HCIE-Security 备考指南

虚拟系统

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 虚拟系统需要掌握的知识点

■ 掌握防火墙虚拟化原理及配置

虚拟系统简介

虚拟系统（Virtual System）是在一台物理设备上划分出的多台相互独立的逻辑设备。

您可以从逻辑上将一台 NGFW 设备划分为多个虚拟系统。每个虚拟系统相当于一台真实的设备，有自己的接口、地址集、用户/组、路由表项以及策略，并可通过虚拟系统管理员进行配置和管理。

虚拟系统具有以下特点：

- 每个虚拟系统由独立的管理员进行管理，使得多个虚拟系统的管理更加清晰简单，所以非常适合大规模的组网环境。
- 每个虚拟系统拥有独立的配置及路由表项，这使得虚拟系统下的局域网即使使用了相同的地址范围，仍然可以正常进行通信。
- 可以为每个虚拟系统分配固定的系统资源，保证不会因为一个虚拟系统的业务繁忙而影响其他虚拟系统。
- 虚拟系统之间的流量相互隔离，更加安全。在需要的时候，虚拟系统之间也可以进行安全互访。
- 虚拟系统实现了硬件资源的有效利用，节约了空间、能耗以及管理成本。

虚拟系统及其管理员

介绍根系统与虚拟系统、根系统管理员与虚拟系统管理员。

虚拟系统

NGFW 上存在两种类型的虚拟系统：

- 根系统（root）

  根系统是 NGFW 上缺省存在的一个特殊的虚拟系统。即使虚拟系统功能未启用，根系统也依然存在。此时，管理员对 NGFW 进行配置等同于对根系统进行配置。启用虚拟系统功能后，根系统会继承先前 NGFW 上的配置。

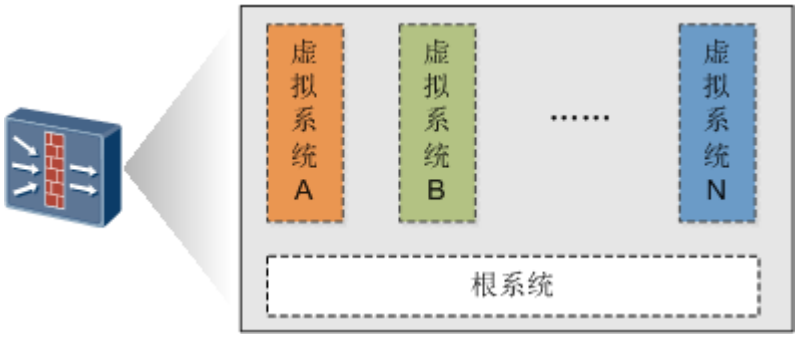
在虚拟系统这个特性中，根系统的作用是管理其他虚拟系统，并为虚拟系统间的通信提供服务。

- 虚拟系统(VSYS)

  虚拟系统是在 NGFW 上划分出来的、独立运行的逻辑设备。

虚拟系统划分的逻辑结构如图 1 所示。

图 1 虚拟系统划分的逻辑示意图



为了实现每个虚拟系统的业务都能够做到正确转发、独立管理、相互隔离，NGFW 主要实现了几个方面的虚拟化：

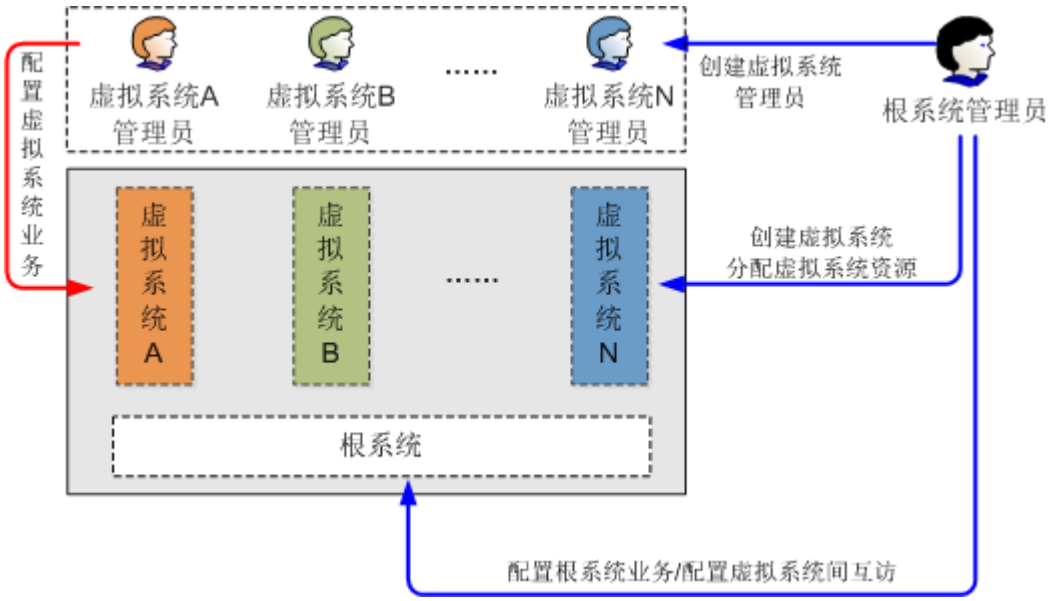
- 资源虚拟化：每个虚拟系统都有独享的资源，包括接口、VLAN、策略和会话等。根系统管理员分配给每个虚拟系统，由各个虚拟系统自行管理和使用。
- 配置虚拟化：每个虚拟系统都拥有独立的虚拟系统管理员和配置界面，每个虚拟系统管理员只能管理自己所属的虚拟系统。
- 业务虚拟化：每个虚拟系统都可以配置独立的路由、策略及其他防火墙业务，只有属于该虚拟系统的报文才会受到这些配置的影响。

通过以上几个方面的虚拟化，当创建虚拟系统之后，每个虚拟系统的管理员都像在使用一台独占的设备。

管理员

根据虚拟系统的类型，管理员分为根系统管理员和虚拟系统管理员。如图 2 所示，两类管理员的作用范围和功能都不相同。

图 2 管理员功能逻辑示意图



- 根系统管理员

  启用虚拟系统功能后，设备上已有的管理员将成为根系统的管理员。管理员的登录方式、管理权限、认证方式等均保持不变。根系统管理员负责管理和维护设备、配置根系统的业务。

  只有具有虚拟系统管理权限的根系统管理员（本章节后续内容中提及的根系统管理员都是指此类管理员）才可以进行虚拟系统相关的配置，如创建、删除虚拟系统，为虚拟系统分配管理员和资源等。

- 虚拟系统管理员

  创建虚拟系统后，根系统管理员可以为虚拟系统创建一个或多个管理员。虚拟系统管理员的作用范围与根系统管理员有所不同：虚拟系统管理员只能进入其所属的虚拟系统的配置界面，能配置和查看的业务也仅限于该虚拟系统；根系统管理员可以进入所有虚拟系统的配置界面，如有需要，可以配置任何一个虚拟系统的业务。

  为了正确识别各个管理员所属的虚拟系统，虚拟系统管理员用户名格式统一为“管理员名@虚拟系统名”。

虚拟系统的资源分配

合理地分配资源可以对单个虚拟系统的资源进行约束，避免因某个虚拟系统占用过多的资源，导致其他虚拟系统无法获取资源、业务无法正常运行的情况。

安全区域、策略、会话等实现虚拟系统业务的基础资源支持定额分配或手工分配，其他的资源项则是各个虚拟系统一起共享抢占。

资源分配

定额分配和手工分配的资源如表 1 所示。

表 1 定额分配和手工分配的资源

资源名称	分配方式	说明
SSL VPN 虚拟网关	定额分配	虚拟系统创建时固定分配给虚拟系统 4 个 SSL VPN 虚拟网关。
安全区域	定额分配	虚拟系统创建时固定分配给虚拟系统 8 个安全区域，包括 4 个缺省的安全区域和 4 个自定义的安全区域。
会话数	手工分配	-
新建会话速率	手工分配	新建会话速率表示虚拟系统每秒可新建的会话数。
在线用户数	手工分配	-
SSL VPN 并发用户数	手工分配	-
用户数	手工分配	-
用户组	手工分配	-
策略数	手工分配	指所有策略的总数，包括安全策略、NAT 策略、带宽策略、认证策略、审计策略和策略路由。
最大带宽数	手工分配	指虚拟系统所有接口入方向的最大带宽。

手工分配资源时可配置保证值和最大值。

- 保证值：虚拟系统可使用某项资源的最小数量。这部分资源一旦分配给虚拟系统，就被该虚拟系统独占。
- 最大值：虚拟系统可使用某项资源的最大数量。虚拟系统可使用的资源能否达到最大值视其他虚拟系统对该项资源的使用情况而定。

例如，NGFW 上配置了 10 个虚拟系统。假定 NGFW 会话数的整机规格为 500000，虚拟系统 A 的会话数保证值为 10000、最大值为 50000。虚拟系统 A 可建立的会话数一定能达到 10000，但能否达到最大值 50000，则视其他虚拟系统的会话资源使用情况而定。如果其他 9 个虚拟系统和根系统当前的会话数小于 450000，虚拟系统 A 可建立的会话数就能达到 50000。

根系统管理员需要根据每个虚拟系统的网络需求分配资源。例如，一个虚拟系统连接的是公司的服务器区域，为服务器提供安全防护。另一个虚拟系统连接的是公司某个部门的工作区域，管理该部门中 20 个员工的上网行为。两个虚拟系统所需要的资源是不同的：第一个虚拟系统需要很多的会话资源，但不需要任何的用户资源；第二个虚拟系统必须要有足够的用户资源，但需要的会话资源则较少。

资源抢占

共享抢占的资源包括：

- 地址和地址组
- 地区和地区组
- 自定义服务和自定义服务组
- 自定义应用和自定义应用组
- NAT 地址池
- 时间段
- 带宽通道
- 静态路由条目
- 各种表项，如 Server-map 表、IP-MAC 地址绑定表、ARP 表、MAC 地址表等

虚拟系统的分流

通过分流能将进入设备的报文送入正确的虚拟系统处理。

NGFW 上未配置虚拟系统时，报文进入 NGFW 后直接根据根系统的策略和表项（会话表、MAC 地址表、路由表等）对其进行处理。NGFW 上配置了虚拟系统时，每个虚拟系统都相当于一台独立的设备，仅依据虚拟系统内的策略和表项对报文进行处理。因此，报文进入 NGFW 后，首先要确定报文与虚拟系统的归属关系，以决定其进入哪个虚拟系统进行处理。我们将确定报文与虚拟系统归属关系的过程称为分流。

