华为防火墙技术基础

一、防火墙的基本概念

1、防火墙的概念最早源于建筑领域，意在不让火势/火灾从一个区域蔓延至另一个区域

2、而后防火墙的概念被引入进通信领域，目的是在逻辑上阻止一个网络有针对性的对另一个网络发起的攻击/打击

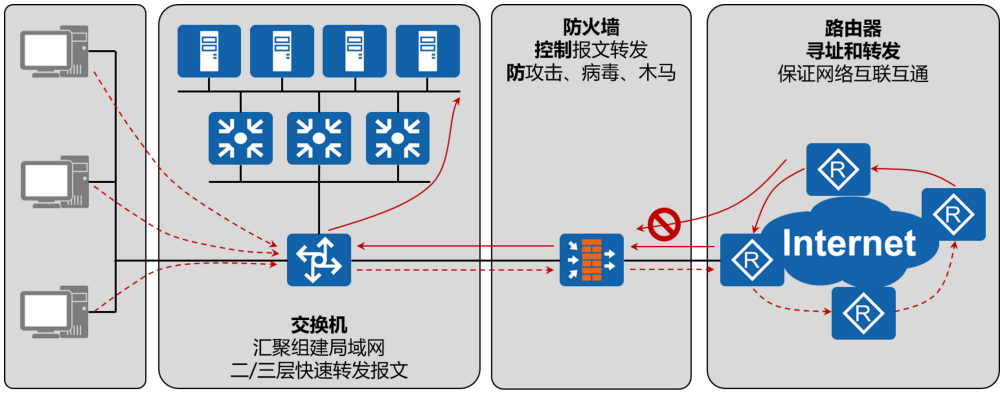
3、在条件允许的情况下，尽量不要让防火墙成为面向网络的第一人，最好让一台边界路由器直接面向互联网络，防火墙工作在边界路由器内部

4、将防火墙打造成一台3宿主堡垒主机是建议的配置，令防火墙可以清楚的区分出Untrust区域、Trust区域、DMZ区域

二、防火墙与路由器/交换机的对比

1、交换机/路由器的本质是根据MAC地址表/路由表进行数据帧/数据包的转发/路由

2、防火墙的本质是在一个已经联通的网络中对传输的数据进行控制，以达到防止病毒、木马、蠕虫等网络攻击



三、防火墙与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需求	基于对网络数据包路由而产生
目的	保证任何非允许的数据包【不通】	保持网络和数据的【联通】
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	采用的是状态化包过滤，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
防范攻击能力	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

四、防火墙的发展历史

最早的防火墙可追溯至上世纪80年代末期，距今已有二十多年的历史。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：

阶段一：1989年至1994年：

1、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

2、随后出现了代理防火墙ALG【Application Layer Gateway | 应用层网关】，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

