

HCIE-Security 备考指南

安全策略



HCIE 只是一个开始....

HCIE 仅是一个证书...懂得做人和处事比证书和技能更重要...

希望大家顺利通过 HCIE，取得更好的职业发展！

目 录

HCIE-Security 安全策略需要掌握的知识点.....	1
安全策略简介.....	1
安全原理描述.....	2
安全策略配置指导.....	8
配置安全策略.....	13
策略冗余分析.....	17
策略命中分析.....	19
应用风险调优.....	20
举例：配置安全策略.....	27
HCIE-Security 模拟面试问题及面试建议.....	32

HCIE-Security 安全策略需要掌握的知识点

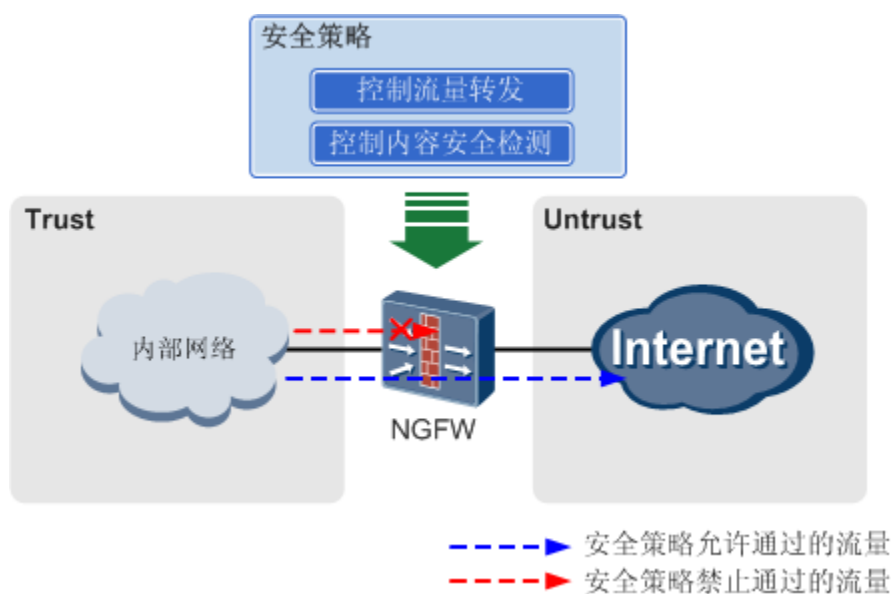
- 描述防火墙的安全策略原理及功能
- 描述防火墙的智能安全策略工作原理

安全策略简介

介绍下一代防火墙安全策略的定义和特点。

如图1所示，安全策略是控制设备对流量转发以及对流量进行内容安全一体化检测的策略。

图1 下一代防火墙的安全策略



设备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，就能实现包括反病毒、入侵防御、URL 过滤、文件过滤、内容过滤、应用行为控制、邮件过滤在内的内容安全功能。

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。

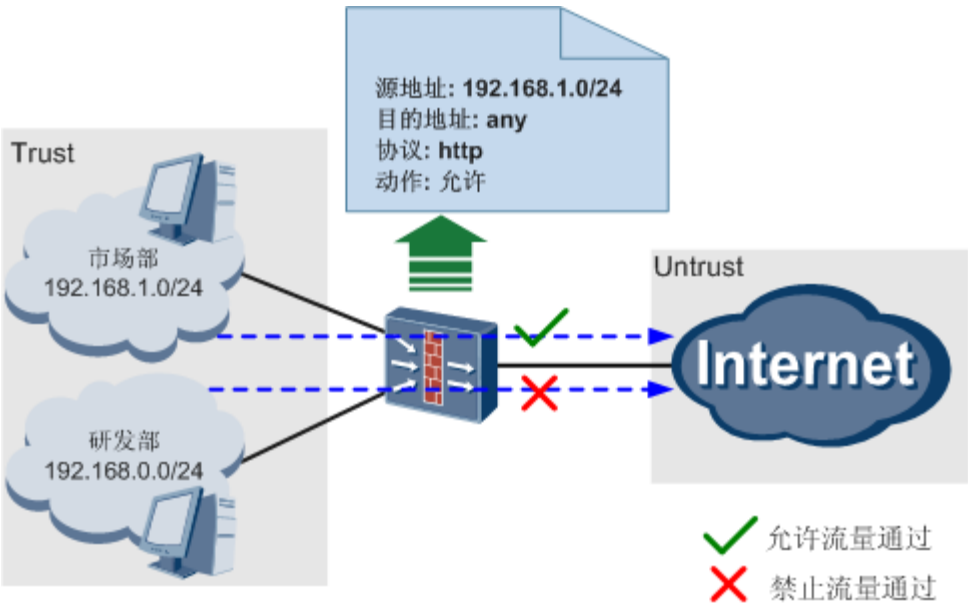
安全原理描述

安全策略实现了基于用户和应用的流量转发控制，而且还可以对流量的内容进行安全检测和处理。

传统防火墙的包过滤

传统防火墙根据五元组（源地址、目的地址、源端口、目的端口、协议类型）的包过滤规则来控制流量在安全区域间的转发。如图 1 所示，如果希望只有市场部的主机（192.168.1.0/24 网段）能够浏览 Internet 网页，则需要在 Trust 和 Untrust 区域间配置源地址为 192.168.1.0/24、目的地址为 any、协议为 HTTP（或目的端口为 80）、动作为允许的包过滤规则。

图 1 传统防火墙的包过滤



传统防火墙的包过滤反映了传统网络的特点，但随着互联网技术的不断发展，新时代网络对网络安全有了新的需求。传统网络与新时代网络特点的对比如表 1 所示。

表 1 传统网络与新时代网络对比	
传统网络的特点	新时代网络特点
用户等于 IP（例如市场部=192.168.1.0/24），用户的区分只能通过网段或安全区域的划分来实现。如果用户的 IP 地址不固定，则无法将用户与 IP 地址关联。	企业管理者希望将用户与 IP 地址动态关联起来，从而能够以可视化方式查看用户的活动，根据用户信息来审计和控制穿越网络的应用程序和内容。

表 1 传统网络与新时代网络对比	
传统网络的特点	新时代网络特点
应用等于端口，例如浏览网页的端口为 80，FTP 的端口为 21。如果想允许或限制某种应用，直接允许或禁用端口就能解决问题。	大多数应用集中在少数端口（例如 80 和 443），应用程序越来越 Web 化（例如 Web QQ、Web Mail）。允许访问 80 端口将不仅仅是允许浏览 Internet 网页，同时也可使用多种多样的基于网页的应用程序。
网络是黑白分明的，只有安全和不安全之分，即要么是安全的应用，要么是不安全的应用。对于不安全的应用全部拒绝即可，不会影响正常业务。	正常的应用程序常常会伴随不安全的流量。网络攻击由传统的单包攻击转为木马、黑客等信息窃取技术，应用和数据库存在大量的风险。

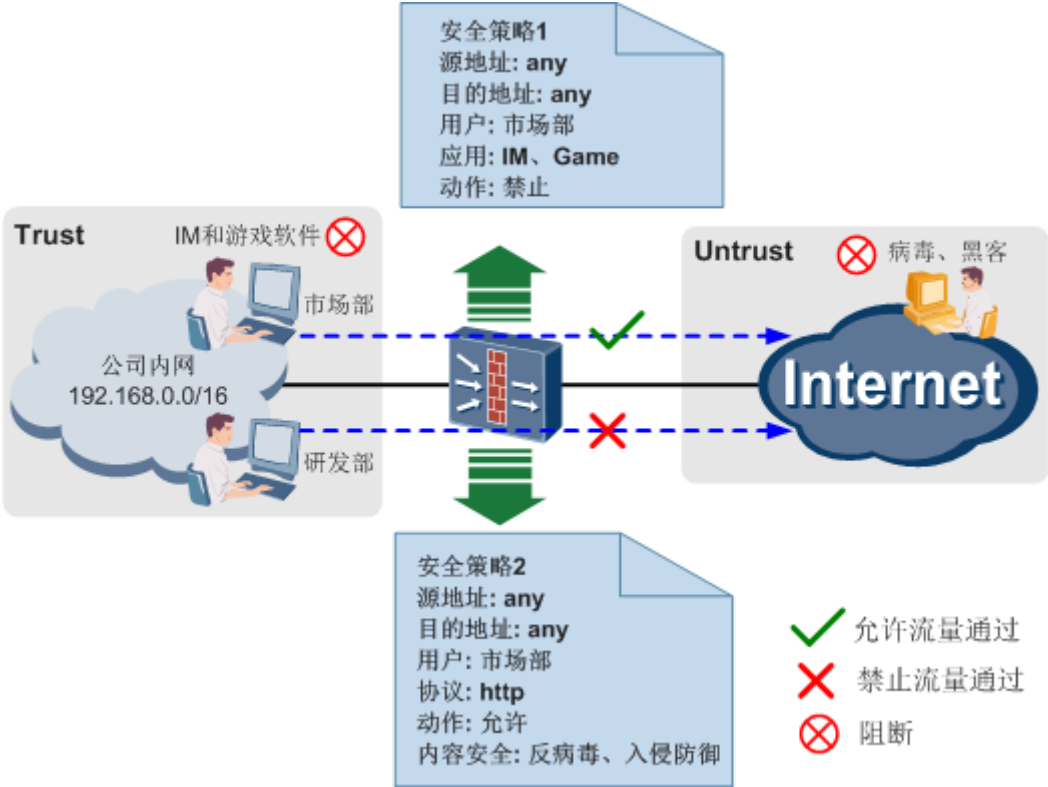
针对新时代网络的特点，防火墙越来越需要用户与应用的识别能力，以确保流量控制更精细、更可视；同时防火墙还需要对流量的内容进行安全检测与处理。

