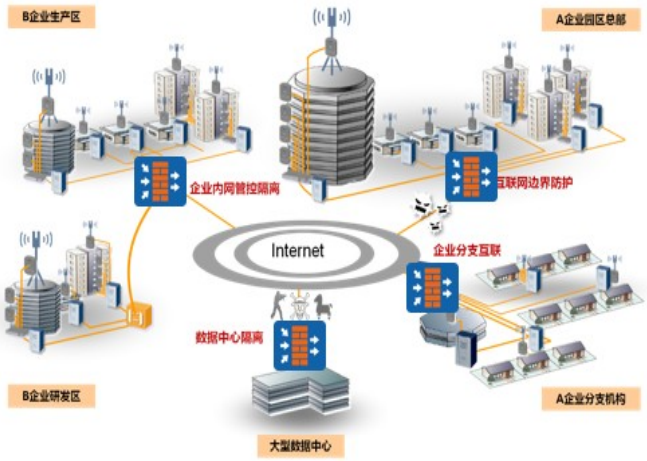
防火墙技术基础

前言

- “防火墙”一词起源于建筑领域，用来隔离火灾，阻止火势从一个区域蔓延到另一个区域。引入到通信领域，防火墙这一具体设备通常用于两个网络之间有针对性的、逻辑意义上的隔离。当然，这种隔离是高明的，既能阻断网络中的各种攻击又能保证正常通信报文的通过。
- 如何使用防火墙保护网络免受攻击和入侵？如何对外隐藏企业的内部网络？如何从应用层对用户的行为进行控制？这些都是本课程所要讲述的内容。

为什么需要防火墙



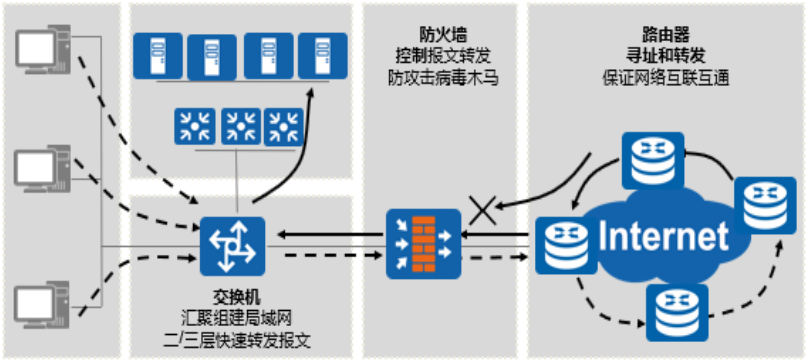
- 防火墙主要用于保护一个网络区域免受来自另一个网络区域的网络攻击和网络入侵行为。

- “防火墙”一词起源于建筑领域，用来隔离火灾，阻止火势从一个区域蔓延到另一个区域。引入到通信领域，防火墙这一具体设备通常用于两个网络之间有针对性的、逻辑意义上的隔

离。当然，这种隔离是高明的，隔离的是“火”的蔓延，而又保证“人”的穿墙而过。这里的“火”是指网络中的各种攻击，而“人”是指正常的通信报文。

- 用通信语言来定义，防火墙主要用于保护一个网络区域免受来自另一个网络区域的网络攻击和网络入侵行为。因其隔离、防守的属性，灵活应用于网络边界、子网隔离等位置，具体如企业网络出口、大型网络内部子网隔离、数据中心边界等等。

防火墙与交换机、路由器对比



- 路由器与交换机的本质是转发，防火墙的本质是控制。

- 防火墙与路由器、交换机是有区别的。路由器用来连接不同的网络，通过路由协议保证互联互通，确保将报文转发到目的地；交换机则通常用来组建局域网，作为局域网通信的重要枢纽，通过二层/三层交换快速转发报文；而防火墙主要部署在网络边界，对进出网络的访问行为进行控制，安全防护是其核心特性。路由器与交换机的本质是转发，防火墙的本质是控制。
- 现阶段中低端路由器与防火墙有合一趋势，主要也是因为二者互相功能兼具，变成 all in one 的目标，华为也发布了

一系列中低端设备。

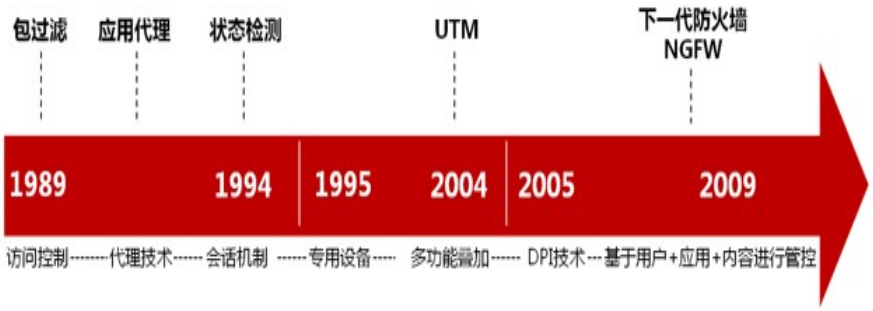
防火墙和路由器实现安全控制的区别

	防火墙	路由器
背景	产生于人们对于安全性的需求。	基于对网络数据包路由而产生的。
目的	保证任何非允许的数据包“不通”。	保持网络和数据的“通”。
核心技术	基于状态包过滤的应用级信息流过滤。	路由器核心的ACL列表是基于简单的包过滤。
安全策略	默认配置即可以防止一些攻击。	默认配置对安全性的考虑不够周全。
对性能的影响	采用的是状态包过滤，规则条数，NAT的规则数对性能的影响较小。	进行包过滤会对路由器的CPU和内存产生很大的影响。
防攻击能力	具有应用层的防范功能。	普通路由器不具有应用层的防范功能。

- 目前市面上的路由器基本都带有简单的防火墙功能，不论是消费级还是企业级，可以实现一些诸如包过滤，IP 过滤这样的功能。那么为什么还需要硬件防火墙呢？两者之间的差别如下：
- 背景：
- 路由器的产生是基于对网络数据包路由而产生的。路由器需要完成的是将不同网段的数据包进行有效的路由管理。路由器所关心的是：能否将不同的网段的数据包进行路由从而进行通讯。
- 防火墙是产生于人们对于安全性的需求。数据包是否可以正确的到达、到达的时间、方向等不是防火墙关心的重点，重点是这个数据包是否应该通过、通过后是否会对网络造成危害。
- 目的：
- 路由器的根本目的是：保持网络和数据的“通”。
- 防火墙根本的的目的是：保证任何非允许的数据包“不通”。

- 核心技术：
- 路由器核心的 ACL 列表是基于简单的包过滤，属于 OSI 第三层过滤。从防火墙技术实现的角度来说，防火墙是基于状态包过滤的应用级信息流过滤。
- 安全策略：
- 路由器的默认配置对安全性的考虑不够周全，需要做高级配置才能达到一些防范攻击的作用，其针对安全性的规则的部分比较复杂，配置出错的概率较高。
- 有些防火墙的默认配置即可以防止各种攻击，更人性化的防火墙都是使用图形界面进行配置的，配置简单、出错率低。

防火墙的发展历史

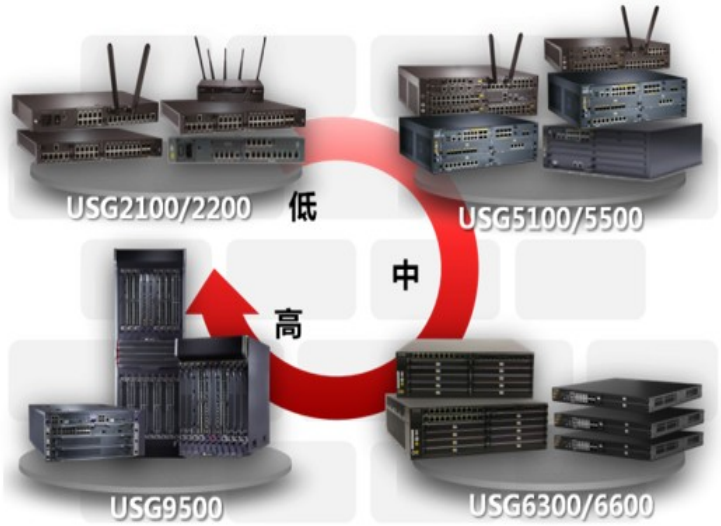


- 最早的防火墙可以追溯到上世纪 80 年代末期，距今已有二十多年的历史。在这二十多年间，防火墙的发展过程大致可以划分为下面三个时期：
- 1989 年至 1994 年：
- 1989 年产生了包过滤防火墙，实现简单的访问控制，称之为第一代防火墙。
- 随后出现了代理防火墙，在应用层代理内部网络和外部

网络之间的通信，属于第二代防火墙。代理防火墙安全性较高，但处理速度慢，而且对每一种应用开发一个对应的代理服务是很难做到的，因此只能对少量的应用提供代理支持。

- 1994 年业界发布了第一台基于状态检测技术的防火墙，通过动态分析报文的状态来决定对报文采取的动作，不需要为每个应用程序都进行代理，处理速度快而且安全性高。状态检测防火墙被称为第三代防火墙。
- 1995 年至 2004 年：
- 在这一时期，状态检测防火墙已经成为趋势。除了访问控制功能之外，防火墙上也开始增加一些其他功能，如 VPN。
- 同时，一些专用设备也在这一时期出现了雏形。例如，专门保护 Web 服务器安全的 WAF（Web Application Firewall，Web 应用防火墙）设备。
- 2004 年业界提出了 UTM（United Threat Management，统一威胁管理）的概念，将传统防火墙、入侵检测、防病毒、URL 过滤、应用程序控制、邮件过滤等功能融合到一台防火墙上，实现全面的安全防护。

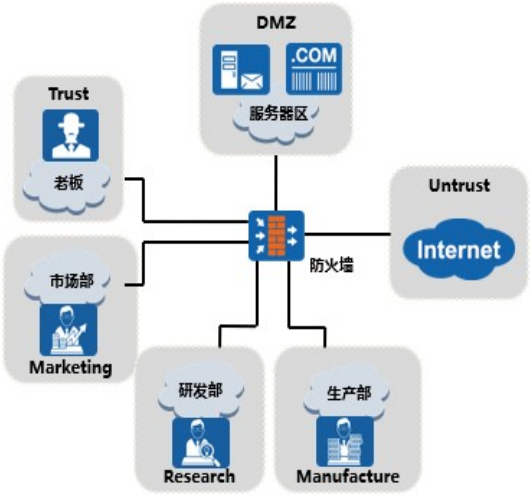
华为防火墙产品



- 华为防火墙产品主要包括 USG2000、USG5000、USG6000 和 USG9500 四大系列，涵盖低、中、高端设备，型号齐全功能丰富，完全能够满足各种网络环境的需求。其中，USG2000 和 USG5000 系列定位于 UTM 产品，USG6000 系列属于下一代防火墙产品，USG9500 系列属于高端防火墙产品。
- USG2100 集防火墙、UTM、VPN、路由、无线（WIFI/3G）等于一身，即插即用，配置方便，可以为为客户提供安全、灵活、便捷的一体化组网和接入解决方案。
- USG6000 作为华为面向下一代网络环境的防火墙产品，提供以应用层威胁防护为核心的下一代网络安全，让网络管理员重新掌控网络，看得更清、管得更细、用得更易。具有最精准的应用访问控制、6000+应用识别、多种用户认证技术、全面的未知威胁防护、最简单的安全管理、最高的全业务性能体验等优点。
- USG9500 是业界首款 T 级数据中心防火墙，成功通过了业界权威第三方安全测评机构美国 NSS 实验室的测试，获评为业界最快的防火墙。USG9500 采用分布式软硬件设计，融

合了多种行业领先的专业安全技术，将交换、路由、安全服务整合到统一的设备中，在大型数据中心、大型企业、教育、政府、广电等行业和典型场景得到广泛应用。

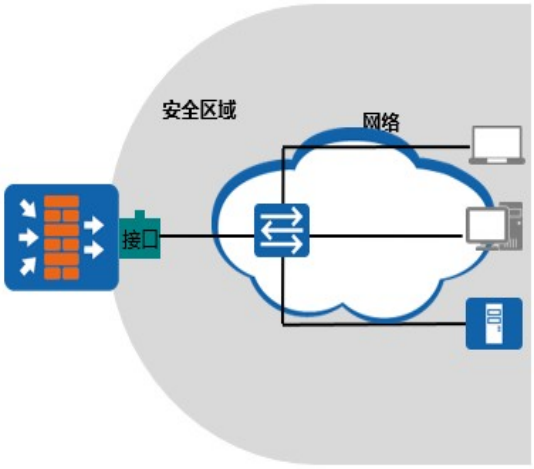
为什么需要安全区域



- 防火墙上如何来区分不同的网络呢?

