**专利申请信息表**

|  |  |
| --- | --- |
| **请您核实以下申请信息是否正确** | |
| **申　请　人** | 南京赛宁信息技术有限公司  统一社会信用代码：91320115080271299G |
| **发明名称** | 一种网络靶场中虚拟管理网络构建方法与系统 |
| **专利申请人**  **地址/邮编** | 南京市江宁区秣周东路12号 211100 |
| **发明人名单** | 詹志，谢峥，高庆官 |
| **第一发明人**  **身份证号** | 36250219990210463X |
| **联系人**  **联系方式** | 姓名：詹志  电话：13361875998  E-mail：1782865441@qq.com |
| **邮寄地址** | 南京市江宁区秣周东路12号2号楼16楼 |
| **费减类型** |  按85%比例享受费减  按70%比例享受费减 不享受费减 |
| **专利申请选项** |  提前公开  指定公开时间   申请时请求实质审查  申请时不请求实质审查  基于相同技术方案的发明与实用新型同日申请（同日申请的发明不得提加快审查）   请求实质审查时申请延迟审查（可选1年、2年、3年），选定后无法改变与撤销 |

本发明公开了一种网络靶场中虚拟管理网络构建方法与系统，本发明方法包括：创建外部管理网络交换机和外部核心路由器；创建拓扑实例内部业务网络交换机；创建拓扑实例内部管理网络交换机，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和一个流量发生器；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；内部核心路由器和外部核心路由器连接的端口开启SNAT，内部管理网络交换机设置ACL规则。本发明实现了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，提高了信令流量接收和响应的效率，实现了负载均衡。

指定图1为摘要附图

1. 一种网络靶场中虚拟管理网络构建方法，其特征在于，包括如下步骤：

创建外部管理网络交换机和外部核心路由器；靶场平台和所述外部核心路由器接入所述外部管理网络交换机，所述外部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；

创建拓扑实例内部业务网络交换机，每个业务网络交换机对应拓扑实例内部一个独立的业务子网；业务子网的网段从预设的范围内随机选取；

创建拓扑实例内部管理网络交换机，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用于管理操作的内部代理节点；所述内部代理节点包括虚拟配置采集代理节点和/或流量发生器；每个内部管理网络交换机的网段根据对应的内部业务网络交换机所在网段计算；每个拓扑实例中的虚拟业务节点创建时需要接入对应的内部业务网络交换机以及所述内部业务网络交换机对应的内部管理网络交换机；

根据所述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，将内部核心路由器与所述外部核心路由器连接；

所述内部核心路由器和所述外部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器设置默认路由，网关为内部核心路由器和外部核心路由器连接的端口IP；

所述内部管理网络交换机设置ACL规则，只允许内部代理节点和靶场平台通信。

2. 根据权利要求1所述的一种网络靶场中虚拟管理网络构建方法，其特征在于，一个业务子网获取网段的随机算法如下：

使用集合Set<E> 记录当前拓扑已经分配的子网值，Lock<Set<E>>为拓扑实例的业务子网分配锁；

根据随机函数获得的数值确定当前网络子网值Vcidr；

等待获取锁；

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；

将Vcidr加入到Set<E>中后，释放锁；

当前业务子网的网段为“A.”+ IntToStr((Vcidr >> 8) & 0xFF + 128) + “.” + IntToStr(Vcidr & 0xFF) + “.” + “0/24”；其中A为预设的固定值。

3. 根据权利要求2所述的一种网络靶场中虚拟管理网络构建方法，其特征在于，如果一个业务网络交换机对应的网段为A.b.c.0/24，那么其对应的内部管理网络交换机的网段为A.(b-128).c.0/24。

4. 根据权利要求1所述的一种网络靶场中虚拟管理网络构建方法，其特征在于，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的算法如下：

使用集合Set<N>存放接入各内部管理网络交换机的节点数量，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，当前内部核心路由器标记为R，初始化值为0，当前节点总数计数标记为C，初始化值为0，设固定T台接入节点分配一个内部核心路由器；

