[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
**H04L 12/24**
H04L 12/28

[12] 发明专利申请公开说明书

[21] 申请号 200410038976.4

[43] 公开日 2005 年 11 月 16 日

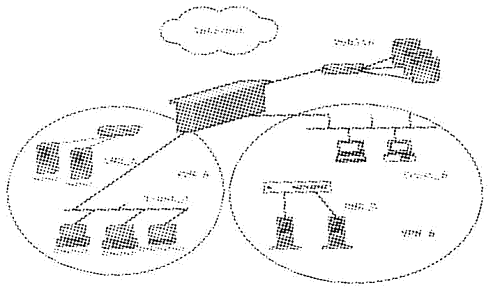
[11] 公开号 CN 1697396A

[22] 申请日 2004.5.10
[21] 申请号 200410038976.4
[71] 申请人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼
[72] 发明人 熊 鹰
权利要求书 2 页 说明书 8 页 附图 2 页

[54] 发明名称 基于防火墙实现本地虚拟私网络的方法

[57] 摘要

本发明提出了一种基于防火墙划分本地虚拟私网络区域的方法，其特征在于：包括如下步骤：步骤一，首先在防火墙的接口属性表中配置 VPN 属性值，即 VPN－ID；步骤二，在路由表的查找键值中也要增加 VPN－ID 域，也即 VPN－ID 和目标 IP 作为查找键值；步骤三，在安全策略表的查找键值中要同时增加 VPN－ID。 本发明在防火墙设备上实现本地 VPN 区域的划分，或者从另一个角度说，实现多个安全实体的防火墙资源共享；同时，实现了多个安全 VPN 实体间的访问控制和各个安全实体内各个安全区域的访问控制，为本地 VPN 应用提供方便实用的解决方案。



ISSN1008-4274

1、一种基于防火墙划分本地虚拟私网络区域的方法，其特征在于：包括如下步骤：

步骤一，首先在防火墙的接口属性表中配置VPN属性值VPN-ID；

步骤二，在路由表的查找键值中也要增加VPN-ID的域，即以VPN-ID和目标IP作为查找键值；

步骤三，在安全策略表的查找键值中同时增加VPN-ID。

2、根据权利要求 1 所述的基于防火墙划分本地虚拟私网络区域的方法，其特征在于：所述的步骤一和步骤二之间，如果防火墙内提供专门的服务器或支持 NAT，则在服务器表的查找键值中增加 VPN-ID 域和目标 IP 地址。

3、根据权利要求 1 或 2 所述的基于防火墙划分本地虚拟私网络区域的方法，其特征在于：所述的步骤四之后，包括：所述的防火墙如果支持 NAT 转换，则在 NAT 转换表的查找键值中增加 VPN-ID 域。

4、根据权利要求 1 所述的基于防火墙划分本地虚拟私网络区域的方法，其特征在于：还包括：在防火墙的接口属性表中配置为安全区域编号 ZONE-ID；在安全策略表的查找键值中要增加 ZONE-ID。

5、根据权利要求 1 所述的基于防火墙划分本地虚拟私网络区域的方法，其特征在于：所述的步骤一，具体包括：为防火墙的每一个内部接口通过接口属性表，增加一个 VPN-ID，所有 VPN-ID 相同的接口所连接内部网络构成一个本地的虚拟私网络。

6、根据权利要求 1 所述的基于防火墙划分本地虚拟私网络区域的方法，其

特征在于：所述的步骤二，具体包括：根据报文的目的 IP 地址和 VPN-ID，查路由表，如果找到，则记录相应的路由信息；如果未找到，则查路由表，以确定是否访问公网地址；如果最后仍查不到路由，则按照系统确定的策略丢弃或者作重定向等其它处理。

7、根据权利要求 1 所述的基于防火墙划分本地虚拟私网络区域的方法，其特征在于：所述的步骤二，如果各 VPN 的私网地址均使用 RFC1918 确定的私网地址，则可以根据目的 IP 地址的类型，只查私网路由表或只查公网路由表。