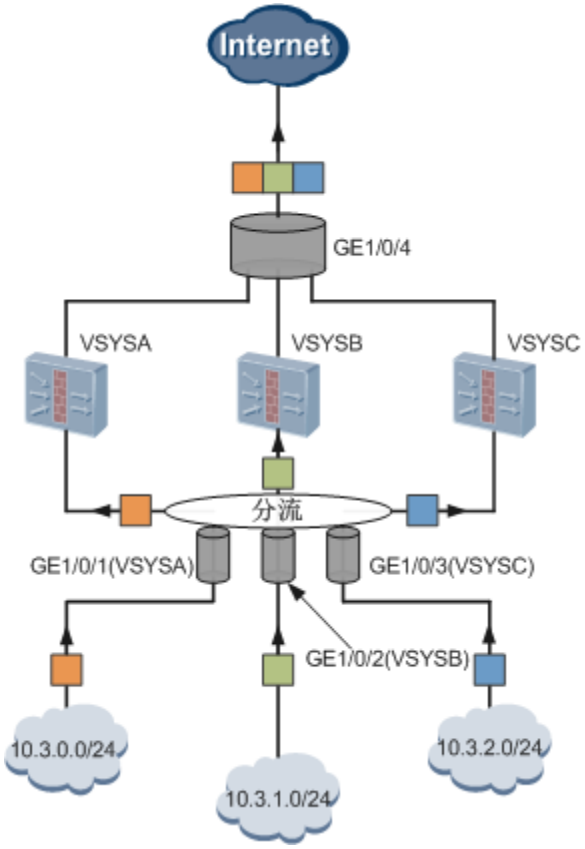
NGFW 支持基于接口分流和基于 VLAN 分流两种分流方式。接口工作在三层时，采用基于接口的分流方式；接口工作在二层时，采用基于 VLAN 的分流方式。

基于接口分流

将接口（包括 GigabitEthernet 和 GigabitEthernet 子接口）与虚拟系统绑定后，从此接口接收到的报文都会被认为属于该虚拟系统，并根据该虚拟系统的配置进行处理。

如图 1 所示，虚拟系统 VSYSA、VSYSB、VSYSC 有专属的内网接口 GigabitEthernet 1/0/1、GigabitEthernet 1/0/2、GigabitEthernet 1/0/3。GigabitEthernet 1/0/1、GigabitEthernet 1/0/2、GigabitEthernet 1/0/3 接收到的报文经过分流，将分别送入 VSYSA、VSYSB、VSYSC 进行路由查找和策略处理。

图 1 基于接口分流示意图



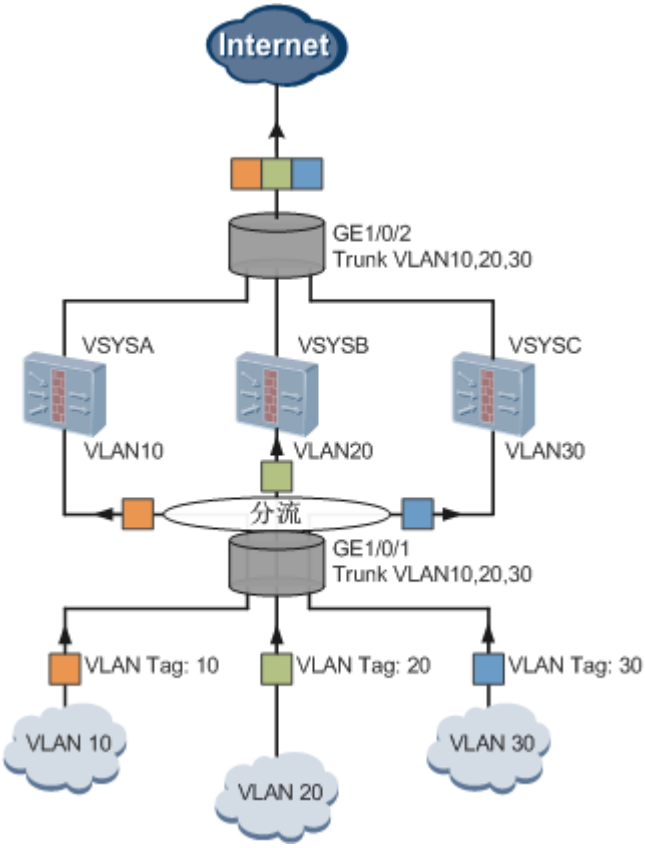
基于 VLAN 分流

将 VLAN 与虚拟系统绑定后，该 VLAN 内的报文都将被送入与其绑定的虚拟系统进行处理。

如图 2 所示，NGFW 的内网接口 GigabitEthernet 1/0/1 为 Trunk 接口，并允许 VLAN10、VLAN20 和 VLAN30 的报文通过。VLAN10、VLAN20、VLAN30 分别绑定虚拟系统 VSYSA、VSYSB 和 VSYSC。对于 GigabitEthernet 1/0/1 接收到的报文，NGFW 会根据报文帧头部的 VLAN Tag 确定报文所属的 VLAN，再根据 VLAN 与虚拟系统的绑定关系，将报文引入相应的虚拟系统。

报文进入虚拟系统后，根据该虚拟系统的 MAC 地址表查询到出接口，确定报文出入接口的域间关系，再根据配置的域间策略对报文进行转发或丢弃。

图 2 基于 VLAN 分流示意图



虚拟系统间的互访

虚拟系统之间能够通过虚拟接口实现互访。

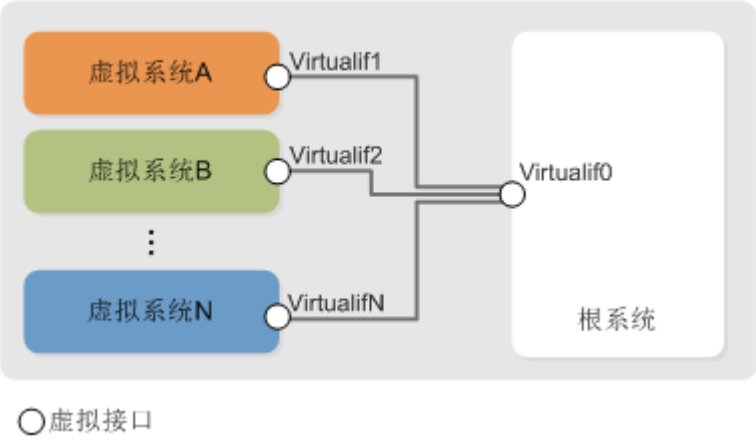
虚拟接口

虚拟接口是创建虚拟系统时系统自动为其创建的一个逻辑接口，作为虚拟系统自身与其他虚拟系统之间通信的接口。与设备上其他的接口不同的是，虚拟接口不配置 IP 地址也能生效。虚拟接口名的格式为“Virtualif+接口号”，根系统的虚拟接口名为 Virtualif0，其他虚拟系统的 Virtualif 接口号从 1 开始，根据系统中接口号占用情况自动分配。

如图 1 所示，各个虚拟系统的虚拟接口和根系统的虚拟接口之间默认通过一条“虚拟链路”连接。如果将根系统和虚拟系统视为独立的设备，将虚拟接口视为设备之间通信的接口，通过将虚拟接口加入安全区域并按照配置一般设备间互访的思路配置路由和安全策略，就能实现虚拟系统与根系统之间的互访。

另外，由于每个虚拟系统和根系统都是连通的，可以将根系统视为一台连接多个虚拟系统的“路由器”，通过这台“路由器”的中转，可以实现两个虚拟系统之间的互访。

图 1 虚拟接口



下面将具体介绍虚拟系统与根系统之间互访以及两个虚拟系统之间互访的配置方法。

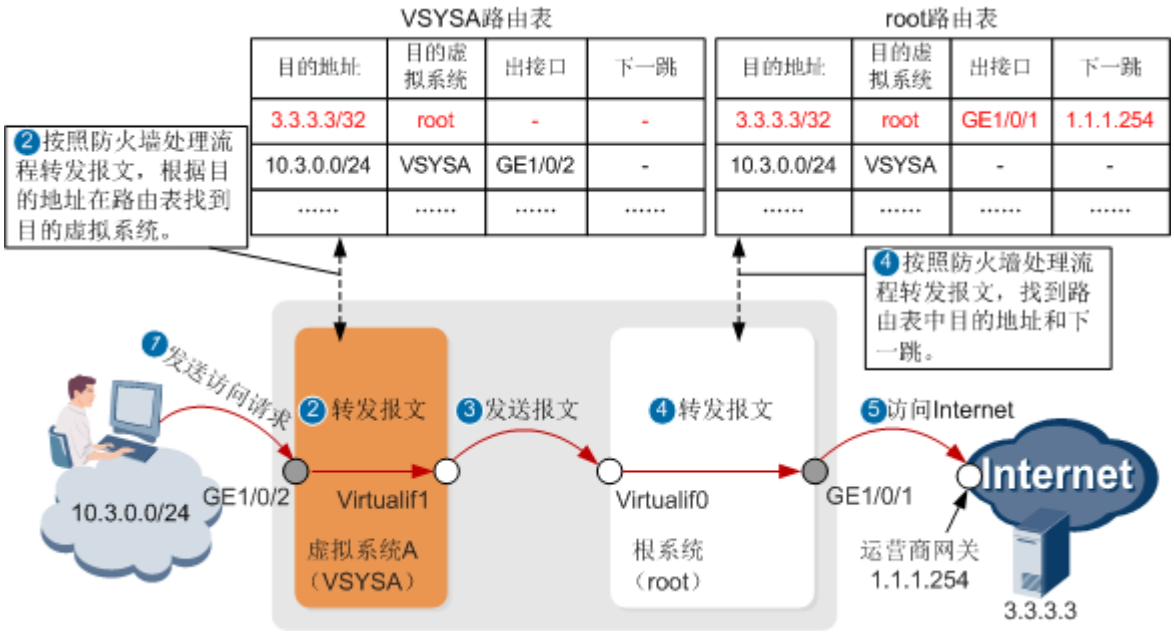
虚拟系统与根系统之间互访

以下场景中需要配置虚拟系统与根系统之间互访：

- 虚拟系统内的主机需要访问根系统管理的主机。
- 当公网地址不足时，不能给每一个虚拟系统分配一个公网接口和公网 IP 地址。所有虚拟系统需要通过根系统的公网接口来访问 Internet。此时虚拟系统主机访问 Internet 的流量需要经过根系统的中转。

如图 2 所示，可以通过配置路由和安全策略实现虚拟系统主机 10.3.0.0/24 通过根系统的公网接口 GE1/0/1 访问 Internet 服务器 3.3.3.3。

图 2 虚拟系统访问根系统示意图



路由的配置方法如下：

1. 在 VSYSA 中配置一条静态路由，目的地址是 3.3.3.3，目的虚拟系统选择 root。
2. 在根系统中配置一条静态路由，目的地址是 3.3.3.3，出接口是 GE1/0/1，下一跳是运营商所提供的网关地址。完成正向路由的配置。
3. 在根系统中配置一条静态路由，目的地址是 10.3.0.0/24，目的虚拟系统选择 VSYSA。
4. 在 VSYSA 中配置一条静态路由，目的地址是 10.3.0.0/24，出接口是 GE1/0/2。完成反向路由的配置。

