虚拟专用网的可扩展性研究*)

Scalability Research of Virtual Private Network

刘桂开　雷振明

(北京邮电大学信息工程学院　北京100876)

Abstract Analyzes VPN scalability in architecture, management and routing. According to establishing BGP/MPLS VPN, some methods that can enhance VPN scalability are proposed. Finally some general principles during establishing large-scale VPN are summarized.

Keywords Virtual Private Network (VPN), Scalability, Network architecture, VPN management, VPN routing

大型网络的可扩展性往往不容易解决,是一个难点,但又是重点,在网络设计和具体的构建过程中都必须着重考虑,因为可扩展性问题解决不好,会严重影响网络规模的发展,也会影响到网络的性能,甚至会影响到网络技术的可行性。曾经为了解决无连接网络和面向连接网络的结合问题而提出的叠加模型,由于存在管理上的复杂性和严重的可扩展性问题,使得这种网络技术的发展受到了制约。因为虚拟专用网需要建立在公用网络基础上,所以它的可扩展性尤为重要,直接关系到虚拟专用网配置和管理的复杂性,同时对虚拟专用网设备之间的互通也有很重要的影响。

1. 虚拟专用网体系结构的可扩展性分析

虚拟专用网体系结构一般包括这些部分:VPN 拓扑结构,网络结构,VPN 的独立性、扩展能力、冗余和操作的透明性。VPN 的拓扑结构是指 VPN SITE 之间的虚拟链路集合,虚拟链路可以通过建立隧道来实现。拓扑结构可以是 Full-mesh、Partial-mesh 和 Hub-and-Spoke 等,选用哪种拓扑结构,要依据具体的环境和客户的要求来决定,如小型的 VPN 可以采用 Full-mesh 拓扑结构,但对大型 VPN 却很不合适,它的可扩展性会很差,有着 $O(n^2)$的复杂度。

网络结构是指 VPN 与底层网络之间的逻辑结构,有扁平结构和分级结构之分。基于客户边缘设备的 VPN(CPE-based VPN)就是一种扁平结构,对 VPN 的配置、管理以及隧道的建立,都是在 CPE 之间进行。另一类 VPN 是基于网络的 VPN(Network-based VPN),它是一种分级结构,允许业务提供商(ISP)的一个边缘设备(PE)可以连接许多的 CPE,对 VPN 的配置、管理以及隧道的建立,都是在 PE 之间进行。与一个 VPN 相关的 PE 的数目相对于 CPE 来说要少得多,因此,基于网络的 VPN 的可扩展性要优于基于客户边缘设备的 VPN。也就是说,分级的网络结构可以提高 VPN 的可扩展性。

VPN 的独立性是相对于底层网络或骨干网来说的,虽然 VPN 需要依托公用网络,但依赖的程度却是可以变化的,尽量做到相互独立会带来许多的优点。具体来说,VPN 的独立性包括地址空间的独立性、路由的独立性和骨干网技术的独立性。地址空间的独立性是指 VPN 与底层网络使用不同的地址空间,底层网络使用公网地址空间,而 VPN 使用专网地址空间。这样,不仅有利于 VPN 的配置和管理,而且也增强了 VPN 的可移植性。路由的独立性是指 VPN 的路由技术可以完全独立于底层网络,即它们各自使用的是独立的路由系统,VPN 的路由不会传播到底层网络,既有利于 VPN 的安全性,又减少了底层网络的路由处理负担,增强了网络的可扩展性。骨干网技术的独立性是指 VPN 实现机制应该独立于底层网络或骨干网技术,有利于 VPN 的扩展,如跨多个 ISP 域的 VPN 就不会要求 ISP 支持特定的技术。由以上分析可知,独立性越强的 VPN 具有更好的可扩展性。

VPN 的扩展能力本身就是 VPN 可扩展性中的一部分,可扩展性越好,越有利于 VPN 的扩展,包括将 VPN 扩展到多个 ISP 域、扩展到远程用户接入以及 VPN 之间的互连等。

冗余可以提高网络的可靠性,它与网络的可扩展性是一对矛盾。因为网络的冗余程度越高,网络就越复杂,从而会影响网络的可扩展性,所以,在建立 VPN 时,要采取某种平衡的方案,既要保证网络具有一定的可靠性,又要不影响网络的可扩展性。

操作的透明性与 VPN 的独立性有关,独立性越强,说明 VPN 在逻辑上与底层网络的分离越明显,二者之间的相互干扰就越小,互不干扰的操作称为 VPN 和底层网络在这些操作上是透明的。

