# 防火墙总结

来源：网络 作者：心如止水 更新时间：2024-09-24

*第一篇：防火墙总结大石头中心校构筑校园消防安全“防火墙”工作总结学校消防安全工作是学校综合治理的重要内容,关系到学校财产安全和教师员工的生命安全。对于这项工作,我们从来不敢有丝毫懈怠与麻痹大意。为了深入贯彻实施《中华人民共和国消防法》，切...*

**第一篇：防火墙总结**

大石头中心校

构筑校园消防安全“防火墙”工作总结

学校消防安全工作是学校综合治理的重要内容,关系到学校财产安全和教师员工的生命安全。对于这项工作,我们从来不敢有丝毫懈怠与麻痹大意。为了深入贯彻实施《中华人民共和国消防法》，切实加强火灾防控工作，创新校园消防安全管理模式，提升学校消防安全管理水平，提高我校师生消防安全意识和自救自护能力，保证全校师生的人身、财产安全，根据市政府统一部署和《敦化市构筑社会消防安全“防火墙”工程实施方案》，根据市教育局的要求，我校全面深入制定计划，在实际工作中能坚持做到不断总结经验教训,不断改进和完善工作方法,提高安全防范能力,将事故隐患减少到最低指数,最大可能的提供安全保障,确保学校发展不受影响。以下是构筑校园消防安全“防火墙”三年工作总结：

一、宣传发动，统一思想，营造创建学校消防安全工作氛围

学校在学生安全方面所采取的一系列措施，充分利用学校的校园网、宣传橱窗、黑板报、学校广播等宣传阵地进行大力宣传。对师生进行交通安全、防电、防火、预防食物中毒、预防手足口病等教育，学校建立了义务消防队，对有关人员定期培训，熟悉消防防备，掌握火警处置及启动消防设施设备的程序和方法。我校加大“防火墙”工程主题的宣传，普及消防知识，组织学生进行了消防安全演练，教给学会正确使用灭火器以及掌握逃生的方法，使每一位学生普遍掌握火警电话，知道如何报警等基本常识。另外学校加强了值班管理制度，1

值班领导和教师要提前到岗，严禁校外人员进入学校，从而保证学生的安全。

通过学习宣传，大家统一了思想，提高了认识。因此，把安全防范和教学质量作为学校一切工作中最主要的两件事来抓，做到“两手都硬”。同时重视并抓好学校消防安全工作。近几年，教学资源和教学设施还不能完全跟上变化的形势，还不能满足教学的需要。因此，校园不安全因素较以前增多，校园发生安全事故的可能性比以前大大增加。这就给学校的消防安全工作提出了更高的要求，决不能掉以轻心，麻痹大意。再者，创建平安学校是实践“三个代表”重要思想的具体体现，这对于坚持社会主义办学方向，全面贯彻党的教育方针，构建社会主义和谐社会，培养合格的社会主义事业建设者和接班人同样具有重要意义。

在教育活动中，每学期学校做到了“六个一”即：一份计划、一次国旗下讲话、一次安全知识讲座、一堂主题班会、一次图片展览、一期黑板报。同时，对创建中的典型事例和经验做法及时利用校广播加以宣传报道，积极营造创建学校消防安全工作的良好氛围。

二、健全组织，落实责任，探索创建学校消防安全工作新机制

学校领导高度重视学校消防安全工作，成立了由张校长总负责的消防安全工作领导小组。

组 长：张 波（校长）负责学校的全面安全防火工作

副组长：赵永成（德育副校长）协助校长做好学校安全防火工作、各领导办公室安全防火工作

胡学文（教学副校长）协助校长做好学校安全防火工作、各教师办公室安全防火工作

刘书昌（工会主席）具体负责学校安全防火工作

组 员：陈 赞（支部副书记）负责宿舍、卫生室、图书室、档案室、会议室安全防火工作

高永清(教导主任)负责实验室、微机室、多功能室安全防火工作

宋立刚（少先队辅导员）负责各班级安全防火工作 李志强（总务主任）负责食堂、商店、库房、村小学安全防火工作

朱 哲（保卫干事）负责警务室、值班室安全防火工作 武吉富（保卫科长）负责学校安全防火检

贯彻实施《消防法》和《吉林省消防条例》，认真落实“政府统一领导、部门依法监管、单位全面负责、公民积极参与”的消防工作原则，学校把消防安全工作具体任务落实到班级负责人，按照“谁主管，谁负责”的原则，各层次负责人分别和下属各部门责任人签订消防安全责任书。这样明确分工，责任到人，使全校创建最安全学校工作“事事有人做，人人有事做”，形成了“上下联动，齐抓共管” 的管理格局。学校消防安全工作领导小组具体统筹、组织、协调学校消防安全工作的日常督查、记载等工作。做到工作有计划、有布置、有检查。把此项工作落到实处，推进学校消防安全管理创新，前移火灾预防关口，提升学校火灾防控水平

三、完善制度，奖惩结合，落实创建各项措施

1、落实消防安全责任制：制定各岗位消防安全职责，学校逐级与消防安全责任人之间签订消防安全责任书。

2、建立、完善和落实消防安全规章制度：学校建立了《消防安 3

全宣传教育制度》《防火巡查、检查制度》《安全疏散设施管理制度》《消防器材、设施维护保养制度》、《灭火和应急疏散预案演练制度》。按照“安全第一，预防为主”的原则，要求各责任部门、责任人对安全工作做到“每天必查，有查必记，有患必除”，保证安全工作一项不漏，一个盲点不留，一个隐患不存。

3、坚持落实学校消防安全工作的考核机制。

4、完善消防基础设施：按国家规范配置灭火器，电器产品的安装、使用和线路敷设符合国家规范，无私拉乱接电气线路，学生宿舍内无违章用电的行为，疏散通道畅通，学生宿舍外窗无影响安全疏散和应急救援的栅栏，图书室、学校宿舍置火灾应急照明。

5、加强防火巡查、检查，及时消防火灾隐患：学校每月组织开展一次防火检查。防火巡查对查出的火灾隐患要及时整改。

6、制定应急疏散预案，适时组织开展演练：学校每年组织开展1-2次应急疏散预案演练。

四、以人为本，“三防”齐抓，构建创建工作网络、加强消防消安全宣传教育工作，强化“四个能力”建设。

1、将消防安全教育纳入学校的日常教学内容，每个学期每个班级都安排2节消防安全知识课。

2、每个学期组织学生接受一次消防安全教育。

3、在校园内或学生宿舍都有永久性消防安全宣传标语，在校园内开辟1个消防安全教育宣传栏。

4、学校组织开展了“消防安全宣传教育月”活动。向学生传授日常防火、火场逃生自救等消防常识。

五、输导结合，形式多样，重视法制宣教工作

采取多种形式，开展安全教育。学校利用升旗、班会、健康教育课对学生进行安全意识教育和自救自护的常识教育。组织师生开展消防疏散演练活动，教会学生火灾逃生自救的方法。

学校消防安全工作是学校工作的重要组成部分。做好这项工作是维护稳定大局的需要，是学校生存、发展的需要。我校消防安全工作，取得了一些成绩，但与上级领导的要求相比，与日益变化的客观形势要求相比还存在一定的差距。三年“防火墙”工程虽已结束，但我们绝不会松懈、放松警惕，我们仍将一如既往，加大工作力度，促使我校消防安全学校工作再上新的台阶。

2024年10月28日

**第二篇：防火墙**

防火墙技术： 包过滤：

电路级网关、应用网关、代理服务器、状态检测、自适应代理型防火墙

电路级网关用来监控受信任的客户或服务器与不受信任的主机间的TCP握手信息,这样来决定该会话是否合法,电路级网关是在OSI模型中会话层上来过滤数据包,这样比包过滤防火墙要高两层。另外，电路级网关还提供一个重要的安全功能：网络地址转移(NAT)将所有公司内部的IP地址映射到一个“安全”的IP地址，这个地址是由防火墙使用的。有两种方法来实现这种类型的网关，一种是由一台主机充当筛选路由器而另一台充当应用级防火墙。另一种是在第一个防火墙主机和第二个之间建立安全的连接。这种结构的好处是当一次攻击发生时能提供容错功能。

防火墙一般可以分为以下几种：包过滤型防火墙、电路级网关型防火墙、应用网关型防火墙、代理服务型防火墙、状态检测型防火墙、自适应代理型防火墙。下面分析各种防火墙的优缺点。

包过滤型防火墙 它是在网络层对数据包进行分析、选择，选择的依据是系统内设置的过滤逻辑，也可称之为访问控制表。通过检查数据流中每一个数据包的源地址、目的地址、所用端口、协议状态等因素，或它们的组合来确定是否允许该数据包通过。它的优点是：逻辑简单，成本低，易于安装和使用，网络性能和透明性好，通常安装在路由器路由器

