在 VPN 3000 集中器上为 IPSec 配置 NAT 透明模式

目录

简介

网络地址转换(NAT)的开发可以解决互联网协议版本4(IPV4)用完地址空间这一问题。现在，家庭用户和小型办公室网络使用 NAT 作为购买注册地址的替代方案。公司单独实现 NAT 或使用防火墙以保护他们的内部资源。

多对一，最常用的实施NAT解决方案是将几个专用地址映射到单个可路由(公用)地址；这也称为端口地址转换 (PAT)。关联在端口级别实现。PAT解决方案为不使用任何端口的IPSec数据流制造了一个问题。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco VPN 3000 集中器
- Cisco VPN 3000 客户端版本 2.1.3 及更高版本
- 适用于 NAT-T 的 Cisco VPN 3000 客户端和集中器版本 3.6.1 以及更高版本

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

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

封装安全有效载荷

协议 50（封装安全负载 [ESP]）处理加密/封装的 IPSec 数据包。大多数PAT设备都不能与ESP结合使用，因为它们已被编程为其运行只能采用传输控制协议（TCP）、用户数据协议(UDP)和互联网控制消息协议(ICMP)。另外，PAT 设备无法映射多个安全参数索引 (SPI)。VPN 3000客户端的NAT透明模式可以把ESP封装在UDP内，并将它发送到一个协商端口，从而解决此问题。VPN 3000集中器上活跃的属性名称是通过NAT的IPSec。

新的协议NAT-T是一种IETF标准(仍然处于本文编写的草稿阶段)，还能够在UDP中封装IPSec信息包，但需要在端口4500上运行。该端口不可配置。

NAT 透明模式如何工作？

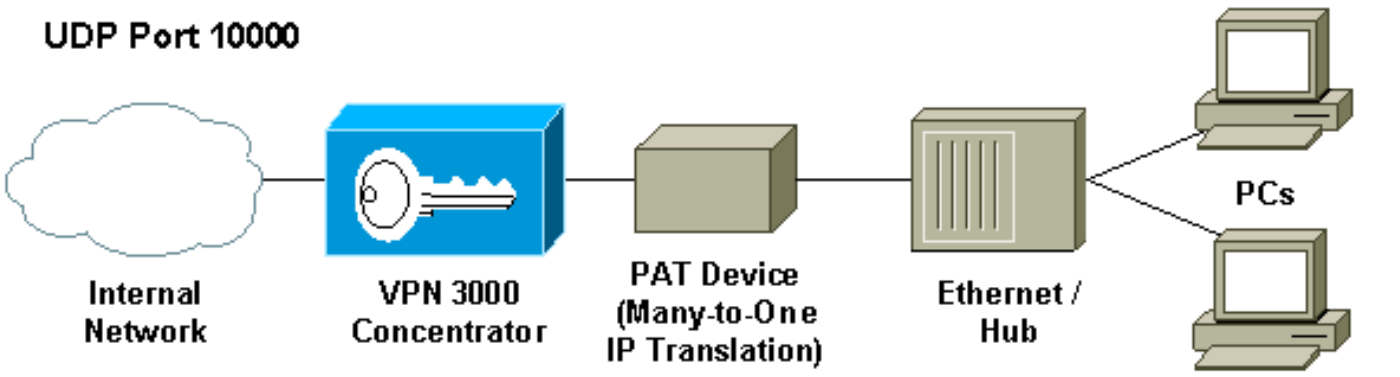
在 VPN 集中器上激活 IPSec 透明模式将创建不可见的过滤器规则，并将它们应用于公共过滤器。然后，配置的端口号将在 VPN 客户端连接时以透明方式传递给 VPN 客户端。在入站端，从该端口发出的UDP入站流量直接传递到IPSec，进行处理。数据流解密并解封，然后以常规方式路由。在出站端，进行IPSec加密、封装，然后应用UDP报头(如果这样配置)。在三种情况下，运行时间过滤器规则会从适当过滤器中撤销并删除。当UDP的IPSec禁止用于某个组时，当某个组被删除时，或者当该端口上的SA UDP的最新活动IPSec被删除时。发送 Keepalive 以防止 NAT 设备因处于不活动状态而关闭端口映射。

