802.1x在分布式防火墙中的应用

周 晓,王芙蓉,郭 毅
(华中科技大学 电子与信息工程系,湖北 武汉 430074)

摘 要:随着企业认识到网络安全的重要性,他们希望进入企业内网的是合法的用户和安全的主机。802.1x只能对用户进行认证,分布式防火墙只能检测主机是否安全。文中从分析802.1x认证原理和过程入手,提出802.1x在分布式防火墙中的应用方案,使得经过授权的用户只有使用符合企业安全定义的主机才能进入内网,更深层次地保证了网络的安全性。

关键词:802.1x;分布式防火墙;EAP包;主机完整性;RADIUS
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2006)12-0244-03

Application of 802.1x in Distributed Firewall System

ZHOU Xiao, WANG Fu-rong, GUO Yi
(Electronic & Info. Eng. Dept., Huazhong Univ. of Sci. & Tech., Wuhan 430074, China)

Abstract: As the enterprises become aware of the importance of security issue in their network, they seek a way to guarantee that all the users and hosts accessing the Intranet are legal and safe. 802.1x only authenticates the users, and distributed firewall system only checks the hosts. Based on the analysis of 802.1x's authentication theory and process, propose an application solution to apply the 802.1x in the distributed firewall system, making that only the authenticated users can access the Intranet via the legal hosts defined by enterprise, which secures the network in a higher level.

Key words: 802.1x; distributed firewall; EAP packet; host integrity; RADIUS

0 引 言

IEEE802.1委员会提出的802.1x协议起源于802.11协议,其实现基于以太网交换机,可以对用户进行认证、授权,从而为运营商提供了一种更实用、更安全的用户管理方式。它的认证计费方式主要是通过认证前后打开/关闭用户接入端口实现对用户接入的控制,可以实现在LAN设备的物理接入级对接入设备进行认证和控制。802.1x认证具有简洁高效、容易实现、安全可靠等特点,并可以通过设备实现Mac、端口、账户和密码等绑定技术,确保网络的安全。

分布式防火墙,英文名为"Distributed Firewall",是在目前传统的边界式防火墙基础上开发的,但目前主要是以软件形式出现的,近年来日益成为网络安全的热点话题。分布式防火墙的理念是"集中式管理、分布式防护",基于C/S模式 能真正克服高速网络带来的检测困难的问题。它布署在主机,同时提供入侵检测和应用层防护。入侵检测引擎安装在主机上,单机上的网络流量有限,因此其发现入侵的及时性与准确性都较高。

随着企业对网络安全的重视与日俱增,网络安全产品也必须不断自我完善。据统计,80%的攻击和越权访问来自于内部,因此企业希望进入内网的主机都是安全可信的。802.1x虽然能够对用户进行认证、授权,却不能确保用户所使用的主机是否"安全";分布式防火墙可以检测出主机是否"安全",却不知道使用主机的用户是否合法。如果能将802.1x和分布式防火墙有机地整合,就能保证只有得到授权的用户在一台符合企业安全定义的主机上访问内网,从而更深层次地保证了网络的安全性[1]。

文中将论述802.1x协议的原理,并探讨它在分布式防火墙中的应用和解决方案。

1 802.1x协议

1.1 802.1x认证的体系结构

802.1x协议的体系结构包括3个重要部分[2]:客户端(Supplicant System)、认证系统(Authenticator System)、认证服务器(Authentication Server System)。

1)客户端是需要接入LAN,及享受switch提供服务的设备(如PC机)。客户系统安装一个客户端软件,用户通过启动客户端软件发起802.1x协议的认证过程。为支持基于端口的接入控制,客户端系统须支持EAPOL(EAP Over LAN)协议。

2)认证系统是根据客户的认证状态控制物理接入的设备,通常为交换机。交换机在客户端和认证服务器间充当代理角色(Proxy)。交换机与客户端之间通过EAPOL

收稿日期:2006-03-13
作者简介:周 晓(1982-),男,湖南长沙人,硕士研究生,主要从事网络安全方面的研究;王芙蓉,教授,主要从事移动通信以及网络安全的研究。

