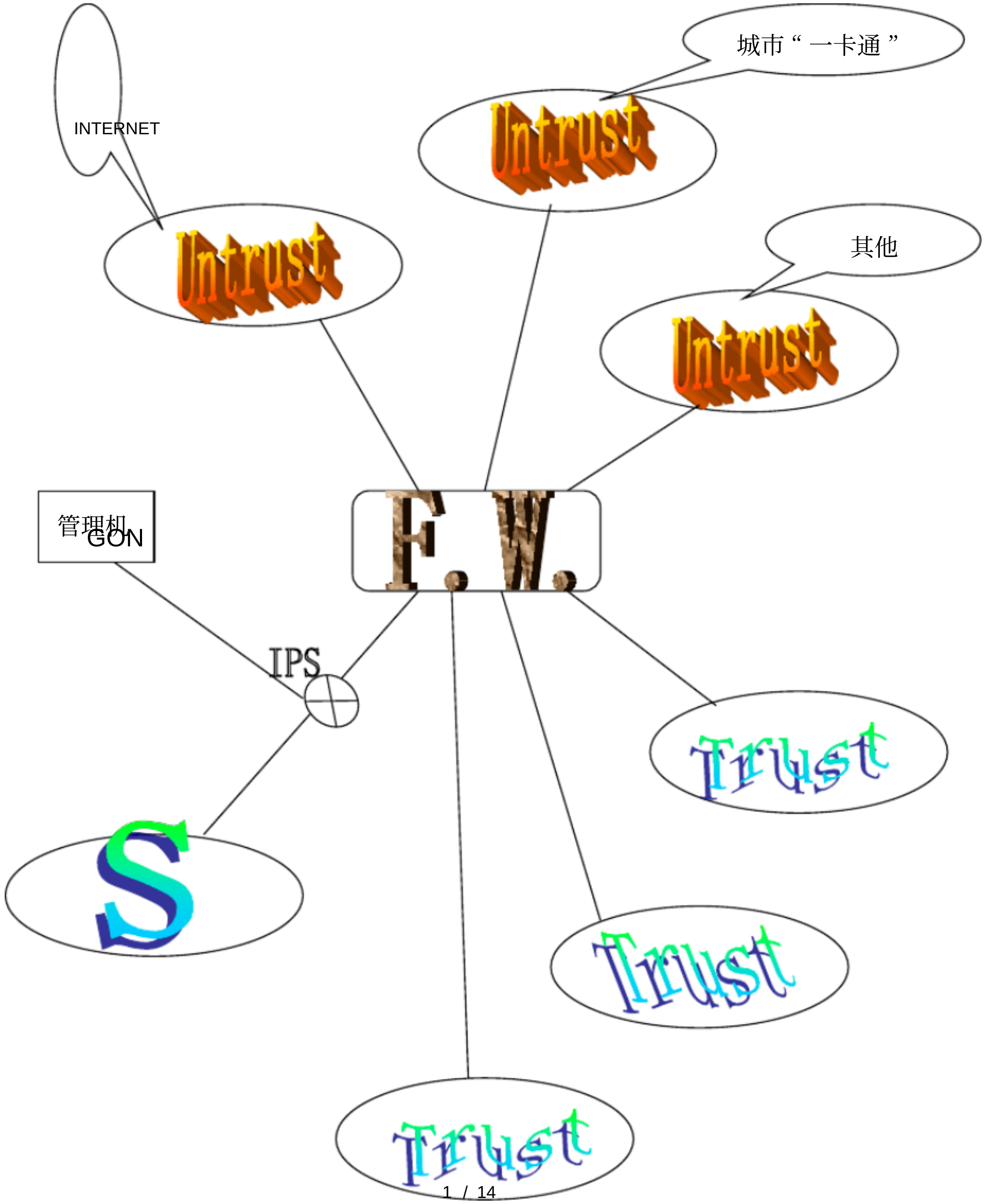
目　　录

网络安全构架原理框图


城市“ 一卡通 ”
INTERNET
Untrust
Untrust
其他
Untrust
管理机
GON
F.W.
IPS
Trust
Trust
Trust

网络防火墙的系统解决方案

随着计算机技术应用的普及， 各个组织机构的运行越来越依赖和离不开计算机，各种业务的运行架构于现代化的网络环境中。

企业计算机系统作为信息化程度较高、 计算机网络应用情况比较先进的一个特殊系统，其业务也同样地越来越依赖于计算机。保证业务系统和工作的正常、可靠和安全地进行是信息系统工作的一个重要话题。 但是由于计算机系统的安全威胁，给组织机构带来了重大的经济损失， 这种损失可分为直接损失和间接损失：直接损失是由此而带来的经济损失，间接损失是由于安全而导致工作效率降低、机密情报数据泄露、 系统不正常、 修复系统而导致工作无法进行等。 间接损失往往是很难以数字来衡量的。 在所有计算机安全威胁中， 外部入侵和非法访问是最为严重的事。

一、 防火墙 概念

Internet 的迅速发展提供了发布信息和检索信息的场所，但也带来了信息污染和信息破坏的危险 ，人们为了保护其数据和资源的安全，部署了 防火墙 。防火墙 本质上是一种保护装置，它保护数据、资源和用户的声誉。

防火墙 原是设计用来防止火灾从建筑物的一部分传播到另一部分的设施。 从理论上讲， Internet 防火墙 服务也有类似目的，它防止 Internet（或外部网络）上的危险（ 病毒、资源盗用等）传播到网络内部。 Internet（或外部网络） 防火墙 服务于多个目的：