8、根据权利要求 4 所述的基于防火墙划分本地虚拟私网络区域的方法，其特征在于：所述的步骤三，根据步骤二得到的出接口信息，进一步从出接口属性表中得到目标 VPN-ID 和 ZONE-ID 信息，从而根据源 VPN-ID、源 ZONE-ID 以及源 IP 地址等信息，再查安全策略表，如果策略通过，则转发报文；否则，系统确定的策略丢弃或者作重定向等其它处理。

9、根据权利要求 3 所述的基于防火墙划分本地虚拟私网络区域的方法，其特征在于：不同 VPN 通过 NAT 转换表，共享防火墙的公网地址资源，实现公网地址资源的复用和/或内部 VPN 的互访。

# 基于防火墙实现本地虚拟私网络的方法

## 技术领域

本发明涉及一种虚拟私网络的实现方法，特别是涉及基于防火墙技术构建安全的可相互隔离的本地虚拟私网络的方法。

## 背景技术

虚拟私网络（VPN）由于其灵活、便宜、安全等优点，已得到越来越广泛的使用。简单地说，VPN就是利用开放的公众网络建立专用数据传输通道，将远程的分支机构、商业伙伴等连接起来，形成的一种逻辑的闭合用户群。一般而言，VPN有一定的地理跨度。有多种方案可以实现这种VPN，如基于用户CPE设备的点到点的方案和基于ISP的运营商提供的VPN方案。

现有技术中，MPLS VPN是一种运营商提供的VPN解决方案之一，它适合于运营商大规模部署，同时也需要运营商多台设备的配合，是一种复杂的解决方案，需要一整套与MPLS相关的标签协议、路由协议来实现，而且需要设备支持MPLS标记，因此，如果希望在类似于某一个大厦内的本地VPN隔离和安全防范中，这种方案由于成本和管理原因，并不适用；而且也不能实现防火墙的安全区域的功能。

目前的防火墙设备，一般均假定只有一个公司实体来使用，一般安全等级最高的安全区域可以任意访问其它低等级的区域，如果在本地的防火墙之下有多个公司同时使用时，不同公司应有各自私有的安全区域，不同公司的区域之间禁止互访，所以目前的防火墙不能应用于这种场合。

由于本地情况下需要实现VPN的情况广泛存在，比如，上文中提到的某一个大厦内有多个公司的情况；或者，一个公司的内部（同一个防火墙下），不同的部门需要保密的情况，而本地一般都具有防火墙设备。如果能在防火墙上实

现VPN的划分，则既可以实现本地VPN隔离和安全防范，又可以实现对外的防火墙安全防范；并且并不增加新的设备，管理起来也会更加方便。

## 发明内容

本发明要解决的技术问题是提出一种基于防火墙实现本地虚拟私网络的方法，本发明所述方法为防火墙的安全增加一层本地VPN的隔离保护，可实现保护机制更为灵活的本地虚拟私网络。

本发明所述一种基于防火墙划分本地虚拟私网络区域的方法，包括如下步骤：

步骤一，首先要在防火墙的接口属性表中配置VPN属性值，即VPN-ID;

步骤二，在路由表的查找键值中也要增加VPN-ID域，也即VPN-ID和目标IP作为查找键值;

步骤三，在安全策略表的查找键值中要同时增加VPN-ID。

如上所述的基于防火墙划分本地虚拟私网络区域的方法，步骤一和步骤二之间，还包括：如果防火墙内提供专门的服务器或支持NAT，则在服务器表的查找键值中增加VPN-ID域和目标IP地址;

如上所述的基于防火墙划分本地虚拟私网络区域的方法，在所述的步骤三之后，还包括如果防火墙如果支持NAT，则在NAT转换表的查找键值中增加VPN-ID域。

本发明在防火墙设备上实现本地VPN区域的划分，或者从另一个角度说，实现多个安全实体的防火墙资源共享；同时，实现了多个安全VPN实体间的访问控制和各个安全实体内各个安全区域的访问控制，为本地VPN应用提供方便实用的解决方案。

**附图说明**

图 1 为本发明基于防火墙的本地 VPN 组网示意图;

图 2 为本发明所述方法中设置防火墙各表的示意图;