- 防火墙主要部署在网络边界起到隔离的作用，那么在防火墙上如何来区分不同的网络呢？

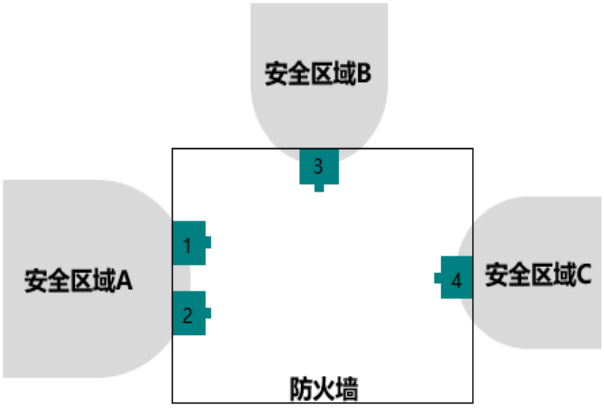
安全区域



- 防火墙通过安全区域来划分网络、标识报文流动的“路线”。

- 为了在防火墙上区分不同的网络，我们在防火墙上引入了一个重要的概念：安全区域（Security Zone），简称为区域（Zone）。安全区域是一个或多个接口的集合，是防火墙区别于路由器的主要特性。防火墙通过安全区域来划分网络、标识报文流动的“路线”，一般来说，当报文在不同的安全区域之间流动时，才会受到控制。
- 我们都知道，防火墙通过接口来连接网络，将接口划分到安全区域后，通过接口就把安全区域和网络关联起来。通常说某个安全区域，就可以表示该安全区域中接口所连接的网络。接口、网络和安全区域的关系如图所示。

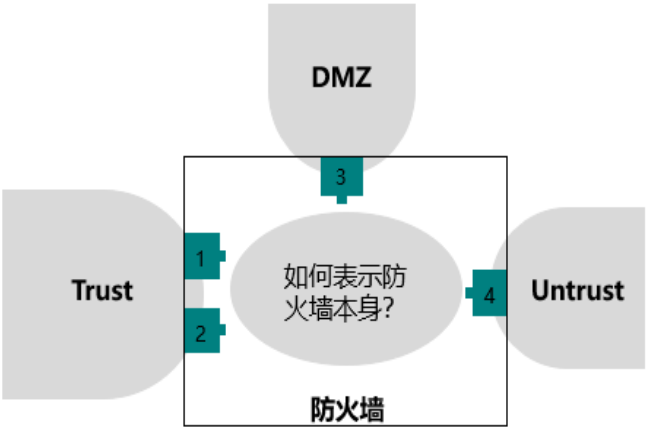
将接口划分到安全区域



- 通过把接口划分到不同的安全区域中，就可以在防火墙上划分出不同的网络。

- 通过把接口划分到不同的安全区域中，就可以在防火墙上划分出不同的网络。如图所示，我们把接口 1 和接口 2 放到安全区域 A 中，接口 3 放到安全区域 B 中，接口 4 放到安全区域 C 中，这样在防火墙上就存在了三个安全区域，对应三个网络。
- 在华为防火墙上，一个接口只能加入到一个安全区域中。

默认安全区域：Trust、DMZ和Untrust



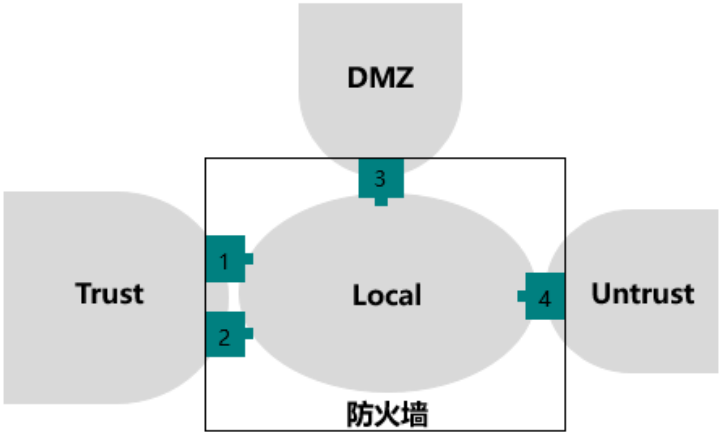
- 华为防火墙产品默认提供了Trust、DMZ和Untrust三个安全区域。

- 华为防火墙产品上默认已经提供了三个安全区域，分别是 Trust、DMZ 和 Untrust：
- Trust 区域，该区域内网络的受信任程度高，通常用来定义内部用户所在的网络。
- DMZ 区域，该区域内网络的受信任程度中等，通常用来定义内部服务器所在的网络。
- Untrust 区域，该区域代表的是不受信任的网络，通常用来定义 Internet 等不安全的网络。
- 在网络数量较少、环境简单的场合中，使用默认提供的安全区域就可以满足划分网络的需求。在网络数量较多的场合，还可以根据需要创建新的安全区域。
- 如图所示，假设接口 1 和接口 2 连接的是内部用户，那我们就把这两个接口划分到 Trust 区域中；接口 3 连接内部服务器，将它划分到 DMZ 区域；接口 4 连接 Internet，将它划分到 Untrust 区域。
- 当内部网络中的用户访问 Internet 时，报文在防火墙上的路线是从 Trust 区域到 Untrust 区域；当 Internet 上的用户

访问内部服务器时，报文在防火墙上的路线是从 Untrust 区域到 DMZ 区域。

- 注：DMZ（Demilitarized Zone）起源于军方，是介于严格的军事管制区和松散的公共区域之间的一种部分管制的区域。防火墙引用了这一术语，指代一个与内部网络和外部网络分离的安全区域。
- 除了在不同网络之间流动的报文之外，还存在从某个网络到达防火墙本身的报文（例如我们登录到防火墙上进行配置），以及从防火墙本身发出的报文，如何在防火墙上标识这类报文的路线呢？

Local区域



- 防火墙上提供了Local区域，代表防火墙本身。

- 防火墙上提供了 Local 区域，代表防火墙本身。凡是由防火墙主动发出的报文均可认为是从 Local 区域中发出，凡是需要防火墙响应并处理（而不是转发）的报文均可认为是由 Local 区域接收。
- Local 区域中不能添加任何接口，但防火墙上所有接口本身都隐含属于 Local 区域。也就是说，报文通过接口去往某个网络时，目的安全区域是该接口所在的安全区域；报文通过接

口到达防火墙本身时，目的安全区域是 Local 区域。

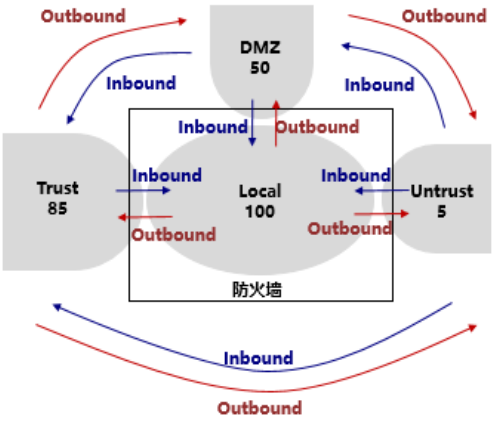
安全区域、受信任程度与安全级别

安全区域	安全级别	说明
Local	100	设备本身，包括设备的各接口本身。
Trust	85	通常用于定义内网终端用户所在区域。
DMZ	50	通常用于定义内网服务器所在区域。
Untrust	5	通常用于定义Internet等不安全的网络。

- 受信任程度：Local > Trust > DMZ > Untrust

- 不同的网络受信任的程度不同，在防火墙上用安全区域来表示网络后，怎么来判断一个安全区域的受信任程度呢？在华为防火墙上，每个安全区域都有一个唯一的安全级别，用 1～100 的数字表示，数字越大，则代表该区域内的网络越可信。对于默认的安全区域，它们的安全级别是固定的：Local 区域的安全级别是 100，Trust 区域的安全级别是 85，DMZ 区域的安全级别是 50，Untrust 区域的安全级别是 5。

安全域间、安全策略与报文流动的方向

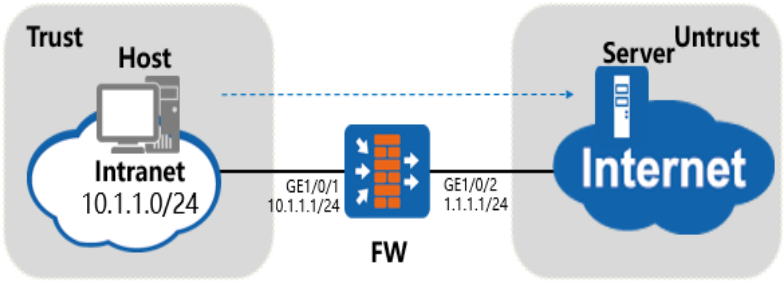


- “安全域间”是两个安全区域之间的唯一“道路”；
- “安全策略”即在“道路”上设立的“安全关卡”。

- 任意两个安全区域都构成一个安全域间（Interzone），并具有单独的安全域间视图，大部分的安全策略都需要在安全域间视图下配置。
- 安全域间这个概念用来描述流量的传输通道。它是两个“区域”之间的唯一“道路”，如果希望对经过这条通道的流量进行控制，就必须在通道上设立“关卡”，也就是安全策略。报文在两个安全区域之间流动时，我们规定：报文从低级别的安全区域向高级别的安全区域流动时为入方向（Inbound），报文从由高级别的安全区域向低级别的安全区域流动时为出方向（Outbound）。报文在两个方向上流动时，将会触发不同的安全检查。图中标明了 Local 区域、Trust 区域、DMZ 区域和 Untrust 区域间的方向。
- 通常情况下，通信双方一定会交互报文，即安全域间的两个方向上都有报文的传输。而判断一条流量的方向应以发起该条流量的第一个报文为准。
- 通过设置安全区域，防火墙上的各个安全区域之间有了等级明确的域间关系。不同的安全区域代表不同的网络，防火

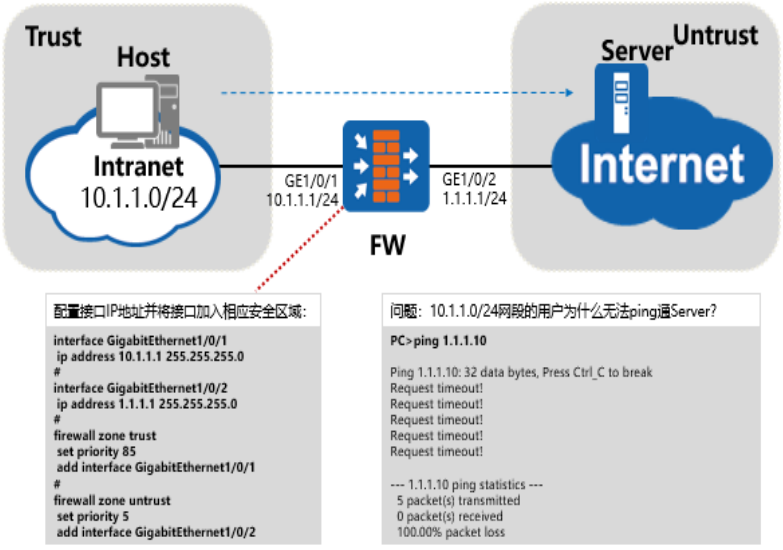
墙成为连接各个网络的节点。以此为基础，防火墙就可以对各个网络之间流动的报文实施管控。

安全区域配置案例



- 如图所示，在一个测试用的网络环境中，NGFW作为安全网关。为了使10.1.1.0/24网段的用户可以正常访问Server（1.1.1.10），需要在NGFW上配置安全区域。网络环境如图所示。

