出现一个对话框，要求确认确实需要将新的配置变为当前运行的配置。



在点击 确定之后，CorePlus的 配置重新加载过程就会发生，在一个很短的延时之后，Web界面将试图再次连接到安全网关。



如果CorePlus没有在30秒钟（这个时间长度可以被设置）内检测到连接，那么CorePlus将会恢复到上一次的配置。这是为了确保新的配置不会意外地把管理人员关在了外面。在配置重新加载完成并成功地建立了连接，一个成功的消息就会被显示出来，表示配置的重新加载已经成功。



配置的重新加载是CorePlus管理人员经常会执行的一个操作过程。通常情况下，配置的重新加载会花费一点点时间，并因此而引起正在通过的数据流有一些轻微的延时增大。同时，Clavister安全网关上处于活动状态的用户连接有可能有很少量的丢失。

提示：提交更改应该有多频繁

由管理员来决定在激活一个新配置之前对配置进行多少次的更改。有些时间，小批量地激活配置有助于检查所计划的配置更改中的小的变化。然而，不建议在很长时间内不进行提交配置的操作，比如超过一个晚上，因为任何原因导致的系统中断都会引起新的配置丢失。

自动退出登录

如果在较长一段时间（缺省时间为15分钟）里没有通过Web界面的活动，CorePlus将自动使用户退出登录。如果管理员再次通过相同的Web浏览器会话进行登录，他将返回到退出登录发生时的操作点上，并且，已保存（但未提交）的更改不会丢失。

设置互联网访问

接下来，我们该看看如何设置公共互联网的访问了。设置向导在前面的章节中已有描述，提供了以下四种选项：

A. 静态 - 手动配置。

B. DHCP - 自动配置。

C. PPPoE设置。

D. PPTP设置。

通过Web界面来对这些不同的连接类型进行手动配置的步骤将在下面进行讨论。

A. 静态 - 手动配置

手动配置意味着将要直接连接到ISP，并且所有连接到ISP的接口相关的IP地址都是固定的值，由ISP提供，需要手动输入到CorePlus中。

注意：接口的DHCP选项应该被禁止

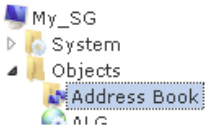
在静态配置Internet连接的情况下，DHCP选项必须被禁止（缺省状态），该选项位于用于连接到ISP的接口属性里。

最初始的步骤就是在CorePlus的 地址薄中设置一些IP地址对象。我们假设这一节中物理接口使用 If2 连接到互联网，该接口的IP地址为 10.5.4.35，ISP的网关IP地址为 10.5.4.1，并且它们都属于10.5.4.0/24这个网络。

注意：在这里使用私有地址仅出于示例的目的

每个具体安装中的IP地址都可能和这些IP地址不同，但是这里所使用的地址仅是为了说明如何完成设置。同时，这些地址为私有地址，而在现实的环境中，ISP将会使用公有的IP地址。

现在，就让我们来添加网关的 IP4 地址 对象，我们把它命名为 wan_gw ，并为它分配这样的IP地址。ISP的网关是从Clavister安全网关访问公共互联网的第一跳。请转到Web界面 10.5.4.1导航树的 系统 > 对象 > 地址薄。



地址薄中的当前内容将会被显示出来，并且也包含了一系列预定义的对象，这些对象由CorePlus在首

次运行时根据对接口进行扫描的结果来创建。下面的这个屏幕快照显示了VSG初始的地址薄。

注意：all-nets地址

all-nets
这个IP地址对象是一个通配地址，不应该随意改变。它可以被用于CorePlus中的多种类型的涉及IP地址和网络范围的规则。

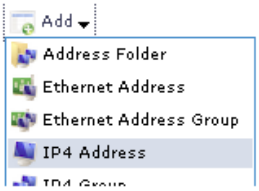
Name	Address	User Auth Groups	Comments
all-nets	0.0.0.0/0		All possible networks
If1_ip	192.168.1.1		
If1_net	192.168.1.0/24		
If2_ip	0.0.0.0		
If2_net	0.0.0.0		
If3_ip	0.0.0.0		
If3_net	0.0.0.0		
localhost	127.0.0.1		Localhost, for non-management High Availability cluster interfaces

缺省情况下，在第一次运行的时候，与一个接口相关的两个IP地址对象会被CorePlus自动创建。一个IP地址对象通过物理接口的名称和后缀 _ip 的组合来被命名，通过这个组合来为一个接口分配IP地址。另一个地址对象由这个接口的名称和后缀 _net 的组合来命名。

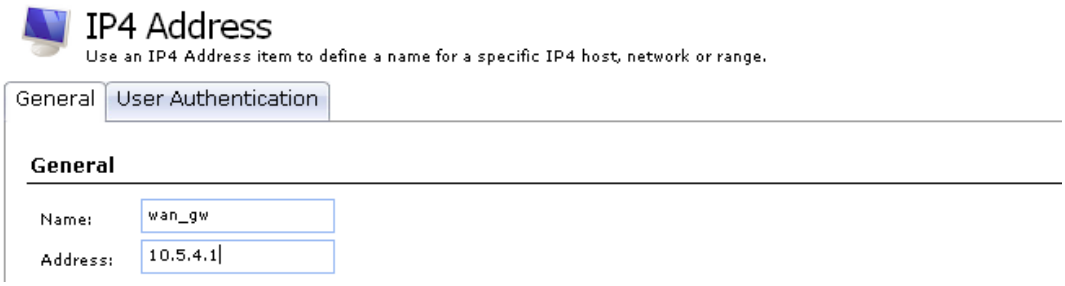
提示：创建地址薄文件夹

如果需要，也可以创建新的文件夹，以提供一种方便的方法来把相关的IP地址对象组织在一起。

现在，请点击列表左上方的 添加 按钮并选择 IP4 地址 选项以添加一个新的地址到这个文件夹中。



在这个IP4地址的属性输入框中输入此对象的详细信息。如下面所示，我们已经为此地址对象输入了 10.5.4.1 这样的IP地址，其名称为 wan_gw。这是ISP的路由器的IP地址，它是我们连接到互联网的一个网关。

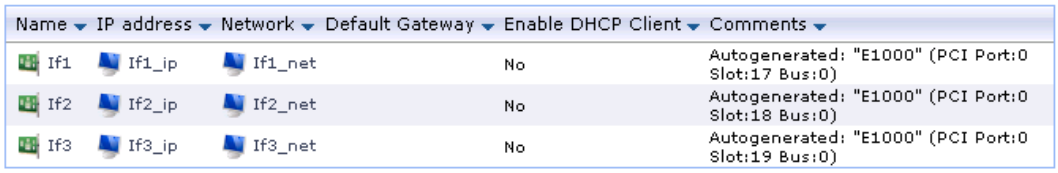


点击 确定 按钮以保存所输入的值。

接下来设置 If2_ip 为 10.5.4.35。这是 If2 接口的IP地址，这个接口将要连接到ISP的网关。

最后，IP4地址对象 If2_net 被设置为 10.5.4.0/24。 If2_ip 和 wan_gw 必须都是属于这个网络的，这样，这个接口才有可能和ISP进行通信。

这3个IP地址对象将被用于配置连接到互联网的接口，在这个例子中这个接口为 If2。在导航树中选择 接口 > 以太网 以显示物理接口的列表。



在列表中点击将要连接到互联网的那个接口。这个接口的属性就会出现，在这里就可以输入相关的设置或对已有配置进行更改了。

点击 确定 以保存更改。虽然所做的更改已被CorePlus记忆，但并没有被激活，并且这些配置不会被激活，直到管理人员明确要求CorePlus激活对配置所做出的更改。

要记住，在使用静态IP地址的时候， 不 应该启用接口上的DHCP，并且必须指定 缺省网关（ISP的路由器）的IP地址。正如在后面的部分将要更详细的解释的那样，指定 缺省网关 还具有一个额外的效果，那就是会自动向CorePlus的路由表中添加缺省路由。

此时，到互联网的配置已完成，但是内部的数据流尚不能到达互联网，来自互联网的数据流也不能进入到内网，因为所有的数据流都需要在CorePlus中的最少两个配置对象存在的情况下才可以经过Clavister安全网关流入或流出：

- 一条 IP 规则 ，它需要在CorePlus的 IP规则集 中被定义，以明确地允许数据流从一个指定的源网络和源接口流动到一个指定的目标网络和目标接口。
- 要在CorePlus的路由表中定义的 路由 ，它要指定通过哪个接口，CorePlus才可以找到数据流的目标IP地址。

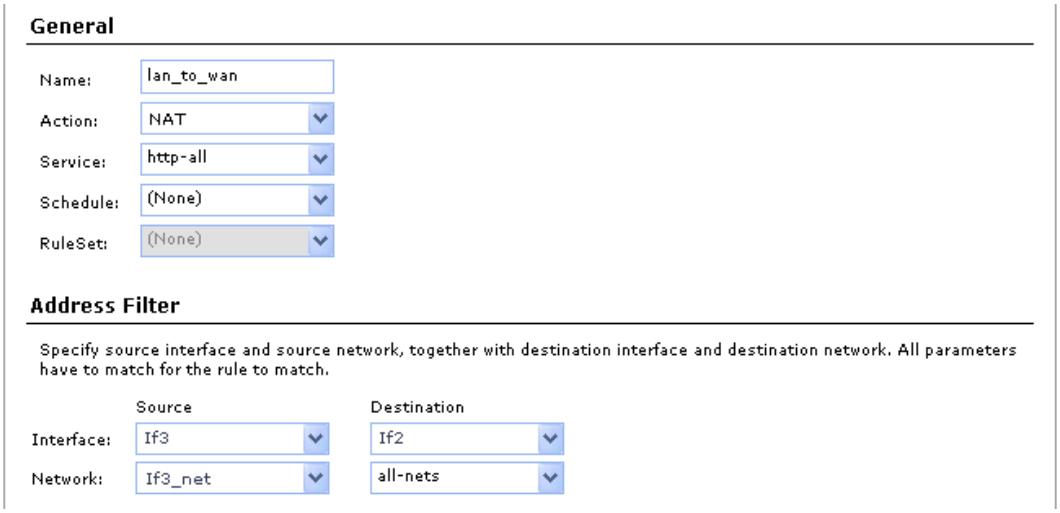
  如果找到多条匹配的路由，CorePlus将采用最小的（也就是最窄的）路由范围。

因此，我们必须首先定义一条IP规则，以允许来自于一个特定源接口和源网络的数据流通过。在这个例子中，让我们假设我们想要允许通过 If3 接口连接到Clavister安全网关的内部网络If3_net的web数据流访问公共互联网。

要完成这一点，我们首先转到导航树的 规则 > IP规则集 > 主规则集 。

一个空的 main IP规则集现在将显示出来。在左上方点击 添加 按钮，并从菜单中选择 IP规则 。

这个新的IP规则的属性将显示出来。在这个例子中，我们将命名其为 lan_to_wan。规则 动作 设置为 NAT （将在下面进行更进一步地解释）。 服务 被设置为 http-all ，这个服务适合于绝大多数的web浏览（该服务同时允许HTTP和HTTPS连接）。源接口和源网络以及目标接口和目标网络在此规则的 地址过滤器 中设置。



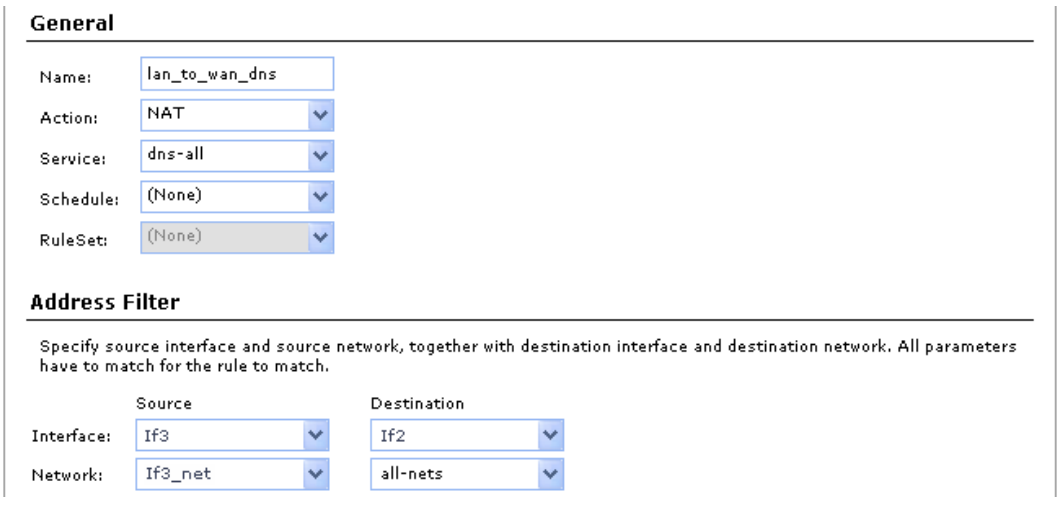
这条规则中所指定的目标网络需要被指定为预定义的IP4地址对象 。之所以要使用这个，主要原因是因为我们不能提前预知web浏览的目标IP地址，而且，这样做可以允许浏览任何IP地址。IP规则被以自上而下的顺序进行处理，首条匹配的规则将被服 all-nets从。这样的一条 all-nets 规则应该被置于整个规则集的底部，因为其它具有更窄目标地址的规则应该在这条规则之前先被触发 。

