

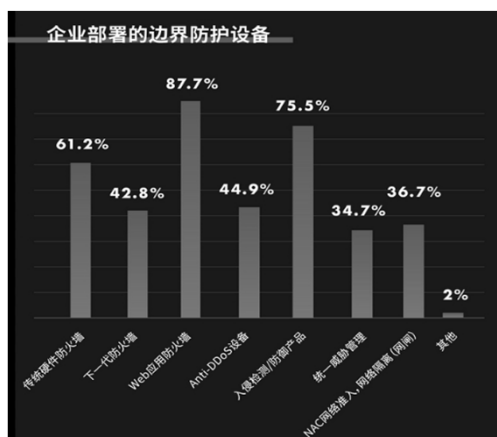
网络防火墙



边界防护

FreeBuf企业安全系列之

2020国内WAF 产品研究报告



内容提纲

- 1 防火墙概述
- 2 防火墙的工作原理
- 3 防火墙体系结构
- 4 防火墙技术发展趋势
- 5 防火墙的选购和使用

一、基本概念

防火墙的基本概念


- 防火墙（Firewall）是在两个网络之间执行访问控制策略的一个或一组安全系统。它是一种计算机硬件和软件系统集合，是实现网络安全策略的有效工具之一，被广泛地应用到Internet与Intranet之间。
 - 所有的内部网络与外部网络之间的通信都必须经过防火墙进行检查与连接，只有授权允许的通信才能获准通过防火墙。
 - 防火墙可以阻止外界对内部网资源的非法访问，也可以防止内部对外部的不安全访问。


防火墙的基本概念

- 防火墙本身必须具有很强的抗攻击能力，以确保其自身的安全性。防火墙简单的可以只用路由器实现，复杂的可以用主机、专用硬件设备及软件甚至一个子网来实现（体系结构部分将详细介绍）。




网络防火墙的主要功能

- 保护脆弱和有缺陷的网络服务
 - 集中化的安全管理
 - 加强对网络系统的访问控制
 - 加强隐私
 - 对网络存取和访问进行监控审计
- 



网络防火墙的主要功能(1/5)

- 保护脆弱和有缺陷的网络服务
 - 防火墙通过过滤不安全的服务而降低风险，能极大地提高一个内部网络的安全性。
 - 例如，防火墙可以禁止Telnet、FTP进出受保护网络，避免外部攻击者利用这些脆弱的协议来攻击内部网络。
- 

网络防火墙的主要功能(2/5)

- 集中化的安全管理

- 通过以防火墙为中心的安全方案配置，能将所有安全软件配置在防火墙上，集中安全管理更经济。

- 例如，网络访问时，一次一密口令系统和其它的身份认证系统不必分散在各个主机上，而集中在防火墙上。

网络防火墙的主要功能(3/5)

- 加强对网络系统的访问控制

- 一个防火墙的主要功能是对整个网络的访问控制。

- 比如，防火墙可以屏蔽部分主机，使外部网络无法访问。同样，可以屏蔽部分主机的特定服务，使得外部网络可以访问该主机的其它服务，但无法访问该主机的特定服务。

网络防火墙的主要功能(4/5)

- 加强隐私
 - 保护内网信息，避免泄露内部网络的某些安全漏洞。
 - 使用防火墙就可以屏蔽泄露网络内部细节的服务，如Finger 服务，DNS服务。
 - Finger显示了主机的所有用户的注册名、真名，最后登录时间和使用shell类型等。
 - 内网的DNS将暴露内部主机的域名和IP地址信息。

网络防火墙的主要功能(5/5)

- 对网络存取和访问进行监控审计
 - 如果所有的访问都经过防火墙，那么，防火墙就能记录下这些访问并作出日志记录，同时也能提供网络使用情况的统计数据。
 - 当发生可疑动作时，防火墙能进行适当的报警，并提供网络是否受到监测和攻击的详细信息。

二、分类

防火墙分类（一）

- 按照软、硬件形式划分
 - 软件防火墙：运行于特定的计算机上，它需要客户预先安装好的计算机操作系统的支持，一般来说这台计算机就是整个网络的网关。
 - 硬件防火墙：基于PC架构，这些PC架构计算机上运行一些经过裁剪和简化的操作系统。至少应具备三个端口，分别接内网，外网和DMZ区。
 - 芯片级防火墙：基于专门的硬件平台，没有操作系统。专有的ASIC芯片促使它们比其他种类的防火墙速度更快，处理能力更强，性能更高。

防火墙分类（二）

- 从防火墙技术分
 - 包过滤(Packet filtering)型：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。
 - 应用代理(Application Proxy)型：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。

防火墙分类（三）

- 从防火墙结构分
 - 单一主机防火墙：与一台计算机结构差不多。需要连接一个以上的内、外部网络。用硬盘来存储防火墙所用的基本程序，如包过滤程序和代理服务器程序等，有的防火墙还把日志记录也记录在此硬盘上。
 - 路由器集成防火墙：许多中、高档的路由器中已集成了防火墙功能。
 - 分布式防火墙：防火墙已不再是一个独立的硬件实体，而是由多个软、硬件组成的系统。不是只是位于网络边界，而是渗透于网络的每一台主机，对整个内部网络的主机实施保护。

防火墙分类（四）

■ 从防火墙应用部署位置分

- 边界防火墙：位于内、外部网络的边界，所起的作用的对内、外部网络实施隔离，保护边界内部网络。这类防火墙一般都是硬件类型的，价格较贵，性能较好。也称为“网络防火墙”。
- 个人防火墙：安装于单台主机中，防护的也只是单台主机。这类防火墙应用于广大的个人用户，通常为软件防火墙，价格最便宜，性能也最差。
- 混合式防火墙：可以说就是“分布式防火墙”或者“嵌入式防火墙”，它是一整套防火墙系统，由若干个软、硬件组件组成，分布于内、外部网络边界和内部各主机之间，既对内、外部网络之间通信进行过滤，又对网络内部各主机间的通信进行过滤。它属于最新的防火墙技术之一，性能最好，价格也最贵。

防火墙分类（五）

■ 从防火墙性能分：分为百兆级、千兆级、万兆级防火墙

- 因为防火墙通常位于网络边界，所以不可能只是十兆级的。这主要是指防火的通道带宽 (Bandwidth)，或者说是吞吐率。当然通道带宽越宽，性能越高，这样的防火墙因包过滤或应用代理所产生的延时也越小，对整个网络通信性能的影响也就越小。

防火墙分类（六）

- 网络防火墙按照实现技术来分，主要可分为两类：一类是网络级防火墙，另一类是应用级防火墙。

防火墙的类型（六）

- 网络级防火墙，也称为包过滤防火墙。
 - 这是一种具有特殊功能的路由器，作用在网络层和传输层。
 - 根据分组包头源地址，目的地址和端口号、协议类型等标志确定是否允许数据包通过。
 - 只有满足过滤逻辑的数据包才被转发到相应的目的地出口端，其余数据包则从数据流中丢弃。

防火墙的类型（六）

- 应用级防火墙：也叫应用网关（**Application Gateway**）。
 - 它作用在应用层，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。

三、相关概念：个人防火墙

个人防火墙

- 个人防火墙就是一个位于用户计算机和它所连接的网络之间的程序。
 - 在用户的计算机和网络进行通讯时，执行预设的访问控制规则，以“允许”或“拒绝”计算机和网络之间的通讯；
 - 最大限度地阻止网络中的黑客或恶意代码访问用户的计算机。

四、相关概念：病毒防火墙

防火墙与“病毒防火墙”

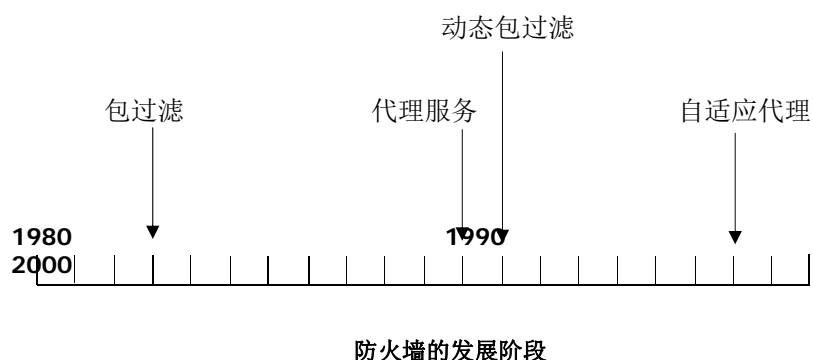
- “病毒防火墙”：病毒实时检测和清除系统，是反病毒软件的一种工作模式。
 - 不是对进出网络的病毒进行监控，而是对所有的系统应用程序进行监控，由此来保障用户系统的“无毒”环境。
 - 而网络防火墙并不监控全部的系统应用程序，它只是对存在网络访问的那部分应用程序进行监控。利用网络防火墙，可以预防黑客入侵，防止木马盗取机密信息等。
 - 说明：现在有不少网络防火墙也可以查杀病毒

内容提纲

- 1 防火墙概述
- 2 防火墙的工作原理
- 3 防火墙体系结构
- 4 防火墙技术发展趋势
- 5 防火墙的选购和使用

技术的发展过程(1/3)

下图表示了防火墙技术的简单发展阶段



技术的发展过程(2/3)

- 第一代防火墙：1983年第一代防火墙技术出现，它几乎是与路由器同时问世的。它采用了包过滤（**Packet filter**）技术，可称为简单包过滤（静态包过滤）防火墙。
- 第二代防火墙：1991年，贝尔实验室提出了第二代防火墙——应用型防火墙（代理防火墙）的初步结构。

技术发展过程(3/3)

- 第三代防火墙：1992年，USC信息科学院开发出了基于动态包过滤（Dynamic packet filter）技术的第三代防火墙，后来演变为目前所说的状态检测（Stateful inspection）防火墙。1994年，以色列的CheckPoint公司开发出了第一个采用状态检测技术的商业化产品。
- 第四代防火墙：1998年，NAI公司推出了一种自适应代理（Adaptive proxy）防火墙技术，并在其产品Gauntlet Firewall for NT中得以实现，给代理服务防火墙赋予了全新的意义。具有应用代理的安全性，但不采用应用代理的数据传送方式，而采用包过滤的传送方式，由此取得安全和效率的一个折中

一、包过滤技术

防火墙的包过滤技术

- 包过滤防火墙从数据包中提取收发IP地址，TCP端口等信息，按预先设置的规则过滤。滤除不符合规定的IP包。
- 包过滤防火墙通常是一个具有包过滤功能的路由器。因为路由器工作在网络层，因此包过滤防火墙又叫网络层防火墙。

防火墙的包过滤技术

Source	Destination	Permit	Protocol
Host A	Host C	Pass	TCP
Host B	Host C	Block	UDP

