SAFE VPN

IPSec 虚拟专用网系统介绍

目录

Cisco Systems

Empowering the Internet Generation™

作者简介

Jason halpern 是这本白皮书的主要作者，也是美国加利福尼亚州圣何塞思科总部参考实施项目的首席设计师：Sean Convery 和 Roland Saville 为本文提供了鼎力支持，他们三个人都是有关 VPN 和安全问题的网络专家。

摘要

本文的主要目的是向感兴趣的人士提供设计和实施企业 IP 安全(IPSec)虚拟专用网(VPN)最佳惯例信息资料。适用于大企业的 SAFE 白皮书，以及适用于中小型企业和远程用户网络的 SAFE 白皮书，都可在 SAFE 网站查询到，网址：http://www.cisco.com/go/safe。这些资料旨在为网络安全设计提供最佳惯例信息，包括部分 VPN 配置内容和设计指南。本文就 IPSec VPN 在当今网络中的地位进行了进一步的讨论，对一些特殊设计情况和实质性建议进行了研讨。虽然您在阅读本文时，无需首先阅读两份安全设计资料中的任何一份，但是我们建议您在阅读本文前，首先浏览一下最适合您的网络规模的材料。例如，拥有大型网络的企业可能要首先参考大型企业 SAFE 白皮书。系统实施的结果将把 VPN 会话限在总体安全设计的环境内，SAFE 代表着一种基于系统的安全和 VPN 设计方式。这类方式主要针对的是总体设计目标，并将这些目标转换成相关配置和拓扑结构。SAFE 是在思科及其合作伙伴产品的基础上构建的。

本文首先对体系结构进行了综述，然后就一些尚在研究中的设计问题进行了详细的介绍。文章就下列设计领域展开了详尽论述：

- 远程用户 VPN 设计
- 小型网络 VPN 设计
- 中型网络 VPN 设计
- 大型网络 VPN 设计（带外部网连接）
- 分布式大型网络 VPN 设计

每项设计都拥有多个模块，以解决 VPN 技术各个方面的问题。有关模块的概念在 SAFE 安全白皮书中进行了介绍。各个设计或模块（适用时）所涉及的主题内容列举如下：

- 总体设计最佳惯例
- 高可用性
- 可扩展性
- 性能
- 识别
- 安全管理
- 网址转换（NAT）
- 安全性
- 路由选择
- 外部网情况考虑

设计讨论完毕后，在附录 A 中就 SAFE 的验证实验进行了介绍，这其中包括配置概览。附录 B 是介绍有关 VPN 的重要章节，建议对 VPN 基本概念不十分熟悉的读者，在阅读本文前，首先浏览这一章节。附录 C 收录了本文中所使用的大量技术词汇的定义。

读者对象

虽然本文是一份技术材料，但也可视读者的情况，而阅读不同层次的内容。例如，网络主管可阅读各部分的前言介绍内容，以获得 VPN 设计策略和构思的全面综合信息。网络工程师和设计师可阅读全文，以获得设计信息和详细的威胁因素分析，配备相关设备实际配置快照。由于本文涵盖了多种 VPN 部署情况，首先阅读本文的简介部分，然后，再浏览您欲部署的 VPN 类型，将对您有极大的助益。

说明

本文的前提是您已拥有有关的安全策略。思科公司建议您不要在缺乏有关安全策略的情况下部署 VPN 或任何安全技术。本文假设您了解在您的网络中哪些数据非常敏感，因而在互联网传输过程中需要予以适当保护。虽然网络安全问题在文中有所涉及，但不是本文所要讨论的主要内容，因而未加详述。本文中的安全问题只是在涉及 VPN 技术时，才会予以讨论。有兴趣了解有关网络安全详尽内容的读者，应浏览 SAFE 安全文件，以获得详尽的设计指导，网址：http：//www.cisco.com/go/safe。

遵循本文中的要求无法确保您能获得一个绝对安全的环境，也无法保证您不受到任何攻击。要实现绝对的安全，只能将系统与网络隔离，再把它封闭起来，放在 Fort Knox 的地下室中。这样一来，您的数据就会非常安全，但却无法使用。然而，您可以参考本文和 SAFE 安全文件中的指导，建立一个健全的安全策略，时刻关注黑客和安全社区的最新发展动态，运用有效的管理措施维护和监控所有系统，从而达到理想的安全性能。

虽然本文中包含了有关 VPN 技术多层面的大量详尽内容，但其讨论部分却并非冗长。尤其是，与 VPN 有关的若干技术并未提及。首先，未讨论认证授权(CA)部署。只介绍了识别策略，包括 X509 V3 数字证书，以及其他识别技术。CA 在企业中部署的最佳惯例则未讨论。CA 及其相关部署技术如在本文中详细论述，则本文可能无法充分地描述识别和 VPN 的其他相关领域。此外，由于大多数网络还未部署全功能的 CA 环境，讨论如何在不具备这种环境的情况下安全部署网络更为重要。其次，本文中的 VPN 设计假设客户现场存在 VPN 设备并由客户进行控制。虽然 VPN 如果由电信服务供应商管理，这些拓扑结构就不会有显著的变化，但这种类型的网络管理和配置则有着很大的差别。因而，本文可用于对电信服务供应商的 VPN 服务进行评价，但不可用作外包 VPN 的最佳惯例。第三，围绕有关如何保持 VPN Qos 问题的详细的分析材料，在本文中并未提供。就如何在 VPN 中提供独具特色的服务级别，以及确保可靠的关键任务数据吞吐量而言，Qos 是一个关键组成部分，本文就许多其他重要的设计情况进行了介绍。但是，仅对这些问题进行分析就占用了本文第一版的分配资源。

第四，本文假设当 VPN 被选为两站点间的连接网络时，它是这些站点进行交流的唯一方式。分离隧道可用于非安全站点到站点通信。有关如何利用 IPSec 备份专用 WAN 链路，以及在按需拨号路由选择(DDR)环境中 IPSec 的使用未做说明。所提供的拓扑结构可用于备份，尽管周围网络中的路由选择和其他内容在这里未做介绍。第五，SAFE 使用了思科公司及其合作伙伴的产品，但是，本文并未专门指定产品名称，部件是根据功能，而非型号或名称进行介绍的。

在 SAFE 验证期间，真正的产品是按本文中所描述的实际网络实施进行配置的。实验和结果，以及实验的配置快照都包含在附录 A“验证实验”中。最后，本文并未对动态隧道端点搜索机制进行分析或讨论。在部分或全部网状网络中，动态对等搜索机制发挥了最佳性能，在这种网络中，偶尔会要求分支到分支连接。由于这些网络类型在大规模部署中从未部署过，而且问题迄今为止还不十分清楚，本文就那些更多依靠静态中心辐射式网络设计、而非动态的部分或全部网状网络设计的网络进行了讨论。

本文中“黑客”一词是指恶意试图获得未授权网络资源接入的个人。虽然，“破坏者”一词更适合这类个人，但这里所采用的黑客一词更方便阅读。

体系结构概述

设计基础

SAFE VPN 尽可能贴切地模拟了当今网络的功能需求。根据网络所需功能的不同，实施决策也会有所变化。但是，按优先顺序排列的下列设计目标，将引导决策的确立过程。

- 安全连接
- 可靠性、性能和可扩展性
- 高可用性选项
- VPN 用户和设备验证
- 安全管理
- IPSec 使用前后的安全和攻击减缓

首先，也是最重要的一点，SAFE VPN 需要为要求配备它的场所和用户提供专用、独特的通讯手段。它必须以安全的方式执行上述功能，并与此同时，尽可能多地保留传统的专用 WAN 连接特性。它必须可在 SAFE 安全体系结构的基础上，与现行网络设计集成。

SAFE VPN 准则

下列准则代表了影响着 SAFE VPN 内几乎每一种设计的出色设计构思，它们收入在文章中的起始部分，因而避免了在文章后部的多次重复提及。SAFE VPN 的前提是遵循原始 SAFE 白皮书的安全准则。但是，与从前的 SAFE 安全资料相比，它更加依赖资料中有关准则的部分。虽然，VPN 设计因企业规模而有着很大差异，下面的最佳惯例却基本相同。因此，有关的设计讨论也较为近似。在准则中，假计用户和网站是您所在企业的成员并在您的控制域内；对外部网的安全性进行了单独的设计讨论。在阅读了 VPN 准则之后，作者意在使您得出与他相同的结论。

识别和 IPSec 接入控制

在当今的站点到站点远程接入 VPN 中，设备如何以一种安全可控的方式进行识别是一个重要问题。在远程接入 VPN 中，出现了用户验证和设备验证。当远程设备验证时，一些接入控制级别需予以设置，以便只允许隧道中的数据出现。

设备验证采用了预共享密钥或数字证书，以提供设备身份，预共享密钥有三种：通配符、分组和独立。独立预共享密钥与某一 IP 地址有关，分组预共享密钥与一组名称有关，仅适用于当今的远程接入。通配符预共享密钥与确定某一对等身份的独立信息无关。任何拥有该密钥的设备都可成功地通过验证。因此，通配符共享密钥不可应用于站点到站点设备验证。作者认为这样做会带来问题。当使用通配符预共享密钥时，网络中的每台设备都使用同一密钥。如果网络中的一台设备出现问题，由于通配符预共享密钥已确定，因而也会危及所有设备。被破坏的预共享密钥易于遭到中间人攻击。凭借密钥，黑客可与您的网络中任何远程站点接入策略允许的设备连接。动态加密映射可通过接受任意 IP 地址的互联网密钥交换(IKE)，促进这种攻击。在最低限度下，您也应该考虑在两设备间使用独立预共享密钥。但是，很明显，这种设备在大型网络中无法扩展。考虑到预共享密钥的严格性以及更换的频率，它们不可能提供严格的设备验证。

数字证书与独立预共享密钥相比，可更理想地扩展，因为它允许一台设备验证其他设备，但不具备通配符密钥的安全特性。数字证书与 IP 地址无关，而是与企业 CA 认可的设备上独特的标志信息有关。如果黑客入侵或窃取了一台带数字证书的设备，管理员可废除该数字证书。并公布一个新的证书废除名单(CRL)，以通知所有其他设备。CRL 包含经 CA 认可的废除证书名单。当一台设备接收到隧道建立申请，并将数字证书用作身份识别证据时，该设备会针对 CRL 对证书进行核查。在隧道验证和建立过程中，生成数字证书或废除已接收证书的设备，必须了解确切的时间(最好为协调通用时间[UTC])。时间也用于确定 CRL 何时过期，以便获取新 CRL。虽然，可选择是否对核查 CRL 进行配置，当数字证书部署时，远程和头端设备必须始终配备这项功能。与预共享密钥相比，这是数字证书唯一的废除方案，前者只是简单地从未受到侵害的设备中清除。

数字证书也提供了更多的密钥加密(更多种子位)、公共/专用密钥对老化和非拒绝模式。但是，数字证书鉴于其特性的复杂性，的确要求额外的管理资源用于部署和管理。采用第三方管理 CA 以及企业管理 CA 可能会对推进外部网 VPN 的部署有帮助。如果 VPN 的规模超出 20 台设备，或甚至很快就有严格的设备验证需求，那么，可以考虑使用数字证书。目前，管理员向远程接入客户机部署数字证书的负担已变得日趋沉重。

一般情况下，由于远程 IP 地址是动态的，通配符或分组预共享密钥通常用于远程接入客户机的设备验证。如前所述，这种验证类型无法提供严格的设备验证。但是，由于远程接入客户机经常接收动态 IP 地址，这是唯一的预共享密钥。利用一种严格的用户验证方案，如一次性口令(OTP)，缺乏严格的设备验证的问题就显得不那么突出。在远程接入 VPN 中，无法顺利通过验证的用户，就无权接入网络。

在设备和用户验证完成后，IPSec 接入控制就相继出现。通常情况下，根据 IPSec 制定的标准，对允许穿越隧道的网络、主机和端口在安全策略数据库(SPD)中进行了定义。该数据库可利用访问控制目录(ACL)进行调用。这些 ACL 有时被称为“加密 ACL”或“网络规则”。您可以考虑将加密 ACL 用于基础网络安全接入控制，但思科公司建议您不要采取这种方式，因为它会使配置显著复杂化。与其如此，您不如将入站 ACL 用于 VPN 设备的站点到站点信息流。就远程接入流量过滤而言，当用户经由扩展验证(XAUTH)成功完成验证时，通过加载用户计划授权信息，接入控制会动态生成。

IPSec

IPSec 提供了多种安全特性，对于管理员如何确定其工作方式提供了可配置选择：数据加密、设备验证，以及保密、数据完整性、地址隐藏和安全机构(SA)密钥老化等功能。IPSec 标准要求使用数据完整性或数据加密二种功能之一，具体使用哪个可任选。思科公司强烈建议加密和完整性二者都使用。由于在 1999 年的上次比赛中，价值 50000 美元、采用单一数据加密标准（DES）的设备受到黑客攻击，历时达 22 小时 15 分钟，因此，思科公司建议您不要将它用于数据加密。取而代之，思科公司建议您使用三重 DES(3DES)。数据完整性分两类：128 位强度 Messaqe Digests(MD-5)-HMAC 或 160 位强度安全散列算法(SHA)-HMAC。由于 SHA 的位强度更大，故公认更安全。思科公司建议使用 SHA，因为安全性的提高在重要性上超过了处理器开支的少许增长(实际上，在某些硬件实施中，有时 SHA 要快于 MD5)。IPSec 的两种方案都提供了可改变 SA 的使用周期的能力。当隧道数据的敏感度，迫使需更积极地对每个设备进行加密密钥替代和重新验证时，您可以考虑改变使用周期的缺省值。在美国以外的国家使用严格加密算法，有时会受到地方进口和使用法律的限制。这些严格的加密算法不能向某些国家或客户出口。欲了解详尽信息，请参考 http：//www.cisco.com/wwl/expert/enypto。

改变这些数值会提高安全水平；但与此同时， 也提高了处理器开支。SA 重新加密的缺省行为是在旧密钥基础上构建新密钥，从而节省了处理资源。通过在每次全新快速模式(QM)SA 需要生成新密钥时完成 Diffie-Hellman(DH)乘幂，Perfect Forward Secrecy(PFS)会在新资料的基础上，生成一个新密钥。同样，该选项会提高安全水平，但与此同时，也会加大处理器开支。思科公司建议您不要改变使用周期和实施 PFS，除非数据敏感度对其提出强制性要求。如果您选择改变这些数值，在确定网络设计时，应考虑该变量。Diffie-Hellman 乘幂的强度可配置：组 1(768 位)、2(1024 位)和 5(1536 位)都可获支持。建议采用组 2。在整个 SAFE VPN 体系结构中，至少需采用下列模式：IKE 3DES、SHA-HXXAC、DH 组 2、预共享密钥、IPSec 3DES、SHA-HXXAC、无 PFS 和隧道模式。

IP 编址

正确的 IP 编址对于用作大型 IP 网络的 VPN 的成功有着重要意义。为保持可扩展性、性能和可管理性，强烈建议远程站点使用主网的子网，以便进行归纳。这样一来，加密 ACL 将为每个本地网络都包含一行，如果本地网络自身可归纳的话，可能为一次输入。例如，远程站点网络 10.1.1.0/24 可归纳入主网 10.0.0.0/8。如果 10.1.1.0/24 子网的主机需要通过头端连接 10.0.0.0 网络中的其他子网，一次 ACL 输入就足够了。如果无法将远程网络归纳入一个主网，那么每个地方网络到远程网络都需要在远程站点输入一次。增加 ACL 输入会降低性能，使故障查寻复杂化和影响可扩展性，因为需要 ACL 经常与头端的新网络保持一致，而需在远程站点进行调整。每次 ACL 输入都将构建一个单独的隧道(两个 IPSec SA)。适当的子网化还可支持简化的路由器头端配置，以实现分支到分支相互交流，要对所有设备的信息流进行归类，所需的隧道也较少。IP 编址还可影响 VPN 的多个方面，包括重叠网络的远程管理连接。

多协议隧道

IPSec 作为一种标准，只支持单点广播流量。对于多协议或 IP 多点广播隧道，必须使用另一种隧道协议。由于其点到点协议(PPP)连接，第二层隧道协议(L2TP)最适合远程接入 VPN。通用路由选择封装(GRE)最适合站点到站点 VPN。GRE 通常用于多点广播分组，如路由选择协议的隧道生成。这些隧道协议都不支持数据加密或分组完整性。IPSec 的 GRE 和 L2TP 应用纯用于非 IP 单点广播支持-而非其他安全性。L2TP 还可简化远程接入客户机地址分配。分组将首先由备用隧道协议封装，然后，由 IPSec 封装。GRE 还允许一组 IPSec SA 将流量从一个站点传输至另一个站点。通常，IPSec 需要一组特殊的 IPSec SA 为各个本地网到各个远程网提供隧道功能。GRE 可封装所有流量，而无需顾及其来源和目的地。当需要分组隧道支持时，最好使用 GRE 或 L2TP，而非 IP 单点广播类型。

网络地址转换

NAT 可发生于 IPSec 之前或之后。了解 NAT 何时发生是十分重要的，因为在某些情况下，由于隧道构建受阻或信息流穿过隧道，NAT 都可能对 IPSec 构成影响。除非提供接入是必须的，否则将 NAT 应用于 VPN 流量将不失为上策。

IPSec 之后的 NAT

您可能会考虑在 IPSec 隐藏地址加密后使用 NAT，但是，这不会有什么益处，因为通过加密，将隧道用于传输设备的真实 IP 地址已被隐藏。只有 IPSec 对等的公共 IP 地址可见，这些地址的隐藏并未提供真正的额外安全性。IPSec 封装之后的 NAT 应用通常在出现 IP 地址预留的情况下才会发生。实际上，在宾馆、电缆/数字用户线(DSL)住宅部署和企业网络中，这种情况经常出现。在这些情况下，现使用的 NAT 类型，其应用可能会与 IPSec 隧道的构建产生影响。

当 IPSec 把验证报头(AH)模式应用于分组完整性时，如果出现一到一地址转换，则将使特征检验失效。由于特征检验部分得自于 AH 分组的 IP 报头内容，当 IP 报头改变时，特征检验也会失效。在这种情况下，分组会表现为在发送过程中被修改，当远程对等方收到时，将会迅速被丢弃。但是，当 IPSec 采用 ESP 时，设备将能够成功地在 VPN 上发送分组，甚至当封装后出现一到一地址转换时，也是如此。这种情况是可能的，因为 ESP 不会使用 IP 报头内容，使分组的完整性得以确认。在出现多到一地址转换(又名端口地址转换)的情况下，IP 地址：源 IKE 端口和用户数据报协议(UDP)端口 500 都会发生改变。一些设备不支持源于 UDP500 以外的 IKE 请求，执行多到一 NAT 的一些设备无法正确处理 ESP 或 AH。请注意，ESP 和 AH 都是位于 IP 顶部，不使用端口的高层协议。

由于多到一地址转换，在许多部署远程接入客户机的环境中，是一种通常现象，有一种称之为 NAT 透明度的特殊机制，可克服这些 NAT 问题。NAT 透明度可将 IKE 和 ESP 分组重新封装入另一传输层协议，如 UDP 或 TCP，那层的地址转换设备知道如何将其正确转换。这种机制还允许客户机绕过网络的接入控制，这种网络支持 TCP 或 UDP，但却会阻碍加密信息流动。注意，这种特性无论如何不会影响传输的安全性。NAT 透明度将获取被 IPSec 保护的分组，然后在 TCP 或 UDP 中再次封装。

IPSec 之前的 NAT

当两个站点通过 IPSec 连接，如果因站点的网址重复，隧道就不会建立，因为 VPN 端接设备无法确定向哪个站点提交分组。在 IPSec 之前使用 NAT，由于将一组重叠网络转换入一个独特的网址范围，不会与 IPSec 隧道建立冲突，因而可克服这些缺陷。这是建议使用 NAT 的唯一场合。但是，要知道一些协议在分组数据分段中植入了 IP 地址。通常当出现地址转换时，要确定是否为协议通晓设备执行的地址转换，不仅在 IP 报头中，也包括分组的数据分段。如果由于植入了 IP 地址，分组在进入隧道前无法正确转换地址，那么，当分组离开隧道时，远程应用就无法接收到植入在数据分段中的正确 IP 地址。在这种情况下，应用可能无法正常发挥功能。当今的许多远程接入 VPN 客户机支持使用头端端接 VPN 设备所分配的虚拟地址。利用这一虚拟地址，远程站点的设备可与远程接入客户机连接。这实际上是由穿越隧道的所有分组的一到一地址转换来完成的。如果 VPN 客户机无法正确完成分组的地址转换，或出现了一个不支持的新应用，那么，应用就可能无法发挥功效。

总之，在您的站点和远程接入 VPN 客户机虚拟地址池，它与您通过 IPSec 连接的其他设备地址不重复，此时可使用地址范围。如果不可能的话，仅在这种情况下使用 NAT，以支持连接。不要隐藏 VPN 设备的公共对等地址，因为这样并未提供真正的安全增值，而且可能会造成连接出现问题。当您认为 NAT 有介入而且远程接入客户机无法成功地建立隧道或在已建立的隧道上发送分组时，可考虑实施 NAT 透明度模式。要知道 NAT 透明度模式并不会解决与对 NAT 不友好的客户机应用相关的连接问题。

单一目的和多目的设备

在网络设计过程中，您需要选择是在联网或安全设备中采用集成功能，还是采用 VPN 设备的特殊功能。集成功能通常是很吸引人的，因为您可以在现行设备上实施，且该设备经济有效，其特性可与其他设备互操作，从而提供功能更理想的解决方案。指定的 VPN 设备通常在对功能的要求很高、或性能要求使用特殊硬件时，才会使用。当决定了采取何种选项，可根据设备的容量和功能对决策进行权衡，并与集成设备的功能优势相对照。例如，有时您可以选拔集成型高容量 CiscoIOS 路由器和 IPSec 加密软件，而非较小型的 CiscoIOS Router 以及相关 VPN 设备。在整个体系结构中，两类系统都有所使用。由于 IPSec 是一种要求严格的功能，随着设计规模的提高，选择 VPN 设备取代集成型路由器或防火墙的可行性也日趋增大。注意，对 VPN 设备这一概念的了解不是件容易的事情。当今的许多 VPN 设备可提供理想的性能和 VPN 管理选项，与此同时，也提供有限的路由选择，防火墙或 COS 功能，而它们可能与集成设备有关。如果所有这些高级功能都得以实现，从性能和部署选项的角度来看，这种设备也开始越来越像集成型设备。同样，除了路由选择和安全特性的全面实施以外，可支持全部 VPN 功能的 VPN 路由器，可在 VPN 单独环境中进行配置，其特征更象一种应用。

入侵检测、网络接入控制、信任和 VPN

在考虑 VPN 技术的部署时，请记住，通过这样做，您正在扩展网络的安全范围，从而将一些通常并不重视高安全性的领域容纳了进来，它们包括：

- 员工家庭
- 机场
- 宾馆
- 网吧

作为一家机构，需要首先回答的问题是 VPN 技术自身和使用它的周围应用和硬件的信任程度如何。得出结论的一个好办法是回答下列问题：作为一家机构，您是希望信任来自 VPN 的个人或远程站点，就像信任通过专用 WAN 链路连接的本地员工和站点一样吗?如果您的答案为“是”，那么，您就应该部署 VPN 技术，就如同您部署当今的专用 WAN 链路和调制解调器池一样。但是，这只是思科公司的情况，对其大部分 VPN 链接的客户的信任则应相对谨慎。因此，IPSec VPN 在部署时，周围通常环绕着多层接入控制和入侵检测。虽然配备 3DES 的 IPSec 十分安全，存储密钥的人为不安全性和设备的配置错误，为保证其他安全性能造成了极大的不确定性；更不要提膝上型电脑失窃和特洛伊木马了。本文主要是为后者而写的。如果您遭遇到前面的情况，您会发现这里的许多信息都是极有价值的，虽然您可能会觉得这些设计太注重于安全了。

网络入侵检测系统

网络入侵检测系统(NTDS)是一项用于减少与扩展安全范围有关风险的技术。有 VPN 设计中，NIDS 完成了两项基本功能。首先，NIDS 可用于分析源自或送至 VPN 设备的信息流。在这里，NIDS 将检测从远程站点或远程用户穿过 VPN 的攻击。因为我们知道该信息流的初始地，发生欺骗行为的机率较低，任何攻击都会引发来自 NTDS 的强烈反应。这种反应包括规避或 TCP 重设。NIDS 在许多 VPN 环境中都发挥着关键作用，因为大多数 VPN 安全策略表明，第三层和第四层 VPN 网络接入几乎是无所不在的。这种设置提高了对 NIDS 捕获和停止大多数源于远程站点的攻击的依赖性。其次，NIDS 可用于加密后，确认仅仅是加密信息流被发送并由 VPN 设备接收。通过将 NIDS 调至任一非 VPN 分组报警，您可确认只有加密分组流过网络。这种设备可防止 VPN 设备的任何错误配置，因而可阻止未加密信息流穿过设备。该功能在大型网络 VPN 设计中进行了更详细的论述。

网络接入控制

除 NIDS 以外，通常使用防火墙的接入控制应该在 VPN 设备前后设置。随着信息流向园区网，当在 VPN 设备内部实施控制时，可确保只有许可的相应地址范围和协议得到支持，如前所述，VPN 接入的大多数策略倾向于允许远程用户使用之上几乎所有协议。因此，要对您不希望远程用户社区接入的协议进行定义，与定义希望接入的协议相比，则相对简单

在更大型的部署中，将各类 VPN 与离散的网络接入控制点分隔开来会有所帮助。这可以通过为各类 VPN 提供专用防火墙接口来完成，如同在大型 VPN 设计中所做的一样。该设置支持不同 VPN 应用享有不同的信任级别。例如，一家机构可能会认为它信任站点到站点 VPN 要比信任远程接入 VPN 多一些。这种更好的信任是源于，在站点到站点的情况下，您知道您的远程对等设备 IP 地址并在使用数字证书，而在远程接入 VPN 的情况下，您通常不知道您的远程对等设备的地址，并且依赖于与次级验证相结合的分组预共享密钥，以允许您的用户接入网络。当按这种方式部署时，VPN 信息流可根据它所抵达的接入控制设备的接口进行过滤。