路由器是用来连接不同网络或网段的装置，它能够根据信道的情况自动选择并设定路由，以最佳路径，按前后顺序发送信号。路由器构成了 Internet的骨架。路由器的处理速度与可靠性直接影响着网络互连的速度与质量。[全文] 上。缺点是：很难准确地设置包过滤器，缺乏用户级的授权；包过滤判别的条件位于数据包的头部，由于ＩＰＶ４的不安全性，很可能被假冒或窃取；是基于网络层的安全技术，不能检测通过高层协议而实施的攻击。

电路级网关型防火墙 它起着一定的代理服务作用，监视两主机建立连接时的握手信息，判断该会话请求是否合法。一旦会话连接有效后，该网关仅复制、传递数据。它在ＩＰ层代理各种高层会话，具有隐藏内部网络信息的能力，且透明性高。但由于其对会话建立后所传输的具体内容不再作进一步地分析，因此安全性低。

应用网关型防火墙 它是在应用层上实现协议过滤和转发功能，针对特别的网络应用协议制定数据过滤逻辑。应用网关通常安装在专用工作站工作站

工作站是一种以个人计算机和分布式网络计算为基础，主要面向专业应用领域，具备强大的数据运算与图形、图像处理能力，为满足工程设计、动画制作、科学研究、软件开发、金融管理、信息服务、模拟仿真等专业领域而设计开发的高性能计算机。

系统上。由于它工作于应用层，因此具有高层应用数据或协议的理解能力，可以动态地修改过滤逻辑，提供记录、统计信息。它和包过滤型防火墙有一个共同特点，就是它们仅依靠特定的逻辑来判断是否允许数据包通过，一旦符合条件，则防火墙内外的计算机系统建立直接联系，防火墙外部网络能直接了解内部网络结构和运行状态，这大大增加了实施非法访问攻击的机会。

代理服务型防火墙 代理服务器服务器

服务器是指在网络环境下运行相应的应用软件，为网上用户提供共享信息资源和各种服务的一种高性能计算机，英文名称叫做Server。[全文] 接收客户请求后，会检查并验证其合法性，如合法，它将作为一台客户机向真正的服务器服务器

服务器是指在网络环境下运行相应的应用软件，为网上用户提供共享信息资源和各种服务的一种高性能计算机，英文名称叫做Server。发出请求并取回所需信息，最后再转发给客户。它将内部系统与外界完全隔离开来，从外面只看到代理服务器，而看不到任何内部资源，而且代理服务器只允许被代理的服务通过。代理服务安全性高，还可以过滤协议，通常认为它是最安全的防火墙技术。其不足主要是不能完全透明地支持各种服务、应用，它将消耗大量的ＣＰＵ资源，导致低性能。

状态检测型防火墙 它将动态记录、维护各个连接的协议状态，并在网络层对通信的各个层次进行分析、检测，以决定是否允许通过防火墙。因此它兼备了较高的效率和安全性，可以支持多种网络协议和应用，且可以方便地扩展实现对各种非标准服务的支持。

自适应代理型防火墙 它可以根据用户定义的安全策略，动态适应传送中的分组流量。如果安全要求较高，则最初的安全检查仍在应用层完成。而一旦代理明确了会话的所有细节，那么其后的数据包就可以直接经过速度快得多的网络层。因而它兼备了代理技术的安全性和状态检测技术的高效率。

防火墙技术虽然出现了许多，但总体来讲可分为“包过滤型”和“应用代理型”两大类。前者以以色列的Checkpoint防火墙和美国Cisco公司的PIX防火墙为代表，后者以美国NAI公司的Gauntlet防火墙为代表。

(1).包过滤(Packet filtering)型

包过滤型防火墙工作在OSI网络参考模型的网络层和传输层，它根据数据包头源地址，目的地址、端口号和协议类型等标志确定是否允许通过。只有满足过滤条件的数据包才被转发到相应的目的地，其余数据包则被从数据流中丢弃。

包过滤方式是一种通用、廉价和有效的安全手段。之所以通用，是因为它不是针对各个具体的网络服务采取特殊的处理方式，适用于所有网络服务；之所以廉价，是因为大多数路由器都提供数据包过滤功能，所以这类防火墙多数是由路由器集成的；之所以有效，是因为它能很大程度上满足了绝大多数企业安全要求。

在整个防火墙技术的发展过程中，包过滤技术出现了两种不同版本，称为“第一代静态包过滤”和“第二代动态包过滤”。

●第一代静态包过滤类型防火墙

这类防火墙几乎是与路由器同时产生的，它是根据定义好的过滤规则审查每个数据包，以便确定其是否与某一条包过滤规则匹配。过滤规则基于数据包的报头信息进行制订。报头信息中包括IP源地址、IP目标地址、传输协议(TCP、UDP、ICMP等等)、TCP/UDP目标端口、ICMP消息类型等。

●第二代动态包过滤类型防火墙

这类防火墙采用动态设置包过滤规则的方法，避免了静态包过滤所具有的问题。这种技术后来发展成为包状态监测(Stateful Inspection)技术。采用这种技术的防火墙对通过其建立的每一个连接都进行跟踪，并且根据需要可动态地在过滤规则中增加或更新条目。

包过滤方式的优点是不用改动客户机和主机上的应用程序，因为它工作在网络层和传输层，与应用层无关。但其弱点也是明显的：过滤判别的依据只是网络层和传输层的有限信息，因而各种安全要求不可能充分满足；在许多过滤器中，过滤规则的数目是有限制的，且随着规则数目的增加，性能会受到很大地影响；由于缺少上下文关联信息，不能有效地过滤如UDP、RPC（远程过程调用）一类的协议；另外，大多数过滤器中缺少审计和报警机制，它只能依据包头信息，而不能对用户身份进行验证，很容易受到“地址欺骗型”攻击。对安全管理人员素质要求高，建立安全规则时，必须对协议本身及其在不同应用程序中的作用有较深入的理解。因此，过滤器通常是和应用网关配合使用，共同组成防火墙系统。

(2).应用代理(Application Proxy)型

应用代理型防火墙是工作在OSI的最高层，即应用层。其特点是完全“阻隔”了网络通信流，通过对每种应用服务编制专门的代理程序，实现监视和控制应用层通信流的作用。其典型网络结构如图所示。

在代理型防火墙技术的发展过程中，它也经历了两个不同的版本，即：第一代应用网关型代理防火和第二代自适应代理防火墙。

第一代应用网关(Application Gateway)型防火墙

这类防火墙是通过一种代理(Proxy)技术参与到一个TCP连接的全过程。从内部发出的数据包经过这样的防火墙处理后，就好像是源于防火墙外部网卡一样，从而可以达到隐藏内部网结构的作用。这种类型的防火墙被网络安全专家和媒体公认为是最安全的防火墙。它的核心技术就是代理服务器技术。

第二代自适应代理(Adaptive proxy)型防火墙

它是近几年才得到广泛应用的一种新防火墙类型。它可以结合代理类型防火墙的安全性和包过滤防火墙的高速度等优点，在毫不损失安全性的基础之上将代理型防火墙的性能提高10倍以上。组成这种类型防火墙的基本要素有两个：自适应代理服务器(Adaptive Proxy Server)与动态包过滤器(Dynamic Packet filter)。

在“自适应代理服务器”与“动态包过滤器”之间存在一个控制通道。在对防火墙进行配置时，用户仅仅将所需要的服务类型、安全级别等信息通过相应Proxy的管理界面进行设置就可以了。然后，自适应代理就可以根据用户的配置信息，决定是使用代理服务从应用层代理请求还是从网络层转发包。如果是后者，它将动态地通知包过滤器增减过滤规则，满足用户对速度和安全性的双重要求。

代理类型防火墙的最突出的优点就是安全。由于它工作于最高层，所以它可以对网络中任何一层数据通信进行筛选保护，而不是像包过滤那样，只是对网络层的数据进行过滤。

另外代理型防火墙采取是一种代理机制，它可以为每一种应用服务建立一个专门的代理，所以内外部网络之间的通信不是直接的，而都需先经过代理服务器审核，通过后再由代理服务器代为连接，根本没有给内、外部网络计算机任何直接会话的机会，从而避免了入侵者使用数据驱动类型的攻击方式入侵内部网。

代理防火墙的最大缺点就是速度相对比较慢，当用户对内外部网络网关的吞吐量要求比较高时，代理防火墙就会成为内外部网络之间的瓶颈。那因为防火墙需要为不同的网络服务建立专门的代理服务，在自己的代理程序为内、外部网络用户建立连接时需要时间，所以给系统性能带来了一些负面影响，但通常不会很明显。

**第三篇：防火墙知识点**

第一章

1.防火墙定义：防火墙是位于两个（或多个）网络之间，实施访问控制策略的一个或一组组件的集合。（或者防火墙是设置在本地计算机或内联网络与外联网络之间，保护本地网络或内联网络免遭来自外部网络的威胁和入侵的一道屏障。）

