**专利技术交底书**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **企业名称：** | 申请人为单位时填写 | | **统一社会信用代码：** |  |
| **申请人姓名：** | 詹志 | | **申请人身份证号：** | 申请人为自然人时填写 |
| **专利名称：** | 一种网络靶场中虚拟管理网络的设计和实现 | | | |
| **通讯地址:** |  | | **邮编:** |  |
| **是否同步申请实质审查：** | 是/否 | | **是否申请**  **提前公布：** | 是/否 |
| **技术联系人：** | **姓名：詹志**  **电话：13361875998**  **E-mail：1782865441@qq.com** | | | |
| **发明人（可以写多个）：** | |  | | |
| **第一发明人的身份证号码：** | |  | | |

|  |
| --- |
| **一、技术领域 ：**本发明或实用新型属于何技术领域，可以在哪些领域应用。 |
| 计算机、软件领域、网络安全 |
| **二、背景技术：**（即现有技术）1、介绍所属技术领域的现有技术，尤其是与本发明欲改进的核心技术有关的技术现状。2、可从大的技术背景（该技术领域的总体状况）和小的技术背景（与本发明改进的具体技术密切相关的技术状况）两个方面进行介绍。3、如果现有技术出自专利文献、期刊、书籍等，则提供出处。现有技术有相关附图的，最好一并提供并结合附图说明。 |
| 网络靶场是一种基于虚拟化技术，对真实网络环境的仿真，作为支撑网络空间安全技术验证，网络武器装备试验，攻防对抗演练和网络风险评估的平台。  在将靶场中某个拓扑构建完成后，还需要对拓扑中的虚机实例进行网络配置、信息采集、流量发生等管理操作。这些操作都需要通过预先建立好的虚拟管理网络，来实现将外部网络中信令流量到达指定的内部虚机。  本专利提出一种机制，来构建出拓扑实例中用于管理操作的虚拟管理网络，支持接入外部网络的靶场平台发送的网络配置、信息采集、流量发生等信令流量路由到具体拓扑实例节点中，完成拓扑实例构建后执行的各类节点实例管理操作。 |
| |  | | --- | | **三、现有技术存在的问题：**1、客观评价现有技术的缺点，会带来哪些问题（这些缺点是针对本发明的优点来说的，本发明正是要解决这些问题和缺点，本发明不能解决的问题和缺点不必写）。2、如果找不到对比技术方案及其缺点，可用反推法，根据本发明的优点来找出对应的缺点。3、缺点可以是成本高、结构复杂、性能差、工艺繁琐等类似问题。4、针对前面现有技术的所有缺点，逐一正面描述本发明所要解决的技术问题。 | | 1. 用于管理操作的信令流量的网络路由和拓扑实例节点之间的业务流量的网络路由没有完全独立，实例节点之间的业务流量会影响信令流量接收和响应。容易造成管理操作执行异常。 2. 拓扑实例节点可以通过虚拟管理网络攻击到靶场平台，异常流量可以发送到靶场平台，容易造成靶场平台的不稳定。 3. 虚拟管理网络没有针对大规模网络做负载均衡，信令流量的接收和发送容易出现单点故障，造成管理操作执行异常。 | |
| |  | | --- | | **四、本发明或实用新型采用的技术方案：**本部分是专利文件中最重要的部分，越详细越好。  1、阐明本发明是通过什么样的技术方案来解决其技术问题的（即实现发明目的），不能只有原理，也不能只作功能介绍，应当详细描述本发明的各个发明改进点及相应的技术方案。  2、技术方案应当清楚、完整地描述本发明的技术特征（如构造、组织、形状等）以及作用、原理，以使本领域普通技术人员能够实施本发明为准。  3、对于不同类型的发明创造需采用不同的描述方式来说明其技术方案。