控制策略

根据策略决定如何处理数据包

数据包

数据包



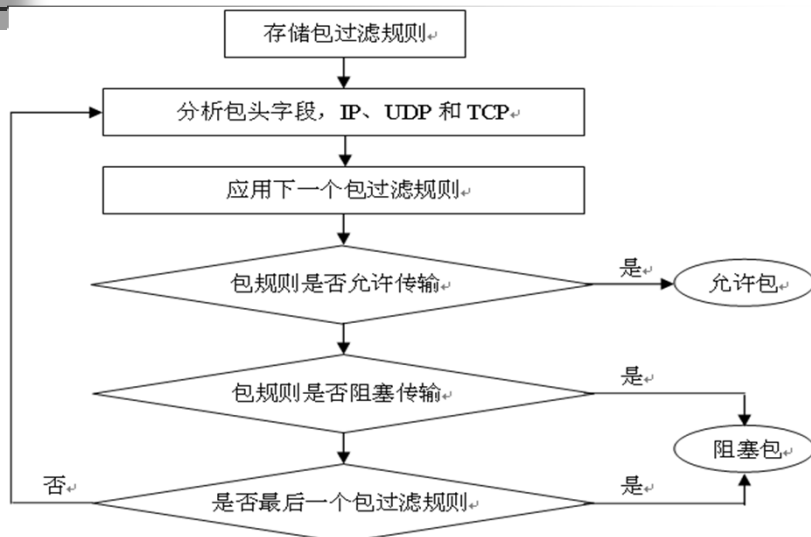
包头中的主要信息

- 包过滤防火墙利用的包头信息
 - IP协议类型(TCP、UDP, ICMP等);
 - IP源地址和目标地址;
 - IP选择域的内容;
 - TCP或UDP源端口号和目标端口号;
 - ICMP消息类型。

包过滤操作的六项要求

- 六项要求:
 - ① 包过滤设备必须存 规则4、5说明规则以正
 - ② 当包到达端口时, 确顺序放置很重要
头中的字段。
 - ③ 包过滤规则的存储顺序与应用顺序相同;
 - ④ 如果一条规则阻 规则6依据的原理是: 未明
 - ⑤ 如果一条规则允 确表示允许的便被禁止。
 - ⑥ 如果一个包不满足任何一条规则, 该包就被阻塞。

包过滤操作的要求



包过滤规则实例（1/3）

规则	包的方向	源地址	目的地址	协议	源端口	目的端口	是否通过
A	出	内部	Internet	TCP	>1023	80	允许
B	入	Internet	内部	TCP	80	>1023	允许

HTTP包过滤规则

包过滤规则实例（2/3）

规则	包的方向	源地址	目的地址	协议	源端口	目的端口	是否通过
A	出	内部	外部	TCP	>1023	23	允许
B	入	外部	内部	TCP	23	>1023	允许
C	双向	任意	任意	任意	任意	任意	拒绝

Telnet包过滤规则

包过滤规则实例（3/3）

- 假设内部网络服务器的IP地址是199.245.180.1，服务器提供电子邮件功能，SMTP使用的端口为25。Internet上有一个hacker主机可能对内部网构成威胁，可以为这个网络设计以下过滤规则：
 - 规则1：我们不相信从hacker来的连接；
 - 规则2：允许其他站点和电子邮件服务器的连接；

规则	包的方向	源地址	目的地址	协议	源端口	目的端口	是否通过
A	入	hacker	内部	任意	任意	任意	拒绝
B	入	任意	199.245.180.1	TCP	任意	25	允许
C	出	199.245.180.1	任意	TCP	25	任意	允许

Cisco路由器包过滤规则

- Cisco路由器是使用较广泛的网络设备，以之为例说明包过滤规则在网络中的实际使用。
- Cisco路由器的访问列表被定义为应用于Internet地址的一系列允许和拒绝条件的集合，这些条件用来完成包过滤规则。
 - 路由器逐个测试包与访问列表中的条件，第一个匹配便可以决定路由器接受或拒绝该包，路由器也就同时停止比较剩余访问列表。

Cisco路由器包过滤规则

- Cisco路由器有两类访问列表：
 - 标准访问列表（Standard Access Control List）：只通过单一的IP地址用于匹配；
 - 扩展访问列表（Extended Access Control List）：使用协议类型等选项信息用于匹配操作。

Cisco的标准访问列表（1/3）

- 标准访问列表的语法规则如下：
- **access-list list-number (permit|deny) source-ip-address wildcard-mask**
 - list-number 是从1~99的整数，用于标识序号；
 - address与wildcard-mask都是32bit的值。
 - 在wildcard-mask中与“1”相关的地址位在比较中忽略，全零部分是必须要配的部分。
 - 如果wildcard-mask的值没有规定，默认为0.0.0.0。
 - 标准访问列表只考虑数据包的源IP地址，不考虑目标地址。
 - 将ACL进行网络接口配置时，可以通过in和out参数控制数据包的方向，是流入还是流出。
- **no access-list list-number**
 - /*用于删除指定编号的访问列表*/

Cisco的标准访问列表（2/3）

- **access-list 1 permit 199.245.180.0 0.0.0.255**
- **access-list 1 permit 132.23.0.0 0.0.255.255**
 - 若两条规则为对流入数据的控制；
 - 两条规则允许来自C类网的199.245.180.0 和B类网的132.23.0.0 主机通过Cisco路由器的包过滤，进行网络访问。

Cisco的标准访问列表 (3/3)

- 假设一A类网络67.0.0.0连接到过滤路由器上。使用下面的ACL进行流出控制：
 - **access-list 3 permit 67.23.2.5 0.0.0.0**
 - **access-list 3 deny 67.23.0.0 0.0.255.255**
 - **access-list 3 permit 67.0.0.0 0.255.255.255**
- 规则13 该列表实现以下安全策略：允许来自67.23.2.5主机的流量，阻止所有其它来自网络67.23.0.0的流量，允许来自67.0.0.0的所有其他子网的流量。

Cisco的扩展访问列表(1/3)

- 扩展访问表：该类表可以基于源和目的IP地址及协议信息进行过滤接口流量。其语法规则如下：
- **access-list list-number (permit|deny) protocol source source-mask destination destination-mask [operator operand]**
 - list-number=100~199，序号用于表示一个或多个permit/deny条件
 - protocol={ip,tcp,udp,icmp}
 - 源匹配时，与source-mask中的1对应的地址位被忽略，与0对应的位参与匹配
 - 目的匹配方法与源相同
 - [operator operand]用于比较端口号等信息
 - operator={lt,eq,gt,neq}，operand是端口号

Cisco的扩展访问列表(2/3)

- 假设网络策略拒绝从132.124.23.55到你的网络199.245.180.0的SMTP连接，扩展访问表设置如下：
 - `no access-list 101`
 - `access-list 101 deny tcp 132.124.23.55 0.0.0.0 199.245.180.0 0.0.0.255 eq 25`
 - `access-list 101 permit any any`
- 规则1删除以前的扩展访问列表101
- 规则2拒绝从主机132.124.23.55到网络199.245.180.0的目的端口为25的SMTP包
- 规则3允许从任意主机来的任意包通过，无本规则将拒绝任何包

Cisco的扩展访问列表(3/3)

- 设内部网络为133.34.0.0，一个扩展访问表的例子：
- `No access-list 101`
 - 注释：删除已有的访问表101
- `access-list 101 permit tcp 0.0.0.0 255.255.255.255 133.34.0.0 0.0.255.255 gt 1023`
 - 注释：允许任何发往内网中端口大于1023号的TCP连接
- `access-list 101 permit tcp 0.0.0.0 255.255.255.255 133.34.12.3 0.0.0.0 eq 25`
 - 注释：允许任何到主机133.34.12.3的SMTP端口的连接
- `access-list 101 permit icmp 0.0.0.0 255.255.255.255 133.34.0.0 255.255.255.255`
 - 注释：允许发来的差错反馈信息的icmp消息

包过滤技术的特点（1/2）

- 包过滤技术的优点：
 - 用一个放置在重要位置上的包过滤路由器即可保护整个网络，这样，不管内部网的站点规模多大，只要在路由器上设置合适的包过滤，各站点均可获得良好的安全保护；
 - 包过滤工作对用户来说是透明的。包过滤不需用户软件支持，也不要对客户机做特殊设置；
 - 包过滤技术是一种有效而通用的控制网络流量的方法，经常作为不可信网络的第一层防卫；可以有效阻塞公开的恶意站点的信息流。

包过滤技术的特点（2/2）

- 包过滤技术的缺点：
 - 安全判决的信息不足，仅依赖网络层和传输层信息，如IP地址、端口号、TCP标志等，只能“就事论事”地进行安全判决。由于缺少信息，一些协议如RPC、UDP难以有效过滤；
 - 支持规则的数量有限，规则过多则会降低网络效率。
 - 正确制定规则并不容易
 - 不可能引入认证机制

包过滤路由器与普通路由器(1/2)

- 普通路由器只简单地查看每一数据包的目的地地址，并选择数据包发往目标地址的最佳路径。当路由器知道如何发送数据包到目标地址，则发送该包；如果不知道如何发送数据包到目标地址，则返还数据包，通知源地址“数据包不能到达目标地址”。
- 过滤路由器将更严格地检查数据包，除了决定是否发送数据包到其目标外，还决定它是否应该发送。“应该”或“不应该”由站点的安全策略决定，并由过滤路由器强制执行。

包过滤路由器与普通路由器(2/2)

- 在对包作出路由决定时，普通路由器只依据包的目的地地址引导包，而包过滤路由器要依据路由器中的包过滤规则作出是否引导该包的决定
- 包过滤路由器以包的目标地址、包的源地址和包的传输协议为依据，确定允许或不允许某些包在网上传输。

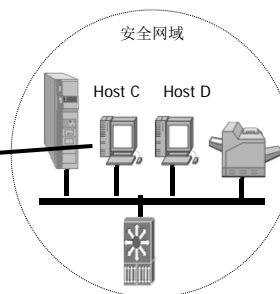
二、状态检测技术

基于状态检查的包过滤技术

存在什么安全问题？

1024以上的临时端口

Web 服务器：TCP
202.119.80.12:80



内部网络允许用户访问Web站点，如果是简单包过滤

对于进入的包必须开放以下规则：

所有源 TCP端口为80，IP地址任意，目标 内部IP，端口号大于1024。

状态检测技术

- 状态检测防火墙又称动态包过滤防火墙。状态检测防火墙在网络层由一个检查引擎截获数据包，抽取出与应用层状态有关的信息，并以此作为依据决定对该数据包是接受还是拒绝。
 - 检查引擎维护一个动态的状态信息表并对后续的数据包进行检查。一旦发现任何连接的参数有意外变化，该连接就被中止
 - 它在协议底层截取数据包，然后分析这些数据包，并且将当前数据包和状态信息与前一刻的数据包和状态信息进行比较，从而得到该数据包的控制信息，来达到保护网络安全的目的

