

第 6 篇 增强网络安全性

第 18 章 增强网络安全性

第18章 增强网络安全性

随着网络技术的发展，网络安全得到了越来越多的重视，在网络建设和维护中，网络安全成为了一个不可或缺的部分。网络安全的范围十分广泛，包括了网络的方方面面。

本章首先对网络安全进行了基础而概括性的阐述，随后着重介绍了增强网络安全的几个主要部分，包括业务隔离、访问控制、认证授权、传输安全 and 安全防御等。

18.1 本章目标

课程目标

学习完本课程，您应该能够：

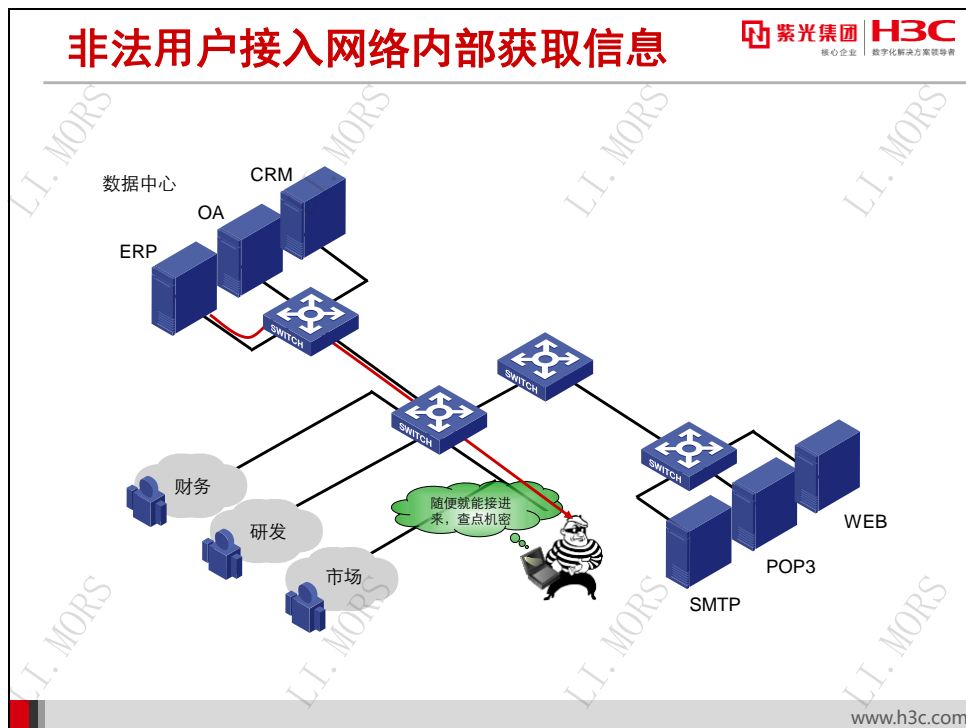
- 了解网络安全的内容
- 理解业务隔离、访问控制和防御网络攻击的手段
- 应用状态检测防火墙技术
- 对网络设备进行安全加固



www.h3c.com

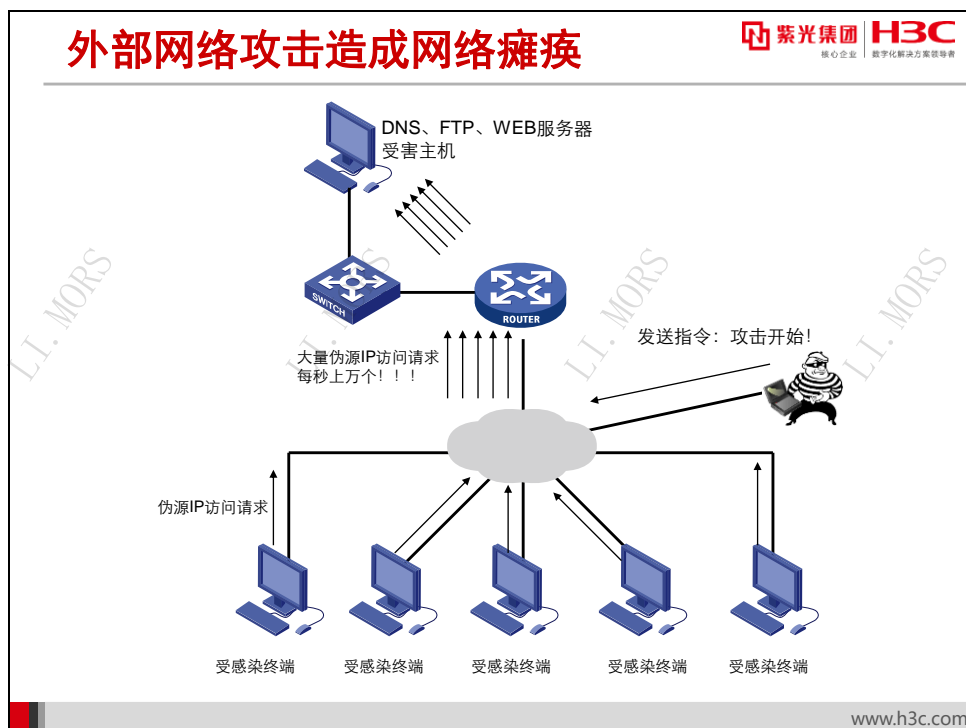
18.2 网络安全概述

18.2.1 网络安全威胁的来源



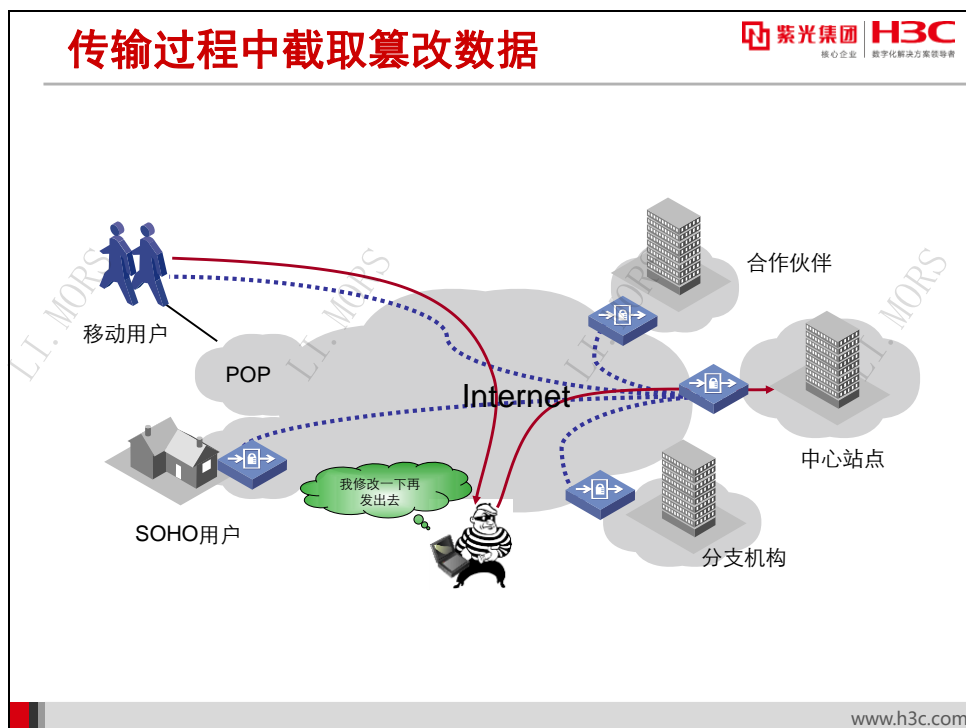
上图是一个非法用户接入网络内部获取信息的案例。某单位的内网信息化程度很高，有线无线的混合组网使单位内部随时随地可以接入网络，但网络上缺乏相应的安全保障手段。一个不怀好意的用户通过有线方式或无线方式轻易的接入内网，攻击服务器获取机密数据并传播病毒木马，发起网络攻击使内网用户无法正常使用网络。

实际上，真正使企业遭受重大损失的安全事件，大部分都是来自于内部。



上图是一个外部网络攻击造成网络瘫痪的案例。某企业的服务器直接连接在 Internet 上对外部人员提供服务（网站，FTP 下载），但缺乏相应的安全保障手段，一个不怀好意的用户通过某些方式在 Internet 上控制一部分缺乏安全保护的主机为己所用，在某一时刻，下达攻击指令，大量的主机发送攻击报文，对这个企业的服务器发起攻击，导致服务器过载，无法正常提供服务。

以破坏阻断正常服务为目的的大规模网络攻击让网络管理人员越来越头疼。



上图是一个传输过程中截取篡改数据的案例。某企业的分支机构和总部之间通过 Internet 互联，但缺乏相应的安全保障手段，分支单位到总部的数据直接在 Internet 上传播，一个不怀好意的用户通过某些方式在 Internet 上截取监听这些数据，并伪造相应的报文发送给总部或者分支机构，骗取对方信任，获取机密的数据。

分支机构和总部之间的远程网络连接不得不借助 Internet 的网络资源，而如何在 Internet 这个不安全的网络环境上安全的传输数据成为了网络管理人员需要考虑的问题。

网络安全威胁的来源

紫光集团 H3C
核心企业 数字化转型领导者

- 按照网络安全威胁存在的位置来划分：

- 来自于网络内部的安全威胁
- 来自于网络外部的安全威胁
- 来自于数据传输过程中的安全威胁

- 从网络层次、业务或应用角度来分析：

- 来自于设备自身物理上安全威胁
- 来自于网络层的安全威胁
- 来自于应用层的安全威胁
- 来自于病毒的安全威胁
- 来自于安全制度漏洞带来的威胁

www.h3c.com

按照网络安全威胁存在的网络位置，其可以分为以下几类：

- 来自内网的安全威胁；
- 来自外网的安全威胁；
- 来自传输过程中的安全威胁。

如果从网络层次、业务或应用角度来分析，网络安全威胁的来源可以分为以下几类：

- 来自于设备自身物理上安全威胁；
- 来自于网络层的安全威胁；
- 来自于应用层的安全威胁；
- 来自于病毒的安全威胁；
- 来自于安全制度漏洞带来的威胁。

18.2.2 网络安全范围

网络安全关注的内容

- 有效的访问控制
- 有效识别合法的和非法的用户
- 有效的防伪手段，重要的数据重点保护
- 内部网络的隐蔽性
- 外网攻击的防护
- 内外网病毒防范
- 行之有效的安全管理手段

紫光集团 H3C
核心企业 数字化解决方案领导者
www.h3c.com

在进行网络安全防护的时候都需要关注的内容包括：

- **有效的访问控制：**控制每一个用户的访问权限，确保每一个用户仅仅能够访问自己所必须访问的网络资源。
- **有效识别合法的和非法的用户：**如何鉴别用户的合法性，防止非法用户接入网络，针对于用户接入的手段多种多样，需要采取不同的鉴别用户方法。
- **有效的防伪手段，重要的数据重点保护：**在数据传输过程采取加密和防伪措施，防止数据被截取和恶意篡改伪造数据，在网络中，对最重要的部分（如服务器区域）加强安全防御措施。
- **内部网络的隐蔽性：**面对外部网络，尽量屏蔽内部网络信息，断绝从外部主动向内部网络发起攻击的可能。
- **外网攻击的防护：**对于外网对内网发起的攻击部署相应的防御手段，使内网免受外网的攻击。
- **内外网病毒防范：**如今，能够自我复制、自动传播的蠕虫病毒对网络的危害越来越大，如何防止病毒通过各种途径进入网络和控制病毒在网络中的传播，以及减轻病毒发作时带来的危害是网络安全需要考虑的重要内容。
- **行之有效的安全管理手段：**仅仅依靠各种技术手段来实现网络安全是远远不够的，需要通过提高安全防范意识，制定安全规范制度，及时发现和弥补安全漏洞，来不断完善整个网络的安全防护体系。