遍历Set<N>，对于其中的一个元素Nx，做如下判断：

如果Nx > T/2, Map<M,I>记录key=x, value=R；R = R + 1；

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。

5. 根据权利要求1所述的一种网络靶场中虚拟管理网络构建方法，其特征在于，将内部核心路由器与外部核心路由器连接时，根据如下算法分配连接线路所占用的网段：

使用集合Set<R> 记录当前靶场平台已经分配的连线子网值，Lock<Set<R>>为靶场平台的子网网段分配锁；

根据随机函数获得的数值确定当前网络子网值Vcidr；

等待获取锁；

检查Set<R>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<R>中；

将Vcidr加入到Set<R>中后，释放锁；

当前连线的网段为“B.”+ IntToStr((Vcidr >> 14) & 0xFF) + “.” + IntToStr((Vcidr >> 6) & 0xFF) + “.” + IntToStr((Vcidr & 0xFC)<<2) + “/30”；其中B为预设的固定值。

6. 根据权利要求1所述的一种网络靶场中虚拟管理网络构建方法，其特征在于，虚拟配置采集代理节点和流量发生器通过定期轮询和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，具体包括：

所述内部核心路由器开启SNAT，和外部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；

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；

内部代理节点都定时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以及自己的代理类型；

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ID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任务，靶场平台会生成一个任务单。

7. 根据权利要求6所述的一种网络靶场中虚拟管理网络构建方法，其特征在于，所述任务单字段包括节点ID，节点管理IP，节点接入的内部管理网络交换机的唯一ID，管理操作实际执行的代理类型，管理操作执行的内容以及任务单状态。

8. 一种网络靶场中虚拟管理网络构建系统，其特征在于，包括：

预创建模块，用于创建外部管理网络交换机和外部核心路由器；靶场平台和所述外部核心路由器接入所述外部管理网络交换机，所述外部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；

业务网络交换机创建模块，用于创建拓扑实例内部业务网络交换机，每个业务网络交换机对应拓扑实例内部一个独立的业务子网；业务子网的网段从预设的范围内随机选取；

内部管理网络交换机创建模块，用于创建拓扑实例内部管理网络交换机，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用于管理操作的内部代理节点；所述内部代理节点包括虚拟配置采集代理节点和/或流量发生器；每个内部管理网络交换机的网段根据对应的内部业务网络交换机所在网段计算；每个拓扑实例中的虚拟业务节点创建时需要接入对应的内部业务网络交换机以及所述内部业务网络交换机对应的内部管理网络交换机；

内部核心路由器创建模块，用于根据所述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，将内部核心路由器与所述外部核心路由器连接；

规则配置模块，用于所述内部核心路由器和所述外部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器设置默认路由，网关为内部核心路由器和外部核心路由器连接的端口IP；以及所述内部管理网络交换机设置ACL规则，只允许内部代理节点和靶场平台通信。

9. 一种计算机系统，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序/指令，其特征在于，所述计算机程序/指令被处理器执行时实现根据权利要求1-7任一项所述的一种网络靶场中虚拟管理网络构建方法的步骤。

10. 一种计算机程序产品，包括计算机程序/指令，其特征在于，所述计算机程序/指令被处理器执行时实现根据权利要求1-7任一项所述的一种网络靶场中虚拟管理网络构建方法的步骤。

**一种网络靶场中虚拟管理网络构建方法与系统**

**技术领域**

本发明涉及一种网络靶场中虚拟管理网络构建方法与系统，属于网络安全技术领域。

**背景技术**

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拟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拟机。现有网络靶场管理操作存在如下不足：

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。

**发明内容**

发明目的：针对上述现有技术存在的问题，本发明目的在于提供一种网络靶场中虚拟管理网络构建方法与系统，支持接入外部网络的靶场平台发送的用于管理操作的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，实现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，提高信令流量接收和响应的效率以及实现负载均衡。

技术方案：为实现上述发明目的，本发明采用如下技术方案：

一种网络靶场中虚拟管理网络构建方法，包括如下步骤：

创建外部管理网络交换机和外部核心路由器；靶场平台和所述外部核心路由器接入所述外部管理网络交换机，所述外部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；

创建拓扑实例内部业务网络交换机，每个业务网络交换机对应拓扑实例内部一个独立的业务子网；业务子网的网段从预设的范围内随机选取；

创建拓扑实例内部管理网络交换机，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用于管理操作的内部代理节点；所述内部代理节点包括虚拟配置采集代理节点和/或流量发生器；每个内部管理网络交换机的网段根据对应的内部业务网络交换机所在网段计算；每个拓扑实例中的虚拟业务节点创建时需要接入对应的内部业务网络交换机以及所述内部业务网络交换机对应的内部管理网络交换机；