只需一条规则，因为任何由一条 NAT 规则控制的数据流都将被CorePlus的状态引擎所控制。这意味着这条规则将允许从源网络到目标网络的 连接 ，同时也明确地允许了任何属于这些连接的返回的数据流。

在上面，我们所选择的服务名为 http_all ，它是在CorePlus中预定义的。比较明智的做法是在一条IP规则中尽可能地严格地限制服务，这样做可以提供最高的安全性。可以创建自定义的服务对象，也可以创建新服务，它们都可以与已有的服务进行组合。

我们也可以把规则的 动作 指定为 Allow，但这要求所有受保护本地网络中的主机都具有公有的IP地址。 通过使用 ，CorePlus将使用目标接口的IP地址作为源IP。这意味着外部的主机将发送他们的响应到这个接口的IP，然后，CorePlus就会自动把数据流重定向到发起连接的本地主机。因此，只有连接外部的接 NAT口才需要一个公有的IP地址，同时，内部的网络拓扑也会因此而被隐藏。

要允许web浏览，DNS查询也需要被允许，以使URL可以被解析为IP地址。名为 http_all 的服务并不包含DNS协议，因此我们需一个类似的IP规则以允许DNS查询。这可以通过一条IP规则来实现，这条规则使用一个自定义的服务，这个服务同时结合了 HTTP 和 DNS 协议，但推荐的方法是创建一条完全不同的新规则，只需复制上面的规则，只需把服务指定为 dns- 。这种方法在检查配置时使人一目了然，易于发现并解决问题。下面的屏幕快照显示了一条新的规 all则，名为 lan_to_wan_dns ，创建它的目的就是为了允许DNS查询。



这条规则同时也指定了用于DNS请求的动作为 NAT ，因此所有的DNS请求数据流由CorePlus发送的时候使用了外部接口的IP地址作为源IP地址。

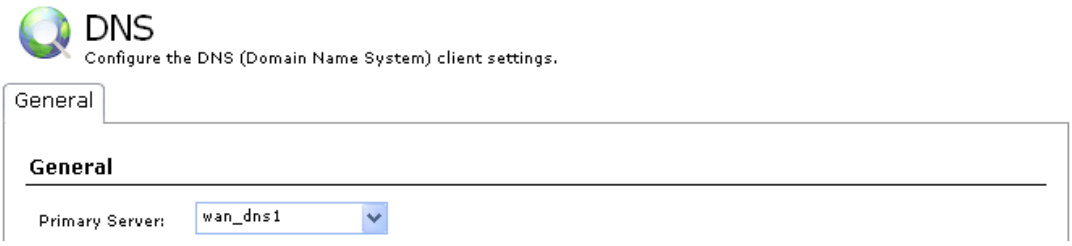
为了使互联网连接能够正常工作，我们也需要定义一条路由，这样的话，CorePlus才可以知道web数据流应该经由哪个接口离开Clavister安全网关。这条路由将定义名为 all-nets 的网络可以在哪个接口上找到。如果我们转到导航树中，点击 路由 > 路由表 > Main ，打开缺省的主路由表，所需的路由就应该会被显示出来，如下图所示。

这条必需的 all-nets 路由，事实上是自动添加的，如果我们在前面为一个特定的以太网接口设置其所需的IP4地址对象地同时也添加了 缺省网关 ，这条路由就会被自动添加。

注意：禁止自动路由生成

在接口属性中有一个 “使用此接口上指定的缺省网关来自动添加缺省路由” 的设置，禁用或启用此选项就可以禁用或启用自动路由生成。

作为设置步骤的一部分，推荐在CorePlus中设置最少一个DNS服务器。这个DNS服务器或服务器组（最多可以配置三个）将被CorePlus解析URL的时候使用，主要是在配置中使用了URL来代替具体的IP地址的情况下。让我们来假设一个名为 wan_dns1 的IP地址对象已经被定义在了地址薄中，它是第一台DNS服务器的IP地址。在导航树中选择 系统 > DNS ，DNS服务器对话框就会打开，并可以从地址薄中为其分配这个对象（wan_dns1）来作为首台DNS服务器。



B. DHCP - 自动配置

所有建立Internet连接所必需的IP地址也可以自动地从一个ISP的DHCP服务器处获取，只需启用连接到这个ISP的接口上的 DHCP 客户端 选项即可。我们可以在导航树中选择 以太网 > 接口 ，来显示所有接口的列表，并在相应接口上启用此选项。

在列表中点击 If2 接口，以显示它的属性。

在上面的屏幕快照中，该接口的DHCP已经被启用了，如果需要自动获取IP地址，那么这个设置就是必须的。通常情况下，一个DHCP 主机名 并不需要被指定，但有时候这个主机名也可以被ISP用于唯一性地把Clavister安全网关识别为DHCP服务器的一个特定的DHCP客户端。

在到ISP的连接上，所有必需的IP地址都被自动地从ISP处通过DHCP获取，并且CorePlus将会自动地使用这些信息在地址薄中设置相关的地址对象。

对于CorePlus来说，要想获悉在哪个接口上可以找到公共互联网，就需要添加一条 路由到CorePlus的 主路由表中，这样，CorePlus就可以知道哪个接口是连接到ISP的，并从这个接口上找到 all-nets 这个网络，但这条路由必须具有正确的 缺省网关 的IP地址。这个 all-nets 路由被CorePlus在DHCP地址获取过程中自动添加。

在所有的IP地址都通过DHCP被设置好，并且一条 all-nets 路由也被添加了，同时到达互联网的连接也已经被配置了，但没有数据流可以流入或流出到互联网，因为还没有定义IP规则以允许这些数据流通过。如同在选项 ）中所做的一样，我们必须因此而定义一条IP规则，以允许来自于一个特定的源接口和源网络（在（A这个例子中就是网络 If3_net 和接口 If3） 的流量到达目标网络 all-nets ，并且其目标接口为 If2.

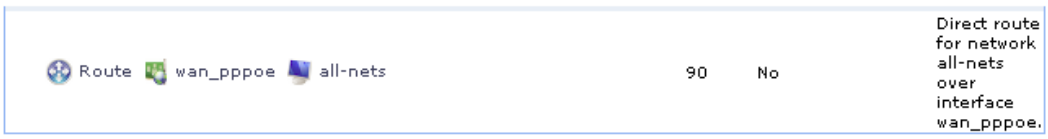
C. PPPoE 设置

对于PPPoE连接来说，我们必须创建一个PPPoE通道接口，并把它与一个物理以太网接口相关联。假设这个物理接口为 If2 ，并且已被创建的PPPoE通道对象被命名为 wan_pppoe 。在导航树中转到 接口 > PPPoE ，并选择 添加 > PPPoE 通道 。这些值现在就可以被输入到PPPoE通道的属性对话框中了。

您的ISP将会为上面的对话框中的 pppoe_username 和 pppoe_password 供正确的值。

现在，PPPoE通道接口就可以被如同物理接口一样对待并使用了，其使用范围包括已定义在CorePlus中的规则集等。

在这里也同样需要一条与PPPoE通道相关的路由来允许数据流通过PPPoE通道本身，在定义通道的时候，这样的路由会被自动创建于 main 路由表中。如果我们在导航树中转到 路由 > 路由表 > Main ，我们就可看到这条路由。



如果PPPoE通道对象被删除，这条路由也就会自动被删除。

这时，仍然不会有数据流流过这个通道，因为没有定义相应的规则。如同在上述的选项 A 中所做的一样，我们必须因此而定义一条IP规则，以允许来自于一个特定的源接口和源网络（在这个例子中就是网络 If3_net 和接口 If3） 的流量到达目标网络 all-nets ，并且其目标接口就是我们前面定义的PPPoE。

D. PPTP 设置

对于PPTP连接方式来说，需要创建一个PPTP客户端接口对象。让我们假设这个PPTP通道被命名为

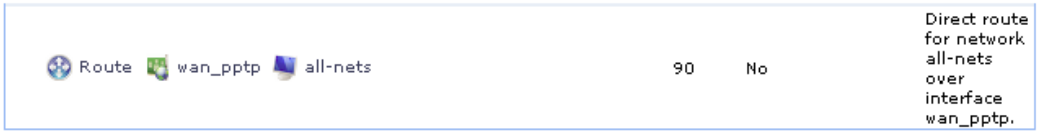
wan_pptp ，且其远程端点为 10.5.4.1 ，已经被作为一个IP4地址对象定义成了 pptp_endpoint 。在导航树中，点击 接口 > PPTP/L2TP 客户端 ，并选择 添加 > PPTP/L2TP 客户端 。这些值现在就可以被输入到属性对话框中，同时要注意应该选择 PPTP 作为其通道协议。

您的ISP将为您提供远程端点、 pptp_username、 pptp_password 等正确的值。在定义通道时无需指定接口，因为CorePlus会在自身的路由表中查找 远程端点 的IP地址来判断要使用哪个接口。

PPTP客户端通道接口现在就可以被作为一个物理接口被CorePlus规则集中的策略来对待和使用了。

在这里同样也需要有一条与PPTP通道相关的路由来允许数据流能够通过CorePlus本身，这条路由在定义通道时被自动添加到 main 路由表当中。这条路由的目标网络应该是为这个通道指定的 远程网络 ，如果用于访问互联网，这个目标网络应该为 all-nets。

如果我们在导航树中转到 路由 > 路由表 > Main ，我们就可以看到这条路由。



如果PPTP通道对象被删除，这条路由也会被自动删除。

这时，仍然不会有数据流通过这个通道，因为还没有定义IP规则来允许数据包通过。如同我们在选项 A
中所做的一样，我们必须定义一条IP规则，来允许来自于特定的源网络和源接口（在这个例子中，网络为 If3_net 和接口 If3） 流动到目标网络all-nets，而目标接口就是我们定义的PPTP通道。

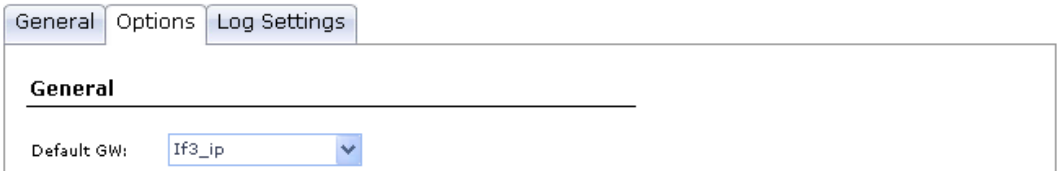
DHCP服务器设置

如果Clavister安全网关要扮演一个DHCP服务器的角色，那么，就可以通过以下的方法来进行设置：

首先创建一个IP4地址对象，这个地址对象用于定义要分配出去的地址范围。在这里，我们将假设这个对象的名称为 dhcp_range。我们也将假设有一个IP4地址对象 dhcp_netmask 已经被创建，它指定了子网掩码。

现在我们就可以创建一个DHCP服务器对象了，其名称为 dhcp_lan ，它将仅在 If3 接口上生效。要实现这一点，请点击 系统 > DHCP > DHCP服务器 ，并选择 添加 > DHCP服务器。我们现在就可以指定这个服务器的属性了。

另外，很重要的一点就是为这个服务器指定 缺省网关 。这将被分配给位于内部网络中的DHCP客户端，这样，它们就会知道可以在哪里找到公共互联网了。缺省网关总是配置了DHCP服务器的接口IP地址，在这个例子中，就是 If3_ip 。

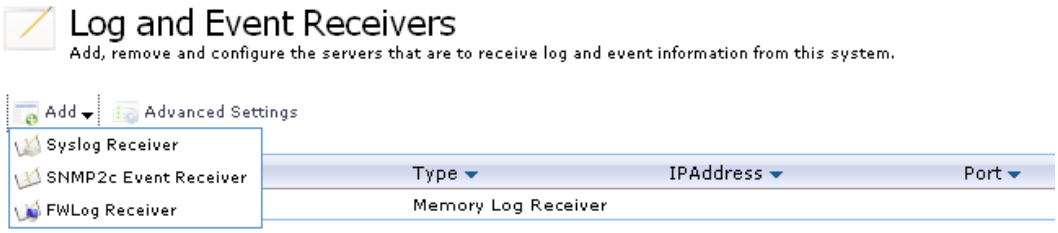


同时，在这个 选项 中，我们应该指定DNS地址，DNS地址也要和DHCP租约一起分配出去。这可以被设置为类似于 dns1_address 的IP地址对象。

Syslog服务器设置

尽管日志已被启用，但仍不会有日志消息被捕捉到，除非最少配置了一台日志服务器，以用于接收这些日志，这需要在CorePlus中进行配置。 Syslog 是最为通用的日志服务器类型之一。