基于状态检查的包过滤技术

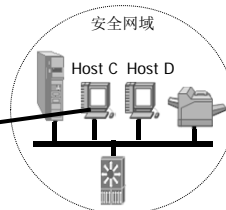
网络中的连接状态表

Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.9.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	1033	173.66.32.122	25	Established
192.168.1.106	1035	177.231.32.12	79	Established
223.43.21.231	1990	192.168.1.6	80	Established
219.22.123.32	2112	192.168.1.6	80	Established
210.99.212.18	3321	192.168.1.6	80	Established
24.102.32.23	1025	192.168.1.6	80	Established
223.212.212	1046	192.168.1.6	80	Established

基于状态检查的包过滤技术

Web 服务器：TCP

202.119.80.12:80



状态检查包过滤

进入的数据包，目标为内部的 **1024** 以上的端口且
它的信息与连接状态表里某一条记录匹配，才允许进入

状态检测技术：优点

- 状态检测防火墙克服了包过滤防火墙和应用代理服务器的局限性，能够根据协议、端口及源地址、目的地址的具体情况决定数据包是否可以通过。
 - 对于每个安全策略允许的请求，状态检测防火墙启动相应的进程，可以快速地确认符合授权标准的数据包，这使得本身的运行速度很快。
 - 跟踪通过防火墙的网络连接和包，这样它就可以使用一组附加的标准，以确定是否允许和拒绝通信。
- 防火墙的状态监视器还能监视RPC(远程调用请求)和UDP的端口信息。包过滤防火墙和代理服务防火墙都不支持此类端口的检测

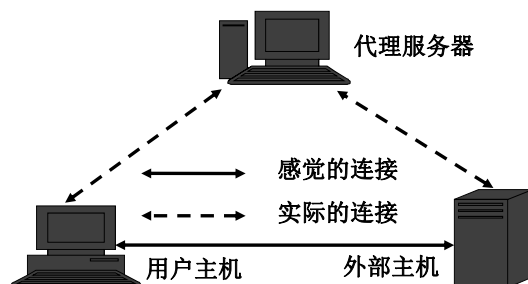
状态检测技术：缺点

- 状态检测防火墙的安全特性是最好的，但其配置非常复杂，会降低网络效率。

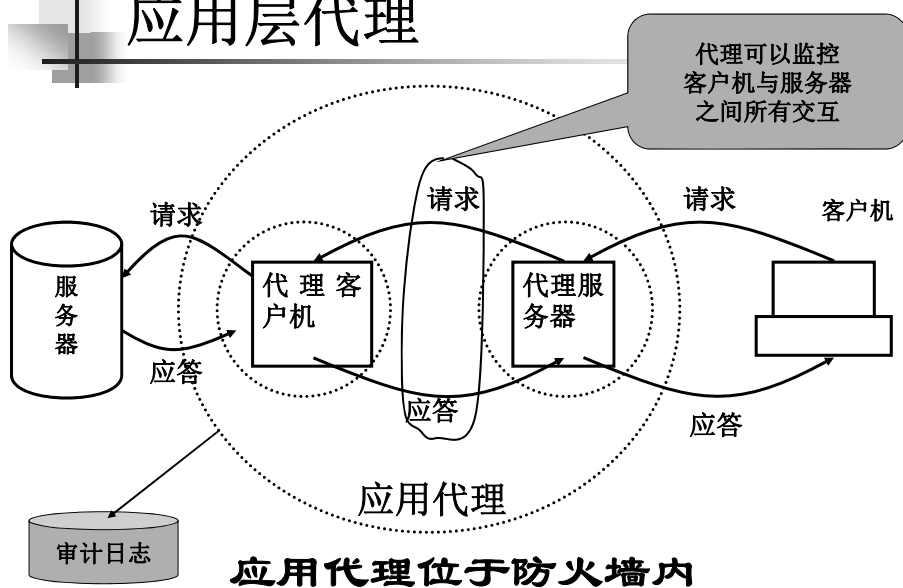
三、代理服务技术

应用级代理

- 应用代理是代理内部网络用户与外部网络服务器进行信息交换的程序。
- 它将内部用户的请求确认后送达外部服务器，同时将外部服务器的响应再回送给用户。



应用层代理



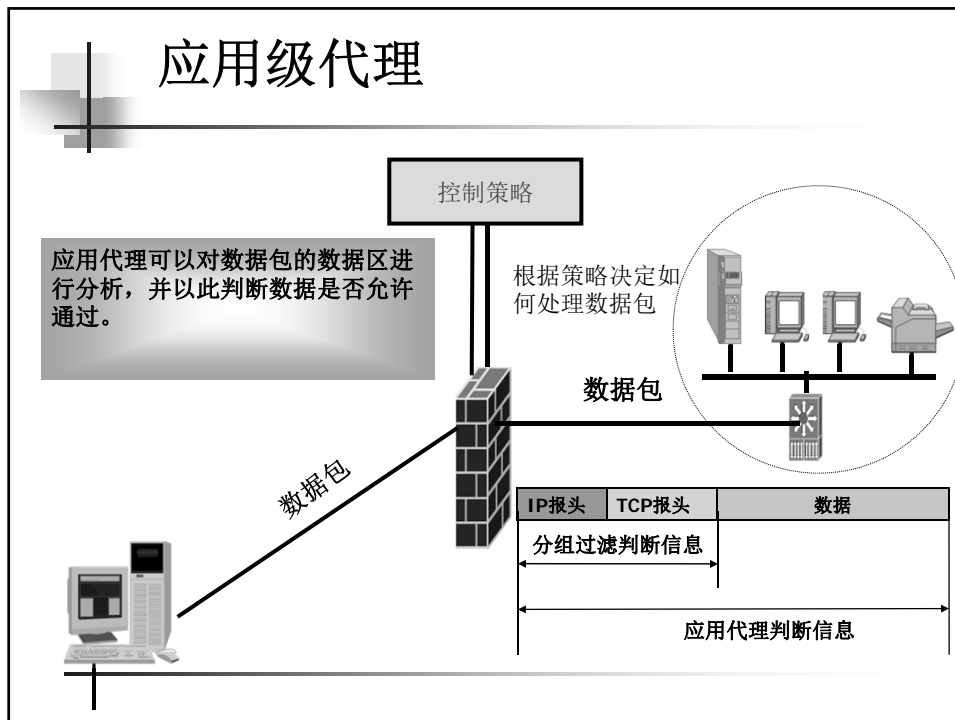
应用级代理的优点

- 由于代理直接和应用程序交互，它可以根据应用上下文进行决策和判定，而不仅仅依据IP地址和端口号。可以做出更为准确的判定。

应用级代理

- 问题：网络内部如果有一个存在安全漏洞的应用，但厂商尚未发布相应的补丁信息来弥补该缺陷，怎么办？
 - 应用代理可以有效解决该问题，应用代理可以被配置来识别尝试攻击应用程序安全漏洞的恶意流量，进而保护运行了不安全应用的系统。

应用级代理



应用级代理 VS 包过滤技术

- 以HTTP流量为例：
 - 包过滤技术仅仅知道应该允许或者拒绝HTTP流量；
 - 应用级代理可以配置来过滤具体HTTP流量类型的数据；
 - 防火墙管理员的管理带来极大的伸缩性，可以严格控制什么流量将会被允许，什么流量将被拒绝。

应用级代理的优点

- 允许用户“直接”访问Internet: 在相应后台软件的支持下, 代理服务系统允许用户从自己的系统访问Internet, 但不允许数据包直接传送而是通过双穴主机或堡垒主机间接传送
- 适合于做日志

应用级代理的缺点(1/2)

- 对每一类应用, 都需要专门的代理。大多数代理服务器只能处理相对较少的应用。
- 应用代理往往比包过滤防火墙性能要差。
 - 应用代理在应用层处理报文, 要求应用代理服务器花费更多的时间来处理报文, 造成数据传输的延迟。
- 应用代理服务器比相应的包过滤防火墙更加昂贵。
 - 应用代理服务器对硬件的要求通常较高, 升级的成本也较高。
- 不能使用户免于协议本身缺点的限制

应用级代理的缺点(2/2)

- 有些服务要求建立直接连接，无法使用代理
 - 比如聊天服务、或者即时消息服务

代理服务器的实现

- 应用级代理服务器
- 回路级代理服务器
- 公共代理服务器(适用于多个协议)
- 专用代理服务器(只适用于单个协议)
- 智能代理服务器

自适应代理技术(1/2)

- 新型的自适应代理(Adaptive proxy)防火墙，本质上属于代理服务技术，但它也结合了动态包过滤(状态检测)技术
 - 自适应代理技术是在商业应用防火墙中实现的一种革命性的技术。组成这类防火墙的基本要素有两个：自适应代理服务器与动态包过滤器。它结合了代理服务防火墙安全性和包过滤防火墙的高速度等优点，在保证安全性的基础上将代理服务器防火墙的性能提高10倍以上

自适应代理技术(2/2)


- 在自适应代理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代理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器从应用层代理请求，还是使用动态包过滤器从网络层转发包。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重要要求



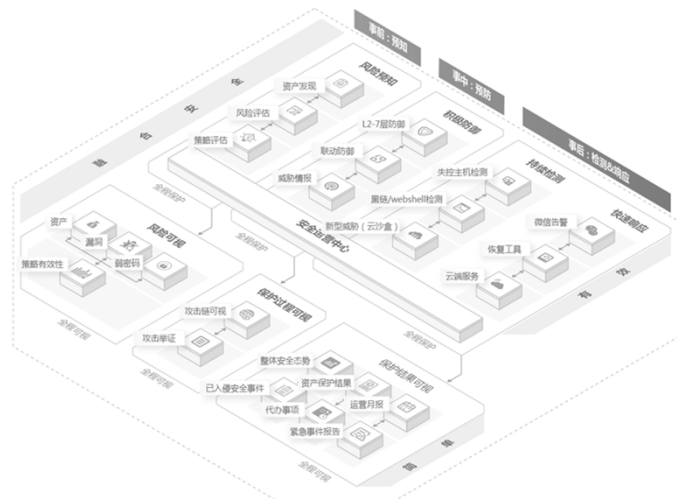
四、下一代防火墙



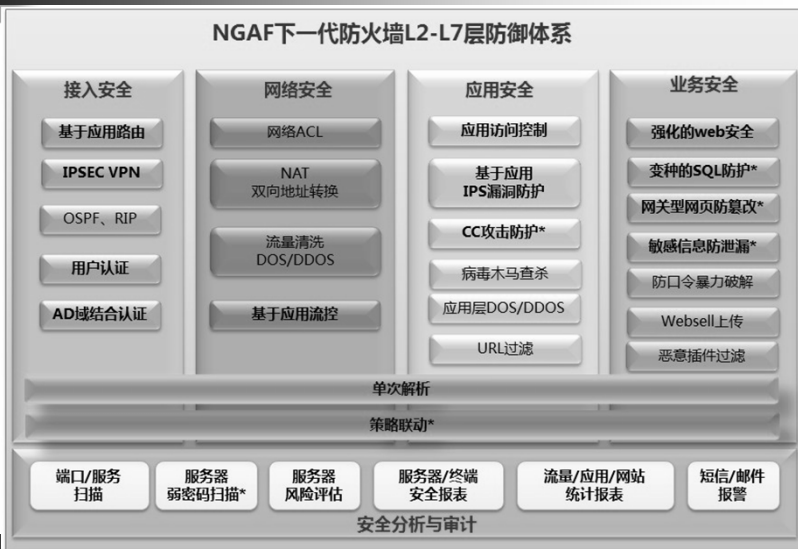
下一代防火墙

- Gartner, 2009 《Defining the Next-Generation Firewall》, 下一代防火墙定义: 一种深度包检测防火墙, 超越了基于端口、协议的检测和阻断, 增加了应用层的检测和入侵防护
 - 针对应用、用户、终端及内容的高精度管控
 - 外部安全智能
 - 一体化引擎多安全模块智能数据联动
 - 可视化智能管理
 - 高性能处理架构
 - 本质上是前面介绍哪种防火墙?
- 