1、限制人们从一个特别的控制点进入；
2、防止入侵者接近你的其它防御设施；
3、限定人们从一个特别的点离开；
4、有效地阻止破坏者对你的计算机系统进行破坏。

防火墙 常常被安装在内部网络连接到因特网（或外部网络）的节点上。

（一） 防火墙 的优点

1、防火墙 能够强化安全策略

因为网络上每天都有上百万人在收集信息、 交换 信息，不可避免地会出现个别品德不良，或违反规则的人， 防火墙 就是为了防止不良现象发生的 “交通警察 ”，它执行站点的安全策略，仅仅容许 “认可的 ”和符合规则的请求通过。

2、防火墙 能有效地记录网络上的活动

因为所有进出信息都必须通过 防火墙 , 所以防火墙 非常适用于收集关于系统和网络使用和误用的信息。 作为访问的唯一点， 防火墙 能在被保护的网络和外部网络之间进行记录。

3、防火墙 限制暴露用户点

防火墙 能够用来隔开网络中的两个网段， 这样就能够防止影响一个网段的信息通过整个网络进行传播。

4、防火墙 是一个安全策略的检查站

所有进出的信息都必须通过 防火墙 ，防火墙 便成为安全问题的检查点， 使可疑的访问被拒绝于门外。

（二） 防火墙 的不足

防火墙 的缺点主要表现在以下几个方面。

1、不能防范恶意的知情者

防火墙 可以禁止系统用户经过网络连接发送专有的信息， 但用户可以将数据复制到磁盘、磁带上，放在公文包中带出去。如果入侵者已经在 防火墙 内部，防火墙 是无能为力的。 内部用户可以偷窃数据， 破坏硬件和软件， 并且巧妙地修改程序而不接近 防火墙 。对于来自知情者的威胁， 只能要求加强内部管理， 如主机安全和用户教育等。

2、不能防范不通过它的连接

防火墙 能够有效地防止通过它的传输信息， 然而它却不能防止不通过它而传输的信息。 例如，如果站点允许对 防火墙 后面的内部系统进行拨号访问， 那么防火墙 绝对没有办法阻止入侵者进行拨号入侵。

3、不能防备全部的威胁

防火墙 被用来防备已知的威胁， 如果是一个很好的 防火墙 设计方案， 就可以防备新的威胁，但没有一扇 防火墙 能自动防御所有新的威胁。

4、防火墙 不能防范 病毒

防火墙 一般不能消除网络上的 病毒 。

二、 防火墙 技术

一提到 网络安全人们首先想到的是 防火墙 。 防火墙 系统针对的是来自系统外部的攻击， 一旦外部入侵者进入了系统， 他们便不受任何阻挡。 认证 手段也与此类似，一旦入侵者骗过了 认证 系统，便成为了内部人员。

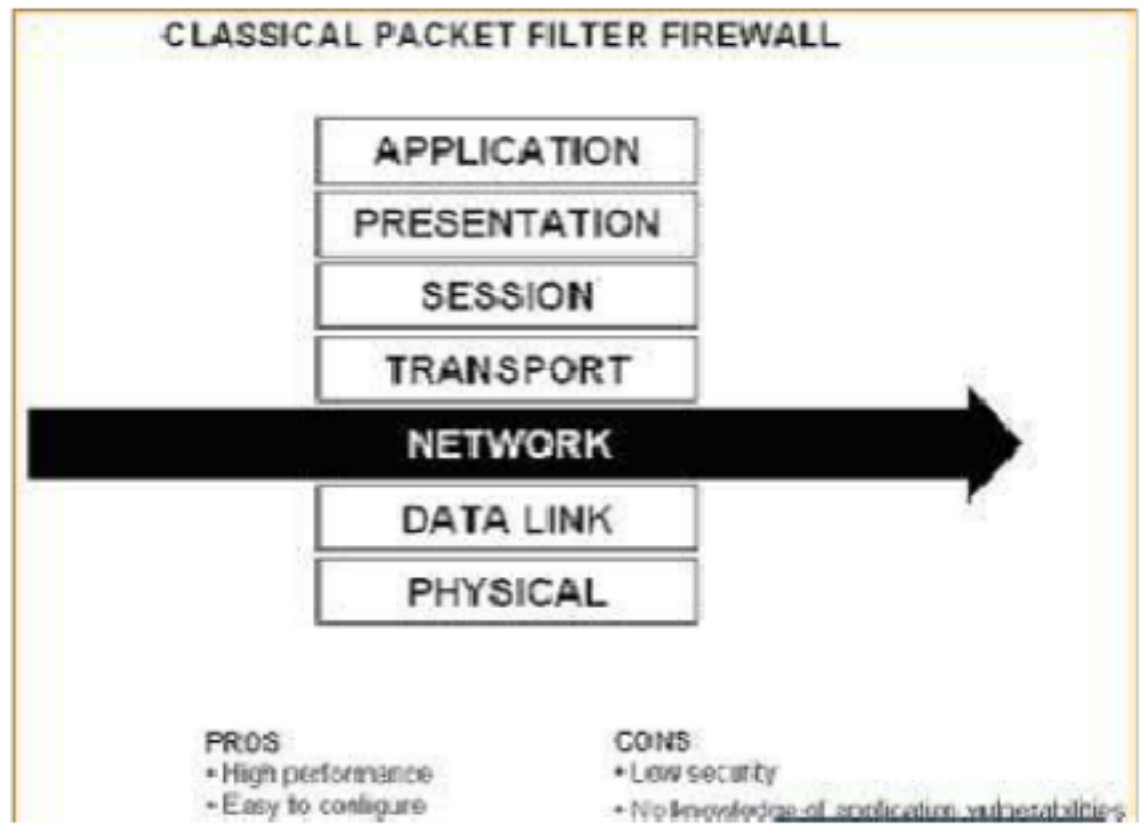
防火墙 的基本类型有： 包过滤型、代理服务型和状态包过滤型复合型 。

（一）包过滤型 防火墙

包过滤（Packet Filter）通常安装在 路由 器上， 并且大多数商用 路由 器都提供了包过滤的功能。 包过滤是一种保安机制， 它控制哪些数据包可以进出网络而哪些数据包应被网络所拒绝。