2.防火墙位置：物理位置，安装在内联网络与外联网络的交界点上；对于个人防火墙来说，是指安装在单台主机硬盘上的软件系统。

逻辑位置：防火墙与网络协议相对应的逻辑层次关系。3.防火墙理论特性：根据信息安全理论对其提出的要求而设置的安全功能，是各种防火墙的共性作用。

防火墙从理论上讲是分离器、限制器和分析器，即防火墙要实现四类控制功能： 方向控制：防火墙能够控制特定的服务请求通过它的方向； 服务控制：防火墙可以控制用户可以访问的网络服务类型； 行为控制：防火墙能够控制使用特定服务的方式； 用户控制：防火墙能够控制能够进行网络访问的用户。4.防火墙规则（1）过滤规则

（2）设计原则：a.拒绝访问一切未予特许的服务：这个原则也被称为限制性原则，在该规则下，防火墙阻断所有的数据流，只允许符合开放规则的数据流进出。

b.允许访问一切未被特许拒绝的服务：该规则也被称为连通性原则，在该规则下，防火墙只禁止符合屏蔽规则的数据流，而允许转发其他所有数据流。5.防火墙分类

按采用的主要技术划分：包过滤型防火墙、代理型防火墙 按具体实现划分：（1）多重宿主主机：安放在内联网络和外联网络接口上的一台堡垒主机，它提供最少两个网络接口，一个与内联网络连接，另一个与外联网络连接。

（2）筛选路由器：用一台放置在内联网络与外联网络之间的路由器来实现。它对进出内联网络的所有信息进行分析，并按照一定的信息过滤规则对进出内联网络的信息进行限制，允许授权信息通过，拒绝非授权信息通过。

（3）屏蔽主机：由内联网络和外联网络之间的一台过滤路由器和一台堡垒主机构成。它强迫所有外部主机与堡垒主机相连接，而不让他们与内部主机直接相连。

（4）屏蔽子网：它对网络的安全保护通过两台包过滤路由器和在这两个路由器之间构筑的子网来实现。6.防火墙的优点

（1）防火墙是网络安全的屏障

（2）防火墙实现了对内网系统的访问控制（3）部署NAT机制

（4）提供整体安全解决平台（5）防止内部信息外泄（6）监控和审计网络行为

（7）防火墙系统具有集中安全性

（8）在防火墙上可以很方便的监视网络的信息流，并产生警告信息。7.防火墙的缺点（1）限制网络服务

（2）对内部用户防范不足（3）不能防范旁路连接（4）不适合进行病毒检测（5）无法防范数据驱动型攻击（6）无法防范所有威胁

（7）配置问题。防火墙管理人员在配置过滤规则时经常出错。（8）无法防范内部人员泄露机密信息（9）速度问题

（10）单失效点问题

第二章

1.TCP/IP包头 2.包过滤技术

（1）概念：又称为报文过滤技术，执行边界访问控制功能，即对网络通信数据进行过滤。（2）技术原理：（3）过滤对象：a.针对IP的过滤，查看每个IP数据包的包头，将包头数据与规则集相比较，转发规则集允许的数据包，拒绝规则集不允许的数据包。

b.针对ICMP的过滤。阻止存在泄漏用户网络敏感信息的危险的ICMP数据包进出网络；拒绝所有可能会被攻击者利用、对用户网络进行破坏的ICMP数据包。

c.针对TCP的过滤，常见的为端口过滤和对标志位的过滤。d.针对UDP的过滤，要么阻塞某个端口，要么听之任之。（4）优点：包过滤技术实现简单、快速；

包过滤技术的实现对用户是透明的；

包过滤技术的检查规则相对简单，因此操作耗时极短，执行效率非常高

（5）缺点：

包过滤技术过滤思想简单，对信息的处理能力有限；

当过滤规则增多时，对过滤规则的维护是一个非常困难得问题； 包过滤技术控制层次较低，不能实现用户级控制。

3.状态检测技术

（1）技术原理：状态检测技术根据连接的“状态”进行检查，当一个连接的初始数据报文到达执行状态检测的防火墙时，首先要检查该报文是否符合安全过滤规则的规定。如果该报文与规定相符合，则将该连接的信息记录下来并自动添加一条允许该连接通过的过滤规则，然后向目的地转发该报文。以后凡是属于该连接的数据防火墙一律予以放行，包括从内向外和从外向内的双向数据流。在通信结束、释放该连接以后，防火墙将自动删除该连接的过滤规则。动态过滤规则存储在连接状态表中，并由防火墙维护。

（2）状态：状态根据使用的协议的不同而有不同的形式，可以根据相应协议的有限状态机来定义，一般包括NEW ,ESTABLISHED ,RELATED ,CLOSED。（3）状态检测技术的优点

安全性比静态包过滤技术高；

与静态包过滤技术相比，提高了防火墙的性能。

（4）状态检测技术的缺点

主要工作在网络层和传输层，对报文的数据部分检查很少，安全性还不够高； 检查内容多，对防火墙的性能提出了更高的要求。

4.代理技术

（1）代理的执行分为以下两种情况：一种情况是代理服务器监听来自内联网络的服务请求；另一种情况是内部主机只接收代理服务器转发的信息而不接收任何外部地址主机发送的信息。

（2）代理代码：

（3）代理服务器的实现：双宿主网关的IP路由功能被严格禁止，网卡间所有需要转发的数据必须通过安装在双宿主网关上的代理服务器程序控制。由此实现内联网络的单接入点和网络隔离。

（4）代理技术优点：

代理服务提供了高速缓存；

代理服务器屏蔽了内联网络，所以阻止了一切对内联网络的探测活动； 代理服务在应用层上建立，可以更有效的对内容进行过滤；

代理服务器禁止内联网络与外联网络的直接连接，减少了内部主机直接受到攻击的危险；

代理服务可以提供各种身份认证手段，从而加强服务的安全性； 代理防火墙不易受IP地址欺骗的攻击；

代理服务位于应用层，提供了详细的日志记录，有助于进行细致的日志分析和审计； 代理防火墙的过滤规则比包过滤防火墙的过滤规则更简单。（5）代理技术的缺点

代理服务程序很多都是专用的，不能够很好的适应网络服务和协议的发展； 在访问数据流量较大的情况下，代理技术会增加访问的延时，影响系统的性能； 应用层网关需要用户改变自己的行为模式，不能够实现用户的透明访问； 应用层代理还不能够支持所有的协议；

代理系统对操作系统有明显的依赖性，必须基于某个特定的系统及其协议； 相对于包过滤技术来说，代理技术执行的速度较慢。

第三章

1.过滤路由器的实现：过滤路由器对经过它的所有数据流进行分析，按照预定义的过滤规则，也就是网络安全策略的具体实现，对进出内联网络的信息进行限制。允许经过授权的信息通过，拒绝非授权的信息通过。2.过滤路由器优缺点

（1）过滤路由器优点：快速、性能高、透明、容易实现

过滤路由器是从普通路由器发展而来，继承了普通路由器转发速率快的优点； 购买过滤路由器比单独购买独立的防火墙产品具有更大的成本优势； 过滤路由器对用户来说是完全透明的； 过滤路由器的实现极其简单。（2）缺点：

过滤路由器配置复杂，维护困难；

过滤路由器只针对数据包本身进行检测，只能检测出部分攻击行为； 过滤路由器无法防范数据驱动式攻击；

过滤路由器只针对到达它的数据包的各个字段进行检测，无法确定数据包发出者的真实性；

随着过滤规则的增加，路由器的吞吐量会下降；

过滤路由器无法对数据流进行全面的控制，不能理解特定服务的上下文和数据。2.过滤规则（1）表3—1给图填数据

（2）由规则生成策略（协议具有双向性，一写就写俩）（3）逐条匹配深入原则（填空）3.屏蔽冲突：当排在过滤规则表后面的一条规则能匹配的所有数据包也能被排在过滤规则表前面的一条过滤规则匹配的时候，后面的这条过滤规则将永远无法得以执行，这种冲突称为屏蔽冲突。4.堡垒主机

（1）定义：堡垒主机是一种网络完全机制，也是安全访问控制实施的一种基础组件。通常情况下堡垒主机由一台计算机担当，并拥有两块或者多块网卡分别连接各内联网络和外联网络。

（2）作用：隔离内联网络和外联网络，为内联网络设立一个检查点，对所有进出内联网络的数据包进行过滤，集中解决内联网络的安全问题。（3）设计原则：

a.最小服务原则：尽可能减少堡垒主机提供的服务，对于必须设置的服务，只能授予尽可能低的权限；

b.预防原则：用户必须加强与堡垒主机的联系，对堡垒主机的安全情况进行持续不断的监测，仔细分析堡垒主机的日志，及时对攻击行为作出响应。（4）类型

a.内部堡垒主机 b.外部堡垒主机 c.牺牲主机

5.多重宿主主机防火墙实现方法

采用一台堡垒主机作为连接内联网络和外联网络的通道，在这台堡垒主机中安装多块网卡，每一块网卡都连接不同的内联子网和外联网络，信息的交换通过应用层数据共享或者应用层代理服务实现，而网络层直接的信息交换是被绝对禁止的。与此同时，在堡垒主机上还要安装访问控制软件，用以实现对交换信息的过滤和控制功能。