下一代防火墙



下一代防火墙



下一代防火墙



内容提纲

- 1 防火墙概述
- 2 防火墙的工作原理
- 3 防火墙体系结构
- 4 防火墙技术发展趋势
- 5 防火墙的选购和使用

防火墙体系结构

- 防火墙体系结构一般有四种：
 - 过滤路由器或屏蔽路由器结构结构（ **Packet-filtering Router or Screening Router** ）
 - 双穴主机或双宿主机结构 (**Dual Homed Gateway**)
 - 屏蔽主机或主机过滤结构(**Screened Host Gateway**)
 - 过滤子网或屏蔽子网结构(**Screened Subnet**)

相关概念：堡垒主机

- 堡垒主机（**Bastion Host**）：被网络管理员认定为网络安全核心点的系统，必须具有很强的安全性：
 - 安全的操作系统；
 - 关闭不必要的服务；
 - 避免安装不必要的软件；
 - 有限制地访问磁盘，一般能够访问配置文件即可；
 - ...
- 堡垒主机常常充当内部网络或防火墙中应用代理的角色。
- 堡垒主机是最显露的主机，因此也应当是最安全的主机。

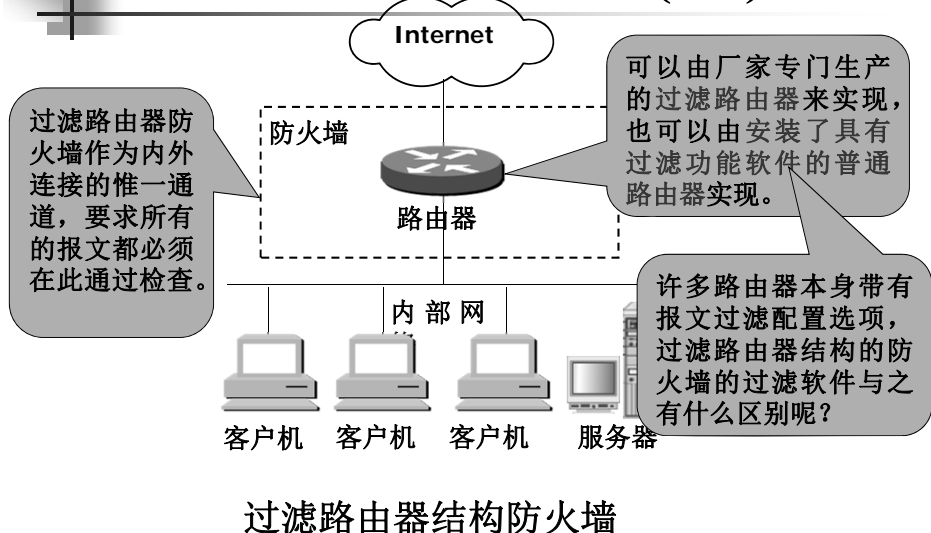
Bastion Host

- **Bastion Host**
 - highly secure host system
 - A system identified by the firewall administrator as a critical strong point in the network's security
 - The bastion host serves as a platform for an application-level or circuit-level gateway

相关概念：DMZ区

- **中立区或非军事化区域（Demilitarized Zone：DMZ）**
 - 存在于企业内部网络和外部网络之间的一个小型网络。
 - 由屏蔽路由器建立或阻塞路由器建立。
 - DMZ用来作为外网和内网的缓冲区以进一步隔离公网和内部私有网络。
 - DMZ放置一些必须公开的服务器

一、过滤路由器结构(1/2)



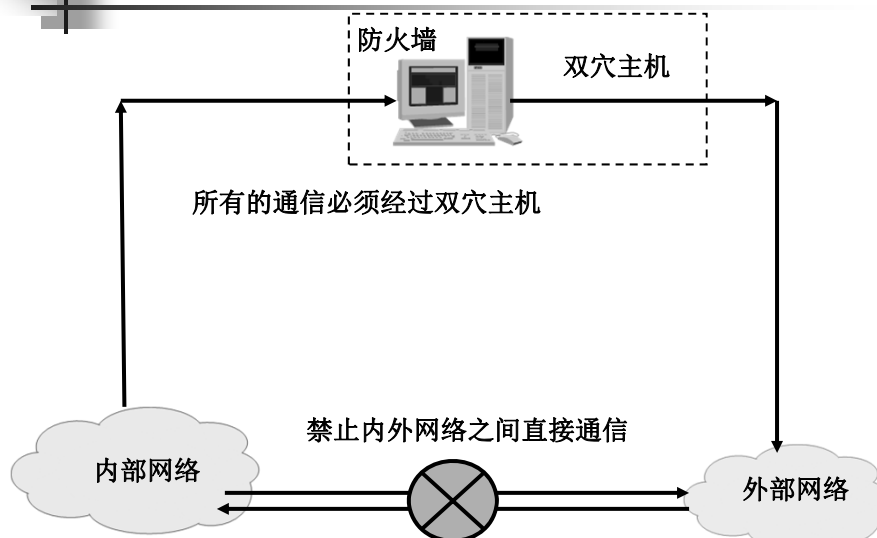
一、过滤路由器结构(2/2)

- 过滤路由器结构是最简单的防火墙结构。
- 缺点：
 - 没有或有很简单的日志记录功能，网络管理员很难确定网络系统是否正在被攻击或已经被入侵。
 - 规则表随着应用的深化会变得很大而且很复杂。
 - 依靠一个单一的部件来保护网络系统，一旦部件出现问题，会失去保护作用，而用户可能还不知道。

二、双穴主机体系结构(1/3)

- 定义：用一台装有两块网卡的堡垒主机（称为双穴主机或双宿主主机）做防火墙。两块网卡各自与受保护网和外部网相连，每块网卡都有独立的IP地址。堡垒主机上运行着防火墙软件(应用层网关)，可以转发应用程序，也可提供服务等功能。
- 有文献称为：双穴主机网关结构(Dual Homed Gateway)

二、双穴主机体系结构(2/3)



二、双穴主机体系结构(3/3)

■ 优点:

- 双穴主机网关优于屏蔽路由器的地方是堡垒主机的系统软件可用于维护系统日志、硬件拷贝日志或远程日志。这对于日后的检查非常有用，但这不能帮助网络管理者确认内网中哪些主机可能已被黑客入侵。

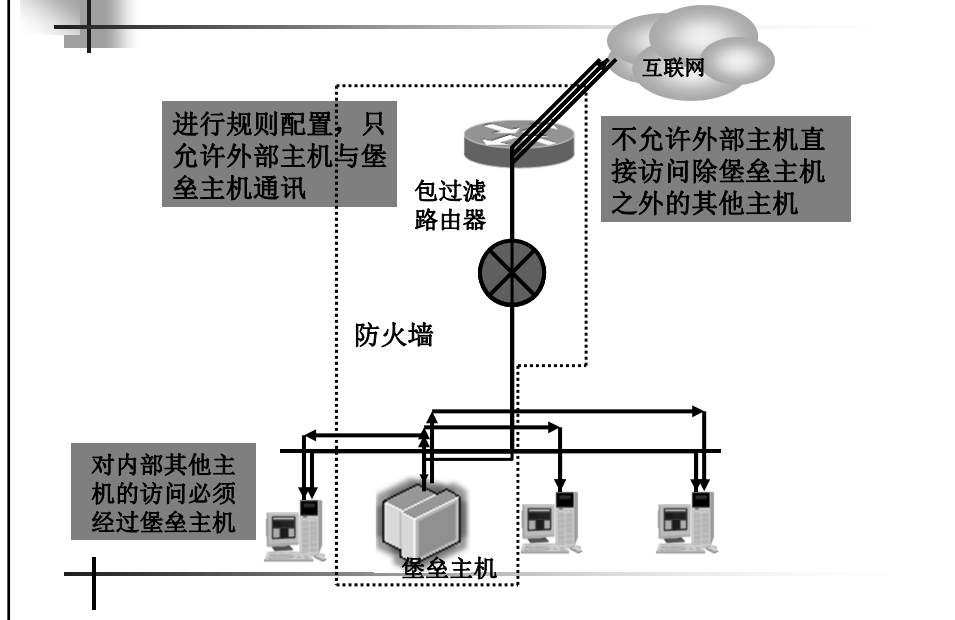
■ 缺点:

- 如何保护堡垒主机？一旦入侵者侵入堡垒主机并使其只具有路由功能，则任何网上用户均可以随便访问内部网络。

三、屏蔽主机体系结构(1/3)

- 定义：屏蔽主机体系结构包括：一个分组（包）过滤路由器(或称为屏蔽路由器)连接外部网络，再通过一个堡垒主机与内部网络相连，通常在路由器上设立过滤规则，并使这个堡垒主机成为从外部网络惟一可直接到达的主机，这确保了内部网络不受未被授权的外部用户的攻击。
 - 来自外部网络的数据包先经过屏蔽路由器过滤，不符合过滤规则的数据包被过滤掉；符合规则的包则被传送到堡垒主机上。其代理服务软件将允许通过的信息传输到受保护的内部网上。

三、屏蔽主机体系结构(2/3)