3、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

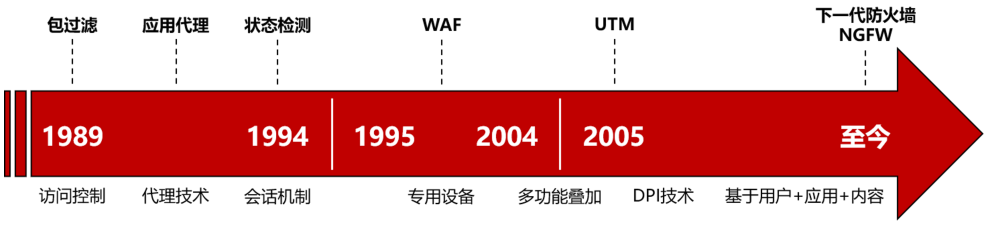
阶段二：1995年至2004年：

1、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它功能，如VPN等

2、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

阶段三：2005年至今：

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



五、华为全系列防火墙产品

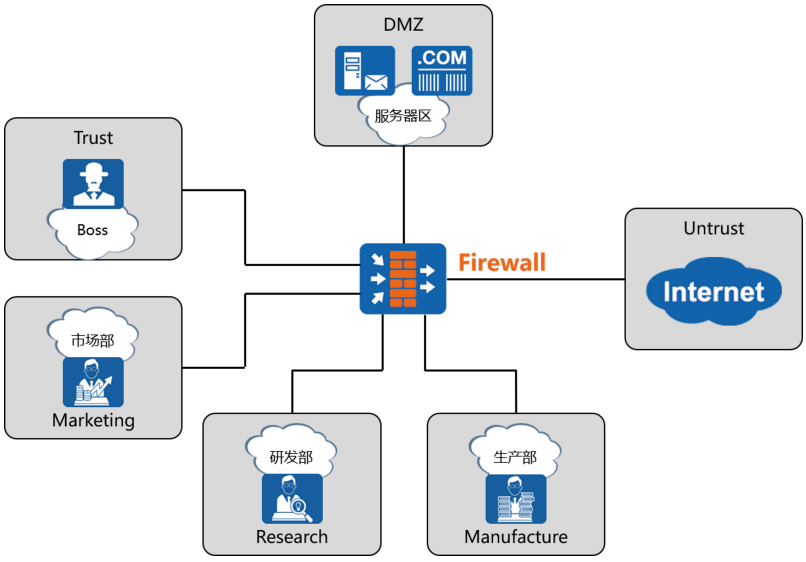
华为提供从低端至高端的全系列防火墙产品

低端：USG2100、USG2200【常用于SOHO办公、小型办公室】

终端：USG5500、USG6000系列【常用于各大企业、公司】

高端：USG9500【常用于IDC机房】

六、防火墙的安全区域

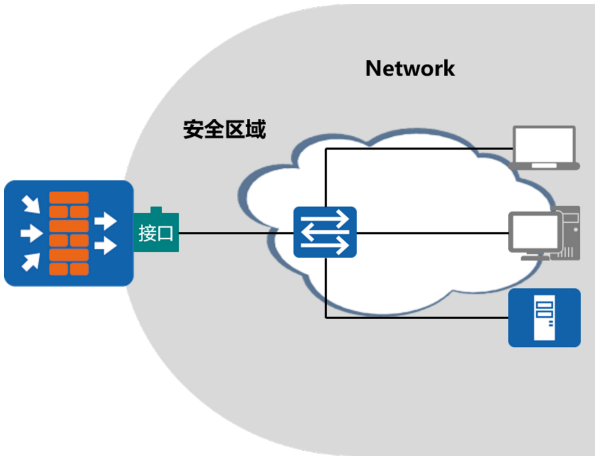


1、为了在防火墙上区分不同的网络，引入了安全区域【Security Zone】，简称为区域【Zone】的概念

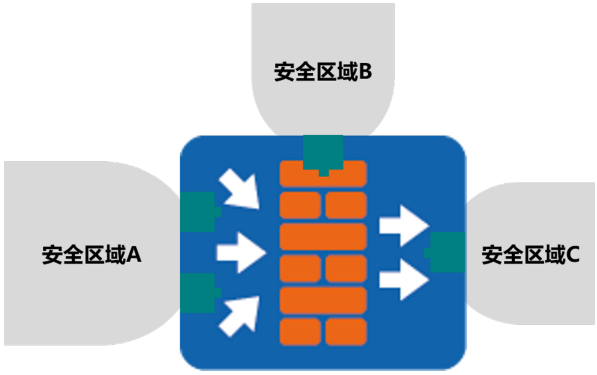
2、安全区域是一个或多个接口的集合，是防火墙区别于路由器的主要特性

3、防火墙通过安全区域来划分网络、标识数据流动的【路线】，当数据在不同的安全区域之间流动时，才会受到控制

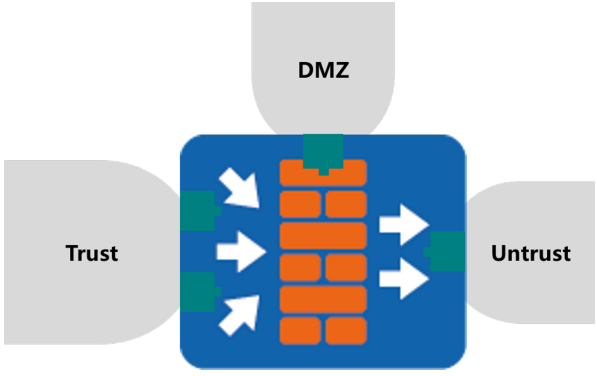
4、防火墙通过接口来连接网络，将接口划分到安全区域后，通过接口就把安全区域和网络关联起来