首先，我们创建一个IP4地址对象，名称就叫做 syslog_ip ，它被设置为服务器的IP地址。我们接下来配置要从CorePlus发送的日志消息到syslog服务器，在导航树中选择 系统 > 日志与事件接收器 ，然后选择 添加 > Syslog接收器。



Syslog服务器属性对话框现在将出现。我们为这个服务器指定一个名称，例如 my_syslog，并指定 syslog_ip 对象作为它的IP地址。

提示：地址薄对象的命名

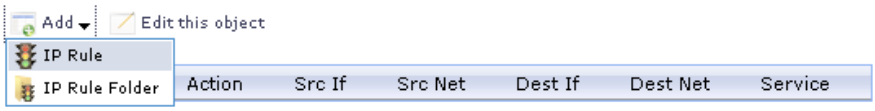
CorePlus的地址薄以字母顺序的方式来组织，因此在为IP地址对象选择名称的时候，最好使这个名称的前一部分为一个描述性的部分。在这个例子中，使用 syslog_ip 作为名称，而不是 ip_syslog。

允许 ICMP Ping 请求

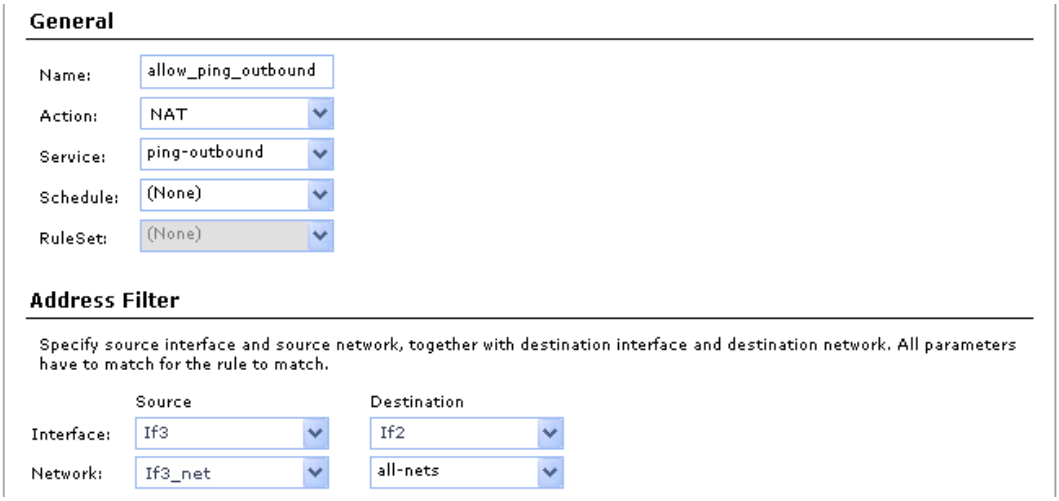
作为更进一步设置IP规则的一个例子，允许ICMP Ping 请求通过Clavister安全网关可能就显得非常重要了。如我们早些时候所讨论的，CorePlus将丢弃所有数据包，除非有一条IP规则明确地允许了某种数据包。让我们设想我们希望允许ping外部的主机，使用ICMP协议，发起ping的主机位于内部的 If3_net 这个网络中。

在CorePlus中可以定义数个规则集，但在缺省情况下仅只有一个规则集，这个缺省定义的规则集其名称为 main。要向这个规则集中添加一条规则，请首先在导航树中选择 规则 > IP规则集 > main 。

main 规则集中的列表内容现在将显示出来。点击 添加 按钮，并选择 IP规则。



一个新建IP规则的属性将会显示出来，此刻我们就可以添加一条规则，在这个例子中，它的名称为 allow_ping_outbound。



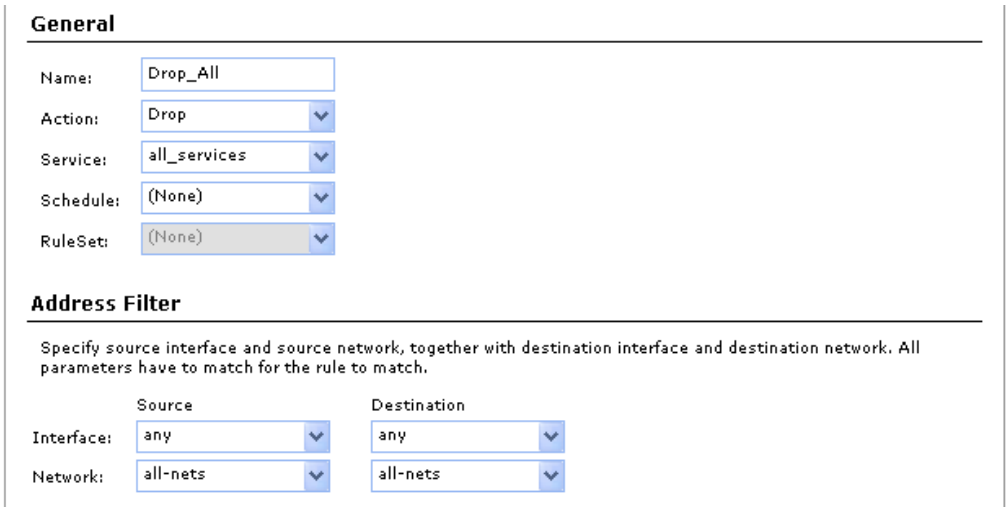
同样，这条IP规则的动作为 NAT，并且在受保护的主机都只是具有私有的IP地址的情况下必须这样做。ICMP请求将被从Clavister安全网关发出，其源IP为连接到ISP的接口，也就是源接口的IP地址。进行响应的主机将返回IMCP应答给这个单主机IP，并且CorePlus将转发这些响应给正确的私的IP地址。

添加一条Dorp All的规则

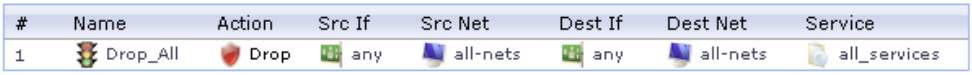
自上而下的IP规则集扫描机制已经在前面进行过讨论了。如果 没有为一个要新建的连接找到匹配的IP规则，那么， 缺省规则就会被触发。这个规则是隐藏的，并且不能被修改，它的动作是丢弃所有此类的数据流，并为丢弃操作生成日志消息。

为了获得这些被丢弃的数据流的日志信息，我们推荐您创建一条丢弃所有的规则作为 main 规则集中的最后一条规则。这条规则的 动作 应该为 Drop ，源和目标网络都设置为 all-nets，源和目标接口都设置为 any。

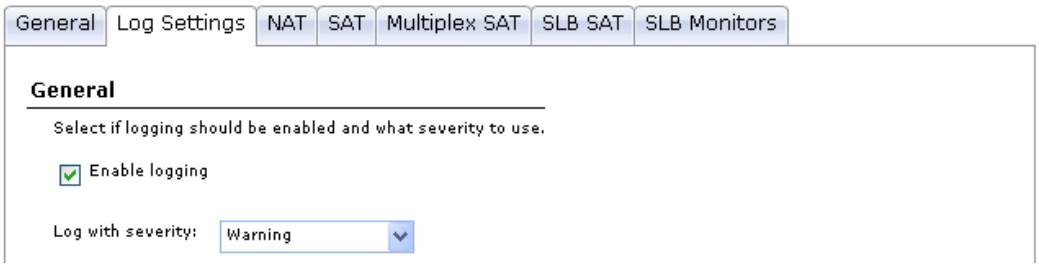
这条规则的服务必须同时也被指定，而且应该被指定为 all_services，这样才可以捕获所有类型的数据流。



如果这是唯一定义的规则，那么 main IP规则集中将会显示如下。



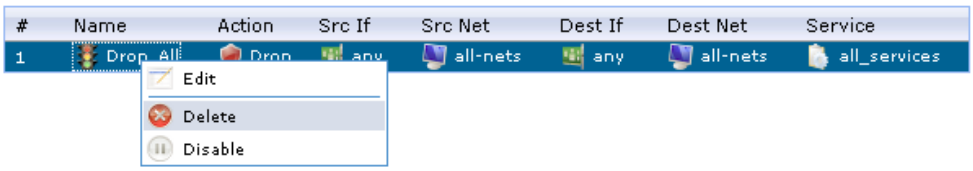
现在就可以启用这条规则的日志消息记录了，并可以选择您感兴趣的等级，只需点击 日志设置 页，并选中 启用日志 选项框。所有由这条规则生成的日志消息，都会被赋予显示在日志消息文本框中的等级。等级是由管理人员来指定的，依赖于他们决定如何对这些消息进行分类。



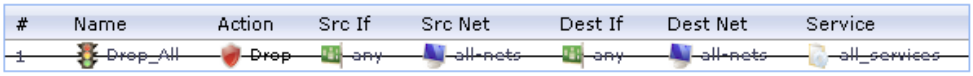
删除配置对象

如果在编辑的时候从配置中删除一些信息，那么这些被删除的内容就会在列表中被用横线标记，同时，配置仍然不会立刻生效。这些被删除的条目仅在配置的更改被提交后才完全消失。

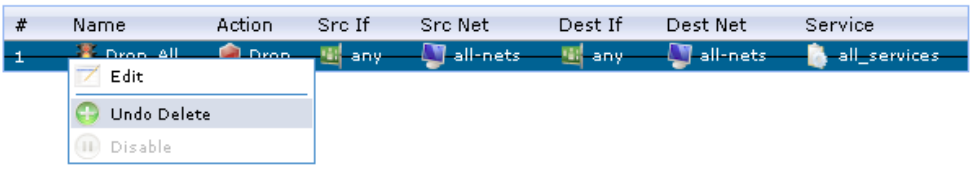
例如，我们可以删除这条我们在前面上段所创建的丢弃所有的IP规则，通过右击这条规则，并在上下文菜单中选择删除。



这条规则现在就会被用一条横线进行标记的方式显示出来。



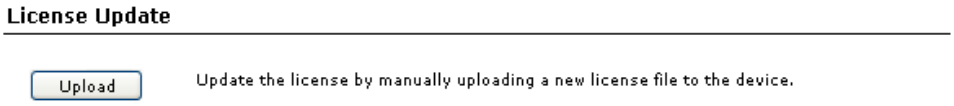
我们可以恢复删除，只要再次右击这条规则，并在随之出现的上下文菜单中选择 撤销删除 即可。



上传一个许可证

如果CorePlus没有加载一个有效的许可证，那么它就只能运行在 演示模式下，这意味着它将在开机后正常运行2小时就停止工作。要取消这种运行时间的限制，就必须上传一个有效的许可证到Clavister安全网关。

要完成此操作，就需要如 第 3.2 节“Web界面和向导设置”一节的最后一部分中所描述的内容进行操作。这个许可证可以通过点击 维护菜单中的 许可证 选项，然后再点击 上传 钮的方式被直接上传给CorePlus。



现在，点击 浏览 按钮，以从本地文件系统中选择合适的许可证文件，然后点击 上传许可证 按钮，把此许可证发送给CorePlus。

一旦上传许可证的操作完成，2小时的限制就会被解除，同时，CorePlus将受到这个许可证里的约束性项目的约束。

3.4. CLI设置

本章描述使用CLI命令来进行设置的步骤，而非设置向导了。

CLI的界面可以通过两种途径来访问：

- 在本地网络中，通过SSH（Secure Shell）客户端访问IP地址 192.168.1.1 来连接到CLI操作界面。网络连接的设置和 第 3.2 节 “Web界面和向导设置” 一节中所描述的一样，工作站的接口的静态IP地址必须进行设置，且这个地址应该与Clavister安全网关的接口处于相同的一个网络。

  如果工作站的连接有问题，可以在 第 3.5 节 “对设置进行排错” 一节中找到帮助清单。

- 通过CorePlus自己的控制台端口。在VMware上，CorePlus的控制台就是虚拟机器的控制台。

下面列出的CLI命令都被进行了分组，它们与设置向导中可用选项一一对应。

确认连接

一旦建立了到CLI的连接，按下 回车 键将会得到CorePlus的响应。这样的响应是一个正常的CLI提示符，如果您使用VMware虚拟机器控制台，将不需要输入 用户名/口令的组合（可以在以后设置用于控制台访问的口令）。

```
Device:/>
```