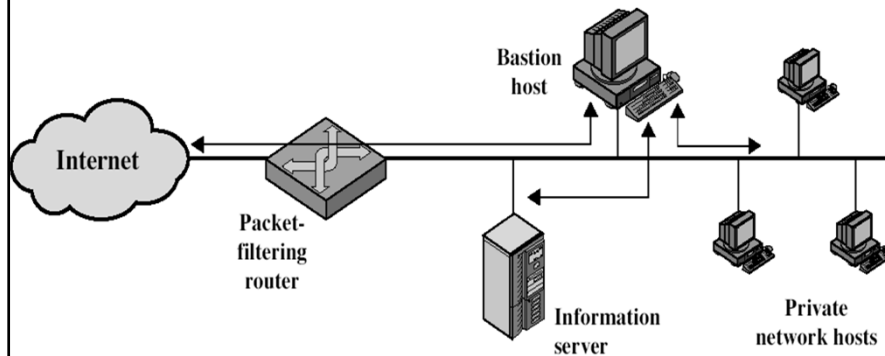


三、屏蔽主机体系结构(3/3)

- 优点:
 - 如果受保护网络是一个虚拟扩展的本地网, 即没有子网和路由器, 那么内网的变化不影响堡垒主机和屏蔽路由器的配置。
 - 危险区域只限制在堡垒主机和屏蔽路由器。
- 缺点:
 - 堡垒主机与其他主机在同一个子网, 一旦包过滤路由器被攻破, 整个内网和堡垒主机之间就再也没有任何阻挡。
 - 一旦入侵者侵入堡垒主机并使其只具有路由功能, 则任何网上用户均可以随便访问内部网络 (与双穴主机结构弱点一样)。

Screened host firewall system

- **Screened host firewall system (single-homed bastion host)**



single-homed bastion host

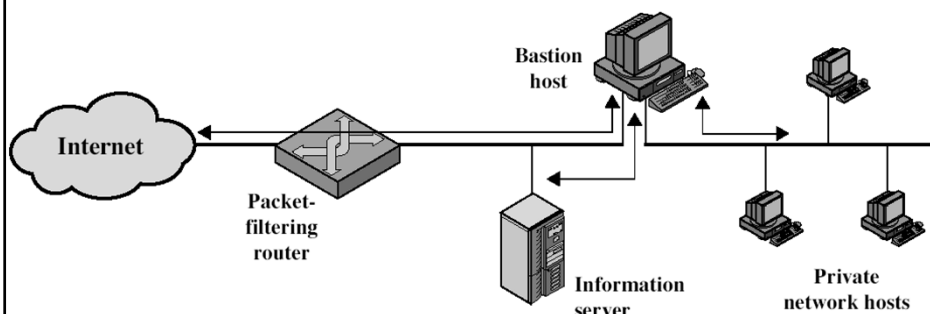
- **Screened host firewall, single-homed bastion configuration**
- **Firewall consists of two systems:**
 - A packet-filtering router
 - A bastion host
- **Configuration for the packet-filtering router:**
 - Only packets from and to the bastion host are allowed to pass through the router
- **The bastion host performs authentication and proxy functions**

single-homed bastion host

- Greater security than single configurations because of two reasons:
 - This configuration implements both packet-level and application-level filtering (allowing for flexibility in defining security policy)
 - An intruder must generally penetrate two separate systems
- This configuration also affords flexibility in providing direct Internet access (public information server, e.g. Web server)

Screened host firewall system

- Screened host firewall system (dual-homed bastion host)



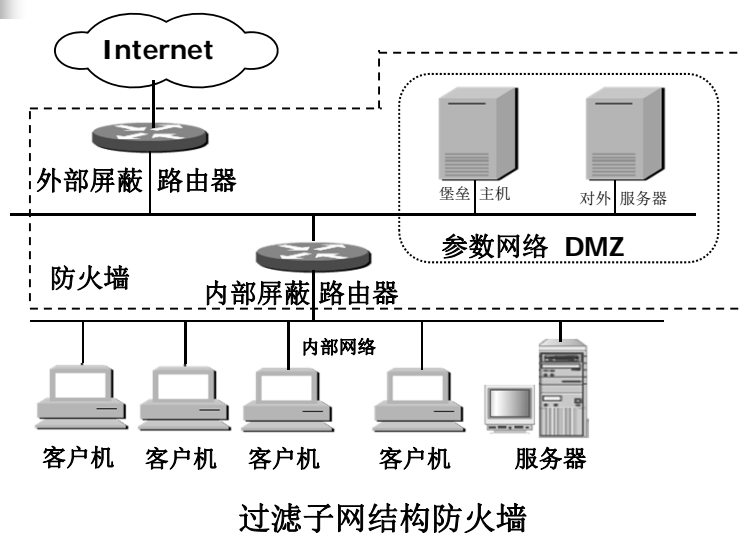
Firewall Configurations

- **Screened host firewall, dual-homed bastion configuration**
 - The packet-filtering router is not completely compromised
 - Traffic between the Internet and other hosts on the private network has to flow through the bastion host

四、过滤子网体系结构(1/7)

- 在外界网络和内部网络之间建立一个双方都可以访问的独立网络（过滤子网），用两台分组过滤路由器将这一子网分别与内部网络和外部网络分开：

四、过滤子网体系结构(2/7)



四、过滤子网体系结构(3/7)

- 过滤子网
 - 也常常被称为DMZ（Demilitarized Zone）区或参数网络或周边网络或屏蔽网络，它可以只包含堡垒主机，也可以增加需要对外提供服务的Web服务器。
 - 过滤子网不提供外部网络和内部网络之间的通路。
 - 它是在内/外部网之间另加的一个安全保护层，相当于一个应用网关。如果入侵者成功地闯过外层保护网到达防火墙，参数网络就能在入侵者与内部网之间再提供一层保护。
 - 如果过滤子网中的堡垒主机被攻破会有什么后果？

四、过滤子网体系结构(4/7)

- 如果入侵者仅仅侵入到过滤子网中的的堡垒主机，他只能偷看到过滤子网的信息流而看不到内部网的信息，过滤子网的信息流仅往来于外部网到堡垒主机。没有内部网主机间的信息流(重要和敏感的信息)在过滤子网中流动，所以堡垒主机受到损害也不会破坏内部网的信息流

四、过滤子网体系结构(5/7)

- 堡垒主机
 - 在过滤子网结构中，堡垒主机与过滤子网相连，而该主机是外部网服务于内部网的主节点。
 - 在内、外部路由器上建立包过滤，以便内部网的用户可直接操作外部服务器；
 - 在主机上建立代理服务，在内部网用户与外部服务器之间建立间接的连接。
 - ✓ 接收外来电子邮件并分发给相应站点；
 - ✓ 接收外来FTP并连到内部网的匿名FTP服务器；
 - ✓ 接收外来的有关内部网站点的域名服务。

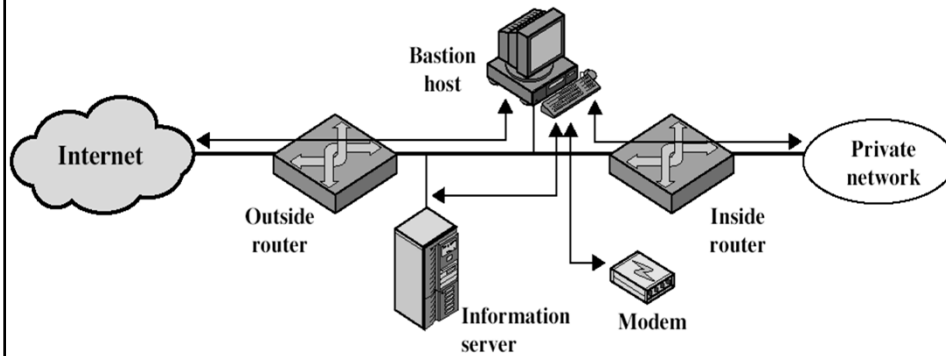
四、过滤子网体系结构(6/7)

- 内部路由器
 - 主要功能是保护内部网免受来自外部网与过滤子网的侵扰。
 - 内部路由器可以设定，使过滤子网上的堡垒主机与内部网之间传递的各种服务和内部网与外部网之间传递的各种服务不完全相同。
 - 内部路由器完成防火墙的大部分包过滤工作，它允许某些站点的包过滤系统认为符合安全规则的服务在内/外部网之间互传。
 - 根据各站点的需要和安全规则，可允许的服务是如下的外向服务：Telnet、FTP、WAIS、Archie、Gopher或其它服务。

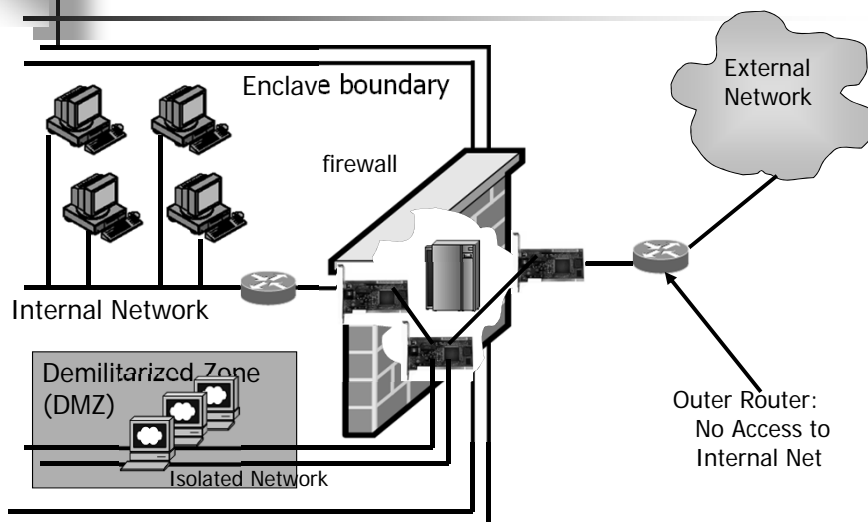
四、过滤子网体系结构(7/7)

- 外部路由器
 - 既可保护过滤子网又保护内部网。实际上，在外部路由器上仅做一小部分包过滤，它几乎让所有过滤子网的外向请求通过。它与内部路由器的包过滤规则基本上相同。
 - 外部路由器的包过滤主要是对过滤子网上的主机提供保护。一般情况下，因为过滤子网上主机的安全主要通过主机安全机制加以保障，所以由外部路由器提供的很多保护并非必要
 - 真正有效的任务是阻隔来自外部网上伪造源地址进来的任何数据包。这些数据包自称来自内部网，其实它是来自外部网