下一代防火墙的安全策略

下一代防火墙的安全策略不仅可以完全替代包过滤的功能，还进一步实现了基于用户和应用的流量转发控制，而且还可以对流量的内容进行安全检测和处理。下一代防火墙的安全策略可以更好的适应新时代网络的特点，满足新时代网络的需求。

如图 2 所示，制定安全策略 1 可以阻止市场部的用户使用 IM 和游戏应用，制定安全策略 2 允许市场部的用户浏览 Internet 网页并且对浏览的内容进行检测，防止病毒和黑客的入侵。默认安全策略会禁止研发部员工访问 Internet。

图 2 下一代防火墙的安全策略



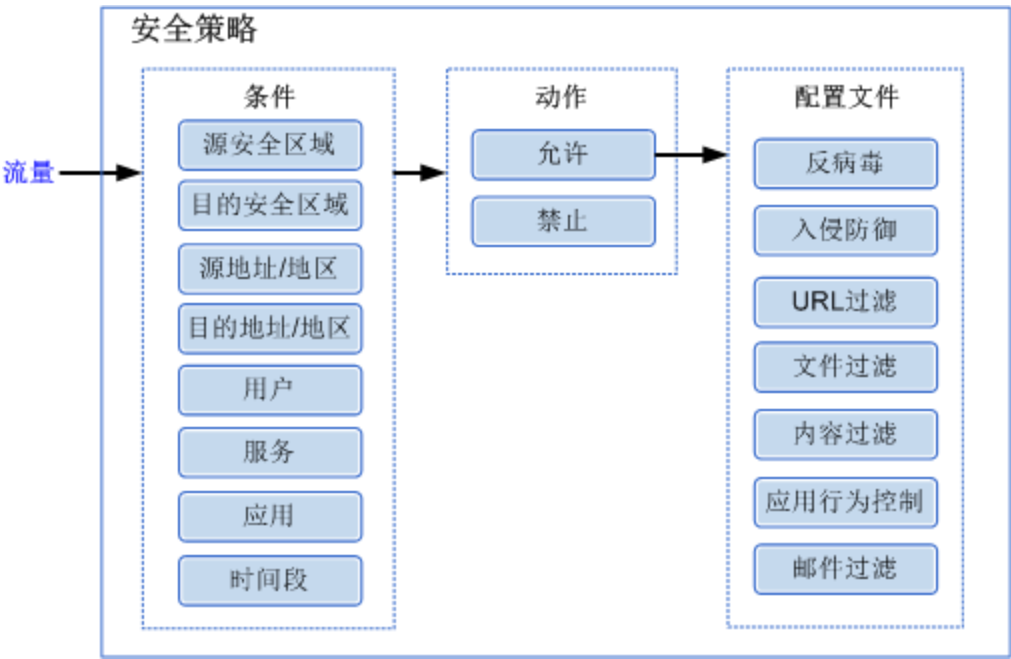
与图1的传统安全策略相比，下一代防火墙的安全策略体现了以下优势：

- 能够通过“用户”来区分不同部门的员工，使网络的管理更加灵活和可视。
- 能够有效区分协议（例如 HTTP）承载的不同应用（例如网页 IM、网页游戏等），使网络的管理更加精细。
- 能够通过安全策略实现内容安全检测，阻断病毒、黑客等的入侵，更好的保护内部网络。

下一代防火墙安全策略处理流程

下一代防火墙（NGFW）的安全策略处理流程如图3所示。

图3 下一代防火墙安全策略的处理流程



流量通过 NGFW 时，安全策略的处理流程如下：

1. 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。
2. 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”）。
3. 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，则继续进行步骤 4 的处理；如果没有引用安全配置文件，则允许此流量通过。
4. 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。

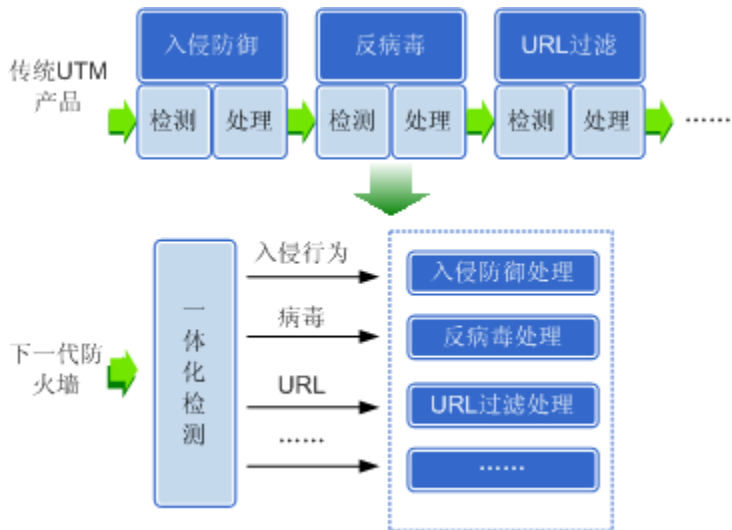
一体化检测是指根据安全配置文件的条件对流量的内容进行一次检测，根据检测的结果执行安全配置文件的动作。如果其中一个安全配置文件阻断此流量，则 NGFW 阻断此流量。如果所有安全配置文件都允许此流量转发，则 NGFW 允许此流量转发。

如[图 4](#)所示，与传统 UTM 产品在每个 UTM 模块（AV、IPS、URL 过滤）都进行内容检测相比，下一代防火墙只进行一次检测和处理，系统性能大幅度提升。

另外，NGFW 的所有内容安全功能都可以通过安全策略引用安全配置文件实现，真正做到了配置的一体化，降低了配置难度。

图 4 传统 UTM 产品与下一代防火墙的对比

表 2 安全配置文件功能	
安全配置文件	功能
反病毒	反病毒特性可以对网络中传输的文件进行病毒检测和处理，避免由病毒引起的数据破坏、系统崩溃等情况发生，保证内部网络安全。
入侵防御	入侵防御通过比较流量内容与入侵防御特征库来实现攻击检测，有效防御来自应用层的攻击，例如缓冲区溢出攻击、木马、后门攻击、蠕虫等。
URL 过滤	URL 过滤可以对用户的 URL 请求进行管控，允许或禁止用户访问某些网页资源，达到规范上网行为的目的。
文件过滤	文件过滤通过阻断特定类型的文件传输，能够降低内部网络执行恶意代码和感染病毒的风险，还能防止员工将公司机密文件泄漏到互联网。
内容过滤	内容过滤可以阻断包含特定关键字的流量，防止机密信息的泄露及敏感信息的传输。
应用行为控制	应用行为控制可以管理内网用户的 HTTP 和 FTP 行为，包括：浏览网页、发帖、代理上网、上传和下载等行为。
邮件过滤	邮件过滤可以对邮件收发行为进行管控，包括防止垃圾邮件和匿名邮件泛滥，控制违规收发等。



安全策略可以引用的安全配置文件及其功能如表 2 所示。

安全配置文件的搭配使用

合理搭配使用安全配置文件既可以实现强大的内容安全防护功能，又可以避免系统资源的浪费。

下面介绍一些安全配置文件搭配使用的技巧，如表 3 所示。

表 3 安全配置文件搭配使用		
功能	作用	安全配置文件
服务器防护	保证提供对外访问的服务器免受病毒和入侵行为的危害。	<ul style="list-style-type: none">反病毒：对传输到服务器的文件进行病毒检测和处理。入侵防御：防御对服务器的应用层攻击。文件过滤：保护文件服务器和 Web 服务器。邮件过滤：保护邮件服务器。
Web 访问防护	保证内网用户访问 Web 网站和下载文件时免受病毒和入侵行为的危害。	<ul style="list-style-type: none">URL 过滤：过滤掉非法网站和恶意网站，降低感染病毒和受到攻击的风险。反病毒：阻断 Web 访问时的病毒下载。入侵防御：阻断 Web 访问时的入侵行为。
数据泄露防护	防止公司的机密信息泄露到 Internet，保证公司的信息安全。	<ul style="list-style-type: none">文件过滤：阻断员工向外发送公司核心类型的文件，降低机密信息泄露的风险。