协议进行通讯,交换机与认证服务器间通过 EAPORADIUS 或 EAP 承载在其他高层协议上,以便穿越复杂的网络到达认证服务器;交换机要求客户端提供 Identity,接收到后将 EAP 报文承载在 RADIUS 格式的报文中(802.1x 协议在 Switch 内终结并转换成标准的 RADIUS 协议报文),再发送到认证服务器,返回等同。交换机有 2 个逻辑端口:受控端口和不受控端口,对应于不同用户的端口。不受控端口始终处于双向连通状态,主要用来传递 EAPOL 协议帧,保证客户端始终可以发出或接受认证;受控端口只有在认证通过之后才打开,用于传递网络资源和服务。如果用户未通过认证,受控端口处于未认证状态,则用户无法访问认证系统提供的服务。交换机根据认证结果控制端口是否可用。

3)认证服务器对客户进行实际认证,通常为 RADIUS 服务器,该服务器可以存储有关用户的信息。例如,用户的账号、密码以及用户所属的 VLAN,CAR 参数、优先级、用户的访问控制列表等。认证服务器核实客户的 Identity,通知交换机是否允许客户端访问局域网和交换机提供的服务。认证服务器接受认证系统传递过来的认证需求,认证完成后将认证结果下发给认证系统完成对端口的管理。

1.2 EAP 的包结构

EAP(Extensible Authentication Protocol)作为一种认证消息承载机制可以允许认证者和请求者之间采用灵活的方案进行认证,并且对将来出现的更先进、合理的认证技术具有很好的兼容性[3]。EAP 的这些特性主要通过扩展 EAP 中厂家定义的"EAP 类型"域实现,EAP 的包结构定义于 IETF 提交的 RFC3748 中,具体格式如下:

0-1-2-3-4-5-6-7-8-9-0-1-2-3-4-5-6-7-8-9-0-1-2-3-4-5-6-7-8-9-0-1

Code	Identifier	Length
Data…		

EAP 包分 4 个部分:

(1)Code: 1 个字节,表示了 EAP 数据包的类型,Code 的值指定如下:1 为 Request;2 为 Response;3 为 Success;4 为 Failure。

(2) Identifier: 1 个字节,辅助进行 Request 和 Response 的匹配。

(3)Length: 2 个字节,表示 EAP 数据包的长度。

(4)Data: 0 或多个子节,其格式由 Code 的值来决定。

EAP 是一个可扩展的认证协议,可以通过定义"EAP 类型"域实现扩展,也可以在 Data 域中添加需要的信息实现扩展,后者在技术上实现起来比较简单,只要在 EAP 包交付 RADIUS 服务器之前将添加的信息剥离出去便不会影响整个认证流程。

1.3 802.1x 的认证过程

用户接入网络时,交换机端口状态一般为非授权(Unauthorized),只有在启动 802.1x,输入合法的用户名和正确的密码,并通过验证后,端口状态才会改为授权(Authorized),此时允许客户端通过端口进行正常通讯[4]。具体认证流程如图 1 所示。