Screened-subnet firewall system



Screened Subnet Firewall Architecture



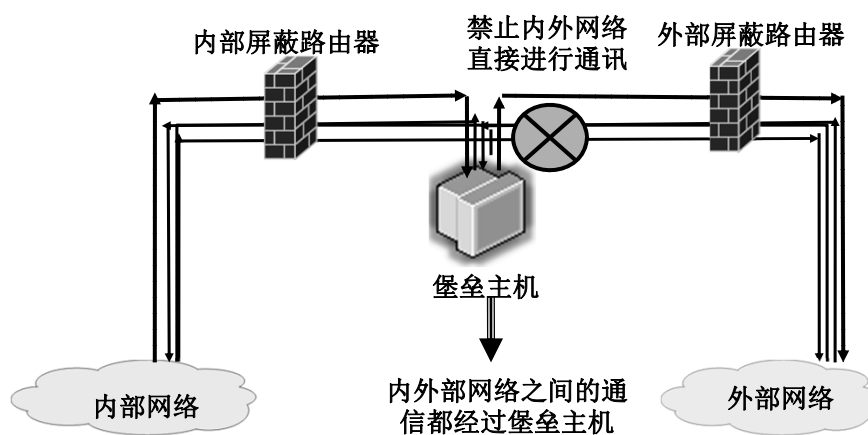
Screened subnet firewall configuration

- **Most secure configuration of the three**
- **Two packet-filtering routers are used**
- **Creation of an isolated sub-network**

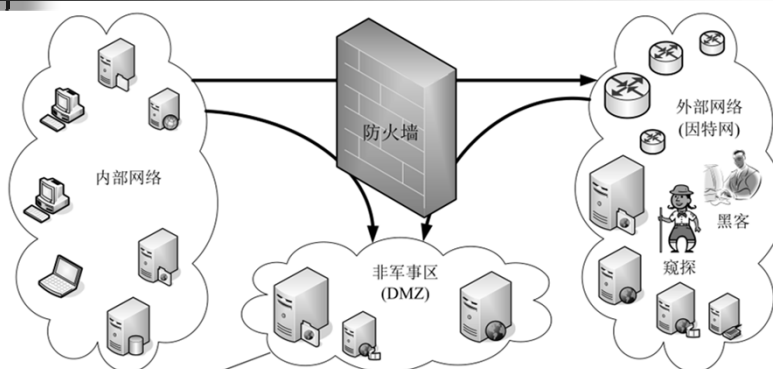
Screened subnet firewall

- **Advantages:**
 - **Three levels of defense to thwart intruders**
 - **The outside router advertises only the existence of the screened subnet to the Internet (internal network is invisible to the Internet)**
 - **The inside router advertises only the existence of the screened subnet to the internal network (the systems on the inside network cannot construct direct routes to the Internet)**

过滤子网体系结构



过滤子网体系结构



为了配置和管理方便，通常将内部网中需要向外部提供服务的服务器设置在单独的网段，这个网段被称为非军事区(DMZ)。DMZ是防火墙的重要概念，在实际应用中经常用到。DMZ是周边网络，位于内部网之外，使用与内部网不同的网络号连接到防火墙，其中部署了Web服务器、ftp服务器、通信服务器等对外提供公共服务。DMZ隔离内外网络，并为内外网之间的通信起到缓冲作用。

https://blog.csdn.net/qz_36119152

混合结构的防火墙

- 不同结构防火墙的组合
 - 使用多堡垒主机；
 - 合并内部路由器与外部路由器；
 - 合并堡垒主机与外部路由器；
 - 合并堡垒主机与内部路由器；
 - 使用多台内部路由器；
 - 使用多台外部路由器；
 - 使用多个过滤子网；
 - 使用双穴主机与过滤子网。

内容提纲

- 1 防火墙概述
- 2 防火墙的工作原理
- 3 防火墙体系结构
- 4 防火墙技术发展趋势
- 5 防火墙的选购和使用

用户对防火墙的要求越来越高

- 网络安全是通过技术与管理相结合来实现的，良好的网络管理加上优秀的防火墙技术是提高网络安全性能的最好选择。随着新的攻击手段的不断出现，以及防火墙在用户的核心业务系统中占据的地位越来越重要，用户对防火墙的要求越来越高

发展趋势

- 为适应Internet的发展，未来防火墙技术的发展趋势为：
 - ✓ 智能化：防火墙将从目前的静态防御策略向具备人工智能的智能化方向发展；
 - ✓ 高速度：防火墙必须在运算速度上做相应的升级，才不至于成为网络的瓶颈；
 - ✓ 并行体系结构：分布式并行处理的防火墙是防火墙的另一发展趋势；

发展趋势

- 为适应Internet的发展，未来防火墙技术的发展趋势为：
 - ✓ 多功能：未来网络防火墙将在保密性、包过滤、服务、管理和安全等方面增加更多更强的功能；（All-In-One技术）
 - ✓ 专业化：电子邮件防火墙、FTP防火墙等针对特定服务的专业化防火墙将作为一种产品门类出现；
 - ✓ 防病毒：现在许多防火墙都内置了病毒和内容扫描功能。
 - ✓ IPv6网络需求：下一代网络的新需求

发展趋势

- 网络的防火墙产品还将把网络前沿技术，如Web页面超高速缓存、虚拟网络和带宽管理等与其自身结合起来。

发展趋势



内容提纲

- 1 防火墙概述
- 2 防火墙的工作原理
- 3 防火墙体系结构
- 4 防火墙技术发展趋势
- 5 防火墙的选购和使用

一、评价标准

115

防火墙的评价标准

- 防火墙的评价标准用于评价一个防火墙的综合性能。主要的评价指标包括：
 - 并发连接数
 - 吞吐量
 - 安全性
 - 稳定性
 - ...

并发连接数（1/5）

- 并发连接数是指防火墙或代理服务器对其业务信息流的处理能力，是防火墙能够同时处理的点对点连接的最大数目。
- 并发连接数反映出防火墙设备对多个连接的访问控制能力和连接状态跟踪能力。

并发连接数（2/5）

- 简单说，并发连接数就是防火墙所能处理的最大会话数量。
- 防火墙里有一个并发连接表，是防火墙用以存放并发连接信息的地方。
 - 并发连接表的大小，就是防火墙所能支持的最大并发连接数。

并发连接数（3/5）

- 并发连接数的增大意味着内存资源的消耗增加
 - 以每个并发连接表项占用300B计算，1000个并发连接将占用 $300\text{B} \times 1000 \times 8\text{bit/B} \approx 2.3\text{Mb}$ 内存空间；
10000个并发连接将占用23Mb内存空间
100000个并发连接将占用230Mb内存空间，
- 如果试图实现1000000个并发连接的产品，产品需要提供2.24Gb内存空间。

并发连接数（4/5）

- 并发连接数的增大应充分考虑CPU的处理能力。
 - CPU的主要任务是把网络上的流量从一个网段尽可能快速地转发到另外一个网段上，并且在转发过程中对此流量按照一定的访问控制策略进行许可检查、流量统计和访问审计等操作。
 - 如果贸然增大系统的并发连接表，势必影响防火墙对连接请求的处理延迟，造成某些连接超时，致使连接报文重发，最后形成雪崩效应，致使整个防火墙系统崩溃。

并发连接数（5/5）

- 物理链路的实际承载能力将影响防火墙发挥出其对海量并发连接的处理能力。
- 由于防火墙通常都部署在Internet出口处，在客户端PC与目的资源中间的路径上，总是存在着瓶颈链路。
 - 瓶颈链路可能是2Mbps专线，也可能是512Kbps乃至64Kbps的低速链路。
- 拥挤的低速链路根本无法承载太多的并发连接，即便是防火墙能够支持大规模的并发访问连接，也无法发挥出其原有的性能。

吞吐量（1/2）

- 网络中的数据是由一个个数据包组成，防火墙对每个数据包的处理要耗费资源。
- 吞吐量是指在保证丢失数据帧的情况下，设备能够接受的最大速率。

吞吐量（2/2）

- 吞吐量的测试方法：
 - 在测试中以一定速率发送一定数量的帧，并计算待测设备传输出去的帧；
 - 如果发送给设备的帧与设备发出的帧数量相等，那么将发送速率提高并重新测试；
 - 如果发送给设备的帧多于设备发出的帧，则适当降低发送速率重新测试，直至得出最终结果。

应用识别及分析能力

- 对应用网关防火墙而言，关键的性能指标不再是网络层吞吐量，而是应用识别及分析。
 - 首先要考察防火墙能够劫持多少种网络应用，其次是应用识别和控制的精细度，如是否支持对应用子功能的识别及控制。另外，应用特征库的更新速度也很重要

安全性

- 防火墙自身的安全性主要体现在自身设计和管理两个方面。
 - 设计的安全性关键在于操作系统，只有自身具有完整信任关系的操作系统才可以谈论系统的安全性。
 - 防火墙自身的安全实现直接影响整体系统的安全性。

稳定性

- 有些防火墙尚未最后定型或经过严格的大量测试就被推向了市场，其稳定性可想而知。防火墙的稳定性可以通过几种方法判断：
 - 从权威的测评认证机构获得。考察产品是否获得更多的国家权威机构的认证、推荐和入网证明，来间接了解其稳定性。
 - 实际调查，这是最有效的办法：考察这种防火墙是否已经有了使用单位、其用户量如何，特别是用户对于产品的评价。
 - 自己试用。在自己的网络上进行一段时间的试用。

高性能

- 高性能是防火墙的一个重要指标，它直接体现了防火墙的可用性。
- 如果由于使用防火墙而带来了网络性能较大幅度的下降，就意味着安全代价过高。
 - 一般来说，包过滤防火墙加载上百条规则，其性能下降不应超过 5 %。

功能灵活

- 对通信行为的有效控制，要求防火墙设备有一系列不同级别，满足不同用户的各类安全控制需求。
 - 对普通用户，只要对 IP 地址进行过滤即可；
 - 如果是内部有不同安全级别的子网，有时则必须允许高级别子网对低级别子网进行单向访问

管理简便

- 网络技术发展很快，各种安全事件不断出现，这就要求安全管理员经常调整网络安全策略。
 - 防火墙的管理在充分考虑安全需要的前提下，必须提供方便灵活的管理方式和方法，这通常体现为管理途径、管理工具和管理权限。
 - 可视化管理

抵抗拒绝服务攻击

- 在当前的网络攻击中，拒绝服务攻击是使用频率最高的方法。
- 很多防火墙本身都存在拒绝服务攻击漏洞。

防火墙标准

■ 国标

序号	标准编号	标准名称	代替标准号	实施日期
1.	GB/T 20281-2020	信息安全技术 防火墙安全技术要求和测试评价方法	GB/T 20010-2005, GB/T 20281-2015, GB/T 31505-2015, GB/T 32917-2016	2020-11-01
2.	GB/T 22240-2020	信息安全技术 网络安全等级保护定级指南	GB/T 22240-2008	2020-11-01
3.	GB/T 25066-2020	信息安全技术 信息安全产品类别与代码	GB/T 25066-2010	2020-11-01
4.	GB/T 25067-2020	信息技术 安全技术 信息安全管理体系审核和认证机构要求	GB/T 25067-2016	2020-11-01
5.	GB/T 28454-2020	信息技术 安全技术 入侵检测和防御系统（IDPS）的选择、部署和操作	GB/T 28454-2012	2020-11-01