2. 虚拟专用网管理的可扩展性分析

VPN 的管理包括 VPN 成员管理、访问控制管理和安全管理。

VPN 成员管理就是要确定 VPN 成员和分发 VPN 成员信息,成员的确定是建立 VPN 的第一步。一种方法是手工配置所有与 VPN 有关的设备;另一种方法是客户-服务器模式,成员信息存放在一个服务器上,需要成员信息的 VPN 设备通过访问此服务器获取信息;第三种方法是通过路由协议来传播成员信息。可以看出,手工配置只适应于小型的 VPN,客户-服务器模式可以用于大型的 VPN,但有很大的局限性,因为服务器容量不够或出现故障都会影响整个 VPN 的建立,所以对构建大型的 VPN,通过路由协议来传播成员信息比较合适。

访问控制是为了保证 VPN 的专用性,控制什么样的用户可以访问到什么样的 VPN 资源。访问控制的策略信息需

*)本文由国家重大自然科学基金项目"高速信息网中关键基础问题"(项目编号:69896240)资助。刘桂开　博士生,主要研究方向:宽带 ATM 和 IP 技术。雷振明　教授,博士生导师。

要配置到相关的 VPN 设备，而且还要加以维护。对大型 VPN 来说，不能完全依靠手工操作来进行，要尽量减少手工参与才有利于 VPN 管理的可扩展性。

安全管理主要是针对安全级别要求高的 VPN 来说的，因为需要对用户信息或数据进行加密和认证，于是，密钥管理就成了 VPN 管理的一个非常关键的部分，它包括密钥的产生、交换和维护。密钥管理的目标是既要满足安全要求，又要易于管理。

综上所述，要提高 VPN 管理的可扩展性就是要尽量减少手工参与 VPN 成员信息和策略信息的配置和维护。

3. 虚拟专用网路由的可扩展性分析

现在实现第三层 VPN 的机制主要有两种，一种是集成模式（Piggybacking Mode），另一种是叠加模式（Overlay Mode）。用集成模式构建的 VPN 与底层网络位于同一个平面，VPN 的路由完全依赖于底层网络的路由，VPN 路由的可扩展性同样依赖于底层网络路由的可扩展性。用叠加模式构建的 VPN 在逻辑上是叠加于底层网络之上，它就象一个真实的网络一样，具有独立的路由系统，其路由可扩展性相当于一个非虚拟网络的路由可扩展性。因此，大型 VPN 与非虚拟网络一样，不仅具有相同的路由复杂性，而且非虚拟的大型网络所面临的路由可扩展性问题同样适应于大型 VPN。一般来说，要设计一个具有可扩展性的路由系统需要从如下一些方面进行考虑：建立分级路由，引入故障隔离方法，尽可能减少路由处理负担，定义易管理的路由策略和由其他系统辅助路由处理等。

建立分级路由是为了减少一个路由域中路由器的数量，原因是如今的大型网络都由大量的路由器组成，而且具有复杂的拓扑结构，导致了路由器之间数目庞大的邻接关系。而现阶段的路由协议面对如此复杂的结构显得处理能力不够，所以，建立分级路由是一种明智的方法。

故障隔离是一种具有可扩展性的路由设计所必须具备的能力，它需要定位出现的问题或故障，防止它们扩散到整个网络、消耗路由器资源以致引起全网的不稳定。上述建立分级路由的方法将一个大的路由域分成了许多小的路由域，在一定程度上达到了故障分离的目的。

尽可能减少路由处理负担是指避免携带没有必要的路由信息和减小路由波动带来的冲击，这样可以节省路由器资源的消耗、简化路由的复杂性和维持全网的稳定。所采用的方法有：无类域间路由（CIDR）和路由聚合；可能的话，利用缺省路由；减少可选路径；在边界使用静态路由等。

路由策略就是要定义路由过滤和路由选择的标准，达到流量控制、保护路由信息的完整性和高效发送流量的目的。要使路由策略易于管理，有如下一些基本原则：在满足要求的前提下，尽量使策略简单；尽可能采取自动操作，尽量避免手工操作；尽可能避免基于个体前缀的策略；避免产生异议的策略；可能的话，使用其他系统辅助路由策略处理。

使用其他系统辅助路由处理是为了减轻路由器的处理负担，把复杂的路由信息处理和策略信息处理从路由器移到其他的系统，这样，路由器只需承担转发数据的任务，不会因为过度消耗路由器的资源而影响全网的性能。

