巧配PIX思科防火墙加固企业网络 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/250/2021_2022__E5_B7_A7_E9_85_8DPIX_E6_c101_250965.htm PIX（Private Internet Exchange）防火墙是Cisco 产品系列中称得上佼佼者的防火墙产品。PIX防火墙可以部署到各种各样的设计方案中。简单的情况如下，PIX防火墙可能只有两个接口，一个接口连接至受保护的内部网络（内部接口），而另一个接口则连接到公共网络（外部接口），一般来说就是指因特网。这里所谓的内部和外部具有特别的意义，且各个接口在PIX 防火墙配置中分别被命名为Inside接口（内部）和Outside接口（外部）。为了让公司能够利用与因特网的连接，通常某些服务器必须对于外部世界是可访问的，这些可访问的服务器包括DNS、SMTP以及企业能够拥有的任何公用Web服务器。DNS服务器必须是可访问的，这样才能将主机名字转换成可用于数据报寻址的IP地址。虽然这些服务器可以放在防火墙之后的内部网络中，但是强烈建议不要这样做。因为这些主机中的任意一台受到侵害后，都会导致入侵者能够方便的访问到内部网络。而如果这些服务器放置在DMZ中，则PIX防火墙能够允许内部用户不加限制的访问这些主机，而同时限制外部用户来访问这些主机。 从市场所占份额来说，状态数据报防火墙是主导类型的防火墙产品。大多数的市场都显示，PIX防火墙或Chechpoint 软件公司的Firewall经常占据市场中的第一位。在PIX防火墙的具体配置中共有58个PIX独有特性，这些特性中有些功能非常明显，而有些却略显隐蔽；有些特性是默认启动的，而有些则需要手动进行配置。下面我们就来看下

一些在企业组网中需要特别“ 关注 ”特性的配置方法，以便充分利用PIX防火墙，为企业网络提高安全系数。 手动配置TCP Intercept 思科从IOS 11.2版本中首次在路由器产品中引用了TCP Intercept（TCP截获）特性，在PIX5.2以上版本中也引入了相同的特性，这个功能特性虽然是默认启用的，但是仍需要一些手动设置。 该特性能够为隐藏在防火墙后的主机设备提供保护，抵御成为“ SYN泛洪 ”的特定类型网络攻击。使用SYN泛洪，攻击者通过好像发自不存在或不可达主机的连接请求，有效的使受害系统负荷过重，从而达到拒绝向目标主机提供服务的目的。SYN防洪巧妙的利用了操作系统为每条新的TCP连接请求分配内存和其他资源的原理。即使主机和服务器能够支持大量的连接，它们所能处理的未完成连接的数目仍然是有限的。 由于TCP是双向和全双工的，所以它在两个方向上都要建立连接。为了建立从服务器到客户端的连接，服务器设置SYN位并包括他自己的顺序号以便请求建立从服务器到客户端的连接，服务器设置SYN位置承载对来自客户端的初始连接请求的确认（ACK位）的分段重并发送给客户端。此后，服务器等待第3步：从客户端发来的对服务器到客户端的连接请求的确认。这个过程通常被成为TCP的“ 3次握手 ”。 如果应答者服务器没有在特定的TCP时间间隔内接收到应答，那么服务器会重传设置有SYN和ACK位的分段。根据具体的TCP实现，重传的次数一般是4次，重传的时间间隔开始是1秒，然后一次加倍。如果服务持续的接受连接请求，那么资源可能很快就会被这些半开放的请求耗尽，这样就不能再接受其他传入请求，从而拒绝了那项服务。 TCP Intercept通过启用此特性实现保护的主机设备

截获连接，以及对连接请求进行应答来解决这个问题。它代表客户端建立了从PIX到受保护的主机的第二条连接。如果客户端正常的完成连接，那么PIX防火墙透明地将这两条连接结合在一起，最后的结果是建立了一条在客户端和服务器之间的直接连接。 PIX防火墙使用了更短的超时时间间隔，而且如果在这个时间间隔内连接没有完成，那么PIX就会放弃与客户端的未完成连接，并且向受保护的服务器发送 RST位，结束PIX到服务器的连接，从而释放掉服务器资源。除了更短的超时之外，TCP Intercept还加入了可配置的阈值。阈值会对连接总数以及最近1分钟内的连接速率进行监控。如果这两个指标中任何一个超过了阈值，TCP Intercept都会从最久的连接开始断掉半开放的连接，知道连接的数目或速率降到阈值以下。 在PIX防火墙上，半开放连接称作初期连接。阈值可以通过static 命令的可选参数进行设置。阈值默认值为0，这样就有效的禁用了TCP Intercept.而若将这些初期连接参数设置为任何非零数值，就可以启用TCP Intercept.它有效的替代了称作Flood Defender的旧PIX特性。这个旧特性只允许对每个主机和服务上的初期连接总数进行限制。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com