安全区域配置命令



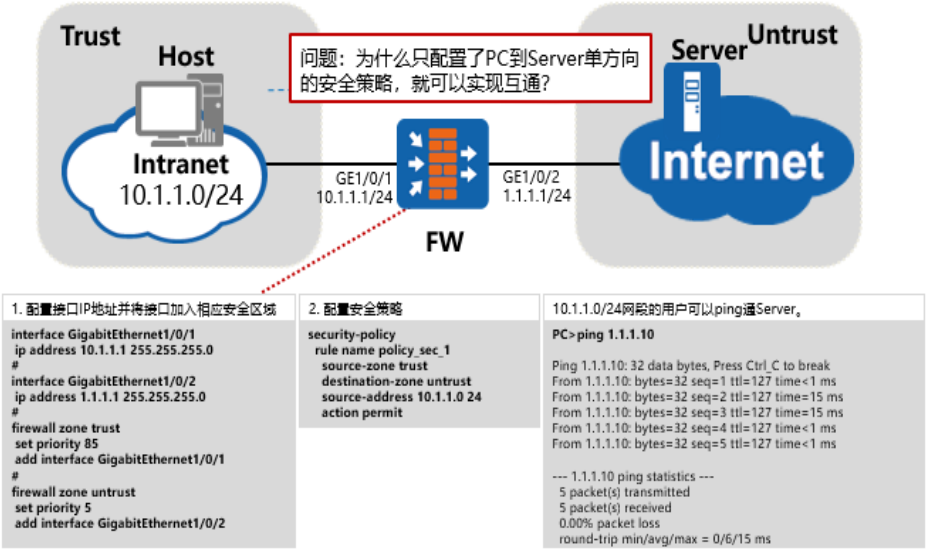
缺省包过滤

类型	源地址	源端口	目的地址	目的端口	动作
缺省包过滤	任意				允许/拒绝

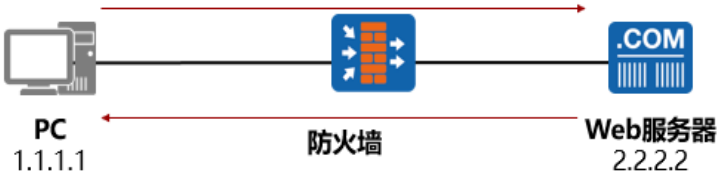
- 如果防火墙域间没有配置安全策略，或查找安全策略时，所有的安全策略都没有命中，则默认执行域间的缺省包过滤动作（拒绝通过）。

- 如果没有配置任何安全策略，防火墙是不允许报文在安全区域之间流动的。
- 缺省包过滤是对所有报文都生效的缺省的安全策略。默认情况下，缺省包过滤的动作是拒绝通过。

安全策略配置命令



包过滤技术



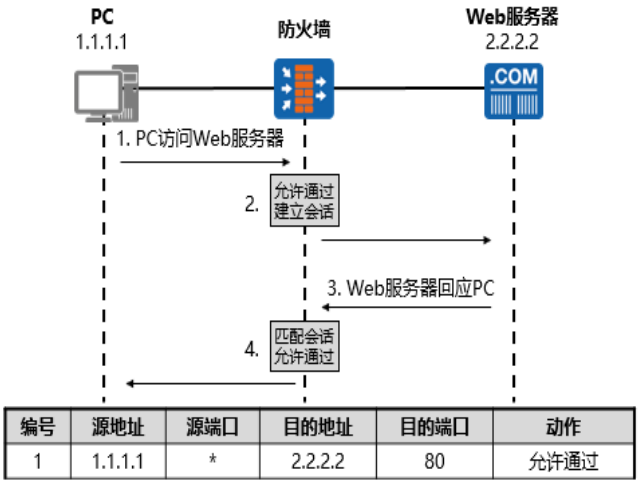
编号	源地址	源端口	目的地址	目的端口	动作
1	1.1.1.1	*	2.2.2.2	80	允许通过
2	2.2.2.2	80	1.1.1.1	*	允许通过

- 实现包过滤的核心技术是访问控制列表。
- 包过滤防火墙只根据设定好的静态规则来判断是否允许报文通过。

- 包过滤防火墙只根据设定好的静态规则来判断是否允许报文通过，它认为报文都是无状态的孤立个体，不关注报文产生的前因后果。
- 如图所示，PC 和 Web 服务器位于不同的网络，分别与防火墙相连，PC 与 Web 服务器之间的通信受到防火墙的控制。当 PC 需要访问 Web 服务器浏览网页时：
- 在防火墙上必须配置规则 1，允许 PC 访问 Web 服务器的报文通过。
- 在规则 1 中，源端口处的*表示任意的端口，这是因为 PC 在访问 Web 服务器时，它的操作系统决定了所使用的源端口，例如，对于 WINDOWS 操作系统来说，这个值可能是 1024~65535 范围内任意的一个端口。这个值是不确定的，所以这里设定为任意端口。配置了这条规则后，PC 发出的报文就可以顺利通过防火墙，到达 Web 服务器。
- Web 服务器将会向 PC 发送回应报文，这个报文也要穿过防火墙才能到达 PC。在状态检测防火墙出现之前，包过滤防火墙还必须配置规则 2，允许反方向的报文通过。

- 在规则 2 中，目的端口也设定为任意端口，因为我们无法确定 PC 访问 Web 服务器时使用的源端口，要想使 Web 服务器回应的报文都能顺利穿过防火墙到达 PC，只能将规则 2 中的目的端口设定为任意端口。
- 如果 PC 位于受保护的网络中，这样处理将会带来很大的安全问题。规则 2 将去往 PC 的目的端口全部开放，外部的恶意攻击者伪装成 Web 服务器，就可以畅通无阻地穿过防火墙，PC 将会面临严重的安全风险。
- “逐包检测”机制，即对设备收到的所有报文都根据包过滤规则每次都进行检查以决定是否对该报文放行，严重影响了设备转发效率，使包过滤防火墙成为网络中的转发瓶颈。

状态检测和会话机制



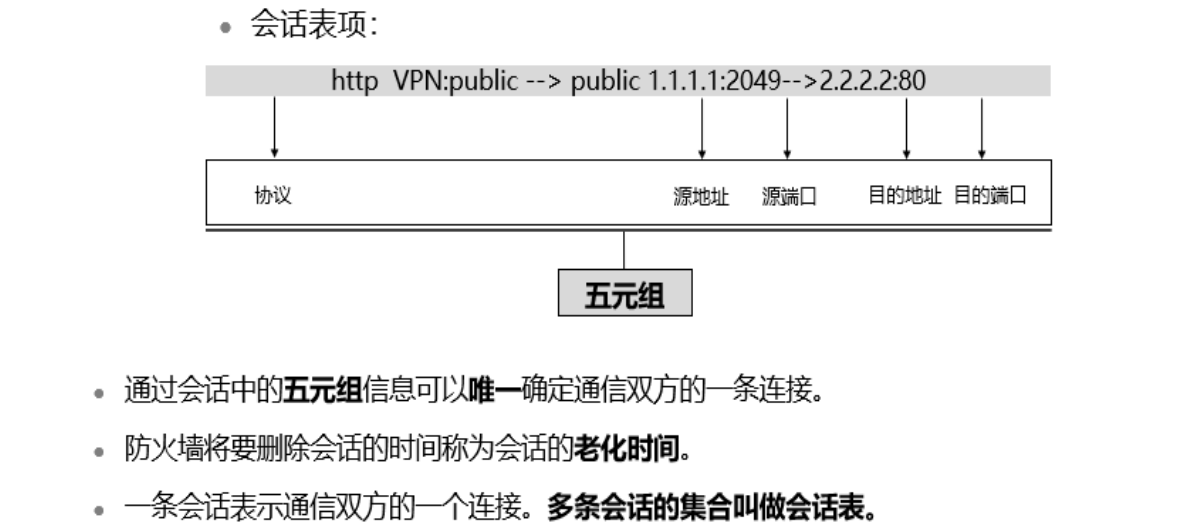
编号	源地址	源端口	目的地址	目的端口	动作
1	1.1.1.1	*	2.2.2.2	80	允许通过

- 如果规则允许通过，状态检测防火墙会将属于同一连接的所有报文作为一个整体的数据流（会话）来对待。

- 状态检测防火墙使用基于连接状态的检测机制，将通信双方之间交互的属于同一连接的所有报文都作为整体的数据流来对待。在状态检测防火墙看来，同一个数据流内的报文不再是孤立的个体，而是存在联系的。为数据流的第一个报文建立会话，数据流内的后续报文直接根据会话进行转发，提高了转发效率。

- 如图所示，状态检测防火墙是这样解决包过滤技术的不足的：
- 首先我们还是需要在防火墙上设定规则 1，允许 PC 访问 Web 服务器的报文通过。
- 当报文到达防火墙后，防火墙允许报文通过，同时还会针对 PC 访问 Web 服务器的这个行为建立会话（Session），会话中包含了 PC 发出的报文信息，如地址和端口等。
- 当 Web 服务器回应给 PC 的报文到达防火墙后，防火墙会把报文中的信息与会话中的信息进行比对，发现报文中的信息与会话中的信息相匹配，并且符合协议规范对后续包的定义，则认为这个报文属于 PC 访问 Web 服务器行为的后续回应报文，直接允许这个报文通过。

会话表项中的五元组信息

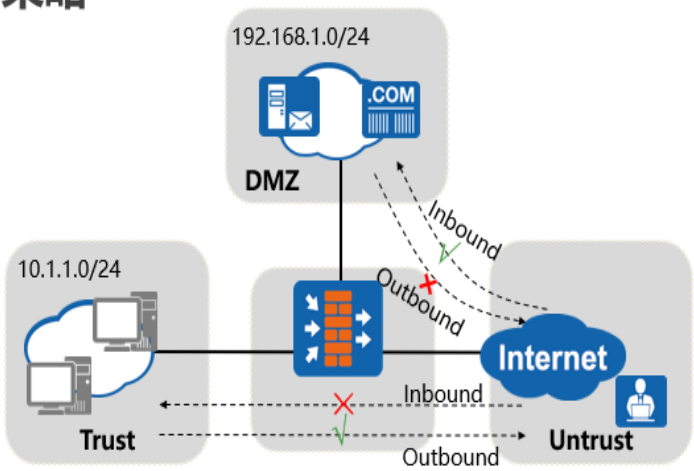


- 会话是通信双方的连接在防火墙上的具体体现，代表两者的连接状态，一条会话就表示通信双方的一个连接。防火墙上多条会话的集合就叫做会话表（Session table）。
- 在图中的会话表项中：
- http 表示协议，1.1.1.1 表示源地址，2049 表示源端口，

2.2.2.2 表示目的地址，80 表示目的端口。

- 源地址、源端口、目的地址、目的端口和协议这五个元素是会话的重要信息，我们将这五个元素称之为“五元组”。只要这五个元素相同的报文即可认为属于同一条流，在防火墙上通过这五个元素就可以唯一确定一条连接。
- 会话是动态生成的，但不是永远存在的。如果长时间没有报文匹配，则说明通信双方已经断开了连接，不再需要该条会话了。此时，为了节约系统资源，防火墙会在一段时间后删除会话，该时间称为会话的老化时间。

安全策略

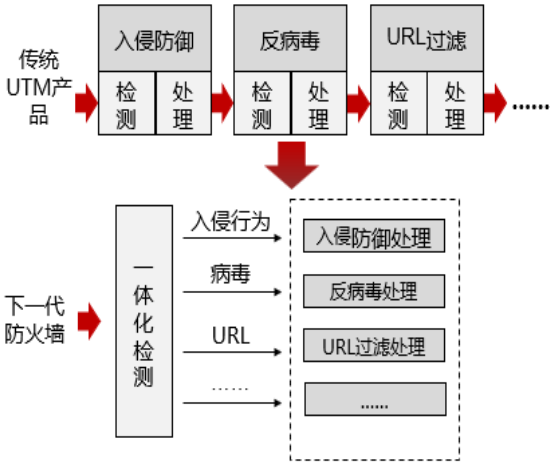


- 安全策略是按一定规则控制设备对安全域间的流量进行转发和内容安全一体化检测的策略。
- 规则的本质是包过滤。

- 防火墙的基本作用是保护特定网络免受“不信任”的网络的攻击，但是同时还必须允许两个网络之间可以进行合法的通信。
- 安全策略就是按一定规则控制设备对安全域间的流量进行转发和内容安全一体化检测的策略。安全域间是防火墙两个“区域”之间的唯一“道路”，安全策略就好比在这条通道上设立的“关卡”。
- 安全策略的作用就是对通过防火墙的数据流进行检验，符合安全策略的合法数据流才能通过防火墙。

- 任意两个安全区域之间都有唯一的一条“道路”（安全域间），具有单独的安全域间视图，大部分的安全策略都需要在安全域间视图下配置。
- 图中的安全策略做到了：
- 外网可以访问目的地址为 192.168.1.0/24 的服务器；服务器不能主动访问外网。
- 源 IP 是 10.1.1.0/24 的数据包可以访问 Internet；Internet 不能主动访问内网。