如果通过一个SSH（Secure Shell）客户端来进行远程连接，就必须首先输入用户名/口令，这个初始的用户名为 admin ，口令也是 admin 。当用户名和口令被CorePlus所接口，一个正常的CLI提示符将出现，这样就可以输入CLI命令了。

改变口令

如需改变管理员的用户名和口令，可以使用 cc 命令来改变当前的CLI对象分类（有时也可以被称为对象上下文 ）到名为 AdminUsers 的 本地用户数据库 。 .

```
Device:/> cc LocalUserDatabase AdminUsers
Device:/AdminUsers>
```

提示：在CLI中使用tab补全

可以在任何时候按下 tab 键，CorePlus将给出所有可能的命令选项的列表。

现在就可以设置用户名/口令了，要注意的是，用户名和口令是区分大小写的。在这个例子中，我们把用户名改为 new_name ，并把口令改为 new_pass。

```
Device:/AdminUsers> set User Admin Name=new_name Password=new_pass
```

新的用户名和口令应该被确保记住，同时，口令应该应该是一种非常难以猜测的组合。下一步就是返回到CLI的对象分类的顶层了。

```
Device:/AdminUsers> cc
Device:/>
```

设置日期和时间

CorePlus的许多功能都依赖于精确的时间，因此，使用 time 命令来设置正确的时间就显得非常重要。一个典型的设置方法如下：

```
Device:/> time -set 2008-06-24 14:43:00
```

请注意，日期需要以 yyyy-mm-dd 的格式输入，而时间为24小时制，且要以 hh:mm:ss 的形式输入。

以太网接口

外部网络连接到Clavister安全网关的连接可以通过不同的以太网接口来实现，这些接口由具体的硬件平台提供。在VMware上，连接是通过hypervisor所提供的虚拟接口来完成的。在第一次启动的时候，CorePlus扫描这些接口，并判断哪些可用，并为它们分配名称。第一个被检测过程检测到的接口总是会成为初始的缺省管理接口，这是不能预告更改的。

CorePlus的所有接口在逻辑上都是相等的，并且，尽管它们的物理性能可能会非常不同，但所有接口都可以执行所有的逻辑功能。在运行在VMware上的CorePlus中，虚拟的 If1 接口总是管理接口。假设一共具有3个虚拟接口，另外的两个接口将CorePlus被指定一个 If2 和 If3 的名称。为了举例的需要，我们将假设 If2 接口将被用于连接到公共互联网，而 If3 接口将被用于连接到一个受保护的、本地的网络。

设置互联网访问

接下来，我们将要看一看如何通过CLI来设置以公共互联网的访问。前面所供述的设置向导提供了下面的四个选项：

A. 静态 - 手动配置。

B. DHCP - 自动配置。

C. PPPoE设置。

D. PPTP设置。

通过CLI来手动配置这几个不同的连接选项的步骤在下面进行讨论。

A. 静态 - 手动配置

首先，我们必须设置或创建一些IP地址对象。假设在这个例子中被用于连接到互联网的接口为 If2，ISP的网关IP地址为 10.5.4.1 ，连接到这个网关的接口为 10.5.4.35 ，它们同属于 10.5.4.0/24 这样的一个网络。

使用私有地址仅是为了示例之用。

每一个现实案例的IP地址都将与这里所述的IP地址不同，但这里所用的地址仅仅只是为了说明如何完成设置。同时，这些地址都是私有的IP地址，而在真实的环境中，ISP将会使用公有的IP地址。

我们首先添加网络IP地址对象，我们称之为 wan_gw。

```
Device:/> add Address IP4Address wan_gw Address=10.5.4.1
```

这是ISP的网关的地址，是到达公共互联网的第一个路由器跳转点。如果这个IP地址对象已经存在，它可以通过下面的命令来指定一个IP地址：

```
Device:/> set Address IP4Address wan_gw Address=10.5.4.1
```

现在，使用这个对象为 If2 接口来设置网关，这个接口被用于连接到ISP：

```
Device:/> set Interface Ethernet If2 DefaultGateway=wan_gw
```

接下来，设置IP对象 If2_ip ，这是连接到ISP的接口的IP地址：

```
Device:/> set IP4Address If2_ip Address=10.5.4.35
```

设置IP对象 If2_net ，这是连接互联网的接口的IP网络地址：

```
Device:/> set IP4Address If2_net Address=10.5.4.0/24
```

我们推荐通过命令对 If2 接口的属性进行验证：

```
Device:/> show Interface Ethernet If2
```

这条命令的典型输出将与下面的信息类似：

```
                  Property  Value
 -------------------------  -------------------------
                      Name:  If2
                        IP:  If2_ip
                   Network:  If2_net
           DefaultGateway:  wan_gw
                Broadcast:  10.5.4.255
                PrivateIP:  <empty>
                    NOCHB:  <empty>
                      MTU:  1500
                   Metric:  100
              DHCPEnabled:  No
            EthernetDevice:  0:If2  1:<empty>
          AutoSwitchRoute:  No
AutoInterfaceNetworkRoute:  Yes
  AutoDefaultGatewayRoute:  Yes
  ReceiveMulticastTraffic:  Auto
     MemberOfRoutingTable:  All
                 Comments:  <empty>
```

在这个接口上设置缺省网关还具有额外的效果，那就是CorePlus将自动地在缺省的 main 路由表创建一条路由，表明这个接口可以连接到 all-nets 这样的网络。这意味着我们无需明确创建这条缺省路由。

尽管一条 all-nets 路由已被自动创建，但仍然没有数据流可以在没有 IP 规则明确允许哪些数据流可以通过的情况下流经Clavister安全网关。让我们假设我们想要允许web浏览，这种浏览是从连接在 If3 接口上的受保护的网络If3_net 到互联网的。一条简单的规则即可完成这样的目的，其 动作 为 Allow ，下面介绍其命令序列。

首先，我们必须改变当前CLI的上下文到名为 main 的 IP规则集 ，命令如下：

```
Device:/> cc IPRuleSet main
```

缺省情况下，有一个名为 main 的主规则集，因此我们也可以创建另一个IP规则集。要注意的是，如果创建了另一个IP规则集，就需要把CLI提示符改变到正确的上下文：

```
Device:/main>
```

现在添加一条IP规则，名为 lan_to_wan ，以允许数据流到达公共互联网：

```
Device:/main> add IPRule name=lan_to_wan
                Action=Allow SourceInterface=If3
                SourceNetwork=If3_net
                DestinationInterface=If2
                DestinationNetwork=all-nets
                Service=http-all
```

如果内网中的主机都具有公有的IP地址，那么这条IP规则就是正确的。但在绝大多数环境中不太现实，因为内部主机一般都配置的是私有的IP地址。在这个例子中，我们必须使用NAT来向外部发送数据流，此时，源IP地址就会被转换成为连接到ISP的接口的接口的IP。要实现此目的，我们只需简单地把上述命令中的 动作 由 Allow 改变为 NAT即可：

```
Device:/main> add IPRule name=lan_to_wan
                Action=NAT SourceInterface=If3
                SourceNetwork=If3_net
                DestinationInterface=If2
                DestinationNetwork=all-nets
                Service=http-all
```

在这条IP规则中所使用的服务为 http-all ，这将允许绝大多数的网络浏览，但不包括DNS协议，因此无法把URL解析成IP地址。要解决这个问题，可以在上面的规则中使用自定义服务，这个自定义的服务为 http-all 和 dns-all 的组合。然后，推荐的方法是提供更高的配置明确性，为DNS另行创建一条IP规则：

```
Device:/main> add IPRule name=lan_to_wan_dns
                Action=NAT SourceInterface=If3
                SourceNetwork=If3_net
                DestinationInterface=If2
                DestinationNetwork=all-nets
                Service=dns-all
```

建议在CorePlus中最少定义一台DNS服务器。这个DNS服务器或服务器组（最大可配置三台）将被用于CorePlus自身对一些URL的解析，特别是在配置中指定了URL而不是IP地址的时候。如果我们假设一个IP地址对象名为 dns1_address 已经被定义了，作为其第一台DNS服务器，那么指定首台DNS服务器的命令就可以是：

```
Device:/> set DNS DNSServer1=dns1_address
```

假设第二个名为 dns2_address 的IP地址对象已被定义，那么指定第二台DNS服务器的命令如下：

```
Device:/> set DNS DNSServer2=dns2_address
```

B. DHCP - 自动配置

所有必需的IP地址都可以自动从ISP的DHCP服务器获得，只需启用连接到ISP的接口上的DNSP选项即可。如果启用了DHCP的这个接口为 If2 ，那么命令就可以是：

```
Device:/> set Interface Ethernet If2 DHCPEnabled=Yes
```

一旦通过DHCP获得了所需的IP地址，CorePlus就会使用这些信息来设置地址薄中的相关的地址对象。

为了使CorePlus可以知道在哪个接口上可以找到公共互联网，同时也需要添加一条 路由到CorePlus的 main 路由表中，这条路由指定了 all-nets 这样的网络可以在连接到ISP的那个接口上被找到，并且这条路由同样也必须具有正确的 缺省网关 IP地址。这条 all-nets 路由会在DHCP地址获取过程中自动被CorePlus添加。一个接口的自动路由生成也可以被手动地启用或禁用。

在所有IP地址都通过DHCP被设置，并且all-nets路由被添加之后，到达互联网的连接就被配置完成了，但是不会有数据流入或流出到互联网，因为现在还没有定义允许流入或流出的IP规则。如同在前面的选项（A）
中所进行的操作一样，我们必须手动定义一条IP规则来允许来自一个指定的源接口和源网络（在这个例子中，网络为 If3_net ，接口为 If3） 数据流通过目标接口 If2 到达目标网络 all-nets 。

C. PPPoE设置

在PPPoE环境下，就要在连接到ISP的接口上创建PPPoE通道接口。这个例子中的接口 If2 ，假设它就是要被连接到ISP的那个接口，下面的命令显示了在这个接口上创建一个PPPoE通道对象，其名称 wan_ppoe ：

```
Device:/> add Interface PPPoETunnel wan_ppoe
               EthernetInterface=If2 username=pppoe_username
               Password=pppoe_password Network=all-nets
```

您的ISP将为 pppoe_username 和 pppoe_password 提供正确的值。

您的ISP将为上面的对话框中的 pppoe_username 和 pppoe_password 提供正确的值。

PPPoE通道接口现在就可以被完全作为一个物理接口，被使用于CorePlus规则集中的不同策略了。

同样，这里也要有一条与PPPoE通道相关的路由，以允许数据流通过，并且这条路由会在通道定义的时候被自动添加到 main 路由表中。如果PPPoE通道对象被删除，这条路由也就会被自动删除。

在此刻，仍然不会有数据流流过此通道，因为没有定义IP规则来允许这些数据流。如同在上面的选项 A
中所做的那产，我们必须定义一条IP规则，它将允许来自特定的源接口和源网络（在这个例子中，网络为 If3_net ，接口为 If3）的数据流通过目标接口，也就是我们已定义的PPPoE通道到达all-nets这样的目标网络。

D. PPTP设置

在PPTP环境中，首先要创建PPTP通道接口。假设我们要创建一个名为 wan_pptp 的PPTP通道对象连接到远程端点 10.5.4.1 ：

```
Device:/> add Interface L2TPClient wan_pptp Network=all-nets
               username=pptp_username Password=pptp_password
               RemoteEndpoint=10.5.4.1 TunnelProtocol=PPTP
```

您的ISP将为您提供正确的 pptp_username 、 pptp_password 的值以及正确的远程端点。

您的ISP将为您提供正确的 pptp_username、 pptp_password 的值以及正确的远程端点。在定义这个通道的时候并没有指定具体的接口，这是因为这将由CorePlus通过在自己的路由表中查找 远程端点 的IP地址来判断。

现在PPTP客户端接口就可以被完全作为一个物理接口，由CorePlus的规则集中的各种策略来使用了。

同样，这里也要有一条与PPTP通道相适应的路由来允许数据流通过，这条路由会在通道被定义的时候被自动地添加到 main 路由表中。这条路由指定的目标网络为 Remote Network ，而用于访问公共互联网的路由的目标网络应该为 all-nets。

所有这些自动添加的路由，在PPTP通道被删除的时候都会被自动删除。

此时，仍然不会有数据流可以通过这个通道，因为没有定义IP规则来允许这样的数据流通过。如同在选项 A 中所做的一样，我们必须定义一条IP规则来允许来自源接口和源网络（在这个例子中，网络为 If3_net ，接口为 If3）的数据流通过我们定义的PPTP这个目标接口到达目标网络 all-nets 。

激活和提交更改

在完成了对CorePlus的配置的更改之后，这些更改将被保存为一个新的配置，但不会被激活。要激活所有自最后一次激活以来所做的新的配置的更改，就必须使用下面的命令：

```
Device:/> activate
```