多重宿主主机有两种经典的实现：第一种是采用应用层数据共享技术的双宿主主机防火墙，另一种是采用应用层代理服务器技术的双宿主网关防火墙。6.双宿主主机防火墙

（1）优点：作为内联网络与外联网络的唯一接口，易于实现网络安全策略；

使用堡垒主机实现，成本较低。（2）缺点：

a.用户账户的存在给入侵者提供了一种入侵途径，入侵者可以通过诸如窃听、破译等多种手段获取用户的账号和密码进而登录防火墙；

b.双宿主主机防火墙上存在用户账户数据库，当数据库的记录数量逐渐增多时，管理 员需要花费大量的精力和时间对其进行管理和维护，这项工作是非常复杂的，容易出错；

c.用户账户数据库的频繁存取将耗费大量系统资源，会降低堡垒主机本身的稳定性和可靠性，容易出现系统运行速度低下甚至崩溃等现象；

d.允许用户登录到防火墙主机上，对主机的安全性是一个很大的威胁。用户的行为是不可预知的，各种有意或者无意的破坏都将给主机带来麻烦，而且这些行为也很难进行有效的监控和记录。

（3）双宿主主机构成（填空）：双宿主主机防火墙是一台具有安全控制功能的双网卡堡垒主机，两块网卡中的一块负责连接内联网络，另一块负责连接外联网络。7.双宿主网关（1）工作原理：在防火墙主机上安装各种网络服务的代理服务器程序。当内联网络中的主机意图访问外联网络时，只需要将请求发送至双宿主网关防火墙相应的代理服务器上，通过过滤规则的检测并获得允许后，再由代理服务器程序代为转发至外联网络指定主机上。而外联网络中的主机所有对内联网络的请求都由（2）优点

a.无需管理和维护用户账户数据库

b.由于采用代理服务器技术，防火墙提供的服务具有良好的可扩展性

c.信息通过代理服务器转发，屏蔽了内联网络的主机，阻止了信息泄露现象的发生（3）缺点

a.入侵者只要攻破堡垒主机就可以直接面对内联网络，因此防火墙主机的安全配置非常复杂且重要

b.防火墙本身的性能是影响系统整体性能的瓶颈

c.单点失效，一旦防火墙主机停止运行，则内联网络的链接将全部中断 d.灵活性较差 8屏蔽主机（1）工作原理

过滤路由器的路由表是定制的，将所有外联网络对内联网络的请求都定向到堡垒主机处，而堡垒主机上运行着各种网络服务的代理服务器组件，外联网络的主机不能直接访问内联网络的主机，对内联网络的所有请求必须要由堡垒主机上的代理服务器进行转发，对于内联网络到发起的连接或由过滤路由器重新定向到堡垒主机，对于特定的主机和特定的服务，则直接访问

（2）优点：a.安全性更高

b.可扩展性高

c.屏蔽主机本身是可靠稳定的

（3）缺点：在堡垒主机和其他内联网络的主机放置在一起，他们之间没有一道安全隔离屏障，如果堡垒主机被攻破，那么内联网络将全部曝光于攻击者的面前 屏蔽子网

（1）非军事区DMZ：又称屏蔽子网，在用户内联网络和外联网络之间构建的一个缓冲区域，目的是最大限度地减少外部入侵者对内联网络的侵害，内部部署了安全代理网关（执行安全代理功能）和各种公用的信息服务器（执行网络层包过滤）

在边界上，通过内部过滤器与内联网络相联，通过外部过滤路由器与外部网络相联。（2）优点：a.内联网络实现了与外联网络的隔离，内部结构无法探测，外联网络只能知道外部路由器和非军事区的存在，而不知道内部路由器的存在，也就无法探测到内部路由器后面的内联网络了

b.内联网络安全防护严密

c.降低了堡垒主机处理的负载量，减轻了堡垒主机的压力，增强了堡垒主机的可靠性和安全性

d.将用户网络的信息流量明确地划分成不同的等级，通过内部路由器的隔离作用，机密信息流受到严密的保护，减少了信息泄露的发生

（3）缺点

第四章 1防火墙性能指标（1）可靠性（2）可用性（3）可扩展性（4）可审计性（5）可管理性（6）成本耗费

2防火墙的评估参数（1）吞吐量（2）时延（3）丢包率（4）并发连接数

（5）工作模式：路由模式，NAT模式，透明模式（6）配置管理

（7）接口的数量和类型（8）日志和审计参数 3防火墙技术的发展趋势

（1）分布式执行和集中式管理：分布式或分层的安全策略执行，集中式管理（2）深度过滤：正常化，双向负载检测，应用层加密和解密，协议一致性（3）建立以防火墙为核心的综合安全体系

（4）防火墙本身的多功能化，变被动防御为主动防御（5）强大的审计与自动日志分析功能（6）硬件化（7）专用化

第六章 入侵检测

1入侵检测：对企图入侵，正在进行的入侵或者已经发生的入侵进行识别的过程 2入侵检测的作用：

（1）识别并阻断系统活动中存在的已知攻击行为，防止入侵行为对受保护系统造成损害

（2）识别并阻断系统用户的违法操作行为或者越权操作行为，防止用户对受保护系统有意或者无意的破坏

（3）检查受保护系统的重要组成部分及各种数据文件的完整性

（4）审计并弥补系统中存在的弱点和漏洞，其中最重要的一点是审计并纠正错误的系统配置信息

（5）记录并分析用户和系统的行为，描述这些行为变化的正常区域，进而识别异常的活动

（6）通过蜜罐等技术手段记录入侵者的信息，分析入侵者的目的和行为特征，优化系统安全策略

（7）加强组织或机构对系统和用户的监督与控制能力，提高管理水平和管理质量

3入侵检测按数据来源划分：

（1）基于主机的入侵检测：通过分析特定主机上的行为来发现入侵，判断的依据是系统内的各种数据及其相关记录 优点：能够确定攻击是否成功

不需要额外的硬件来主持

能够适合加密的环境

可监视特定的系统文件 缺点：额外产生的安全问题

不具有平台无关性，可移植性差

实时性差

依赖性强，检测效果取决于日志系统

占用主机资源，影响主机性能

如果主机数目多，维护和管理代价大

隐蔽性差，对入侵者不透明（2）基于网络的入侵检测 优点：具有平台无关性

不影响受保护主机的性能

对主机来说是透明的

检测范围广，监测主机数量大时相对成本低

实时检测和响应

可检测基于底层协议的攻击行为 缺点：很难发现应用层的攻击行为

很难处理加密传输

对于交换网络的不足

不能及时有效的分析处理大规模的数据

容易受到拒绝服务攻击

很难进行复杂攻击的检测（3）混合式的入侵检测

4入侵检测按检测方法划分：异常检测和滥用检测

（1）异常检测根据系统或者用户的非正常行为或者对于计算机资源的非正常使用检测出入侵行为的检测技术，基础是建立系统正常活动状态或用户正常行为模式的描述模型，异常检测的操作是将用户当前的行为模式或系统的当前状态与该正常模型进行比较，如果当前值超出了预设的阈值，则认为存在着攻击行为（2）滥用入侵检测通过对现有的各种手段进行分析，找到能够代表该攻击行为的特征集合，对当前数据的处理就是与这些特征集合进行匹配，如果匹配成功则说明发生了一次确定的攻击 第七章

1入侵检测的性能指标：有效性（攻击检测率，攻击误警率，可信度），可用性，安全性（抗攻击能力，数据通信机制）

2入侵检测的发展趋势：标准化的入侵检测，高速入侵检测，大规模分布式的入侵检测，多种技术的融合，实时入侵响应，入侵检测的评估，与其他安全技术的联动

VPN篇

1定义：是企业在因特网等公共网络上的延伸，指将物理上分布在不同地点的网络通过公用网络连接成逻辑上的虚拟子网，并采用认证，访问控制，保密性，数据完整性等技术，使得数据通过安全的“加密隧道”在公用网络中进行传输

2原理：在直接和公用网络连接的计算机之间建立一条专用通道，私有网络之间的通信内容经过发送端计算机或者设备打包，通过公用网络的专用通道进行传输，然后在接收端解包，还原成私有网络的通信内容，转发到私有网络中

3按应用范围划分：远程接入VPN，企业内部VPN，企业扩展VPN 4按隧道协议划分：第二层隧道协议，第三层隧道协议 5按隧道建立方式划分：自愿隧道，强制隧道 6特点：具备完善的安全保障机制，具备用户可接受的服务质量保证，总成本低

可扩展，安全性，灵活性

管理便捷

7安全机制：加密技术，认证技术，密钥管理与交换

**第四篇：状态防火墙**

防火墙技术之－－状态防火墙（ＡＳＰＦ）１

2024-08-22 19:06:52 标签：防火墙 状态 ＡＳＰＦ 技术

应用状态防火墙技术介绍

前面讲到了包过滤防火墙的一些细节东西，大家可以发现我一直强调包过滤的核心在于ＡＣＬ，ＡＣＬ起源于防火墙的需要，但是应用远远不止于防火墙。ＡＣＬ需要提前定义分类数据包，然后跟ｐａｃｋｅｔ filtering进行接口绑定然后对流经接口的数据包进行ＡＣＬ匹配，如果匹配便根据ｆｉｒｅｗａｌｌ定义的ｐｅｒｍｉｔ还是ｄｅｎｙ对数据包进行允许还是拒绝（丢弃）处理，如果不匹配ＡＣＬ那么就将数据包丢给全局防火墙默认策略处理，对于默认策略各家厂商定义不同，也可以自定义．