内容安全一体化检测



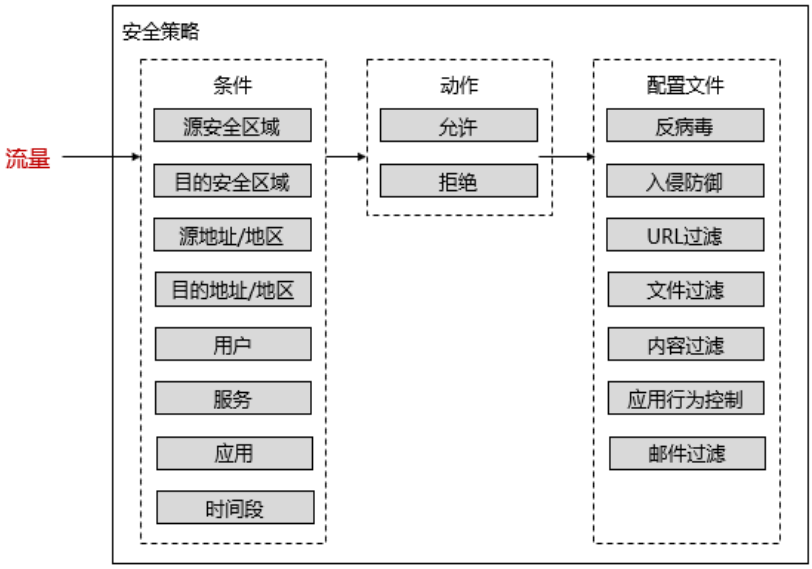
- 一体化检测是指对一条流量的内容只进行一次检测和处理，就能实现包括反病毒、入侵防御在内的内容安全功能。

- 防火墙能够识别出流量的属性，并将流量的属性与安全策略的条件进行匹配。如果所有条件都匹配，则此流量成功匹配安全策略。流量匹配安全策略后，设备将会执行安全策略的动作。
- 如果动作为“允许”，则对流量进行内容安全检测。如果内容安全检测也通过，则允许流量通过；如果内容安全检测没有通过，则禁止流量通过。
- 如果动作为“禁止”，则禁止流量通过。
- 内容安全一体化检测是指使用设备的智能感知引擎对一

条流量的内容只进行一次检测和处理，就可以获取到后续所有内容安全功能所需的数据，就能实现包括反病毒、入侵防御在内的内容安全功能，从而大幅提升设备处理性能。

- 由于一体化检测的高效性，我们往往可以通过配置较宽泛的安全策略条件来匹配一类流量，然后再通过各种内容安全功能来保证网络安全。

NGFW安全策略构成

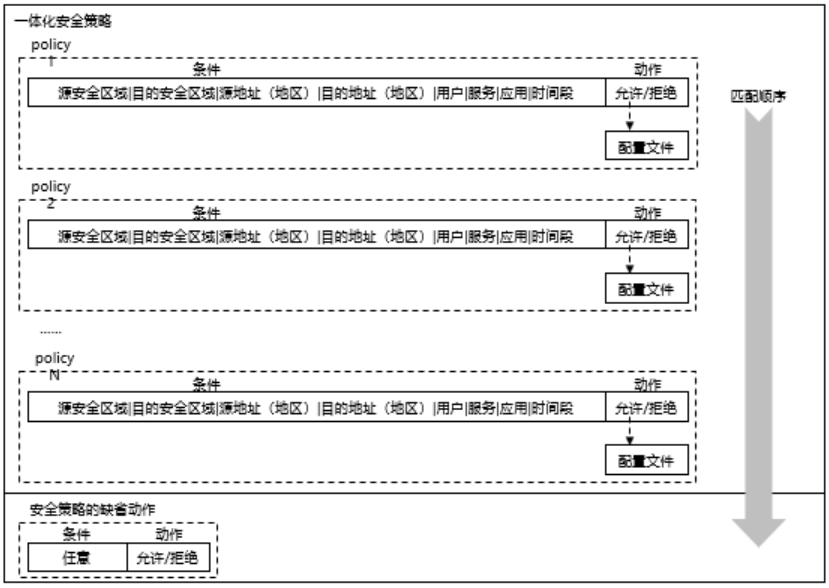


- 流量通过 NGFW 时，安全策略的处理流程如下：
- NGFW 会对收到的流量进行检测，检测出流量的属性，包括：源安全区域、目的安全区域、源地址/地区、目的地址/地区、用户、服务（源端口、目的端口、协议类型）、应用和时间段。
- NGFW 将流量的属性与安全策略的条件进行匹配。如果所有条件都匹配，则此流量成功匹配安全策略。如果其中有一个条件不匹配，则继续匹配下一条安全策略。以此类推，如果所有安全策略都不匹配，则 NGFW 会执行缺省安全策略的动作（默认为“禁止”）。
- 如果流量成功匹配一条安全策略，NGFW 将会执行此安

全策略的动作。如果动作为“禁止”，则 NGFW 会阻断此流量。如果动作为“允许”，则 NGFW 会判断安全策略是否引用了安全配置文件。如果引用了安全配置文件，则继续进行下一步处理；如果没有引用安全配置文件，则允许此流量通过。

- 如果安全策略的动作为“允许”且引用了安全配置文件，则 NGFW 会对流量进行内容安全的一体化检测。
- 一体化检测是指根据安全配置文件的条件对流量的内容进行一次检测，根据检测的结果执行安全配置文件的动作。如果其中一个安全配置文件阻断此流量，则 NGFW 阻断此流量。如果所有的安全配置文件都允许此流量转发，则 NGFW 允许此流量转发。

NGFW安全策略配置逻辑

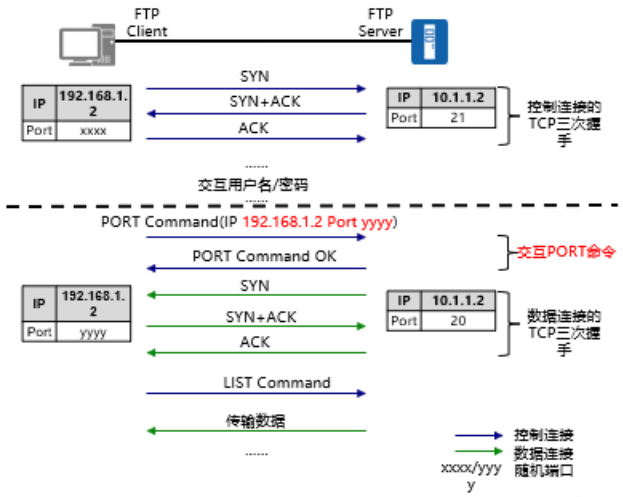


- NGFW 的安全策略应用在全局，安全区域与 IP 地址等一样只是作为可选的匹配条件。而且安全区域支持多选。
- 如果配置了多条安全策略，会从上到下依次进行匹配。如果流量匹配了某个安全策略，将不再进行下一个策略的匹配。所以需要先配置条件精确的策略，再配置宽泛的策略。
- 系统默认存在一条缺省安全策略，如果流量没有匹配到

管理员定义的安全策略，就会命中缺省安全策略（条件均为 any，动作默认为禁止）。

- 每条策略中都包含了多个匹配条件，如安全区域、用户、应用等。流量只有与安全策略的每一个条件都匹配时，才认为匹配了此安全策略。缺省情况下所有的条件均为 any，即所有流量均可以命中该策略。
- 如果一个匹配条件中可以配置多个值，则这些值之间是或的关系。即只要匹配任意一个值，就可以认为与该条件匹配。

多通道协议



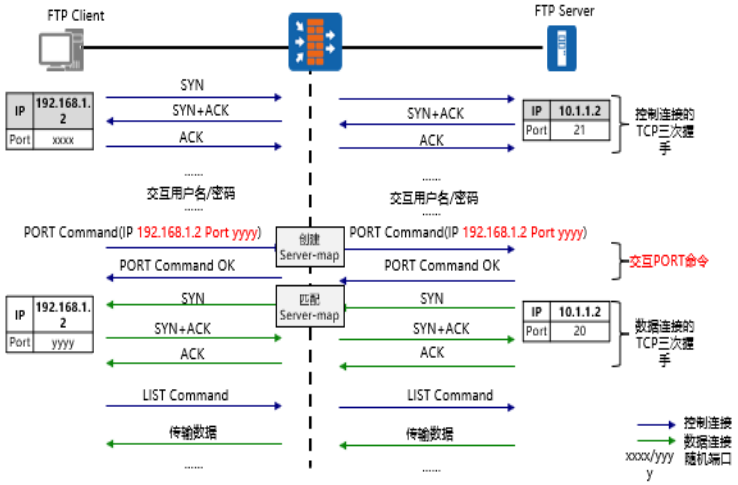
- 遇到使用随机协商端口的协议，单纯的包过滤方法无法进行数据流定义。

- 大部分多媒体应用协议（如 H.323、SIP）、FTP、netmeeting 等协议使用约定的固定端口来初始化一个控制连接，再动态的选择端口用于数据传输。端口的选择是不可预测的，其中的某些应用甚至可能要同时用到多个端口。传统的包过滤防火墙可以通过配置 ACL 过滤规则匹配单通道协议的应用传输，保障内部网络不受攻击，但只能阻止一些使用固定端口的应用，无法匹配使用协商出随机端口传输数据的多通道协议应用，留下了许多安全隐患。
- 单通道协议：通信过程中只需占用一个端口的协议。如：

WWW 只需占用 80 端口。

- 多通道协议：通信过程中需占用两个或两个以上端口的协议。如 FTP 被动模式下需占用 21 号端口以及一个随机端口。
- FTP 协议是一个典型的多通道协议，在其工作过程中，FTP Client 和 FTP Server 之间将会建立两条连接：控制连接和数据连接。控制连接用来传输 FTP 指令和参数，其中就包括建立数据连接所需要的信息；数据连接用来获取目录及传输数据。数据连接使用的端口号是在控制连接中临时协商的。根据数据连接的发起方式 FTP 协议分为两种工作模式：主动模式（PORT 模式）和被动模式（PASV 模式）。主动模式中，FTP Server 主动向 FTP Client 发起数据连接；被动模式中，FTP Server 被动接收 FTP Client 发起的数据连接。模式在一般的 FTP 客户端中都是可以设置的，这里我们以主动模式为例进行讲解。

ASPF与Server-map表



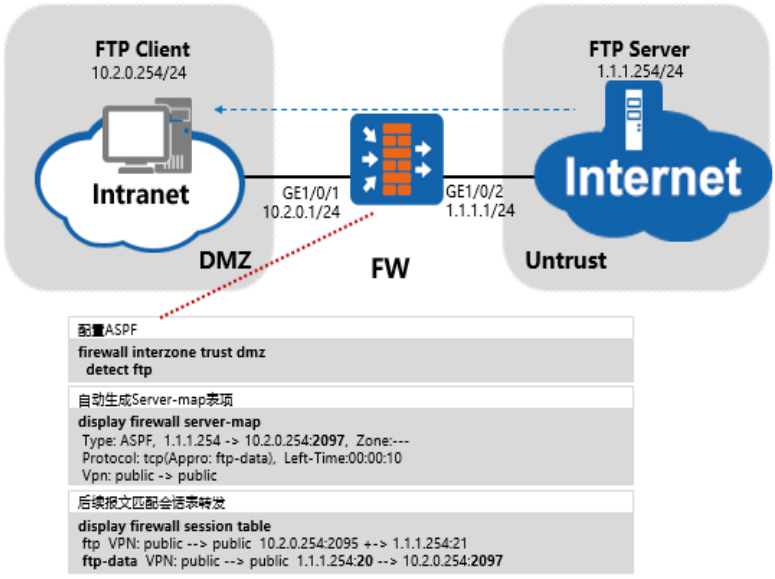
- 设备通过检测报文的应用层数据，自动获取相关信息并创建相应的会话表项，以保证这些应用的正常通信。这个功能称为ASPF，所创建的会话表项叫做Server-map表。