访问控制

- **基于数据流的访问控制**
 - 根据数据包信息进行数据分类
 - 不同的数据流采用不同的策略
- **基于用户的访问控制**
 - 对于接入服务用户，设定特定的过滤属性

访问控制的方法主要包括：

- **基于数据流的访问控制：**访问控制最基本的应用方式，根据数据流中的信息，比如源地址、目的地址、源端口、目的端口等等，来决定这条数据流是否允许通过，此类应用实现简单，但是在用户接入地址频繁发生变化的场景下，针对性略差。
- **基于用户的访问控制：**根据用户的接入信息，决定这个用户能够访问的网络资源有哪些。此类应用实现复杂，需要多个组件配合完成，但因为是面对用户的访问控制，针对性较强。

如果将这两种方法结合起来使用，安全性会大为提升。

用户识别

紫光集团 H3C
核心企业 数字化解决方案领导者

- 对接入用户的认证
 - 内网接入用户的认证和授权
 - 远程接入用户的认证和授权
- 网络设备本身的认证
 - 访问设备时的身份认证授权
 - 路由信息的认证

www.h3c.com

用户识别可分为两个部分来看：

- **对于接入网络的用户认证：**用户是使用网络资源的主体，用户的接入存在很大的不确定性，不确定什么用户接入，不确定用户从哪里接入，我们认为接入网络的用户属于不可信任的单元，接入的用户有可能是非法用户，也有可能是合法的用户但携带有病毒等危险程序，这样的用户都会对网络的健康稳定运行造成威胁。

对于接入的每一个用户，都应进行认证，不仅要验证这个用户是否是合法用户，还要判断他对网络的安全威胁程度有多高，同时，需要本着每个用户仅能访问自己所需的资源的原则，根据用户的信息对用户进行授权，允许该用户访问其必须的资源。

- **对于登录网络设备的用户认证：**网络设备是构成整个网络的基础，网络设备的安全得不到保证，则整个网络的基础就会被动摇，整个网络的安全也就无法谈起。

对于登录网络设备的用户也应进行认证和授权，认证每一个用户的合法性，根据用户的情况授予不同的设备操作权限，每一个用户仅仅拥有他所必须的权限，在安全要求更为严格的环境中甚至要对用户的每一个操作动作都进行认证。

数据加密和防伪

紫光集团 H3C
核心企业 数字化转型领导者

- 数据加密

- 利用公网传输数据不可避免地面临数据窃听的问题
- 传输之前进行数据加密，保证只有与之通信的对端能够解密

- 数据防伪

- 报文在传输过程中，有可能被攻击者截获、篡改
- 接收端需要进行数据完整性鉴别

www.h3c.com

数据加密和防伪主要是用于 Internet 传输数据时的安全保护。

利用 Internet 传输数据的时候，安全性是必须考虑的，在公网上传输数据的时候，数据是否被他人截取是在我们控制之外的事情，因此需要必要的手段来防止数据被截取后让他人了解到数据的内容。数据加密就是通过一系列的算法和协议来保障经过本端加密的数据只能由对端解开的一种安全手段。

在公网传递数据的时候，数据报文除了被有可能被他人截获外，还可能被他人进行篡改伪造，攻击者可以利用篡改后或伪造的数据报文对远端主机进行欺骗，从而达到自己的目的（比如让自己的终端冒充远端终端接入到核心网络中）。因此在一方面要对传输的数据进行加密，另一方面要能够辨别传送来的数据是否真实，是否被修改过。数据防伪就是通过一系列手段来辨别数据在传输过程中是否有被篡改，来辨识数据的真实性。

内部网络的隐蔽性、攻击防护和病毒防范

紫光集团 H3C
核心企业 数字化转型领导者

● 内部网络的隐蔽性

- 隐藏私网内部地址，有效的保护内部主机
- 允许内网用户向外发起连接，禁止外网用户对内网发起连接

● 攻击防护

- 对外网各类攻击的有效防护

● 病毒防范

- 对于外网病毒传入的防范
- 对于内网病毒发作的抑止

www.h3c.com

为了保障内部网络不受到来自外网的恶意攻击，最好的方法是将内网的信息完全屏蔽，让内外网的路由中断，仅允许内网用户单向的向外发起连接，这样外网就无法了解到内网的任何信息，也就无法主动向内网发起攻击，从而起到了保护内网主机的作用。

现今的网络上，网络攻击频发，病毒泛滥严重。在网络安全关注范围中，攻击的抵御和病毒的防范是一个重要的部分。

对于一个网络来说，绝大部分的攻击都是来自于外网，攻击的类型也多种多样，有利用系统安全漏洞的攻击，有利用畸形报文的攻击，有针对系统资源的消耗类攻击，还有利用大流量堵塞网络出口的攻击，因此在攻击抵御的时候，要面面俱到，可以防御各类的攻击，同时由于攻击的方式会不断发展，整个攻击抵御体系和制度也要有足够的发展空间，能够及时发现攻击方式的变化并改进抵御手段。

病毒既可能来自于外网，也可能来自于内网，因此病毒的防御要双管齐下。一方面，阻止病毒进入网络；另一方面，需要对于内网中出现的病毒发作事件能够及时察觉到，同时能够将病毒发作的危害降低到最小，抑止病毒的蔓延。

安全管理

紫光集团 H3C
核心企业 数字化解决方案领导者

- 保证重要的网络设备处于安全的运行环境，防止人为破坏
- 保护好访问口令、密码等重要的安全信息
- 在网络上实现报文审计和过滤，提供网络运行的必要信息
- 制定完善的管理制度，并确保制度得到良好的执行

www.h3c.com

我们常说网络安全是三分技术，七分管理，由此可见管理的重要性。安全管理涉及方方面面，包括，对设备，场地，人员，流量，内容，制度的管理。

以下几个方面在进行安全管理时需要考虑：

- 对于设备和场地的管理，确保设备、线路物理上的安全，不会被盗，被破坏。
- 对于各类安全信息的管理，比如设备/系统的地址，设备/系统的登录用户名/密码信息，设备/系统的超级管理员口令等等安全信息需要妥善保管，控制其传播范围，对于密码等信息还需要定期修改，提高安全性。
- 对于网络流量的管理，对网络上的流量进行分析，及时发现异常情况，对网络上的流量内容进行分析管理，以便于了解每一个用户的每一个行为，在出现安全事件后有据可查。

制定完善的安全管理制度，包括：

- 有完善的处理流程，保证安全事件能够得到有效快速的处理。
- 有着完善的奖惩制度，保障对于安全制度的改进完善做出贡献的人员进行奖励，对于违反安全制度的人员进行惩罚。

18.2.3 安全网络构成

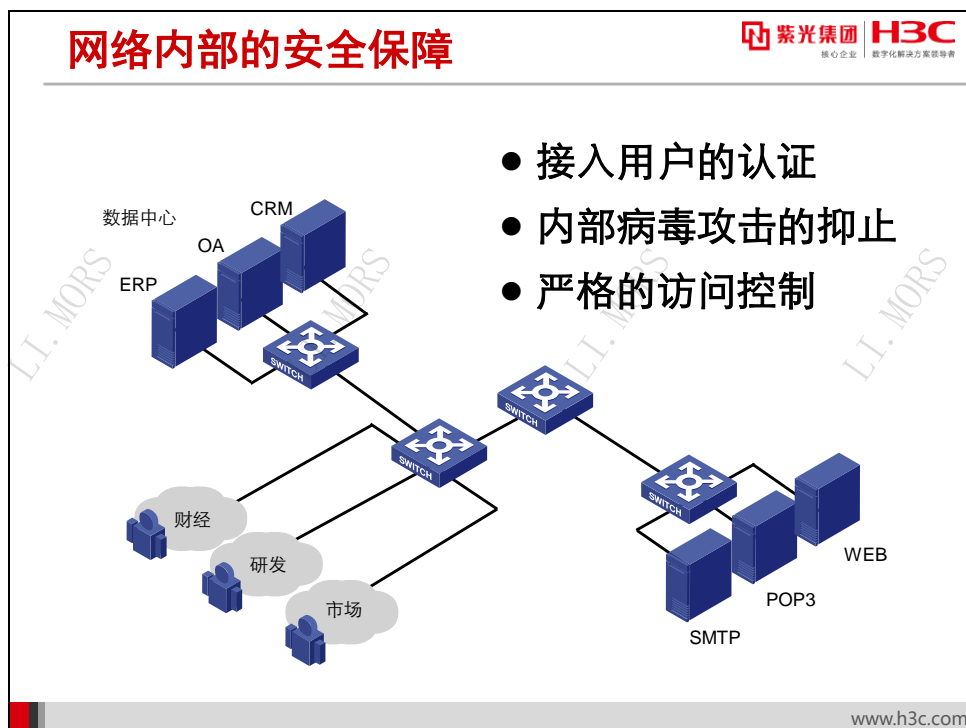
安全网络需要具备的条件

- 能够确保网络内部用户的安全接入，控制内部用户的访问权限
- 能够防范来自外部的攻击等安全威胁
- 能够确保传输过程中的数据安全
- 整个网络拥有完善的安全管理制度

紫光集团 H3C
核心企业 数字化转型领导者
www.h3c.com

从整个网络结构上的划分来看，构建一个安全的网络需要满足以下要求：

- **网络内部的安全：**确保接入内部网络的用户都是安全的，控制内部用户的访问权限，以便于构建一个安全的内部网络环境，同时防止合法的用户获取权限外的信息。
- **对外的安全防御：**在确保了网络内部安全的情况下，安全的威胁主要来自于外部，在构建安全网络的时候，需要充分考虑对于外部安全威胁（攻击、病毒等）的威胁。
- **传输过程中的安全：**在某些情况不可避免要通过 Internet 传送部分业务数据，这时候就需要考虑使用相应的手段来保护数据在传输过程中的安全，防止被他人窃取和篡改。
- **完善的安全管理制度：**只有依靠完善的管理制度，才能够及时发现和分析网络上新出现的攻击事件，完善本网络的安全防御体系；打击对网络的恶意攻击和漏洞探测，以减少网络攻击的发生。



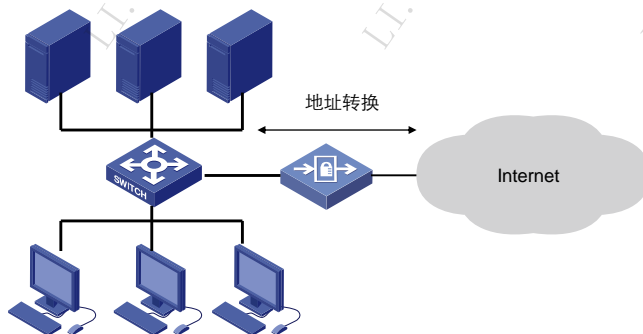
网络内部的安全保障措施主要有以下方面：

- **接入用户的认证：**对于每一个接入用户，无论是直接接入的用户还是通过 VPN 从外网接入的用户，都要进行认证，不仅仅要验证用户的合法性，还要验证用户的安全性，确保每一个接入网络的用户（无论什么接入方式）都是合法，而且是安全的。
- **内网病毒攻击的抑止：**对于异常带入内网的病毒发作时，需要进行抑止，降低病毒发作对网络的影响，减少病毒传染的范围。
- **严格的访问控制：**建议按照最小权限原则对用户进行授权，每一个用户仅能够访问自己所必须的资源，以防止合法用户获取与自身权限不符的信息。