例如：对于设备发明，应当具体说明其零部件的结构及其连接关系，必要时结合附图加以说明；对于方法发明，应当具体说明其工艺方法、工艺流程和条件（如时间、压力、温度、浓度）；涉及机电一体化的发明，对于其中与电路有关的内容应当提供电路图、原理框图、流程图或时序图，并结合附图进行具体说明；对于涉及软件、业务（商务）方法的专利申请，除提供流程图外，还应提供相关的系统模块框图，并按照流程的时间顺序，以自然语言对各步骤进行描述。  4、所有附图应当有相应的文字描述，图中的关键词或注释尽量用中文。所有英文缩写（除了普遍公认有确定含义的）应有中文注释。注意，附图尽可能提供可编辑格式的版本以便代理人调整，如Visio、CAD、PPT等。 | | 针对上述描述的问题。本发明专利，设计了一种虚拟管理网络构建方式，在实现靶场平台能正常向拓扑实例节点发送信令流量的同时，将信令流量和拓扑实例节点之间的业务流量的网络路由分离，同时添加网络防火墙规则，实现拓扑内部实例节点和靶场平台之间的流量控制。同时根据不同拓扑的子网数量，创建出不同的数量的管理网络，实现管理网络信令流量的负载均衡，避免单点造成全局故障。  具体方案详细设计和实现如下：    如上图所示，在拓扑实例1中，虚拟节点a、业务网络交换机a、虚拟节点b、虚拟业务网络路由器、 业务网络交换机b、虚拟节点c、虚拟节点d共7个节点为拓扑实例1的业务节点，即靶场平台用户查看拓扑实例1时，能之间查看到的节点。内部管理网络交换机a、内部管理网络交换机b、内部核心路由器为针对拓扑实例1的业务网络对应构建出的管理网络路由。虚拟配置采集代理a、虚拟配置采集代理b为拓扑实例1中业务网络映射的管理网络对应的配置和采集代理虚拟，用作连接到当前内部管理网络交换机的所有业务节点的配置和采集管理操作。此外，每个业务网络交换机都会对应接入一个流量发生仪trex，用于对当前的业务网络交换机所有接入的业务节点执行流量发生等流量管理操作。这些所有内部管理网络交换机都会统一接入到一个内部核心路由器。内部核心路由器，会和外部预先创建好的SN核心路由连接。同时开启SNAT，支持所有的虚拟配置采集代理以及流量发生仪trex主动向外部的靶场平台上报采集数据、查询配置和流量操作。  下面详细描述虚拟管理网络时如何随着拓扑实例构建的，以及创建出的虚拟管理网络是如何实现靶场平台管理操作的信令流量下发到靶场实例内部的虚拟配置采集代理和流量发生仪器trex的。   1. 创建预定义的SN管理网络交换机和SN核心路由器   在安装靶场平台时，我们会预先建好一个固定的外部网络交换机-SN管理网络交换机，靶场平台所部署的虚拟机会固定接入SN管理网络交换机中。同时也会预先创建好一个SN核心路由器，用于拓扑实例内部的管理网络和外部靶场平台网络之间进行路由。因此，SN管理网络交换机也会预先固定接入到SN核心路由器中。   1. 拓扑实例内部业务网络交换机创建   我们以图中拓扑实例1的业务网络为例。我们会首先分别创建出业务网络交换机a和业务网络交换机b。业务网络交换机a和业务网络交换机b分别是两个独立的子网。这两个子网的值是默认从10.128.0.0/24 到10.255.255.0/24这32768个子网中随机选取两个。一个业务子网获取网段的随机算法如下：  2.1 Set<E> 记录当前拓扑已经分配的子网值，例如{ 1, 2}。Lock<Set<E>>为拓扑实例1的业务子网分配锁。所有的业务子网设置cidr时，需要先获取Lock<Set<E>>锁。  2.2调用Random函数，输入种子为当前时间，获取一个范围为[0,1]的浮点数n。  2.3当前网络子网值Vcidr为32768乘于上一步获取的随机数n，再向下取整。  2.4等待获取Lock<Set<E>>锁  2.5检查Set<E>是否包含当前网络子网值Vcidr，如果包含，Vcidr = Vcidr + 1，直到Vcidr不存在于Set<E>中。例如，如果Vcidr第一次随机的值为1，1已经包含在Set<E>中了，则Vcidr = Vcidr + 1 = 2。2仍然包含在Set<E>中，Vcidr = Vcidr + 1 = 3。3没有在Set<E>中，则Vcidr = 3，可以执行下一步了。  