安全策略的配置方法如下：

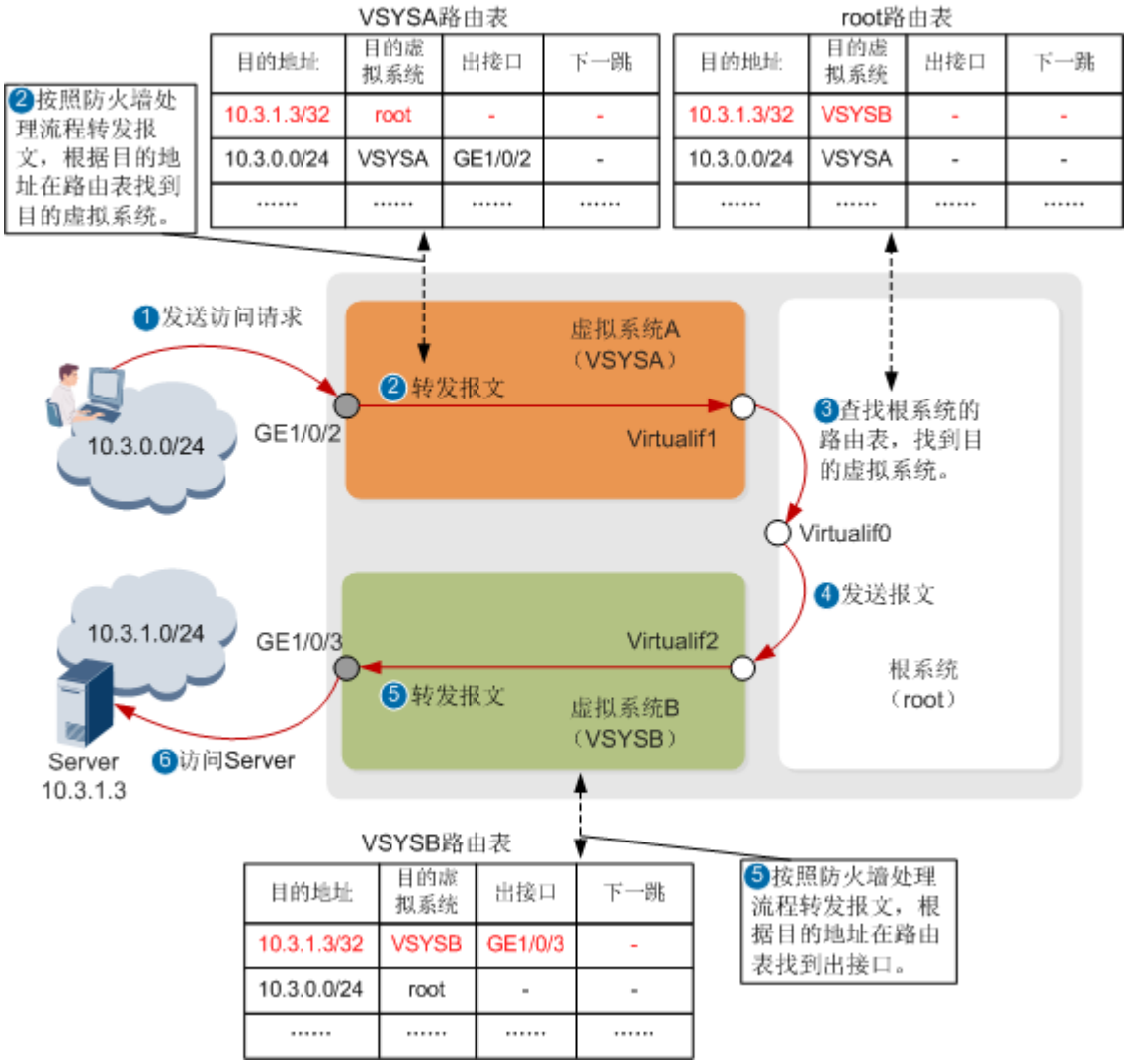
1. 在 VSYSA 中，将接口 GE1/0/2 加入 Trust 区域、Virtualif1 加入 Untrust 区域，配置允许 Trust 区域访问 Untrust 区域的安全策略。
2. 在根系统中，将接口 GE1/0/1 加入 Untrust 区域、Virtualif0 加入 Trust 区域，配置允许 Trust 区域访问 Untrust 区域的安全策略。

完成上述路由和安全策略的配置就可以实现报文的正常转发，但是内网的主机使用的是私网地址 10.3.0.0/24，所以内网的主机如果想要正常访问 Internet，还必须在 VSYSA 或 root 中配置 NAT 策略，进行公网地址和私网地址的转换。在哪个虚拟系统中配置 NAT 策略，取决于哪个虚拟系统的管理员管理和使用公网地址。

两个虚拟系统之间互访

虚拟系统之间互访是通过根系统中转实现的。如图 3 所示，VSYSA 中的用户要访问 VSYSB 中的 Server，需要通过 VSYSA 访问根系统，再通过根系统访问 VSYSB 来实现。

图 3 虚拟系统之间的互访示意图



路由的配置方法如下：

1. 在 VSYSA 中配置一条静态路由，目的地址是 10.3.1.3，目的虚拟系统选择 root。
2. 在根系统中配置一条静态路由，目的地址是 10.3.1.3，目的虚拟系统选择 VSYSB。
3. 在 VSYSB 中配置一条静态路由，目的地址是 10.3.1.3，出接口是 GE1/0/3。完成正向路由的配置。
4. 在 VSYSB 中配置一条静态路由，目的地址是 10.3.0.0/24，目的虚拟系统选择 root。
5. 在根系统中配置一条静态路由，目的地址是 10.3.0.0/24，目的虚拟系统选择 VSYSA。

6. 在 VSYSA 中配置一条静态路由，目的地址是 10.3.0.0/24，出接口是 GE1/0/2。完成反向路由的配置。

安全策略的配置方法如下：

1. 在 VSYSA 中，将接口 GE1/0/2 加入 Trust 区域、Virtualif1 加入 Untrust 区域，配置允许 Trust 区域访问 Untrust 区域的安全策略。
2. 在 VSYSB 中，将接口 GE1/0/3 加入 Trust 区域、Virtualif2 加入 Untrust 区域，配置允许 Untrust 区域访问 Trust 区域的安全策略。

说明：

根系统只根据路由表对虚拟系统之间的访问报文进行转发，不进行其他安全功能的处理，因此不需要在根系统下针对这些报文配置安全策略。

同样，如果期间涉及到公网地址和私网地址之间的转换，也需要在 VSYSA、VSYSB 或 root 中配置 NAT 策略。

虚拟系统私网地址重叠情况的分析

由于虚拟系统对网络和接口进行了隔离，所以不同虚拟系统可以独自规划和使用私网 IP 地址。这就有可能会出现两个虚拟系统网络使用了相同私网 IP 地址的情况。也就是地址重叠的情况。在虚拟系统间通信时，地址重叠会导致一些问题：

- 虚拟系统与根系统之间互访时

  假设两个虚拟系统 VSYSA、VSYSB 所连接的网络主机采用了相同的私网地址（例如 10.3.0.2），但是两者都需要与根系统所连接的同一台服务器（例如 192.168.1.1）通信。

  对于虚拟系统发出的报文，根据路由这些主机发出的报文可以正确转发给服务器。但是对于服务器返回的报文，由于其目的地址均为 10.3.0.2，所以 root 无法判断该报文应该转发给 VSYSA 还是 VSYSB。

  解决此问题的方法就是在两个虚拟系统中配置 NAT 策略。在将报文发送给根系统前，先分别将报文的源地址转换为不冲突的地址网段。这样在根系统看来，就不会出现两个 IP 地址相同的主机。根系统中再配置针对转换后的 IP 地址的路由，就可以正确转发报文了。

- 两个虚拟系统之间互访时

假设两个虚拟系统 VSYSA、VSYSB 所连接的网络主机采用了相同的私网地址（例如 10.3.0.0/24），但是两者需要相互通信。显然它们不能使用各自的原始 IP 地址进行通信，因为这会出现源和目的地址相同或位于同一网段的情况。

此时就需要根系统管理员为每一个虚拟系统配置 NAT 策略进行源地址或目的地址的转换。

假设，VSYSA 中主机要访问 VSYSB 中 IP 地址为 10.3.0.3 的一台服务器，在 VSYSA 中配置源 NAT 策略将报文的源地址转换为 192.168.1.1，在 VSYSB 中配置服务器映射（NAT Server）将服务器的私网地址映射为 192.168.2.1。VSYSA 主机使用新地址 192.168.1.1 来访问 VSYSB 中的服务器。则路由和 NAT 配置如下：

1. 在 VSYSA 中配置源 NAT 策略对报文的源地址进行转换。

转换前源地址	转换后源地址
10.3.0.0/24	192.168.1.1

2. 在 VSYSA 中配置静态路由将访问流量转发至 root。

源虚拟系统	目的地址	目的地址系统	出接口
-	192.168.2.1	root	-

3. 在 root 中配置静态路由将访问流量转发至 VSYSB。

源虚拟系统	目的地址	目的地址系统	出接口
-	192.168.2.1	VSYSB	-

4. 在 VSYSB 中配置服务器映射。

类型	公网地址	私网地址
静态映射	192.168.2.1	10.3.0.3

5. 在 VSYSB 中配置到达 10.3.0.3 的静态路由。

参考上述步骤配置反向路由即可实现正常通信。

虚拟系统应用场景

介绍虚拟系统的应用场景。

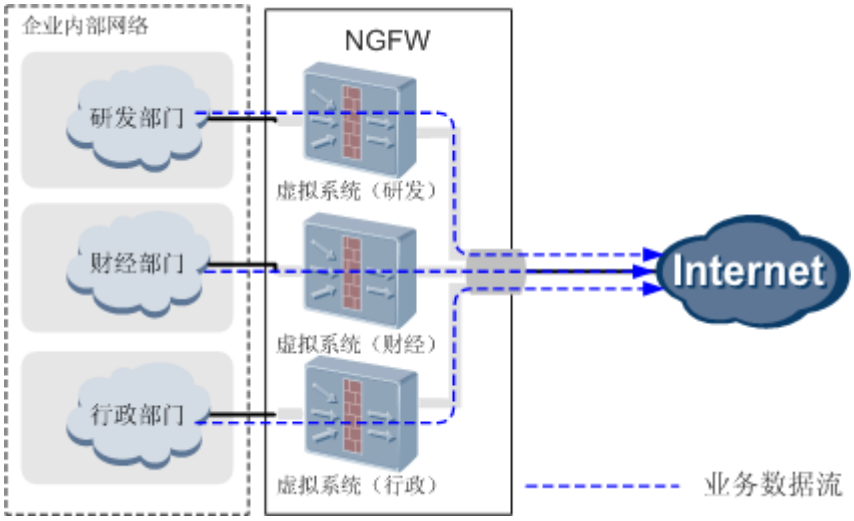
虚拟系统目前主要用于以下几个场景：

大中型企业的网络隔离

通常大中型企业的网络为多地部署，设备数量众多，网络环境复杂。而且随着企业业务规模的不断增大，各业务部门的职能和权责划分也越来越清晰，每个部门都会有不同的安全需求。这些将导致防火墙的配置异常复杂，管理员操作容易出错。通过防火墙的虚拟化技术，可以在实现网络隔离的基础上，使得业务管理更加清晰和简便。