综合起来看，要建立可扩展性好的路由系统，主要有两个方面的要求，一方面是要避免路由器资源的过度消耗，另一方面就是要降低路由的复杂程度。

4. 提高虚拟专用网可扩展性的方法

这里所列出的方法是从构建 BGP/MPLS VPN[3]的过程中总结出来的，有的方法并不具有普遍性。

（1）在 MPLS（多协议标记交换）[4]体系结构上构建 VPN。MPLS 是一种利用标记来转发数据包的技术，开销很小，实现了高速交换，并且能够将无连接网络与面向连接的网络结合在一起，MPLS 已经发展成为一种较为理想的骨干网技术。在 MPLS 体系结构上构建的 VPN，VPN 隧道是两层标记堆栈的 LSP（标记交换路径），数据包的转发不是依靠路由信息，而是依靠标记，这就意味着骨干网中间的路由器并不需要知道任何有关 VPN 路由的信息，即 VPN 对这些路由器是透明的。无疑 VPN 的扩展也只与 MPLS 网络的边缘路由器有关，这样就保证了 VPN 具有了良好的可扩展性。

（2）在 BGP/MPLS VPN 中使用 Route Reflector（RR）。前面提到，Full-Mesh 的拓扑结构不适合构建大型的 VPN。当 VPN 涉及到的骨干网边缘路由器（PE）很多时，PE 之间仍采用 IBGP Full-Mesh 拓扑结构会使网络变得很复杂，同时带来严重的可扩展性问题。为了避免这种情况的发生，我们可以利用 BGP Route Reflector 来提高 VPN 的可扩展性。

（3）PE、RR 和 ASBR（自治系统边缘路由器）都不必保持所有 VPN 的路由。PE 只需保留与之相连的 VPN SITE 的路由信息。RR 可以有多个，两个 AS（自治系统）之间的 ASBR 也可以有多个，每一个 RR 或 ASBR 只需保持所有 VPN 中的一个子集的路由。这样，ISP 需要增加新的 VPN 时就不会受到可扩展性问题的制约。另外，如果多跳 EBGP 连接只存在于 AS 的 RR 之间也有利于增强 VPN 的可扩展性。

（4）一条 VPN 路由可以带有多个 Route Target 属性。Route Target 属性是用于控制 VPN 路由分发的。一条 VPN 路由只能有一个路由区分符 RD（Route Distinguisher），但可以有多个 Route Target 属性。在一个 SITE 属于多个 VPN 的情形下，同一条路由必须用多个 RD 来生成多条路由，分别对应不同的 VPN，但如果采用 Route Target 属性来控制分发，则只需这条路由带上多个 Route Target 属性就可以分发到不同的 VPN。所以，用 Route Target 属性可以达到跟使用 RD 相同的效果，不仅免去了多次分配 RD 的过程，同时也减少了路由的数量，提高了路由的可扩展性。

5. 构建大型虚拟专用网的一般原则

通过对 VPN 在体系结构、管理和路由等方面的可扩展性的分析，加上对具体构建 BGP/MPLS VPN 的总结，可以看出，为了提高 VPN 的可扩展性，在构建大型 VPN 的过程中应遵循以下一些基本原则：

（1）尽可能构建非 Full-Mesh 的拓扑结构。

（2）采用分级的网络结构。

（3）在可能的情况下，VPN 与底层网络之间的独立性越强越好。

（4）在网络冗余性和可扩展性之间要采取某些折衷的方案。

（5）VPN 与底层网络之间的操作透明性越强越好。

（6）尽量减少手工参与 VPN 成员信息和策略信息的配置和维护。

（7）建立分级路由，VPN尽可能拥有自己独立的路由系

（下转第78页）

则同时群体数字签名是(e,r,s)

3.3 群体数字签名的验证

验证者按如下步骤验证:

(1)从签名中心获得用户 u_i 的公钥 y_i,计算:$y=\sum_{i=1}^{n} y_i \bmod n$;

(2)计算:$X=e^{-1}(sG-ry)=(x,y)$,若 X=0,则群体签名失败;否则计算:v=x mod n;

(3)如果 v=r,则接受签名。

4 群体盲数字签名

群体盲数字签名也是从单盲数字签名发展而来,它指多人同时对同一信息进行数字签名而对信息的内容一无所知,而信息的拥有者却可以从签名者对盲化后的信息的数字签名得到对真实信息的数字签名。由于椭圆曲线加密体制的特点,因此基于椭圆曲线加密体制的群体盲数字签名在电子货币构造和电子投票设计等应用中更具潜力,也更易于实现。下面在文[2]的基于非超奇异椭圆曲线上的盲签名方案的基础上设计了一个同时群体盲数字签名方案,该方案的关键是各用户要将经概率生成的 r_i 传送给验证者,便于生成 r,以及验证者对信息的盲化。