2.6将Vcidr加入到Set<E>中后，释放Lock<Set<E>>锁  2.7当前业务子网的网段为“10.”+ IntToStr((Vcidr >> 8) & 0xFF + 128) + “.” + IntToStr(Vcidr & 0xFF) + “.” + “0/24”。即ipv4地址第一段固定为10，第二段的值为Vcidr向右偏移8位后和0xFF进行AND位运算然后加上128，第三段的值为Vcidr和0xFF进行AND位运算，第四段的值固定为0，掩码固定为24位。   1. 拓扑实例内部管理网络构建   步骤2已经创建出了拓扑实例的所有业务网络交换机。交换机所在的网段默认是24位掩码，最多可以支持254个主机接入。一个大型的拓扑实例，会创建出几百甚至上千的业务网络交换机，支持接入十万级别数目的主机接入。为了实现主机的信息采集、网络配置下发和流量发生，不可能靶场平台直接和这些主机接入到同一个内部管理子网中。首先如果都接入到同一个内部管理子网中，这些机器会首先发送ARP广播包，该内部管理子网承载流量压力巨大，同时内部管理子网中的主机数目过多，每个主机的ARP缓存表也过大。其次靶场平台需要通过该内部管理子网下发主机网络配置、信息采集、流量发送等管理信令，所有的信令流量都依赖于同一个内部管理子网，容易造成网络阻塞，信令流量发送和接收失败。同时所有主机都接入到同一个内部管理子网，主机之间可以直接通过该子网直接进行通信，破坏了当前拓扑实例业务网络的逻辑。就此，针对性设计出了下面的内部管理网络构建方案。   * 1. 每个内部业务网络交换机对应一个内部管理网络交换机，每个内部管理网络交换机对应一个虚拟配置采集代理节点，每个内部管理网络交换机对应一个流量发生仪trex。   3.1.1 根据内部业务网络交换机所在网段，计算内部管理交换机的网段。根据步骤2描述的内部业务交换机网络计算算法可以知道，每个业务网络的网段都是不一样的。且所有的业务网络的IPv4网段前9位都是固定的，即前8位的值加起来是10，第9位都是1。如果一个业务网络交换机对应的网段为10.b.c.0/24，那么其对应的内部管理网络交换机的网段为10.(b-128).c.0/24。即一个业务网络交换机所在的网段要得到与其对应的内部管理网络交换机的网段，只需要将业务网络交换机所在网络的网络的第9为从1翻转到0，其它23位都保持一样，掩码也都是24位。  3.1.2 每个拓扑实例中的虚拟业务节点创建时，至少需要接入两个内部的网络交换机，一个是内部业务网络交换机，还有这个内部业务网络交换机对应的内部管理网络交换机。同时该虚拟业务节点设置的默认路由应该为所在的业务网络的路由，不需要针对所在的内部管理网络设置路由。因为虚拟业务节点只会和内部管理网络中的虚拟配置采集节点和流量发生仪器trex直接通信。它们直接的通信是同一个局域网内部，不需要通过任何路由。例如图中的拓扑实例1中的虚拟节点a，它只需要一条默认路由，网关是虚拟业务路由器接入业务网络交换机a的那个端口的ip地址。  3.1.3 每个内部管理网络交换机对应创建一个虚拟配置采集代理节点，该节点只会接入其对应的内部管理网络交换机，负责所有接入该内部管理网络交换机的业务节点的网络配置操作。例如在拓扑实例1中，我们需要针对虚拟节点a设置其接入内部业务网络交换机的那张网卡的DNS设置为1.1.1.1。靶场平台无法直接连接指定拓扑实例中的指定业务节点，下发配置。它是通过拓扑实例中的虚拟配置采集代理节点，下发业务节点的网络配置信息，完成网络配置。关于虚拟配置采集代理系统详细实现可以参考我们公司专利《网络靶场中基于配置代理的自动配置方法与系统》  3.1.4 每个内部管理网络交换机对应创建一个流量发生仪trex，该节点会同时接入当前的内部管理网络交换机和该内部管理网络交换机对应的内部业务网络交换机，负责对该内部业务网络交换机下所有接入的业务节点执行实际的流量发生业务。具体流量发生业务详细描述，可以参考我们公司的专利《一种网络靶场流量自动发生方法与系统》   * 1. 