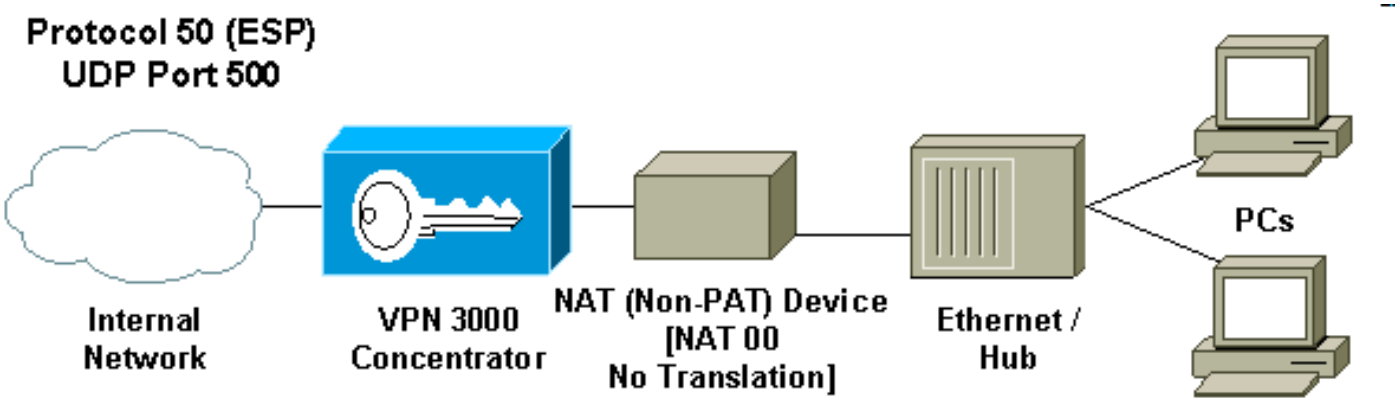
如果NAT-T的IPSec可用于VPN集中器，VPN Concentrator/VPN客户端则使用UDP封装的NAT-T模式。NAT-T的运行方式是：在IKE协商过程中，自动检测VPN客户端和VPN集中器之间的所有NAT设备。您必须保证UDP端口4500的运行没有被阻拦在VPN集中器和NAT-T的VPN客户端之间。并且，如果您正在使用已经使用该端口的早先IPSec/UDP配置，您必须重新配置早期IPSec/UDP配置，以使用不同UDP端口。由于NAT-T是IETF草案，因此如果其他供应商实施此标准，使用多供应商设备则会有帮助。

与 IPSec over UDP/TCP 不同，NAT-T 可以与 VPN 客户端连接和 LAN 到 LAN 连接协同工作。另外，Cisco IOS® 路由器和 PIX 防火墙设备支持 NAT-T。

您不需要启用UDP的IPSec，就能让NAT-T运行。

配置 NAT 透明模式





使用以下过程在 VPN 集中器上配置 NAT 透明模式。

注意： UDP的IPSec配置在每一组，TCP NAT-T的IPSec则在全局中配置。

1. 配置 IPSec over UDP：在 VPN 集中器上，选择 **Configuration > User Management > Groups**。要添加组，请选择 **Add**。要修改现有组，请选择它并单击 **Modify**。点击IPSec选项卡，通过NAT检查IPSec，并通过NAT UDP端口配置IPSec。通过NAT的IPSec的默认端口是10000 (包括源和目的地)，但可以更改此设置。
2. 配置 IPSec over NAT-T 和/或 IPSec over TCP：在 VPN 集中器上，选择 **Configuration > System > Tunneling Protocols > IPSec > NAT Transparency**。选中 **IPSec over NAT-T and/or TCP 复选框**。

如果全部启用，请使用以下优先顺序：

1. IPSec over TCP。
2. IPSec over NAT-T。
3. IPSec over UDP。

使用 NAT 透明模式的 Cisco VPN 客户端配置

要使用IPSec over UDP或NAT-T，您需要在思科VPN客户端3.6版本和更新版本上启用IPSec over UDP。使用IPSec over UDP时，UDP端口由VPN集中器分配，同时NAT-T固定到UDP端口4500。

要使用IPSec over TCP，您需要在VPN客户端启用它，并且配置应该手工使用的端口。

相关信息

- Cisco VPN 3000 系列集中器支持页
- Cisco VPN 3000 系列客户端支持页
- IPSec 支持页面
- 技术支持 - Cisco Systems