4.1 系统初始化

签名中心根据2.1节和2.2节选择椭圆曲线,公开(E(GF(2^m)),a,b,G,m,h,F_x)(要求 m>160)。其中 F_x 是一取椭圆曲线上点的 x 坐标的函数,即 $F_x(U)$ 表示取点 U 的 x 坐标。假设有 n 个用户 u_i 要进行群体盲数字签名,则 u_i 选择自己的私钥 d_i,计算公钥:$y_i=d_iG$,向签名中心发送 y_i,并公开 y_i。

4.2 群体盲数字签名生成(图1)

则数字签名对(c,s)是用户 u_i 对信息 m 的群体盲数字签名。

4.3 群体盲数字签名验证

验证者 V 只需计算下列等式是否成立:

$c=h(m\|F_x(cY+sG,T) \bmod n)$,其中 $F_x(u)$ 表示取点 u 的 x 坐标。

安全分析及结论 上面两个群体数字签名方案是基于有限域 GF(2^n)上非超奇异椭圆曲线加密体制的,因此其安全性基于非超奇异椭圆曲线的安全性,而有限域 GF(2^n)上非超奇异椭圆曲线的安全性是基于椭圆曲线上离散对数难题的,它比基于有限域上的离散对数问题的公钥体制更安全,是值得

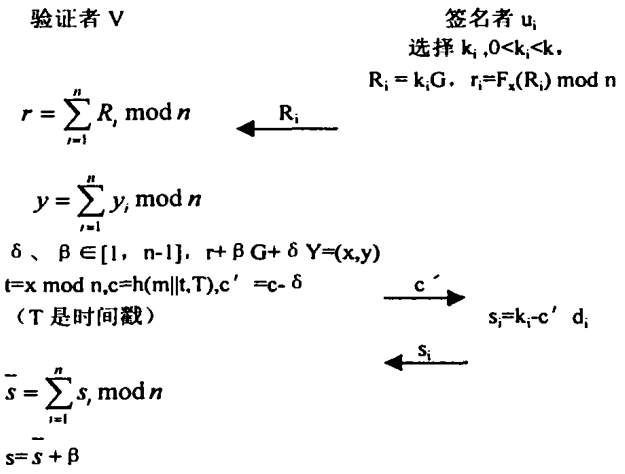

图1

信赖的;另外攻击者想伪造群体(盲)数字签名是不可行的,因为他不知道用户的私钥,即使在传送中获取了某个 r_i,也不可求得用户的私钥,因为他面对的是求解椭圆曲线上的离散对数难题。

基于有限域上的非超奇异椭圆曲线加密体制由于其密钥量小,安全高和灵活性等特点,在公钥体制、数字签名和认证等中的应用具有广泛潜力。本文在文[2]的基础上设计了群体数字签名和群体盲数字签名两种方案,在签名时传送信息量小,具有一定的实用价值。

参 考 文 献

1 刘胜得,郑东,王育民. 域 GF(2n)上安全椭圆曲线及其基点的选取. 电子科学学刊,2000,22(5)

2 张方国,王常杰,王育民. 基于椭圆曲线的数字签名与盲签名. 通信学报,2001,22(8):22~27

3 张龙军,邹涛,沈钧毅. 一种基于椭圆曲线密码体制的盲数字签名方案. 计算机应用,2001,21(3):17~19

4 Chamenisch J L,et al. Blind signature based on the discrete logarithm problem. Rump Session of Eurocrpt'94,1995

5 Harn C,Keisler T. New scheme for digit multisignature. Electro. Lett.,1989,25(15):1002~1003

6 Hardjoiro T,Zheng Y A. Pratical digital multisignature scheme based on discrete logarithm. Advance Cryptology-AUSCRPTO'92,1992

(上接第40页)

统,VPN 路由信息不需要渗透到底层网络的路由系统中。

(8)在路由设计中引入故障隔离方法。

(9)尽可能减少路由处理负担。

(10)定义易管理的路由策略。

(11)可能的话,采用其他系统辅助路由处理。

(12)有条件的话,在 MPLS 体系结构上构建 VPN。

结束语 本文对 VPN 的可扩展性进行了研究,总结了在构建大型 VPN 时应遵循的一些基本原则,但由于 VPN 是一种综合性很强的新技术,而且构建 VPN 的技术和支持 VPN 的设备都还不成熟,因此,对 VPN 的可扩展性还需进行进一步的研究,VPN 的可扩展性仍是 VPN 发展中一项重要的研究内容。

参 考 文 献

1 RFC 2764. A Framework for IP Based Virtual Private Networks

2 RFC 2791. Scalable Routing Design Principles

3 RFC 2547. BGP/MPLS VPNs

4 RFC 3031. Multiprotocol Label Switching Architecture

5 RFC 2796. BGP Route Reflection - An Alternative to Full Mesh IBGP

6 RFC 2917. A Core MPLS IP VPN Architecture