表 3 安全配置文件搭配使用

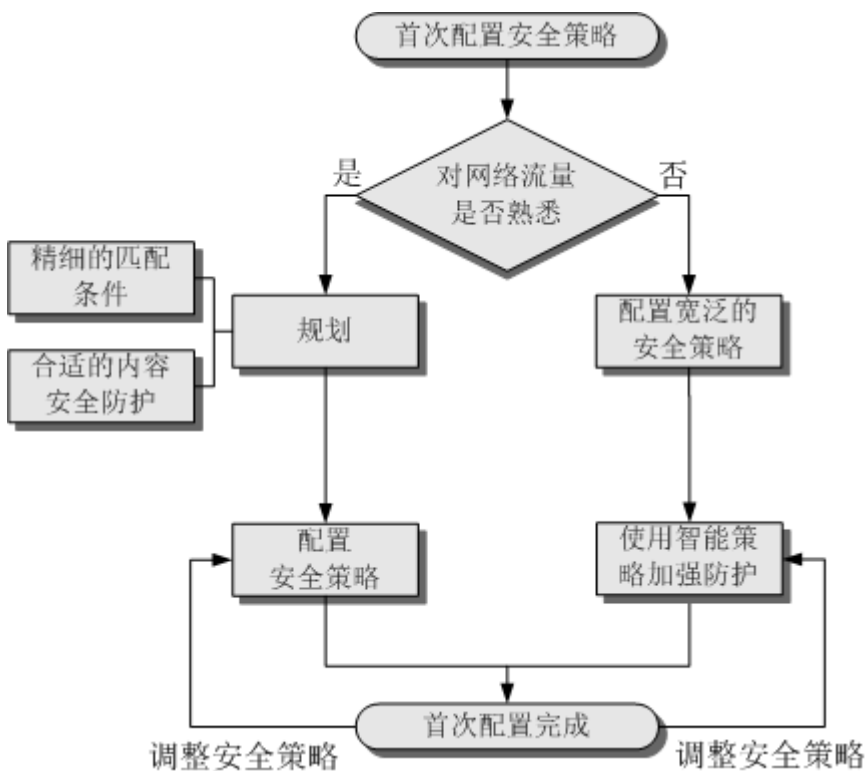
功能	作用	安全配置文件
		<ul style="list-style-type: none"> 内容过滤：对员工向外发送的文件的内容进行过滤，防止机密信息的泄露。
垃圾邮件防范	防止垃圾邮件造成服务器资源和网络资源的浪费。	<ul style="list-style-type: none"> 邮件过滤：邮件过滤中的垃圾邮件过滤功能可以有效的过滤来自垃圾邮件服务器的邮件。 内容过滤：分析出垃圾邮件内容中常见的关键字，通过内容过滤功能过滤掉包含垃圾邮件关键字的邮件。

安全策略配置指导

介绍如何合适的方式配置安全策略。

对业务比较熟悉的管理员可以通过前期的合理规划，完成安全策略的配置。当面对未知的网络流量或对应用自身存在的风险不了解，可以采用智能策略（Smart Policy）进行辅助配置。安全策略的总体配置流程如图 1 所示。

图 1 安全策略的总体配置流程



- 在首次配置安全策略时，管理员可以根据自身对网络流量或及应用属性的掌握程度，灵活选择配置方式。
 - 对于比较熟悉网络中的流量构成并知晓可能存在哪些安全风险的管理员，可以通过[安全策略常规配置思路](#)，对安全策略进行规划；在完成规划后，参考[安全策略](#)章节完成配置。
 - 对于不熟悉网络中的流量构成以及对各种应用自身隐含的风险也了解很少的管理员，通过参考配置[安全策略](#)章节，先配置基本安全策略，例如配置较为宽泛的匹配条件，这样可以为后续的分析提供数据基础；之后再根据智能策略的分析结果进一步调整到细化的策略。
- 在维护周期内，管理员既可以根据实际情况手动调整安全策略，也可以通过智能策略动态维护安全策略。

常规配置方式和智能策略并非完全独立存在。通过常规的安全策略配置方法和智能策略结合使用，既能减轻管理员的工作量，又可以借助机器双重保证网络的安全性。

安全策略常规配置思路

1. 管理员应首先明确需要划分哪几个安全区域，接口如何连接，分别加入哪些安全区域。

例如：GE1/0/1 连接外网加入 Untrust 区域，GE1/0/2 连接服务器群加入 DMZ 区域，GE1/0/3 连接办公网络加入 Trust 区域。

2. 管理员选择根据“源地址”或“用户”来区分企业员工。

- “源地址”适用于 IP 地址固定或企业规模较小的情况。如果选择根据“源地址”，则需要为不同部门的员工规划 IP 和网段。

例如研发员工的 IP 地址都规划在 10.1.0.0/24 网段，市场员工的 IP 地址都规划在 10.1.1.0/24 网段。

- “用户”适用于 IP 地址不固定且企业规模较大的情况。如果选择根据“用户”，则需要为每个员工定义一个“用户”，为每个部门定义一个“用户组”，并且将同一部门的“用户”加入代表部门的“用户组”。

3. 先确定每个用户组的权限，然后再确定特殊用户的权限。包括用户所处的源安全区域和地址，用户需要访问的目的安全区域和地址，用户能够使用哪些服务和应用，用户的网络访问权限在哪些时间段生效等。如果想允许某种网络访问，则配置安全策略的动作为“允许”；如果想禁止某种网络访问，则配置安全策略的动作为“禁止”。

例如：研发员工只能在非工作时间访问外网，且不能使用“娱乐”类别的应用。市场员工可以在任何时间访问外网，但是不能使用“Game”子类别的应用。管理者（特殊用户）可以自由访问外网。

4. 确定对哪些通过防火墙的流量进行内容安全检测，进行哪些内容安全检测。
 - 安全策略的匹配条件决定了对哪些流量进行内容安全检测。例如对市场员工访问 Internet 的 HTTP 流量进行内容安全检测。
 - 配置安全策略时引用哪些配置文件决定了进行哪些内容安全检测。例如引用了反病毒和内容过滤配置文件，就对匹配安全策略的流量进行反病毒和内容过滤检测。
5. 将以上步骤规划出的安全策略的参数一一列出，并将所有安全策略按照先精确（条件细化的、特殊的策略）再宽泛（条件为大范围的策略）的顺序排序。在配置安全策略时需要按照此顺序进行配置。

如图 2 中红框所示，安全策略“policy_sec_management”的“用户”参数比“policy_sec_1”更精确，因此需要先配置“policy_sec_management”。

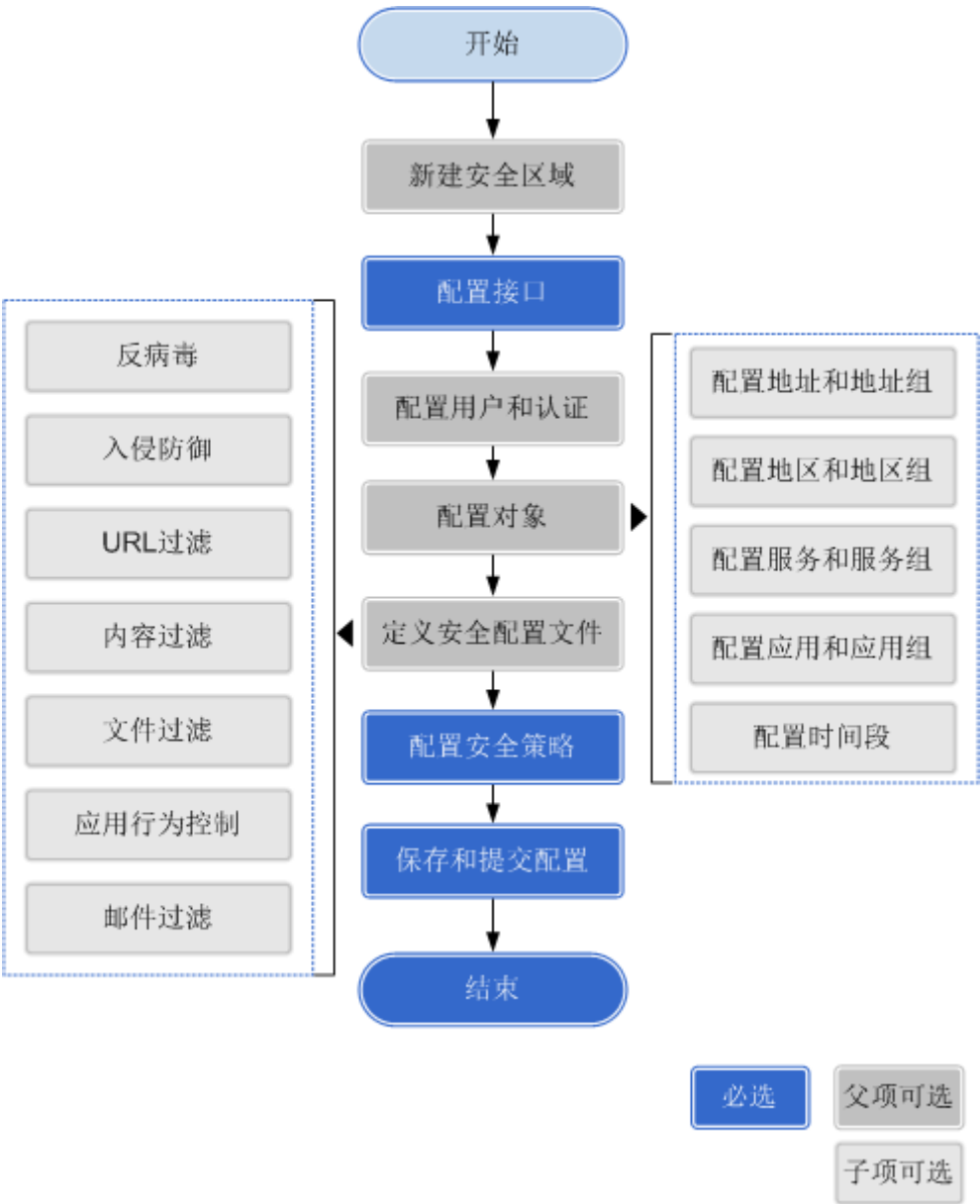
安全策略“policy_sec_1”的“应用”参数比“policy_sec_2”更精确，因此需要先配置“policy_sec_1”。