安全接入Internet

紫光集团 H3C
核心企业 数字化解决方案领导者

- 网络出口启用相应的安全防护手段
- 通过地址转换访问Internet，通过地址转换向外提供WWW、FTP等服务



www.h3c.com

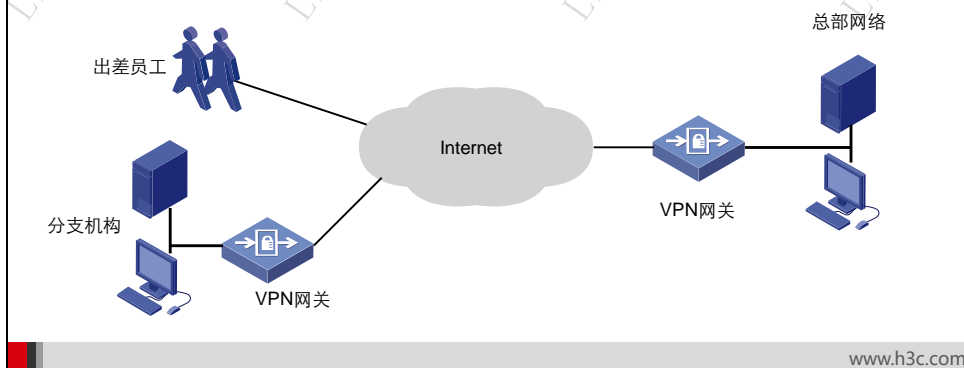
接入 Internet 的安全保障措施主要有以下方面：

- **网络出口启用相应的安全防护手段：**在网络和 Internet 互联的接口上，部署安全防护手段，需要防御外网来的各类网络攻击，防止网络攻击对内网产生影响，需要阻止各类病毒、木马进入内网。
- **通过地址转换访问 Internet：**建议通过地址转换来实现内网对外网的访问，利用地址转换中断内外网的路由联系，使外网不能直接访问内网，对内网进行保护。
- **通过地址转换向外提供 WWW、FTP 等服务：**在需要对外提供服务的时候，考虑采用 NAT 转换方式，把内部服务器的地址映射为外网的地址。

数据传输的安全

紫光集团 H3C
核心企业 数字化转型领导者

- 出差员工通过当地ISP接入到Internet，进而通过VPN接入公司总部
- 办事处及分支机构通过隧道实现与总部的互联，所有的数据均被加密传送



数据传输的安全保障措施主要有以下方面：

- 出差员工通过 VPN 接入公司：出差员工不要直接通过公网发送业务数据到公司，采用 VPN 技术和公司建立隧道，利用加密和防伪技术对业务数据进行处理后，再和公司进行数据交互，防止业务信息被他人截获或篡改。
- 分支机构通过隧道技术安全接入到公司总部：公司的分支机构和公司总部之间通过公网相连的时候，采用 VPN 技术建立隧道，利用加密和防伪技术对业务数据进行处理后，再进行数据交互，防止业务信息被他人截获或篡改。

完善安全管理制度

紫光集团 H3C
核心企业 数字化转型领导者

● 完善的安全管理制度要满足以下条件

- 对于日常工作中遇到的各个方面的安全相关内容，事无巨细，均设定明确的安全要求
- 对于遵守和违反安全制度的行为有着奖惩制度
- 安全制度本身能够不断更新完善

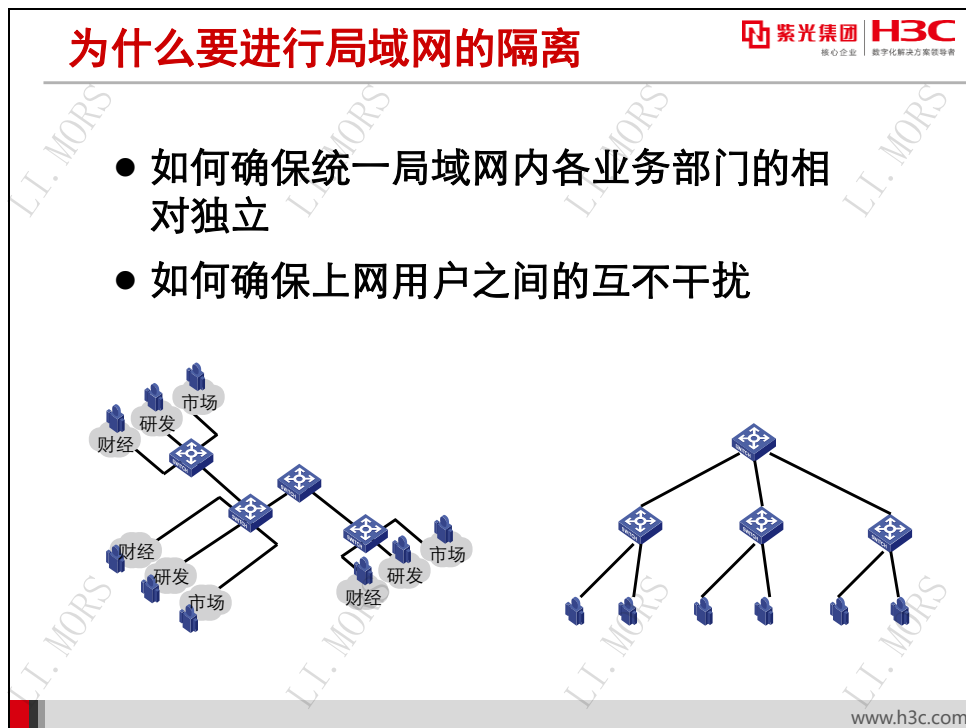
www.h3c.com

完善的安全管理制度主要有以下方面：

- 对于日常工作中遇到的各个方面的安全相关内容，事无巨细，均设定明确的安全要求，让用户的每一个操作都有着规定可以依据，减少给人可以利用的制度漏洞。
- 对于遵守安全制度，主动上报制度漏洞的行为要加以表彰，有着明显的正相引导作用，引导用户遵守制度，主动参与到制度完善的工作中，形成良性循环。
- 对于恶意违反安全规定的行为，要严加惩处，使用户违反安全规定的代价远大于所获得的利益，务必使人不敢轻易违反安全规定，减少用户攻击网络的次数。
- 安全制度本身能够不断更新完善，定期的审视制度本身是否存在漏洞，不断的完善制度，不断根据技术发展更新制度。

18.3 业务隔离

18.3.1 局域网业务隔离



我们来看一下下面两个案例：

- 案例一：某公司内所有的部门同处于一个局域网中，出于安全的考虑，如何能够让不同部门的用户能够互不干扰，如何让各个部门的业务互相隔离？
- 案例二：在某小区，用户通过以太网接入，如何能够防止各个用户直接的互相干扰？如何在保证所有人都能够正常访问 Internet 资源的同时互相隔离？

在这两个案例中，要想达到要求，都需要使用各种局域网的业务隔离手段来满足需求。

局域网业务隔离技术

紫光集团 H3C
核心企业 数字化转型领导者

- 局域网的业务隔离最常用的方式是使用 VLAN 隔离
- VLAN 的扩展技术也是常用手段，如：
 - PVLAN
 - Super VLAN
 - 混合端口

www.h3c.com

局域网业务隔离手段大多是基于 VLAN 技术的。

最常用的局域网业务隔离手段就是使用 VLAN 进行业务隔离。在案例一中，我们可以通过将不同部门的用户分别划到不同的 VLAN 中，不同部门的用户从二层上就被隔离开了，如果一个部门爆发病毒或出现网络攻击，影响范围就局限在一个 VLAN 中，不会影响到其他部门的用户。部门间的数据互访也都要经过三层网关，在三层网关上可以进行互访的控制。

VLAN 技术的一些扩展技术也用于局域网的业务隔离，比如 PVLAN、Super VLAN、hybrid 端口功能。在案例二中，可以通过部署 PVLAN，可以将各个下行接用户的接口相互隔离开，同时所有用户接口都可以和上行的出口互通，这样就既保证了所有人都能够正常访问 Internet 资源，又保证了所有人两两互相隔离的需求。

在一些需求比较复杂的情况下，就需要组合使用 VLAN、PVLAN、Super VLAN、hybrid 端口这几项技术才能达到要求。

18.3.2 广域网业务隔离



我们来看以下两个案例：

- 案例一：某公司的分支机构和公司总部通过 Internet 相连，双方通过公网相互传递业务数据，如何在 Internet 上传输数据的时候不保持数据的独立性，不受到他人的干扰？
- 案例二：在某大型城市综合网络平台上，各个单位均通过该平台互联，各个单位内部内部联系密切，各个系统之间则需要安全隔离，同时各个系统在该城市内部都有着大量的分支机构。如何在同一个网络平台上既保证系统内部的通信正常又保证系统间的安全隔离？

这些案例中都需要使用各种广域网的业务隔离手段来满足需求。



广域网的业务隔离技术中常用的一种技术是使用专线进行业务的物理隔离。即为每个部门或每种业务配置单独的物理线路。

由于专线是独立的线路，带宽是能够独享的，完全能够得到保证；专线业务不和其他业务共享链路，业务的独立性能得到物理上的保障，在各类隔离技术中有着最高的安全性。

在拥有了最高的安全性和最好的带宽保障同时，专线由于需要使用单独的物理资源，因此成本也是最高的。

在分支机构和公司总部相连的时候，如果对于带宽的独享和安全性要求很高的情况下，一般会采用专线方式相连。如银行的总行和分行之间，各个大公司的总部和各大办事处之间一般都采用专线方式，确保自己的业务的独立性，和其他的 Internet 流量隔离开。

广域网业务隔离技术——逻辑隔离

紫光集团 H3C
核心企业 数字化转型领导者

- 广域网的业务隔离可以采用VPN技术来实现，即为每个部门或每种业务配置单独的隧道。
- 隧道种类包括：
 - 二层隧道技术主要有VDPN
 - 三层隧道技术主要有GRE和IPSec
 - 全网状隧道主要有MPLS-VPN

www.h3c.com

还可以使用 VPN 技术来实现广域网的业务隔离，即为每个部门或每种业务配置单独的隧道。这是一种逻辑隔离。常用的 VPN 技术有 L2TP、GRE、IPSec、SSL VPN、MPLS-VPN 等，这些技术均可以实现在公有的网络平台上建立虚拟的私有 VPN 隧道。L2TP、GRE、IPSec、SSL VPN 技术建立的隧道都是点到点的隧道，也就是说，每一条隧道的建立都只能连通两个节点。而 MPLS-VPN 技术则能够在一张公有的网络平台上建立全网状（或点到点）的隧道。

从带宽的保证上来说，所有的 VPN 技术都是在物理通道上虚拟出一条隧道，和其他业务是共享物理带宽的，其带宽的保证需要相应的 QoS 技术来保障，隧道技术本身无法保证其隧道带宽。

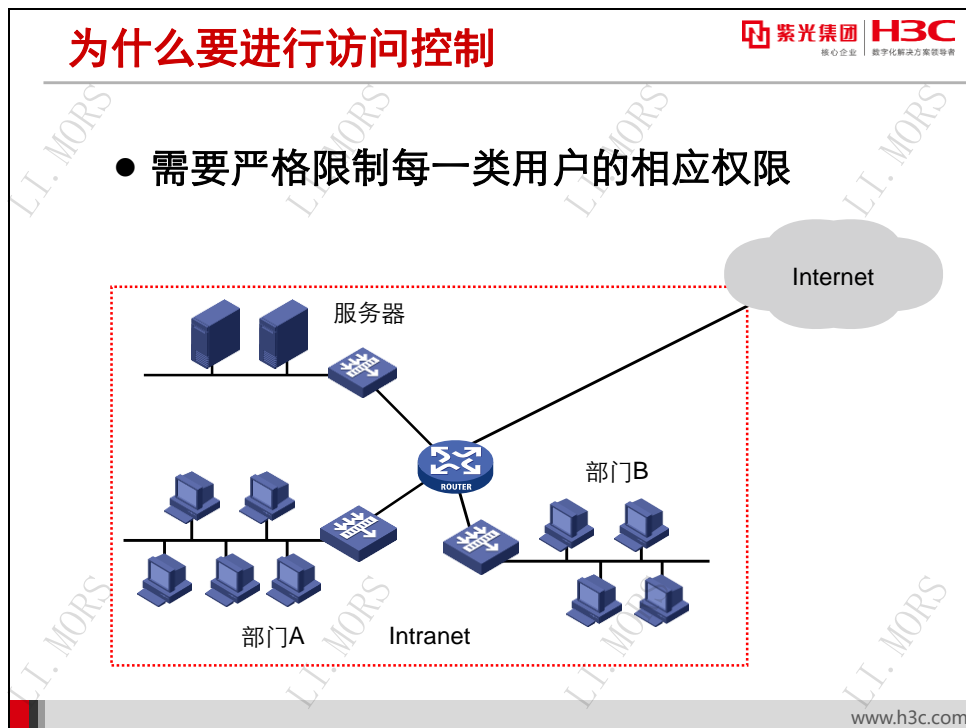
从安全性上来说，由于 VPN 技术仅仅能够做到逻辑隔离，在物理上所有的数据均在同一个物理通道中，存在被其他人截获的可能，因此整体的安全性要低于专线。