- 由于某些特殊应用会在通信过程中临时协商端口号等信息，所以需要设备通过检测报文的应用层数据，自动获取相关信息并创建相应的会话表项，以保证这些应用的正常通信。这

个功能称为 ASPF（Application Specific Packet Filter），所创建的会话表项叫做 Server-map 表。

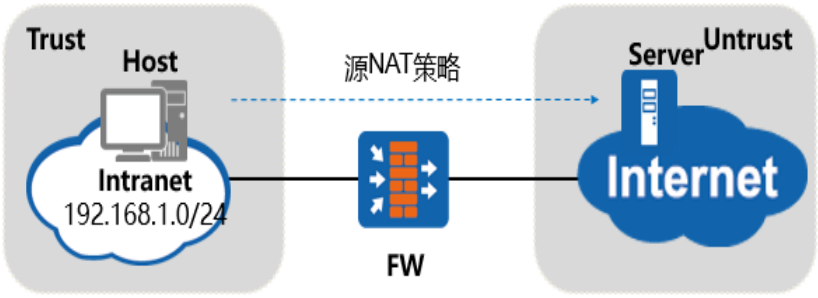
- 对于多通道协议，例如 FTP，ASPF 功能可以检查控制通道和数据通道的连接建立过程，通过生成 server-map 表项，确保 FTP 协议能够穿越设备，同时不影响设备的安全检查功能。
- Server-map 表相当于在防火墙上开通了“隐形通道”，使得像 FTP 这样的特殊应用的报文可以正常转发。当然这个通道不是随意开的，是防火墙分析了报文的应用层信息之后，提前预测到后面报文的行为方式，所以才打开了这样的一个通道。
- Server-map 通常只是用检查首个报文，通道建立后的报文还是根据会话表来转发。
- Server-map 表在防火墙转发中非常重要，不只是 ASPF 会生成，NAT Server 等特性也会生成 Server-map 表。
- 如图所示：
- Server-map 表中记录了 FTP 服务器向 FTP 客户端的 2071 端口号发起的数据连接，服务器向客户端发起数据连接时将匹配这个 Server-map 表转发，而无需再配置反向安全策略。
- 数据连接的第一个报文匹配 Server-map 表转发后，防火墙将生成这条数据连接的会话，该数据连接的后续报文匹配会话表转发，不再需要重新匹配 Server-map 表项。
- Server-map 表项由于一直没有报文匹配，经过一定老化时间后就会被删除。这种机制保证了 Server-map 表项这种较为宽松的通道能够及时被删除，保证了网络的安全性。当后续发起新的数据连接时会重新触发建立 Server-map 表项。

Server-map表



- Server-map 表与会话表的关系如下：
- Server-map 表记录了应用层数据中的关键信息，报文命中该表后，不再受安全策略的控制；
- 会话表是通信双方连接状态的具体体现；
- Server-map 表不是当前的连接信息，而是防火墙对当前连接分析后得到的即将到来报文的预测；
- 防火墙收到报文先检查是否命中会话表；
- 如果没有命中则检查是否命中 Server-map 表；
- 命中 Server-map 表的报文不受安全策略控制；
- 防火墙最后为命中 Server-map 表的数据创建会话表。

私网用户访问Internet场景



- 多个用户共享少量公网地址访问Internet的时候，可以使用源NAT技术来实现。
- 源NAT技术只对报文的源地址进行转换。

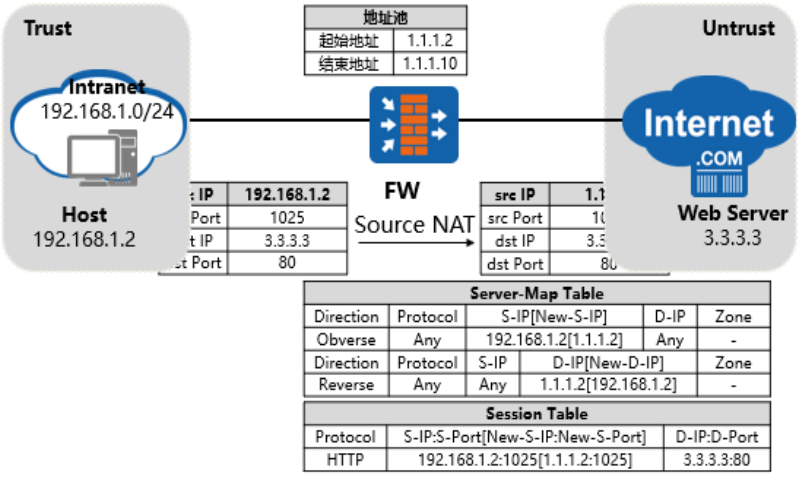
- NAT（Network Address Translation）是一种地址转换技术，可以将 IPv4 报文头中的地址转换为另一个地址。通常情况下，利用 NAT 技术将 IPv4 报文头中的私网地址转换为公网地址，可以实现位于私网的多个用户使用少量的公网地址同时访问 Internet。因此，NAT 技术常用来解决随着 Internet 规模的日益扩大而带来的 IPv4 公网地址短缺的问题。
- 在学校、公司中经常会有多个用户共享少量公网地址访问 Internet 的需求，通常情况下可以使用源 NAT 技术来实现。源 NAT 技术只对报文的源地址进行转换。通过源 NAT 策略对 IPv4 报文头中的源地址进行转换，可以实现私网用户通过公网 IP 地址访问 Internet 的目的。
- 如图所示，FW 部署在网络边界处，通过部署源 NAT 策略，可以将私有网络用户访问 Internet 的报文的源地址转换为公网地址，从而实现私网用户接入 Internet 的目的。

源NAT的两种转换方式

源NAT转换方式	含义	场景
NAT No-PAT	只转换报文的IP地址，不转换端口。	需要上网的私网用户数量少，公网IP地址数量与同时上网的最大私网用户数量基本相同。
NAPT	同时转换报文的IP地址和端口。	公网IP地址数量少，需要上网的私网用户数量大。

- 源 NAT 有多种转换方式，这里我们只介绍其中的两种。
- 不带端口转换的地址池方式（No-PAT）：
- 内部私网用户共享地址池中的 IP 地址，按照一个私网 IP 地址对应一个公网 IP 地址的方式进行转换。地址转换的同时不进行端口转换，地址池中 IP 的个数就是最多可同时上网的私网用户数。适用于某些服务需要使用特定的源端口，不允许进行源端口转换的场景。
- 带端口转换的地址池方式（NAPT）：
- 一般适用于私网用户较多的大中型网络环境，多个私网用户可以共同使用一个公网 IP 地址，根据端口区分不同用户，所以可以支持同时上网的用户数量更多。

NAT No-PAT

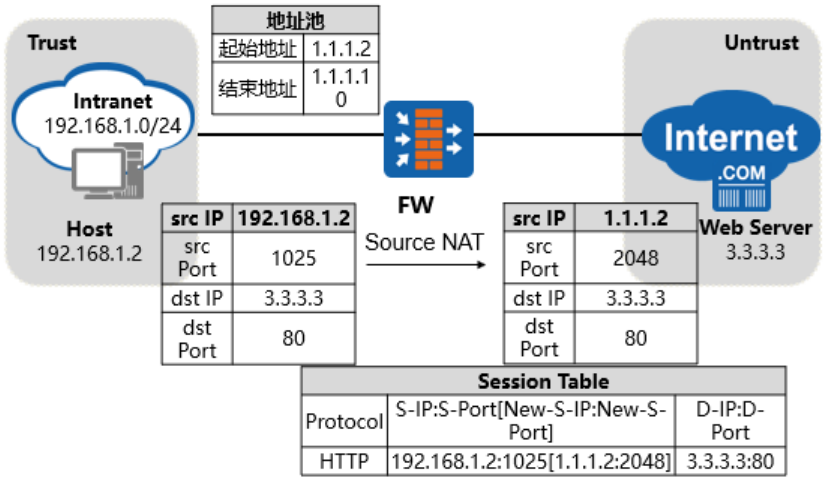


- NAT No-PAT也可以称为“**一对一地址转换**”，**只对报文的地址进行转换，不转换端口。**

- NAT No-PAT 也可以称为“一对一地址转换”，只对报文的地址进行转换，不转换端口。
- NAT No-PAT 方式通过配置 NAT 地址池来实现，NAT 地址池中可以包含多个公网地址。转换时只转换地址，不转换端口，实现私网地址到公网地址一对一的转换。
- 配置 NAT No-PAT 后，设备会为有实际流量的数据流建立 Server-map 表，用于存放私网 IP 地址与公网 IP 地址的映射关系。设备根据这种映射关系对报文的地址进行转换，然后进行转发。
- 如图所示，当 Host 访问 Web Server 时，FW 的处理过程如下：
- FW 收到 Host 发送的报文后，根据目的 IP 地址判断报文需要在 Trust 区域和 Untrust 区域之间流动，通过安全策略检查后继而查找 NAT 策略，发现需要对报文进行地址转换。
- FW 从 NAT 地址池中选择一个空闲的公网 IP 地址，替换报文的源 IP 地址，并建立 Server-map 表和会话表，然后将报文发送至 Internet。

- FW 收到 Web Server 响应 Host 的报文后，通过查找会话表匹配到上一步骤中建立的表项，将报文的目的地址替换为 Host 的 IP 地址，然后将报文发送至 Intranet。
- 此方式下，公网地址和私网地址属于一对一转换。如果地址池中的地址已经全部分配出去，则剩余内网主机访问外网时不会进行 NAT 转换，直到地址池中有空闲地址时才会进行 NAT 转换。

NAPT

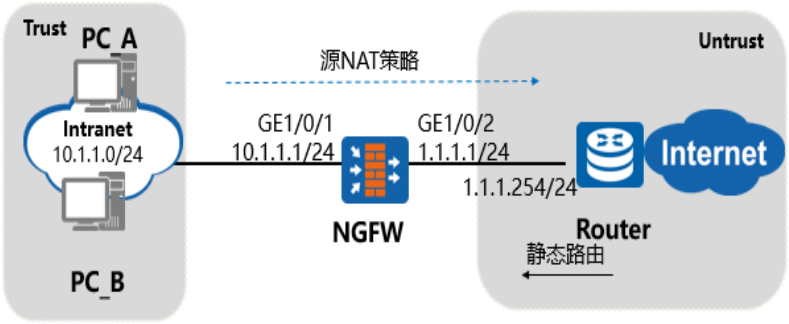


- NAPT属于“**多对一的地址转换**”，在转换过程中**同时转换报文的地址和端口。**

- NAPT 属于“多对一的地址转换”，在转换过程中同时转换报文的地址和端口。
- NAPT 方式通过配置 NAT 地址池来实现，NAT 地址池中可以包含一个或多个公网地址。转换时同时转换地址和端口，即可实现多个私网地址共用一个或多个公网地址的需求。
- 如图所示，当 Host 访问 Web Server 时，FW 的处理过程如下：
- FW 收到 Host 发送的报文后，根据目的 IP 地址判断报文需要在 Trust 区域和 Untrust 区域之间流动，通过安全策略检查后继而查找 NAT 策略，发现需要对报文进行地址转换。

- FW 从 NAT 地址池中选择一个公网 IP 地址，替换报文的源 IP 地址，同时使用新的端口号替换报文的源端口号，并建立会话表，然后将报文发送至 Internet。
- FW 收到 Web Server 响应 Host 的报文后，通过查找会话表匹配到上一步骤中建立的表项，将报文的目的地址替换为 Host 的 IP 地址，将报文的目的端口号替换为原始的端口号，然后将报文发送至 Intranet。
- 此方式下，由于地址转换的同时还进行端口的转换，可以实现多个私网用户共同使用一个公网 IP 地址上网，FW 根据端口区分不同用户，所以可以支持同时上网的用户数量更多。

NAPT配置案例



- 某公司在网络边界处部署了NGFW作为安全网关。为了使私网中10.1.1.0/24网段的用户可以正常访问Internet，需要在NGFW上配置源NAT策略。除了公网接口的IP地址外，公司还向ISP申请了2个IP地址（1.1.1.10～1.1.1.11）作为私网地址转换后的公网地址。网络环境如图所示，其中Router是ISP提供的接入网关。