图 2 安全策略配置顺序

名称	源安全区域	目的安全区域	源地址	目的地址	用户	服务	应用	时间段	动作
policy_sec_management	trust	untrust	any	any	/management	any	Entertainment	any	允许
policy_sec_1	trust	untrust	any	any	any	any	Entertainment	any	禁止
policy_sec_2	trust	untrust	any	any	any	any	any	any	允许

安全策略的常规配置流程如图 3 所示。由图可见安全策略中用到的参数都需要在配置安全策略前创建完成，包括：安全区域、用户和认证、对象和安全配置文件。

图 3 安全策略配置流程图



使用智能策略辅助配置

迎来下一代防火墙之后，安全策略的逻辑变得十分复杂，管理员手动调整安全策略不仅低效且容易出错，产生许多冗余无效的安全策略，不容易被发现；另外，由于应用也会携带一些安全风险，导致许多安全策略本身存在安全隐患。这些问题给管理员带来了新的管理挑战，包括但不限于以下场景需求：

- 精简安全策略，简化管理

随着企业业务的发展，为了持续保证安全性，企业管理员需要不断调整防火墙策略，必然导致防火墙策略数量不断增加，存在大量冗余、无效的策略。加之企业管理员很难判断出哪些策略存在问题，即使判断出来也因为担心影响业务不敢轻易调整。

- 基于最小授权原则进行管控

最小授权原则是指仅允许企业业务必需的应用，超出范围的应用访问必须额外申请。但面对数以千计的应用，企业管理员通常不清楚如何将企业必需的应用映射为设备已定义的应用。目前，大部分使用下一代防火墙的企业通常基于应用类别进行应用管控。例如，如果企业有对外即时通讯的需求，就会允许 IM 类别的所有软件。这种做法管理起来比较简单，却引入了极大的安全隐患。因为业务需求之外的应用很可能包含漏洞、携带恶意代码和后门程序，被攻击者所利用；即使是业务必需的应用，同样也可能存在安全风险，应该进行入侵防御、反病毒、数据防泄漏等进一步的安全防护。

为了降低防火墙安全策略的管理成本，华为公司在下一代防火墙中提出智能策略，作为维护管理的重要工具，满足不同场景中的管理需求，可以迅速提升企业管理员的工作效率和维护质量。智能策略提供以下实用的分析工具，协助企业管理员迅速完成配置和维护工作。

- 策略冗余分析

通过先进的算法协助企业管理员识别完全相同和完全被包含的策略，为配置和维护提供有力参考。

- 策略命中分析

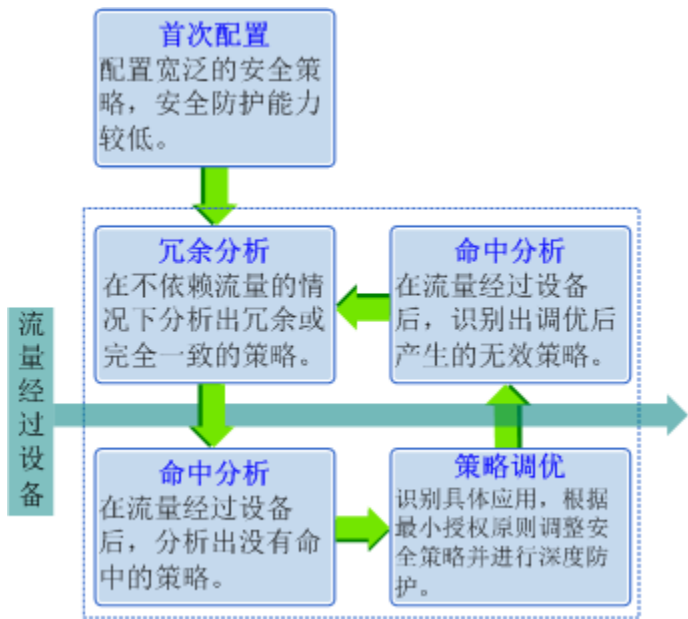
下一代防火墙可以分析出指定时间内没有命中的策略，企业管理员可以选择修改或删除安全策略，还原一个简洁易用的防火墙策略体系。

- 应用风险调优

- 由基于服务（端口）的安全策略向基于应用的安全策略转换，制定符合最小授权原则的安全策略。
- 针对安全策略中应用携带的风险进行深度防护，如部署入侵防御、反病毒等措施进一步保障企业信息安全。

由于企业的网络环境千变万化，防火墙安全策略的时效性难以保证，即企业管理员很难及时发现流量中包含的风险并对安全策略进行相应的调整。如[图 4](#)所示，企业管理员可以在防火墙的整个生命周期中循环使用智能策略的分析工具，从而提高安全策略的时效性，持续保护企业内网安全。

图 4 智能策略使用周期



配置安全策略

介绍安全策略的配置步骤。

操作步骤

1. 选择“策略 > 安全策略 > 安全策略”。
2. 单击“新建”。
3. **可选：**对于常见的办公场景，设备预置了相应的安全策略模板。管理员可以直接选择合适的模板，设备会自动配置相应的应用分类、时间段、动作以及内容安全防护措施。
4. 配置安全策略规则的名称和描述。





参数	说明
名称	输入安全策略规则的名称。名称必须是唯一的，不能有重复的名称。
描述	输入安全策略规则的描述信息。合理填写描述信息有助于管理员正确理解安全策略规则的功能，使规则变得方便选择、查找和维护。

5. 配置安全策略规则的匹配条件。

说明：

- 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。

参数	说明
源安全区域	源安全区域是指流量发出的安全区域。安全区域包括系统缺省存在和用户自定义的安全区域。
目的安全区域	目的安全区域是指流量去往的安全区域。安全区域包括系统缺省存在和用户自定义的安全区域。
源地址/地区	<p>“源地址/地区”是指流量的源 IP 地址或 MAC 地址。当安全策略使用“用户”时，“源地址/地区”可以无需配置。</p> <ul style="list-style-type: none"> • 地址和地址组：管理员可以指定一个单独的 IP/MAC 地址或者 IP 地址范围，还可以通过地址组来划定不方便通过掩码指定的 IP 地址范围、MAC 地址集合。 • 地区和地区组：管理员可以通过指定地区或地址地区组，将某些地区的 IP 地址作为策略的匹配条件。 <p>配置时可以手动输入 IP/MAC 地址或者从下拉列表中选择已有的地址对象。下拉列表中的地址对象包含如下几类：</p> <ul style="list-style-type: none"> •  图标代表地址。 •  图标代表地址组。 •  或国旗图标代表地区，先显示自定义地区再显示预定义地区。地区相当于以地区为单位的 IP 地址集合。 •  图标代表地区组。 <p>说明： 当使用 MAC 地址作为策略匹配条件时，需注意：</p> <ul style="list-style-type: none"> • 如果 NGFW 与内网之间直连或通过二层交换机相连，可以直接以 MAC 地址作为匹配条件。 • 如果 NGFW 与内网之间通过三层网络设备相连，首先需要配置 NGFW 的跨三层 MAC 识别功能，再以 MAC 地址作为匹配条件。
目的地址/地区	<p>“目的地址/地区”是指流量的目的 IP 地址或 MAC 地址。“目的地址/地区”通常代表了用户可以访问的目标主机和服务器。</p> <p>“目的地址/地区”的取值类型和配置方法同“源地址/地区”。</p>
用户	<p>用户是流量的所有者，代表了“谁”发出的流量。用户组是一类具有相同权限的用户的集合。</p> <p>设备可以精确的识别出“用户”，并通过此参数实现基于用户的网络行为控制和网络权限分配。</p>

参数	说明
	用户和用户组通常是企业组织结构的体现。管理员可以根据企业的部门进行分层来创建用户组（部门）和用户。
服务	<p>服务代表了流量的协议类型。服务包括预定义服务和自定义服务。</p> <ul style="list-style-type: none"> 预定义服务是指系统缺省已经存在，可以直接选择的服务类型。预定义服务通常都是知名协议，例如 HTTP、FTP、Telnet 等。 自定义服务是指管理员可以通过指定端口号等信息来自行定义一些协议类型。自定义服务包括三大类： <ul style="list-style-type: none"> 对于 TCP/UDP 报文，通过指定源端口和目的端口来自定义协议类型。 对于 ICMP 报文，通过 ICMP 类型和代码两个字段来自定义协议类型。 对于 IP 报文，通过 IP 报文首部中的协议号来自定义协议类型。 <p>管理员还可以创建服务组，并在其中添加多种预定义服务和已经创建的自定义服务。</p>
应用	<p>应用是指流量的应用类型。应用的定义比服务更加细化一些，是指某一具体的应用程序。应用包括预定义应用和自定义应用。</p> <ul style="list-style-type: none"> 预定义应用是指系统缺省已经存在，可以直接选择的应用类型，例如 BT、PPLive、Thunder 等。 自定义应用是管理员根据应用的特征去自定义的一个新的应用，是预定义应用的补充。 <p>管理员还可以创建应用组，并在其中添加多种预定义应用和已经创建的自定义应用。</p>
时间段	<p>时间段可以控制安全策略的生效时间。时间段可以是周期时间段（每周五晚上 19:00 至 22:00）和连续时间段（2012/5/1 晚上 19:00 至 2012/5/2 晚上 19:00）。</p>