在以上的各类 VPN 技术中，L2TP 和 GRE 本身都没有对数据报文加密。IPSec 和 SSL VPN 技术本身都有完善的对封装的数据报文加密的功能，即使数据被截获，也无法被破解，具有较高的安全性。MPLS-VPN 技术本身也没有对数据报文的加密，但是建立 MPLS-VPN 网络的前提是对整个公有网络平台的绝对控制，因此，安全性要高于不加密的 L2TP 和 GRE 技术。

从应用方式上来说，GRE、IPSec 适用于网络设备之间的点对点隧道建立，一般用于公司总部和各个分支机构之间建立 VPN 隧道。L2TP、IPSec、SSL VPN 都适用于终端和设备之间的隧道建立，一般用于移动办公的个人和公司总部之间建立 VPN 隧道。MPLS-VPN 可以建立全网状的 VPN 隧道，适合于应用于城市综合网络平台的建设。

18.4 访问控制

18.4.1 为什么要进行访问控制



在一个公司内网中，为了防止合法的用户获取权限外的机密信息，整个网络要遵循最小原则赋予每个用户访问权限。例如，在一个公司内部，A、B 两个部门的服务器都放在服务器区域内，部门 A 的普通员工不能访问部门 B 的服务器，同样部门 B 的普通员工不能访问部门 A 的服务器，但是部门 A、B 的领导可以访问所有的服务器，部门 A、B 的部分关键服务器只能让部门 A、B 中的部门关键员工访问。同时还要禁止部门 A、B 员工之间的互访。

如何实现以上这些需求，精确控制每一个人的访问权限呢？最常用的手段就是使用访问控制。

18.4.2 访问控制的实现手段

访问控制的实现手段

紫光集团 H3C
核心企业 数字化解决方案领导者

- 通常情况下使用**ACL**来实现访问控制
 - 2层流分类
 - 3/4层流分类
- 通常情况下在以下地方部署**ACL**
 - 用户接入网络的入口
 - 区域的交汇处

www.h3c.com

访问控制的关键是对数据流的区分，以便于使用不同的控制策略来对待。

对于数据流的区分通常是通过使用 **ACL** 来实现，根据需要，可以使用 **2** 层流的分类规则或 **3/4** 层流的分类规则来对数据流进行区分。

2 层流分类规则可以定义的分类项包括：

- 以太网承载的数据类型
- 数据报文的源/目的 **MAC** 地址
- 以太网的封装格式
- 数据报文所属的 **Vlan ID**
- 数据报文入/出端口

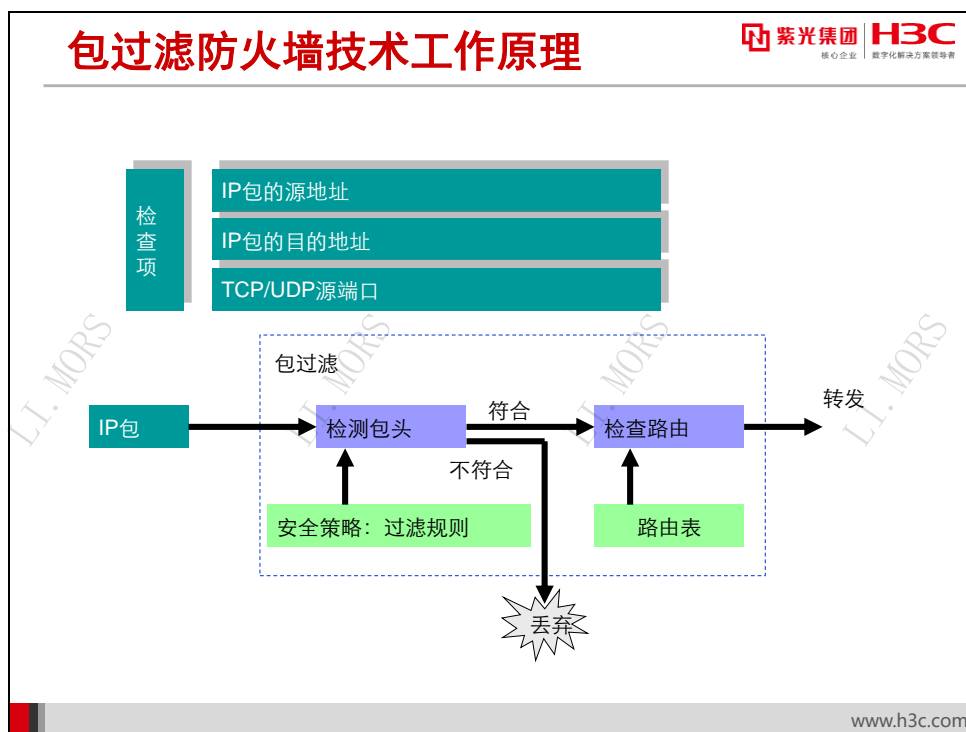
3/4 层流分类规则可以定义的分类项包括以下：

- 数据报文的协议类型
- 数据报文的源/目的 **IP** 地址
- 数据报文的源/目的端口号
- 数据报文的 **DSCP** 值

访问控制一般在以下位置使用：

- **在用户接入的入口使用：**在每一个用户进入网络的时候下发访问控制，控制其能够访问哪些资源，其好处是用户一进入网络就能够被限制访问的区域，访问控制最为严格，缺点是需要了解每一个用户的接入点，对每一个用户精细化控制，配置工作量大，对于接入设备要求也高。
- **在业务区域交汇处使用：**在业务区域交汇处（比如服务器的入口，各个功能区的入口）部署访问控制，在用户跨业务区域进行访问的时候能够被严格控制访问的资源。其优点是配置工作量相对较小，而且能够对关键区域进行比较有效的保护，但缺点是失去了对用户的控制，在功能区域内部也缺乏控制。

18.4.3 防火墙技术



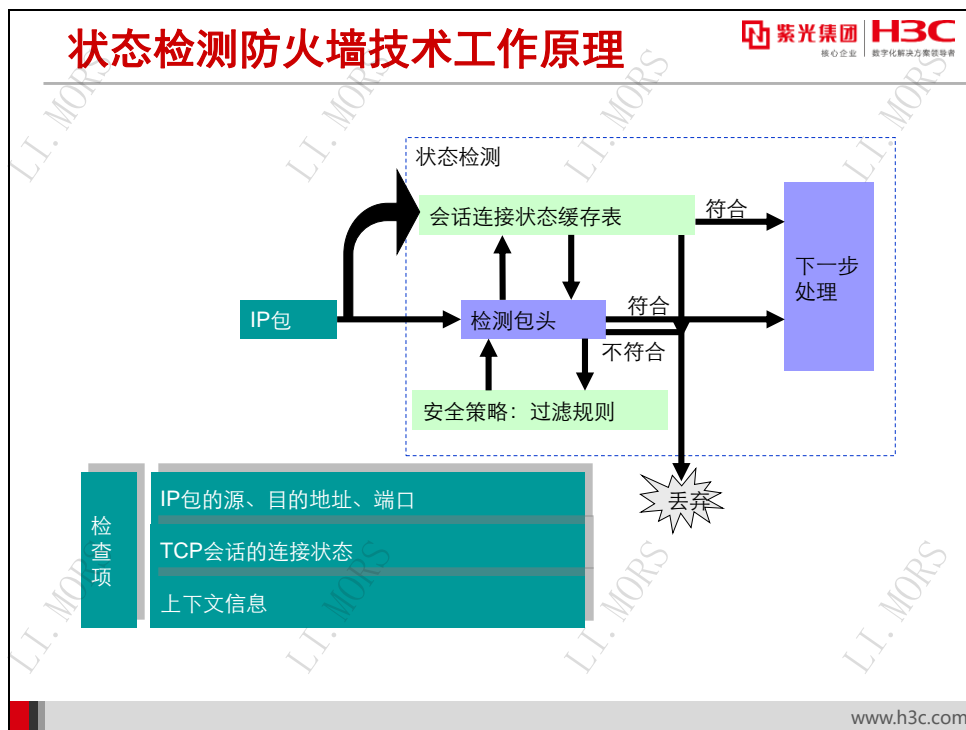
包过滤防火墙技术是最为常见的防火墙技术。包过滤防火墙技术是将 ACL/包过滤应用在设备中，为设备增加了对数据包的过滤功能。

包过滤防火墙技术的实现原理是通过 ACL 实现对 IP 数据包的过滤，对设备需要转发的数据包，先获取数据包的包头信息，包括 IP 层所承载的上层协议的协议号、数据包的源地址、目的地址、源端口和目的端口等，然后和设定的 ACL 规则进行比较，根据比较的结果决定对数据包进行相应的处理（比如丢弃，转发，重标记等等）。

目前的包过滤防火墙技术提供了对分片报文检测过滤的支持。设备将检测报文的类型（非分片报文、首片分片报文和非首片分片报文）；获得报文的三层（IP 层）信息（基本 ACL 规则和不合三层以上信息的高级 ACL 规则）及三层以上的信息（包含三层以上信息的高级 ACL 规则）用于匹配。对于配置了精确匹配过滤方式的高级 ACL 规则，设备需要记录每一个首片分片

的三层以上的信息，当后续分片到达时，使用这些保存的信息对 ACL 规则的每一个匹配条件进行精确匹配。

包过滤防火墙技术为静态防火墙技术，主要根据设备配置的 ACL 来静态的过滤各个报文，并不能分析各个报文之间的关系。



由于包过滤防火墙技术为静态防火墙技术，因此存在如下问题：

- 对于多通道的应用层协议（如 FTP，H.323 等），部分安全策略配置无法预知。
- 无法检测某些来自于传输层和应用层的攻击行为（如 TCP SYN，Java applet 等）。

因此，提出了状态检测防火墙技术——ASPF（Application Specific Packet Filter，基于应用层的包过滤）。ASPF 能够实现的应用层协议检测包括 FTP、HTTP、SMTP、RTSP、H.323（Q.931，H.245，RTP/RTCP）检测等；能够实现的传输层协议检测包括通用 TCP/UDP 检测等。

ASPF 的主要功能包括：

- 能够检查应用层协议信息，如报文的协议类型和端口号等信息，并且监控基于连接的应用层协议状态。对于所有连接，每一个连接状态信息都将被 ASPF 维护，并用于动态地决定数据包是否被允许通过防火墙进入内部网络，以便阻止恶意的入侵。
- 能够检测传输层协议信息（即通用 TCP 和 UDP 协议检测），能够根据源、目的地址及端口号，决定 TCP 或 UDP 报文是否可以通过防火墙进入内部网络。

ASPF 的其它功能包括：

- ASPF 不仅能够根据连接的状态对报文进行过滤，还能够对应用层报文的内容加以检测，提供对不可信站点的 Java Blocking（Java 阻断）功能，用于保护网络不受有害的 Java Applets 的破坏。
- 增强的会话日志功能。可以对所有的连接进行记录，包括：记录连接的时间、源地址、目的地址、使用的端口和传输的字节数。
- 支持应用协议端口映射 PAM（Port to Application Map），允许用户自定义应用层协议使用非通用端口。
- 在网络边界，ASPF 和包过滤防火墙协同工作，能够为企业内部网络提供更全面的、更符合实际需求的安全策略。