VPN 设备的输出过滤（向公共网）也是十分重要的。这种过滤可帮助确保 VPN 设备只见到 IPSec 信息流出入共公共接口。通常，这种过滤可通过带标准 ACL 的路由器来完成，由于用标准 ACL 替代了防火墙，从而可将防火墙安置在 VPN 设备后面，如前所述。该设置与当今的许多部署形成了鲜明的对照，当今的部署都将防火墙安置在 VPN 设备的前面。当安置在前面时，对用户信息流的种类不具备可视性，因为信息流依然是加密的。防火墙在 VPN 设备前所能提供的大多数优势此时已丧失殆尽，因为 IPSec 信息流无法被大多数防火墙智能地过滤。管理员需要在防火墙上开一个洞，以允许信息流过（即用于 IKE 的 UDP500 和用于 ESP 的 IP50)。在这一点上，就像路由器上标准分组过滤器的行为一样。建议使用 VPN 设备自身的过滤输入，以允许只有 IKE 和 ESP 得到支持。如果 NAT 透明度机制得以实施，您应该只允许特别的 UDP 或 TCP 端口连接到 VPN 设备。

通常这种接入控制功能可作为 IPSec 功能，存在于相同的硬件平台。如果您的 VPN 设备也拥有稳定的防火墙，或当远程用户利用拥有 VPN 客户机软件和个人防火墙的膝上电脑连接时，则可做到这一点。

分离隧道

当远程 VPN 用户或站点被允许接入公共网（互联网），与此同时，他未先将公共网络信息流安置在隧道内，就接入了专用 VPN 网络，此时就出现了分离隧道。如果分离隧道未设置，远程 VPN 用户或站点将需要把所有信息传输通过 VPN 头端，在那里将进行加密和审查，然后再发送至公开的公共网。例如，拨打本地互联网接入服务供应商（ISP），并通过 IPSec 客户机上公司连接的远程接入用户，拥有二项选择。一是让用户在 VPN 连接上仅传递公司内部数据。浏览网络可直接通过他的 ISP 进行。第二个选项是让用户将所有信息流（包括互联网信息流）首先传递至头端，然后再路由至公司网络或向外至互联网。对两种技术进行抉择通常要视您对远程站点或用户的信任度而定。为提高这些用户的信任度，可考虑使用额外的安全技术，如个人防火墙或病毒搜索。希望使用分离隧道的远程站点应拥有稳定的防火墙，以便对允许出入远程站点的明码文本信息流进行控制。同样，远程用户（在连接 VPN 的同时和未连接 VPN 时）应运行防火墙以过滤信息流，并完成病毒搜索。甚至在分离隧道不支持的情况下，个人防火墙经常也是十分必要的，因为用户并非总是在 VPN 上连接的。移动用户可能会通过宾馆中的高速互联网接入来连接并浏览网络，此时并未连接公司网络。如果没有个人防火墙，该系统无论何时未连接至 VPN，都会暴露在攻击下。

同样，许多硬件 VPN 设备也使用 NAT，并将其作为防火墙加以利用。以作者的观点看来，NAT 不是一种安全特性，不应该这样部署。即使地址是隐含的，但未进行分组过滤或序列号检查，受 NAT 保护的系统也会暴露于外在的攻击下。一种单纯依靠 NAT 的安全环境并非是一个真正的安全环境。当使用这些设备时，为设置在设备后面的 PC 提供个人防火墙是十分重要的。即使在分离隧道不支持的情况下，如果主机在漫游中（如膝上电脑），此时个人防火墙则是必备的。在考虑到实施分离隧道的安全性风险时，也会很容易得出下述结论，对此完全不必过滤。事实上，不实施分离隧道会给 VPN 头端造成巨大负载，因为所有互联网相关信息流都需要流经头端设备的 WAN 带宽。使用 WAN 资源并非理想的选择，经常会导致在远程站点做出实施相应安全技术的决定，以支持分离隧道的生成。在 SAFE VPN 中，远程站点除了特殊情况外，都假设实施了分离隧道。如果不支持分离隧道，而设计不会改变，那么由于头端的流量负载加大，性能和扩展就会产生少许变化。

部分网状、全部网状、分布式和星型网络

在任一网络拓扑结构上铺设 VPN 时，许多因素都会影响网络的可扩展性和性能。这些因素中包括与明码信息流处理和加密，硬件加速和软件 IPSec，配置复杂性、高可用性、相关安全性（防火墙 IDS 等）。路由选择对等设备的数量和被跟踪的网络。全部网状网络会迅速地陷入可扩展性的困境之中，因为网络中的每台设备都必须通过一个独特的 IPSec 隧道与网络中的其他设备交流。这就是 n(n-1)/2 隧道模式，对于 50 节点网络而言，就是 1225 条隧道，配置的复杂性是巨大的，在某些情况下扩大网络的规模已经变得不现实。许多隧道也都存在性能问题。部分网状网络与全部网状网络相比，有较大的可扩展空间，因为内部分支的连接只是根据需要才建立。与全部网状网络中的设备相同的是，在这种拓扑结构中的限制因素是，在 CPU 合理应用的前提下，设备可支持的隧道数量。这二种网络都可运用一种动态隧道端点搜索机制，以简化配置和提高可扩展性。但是，如同在“说明”一节中所描述的一样，这些网络不在本文的讨论范畴之内。

中心辐射型网络可以更理想地扩展，因为头端集线器站点可扩展，以满足日越发展的分支容量需求。需连接其他远程站点的低容量分支通过集线器站点实现连接。但是，所有流量都渡过集线器站点，而且这种设备要求大量的带宽，因为它包括了所有分支到分支信息流，以及中心辐射信息流。并非所有头端 VPN 设备都支持分支到分支内部通信。远程站点可能要配置分离隧道，视头端所选择的设备类型而定。例如，防火墙模式是在所有站点实施分离隧道，因而无需集线器防火墙处理分支到分支信息流。如果信息流路由选择是区域性的或存在其他要求，而此时大多数信息流并不要求通过集线器站点接入网络，那么，就可以考虑利用分布层来降低头端的带宽要求，因而提高了网络的可扩展性。

互操作性与混合和同种设备部署

虽然 IPSec 是一种已证实的标准，但 Request for Comments(RFC)依然为它的解释留下了充足的空间。另外，互联网草案，如 IKE 模式配置和供应商专用特性，提高了互操作问题出现的可能性。例如 IPSec 判断隧道上/下状态和远程对等设备的可接入性并无一定的标准。因为这些缘故，您应该对供应商产品的互操作信息及其在互操作性评比中的表现情况进行综合评价。通常，发生微许配置和代码（有时）改变，对于在可靠的状态下推动互操作性是必要的。意识到这些变化会影响到设备的安全性，因此，需对这些变化予以了解。此外，为确保单一供应商产品间的互操作性，最好在所有平台上使用同一代码库。这种环境会降低同一供应商产品出现互操作性问题的可能性，因为随着时间的推移电信商会不断进行调整，以符合各种标准的要求，并提高与其他供应商的互操作性。

除了互操作性问题以外，在环境中还出现了其他问题，在这些环境中部署了各类设备以构建 VPN。这些问题的产生根本原因是在于实施运营的 VPN 和其他特性间的互相关系。例如，可考虑用于管理远程用户和管理员的验证、授权、记帐（AAA）协议因素。对这种协议，如终端接入控制器接入控制系统＋（TACAS＋）或远程接入拨入用户服务（RADIUS），在各种设备类型间可能会有差异。如果您的用户数据库对所有设备类型中部署的这些机制中的一种不予支持，那么，这种差异可能会使问题复杂化。用于 IPSec 高可用性和 CA 支持的机制不同于一些路由器、防火墙、集中器和远程接入客户机。最后，还要考虑培训管理员针对多类型设备进行配置、管理、监控和查寻故障所需的额外资源问题。

分段和路径最大传输信元搜索

在所有费用中，分段的开支应予以避免。从 CPU 和内存分配的角度看，分组重新组装对资源是有要求的；一般可以避免分段。允许分段式分组进入您的网络，其结果会产生安全性问题。分段式 IPSec 分组要求在分组经过完整性确认和解密前重新安装。分段大多数时间都发生在分组通过隧道发送，并且封装分组太大，不适合隧道路径上的最小链路时。只要过滤不妨碍互联网控制信息协议（ICMP）信息，路径最大传输信元搜索（PMTUD）就会对通过隧道发送分组而不致造成分段的主机所使用的最大 MTU 进行确定。为支持您的网络中的 PMTUD，不要过滤 ICMP 类型 3、代码 4 的信息。如果发生 ICMP 过滤，而且您的管理员无法控制，您必须或者人为调降 VPN 端接设备上的 MTU，产给予 PMTUD 本地的支持，或者清涂不分段（DF）位并强迫分段。在这种环境中，不支持 PMTUD，而且在 IP 报头中未设置 DF 位的主机所生成的分组，在 IPSec 封装前将经历分段。由不支持 PMTUD 的主机所生成的分组，将把它用于本地，以便与隧道上静态配置的 MTU 相符。当您在隧道上人为设置 MTU 时，您必须将它尽量设置得较低，以允许分组穿过路径上的最小链路；否则，规模太大，不适合最小链路的分组将被丢弃，如果 ICMP 过滤情况发生，则不会提供任何反馈信息。请注意，封装的多层将增加分组的与层有关的开支。例如，GRE 和 ESP 隧道协议经常共同使用。在这种情况下，GRE 在经历 ESP 再次封装前，将向分组添加 24 个字节的开支。当使用 3DES 和 SHA 时，ESP 会添加 56 个字节的额外开支。由于 ESP 和 GRE 支持 PMTUD，分段的可能性即降低，根据 VPN 端接设备的不同，在隧道上设置 MTU 的方式也会有所改变。改变 MTU 的各种隧道包括隧道接口（路由器）、TCP 最大分段规模（防火墙）、策略路由选择（路由器）、清除/设置/复制 DF 位（路由器）、OS 应用级别（VPN 客户机，以及物理/逻辑接口（任一 VPN 设备）等）。

网络运营

在中央 IT 模式运营中，需要通过中央站点 VPN 对远程站点进行管理。VPN 设备可支持多种配置选项，以确定隧道端点，视所采用的方式而定，这些选项可能会对网络的管理性能产生影响。要高效地管理远程设备，您必须在您的管理应用所在的站点使用静态加密映像。您不可以在头端和动态加密映像。动态加密映像只接受进入的 IKE 请求，但无法初始化它们，因此，要始终保证在远程设备和头端站点间存在一条隧道。静态加密映像配置包括远程对等设备的静态 IP 地址，因此，远程站点必须使用静态 IP 地址来支持远程管理。

一些管理服务，例如，普通文件传输协议（TFTP），将最近的接口用作生成分组的源地址。因为这一缘故，当设置加密 ACL 以确保信息流穿过隧道到达头端时，您应该十分谨慎。您应该在 VPN 设备上实施只读简单网络管理协议（SNMP）接入，以便通过 IPSec 管理信息库（MIB）获取有关信息。您只能在安全接口上支持 SNMP 接入。IPSec MIB 可通过隧道原始表格和隧道故障表格，跟踪隧道统计信息和隧道状态。原始表格收集了有关隧道的各种属性和统计信息；故障表格收集了隧道故障的原因和故障发生时间。当在任意规模的网络中监控和查寻设备故障时，这种信息是十分重要的。除了命令行接口（CLI）以外，可考虑将 MIB 用于大型部署的故障查寻和主动监控。当今的大多数配置工具都假设环境是环保型的。因为这一缘故，您应该首先部署这些工具，甚至在初始阶段也应该如此，以便当步入生产阶段时，减轻配置的压力。

为安全地管理远程设备，必须在验证和隧道加密以外，实施一些形式的用户验证，其中隧道加密是在建立隧道时生成的。管理工具要求输入静态用户名/口令组，以便对远程设备进行配置，而无需管理员介入。不要使用相同的用户名/口令组接入您用于日常管理的管理设备。要确保固定式的用户名/口令组要不断更新。管理员应运用验证来接入设备，尤其是 OTP。还可考虑一点，那就是用户验证协议可能会在隧道上运行，以便向头端的 AAA 服务器提出请示。如果设备出现故障或配置错误，管理工具和远程管理员就无法管理设备。在这种情况下，可考虑使用本地静态用户名/口令组，或仅为远程管理目的而设定的静态加密映像输入。如果用隧道建立的设备验证需要数字证书，远程设备可能会失去接入 CA，以便根据 CRL 对许可证进行确认的机会。如果要求 CRL 检查的缺省设置未改变，隧道建立就不会生成。当使用许可证时，时间同步化对许可证定期检验是必须的，因此，所有 VPN 设备都应采用 NTP 协议（采用经验证的 NTP），以使时间实现同步化。为避免“鸡生蛋，蛋生鸡”的问题，要确保 CRL 和 NTP 拥有一条不依赖数字证书的路经。可考虑为这些极端环境的设备验证，定义一个备份预共享密钥。如果您将不同的 ACL、IPSec 转换和对等声明用于静态输入，配置错误就不大可能造成无法接入设备。

最后，一项公共的管理任务是更新 VPN 远程接入客户机软件的版本。为减轻这一负担，一些 VPN 集中器采用了一种机制，即当远程接入用户下一次连接头端时，将新客户机软件发送出去。这样一来，就可允许您的企业管理大量始终在运行中的客户机。

HSRP

就基于路由器的解决方案而言，您可能会考虑将热待机路由器协议（HSRP）用于弹性问题。用 IKE 对等设备高可用性的 HSRP 无法配置。目前，路由器无法听取 HSRP 虚拟 IP 地址的 IKE 请求。这就是对等设备间 IPSec 点到点关系的结果，此时设备不可能通过单一隧道与两台远程设备建立连接。您可将虚拟 IP 地址用于非 VPN 信息流弹性。当下一跳转设备，如防火墙，需要提供两 VPN 端接设备弹性时，这种方式会有所帮助。

压缩

第二层压缩未提供 VPN 信息流链路带宽削减功能。压缩是通过找寻数据流信息重复事例，并用较小的表达方式（一种独特的位组）来代替它们，以便传输来完成的。在接收数据流时，远程设备会用原始数据替代独特的位组。在 VPN 信息流中，无类似位的重复信息。加密使数据流随机化到了如此程度，几乎没有压缩算法再可提供任何缩减。如果事实不是如此，加密算法也就没有那么强的加密功能了。IP 第三层压缩称之为 IPComp。第三层压缩，发生于加密之前，的确可使数据量降低，这些数据将加密生成中到大型分组。加密数据减少使加密吞吐量得到了实质性的提高。考虑到第三层压缩在当今的大多数硬件加速器中都不支持，因而当使用时，对 CPU 要求非常严格。如果您选择实施软件压缩，要确保在确定网络设计时，将这一因素考虑进去。

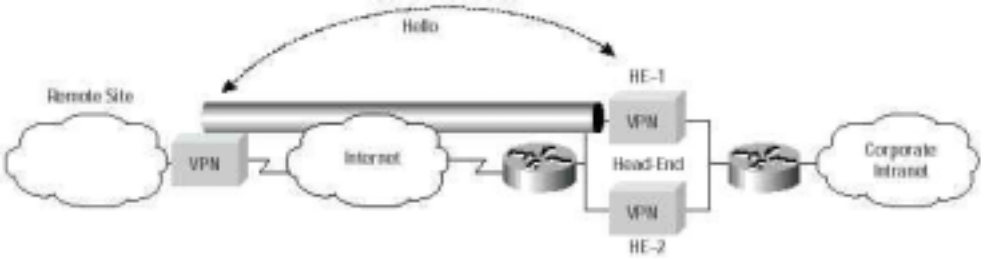
远程接入用户要求

移动办公者和远程办公者一样，无论在路上，还是在办公室，都有着同样的需求。他们很可能要接入下列内容：域名系统（DNS）以解决互联网主机和域名问题，Windows 互联网命名服务（WINS）以解决 Windows 域的主机问题，以及虚拟 IP 地址，以便允许他们接入公司内部网。在验证成功后，建立隧道期间，这些数值可通过 ISAKMP 配置方式（IKE MODCFG）输入远程客户机。虚拟地址此时可被任一内部网上的设备用于连接客户机。当用户不在办公室和不在控制区时，思科公司建议您对他们到内部网和互联网的连接进行控制。如果您选择分离隧道要确保安装、更新和运行个人防火墙，以及在远程接入客户机上拥有一个有效的安全策略。否则，如果由某些小程序、特洛伊木马或其他外源获得了客户机的控制权，在受到干扰后，它可能会被用于攻击企业网络。思科公司建议您在未实施防火墙的情况下，不要在客户机上实施分离隧道。

高可用性

由于 IPSec 隧道在发送数据时，未获得已接收到数据的远程对等设备的确认或反馈，设备应对远程对等设备的状态进行跟踪。否则，如果设备失去了对等设备的接入能力，隧道将变成一个黑洞，即使它依然表现为已建立也是如此。目前，有二种机制可用于确定远程对等设备的可用性和隧道建立状态：路由选择和 IKE 保持激活信息。路由器可支持两种机制，而防火墙、集中器和远程接入客户机则支持 IKE 保持激活信息。

图 1.IKE 保持激活信息的高可用性示例

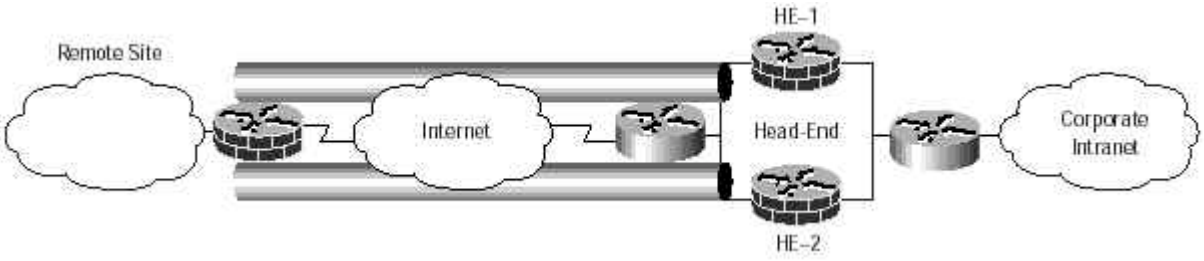


远程站点　　问候信息　　头端　　公司内部网

注:在任何规定时间都有一条隧道保持激活状态

在 IKESA 上发送 IKE 保持激活信息,以确定远程站点 IKE 对等设备的可接入性。当对等设备不再可接入时,就建立一条新隧道。在这种环境出现故障的情况下,建立新路径将在建立新隧道完成后实施。如果主设备恢复在线,设备将继续把备用设备用于端接,而不会抢先占用。请注意就这种机制而言,每个远程站点拥有到头端的单一路径。

图 2.路由选择协议的高可用性示例



远程站点　　头端　　公司内容网

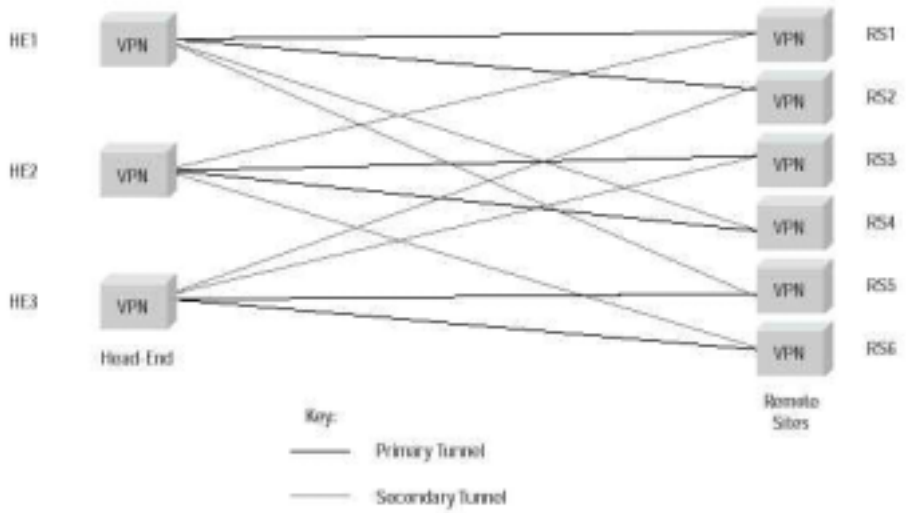
注：两条隧道保持同时激活。

与之相比，路由选择使用了两条路径。路由选择协议将在 IPSec 保护 GRE 隧道上发送，以便对远程网络的可接入性进行跟踪。将路由选择协议用于高可用性的远程站点，将建立两个 IPSec 保护 GRE 隧道，到各个头端。路由选择更新将穿越两种隧道到达远程站点，然后，将信息流提交给可接入目的网络的头端。从远程站点的角度，有两条路径到头端。可考虑将其中一条定为主隧道，以避免非对称路由选择。这种设置是通过为链路中的一条调整路由选择协议的成本来完成的。在隧道出现故障的情况下，一旦路由选择协议意识到路径不再可用，就会很快发生合并现象，在故障恢复过程中，使用路由选择协议的远程站点将有选择地恢复其主要感兴趣的路径。

集中器和防火墙头端经常可支持激活/待机配置中的故障转换功能。当主设备出现故障时，备用设备将承继主设备的 IP 和媒体接入控制（MAC）地址，隧道重建立过程将被启动。路由器可在激活/激活配置中发挥功能。两种头端设备都将允许隧道建立。您可以考虑在头端把 IKE 保持激活信息用干混合远程站点设备支持。当今的保持激活信息没有 IETF 标准，因此，该机制只能在单一供应商产品上发挥效能。如果在远程站点发生暂时的连接丢失，可以利用备用（但总是处于激活状态）头端设备建立一个新隧道。因为除非路由选择协议在隧道上运行，否则隧道建立不会影响路由选择表格，头端的路由选择状态也不会改变。当隧道在头端间交换时，由于远程站点的不确定性，下一跳转路由器将无法确定哪个激活的头端设备拥有到远程站点的有效路径。不确定性将在远程站点暂时推动 WAN 连接时发生。当前设备间的 IPSec 故障转换是无边界的，在备用设备上要求拥有新隧道建立机制。

总之，当在头端使用 VPN 集中器或 VPN 防火器时，应将 IKE 保持激活信息用于高可用性。当在头端使用 VPN 路由器时，应将路由选择弹性用于高可用性。

图 3.故障过程中负载的分散机制



头端　远程站点　图例　主隧道　备用隧道

当头端隧道端接设备故障时，其负载应在其他头端设备间平等共享。在故障过程中负载分散方面，该过程主要有助于头端的弹性和可扩展性。遗憾的是，它也增加了配置的复杂性。故障过程中的负载分散机制只是在激活/激活配置中可用，而非激活/待机配置，因为，负载分配不可能发生于待机设备。不考虑所选机制的高可用性问题，头端设备不应部署在使 CPU 利用率在故障后高于 50%的配置。50%的目标包括由 IPSec 和其他支持特性（防火墙、路由选择、IDS、日志等）所造成的全部开支。在一些环境中，在稳定、可靠的方式下，有可能实现更高的 CPU 利用率。但是，在故障环境中，当部署有数百个站点时，路由协议合并或新隧建立所需的处理能力，将对拥有充足空间可靠地恢复的设计进行支持。

当前大型 VPN 中一个最常见的问题是陈旧的 SA,当位于隧道末端的设备维持了隧道的状态,但另一远程端却未能保持时,就会出现这种情况。在链路故障、配置错误、故障查寻、系统维护，或全面设备故障的情况下，状态丢失都可能发生。通过去除陈旧隧道的状态，并设置一条新隧道，IKE 保护激活信息可充分解决这一问题。但是，路由选择协议弹性可保持隧道随时畅通无阻，因此，更可能陷入陈旧 SA 的问题。在隧道网络可接入性和隧道状态之间无反馈链路。换而言之，如果网络在隧道上不再可接入，隧道就没有被关闭，直至超时。当远程设备恢复在线时，如果它已丢失隧道状态，它将尝试建立一条新隧道。保持激活状态的设备将收到一条隧道的建立请求。它将使用新隧道传输数据，旧隧道将被关闭。在远程对等设备备份前，继续利用旧隧道传输数据是一个问题，当设备脱机维护时，这也是一个每天都要遇到的系统管理工作。思科公司建议您当头端 VPN 设备脱机维护时，应清除远程设备上的 IKE SA，以促进 IKE 的重新建立。不要改变 IKE SA 使用周期。虽然，该解决方案会更快地使隧道到期，在这些情况下会使管理工作更加简化，但是处理器使用数量的提高并不能证实其真正的效果。思科公司建议您不要将 IKE 保持激活信息与用于弹性的路由选择协议组合运行，以为保持当前的状态提供支持。同时运行两种机制会显著地降低可扩展性，就 CPU 的总计开支而言。

思科公司的一种新型 IKE 保持激活信息，称之为空端对等检测（DPD），可以较低的 CPU 价格提供与 IKE 保持激活信息相同的功能。它的机理是通过仅向从未发送或接收过出入数据的设备发送 IKE 对等可接入性探针，来发挥效能。IKE 保持激活信息可向所有 IKE 对等发送更新信息，这也解释了为什么它是一种类似于发送问候信息的路由选择协议的 CPU 集中过程的原因。在路由选择协议弹性环境中，路由器 VPN 设备可经常在隧道上发送信息流。DPD 并不像路由选择问候信息发送那样发送请求和使用 CPU 那么长时间。最后，即使您的网络中不要求高可用性，也可考虑使用 IKE 保持激活信息，或使用 DPD 来保持隧道当前的状态。这种设置会减轻管理负担。

分支机构和头端分析

下面即将讨论的中小型设计可用于两种可能的配置中。在第一种配置中，设计是作为一家较大型机构的一个分支机构，构建于配置中，在 SAFE 企业中进行了介绍。在第二种配置中，设计是一家机构网络的头端。这种头端可能拥有到相同机构其他办公室的 VPN 连接。例如，一个大型的法律事务处可能会将中型网络设计用作其头端，而将若干小型网络设计用于其他部门。全天候远程办公者可能通过在远程网络设计中讨论过的一些选项进入头端。

还有一个例子就是大型的汽车制造公司，它可能会将 SAFE 企业设计作为其总部，而在本文中所讨论的许多设计则作为它的远程机构和远程办公者。在适合的情况下，对设计需要做出的修改在各节中进行了讨论。

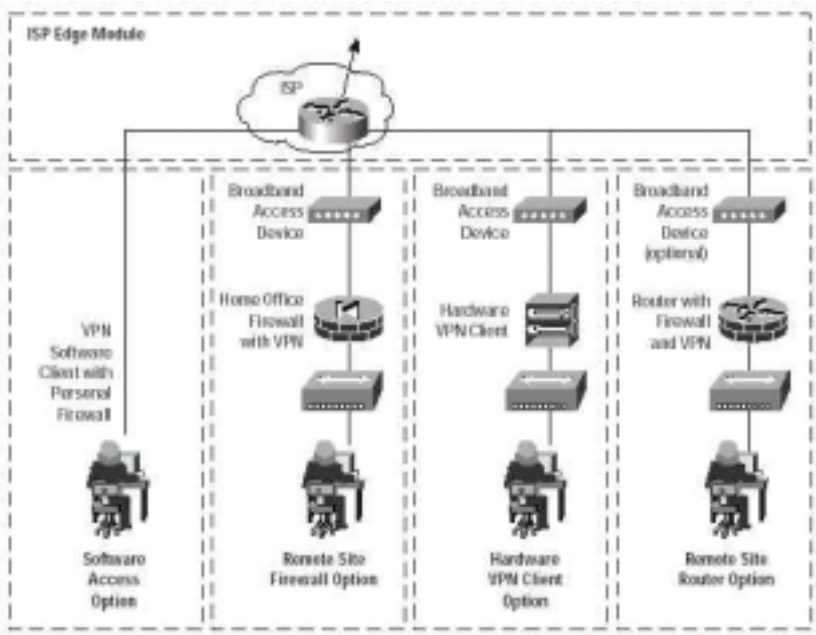
远程用户设计

本节将讨论为远程用户提供 VPN 到 SAFE 设计内头端站点连接的四种选项。远程连接适用于移动和家庭办公者。这些设计主要是提供从远程站点到公司总部的连接，通过一些方式，包括互联网。四个选项列举如下：