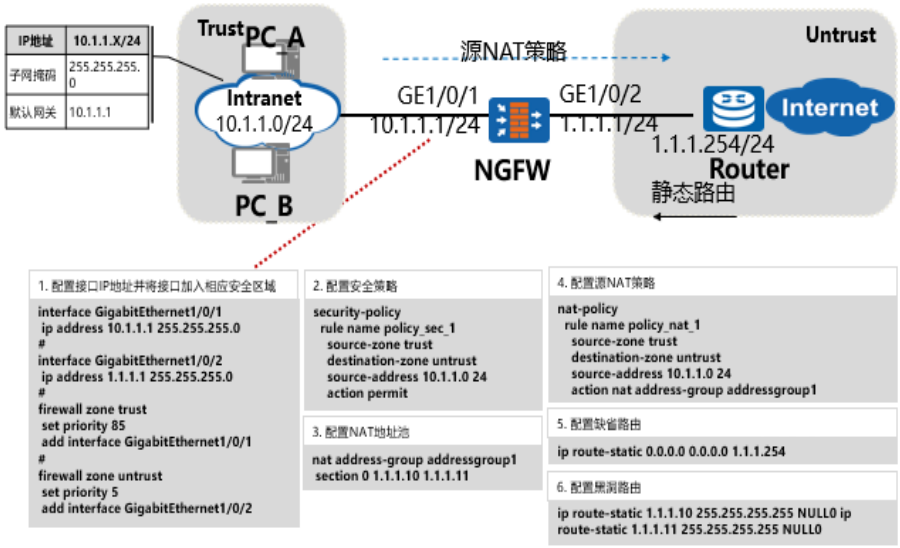
- 配置思路：
- 1. 配置接口 IP 地址和安全区域，完成网络基本参数配置。
- 2. 配置安全策略，允许私网指定网段与 Internet 进行报文交互。
- 3. 配置 NAT 地址池。
- 4. 配置源 NAT 策略，实现私网指定网段访问 Internet 时自动进行源地址转换。

- 5. 在 NGFW 上配置缺省路由，使私网流量可以正常转发至 ISP 的路由器。
- 6. 在 NGFW 上配置黑洞路由，避免 NGFW 与 Router 之间产生路由环路。
- 7. 在私网主机上配置缺省网关，使私网主机访问 Internet 时，将流量发往 NGFW。
- 8. 在 Router 上配置静态路由，使从 Internet 返回的流量可以被正常转发至 NGFW。

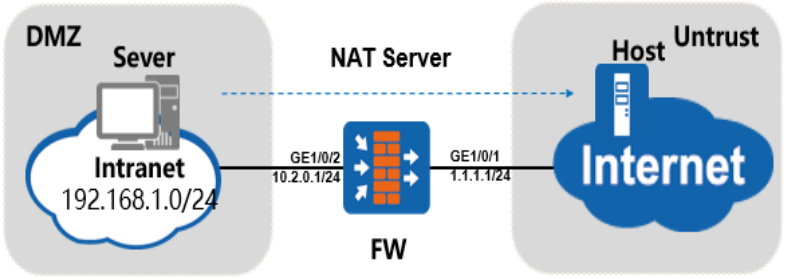
数据规划

项目		数据	说明
GigabitEthernet 1/0/1		IP地址：10.1.1.1/24 安全区域：Trust	私网主机需要将10.1.1.1配置为默认网关。
GigabitEthernet 1/0/2		IP地址：1.1.1.1/24 安全区域：Untrust	实际配置时需要按照ISP的要求进行配置。
允许访问Internet的私网网段		10.1.1.0/24	-
转换后的公网地址		1.1.1.10 ~ 1.1.1.11	由于私网地址比公网地址多，无法做到地址一一映射，所以需要开启允许端口转换，通过端口转换实现公网地址复用。
路由	NGFW缺省路由	目的地址：0.0.0.0 下一跳：1.1.1.254	为了使私网流量可以正常转发至ISP的路由器，可以在NGFW上配置去往Internet的缺省路由。
	NGFW黑洞路由	目的地址： 1.1.1.10 ~ 1.1.1.11 下一跳：NULL 0	为了避免Internet用户主动访问转换后的公网地址时，NGFW和Router之间形成路由环路。
	Router静态路由	目的地址： 1.1.1.10 ~ 1.1.1.11 下一跳：1.1.1.1	由于转换后的公网地址不存在实际接口，通过路由协议无法直接发现，所以需要在Router上手工配置静态路由。通常需要联系ISP的网络管理员配置。

NAPT配置命令



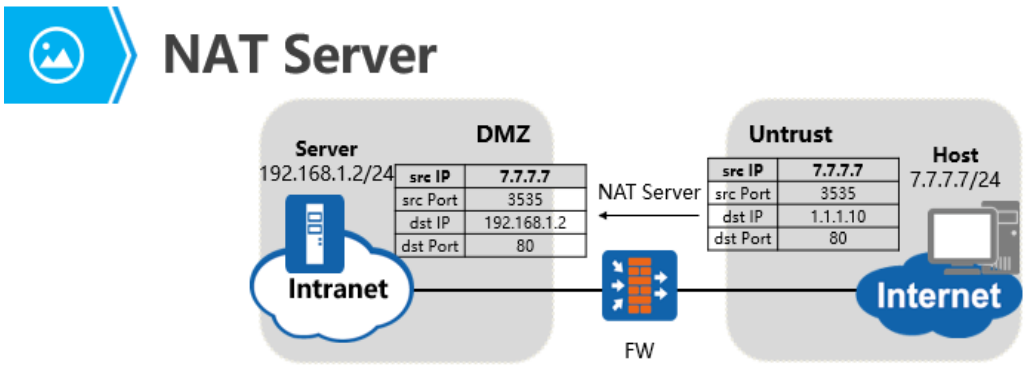
公网用户访问私网内部服务器场景



- 通过NAT Server（服务器映射）功能，可以实现外部网络用户通过公网地址访问私网内部服务器的需求。
- NAT Server功能即将某个公网IP地址映射为服务器的私网IP地址。

- 通过 NAT Server（服务器映射）功能，可以实现外部网络用户通过公网地址访问私网内部服务器的需求。
- 学校或公司会提供 Web、FTP 等服务供公网中的用户访问，服务器一般部署在私网，通过服务器映射功能使公网用户可以访问到这些位于私网的服务器。

- 如图所示，FW 提供服务器映射功能，将某个公网 IP 地址映射为服务器的私网 IP 地址，相当于为外部网络提供一个“接口”，使外部网络的用户可以通过该公网 IP 地址来访问私网内部服务器。



Server-Map Table			
Direction	Protocol	S-IP	D-IP:D-Port[New-D-IP:New-D-Port]
Obverse	TCP	Any	1.1.1.10:80[192.168.1.2:80]

Session Table		
Protocol	S-IP:S-Port	D-IP:D-Port[New-D-IP:New-D-Port
HTTP	7.7.7.7:3535	1.1.1.10:80[192.168.1.2:80]

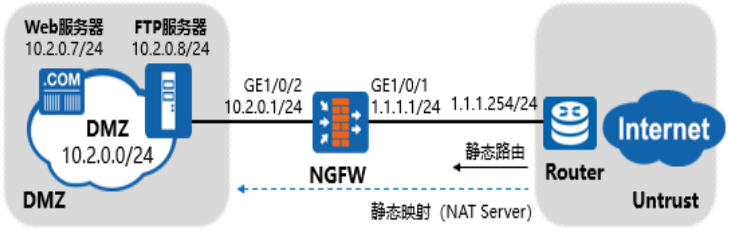
  - NAT Server提供了公网地址和私网地址的静态映射关系。
  - 在进行地址映射的过程中可以选择是否允许端口转换。

- 通常情况下，出于安全的考虑，不允许外部网络主动访问内部网络。但是在某些情况下，还是希望能够为外部网络访问内部网络提供一种途径。例如，公司需要将内部网络中的资源提供给外部网络中的客户和出差员工访问。NAT Server 也称静态映射，是一种转换报文目的 IP 地址的方式，它提供了公网地址和私网地址的映射关系，将报文中的公网地址转换为与之对应的私网地址。
- 在使用 NAT Server 功能时，外网的用户向内部服务器主动发起访问请求，该用户的 IP 地址和端口号都是不确定的，唯一可以确定的是内部服务器的 IP 地址和所提供服务的端口号。所以在配置 NAT Server 成功后，设备会自动生成 Server-map 表项，用于存放 Globle 地址与 Inside 地址的映射关系。设备根据这种映射关系对报文的地址进行转换并转发。每个生

效的 NAT Server 都会生成正反方向两个静态的 Server-map。该表项将一直存在除非静态映射的配置被删除。

- 在 FW 上配置 NAT Server，确定公网地址和私网地址的映射关系。配置完成后，FW 将会自动生成 Server-Map 表项，用于存放公网地址和私网地址的映射关系。
- 如图所示，当 Host 访问 Server 时，FW 的处理过程如下：
- FW 收到 Internet 上用户访问 1.1.1.10 的报文的首包后，查找并匹配到 Server-Map 表项，将报文的目的 IP 地址转换为 192.168.1.2。
- FW 根据目的 IP 地址判断报文需要在 Untrust 区域和 DMZ 区域之间流动，通过域间安全策略检查后建立会话表，然后将报文发送至 Intranet。
- FW 收到 Server 响应 Host 的报文后，通过查找会话表匹配到上一步骤中建立的表项，将报文的源地址替换为 1.1.1.10，然后将报文发送至 Internet。
- 后续 Host 继续发送给 Server 的报文，FW 都会直接根据会话表项的记录对其进行转换，而不会再去查找 Server-map 表项。
- 另外，FW 在进行地址映射的过程中还可以选择是否允许端口转换，是否允许服务器采用公网地址上网，以满足不同场景的需求。

NAT Server配置案例



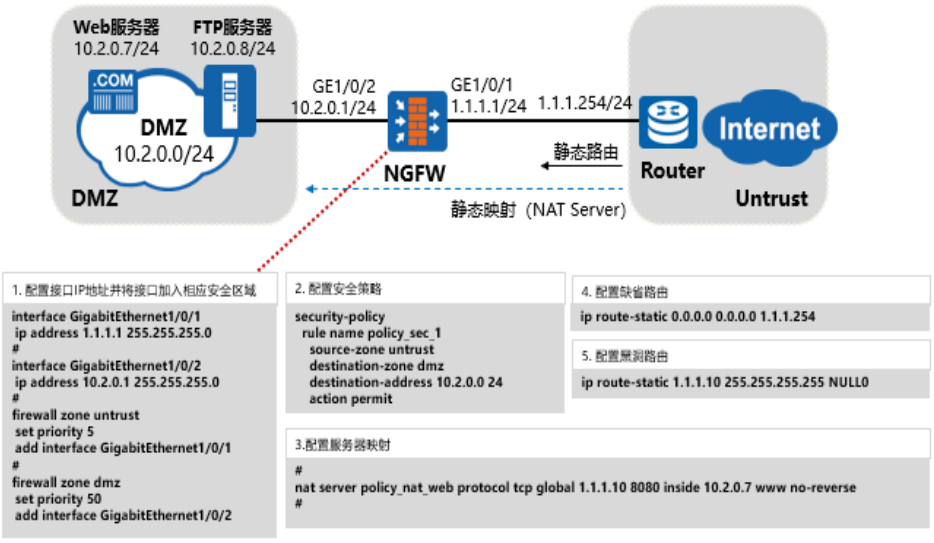
- 某公司在网络边界处部署了NGFW作为安全网关。为了使私网Web服务器能够对外提供服务，需要在NGFW上配置服务器静态映射功能。除了公网接口的IP地址外，公司还向ISP申请了一个IP地址（1.1.1.10）作为内网服务器对外提供服务的地址。网络环境如图所示，其中Router是ISP提供的接入网关。

- 配置思路：
- 1. 配置接口 IP 地址和安全区域，完成网络基本参数配置。
- 2. 配置安全策略，允许外部网络用户访问内部服务器。
- 3. 配置服务器映射功能，创建静态映射，映射内网 Web 服务器。
- 4. 在 NGFW 上配置缺省路由，使内网服务器对外提供的服务流量可以正常转发至 ISP 的路由器。
- 5. 在 NGFW 上配置黑洞路由，避免 NGFW 与 Router 之间产生路由环路。
- 6. 在 Router 上配置到服务器映射的公网地址的静态路由。

数据规划

项目		数据	说明
GigabitEthernet 1/0/1		IP地址：1.1.1.1/24 安全区域：Untrust	实际配置时需要按照ISP的要求进行配置。
GigabitEthernet 1/0/2		IP地址：10.2.0.1/24 安全区域：DMZ	内网服务器需要将10.2.0.1配置为默认网关。
服务器映射		名称： policy_nat_web 公网地址：1.1.1.10 私网地址：10.2.0.7 公网端口：8080 私网端口：80	通过该映射，使用外网用户能够访问1.1.1.10，且端口号为8080的流量能够送给内网的Web服务器。 Web服务器的私网地址为10.2.0.7，私网端口号为80。
路由	缺省路由	目的地址：0.0.0.0 下一跳：1.1.1.254	为了内网服务器对外提供的服务流量可以正常转发至ISP的路由器，可以在NGFW上配置去往Internet的缺省路由。
	黑洞路由	目的地址：1.1.1.10 下一跳：NULL 0	为了避免外网用户访问Global地址但没有匹配到Server-Map的报文，在NGFW和Router之间形成路由环路。