6. 配置安全策略规则的动作。

选择对匹配安全策略的流量进行的控制动作，包括：

- 允许：如果动作为允许，则设备会判断安全策略是否引用了配置文件。如果没有引用内容安全配置文件，则允许符合条件的流量通过。如果引用了配置文件，则最终流量是否能够通过还需要根据内容安全检测的结果而定。
- 禁止：表示拒绝符合条件的流量通过。

7. 配置安全策略引用内容安全的配置文件。

在这里可以选择已经创建的安全配置文件，还可以新建安全配置文件。各个配置文件的作用如下：

参数	说明
反病毒	反病毒特性可以对网络中传输的文件进行病毒检测和处理，避免由病毒引起的数据破坏、系统崩溃等情况发生，保证内部网络安全。
入侵防御	入侵防御通过比较流量内容与入侵防御特征库来实现攻击检测，有效防御来自应用层的攻击，例如缓冲区溢出攻击、木马、后门攻击、蠕虫等。
URL 过滤	URL 过滤可以对用户的 URL 请求进行访问控制，允许或禁止用户访问某些网页资源，达到规范上网行为的目的。
文件过滤	文件过滤通过阻断特定类型的文件传输，可以降低内部网络执行恶意代码和感染病毒的风险，还可以防止员工将公司机密文件泄漏到互联网。
内容过滤	内容过滤可以阻断包含特定关键字的流量，防止机密信息的泄露及敏感信息的传输。
应用行为控制	应用行为控制可以管理内网用户的 HTTP 和 FTP 行为，包括：浏览网页、发帖、代理上网、上传和下载等行为。
邮件过滤	邮件过滤可以对邮件收发行为进行管控，包括防止垃圾邮件和匿名邮件泛滥，控制违规收发等。

8. 配置记录日志功能。

- 选中“记录策略命中日志”后，设备将记录匹配安全策略规则的流量的日志，即策略命中日志。
- 选中“记录会话日志”后，设备将记录匹配安全策略规则的会话日志。

9. 配置会话老化时间。

在真实网络环境中，会有一些特殊业务在长时间内没有报文传输，这种情况下 NGFW 为了避免消耗性能会清理无用的会话连接。但在实际使用场景中又需要 NGFW 记录该连接状态，避免正常的业务中断（如数据库服务），因此 NGFW 提供了基于策略的老化时间配置，保持特定的会话连接。

10. 配置自定义长连接。

该功能只针对匹配策略的 TCP 应用报文生效。与“配置会话老化时间”相比，该功能提供了更为细的粒度管理（“配置会话老化时间”对 TCP、UDP 应用均生效），以及更长时间的会话保持（“配置会话老化时间”只支持到秒级）。

选中“自定义长连接”对应的“启用”，开启自定义长连接功能，并配置长连接时间。



说明：

在[会话表与长连接](#)中，详细介绍了基于安全域间和服务集的会话老化时间配置方法，对于几种配置并存

的情况，其优先级关系如下所示：

基于策略的自定义长连接 > 基于安全域间的自定义长连接 > 基于策略的老化时间 > 基于服务集的老化时间

11. 单击“确定”，完成安全策略的配置。
12. 单击界面右上角的“保存”，在弹出的对话框中单击“确定”。
13. **可选：**单击界面右上角的“提交”，在弹出的对话框中单击“确定”。

对以下内容安全的配置文件进行新建、修改和删除操作时，需要使用“提交”使之生效，进而保证引用其的安全策略也生效。

- [入侵防御](#)
- [URL 过滤](#)
- [文件过滤](#)
- [内容过滤](#)
- [邮件过滤](#)

策略冗余分析

介绍策略冗余分析工具的使用方法。

背景信息

策略冗余分析工具可以识别出冗余策略，从而达到精简安全策略的目的。设备会分析安全策略中除地区以外的所有匹配条件，包括：

- 源安全区域
- 目的安全区域
- 源地址
- 目的地址
- 用户

- 服务
- 应用
- 时间段



说明：

设备只对动作相同的安全策略做冗余分析。

设备会将高优先级的策略依次与低优先级的策略进行遍历比较，如果符合以下两种情况的任意一种便会认定为完全冗余，并列出分析结果帮助管理员进一步分析处理。

- 所有匹配条件完全相同的安全策略，则低优先级的安全策略会被认定为完全冗余。
- 安全策略 A 的所有匹配条件被安全策略 B 完全包含，并且该安全策略 A 的优先级低于安全策略 B，则安全策略 A 会被认定为完全冗余。

策略冗余分析可以在没有流量经过设备时进行静态分析，因此该分析可以在配置安全策略后立即开始。

缺省的 default 策略不参与策略冗余分析。安全策略中的安全策略配置文件不作为分析对象，即只关注安全策略中的匹配条件和动作。

策略冗余分析


1. 选择“策略 > 安全策略 > 策略冗余分析”。
2. 单击“开始分析”。

如下图所示，冗余分析结果会按照安全策略的优先级由上到下显示与之存在冗余的安全策略。

<div> 开始分析 停止分析 删除 </div>									
策略名称	冗余标识	源地址/地区	目的地址/地区	源用户	服务	应用	时间段	动作	配置
<input type="checkbox"/> MKT_allow_Social_...		any	any	/marketing	any	Facebook 超文本传输协议 安全套接层协议 安全超文本传输协议 Twitter SIPnetworking	any	允许	
<input type="checkbox"/> MKT_allow_twitter	完全冗余	any	any	/marketing	any	超文本传输协议 安全套接层协议 安全超文本传输协议 Twitter	any	允许	
<input type="checkbox"/> NonR2D_allow_Med...		any	any	/hr /marketing	any	any	any	允许	
<input type="checkbox"/> MKT_allow_Media_S...	完全冗余	any	any	/marketing	any	any	any	允许	

处理建议

由于安全策略是由上至下匹配命中的，也就是说排名越靠前的策略地位越重要，影响越大。因此在处理冗余策略时，建议也按照这个顺序进行。根据企业的实际情况，企业管理员可以选择修改或删除冗余的安全策略。

- 若确认安全策略应为继续保留，只需要进行修改，可以单击策略名称或单击对应的，进入修改安全策略页面。
- 若确认安全策略确实存在冗余关系，可勾选安全策略对应的复选框，将该策略删除。

调整完冗余的安全策略后，与其相关的分析结果会自动刷新。

策略命中分析

介绍策略命中分析工具的使用方法。

背景信息

由于命中分析结果与策略的匹配命中强相关，因此在进行命中分析前，请尽量让设备正常运行（有流量经过）一段时间，以保证分析结果会更准确、全面。

如果符合以下两种情况的任意一种便会认定为未命中，并列分析结果帮助管理员进一步分析处理。

- 实际流量不满足安全策略的匹配条件。
- 存在深度冗余，例如 IP 地址和用户的冗余、服务和应用的冗余。由于高优先级策略先命中，导致低优先级的策略未命中。

缺省的 default 策略不参与策略命中分析。

策略命中分析

1. 选择“策略 > 安全策略 > 策略命中分析”。
2. 设备会自动开始分析，并按照安全策略优先级顺序呈现分析结果，如下图所示。

 说明：

可以通过“刷新”按钮实时刷新分析结果。

策略命中分析									
删除 刷新		今天							
策略名称	命中结果	源地址/地区	目的...	源用户	服务	应用	时间段	动作	配置
<input type="checkbox"/> allow_port_tcp_554	未命中	any	any	any	rtsp	any	any	允许	
<input type="checkbox"/> MKT_allow_VIP	未命中	10.174.64.0/24	any	/marketing	any	any	any	允许	
<input type="checkbox"/> MKT_allow_IM	未命中	any	any	/marketing	any	QQ_IM MSN_IM ICQ_IM GoogleTalk_I BearShare 超文本传输协 Jabber 安全套接层协 查看全部...	any	允许	
<input type="checkbox"/> R2D_allow_mysql	未命中	any	any	/r2d	any	MySQL关系型	any	允许	
<input type="checkbox"/> R2D_allow_cvs	未命中	any	any	/r2d	any	CVS	any	允许	
<input type="checkbox"/> MKT_allow_Social_Networking	未命中	any	any	/marketing	any	Facebook 超文本传输协 安全套接层协 安全超文本传 Twitter Slnetworking	any	允许	
<input type="checkbox"/> MKT_allow_twitter	未命中	any	any	/marketing	any	超文本传输协 安全套接层协 安全超文本传 Twitter	any	允许	
<input type="checkbox"/> MKT_allow_Media_Sharing	未命中	any	any	/marketing	any	any	any	允许	

设备缺省显示当天（“今天”）的策略命中分析结果，另外，“最近 3 天”、“最近一周”和“最近一个月”的策略命中分析结果，在界面的右上角以供选择。

说明：

查询分析结果的维度不同，所需要的时间也不同：

- “今天”的分析结果至少需要在流量经过设备后 15 分钟。
- “最近 3 天”、“最近一周”和“最近一个月”的分析结果至少需要在流量经过设备后 1 个小时。

处理建议

由于安全策略是由上至下匹配命中的，也就是说排名越靠前的策略地位越重要，影响越大。因此在处理未命中的策略时，建议也按照这个顺序进行。根据企业的实际情况，企业管理员可以选择修改或删除未命中的策略。