那么从包过滤技术的分析中大家可以看到，包过滤是静态的，静态的原因在于提前需要定义ＡＣＬ及策略，而且包过滤关注协议的ＩＰ层，也就是三层以下．这样来说她的处理就显的简单而单一．熟悉网络技术的人都知道，其实我们的业务应用更加复杂，除了复杂的协议状态机转换，许多的协议都是多通道的，这样来说这些状态及应用层信息一般来说都非静态的，会根据报文的交互进行状态机转换．所以包过滤将显的心有余而力不足．在这样的需求下基于应用状态的防火墙技术（ＡＳＰＦ）诞生了． 那么ＡＳＰＦ采用什么样的方式来处理数据包呢？首先ＡＳＰＦ所关心的对象已经发生变化，不再是ＩＰ包头，不再是单纯的五元组信息，而是关心技术ＩＰ层的连接的数据流信息，当然这个数据流信息包括如ＴＣＰ的三次握手建连接，四次握手终结连接的状态机ＦＳＭ变化，还包括应用层如ＦＴＰ协议的控制与数据通道的建立及解除等等．那么在这个过程中有这样几个问题需要注意：

１）ＡＳＰＦ关注数据流，那么如何识别一条数据流？

ＡＳＰＦ的处理一般是基于ｓｅｓｓｉｏｎ（会话）的，所有属于同一会话的所有数据包都被堪称一条流并统一对待．那么会话是一个什么的东西呢？会话一般包括如下这样信息：

协议 状态（老化时间）源ＩＰ（源端口）－－＞目的ＩＰ（目的端口）目的ＩＰ（目的端口）＜－－源ＩＰ（源端口）

如上所示一条会话是有如上七元组来标示的，如果一个数据包可以匹配会话的话就称为同一数据流．

２）如何确定一应用性连接的正确性？

所谓的状态防火墙就是对协议的状态进行动态监控，如果状态转化不符合协议定义，那么这样的报文将被ＤＲＯＰ掉．只有那些完全匹配符合协议状态机的报文将会呗正确投递到相应的模块进行处理．那么如何来确定一条应用性连接的正确性呢？答案就是状态转换表，也就是所谓的状态机（ＦＳＭ）．下面来举个例子说明： ＴＣＰ的ＦＳＭ：

ＮＯＮＥ－－－＞ＳＹＮ＿ＳＥＮＴ，receiveｄ ＴＣＰ＿ＳＹＮ ＴＣＰ＿ＳＥＮＴ－－－＞ＳＹＮ＿ＲＣＶ，receiveｄ ＴＣＰ＿ＳＹＮ＿ＡＣＫ

ＳＹＮ＿ＲＣＶ－－－＞ＥＳＴＡＢＬＩＳＨ，receiveｄ ＴＣＰ＿ＡＣＫ

ＥＳＴＡＢＬＩＳＨ－－－＞ＥＳＴＡＢＬＩＳＨ，receiveｄ ＴＣＰ＿ＡＣＫ

ＥＳＴＡＢＬＩＳＨ－－－＞ＴＩＮ＿ＷＡＩＴ，receiveｄ ＴＣＰ＿ＦＩＮ

ＦＩＮ＿ＷＡＩＴ－－－＞ＦＩＮ＿ＷＡＩＴ，receiveｄ ＴＣＰ＿ＡＣＫ

ＦＩＮ＿ＷＡＩＴ－－－＞ＦＩＮ＿ＷＡＩＴ，receiveｄ ＴＣＰ＿ＦＩＮ

ＦＩＮ＿ＷＡＩＴ－－－＞ＣＬＯＳＥＤ，receiveｄ ＴＣＰ＿ＡＣＫ 上面就详细的表述了ＴＣＰ的ＦＳＭ状态机转换及触发条件，会话会维护每种支持协议的状态机，ＡＳＰＦ会依赖会话管理模块进行状态动态监控以实现动态防火墙处理．还有一点需要注意的是，不同的系统可能对如ＵＤＰ，ＩＣＭＰ这样的无状态的协议的定义是不同的，处理上也有一些差异，在这里不再详细讲述，轻关注会话管理详细讲解． ３）如何检测应用层内容的合法性（如Ｊａｖａ ａｐｐｌｅｔｓ）？ ＡＳＰＦ还可以对应用层的报文的内容加以检测，如Ｊava ｂｌｏｃｋｉｎｇ等，对不信任站点的ｊａｖａ阻断功能，当然这方面的ＡＳＰＦ检测是有限的，对于应用层数据的合法性的检测更多的依赖ＷＥＢ过滤技术进行．Java Blocking是对通过HTTP协议传输的Java Applets程序进行阻断。当配臵了Java Blocking后，用户为试图在Web页面中获取包含Java Applets程序而发送的请求指令将会被阻断。４）如何保证传输层（应用层）数据通道的正确建立？

传输层协议检测一般指通用的ＴＣＰ／ＵＤＰ检测，与应用层数据不同，传输层协议检测主要关注传输层数据（插口地址）．对于ＡＳＰＦ要求返回ａｓｐｆ外部接口的报文要跟出ＡＳＰＦ接口报文完全匹配，也就是说五元组要完全匹配。否则返回的数据报文将被丢弃处理。

至此介绍了一些ＡＳＰＦ实现需要的一些概念，准备，那么下面将详细的介绍ＡＳＰＦ的细节．（未完待续，尽请关注防火墙技术之－－状态防火墙２）

防火墙技术之－－状态防火墙ＡＳＰＦ（２）

2024-08-22 21:07:11 标签：防火墙 状态 ＡＳＰＦ 技术

应用状态防火墙功能介绍

前面介绍了ＡＳＰＦ的基本原理，跟踪协议状态机以实现对应用层状态的动态监控，所以状态防火墙被称为动态防火墙。动态就在于状态机是动态变化的，这样的处理使得对数据的过滤更加周全，更加深入。本文想细致区分状态防火墙的功能，以期能更深入的了解状态防火墙技术。综合来说ＡＳＰＦ可以具有如下几个方面的功能：

支持应用层协议检测，包括：ＦＴＰ，ＨＴＴＰ，ＳＭＴＰ，ＲＳＴＰ，Ｈ３２３，ＳＩＰ等

      

支持通用ＴＣＰ、ＵＤＰ通道检测 支持会话状态动态管理 支持ＩＰ分片报文检测

支持端口到应用的映射（ＰＡＭ）支持Ｊａｖａ阻塞 支持会话日志与调试跟踪

下面将逐个对这些功能进行分析： １.应用层协议检测

ａ．ＳＭＴＰ（简单邮件传输协议）：ＡＳＰＦ检测基于ＴＣＰ／ＩＰ传输的ＳＭＴＰ应用，包括对ＳＭＴＰ协议状态机转换的检测，错误的状态报文将被阻塞或丢弃．

ｂ．ＨＴＴＰ检测：ＨＴＴＰ是超文本传输协议，ＡＳＰＦ检测基于ＴＣＰ／ＩＰ传输的ＨＴＴＰ应用，ＨＴＴＰ是无状态的协议因此ＡＳＰＦ检测应用协议的状态完全等同于通用ＴＣＰ检测．对于ＨＴＴＰ协议，ＡＳＰＦ提供的对来自制定网段或主机的ＨＴＴＰ传输的Ｊａｖａ applets的检测和过滤．

ｃ．ＦＴＰ检测：ＡＳＰＦ检测基于ＴＣＰ／ＩＰ的ＦＴＰ应用，包括对ＦＴＰ控制通道的状态机进行检测，错误的状态转换报文将被阻塞丢弃．支持对ＰＡＳＶ和ＰＯＲＴ两种方式的数据通道协商的检测，并根据协商参数动态创建数据通道的会话状态表和临时访问控制列表． ｄ．ＲＳＴＰ检测：ＲＳＴＰ实时流传输协议．ＡＳＰＦ检测基于ＴＣＰ／ＩＰ传输的ＲＳＴＰ应用．包括对ＲＳＴＰ控制通道重媒体传输通道（基于ＵＤＰ的ＲＴＰ／ＲＴＣＰ）参数协商的检测，并动态创建媒体通道的会话状态表和临时访问控制列表．