尽管新配置现在已被激活，但它不能成为永久性被激活的配置，除非在 激活

后的30秒钟之内发布下面的命令：

```
Device:/> commit
```

要使用两条命令的主要原因是防止配置意外地把管理人员锁在外部。如果被锁在外面的情况确实发生了，那么第二条命令将不会被收到，因此，CorePlus将在30秒钟（这个时间段可以被更改）之后把配置恢复到初始的配置。

DHCP服务器设置

如果Clavister安全网关要作为一个DHCP服务器，那以就要通过下面的方式来设置：

首先要定义一个IP地址对象，它包含了要向用户分配的地址范围。在这里，我们将使用 192.168.1.10-192.168.1.20 这样的IP范围作来示例，这个DHCP服务器被配置在 If3 接口上，这个接口连接到受保护的网络 If3_net。

```
Device:/> add Address IP4Address dhcp_range
               Address=192.168.1.10-192.168.1.20
```

这样，DHCP服务器就可以通过这个IP地址对象在适当的接口上配置完成了。在这个例子中，我们把创建的这个DHCP服务器对象称为 dhcp_lan ，并假设DHCP服务器将运行在 If3 这个接口上：

```
Device:/> add DHCPServer dhcp_lan IPAddressPool=dhcp_range
               Interface=If3 Netmask=255.255.255.0
               DefaultGateway=If3_ip
               DNS1=dns1_address
```

非常重要的一点就是要为DHCP服务器指定 缺省网关 ，因为这个缺省网关将要被发布给位于内部网络中的DHCP客户端，这样它们就可以知道在哪里可以找到公共互联网了。缺省网关一般都是DHCP服务器在其上运行的接口的地址。在这个例子中，就是 If3_ip。

NTP服务器设置

网络时间协议 （NTP） 服务器可以可选性地进行配置，以维护系统的日期和时间的准确性。下面的命令用于设置和两台NTP服务器的时间同步，这两台时间服务器中的一台的主机名为 pool.ntp.org ，另一台的IP地址为 10.5.4.76 ：

```
Device:/> set DateTime TimeSyncEnable=Yes
               TimeSyncServer1=dns:pool.ntp.org
               TimeSyncServer2=10.5.4.76
```

主机名前所加的前缀 dns: 是为了表示其后的内容必须被DNS服务器（这是在CLI中使用命令时的一个约定）解析为一个IP地址。

Syslog服务器设置

虽然有可能日志已被启用，但仍然不会有日志消息被捕获，除非设置了一台服务器来接收这些日志，Syslog 就是最常用的一种服务器类型。如果Syslog服务器的地址为 195.11.22.55 那么创建一个名为 my_syslog 的日志接收器对象来接收日志的命令就可以是：

```
Device:/> add LogReceiverSyslog my_syslog IPAddress=195.11.22.55
```

允许ICMP Ping 请求

作为设置IP规则的一个更进一步的例子，允许ICMP Ping 通过Clavister安全网关就显得非常有用。如同我们在前面讨论的那样，CorePlus会丢弃所有的数据包，除非有一条IP规则明确地允许了这样的数据包。让我们假设我们希望允许内部的 If3_net

网络中的计算机使用ICMP协议去ping外部的主机。允许此操作的命令在下面介绍。

首先，我们必须改变当前的CLI上下文到名为 main 的 IP规则集 ，命令如下：

```
Device:/> cc IPRuleSet main
```

接下来来添加一条名为 allow_ping_outbound 的IP规则来允许ICMP ping通过：

```
Device:/main> add IPRule name=allow_ping_outbound
                Action=NAT SourceInterface=If3
                SourceNetwork=If3_net
                DestinationInterface=If2
                DestinationNetwork=all-nets
                Service=ping-outbound
```

再一次，我们使用 NAT 来作为这条IP规则的动作，这是因为受保护的本地主机都只有私有IP地址。ICMP请求将被从Clavister安全网关发出，其源地址为连接到ISP的接口的IP地址。进行响应的主机将返回ICMP应答给这个唯一的IP地址，然后CorePlus将转发响应到正确的私有的IP地址。

添加一条Dorp All规则

IP规则集的扫描是一种自顶向下的方式。如果 没有 为要新建的连接找到匹配的IP规则，那么，缺省规则
就会被触发。这条规则是隐藏的，并且不可以被改变，并且其动作为丢弃所有类似的数据流，并为这种丢弃动作生成一条日志消息。

为了获得对所丢弃的数据流而生成的日志的控制权，推荐创建一条全部丢弃的规则作为 main IP规则集中的最后一条。这条规则的 动作 为 Drop ，其源和目标网络需要被设置为 all-nets ，并且源和目标接口需要被设置为 any。

这条规则的服务也必须同时被指定为 all_services ，这样才可以捕获所有的数据流。创建这样一条规则的命令为：

```
Device:/main> add IPRule name=drop_all
                Action=Drop SourceInterface=any
                SourceNetwork=any
                DestinationInterface=any
                DestinationNetwork=all-nets
                Service=all_services
```

上传许可证

如果没有加载有效的许可证，CorePlus将运行在 演示模式 ，这意味着它将在正常启动2小时后停止运行。要解除这个限制，就必须上传一个有效的许可证到Clavister安全网关。

要达到此目的，请您按照 第 3.2 节 “Web界面和向导设置”中的最后一部分所描述的，下载一个许可证。使用一个 Secure Copy （SCP）客户端（参阅CorePlus管理员手册以获取更多关于SCP使用的信息）直接上传这个许可证到CorePlus。一旦许可证的上传完成，2小的限制就会被删除，并且CorePlus将会在此许可证的约束条件的限制下进行工作。

3.5. 对设置进行排错

这部分附加内容的目的是处理连接到一个管理工作站到一台Clavister安全网关时可能发生的连接问题。

如果在Clavister安全网关加电，并且CorePlus已经启动后，管理接口无响应，那么就可以通过几个简单的步骤来排除基本的连接问题：

1. 检查是否使用的是正确的接口。

最明显的问题就是使用了错误的接口以进行管理工作站的初始的连接。只有CorePlus首次启动时找到的第一个接口才可以被使用来进行初始的基于浏览器的连接。

2. 检查工作站的IP地址配置是否正确。

第二个最明显的问题就是运行web浏览器的管理工作站的IP地址没有被正确地配置。

3. 使用 ifstat CLI 命令。

为了更进一步地检查连接问题，可以在CorePlus启动后使用VMware控制台。当您在控制台中按下回车键时，CorePlus将用一个标准的CLI提示符来响应。现在，请输入下面的命令几次：

```
Device:/> ifstat <if-name>
```

参数 <if-name> 是CorePlus中管理接口的名称。在缺省情况下，它就是VMware的 If1 接口。这个命令将显示与这个接口相关的一些计数器信息。而 ifstat 命令则可以显示所有VMware接口的名称列表。

如果 Input 结果中的硬件部分的输入计数器并不增加，那么问题就很有可能出在线缆上。然而，也有可能是因为这些数据包一开始就没有到达Clavister安全网关。如果有可能，可以使用一些抓包工具来进行确认。

如果 Input 计数器持续增加，那么管理接口就有可能没有被正确地连接到物理网络中。这也有可能是所连接的主机或路由器中存在不正确的路由信息而导致的。

4. 使用 arpsnoop CLI 命令。

最后的一个诊断测试就是试一下使用这条控制台命令：

```
Device:/> arpsnoop -all
```

这将显示不同接口上所接收到的 ARP 包，这就可以被用来确认各个接口上的连接是否正确。

第 4 章 许可证

每台运行在VMware上的虚拟的CorePlus都需要一个唯一与其相关的许可证文件（.lic）。您可以访问Clavister网站里的 许可证中心 ，并选择 注册新的许可证，然后将其下载到本地磁盘。然后这个下载好的许可证文件就可以被上传到虚拟的Clavister安全网关了。

获取一个许可证

要获取一个许可证，许可证中心将需要您输入一个唯一的 注册密钥，这个密钥（密钥在有些情况下也被称为 许可证号）在您完成采购之后，由Clavister来提供。

在获取一个许可证的时候，许可证中心也将需要您提供一个与某个虚拟的机器的虚拟以太网接口相关的MAC地址。VMware为每台虚拟机上的虚拟接口分配唯一的虚拟MAC地址，这些MAC地址可以通过首次使用CorePlus的控制台命令来获得：

```
Device:/> ifstat
```

这个命令将会给出虚拟接口名称的列表。要获得任意一个接口的MAC地址，请使用命令：

```
Device:/> ifstat <interface_name>
```

MAC地址的字段名称 HW address。

检查许可证内容

）的内容。用于VMware的CorePlus的许可
可以在一个标准的文本器中检查一个Clavister许可证（.lic证包含下面一行：

```
Virtual Hardware: Yes
```

许可证的内容同时也指定了在这台虚拟机器上可以有多少个可用的虚拟接口。这个缺省值可以通过购买合适的许可证来进行升级。

上传许可证

把用于VMware的CorePlus的许可证上传到一个已安装的虚拟CorePlus上的方法和上传到普通的非虚拟机器上的方法是一样的。在Web界面的菜单栏中，选择 维护 > 更新 ，然后点击 浏览 按钮，选择要上传的许可证文件，然后将其上传。一旦完一个正确的许可证被上传，演示模式就会被结束，同时，CorePlus将接受按照许可证的限制性条目的约束。

VMware和CorePlus的锁定模式

当CorePlus运行在演示模式（也就是说，没有有效的许可证）两个小时之后，它将进 锁定模式。

在VMware上运行的CorePlus进入了 锁定模式之后，它将消耗所有的VMware资源。一旦这种情况发生，就需要关闭CorePlus虚拟机实例，因为不能对CorePlus本身进行更进一步的操作，除非它被重新启动。换句话来说，一旦CorePlus进入 锁定模式，重新启动CorePlus就 只能 通过VMware的管理接口来完成了。

关于CorePlus许可证的常规信息可以在 CorePlus Administrators Guide 中找到。

第 5 章 系统管理

VMware上的升级

在VMware上运行CorePlus的时候，对CorePlus的升级可以像在一台单独的物理的计算机上的升级一样，只需在正常的CorePlus的用户界面中通过安装升级包就可完成升级过程。

虚拟网络的性能

在使用一个VMware虚拟网络的时候，如果使用VMware的 自定义（非桥接）模式通过一个虚拟网络把一个虚拟的接口连接到另一个虚拟的接口，数据流的吞吐量将会有少许降低。这是因为处理能力的一部分还要被用于实现虚拟的网络。

要避免这种性能的损失以增加吞吐量使其达到“线速”，推荐使用VMware的 桥接模式来把CorePlus的虚拟接口直接连接到物理的以太网接口。

资源分配

VMware为管理人员提供了为每个虚拟进程保证以及限制资源分配的选项。对一台单独的虚拟安全网关进行资源保证非常重要，这可以避免其它的虚拟安全网关消耗光了所有可用的资源，因为这些其它的虚拟安全网关可能正在被持续攻击或进程被冻结。出于同样的原因，限制单台虚拟安全网关所消耗的资源也是值得推荐的。

多核处理

如果是在多核处理器上运行VMware，可以强制一台虚拟机器使用单独的核以改善性能。

在Microsoft Windows上运行标准的VMware的时候，Windows的set affinity命令可以用于实现此目的。这个命令的结果就是在任务管理器中显示一个处理器的列表，然后右击想要为其分配单独的核的特定的VMware进程。