当设备上配置了应用层协议检测后，ASPF 可以检测每一个应用层的会话，并创建一个状态表和一个临时访问控制表（TACL，Temporary Access Control List）。状态表在 ASPF 检测到第一个外发报文时创建，用于维护一次会话中某一时时刻会话所处的状态，并检测会话状态的转换是否正确。TACL 的表项在创建状态表项的同时创建，会话结束后删除，它相当于一个扩展 ACL 的 permit 项。TACL 主要用于匹配一个会话中的所有返回的报文，可以为某一应用返回的报文在防火墙的外部接口上建立一个临时的返回通道。

下面以 FTP 检测为例说明多通道应用层协议检测的过程。假设 FTP Client 以 1333 端口向 FTP Server 的 21 端口发起 FTP 控制通道的连接，通过协商决定由 Server 端的 20 端口向 Client 端的 1600 端口发起数据通道的连接，数据传输超时或结束后连接删除。

FTP 检测在 FTP 连接建立到拆除过程中的处理如下：

- 1) 检查从出接口上向外发送的 IP 报文，确认为基于 TCP 的 FTP 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 和状态表。
- 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 TACL；对于数据连接，不进行状态检测。
- 4) 对于返回报文，根据协议类型做相应匹配检查，检查将根据相应协议的状态表和 TACL 决定报文是否允许通过。
- 5) FTP 连接删除时，状态表及 TACL 随之删除。

单通道应用层协议（例如 SMTP，HTTP）的检测过程比较简单，当发起连接时建立 TACL，连接删除时随之删除 TACL 即可。

状态检测防火墙功能常用配置命令

紫光集团 H3C
核心企业 数字化转型领导者

- 创建一个ASPF策略

```
[Router] aspf policy aspf-policy-number
```

- 在一个接口的指定方向上应用ASPF策略

```
[Router-Ethernet0] aspf policy aspf-policy-number  
{ inbound | outbound }
```

www.h3c.com

下面我们来介绍一下状态检测防火墙的常用配置命令。

创建一个 ASPF 策略，此配置为必选配置。在系统视图下配置：

```
aspf policy aspf-policy-number
```

在缺省情况下，没有创建 ASPF 策略。

在一个接口的指定方向上应用 ASPF 策略，此配置为必选配置。在接口视图下配置：

```
aspf policy aspf-policy-number { inbound | outbound }
```

缺省情况下，没有接口应用了 ASPF 策略。

状态检测防火墙功能常用维护命令

紫光集团 H3C
核心企业 数字化转型领导者

- 显示一个特定ASPF策略

```
[Router] display aspf policy aspf-policy-number
```

- 显示ASPF的会话信息

```
[Router] display aspf session [ verbose ]
```

www.h3c.com

要显示一个特定 ASPF 策略，在任意视图下使用命令：

display aspf policy aspf-policy-number

用 **display aspf policy** 命令显示一个特定 ASPF 策略 1 的示例如下：

```
<Sysname> display aspf policy 1
[ASPF Policy Configuration]
Policy Number 1:
Log:                disable
SYN timeout:        30    s
FIN timeout:         5    s
TCP timeout:        3600  s
UDP timeout:        30    s
Detect Protocols:
ftp timeout 120
tcp timeout 3600
```

要显示 ASPF 的会话信息，在任意视图下使用命令：

display aspf session [verbose]

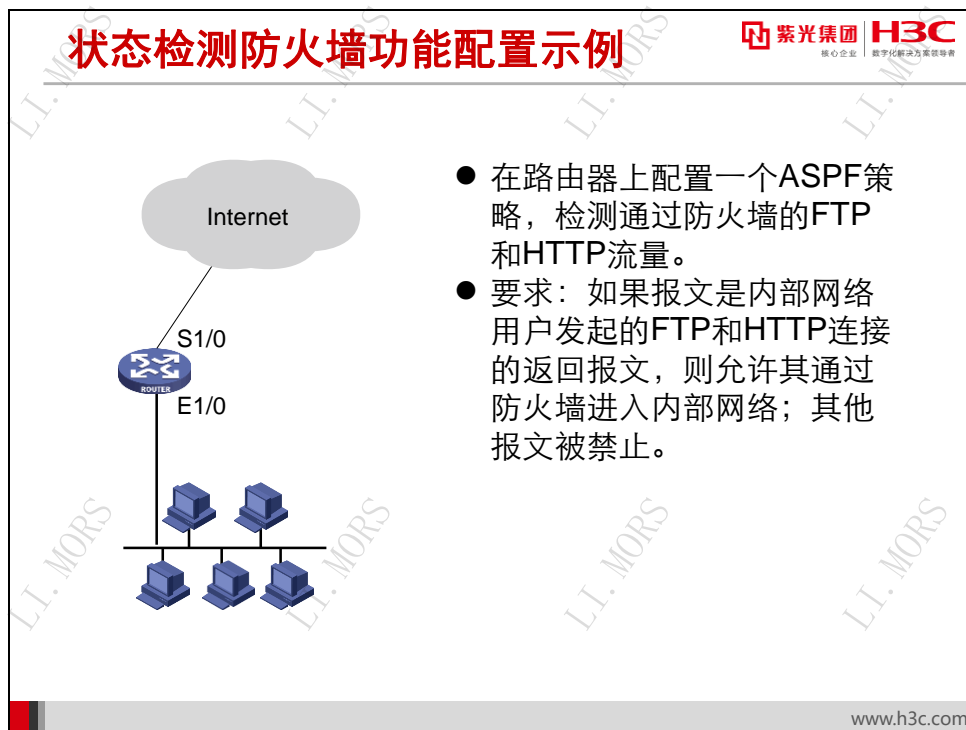
用 **display aspf session** 命令显示 ASPF 会话信息的示例如下：

```
<Sysname> display aspf session
[Established Sessions]
Session Initiator      Responder      Application    Status
212BA84 169.254.1.121:1427 169.254.1.52:0 ftp-data      TCP_DOWN
7148124 100.1.1.1:1027      200.1.1.2:21  ftp          FTP_CONXN_UP
```

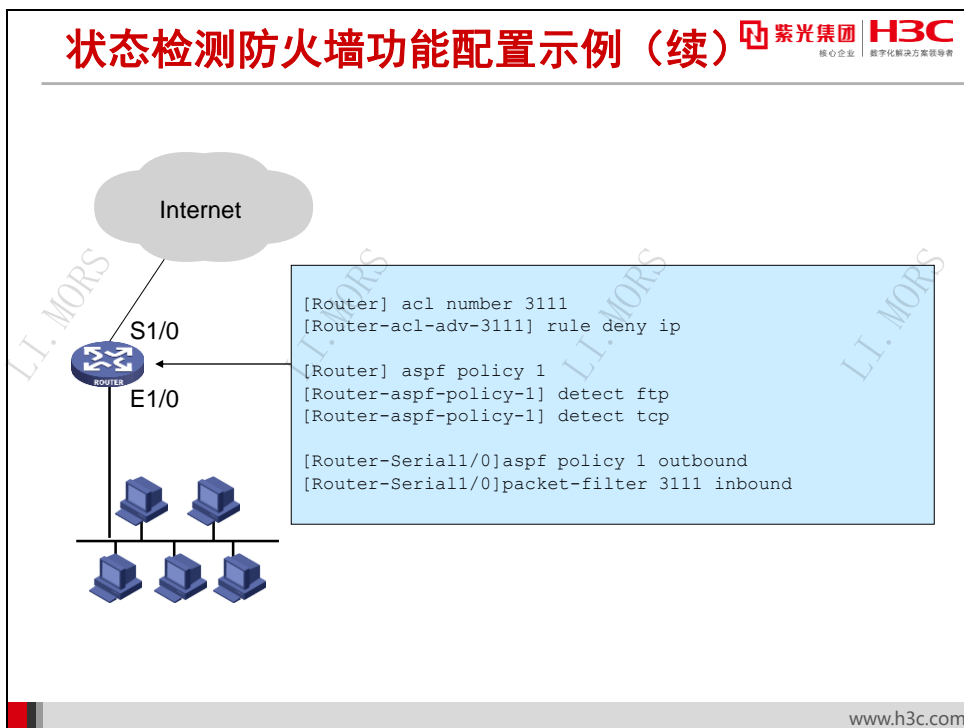
用 **display aspf session** 命令显示 ASPF 会话详细信息的示例如下：

```
[Sysname] display aspf session verbose
[Session 0x7148124]
Initiator: 100.1.1.1:1027      Responder: 200.1.1.2:21
```

```
Application protocol: ftp           Status: FTP_CONXN_UP
Transport protocol: 6              Port: 21
Child: 0x0                        Parent: 0x0
Interface: Ethernet1/1            Direction: outbound
Timeout 01:00:00                 Time left 01:00:00
Initiator Bytes/Packets sent: 350/8
Responder Bytes/Packets sent: 324/6
Initiator tcp SeqNumber/AckNumber: 141385146/134665684
Responder tcp SeqNumber/AckNumber: 134665683/141385146
```



在本例中，某公司通过一台路由器的接口 **Serial1/0** 访问 **Internet**，路由器与内部网通过以太网接口 **Ethernet1/0** 连接。希望通过设备配置实现仅允许内部网络用户主动向外发起 **FTP** 和 **HTTP** 连接，不允许外部网路向内发起 **FTP** 和 **HTTP** 连接。同时不允许其他应用连接。这种需求下就需要同时使用包过滤防火墙和状态检测防火墙的功能，在路由器的相应接口上应用该功能，并配置相应的 **ASPF** 策略。



本例的实际配置如下。此处省略了与防火墙无关的配置。

首先配置访问控制列表，以禁止所有报文：

```

[Router] acl advanced 3111
[Router-acl-ipv4-adv-3111] rule deny ip
  
```

其次创建 **ASPF** 策略，该策略检测应用层 **FTP** 和 **HTTP** 协议

```

[Router] aspf-policy 1
[Router-aspf-policy-1] detect ftp [Router-aspf-policy-1] detect http
  
```

最后在接口上应用定义好的策略，并应用访问控制列表：

```

[Router-Serial1/0] aspf policy 1 outbound
[Router-Serial1/0] packet-filter 3111 inbound
  
```

18.5 认证与授权

18.5.1 AAA 体系结构



AAA 是 Authentication, Authorization and Accounting（认证、授权和计费）的简称，它提供了一个用来对认证、授权和计费这三种安全功能进行配置的一致性框架，实际上是网络安全的一种管理机制。