根据所述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，将内部核心路由器与所述外部核心路由器连接；

所述内部核心路由器和所述外部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器设置默认路由，网关为内部核心路由器和外部核心路由器连接的端口IP；

所述内部管理网络交换机设置ACL规则，只允许内部代理节点和靶场平台通信。

作为优选，一个业务子网获取网段的随机算法如下：

使用集合Set<E> 记录当前拓扑已经分配的子网值，Lock<Set<E>>为拓扑实例的业务子网分配锁；

根据随机函数获得的数值确定当前网络子网值Vcidr；

等待获取锁；

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；

将Vcidr加入到Set<E>中后，释放锁；

当前业务子网的网段为“A.”+ IntToStr((Vcidr >> 8) & 0xFF + 128) + “.” + IntToStr(Vcidr & 0xFF) + “.” + “0/24”；其中A为预设的固定值。

作为优选，如果一个业务网络交换机对应的网段为A.b.c.0/24，那么其对应的内部管理网络交换机的网段为A.(b-128).c.0/24。

作为优选，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的算法如下：

使用集合Set<N>存放接入各内部管理网络交换机的节点数量，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，当前内部核心路由器标记为R，初始化值为0，当前节点总数计数标记为C，初始化值为0，设固定T台接入节点分配一个内部核心路由器；

遍历Set<N>，对于其中的一个元素Nx，做如下判断：

如果Nx > T/2, Map<M,I>记录key=x, value=R；R = R + 1；

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。

作为优选，将内部核心路由器与外部核心路由器连接时，根据如下算法分配连接线路所占用的网段：

使用集合Set<R> 记录当前靶场平台已经分配的连线子网值，Lock<Set<R>>为靶场平台的子网网段分配锁；

根据随机函数获得的数值确定当前网络子网值Vcidr；

等待获取锁；

检查Set<R>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<R>中；

将Vcidr加入到Set<R>中后，释放锁；

当前连线的网段为“B.”+ IntToStr((Vcidr >> 14) & 0xFF) + “.” + IntToStr((Vcidr >> 6) & 0xFF) + “.” + IntToStr((Vcidr & 0xFC)<<2) + “/30”；其中B为预设的固定值。

作为优选，虚拟配置采集代理节点和流量发生器通过定期轮询和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，具体包括：

所述内部核心路由器开启SNAT，和外部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；

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，所述内部代理节点指代虚拟配置采集代理节点和流量发生器；

内部代理节点都定时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以及自己的代理类型；

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ID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任务，靶场平台会生成一个任务单。

作为优选，所述任务单字段包括节点ID，节点管理IP，节点接入的内部管理网络交换机的唯一ID，管理操作实际执行的代理类型，管理操作执行的内容以及任务单状态。

一种网络靶场中虚拟管理网络构建系统，包括：

预创建模块，用于创建外部管理网络交换机和外部核心路由器；靶场平台和所述外部核心路由器接入所述外部管理网络交换机，所外部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；

业务网络交换机创建模块，用于创建拓扑实例内部业务网络交换机，每个业务网络交换机对应拓扑实例内部一个独立的业务子网；业务子网的网段从预设的范围内随机选取；

内部管理网络交换机创建模块，用于创建拓扑实例内部管理网络交换机，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用于管理操作的内部代理节点；所述内部代理节点包括虚拟配置采集代理节点和/或流量发生器；每个内部管理网络交换机的网段根据对应的内部业务网络交换机所在网段计算；每个拓扑实例中的虚拟业务节点创建时需要接入对应的内部业务网络交换机以及所述内部业务网络交换机对应的内部管理网络交换机；

内部核心路由器创建模块，用于根据所述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，将内部核心路由器与所述外部核心路由器连接；

规则配置模块，用于所述内部核心路由器和所述外部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器设置默认路由，网关为内部核心路由器和外部核心路由器连接的端口IP；以及所述内部管理网络交换机设置ACL规则，只允许内部代理节点和靶场平台通信。

一种计算机系统，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序/指令，所述计算机程序/指令被处理器执行时实现所述的一种网络靶场中虚拟管理网络构建方法的步骤。

一种计算机程序产品，包括计算机程序/指令，所述计算机程序/指令被处理器执行时实现所述的一种网络靶场中虚拟管理网络构建方法的步骤。

有益效果：与现有技术相比，本发明具有如下优点：

1. 本发明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. 本发明设计的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外部核心路由器，节约外部核心路由器需要连接的网络网段，减少外部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. 本发明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。