如果是在ESX或ESXi上，VMware就是基础的操作系统了，通过VMware管理界面就可以强制一台虚拟机器来使用一个单独的核了。

增加虚拟接口的数量

下面的步骤可以用来为CorePlus增加可用的虚拟接口的数量：

1. 在VMware中添加额外的虚拟接口。所胡虚拟接口都必须配置为一个 E1000 设备。

   VMware产品版本自身可能会有一个可以添加的最大虚拟接口数，这个因素可能会对我们的添加构成限制。

   在VMware中添加一个虚拟接口的时候，要确保在启动虚拟机器之前，虚拟机属性 中的相应接口的加电时即连接 选项被选中。

2. 获取一个新的许可证，以允许有额外的接口，并把新的许可证上传给CorePlus。

3. 如果CorePlus仍然没有检测到所有的接口，请运行CLI命令 pciscan，就可以把任何新接口都添加到配置中。完整的CLI命令为：

   ```
   Device:/> pciscan -cfgupdate
   ```

   下图是一个控制台的输出示例，它显示了 pciscan 命令被用于添加一个新的 If4 接口到CorePlus的配置。

4. 接下来请输入CLI命令 activate ，以及 commit ，以保存更新后的配置。

第 6 章 隔离VLAN

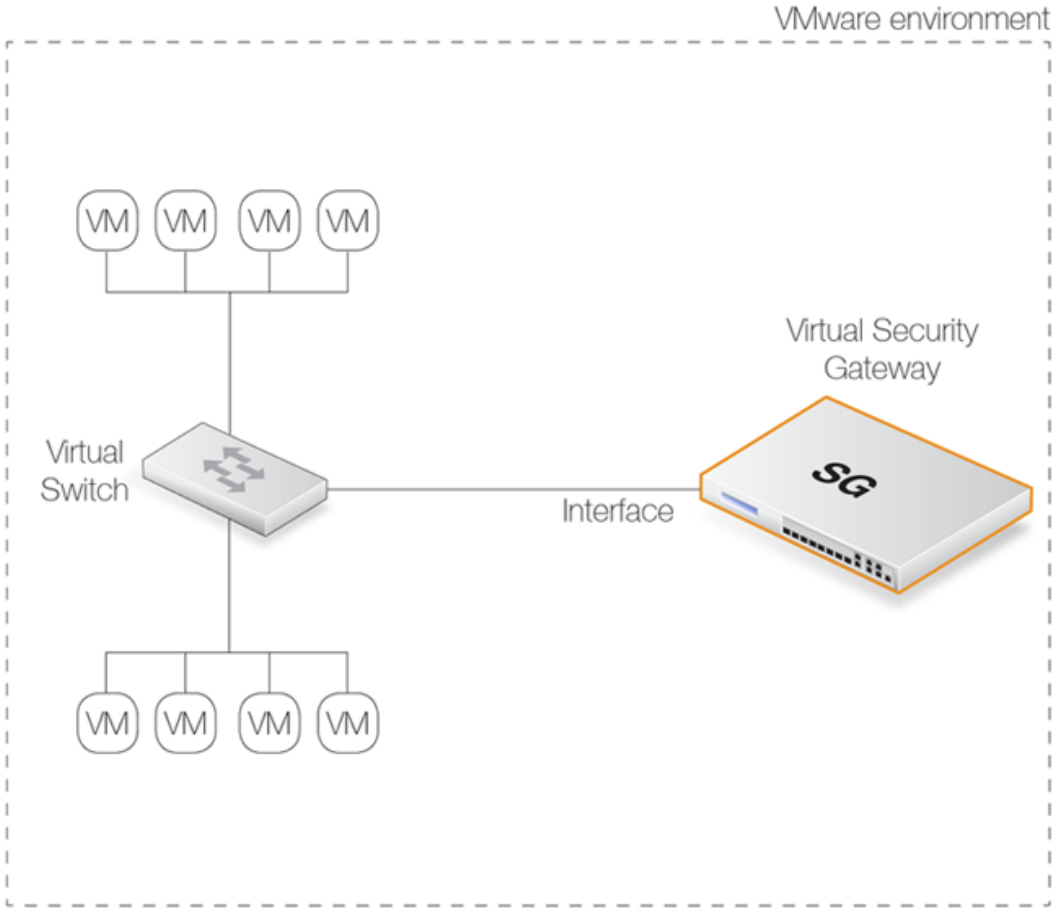
问题

在VMware的ESX或ESXi的现实安装实例中，有可能有许多台虚拟机器的实例，同时我们想要把这些机器都连接到一个单独的 虚拟网络中。为了实现此目标，我们把它们定义到一个虚拟 交换机上的一个单独的 端口组 中，同时，这个端口组具有一个特定的 VLAN ID。这样，虚拟机就可以被连接到一个单独的虚拟网络中了。

假设我们现在有第二组虚拟机器，它们也要用类似的方法通过另一个端口组来连接到相同的虚拟交换机。

来自这两个组的所有虚拟机器有可能需要和一台虚拟的Clavister安全网关进行通信。那么这台安全网关也需要通过这台交换机上的另一个端口组连接到这台虚拟交换机。这样的安排在下面的图中进行详细解释。标记为“VM”的方框代表了不同的虚拟机器。

图 6.1. 连接VLAN

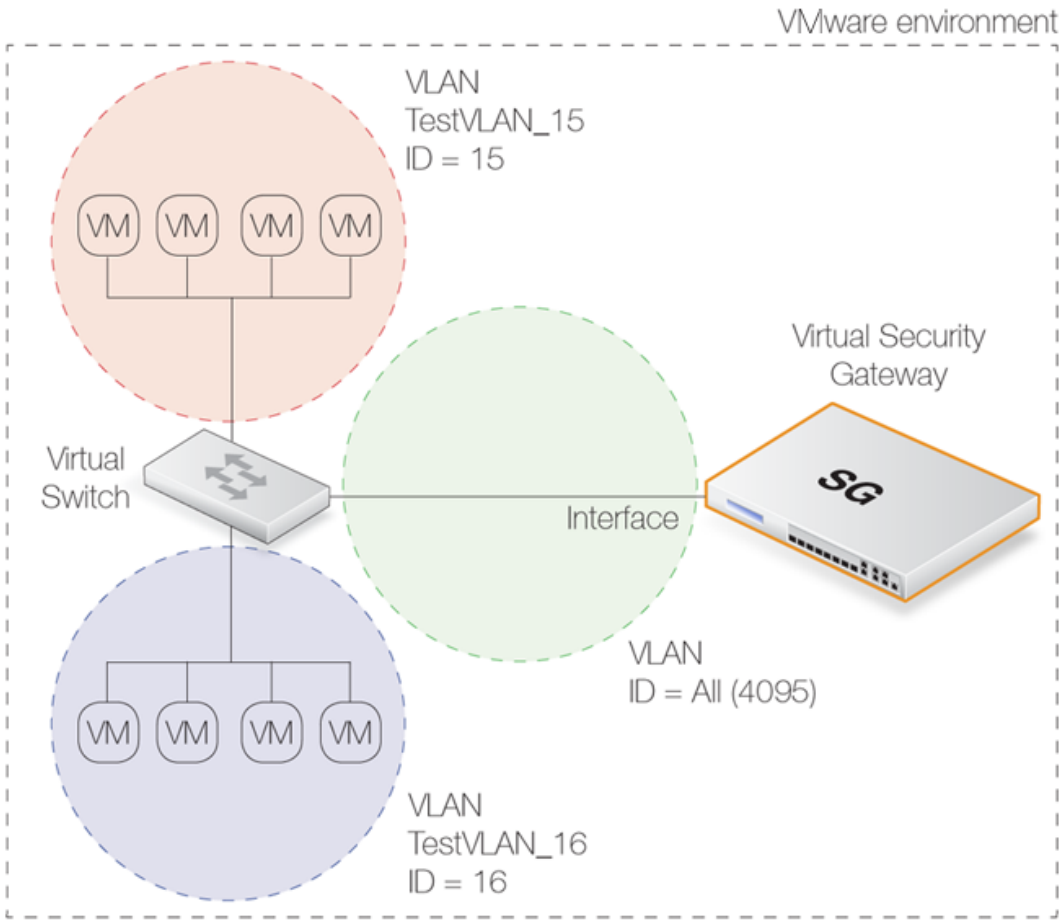


虚拟交换机将照例允许这两组虚拟机器互相通信。然而，最常见的需求却是要求它们应该通过虚拟的Clavister安全网关来进行通信，这样，所有的数据流才可以完全处于CorePlus的控制之下。

解决方案

实现隔离的办法就是让两个虚拟机器组使用不同的VLAN ID，并通过第三个VLAN连接到Clavister安全网关。下图详细描述了这种部署。

图 6.2. 隔离VLAN



该方案的关键点：

1. 分别用于两组虚拟机器的端口组必须被指定为不同的VLAN ID。

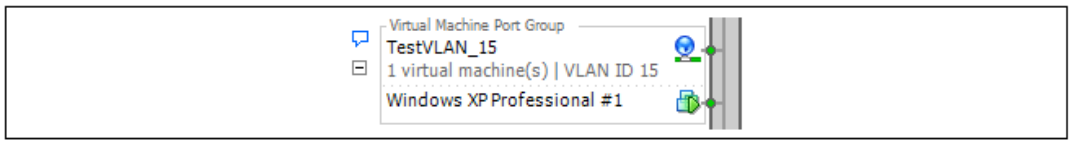
   上面的图示中的两个虚拟机器网络中的一个被设置为VLAN，名称为 TestVLAN_15 ，VLAN ID为15。另外的一个网络则被设置为名为 TestVLAN_16 ，其VLAN ID为16。使用不同ID的意义在于两个VLAN不能互相通信。

2. 连接到安全网关的虚拟交换机上的虚拟机器端口组应该允许所有VLAN ID存在于这个端口组中。通过在基础架构客户端中把VLAN ID指定为 4095 （这个ID在客户端中显示为VLAN ID ）即可。在安全网关上，只有与这个端口组相连接的接口才应该存在于这个接口组中，作为一ALL个VLAN trunk （所有VLAN ID都可以存在于这个trunk中）。

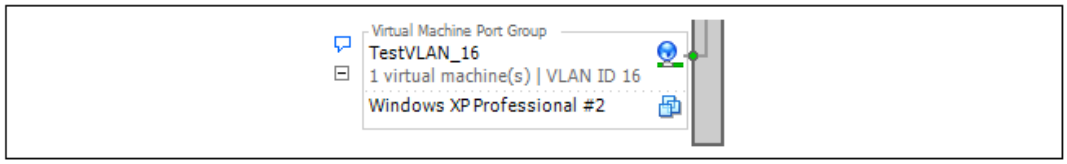
3. 虚拟交换机上的每一个VLAN ID都需要在CorePlus中为所连接的接口定义一个相应的 VLAN 接口，并使其具有相同的VLAN ID。

   换句话来说，就是为VLAN TestVLAN_15 定义一个CorePlus的VLAN接口对象，并使其VLAN ID为 15，并为VLAN TestVLAN_16 创建第二个VLAN接口对象，并指定其VLAN ID为 。两个VLAN接口都被配置在连接到这台虚拟交换机的接口上。这将允许CorePlus与这些不同的V16LAN进行通信。

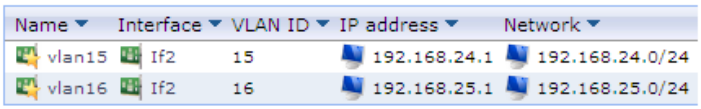
在VMware基础架构客户端中，虚拟交换机将包含两个 虚拟机器端口组，如下面的部分屏幕快照所示。第一个端口组用于 TestVLAN_15：



第二个端口组用于 TestVLAN_16：



下面是屏幕快照的一部分，它显示了通过Web界面查看配置时CorePlus中的VLAN设置。虚拟接口 if2 是连接到虚拟交换机的接口：



Name	Interface	VLAN ID	IP address	Network
vlan15	If2	15	192.168.24.1	192.168.24.0/24
vlan16	If2	16	192.168.25.1	192.168.25.0/24

用于VLAN的IP地址 192.168.24.1 和 192.168.25.1，都是随便选择的内部IP地址。因此，连接到VLAN vlan15 的客户端必须将其缺省网关配置 192.168.24.1。而 vlan16 上的客户端必须将自己的缺省网关配置为 192.168.25.1。

这种方案的优点

使用VLAN的这种方案的关键优点在于，所有在虚拟机器和CorePlus之间流动的数据流都发生在虚拟的VMware网络设置之内，并且无需离开虚拟的环境而进入到“现实世界”。对于性能和控制来说，其好处是不言而喻的。

如果要通过虚拟的Clavister安全网关来访问互联网，那么数据流显然就要离开虚拟环境了。

VMware参考

VMware自身也在其标题为 Fully Collapsed DMZ 一节中对这种方法进行了讨论，文档的标题为 DMZ Virtualization with VMware Infrastructure。这种方法被描述于 “virtualizing the entire DMZ”之中。

第 7 章 创建虚拟机器

通常情况下，无需在VMware上从头创建一台新的虚拟机器，因为可以从Clavister客户服务网站上下载CorePlus，其格式适合于直接导入到VMware，用于自动创建虚拟机。在ESX和ESXi上也可以有另一种方法：

- 从Clavister客户服务网站上下载非VMware软件安装包的标准的CorePlus ISO 文件镜像。
- 创建一台适合运行CorePlus的新的VMware虚拟机器。
- 启动新的虚拟机器。
- 导入 ISO 镜像文件到虚拟机器并启动它。

在下载了 ISO 文件镜像之后，下面的部分对后续的步骤进行描述。

创建一台ESX/ESXi虚拟机器

要为CorePlus创建一台新的虚拟机器，其步骤为：

1. 在基础架构客户端的 Getting started 页中点击 创建一台新的虚拟机器 选项，向导将会启动。
2. 选择 自定义 选项。
3. 给新的虚拟机器指定一个合适的名称。
4. 为虚拟机器选择资源并点击 下一步。资源就是将被用于一个集群中的VMware主机。
5. 选择要使用的数据存储设置。
6. 选择 Guest O/S 为 Other 64 bit。
7. 处理器数量请选择 1。
8. 选择内存大小，不能少于 256 Mbytes 并点击下一步。。所分配的内存可以更大一些，这要取决于您所购买的CorePlus的许可证。
9. 选择要使用的网络适配器。网络适配器就是以后的安全网关的接口。最多可以有4个适配器，但是其类型必须为 E1000。
10. 选择存储适配器类型为 SCSI adaptor bus logic。
11. 创建一个新的虚拟磁盘。
12. 精确设置磁盘容量为2GBytes。
13. 下一步高级选项对话框就会出现。点击 下一步 以跳过。
14. 虚拟机器的配置摘要就会出现。如果检查所有设置都正确，请点 完成 。