ｅ．Ｈ３２３检测：Ｈ３２３是ＩＴＵ－Ｕ制定的分组网络的多媒体传输协议．ＡＳＰＦ检测基于ＴＣＰ／ＩＰ传输的Ｈ３２３应用，包括对Ｑ９３１呼叫信令的检测，用于检测和维护动态创建Ｈ２４５媒体控制通道，ＡＳＰＦ检测基于Ｈ２４５媒体控制通道重媒体传输通道（基于ＵＤＰ的ＲＴＰ／ＲＴＣＰ）参数协商的检测，并动态创建媒体通道的状态表和临时访问控制列表． ２.通用的ＴＣＰ／ＵＤＰ协议检测

ＡＳＰＦ检测ＴＣＰ会话的发起和结束的状态转换过程，包括会话发起的３次握手和关闭的４次握手，根据这些状态来创建．更新和删除会话状态表和临时访问控制表．当检测到第一个临时访问控制和允许表项，以允许该会话所有的相关的报文能通过防火墙，而且它非相关报文则呗阻塞和丢弃，ＴＣＰ检测是其他基于ＴＣＰ应用层协议的基础． ＵＤＰ协议没有连接和状态的概念．当ＡＳＰＦ检测到ＵＤＰ会话发起的第一个数据包时，ＡＳＰＦ开始维护这些会话相关的状态，并创建一个ＴＡＣＬ（临时访问控制列表）允许表项，ＡＳＰＦ以为发起方收到的第一个接受方回送的ＵＤＰ数据流的时候，此会话建立其他的与此回话无关的报文则被阻塞和丢弃，ＵＤＰ检测是其他基于ＵＤＰ的应用层协议检测的基础。３.会话状态动态管理

ＡＳＰＦ支持通过配臵会话超时时间实现会话状态信息的管理。用户可以通过对ＴＣＰ的ＳＹＮ等状态等待超时老化时间进行配臵管理，达到根据会话时间对会话状态进行管理的目的。此外，在应用层协议检测中提到，对于存在状态机转换的应用层协议，ＡＳＰＦ也支持根据ＦＳＭ的正确性与否管理会话状态信息的目的。ＡＳＰＦ可以实现会话状态的自动创建与删除。４.ＩＰ分片报文检测

如果ＩＰ报文内容大于接口ＭＴＵ的大小，数据包将会被分片，形成多个更小的ＩＰ包，在所有分片后的ＩＰ数据包中只有第一个分片包含了完整的ＩＰ包信息，其他分片只有ＩＰ地址信息。ＡＳＰＦ检测根据ＴＣＰ的分片标识把收到的报文区分为非分片和分片首片及非首片报文三类报文。

ＡＳＰＦ记录所有被分片报文的状态信息以提供对分片报文正常检测和过滤的支持，对于首片报文，ＡＳＰＦ根据报文的ＩＰ层信息及ＩＰ层以外的信息创建会话状态表与ＴＡＣＬ表，当所有后续分片到达时，ＡＳＰＦ使用保存的会话信息和ＴＡＣＬ中的每一匹配条件进行精确匹配。

５.端口到应用的映射（ＰＡＭ）

应用层协议使用通用的端口进行通信，ＰＡＭ允许用户对不同应用定义一组新的端口号，用于应用使用非通用端口时的情况，如应用在８１号端口提供ｈｔｔｐ，就可以用ＰＡＭ指定，从而知道８１端口是ｈｔｔｐ数据。６.Ｊａｖａ阻塞功能

由于恶意的applets对用户计算机资源造成破坏，用户需要限制未经用户允许的Ｊａｖａ appletｓ下载至用户网络中，Ｊａｖａ ｂｌｏｃｋｉｎｇ功能便可以实现对来自不可信任站点的applets的过滤。而实现上是采用ＡＣＬ定义站点的信任与否，当检测到报文是不可信任的站点的applets时采取丢弃操作。

（未完待续－－请关注防火墙之－－状态防火墙（３））

防火墙技术之---状态防火墙ASPF（3）

2024-08-23 09:41:09 标签：防火墙 ASPF 状态 技术

状态防火墙ASPF工作原理 一般来说跟其他安全业务一样，ASPF也是基于会话管理模块的，我们知道会话session是动态的，所以ASPF也是动态的，有状态跟踪的，另外ASPF的精髓还在于出报文打开一个安全的通道，返回报文在这个安全的通道中传输，而维护这个安全通道的依然是访问控制列表ACL，当然这儿的ACL称为临时访问控制列表TACL，之所以称为临时，因为它是动态的用过即删，首报文动态创建TACL，然后返回报文检查是否匹配TACL，如果完全匹配责放行，如果不匹配责丢弃。说来说去，大家也许可以看到之所以称状态防火墙ASPF是动态防火墙，原因在于两点： 1.ASPF是以session为基础的，session的动态性决定了ASPF的动态性。

2.ASPF需要创建TACL打开报文返回的安全通道，TACL是动态创建和删除的，所以注定ASPF是动态的。

理解了以上两点，那么你也就从心里开始接受ASPF了，因为这是ASPF的精华核心。下面介绍一下ASPF维护的两个表：

a 会话状态表

前面也讲到了会话表项是一个七元组：

协议 状态（老化时间）源IP（源端口）-->目的IP（目的端口）目的IP（目的端口）<--源IP（源端口）（用于返回报文匹配）

可以看出一条会话其实就可以理解为一个TCP连接（当然不一定是TCP会话），会话状态表维护了一个会话中某一个时刻会话所处的状态，用于匹配后续的发送报文，并检测会话状态的转换是否是正确的。session table是在检测到第一个报文时创建的，随着不同的状态触发条件会进入到不同的状态中并维护。ASPF于包过滤的最大区别就在于ASPF考虑到会话的上下文，不仅包括当前的会话状态，还记录了本次会话之前的通信信息，具有更好的灵活性与安全性，这也是ASPF动态过滤的关键。b 临时访问控制列表TACL

虽然被称为TACL，但是它独立于ACL，更确切的说是利用了ACL访问控制的思想，是动态的，非静态配臵指定的。TACL在创建session table时创建，会话结束后自动删除，依赖于session的，从功能上说它相当于一个扩展的ACL的permit项，用于匹配一个会话中所有应答报文。

下面以FTP为例来说明一下ASPF多通道应用层协议检测的过程：

如上图所示假设FTP client向FTP server的21号端口发起FTP控制通道的连接，通过协商由服务器端的21端口想客户端的20号端口发起数据通道的连接，数据传输超时或结束连接删除。

FTP检测在FTP连接建立到关闭的过程中的处理如下：

1.检查从出接口向外发送的IP报文，确认为基于TCP的IP报文 2.检查端口号确认连接为控制连接，建立返回报文的TACL和session table

3.检查FTP控制连接报文，解析FTP指令，根据指令更新状态表，如果包含数据通道建立指令，则创建数据连接的临时访问控制列表，对数据连接不进行状态处理。

4.对于返回报文，根据协议类型做相应的匹配检查，检查将根据ingredients的协议的状态表和TACL决定报文是否允许通过。

5.FTP连接删除时，会话状态表及TACL随之删除。

以上介绍了ASPF是如何处理多通道协议的应用协议检查的。对于像SMTP.HTTP等单通道协议的检测过程就相对较为简单，当发起连接时建立会话状态表和TACL，连接删除是系统自动删除。

而对于传输层协议TCP/UDP检测，跟应用层协议检测不同，传输层协议检测只是简单的五元组信息检查，要求返回报文必须完全跟原报文sip，sport，dip，dport和proto一致才可以放行，否则直接丢弃。

上面介绍就是ASPF的工作原理。

**第五篇：防火墙基础知识**

防火墙基础知识

3.3 包过滤包过滤技术(Ip Filtering or packet filtering)的原理在于监视并过滤网络上流入流出的Ip包，拒绝发送可疑的包。由于Internet 与Intranet 的连接多数都要使用路由器，所以Router成为内外通信的必经端口，Router的厂商在Router上加入IP Filtering 功能，这样的Router也就成为Screening Router 或称为Circuit-level gateway.网络专家Steven.M.Bellovin认为这种Firewall 应该是足够安全的，但前提是配置合理。然而一个包过滤规则是否完全严密及必要是很难判定的，因而在安全要求较高的场合，通常还配合使用其它的技术来加强安全性。

Router 逐一审查每份数据包以判定它是否与其它包过滤规则相匹配。(注：只检查包头的内容，不理会包内的正文信息内容)过滤规则以用于IP顺行处理的包头信息为基础。包头信息包括: IP 源地址、IP目的地址、封装协议(TCP、UDP、或IP Tunnel)、TCP/UDP源端口、ICMP包类型、包输入接口和包输出接口。如果找到一个匹配，且规则允许这包，这一包则根据路由表中的信息前行。如果找到一个匹配，且规则允许拒绝此包，这一包则被舍弃。如果无匹配规则，一个用户配置的缺省参数将决定此包是前行还是被舍弃。

\*从属服务的过滤包过滤规则允许Router取舍以一个特殊服务为基础的信息流，因为大多数服务检测器驻留于众所周知的TCP/UDP端口。例如，Telnet Service 为TCP port 23端口等待远程连接，而SMTP Service为TCP Port 25端口等待输入连接。如要封锁输入Telnet、SMTP的连接，则Router舍弃端口值为23,25的所有的数据包。典型的过滤规则有以下几种：