图 3 是本发明所述的防火墙各表的结构示意图;

图 4 为本地 VPN 的报文处理的流程图。

**具体实施方式**

本发明中，所述的本地 VPN 的概念与通常的 VPN 有所不同，它由同在本地的连接到一个共同的防火墙设备上的多个公司或站点实体构成，这些实体之间逻辑上互相隔离，形成不同的 VPN 域，也即这些实体之间不可以直接互访，而且可以使用重叠的 IP 地址。

本发明所述的 VPN 只有本地意义，至于这些 VPN 是否在跨越防火墙后，与远端其它的网络实体建立 VPN 关系。

本地 VPN 典型的应用，其组网如图 1 所示：某一大厦中物业提供一台防火墙，大厦中的各个公司可以接入到防火墙的一个或多个接口上，彼此之间形成不同的 VPN；同一公司内所属的各防火墙接口还可以配置不同的安全区域，以实现公司内部的安全控制；大厦提供统一的 Internet 出口，并且由专门的服务器提供一些增值业务，比如信息发布的 Web 服务和 VOD 点播等服务。

上面以大厦中的多个公司为例说明该问题，实际上有着该需求的不仅限于这一种应用场合。比如，在一个公司内部如果有需要严格隔离和划分的单位，也可以使用这种方式，这时 VPN 只是多了一个安全隔离层面。

本发明的技术方案，如下所述：

步骤一，首先要在防火墙的接口属性表中配置VPN属性值，即VPN-ID;

步骤二，在路由表的查找键值中也要增加VPN-ID域，也即VPN-ID + 目标IP作为查找键值;

步骤三，在安全策略表的查找键值中要同时增加VPN-ID。

在所述的步骤一和步骤二之间，还包括：如果防火墙内提供专门的服务器或支持NAT，则在服务器表的查找键值中增加VPN-ID域和目标IP地址；

在所述的步骤三之后，还包括：如果防火墙同时支持NAT，还需要在NAT转换表的查找键值中增加VPN-ID域。

图 2 是本发明所述方法中设置基于防火墙本地 VPN 的方法示意图，为了实现基于接口/子接口划分 VPN 区域，本发明对防火墙的接口属性表、路由表、策略表、NAT 绑定表、内部服务器地址映射表进行了设置，实现了基于防火墙的本地 VPN 区域划分。

结合图 2，具体的步骤说明如下：

步骤 201：用户首先要在接口属性表中配置 VPN 属性，即 VPN-ID；即为防火墙的每一个接口通过接口属性表，增加一个 VPN-ID，所有 VPN-ID 相同的接口所连接内部网络构成一个本地的虚拟私网络。一般连接公网的接口的 VPN-ID 设为 0。

同时，如果 VPN 内部需要设置安全区域，也需要基于接口进行划分，所以接口属性表中还可以配置安全区域编号，也即 ZONE-ID。

报文从接口进入时，需要获取这两个参数以进行后续的处理，参见图 2 中的表 201，接口属性表中还可以有许多其它属性，比如 MTU、封装类型等，不同的系统中可以有不同设置，本发明对此没有限制。

步骤 202：防火墙中一般要实现静态或动态服务器映射，以完成灵活的目标访问功能。为了实现 VPN 的隔离，需要在服务器表的查找键值中增加 VPN-ID 域，同时，查找键值中必须包括目标 IP 地址。

所述的增加 VPN-ID 域是指在原有的表项的内容上增加一个 VPN-ID 得到一个新表，在新表中如果两个表项未只有 VPN-ID 不同，其余的部分相同，则被认为是两个不同的表项。这样在新表看来，所有的表项按 VPN-ID 划分成多个区域，不同的 VPN-ID 域中，可以有相同的项目，而同一个域中，不能出现相同的项目。以下其他步骤中，所述的增加 VPN-ID 域的含义相同。

可选地，服务器表也可以包括其它内容如 IP 协议号、TCP/UDP 端口号。参见图 2 中的表 202，服务器表可以有许多属性，比如应用协议类型、连接数量、目标地址 NAT 等，不同的系统中可以有不同设置，本发明对此没有限制。