导入ISO文件

下一组步骤用于说明如何导入CorePlus的 ISO 文件到新创建的虚拟机器。

1. 在VMware的导航菜单中，选择网络创建的虚拟机器并编辑其设置。
2. 在 硬件 页中，转到 CD/DVD 驱动器 ，并启用 Datastore ISO 文件 选项。
3. 点击 流利 按钮，并选择要导入的CorePlus ISO 文件。

4. 启用 Connect at power on 选项并点击 OK。

启动安全网关

现在启动CorePlus使其运行：

1. 启动虚拟机器并选择 Console 页。
2. 选中 Transfer system from CD项。这将把CorePlus的可执行文件放置到前面创建的虚拟磁盘中。
3. 一个蓝色的控制台屏幕现在就会出现，其中列出了可用的虚拟磁盘。选择前面所创建的磁盘。
4. 在问题 Transfer system to disk? 出现后，输入 Yes。
5. 当 Press any key to reboot 消息出现时，按任意键。

CorePlus现在将在虚拟机器中启动，并将在控制台中显示启动事件序列，而且可以在其中使用CLI命令。

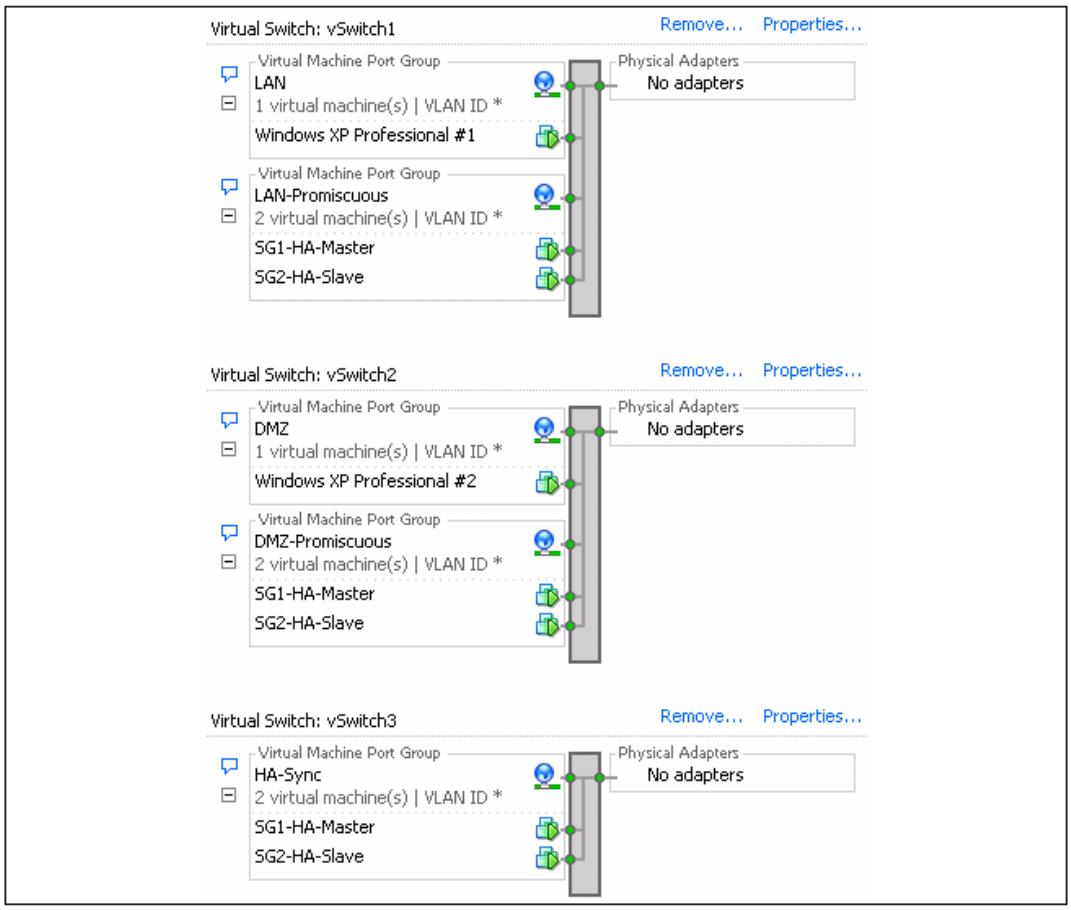
第 8 章 VMware上的HA设置

这一节提供了额外的信息，以用于在VMware上进行正确地HA集群的设置，这需要集群中的两台Clavister安全网关分别运行在不同的VMware虚拟机器上。

按照常规步骤完成两台不同的Clavister安全网关的初始的设置，使它们作为互不相干的两台设备独立工作。在每一台设备上都要运行 HA设置向导 才可以创建HA集群，但在这之前，首先要正确地配置VMware虚拟网络以列举硬件连接，这些连接通常情况下将出现在主设备和从设备中。这一步的关键点在于创建VMware 虚拟交换机，这样，集群中的两台安全网关上相互匹配的接口对才可以通过一台虚拟交换机上的组连接到一起，这台虚拟交换机此时运行在 混杂模式 。

下面是一个屏幕快照，它显示了用于一台ESXi服务器的VMware infrastructure客户端的 配置 一节中的设置：

图 8.1. HA配置中的虚拟交换机的设置



该图显示虚拟交换机1到3的设置。虚拟交换机0没有被显示，因为这是用于管理工作站的。这3台虚拟交换机的目的在下面描述：

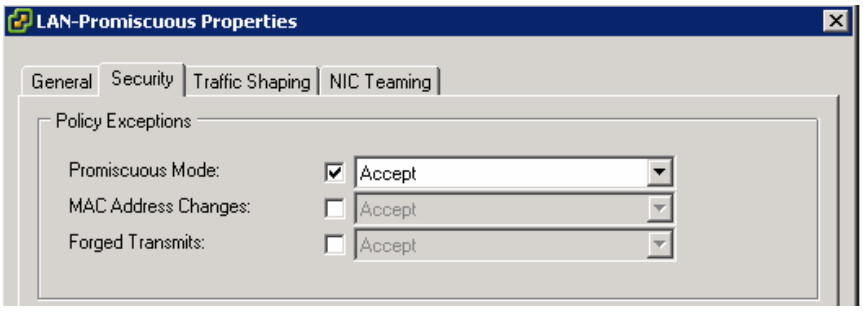
交换机1

如果我们观察屏幕快照中的 交换机1 ，我们就会发现这台交换机里定义了两个组：

- 第一个组为 LAN 组，它把Clavister安全网关外面的普通网络连接到集群的 LAN 接口。
- 第二个组为 LAN-Promiscuous 组，它把两台安全网关上的 LAN

接口连接在一起。正如这个组的名称所指出的，这个组必须运行于 混杂模式，这意味着交换机不使用ARP请求来判断哪台主机位于哪个接口。相反，它通过所有的接口来发送数据流。

图 8.2. 在VMware中设置混杂模式



交换机2

交换机2 的结构和 交换机1 一样，但此时，它是两台安全网关的 DMZ 接口，它们被通过第二个混杂的组连接在一起。如果外部的网络将要通过集群的 DMZ 接口连接到安全网关，那么，就可以通过第一个组来实现这种连接。

交换机3

交换机3 是一台只具有一个组的虚拟交换机。它被用于把每一台安全网关的 Sync 接口连接在一起。

第 9 章 FAQ

本附加内容收集了 日常问答部分中的一些答案，用于帮助解决运行在VMware上的CorePlus的各种问题。

问题汇总

1. CorePlus的2小时演示模式到期，我该怎么办？
2. 在VMware上对CorePlus进行升级有什么特别之处吗？
3. 我如何从VMware的控制台窗口中退出（释放焦点）？
4. 我所有的虚拟接口都必须被配置为E1000 NICs吗？
5. 我该如何管理多台虚拟的安全网关？
6. 我该如何操作才可以改变CorePlus的设备ID？
7. 我该如何隔离不同的虚拟网络？

问答

1. CorePlus的2小时演示模式到期，我该怎么办？

，并对任何操作不进行响应，同时，它将耗尽所有的VMware的资源。在这种情况下，VMware虚拟机器必须被关机，然后再重新启动，2小时之后CorePlus将进入锁定模式这样，CorePlus的重新启动也会使重新进入一个2小的评估期。

2. 在VMware上对CorePlus进行升级有什么特别之处吗？

没有。CorePlus在VMware上的升级操作和它在其它非VMware环境下的操作一样。

3. 我如何从VMware的控制台窗口中退出（释放焦点）？

VMware将一直保持其焦点于控制台窗口中。如需点击控制台窗口以外的目标，请按下组合键 Ctrl-Alt 。

4. 我所有的虚拟接口都必须被配置为E1000 NICs吗？

是的。如果虚拟接口没有被配置为E1000，那么CorePlus将不会使用这个接口。任何所添加的接口都必须被强制为E1000。

5. 我该如何管理多台虚拟的安全网关？

运行于同一台hypervisor上的不同的安全网关上的用于进行管理的虚拟以太网接口的IP地址必须各不相同。

6. 我该如何操作才可以改变CorePlus的设备ID？

由Clavister提供的即用型VMware虚拟机器的镜像都具有相同的 设备ID，这在使用InControl管理客户端的时候会产生问题。要为一台虚拟的安全网关生成一个唯一的ID，请进入到引导菜单，并选择恢复到缺省配置选项。

7. 我该如何隔离不同的虚拟网络？

如果有多组不同的虚拟机器被通过不同的端口组连接到了一个虚拟交换机，可以通过划分VLAN并指定不同的VLAN ID来分享这些不同组的虚拟机器。在 第 6 章 隔离VLAN 中有更进一步的描述。

8. 在重新启动了CorePlus之后，如何分辨哪个网络适配器是新添加的？

在启动虚拟机器之前，在VMware客户端中，转到 虚拟机属性 ，并查看网络适配器以验证 Connect at power on 选项框是否被选中。如果新添加的接口仍然没有被CorePlus检测到，请输入CLI命令：

```
Device:/> pciscan -cfgupdate
```

这将扫描所有的新接口。然后请通过命令来保存配置的更新：

```
Device:/> activate
```

接下来：

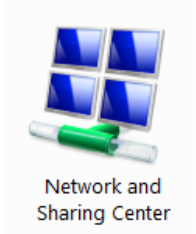
```
Device:/> commit
```

附录 A. Vista的IP设置

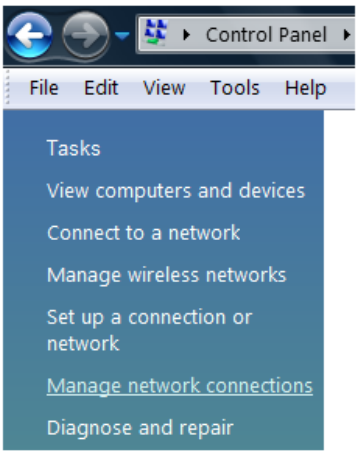
如果一台运行Microsoft Vista的PC机被用作CorePlus的管理工作站，那么这台计算机上连接到Clavister安全网关的接口就必须被配置为属于 192.168.1.0/24 这个网络中的一个IP地址，并且不能与安全网关自己的IP地址192.168.1.1的地址相同。

假设我们要使用 192.168.1.30 这样的地址来管理安全网关，以下的步骤就可以用来在Vista上进行此IP地址的设置：

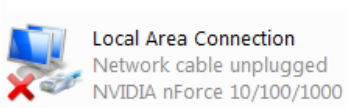
1. 点击Windows的 开始 按钮。
2. 在开始菜单中选择 控制面板 。
3. 在控制面板中选择 网络与共享中心 。