- 软件接入选项—拥有软件 VPN 客户机和 PC 个人防火墙软件的远程用户
- 远程站点防火墙选项—受指定防火墙保护的远程站点，可向公司总部提供防火墙保护和 IPSec VPN 连接；WAN 连接通过 ISP 提供的宽带接入设备提供（即 DSL 或电缆调制解调器）
- 硬件 VPN 客户机选项—使用指定硬件 VPN 客户机的远程站点，可向公司总部提供 IPSec VPN 连接；WAN 连接通过 ISP 提供的宽带接入设备提供。
- 远程站点路由器选项—使用路由器的远程站点，可向公司总部提供防火墙保护和 IPSec VPN 连接。该路由器可以提供直接宽带接入，或穿越 ISP 提供的宽带接入设备。

在下面的设计指南一节中将对这些设计的具体内容逐一详细讨论。

图 4.远程用户模块的详细模型



ISP 边缘模块　宽带接入设备　宽带接入设备　宽带接入设备（可选）

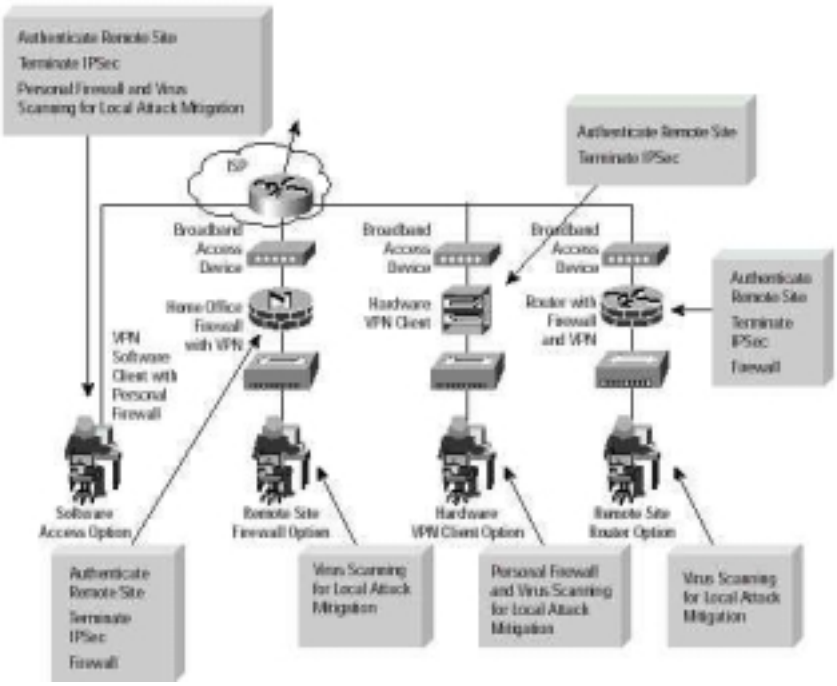
带 VPN 的家庭办公防火墙　硬件 VPN 客户机　带防火墙和 VPN 的路由器

带个人防火墙的 VPN 软件客户机　软件接入选项　远程站点防火墙选项　硬件 VPN 客户机选项远程站点路由器选项

关键 VPN 设备

- **宽带接入设备**－提供宽带网（DSL、有线等）的接入功能
- **VPN 防火墙**－在远程站点和公司头端间提供端到端加密隧道；提供远程站点资源的网络级保护以及信息流的过滤功能
- **个人防火墙软件**－为个人 PC 提供设备级保护
- **VPN 防火墙路由器选项**－在远程站点和公司头端间提供安全的端到端加密隧道；提供远程站点资源的网络级保护以及信息流的过滤功能
- **远程接入 VPN 客户机**－在个人 PC 和公司头端间提供安全的端到端加密隧道的软件解决方案
- **VPN 硬件客户机**－在远程站点和公司头端间提供安全的端到端加密隧道

图 5.　远程用户模块－VPN 的详细模型



验证远程站点

端接 IPSe

个人防火墙和病毒扫描

适用于本地攻击缓解

验证远程站点

端接 IPSec

宽带接入设备　宽带接入设备　宽带接入设备

带 VPN 的家庭办公防火墙　硬件 VPN 客户机　带防火墙和 VPN 的路由器

验证远程站点

端接 IPSec

防火墙

带个人防火墙的 VPN 软件客户机
软件接入选项　远程站点防火墙选项　硬件 VPN 客户机选项 远程站点路由器选项
验证远程站点　　用于本地攻击缓解的病毒扫描　用于本地攻击缓解的个人防火墙和病毒扫描　　用于本地攻击缓解的病毒扫描
端接 IBSec
防火墙

设计指南

在下文中将对远程用户连接选项的具体内容进行详细介绍。假设所有设备都拥有单一的本地网络。在这些设计中，所有 VPN 设备都进行配置，缺省路由设置成 ISP 下一跳转设备。假设客户端设备（CPE）未执行 NAT 功能。这些设计中的性能通常受到来自媒体类型或上载带宽电信服务供应商的限制。

软件接入选项

软件接入选项是针对移动和家庭办公用户的。对远程用户的所有要求是一台带 VPN 客户机软件的 PC 机，以及互联网连接，或通过拨入或以太网连接的 ISP 网络。VPN 客户机软件的主要功能是建立一个从客户机设备到 VPN 头端设备的安全加密隧道。当防火墙和客户机自身的过滤开始发生作用时如果接入权通过策略下达，此时网络的接入和授权都是由总部所在地来控制的。远程用户首先验证，然后接收 IP 参数，如虚拟 IP 地址，它被用于所有 VPN 信息流和名称服务器的场所（DNS 和 WINS）。分离隧道也可通过中央站点启用或停用。就 SAFE 设计而言，分离隧道是禁用的。对于拥有已建立隧道的所有远程用户，通过公司连接接入互联网而言，它是不可或缺的。当连接至互联网或 ISP 网络时，由于远程用户不总是希望建立隧道，因而建议使用个人防火墙软件来减少 PC 的未授权接入。同时建议用病毒扫描软件来缓解影响 PC 的病毒和特洛伊马程序。

IKE 保持激活信息被用于确定头端可用性机制。头端设备验证可通过分组预共享密钥来完成，OTP 被用于通过 XAR TH 的用户验证。这一选项中的安全管理包括在隧道上发布策略，以及新 VPN 客户机更新通知。如果多到一 NAT 出现于客户机和头端之间，NAT 透明度模式应予以实施。该选项的唯一替代内容是在下列选项之一中做出选择。与之相比，后者允许通过分离隧道的互联网接入，并可通过集成型防火墙/VPN 设备提供更强大的安全特性管理功能。

远程站点防火墙选项

远程站点 VPN 防火墙选项是针对家庭办公用户或极小型分支办事处的。凭借该选项，远程站点将有望从电信服务供应商那里获得某些形式的宽带接入。VPN 防火墙是安装在 DSL 或有线调制解调器背面的。VPN 防火墙建立了一个到 VPN 头端设备的隧道，可通过 NAT 提供互联网接入，以及审查和过滤功能。远程站点网络的个人 PC，除非是在途中，需要通过互联网接入公司内部网，否则，无需利用 VPN 客户机软件访问公司资源。在这种远程站点配置中，鉴于企业级防火墙特性的实施，分离隧道被禁用。建议使用病毒扫描软件来缓解分离隧道遭遇的风险。

正确的地址归纳应予以实施，以减轻管理工作的压力，并在需要时为远程站点内的相互交流提供支持。公司网络和互联网的接入和授权是受远程站点防火墙和 VPN 头端设备控制的。远程站点防火墙的配置和安全管理可以通过从防火墙的公共边缘到后面的公司总部的 IPSec 隧道来完成。这种设置可确保远程站点用户无需对家庭办公防火墙的配置执行任何配置调整。该远程站点可接入公司网络的个别用户，无需经过该选项中的用户验证。我假设环境是受控制的。如果环境不受控制，可考虑在头端防火墙设立用户验证。VPN 会使用设备预共享密钥验证。鉴于是大型部署，建议使用数字证书。DPD 类型的 IKE 保持激活信息将被用于高可用性机制，以确保头端的可用性。VPN 上未采用 NAT 转换本地网络，因为假设网络不会与其他网络重叠。

硬件 VPN 客户机选项

硬件 VPN 客户机选项等同于远程站点防火墙选项，除了硬件 VPN 客户机不拥有住宅防火墙。这种选项要求在个人主机上使用个人防火墙，尤其当实施分离隧道时。没有个人防火墙，VPN 设备后面的个人主机安全性则将依赖于攻击者无法跨越 NAT。这种依赖性是基于下述原因，当分离隧道实施时，到互联网的连接将通过一个简单的多到一地址转换，而不经过第四层和更高层的任何过滤。如果分离隧道禁用，所有互联网接入都必须通过公司总部。这种设置会部分缓和对终端系统防火墙的要求。

硬件 VPN 客户机提供了两种主要优势。首先，就 VPN 软件客户机而言，公司网络和互联网的接入和授权是受总部中央控制的。VPN 硬件客户机设备自身的配置和安全性管理都是通过中央站点的安全插件层（SSL）连接来完成的。这种设置可确保远程站点用户无需对硬件 VPN 客户机进行任何配置调整。硬件 VPN 客户机选项的第二个优势是，远程站点网络上的个人 PC，无论安装的 OS 为何种类型，无需借助 VPN 客户机软件接入公司资源。但是，在远程站点接入公司网络的个人用户凭借该选项则无需进行验证。硬件客户机可按两种模式运行。在第一种模式中，硬件客户机后面的所有用户，通过使用多到一 NAT，在公司内部网上将显现为一个用户。在第二种模式中，接入未带 NAF 的公司内部网的所有设备，以及内容网的主机，一旦隧道建立后，都可初始化到硬件客户机背后主机的连接。在 SAFE VPN 中部署了后一种模式。第一种模式管理简便，因而更具有可扩展性，但第二种模式更具备多样化的特性。二种模式所提供的安全级别是相同的。

利用静态配置的分组预共享密钥，VPN 硬件客户机将通过 VPN 头端集中器的设备验证。我们假设环境是受控制的。如果环境不受控制，可考虑在头端防火墙实施用户验证。鉴于是大型部署，建议使用数字证书。DPD 类型的 IKE 保持激活信息将被用于高可用性机制，以确保头端的可用性。

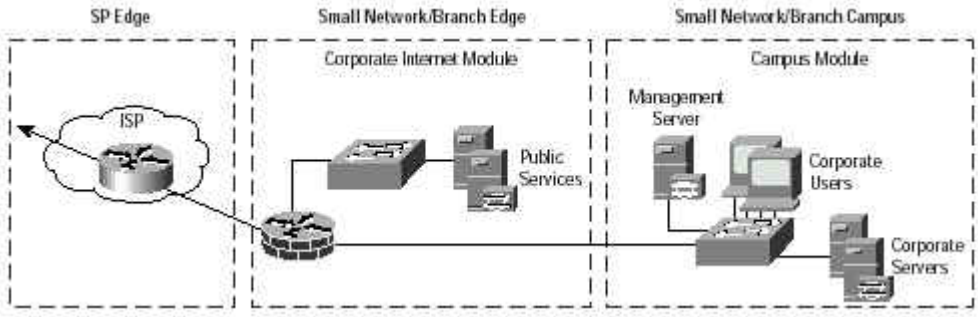
远程站点路由器选项

远程站点路由器选项几乎等同于远程站点防火墙选项，只是有少许例外。第一，由于该路由器是一种特性全面的路由器，因此，可支持一些高级应用如 Cos。Cos 可用于使公司内部网接入优先于互联网网络冲浪。第二，有一种选项可将 VPN 防火墙和宽带接入设备的功能集成入单一设备。它要求您的 ISP 允许您对宽带路由器本身进行管理，这种情况并非普遍现象。IKE 保持激活信息或路由协议将被用于高可用性机制，以确保头端可用性。

小型 VPN 设计

小型 VPN 设计采用了与 SAFE 安全技术小型网络设计相同的拓扑结构。这种设计可支持站点到远程接入 VPN，在配置一节中对此进行了一些解释。对这项设计的讨论大多数都是基于这样一个前提，即这种设计作为公司的头端运营。当用作分支机构时，设计应做的调整也包括在内。这种小型网络 VPN 设计包含在小型网络公司互联网模块中。整个小型 VPN 设计在下图中进行了介绍。

图 6.小型网络的详细模型



边缘　　小型网络/分支机构边缘　　小型网络/分支机构园区网

公司互联网模块　　园区网模块

公共服务　　管理服务器

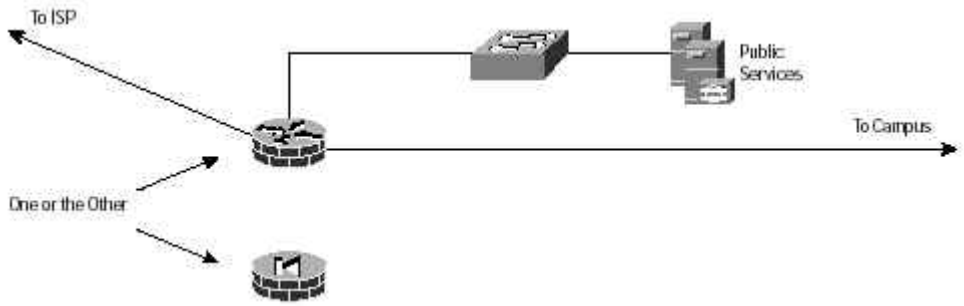
公司用户

公司服务器

公司互联网模块

公司互联网模块为内部用户提供了互联网服务接入功能和互联网用户访问公共服务器中的信息的功能。它还为远程场所和远程办公者提供了 VPN 接入功能。

图 7.小型网络公司互联网模块的详细模型



到 ISP

公共服务

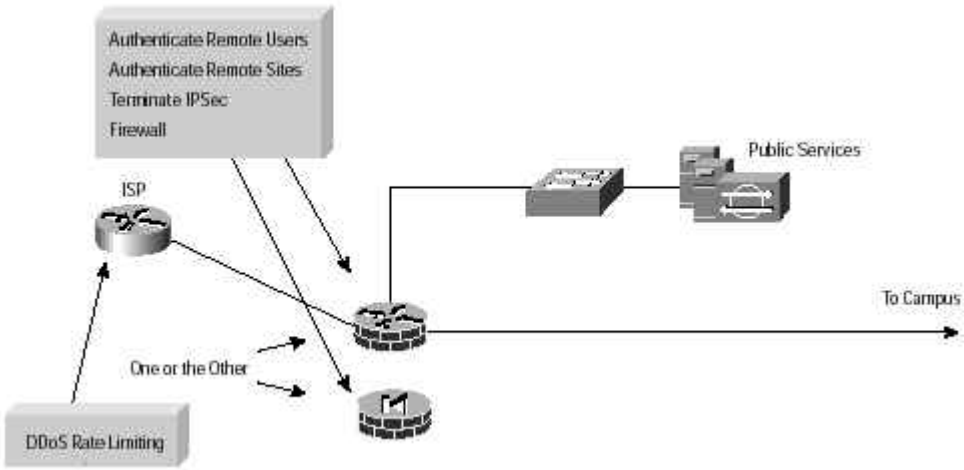
到园区网

一个或多个设备

关键 VPN 设备

- 防火墙或防火墙路由器—提供资源的网络组保护和信息流状态过滤功能
- RADIUS 验证服务器—提供远程接入连接验证（位于园区网）

图 8.小型网络公司互联网模块 VPN 的详细模型



验证远程用户

端接

防火墙

公共服务

到园区网

一个或多个设备

速率限制

设计指南

在小型 VPN 网络设计中，该模块堪称为极至。VPN 功能被压缩入一个机箱，但依然执行着路由选择、NAT、IDS 和防火墙功能。在确定如何实施该功能时，提及了两种主要替代措施。第一是使用带防火墙和 VPN 功能的路由器。这种选择为小型网络带来了极大的灵活性，因为路由器将支持在当今网络中可能是不可或缺的所有高级服务。作为一种替代措施，可使用带 VPN 的专用防火墙来取代路由器。这种设置给部署造成了一些限制。首先，防火墙通常都只是以太网，要求对相应的 WAN 协议进行一些转换。在目前的环境中，大多数有线和 DSL 路由器/ 调制解调器都是由电信服务供应商提供的，可用于连接以太网防火墙。如果设备要求 WAN 连接（如电信供应商的 DSL 电路），那么，就必须使用路由器。使用专用防火墙不具备轻松配置安全性和 VPN 服务的优势，当发挥防火墙功能时，可提供改进性能。无论选用哪种设备，都要考虑一些 VPN 的因素。请注意，路由器倾向于允许信息流通过，而防火墙的缺省设置则倾向于阻止信息流通过。

无论选择何种硬件平台，在设计中所实施的 VPN 功能都是近似的。路由器和防火墙都可支持防火墙保护，基本 NIDS、NAT 和 IPSec。除非小型设计被用作大型设计（在后面讨论）的分支机构。否则头端不存在弹性，所以，选择基础隧道模式是无庸置疑的，没有其他选项。在下面的章节中将对 A 型网络的特殊设计模式进行讨论。

身份

在远程地点到站点到站点 VPN 连接中，预共享密钥和 IPSec 对等 IP 地址被用于 IPSec 设备的身份识别。尽管这种情况没有安全数字证书，但是对于小型 VPN，预共享密钥可以轻松管理，因为网站的数量一般都不足十个。

远程接入 VPN 连接采用了双项验证方案，在 RADIUS 的备用用户验证的设备上采用了通配符预共享密钥。由于验证不包括 OTP，就要更多地依赖用户对严格的口令的选择。口令也应快速老化，在一定次数的登录尝试失败后，用户就会被拒之于 VPN 之外。如果有人盗走了用户的膝上电脑而工厂未及时得到通知这样可帮助抵御疯狂的破坏行为。请注意，这种验证方案不十分严格，如果两种验证方案中的一种受影响，那么，机构可能就会只剩下很脆弱的一个防范层。

安全性

从安全性的角度来看，状态防火墙软件只支持 IKE 和 ESP 信息流端接。VPN 设备的接口信息流从这里加密，然后，通过设备的防火墙功能再次过滤。它允许小型网络 VPN 的管理员对允许进入网络的协议类型进行确定。

可扩展性

这类设计的可扩展性不是很强。它是专门为不到 20 个远程站点和不到 50 个远程同步用户而设计的。但是，该设计可以满足大多数小型网络的需求。

安全管理

设备自身的安全管理可使用安全和非安全协议，如安全壳程序协议（SSH）、SNMP、TFTP 和系统日志等的组合来完成。有关远程站点管理，管理信息流可通过 IPSec VPN 连接发送至该站点。这种设置允许管理功能在加密状态下通过互联网。远程 VPN 设备本身并非 IPSec 隧道的一个组成部分，需要通过单独的隧道进行管理，以支持管理主机和远程设备外部接口间的安全互联。

NAT

在配置中，NAT 只是用于小型网络连接到互联网。内部站 点 VPN 通信可以绕过 NAT，在使用非重叠 RFC-1918 编址的情况下，可允许所有信任用户用其真实的 IP 地址进行交流。对于远程用户，这种“真实”的地址是输入其 VPN 客户机的虚拟地址。

路由选择协议

除了一些简单的静态路由器以外，在配置中并不需要路由选择。所有内部客户都缺省地路由选择至 VPN 设备，再由 VPN 设备缺省选择至 ISP。到远程站点的静态路由是需要的，因为在分组路由选择至外部接口后，它就被加密并发送给远程对等设备。

外部网

这类设计对外部网环境并非十分有助益。如果需要外部网连接，将链路安置在一台单独 VPN 设备这一过程就应被予以极大的关注。该设备必须位于与设计中原始 VPN 设备的部分段相隔的地方。这种设置允许信息流独立处理，与公司 VPN 信息流相隔离，并可减少错误配置的机会。

性能

在目前的小型网络中，WAN 连接一般是限制因素。当 VPN 信息流与标准互联网信息流相混合时，要注意避免您的互联网链路被 VPN 信息流充斥。允许远程站点使用分离隧道对此会有所帮助。因为大多数 VPN 设备尚未具备可限制 VPN 流量设备用户量的能力，头端混合流量需要特别关注。

替代选项

小型 VPN 设计最突出的需求是对远程用户的严格验证。这种验证可通过向小环境中添加 OTP 来实现。在本设计中未收入，因为许多小网络的经济实力不允许使用 OTP 技术。本设计的另一偏差因素与提高网络容量或将各种安全功能分配到各个设备有关。如果这结变化被融入，设计会开始看上去越来越像将在后面读者论坛的中型 VPN 设计。除了采取全面中型设计以外，第一步是添加一个专用远程接入 VPN 集中器，以提高远程用户社区的管理性能。

分支机构和独立性

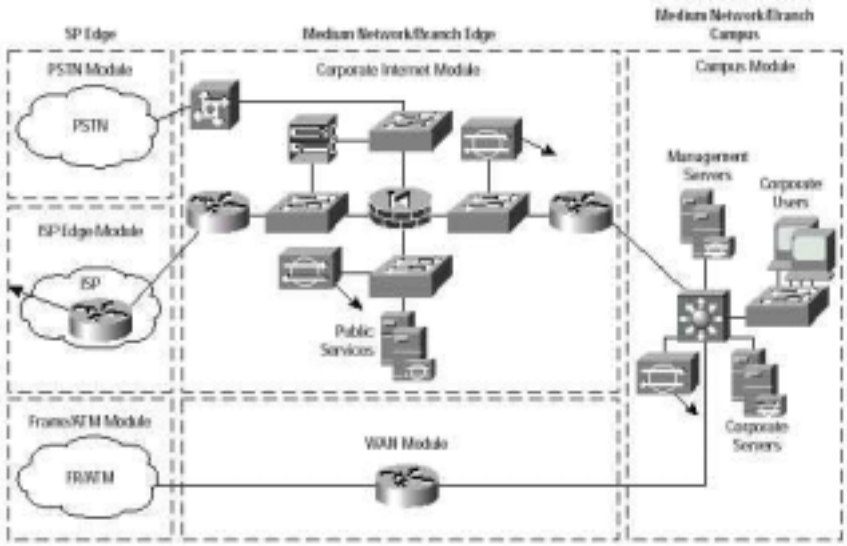
选择适合分支机构使用的 VPN 设备类型越来越多地受到来自头端弹性类型的支配。如果总部未能以各种形式对 IPSec 高可用性加以利用，或如果总部正在使用某种 IKE 保持激活信息机制，那么，小型分支机构的设备选择将按照上述相同的选择标准予以落实。但是如果头端将 GRE IPSec 用于支持高可用性，小型 VPN 设备就需要支持路由选择协议和 GRE 封装。目前，许多防火墙无法提供这种功能。可考虑将 VPN 信息流的优先权置于网络冲浪和其他信息流之上。

另外，作为一家分支机构，VPN 设备更可能从远程站点进行管理，使加密 ACL 会产生少许不同。

中型 VPN 设计

中型网络 VPN 设计采用了与 SAFE 安全技术的中型网络设计相同的拓扑结构。该设计可支持站点到站点和远程接入 VPN。对这项设计的讨论大多数都是基于这样一个前提，即这种设计将作为公司头端运营。当用作分支机构时，设计应做的调整也包括在内。中型 VPN 设计包含在中型网络公司互联网模块中。整个中型网络设计在下图中进行了介绍。

图 9.中型网络的详细模型

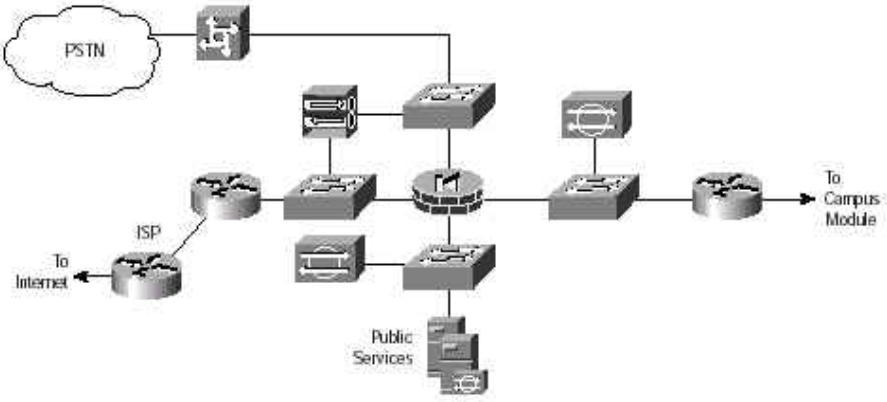


边缘	中型网络/分支机构边缘	中型网络/分支机构园区网
PSIN 模块	公司互联网模块	园区网模块
ISP 边缘模块	公共服务	公司用户
帧/ATM 模块	WAN 模块	公司服务器

公司互联网模块

公司互联网模块的目标是为内部用户提供互联网服务接入功能和互联网用户接入公共服务器上的信息（超级文本传输协议 IHTTPJFTP、简单邮件传输协议 ISMTPJ 和 DNS）。另外，该模块还可端接远程用户和远程站点，以及传统拨入用户的 VPN 信息流。