- 若确认安全策略应为继续保留，只需要进行修改，可以点击策略名称，进入修改安全策略页面。
- 若确认安全策略不需要保留，可勾选安全策略对应的复选框，将该策略删除。

调整完未命中的安全策略后，与其相关的分析结果会自动刷新。

应用风险调优

介绍应用风险调优工具的使用方法。

前提条件

在设备上已配置宽泛的安全策略，例如较大的 IP 地址范围等，总之尽可能让所有必要流量通过防火墙，并稳定运行足够的时间。在运行过程中，应尽可能还原企业日常运作中网络环境，使通过防火墙的流量多样化。



说明：

应用风险调优只分析防火墙允许通过的流量，因此在配置宽泛的安全策略时，请将命中安全策略的关键流量的动作设置为“允许”。

背景信息

应用风险调优能够解决如下问题：

- 识别安全策略中包含的应用类别，将基于服务（端口）的安全策略转换为基于应用的安全策略。
- 识别安全策略中包含的应用风险，并对相应的风险进行深度防护，即在安全策略中配置入侵防御、反病毒等配置文件。

NGFW 的智能感知引擎为常用应用定义了相应的风险类型，而对于各类风险类型提供了相应的防护措施，即内容安全，风险类型和防护措施的对应关系如[表 1](#)所示。

表 1 风险类型和防护措施的对应关系		
风险分类	风险类型	防护措施
安全类风险	可被利用、承载恶意软件、具有躲避特征	入侵防御、反病毒、URL 过滤
泄漏类风险	隧道协议、造成数据泄漏	文件过滤、内容过滤
办公效率下降类风险	造成工作效率下降、消耗网络带宽	带宽控制或禁用该应用

对于安全类风险和泄漏类风险系统提供了相应的防护措施。对于办公效率下降类风险，可参考[带宽管理](#)章节对相应的应用进行带宽控制，或在安全策略中禁止此类应用。



说明：

设备不会对动作为“禁止”的策略进行应用风险调优，即只针对存在安全风险隐患（动作为“允许”）的安全策略进行应用风险调优。

应用风险分析

- 1. 选择“策略 > 安全策略 > 应用风险调优”。
- 2. 设备会自动开始分析，并呈现分析结果，如图 1 所示。

说明：

可以通过“刷新”按钮实时刷新分析结果。

图 1 应用风险分析



设备缺省显示“最近一个月”的应用风险分析结果，另外，“今天”、“最近 3 天”和“最近一周”的应用风险分析结果，在界面的右上角以供选择。

说明：

- 使用界面右上角的“只显示未处理”，分析结果中将会过滤掉状态为“已处理”的安全策略，只显示状态为“未处理”的安全策略，可以让企业管理员聚焦于调优动作。
- 查询分析结果的维度不同，所需要的时间也不同：
 - “今天”的分析结果至少需要在流量经过设备后 15 分钟。
 - “最近 3 天”、“最近一周”和“最近一个月”的分析结果至少需要在流量经过设备后 1 个小时。

- 3. 分析结果中各项信息如表 2 所示。

表 2 应用风险分析结果	
项目	描述
总体安全评分	对设备中所有安全策略的综合评分，得分越高表示安全系数越高，相反低分数表示存在风险。
策略名称	存在安全风险，待调优的安全策略名称。
风险级别	取值范围 1~5，表示风险依次增高。 策略的风险级别是由安全策略中包含的应用，根据智能感知引擎中为应用定义的风险类型，使用既定算法计算出对应的风险值。总的来说，安全策略包含风险类型越多，风险级别越高。
总流量	安全策略命中的总流量。
应用	在已命中安全策略的流量中，设备识别出的所有应用。
流量（接收/发送）	应用的流量信息，包括： <ul style="list-style-type: none"> 在已命中安全策略的流量中，指定应用的流量占比。 设备接收和发送指定应用流量的对比，绿色表示设备接收的流量，黄色表示设备发送的流量。
安全风险	安全策略中所有应用对应的风险总类别。 例如安全策略中包含应用 a 和应用 b，a 包含“可被利用”风险，b 包含“具有躲避特征”风险，则该安全策略的安全风险包括“可被利用”风险和“具有躲避特征”风险。
状态	安全策略的调优状态： <ul style="list-style-type: none"> 未处理：表示从未调优过安全策略。 已处理：表示为已调优过，但仍然存在风险的安全策略。可根据实际情况选择是否继续调优。

处理建议

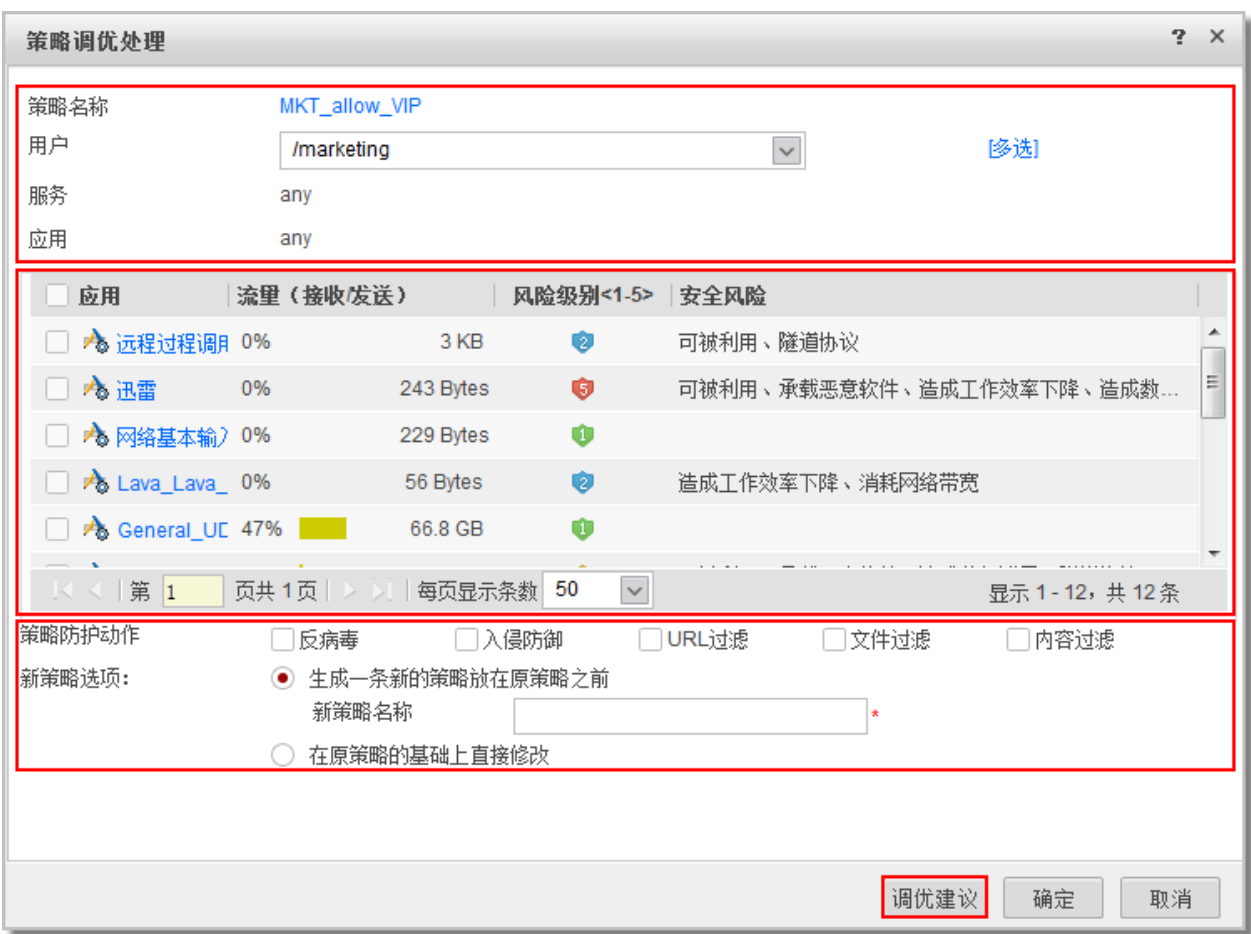
设备提供“按调优建议批量处理”和逐条策略的“调优处理”，前者遵循通用的安全策略调优规则，较为方便快捷，但由于企业的网络环境千差万别，设备也提供了针对每条策略单独进行“调优处理”，在调优界面配置调优细则，在实际应用中会更为可靠。下面以调优界面为基础，介绍调优过程中的相关说明和注意事项。管理员根据企业的自身情况，可以在调优界面中通过选择具体的应用、安全策略配置文件等进行手动调优，也可以使用“调优建议”按钮自动处理。



说明：

调优界面中的“调优建议”与“按调优建议批量处理”的作用功能相同。区别在于“按调优建议批量处理”是为所有待调优的安全策略执行“调优建议”动作。“按调优建议批量处理”支持异步，即在批量调优过程中，企业管理员可以进行其他配置操作，提高维护效率。

图 2 策略调优界面



如图 2 所示，调优界面由上至下可分为策略基本信息、应用信息、深度防护动作和新策略选项。

- 策略基本信息：包含了原安全策略的名称和已配置的用户、服务以及应用/应用组，这些信息可为后续的调优提供参考。
- 应用信息：包括在已命中安全策略的流量中，设备识别出的所有应用，以及原安全策略中已配置的应用。这些信息可以帮助企业管理员了解网络中的流量构成以及命中情况，根据实际情况增加或减少相关的应用，作为安全策略的匹配条件，以符合最小授权原则。
- 深度防护动作：设备提供的深度防护措施，即会引用配置缺省的安全策略配置文件（default）。企业管理员可根据应用的风险类型配置对应的深度防护措施。
- 新策略选项：调优的最终结果是基于原有的安全策略修改或新生成一条安全策略。