根据内部管理网络交换机接入的节点数量，创建内部核心路由器，同时将内部核心路由器与外部预先建立的SN核心路由器连接。   3.2.1 根据内部管理网络交换机接入节点数量创建出合理数量的内部核心路由器，来做靶场平台和内部管理网络交换机接入的虚拟代理直接的信令流量的负载均衡。现在默认固定每300台接入节点，分配一个内部核心路由器。具体算法如下：  3.2.1.1 当前有内部管理网络交换机a、b、c、d、e，接入它们的节点数量，分别为Na、Nb、Nc、Nd、Ne， 用Set(N)存放，当前节点总数计数标记为C，初始化值为0。每个内部管理网络交换机接入的内部核心路由器标记记录为Ia、Ib、Ic、Id、Ie， 使用Map<M,I>记录内部管理网络交换机和其对于内部核心路由器标记的映射关系，当前路由标记为R，初始化值为0。默认固定T台接入节点分配一个内部核心路由器。T默认值为300。  3.2.1.2 遍历Set(N)，对于其中的某一个元素的值Nx来说，做下面操作  3.2.1.3 如果Nx > T/2, Map<M,I>记录key=x, value=R。R = R + 1。  3.2.1.4 如果Nx < T/2, C = C + Nx, 如果C < T, Map<M,I>记录key=x, value=R。如果C > T，Map<M,I>记录key=x, value = R + 1。C = 0, R = R+1。  执行完以上算法，保证每个内部核心路由器所接入的内部管理网络路由器下面所有接入的业务节点总数不超过T，需要创建的内部核心路由器的数量为R，每个管理网络路由器对于需要接入的内部核心路由器关系可以查询Map<M,I>    3.2.2 内部核心路由器与SN核心路由器连接时，需要合理分配连接线路所占用的网段。  每一条内部核心路由器与SN核心路由器的连接线路所占用的网段的掩码都是30位。网段需要在所有拓扑实例之间不重复。即获取分配的网段之前，先需要获取一个靶场平台唯一的锁。且该网络网段前8位值默认位99。即网段值的范围为99.0.0.0/30 到99.0.0.252/30。即共有2的22次方4194304个子网可以选择。具体获取子网网段的算法类似于上面提到的步骤2。  3.2.2.1 Set<E> 记录当前靶场平台已经分配的连线子网值，例如{ 1, 2}。Lock<Set<E>>为靶场平台的子网网段分配锁Lock<P>, 所有的内部核心路由器与SN核心路由器连接线路的子网设置cidr时，需要先获取Lock<P>锁。  3.2.2.2调用Random函数，输入种子为当前时间，获取一个范围为[0,1]的浮点数n。  3.2.2.3当前网络子网值Vcidr为4194304乘于上一步获取的随机数n，再向下取整。  3.2.2.4等待获取Lock<P>锁  3.2.2.5检查Set<E>是否包含当前网络子网值Vcidr，如果包含，Vcidr = Vcidr + 1，直到Vcidr不存在于Set<E>中。例如，如果Vcidr第一次随机的值为1，1已经包含在Set<E>中了，则Vcidr = Vcidr + 1 = 2。2仍然包含在Set<E>中，Vcidr = Vcidr + 1 = 3。3没有在Set<E>中，则Vcidr = 3，可以执行下一步了。  3.2.2.6将Vcidr加入到Set<E>中后，释放Lock<P>锁  3.2.2.7当前连线的网段为“99.”+ IntToStr((Vcidr >> 14) & 0xFF) + “.” + IntToStr((Vcidr >> 6) & 0xFF) + “.” + IntToStr((Vcidr & 0xFC)<<2) + “/30”。即ipv4地址第一段固定为99，第二段的值为Vcidr向右偏移14位后和0xFF进行AND位运算，第三段的值为Vcidr向右偏移6位后和0xFF进行AND位运算，第四段的值为Vcidr先和0xFC进行AND位运算，然后向左偏移2位，掩码固定为30位。   * 1. 