.允许特定名单内的内部主机进行Telnet输入对话

.只允许特定名单内的内部主机进行FTP输入对话

.只允许所有Telnet 输出对话

.只允许所有FTP 输出对话

.拒绝来自一些特定外部网络的所有输入信息

\* 独立于服务的过滤

有些类型的攻击很难用基本包头信息加以鉴别，因为这些独立于服务。一些Router可以用来防止这类攻击，但过滤规则需要增加一些信息，而这些信息只有通过以下方式才能获悉：研究Router选择表、检查特定的IP选项、校验特殊的片段偏移等。这类攻击有以下几种:.源IP地址欺骗攻击

入侵者从伪装成源自一台内部主机的一个外部地点传送一些信息包；这些信息包似乎像包含了一个内部系统的源IP地址。如果这些信息包到达Router的外部接口，则舍弃每个含有这个源IP地址的信息包，就可以挫败这种源欺骗攻击。

.源路由攻击源站指定了一个信息包穿越Internet时应采取的路径，这类攻击企图绕过安全措施，并使信息包沿一条意外(疏漏)的路径到达目的地。可以通过舍弃所有包含这类源路由选项的信息包方式，来挫败这类攻击。

.残片攻击入侵者利用Ip残片特性生成一个极小的片断并将TCP报头信息肢解成一个分离的信息包片断。舍弃所有协议类型为TCP、IP片断偏移值等于1的信息包，即可挫败残片的攻击。从以上可看出定义一个完善的安全过滤规则是非常重要的。通常，过滤规则以表格的形式表示，其中包括以某种次序排列的条件和动作序列。每当收到一个包时，则按照从前至后的顺序与表格中每行的条件比较，直到满足某一行的条件，然后执行相应的动作(转发或舍弃)。有些数据包过滤在实现时，“动作”这一项还询问，若包被丢弃是否要通知发送者(通过发ICMP信息),并能以管理员指定的顺序进行条件比较，直至找到满足的条件。以下是两个例子: \* 例 一

某公司有一个B类地址 123.45.0.0,它不希望Internet上的其他站点对它进行访问。但是，该公司网中有一个子网123.45.6.0 用于和某大学合作开发项目，该大学有一个B类地址 135.79.0.0，并希望大学的各个子网都能访问123.45.6.0 子网。但是，由于135.79.99.0 子网中存在着不安全因素，因此，它除了能访问123.45.6.0 子网之外，不能访问公司网中的其它子网。为了简单起见，假定只有从大学到公司的包，表一中列出了所需的规则集。

表 一

规 则

源

地 址

目 的 地 址

动

作

A

135.79.0.0

123.45.6.0

permit

B

135.79.99.0

123.45.0.0

deny

C

0.0.0.0

0.0.0.0

deny

其中0.0.0.0代表任何地址，规则C是缺省规则，若没有其它的规则可满足，则应用此规则。如果还有从公司到大学的包，相对称的规则应加入到此表格中，即源地址与目的地址对调，再定义相应的动作。

现在，我们按照规则ABC的顺序来进行过滤和按照BAC的顺序来进行过滤后采取的动作的结果如表二所示(注意：两种动作的结果有不同)

表

二 Packet 源 地 址

目 的 地 址

希望的动作 执行ABC后 执行BAC后

135.79.99.1

123.45.1.1

deny

deny(B)

deny(B)

\* 2

135.79.99.1

123.45.6.1

permit

permit(A)deny(B)3

135.79.1.1

123.45.6.1

permit

permit(A)permit(A)4

135.79.1.1

123.45.1.1

deny

deny(C)

deny(c)

从表二可以看出，以ABC的顺序来应用规则的Router能达到预想的结果： 从135.79.99.0子网到公司网的包(如包1)都被拒绝(根据规则B)，从135.79.99.0子网到123.45.6.0子网的包(如包2)将被转发(根据规则A)，从大学中的其它子网到123.45.6.0的子网包(如包3)也将被转发(根据规则A)，从大学中的其它子网到公司中的其它字网的包(如包4)都被拒绝(根据规则C)。若以BAC的顺序来应用规则，则不能达到预计的目的。实际上，在上面的规则外集中存在着一个小错误，正是由于这个错误，导致了以ABC的顺序和以BAC的顺序来应用规则而出现了不同的结果。该错误就是:规则B似乎用于限制135.79.99.0子网访问公司网，但实际上这是多余的。如果将这条规则去掉，那么顺序ABC和BAC都将归结为AC顺序。以AC的顺序进行过滤后的结果如表三所示。

表

三

Packet

源 地 址

目 的 地 址

希望的动作

AC 动作

135.79.99.1

123.45.1.1

deny

deny(C)

135.79.99.1

123.45.6.1

permit

permit(A)

135.79.1.1

123.45.6.1

permit

permit(A)

135.79.1.1

123.45.1.1

deny

deny(C)

\* 例 二如图一所示的网络，由包过滤的Router作为在内部被保护的网络与外部不安全的网络之间的第一道防线。假设网络的安全策略为:从外部主机来的Internet Mail 在一个指定的网关上接收，同时你不信任外部网络上一个名叫HPVC的主机，准备拒绝任何由它发起的网络通信。

本例中，关于使用SMTP的网络安全策略必须转移为包过滤规则。可以将网络安全规则转换成下述用语言表示的规则：

规则1: 拒绝从主机HPVC发起的连接。

规则2：允许连接到我们的E-Mail网关。这些规则可以用下面的表四来表示。星号(\*)表示可以匹配该列的任何值。

表

四规则

动作

本地

本地

远地主机

远地

说明

序号

主机

端口号

端口号

Block

\*

\*

HPVC

\*

Block traffic from

HPVC 2

Allow Mail-GW 25

\*

\*

Allow Connection to Our

Mail gateway

对于表四所示的规则1而言，在远地主机栏中填入了HPVC，而其它所有栏的内容都是星号；在动作栏填入阻塞。这条规则的意义可以理解为：阻塞所有从远地主机HPVC发起的从它的任意端口到我们本地任意主机的任意端口的连接。对于表四所示的规则2而言，在本地主机和本地端口号两栏中都有内容，而其它栏都是星号；在动作栏填入允许。这个规则的意义可以理解为：允许从任意远地主机的任意端口发起的到本地主机Mail-GW的25号端口连接(端口25是为SMTP保留的)规则是按照它们在表中的顺序来执行的。如果一个分组不符合任何规则，则它将被拒绝。

在表四中对规则的描述有一个严重的问题，它允许任意外部主机从端口25发起一个呼叫。端口25是为SMTP保留的，但是一个外部主机有可能利用这个权利从事其它活动。这条规则的一个更好的描述方案是允许本地主机发起呼叫，同远地主机的端口25进行通信。这使得本地主机可以向远地站点发送电子邮件。如果远地主机不是用端口25执行SMTP，则SMTP的发送进程将不能发送电子邮件。这等价与远地主机不支持电子邮件。一个TCP连接是一个全双工连接，信息双向流动。在表四所示的包过滤规则中没有明确指定被发送报文分组中信息的传递方向，即是从本地主机发送远地站点，还是从远地站点发送到本地主机。当一个TCP包在某一个方向上传递时，它必须被接收方确认。接收方通过设置TCP ACK标志来发送应答帧。TCP ACK标志也被用来确认TCP建立连接请求，ACK包将在所有TCP连接上发送。当一个ACK包被发送后，发送方向就逆转过来，包过滤规则应该考虑为响应控制或数据包而发回的ACK包。对于下面的表五中的规则1,在源主机栏中填入199.245.180.0,在目标主机端口号栏中填入25,其它栏中都填入星号,在动作栏中填入允许.整个规则的意义为:允许所有从网络199.245.180.0任意端口发起的任意目标主机端口号为25的连接(其中199.245.180.0是一个C类网络地址,主机号字段为0表示网络上任意一台主机).基于以上的讨论,修改后的包过滤规则如表五中所示.表

五

SMTP的包过滤规则规则 动作

源主机

源端

目标主机

远地

TCP标识

说明

序号

口号

端口号

/IP选项 Allow 199.245.180.0 \*

\*

Allow packet

from Network

199.245.180.02 Allow

\*

199.245.180.0 \*

TCP ACK Allow return

acknowledgement

对于表五中的规则2,在源端口号栏中填入25,在目标主机栏中填入199.245.180.0,在TCP标志和IP选项栏中填入TCP ACK,其它栏中都填入星号,在动作栏中填入允许.整个规则的意义为:允许所有从任何外部网络主机上源端口号25发起的到任意本地主机(在网络199.245.180.0上)任意端口号的TCP ACK标志置位的连接.表五中的两条过滤规则合并起来的效果是:允许网络199.245.180上的任意主机同任何外部网络主机的SMTP端口建立连接.由于包过滤器只工作在OSI模型的第二和第三层(数据层和网络层).它无法绝对保证返回的TCP确认帧中是否属于同一个连接.在实际应用中,这个策略运行得很好,因为TCP维护连接两侧的状态信息,它们知道将要发送或接收的序号和确认信息.同时,一些上层应用服务,例如TELNET ,SMTP 和FTP等,只能接受遵循应用层协议规则的包,想要伪造包含正确应答信息的包是非常困难的.如想要使安全程度更高,可考虑和应用层网关一起使用(下节将会讨论).罗罗嗦嗦说了一大通,可以综述为下面两点:包过滤路由器的优点:

绝大多数Internet 防火墙系统只用一个包过滤路由器.与设计过滤器和匹配Router不同的是,执行PACKET FILTER 所用的时间很少或几乎不需要什么时间.因为Internet 访问一般被提供给一个WAN接口.如果通信负载适中且定义的过滤很少的话,则对Router性能没有多大影响.最后一点,包过滤路由器对终端用户和应用程序是透明的,因此不需要专门的用户培训或在每主机上设置特别的软件.包过滤路由器的局限性:

定义包过滤器可能是一项复杂的工作,因为网管员需要详细地了解Internet 各种服务、包头格式和他们在希望每个域查找的特定的值。如果必须支持复杂的过滤要求的，则过滤规则集可能会变得很长和很复杂，从而很难管理。存在几种自动测试软件，被配置到Router上后即可校验过滤规则。这可能对未检测到的易损部件开放了一个地点。一般来说，一个路由器和信息包吞吐量随过滤器数量的增加而减少。Router 被优化用来从每个包中提取目的IP地址、查找一个相对简单的路由表，而后将信息包顺向运行到适当转发接口。如果过滤可执行，Router还必须对每个包执行所有过滤规则。这可能消耗CPU的资源，并影响一个完全饱和的系统性能。

3.4 应用网关

为了克服与包过滤路由器相关联的某些弱点,防火墙需要使用应用软件来转发和过滤Telnet和Ftp等服务的连接。这样一种应用叫做代理服务，而运行代理服务软件的主系统叫做应用网关。应用网关和包过滤路由器可以组合在一起使用，以获得高于单独使用的安全性和灵活性。作为一个例子，请考虑一个用包过滤路由器封锁所有输入Telnet 和Ftp 连接的网点。路由器允许Telnet和Ftp包只通过一个主系统，即Telnet/Ftp应用网关，然后再连接到目的主系统，过程如下：

1.用户首先把Telnet连接到应用网关，并输入内部主系统的名字；

2.网关检验用户的源IP地址，并根据任何合适的访问准则接受或拒绝；

3.用户可能需要证明自己的身份（可使用一次性口令装置）；

4.代理服务软件在网关和内部主系统之间建立Telnet连接；

5.于是，代理服务软件在两个连接之间传送数据；

6.应用网关记录连接情况。这一例子指出了使用代理服务软件的几个好处。第一，代理服务软件只允许有代理的服务通过。换句话说，如果应用网关包含Telnet和Ftp的代理软件，则只有Ftp和Telnet被允许进入受保护的子网，而其它所有服务都完全被封锁住。对有些网点来说，这种程度的安全性是很重要的，因为它保证，只有那些被认为“可信赖的”服务才被允许通过防火墙。它还防止其他不可靠的服务不会背着防火墙管理人员实施。使用代理服务的另一好处是可以过滤协议。例如，有些防火墙可以过滤FTP连接，并拒绝使用FTP 协议中的 put 命令。如果人们要保证用户不能写到匿名FTP服务器软件，则这一点是很有用的。应用网关有三种基本的原型，分别适用于不同的网络规模。

\* 双穴主机网关（Dual-Homed Gateway）

\* 屏蔽主机网关（Screened Host Gateway)

\* 屏蔽子网网关（Screened Subnet Gateway）这三种原型有一个共同的特点，就是都需要一台主机（如上面所述一样）,通常称为桥头堡主机(Bastion Host)。该主机充当应用程序转发者、通信登记者以及服务提供者的角色。因此，保护该主机的安全性是至关重要的，建立防火墙时，应将较多的注意力放在该主机上。

\* 双穴主机网关该原型的结构如下图所示。其中，桥头堡主机充当网关，因此，需要在此主机中装两块网卡，并在其上运行防火墙软件。受保护网与Internet之间不能直接进行通信，必须经过桥头堡主机，因此，不必显示地列出受保护网与不受保护网之间的路由，从而达到受保护网除了看到桥头堡主机之外，不能看到其他任何系统的效果。同时，桥头堡主机不转发TCP/IP包，网络中的所有服务都必须由此主机的相应代理程序支持。

由于双穴主机网关容易安装，所需的硬件设备也较少，且容易验证其正确性，因此，这是一种使用较多的纺火墙。双穴主机网关最致命的弱点是:一旦防火墙被破坏，桥头堡主机实际上就变成了一台没有寻径功能的路由器，一个有经验的攻击者就能使它寻径，从而使受保护网完全开放并受到攻击。例如，在基于Unix的双穴主机网关中，通常是先修改一个名叫IPforwarding的内核变量，来禁止桥头堡主机的寻径能力，非法攻击者只要能获得网关上的系统特权，就能修改此变量，使桥头堡主机恢复寻径能力，以进行攻击。

\* 屏蔽主机网关

该原型的结构如下图所示。其中，桥头堡主机在受保护网中，将带有包屏蔽功能的路由器置于保护网和Internet之间，它不允许Internet对保护网的直接访问，只允许对受保护网中桥头堡主机的访问。与双穴网关类似，桥头堡主机运行防火墙软件。屏蔽主机网关是一种很灵活的防火墙，它可以有选择地允许那些值得信任的应用程序通过路由器。但它不像双穴网关，只需注意桥头堡主机的安全性即可，它必须考虑两方面的安全性，即桥头堡主机和路由器。如果路由器中的访问控制列表允许某些服务能够通过路由器，则防火墙管理员不仅要管理桥头堡主机中的访问控制表，还要管理路由器中的访问控制列表，并使它们互相协调。当路由器允许通过的服务数量逐渐增多时，验证防火墙的正确性就会变得越来越困难。\* 屏蔽子网网关该原型的结构如下图所示。其中，一个小型的独立网络放在受保护网与Internet之间，对这个网络的访问受到路由器中屏蔽规则的保护。因此，屏蔽子网中的主机是唯一一个受保护网和Internet都能访问到的系统。从理论上来说，这也是一种双穴网关的方法，只是将其应用到了网络上。防火墙被破坏后，它会出现与双穴主机网关同样的问题。不同的是，在双穴主机网关中只需配置桥头堡主机的寻径功能，而在屏蔽子网网关中则需配置三个网络（受保护网、屏蔽子网和Internet）之间的寻径功能，即先要闯入桥头堡主机，再进入受保护网中的某台主机，然后返回包屏蔽路由器，分别进行配置。这对攻击者来说显然是极其困难的。另外，由于Internet很难直接与受保护网进行通信，因此，防火墙管理员不需指出受保护网到Internet之间的路由。这对于保护大型网络来说是一种很好的方法。应用网关的一个缺点是，就Telnet 等客户机--服务器协议来说，需要采取两个步骤来连接输入信息或输出信息。有些应用网关需要经过修改的客户机，这一点既可看作是缺点，也可看作是优点，视修改的客户机是否更加容易使用防火墙而定。Telnet应用网关不一定需要经过修改的Telnet客户机，但是，它需要修改用户行为：用户必须连接到防火墙(但不记录)，而不是直接连接到主系统。但是，经过修改的Telnet客户机可以使防火墙透明，因为它允许用户用Telnet命令规定目的系统(不是防火墙)。防火墙起着通向目的系统通道的作用，从而拦截连接，再按需完成其他步骤，如查询一次性口令。用户行为仍然是相同的，但其代价是每个系统需要一个经过修改的客户机。除了Telnet 外，应用网关一般用于Ftp 和电子邮件，同时也用于XWindows和其他某些服务。有些Ftp应用网关包括拒绝特定主系统的put 和get 命令的能力。例如，一个已同内部系统(如匿名Ftp服务器)建立Ftp对话(通过Ftp应用网关)的外部用户，可能试图把文件上装到服务器。应用网关可以过滤Ftp协议,并拒绝把所有puts命令发送给匿名Ftp服务器；这将保证没有文件能上装到服务器，而且所提供的确信程度要高于只依赖由设置正确的匿名Ftp服务器进行的文件许可。电子邮件应用网关可集中收集电子邮件，并把它分发给内部主系统和用户。对外部用户来说，所有内部用户都拥有电子邮件地址，其格式为：user@emailhost 其中,emailhost是电子邮件网关的名字。网关会接受外部用户的邮件，然后按需把邮件转发到其他内部系统。从内部系统发送电子邮件的用户可以从其主系统直接发送电子邮件，否则在内部系统名字只有受保护的子网知道的情况下，邮件会发送给应用网关，然后应用网关着把邮件转发给目的主系统。有些电子邮件网关使用更加安全的sendmail程序版本来接收电子邮件

本文档由站牛网zhann.net收集整理，更多优质范文文档请移步zhann.net站内查找