这里的网络安全主要是指访问控制，包括：

- 哪些用户可以访问网络服务器；
- 具有访问权的用户可以得到哪些服务；
- 如何对正在使用网络资源的用户进行计费。

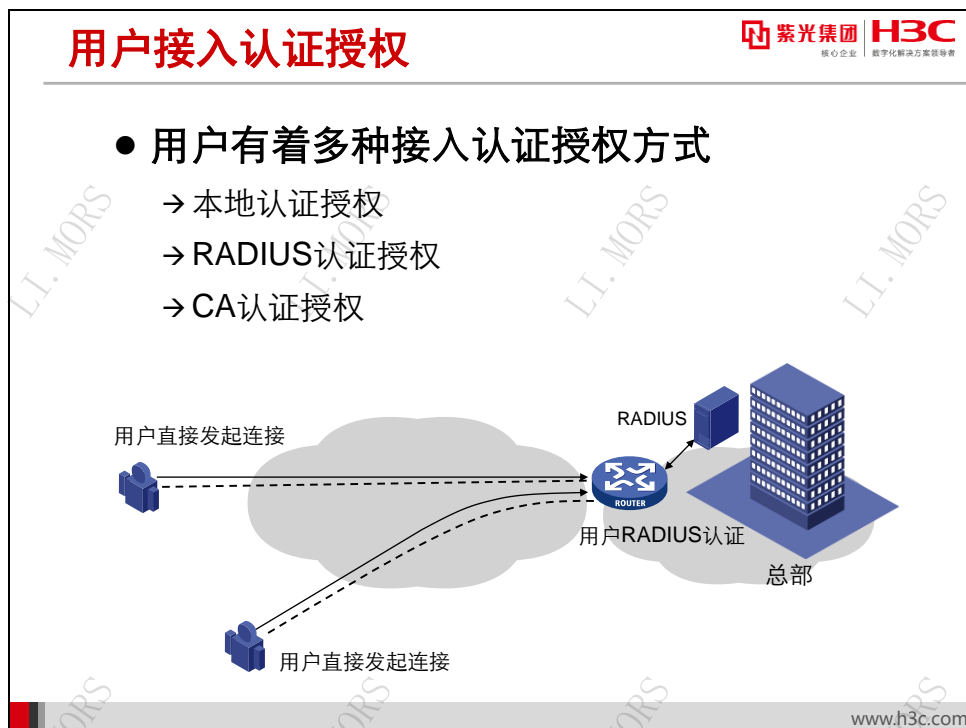
针对以上问题，AAA 必须提供下列服务：

- **认证功能。** AAA 支持以下认证方式：
 - ◆ 不认证（none）：对用户非常信任，不对其进行合法性检查，一般情况下不采用这种方式。
 - ◆ 本地认证（local）：将用户信息（包括本地用户的用户名、密码和各种属性）配置在设备上。本地认证的优点是速度快，可以降低运营成本；缺点是存储信息量受设备硬件条件限制。

- ◆ 远端认证：支持通过 RADIUS 协议或 HWTACACS 协议进行远端认证，由设备（如交换机、路由器）作为 Client 端，与 RADIUS 服务器或 TACACS 服务器通信。对于 RADIUS 协议，可以采用标准或扩展的 RADIUS 协议，与 CAMS 等系统配合完成认证。
- 授权功能。AAA 支持以下授权方式：
 - ◆ 直接授权（none）：对用户非常信任，直接授权通过，此时用户的权限为系统的默认权限。
 - ◆ 本地授权（local）：根据设备上为本地用户帐号配置的相关属性进行授权。
 - ◆ HWTACACS 授权：由 TACACS 服务器对用户进行授权。
 - ◆ RADIUS 授权：RADIUS 授权是特殊的流程。只有在认证和授权的 RADIUS 方案相同的条件下，RADIUS 授权才起作用，同时将 RADIUS 认证回应报文中携带的授权信息下发。
- 计费功能。AAA 支持以下计费方式：
 - ◆ 不计费(none)：不对用户计费。
 - ◆ 本地计费（local）：本地计费是为了支持本地用户的连接数限制管理，实现了对用户接入数的统计功能。
 - ◆ 远端计费：支持通过 RADIUS 服务器或 TACACS 服务器进行远端计费。

AAA 一般采用客户机/服务器结构。客户端运行于被管理的资源侧，服务器上集中存放用户信息。因此，AAA 框架具有良好的可扩展性，并且容易实现用户信息的集中管理。AAA 可以通过多种协议来实现，目前设备中的 AAA 是基于 RADIUS 协议或 HWTACACS 协议来实现的。

18.5.2 认证授权应用



若一个公司有部分用户需要移动办公，通过 Internet 接入到公司内网中，如何保证接入的用户合法性呢？

对于此种需求，需要分两步来实现。第一步，用户通过某种技术连接总部网络，这一步有各类的 VPN 技术可以实现。第二步，总部对连接的用户进行认证授权。在这里我们仅分析对接入用户的认证授权部分。

对于远程接入的用户，一般可以采用以下三种认证方式：

- 本地认证
- RADIUS 认证
- 证书认证

对于远程接入的普通用户，一般推荐使用 RADIUS 认证或者证书认证。

采用远端认证的优点是用户管理规范，用户的管理和设备的管理分离，便于多个系统的用户名/密码统一管理，远端认证方便为多个系统服务，便于远程接入用户的用户名/密码和其他系统的登陆用户名/密码统一管理，同时便于大量用户的管理。远端认证中最常见的是 RADIUS 认证，使用 RADIUS 服务器可以进一步提高接入的安全性，比如采用对登录用户的行为认证，控制每一个用户进行的操作，比如采用服务器和 token 卡配合，进行双因素动态密码认证。同时 RADIUS 服务器的适应性比较广泛，大部分网络设备均可以支持 RADIUS 协议。

采用证书认证的优点是用户管理规范，安全性更高，证书不仅能够进行认证，同时还有数据防伪功能；采用证书管理，用户的管理和设备的管理分离，证书服务器可以为多个系统颁发

证书,便于远程接入用户和其他系统用户的统一管理,同时证书服务器便于对大量用户的管理。但证书认证对设备要求较高,需要支持证书认证功能。



当网络设备需要远程维护时,如何保证接入到设备用户的合法性呢?

对于此种需求,需要分两步来实现。第一步,用户通过某种技术远程登录到设备上。第二步,对登录设备的用户进行认证授权。在这里我们仅分析对登录设备用户的认证授权部分。

对于远程登录设备的用户,一般可以采用以下两种认证方式:

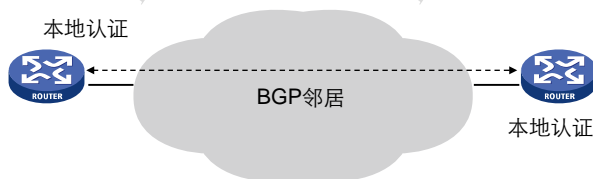
- 本地认证授权
- 远端认证授权
- 对于远程登录设备的管理用户,以上两种方式均有大量应用。

采用本地认证的优点是用法简单,无需其他设备配合,部署简单,只要网络设备正常就可以完成认证。缺点是不利于统一用户管理,同时用户名/密码配置在网络上设备上,定期修改密码工作量较大。

采用远端认证的优点是用户管理规范,用户的管理和设备的管理分离,便于多个系统的用户名/密码统一管理,远端认证中最常见的是 **RADIUS** 认证,使用 **RADIUS** 服务器可以进一步提高接入的安全性,比如采用对登录用户的行为认证,控制每一个用户进行的操作。缺点是组网方式较为复杂,网络设备无法独立完成认证,认证过程需要 **RADIUS** 服务器配合完成,增加了网络中的故障点。远程维护时网络中可能存在异常,导致认证不能完成。

设备间协议认证

- 设备间的协议认证大多采用本地认证



当网络中存在部分安全性比较低的链路时，为了保证协议运行的稳定性，都会对网络协议（如链路层协议，隧道协议，路由协议）进行认证，防止异常接入的情况发生。

网络协议认证有以下特征：


- 要求认证的用户名/密码管理权限和设备管理权限统一；
- 协议认证的用户数量较少，认证的用户名密码不会经常变化。

根据网络协议认证的特征，设备本地认证是一个很好的选择。采用本地认证的优点是用法简单，无需其他设备配合，部署简单，只要网络设备正常就可以完成认证。

18.6 传输安全

保证数据机密性和完整性

- 确保数据的机密性，即防止数据被未获得授权的查看者理解
 - 对称密钥加密和非对称密钥加密
- 确保数据的完整性，即发觉数据是否被篡改
 - 摘要算法和数字签名



核心企业 | 数字化解决方案领导者

www.h3c.com

在一个不安全的环境中传输重要数据时，首先应确保数据的机密性，即防止数据被未获得授权的查看者理解，从而防止信息内容泄露，保证信息安全性。

对于数据机密性的保障，需要对数据进行加密。加密算法根据其工作方式的不同，可以分为对称加密算法和非对称加密算法两种。

在对称加密算法中，通信双方共享一个秘密，作为加密/解密的密钥。这个密钥既可以是直接获得的，也可以是通过某种共享的方法推算出来的。由于任何具有这个共享密钥的人都可以对密文进行解密，所以，对称加密算法的安全性完全依赖于密钥本身的安全性。因为对称密钥加密方法执行效率一般比较高，对称密钥加密算法适用于能够安全地交换密钥且传输数据量较大的场合。目前有不少对称密钥加密算法的标准，包括 DES、3DES、RC4、AES 等。

非对称加密算法也称为公开密钥算法。此类算法为每个用户分配一对密钥：一个私有密钥和一个公开密钥。私有密钥是保密的，由用户自己保管。公开密钥是公诸于众的，其本身不构成严格的秘密。这两个密钥的产生没有相互关系，也就是说不能利用公开密钥推断出私有密钥，安全性较高。非对称加密算法的弱点在于其速度非常慢，吞吐量低。因此不适宜于对大量数据的加密。非对称密钥的算法中最著名和最流行的是 RSA 和 DH。

在一个不安全的环境中传输数据时，还需要确保数据的完整性，即发觉数据是否被篡改。

为了保证数据的完整性，通常使用摘要算法（HASH）。采用 HASH 函数对一段长度可变的数据进行 hash 计算，会得到一段固定长度的结果，该结果称之为原数据的摘要，也称之为消息验证码（Message Authentication Code，MAC）。摘要中包含了被保护数据的特征，如果

该数据稍有变化，都会导致最后计算的摘要不同。另外 HASH 函数具有单向性。也就是说无法根据结果导出原始输入，因而无法构造一个与原报文有相同摘要的报文。

数字签名是指使用密码算法对待发的数据进行加密处理，生成一段信息，附着在原文上一起发送，这段信息类似现实中的签名或印章，接收方对其进行验证，判断原文真伪。

数字签名技术是在网络虚拟环境中确认身份的重要技术，完全可以代替现实过程中的“亲笔签字”，在技术和法律上有保证。

数字签名可以保证信息传输的完整性，确认发送者的真实身份并防止交易中的抵赖发生。

18.7 安全防御

18.7.1 使用 NAT 进行安全防御

使用NAT进行安全防御

紫光集团 H3C
核心企业 数字化解决方案领导者

- 使用NAT进行安全防御的好处
 - 实现内部主机的隐藏
 - 有效阻断内外网的路由，禁止外部主机直接访问内部网络

www.h3c.com

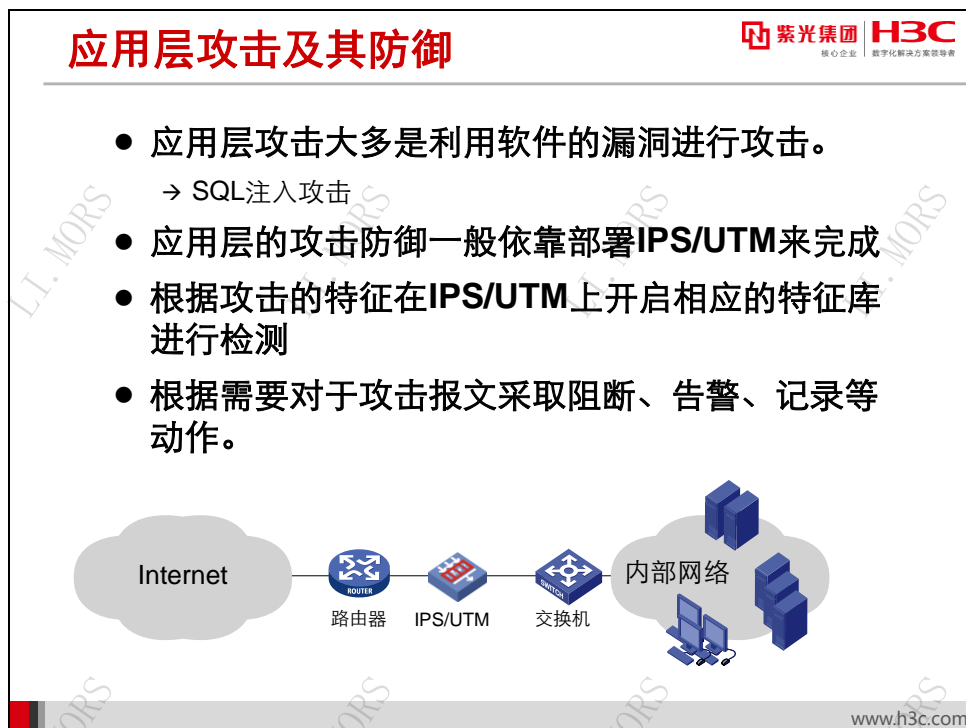
NAT（Network Address Translation，网络地址转换）是将 IP 数据报报头中的 IP 地址转换为另一个 IP 地址的过程。网络地址转换是对 Internet 隐藏内部地址，防止内部地址公开。