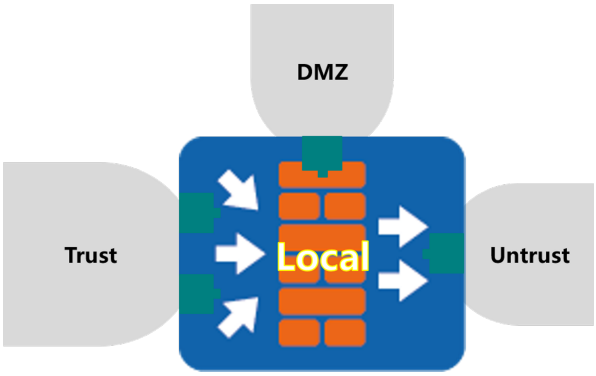
5、通过把接口划分至不同的安全区域中，便可在防火墙上划分出不同的网络
6、华为防火墙上，一个接口在同一时间内仅可加入至一个安全区域



七、防火墙上默认的安全区域
1、在华为的防火墙上，默认存在3个安全区域：
1.1、Trust【信任区域】
1.2、DMZ【非军事化区域】
1.3、Untrust【非信任区域】



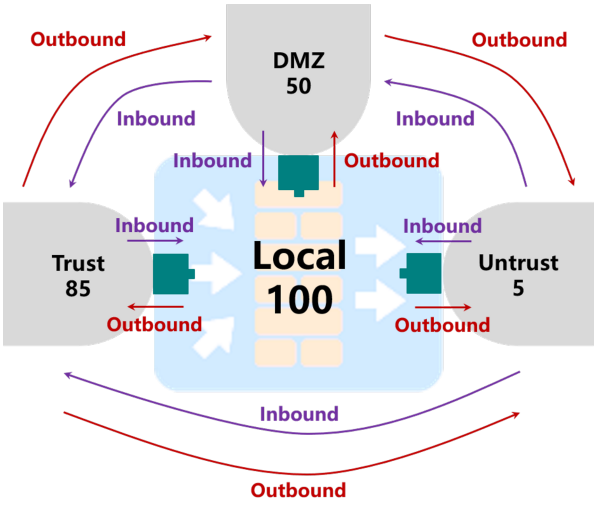
2、防火墙使用【Local】区域，标识防火墙本身
2.1、由防火墙主动发出的数据均可认为是从Local区域中发出
2.2、需要防火墙响应并处理【而非转发】的数据同样均可认为是由Local区域接收
2.3、Local区域中不能添加任何接口，防火墙上所有接口默认隐含属于Local区域
2.4、数据通过接口去往某个网络时，目的安全区域是该接口所在的安全区域
2.5、数据通过接口到达防火墙本身时，目的安全区域是Local区域



八、安全区域、受信任程度与安全级别
受信任程度：Local > Trust > DMZ > Untrust

安全区域	安全级别	具体阐述
Local	100	设备本身，包括设备的各接口本身
Trust	85	常用于定义内网终端用户所在的区域
DMZ	50	常用于定义内网服务器所在的区域
Untrust	5	常用于定义Internet等不安全的外网

九、安全域间、安全策略与数据流动方向
1、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
2、安全域间用来描述流量的传输通道，其为两个【区域】之间的唯一【道路】
3、若希望对经过这条通道的流量进行控制，则必须在通道上设立【关卡】，即安全策略
4、数据在两个安全区域之间流动时的规则：
4.1、数据由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】
4.2、数据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】



5、数据在两个方向上流动时，将会触发不同的安全检查
6、通信双方一定会交互数据，即安全域间的两个方向上均有数据的传输【数据的双向传输】
7、判断一条流量的方向应以发起该条流量的第一个数据为基准

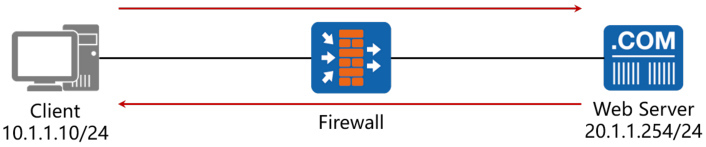
十、防火墙的缺省包过滤行为
若防火墙域间没有配置安全策略；或在查找安全策略时，所有的安全策略都没有【命中】，则默认执行域间的缺省包过滤动作为【拒绝通过】

类型	源地址	源端口	目标地址	目标端口	动作
缺省包过滤	任意				允许/拒绝

十一、包过滤技术

1、实现包过滤的核心技术是访问控制列表

2、包过滤防火墙只根据设定好的静态规则来判断是否允许数据通过



编号	源地址	源端口	目标地址	目标端口	动作
1	10.1.1.10	*	20.1.1.254	80	允许通过
2	20.1.1.254	80	10.1.1.10	*	允许通过