**附图说明**

图1为本发明实施例的方法流程图。

图2为本发明实施例中示意的一个拓扑实例构建结果图。

**具体实施方式**

下面将结合附图和具体实施例，对本发明的技术方案进行清楚、完整的描述。

如图1所示，本发明实施例公开的一种网络靶场中虚拟管理网络构建方法，主要包括如下步骤：首先，创建外部管理网络交换机和外部核心路由器，靶场平台和外部核心路由器接入外部管理网络交换机，外部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；接着，创建拓扑实例内部业务网络交换机，每个业务网络交换机对应拓扑实例内部一个独立的业务子网；业务子网的网段从预设的范围内随机选取；然后，构建拓扑实例内部管理网络，具体包括：

首先，创建拓扑实例内部管理网络交换机，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用于管理操作的内部代理节点；所述内部代理节点包括虚拟配置采集代理节点和/或流量发生器；每个内部管理网络交换机的网段根据对应的内部业务网络交换机所在网段计算；每个拓扑实例中的虚拟业务节点创建时需要接入对应的内部业务网络交换机以及所述内部业务网络交换机对应的内部管理网络交换机；

接着，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，将内部核心路由器与外部核心路由器连接；

然后，内部核心路由器和外部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器设置默认路由，网关为内部核心路由器和外部核心路由器连接的端口IP；

最后，内部管理网络交换机设置ACL规则，只允许内部代理节点和靶场平台通信。

本发明实施例所述的一种网络靶场中虚拟管理网络构建方法，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。

下面以图2所示的拓扑实例1为例，具体说明本发明方案的详细设计和实现。如图2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，能直接查看到的节点。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外部核心路由连接。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。

步骤1. 创建预定义的外部管理网络交换机和外部核心路由器。

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-外部管理网络交换机，部署靶场平台的虚拟机会固定接入外部管理网络交换机中。同时也会预先创建好一个外部核心路由器，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，外部管理网络交换机也会预先固定接入到外部核心路由器中。

步骤2. 创建拓扑实例内部业务网络交换机。

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：

步骤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。

步骤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。

步骤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。

步骤2.4等待获取Lock<Set<E>>锁。

步骤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。

步骤2.6将Vcidr加入到Set<E>中后，释放Lock<Set<E>>锁。

步骤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。

步骤3.构建拓扑实例内部管理网络。

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。

步骤3.1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。具体步骤如下：

步骤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第9位从1翻转到0，其它23位都保持一样，掩码也都是24位。

步骤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。

步骤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专利申请文件CN117857290A《网络靶场中基于配置代理的自动配置方法与系统》。

步骤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，可以参考专利文件CN117749639B《一种网络靶场流量自动发生方法与系统》。

步骤3.2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外部核心路由器连接。具体步骤如下：

步骤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：

步骤3.2.1.1 设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。

步骤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

步骤3.2.1.3 如果Nx > T/2, Map<M,I>记录key=x, value=R。R = R + 1。

步骤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>。

步骤3.2.2 内部核心路由器与外部核心路由器连接时，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外部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。

步骤3.2.2.1 Set<R> 记录当前靶场平台已经分配的连线子网值，例如{ 1, 2}。Lock<Set<R>>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外部核心路由器连接线路的子网设置cidr时，需要先获取Lock<P>锁。

步骤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。

步骤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。

步骤3.2.2.4等待获取Lock<P>锁。

步骤3.2.2.5检查Set<R>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<R>中。例如，如果Vcidr第一次随机的值为1，1已经包含在Set<R>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<R>中，则Vcidr = 3，可以执行下一步了。

步骤3.2.2.6将Vcidr加入到Set<R>中后，释放Lock<P>锁。

步骤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。

步骤3.3内部核心路由器和外部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，网关为内部核心路由器和外部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：

步骤3.3.1 拓扑实例内部的核心路由器开启SNAT。和外部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。

步骤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。

步骤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。

步骤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。

步骤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表：

表1：任务单字段

|  |  |  |  |
| --- | --- | --- | --- |
| 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 |

具体步骤如下：

步骤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。

步骤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。

步骤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《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》。本发明只介绍如何构建虚拟管理网络下发信令流量。

步骤3.4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：

步骤3.4.1 拒绝掉所有ipv4协议和ipv6协议的流量包，优先级为1001

步骤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。

基于相同的发明构思，本发明实施例公开的一种网络靶场中虚拟管理网络构建系统，包括：

预创建模块，用于创建外部管理网络交换机和外部核心路由器；靶场平台和所述外部核心路由器接入所述外部管理网络交换机，所述外部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；