二、防火墙产品

防火墙产品

图 2：中国IT安全市场各子市场占比，2013年

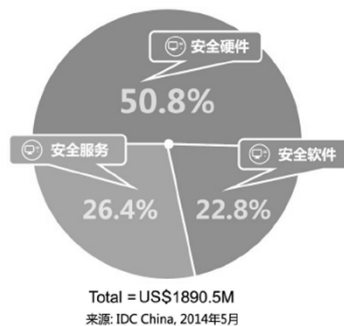
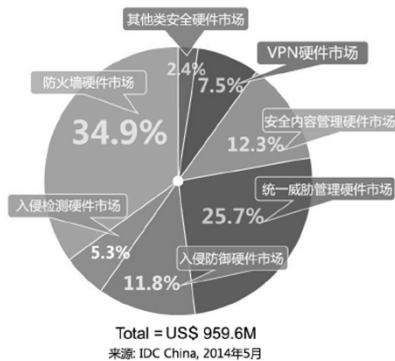
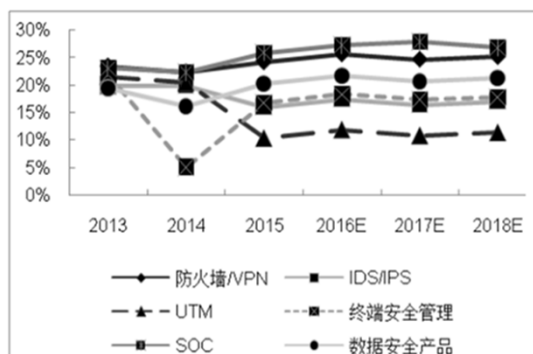


图 3：中国IT安全硬件市场各子市场占比对比，2013年



防火墙产品

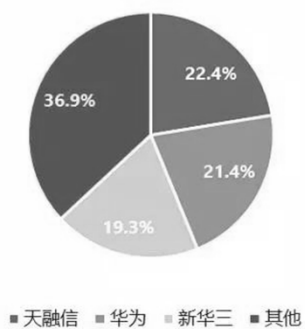


数据来源：公开资料整理

防火墙产品



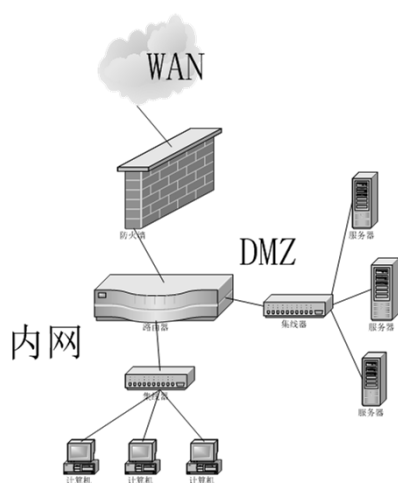
2018年中国防火墙硬件市场份额



三、典型应用

典型应用之一

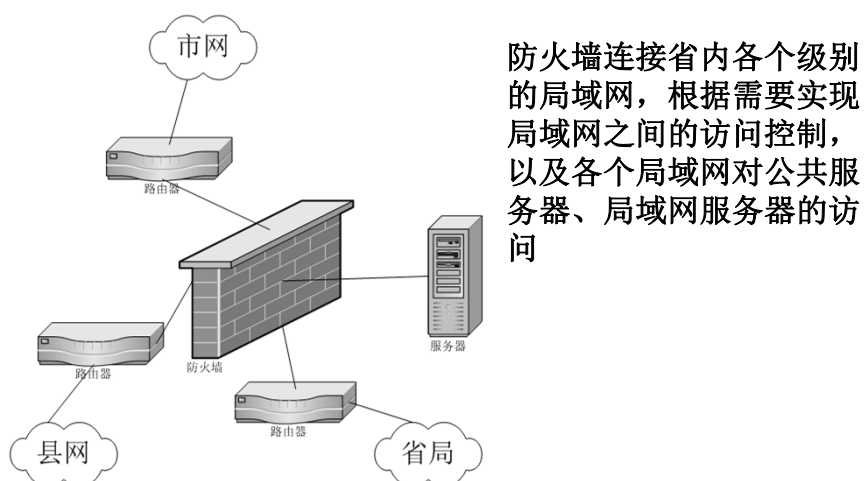
Internet与企业、政府等内部网络之间的应用



防火墙连接WAN和内网，实现内网对Internet的访问，同时实现DMZ区管理，允许WAN和内网对DMZ区服务器的特定的服务端口的访问，根据客户要求允许或禁止DMZ对内网和WAN的访问。

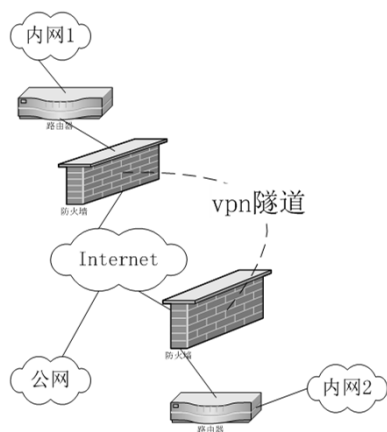
典型应用之二

企业、政府等多个内部网络
中的应用



典型应用之三

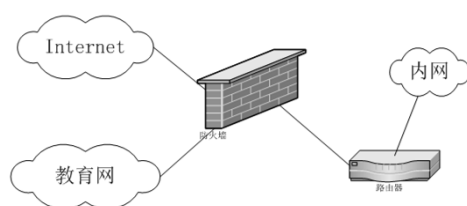
VPN的应用



通过防火墙的隧道VPN和拨号VPN的功能，实现公网对防火墙内部网络的直接访问以及多个防火墙各自的内部网络之间的访问，基于IPsec协议的VPN保证了数据传输的安全性、完整性和高效性。

典型应用之四

双通道以及多通道的实现



通过防火墙的策略路由功能，
实现内网对多个外网的访问，
同时对访问的用户和访问的
服务进行控制

四、工作步骤

创建防火墙的步骤

第一步：制定安全策略

- 内部员工访问互联网的限制
- 外网访问内部网的策略
- 进入公网的数据加密策略

创建防火墙的步骤

第二步：搭建安全体系结构

- 安全策略转化为安全体系结构
 - 对外服务器的配置
 - DMZ的设置

创建防火墙的步骤

第三步：制定规则次序

- 规则先后的次序决定防火墙的功能
 - 防火墙顺序检查规则，一旦匹配，则停止检查并执行这条规则。

创建防火墙的步骤

第四步：落实规则集（12方面）

- 切断默认
- 允许内部出网
- 添加锁定
- 丢弃不匹配的信息包
- 丢弃并不记录
- 允许DNS访问
- 允许邮件访问
- 允许WEB访问
- 阻塞DMZ
- 允许内部的POP访问
- 强化DMZ的规则
- 允许管理员访问

创建防火墙的步骤

第五步：注意更换控制

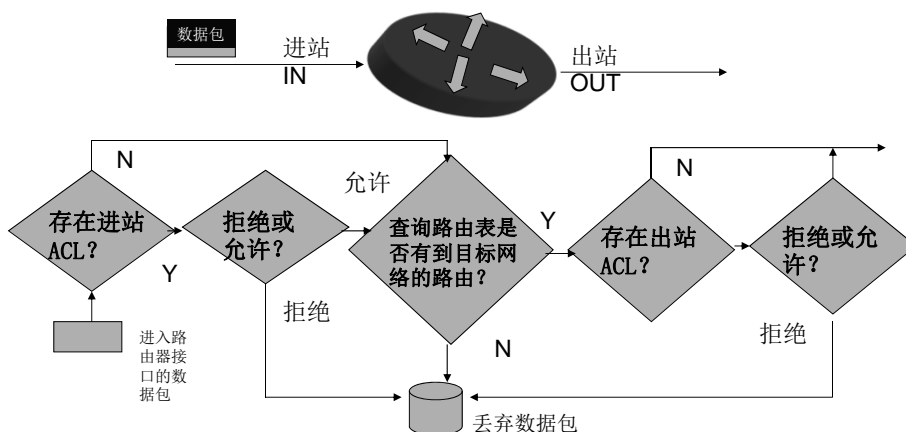
- 规则变动是注释中记录信息
 - 规则更改者的名字
 - 规则变更的日期和时间
 - 规则变更的原因

第六步：审计工作

创建防火墙的步骤

- 规则变动是注释中记录信息
 - 规则更改者的名字
 - 规则变更的日期和时间
 - 规则变更的原因

路由器使用ACL处理数据包的过程



访问控制列表（ACL）分类

- 标准IP ACL：
 - 只对数据包的源IP地址进行检查
 - 其列表号1-90或1300-1999。
- 扩展IP ACL：
 - 对数据包的源和目标IP地址进行检查
 - 源和目标端口号
 - 其列表号100-199或2000-2699

访问控制列表命令格式

命令字

标准IP ACL

访问控制列表编号

对符合匹配的
数据包所采取
的动作

数据包源地址

Access-list Access-list-number (deny/permit) source-address [source-wildcard]

数据包源地址通配符掩码

协议

数据包源地址

■ 扩展IP ACL

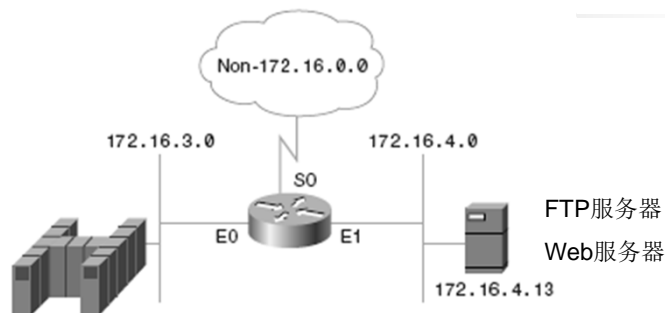
Access-list Access-list-number (deny/permit) protocol source-address source-wildcard [operator port] destination-address destination-wildcard [operator

数据包源地址通配符掩码

逻辑操作：eq、neq、gt、lt、range

判断包头的ACK，若设置，则匹配

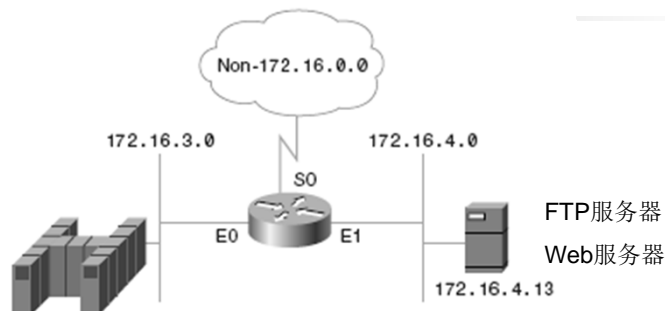
ACL配置实例：允许一个源通信量通过



Permitting traffic from source network 172.16.0.0

```
access-list 1 permit 172.16.0.0 0.0.255.255
interface ethernet 0
ip access-group 1 out
interface ethernet 1
ip access-group 1 out
```