3、在上述案例的规则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

4、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

5、若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

注：【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

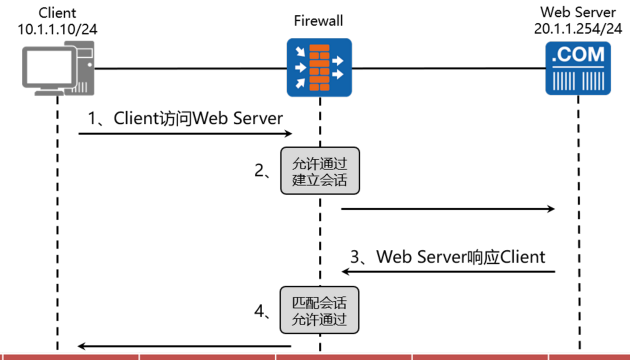
十二、状态检测与会话机制

1、若规则允许通过，状态检测防火墙会将属于同一连接的所有数据作为一个整体的数据流【会话】来对待

2、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

3、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

4、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



编号	源地址	源端口	目标地址	目标端口	动作
1	10.1.1.10	*	20.1.1.254	80	允许通过

5、状态检测防火墙以如下方式解决包过滤技术的不足的：

5.1、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

5.2、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

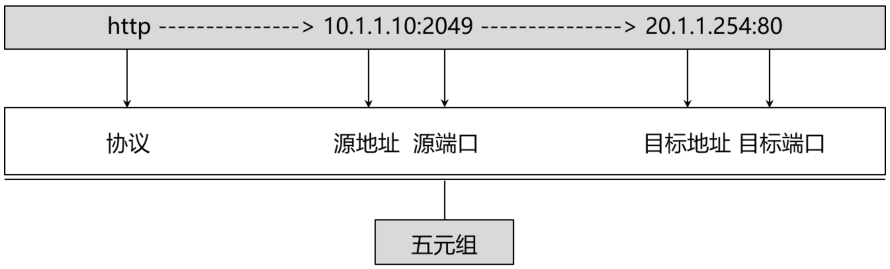
5.3、当Web服务器回应给PC的报文到达防火墙后，防火墙会把报文中的信息与会话中的信息进行比对，发现报文中的信息与会话中的信息相匹配，并且符合协议规范对后续包的定义，则认为这个报文属于PC访问Web服务器行为的后续回应报文，直接允许这个报文通过

十三、会话表项中的五元组信息

1、通过会话中的【五元组信息】可以唯一确定通信双方的一条连接

2、防火墙将要删除会话的时间称为会话的老化时间

3、一条会话表示通信双方的一个连接，多条会话的集合叫做会话表



十四、内容安全一体化检测

1、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

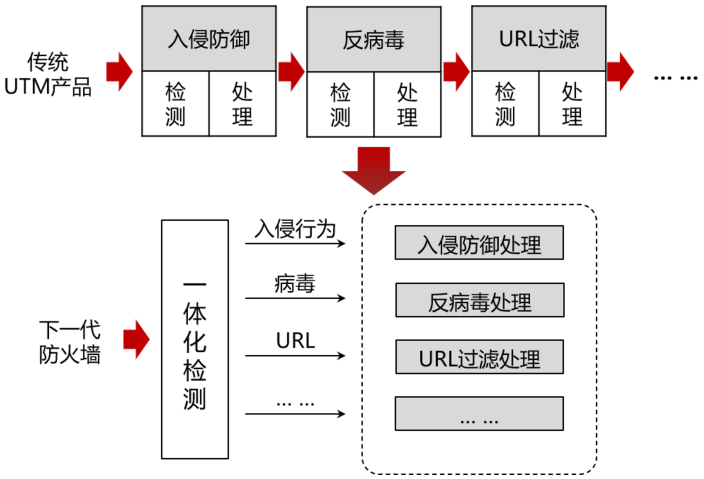
2、防火墙能够识别出流量的属性，并将流量的属性与安全策略的条件进行匹配。如果所有条件都匹配，则此流量成功匹配安全策略。流量匹配安全策略后，设备将会执行安全策略的动作