在内部网络与 Internet 相连的位置使用 NAT 技术对于网络安全来说有如下的好处：

- 内部用户仍然能够透明的访问外部网络，内部用户不会感受到地址转换的存在，在部署了 NAT 技术后访问外网业务的可用性不会受到影响。
- 采用了 NAT 技术后，发出到外网的数据信息的源地址都经过了转换，内网地址信息被屏蔽掉了，使外部人员无法获致内部网络的信息，也就没有了攻击的对象。
- 采用 NAT 技术后，内部网络的 IP 地址在互联网上永远不会被路由，内外网的路由被隔断，外网的主动攻击无法到达内网。
- 在两个内部网络相互连接的时候，采用双向 NAT 技术，可以避免两个网络的地址互相影响，避免由于地址冲突引发的网络安全问题。

总之，在与 Internet（或其他网络）相连的位置使用 NAT（网络地址转换）技术是一种非常行之有效的安全防御手段。

18.7.2 网络攻击与防御



应用层攻击大多是利用软件的漏洞进行攻击。

SQL 注入攻击是其中一个典型的例子。攻击者利用 Web 应用程序（网页程序）对用户的网页输入数据缺少必要的合法性判断的程序设计漏洞，将恶意的 SQL 命令注入到后台数据库。

在网站管理登录页面要求帐号密码认证时，如果攻击者在“UserID”输入框内输入“admin”，在密码框里输入“anything' or 1='1'”，交页面后，查询的 SQL 语句就变成了：Select from user where username='admin' and password='anything' or 1='1'。不难看出，由于“1='1'”是一个始终成立的条件，判断返回为“真”，密码的限制形同虚设，不管用户的密码是不是 Anything，他都可以以 admin 的身份远程登录，获得后台管理权，在网站上发布任何信息。

从上面这个例子可以看出，应用层攻击的针对性很强，都是针对某一个软件漏洞发起的攻击，由于网络上的软件漏洞层出不穷，针对每一个漏洞的攻击方式都不尽相同，而且每天都有新的漏洞被发现，同时也有老的漏洞被修复，这就使得应用层的攻击手段多种多样，经常发生变化，新的攻击方式层出不穷。

应用层攻击的特点是攻击手段多样，作用在应用层上，针对性强，新的攻击方式层出不穷。这就需要防御手段具备分析应用层内容的功能，能够匹配大量的攻击特征，能够迅速的更新辨别手段，以便于防御新的应用层攻击。

考虑到 IPS 设备具备大容量攻击特征库，能够匹配多种攻击特征，特征库可以实时更新的特点，通常采用 IPS 设备来完成应用层攻击。在 IPS 上开启防攻击的特征库，对于匹配中攻击

特征的报文根据情况采取阻断、告警、记录等动作，并实时更新特征库，以保证能够检测出最新的应用层攻击手段。

畸形报文攻击及其防御

紫光集团 H3C
核心企业 数字化解决方案领导者

- 典型畸形报文攻击
 - TearDorp攻击、Ping of death攻击、畸形TCP报文攻击
- 畸形报文攻击一般有较为明显的特征，可根据特征进行分辨，对于攻击进行防范
 - 防范ping of death攻击：检测Ping请求报文的长度是否超过65535字节，若超过，则直接丢弃
 - 防范Tear Drop攻击：缓存分片信息，每一个源、目的IP、报文ID相同的构成一组，在缓存的组数达到最大时，直接丢弃后续分片，同时根据缓存的分片信息，分析IP报文分段的合法性，直接丢弃不合法的IP报文

www.h3c.com

畸形报文攻击是通过向目标系统发送有缺陷的 IP 报文，使得目标系统在处理这样的 IP 包时会出现崩溃，给目标系统带来损失。

下面举几种常见的畸形报文攻击方式。

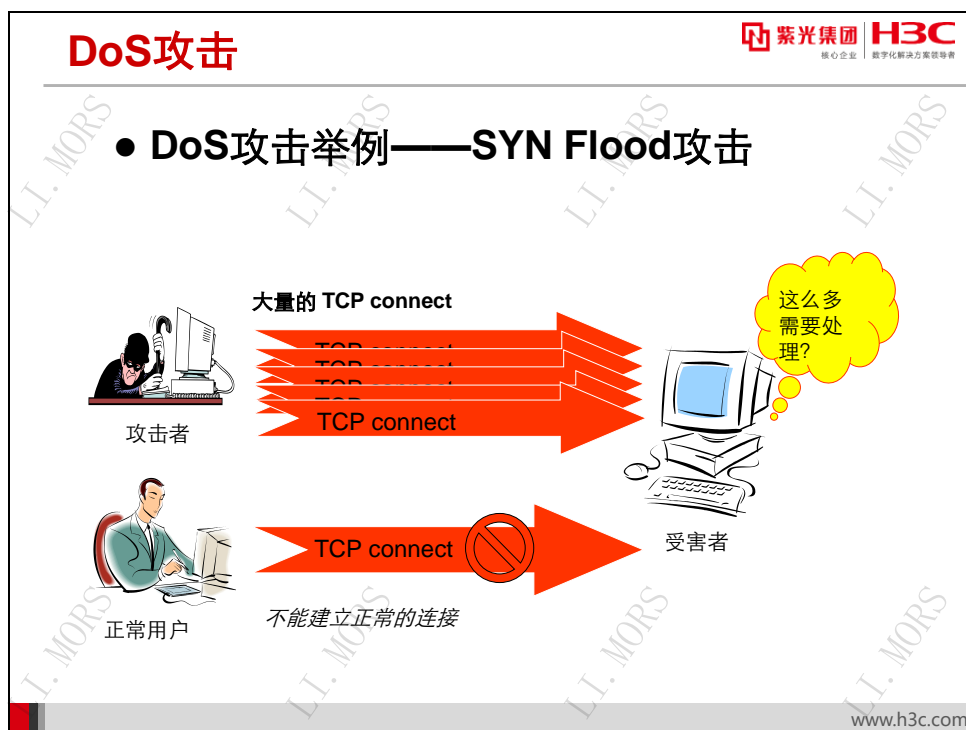
- **Ping of Death:** Ping of Death 攻击，就是利用一些超大尺寸的 Ping 请求报文对系统进行的一种攻击，这种攻击通过发送大于 65536 字节的 ICMP 包使操作系统崩溃。通常网络上不可能发送大于 65536 个字节的 ICMP 包，但攻击者可以把报文分割成片段，然后攻击报文到达目标主机后进行重组，最终会导致被攻击目标缓冲区溢出。
- **Teardrop:** Teardrop 类的攻击利用 UDP 包重组时重叠偏移的漏洞来对目标系统进行攻击。Linux 和 Windows NT 以及 95/98 更容易遭受这些攻击。Teardrop 攻击会导致蓝屏死机，并显示 STOP 0x0000000A 错误。虽然大多数操作系统打了防止这种攻击的补丁，但 Teardrop 仍然会耗费处理器的资源和主机带宽。
- **畸形 TCP 报文攻击:** TCP 报文包含 6 个标志位：URG、ACK、PSH、RST、SYN、FIN，不同系统对这些标志位组合的处理是不同的，畸形 TCP 报文攻击就是通过构造这 6 个标志位为特定数值的报文发给目标系统，导致目标系统处理出错，由此构成对目标系统的攻击。典型构造标志位的手段有设置 6 个标志位全为 1、设置 6 个标志位全为 0、设置 SYN 和 FIN 位同时为 1。

由上面几个例子可以看出，畸形报文攻击主要是通过构造特殊的 IP 报文发送给目标系统来进行攻击的，攻击报文均属于异常报文，较为容易判断。

畸形报文攻击的攻击报文一般都具有明显的特征，比较容易和正常报文区分开，只需要针对每种攻击的特征进行针对性的报文过滤即可。比如：

- 针对 Ping of Death 攻击，可以通过检测 Ping 请求报文的长度是否超过 65536 字节来辨别是否为攻击报文，若长度超过 65536 字节，则直接丢弃该报文。
- 针对 Tear Drop 攻击，可以通过缓存分片信息，每一个源、目的 IP、报文 ID 相同的构成一组，最大缓存 10000 组，在缓存的组数达到最大时，直接丢弃后续分片，同时根据缓存的分片信息，分析 IP 报文分段的合法性，直接丢弃不合法的 IP 报文的方式来抵御攻击。
- 针对畸形 TCP 报文攻击，可以通过判断 TCP 报文标志位来判断报文是否为攻击报文，对于 6 个标志位全为 1 或 6 个标志位全为 0 或 SYN 和 FIN 位同时为 1 的报文直接丢弃。

由于畸形报文攻击都是构造异常的数据报文来进行攻击的，从 IP 层和 TCP/UDP 层就可以辨别出是否为攻击报文，因此防火墙、IPS 和部分路由器/以太网交换机均可以对畸形报文进行有效的抵御。



拒绝服务型（Deny of Service, DoS）攻击是使用大量的数据包攻击系统，使系统无法接受正常用户的请求，或者主机挂起不能提供正常的工作。主要有 SYN Flood、Fraggle 等。和其他类型的攻击不同，DoS 攻击并不是去寻找进入内部网络的入口，而是间接影响合法用户对服务的请求。

下面以 SYN Flood 攻击为例说明一下拒绝服务类攻击的攻击原理。


由于资源的限制，TCP/IP 协议栈的实现只能建立有限个 TCP 连接。而 SYN Flood 攻击正是利用这一点。它构造一个源地址是伪造的（甚至根本不存在该地址）SYN 报文，向服务器发起连接，服务器收到此报文后用 SYN-ACK 应答，而此应答发出去后，不会收到 ACK 报文，这样便形成了一个 TCP 半连接。如果攻击者发送大量这样的 SYN 报文，会在被攻击主机上出现大量的半连接，消耗尽其资源，使正常的用户无法访问。直到半连接超时。

SYN Flood 攻击的特点是利用合法的报文对目标系统进行攻击。从对于攻击报文的结构和组成分析来看，无法分辨出攻击报文。

拒绝服务类攻击大多类似于 SYN Flood 攻击，利用大量合法的报文攻击目标系统，消耗目标系统有限的资源，从而达到影响合法用户对服务的请求的目的。

DoS攻击防御

- 通过Syn Cookie机制防范Syn Flood攻击。
- 通过限制单个源地址的每秒连接数来防范Connection Flood攻击。
- 通过流量阈值模型、反向认证等方式来防范UDP Flood、ICMP Flood、HTTP Get Flood、DNS Flood等DDoS攻击。
- 通过攻击特征规则检测可发现常见DoS攻击工具的控制报文，从而切断DoS攻击工具的控制通道。



核心企业 | 数字化解决方案领导者

www.h3c.com

拒绝服务类攻击的特点是利用合法的报文对目标系统进行攻击，因此没有很好的方法来辨别攻击报文。为了确保目标系统不会瘫痪，一般采取限制此类报文的接收速率或不处理此类报文的方式来进行防御，比如限制每秒建立的 TCP/UDP 半连接数量，拒绝处理 ICMP 地址不可达报文，这样可以保护目标系统不瘫痪，但代价是合法用户的业务也会受到影响。比如，若限制了 TCP/UDP 的半连接建立速度，在抵御攻击报文的同时，也拒绝了大量合法的半连接建立；若关闭了 ICMP 地址不可达报文处理功能，避免了遭受攻击的同时，使利用此功能的正常功能也无法使用了。