图 10.中型网络公司互联网模块的详细模型



到园区网模块

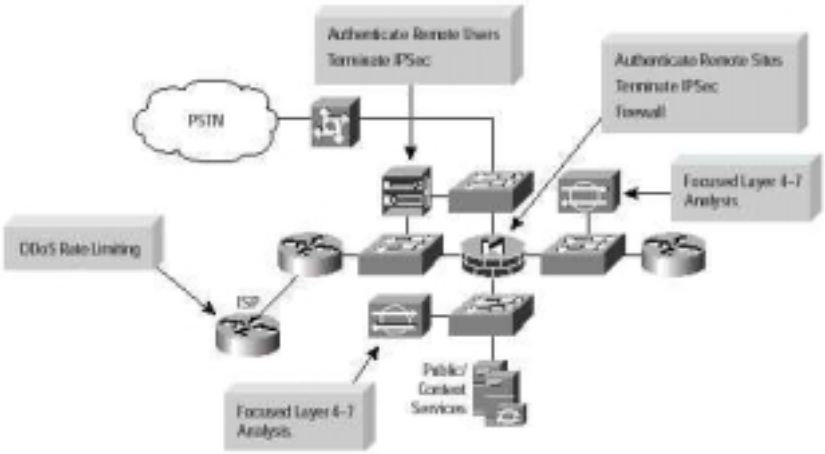
到互联网

公共服务

关键 VPN 设备

- **VPN 防火墙**—提供资源的网络级保护和信息流状态过滤功能，为远程用户提供独特的安全性能；验证信任远程站点和利用互联网隧道连接能力提供
- **VPN 集中器**—验证个别远程用户和端接其 IPSec 隧道
- **NIDS 应用**—提供模块第 4—7 层的关键网络分段的监控功能

图 11.中型网络公司互联网模块 VPN 的详细模型



验证远程用户端接 IPSec

验证远程用户端接 IPSec

防火墙

第 4—7 层集中分析

速率限制

第 4—7 层集中分析　　公共/内容服务

设计指南

中型 VPN 设计将站点到站点和远程接入 VPN 信息流分隔到了两台独立设备上。这种设置可实现更理想的性能，因为每台设备都只是与一类 VPN 相关。通过转移至专用远程接入 VPN 设备，远程用户社区的管理能力也得以提高。站点到站点 VPN 是在模块核心的专用防火墙上完成的。因为弹性不是设计的一部分，同小型设计一样，使用了标准隧道模式 IPSec。

身份

在远程地点到站点到站点 VPN 连接中，数字证书和 IPSec 对等 IP 地址被用于确认对等设备的身份。这样就提供了在标准预共享密钥基础上更理想的安全和管理性能。

远程接入 VPN 连接采用了双项验证方案，在通过 OTP 的备用用户验证的设备上采用了通配符预共享密钥。

安全性

从安全性角度来看，边缘路由器只允许 IKE 和 ESP 信息流端接 VPN 设备的公共接口。信息流从这里加密，然后，如果它是远程接入 VPN 信息流，就穿过防火墙；或在站点到站点 VPN 中，利用防火墙功能进行本地过滤。在过滤发生后，随着信息流被发送至公共服务网段，或路由选择至园区网。NTDS 的配置使其能规避防火墙的某些报警。

可扩展性

这种设计与小型设计相比有更强的可扩展性。凭借硬件加密，该设计可轻松地支持 500 名同步远程用户和 50 个远程站点。根据各远程站点和客户使用带宽量的不同，这些数字可大可小。如果您想提高本设计的上限，但却没有大型设计所需的经济实力，可以考虑下面的“替代选项”。

安全管理

VPN 设备的安全管理可利用安全和非安全混合协议来完成，这些协议包括 SSN、SSL、SNMP、TFTP 和系统日志等。有关远程站点管理，管理信息流可通过 IPSec VPN 连接，发送至该地点。这样一来，可允许管理功能在加密状态下通过互联网。远程 VPN 设备本身并非 IPSec 隧道的一个组成部分，需要通过单独的隧道进行管理，以支持管理主机和远程设备外部接口间的安全互联。

NAT

在配置中，NAT 只是用于内部用户连接到互联网。内部站点 VPN 通信可绕过 NAT，在使用非重叠 RFC 1918 编址的情况下，可允许所有信任用户用其真实 IP 地址进行交流。远程用户由集中器分配了一个虚拟 IP 地址，是由 AAA 服务器提供的。在 VPN 集中器上 NAT 透明度模式得以启用，以加速远程接入客户机连接。

路由选择

所有内部用户的信息流都路由选择至 VPN 防火墙，然后，再把远程接入客户机信息流路由选择至 VPN 集中器，并通过缺省配置将所有其他信息流路由选择至边缘路由器。其结果，远程站点信息流会触发加密 CL。

外部网

这种设计具有一种独立的 VPN 设备，它通过一个新接口与主防火墙连接，可轻松地为外部网连接提供支持。根据外部网种类的不同，这种连接可路由选择至防火墙，或直接连接园区网（假设设备拥有本地防火墙保护特性）。

性能

同小型网络一样，WAN 连接可能成为设计的限制因素。设计中的设备可轻松地使一条或多条 DS3 链路（45MPS）饱合。这种规模的大多数网络拥有较低的带宽，因此，网络需要仔细设计，以避免过溢现象的发生。允许远程站点使用分离隧道可帮助防止过溢。因为大多数 VPN 设备尚未具备可限制 VPN 流量或设备用户量的能力，头端的混合流量需要特别关注。

替代选项

专用站点到站点 VPN 设备

在这种设计中最常见的添加内容是凭借远程接入 VPN 集中器在同一网络或并行网络上添加专用站点到站点 VPN 设备。许多客户选择这一选项，因为他们喜欢将其 VPN 和防火墙功能分离至两台独立设备上。这样，防火墙就可以只执行防火墙保护，并允许站点到站点 VPN 设备只关注 IPSec。这种设备会为中型网络带来更高的可扩展性和管理性能。

分支机构和独立性

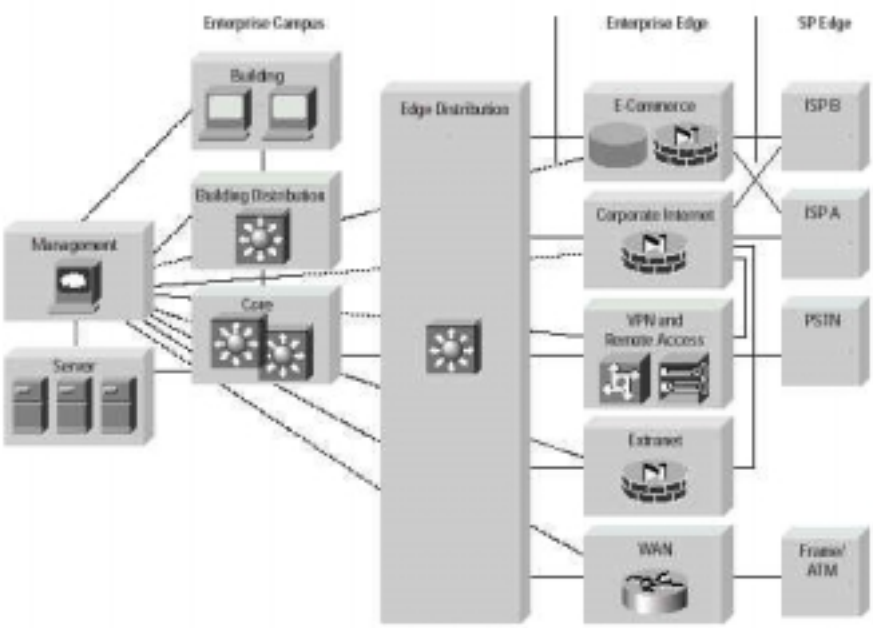
当在分支机构中进行配置时，可能不需要专用远程接入 VPN 集中器，因为这项服务将由总部负责提供。站点到站点功能可依旧存在于防火墙上，如果头端将 GRE IPSec 当作其主要隧道的话。如果使用了 GRE，站点到站点 VPN 需要转移到一个支持 GRE 的基于路由器的专用平台上。

另外，作为一家分支机构，VPN 设备更可能从远程站点进行管理。使用加密 ACL 会产生少许不同，还有一些设备，如边缘路由器，会位于 VPN 之外，因而需要一种单独的管理模式，这种管理可以通过离散隧道或使用应用级安全（SSH）协议来完成。请注意，并非所有管理协议都拥有安全可变异性。可考虑将 VPN 信息流的优先权设置在网络冲浪和其他信息流前面。

大型 VPN 设计

大型 VPN 设计采用了与 ISAFE 安全技术的大型企业网络设计相同的拓扑结构。大型网络 VPN 设计包含在大型企业 VPN 和远程接入模块中，可支持站点到站点和远程接入 VPN。该模块经重新设计，可提供高速的高可用性 VPN 端接功能。整个大型设计在下图中进行了介绍。

图 12.　大型网络的详细模型



企业园区网　　企业边缘　　SP 边缘

构建

边缘分布　　电子商务

管理　　构建分布　　公司互联网

核心　　VPN 和远程接入

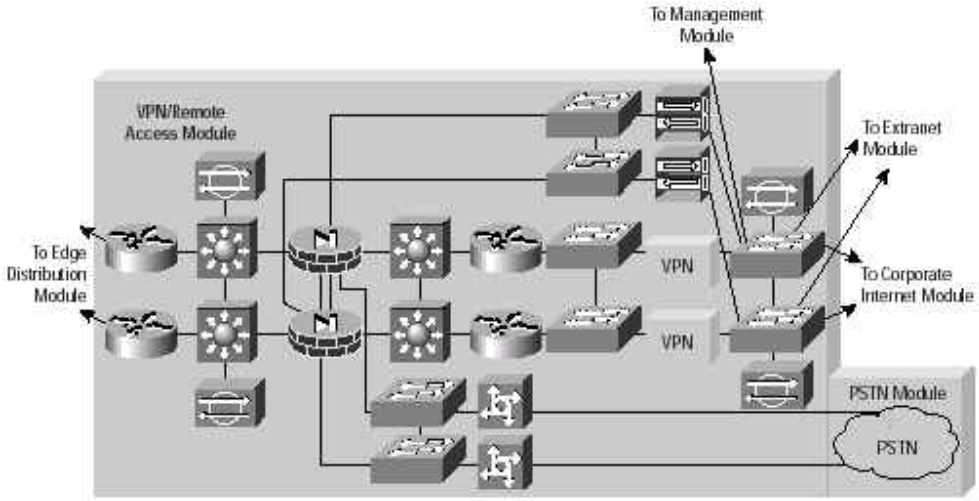
服务器　　外部网

帧中继/ATM

VPN 和远程接入模块

VPN 远程接入模块提供了远程用户、远程站点 VPN 信息流的端接功能，以及传统拨入用户的端接功能。设计师为站点到站点 VPN 端接提供了 VPN 路由器或 VPN 防火墙二种选择。该设备在下面的模块布局介绍中被标为“VPN “。由于 VPN 的高速需要，目标定义设备在整个模块中进行了部署，提供了不同的功能。

图 13.　VPN 和远程接入模块的详细模式



VPN/远程接入模块　　到管理模块

到外部网模块

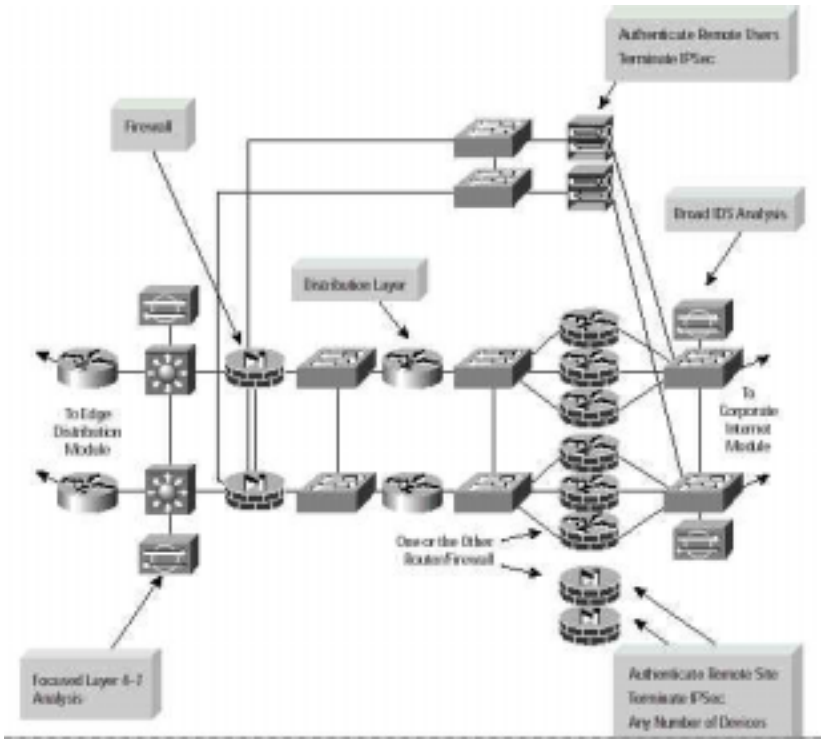
到边缘分布模块　　到公司互联网模块

PSIN 模块

关键 VPN 服务

- **内容防火墙**－为资源提供了网络级保护和信息流状态过滤
- **分布路由器**－跟踪 VPN 路由器的远程站点网络可用性
- **VPN 集中器**－利用 XAUTH 验证个别远程用户和端接其 IPSec 隧道
- **VPN 路由器**－验证信任远程站点和利用 GRE/IPSec 隧道提供连接功能
- **VPN 防火墙**－验证信任远程站点和提供远程站点信息流的状态过滤
- **NTDS 应用**－提供模块第 4－7 层的关键网络分段的监控功能

图 14.　大型网络 VPN 和远程接入模块 VPN 的详细模型



验证远程用户端接 IPSec

防火墙

宽型 IDS 分析

分布层

到边缘分布模块　　到公司互联网模块

一个或多个路由器/防火墙

第 4—7 层集中分析　　验证远程用户端接 IPSec

任意数量的设备

设计指南

模块的核心 VPN 需求是验证远程设备和端接 IPSec。多 VPN 端接设备可生成千兆位信息流负载，因而需要在模块中提供高速第三层交换功能，从端接设备的出口到边缘分析模块的入口。因为这一缘故，由于需要针对特殊服务提供分组归类，所以，内部路由选择和分布层功能是利用高速第三层交换来完成的。这些因素也推动了对下列功能的需要—用于状态审查的千兆位线速防火墙，在模块中所有信息流的过滤，以及用于攻击检测的高速 IDS。因为信息流来自企业网络外部的不同来源，所以，决定为这些服务中的每一项都提供一个独立的防火墙接口。有关这些服务的 VPN 功能设计构思在下面进行论述。外部网 VPN 在本文后面的外部网模块中进行了介绍。

远程接入 VPN

远程接入 VPN 信息流是由公司互联网模块接入路由器提交的，在作为远程接入 VPN 分段一部分的 IP 地址和协议的出口点进行了首次过滤。这些协议包括 IKE、ESP/UDD、NAT 透明度端口（如，UDP 端口 10000 在本文亦有所提及）。配置中的集中器只是针对隧道端接 IPSec 进行了配置。NAT 透明度模式在 VPN 集中器上的启用加速了远程接入客户机的连接。考虑到远程接入客户机的高安全风险，不允许使用分离隧道。一旦连接后，DNS、WINS 和虚拟 IP 地址都将输入远程接入客户机。在成功地验证后，分组级授权过滤器将被应用到用户的信息流。集中器被装备以硬件加速，以满足大型企业的可扩展性和性能需求。负载均衡功能被启用，以便为头端提供动态远程接入客户机负载均衡。继远程接入隧道端接之后，所有互联网或内部网信息流将通过防火墙发送，以确保 VPN 用户信息流得到相应地审查和过滤。

站点到站点 VPN

下面的讨论适用于两种站点到站点端接选项。VPN 所选择的拓扑结构为中心辐射型。分支使用 10.0.0.0/8 网络的可归纳子网。站点到站点 VPN 信息流是从公司互联网模块接入路由器提交的，在作为远程接入 VPN 分段一部分的 IP 地址和协议的出口点进行了首次过滤。这些协议包括 IKE 和 ESP。目标 IP 地址被限制于头端端接设备公共接口的 IP 地址，源地址被限制为已知静态远程站点 IP 地址。虽然过滤源地址提供了额外的安全性，如果动态地址远程站点可以得到支持，那么，这就不可能实现。可扩展性是一个问题。每个静态远程站点要求每台接入路由器配备 4 条 ACL 线（两个对等和每个对等一个 ESP 和 IKE 输出）。VPN 设备经配置可支持 IPSec（GRE 为可选支持内容）的隧道端接。这种设计规模的远程站点必须拥有防火墙保护功能；否则将难以满足网络的性能和可扩展性要求，如果所有信息流都路由选择至集线器站点的话。

远程站点参照 SAFE 安全技术中的中小型网络设计实施了防火墙保护。考虑到负载压力，VPN 设备配备了硬件加速功能，继站点到站点信息流端接后，所有内部网流量都通过防火墙发送，以使状态审查和通过分布路由选择层过滤。该层之所以能存在，是因为 VPN 路由器选项中，站点到站点 VPN 信息流必须从防火墙发送到可接入远程站点的 VPN 路由器。在故障情况下，可接入性可能会发生变化。但是，因为这些防火墙无法听取路由选择更新信息，所以不能确定哪台设备享有可接入性。分布路由选择层可允许分组通过 HSRP 接口的入口发送至单一 IP 地址，从而为防火墙提供支持。在出口处，它可利用路由选择协议来确定远程站点的可接入性。

适用于站点到站点 VPN 的 VPN 路由器选项

路由选择协议弹性被选为这种头端的高可用性机制。由于远程站点存在着不确定性因素，因而远程只限制于 VPN 路由器，如同在高可用性原则中所讨论过的一样。头端路由器的配置使其可以支持 IPSec 和 GRE。源于远程站点的路由选择协议更新，可通过主要的和备用隧道向头端播放，并在后端向分布路由器重新分布。在开放最短路径优先(OSPF)协议中选择了改进内部网关路由选择协议(EIGRP)，因为它的 CPU 开销较低，从头端的角度看，只有多点到点链路存在。所有远程站点的配置使其得以在头端 VPN 路由器故障的情况下，完成负载分散工作。在拥有数百节点的大型网络中，请遵循思科公司有关路由选择协议的最佳实施方法。

适用于站点到站点 VPN 的 VPN 防火墙选项

IKE 保持激活信息弹性被选为这种头端设备的高可用性机制。VPN 防火墙、VPN 路由器和 VPN 集中器都位于远程地点。头端 VPN 防火墙被配置成只可支持 IPSec。VPN 防火墙静态分配至远程站点网络，以触发输出隧道的建立。在设备故障的情况下，备用设备将在这种状态下，支持远程站点连接继续发挥作用。目前，在(所有 VPN 防火墙中)IPSec 隧道状态，站点到站点 VPN 信息流过滤发生在内部防火墙上，而非 VPN 防火墙，这样就可以为 VPN 端接提供尽可能多的空间。

身份

就远程地点到站点到站点的 VPN 连接而言，数字证书被用于严格和可扩展的设备验证。远程接入 VPN 连接采用了一种双项验证方案，它拥有设备分组预共享密钥，以及通过 OTP 的备用用户验证。

安全性

鉴于公司内部网的高水平接入，该模块采用了高水平的安全机制。VPN 防火墙上的状态防火墙软件只允许 IKE 和 ESP 信息流端接 VPN 防火墙的公共接口。VPN 集中器在其公共接口上只支持 ESP、IKE 和 UDP 端口 10000。发生在信息流传送至远程接入和 VPN 模块之前的过滤过程，只允许下列信息流通过：

- ESP、IKE、VDP 端口 10000，从任一地址到 VPN 集中器的公共和虚拟集群器 IP 地址
- ESP 和 IKE，从已知静态 IP 地址远程站点到 VPN 防火墙的公共 IP 地址
- ESP 和 IKE，从已知静态 IP 地址远程站点到 VPN 路由器的公共 IP 地址

上面未列出的信息流触发 IDS 检测器的严重损害报警。解密后，所有源于 VPN 的信息流都会快速提交给内部防火墙，然后过滤并接受状态审查。虽然信息流被提交给内部路由器，那个分段上的 IDS 会执行详细的第 4-7 层信息流分析。如果 IDS 在流动中检测到攻击，它会对防火墙的信息流进行规避。思科公司建议利用内部的 IDS 部署规避机制，因为分段中所使用的地址均为专用 10000 网址。利用 10000 网址实施欺骗的可能性即大幅度降低，即使发生发送该信息流的远程站点和用户通过分析隧道 SA，也很容易确认。

可扩展性

这种设计有极强的可扩展性。根据远程站点的不同带宽需求，该模块可支持 100-250 条远程站点隧道/设备，利用极低带宽远程站点时则可能会更多。因为环绕 VPN 设备的基础设施是专为高速需求而设计的，这种因素就不是一种限制因素。就大规模 VPN 设计而言，主要限制因素（鉴于所选择的高可用性机制）应用可端接的远程站点数量。远程接入用户端接可扩展到 5000 或更多同步用户。

安全管理

所有设备的安全管理是通过利用安全和非安全协议的组合来完成的，这些协议包括 SSH、SNMP、TFTP 和系统日志。该模块的所有管理工作都是通过带外管理网络来实施的。

NAT

NAT 未在该模块中使用。我们绕过了 NAT，以方便内部站点的 VPN 通信，通过使用非重叠 RFC1918 编址，可允许所有信任对象利用其真实 IP 地址进行交流。NAT 被用于公司互联网模块，但是当分离隧道被禁用时，可通过远程接入客户机转换 VPN 上使用的专用地址，以支持互联网接入。

路由选择

边缘分布知道远程用户和站点使用的是哪个子网。边缘分布路由器可利用一种缺省网络，以确定远程接入和 VPN 模块中这些子网的可接入性。所使用的缺省网络为内部防火墙和 IDS 分段。这样一来边缘分布路由器可利用其两个内部路由器，通过广告跟踪 VPN 模块的可用性。内部路由器也可以通过动态路由选择更新，反过来跟踪内部网可接入性，并将所有远程用户和站点目标信息流静态路由选择至防火墙。防火墙可将远程接入信息流静态路由选择至 VPN 集中器分段，并将远程站点信息流静态路由选择至分布路由器上的 HSRP 虚拟地址。当 VPN 路由器端接站点到站点信息流时，分布路由器可运行相同的路由选择协议，接收与远程站点网络可用性有关的更新内容。分布路由器还可为主企业网在路由选择表格中输入一条静态路径，以便重新分布，以使远程站点拥有接入公司内部网的能力。否则，远程站点就不可能接入主网，因为路由选择协议并不通过防火墙。

外部网

虽然您可以将 VPN 防火墙或 VPN 路由器用于外部网端接，但我们还是认真地建议您不要将合作伙伴或客户信息流与公司内部网信息流混在一起。为此我们在下面的章节中对外部网模块进行了介绍。

性能

大量的远程站点和用户将迫使系统采用高速低延迟硬件加速机制。鉴于网络的带宽需求，需要高速 WAN 链路，如 OC－3（155mpbs）或更高水平的速度。由于远程站点实施了分离隧道，这种设置会提高一些头端带宽需求，但禁用分离隧道的高速 DSL / 有线用户则可使数据群数量显著加大，VPN 集中器可支持对设备的用户数量进行限制，但是，不可以对每位用户的吞吐量进行限制。

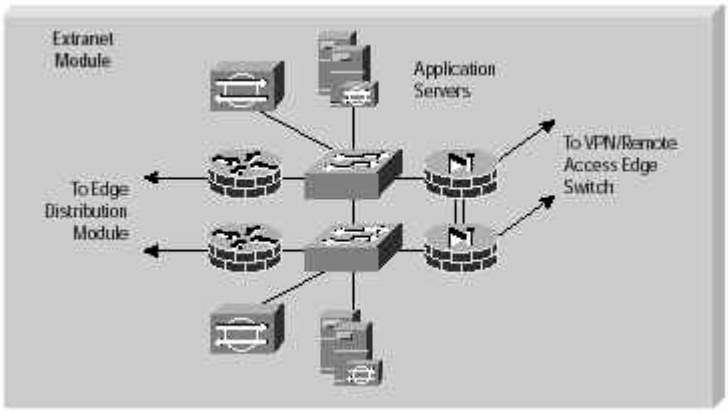
替代选项

如果选择了 VPN 路由器解决方案而且所需设备数量依然维持在低水平，那么，利用 VPN 路由器上的多 HSRP 分组来取代路由选择的分布层。但是，该解决方案并不能随着头端的扩充而发展。如果选择了 VPN 防火墙，可考虑在 VPN 防火墙上实施接入控制，因而无需将分布层路由器和内部防火墙连接在一起。如果个人防火墙软件按原则中的规定成功地部署，可考虑在头端实施远程接入客户机分离隧道，以降低性能要求。在这种设计中，相同的 WAN 基础设备被用于互联网接入、电子商务和 VPN。鉴于网络的性能要求，可能需要购置这种规模的专用 VPN WAN 基础设备。这种解决方案要求边缘的低带宽管理，因为只有 VPN 信息流被路由选择。您可以考虑将数字证书用于远程接入用户设备验证；但是，鉴于可扩展性要求，部署将极为困难。

外部网模块

外部网模块用于安全地端接站点到站点和基于远程接入的外部网，以便业务合作伙伴接入应用服务器。冗余 VPN 防火墙提供了 VPN 端接过滤和状态防火墙保护功能。N IDC 和主机 IDC（H IDC），鉴于数据的敏感性和用户控制域外接入数据的要求，需要加以部署。

图 15．大型外部网模块的详细模型



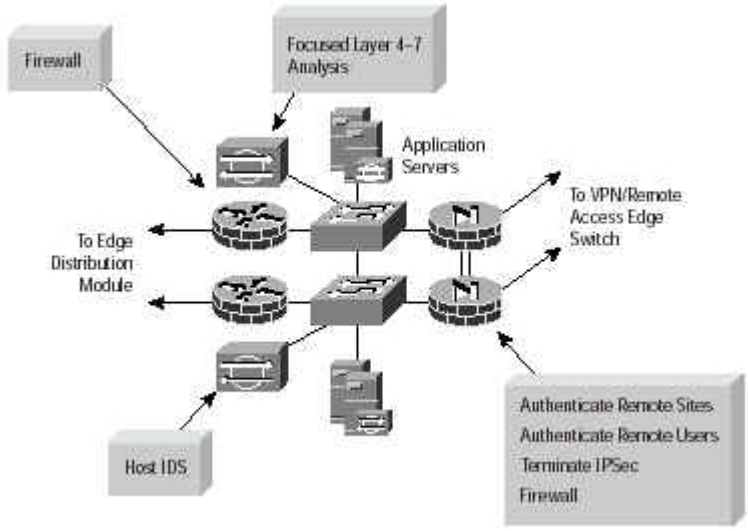
以太网模块　　应用服务器

到边缘分布模块　　到ＶＰＮ／远程接入边缘交换机

关键 VPN 设备

- **内部防火墙路由器**－－提供接入控制、状态防火墙保护和到公司内部网的接入能力
- **VPN 防火墙**－－验证某些信任远程站点并提供远程站点信息流的接入控制功能
- **NIDC 应用一**提供模块中关键网络分段的监控功能