如图 1 所示，企业内部网络通过 NGFW 的虚拟系统将网络隔离为研发部门、财经部门和行政部门。各部门之间可以根据权限互相访问，不同部门的管理员权限区分明确。企业内网用户可以根据不同部门的权限访问 Internet 的特定网站。

图 1 大中型企业的网络隔离典型应用图

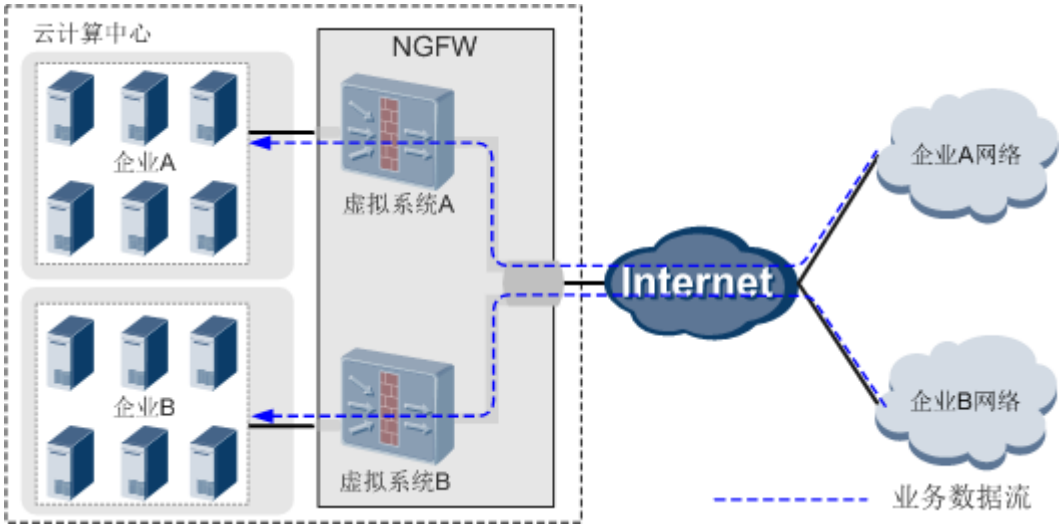


云计算中心的安全网关

新兴的云计算技术，其核心理念是将网络资源和计算能力存放于网络云端。网络用户只需通过网络终端接入公有网络，就可以访问相应的网络资源，使用相应的服务。在这个过程中，不同用户之间的流量隔离、安全防护和资源分配是非常重要的一环。通过配置虚拟系统，就可以让部署在云计算中心出口的 NGFW 具备云计算网关的能力，对用户流量进行隔离的同时提供强大的安全防护能力。

如图 2 所示，企业 A 和企业 B 分别在云计算中心放置了服务器。NGFW 作为云计算中心出口的安全网关，能够隔离不同企业的网络及流量，并根据需求进行安全防护。

图 2 云计算中心的安全网关典型应用图



使用限制与注意事项

介绍虚拟系统在使用中的限制和注意事项。

使用限制

NGFW 的大部分功能在虚拟系统中都能配置，具体请参见虚拟系统功能支持列表。但部分功能存在一些配置上的限制，具体如表 1 所示。

表 1 虚拟系统功能使用限制

功能	使用限制
管理员	虚拟系统管理员不能通过 Console 口登录设备。
特征库升级和系统软件升级	只能在根系统中进行特征库和系统软件的升级操作。
配置文件管理	虚拟系统管理员可以通过 Web 界面或 CLI 界面查看、保存自己管理的虚拟系统的配置。但配置文件的导入、导出只能通过 Web 界面。
SSH	支持虚拟系统管理员通过 STelnet 方式登录虚拟系统，但本地密钥对只能在根系统生成，所有虚拟系统共用根系统的配置。
服务端口	所有服务端口都只能在根系统中修改，如 HTTP 服务端口、HTTPS 服务端口、SSH 服务端口等。
证书	只能在根系统中进行证书的相关配置，如申请、导入和删除证书，上传 CRL 列表，配置证书过滤规则等，所有虚拟系统共用根系统的配置。
用户与认证	只能在根系统中配置认证页面，所有虚拟系统共用根系统的配置。
日志和报表	只能在根系统中配置日志服务器，所有虚拟系统共用根系统的配置。

注意事项

在分配接口或 VLAN 前，如果接口、VLAN 以及与 VLAN 对应的 VLANIF 存在以下情况是不可分配的，需要将相关配置清除或者解除特性的引用才可以分配。

- 接口或 VLAN 已经被分配给其他虚拟系统
- 接口或 VLANIF 在双机热备中被作为心跳口
- 接口或 VLANIF 已经配置为特征库升级时用于发送升级请求报文的接口
- 接口或 VLANIF 已经被策略引用
- 接口或 VLANIF 已经配置了 TCP 代理或 IPv6 功能、加入了安全区域或 Link-Group
- 接口是 Eth-Trunk 的成员接口或被切换为二层接口

如果接口存在以下配置，在分配时相关配置会被自动清除。

- 接口上配置了 IP 地址
- 接口已经应用了 IPSec
- 接口上应用了 DDoS 攻击防范

由于 Trunk 和 Hybrid 类型的二层接口以及配置子接口的三层接口可能同时被多个虚拟系统使用，所以在各个虚拟系统的“面板”的“接口流量统计信息”中，此类接口的流量数据将会是各个虚拟系统的总和数据。

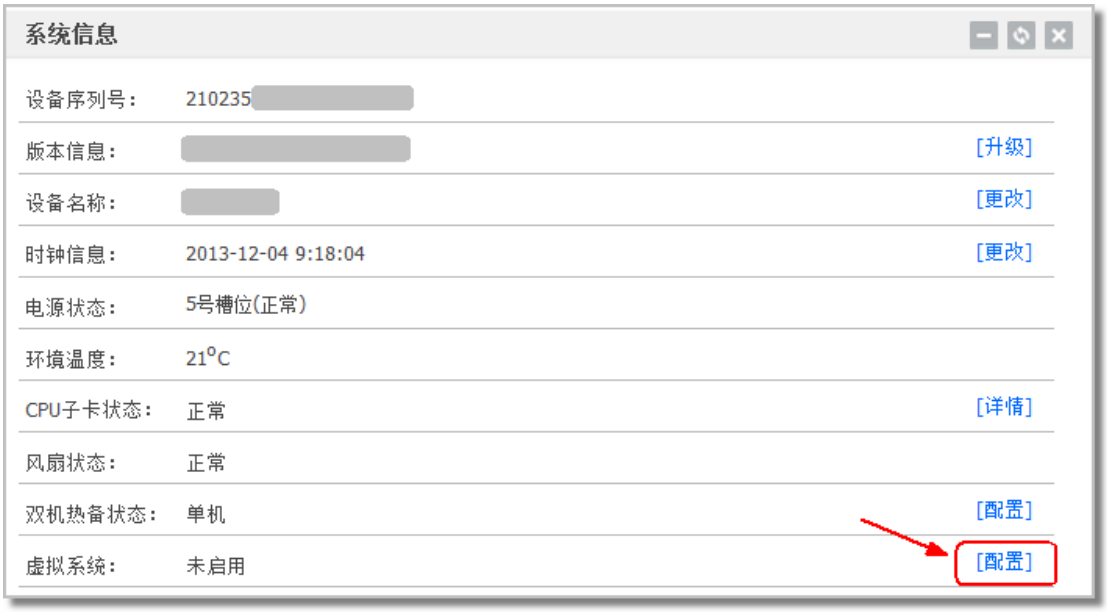
启用虚拟系统

启用虚拟系统功能后，才能配置资源类和创建虚拟系统。

操作步骤

1. 进入“面板”，在“系统信息”窗格中，单击“虚拟系统”所在行的“配置”。

   图 1 启用虚拟系统功能



2. 选中“启用”。

3. 单击“应用”。

Web 界面的变化

虚拟系统功能启用后，设备的 Web 界面会有如下的变化：

- Web 界面的右上角出现“虚拟系统”下拉选单。如图 2 所示，如果管理员在 NGFW 上创建了多个虚拟系统，可以通过单击下拉列表中的虚拟系统名称，进入虚拟系统的配置界面。其中，“root”是根系统，“vsysa”和“vsysb”是管理员创建的虚拟系统。

图 2 进入虚拟系统配置界面

- “系统”版块的菜单导航树中，出现“虚拟系统”节点。

图 3 虚拟系统配置节点

配置资源类

在创建虚拟系统前，请先完成资源类的配置。

背景信息

由于 NGFW 上所创建的虚拟系统会共同使用 NGFW 的资源，为避免因某个虚拟系统占用大量资源，导致其他虚拟系统无法获取资源、业务无法正常运行的情况，需要对单个虚拟系统允许使用的资源进行约束。

虚拟系统的资源分配是通过在资源类中规划资源数，再将资源类绑定虚拟系统来实现的。

说明：

一个资源类可以同时被多个虚拟系统绑定。当多个虚拟系统的资源需求相同时，根系统管理员只需要为这些虚拟系统配置一个资源类即可。

说明：

资源类 r0 默认与根系统绑定，不能删除、不能修改名称。

操作步骤

1. 查看资源的使用情况。

   由于根系统为多个虚拟系统分配资源，在分配资源前，根系统管理员需要查看剩余资源，以保证资源的正确分配。

   a. 选择“系统 > 虚拟系统 > 资源类”。

b. 单击“剩余资源”，显示剩余资源信息。

参数	说明
资源名称	-
剩余值	剩余值=整机规格-已分配的资源数-根系统已使用的资源数。 分配给虚拟系统的资源的保证数量不应超过当前的剩余值。

2. 单击“新建”，配置资源类的各项参数。

参数	说明
名称	输入资源类的名称。
描述	输入资源类描述信息。 合理填写描述信息有助于管理员正确理解资源类的功能，便于查找和维护。
资源名称	可分配的资源的名称。 其中，“策略数”是指所有策略的总数，包括安全策略、NAT 策略、带宽策略、认证策略、审计策略和策略路由；“最大带宽”是指虚拟系统所有接口（包括虚拟接口）入方向的最大带宽；“新建会话速率”是指虚拟系统每秒可新建的会话数。
保证值	虚拟系统可使用某项资源的最小数量。这部分资源一旦分配给虚拟系统，就被该虚拟系统独占。
最大值	虚拟系统可使用某项资源的最大数量。虚拟系统可使用的资源能否达到最大值视其他虚拟系统使用该项资源的情况而定。