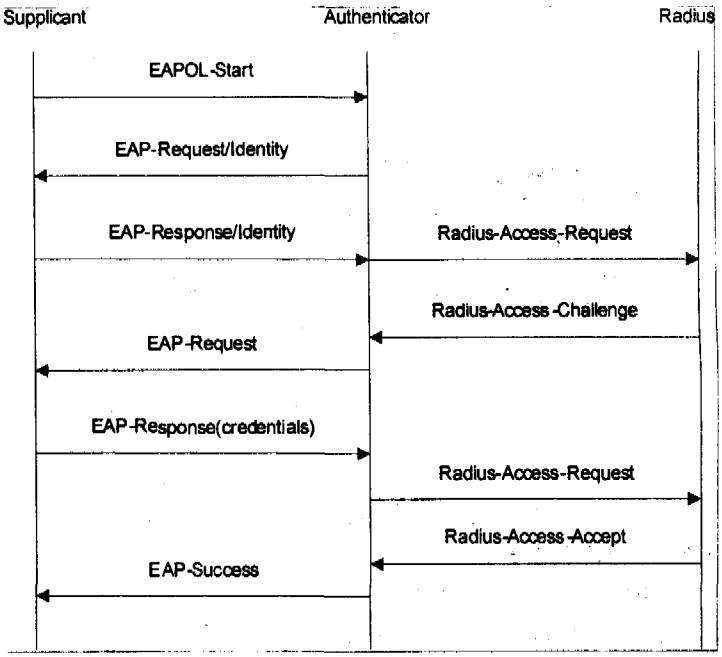

图 1　802.1x 认证过程

若认证最后一步为 EAP－Success,即认证成功;若为 EAP－Failure,则认证失败。

2 802.1x 在分布式防火墙中的应用

2.1 总体设计方案

802.1x 在分布式防火墙应用后的系统图如图 2 所示。装有分布式防火墙客户端的主机从中央策略服务器取得企业定义的安全策略,然后应用于主机。其中一个很重要的策略就是主机完整性策略(Host Integrity,以下简称 HI),它的作用是检查主机的安全状况是否完整,是否装有杀毒软件,病毒库是否更新等等,这些都可以由企业根据自身要求来定义。客户端取得策略之后就会对主机完整性作检测,得出 HI 通过或者失败的结论。值得注意的是,由于分布式防火墙自身的特点,无论交换机的端口状态如何,客户端都能顺利地从中央策略服务器拿到最新的安全策略[5]。

由于 EAP 是可扩展的协议,可以将分布式防火墙的 HI 信息添加到 EAP 包内,然后在交换机和 RADIUS 服务器之间加入一个中转服务器,中转服务器把添加在 RADIUS 包中的 HI 信息提取出来,然后把 RADIUS 包转发给 RADIUS 服务器。中转服务器的另一个作用是收到 RADIUS 服务器的 EAP Authentication Result 之后,结合 HI 的结果,给出交换机打开/关闭端口的指令。关键是如何在交换机和 RADIUS 服务器之间加入中转服务器,其实只需要在交换机的设置中将 RADIUS 服务器的 IP 设置为中转服务器的 IP,而在 RADIUS 服务器的设置中将

交换机的 IP 设置为中转服务器的 IP,这样交换机把中转服务器当作 RADIUS 服务器,而 RADIUS 服务器把中转服务器当成了交换机。

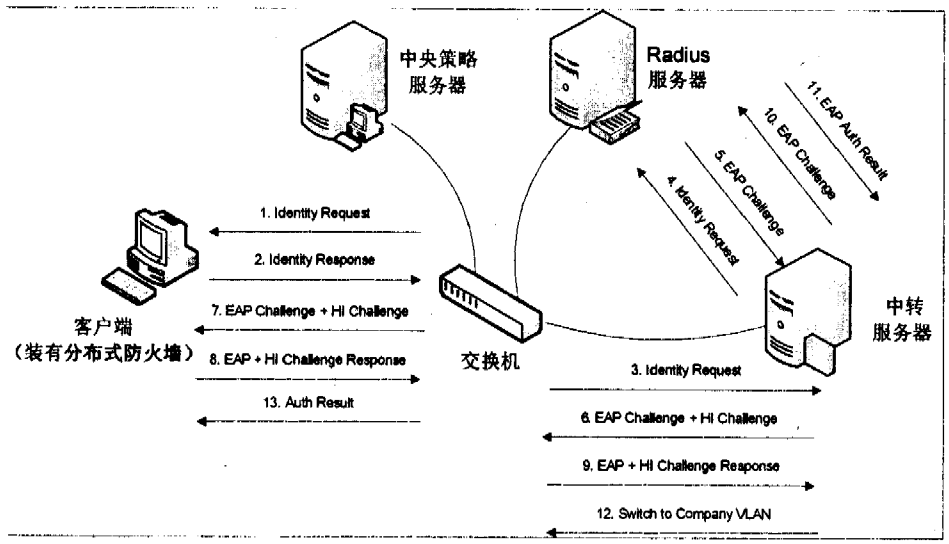

图 2 改进后的 802.1x 系统图和认证过程

2.2 新的认证过程

如图 2 所示,认证过程为:

1)装有分布式防火墙客户端的主机接入交换机,交换机探测到有设备接入,向该设备发送 EAP - Request/Identity 包,发起 802.1x 认证。

2)用户在 802.1x 客户端上输入用户名和密码,发送 EAP - Response 包作为响应。

3)交换机构造出一个 RADIUS 包,把 EAP 包作为 RADIUS 包的一个属性,发给它所认为的"RADIUS 服务器",中转服务器。

4)中转服务器不做任何改动,将这个包转发给 RADIUS 服务器。

5)RADIUS 服务器产生一个 EAP - Challenge,发给中转服务器,其类型可以为 MD5 - Challenge,EAP - TLS,PEAP 等。

6)中转服务器收到 EAP - Challenge 后,在这个包中加入 HI - Challenge,然后发给交换机。

7)交换机把 EAP 包从 RADIUS 包中取出来,重新构造一个 802.1x Challenge Request,发给待认证的主机。

8)802.1x 客户端和分布式防火墙客户端都收到这个包,802.1x 客户端发出 EAP - Challenge - Response,此时,防火墙客户端截取这个响应包,将 HI 检测的结果添加进去,然后将包发给交换机

9)交换机收到这个 802.1x 包,重新构造一个 RADIUS 包然后发给中转服务器。

10)中转服务器收到 RADIUS 包后,将 HI 检测结果从包中提取出来,然后将不含 HI 检测结果的包转发给 RADIUS 服务器。

11)RADIUS 将 EAP 认证结果包发给中转服务器。

12)中转服务器收到包后,结合 HI 检测的结果,得出打开/关闭交换机端口的结果,然后将结果发给交换机。通常只有在 EAP 认证成功并且 HI 检测通过的情况下才打开端口,其他情况下都关闭端口。

13)交换机将认证结果发给待认证的主机,交换过程完毕。

从认证过程可以看出,由于中转服务器的存在,可以做到既不影响正常的 802.1x 认证,又能实现对主机的完整性的检测,从而满足企业对于只有合法用户使用符合企业安全定义的主机才能进入内网的要求。

3 结束语

分析了 802.1x 的认证原理和认证过程,从中得出了 802.1x 认证和分布式防火墙检测结合的可能性,并提出了 802.1x 在分布式防火墙中应用的解决方案,满足了企业对于网络安全的新要求,真正做到了"人无我有,人有我优"。

提出的解决方案可以有效地阻止非法用户和不安全的主机进入内网,也保证了企业内部有线局域网的安全。但是 EAP 信息包的处理会对网络性能(吞吐量)造成一些负面影响,应进一步研究提高其性能的方法。只要今天为网络安全而工作,明天就能工作在安全网络中。

参考文献:

[1] 王英红.用分布式防火墙堵住内部网的漏洞[J].计算机安全,2002(23):13-15.

[2] IEEE. IEEE standard for local and metropolitan area networks——Port-Based Network Access Control[S]. USA:[s. n.],2001.

[3] IEEE. RFC3748 Extensible Authentication Protocol (EAP) [EB/OL]. 2004-05. http://www.rfc-archive.org/getrfc.php? rfc=3748.

[4] 朱海龙,张国清.基于 802.1x 的以太网接入技术[J].计算机工程,2003(9):10-11.

[5] Ioannidis S, Keromytis A D, Bellovin S M, et al. Implementing a Distributed Firewall[C]// In ACM 2000. USA:[s. n.],2002.