NAT Server配置命令

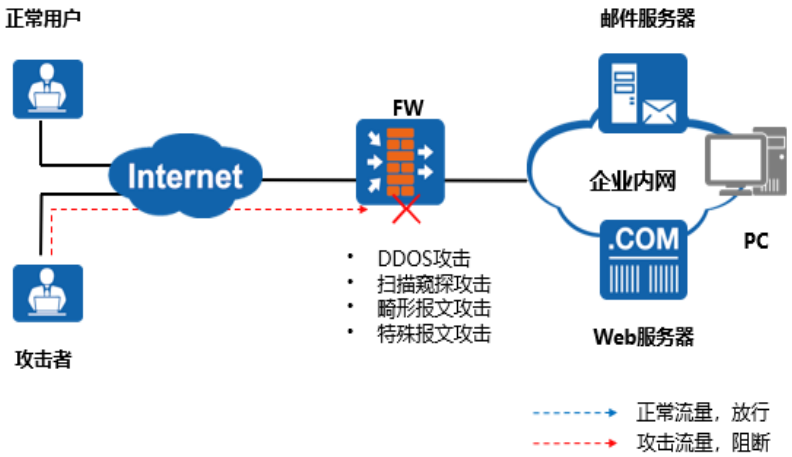


- 对于同一个内部服务器发布多个公网 IP 供外部网络访问的场景，如果不同公网 IP 所在的链路规划在不同的安全区域，可以通过配置针对不同的安全区域发布不同的公网 IP 的 NAT Server 来实现。如果不同公网 IP 所在的链路规划在同一个安全区域，可以通过配置指定 no-reverse 参数的 NAT Server 来

实现。指定 no-reverse 参数后，可以配置多个 global 地址和同一个 inside 地址建立映射关系。

- 另外，指定 no-reverse 参数后，设备生成的 Server-map 表只有正方向，内部服务器主动访问外部网络时，设备无法将内部服务器的私网地址转换成公网地址，内部服务器也就无法主动向外发起连接。因此，通过指定 no-reverse 参数可以禁止内部服务器主动访问外部网络。

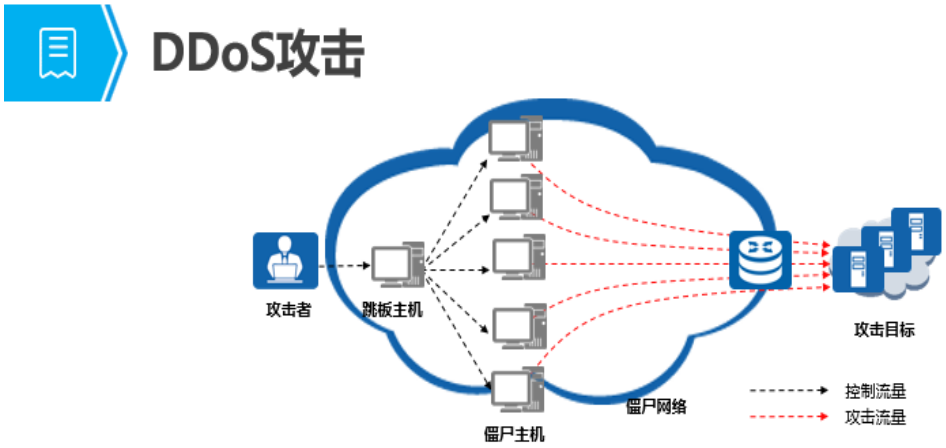
攻击防范应用场景



- 防火墙可以防范各种常见的DDoS攻击和传统的单包攻击。

- 通常情况下，在大中型企业、数据中心等网络中往往部署着服务器，而服务器（如邮件服务器、Web 服务器等）已成为网络攻击的重点。目前有针对性的攻击往往采用大流量的 DDoS 类型的攻击，如常见的 SYN Flood、UDP Flood、ICMP Flood、HTTP Flood、HTTPS Flood、DNS Flood 和 SIP Flood 攻击，这些 DDoS 类型的攻击不仅造成网络带宽拥塞，同时还严重威胁着服务器正常提供业务，甚者造成服务器宕机。
- 通过在以上网络的内网出口处部署 FW 设备，可以很好的防范各种常见的 DDoS 攻击，而且还可以对传统单包攻击进行有效的防范。

- FW 部署在企业内网出口处并开启攻击防范功能，FW 能够区分出正常流量和攻击流量，对正常流量进行放行，对于攻击流量进行阻断。从而有效保障了企业内网服务器和 PC 的正常运行，使服务器能够响应正常用户的业务需求，内网用户的 PC 能够正常工作。在这里我们主要介绍常见单包攻击的防御配置。



- DDoS（Distributed Denial of Service）即分布式拒绝服务。DDoS 攻击是指攻击者通过控制大量的僵尸主机，向被攻击目标发送大量精心构造的攻击报文，造成被攻击者所在网络的链路拥塞、系统资源耗尽，从而使被攻击者产生拒绝向正常用户的请求提供服务的效果。
- 如图所示，首先，攻击者通过各种手段，取得了网络上大量在线主机的控制权限。这些被控制的主机称为僵尸主机，攻击者和僵尸主机构成的网络称为僵尸网络。当被攻击目标确定后，攻击者控制僵尸主机向目标发送大量的攻击报文，导致被攻击目标的网络链路拥塞、系统资源耗尽。
- 目前，互联网中存在着大量的僵尸主机和僵尸网络，在

商业利益的驱使下，DDoS 攻击已经成为互联网面临的重要安全威胁。

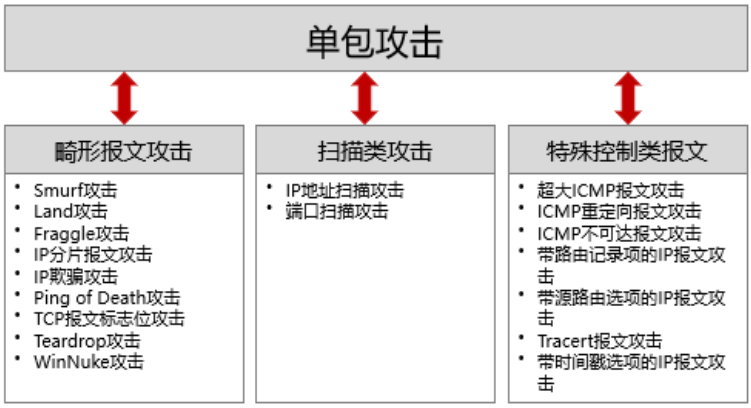
- 根据采用的攻击报文类型的不同，网络中目前存在多种 DDoS 攻击类型。NGFW 可以防范以下几种常见的 DDoS 攻击：SYN Flood、UDP Flood、ICMP Flood、HTTP Flood、HTTPS Flood、DNS Flood 和 SIP Flood 攻击。

SYN Flood和UDP Flood攻击防御配置命令

	功能		命令行
配置DDoS防范参数	开启流量统计功能。		anti-ddos flow-statistic enable
	配置DDoS流量统计抽样比。		anti-ddos statistic sampling-fraction sampling-fraction
	设置启动攻击防范和停止攻击防范的时间延迟。		anti-ddos defend-time start-delay start-delay end-delay end-delay
	配置源IP监控表的老化时间。		anti-ddos source-ip detect aging-time time
配置SYN Flood	配置全局SYN Flood攻击防御功能。		anti-ddos syn-flood source-detect [alert-rate alert-rate]
	配置接口SYN Flood攻击防御功能。		anti-ddos syn-flood source-detect [alert-rate alert-rate]
配置UDP Flood	配置全局UDP Flood攻击防范功能。	配置基于全局的UDP Flood攻击防范功能。	anti-ddos udp-flood dynamic-fingerprint-learn [alert-speed alert-speed]
		配置动态指纹的学习方式。	anti-ddos udp-fingerprint-learn offset offset fingerprint-length fingerprint-length
		启用报文长度学习功能。	anti-ddos udp-fingerprint-learn packet-length enable
	配置接口UDP Flood攻击防范功能。	配置基于接口的UDP Flood攻击防范功能。	anti-ddos udp-flood relation-defend source-detect [alert-speed alert-speed]
	配置全局UDP分片攻击防范功能。	配置基于全局的UDP分片报文攻击防范功能。	anti-ddos udp-frag-flood dynamic-fingerprint-learn [alert-speed alert-speed]
	配置接口UDP分片攻击防范功能。	配置基于接口的UDP分片报文攻击防范功能。	anti-ddos udp-frag-flood [alert-speed alert-speed]

- 开启每种 DDoS 攻击防范前，请先配置防范参数。
- 注：此处只列出 SYN Flood 和 UDP Flood 的攻击防御配置命令，其他 DDOS 攻击防御技术（如 ICMP Flood、HTTP Flood、HTTPS Flood、DNS Flood 和 SIP Flood 等）的攻击防御配置命令，以及详细的配置注意事项请参考相应型号的防火墙产品文档。

单包攻击



- 单包攻击是最常见的DoS攻击，一般都是以个人为单位的黑客发动的。

- 最常见的 DoS（（Denial of Service））攻击就是我们常常提到的单包攻击。这类攻击一般都是以个人为单位的黑客发动的，攻击报文也比较单一，虽然破坏力强大，但是只要掌握了攻击的特征，防御起来还是比较容易的。
- 单包攻击包括扫描类攻击、畸形报文类攻击和特殊报文类攻击。
- 扫描类攻击主要包括 IP 地址扫描和端口扫描，IP 地址扫描是指攻击者发送目的地址不断变化的 IP 报文（TCP/UDP/ICMP）来发现网络上存在的主机和网络，从而准确的发现潜在的攻击目标。端口扫描是指通过扫描 TCP 和 UDP 的端口，检测被攻击者的操作系统和潜在服务。攻击者通过扫描窥探就能大致了解目标系统提供的服务种类和潜在的安全漏洞，为进一步侵入系统做好准备。
- 畸形报文类攻击是指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 报文时发生错误，或者造成系统崩溃，影响目标系统的正常运行。主要的畸形报文攻击有 Ping of Death、Teardrop 等。

- 特殊报文类攻击是指攻击者利用一些合法的报文对网络进行侦察，这些报文都是合法的应用类型，只是正常网络很少用到。主要的特殊报文攻击有超大 ICMP 报文控制、Tracert 和时间戳选项 IP 报文控制等。
- 单包攻击防御是防火墙具备的最基本的防范功能，华为全系列防火墙都支持对单包攻击的防御。

单包攻击防御的配置建议

- 不建议开启比较消耗防火墙的性能的防御功能。

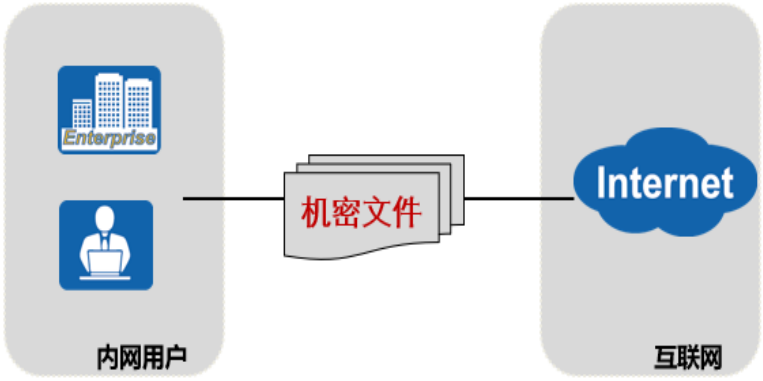
- 建议开启的单包攻击防御一般是现网比较常见的攻击，这种攻击开启以后，防火墙可以很好的进行防御，对性能等方面没有影响。而扫描类攻击在防御过程中比较消耗防火墙的性能，所以不建议开启。

单包攻击防御的配置命令

功能	命令行
开启Smurf攻击防御功能	firewall defend smurf enable
开启Land攻击防御功能	firewall defend land enable
开启Fraggle攻击防御功能	firewall defend fraggle enable
开启WinNuke攻击防御功能	firewall defend winnuke enable
开启Ping of Death攻击防御功能	firewall defend ping-of-death enable
开启带时间戳记录选项的IP报文攻击防御功能	firewall defend time-stamp enable
开启带路由记录选项的IP报文攻击防御功能	firewall defend route-record enable