更详细的调优界面信息请参见表 3。

表 3 调优界面信息	
策略基本信息	
策略名称	待调优安全策略的名称，可单击名称链接进入安全策略修改界面，详细操作请参考

表 3 调优界面信息	
策略基本信息	
	安全策略 。
用户	待调优安全策略中已配置的“用户”信息，可在此直接修改策略中的用户/用户组信息。
服务	待调优安全策略中已配置的“服务”信息，此处只为调优提供相应的参考。
应用	待调优安全策略中已配置的“应用”信息，此处只为调优提供相应的参考。
应用信息	
应用	<p>应用名称，包括：</p> <ul style="list-style-type: none"> 在已命中安全策略的流量中，设备识别出的所有应用。 原安全策略中已配置的应用。 <p>单击名称链接查看该应用的更多属性。</p>
流量（接收/发送）	<p>应用的流量信息，包括：</p> <ul style="list-style-type: none"> 在已命中安全策略的流量中，指定应用的流量占比。 设备接收和发送指定应用流量的对比，绿色表示设备接收的流量，黄色表示设备发送的流量。 设备接收和发送指定应用的总流量。
风险级别<1-5>	<p>取值范围 1~5，表示风险依次增高。</p> <p>应用的风险级别是由智能感知引擎中为应用定义的风险类型，使用既定算法计算出对应的风险值。总的来说，应用包含风险类型越多，风险级别越高。</p>
安全风险	华为智能感知引擎为常用应用定义了相应的风险类型。
其他	
策略防护动作	<p>缺省选中的安全防护动作继承原有安全策略中的配置。智能感知引擎针对安全风险类型定义的安全防护措施，对应关系请参考表 2。</p> <p>目前应用风险调优工具只支持引用设备缺省存在的安全策略配置文件（default），如需引用自定义配置文件请另行修改安全策略。</p>
新策略选项	<ul style="list-style-type: none"> 生成一条新的策略放在原策略之前：不改变当前策略的配置，生成一条新的安全策略，优先级高于当前策略。 若对采用该方式调优过的安全策略再次进行调优，且仍然选择生成一条新的安全策略，则设备实际会修改原来已生成的安全策略并重命名，不会再生成新的安全策略。这种处理方式主要是为了避免多次调优生成过多的安全策略。例如，对安全策略 A 进行调优，生成安全策略 A1，再次对 A 进行调优，则修改并重命名 A1，不会引入新的安全策略。 但以上情况不适用于保存配置并重启后再次调优，即如果在调优后保存配置并重启，再次进行调优并选择生成一条新的安全策略，最终会生成一条新的策略，不会修改上次调优生成的安全策略。例如，对安全策略 A 进行调优，生成安全策略 A1，保存配置重启后再次对 A 进行调优，则会生成新的安全策略 A2。 在原策略的基础上修改：修改当前策略，为其配置应用或深度防护措施。

表 3 调优界面信息

策略基本信息	
调优建议	遵循通用的安全策略调优规则进行处理，具体调优内容请参见下文。

通过调优建议处理前后的对比，介绍“调优建议”功能的作用。初始调优界面如图 3 所示，单击“调优建议”后调优界面如图 4 所示。

图 3 调优前界面

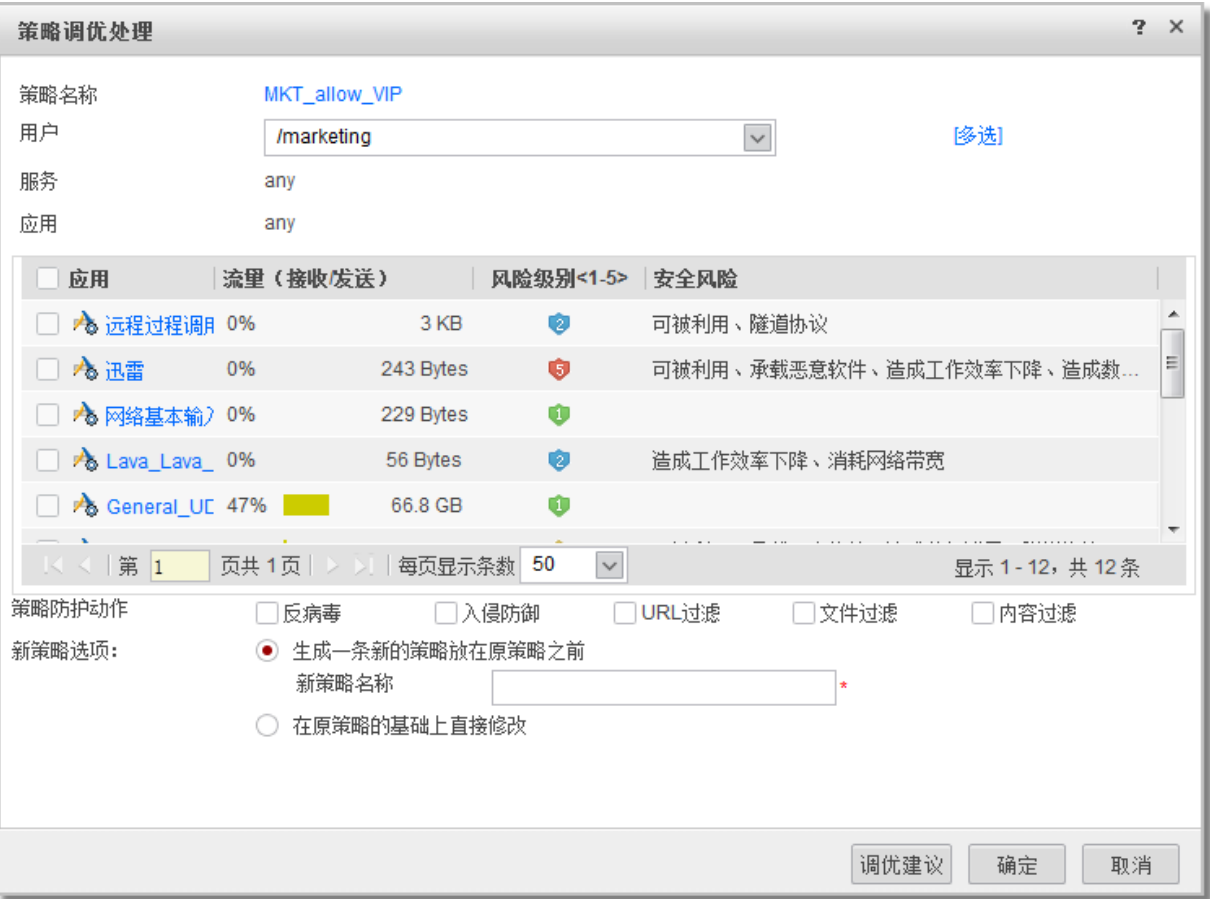
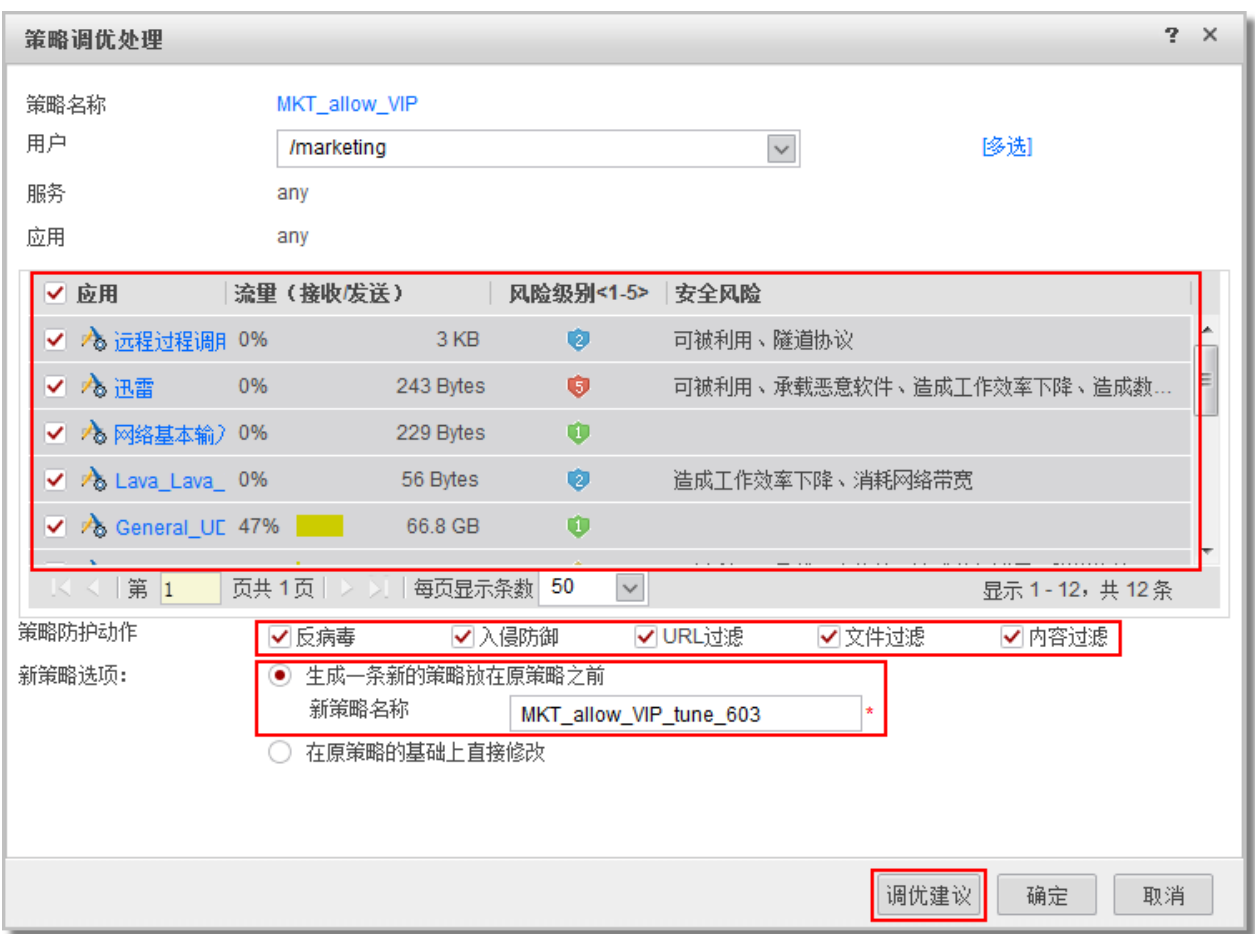