图 1 6．大型外部网模块 VPN 的详细模型



防火墙　　第 4一 7 层集中分析

应用服务器

到边缘分布模块　　到 VPN／远程接入边缘交换机

主机 IDC　　验证远程站点

验证远程用户

端接 IPSec

防火墙

设计指南

该模块必须以一种适用于关键任务应用的高可用性和安全模式端接站点到站点和远程接入 VPN。安全必须是高水平的，因为端接 VPN 防火墙的远程站点接入设备不在企业管理员的控制之下，而且有时还被允许无需用户验证即可接入与公司内部隔一个跳转的应用服务器。无需基于标准的 IPSec 高可用性机制即可保证高可用性，这种想法是不现实的，降非使用同一供应商的产品。因此，除非存在这种情况，否则不要考虑模块可获得高可用性。有两种 VPN 防火墙被用于保护可能出现故障的设备或链路。远程 VPN 设备可由任意数量的 IPSec 设备构成。VPN 防火墙可配置成只支持 IPSec。鉴于数据的敏感性和可靠性的关系，使用了ＰＦＳ分组 2。

身份

在业务合作伙伴连接方面应用了数字证书来确认对等设备的身份，第三方数字证书供应商可作为您和您的业务合作伙伴的中间桥梁，并可提供更严格、更具可扩展性的设备验证。进入站点到站点 VPN 的用户无需用户验证。为此，建议应用服务器配备严格的应用级安全性能。远程接入 VPN 连接采用了一种双项验证方案，在设备上设立了分组预共享密钥，并通过 OTP 实施了备用用户验证。尽管使用了 OTP，但根据远程用户的数量不同，相关的费用可能会很高。虽然思科公司不建议您部署静态用户名和口令组，但如果您这样做了的话，应加速口令的老化进程。

安全性

鉴于合作伙伴连接所要求的高接入能力，该模块向世人展示了高水平的安全。VPN 防火墙上的状态防火墙软件可以支持 IKE 和 ESP 信息流端接其公共接口。公共互联网模块的过滤功能只支持 IKE 和 ESP 信息流到 VPN 防火墙的公共 IP 地址，如果远程设备的 IP 地址不是静态的，那么，基于源 IP 地址的过滤就无法实施。就远程接入 VPN 而言，这是常见的情况。除了 IKE 和 ESP 以外，导向 VPN 防火墙的其他信息流都会触发远程接入和 VPN 模块中的 IDC 检测器，使其发出严重危害告警。VPN 防火墙应只端接本地内部子网的 VPN 信息流。您应该在 VPN 防火墙上实施严格的输入ＡＣＬ，以完成这一工作。在 VPN 应用中，不可能控制远程设备分离隧道，除非您提供设备 / 软件。

如果不为 VPN 防火墙配置到内部网的路径，它就会向本地连接 OOB 管理网络发送分组，而不会向其它地方发送。内部防火墙路由器拥有接入控制功能，只支持应用服务器的 IP 地址，以及允许使用的服务通到内部网。应用服务器可将ＨIDC 用于本地攻击缓解，以便不受干扰，避免为黑客提供接入内部网的机会。如果部署在应用服务器子网上的ＮIDC 检测到攻击，它会发出严重危害告警。

可扩展性和性能

该模块是为大中型外部网而设计的。它利用硬件加速提供高速、低延迟的 VPN。外部模块将支持 200 多个远程站点和 500 多个远程同步用户。如果数量更大，应该增加更多的 VPN 设备。这需要路由选择层为应用服务器提供缺省路由。因为设备只支持外部网应用，就可实现高性能。

安全管理

利用安全和非安全混合协议（包括 SSＮ、ＳＮＭＤ、TFTP 和系统日志）可确保所有设备的安全管理。模块的所有管理工作都将通过 OOB 管理网络来完成。

NAT

只有连接远程站点的地址空间与应用服务器重叠时才可在 VPN 防火墙上使用 NAT。

路由选择

动态路由选择被用于内部防火墙路由器，以使应用网络信息流发送至边缘分布路由器。VPN 防火墙的路由不应存在于任何内部网络。

替代选项

主要的替代选项是使用 SSＬ和部署不同的设计。IPSec 的使用是以“永续运行”网络到网络接入是一种需求作为假设前提的。在设计中，合作伙伴网络的多台主机可接入应用分段。如果单一应用到应用接入是必须的，可考虑使用 SSＬ。

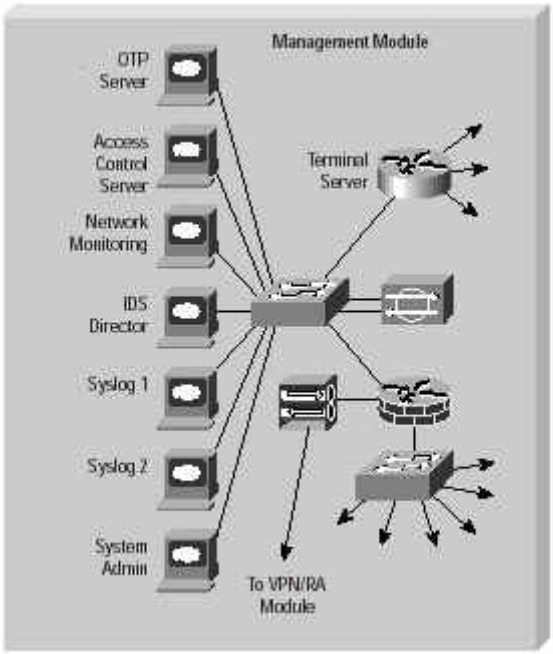
数字证书可为远程站点和用户提供更严格的设备验证，如原则规定中所述，但部署是一项显著的管理负担。除了设备验证以外，站点到站点信息流的用户验证也可以实施，但是，这种设备要求用户利用用户名 / 口令，首先连接快速应用，如 Telnet 或 Web。与应用级安全性相比，这种环境可能不会更安全，除非使用 OTP，而 OTP 会提高成本。

使用 VPN 路由器可以替代 VPN 防火墙。因为 VPN 路由器支持多数字证书身份，您将可同时使用内部 CA 和第三方或业务合作伙伴 CA。第一身份用于将 VPN 路由器识别为存在于您的网络基础设施中的设备，第二身份是用于合作伙伴设备的设备验证。因为该模块安装了远程接入和 VPN 模块，可能需要进行集成。您可能考虑在同一设备上端接合作伙伴和内部用户 VPN 信息流，但设备不允许这样做。在远程接入和 VPN 模块的防火墙中添加另一个接口以实现信息流分段是无理由的。

管理模块

管理模块的主要目的是推动企业 SAFE 体结构内所有设备和主机的安全管理。

图 17．大型管理模块的详细模型

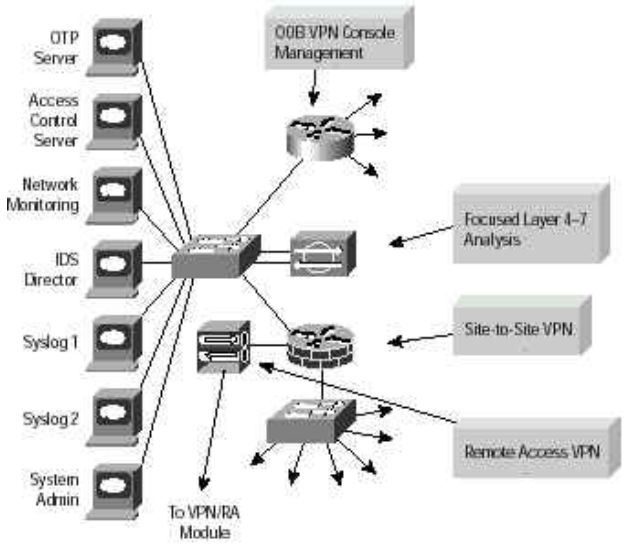


OTP 服务器　　管理模块
接入控制服务器　　终端用户
网络监控器
IDC 导向器
系统日志
系统管理　　到 VPN / RA 模块

关键 VPN 设备

- **防火墙和 VPN 路由器**－验证信任远程站点，提供状态过滤和 OOB 管理接入控制
- **VPN 集中器**－验证远程管理器和端接其 IPSec 隧道
- **NIDC 应用**－提供模块关键网络分段和 VPN 端接信息流的第 4－7 层监控功能

图 1 8．大型管理模块 VPN 的详细模型



OTP 服务器　　OOB　DN 控制台管理

接入控制服务器

网络监控器

IDC 导向器　　第 4－7 层集中分析

系统日志　　站点到站点 VPN

系统管理　　远程接入 VPN

设计指南

模块的功能几乎与原始 SAFE 安全企业技术中所描述的一致，只对内容的改变进行讨论。请参考 SAFE 安全技术资料以了解在这里未能讨论的信息。主要变化包括添加 VPN 集中器，以加速管理网络管理员的安全远程接入。如果该ＯＰＮ应用未能正确实施，就存在着高风险，尤其是影响整个网络。总而言之，这是一种在整个企业网中拥有每台系统接入能力的模块。凭借这种调整，现在，它可通过 VPN 集中器连接互联网。因此，在安全地实施设计过程中，每一步都采取了预防措施。

NAT

NAT 透明度模式在 VPN 集中器上被启用，以加速远程接入客户机连接。

身份

远程接入 VPN 连接采用了一种双项验证方案，将数字证书用于设备验证，并通过 OTP 实施备用用户验证。这种情况在 SAFEVPN 体系结构中堪称是唯一的，体系结构要求严格的设备验证和严格的用户验证。

安全性

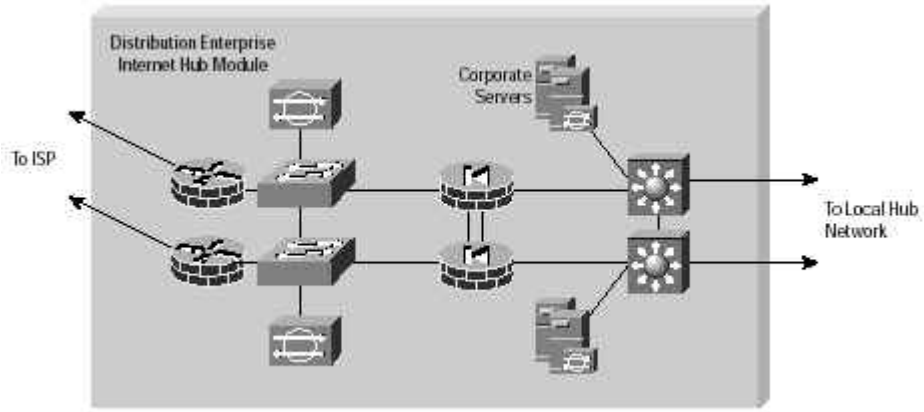
VPN 集中器被配置成只支持 IPSec。VPN 集中器的公共接口将只接受 IKE、ESP 和 UDP 端口 10000 分组，它们是发送给管理 VPN 集中器的。远程接入和 VPN 模块的边缘ＮIDC，如果有 IKE、ESP 或 UDP10000 以外的信息流导入管理 VPN 集中器，它将触发严重危害告警。带预共享密钥和其他敏感信息的配置信息极可能会穿越隧道。清楚这一点后，黑客可使用在管理信息流中发现的典型信息来猛烈攻击加密分组。因此，PFS 分组 2 在模块中被强迫置入。除非个人防火墙软件得以成功部署，或管理网通过状态防火墙被授予互联网接入权，否则，远程管理员不应支持分离隧道。即使如此，您也应考虑到可能的影响因素。在成功验证后，您应将管理员过滤器应用于隧道化信息流。管理

员只应对要使用的管理网应用拥有接入权。这种设备可帮助您缓解用户授予优先权错误配置的可能性，这种优先权可允许远程用户为非管理信息流建立隧道分流。在分组加密以及用户和接口过滤器应用后，信息流被提交给防火墙路由器，以便实施状态审查和另一轮过滤。只有在这种情况出现后，远程管理器信息流才可接入管理网设备。当接入设备时，管理模块中的ＮIDC 将规避ＶＰＮ集中器中可能显现为攻击或并非管理信息流的信息。

分布集线器模块

分布集线器模块用于端接基于站点到站点 VPN，并可提供 VPN 支持的小型分支站点，以及大型企业远程接入和 VPN 模块头端间的中间层。该层允许本地Ａ型分支站点互联，无需向企业集线器站点发送信息流。

图 1 9．分布 VPN 模块的详细模型

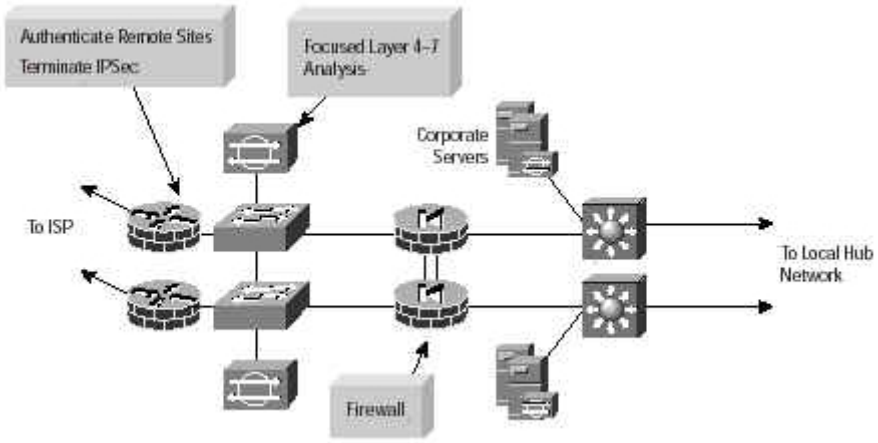


分布企业互联网集线器模块　　公司服务器
到ＩＳＰ　　到本地集线器网络

关键 VPN 设备

- VPN 路由器－验证信任远程站点，提供远程站点信息流的状态过滤和接入控制功能
- **防火墙－提供状态防火墙保护和过滤功能**
- **ＮIDC 应用**－提供模块关键网络分段的第 4－７层监控功能

图 20．分布 VPN 模块 VPN 的详细模型



验证远程站点端接　　第 4－7 层集中分析

公司服务器

到 ISP

到本地集线器网络

防火墙

设计指南

VPN 路由器负责端接远程站点和企业头端的信息流。大多数流量为分支到分支信息流。防火墙可为远程站点和本地服务间的所有信息流提供状态防火墙和过滤功能。部署 NIDC 是为检测远程站点的签名攻击和本地服务的受干扰情况的。服务通常包括数据库和应用，如邮件。我们做出了下列假设：

- 要求到分布集线器的分支高可用性
- 要求到头端集线器的分布层高可用性
- 可存在多台分布集线器，互联通过头端完成
- 通过分布集线器实施分支到分支互联

为此，在分布集线器站点和头端应部署 VPN 路由器，以便路由选择远程站点间的分组。分支可以是任何 VPN 设备，尽管 VPN 路由器的高可用性只有当把路由选择进协议用于高可用性时才能得以维持，由于在两隧道到头端之间利用了路由选择协议，分布 VPN 路由器可跟踪头端的可接入性。由于ＥＩＧＲＰ较低的ＣＰＵ成本，它被选用于ＯＳＰＦ。分布路由器可利用两个 HSRP 分组跟踪链路状态。因为每台 VPN 路由器被用作远程站点和独立组中的一个主设备，因此需要二个分组。在 VPN 路由器出现故障后，备用 VPN 路由器将接管假设为远程站点备用组的负载。因为分层防火墙无法接收路由选择更新信息，这将允许它们向拥有远程站点接入能力的有效 VPN 路由器发送分组。

假设远程 VPN 设备由一些拥有远程 VPN 路由器所确保高可用性的 VPN 设备组成。分支和分层本地网应使用企业主网的可归纳子网。分层站点不需要设置分离隧道，因为假设头端和分支站点都拥有该功能。如果远程站点没有这项功能，配置就会把改进性能和可扩展性需求指向头端和分层站点。模块假设分布层配备了两台 VPN 路由器。如果为满足网络各层的负载需求而要配备两台以上的设备，您应部署故障负载分散机制。

身份

就远程地点到站点到站点 VPN 连接而言，可将数字证书用于严格和可扩展的设备验证。

安全性

应予以说明的是，当信息流从分支流向分支或从分支流向头端时分支，不会有 IDC 或防火墙保护功能发挥效用。因为防火墙和 IDC 设施存在于头端，因而没有理由执行该功能两次，当有远程站点接入本地服务时，状态防火墙保护和过滤机制将发生作用。对 VPN 路由器公共接口输入信息的过滤功能，只支持已知静态 IP 地址远程站点和头端的 ESP 和 IKE。

可扩展性

模块旨在提高大型企业中心辐射网络的可扩展性。该分布层拥有可扩展至 200 或更多远程站点的能力。

安全管理

所有设备的安全管理都是通过安全和非安全混合协议来完成的，它们包括 SSH、SNMP、TFTP 和系统日志。模块中的所有管理工作都是通过到头端管理模块的带内 VPN 隧道来实施的。

NAT

NAT 在本模块中未使用，因为所有编址的处理对 VPN 是专用的，除了 VPN 信息流外，不允许互联网接入。

路由选择

VPN 路由器拥有到互联网的缺省路径。该路径涉及所有公共 IKE 对等，以及远程和头端站点专用网络。只有本地网络是静态路由至防火墙组的。本地分层防火墙负责向各虚拟 HSRP 地址提交远程站点一半的流量。指向头端的信息流被发送至 HSRP 分组和基于 IP 地址的负载均衡机制。

性能

多分支，以及对分支对分支互联的需要推动了对 VPN 设备低延迟、高性能的需求。鉴于这些设备的带宽容量和远程站点的数量，需要配备高速 WAN 链路，如 DS3（45xxbps）或更高速的产品。

替代选项

如果远程站点不支持分离隧道，而分布层需要执行这一功能，可考虑在中小型厂商设计中所列举的分离隧道的方案。现行的分布集线器模块将不适合分离隧道，因为它会在防火墙和 VPN 路由器间的同一线路上将解密和明码互联网信息流进行混合。如果为满足性能需求要配备两台以上的 VPN 路由器，可添加更多的 VPN 路由器，并考虑在现有 VPN 路由器分段前添加 WAN 路由选择层。请注意，这是一种与大型企业头端类似的设计，因此，应配置故障负载分散机制，以提高可扩展性。为建立这种路由选择机制，应用协议取代多 HSRP 分组，以支持可扩展性。

迁移策略

SAFE VPN 是 VPN 实施向导。这里所推荐的设计不是用作向所有现行网络提供 VPN R 的设计方案。实际上，SAFE VPN 是一种模块，可为网络设计师设计，实施企业 VPN，以满足其安全性和连接需求。

提供支持把远程用户和站点数量，及其相关性能、应用和可靠性要求归纳成目录，应成为迁移现行网络至 VPN 的首项活动。下一步是设计一个网络，以安全、可扩展的方式支持这些要求。有关 VPN 安全性和 VPN 部署的基本建议在本文的原则部分进行了深入的探讨。在将这些构思应用到现行网络的效果进行确定后，网络设计师将研究如何把它们应用于现行网络基础设施。

体系结构拥有充足的灵活性，为 SAFE VPN 被大多数网络所接受提供支持。SAFE VPN 允许设计师就各个网络功能对 VPN 应用进行说明，几乎可以各自独立进行。每个模块都装备齐全，可连接至体系结构中其他的 VPN 支持模块。因为 VPN 是一种网络接入替代技术，可与现行专用链路连接网络合并部署。单一目的 VPN 设备通过将新功能与现行基础设施分隔简化了迁移过程，因而降低了对网络构成不利影响的可能性。当着手开始制作时，简单的路由选择接入即可开通。

这是详细介绍 SAFE 体系结构的第三份白皮书。与 SAFE 企业版和 SAFE SM B 相结合后可对各种规模网络的 VPN 安全性需求和实施进行系统说明。作者十分清楚，文中的许多领域需要深入研究、解释和改进。这些领域包括（但不限制于）下列内容：

- VPN 管理的深入分析和实施
- Cos 语言和实施
- VPN 和 DDR 共存
- 有关身份、目录服务、AAA 技术和 CA 分析和实施的深入分析
- 有关园区网和无线 VPN 设计、管理和实施的深入分析

附录A：验证实验室

这里提供了一份 SAFE VPN 实施参考资料，用于确认文中所述功能。该附录对设备的配置，就其与各模块 VPN 功能的关系进行了详细介绍。它收录了各模块内设备的配置情况，以及通用设备配置的总体指南。下面是实验室中现场设备的配置概述。作者建议您不要将这些配置直接用于制作网络。请注意，VPN 设备的接入控制，用于确保只有 IKE（UDP 端口 500）和 ESP（IP 协议 50）接入的机制在本文中并未介绍；对于这些配置，请参考 SAFE 安全技术资料。

总体指南

本节中所展示的样本命令与本文前面所论述过的 SAFE VPN 原则相对应。

```
 SAFE VPN Configuration parameters
!下面样本命令用于支持大多数基本配置选项，它们出现于SAFE VPN实验室的所有VPN路由器。
SAFE VPN standard IKE policy
crypto isakmp policy 10
encr 3des
authentication rsa-sig
group 2
hash sha
!
! Typical CA identity
!
crypto ca identity safevpn
enrollment mode ra
enrollment url http://172.16.128.50:80/certsrv/mscep/mscep.dll
!
!
!
! High entropy and unique per-address pre-shared key
!
crypto isakmp key 7Q!r$y$+xE address 172.16.144.3
!
! Digital Certificates (CA,RA, encryption and signing)
!
crypto ca certificate chain safevpn
certificate 613500AA000000000007
308203EB 30820395 A0030201 02020A61 3500AA00 00000000 07300D06 092A8648
86F70D01 01050500 306C310B 30090603 55040613 02555331 0B300906 03550408
13024341 3111300F 06035504 07130853 616E204A 6F736531 1B301906 0355040A
13124369 73636F20 53797374 656D732C 20496E63 310D300B 06035504 0B130456
53454331 11300F06 03550403 1308496E 7465726E 6574301E 170D3031 30363230
32333230 35385A17 0D303230 36323032 33333035 385A3027 31253023 06092A86
4886F70D 01090213 16523236 32312D31 2E736166 652D736D 616C6C2E 636F6D30
819F300D 06092A86 4886F70D 01010105 0003818D 00308189 02818100 9F88ECFF
D3213656 C027D6AC 08076401 16D75A25 643E8881 CA2BA5B1 6215C0A7 9C80C831
```

6A469DB5 72B1A530 72492649 D42812B2 AB26E536 61CEFFFE 468CADE4 A9A498F2
F2E134F4 F2780C81 B5C1B1CB 45EE5DBD 336F5842 954F37CE E81FACCD 384CB388
141BD5E1 1015DB15 AF2BDD5F 2D67BB19 D9708F68 58A99A8E 5DEC20F1 02030100
01A38202 18308202 14300B06 03551D0F 04040302 05A0301D 0603551D 0E041604
1442A32E 697145AF 42211881 2396DA0B 96C39C74 003081A5 0603551D 2304819D
30819A80 14BFB4E5 C7D8D6B6 55FCC1CB 6F5B2C48 1C1C1A34 02A170A4 6E306C31
0B300906 03550406 13025553 310B3009 06035504 08130243 41311130 0F060355
04071308 53616E20 4A6F7365 311B3019 06035504 0A131243 6973636F 20537973
74656D73 2C20496E 63310D30 0B060355 040B1304 56534543 3111300F 06035504
03130849 6E746572 6E657482 102E9E46 057DECA2 8C42F3BF 9C90639D 3F302406
03551D11 0101FF04 1A301882 16523236 32312D31 2E736166 652D736D 616C6C2E
636F6D30 73060355 1D1F046C 306A3032 A030A02E 862C6874 74703A2F 2F696E74
65726E65 742D6D73 61632F43 65727445 6E726F6C 6C2F496E 7465726E 65742E63
726C3034 A032A030 862E6669 6C653A2F 2F5C5C69 6E746572 6E65742D 6D736163
5C436572 74456E72 6F6C6C5C 496E7465 726E6574 2E63726C 3081A206 082B0601
05050701 01048195 30819230 4606082B 06010505 07300286 3A687474 703A2F2F
696E7465 726E6574 2D6D7361 632F4365 7274456E 726F6C6C 2F696E74 65726E65
742D6D73 61635F49 6E746572 6E65742E 63727430 4806082B 06010505 07300286
3C66696C 653A2F2F 5C5C696E 7465726E 65742D6D 7361635C 43657274 456E726F
6C6C5C69 6E746572 6E65742D 6D736163 5F496E74 65726E65 742E6372 74300D06
092A8648 86F70D01 01050500 03410024 8B79077E 37C7C8EA 1C53FAAB 92264274
1E875C7A 809618B0 5A5B1719 5F4FC690 9B8D8320 14ACD7DD 0F8035F8 CA18644D
79588D7F 156F4EA4 805952FA B39EC8
quit
certificate ra-sign 47364E9E000000000002
30820456 30820400 A0030201 02020A47 364E9E00 00000000 02300D06 092A8648
86F70D01 01050500 306C310B 30090603 55040613 02555331 0B300906 03550408
13024341 3111300F 06035504 07130853 616E204A 6F736531 1B301906 0355040A
13124369 73636F20 53797374 656D732C 20496E63 310D300B 06035504 0B130456
53454331 11300F06 03550403 1308496E 7465726E 6574301E 170D3031 30363230
32323232 31345A17 0D303230 36323032 32333231 345A3081 9D312030 1E06092A
864886F7 0D010901 16116164 6D696E40 73616665 76706E2E 636F6D31 0B300906
03550406 13025553 310B3009 06035504 08130243 41311330 11060355 0407130A
54686520 56616C6C 65793116 30140603 55040A13 0D534146 45205650 4E20496E
632E311C 301A0603 55040B13 13534146 45205650 4E204272 61696E74 72757374
31143012 06035504 03130B53 41464520 56504E20 43413081 9F300D06 092A8648
86F70D01 01010500 03818D00 30818902 818100BB 73EF0897 57DFDC7C 0F72482D
39EE9562 E1291155 AB6F5627 338BE5A7 BF2F2904 BD643F7A 63EF9EDB 75ED8C44
D006503E 1A88D16D 45AF4E31 E5B01EBE 1BC829E0 4A5A3701 E3CC67B5 270BB2DE
80561B60 96732CD6 D6FF7601 4920A82B ADBA0EF0 F3AA24D2 D5D2D64F 21EDB990
3E51A64F 3C1DCBA6 94AA6B3F 21DED3BC FB392102 03010001 A382020C 30820208
300E0603 551D0F01 01FF0404 030206C0 30150603 551D2504 0E300C06 0A2B0601
04018237 14020130 1D060355 1D0E0416 0414726C 201817B0 D5C56A58 DEEB6024
5FF2DED6 B6BE3081 A5060355 1D230481 9D30819A 8014BFB4 E5C7D8D6 B655FCC1
CB6F5B2C 481C1C1A 3402A170 A46E306C 310B3009 06035504 06130255 53310B30
09060355 04081302 43413111 300F0603 55040713 0853616E 204A6F73 65311B30
19060355 040A1312 43697363 6F205379 7374656D 732C2049 6E63310D 300B0603
55040B13 04565345 43311130 0F060355 04031308 496E7465 726E6574 82102E9E

```
46057DEC A28C42F3 BF9C9063 9D3F3073 0603551D 1F046C30 6A3032A0 30A02E86
2C687474 703A2F2F 696E7465 726E6574 2D6D7361 632F4365 7274456E 726F6C6C
2F496E74 65726E65 742E6372 6C3034A0 32A03086 2E66696C 653A2F2F 5C5C696E
7465726E 65742D6D 7361635C 43657274 456E726F 6C6C5C49 6E746572 6E65742E
63726C30 81A20608 2B060105 05070101 04819530 81923046 06082B06 01050507
3002863A 68747470 3A2F2F69 6E746572 6E65742D 6D736163 2F436572 74456E72
6F6C6C2F 696E7465 726E6574 2D6D7361 635F496E 7465726E 65742E63 72743048
06082B06 01050507 3002863C 66696C65 3A2F2F5C 5C696E74 65726E65 742D6D73
61635C43 65727445 6E726F6C 6C5C696E 7465726E 65742D6D 7361635F 496E7465
726E6574 2E637274 300D0609 2A864886 F70D0101 05050003 41006094 1ACE2B69
CF9729A0 6325E48B 2C2D1C21 493748A6 9CCAD32E F1CE0C5E A1C51CD0 3C5404A6
AD6CACF6 4381884D 1128C62A CD8C6DB5 76D205BA 68FDC8E8 86CA
quit
certificate ca 2E9E46057DECA28C42F3BF9C90639D3F

308202A0 3082024A A0030201 0202102E 9E46057D ECA28C42 F3BF9C90 639D3F30
0D06092A 864886F7 0D010105 0500306C 310B3009 06035504 06130255 53310B30
09060355 04081302 43413111 300F0603 55040713 0853616E 204A6F73 65311B30
19060355 040A1312 43697363 6F205379 7374656D 732C2049 6E63310D 300B0603
55040B13 04565345 43311130 0F060355 04031308 496E7465 726E6574 301E170D
30313036 30363139 35373538 5A170D30 33303630 36323030 3632355A 306C310B
30090603 55040613 02555331 0B300906 03550408 13024341 3111300F 06035504
07130853 616E204A 6F736531 1B301906 0355040A 13124369 73636F20 53797374
656D732C 20496E63 310D300B 06035504 0B130456 53454331 11300F06 03550403
1308496E 7465726E 6574305C 300D0609 2A864886 F70D0101 01050003 4B003048
024100BF 6EDF974C 2BAB7BD1 7146096A 11413145 663A67F9 3B8893B0 585F188E
41CBBEB4 24C2C154 EAC65101 CF43AC28 D970A6CF 4448E9E2 CA0B7288 76AF561C
871B4102 03010001 A381C730 81C4300B 0603551D 0F040403 0201C630 0F060355
1D130101 FF040530 030101FF 301D0603 551D0E04 160414BF B4E5C7D8 D6B655FC
C1CB6F5B 2C481C1C 1A340230 73060355 1D1F046C 306A3032 A030A02E 862C6874
74703A2F 2F696E74 65726E65 742D6D73 61632F43 65727445 6E726F6C 6C2F496E
7465726E 65742E63 726C3034 A032A030 862E6669 6C653A2F 2F5C5C69 6E746572
6E65742D 6D736163 5C436572 74456E72 6F6C6C5C 496E7465 726E6574 2E63726C
30100609 2B060104 01823715 01040302 0100300D 06092A86 4886F70D 01010505
00034100 7E74B2F7 15D185EC 5C89DE9C 0F0E0E12 6F90397F 4AAE9E26 6D0025F6
F0A06935 F3D842F6 98689B35 FDF175F7 8CBDDEE6 6201B69A 415624A5 6D130AEE ACA5B1
F1
quit
certificate ra-encrypt 47364F88000000000003
30820456 30820400 A0030201 02020A47 364F8800 00000000 03300D06 092A8648
86F70D01 01050500 306C310B 30090603 55040613 02555331 0B300906 03550408
13024341 3111300F 06035504 07130853 616E204A 6F736531 1B301906 0355040A
13124369 73636F20 53797374 656D732C 20496E63 310D300B 06035504 0B130456
53454331 11300F06 03550403 1308496E 7465726E 6574301E 170D3031 30363230
32323232 31345A17 0D303230 36323032 32333231 345A3081 9D312030 1E06092A
864886F7 0D010901 16116164 6D696E40 73616665 76706E2E 636F6D31 0B300906
03550406 13025553 310B3009 06035504 08130243 41311330 11060355 0407130A
```