网络中的应用虽然很多， 但其最终的传输单位都是以数据包的形式出现， 这种做法主要是因为网络要为多个系统提供共享服务。 例如， 文件传输时， 必须将文件分割为小的数据包， 每个数据包单独传输。 每个数据包中除了包含所要传输的数据（内容），还包括源地址、目标地址等。

数据包是通过互联网络中的 路由 器，从源网络到达目的网络的。 路由 器接收到的数据包就知道了该包要去往何处， 然后 路由 器查询自身的 路由 表，若有去往目的的 路由，则将该包发送到下一个 路由 器或直接发往下一个网段； 否则， 将该包丢掉。与 路由 器不同的是， 包过滤 防火墙 ，除了判断是否有到达目的网段的 路由 之外，还要根据一组包过滤规则决定是否将包转发出去。



1、工作机制

包过滤技术可以允许或禁止某些包在网络上传递，它依据的是以下的判断：

对包的目的地址作出判断

对包的源地址作出判断

对包的传送 协议（端口号）作出判断

一般地，在进行包过滤判断时不关心包的具体内容。 包过滤只能让我们进行类似以下情况的操作， 比如：不让任何工作站从外部网用 Telnet 登录、允许任何工作站使用 SMTP 往内部网发电子邮件。

但包过滤不能允许我们进行如下的操作，如：允许用户使用 FTP，同时还限制用户只可读取文件不可写入文件、 允许某个用户使用 Telnet登录而不允许其他用户进行这种操作。

包过滤系统处于网络的 IP 层和 TCP 层，而不是应用层，所以它无法在应用层的具体操作进行任何过滤。以 FTP 为例， FTP 文件传输 协议 应用中包含许多具体的操作，如读取操作、写入操作、删除操作等。再有，包过滤系统不能识别数据包中的用户信息。

2、性能特点

因为包过滤 防火墙 工作在 IP 和 TCP 层，所以处理包的速度要比代理服务型防火墙 快

提供透明的服务，用户不用改变客户端程序

因为只涉及到 TCP 层，所以与代理服务型 防火墙 相比，它提供的安全级别很低

不支持用户 认证，包中只有来自哪台机器的信息却不包含来自哪个用户的信息

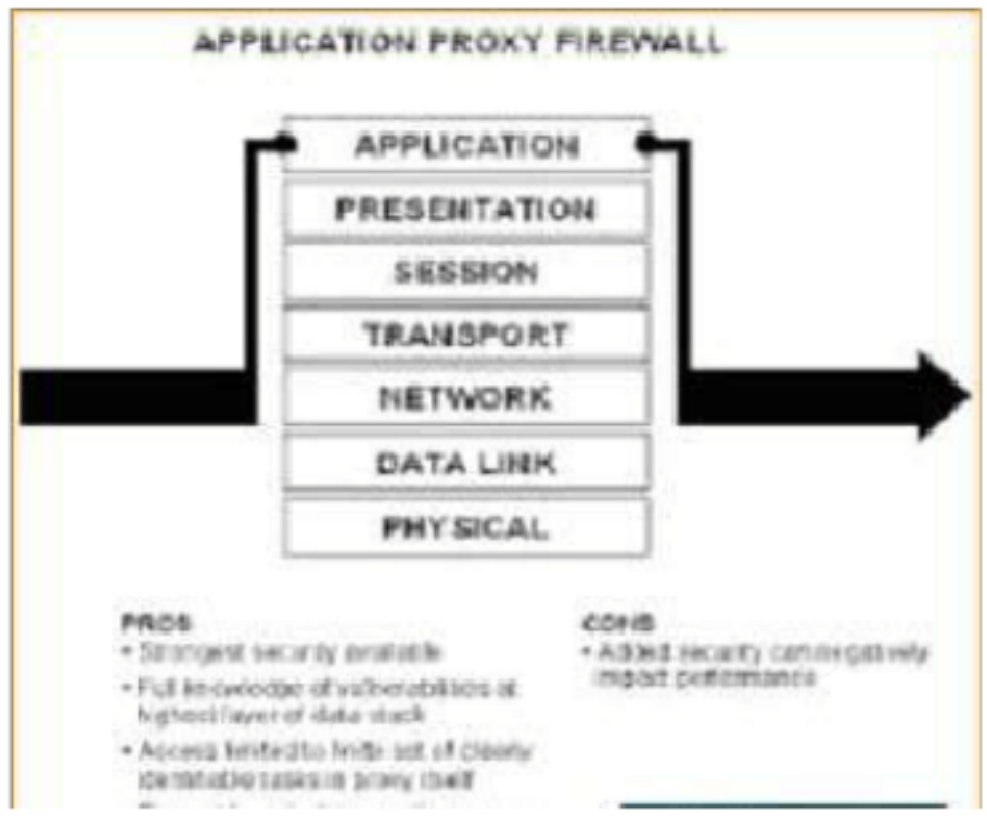
不提供日志功能

包过滤 防火墙 的典型代表是早期的 CISCOPIX 防火墙 。

（二）代理服务型 防火墙

代理服务（ Proxy Service）系统一般安装并运行在双宿主机上。双宿主机是一个被取消 路由 功能的主机，与双宿主机相连的外部网络与内部网络之间在网络层是被断开的。 这样做的目的是使外部网络无法了解内部网络的拓扑。 这与包过滤 防火墙 明显不同，就逻辑拓扑而言，代理服务型 防火墙 要比包过滤型更安全。