内部核心路由器和SN核心路由器连接的端口开启SNAT，虚拟配置采集代理节点和流量发生仪trex设置默认路由，网关位内部核心路由器和SN核心路由器连接的端口ip。虚拟配置采集代理节点和流量发生仪trex通过定期轮询、反向连接机制主动请求靶场平台获取用户管理操作生成的任务单。   经过上面3.1、3.2步骤，虚拟管理网络初步建立起来了。但是靶场平台是无法ping通拓扑实例中的虚拟配置采集代理节点以及流量发生仪trex。因为靶场平台是无法路由到拓扑实例内部的网络的。一个靶场平台会创建很多个拓扑实例，不同的拓扑实例内部的管理网络网段是会重复的。因此如果从靶场平台出发，给定一个虚拟配置采集代理节点的ip，是无法确认到达这个ip，是需要经过哪个内部核心路由器的。  因此拓扑实例内部的虚拟配置采集代理节点和流量发生仪trex节点需要采用反向连接的方式，才可以和外部的靶场平台进行通信。具体配置过程如下：  3.3.1 拓扑实例内部的核心路由器开启SNAT。和SN核心路由器连接的端口所在的网络为SNAT的外部网络。其它端口均为内部网络。  3.3.2 下面统一用内部代理节点一词来统一指代拓扑实例内部的虚拟配置采集代理节点和流量发生仪trex  3.3.2 每个内部代理节点设置默认路由，网关为其接入的内部管理网络交换机连接的内部核心路由器  3.3.3 内部代理节点都需要设置一个定时任务，每隔T时间，T默认为60s向靶场平台发送心跳，并携带其所属内部管理网络交换机的唯一id，mgmtNetworkId，以及自己的代理类型，分为CONFIG和FLOW。CONFIG代表虚拟配置采集代理，FLOW代表流量发生仪trex。  3.3.4 靶场平台收到拓扑实例内部代理节点的心跳请求，会获取到请求中携带的bizNetworkId，和代理类型。如果有用户在靶场平台上操作，给指定的靶场实例内部节点下发网络配置信息。例如给拓扑实例1中的虚机节点1，配置其端口g0/1 dns 为1.1.1.1，靶场平台会生成一个任务单，任务单字段设计如下：   |  |  |  |  | | --- | --- | --- | --- | | 字段名称 | 类型 | 含义 | 示例 | | node\_id | 字符串 | 节点id | 6e345adda9a44f338f8a9cde6957d38d | | node\_mgmt\_ip | Ip格式字符串 |  | 10.60,60.10 | | node\_access\_mgmt\_network\_id | 字符串 | 节点接入的内部管理网络交换机的唯一id | 8ce9abd0-cce1-4ad5-b657-6ca1f100f1b9 | | proxy\_type | 枚举，CONFIG或者FLOW | 管理操作实际执行的代理类型 | CONFIG | | proxy\_content | json格式字符串 | 管理操作执行的内容 | {  "access\_info": {  "protocol": "ssh",  "username": "root",  "password": "Xctfoj01"  },  "commands\_info": [  {  "command": "echo \"nameserver 1.1.1.1\" >> /etc/resolv.conf"  }  ]  } | | state | 枚举数字，0，1，2，3，默认为0 | 当前任务单状态。0代表初始化，1代表执行中，2代表成功，3代表失败 | 0 |   3.3.4.1 当靶场平台收到某一个拓扑实例内部代理节点的心跳请求时，会获取到请求中携带的mgmtNetworkId和代理类型。  3.3.4.2 然后靶场平台会查询生成的任务单。如果任务单的node\_access\_mgmt\_network\_id和proxy\_type和请求中的mgmtNetworkId、代理类型一致的话，且任务单的state状态为0的话，则将任务单作为响应体返回给对应的请求。