ACL配置：外网只能访问WEB不能访问FTP




```
access-list 110 permit 172.16.3.0 0.0.0.255 host 172.16.4.13 eq 21
access-list 110 permit 172.16.3.0 0.0.0.255 host 172.16.4.13 eq 20
access-list 110 deny any host 172.16.4.13 eq 21
access-list 110 deny any host 172.16.4.13 eq 20
access-list 110 permit any host 172.16.4.13 eq 80
interface ethernet 1
ip access-group 110 out
```



进一步讨论防火墙的不足



防火墙的不足(1/4)

- 防火墙不能防范不经过防火墙的攻击。
 - 传统的防火墙在工作时，入侵者可以伪造数据绕过防火墙或者找到防火墙中可能敞开的后门。
 - 防火墙不能防止来自网络内部的攻击和安全问题
 - 网络攻击中有相当一部分攻击来自网络内部，对于那些对企业心怀不满或假意卧底的员工来说，防火墙形同虚设。防火墙可以设计为既防外也防内，但绝大多数单位因为不方便，不要求防火墙防内。
 - 由于防火墙性能上的限制，因此它通常不具备实时监控入侵的能力。
- 

防火墙的不足(2/4)

- 防火墙不能防止策略配置不当或错误配置引起的安全威胁。
 - 防火墙是一个被动的安全策略执行设备，就像门卫一样，要根据政策规定来执行安全，而不能自作主张。
- 防火墙不能防止受病毒感染的文件的传输。
 - 防火墙本身并不具备查杀病毒的功能，即使集成了第三方的防病毒的软件，也没有一种软件可以查杀所有的病毒。

防火墙的不足(3/4)

- 防火墙不能防止利用服务器系统和网络协议漏洞所进行的攻击。
 - 黑客通过防火墙准许的访问端口对该服务器的漏洞进行攻击，防火墙不能防止。
- 防火墙不能防止数据驱动式的攻击。
 - 当有些表面看来无害的数据邮寄或拷贝到内部网的主机上并被执行时，可能会发生数据驱动式的攻击
- 防火墙不能防止内部的泄密行为。
 - 防火墙内部的一个合法用户主动泄密，防火墙是无能为力的。

防火墙的不足(4/4)

- 防火墙不能防止本身的安全漏洞的威胁。
 - 防火墙保护别人有时却无法保护自己，目前还没有厂商绝对保证防火墙不会存在安全漏洞。因此对防火墙也必须提供某种安全保护。
 - 由于防火墙的局限性，因此仅在内部网络入口处设置防火墙系统不能有效地保护计算机网络的安全，而入侵检测系统(Intrusion Detection System—IDS)可以弥补防火墙的不足

NSA防火墙攻击工具



名称	类型	描述
BANANAGLEE	植入	重启不持续的防火墙植入程序。在Cisco ASA和PIX上运行
BARGLEE	植入	未证实的Juniper NetScreen 5.x防火墙植入程序
BEECHPONY	植入	防火墙植入程序 (BANANAGLEE前身)
BENIGNCERTAIN	工具	从思科PIX防火墙提取VPN密钥
BILLOCEAN	工具	从飞塔Fortigate防火墙（可能有其它）提取序列号
BLATSTING	植入	部署EGREGIOUSBLUNDER 和ELIGIBLEBACHELOR防火墙植入程序
BOOKISHMUTE	漏洞	未知防火墙的漏洞利用
EGREGIOUSBLUNDER	漏洞	飞塔FortiGate防火墙的远端控制设备（RCE）。影响的型号：60、60M、80C、200A、300A、400A、500A、620B、800、5000、1000A、3600和3600A

Equation group victims map

Equus group victims map

THE EQUUS GROUP

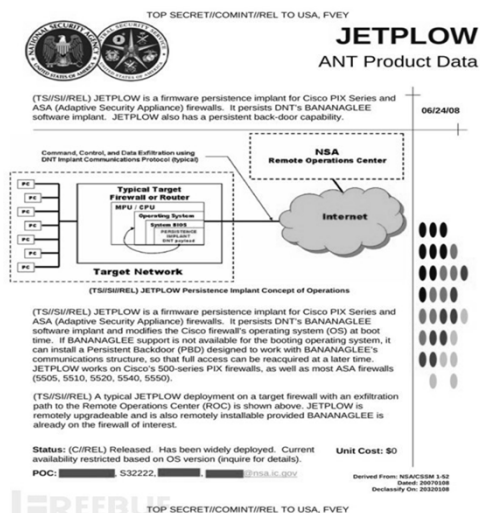
SECRET

名称	类型	描述
ELIGIBLEBACHELOR	漏洞	在TOS操作系统版本3.2.100.010、3.3.001.050、3.3.002.021和3.3.002.030上运行的天融信防火墙漏洞利用
ELIGIBLEBOMBHELL	漏洞	天融信防火墙RCE，影响的版本：从3.2.100.010.1_pbc_17_iv_3到3.3.005.066.1
ELIGIBLECANDIDATE	漏洞	天融信防火墙RCE，影响的版本：从3.3.005.057.1到3.3.010.024.1
EPICBANANA	漏洞	思科ASA特权升级(版本711、712、721、722、723、724、80432、804、805、822、823、824、825、831、832)和思科PIX(版本711、712、721、722、723、724、804)
FEEDTROUGH	植入	Juniper NetScreen防火墙上的持续植入程序，部署BANANAGLEE和ZESTYLEAK
FLOCKFORWARD	漏洞	通过ELIGIBLEBOMBHELL传送现成有效荷载。影响在TOS 3.3.005.066.1上运行的天融信防火墙
POLARPAWS	植入	未知厂商的防火墙植入程序
POLARSNEEZE	植入	未知厂商的防火墙植入程序

牆的
P服

[illegible]

- NSA针对思科PIX系列和ASA防火墙的攻击工具 JETPLOW

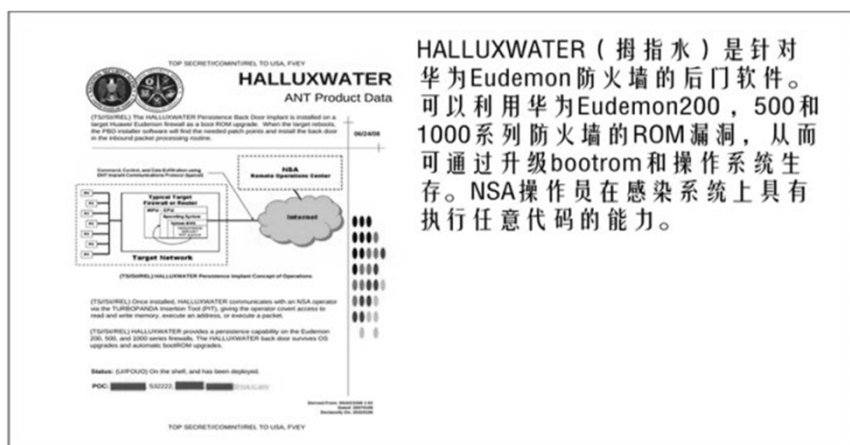


TOP SECRET//COMINT//SI, CIA//SI

HALLUXWATER
ANT Product Data

(CLASSIFIED) The HALLUXWATER Presence Backdoor engine is installed on a target machine (customer based on a base ROM image). When the target initiates the FWI module, the software will find the needed patch points and install the backdoor on the selected patching programming mode.

SECRET

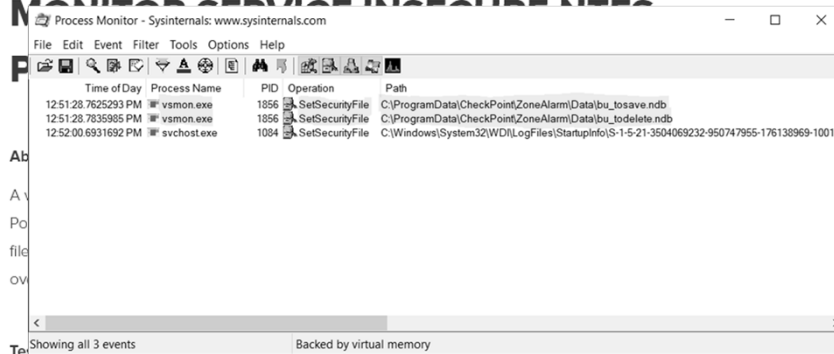


防火墙安全漏洞

ADVISORY Yorick Koster, December 2019

ZONEALARM TRUEVECTOR INTERNET

MONITOR SERVICE INSURANCE



This vulnerability was successfully verified on ZoneAlarm Free Firewall v15.8.023.18219/TrueVector Internet Monitor v15.8.7.18219.

防火墙安全漏洞



ABOUT

Search ...



< BACK

MISC

March 23, 2020 by Kevin Kelpen

VMware NSX-T Distributed Firewall can be bypassed by default

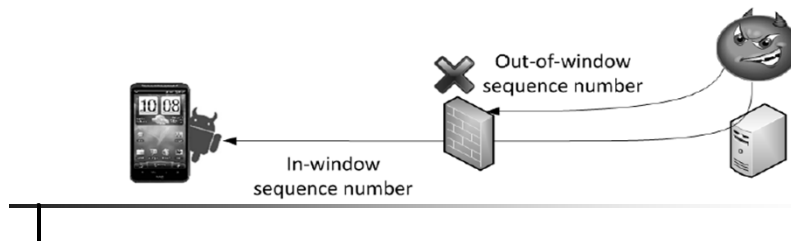
We recently came across an issue when playing around with VMware NSX-T which not anyone might be aware of when getting started with it. Because many of our customers start with transitioning to NSX-T, we want to share this with you. In short, the Distributed Firewall (DFW) of NSX-T can be easily bypassed in the default configuration because it only works effectively if at the same time, the *SpoofGuard* feature is enabled on all logical switch ports which is not the case by default.

防火墙安全漏洞

2012 IEEE Symposium on Security and Privacy

Firewall-enabled side channels

- Sequence-number-checking firewalls
 - Drop out-of-window (likely random or malicious packets)
 - Cut down resource waste and “supposedly” improve security
- However, we turn it into a side channel attack!

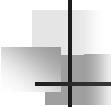


防火墙安全漏洞


2012 IEEE Symposium on Security and Privacy

Popularity of sequence-number-checking firewalls

- 33% of the 179 tested carriers deploy such firewalls
 - Vendors: Checkpoint, Cisco, Juniper
 - Could be used in other networks as well



本章小结



讨论

- 防火墙的未来



作业