由于内部网络和外部网络在网络层是断开的， 所以要实现内外网络之间的应用通讯就必须在网络层之上。 代理系统是工作在应用层， 代理系统是客户机和真实 服务器 之间的中介， 代理系统完全控制客户机和真实 服务器 之间的流量， 并对流量情况加以记录。 目前, 代理服务型 防火墙 产品一般还都包括有包过滤功能。



1、工作机制

代理服务型 防火墙 按如下标准步骤对接收的数据包进行处理：

接收数据包

检查源地址和目标地址

检查请求类型

调用相应的程序

对请求进行处理

下面， 我们以一个外部网络的用户通过 Telnet 访问内部网络中的主机为例, 详细介绍这些标准步骤。

接收数据包

外部网络的 路由 器将外部网络主机对内部网络资源的请求 路由 至防火墙 的外部网卡。 同样， 内部网络中的主机通过内部网络中的 路由 选择信息将对外部网络资源的请求 路由 至防火墙 的内部网卡。

在本例中， 当外部网络用户通过 Telnet 请求对内部网络中的主机进行访问时， 路由 信息将该请求传送至 防火墙 的外部网卡上。

检查源地址和目标地址

一旦 防火墙 接收到数据包， 它必须确定如何处理该数据包。 首先， 防火墙 检查数据包中的源地址并确定该包是由哪块网卡接收的。 这样做是为了确定数据包是否有 IP 地址欺骗的行为， 例如， 如果发现从外部网卡接收的一个数据包中的源地址属于内部网络的地址范围， 则表明这是地址欺骗行为， 防火墙 将拒绝继续对该包进行处理并将此事件记录到日志中。

接下来, 防火墙 对包中的目标地址进行检查并确定是否需要对该包做进一步处理。这一点与包过滤类似, 即检查是否允许对目标地址进行访问。

本例中， Telnet 的目标地址是内部网络的某台主机， 防火墙 是通过外部网卡收到该 Telnet 请求的， 且发现请求包中没有地址欺骗行为， 防火墙 接收了该数据包。

检查请求类型

防火墙 检查数据包的内容 （请求的服务端口号） 并对照 防火墙 中已配置好的各种规则， 以便确定是否向数据包提供相应的服务。 如果 防火墙 对所请求的端口号不提供服务，则将这一企图作为潜在的威胁记录下来并拒绝该请求。

本例中，数据包的内容表明请求服务是 Telnet，即请求端口号为 23 且防火墙 的配置规则是支持这类请求的服务。

调用相应的程序

由于 防火墙 对所请求的服务提供支持， 所以防火墙 利用其他配置信息将该服务请求传送至相应的代理服务。

本例中， 防火墙 将 Telnet 请求传送给 Telnet 代理进行处理。

对请求进行处理

现在代理服务以目的主机的身份并采用与应用请求相同的 协议 对请求进行响应。应用请求方认为它是与目标主机进行对话。

然后，代理服务通过另一块网卡以自己真实的身份代替客户方， 向目标主机发送应用请求。 如果应用请求成功， 则表明客户端至目标主机之间的应用连接成功地建立了。 注意， 与包过滤 防火墙 不同， 代理服务型 防火墙 是通过两次连接实现客户机至目标主机之间的连接的，即客户机至 防火墙 、防火墙 至目标主机。

另外，通过对 防火墙 进行适当的配置， 可以在 防火墙 替客户机向目标主机发送应用请求之前对客户方进行身份验证。验证方法包括 SecureID、S/Key、RADIUS 等。

本例中，客户方现与 防火墙 建立 Telnet 连接，然后防火墙 立即向客户方发出身份验证要求。 若验证通过， 则防火墙 替客户方向目标主机发送应用请求； 否则，防火墙 断开它与客户方已建立的连接。