3、若动作为“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

4、若动作为“禁止”，则禁止流量通过

5、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

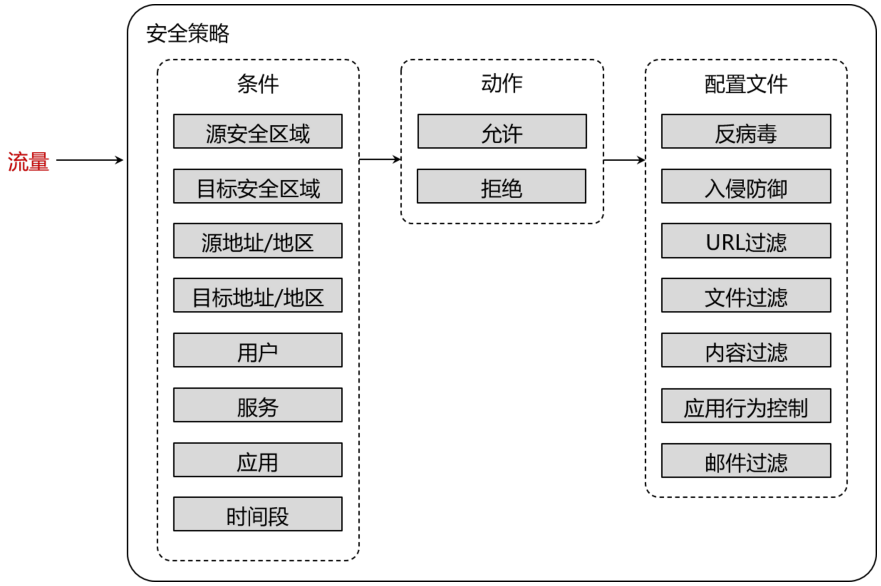
5、由于一体化检测的高效性，我们往往可以通过配置较宽泛的安全策略条件来匹配一类流量，然后再通过各种内容安全功能来保证网络安全



十五、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



1、NGFW将流量的属性与安全策略的条件进行匹配，若所有条件都匹配，则此流量成功匹配安全策略；若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，若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】

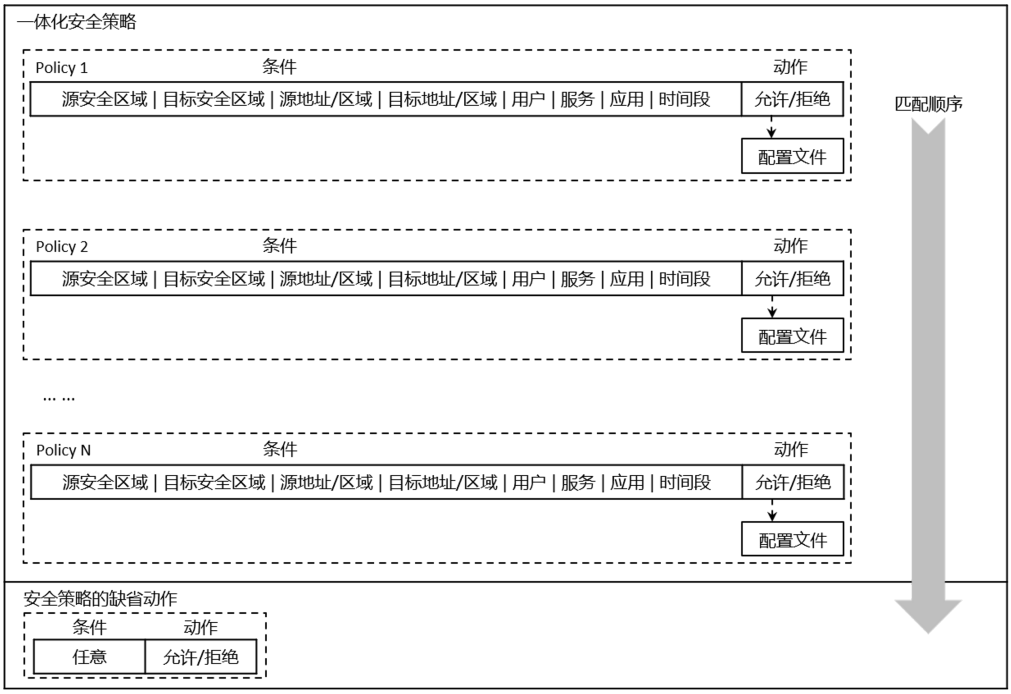
2、若流量成功匹配一条安全策略，NGFW将会执行此安全策略的动作。若动作为【禁止】，则NGFW会阻断此流量；若动作为【允许】，则NGFW会判断安全策略是否引用了安全配置文件，若引用了安全配置文件，则继续进行下一步处理；如果没有引用安全配置文件，则允许此流量通过