3. 单击“确定”。

创建虚拟系统并分配资源

创建虚拟系统并为其分配资源。

背景信息

创建虚拟系统时，需要为其绑定资源类，使虚拟系统的会话、策略等资源得到保证。

为了完成虚拟系统业务的配置，根系统管理员还需要根据实际的组网需求为虚拟系统分配接口、VLAN。

操作步骤

1. 选择“系统 > 虚拟系统 > 虚拟系统”。

2. 单击“新建”，选择“基础配置”页签，配置各项参数。

参数	说明
名称	输入虚拟系统的名称。
描述	输入虚拟系统描述信息。 合理填写描述信息有助于管理员正确理解虚拟系统的功能，便于查找和维护。
资源类	绑定指定的资源类，取值如下： • 不选择资源类，以及选择“NONE”时，该虚拟系统的会话和策略等资源将抢占根系统的可用资源。当根系统资源已经被其他虚拟系统抢占完时，该虚拟系统将无资源可用。 • 选择“新建资源类”，创建新的资源类，与该虚拟系统绑定。 • 选择已存在的资源类，与该虚拟系统绑定。

3. 根据实际组网规划，为虚拟系统分配接口或 VLAN。

   • 选择“接口分配”页签，为虚拟系统分配接口。

   可分配的接口包括未被其他虚拟系统使用的三层以太网接口、子接口。

   • 选择“VLAN 分配”页签，为虚拟系统分配 VLAN。

   VLAN 中包含的二层接口或 VLANIF 会随 VLAN 分配给相应的虚拟系统。

4. 单击“确定”。

5. 单击界面右上角的“保存”，在弹出的对话框中单击“确定”。

后续处理

配置完成后，可以进行如下操作：

- 在“虚拟系统列表”中查看已创建的虚拟系统及分配的资源内容。
- 在“虚拟系统列表”中勾选虚拟系统，单击“当前资源使用信息”，查看指定虚拟系统的资源使用情况。
- 选择指定虚拟系统，单击  ，进入该虚拟系统的管理员页面。

如果在创建虚拟系统后，有一些虚拟系统不再需要使用，则可以在“虚拟系统列表”中勾选虚拟系统后，单击“删除”，然后在弹出的确认框中单击“确定”。系统将自动清除该虚拟系统的所有配置，回收所有已分配的资源，并将该虚拟系统删除。

配置虚拟系统与根系统互访

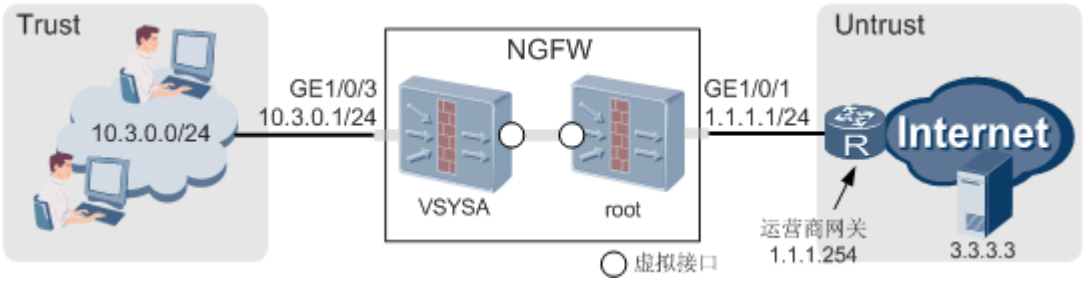
为实现虚拟系统与根系统间的通信，需要配置虚拟系统与根系统互访的路由和安全策略。

背景信息

配置虚拟系统与根系统互访时，可以将虚拟系统和根系统视为两台独立的设备。这两台设备间要能互访，需要在每台设备上配置正确的路由和安全策略。

如图 1 所示，虚拟系统 VSYSA 的用户要通过属于根系统的公网接口 GE1/0/1 访问 Internet 服务器 3.3.3.3，VSYSA 和根系统中需要分别完成如下配置。

图 1 虚拟系统和根系统间互访



操作步骤

1. 在 VSYSA 中配置路由和安全策略。

   a. 在界面右上角的“虚拟系统”下拉菜单中选择“vsysa”，进入 VSYSA。

   b. 选择“网络 > 路由 > 静态路由”。

   c. 单击“新建”，按如下参数配置到 Internet 的静态路由。

源虚拟系统	vsysa
目的地址/掩码	3.3.3.3/255.255.255.255
目的虚拟系统	root
下一跳	-
出接口	-

   d. 重复上述步骤，按如下参数配置到 VSYSA 内用户的静态路由。

源虚拟系统	vsysa
目的地址/掩码	10.3.0.0/255.255.255.0

目的虚拟系统	vsysa
下一跳	-
出接口	GE1/0/3

e. 选择“网络 > 接口”。

f. 单击“Virtualif1”接口对应的  按钮，将接口加入 Untrust 区域。

说明：

Virtualif 的编号会根据系统中 ID 占用情况自动分配。所以实际配置时，可能不是 Virtualif1。虚拟系统与 Virtualif 的对应关系可以在本系统的“接口列表”中看到。

g. 选择“策略 > 安全策略”。

h. 单击“新建”，按如下参数配置安全策略。

名称	to_internet
源安全区域	trust
目的安全区域	untrust
源地址/地区	10.3.0.0/24
目的地址/地区	3.3.3.3/32
动作	允许

2. 在根系统中配置路由和安全策略。

a. 在界面右上角的“虚拟系统”下拉菜单中选择“root”，进入根系统。

b. 选择“网络 > 路由 > 静态路由”。

c. 单击“新建”，按如下参数配置到 Internet 的静态路由。

源虚拟系统	root
目的地址/掩码	3.3.3.3/255.255.255.255
目的虚拟系统	root
下一跳	1.1.1.254
出接口	GE1/0/1

d. 重复上述步骤，按如下参数配置到 VSYSA 内用户的静态路由。

源虚拟系统	root
目的地址/掩码	10.3.0.0/255.255.255.0
目的虚拟系统	vsysa

下一跳	-
出接口	-

e. 选择“网络 > 接口”。

f. 单击“Virtualif0”接口对应的按钮，将接口加入 Trust 区域。

g. 选择“策略 > 安全策略”。

h. 单击“新建”，按如下参数配置安全策略。

名称	vsys_to_internet
源安全区域	trust
目的安全区域	untrust
源地址/地区	any
目的地址/地区	any
动作	允许

配置虚拟系统间互访

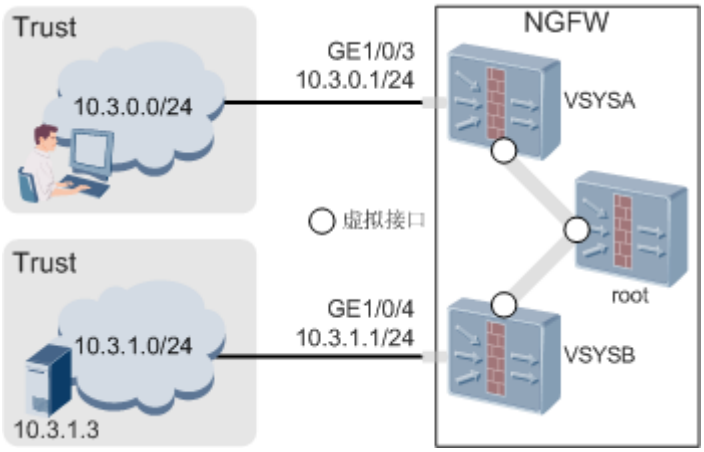
为实现两个虚拟系统间的通信，需要配置虚拟系统间互访的路由和安全策略。

背景信息

如图 1 所示，VSYSA 中的用户要访问 VSYSB 中的 Server，需要通过 VSYSA 访问根系统，再通过根系统访问 VSYSB 来实现。根系统就相当于一台路由器，负责连接两个虚拟系统，中转虚拟系统之间互访的报文。

建议您仔细阅读两个虚拟系统之间互访中的内容，理解虚拟系统间互访的原理，以便您能正确的进行配置。

图 1 虚拟系统间互访



操作步骤

1. 在根系统中配置 VSYSA 和 VSYSB 互访的路由。

> **说明：**
>
> 根系统只根据路由表对虚拟系统之间的访问报文进行转发，不进行其他安全功能的处理，因此不需要在根系统下针对这些报文配置安全策略。

   a. 在界面右上角的“虚拟系统”下拉菜单中选择“root”，进入根系统。

   b. 选择“网络 > 路由 > 静态路由”。

   c. 单击“新建”，按如下参数配置到 VSYSB 的静态路由。

源虚拟系统	root
目的地址/掩码	10.3.1.0/255.255.255.0
目的虚拟系统	vsysb
下一跳	-
出接口	-

   d. 重复上述步骤，按如下参数配置到 VSYSA 的静态路由。

源虚拟系统	root
目的地址/掩码	10.3.0.0/255.255.255.0
目的虚拟系统	vsysa
下一跳	-
出接口	-

2. 在 VSYSA 中配置路由和安全策略。

   a. 在界面右上角的“虚拟系统”下拉菜单中选择“vsysa”，进入 VSYSA。

   b. 选择“网络 > 路由 > 静态路由”。

   c. 单击“新建”，按如下参数配置到 VSYSB 内服务器的静态路由。

源虚拟系统	vsysa
目的地址/掩码	10.3.1.3/255.255.255.255
目的虚拟系统	root
下一跳	-
出接口	-

d. 重复上述步骤，按如下参数配置到 VSYSA 内用户的静态路由。

源虚拟系统	vsysa
目的地址/掩码	10.3.0.0/255.255.255.0
目的虚拟系统	vsysa
下一跳	-
出接口	GE1/0/3

e. 选择“网络 > 接口”。

f. 单击“Virtualif1”接口对应的  按钮，将接口加入 Untrust 区域。

说明：

Virtualif 的编号会根据系统中 ID 占用情况自动分配。所以实际配置时，可能不是 Virtualif1。虚拟系统与 Virtualif 的对应关系可以在本系统的“接口列表”中看到。

g. 选择“策略 > 安全策略”。

h. 单击“新建”，按如下参数配置安全策略。

名称	to_server
源安全区域	trust
目的安全区域	untrust
源地址/地区	10.3.0.0/24
目的地址/地区	10.3.1.3/32
动作	允许