2、性能特点

提供的安全级别高于包过滤型 防火墙

代理服务型 防火墙 可以配置成唯一的可被外部看见的主机以保护内部主机免受外部攻击

可以强制执行用户 认证

代理工作在客户机和真实 服务器 之间，完全控制会话， 所以能提供较详细的审计日志

代理的速度比包过滤慢

代理服务型 防火墙 中的佼佼者 AXENT Raptor 完全是基于代理技术的软件 防火墙 。

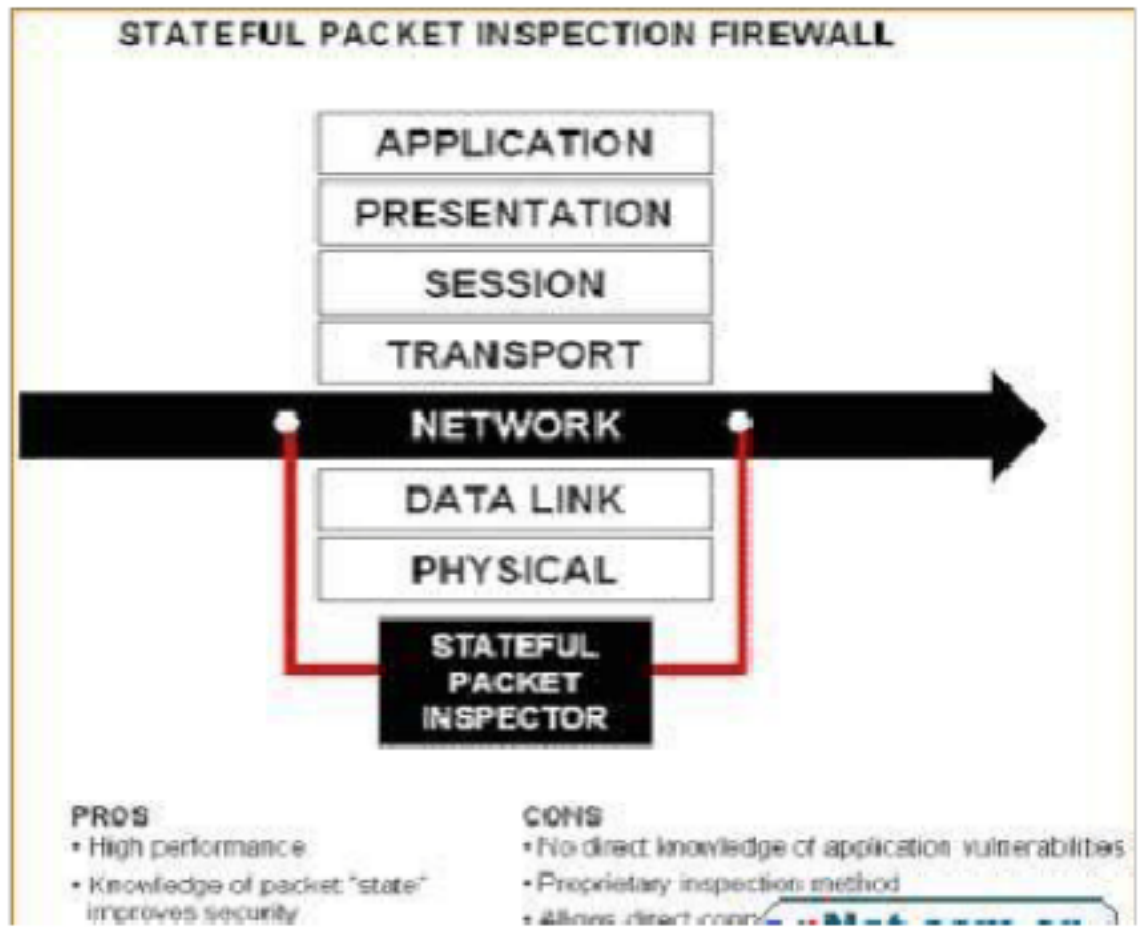
随着因特网络技术的发展， 不论在速度上还是在安全上都要求 防火墙 技术也要更新发展，基于上下文的动态包过滤 防火墙 就是对传统的包过滤型和代理服务型防火墙 进行了技术更新。

（三）状态包过滤型 防火墙

为了克服包过滤模式明显的安全性不足的问题 ，一些包过滤型 防火墙 厂商推出了状态包过滤的概念。 在包过滤技术的基础上， 通过基于上下文的动态包过滤模块检查， 增强了安全性检查。 它不再只是分别对每个进来的包简单地就地址进行检查， 动态包过滤型 防火墙 在网络层截获进来的包， 直到足够的数量， 以便能够确定此试图连接的有关 “状态 ”。然后用 防火墙 系统内核中 “专用的检查模块 ”对这些包进行检查。安全决策所需的相关状态信息经过这个 “专用的检查模块 ”检查之后， 记录在动态状态表中， 以便对其后的数据包通讯进行安全评估。 经过

检查的包穿过 防火墙，在内部与外部系统之间建立直接的联系。

尽管基于上下文的状态包过滤检查的方法明显地提高了安全性，但它仍然无法与应用层代理 防火墙 相比。动态包过滤 防火墙 的典型代表是 CHECKPOINT FIREWAL-1 防火墙 。下图显示的是基于上下文的动态包过滤 防火墙 的逻辑结构。



TCP/IP 的灵活设计和 Internet 的普遍应用为网络 黑客 技术的发展提供了基础，黑客 技术很容易被别有用心或喜欢炫耀的人们掌握，由此 黑客 数量剧增。加之网络连接点多面广， 客观上为 黑客 的入侵提供了较多的切入点。 企业计算机网络中内部网上的信息有许多是属于机密数据， 一旦被不怀好意的 黑客 窃取或被竞争对手得到， 都将带来难以估量的损失。 为了使信息系统在保障安全的基础上被正常访问， 需要一定的设备来对系统实施保护， 保证只有合法的用户才可以访问系统。就目前看，能够实现这种需求的性能价格比最优的设备就是 防火墙 。

本着经济、高效的原则， 有必要将内部网和外部不信任网络、 内部网络中主要的应用 服务器 和内部其它网段用 防火墙 隔离保护，以实现对内部网以及主机系统的访问控制和边界安全的集中管理。