同时将任务单的state设置为1  3.3.4.2 内部代理节点收到心跳请求的响应后，就可以开始实际执行任务单proxy\_content中描述的操作任务了。具体如何执行，请参考我们公司专利《网络靶场中基于配置代理的自动配置方法与系统》和《一种网络靶场流量自动发生方法与系统》。本专利只介绍如何构建虚拟管理网络下发信令流量。   * 1. 内部管理网络交换机设置ACL规则，只允许内部管理网络中的虚拟配置采集代理节点和流量发生仪trex和靶场平台通信。以下统一使用内部代理节点来指代虚拟配置采集代理节点和流量发生仪trex。具体规则设置如下：   3.4.1 拒绝掉所有ipv4协议和ipv6协议的流量包，优先级为1001  3.4.2 允许源ip和目的ip为内部代理节点接入管理网络交换机的端口ip的流量包，优先级为1002，比上一个优先级更大。  至此，我们就完成了虚拟管理网络的构建，以及针对当前虚拟管理网络构建的实现方式，拓扑实例内部的代理节点获取靶场平台管理操作的信令流量需要进行的反向连接方式的改造。 | |  | |
| **五、本发明或实用新型的关键改进点：**提炼出技术方案的关键改进点（即哪些改进点是重点想要保护的创新内容），列出1、2、3……以提醒代理人注意，便于代理人撰写权利要求书。 |
| 1. 设计了网络靶场中独立的内部虚拟管理网络，实现用于管理操作的信令流量和靶场拓扑实例中的业务节点直接的业务流量网络路由完全分开。保证了管理信令流量有独立网络路由，提高了管理操作的信令流量接收和响应的效率。避免因无法预测的业务流量影响靶场平台管理操作正常进行。 2. 内部虚拟管理网络中的虚拟配置采集代理节点和流量发生仪器trex采用定期轮询和反向连接机制获取靶场平台下发的管理操作信息，结合内部核心路由器的SNAT机制，避免内部管理网络直接连接到外部预创建的SN核心路由器，节约SN核心路由器需要连接的网络网段，减少SN核心路由器路由转发压力。提高管理操作的信令流量接收和响应的效率。 3. 根据内部业务管理网络数量创建对应内部虚拟管理网络，有效达到管理操作的信令流量负载均衡的目的。 |
| **六、本发明或实用新型取得的有益效果：**结合本发明创造，写明其与现有技术相比具有的优点：比如产率、质量、精度和效率的提高，能耗、原材料、工序的节省；加工、操作、控制、使用的简便等。注意要结合技术方案中的改进点说明，做到有理有据。 |
| 1. 设计了网络靶场中独立的内部虚拟管理网络，实现用于管理操作的信令流量和靶场拓扑实例中的业务节点直接的业务流量网络路由完全分开。保证了管理信令流量有独立网络路由，提高了管理操作的信令流量接收和响应的效率。避免因无法预测的业务流量影响靶场平台管理操作正常进行。 2. 内部虚拟管理网络中的虚拟配置采集代理节点和流量发生仪器trex采用定期轮询和反向连接机制获取靶场平台下发的管理操作信息，结合内部核心路由器的SNAT机制，避免内部管理网络直接连接到外部预创建的SN核心路由器，节约SN核心路由器需要连接的网络网段，减少SN核心路由器路由转发压力。提高管理操作的信令流量接收和响应的效率。 3. 根据内部业务管理网络数量创建对应内部虚拟管理网络，有效达到管理操作的信令流量负载均衡的目的。 |
| **七、本发明或实用新型的替代方案：**1、如有替代方案，请详尽写明，以提供足够多的具体实施方式，有助于使专利的保护范围更宽。2、替代方案可以是部分结构、器件、方法步骤的替代，也可以是完整技术方案的替代。 |
|  |

注意：

1.代理人并不是技术专家，交底书要使代理人能看懂，尤其是背景技术和详细技术方案，一定要写的全面、清楚。

2.英文缩写有中文译文，避免使用英文单词，最好在术语解释部分给出。

3.**全文对同一事物的叫法应统一，避免出现一种东西多种叫法。**

4.认为需要保密的地方可在交底书中注明，对代理人不必保密。

5.专利法规定：

1）专利必须是一个技术方案，应该阐述发明目的是通过什么技术方案来实现的，不能只有原理，也不能只做功能介绍；

2）专利必须充分公开，以本领域技术人员不需付出创造性劳动即可实现为准。