3. 在 VSYSB 中配置路由和安全策略。

a. 在界面右上角的“虚拟系统”下拉菜单中选择“vsysb”，进入 VSYSB。

b. 选择“网络 > 路由 > 静态路由”。

c. 单击“新建”，按如下参数配置到 VSYSB 内服务器的静态路由。

源虚拟系统	vsysb
目的地址/掩码	10.3.1.0/255.255.255.0
目的虚拟系统	vsysb
下一跳	-
出接口	GE1/0/4

d. 重复上述步骤，按如下参数配置到 VSYSA 内用户的静态路由。

源虚拟系统	vsysb
目的地址/掩码	10.3.0.0/255.255.255.0
目的虚拟系统	root
下一跳	-
出接口	-

e. 选择“网络 > 接口”。

f. 单击“Virtualif2”接口对应的按钮，将接口加入 Untrust 区域。

g. 选择“策略 > 安全策略”。

h. 单击“新建”，按如下参数配置安全策略。

名称	vsysa_to_server
源安全区域	untrust
目的安全区域	trust
源地址/地区	10.3.0.0/24
目的地址/地区	10.3.1.3/32
动作	允许

创建虚拟系统管理员

创建虚拟系统管理员、配置管理员的登录方式和登录接口。

背景信息

创建虚拟系统后，根系统管理员可以为虚拟系统创建一个或多个管理员。使用这些管理员账号登录设备，可以配置虚拟系统的业务。根系统管理员需要进入虚拟系统的配置界面才能创建虚拟系统管理员，创建虚拟系统管理员的方法与创建根系统管理员的方法相同。

数据规划

项目	数据
管理员	用户名：admin@vsysa 认证类型：本地认证 密码：Vsysadmin@123 角色：系统管理员 信任主机：10.3.0.99/32 和 10.3.0.100/32

项目	数据
登录接口	接口：GE1/0/3 安全区域：Trust IP 地址：10.3.0.1/24 所属虚拟系统：VSYSA **说明：** 虚拟系统的登录接口也可以是属于根系统的接口。
登录方式	HTTPS 登录 Web

说明：

假设已完成虚拟系统 VSYSA 的创建，GE1/0/3 已经分配给虚拟系统。在此基础上，以下操作步骤只介绍配置管理员和登录接口的相关内容。

操作步骤

1. 创建虚拟系统管理员。

   a. 在界面右上角的“虚拟系统”下拉菜单中选择“vsysa”，进入 VSYSA。

   b. 选择“系统 > 管理员 > 管理员”。

   c. 单击“新建”，配置各项参数。

说明：

虚拟系统管理员用户名必须带后缀“@*虚拟系统名称*”。

如果使用第三方认证服务器对虚拟系统管理员进行认证，认证服务器上配置的用户名不需要带后

缀“@*虚拟系统名称*”。例如，认证服务器需要对虚拟系统 VSYSA 的管理员 admin@vsysa 进行认证时，认证服务器上配置的用户名应该是 admin。

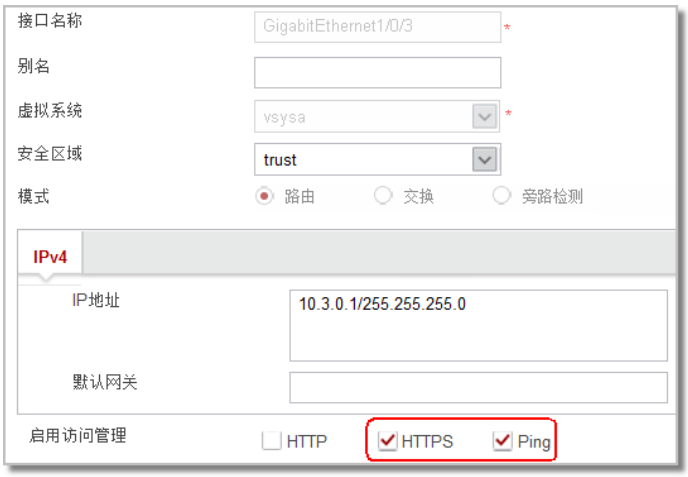
说明：

信任主机指定了可以登录设备的主机 IP 地址范围。如果管理员 PC 的 IP 地址固定，可以配置信任主机，只允许管理员从这些 IP 地址登录设备。如果管理员 PC 的 IP 地址经常变动，则不建议配置信任主机。因为管理员 PC 的 IP 地址不在信任主机所指定的 IP 地址范围内时，会导致管理员无法登录设备。

2. 配置登录接口。

   a. 选择“网络 > 接口”。

   b. 单击 GE1/0/3 接口对应的按钮，配置各项参数。



说明：

访问管理中选中“HTTPS”，表示允许管理员通过 HTTPS 协议登录 Web 界面。您也可以选择使用 HTTP 协议，但出于安全性的考虑，建议您使用 HTTPS 协议。

选中“Ping”，表示允许接口对 ping 请求做出响应。为了方便管理员检测管理员 PC 到登录接口的连接是否畅通，建议选中此项。

3. 启用 HTTPS 服务。

   a. 在界面右上角的“虚拟系统”下拉菜单中选择“root”，进入根系统。

   b. 选择“系统 > 管理员 > 设置”，查看 HTTPS 服务是否已经启用。若未启用，启用并配置端口号。

c. 单击“应用”。

4. 单击界面右上角的“保存”，在弹出的对话框中单击“确定”。

后续处理

完成上述配置后，虚拟系统管理员可以按照如下步骤登录虚拟系统：

1. 在管理员 PC 中打开网络浏览器，访问需要登录设备的 IP 地址“https://10.3.0.1:*端口号*”。

   说明：

   输入 IP 地址登录后，浏览器可能会给出证书不安全的提示，此时可以选择继续浏览。

2. 在登录界面中输入管理员的用户名“Admin@vsysa”和密码“Vsysadmin@123”，单击“登录”，进入虚拟系统 Web 界面。

举例：通过虚拟系统隔离企业部门（三层接入，虚拟系统共用根系统公网接口）

企业内划分为多个部门，各部门间职能和权责划分明确，需要制定不同的网络管理策略，导致配置复杂。NGFW 作为企业网络的出口网关，通过虚拟系统功能实现对不同部门网络的区分管理，降低配置难度。

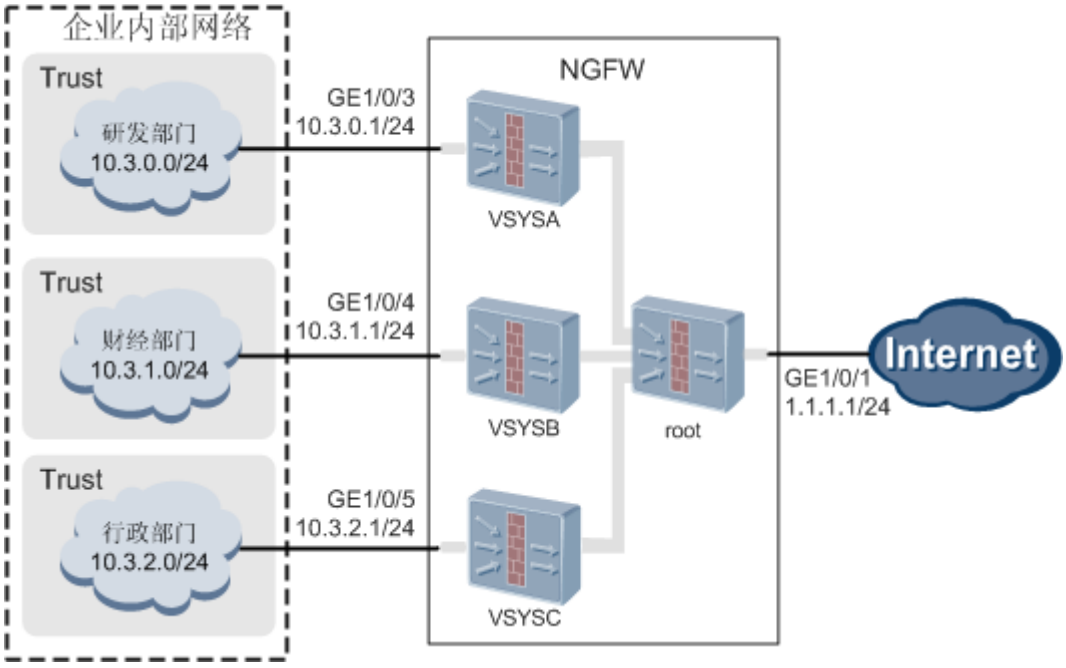
组网需求

某中型企业 A，购买一台防火墙作为网关。由于其内网员工众多，根据权限不同划分为研发部门、财经部门、行政部门三大网络。需要分别配置不同的安全策略。具体要求如下：

- 由于只有一个公网 IP 和公网接口，公司内网所有部门都需要借用同一个接口访问 Internet。
- 财经部门禁止访问 Internet，研发部门只有部分员工可以访问 Internet，行政部门则全部可以访问 Internet。
- 三个部门的业务量差不多，所以为它们分配相同的虚拟系统资源。

通过虚拟系统就可以实现上述需求。组网图如图 1 所示。

图 1 网络隔离组网图（三层接入，虚拟系统共用根系统公网接口）



数据规划

项目	数据	说明
root	• 公网接口：GE1/0/1 • 公网接口所属安全区域：Untrust • 公网接口 IP 地址：1.1.1.1/24 • 私网接口：root 的虚拟接口 Virtualif0 • 私网接口所属安全区域：Trust • 运营商接入网关 IP 地址：1.1.1.254/24	在本例中，所有部门都要通过根系统才可访问 Internet，而且各个部门的私网地址是统一规划的，没有重叠的情况。所以在根系统中统一配置 NAT 策略。
VSYSA	• 虚拟系统名：VSYSA • 公网接口：VSYSA 的虚拟接口 • 公网接口所属安全区域：Untrust • 私网接口：GE1/0/3 • 私网接口 IP 地址：10.3.0.1/24 • 私网地址范围：10.3.0.0/24 • 私网接口所属安全区域：Trust • 管理员：admin@vsysa	-

项目	数据	说明
	• 允许访问 Internet 的地址范围：10.3.0.2～10.3.0.10	
VSYSB	• 虚拟系统名：VSYSB • 公网接口：VSYSB 的虚拟接口 • 公网接口所属安全区域：Untrust • 私网接口：GE1/0/4 • 私网接口 IP 地址：10.3.1.1/24 • 私网地址范围：10.3.1.0/24 • 私网接口所属安全区域：Trust • 管理员：admin@vsysb	-
VSYSC	• 虚拟系统名：VSYSC • 公网接口：VSYSC 的虚拟接口 • 公网接口所属安全区域：Untrust • 私网接口：GE1/0/5 • 私网接口 IP 地址：10.3.2.1/24 • 私网地址范围：10.3.2.0/24 • 私网接口所属安全区域：Trust • 管理员：admin@vsysc	-
资源类	• 名称：r1 • 会话保证值：10000 • 会话最大值：50000 • 用户数：300 • 用户组：10 • 策略数：300 • 最大带宽：100000Kpbs	三个部门的业务量差不多，所以为它们分配相同的虚拟系统资源。