三、 防火墙 方案具体实现

（一）产品选型原则

在进行 防火墙 产品选型时， 除了必须遵循网络安全体系设计原则外， 还要求 防火墙 至少应包含以下功能：

1、访问控制：通过对特定网段和特定服务建立的访问控制体系，将绝大多数攻击阻止在到达攻击目标之前；

2、攻击监控：通过对特定网段、服务建立的攻击监控体系，可实时地检测出绝大多数攻击，并采取相应的行动（如断开网络连接、记录攻击过程、跟踪攻击源等）；

3、加密通讯：主动的加密通讯，可使攻击者不能了解、修改敏感信息；

4、身份 认证：良好的 认证 体系可防止攻击者假冒合法用户；

5、多层防御：攻击者在突破第一道防线后，延缓或阻断其到达攻击目标；

6、隐藏内部信息：使攻击者不能了解系统内的基本情况；

7、安全监控中心：为信息系统提供安全体系管理、监控，保护及紧急情况服务。

在实际的网络中， 保障网络安全与提供高效灵活的网络服务是矛盾的。 从网络服务的可用性、灵活性和网络性能考虑， 网络结构和技术实现应该尽可能简捷，不引入额外的控制因素和资源开销。 但从网络安全保障考虑， 则要求对网络系统提供服务的种类、时间、对象、地点甚至内容有尽可能多的了解和控制能力，实现这样附加的安全功能不可避免地要耗费有限的网络资源或限制网络资源的使用，从而对网络系统的性能、服务的使用方式和范围产生显著影响。此外，保障网络安全常常还涉及到额外的硬件、 软件投入及网络运行管理中的额外投入， 由此可见， 保障网络的安全是有代价的。 对安全性的追求可以是无限的， 但费用也会随之增长。以 防火墙 建立一套安全系统，可充分兼顾以下因素：

1、安全性与方便

一般来说， 网络使用的方便性会因采用了网络安全措施而降低。 防火墙 无论从安装、配置到策略调整都在同一个 GUI 界面下完成，管理十分方便快捷，网络管理员的额外工作强度很小。 此外，防火墙 内外网卡透明设置也极大地方便了内部用户，内部工作站（包括 服务器 ）不必增加任何额外的配置。

2、安全性与性能

对网络来说，安全措施是靠网络资源来完成的，它或者是占用主机 CPU 和内存，或者是占用网络带宽， 或者是增加信息处理的过程， 所有这些都可以导致整体性能降低 防火墙 拥有独特的状态包过滤技术， 在安全性和速度之间可以自动找到理想的平衡点。

3、安全性与成本

采用网络安全措施或建立网络安全系统都会增加额外的成本， 这里包括购买硬件、软件的花费，系统设计和实施费用，管理和维护安全系统的费用。

（二） 防火墙 具体实现

1、部署边界 防火墙

设置边界 防火墙 的正确位置应该在内部网络与外部网络之间。 防火墙 设置在此位置上， 防火墙 的内外网卡分属于内部和外部网段。 内部网络和外部网络被完全隔离开， 所有来自外部网络的服务请求只能到达 防火墙 ，防火墙 对收到的数据包进行分析后将合法的请求传送给相应的服务主机， 对于非法访问加以拒绝。 内部网络的情况对于外部网络的用户来说是完全不可见的。 由于 防火墙 是内部网络和外部网络的唯一通讯信道， 因此 防火墙 可以对所有针对内部网络的访问进行详细的记录， 形成完整的日志文件。 防火墙 要保护的网络与外部网络应该只有唯一的连接通路， 如果 防火墙 后还有其它通路， 防火墙 将被短路， 无法完成保护内部网络的工作。如果内部网络有多个外部连接， 就应该在每个入口处都放置 防火墙 。

设置边界 防火墙 ，我们可以有效的防范来自外部网络的攻击。 设置 防火墙 后内部网与外部网进行了有效的隔离， 所有来自外部网络的访问请求都要通过 防火墙 的检查，安全有了很大的提高。

边界 防火墙 可以完成以下具体任务：

通过源地址过滤，拒绝外部非法 IP 地址，有效的避免了外部网络上与业务无关的主机的越权访问 防火墙 可以只保留有用的服务，将其他不需要的服务关闭，可将系统受攻击的可能性降低到最小限度， 使 黑客 无机可乘边界 防火墙 可以制定访问策略，只有被授权的外部主机可以访问内部网络的有限的 IP 地址，保

证外部网络只能访问内部网络中必要的资源，　与业务无关的操作将被拒绝由于外部网络对 DMZ 区主机的所有访问都要经过　防火墙，防火墙 可以全面监视外部网络对内部网络的访问活动，　并进行详细的记录，　通过分析可以得出可疑的攻击行为对于远程登录的用户，如　telnet 等，防火墙 利用加强的 认证 功能，可以有效的防止非法入侵安装了边界　防火墙 后，网络的安全策略由 防火墙 集中管理，因此 黑客 无法通过更改某一台主机的安全策略来达到控制其他资源访问权限的目的边界 防火墙 可以进行地址转换工作，　外部网络不能看到内部网络的结构，　使 黑客 攻击失去目标以上的内容充分说明，　企业的计算机网络安装了边界　防火墙 后，可以实现内部网络与外部网络的有效隔离，　防止来自外部网络的非法攻击。　同时，保证了 DMZ 区服务器 的相对安全性和使用便利性。

2、部署内部 防火墙

企业的计算机网络是一个多层次、　多节点、多业务的网络，　各节点间的信任程度较低，　但由于业务的需要，　各节点和 服务器 群之间又要频繁的　交换 数据。通过在 服务器 群的入口处设置内部　防火墙，可以制定完善的安全策略，　有效的控制内部网络的访问，具体可以实现以下功能：

内部 防火墙 可以精确制定每个用户的访问权限，　保证内部网络用户只能访问必要的资源对于拨号备份线路的连接，　通过强大的 认证 功能，实现对远程用户的管理内部 防火墙 可以记录网段间的访问信息，　及时发现误操作和来自内部网络其他网段的攻击行为　防火墙 通过安全策略的集中管理，　每个网段上的主机不必再单独设立安全策略，降低人为因素导致的网络安全问题。