步骤 203：为了实现 VPN 域间的路由隔离，在路由表的查找键值中也要增加 VPN-ID 域，也即 VPN-ID + 目标 IP 作为查找键值。参见图 2 中的表 203，对于路由表项的其他内容，本发明没有限制。

步骤 204：为了实现基于 VPN 域和安全区域间的策略，在安全策略表的查找键值中要增加 VPN-ID。如果 VPN 内部设置有安全区域，同时还要增加 ZONE-ID。对于基于 IP 的安全策略，在查找键值中一般包括源/目标 IP 地址。

可选地，还可以包括 IP 协议号、TCP/UDP 端口号等域。安全策略表的属性中一般有是否过滤、是否作带宽管理等各种策略内容，本发明对此没有限制。

如果在 VPN 内使用私网地址，一般是 RFC1918 中建议的地址，用户需要访问 Internet，或如果安全策略允许时，访问其它 VPN 内的用户，需要作网络地址转换。

参见图 2 中的表 205，为了支持不同 VPN 使用公共的 NAT 地址池，需要在 NAT 转换表的查找键值中增加 VPN-ID 域，通常，在查找键值中还包括源 IP 地址，可选地，还可以包括 IP 协议号、TCP/UDP 端口号等域。NAT 转换表的属性中一般有转换后的 IP 地址等内容，本发明对此没有限制。

NAPT(Network Address Port Translation，网络地址-端口转换)与 NAT 类似，也可以同样适用于本发明。

参见图 3 中的 210-212，以上几类表均以树的形式存在；

210：是一个哈希桶。在对表项键值进行哈希后，取哈希值的前 N 位在该桶内进行索引，可以初步分开不同的表项；

211：是树的分叉节点。当有两个或多个表项进行哈希后，如果落在同一个哈希桶内，则需要用到分叉节点进行区分；

212：是叶子节点，存放表项的具体内容。

下面通过经过本发明方法设置的放火墙对报文的处理，进一步说明本发明的技术方案：

图 3 为本地 VPN 的报文处理的流程图。

报文从物理端口进入到防火墙中。这里的物理端口一般是指以太网口，也可以是指 ATM 等其它类型的端口。报文处理的具体步骤如下：

步骤 301：报文针对不同的物理链路，查对应的接口属性表，如果是子接口，比如以太网的 VLAN 子接口，则查对应的子接口属性表。按照链路层信息进行的分类和处理，比如区分单播、多播和广播包，并进行必要的报文合法性检查。之后，携带接口属性表中配置的 VPN-ID 和 ZONE-ID 信息，转下一步。

步骤 302：在进行 IP 层的处理之前，先要进行基本的 IP 报文合法性检查，主要是 RFC1812 中规定的处理。之后查服务器表，以确定是否配置有专门的服务器或是否有目的地址 NAT 映射。

查服务器的步骤是可选的，如果不提供专门的服务器，且不支持目的 IP 地址 NAT，则此步骤可省略。

步骤 303：根据报文的目的 IP 地址和 VPN-ID，查路由表，如果命中，则记录相应的路由信息；如果未命中，则以 VPN-ID=0 来查路由表，以确定是否访问公网地址。

这里可以有一些可选的优化，比如，如果各 VPN 的私网地址均使用 RFC1918 确定的私网地址，则可以根据目的 IP 地址的类型，只查 VPD-ID 对应的私网路由表或只查 VPN-ID=0 对应的公网路由表。如果最后仍查不到路由，则按照系统确定的策略丢弃或者作重定向等其它处理。

步骤 304：在步骤 303 中查到路由表后，可以得到出接口信息，进一步从出接口属性表中得到目标 VPN-ID 和 ZONE-ID 信息，从而根据源 VPN-ID、源 ZONE-ID 以及源 IP 地址等信息，再查策略表，以确定访问是否允许，是否要进行地址转换以及其它策略动作。如果策略通过，则转发报文。