配置思路

1. 根系统管理员分别创建虚拟系统 VSYSA、VSYSB、VSYSC 并为每个虚拟系统分配资源和配置管理员。
2. 根系统管理员为内网用户访问 Internet 配置路由和 NAT 策略。
3. 研发部门的管理员登录设备，为虚拟系统 VSYSA 配置 IP 地址、路由和安全策略。
4. 财经部门的管理员登录设备，为虚拟系统 VSYSB 配置 IP 地址、路由和安全策略。
5. 行政部门的管理员登录设备，为虚拟系统 VSYSC 配置 IP 地址、路由和安全策略。

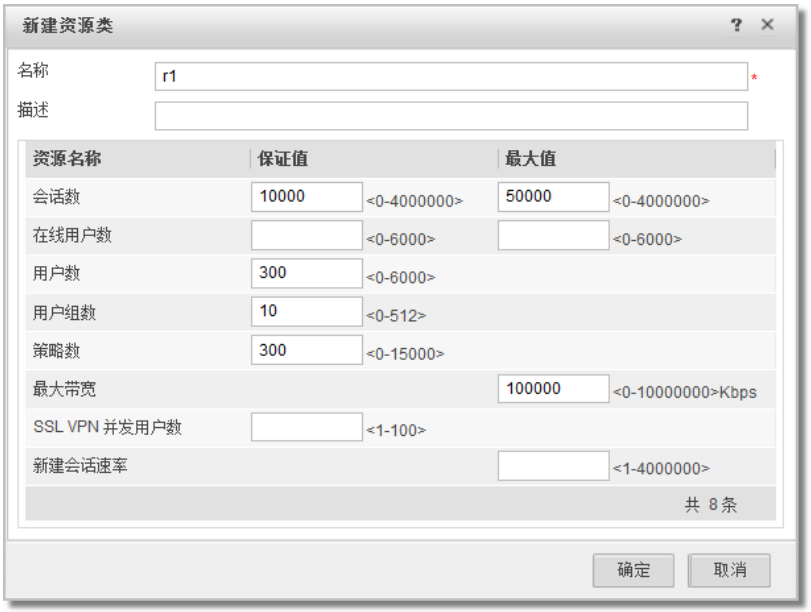
操作步骤

1. 根系统管理员分别创建虚拟系统 VSYSA、VSYSB 和 VSYSC，并为其分配资源。

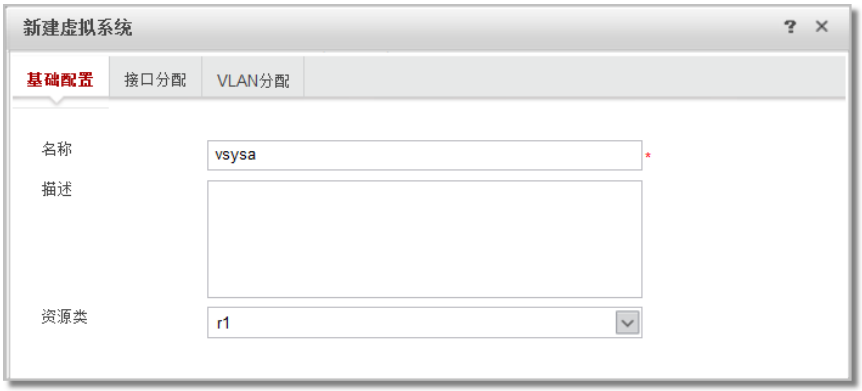
   a. 使用根系统管理员账号登录设备 Web 界面。

   b. 选择“面板”，在“系统信息”面板中单击“虚拟系统”对应的“配置”按钮，勾选“虚拟系统”对应的“启用”按钮，单击“应用”。

   c. 选择“系统 > 虚拟系统 > 资源类”，单击“新建”，按如下参数配置资源类。



   d. 选择“系统 > 虚拟系统 > 虚拟系统”，单击“新建”，按如下参数完成虚拟系统 VSYSA 的基础配置。



   e. 选择“接口分配”页签，单击按钮将接口 GE1/0/3 分配给 VSYSA。

f. 单击界面右上角的“保存”，保存配置。

g. 参考上述步骤继续创建 VSYSB 和 VSYSC，并将接口 GE1/0/4 分配给 VSYSB，将接口 GE1/0/5 分配给 VSYSC。

2. 根系统管理员为虚拟系统创建管理员。

a. 在界面右上角的“虚拟系统”下拉菜单中选择“vsysa”后，进入虚拟系统“vsysa”中。

b. 选择“系统 > 管理员 > 管理员”，单击“新建”，配置各项参数。

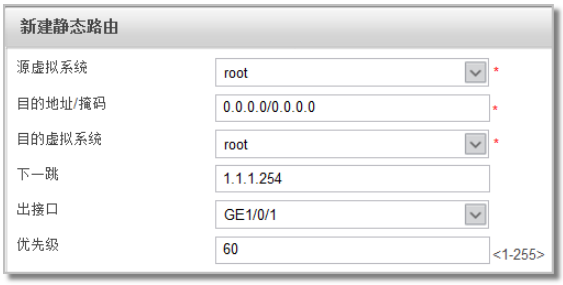
c. 参考上述步骤为虚拟系统 VSYSB 和 VSYSC 创建管理员“admin@vsysb”和“admin@vsysc”。

3. 根系统管理员为内网用户访问 Internet 配置路由、安全策略和 NAT 策略。

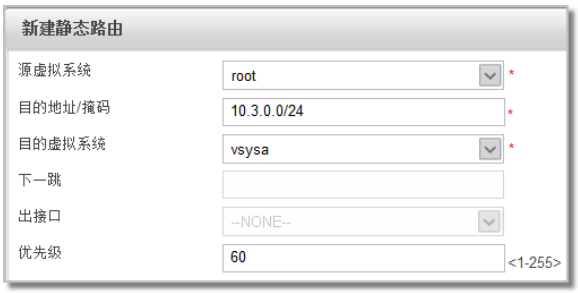
   a. 选择“网络 > 接口”，单击 GE1/0/1 接口对应的按钮，按如下参数为其配置 IP 地址和安全区域。

   b. 参考上述步骤将 Virtualif0 接口加入 Trust 区域。

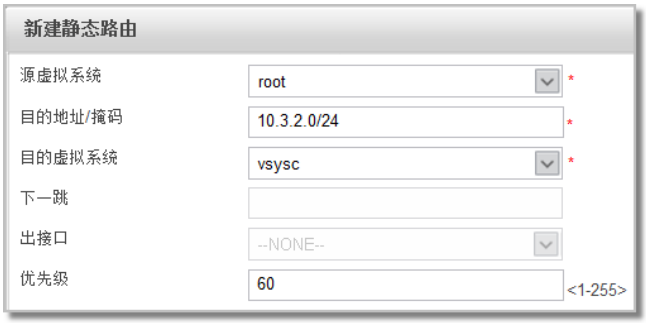
   c. 选择“网络 > 路由 > 静态路由”，单击“新建”，按如下参数配置静态路由。



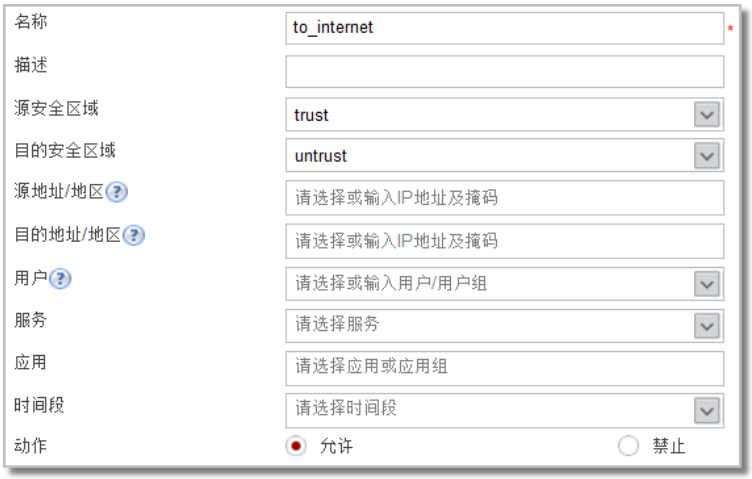
   d. 单击“新建”，按如下参数配置静态路由。这条静态路由的作用是将 VSYSA 内员工访问 Internet 的回程流量引入 VSYSA。



   e. 单击“新建”，按如下参数配置静态路由。这条静态路由的作用是将 VSYSC 内员工访问 Internet 的回程流量引入 VSYSC。



f. 选择“策略 > 安全策略 > 安全策略”，单击“新建”，按如下参数配置安全策略。这条安全策略的作用是允许内网的员工访问 Internet。虚拟系统管理员可以针对内网员工的 IP 地址配置严格的安全策略，所以根系统管理员在配置策略时不需要详细指定地址范围，直接选择“any”即可。



g. 选择“策略 > NAT 策略 > 源 NAT > 源 NAT”，单击“新建”，按如下参数配置 NAT 策略。

4. 研发部门的管理员为虚拟系统 VSYSA 配置 IP 地址、路由和安全策略。

a. 使用虚拟系统 A 管理员账号“admin@vsysa”登录设备 Web 界面。

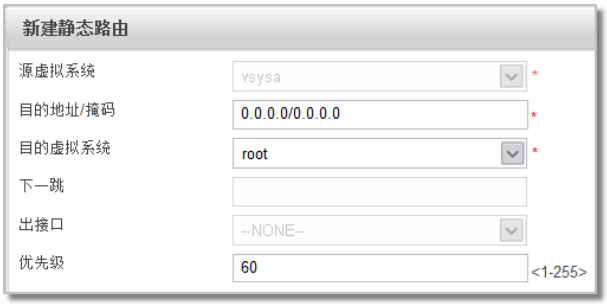
b. 选择“网络 > 接口”，单击 GE1/0/3 接口对应的按钮，按如下参数为其配置 IP 地址和安全区域。

c. 参考上述步骤将 Virtualif1 接口加入 Untrust 区域。

说明：

Virtualif 的编号会根据系统中 ID 占用情况自动分配。所以实际配置时，可能不是 Virtualif1。虚拟系统与 Virtualif 的对应关系可以在本系统的“接口列表”中看到。

d. 选择“网络 > 路由 > 静态路由”，单击“新建”，按如下参数配置静态路由。这条静态路由的作用是将 VSYSA 内员工访问 Internet 的流量引入根系统。