综上所述，企业计算机网络中设置　防火墙 后，一方面可以有效地防范来自外部网络的攻击行为，　另一方面可以为内部网络制定完善的安全访问策略，　从而使得整个企业网络具有较高的安全级别。

四、 防火墙 方案特点

一个优秀的网络安全保障系统必须建立在对网络安全需求与环境的客观分析评估基础上，在网络的应用性能及价格和安全保障需求之间确定一个　“最佳平衡点 ”，使得网络安全保障引入的额外开销与它所带来的效益相当。根据企业计算机网络的具体特点，我们建议采用的　防火墙 安全系统具有以下几个特点：

1、设备费用比较低廉

这主要包括，一次性购入成套的安全设备，　利用其配套软件设置来实现安全等级，比如说 防火墙 检测条例设置。

2、人员费用相对较低

无须聘请国外专业的安全公司来参与企业内部网的建设，　但是可以聘请一到两个对于安全规划和实施较有经验的国内专业安全公司定企业内部网的规划，　同时系统的安全性维护主要由内部技术人员兼职完成。

3、统一部署安全策略

即在安全专家的指导下，　建立统一安全制度，　消灭一般由于系统配置不当造成的明显安全漏洞。

4、良好的升级扩展性

一套相对安全的安全系统并不意味着永远保持　“相对的安全性 ”，当企业的关键性业务发展到某个程度时，　或许需要提高企业内部网的安全性能，　这就要求原

先的系统具有良好的可扩展性。 这主要体现在， 可以通过适当地追加投资大幅度增加企业内部网络的安全性能。 但安全系统的基本模式不发生巨大变化， 以免导致管理上的困难

入侵检测

安全扫描通常采用两种策略，第一种是 被动式策略 ，第二种是 主动式策略 。所谓被动式策略就是基于主机之上， 对系统中不合适的设置， 脆弱的口令以及其他同安全规则抵触的对象进行检查； 而主动式策略是基于网络的， 它通过执行一些脚本文件模拟对系统进行攻击的行为并记录系统的反应，从而发现其中的漏洞。利用被动式策略扫描称为系统安全扫描， 利用主动式策略扫描称为网络安全扫描。

一、目前安全扫描主要涉及的检测技术

这里进一步介绍安全扫描的四种检测技术：

① 基于应用的检测技术，它采用被动的，非破坏性的办法检查应用软件包的设置，发现安全漏洞。

② 基于主机的检测技术， 它采用被动的， 非破坏性的办法对系统进行检测。通常，它涉及到系统的内核，文件的属性，操作系统的补丁等问题。这种技术还包括口令解密， 把一些简单的口令剔除。 因此，这种技术可以非常准确的定位系统的问题，发现系统的漏洞。它的缺点是与平台相关，升级复杂。

③ 基于目标的漏洞检测技术，它采用被动的，非破坏性的办法检查系统属性和文件属性，如数据库，注册号等。通过消息文摘算法，对文件的加密数进行检验。这种技术的实现是运行在一个闭环上，不断地处理文件，系统目标，系统目标属性， 然后产生检验数， 把这些检验数同原来的检验数相比较。 一旦发现改变就通知管理员。

④ 基于网络的检测技术，它采用积极的，非破坏性的办法来检验系统是否有可能被攻击崩溃。 它利用了一系列的脚本模拟对系统进行攻击的行为， 然后对结果进行分析。 它还针对已知的网络漏洞进行检验。 网络检测技术常被用来进行穿透实验和安全审记。 这种技术可以发现一系列平台的漏洞， 也容易安装。但是，它可能会影响网络的性能。

优秀的安全扫描产品应该是综合了以上 4 种方法的优点，最大限度的增强漏洞识别的精度。

二、安全扫描在企业部署安全策略中处于重要地位

从前面的介绍可以看出安全扫描在维护计算机安全方面起到的重要作用， 但仅仅装备安全扫描软件是不够的。

现有的信息安全产品中主要包括以下几个部分（安全扫描属于评估部分） ：防火墙，反病毒，加强的用户认证，访问控制和认证，加密，评估，记录报告和预警，安全固化的用户认证，认证，物理安全 。这样，在部署安全策略时，有许多其它的安全基础设施要考虑进来， 如防火墙，病毒扫描器， 认证与识别产品，访问控制产品，加密产品，虚拟专用网等等。 如何管理这些设备，是安全扫描系统和入侵侦测软件（入侵侦测软件往往包含在安全扫描系统中）的职责 。通过监视事件日志，系统受到攻击后的行为和这些设备的信号，作出反应。这样，安全扫描系统就把这些设备有机地结合在一起。 因此，而安全扫描是一个完整的安全解决方案中的一个关键部分，在企业部署安全策略中处于非常重要的地位。

大家可能已经注意到防火墙和安全扫描的同时存在，这是因为防火墙是不够的。防火墙充当了外部网和内部网的一个屏障， 但是并不是所有的外部访问都是通过

防火墙的。 比如，一个未经认证的调制解调器把内部网连到了外部网， 就对系统的安全构成了威胁。 此外，安全威胁往往并不全来自外部， 很大一部分来自内部。另外，防火墙本身也很有可能被黑客攻破。