3、若安全策略的动作为【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

4、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；若其中一个安全配置文件阻断此流量，则NGFW阻断此流量；若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

十六、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，且安全区域支持多选



1、若配置了多条安全策略，会从上到下依次进行匹配，若流量匹配了某个安全策略，将不再进行下一个策略的匹配；因此需要先配置条件精确的策略，再配置宽泛的策略

2、系统默认存在一条缺省安全策略，若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】

3、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

4、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

5、若一个匹配条件中配置了多个值，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

十七、多通道协议

1、使用随机协商端口的协议，单纯的包过滤无法进行数据流定义

2、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

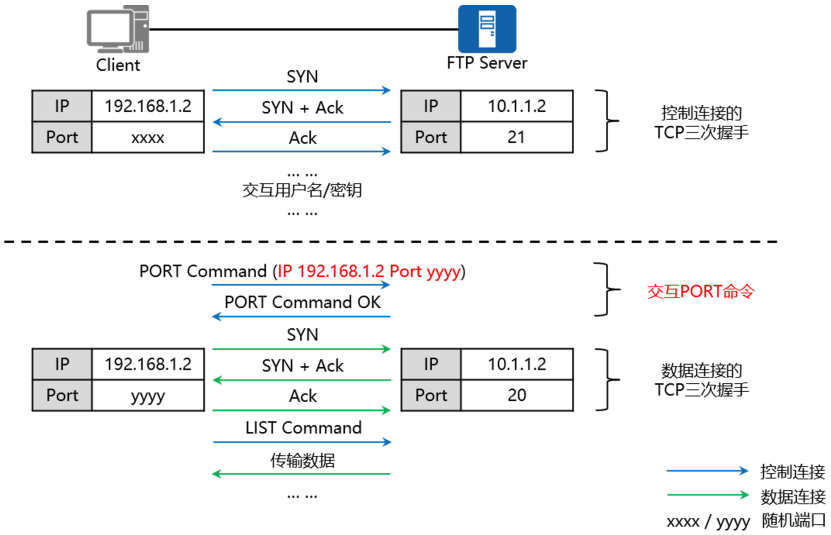
3、端口的选择是不可预测的，其中的某些应用甚至可能要同时用到多个端口

4、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

5、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

6、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

7、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



十八、ASPF与Server-map表

1、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

2、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

3、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

4、该通道不是随意开启的，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

5、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

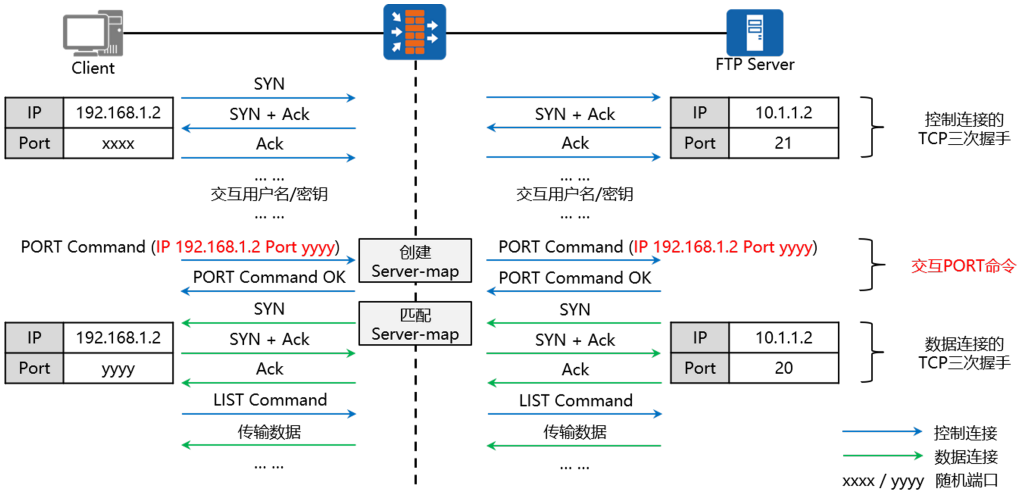
6、Server-map表在防火墙转发中非常重要，不只是ASPF会生成，NAT Server等特性也会生成Server-map表

7、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

8、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

9、Server-map表项由于一直没有报文匹配，经过一定老化时间（47s）后就会被删除

10、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



十九、防火墙安全策略的基本配置

详细配置见实验手册