图 4 调优后界面



综上所述，可见“调优建议”功能主要完成：

- 将有流量命中的应用类型作为策略匹配条件。
- 将有流量命中的应用类型作为深度防护对象，为其配置策略防护动作。
- 使用建议命名生成一条新的安全策略。

注意事项

应用风险调优后请不要立即进行命中分析，这是由于缺少背景流量会将调优生成的策略误分析为未命中策略。

举例：配置安全策略

举例说明如何配置安全策略，保证防火墙流量的正常转发以及实现内容安全的管控。

组网需求

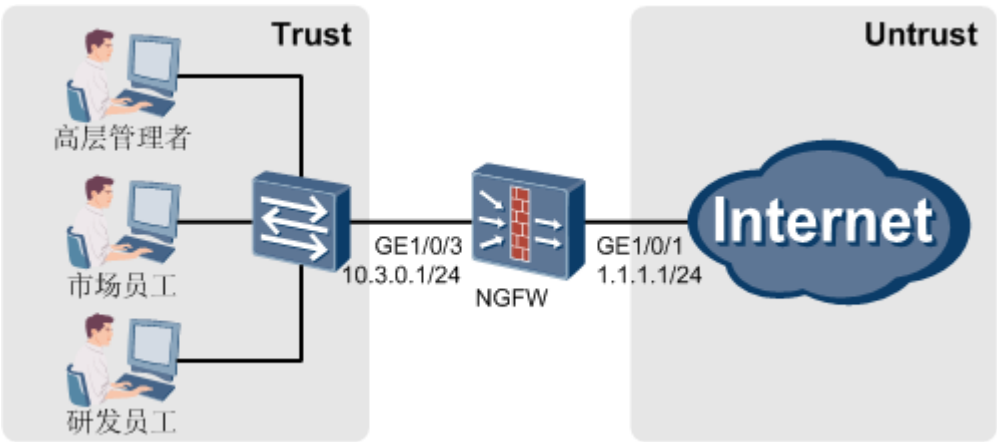
如图1所示，某企业在网络边界处部署了 NGFW 作为安全网关。

企业根据员工级别和职能不同划分了三种用户：高层管理者、市场员工、研发员工，他们能够访问 Internet 的权限不同。具体如下：

- 高层管理者可以自由访问 Internet。
- 市场员工能够访问 Internet，但不能玩游戏，观看网络视频。
- 研发员工不能访问 Internet。

企业还希望对通过 NGFW 的流量进行反病毒和入侵防御检测，保护内部网络安全。

图 1 配置安全策略组网图



数据规划

说明：


本举例的用户已经存在于 NGFW 中，并且已经完成了认证的配置。

项目	数据	说明
高层管理者的安全策略	<ul style="list-style-type: none">• 名称：policy_sec_management• 源安全区域：trust• 目的安全区域：untrust• 用户：management• 动作：允许• 反病毒：default• 入侵防御：default	安全策略 policy_sec_management 的作用是允许高层管理者自由访问 Internet。 本举例使用系统默认存在的反病毒配置文件 default 和入侵防御配置文件 default。
市场员工的安全策略 1	<ul style="list-style-type: none">• 名称：policy_sec_marketing_1• 源安全区域：trust• 目的安全区域：untrust• 用户：marketing• 应用：游戏、媒体共享	安全策略 policy_sec_marketing_1 的作用是禁止市场员工玩游戏，观看网络视频。 游戏代表游戏类应用，媒体共享代表网络视频类应用。

项目	数据	说明
	<ul style="list-style-type: none"> 动作：禁止 	
市场员工的安全策略 2	<ul style="list-style-type: none"> 名称：policy_sec_marketing_2 源安全区域：trust 目的安全区域：untrust 用户：marketing 动作：允许 反病毒：default 入侵防御：default 	安全策略 policy_sec_marketing_2 的作用是允许市场员工访问 Internet。 本举例使用系统默认存在的反病毒配置文件 default 和入侵防御配置文件 default。
研发员工的安全策略	<ul style="list-style-type: none"> 名称：policy_sec_research 源安全区域：trust 目的安全区域：untrust 用户：research 动作：禁止 	安全策略 policy_sec_research 的作用是禁止研发员工访问 Internet。

操作步骤

1. 配置接口 IP 地址和安全区域，完成网络基本参数配置。

- a. 选择“网络 > 接口”。
- b. 单击 GE1/0/1 对应的 ，按如下参数配置。

IP 地址	1.1.1.1
网络掩码	255.255.255.0
安全区域	untrust

- c. 单击“确定”。
- d. 参考上述步骤按如下参数配置 GE1/0/3 接口。

IP 地址	10.3.0.1
网络掩码	255.255.255.252
安全区域	trust

2. 配置高层管理者的安全策略。

- a. 选择“策略 > 安全策略 > 安全策略”。
- b. 单击“新建”。
- c. 按照如下参数配置高层管理者的安全策略。

名称	policy_sec_management
源安全区域	trust

目的安全区域	untrust
用户	/default/management
动作	允许
内容安全	
反病毒	default
入侵防御	default

d. 单击“确定”。

3. 配置市场员工的安全策略。

a. 选择“策略 > 安全策略”。

b. 单击“新建”。

c. 按照如下参数配置市场员工的安全策略 1。

名称	policy_sec_marketing_1
源安全区域	trust
目的安全区域	untrust
应用	游戏、媒体共享 窍门： 由于应用种类繁多，加载过程比较缓慢，推荐在“应用”框中输入需要的应用（如游戏），等待片刻后再在下拉列表中进行选择。
用户	/default/marketing
动作	禁止

d. 单击“确定”。

e. 参考上述步骤按如下参数配置市场员工的安全策略 2。

名称	policy_sec_marketing_2
源安全区域	trust
目的安全区域	untrust
应用	any
用户	/default/marketing
动作	允许
内容安全	
反病毒	default
入侵防御	default

4. 配置研发员工的安全策略。

- a. 选择“策略 > 安全策略”。
- b. 单击“新建”。
- c. 按照如下参数配置研发员工的安全策略。

名称	policy_sec_research
源安全区域	trust
目的安全区域	untrust
用户	/default/research
动作	禁止

- d. 单击“确定”。

结果验证

1. 验证高层管理者是否能够不受限制的访问 Internet，如果是则证明高层管理者的安全策略配置成功。
2. 验证市场员工的用户是否能够访问 Internet，而且访问 Internet 时不能使用 NGFW 定义的游戏和媒体共享应用。如果是则证明市场员工的安全策略配置成功。
3. 验证研发员工用户是否不能访问 Internet。如果是则证明研发员工的安全策略配置成功。
4. 选择“监控 > 日志 > 策略命中日志”，分别查看高层管理者、市场员工、研发员工是否命中正确的安全策略。
5. 选择“监控 > 日志 > 威胁日志”，查看流量是否会被反病毒或入侵防御配置文件阻断。

配置脚本

```
#
interface GigabitEthernet1/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/3
 ip address 10.3.0.1 255.255.255.0
#
firewall zone trust
 add interface GigabitEthernet1/0/3
#
firewall zone untrust
 add interface GigabitEthernet1/0/1
```

```
#
security-policy
rule name policy_sec_management
    source-zone trust
    destination-zone untrust
    user /default/management
    profile av default
    profile ips default
    action permit
rule name policy_sec_marketing_1
    source-zone trust
    destination-zone untrust
    user /default/marketing
    application category Entertainment sub-category Game
    application category Entertainment sub-category Media_Sharing
    action deny
rule name policy_sec_marketing_2
    source-zone trust
    destination-zone untrust
    user /default/marketing
    profile av default
    profile ips default
    action permit
rule name policy_sec_research
    source-zone trust
    destination-zone untrust
    user /default/research
    action deny
```

HCIE-Security 模拟面试问题及面试建议

1. 请说明防火墙安全策略的工程原理。
2. 防火墙安全配置文件有哪些？。