结合了入侵侦测功能后，安全扫描系统具有以下功能：

① 协调了其它的安全设备；

② 使枯燥的系统安全信息易于理解，告诉了你系统发生的事情；

③ 跟踪用户进入，在系统中的行为和离开的信息；

④ 可以报告和识别文件的改动；

⑤ 纠正系统的错误设置；

⑥ 识别正在受到的攻击；

⑦ 减轻系统管理员搜索最近黑客行为的负担；

⑧ 使得安全管理可由普通用户来负责；

⑨ 为制定安全规则提供依据。不过必须注意，安全扫描系统不是万能的。首先，它不能弥补由于认证机制薄弱带来的问题， 不能弥补由于协议本身的问题；此外，它也不能处理所有的数据包攻击， 当网络繁忙时它也分析不了所有的数据流；当受到攻击后要进行调查，离不开安全专家的参与。

三、网络安全和系统安全主要薄弱环节

要正确部署安全策略、 有针对性的使用安全扫描产品， 有必要了解一下安全的主要薄弱环节在哪里。下面提到的三个问题是产生安全漏洞的主要原因：

① 软件自身安全性差。很多软件在设计时忽略或者很少考虑安全性问题，考虑了安全性的软件产品也往往因为开发人员缺乏安全培训、 没有安全经验而造成了安全漏洞。 这样产生的安全漏洞分为两类： 第一类， 是由于操作系统本省设计缺陷带来的安全漏洞， 这类漏洞将被运行在该系统上的应用程序所继承； 第二类是应用软件程序的安全漏洞。第二类漏洞更为常见，更需要得到广泛的关注。

② 安全策略不当。保证系统安全不是仅仅使用个别安全工具就能做到的，需要在对网络进行总体分析的前提下制定安全策略， 并且用一系列的安全软件来实现一个完整的安全解决方案。 常见的错误例子是使用了防火墙而忽略了扫描系统，或者相反。

③ 人员缺乏安全意识。前面阐述的一切都是在技术层面上对网络安全进行分析和讨论， 所有这一切都需要人来完成。 保证系统的安全， 仅靠安全软件是不够的，同时要注重安全管理人才的培养， 提高安全防范意识， 最终做到安全有效的防范。而当前人员安全意识的培养还远远不够， 在现在的网络环境中， 绝大多数漏洞存在的原因在于管理员对系统进行了错误的配置， 或者没有及时的升级系统软件到最新的版本。

四、安全扫描技术的发展趋势

安全扫描软件从最初的专门为 UNIX 系统编写的一些只具有简单功能的小程序，发展到现在， 已经出现了多个运行在各种操作系统平台上的、 具有复杂功能的商业程序。今后的发展趋势，我们认为有以下几点：

① 使用插件（plugin）或者叫做功能模块技术。 每个插件都封装一个或者多个漏洞的测试手段， 主扫描程序通过调用插件的方法来执行扫描。 仅仅是添加新的插件就可以使软件增加新功能， 扫描更多漏洞。在插件编写规范公布的情况下，用户或者第三方公司甚至可以自己编写插件来扩充软件的功能。 同时这种技术使

软件的升级维护都变得相对简单，并具有非常强的扩展性。

② 使用专用脚本语言。这其实就是一种更高级的插件技术，用户可以使用专用脚本语言来扩充软件功能。 这些脚本语言语法通常比较简单易学， 往往用十几行代码就可以定制一个简单的测试， 为软件添加新的测试项。 脚本语言的使用，简化了编写新插件的编程工作， 使扩充软件功能的工作变得更加容易， 也更加有趣。

③ 由安全扫描程序到安全评估专家系统。最早的安全扫描程序只是简单的把各个扫描测试项的执行结果罗列出来， 直接提供给测试者而不对信息进行任何分析处理。 而当前较成熟的扫描系统都能够将对单个主机的扫描结果整理， 形成报表，能够并对具体漏洞提出一些解决方法， 但对网络的状况缺乏一个整体的评估，对网络安全没有系统的解决方案。 未来的安全扫描系统， 应该不但能够扫描安全漏洞，还能够智能化的协助网络信息系统管理人员评估本网络的安全状况，给出安全建议，成为一个安全评估专家系统。

五、用户选择安全扫描产品应注意的问题

谈到这里，也许有些计算机安全管理人员开始考虑购买一套安全扫描系统，那么，购买此类产品需要考虑哪些方面呢？我们认为以下几点是要注意的：

① 可扩充性。对具有比较深厚的网络知识，并且希望自己扩充产品功能的用户来说，应用了功能模块或插件技术的产品应该是首选。

② 软件升级问题。由于当今应用软件功能日趋复杂化、软件公司在编写软件时很少考虑安全性等等多种原因， 网络软件漏洞层出不穷， 这使优秀的安全扫描系统必须有良好的可扩充性和迅速升级的能力。 因此， 在选择产品时， 首先要注意产品是否能直接从因特网升级、 升级方法是否能够被非专业人员掌握， 同时要注意产品制造者有没有足够的技术力量来保证对新出现漏洞作出迅速的反应。

③ 全面的解决方案。前面已经指出，网络安全管理需要多种安全产品来实现，仅仅使用安全扫描系统是难以保证网络的安全的。 选择安全扫描系统， 要考虑产品制造商能否提供包括防火墙、 网络监控系统等完整产品线的全面的解决方案。

④ 人员培训。前面已经分析过，网络安全中人是薄弱的一环，许多安全因素是与网络用户密切相关的， 提高本网络现有用户、 特别是网络管理员的安全意识对提高网络安全性能具有非同寻常的意义。 因此， 在选择安全扫描产品时， 要考虑制造商有无能力提供安全技术培训。