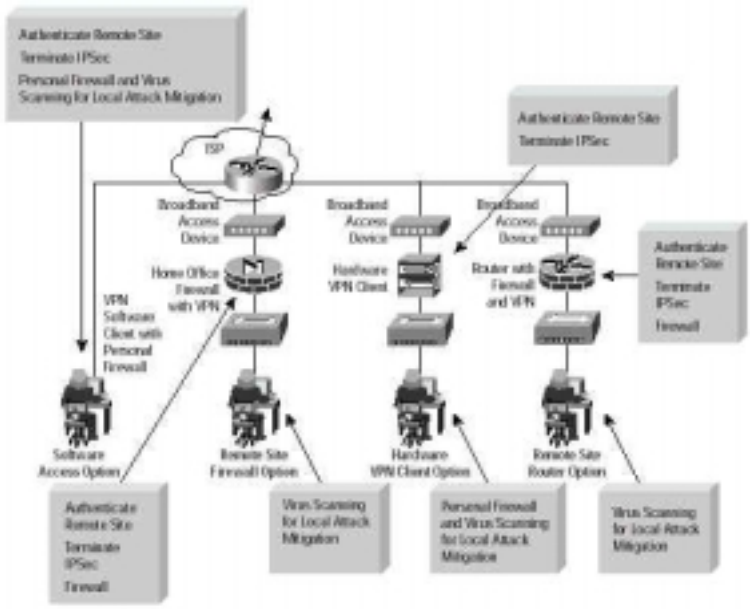
```
54686520 56616C6C 65793116 30140603 55040A13 0D534146 45205650 4E20496E
632E311C 301A0603 55040B13 13534146 45205650 4E204272 61696E74 72757374
31143012 06035504 03130B53 41464520 56504E20 43413081 9F300D06 092A8648
86F70D01 01010500 03818D00 30818902 818100BC 14978E5B 9522DF96 E75DB97B
2556553C 9D9E78C6 A1B634CF D49D05A8 C45D9483 E5EC53F4 6FBA51AC 186FA67C
F2320FE4 B6BDA64C 28D1E646 5298A5BC 968132AD 222D99BE 76EB1EC7 BC8076ED
88F44D24 8F9A24FF E2161187 4CFA012F 5E309430 286D77FF 6A920E61 C8325711
1FFB19D3 51EB83C3 6157DA98 3F25104B EF62BF02 03010001 A382020C 30820208
300E0603 551D0F01 01FF0404 03020430 30150603 551D2504 0E300C06 0A2B0601
04018237 14020130 1D060355 1D0E0416 04146BDB 14526D6C 833A6F9B A033FE55
6B2D3E80 84723081 A5060355 1D230481 9D30819A 8014BFB4 E5C7D8D6 B655FCC1
CB6F5B2C 481C1C1A 3402A170 A46E306C 310B3009 06035504 06130255 53310B30
09060355 04081302 43413111 300F0603 55040713 0853616E 204A6F73 65311B30
19060355 040A1312 43697363 6F205379 7374656D 732C2049 6E63310D 300B0603
55040B13 04565345 43311130 0F060355 04031308 496E7465 726E6574 82102E9E
46057DEC A28C42F3 BF9C9063 9D3F3073 0603551D 1F046C30 6A3032A0 30A02E86
2C687474 703A2F2F 696E7465 726E6574 2D6D7361 632F4365 7274456E 726F6C6C
2F496E74 65726E65 742E6372 6C3034A0 32A03086 2E66696C 653A2F2F 5C5C696E
7465726E 65742D6D 7361635C 43657274 456E726F 6C6C5C49 6E746572 6E65742E
63726C30 81A20608 2B060105 05070101 04819530 81923046 06082B06 01050507
3002863A 68747470 3A2F2F69 6E746572 6E65742D 6D736163 2F436572 74456E72
6F6C6C2F 696E7465 726E6574 2D6D7361 635F496E 7465726E 65742E63 72743048
06082B06 01050507 3002863C 66696C65 3A2F2F5C 5C696E74 65726E65 742D6D73
61635C43 65727445 6E726F6C 6C5C696E 7465726E 65742D6D 7361635F 496E7465
726E6574 2E637274 300D0609 2A864886 F70D0101 05050003 4100A0ED 49063B8B

320DCEC8 F2FC6A7A 0D5F6BE3 C1772559 FE914CE8 C681C685 B7D6B4F7 4785383A
98E8E280 0BAEB8C9 499F44FB 014FB4C2 DB4AEAAD 4B2B82E0 35A6
quit
!
! SAFE VPN standard IPSec SA transform set
!
crypto ipsec transform-set strong esp-3des esp-sha-hmac
!
! Example crypto ACLs for remote management
!
access-list 150 permit ip host 172.16.128.2 host 172.16.144.51
!
! crypto map definition for remote management traffic
!
crypto map main_map 150 ipsec-isakmp
set peer 172.16.128.2
set transform-set strong
match address 150
!
! CEF is enabled on all VPN Devices as this is the optimized path
!
```

```
ip cef
!
```
以下是支持SAFE　VPN实验室　中所有VPN防火墙上的基本配置选项的样本命令。
```
!
! IKE must be explicitly enabled on VPN Firewalls
!
isakmp enable outside
!
! SAFE VPN standard IKE policy
!
isakmp policy 10 authentication rsa-sig
isakmp policy 10 encryption 3des
isakmp policy 10 hash sha
isakmp policy 10 group 2
!
! Typical CA identity
!
ca identity safevpn 172.16.128.50:/certsrv/mscep/mscep.dll
ca configure safevpn ra 1 20
!
! High entropy and unique per-address pre-shared key, hidden
!
isakmp key ******** address 172.16.144.3 netmask 255.255.255.255
!
! SAFE VPN standard IPSec SA transform set
!
crypto ipsec transform-set strong esp-3des esp-sha-hmac
!
! Example crypto ACLs for remote management
!
access-list 103 permit ip host 172.16.128.5 host 172.16.144.51
!
! Crypto map definition for remote management traffic
!
crypto map main_map 150 ipsec-isakmp
crypto map main_map 150 match address 103
crypto map main_map 150 set peer 172.16.144.3
crypto map main_map 150 set transform-set strong
!
```

远程用户设计模块配置

图 21.远程用户网络的攻击缓解规则



验证远程站点

端接 IPSec

个人防火墙和病毒扫描

用于本地攻击缓解

验证远程站点

端接 IPSec

宽带接入设备　　宽带接入设备　　宽带接入设备

带 VPN 的家庭办公防火墙　　硬件 VPN 客户机　　带防火墙和 VPN 的路由器　验证远程站点端接 IPSec 防火墙

软件客户机带个人防火墙

软件接入选项　　远程站点防火墙选项　　硬件 VPN 客户机选项　　远程站点路由器选项

验证远程站点端接 IPSec 防火墙　　病毒扫描用于本地攻击缓解　个人防火墙和病毒扫描，用于本地攻击缓解

病毒扫描用于本地攻击缓解

下列配置示例是用于连接小型企业的远程宽带 VPN 路由器。

```
! Crypto ACL for local network to head-end
!
access-list 103 permit ip 10.5.0.0 0.0.0.255 10.0.0.0 0.255.255.255
!
! Single crypto map entry, no HA
!
crypto map main_map 10 ipsec-isakmp
set peer 172.16.144.3
set transform-set strong
match address 103
```

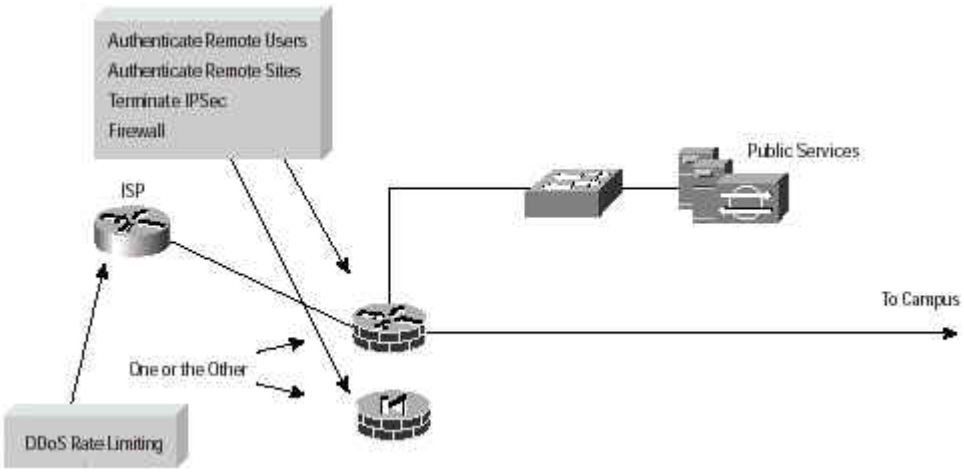
```
!
! Crypto map attached to public interface, we used a LAN interface although a broadband interface could have been used. 3des-sha
encryption used.
!
interface FastEthernet0/1
ip address 172.16.128.2 255.255.255.0
crypto map main_map
!
interface FastEthernet0/0
ip address 10.5.1.2 255.255.255.0
!
! Default route triggers all traffic to hit crypto ACL
!
ip route 0.0.0.0 0.0.0.0 172.16.128.1
!
```

下列配置示例是用于连接到小型企业的远程 VPN 防火墙

```
!
! Crypto ACL for local network to head-end
!
access-list 101 permit ip 10.6.0.0 255.255.255.0 10.0.0.0 255.0.0.0
!
ip address outside 172.16.128.5 255.255.255.0
ip address inside 10.6.1.1 255.255.255.0
!
! Default route to forward packets to IKE peers and remote VPNs
!
route outside 0.0.0.0 0.0.0.0 172.16.128.3 1
!
! Crypto map attached to public interface, 3des-sha encryption used.
!
crypto ipsec transform-set 3dessha esp-3des esp-sha-hmac
crypto map remote1 20 ipsec-isakmp
crypto map remote1 20 match address 101
crypto map remote1 20 set peer 172.16.144.3
crypto map remote1 20 set transform-set strong
crypto map remote1 interface outside
!
! Bypass NAT engine on firewall for traffic bound for VPN
!
access-list nonat permit ip 10.6.0.0 255.255.255.0 10.0.0.0 255.0.0.0
access-list nonat deny ip 10.6.0.0 255.255.255.0 any
!
!nat (inside) 0 access-list nonat
!
```

小型企业配置

图 22.小型企业公司互联网模块 VPN



验证远程用户

验证远程站点

端接 IPSec
防火墙
公共服务
一个或多个
速率限制

下列配置示例是用于小型企业的 VPN 路由器选项，它被视为头端的远程站点

```
!
! Crypto ACLs for local networks to remote sites
!
access-list 107 permit ip 10.4.0.0 255.255.0.0 10.5.0.0 255.255.255.0
!
access-list 108 permit ip 10.4.0.0 255.255.0.0 10.6.0.0 255.255.255.0
!
!ip address outside 172.16.144.3 255.255.255.0
ip address inside 10.4.1.1 255.255.255.0
!
! Default route to forward packets to IKE peers and remote VPNs
!
route outside 0.0.0.0 0.0.0.0 172.16.144.2 1
!
! Bypass firewall access-control for traffic inbound on outside interface
!
```

```
crypto map main_map 30 ipsec-isakmp
crypto map main_map 30 match address 107
crypto map main_map 30 set peer 172.16.128.2
crypto map main_map 30 set transform-set main_map
!
crypto map main_map 40 ipsec-isakmp
crypto map main_map 40 match address 108
crypto map main_map 40 set peer 172.16.128.5
crypto map main_map 40 set transform-set main_map
crypto map main_map interface outside
!
! Dynamic crypto map entry for remote access clients (note: no set peer or ACL)
!
crypto dynamic-map vpnuser 20 set transform-set main_map
crypto map main_map 50 ipsec-isakmp dynamic vpnuser
!
! Commands needed to enable MODCFG and XAUTH
!
crypto map main_map client configuration address initiate
crypto map main_map client authentication vpnauth
!
! List of the networks to bypass NAT when going into the VPN
!
access-list nonat permit ip 10.4.0.0 255.255.0.0 10.5.0.0 255.255.0.0
access-list nonat permit ip 10.4.0.0 255.255.0.0 10.6.0.0 255.255.0.0
access-list nonat permit ip 10.4.1.0 255.255.255.0 10.4.3.0 255.255.255.0
access-list nonat permit ip 10.4.2.0 255.255.255.0 10.4.3.0 255.255.255.0
access-list nonat permit ip 10.4.1.0 255.255.255.0 10.4.2.0 255.255.255.0
!
nat (inside) 0 access-list nonat
!
```

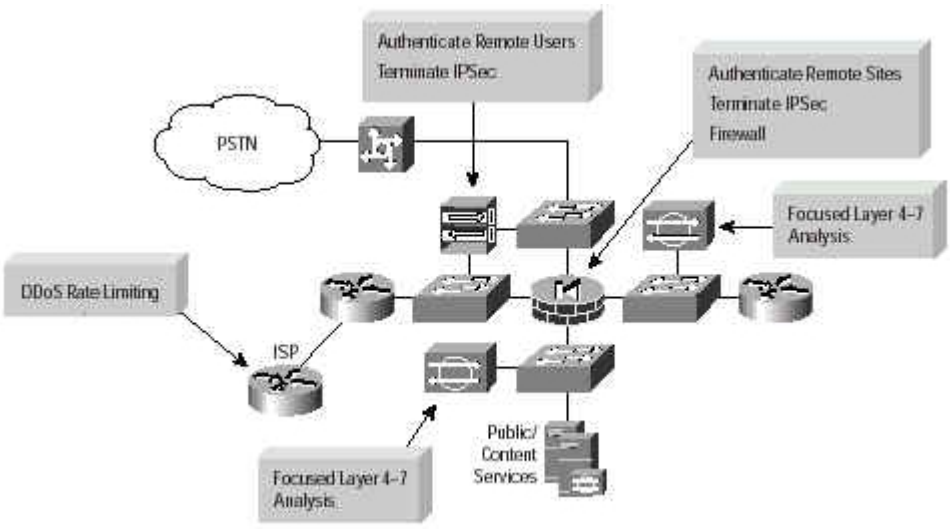
下列配置示例是用于小型企业 VPN 防火墙选项，它被视为头端的远程站点

```
!
! Crypto ACLs for local networks to remote sites
!
access-list 107 permit ip 10.4.0.0 0.0.255.255 10.5.0.0 0.0.0.255
!
access-list 108 permit ip 10.4.0.0 0.0.255.255 10.6.0.0 0.0.0.255
!
! Crypto map entries for VPN Router and VPN Firewall remote sites
!
crypto map main_map 10 ipsec-isakmp
set peer 172.16.128.2
set transform-set strong
match address 107
```

```
crypto map main_map 20 ipsec-isakmp
set peer 172.16.128.5
set transform-set strong
match address 108
!
! Crypto map enabled on public interface
!
interface FastEthernet0/0
ip address 10.4.1.1 255.255.255.0
!
interface Serial1/0
ip address 172.16.132.2 255.255.255.0
crypto map ent1
!
! Default route to forward packets to IKE peers and remote VPNs
!
ip route 0.0.0.0 0.0.0.0 172.16.132.1
!
```

中型企业配置

图 23.中型企业公司互联网模块 VPN



验证远程用户

端接 IPSec　　验证远程用户

端接 IPSec

第 4-7 层集中分析

速率限制

第 4-7 层集中分析　　公共/内容服务

下列配置示例是用于中型企业的 VPN 防火墙，它被视为头端的远程站点。

```
!
! Crypto ACLs for local networks to remote sites
!
access-list remote_concentrators permit ip 10.0.0.0 255.0.0.0 10.9.0.0 255.255.255.0
!
access-list remote_routers permit ip 10.0.0.0 255.0.0.0 10.12.0.0 255.255.255.0
!
access-list remote_firewalls permit ip 10.0.0.0 255.0.0.0 10.11.0.0 255.255.255.0
!
ip address outside 172.16.240.1 255.255.255.0
ip address inside 10.3.4.1 255.255.255.0
!
! Default route to forward packets to IKE peers and remote VPNs local static routes
!
route outside 0.0.0.0 0.0.0.0 172.16.240.2 1
route inside 10.3.1.0 255.255.255.0 10.3.4.2 1
route inside 10.3.2.0 255.255.255.0 10.3.4.2 1
route inside 10.3.3.0 255.255.255.0 10.3.4.2 1
route inside 10.3.8.0 255.255.255.0 10.3.4.1 1
!
! Static route for remote access client virtual IP addresses
!
route vpn 10.3.7.0 255.255.255.0 10.3.5.5 1
!
! Crypto map entries for multiple remote device types
!
crypto map main_map 10 ipsec-isakmp
crypto map main_map 10 match address remote_firewalls
crypto map main_map 10 set peer 172.16.144.5
crypto map main_map 10 set transform-set strong
!
crypto map main_map 20 ipsec-isakmp
crypto map main_map 20 match address remote_routers
crypto map main_map 20 set peer 172.16.144.6
crypto map main_map 20 set transform-set strong
!
crypto map main_map 30 ipsec-isakmp
crypto map main_map 30 match address remote_concentrators
crypto map main_map 30 set peer 172.16.144.7
crypto map main_map 30 set transform-set strong
crypto map main_map interface outside
!
! Bypass NAT for any local network to any remote VPN network
!
```

```
access-list nonat permit ip 10.0.0.0 255.0.0.0 10.9.0.0 255.255.0.0
access-list nonat permit ip 10.0.0.0 255.0.0.0 10.12.0.0 255.255.0.0
access-list nonat permit ip 10.0.0.0 255.0.0.0 10.11.0.0 255.255.0.0
!
nat (inside) 0 access-list nonat
!
```

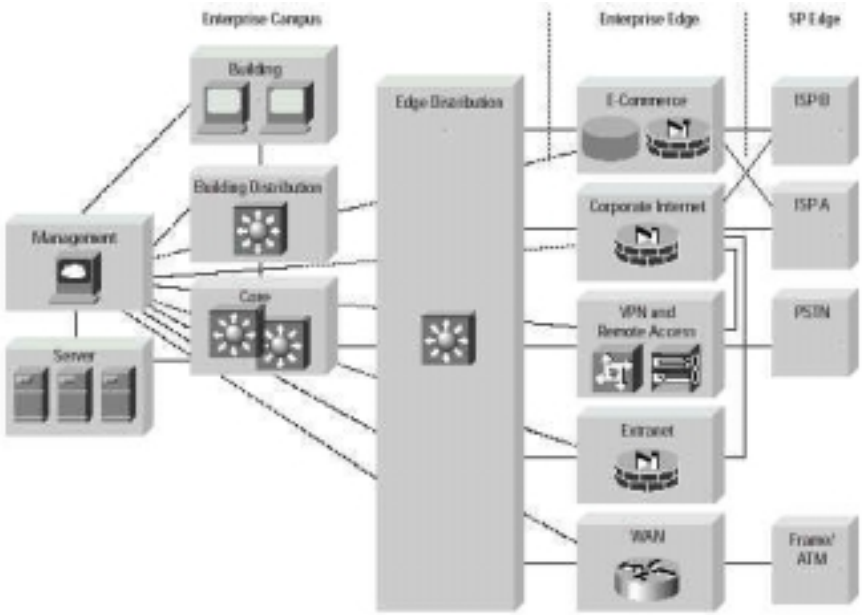
下列配置示例是适用于中型企业的 VPN 防火墙，它被视为大型企业头端的分支机构

```
!
! Crypto ACLs for local networks to large enterprise head-end
!
access-list branch_acl permit ip 10.3.0.0 255.255.0.0 10.0.0.0 255.0.0.0
!
ip address outside 172.16.240.1 255.255.255.0
ip address inside 10.3.4.1 255.255.255.0
!
! Default route to forward packets to IKE peers and remote VPNs local static routes
!
route outside 0.0.0.0 0.0.0.0 172.16.240.2 1
!
route inside 10.3.1.0 255.255.255.0 10.3.4.2 1
route inside 10.3.2.0 255.255.255.0 10.3.4.2 1
route inside 10.3.3.0 255.255.255.0 10.3.4.2 1
route inside 10.3.8.0 255.255.255.0 10.3.4.1 1
!
! DPD-type or Cisco-type IKE Keepalives for high availability enabled
!
crypto isakmp keepalive 10
!
! Crypto map entry for head-end connection
!
crypto map main_map 10 ipsec-isakmp
crypto map main_map 10 match address branch_acl
crypto map main_map 10 set peer 172.16.226.102
crypto map main_map 10 set transform-set strong

crypto map main_map interface outside
!
! Bypass NAT for any local network to any remote VPN network
!
access-list nonat permit ip 10.3.0.0 255.255.0.0 10.0.0.0 255.0.0.0
!
nat (inside) 0 access-list nonat
!
```