业务网络交换机创建模块，用于创建拓扑实例内部业务网络交换机，每个业务网络交换机对应拓扑实例内部一个独立的业务子网；业务子网的网段从预设的范围内随机选取；

内部管理网络交换机创建模块，用于创建拓扑实例内部管理网络交换机，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用于管理操作的内部代理节点；所述内部代理节点包括虚拟配置采集代理节点和/或流量发生器；每个内部管理网络交换机的网段根据对应的内部业务网络交换机所在网段计算；每个拓扑实例中的虚拟业务节点创建时需要接入对应的内部业务网络交换机以及所述内部业务网络交换机对应的内部管理网络交换机；

内部核心路由器创建模块，用于根据所述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，将内部核心路由器与所述外部核心路由器连接；

规则配置模块，用于所述内部核心路由器和所述外部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器设置默认路由，网关为内部核心路由器和外部核心路由器连接的端口IP；以及所述内部管理网络交换机设置ACL规则，只允许内部代理节点和靶场平台通信。

基于相同的发明构思，本发明实施例公开的一种计算机系统，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序/指令，所述计算机程序/指令被处理器执行时实现所述的一种网络靶场中虚拟管理网络构建方法的步骤。

基于相同的发明构思，本发明实施例公开的一种计算机程序产品，包括计算机程序/指令，所述计算机程序/指令被处理器执行时实现所述的一种网络靶场中虚拟管理网络构建方法的步骤。



图1

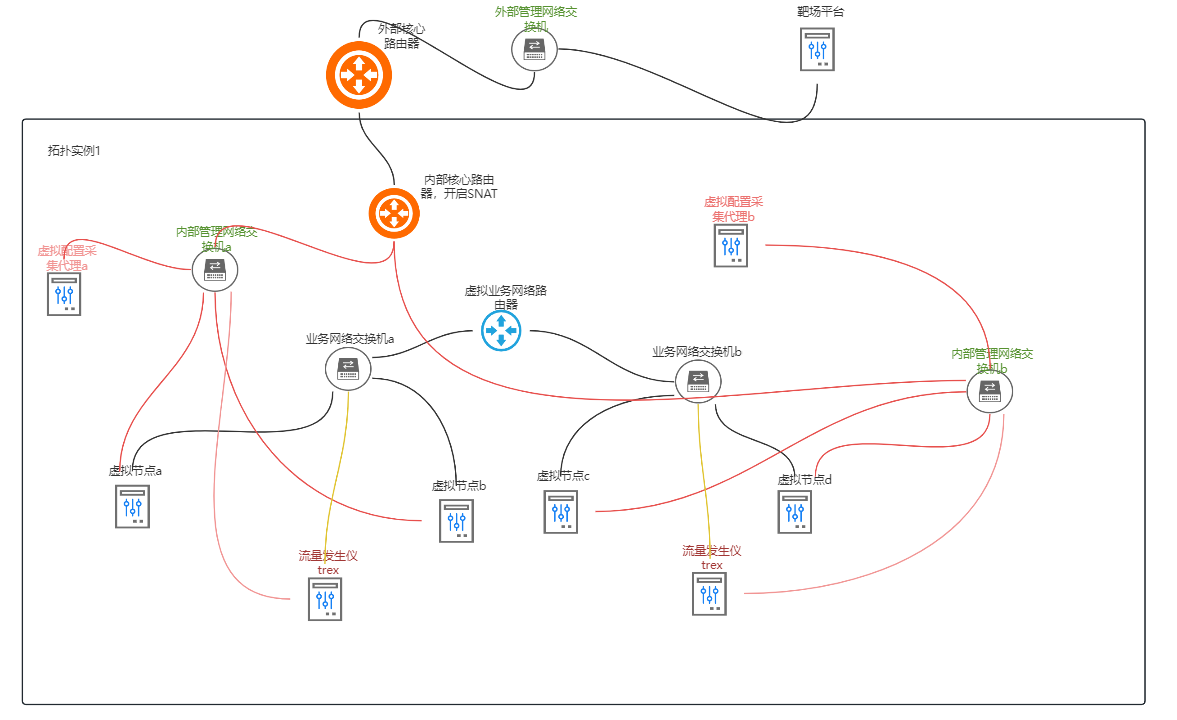


图2