所述的安全策略一般可以分为两种，一是例外禁止，其余允许通过；二是

例外允许，其余禁止通过；也可以是两种策略的组合。进一步，如果是VPN之间的互访，则按目标VPN-ID和ZONE-ID信息和源VPN-ID和ZONE-ID信息在安全策略表中查找对应的安全策略；如果是VPN到公网或公网的VPN的报文，则按目标VPN-ID和ZONE-ID信息或源VPN-ID和ZONE-ID与公网IP查找对应的安全策略。如果通过，则转发报文；如果不通过，则按设定进行重定向或直接丢弃。

步骤305：如果需要进行NAT，则从NAT地址池中分配空闲的地址资源，进行NAT，并创建NAT转换表，以便后续报文可以直接使用该转换表。

步骤306：对报文进行链路层的封装，并转发。

步骤307：后续报文可以直接通过NAT转换表转发，省去第一个包的各个处理环节。

各VPN实体可以通过二/三层交换机或路由器与防火墙相连，配置静态路由或者运行RIP/OSPF等路由协议。

在支持NAT的情况下，不同VPN可以共享宝贵的公网地址资源，实现访问公网（如：Internet）以及内部VPN的互访。

下面通过具体实例说明，经过本发明设置的防火墙是如何实现公网地址的共享：

如图1所示的网络结构中，假定VPN A中的主机1，记为A1，和VPN B中的主机2，记为B2，分别发起一个访问公网主机3的请求报文RA1和RB2；这两个请求在经过步骤301-304的处理后，到步骤305

RA1请求报文从NAT地址池中分配了一个地址和TCP端口号对（a.b.c.d，3000），其的源地址替换为该公网地址后转发，并记录下一个NAT转换关系{VPN_A，A1，（a.b.c.d，3000）}；

同时RB2请求仍然可以从NAT地址池中分配了一个地址和TCP端口号对（a.b.c.d，3001），其的源地址替换为该公网地址后转发，并记录下一个NAT转换关系{VPN_B，B2，（a.b.c.d，3001）}；

当RA1请求的应答从主机3回来时，可以使用目的（IP+TCP+端口号）找到NAT转换关系表{VPN_A，A1，（a.b.c.d，3000）}，从而将目的恢复为VPN A中的主机A1。

同样当RB2请求的应答从主机3回来时，可以使用目的（IP+TCP+端口号）找到NAT转换关系表{VPN_B，B2，（a.b.c.d，3001）}，从而将目的恢复为主机VPN_B中的主机B2。

这样，就实现了VPN A 和VPN B对地址池资源的共享。

如果是VPN之间的互访，最简单的方式是在VPN内使用公网地址，将VPN之间的互访和外部的访问同样对待；也可以通过DNS服务器使用TwiceNAT（两次转换）的方式实现，可以参见《RFC2663 NAT Terminology and Considerations》文献。无论哪种方式，都可以通过策略方便地实现VPN间的互访控制。

最后所应说明的是：以上实施例仅用以说明而非限制本发明的技术方案，尽管参照上述实施例对本发明进行了详细说明，本领域的普通技术人员应当理解：依然可以对本发明进行修改或者等同替换，而不脱离本发明的精神和范围的任何修改或局部替换，其均应涵盖在本发明的权利要求范围当中。