Large-Enterprise Configurations

图 24.SAFE 企业



企业区内网　　企业边缘　SP 边缘

构建　边缘分布　电子商务

管理　　构建分布　　公司互联网

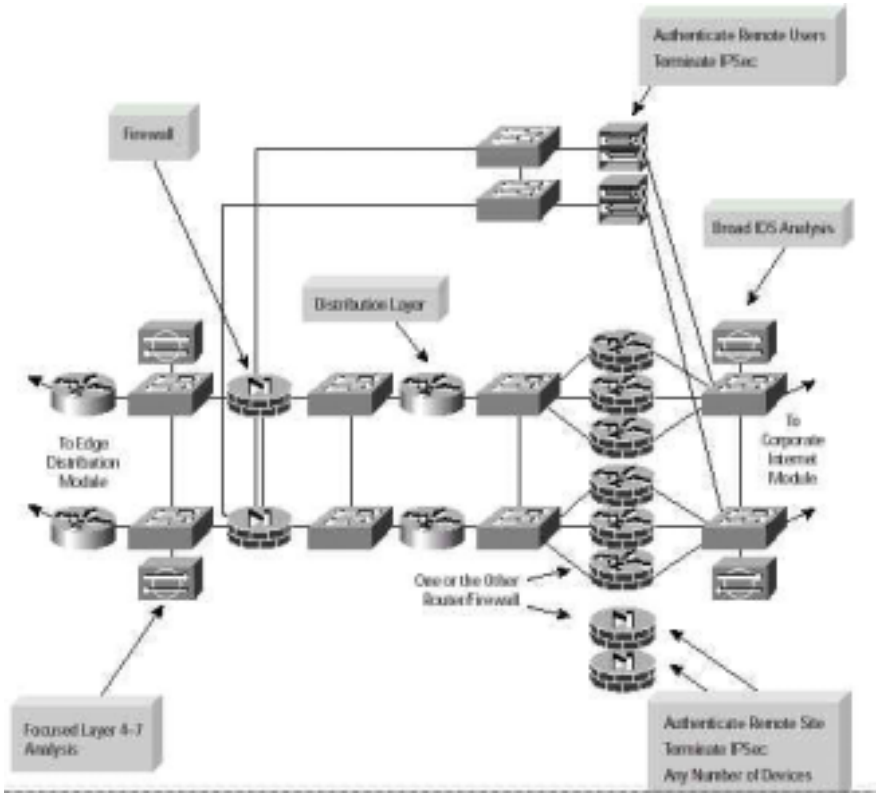
核心　　VPN 和远程接入

服务器　　外部网

帧/AIM

Remote-Access and VPN Module

图25 大型企业VPN/远程接入模块



验证远程用户

端接 IPSec

防火墙

广泛的 IPS 分析

到边缘分布模块 到公司互联网模块

一个或多个路由器/防火墙

第 4-7 层集中分析 验证远程站点

端接 IPSec

任意数量的设备

下列配置示例是用于主分布路由器

```
!
! Internal interface, HSRP running for next-hop firewall
!
interface GigabitEthernet49
ip address 10.1.148.92 255.255.255.0
standby 1 timers 5 15
standby 1 priority 110
standby 1 preempt

standby 1 authentication k&9ng@6
standby 1 ip 10.1.148.100
!
! External interface facing VPN devices, HSRP running for VPN Firewall option
!
interface GigabitEthernet50
ip address 172.16.227.92 255.255.255.0
standby 1 timers 5 15
standby 1 priority 110
standby 1 preempt
standby 1 authentication a(4ir#3
standby 1 ip 172.16.227.200
!
! Routing protocol running on external interface to track VPN devices
! Redistribution of statics to inject 10 network
!
router eigrp 10
redistribute static
network 172.16.0.0
no auto-summary
!
! Static routes to inject entire 10 net into table
!
ip route 10.0.0.0 255.0.0.0 10.1.148.32
```

```
!
! Static routes for sites terminated by VPN Firewall option
!
ip route 10.3.0.0 255.255.0.0 172.16.227.102
ip route 10.7.0.0 255.255.0.0 172.16.227.102
ip route 10.8.0.0 255.255.0.0 172.16.227.102
!
```

下列配置示列是用于备份分布路由器

```
!
! Internal interface, HSRP running for next-hop firewall
!
interface GigabitEthernet49
ip address 10.1.148.93 255.255.255.0
standby 1 timers 5 15
standby 1 priority 100
standby 1 preempt
standby 1 authentication k&9ng@6
standby 1 ip 10.1.148.100
!
! External interface facing VPN devices, HSRP running for VPN Firewall option
!
interface GigabitEthernet50
ip address 172.16.227.93 255.255.255.0
standby 1 timers 5 15
standby 1 priority 100
standby 1 preempt
standby 1 authentication a(4ir#3
standby 1 ip 172.16.227.200
!
! Routing protocol running on external interface to track VPN devices
! Redistribution of statics to inject 10 network
!
router eigrp 10

redistribute static
network 172.16.0.0
no auto-summary
!
! Static routes to inject entire 10 net into table
!
ip route 10.0.0.0 255.0.0.0 10.1.148.32
!
! Static routes for sites terminated by VPN Firewall option
!
```

```
ip route 10.3.0.0 255.255.0.0 172.16.227.102
ip route 10.7.0.0 255.255.0.0 172.16.227.102
ip route 10.8.0.0 255.255.0.0 172.16.227.102
!
```

下列配置示例用于 VPN 防火墙选项（备用项未介绍，因为它拥有相同的配置）。

```
!
! Crypto ACLs for local networks to remote sites
!
access-list remote-firewall-1 permit ip 10.0.0.0 255.0.0.0 10.3.0.0
!
access-list remote-concentrator-1 permit ip 10.0.0.0 255.0.0.0 10.7.0.0
!
access-list remote-router-1 permit ip 10.0.0.0 255.0.0.0 10.8.0.0 255.255.0.0
!
ip address outside 172.16.226.102 255.255.255.0
ip address inside 172.16.227.102 255.255.255.0
!
! Default route to forward packets to IKE peers and remote VPNs local static routes
! All 10.1.0.0 large enterprise remote networks statically routed
!
route outside 0.0.0.0 0.0.0.0 172.16.226.200 1
route inside 10.1.0.0 255.255.0.0 172.16.227.200 1
!
! DPD-type or Cisco-type IKE Keepalives for high availability enabled
!
crypto isakmp keepalive 10
!
! Crypto map entries for multiple remote device types
!
crypto map main_map 10 ipsec-isakmp
crypto map main_map 10 match address remote-firewall-1
crypto map main_map 10 set peer 172.16.240.1
crypto map main_map 10 set transform-set strong
!
crypto map main_map 20 ipsec-isakmp
crypto map main_map 20 match address remote-concentrator-1
crypto map main_map 20 set peer 172.16.128.4
crypto map main_map 20 set transform-set strong
!
crypto map main_map 30 ipsec-isakmp
crypto map main_map 30 match address remote-router-1
crypto map main_map 30 set peer 172.16.128.6
crypto map main_map 30 set transform-set strong
!
crypto map main_map interface outside
```

```
!
! Bypass NAT for any local network to any remote VPN network
!
access-list nonat permit ip 10.1.0.0 255.255.0.0 10.7.0.0 255.255.0.0
access-list nonat permit ip 10.1.0.0 255.255.0.0 10.8.0.0 255.255.0.0
access-list nonat permit ip 10.1.0.0 255.255.0.0 10.3.0.0 255.255.0.0
!
nat (inside) 0 access-list nonat
```

下列配置示例是用于 VPN 路由器选项。这些配置展示了三种头端和三种远程站点配置，配备有故障负载分散机制。

VPN 头端设备 1

```
!
! Crypto ACLs to protect each GRE flow between each peer
!
access-list 100 permit gre host 172.16.226.96 host 172.16.144.101
access-list 101 permit gre host 172.16.226.96 host 172.16.144.103
!
! Crypto map entries for each peer
!
crypto map main_map 10 ipsec-isakmp
set peer 172.16.144.101
set transform-set strong
match address 100
crypto map main_map 20 ipsec-isakmp
set peer 172.16.144.103
set transform-set strong
match address 101
!
! GRE Tunnels for each remote peer
!
!
interface Tunnel0
ip unnumbered FastEthernet0/0
tunnel source FastEthernet0/0
tunnel destination 172.16.144.101
crypto map main_map
!
! Note the bandwidth statement on the next tunnel interface
!
interface Tunnel1
band 5
ip unnumbered FastEthernet0/0
tunnel source FastEthernet0/0
tunnel destination 172.16.144.103
crypto map main_map
```

```
!
!
!
interface FastEthernet0/0
ip address 172.16.226.96 255.255.255.0
crypto map main_map
!
interface FastEthernet0/1
ip address 172.16.227.96 255.255.255.0
!
! Routing protocol configuration, updates are not sent on the public interface - only on the inside and tunnel interfaces.
!
router eigrp 10
passive-interface FastEthernet0/0
network 172.16.0.0
distribute-list 1 out
distribute-list 1 in
no auto-summary
!
access-list 1 permit 10.0.0.0 0.255.255.255
!
! Default route to forward packets to IKE peers and remote VPNs local static routes
!
ip route 0.0.0.0 0.0.0.0 172.16.226.200
!
```

下面列举了上述配置的一个样本路由选择表格。

```
show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is 172.16.226.200 to network 0.0.0.0
172.16.0.0/24 is subnetted, 2 subnets
C 172.16.226.0 is directly connected, FastEthernet0/0
C 172.16.227.0 is directly connected, FastEthernet0/1
10.0.0.0/8 is variably subnetted, 24 subnets, 2 masks
D 10.10.1.0/24 [90/297246976] via 10.10.1.1, 00:33:24, Tunnel0
D 10.10.2.0/24
[90/297249536] via 172.16.227.97, 00:33:32, FastEthernet0/1
D 10.10.3.0/24
[90/297249536] via 172.16.227.98, 00:33:32, FastEthernet0/1
```

```
D EX 10.0.0.0/8 [170/30720] via 172.16.227.93, 00:00:00, FastEthernet0/1
[170/30720] via 172.16.227.92, 00:00:00, FastEthernet0/1
D 10.1.148.0/24 [90/30720] via 172.16.227.93, 00:33:37, FastEthernet0/1
[90/30720] via 172.16.227.92, 00:33:37, FastEthernet0/1
S* 0.0.0.0/0 [1/0] via 172.16.226.200
```

VPN 路由器头端设备 2（节选）

```
!
access-list 100 permit gre host 172.16.226.97 host 172.16.144.101
access-list 101 permit gre host 172.16.226.97 host 172.16.144.102
!
crypto map main_map 10 ipsec-isakmp
set peer 172.16.144.101
set transform-set strong
match address 100
crypto map main_map 20 ipsec-isakmp
set peer 172.16.144.102
set transform-set strong
match address 101
!

interface Tunnel0
band 5
ip unnumbered FastEthernet0/0
tunnel source FastEthernet0/0
tunnel destination 172.16.144.101
crypto map main_map
!
interface Tunnel1
ip unnumbered FastEthernet0/0
tunnel source FastEthernet0/0
tunnel destination 172.16.144.102
crypto map main_map
!
interface FastEthernet0/0
ip address 172.16.226.97 255.255.255.0
crypto map main_map
!
interface FastEthernet0/1
ip address 172.16.227.97 255.255.255.0
!
```

VPN 路由器头端设备 3（节选）

```
!
```

```
access-list 100 permit gre host 172.16.226.98 host 172.16.144.102
access-list 101 permit gre host 172.16.226.98 host 172.16.144.103
!
crypto map main_map 10 ipsec-isakmp
set peer 172.16.144.102
set transform-set strong
match address 100
crypto map main_map 20 ipsec-isakmp
set peer 172.16.144.103
set transform-set strong
match address 101
!
interface Tunnel0
band 5
ip unnumbered FastEthernet0/0
tunnel source FastEthernet0/0
tunnel destination 172.16.144.102
crypto map main_map
!
interface Tunnel1
ip unnumbered FastEthernet0/0
tunnel source FastEthernet0/0
tunnel destination 172.16.144.103
crypto map main_map
!
interface FastEthernet0/0
ip address 172.16.226.98 255.255.255.0
crypto map main_map
!
interface FastEthernet0/1
ip address 172.16.227.98 255.255.255.0
!
```

VPN 路由器远程站点设备 1

```
!
! Crypto ACLs for the primary and secondary GRE tunnels
!
access-list 100 permit gre host 172.16.144.101 host 172.16.226.96
access-list 101 permit gre host 172.16.144.101 host 172.16.226.97
!
! Crypto map for the primary and secondary GRE tunnels
!
crypto map main_map 1 ipsec-isakmp
set peer 172.16.226.96
```

```
set transform-set main_map
match address 100
crypto map main_map 2 ipsec-isakmp
set peer 172.16.226.97
set transform-set main_map
match address 101
!
! GRE tunnel interfaces, note the second has a bandwidth statement to make it secondary
!
interface Tunnel0
ip unnumbered FastEthernet0/0
tunnel source FastEthernet0/1
tunnel destination 172.16.226.96
crypto map main_map
!
interface Tunnel1
bandwidth 5
ip unnumbered FastEthernet0/0
tunnel source FastEthernet0/1
tunnel destination 172.16.226.97
crypto map main_map
!
interface FastEthernet0/0
ip address 10.10.1.1 255.255.255.0
!
interface FastEthernet0/1
ip address 172.16.144.101 255.255.255.0
crypto map main_map
!
! Routing protocol configuration, updates are only sent on the tunnel interfaces.
!
router eigrp 10
passive-interface FastEthernet0/0
passive-interface FastEthernet0/1
network 10.0.0.0
no auto-summary
no eigrp log-neighbor-changes
!
ip route 0.0.0.0 0.0.0.0 172.16.144.2
!
```

下面列举了上述配置的一个样本路由选择表格

```
show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is 172.16.144.2 to network 0.0.0.0
172.16.0.0/24 is subnetted, 1 subnets
C 172.16.144.0 is directly connected, FastEthernet0/1
10.0.0.0/8 is variably subnetted, 24 subnets, 2 masks
C 10.10.1.0/24 is directly connected, FastEthernet0/0
D 10.10.2.0/24 [90/310049536] via 172.16.226.96, 00:43:42, Tunnel0
D 10.10.3.0/24 [90/310049536] via 172.16.226.96, 00:43:42, Tunnel0
D EX 10.0.0.0/8 [170/297249536] via 172.16.226.96, 00:00:00, Tunnel0
D 10.1.148.0/24 [90/297249536] via 172.16.226.96, 00:43:46, Tunnel0
S* 0.0.0.0/0 [1/0] via 172.16.144.2
```

VPN 路由器远程站点设备 2（节选）

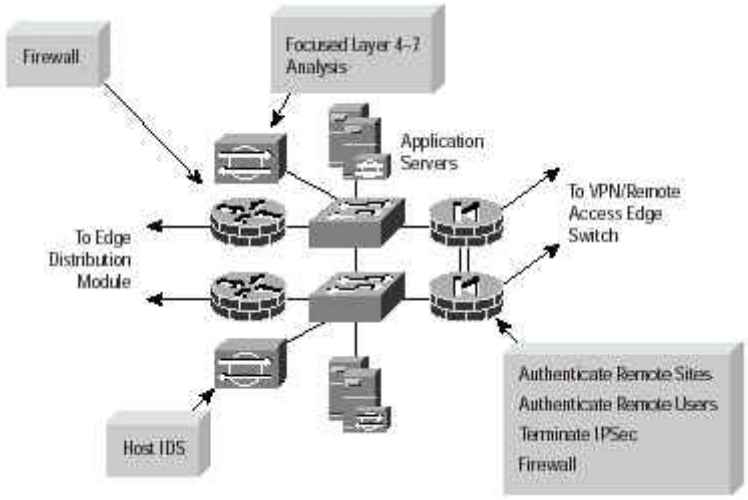
```
!
access-list 100 permit gre host 172.16.144.102 host 172.16.226.97
access-list 101 permit gre host 172.16.144.102 host 172.16.226.98
!
crypto map main_map 1 ipsec-isakmp
set peer 172.16.226.97
set transform-set main_map
match address 100
crypto map main_map 2 ipsec-isakmp
set peer 172.16.226.98
set transform-set main_map
match address 101
!
interface Tunnel0
ip unnumbered FastEthernet0/0
tunnel source FastEthernet0/1
tunnel destination 172.16.226.97
crypto map main_map
!
interface Tunnel1
bandwidth 5
ip unnumbered FastEthernet0/0
tunnel source FastEthernet0/1
tunnel destination 172.16.226.98
```

```
crypto map main_map
!
interface FastEthernet0/0
ip address 10.10.2.1 255.255.255.0
!
interface FastEthernet0/1
ip address 172.16.144.102 255.255.255.0
crypto map main_map
!
```

VPN 路由器远程站点设备 3（节选）

```
!
access-list 100 permit gre host 172.16.144.103 host 172.16.226.98
access-list 101 permit gre host 172.16.144.103 host 172.16.226.96
!
crypto map main_map 1 ipsec-isakmp
set peer 172.16.226.98
set transform-set main_map
match address 100
crypto map main_map 2 ipsec-isakmp
set peer 172.16.226.96
set transform-set main_map
match address 101
!
interface Tunnel0
ip unnumbered FastEthernet0/0
tunnel source FastEthernet0/1
tunnel destination 172.16.226.98
crypto map main_map
!
interface Tunnel1
bandwidth 5
ip unnumbered FastEthernet0/0
tunnel source FastEthernet0/1
tunnel destination 172.16.226.96
crypto map main_map
!
interface FastEthernet0/0
ip address 10.10.3.1 255.255.255.0
!
interface FastEthernet0/1
ip address 172.16.144.103 255.255.255.0
crypto map main_map
!
```

图 26 分布企业集线模块 VPN



防火墙　　第 4-7 层集中分析
　　应用服务器
到边缘分布模块　　到 VPN/远程
　　接入边缘交换机
到边缘分布模块
主机 IDS　　验证远程站点
　　验证远程用户
　　防火墙

The following configurations include the head-end, two sets of highly available distribution layers and a sample remote-site configuration for each layer.

头端、主设备

```
!
! Crypto ACLs to protect GRE traffic from distribution layer
!
access-list 100 permit gre host 172.16.226.96 host 172.16.144.8
access-list 101 permit gre host 172.16.226.96 host 172.16.144.9
access-list 102 permit gre host 172.16.226.96 host 172.16.144.10
access-list 103 permit gre host 172.16.226.96 host 172.16.144.11
!
! Crypto maps for highly available distribution layer
!
crypto map main_map 10 ipsec-isakmp
set peer 172.16.144.8
set transform-set strong
match address 100
crypto map main_map 20 ipsec-isakmp
set peer 172.16.144.9
```

```
set transform-set strong
match address 101
crypto map main_map 30 ipsec-isakmp
set peer 172.16.144.10
set transform-set strong
match address 102
crypto map main_map 40 ipsec-isakmp
set peer 172.16.144.11
set transform-set strong

match address 103
!
! GRE tunnels to distribution layer
!
interface Tunnel1
bandwidth 20
ip unnumbered FastEthernet0/0
tunnel source FastEthernet0/0
tunnel destination 172.16.144.8
crypto map main_map
!
interface Tunnel2
bandwidth 5
ip unnumbered FastEthernet0/0
tunnel source FastEthernet0/0
tunnel destination 172.16.144.9
crypto map main_map
!
interface Tunnel3
bandwidth 20
ip unnumbered FastEthernet0/0
tunnel source FastEthernet0/0
tunnel destination 172.16.144.10
crypto map main_map
!
interface Tunnel4
bandwidth 5
ip unnumbered FastEthernet0/0
tunnel source FastEthernet0/0
tunnel destination 172.16.144.11
crypto map main_map
!
!
!
interface FastEthernet0/0
ip address 172.16.226.96 255.255.255.0
```

```
crypto map main_map
!
interface FastEthernet0/1
ip address 172.16.227.97 255.255.255.0
!
interface FastEthernet4/0
no ip address
shutdown
duplex half
!
! Routing protocols running over tunnels
!
router eigrp 10
passive-interface FastEthernet0/0
network 172.16.0.0
distribute-list 1 out
distribute-list 1 in
no auto-summary
no eigrp log-neighbor-changes
!
access-list 1 permit 10.0.0.0 0.255.255.255
!
!
!
ip route 0.0.0.0 0.0.0.0 172.16.226.200
!
```

分布层分组 1，主设备

```
!
! Crypto ACLs to protect GRE traffic from head-ends and remote site
!
access-list 100 permit gre host 172.16.144.8 host 172.16.226.96
access-list 101 permit gre host 172.16.144.8 host 172.16.226.97
access-list 102 permit gre host 172.16.144.8 host 172.16.128.10
!
! Crypto maps for head-ends and remote sites
!
crypto map main_map 10 ipsec-isakmp
set peer 172.16.226.96
set transform-set strong
match address 100
crypto map main_map 20 ipsec-isakmp
set peer 172.16.226.97
set transform-set strong
match address 101
```

```
crypto map main_map 30 ipsec-isakmp

set peer 172.16.128.10
set transform-set strong
match address 102
!
! GRE tunnel interfaces for head-end and remote sites
!
interface Tunnel1
bandwidth 20
ip unnumbered FastEthernet0/0
tunnel source FastEthernet0/0
tunnel destination 172.16.226.96
crypto map main_map
!
interface Tunnel2
bandwidth 5
ip unnumbered FastEthernet0/0
tunnel source FastEthernet0/0
tunnel destination 172.16.226.97
crypto map main_map
!
interface Tunnel3
ip unnumbered FastEthernet0/0
tunnel source FastEthernet0/0
tunnel destination 172.16.128.10
crypto map main_map
!
interface FastEthernet0/0
ip address 172.16.144.8 255.255.255.0
crypto map main_map
!
! Device serves as primary for first remote site group and secondary for second remote site group
!
interface FastEthernet0/1
ip address 10.30.0.1 255.255.255.0
standby 1 timers 5 15
standby 1 priority 100 preempt delay 2
standby 1 ip 10.30.0.100
standby 1 track FastEthernet0/0
standby 2 timers 5 15
standby 2 priority 90 preempt delay 2
standby 2 ip 10.30.0.101
standby 2 track FastEthernet0/0
!
! Routing protocol running on tunnels
```

```
router eigrp 10
passive-interface FastEthernet0/0
network 172.16.144.0 0.0.0.255
distribute-list 1 out
distribute-list 1 in
no auto-summary
!
access-list 1 permit 10.0.0.0 0.255.255.255
!
! Catch all default route
!
ip route 0.0.0.0 0.0.0.0 172.16.144.2
!
```

分布层分组 1，备用设备

```
!
! Crypto ACLs to protect GRE traffic from head-ends and remote site
!
access-list 100 permit gre host 172.16.144.9 host 172.16.226.96
access-list 101 permit gre host 172.16.144.9 host 172.16.226.97
access-list 102 permit gre host 172.16.144.9 host 172.16.128.10
!
! Crypto maps for head-ends and remote sites
!
crypto map main_map 10 ipsec-isakmp
set peer 172.16.226.96
set transform-set strong
match address 100
crypto map main_map 20 ipsec-isakmp
set peer 172.16.226.97
set transform-set strong
match address 101
crypto map main_map 30 ipsec-isakmp
set peer 172.16.128.10
set transform-set strong
match address 102
!
! GRE tunnel interfaces for head-end and remote sites
!
interface Tunnel1
bandwidth 20
ip unnumbered FastEthernet0/0
tunnel source FastEthernet0/0
tunnel destination 172.16.226.96
crypto map main_map
```

```
!
interface Tunnel2
bandwidth 5
ip unnumbered FastEthernet0/0
tunnel source FastEthernet0/0
tunnel destination 172.16.226.97
crypto map main_map
!
interface Tunnel3
ip unnumbered FastEthernet0/0
tunnel source FastEthernet0/0
tunnel destination 172.16.128.10
crypto map main_map
!
interface FastEthernet0/0
ip address 172.16.144.9 255.255.255.0
crypto map main_map
!
interface FastEthernet0/1
ip address 10.30.0.2 255.255.255.0
! Device serves as secondary for first remote site group and primary for second remote site group
!
interface FastEthernet0/1
ip address 10.30.0.2 255.255.255.0
standby 1 timers 5 15
standby 1 priority 90 preempt delay 2

standby 1 ip 10.30.0.100
standby 1 track FastEthernet0/0
standby 2 timers 5 15
standby 2 priority 100 preempt delay 2
standby 2 ip 10.30.0.101
standby 2 track FastEthernet0/0
!
! Routing protocol running on tunnels
!
router eigrp 10
passive-interface FastEthernet0/0
network 172.16.144.0 0.0.0.255
distribute-list 1 out
distribute-list 1 in
no auto-summary
!
access-list 1 permit 10.0.0.0 0.255.255.255
!
```

```
! Catch all default route
!
ip route 0.0.0.0 0.0.0.0 172.16.144.2
!
```

分布层分组 2，主设备

```
!
! Crypto ACLs to protect GRE traffic from head-ends and remote site
!
access-list 100 permit gre host 172.16.144.10 host 172.16.226.96
access-list 101 permit gre host 172.16.144.10 host 172.16.226.97
access-list 102 permit gre host 172.16.144.10 host 172.16.128.11
!
! Crypto maps for head-ends and remote sites
!
crypto map main_map 10 ipsec-isakmp
set peer 172.16.226.96
set transform-set strong
match address 100
crypto map main_map 20 ipsec-isakmp
set peer 172.16.226.97
set transform-set strong
match address 101
crypto map main_map 30 ipsec-isakmp
set peer 172.16.128.10
set transform-set strong
match address 102
!
! GRE tunnel interfaces for head-end and remote sites
!
interface Tunnel1
bandwidth 20
ip unnumbered FastEthernet0/0
tunnel source FastEthernet0/0
tunnel destination 172.16.226.96
crypto map main_map
!
interface Tunnel2
bandwidth 5

ip unnumbered FastEthernet0/0
tunnel source FastEthernet0/0
tunnel destination 172.16.226.97
crypto map main_map
!
```

```
interface Tunnel3
ip unnumbered FastEthernet0/0
tunnel source FastEthernet0/0
tunnel destination 172.16.128.11
crypto map main_map
!
interface FastEthernet0/0
ip address 172.16.144.10 255.255.255.0
crypto map main_map
!
interface FastEthernet0/1
ip address 10.30.1.1 255.255.255.0
! Device serves as primary for first remote site group and secondary for second remote site group
!
interface FastEthernet0/1
ip address 10.30.1.1 255.255.255.0
standby 1 timers 5 15
standby 1 priority 100 preempt delay 2
standby 1 ip 10.30.1.100
standby 1 track FastEthernet0/0
standby 2 timers 5 15
standby 2 priority 90 preempt delay 2
standby 2 ip 10.30.1.101
standby 2 track FastEthernet0/0
!
! Routing protocol running on tunnels
!
router eigrp 10
passive-interface FastEthernet0/0
network 172.16.144.0 0.0.0.255
distribute-list 1 out
distribute-list 1 in
no auto-summary
!
access-list 1 permit 10.0.0.0 0.255.255.255
!
! Catch all default route
!
ip route 0.0.0.0 0.0.0.0 172.16.144.2
!
```