- 注：此处只列出配置命令，详细的配置注意事项请参考相应型号的防火墙产品文档。

为什么需要应用行为控制

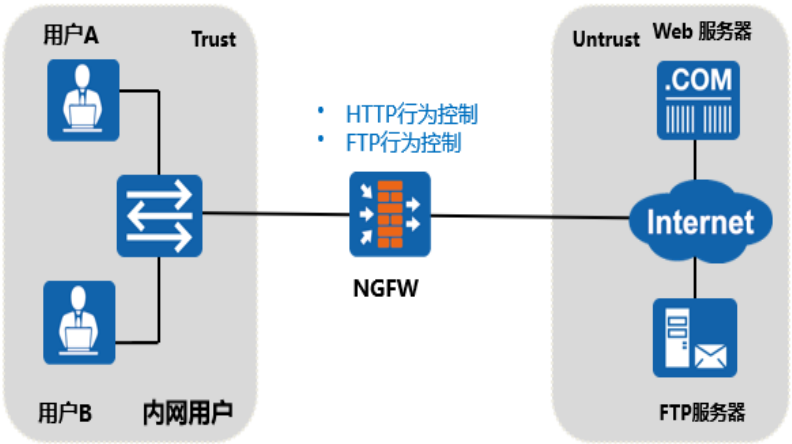


- 传统防火墙可以较好的防御自外至内的攻击，但是对于不属于前面任何一种攻击形式的企业内部的信息泄露等问题却较难控制。
- NGFW的应用行为控制功能能够有效的对内网用户的上网行为进行管理。

- 随着互联网应用的迅速发展，计算机网络在经济和生活的各个领域迅速普及，使得信息的获取、共享和传播更加方便，但同时也产生了如下问题：

- 员工通过网页不受控地对外发布、传播违规信息，影响公司形象甚至带来法律风险。
- 员工上传或发布公司的机密文件到 Internet，导致公司机密泄露。
- NGFW 的应用行为控制功能能够有效的对内网用户的上网行为进行管理。
- 使用限制：
- 应用行为控制功能受 License 控制。License 激活前，应用行为控制功能可配置，但不生效。当 License 过期后，应用行为控制功能不可用。
- 文件上传大小/文件下载大小限制对支持断点续传的文件上传/下载无效。
- HTTP 文件下载控制项用来控制采用 HTTP 协议进行文件下载的操作，如在文件下载页面选择专用的下载工具（如 BT、电驴等）进行下载，将无法对下载工具进行控制。

应用行为控制应用场景



- 应用行为控制常用于企业内部对内网用户的上网（HTTP）行为和FTP行为进行管理。

- 如图所示，在企业内部通常需要对内网用户的 HTTP 行为和 FTP 行为进行管理，不同的用户使用 HTTP 和 FTP 访问

网络资源需要不同的权限，同一用户在不同的时间段具有的权限往往也不同。NGFW 的应用行为控制能够很好的满足上述需求。

- NGFW 作为企业的出口网关部署在内网出口处，通过在 NGFW 上配置应用行为控制功能，当内网用户访问外网时，能够有效管理内网用户的 HTTP 行为和 FTP 行为。
- 在 NGFW 上创建多个应用行为控制配置文件，每个应用行为控制配置文件用来控制用户具有不同的 HTTP 和 FTP 权限。然后通过在安全策略里面引用应用行为控制配置文件、用户和时间段（工作时间、非工作时间）等对象，可以达到对内网用户的 HTTP 行为和 FTP 行为差异化、精细化管理的目的。

应用行为控制特性功能

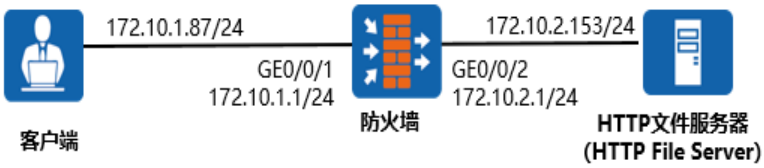
- **HTTP**
  - 浏览网页控制；
  - POST外发内容控制（包括内容大小控制）；
  - HTTP代理控制；
  - 上传、下载文件控制（包括文件大小控制）。
- **FTP**
  - 上传、下载文件控制（包括文件大小控制）；
  - 删除文件控制。

- HTTP POST 操作：HTTP POST 一般用于通过网页向服务器发送信息，例如论坛发帖、表单提交、用户名/密码登录。
- 当允许 HTTP POST 操作时，可以配置告警阈值 a 和阻断阈值 b，对 POST 操作的内容大小进行控制。
- HTTP 浏览网页：采用浏览器进行网页浏览。
- HTTP 代理上网：代理上网是指用户使用代理服务器访

问特定网站，使用该功能时 NGFW 需部署在内网用户和代理服务器之间。

- HTTP 文件上传：当允许文件上传操作时，可以配置告警阈值 a 和阻断阈值 b，对上传的文件大小进行控制。
- HTTP 文件下载：当允许文件下载操作时，可以配置告警阈值 a 和阻断阈值 b，对下载的文件大小进行控制。
- 该控制项用来控制采用 HTTP 协议进行文件下载的操作，如在文件下载页面选择专用的下载工具（如 BT、电驴等）进行下载，将无法对下载工具进行控制。
- FTP 文件上传：当允许文件上传操作时，可以配置告警阈值 a 和阻断阈值 b，对上传的文件大小进行控制。
- FTP 文件下载：当允许文件下载操作时，可以配置告警阈值 a 和阻断阈值 b，对下载的文件大小进行控制。
- 当上传或下载的文件大小、POST 操作的内容大小达到告警阈值时，系统会产生日志信息对设备管理员进行提示。
- 当上传或下载的文件大小、POST 操作的内容大小达到阻断阈值时，系统将阻断上传或下载的文件、POST 操作，并产生日志信息对设备管理员进行提示。
- 缺省情况下，系统未配置告警阈值和阻断阈值，不对上传或下载的文件大小、POST 操作的内容大小进行控制。可以单独配置告警阈值或阻断阈值，也可以同时配置告警阈值和阻断阈值。同时配置告警阈值和阻断阈值时，告警阈值必须小于阻断阈值。

应用行为控制配置实例

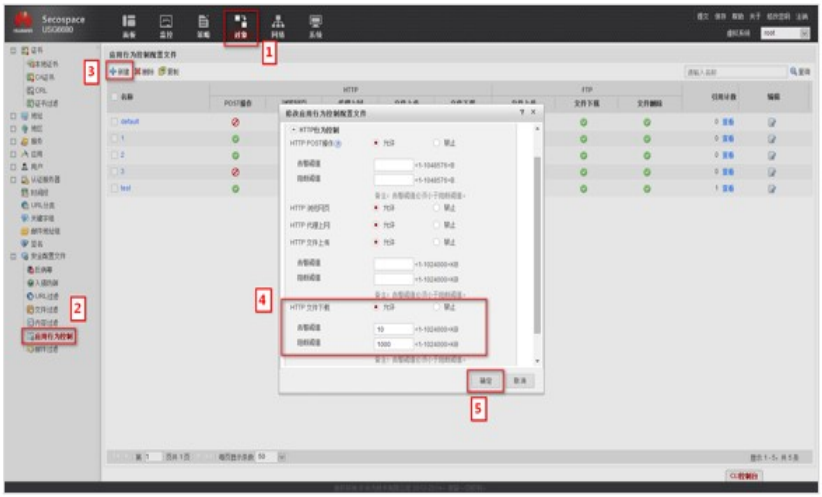


- 组网环境：客户端流量通过防火墙访问服务器。
- 防火墙、客户端、服务器接口IP配置如图所示。

- 配置思路：

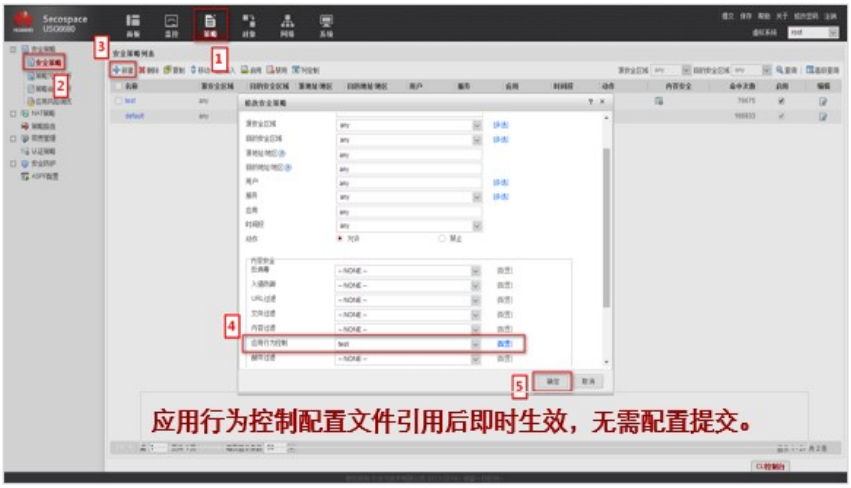
1. 创建应用行为控制的配置文件（Profile），并在其中设置需要控制的行为选项。
2. 在安全策略中创建规则（Rule），并在其中设置需要生效的域、用户、时间等信息。
3. 在规则（Rule）中引用应用行为控制配置文件（Profile）即可生效。

配置实例 - 配置应用行为控制



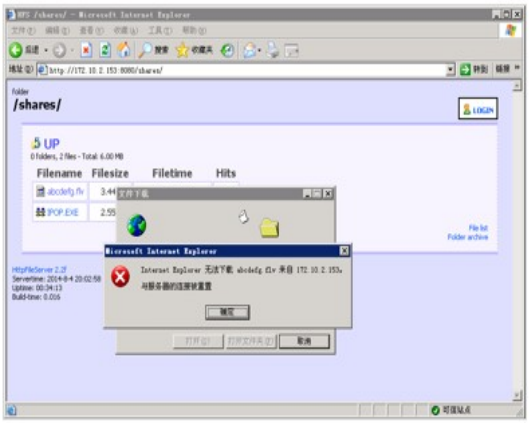
- 新建应用行为控制的配置文件，并配置HTTP下载文件的阈值。

配置实例 - 配置安全策略



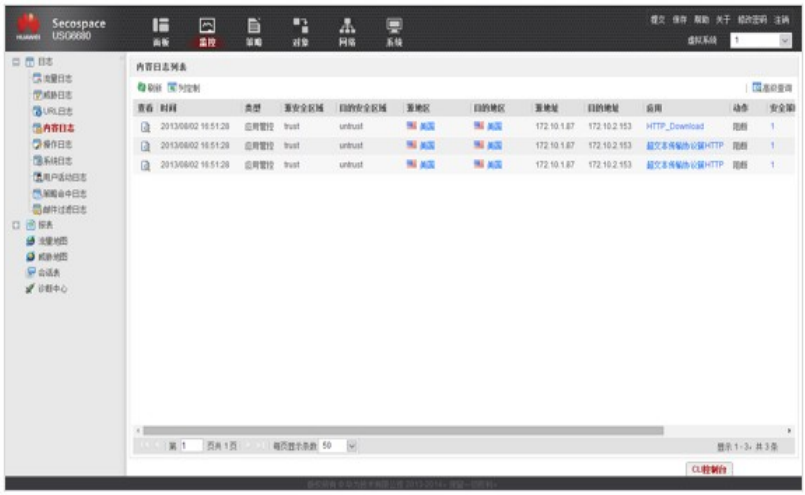
- 新建一条安全策略，并引用应用行为控制配置文件使其生效。

配置实例 - 验证配置



- 设备配置完成后，在客户端通过浏览器访问Web服务尝试下载文件，配置正确的情况下，可以看到文件被成功阻断。

配置实例 - 查看日志



- 在监控日志中可以看到，生成了相应的管控日志（如下图）。

思考题

1. 简答：如何判断防火墙上一个安全区域的受信任程度？

- 1、答案：在华为防火墙上，每个安全区域都有一个唯一的安全级别，用 1 ~ 100 的数字表示，数字越大，则代表该区域内的网络越可信。对于默认的安全区域，它们的安全级别是固定的：Local 区域的安全级别是 100，Trust 区域的安全级别是 85，DMZ 区域的安全级别是 50，Untrust 区域的安全级别是 5。