对于 SYN Flood 攻击，由于 TCP 的三次握手特性，有着更好的防御手段。

防止 SYN Flood 攻击的一个有效的办法就是采用 TCP 代理（运行于防火墙上）。客户发起连接时，TCP 代理并不把 SYN 包直接传递给服务器，而是自己伪装成服务器返回 SYN-ACK，

收到客户的 ACK 后再以当初客户发起连接时的信息向真正的服务器发起连接。当客户和服务 器之间传输的数据通过防火墙时，防火墙只需对它们的序号进行调整就可以了

上述过程中，TCP 代理拦截了所有来自客户端的 TCP 连接请求，它代表服务器建立与客 户机的连接，同时又代表客户机建立与服务器的连接。如果两个连接都成功地建立，防火墙就 会将两个连接进行中继。如果客户端向服务器发起 SYN Flood 攻击，将首先被 TCP 代理检测 出来（根据接收的 SYN 报文速率以及现存的 TCP 半连接数目）并处理，这样防火墙就能很好 的保护服务器不受 SYN Flood 的攻击。同时，防火墙将通过其自身的 TCP 半连接加速老化等 机制防止自身被攻陷。

在直接进行防御的同时，还可以通过攻击特征检测发现 DDOS 攻击工具的控制报文，切断 其控制攻击主机的通道，从源头消除攻击。

18.7.3 设备安全加固

设备安全加固概述

紫光集团 H3C
核心企业 数字化转型方案领导者

- 现有网络上设备的安全威胁包括：
 - 对设备登录权限的安全威胁
 - 对设备管理权限的安全威胁
 - 对设备本身系统的攻击
 - 对设备资源（如MAC表，ARP表）的安全威胁
- 网络设备是整个网络的基础，如果网络 设备的安全无法保障，网络安全更无从 谈起

www.h3c.com


整个网络是由网络设备和相关线路组成，网络设备的安全是整个网络安全稳定运行的前提 条件。如果网络设备的安全都得不到保证，整个网络的安全也就无从谈起。

在网络上，对于网络设备的安全威胁主要有以下几方面：

- 对于设备登录安全的威胁。非法用户通过各种方式（比如 TELNET、SSH、SNMP 等 方式）远程登录到设备上，获取对设备部分或全部的控制权，对设备的稳定运行造成 威胁，从而威胁到整个网络的稳定运行。
- 对于设备管理权限的安全威胁。合法的用户获取到非法的权限，获得对设备更大的操 作权限，对设备的稳定运行造成威胁，从而威胁到整个网络的稳定运行。

- 对于设备本身的攻击。利用设备开启的各类服务，比如 FTP 服务，IP 重定向服务等，对设备的 CPU 进行攻击，使设备无法正常工作，从而威胁到整个网络的稳定运行。
- 对于设备资源的安全威胁。非法用户通过大规模消耗设备的相应资源（比如 ARP 表项，MAC 表项），导致正常用户享受的服务。

设备登录权限安全加固常用手段



- 设备登录用户权限分级，加强口令安全

```
[Router] local-user h3c
[Router-luser-h3c] password hash XXXX
[Router-luser-h3c] service-type telnet
[Router-luser-h3c] authorization-attribute user-role
network-admin
[Router] user-interface con 0
[Router-ui-con0] set authentication password hash XXXX
[Router-ui-con0] authentication-mode password
[Router] user-interface vty 0 4
[Router-ui-vty0-4] authentication-mode scheme
```

www.h3c.com

对于远程接入的用户进行分级管理，对于不同级别的登录用户的口令加强管理，采用密文管理，定期进行更改。对 **CONSOLE** 用户也进行认证。

对登录用户的配置例子如下：

```
local-user h3c
 password hash XXXX
 service-type telnet level 1
user-interface con 0
 set authentication password hash XXXX
 authentication-mode password
user-interface vty 0 4
 authentication-mode scheme
```

设备管理权限安全加固常用手段

紫光集团 H3C
核心企业 数字化转型领导者

- 将设备纳入网管，确保读写团体字的安全，开启Trap功能

```
[Router] snmp-agent
[Router] snmp-agent sys-info version v2c
[Router] snmp-agent community write XXX
[Router] snmp-agent community read XXX
[Router] snmp-agent trap enable
[Router] snmp-agent target-host trap address udp-domain
1.1.1.1 params securityname XXX
[Router] snmp-agent trap source Loopback 0
```

www.h3c.com

将设备纳入网管系统进行管理，确保读写团体字的安全，严禁使用默认的读写团体字，同时开启 TRAP 功能，主动上报设备信息，便于网管及时获知设备异常情况。配置例子如下：

```
snmp-agent
snmp-agent sys-info version v2c
snmp-agent community write XXX
snmp-agent community read XXX
snmp-agent trap enable
snmp-agent target-host trap address udp-domain 1.1.1.1 params securityname XXX
snmp-agent trap source Loopback 0
```

设备管理安全加固常用手段

紫光集团 H3C
核心企业 数字化转型领导者

- 限制能够管理设备的IP地址，包括网管和远程登录

```
[Router] acl number 2001
[Router-acl2001] rule 1 permit source 1.1.1.0 0.0.0.255
[Router] snmp-agent
[Router] snmp-agent community write XXX acl 2001
[Router] snmp-agent community read XXX acl 2001
[Router] telnet server acl 2000
```

www.h3c.com

为了防止非法用户通过 TELNET、SSH、SNMP 等方式登录到设备上，需要对登录用户的 IP 地址进行限制。

在用户接口上，可以通过 ACL 对接入的 TELNET/SSH 用户的 IP 地址进行限制。配置例子如下：

```
acl basic 2001
 rule 1 permit source 1.1.1.0 0.0.0.255
telnet server acl 2001
```

也可以通过 ACL 对 SNMP 网管工作站的 IP 地址进行限制。配置例子如下：

```
acl basic 2001
 rule 1 permit source 1.1.1.0 0.0.0.255
snmp-agent
snmp-agent community write XXX acl 2001
snmp-agent community read XXX acl 2001
```


设备本身系统加固常用手段

紫光集团 H3C
核心企业 数字化转型领导者

- 对用户操作日志进行记录，缺乏存贮介质的采用日志主机

```
[Router] info-center loghost source Loopback0  
[Router] info-center loghost 1.1.1.1
```

- 关闭不必要的服务，比如FTP

```
[Router] undo ftp server
```

- 关闭空闲端口

```
[Router] Interface GigabitEthernet1/1/1  
[Router-GigabitEthernet1/1/1] shutdown
```

www.h3c.com

其他的常用安全加固还包括：

- 开启信息中心，对登录用户的操作进行记录，缺乏存贮介质的设备采取日志主机的方式，将记录传送到日志主机上保存。通过记录操作日志，可以在发生安全事件的时候，查找当时进行的操作，以便于定位事件引发的原因。日志主机的配置例子如下：

```
info-center loghost source Loopback0  
info-center loghost 1.1.1.1
```

- 关闭设备上不必要的服务。例如 FTP 服务。关闭 FTP 服务的配置例子如下：

```
undo ftp server
```

关闭不必要的服务，可以减少设备受到攻击的可能。

- 关闭空闲的端口，可以防止用户私自接入网络。配置例子如下：

```
interface GigabitEthernet1/1/1  
shutdown
```


设备安全加固常用手段

紫光集团 H3C
核心企业 数字化转型领导者

- 根据具体的网络情况，可以考虑增加如下安全加固手段

- 进行MAC地址、IP地址和端口的绑定
- 部署防ARP攻击解决方案
- 部署防异常DHCP服务器接入解决方案
- 在路由协议上增加邻居认证配置
- 在VRRP协议上增加邻居认证配置

www.h3c.com

对于其他的攻击手段，可以根据具体的情况来进行安全加固，例如：

- 进行 MAC 地址、IP 地址和端口的绑定，以防止用户使用 MAC 地址欺骗功能。
- 部署防 ARP 攻击解决方案，防止 ARP 攻击，防止设备和用户的 ARP 表项学习错误。
- 在路由协议上增加邻居认证配置，防止用户冒充对端设备和设备建立路由协议邻居关系，学习到整网路由情况。
- 在 VRRP 协议上增加邻居认证配置，防止对 VRRP 协议的攻击。

18.8 本章总结

本章总结

- 网络安全包括的主要内容
- 可以使用VLAN、VPN等技术进行业务隔离
- 可以使用ACL和防火墙技术进行访问控制
- 认证和授权的实际应用
- 传输过程中数据机密性和完整性保障手段
- NAT技术在网络安全中的作用
- 主要的网络攻击方式和防御手段
- 设备安全加固的方法

18.9 习题和解答

18.9.1 习题

- 广域网进行业务隔离的手段有哪些？（ ）
 - 专线
 - SSL VPN
 - MPLS-VPN
 - IPSec 隧道
- 我们可以利用数据包中的哪些信息来对数据流区分，以便于进行访问控制？（ ）
 - 利用源/目的 MAC 地址
 - 利用源/目的 IP 地址
 - 利用源/目的端口号
 - 利用 URL 信息
- 包过滤防火墙技术可以实现下列哪些需求？（ ）
 - 禁止源地址是 10.1.1.1 的报文通过
 - 禁止目的地址是 20.1.1.1 的报文通过
 - 禁止地址 10.1.1.1 主动去 ping 地址 20.1.1.1
 - 禁止地址 10.1.1.1 主动向地址 20.1.1.1 发起 FTP 连接
- 状态检测防火墙的配置中，哪些是必须配置的？（ ）
 - 全局启动防火墙功能
 - 定义 ASPF 策略
 - 在接口下应用 ASPF 策略
 - 调整 TCP/UDP 协议的检测时间
- 采用逻辑隔离方式进行业务隔离的手段有哪些？（ ）
 - 建立 IPSec 隧道
 - 使用 SSL VPN
 - 组件 MPLS-VPN 网络
 - 使用专线
- 一个安全的网络要满足哪些条件？（ ）
 - 确保接入网络内部的用户合法和安全
 - 接入 Internet 时有着足够的安全防范体系
 - 在 Internet 上传输数据时有着足够的加密和防伪手段
 - 整个网络有着完善的管理制度
- 使用 NAT 技术进行安全防御的好处包括（ ）
 - 使用 NAT 技术后，内网用户访问外网业务的可用性不受影响
 - 使用 NAT 技术后，外部人员无法得到内部网络信息
 - 使用 NAT 技术后，内外网路由被隔断
 - 使用 NAT 技术后，可以避免两个内部网络互联时由于地址冲突引起的问题
- 对于应用层攻击防御说法正确的有（ ）
 - 应用层攻击防御一般的网络设备都可以完成
 - 应用层攻击防御需要采用专业的安全设备来完成

- C. 应用层攻击防御需要实施更新攻击特征库
 - D. 应用层攻击防御可以采用固定的策略一劳永逸的完成
9. 对于 DDOS 攻击说法正确的有 ()
- A. DDOS 攻击以降低被攻击系统服务提供能力为目的
 - B. 对于 DDOS 攻击中的 TCP FLOOD 攻击可以采用 TCP 代理机制进行防御
 - C. 对于 DDOS 攻击中的 FTP FLOOD 攻击可以采取限制每秒的连接建立速度来进行防御
 - D. DDOS 攻击可以通过在网络设备上配置相应的访问控制列表来防御
10. 设备安全加固手段包括以下哪些? ()
- A. 加强自身的密码强度
 - B. 设置自身的访问控制
 - C. 设置访问控制列表控制用户互访
 - D. 关闭 FTP 等服务

18.9.2 习题答案

- | | | | | |
|--------|--------|-------|-------|--------|
| 1、ABCD | 2、ABC | 3、ABC | 4、ABC | 5、ABC |
| 6、ABCD | 7、ABCD | 8、BC | 9、ABC | 10、ABD |