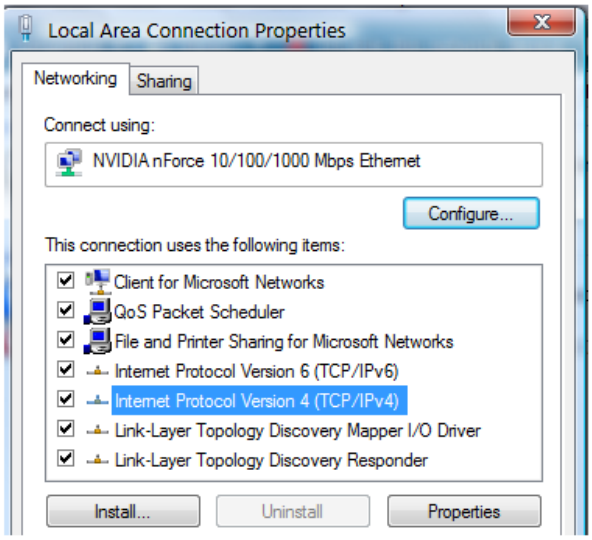
4. 选择 管理网络连接 选项。



5. 以太网接口连接列表就会出现。选择将要连接到安全网关的接口。



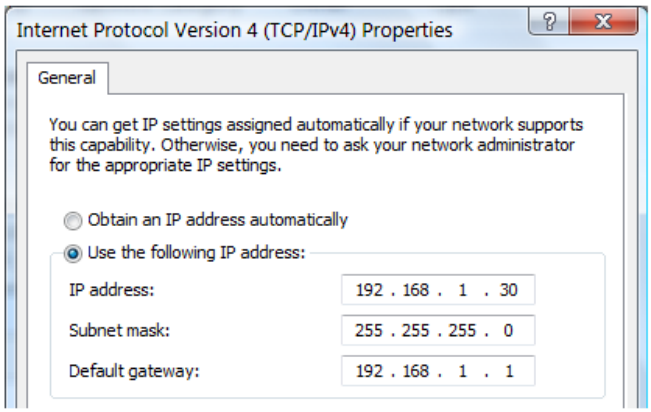
6. 打开所选接口的属性对话框。



选择并显示 互联网协议版本4（TCP/IPv4）的属性。

7. 在属性对话框中，选择 使用下面的IP地址 选项，并输入下面的值：

   - IP地址：192.168.1.30
   - 子网掩码：255.255.255.0
   - 缺省网关：192.168.1.1



DNS地址可以在互联网访问建立之后再行输入。

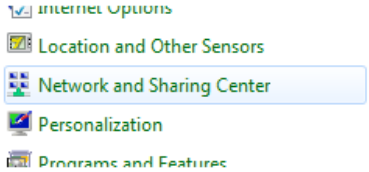
8. 点击 确定 以关闭这个对话框，并关闭自步骤 （1） 以来打开的所有对话框。

附录 B. Windows 7的IP设置

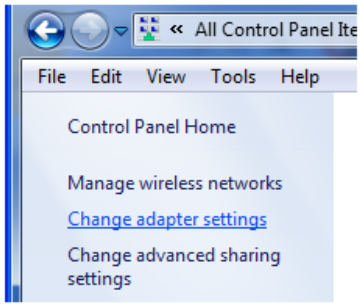
如果一台运行Microsoft Windows 7的PC机被用作CorePlus的管理工作站，那么这台计算机上连接到Clavister安全网关的接口就必须被配置为属于 192.168.1.0/24 这个网络中的一个IP地址，并且不能与安全网关自己的IP地址192.168.1.1的地址相同。

假设我们要使用 192.168.1.30 这样的地址来管理安全网关，以下的步骤就可以用来在Vista上进行此IP地址的设置：

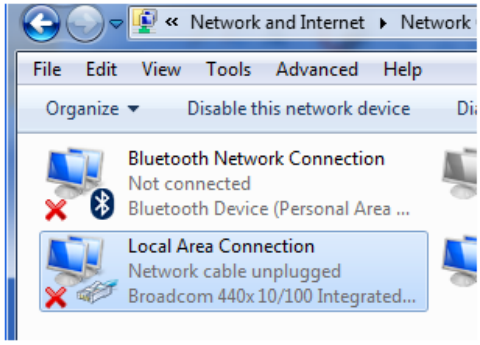
1. 点击Windows的 开始 按钮。
2. 在开始菜单中选择 控制面板 。
3. 在控制面板中选择 网络与共享中心 。



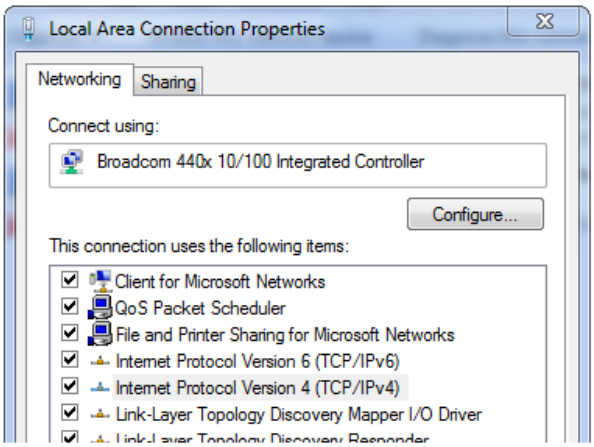
4. 选择 改变适配器设置 选项。



5. 5 适配器列表就会出现，这个列表也将包含以太网接口。选择要连接到安全网关的接口。



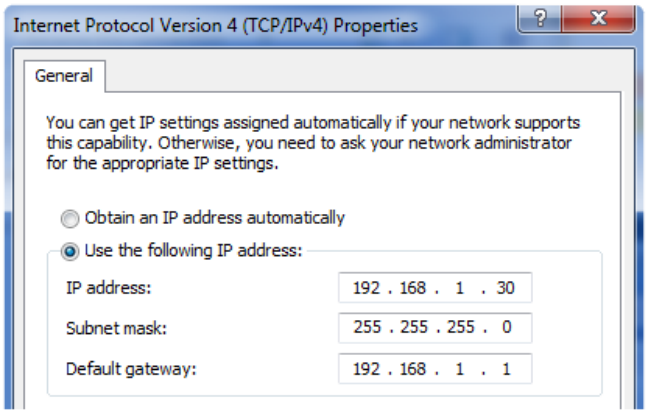
6. 打开所选接口的属性对话框。



选择并显示 互联网协议版本4（TCP/IPv4）的属性。

7. 在属性对话框中，选择 使用下面的IP地址 ，并输入下面的值：

   - IP地址：192.168.1.30
   - 子网掩码：255.255.255.0
   - 缺省网关：192.168.1.1



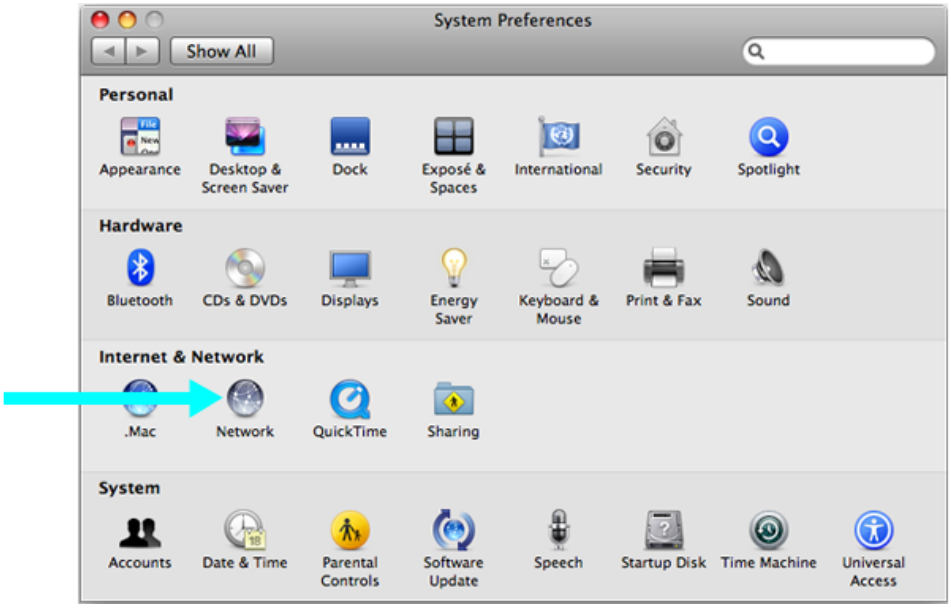
DNS地址可以在互联网访问建立之后再行输入。

8. 点击 确定 以关闭这个对话框，并关闭自步骤 （1） 以来打开的所有对话框。

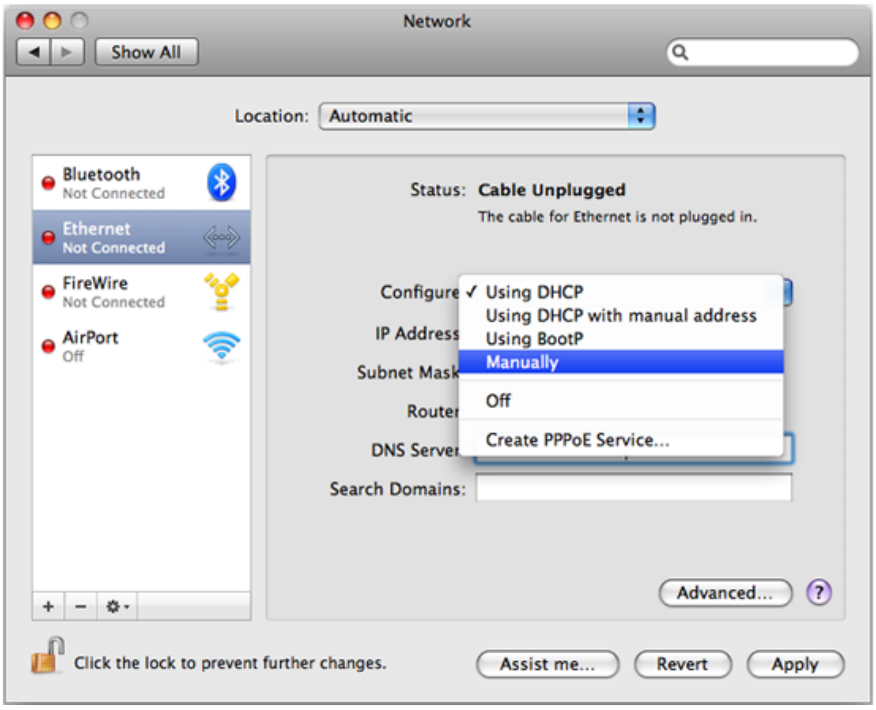
附录 C. Apple Mac的IP设置

Apple
Mac也可以被用作管理工作站以对Clavister安全网关进行初始的设置。要实现此目的，Mac上所选的以太网接口被必须被正确配置一个静态的IP。在Mac的OSX上进行此设置的步骤为：

1. 转到 Apple Menu 并选择 System Preferences 。
2. 点击 Network。

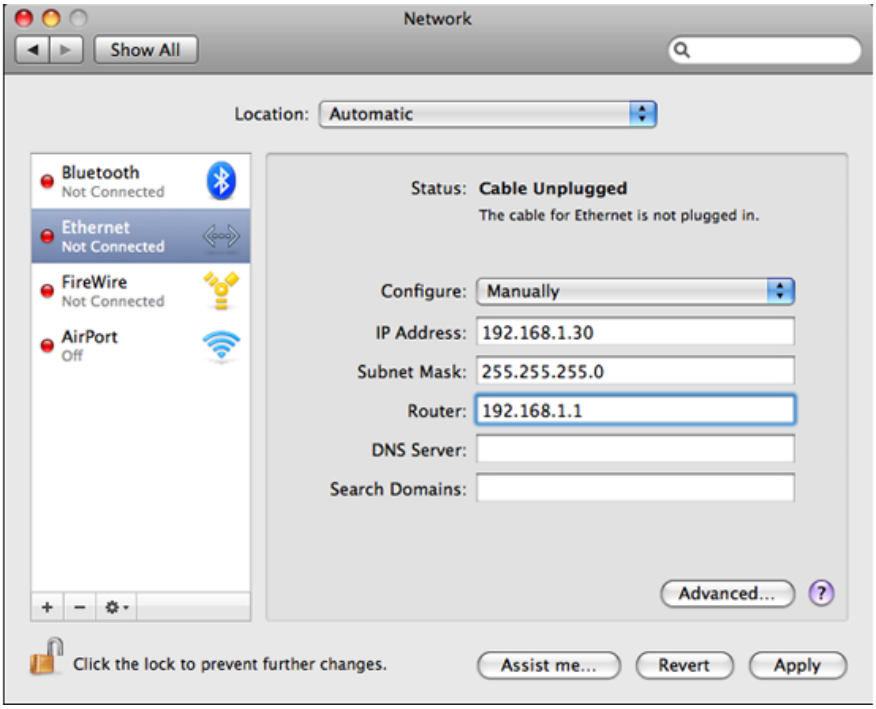


3. 在左侧的菜单上选择 Ethernet 。
4. 在名为 Configure 的下拉式菜单中选择 Manually 。



5. 接下来设置下面的值：

- IP Address:192.168.1.30
- Subnet Mask:255.255.255.0
- Router:192.168.1.1



6. 点击 Apply 来完成静态IP设置。