说明：

在本例中，对网络拓扑和路由配置进行了简化。假设 VSYSA 只有私网跟 Internet 的通信需求，所以在路由配置中将“目的地址/掩码”配置为了 0.0.0.0/0.0.0.0，即缺省所有报文都送往根系统。实际配置时，为了保证路由信息的准确，应该将“目的地址/掩码”配置为特定的允许访问的 Internet 地址范围。错误配置路由可能导致 VSYSA 所连接的多个私网无法正常通信。

e. 单击“新建”，按如下参数配置静态路由。这条静态路由是 VSYSA 内员工访问 Internet 流量的回程路由。

f. 选择“对象 > 地址 > 地址”，单击“新建”，按如下参数配置地址。

g. 选择“策略 > 安全策略 > 安全策略”，单击“新建”，按如下参数配置安全策略。这条安全策略的作用是允许特定网段的员工访问 Internet。

h. 参考上述步骤按如下参数再新建一条禁止所有员工访问 Internet 的策略。这条策略的优先级将比前一条低，所以不需要详细指定地址范围，直接选择“any”即可。

i. 单击界面右上角的“保存”，保存配置。

5. 财经部门和行政部门的管理员分别使用管理员账号“admin@vsysb”和“admin@vsysc”登录设备 Web 界面，为虚拟系统 VSYSB、VSYSC 配置 IP 地址、安全区域及策略。

具体配置过程与研发部门类似，主要有以下几点区别。

- 内网接口的 IP 地址不同。
- 财经部门无需创建地址范围，直接配置一条禁止所有地址范围访问 Internet 的安全策略即可。
- 行政部门无需创建地址范围，直接配置一条允许所有地址范围访问 Internet 的安全策略即可。

结果验证

- 从行政部门的内网主动访问 Internet，如果能够访问成功，说明 IP 地址、VSYSC 的安全策略以及根系统 NAT 策略配置正确。
- 从财经部门的内网主动访问 Internet，如果访问失败，说明 IP 地址和 VSYSB 的安全策略配置正确。
- 从研发部门的内网选择一台允许访问 Internet 的主机，和一台不允许访问 Internet 的主机，如果访问结果符合预期，说明 IP 地址和 VSYSA 的安全策略的配置正确。

配置脚本

根系统的配置脚本

```
#
 sysname NGFW
#
```

```
 vsys enable
#
resource-class r0
#
resource-class r1
 resource-item-limit session reserved-number 10000 maximum 50000
 resource-item-limit policy reserved-number 300
 resource-item-limit user reserved-number 300
 resource-item-limit user-group reserved-number 10
 resource-item-limit bandwidth-ingress reserved-number 0 maximum 100000
#
vsys name vsysa 1
 assign resource-class r1
 assign interface GigabitEthernet1/0/3
#
vsys name vsysb 2
 assign resource-class r1
 assign interface GigabitEthernet1/0/4
#
vsys name vsysc 3
 assign resource-class r1
 assign interface GigabitEthernet1/0/5
#
interface GigabitEthernet1/0/1
 ip address 1.1.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface Virtualif0
#
firewall zone untrust
 set priority 5
 add interface GigabitEthernet1/0/1
#
 ip route-static 0.0.0.0 0.0.0.0 GigabitEthernet1/0/1 1.1.1.254
 ip route-static 10.3.0.0 255.255.255.0 vpn-instance vsysa
 ip route-static 10.3.2.0 255.255.255.0 vpn-instance vsysc
#
security-policy
 rule name to_internet
  source-zone trust
  destination-zone untrust
```

```
  action permit
#
 nat-policy
  rule name nat1
   source-zone trust
   egress-interface GigabitEthernet1/0/1
   source-address address-set 10.3.0.0 16
   action nat easy-ip
#
return
```

虚拟系统 VSYSA 的配置脚本

```
#
interface GigabitEthernet1/0/3
 ip address 10.3.0.1 255.255.255.0
 service-manage ping permit
#
firewall zone trust
 set priority 85
 add interface GigabitEthernet1/0/3
#
firewall zone untrust
 set priority 5
 add interface Virtualif1
#
aaa
 #
 manager-user admin@vsysa
  password cipher %@%@@~QEN4"Db/xmvR'5@=5)``WN]~h`Mwn-{BNPy#ZYE>`6`f]X%@%@
  service-type web telnet ssh
  level 15
  ssh authentication-type password
  ssh service-type stelnet
  authentication-scheme admin_local
 #
 bind manager-user admin@vsysa role system-admin
#
ip address-set ipaddress1 type object
 address 0 range 10.3.0.2 10.3.0.10
#
 ip route-static 0.0.0.0 0.0.0.0 public
```

```
 ip route-static 10.3.0.0 255.255.255.0 GigabitEthernet1/0/3
#
security-policy
 rule name to_internet
  source-zone trust
  destination-zone untrust
  source-address address-set ipaddress1
  action permit
 rule name to_internet2
  source-zone trust
  destination-zone untrust
  action deny
#
return
```

虚拟系统 VSYSB 的配置脚本

```
#
interface GigabitEthernet1/0/4
 ip address 10.3.1.1 255.255.255.0
 service-manage ping permit
#
firewall zone trust
 set priority 85
 add interface GigabitEthernet1/0/4
#
firewall zone untrust
 set priority 5
 add interface Virtualif2
#
aaa
 #
 manager-user admin@vsysb
  password cipher %@%@zG{;O|!gEN4"Db/xmvR'5@=5)``WN]~h`Mwn-{BNPy#ZYE>`6`f]
  service-type web telnet ssh
  level 15
  ssh authentication-type password
  ssh service-type stelnet
  authentication-scheme admin_local
 #
 bind manager-user admin@vsysa role system-admin
#
```

```
 ip route-static 0.0.0.0 0.0.0.0 public
 ip route-static 10.3.1.0 255.255.255.0 GigabitEthernet1/0/4
#
security-policy
 rule name to_internet
  source-zone trust
  destination-zone untrust
  action deny
#
return
```

虚拟系统 VSYSC 的配置脚本

```
#
interface GigabitEthernet1/0/5
 ip address 10.3.2.1 255.255.255.0
 service-manage ping permit
#
firewall zone trust
 set priority 85
 add interface GigabitEthernet1/0/5
#
firewall zone untrust
 set priority 5
 add interface Virtualif3
#
aaa
 #
 manager-user admin@vsysc
  password cipher %@%@zG{;x|!gEN5"Db/6dvR'5@=5)``WN]~h`Mwn-{BNPy#ZYE>`6`f]
  service-type web telnet ssh
  level 15
  ssh authentication-type password
  ssh service-type stelnet
  authentication-scheme admin_local
 #
 bind manager-user admin@vsysa role system-admin
#
 ip route-static 0.0.0.0 0.0.0.0 public
 ip route-static 10.3.2.0 255.255.255.0 GigabitEthernet1/0/5
#
security-policy
```

```
 rule name to_internet
  source-zone trust
  destination-zone untrust
  action permit
#
return
```

虚拟防火墙在各设备的规格

介绍虚拟系统的规格参数。

虚拟系统的相关规格如下：

- 可以创建的虚拟系统个数：
  - USG6310/6320/6510-SJJ：缺省 10 个，可通过购买 License 扩展至 20 个
  - USG6330/6350/6360/6530：缺省 10 个，可通过购买 License 扩展至 50 个
  - USG6370/6380/6390/6550/6570：缺省 10 个，可通过购买 License 扩展至 100 个
  - USG6620/6630：缺省 10 个，可通过购买 License 扩展至 200 个
  - USG6650/6660/6670：缺省 10 个，可通过购买 License 扩展至 500 个
  - USG6680：缺省 10 个，可通过购买 License 扩展至 1000 个
  - ET1D2FW00S00： 缺省 10 个，可通过购买 License 扩展至 500 个
  - ET1D2FW00S01、ET1D2FW00S02：缺省 10 个，可通过购买 License 扩展至 1000 个
- 每个虚拟系统可以配置的 SSL VPN 虚拟网关个数：4
- 每个虚拟系统的安全区域个数：8（缺省 4 个、自定义 4 个）
- 整机支持配置的虚拟系统管理员个数：1024

虚拟系统功能支持列表

介绍虚拟系统中支持配置的功能。

虚拟系统中支持配置的功能如表 1 所示。

表 1 虚拟系统功能支持列表

功能		支持情况	说明
系统	管理员	支持	-
	系统时钟	不支持	-
	SNMP	不支持	-
	跨三层 MAC 识别	支持	访问 SNMP 服务器时间间隔和访问 SNMP 服务器超长时长只能在根系统下设置，虚拟系统下不能修改。
	推送信息配置	支持	仅支持为反病毒（AV）功能配置推送信息。
	信息中心	不支持	-
	文件系统	不支持	-
	特征库升级	不支持	-
	系统更新	不支持	-
	配置文件管理	支持	-
	NetStream	不支持	-
	敏捷网络	不支持	-
高可靠性	双机热备	不支持	-
	Bypass	不支持	-
	Link-group	不支持	-
	IP-Link	支持	-
	BFD	不支持	-
网络	接口	支持	-
	安全区域	支持	-
	DNS	不支持	-
	DHCP	支持	仅支持在接口上配置 DHCP 客户端功能。
	PPP	不支持	-
	PPPoE	不支持	-
智能选路	全局选路策略	不支持	-
	运营商地址库选路	不支持	-
	策略路由	支持	不支持策略路由智能选路。

表 1 虚拟系统功能支持列表			
功能		**支持情况**	**说明**
IP 路由	静态路由	支持	-
	动态路由	不支持	-
对象	用户	支持	不支持单点登录。
	地址和地址组	支持	-
	域名组	支持	-
	地区和地区组	支持	-
	服务和服务组	支持	-
	应用和应用组	支持	-
	证书	支持	仅能引用和查看证书，不能配置证书。
	时间段	支持	-
	ACL	支持	-
	链路健康检查	不支持	-
SSL 解密	SSL 解密	支持	-
策略	安全策略和安全配置文件	支持	• 不支持垃圾邮件过滤功能。 • 不支持配置 URL 分类服务器。
	认证策略	支持	-
	审计策略和审计配置文件	支持	-
	NAT 策略	支持	不支持服务器负载均衡功能。
	带宽策略	支持	-
	配额控制策略	支持	-
	SSL 解密策略	支持	-
VPN	IPSec	不支持	-
	L2TP	不支持	-
	GRE	不支持	-
	BGP/MPLS IP VPN	不支持	-
	SSL VPN	支持	-
安全防护	攻击防范	支持	仅支持 DDoS 攻击防范功能。
	黑名单	支持	-

表 1 虚拟系统功能支持列表			
功能		支持情况	说明
	IP-MAC 绑定	支持	-
	ASPF	支持	-
	IDS 联动	不支持	-
监控	日志和报表	支持	-
	会话表	支持	-
	Server-map 表	支持	-
	系统统计	不支持	-
	远程抓包	不支持	-
	诊断中心	支持	-
IPv6 功能	IPv6 功能	不支持	-
维护功能	端口镜像、重启系统、NTP、NQA、LLDP 等功能	不支持	-

HCIE-Security 模拟面试问题及面试建议

1. 虚拟系统与根系统之间互访流程？
2. 虚拟防火墙应用场景？