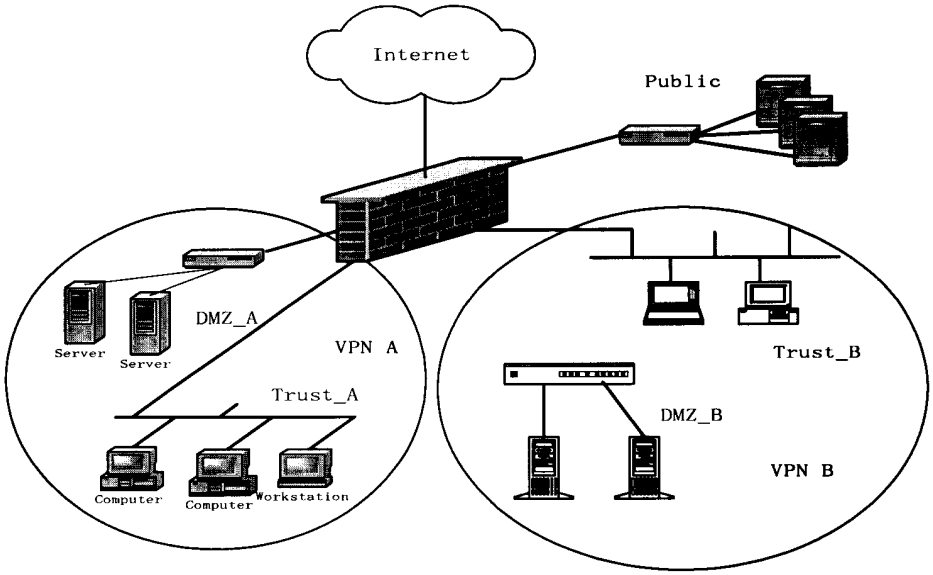

Internet
Public
Server
Server
DMZ_A
VPN A
Trust_A
Computer
Computer
Workstation
Trust_B
DMZ_B
VPN B

图 1

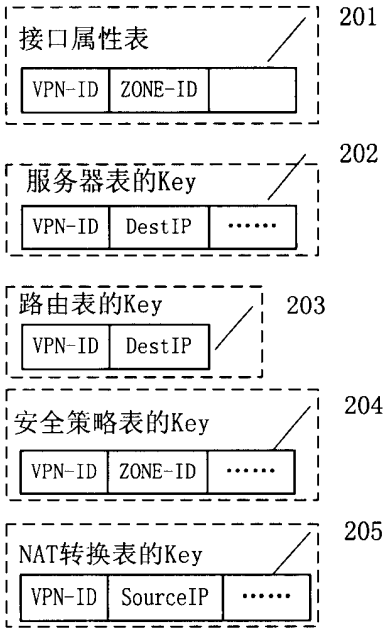

接口属性表
VPN-ID
ZONE-ID
201
服务器表的Key
VPN-ID
DestIP
202
路由表的Key
VPN-ID
DestIP
203
安全策略表的Key
VPN-ID
ZONE-ID
204
NAT转换表的Key
VPN-ID
SourceIP
205

图 2

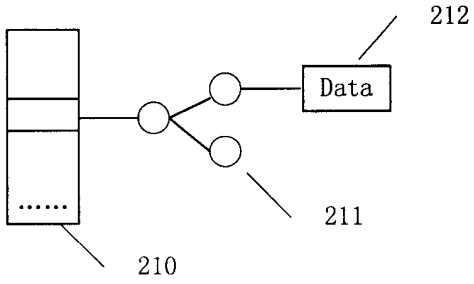

212
Data
211
210

图 3

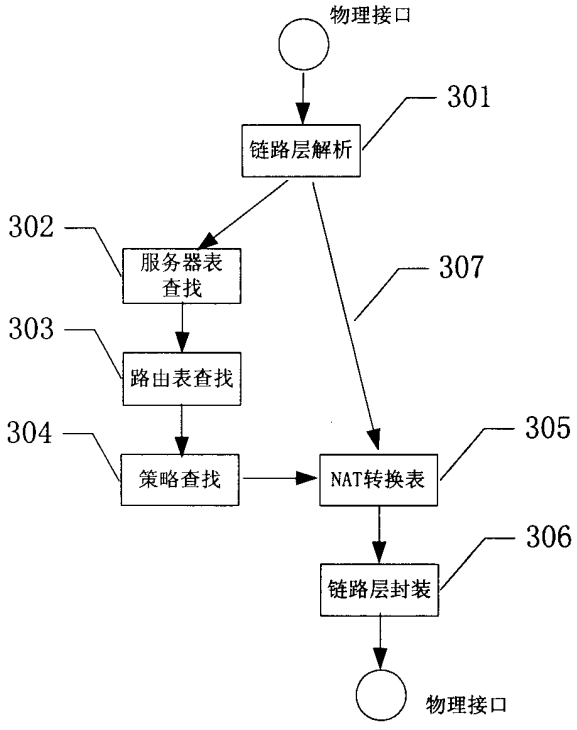

物理接口
301
链路层解析
302
服务器表查找
307
303
路由表查找
304
策略查找
NAT转换表
305
306
链路层封装
物理接口

图 4