分布层分组长 2，备用设备

```
!
! Crypto ACLs to protect GRE traffic from head-ends and remote site
!
```

```
access-list 100 permit gre host 172.16.144.11 host 172.16.226.96
access-list 101 permit gre host 172.16.144.11 host 172.16.226.97
access-list 102 permit gre host 172.16.144.11 host 172.16.128.11
!
! Crypto maps for head-ends and remote sites
!
crypto map main_map 10 ipsec-isakmp

set peer 172.16.226.96
set transform-set strong
match address 100
crypto map main_map 20 ipsec-isakmp
set peer 172.16.226.97
set transform-set strong
match address 101
crypto map main_map 30 ipsec-isakmp
set peer 172.16.128.11
set transform-set strong
match address 102
!
! GRE tunnel interfaces for head-end and remote sites
!
interface Tunnel1
bandwidth 20
ip unnumbered FastEthernet0/0
tunnel source FastEthernet0/0
tunnel destination 172.16.226.96
crypto map main_map
!
interface Tunnel2
bandwidth 5
ip unnumbered FastEthernet0/0
tunnel source FastEthernet0/0
tunnel destination 172.16.226.97
crypto map main_map
!
interface Tunnel3
ip unnumbered FastEthernet0/0
tunnel source FastEthernet0/0
tunnel destination 172.16.128.11
crypto map main_map
!
interface FastEthernet0/0
ip address 172.16.144.11 255.255.255.0
crypto map main_map
!
```

```
interface FastEthernet0/1
ip address 10.30.1.2 255.255.255.0
! Device serves as secondary for first remote site group and primary for second remote site group
!
interface FastEthernet0/1
ip address 10.30.1.2 255.255.255.0
standby 1 timers 5 15
standby 1 priority 90 preempt delay 2
standby 1 ip 10.30.1.100
standby 1 track FastEthernet0/0
standby 2 timers 5 15
standby 2 priority 100 preempt delay 2
standby 2 ip 10.30.1.101
standby 2 track FastEthernet0/0
!
! Routing protocol running on tunnels
!
router eigrp 10
passive-interface FastEthernet0/0

network 172.16.144.0 0.0.0.255
distribute-list 1 out
distribute-list 1 in
no auto-summary
!
access-list 1 permit 10.0.0.0 0.255.255.255
!
! Catch all default route
!
ip route 0.0.0.0 0.0.0.0 172.16.144.2
!
```

分布分组 1 防火墙（节选）

```
!
! Two routes, one for each primary HSRP group
!
route outside 10.20.0.0 255.255.255.0 10.30.0.100 1
route outside 10.20.1.0 255.255.255.0 10.30.0.101 1
!
```

分布分组 1 的远程站点

```
!
! Redundant crypto ACLs for each tunnel to the redundant distribution layer
!
```

```
access-list 100 permit gre host 172.16.128.10 host 172.16.144.8
access-list 101 permit gre host 172.16.128.10 host 172.16.144.9
!
!
!
crypto map main_map 10 ipsec-isakmp
set peer 172.16.144.8
set transform-set strong
match address 100
crypto map main_map 20 ipsec-isakmp
set peer 172.16.144.9
set transform-set strong
match address 101
!
!
!
interface Tunnel1
bandwidth 20
ip unnumbered FastEthernet0/0
tunnel source FastEthernet0/0
tunnel destination 172.16.144.8
crypto map main_map
!
interface Tunnel2
bandwidth 5
ip unnumbered FastEthernet0/0
tunnel source FastEthernet0/0
tunnel destination 172.16.144.9
crypto map main_map
!
interface FastEthernet0/0
ip address 172.16.128.10 255.255.255.0
crypto map main_map

!
interface FastEthernet0/1
ip address 10.20.0.1 255.255.255.0
!
!
!
access-list 1 permit 10.0.0.0 0.255.255.255
!
router eigrp 10
passive-interface FastEthernet0/0
passive-interface FastEthernet0/1
network 10.20.0.0 0.0.0.255
```

```
network 172.16.128.0 0.0.0.255
distribute-list 1 out
no auto-summary
!
!
!
ip route 0.0.0.0 0.0.0.0 172.16.128.1
!
```

分布分组 2 的远程站点

```
!
!
!
access-list 100 permit gre host 172.16.128.11 host 172.16.144.10
access-list 101 permit gre host 172.16.128.11 host 172.16.144.11
!
!
!
crypto map main_map 10 ipsec-isakmp
set peer 172.16.144.10
set transform-set strong
match address 100
crypto map main_map 20 ipsec-isakmp
set peer 172.16.144.11
set transform-set strong
match address 101
!
!
!
interface Tunnel1
bandwidth 20
ip unnumbered FastEthernet0/0
tunnel source FastEthernet0/0
tunnel destination 172.16.144.10
crypto map main_map
!
interface Tunnel2
bandwidth 5
ip unnumbered FastEthernet0/0
tunnel source FastEthernet0/0
tunnel destination 172.16.144.11
crypto map main_map
!
interface FastEthernet0/0
```

```
!
interface FastEthernet0/1
ip address 10.20.128.1 255.255.255.0
!
!
!
access-list 1 permit 10.0.0.0 0.255.255.255
!
router eigrp 10
passive-interface FastEthernet0/0
passive-interface FastEthernet0/1
network 10.20.128.0 0.0.0.255
network 172.16.128.0 0.0.0.255
distribute-list 1 out
no auto-summary
!
!
!
ip route 0.0.0.0 0.0.0.0 172.16.128.1
!
```

附录 B：VPN 指南

对 VPN 的需求

虚拟专用网(VPN)提供了另一种为站点间通信或拨号接入构建专用网络的方式。因为它们在共享基础设施而非专用网络上运行，公司可经济有效地将网络扩展到以前从未实现过联网的地方。例如，在许多国内应用和大多数国际应用中，VPN 与专用 WAN 连接相比，可节约大量成本。因此，VPN 并非采用多种在公司头端端接的独立电路，而是使所有信息流集中到一条连接上。此情况实现了头端处的带宽和成本节约。而无需再维护专用网络，从而带来了进一步的成本节约。

VPN 也为公司内生产效率的提高提供了机会。例如，家庭办公者不必再使用缓慢的拨号接入链路，他们可以更高速地接入，移动人员也可利用目前可在许多宾馆中看到的更高速以太网连接，从而在旅行时访问公司资源。仅是无需交付长话费这一项的成本节约，就使 VPN 在这些情况下的部署顺理成章。最后，公司可利用 VPN 技术来实现新应用和商业流程。例如，汽车业已通过采用基于 VPN 技术的汽车制造网络交换(ANX)，实施了新型电子商务和供应链管理业务模型。

VPN 的类型

目前市场上部署了多种 VPN 技术。下面提供了部分技术和术语的概念，以供网络管理员进一步了解 VPN。人们常常从以下两个角度之一看待 VPN：功能角度或技术角度。功能角度更多地强调 VPN 的目的，而技术角度则强调用于实施 VPN 的特定技术。

功能角度

从功能角度来看，VPN 通常被分为远程接入 VPN 或站点间 VPN。远程接入 VPN 是指个人远程用户，亦即通常所说的移动办公人员经由其 PC 接入公司网络的实施。移动办公人员可能使用传统的拨号接入连接至本地电脑服务供应商，然后启动隧道、接回公司。另一种方式是在以太网等更高速的媒体上启动隧道，这些媒体可在当今的许多宾馆中找到。它最近的一种演变产品即为无线无程接入 VPN，其中移动办公人员利用个人数字助理(PDA)上的无线连接来接入公司网络。在所有这些情况下，PC 或 PDA 上的软件均提供了返回公司的安全连接(通常被称为隧道)。应在允许个人移动办公人员接入公司网络前对其进行验证，针对公司资源的适当访问控制应根据公司安全政策运用于移动办公人员。例如，为企业合作伙伴提供的接入可能需比为员工提供的接入更为严格。

站点间 VPN 指的是实施一个地区的网络经由 VPN 与另一地区的网络相连。网络设备互相验证，随后在站点间建立 VPN 连接。这些设备随后会作为网关，安全地传送目的地为另一站点的信息流。当 VPN 支持和专用 VPN 集中器的路由器或防火墙均提供此功能。站点间 VPN 可进一步作为内部网 VPN 或外部网 VPN。内部 VPN 是指属于同一公司的站点间的连接。此时站点间的连接通常限制性较低。外部网 VPN 是指公司与其业务合作伙伴间的连接。站点间的接入应由双方在各自的网站上紧密控制。

远程接入 VPN 和站点间 VPN 间的区别将随着硬件 VPN 客户机等新设备逐步广为使用而变得模糊。这种设备看来可像是接入网络的单一设备，但实际上在它们的背后可能是一个带多台设备的网络。

技术角度

从技术角度来说，VPN 可根据它们是在第 2 层网络还是在第 3 层网络上运行来分类。应注意的是，ATM 和帧中继网络有时被称为 VPN 网络，这是因为它们使用共享基础实施来向大量用户提供网络服务，然而，本文不将 ATM 或帧中继网络看作 VPN，而是将它们作为专用网络实施。

第 2 层 VPN

第 2 层 VPN 技术运行于开放系统互联(OSI)模型的数据链路层，而第 3 层 VPN 技术，如 IP 安全性(IPSec)则运行于 OSI 模型的网络层。第 2 层 VPN 包括点到点隧道协议(PPTP)和第 2 层隧道协议(L2TP)。

PPTP 是主要用于拨号远程接入 VPN 的较旧的协议。PPTP 在客户/服务器模式下运行。客户机可以是带 PPTP 软件的一台远程 PC 或一台可实施 PPTP 互联网接入服务供应商(TSP)的网络接入服务器(NAS)。服务器可以是拨入路由器、专用 VPN 集中器或实际应用服务器。当 PPTP 隧道的启动由远程 PC 完成时，这节被称为自愿模式。当隧道的启动由 NAS 完成时，则称为被动模式。应注意，在被动模式下，并不要求在最终用户的 PC 上有 PPTP 客户机软件。然而，这也意味着从最终用户 PC 到 ISP 的拨号接入连接无加密等 PPTP 安全服务。

PPTP 在通用路由封装(GRE)的修改版本中封装了点到点协议(PPP)分组并在网上对它们进行传输。在 RFC1701 和 1702 中定义的 GRE，仅是在一个任意网络层协议上执行另一任意网络层协议的封装的机制。因此，PPTP 可用于传输第 3 层协议，如 IP 网络互联分组交换(IPX)、NETBEUI 等。PPTP 依靠 PPP 的验证机制-口令验证协议(PAP)和问题握手验证协议(CHAP)，但人们认为它们并不是很强大。PAP 在链接上以明文的形式发送口令且不安全。CHAP 比 PAP 要安全。CHAP 不以明文形式发送口令，而是发出一个问题，另一方必须响应，从而进行验证。Microsoft 已创建了 CHAP 的强化版本，称为 MS-CHAP，它将 NT 域内的信息用于安全性。互联网工程任务小组(IETF)也在 RFC2284 中定义了 PPP 可扩展验证协议(EAP)，从而实现验证的更强大方式。然而，不是所有的实施现在均支持此协议。Microsoft 还采用了一种称为 Microsoft 点到点加密(MPPE)的协议，以使在 PPTP 链路上提供信息流的加密。MPPE 基于 RSA RC4 加密算法。

L2TP 被广泛地认为是 PPTP 的替代技术，且比 PPTP 更是可扩展性。L2TP 也以客户机/服务器模式运行、与 PPTP 类似，L2TP 隧道可从远程 PC 启动，返回 L2TP 网络服务器(CNS)；或从实施了 L2TP 的接入集中器(LAS)至 LNS。尽管 L2TP 仍使用 PPP，但它根据传输媒体而非使用 GRE 来定义自己的隧道协议。因此，尽管不是所有的实施都支持 L2TP，L2TP 还是可用来传输除 IP 以外的各种第 3 层协议。L2TP 可利用 PAP、CHAP 和 EAP 进行验证。然而，使用 L2TP 的一个重要差别就是它支持 IPSec 的使用，IPSec 可用于对最终用户 PC 到公司网络的信息流进行全程保护。

第 3 层 VPN

第 3 层 VPN 技术可运行在 OSI 模型的网络层上。一般来说，这些 VPN 使用 IP 协议，将其作为网络层协议。第 3 层 VPN 包括多协议标签交换(MPLS)和 IPSec。

MPLS 一般作为站点间 VPN 服务由电信服务供应商提供。电信服务供应商构建基于 IP 的专用网络，并在网络的各站点间提供多客户 IP 连接性。此技术允许单独客户能像拥有连接其站点的专用 IP 网络一样浏览其 MPLS 服务。 为客户提供帧中继或 ATM 等第 2 层专用网络的优势，以及第 3 层网络的可扩展性和易于管理性。此外，因为 MPLS 在专用 IP 网络而非互联网上运行，电信服务供应商可为其客户提供其特色水平的服务(服务质量[QoS])和服务级别协议(CLA)。但是，因为 MPALS 基于电信服务供应商的专用网络，服务的范围被限制在电信服务供应商运营的地点。一般来说，目前几乎没有电信服务供应商间的 MPLS 服务。

以下部分详细介绍了 IPSec VPN。

IPSec

IPSec 是一个开放标准框架，可确保 IP 网络上的安全专用通信。IPSec VPN 使用 IPSec 中定义的服务来确保互联网等公共网络上数据通信的保密性、完整性和验证性。IPSec 中的安全服务由以下两个协议之一提供：验证报头(AH)和封装安全有效负载(ESP)。每个协议都提供了一定的服务。可独立或同时使用，但这两种协议通常不必共用。

验证报头

AH 为 IP 分组提供了无连接数据完整性和数据来源验证。无连接数据完整性意味着原始 IP 分组在从源头传输到目的地的过程中不会被修改。数据来源验证可证实数据的来源，所有这些服务通称为验证。AH 插入到 IP 报头和其余分组内空间的 IP 分组中，AH 中含分组内容的加密检查和，这其中包括传输中不变的 IP 报头部分。计算检查和的缺省加密算法为配有信息摘要 5(MD5) 散列功能的基于散列的信息验证代码(HMAC)和配有 SHA-1 散列功能的 HMAC。散列算法是一种采用可变长度信息并带来独特的固定长度价值的单向算术功能。SHA-1 被公认为较为强大的散列功能，因为它提供了 160 位的验证器价值(加密检查和)，而 MD5 仅生成 128 位验证器。通过利用接收到的信息、计算同样的加密检查和并将其与所获价值比较，接收方可证实信息未在传输中改变。AH 也提供了反重放服务，可根据攻击者截取

的一系列分组及对其重放来防御拒绝服务(Dos)攻击。应注意，如果网络对分组重排序、以便为某些信息流类型提供更高 Dos，则反重放可影响性能。如果到达的分组位于反重放窗口之外，IPSec 将拒绝它们。因为 AH 未采取任何措施来保证分组内容的保密性，它未广泛用于互联网上 IPSec 的实施中。要实现保密性，必须使用 ESP。

封装安全有效负载

封装安全有效负载提供了 IP 信息流的保密性以及验证和反重放功能，保密性通过加密提供。加密是这样一个过程：获得一个信息、将其作为明文，并使其通过算术算法来生成加密文本。解密过程与此相反。加密算法一般依靠称为密钥的一个数值来对数据加密和解密。目前使用的两种主要加密形式为对称加密(即称为共享密钥加密)和非对称加密(也称为公共/专用加密)。对称加密大约比非对称加密快 1000 倍，因此常用于大量数据的加密。较长的密钥一般配有出色设计的加密算法，可实现更高程度的安全性，这是因为此时要想对某一信息解密，需投入更多精力来试用每个可能的密钥(称为密钥空间)。ESP 支持各种对称加密算法来进行数据加密。缺省算法为数据加密标准(DES)，已运用了近 20 年。DES 使用一个 56 位密钥。然而，因为 DES 在强力攻击下较为脆弱，用三种不同的密钥对数据进行三遍加密的三重 DES(3DES)是推荐给大多数企业使用的标准算法。应注意的是，因为美国政府对加密技术出口的限制，3DES 可能在某些国家中不能使用。现在，国家标准和技术协会(NIST)，http://www.nist,go 正在定义一种更快、更安全的新型标准加密算法，称为高级加密标准(AES)。ESP 对更高级的协议信息(如 TCP 报头)和实际数据进行加密。与 AH 不同，ESP 的验证服务不保护分组的 IP 报头。当今大多数 IPSec VPN 实施都使用 ESP。

IPSec 模式

IPSec 可用来在两台主机间从主机到安全网关或两个安全网关间提供安全通信。安全网关是保护 IPSec 服务(即端接 IPSec 连接)并通过隧道将信息流传送至另一边的设备，如路由器、防火墙或专用 VPN 集中器等。IPSec 可在以下两种模式之一运行，处理不同类型的连接，这两种模式为隧道模式和传输模式。在隧道模式下，整个原始 IP 分组在 AH 或 ESP 中封装，然后围绕它放置一个新 IP 报头。在传输模式下，AH 或 ESP 放在原始 IP 报头之后(如上所述)。当 IPSec 连接的一端或两端均为安全网关，且其背后的实际目的地主机还支持 IPSec 的情况下，使用隧道模式。因此，新 IP 报头有网关自己的源地址。两个安全网关间运行在隧道模式的情况下，可通过使用加密来隐藏原始源地址和目的地址。传输模式可在两个终端主机均支持 IPSec 的使用。

安全协定

IPSec 在对等关系而非客户/服务器关系下运行。为使两个设备交换受保护的数据，它们要使用何种加密方法达成共识。对等设备间的协议称为安全协定(SA)。SA 定义了诸多信息：将使用何种验证和加密方法、共享会话密钥、密钥寿命、SA 本身的寿命等。有两种类型的 SA：互联网安全协定密钥管理协议(ISAKMP)SA(也称为 IKE SA)和 IPSec SA。IKE SA 是双向的，在可用于协商进一步通信的双方间提供了一条安全通信渠道。IPSec SA 是单向的，可用于设备间的实际通信。应该意设备间的双向通信必须为至少两个 IPSec SA--每个方向一个。

验证和密钥管理

因为所有密钥都必须进行交换，以使双方能安全通信，所以密钥交换和管理是 IPSec 的一个重要部分。处理 IPSec 中的密钥交换和管理的两种方法为人工密钥和互联网密钥交换(IKE)。IKE 基于 ISAKMP/Oakley。阶段和模式可用来说明设置 IPSec 连接中涉及的步骤。IKE 提供了三种模式来交换密钥信息和设置 SA。前两种模式为第一阶段交换，可用来设置初始安全通道 IKE SA。另一模式是第二阶段交换，对 IPSec SA 进行协商。阶段 1 中的两个模式为主模式和积极模式，阶段 2 的模式称为快速模式。

一个 Diffie-Hellman(DH)乘幂可用来帮助生成强大的初始密钥。在 IKE 继续前，双方必须商定互相验证的方式。在 IKE 阶段主模式交换期间协商验证方法。目前使用的机制有：预共享密钥、加密临时口令和数字证书。预共享密钥涉及每个对等设备上相同密钥的工人安装。加密临时口令和数字证书。预共享密钥涉及每个对等设备上相同密钥的人工安装。加密临时口令包括在每个对等设备上生成非对称加密公共/专用密钥对，然后将每个对等设备的公共密钥人工拷贝至其它每个对等设备。数字认证提供了不拒绝的附加优势，意味着对等设备可证实通信实际发生。在经由 IKESA 进行了设备验证之后，且只有当涉及远程接入客户机时，才发生第二层用户验证。头端向远程用户发出一个扩展验

证(XAUTH)请求，向他/她揭示他/她的用户名-口令/口令代码时。在第一阶段中完成验证后，第二阶段将远程和本地网相连。

与 IPSec 交互的其它技术

NAT

网络地址转换(NAT)很普遍，其同于当今网络的主要原因有三个。首先，地址转换可在众多专用编址设备间共享有限的公共地址。其次，在两个企业选择了相同专用地址空间(比如 RH 1918)的情况下，地址转换将允许每个独立网中的设备互相通信。第三，它提供了地址隐藏。NAT 有两种形式。第一种是一到一转换。例如，10.10.89.45 转换为 171.69.235.35。在本文中，这类地址转换被简称为网络地址转换，或即 NAT。第二种形式是多到一转换。主机发出的每条连接都被分配了与转换后 IP 地址相关的静态指定端口。例如，10.10.89.45 转换为 171.69.235.45.4084，其中 4084 为端口。在本文中这类转换被称为多到一地址转换。

PMTUD

路径最大传输单元发现（PMTUD）机制决定它了特定路径的分组最大传输单元（MIN），在此情况下，最大 MIN 由隧道处理。支持 PMTUD 的主机在 IP 报头中设置不分段（DF）位。ESP 从原始 IP 报头时 DF 位拷贝到新外部 IP 报头。随着分组沿路径传输至其目的地，如果加密分组太大无法适合于下一链路，度图传送加密分组的路由器将发送一个互联网控制信息协议（ICMP）信息（第 3 类目的地不可达，需第 4 代码段，现不需 DF 位符）至发送主机。路由器还将放弃分组，当主机接收到 ICMP 信息的，它降低了其 MIU，以便分组能成功穿越链路，该过程一直继续到分组到达其目的地为止。

际录 C：体系结构分类

VPN 端接设-为站点间 VPN 连接或远程接 VPN 连接而端接 IPSec 隧道。该设备应提供附加服务，以使提供与传统 WAN 或拨号接入连接相同的网络功能。

防火墙——可为基于 IP 的协议维护状态表的状态分组过滤设备。仅当信息流符合所定义的接入控制过滤器或它属于状态表中已确立会话的一部分时，才允许信息流穿过防火墙。

VPN 防火墙——与上面所描述的防火墙一样，比防火墙还提供远程接入 VPN 和站点间 VPN 端接。

路由器——范围广泛的灵活的网络设备，为所有性能要求提供多种路由和安全性服务。大多数设备为模块化设备且有一系列 LAN 和 WAN 物理接口。

VPN 路由器——与上面所描述的路由器一样，此设备提供了站点间和远程接入 VPN 端接。远程接入 VPN 客户机可安装于不同 OS 之上的软件 VPN 客户机软件；能建立单一个 VPN 端接设备的隧道来接入网络资源。

硬件 VPN 客户机——无需要安装在用户工作站上即可模拟软件 VPN 客户机的硬件设备。根据本地用户需求，它建立一系列 VPN 端接设备的隧道来接入网络资源。

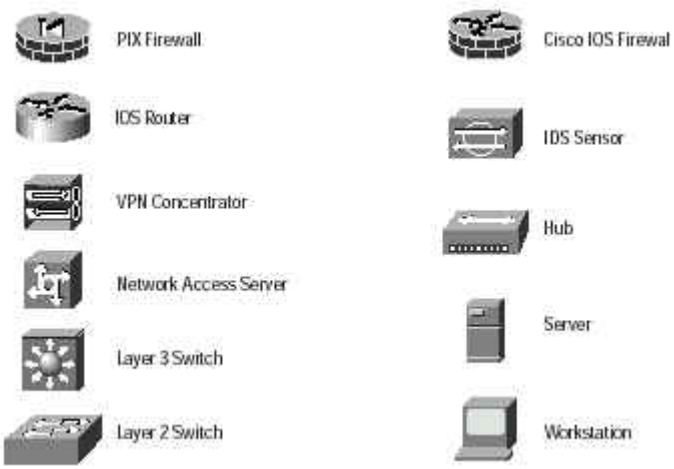
主机 IDS——主机入侵检测系统是一个监控单独主机上行为的软件应用。监控技术可包括验证操作系统和应用呼叫、检查记录文件、文件系统和网络连接。

网络 IDS——网络入侵检测交流。一般使用的无干扰，此设备可获取 LAN 网段上的信息流，并试图特定的信息流与已知攻击签名相匹配。签名包括从基本（简单分组和方向）签名到需状态表和第 7 层应用跟踪的复合（多分组）签名等多种类型。

应用服务器——为企业最终用户直接成间接地提供应用服务，服务可包括工作流、通用办公室和安全应用。

管理服务器——为企业网络的运输至提供网络管理服务。服务可包括通用配置管理、监控网络安全设备和安全功能的运行。

图 27 图例



PIX 防火墙　　Cisco IOS 防火墙
IOS 路由器　　IDS 传感器
VPN 集中器　　集线器
网络接入服务器　　服务器
第三层交换机　　工作站
第二层交换机

图示列表

参考材料

RFC 和草案

RFC 2401 “互联网协议的安全体系结构”
RFC 2402 “IP 验证报头”
RFC 2403 “ESP 和 AH 内的 HMAC-MD5-96 的使用”
RFC 2404 “ESP 和 AH 内的 HMAC-SHA-1-96 的使用”
RFC 2405 “ESP DES-CBC 密码员算法介绍（四）”
RFC 2406 “IP 封装安全有效负载（ESP）”
RFC 2407 “ISAKMP 互联网 IP 安全域说明”
RFC 2408 “互联网安全协议和关键管理协议（ISAKMP）”
RFC 2409 “互联网密钥交换（IKE）”
RFC 24010 “空力密算法及其与 IPSec 的共同使用”
RFC 24011 “IP 安全文件发展计划”
RFC 24012 “OAKLEY 密钥端接协议”
RFC 24018 “专用互联网地址分配”http://www.ietf.org/rfc/rfc1918.txt
RFC 24091 “路径 MTU 搜索”http://www.ietf.org/rfc1191.txt

IKE 内的扩展验证（XAUTH）：http://www.ietf.org/internet-drafts/draft-beaulieu-ike-xauth-01.txt
ISAKMP 配置方法：http://www.ietf.org/internet-drafts/draft-dukes-ike-mode-cfg-01.txt

各种参考信息

DES 受干扰：http://www.rsa.com/rsalabs/des3/

公共/专用密钥的强度：http://www.rsasecurity.com/news/pr/990826-2.html
VoIP 带宽占用：http://www.cisco.com/warp/public/788/pkt-voice-general/bwidth_consume.html

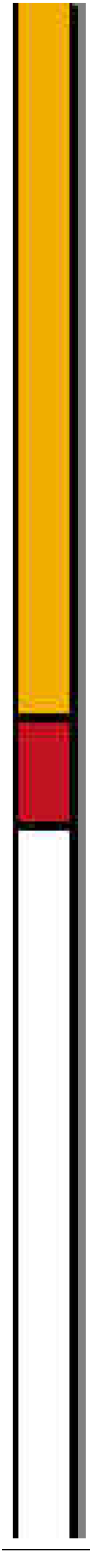
QoS:http://www.cisco.com/warp/customer/cc/pd/iosw/prodlit/iosqds.htm

合作伙伴产品参考信息

Entercept 基于主机的 IDS：http://www.entercept.com
RSA Secure ID OTP 系统：http://www.rsasecurity.com/product/securid/
Ione Alarm Pro 个人防火墙：http://www.zonelabs.com/products/index.html

致谢

作者谨在此公开感谢所有帮助创建 SAFE 体系结构及撰写此文的人。当然，如果没有思科系统公司总部及运作现场所有思科员工的贡献与反馈意见，这一体系结构是不可能成功建立的。此外，还有许多在实验室操作与体系结构验证过程中作出了贡献。感谢 Rahimulah Rahimi 帮助我们构建了设计中的大多数设备。感谢你们大家所作的工作。



思科系统(中国)网络技术有限公司

北京
北京市东城区东长安街一号
东方广场东一办公楼 19-21 层
邮政编码：100045
电话：(8610)65267777
传真：(8610)85181881

广州
广州市天河北路 233 号
中信广场 43 楼
邮政编码:510620
电话:(8620)38770000
传真:(8620)38770077

上海
上海市淮海中路 222 号
力宝广场 32 ~ 33 层
邮政编码:200021
电话:(8621)53966161
传真:(8621)53966750

成都
成都市顺城大街 308 号
冠城广场 23 层
邮政编码:610017
电话:(8628)6528888
传真:(8628)6528999