虚拟化安全无代理 V7.0

最佳实践指南

虚拟化云安全 - 云安全专家组

修订日期 2019-03

目录

1 关于此手册

1.1 使用群体

该手册为半公开手册，涵盖了对不同场景的适用建议，避免发生不必要的问题，供公司内部规划实施人员使用。

请相关部门在规划部署虚拟化无代理产品方案之前参阅此文档以避免部署不当引起的不必要问题。

1.2 阅读前提

阅读者需要具备以下知识:

- 对于虚拟化安全产品的部署，方案有基本的了解。
- 对于常用的虚拟化环境运维任务的名词了解，如 HA, DRS, FT。
- 对于主流的虚拟化环境，云环境的基本了解。

1.3 环境检查

请确保安装部署环境，资源配置，步骤等均符合【安装部署手册】的要求。
对于无代理环境，确保各类平台兼容性符合要求:

- 对于 VMware NSX 环境，参照 VMtool 兼容矩阵及 vSphere NSX 兼容矩阵。
- 对于 HW Fusionsphere 的功能，特性，支持参照这里。
- 对于支持平台及功能列表，参照这里。

对于闭源平台，驱动不一定是默认安装在工具里，如 VMware,需确保驱动安装。

2 Sizing 考量

部署点数，以及资源消耗情况，根据不用的虚拟化平台会有差异，并且跟服务器角色，承载量有关。

2.1 ICS 管理中心

ICS 中控			
虚拟机数量	CPU数量	内存要求	硬盘要求
小于500	2	8	1T
500 - 1000	2	8	1T
1001 - 1500	4	12	1.5T
1501 - 2000	4	12	1.5T
2000 - 2500	8	16	2.5T
2500 - 3000	8	16	2.5T
大于 3000	基于性能承受能力，暂不支持3000以上的部署		

注意 无代理 **7.0.2.3366** 之前的版本最大数量只支持到 **1500**，对于超过 **1500** 虚拟机的部署，需要使用 **7.0.2.3366** 及以上版本；

如果需要硬盘扩容至 **2T** 以上，请使用 **7.0.2.3366** 版本，否则不支持扩容至 **2T** 以上。

2.2 安全虚拟机

NSVM			
单台主机上虚拟机数量	CPU数量	内存要求	硬盘要求
小于25	4	4	默认即可，无要求
25 - 50	4	8	默认即可，无要求
50 - 75	4	12	默认即可，无要求
75 - 100	8	16	默认即可，无要求
大于 100	基于性能承受能力，暂不支持100以上的部署		

建议合理规划计算节点下的虚拟机数量，最佳为 20 左右，量大的情况下需要按照上图增加资源配置。

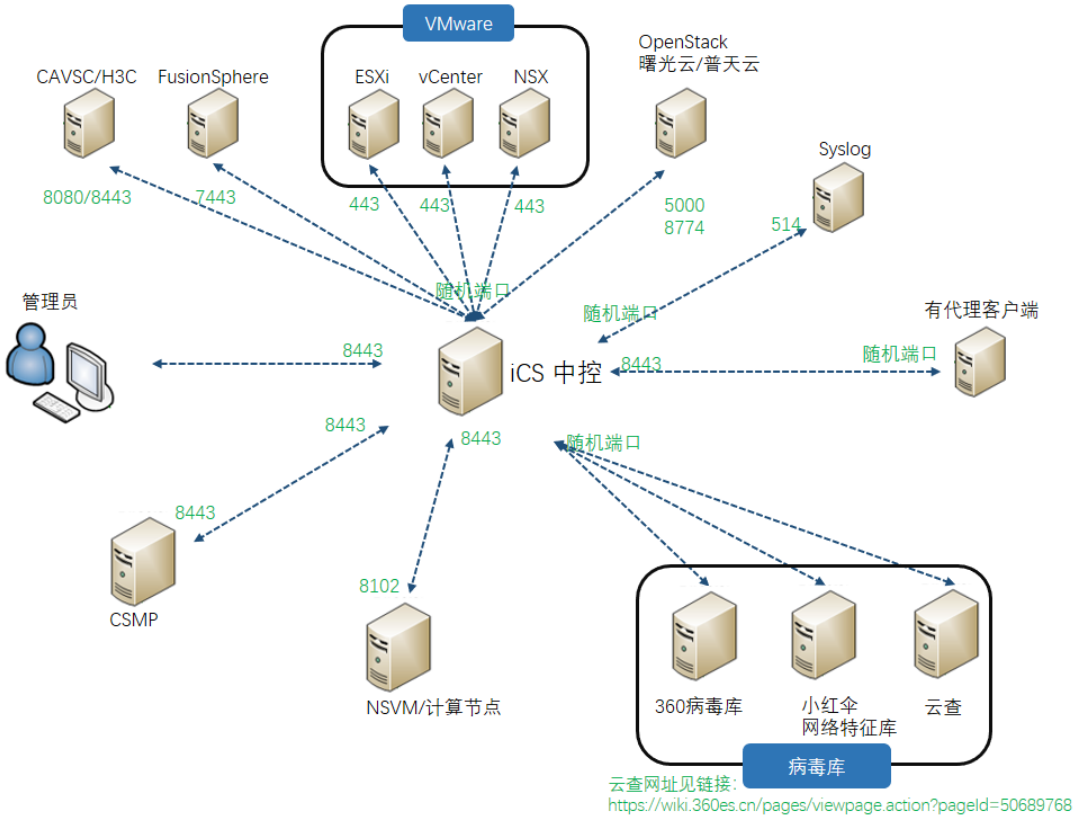
2.3 有代理客户端

- 未装客户端的情况下，如果资源（CPU/内存/硬盘使用量）使用量低于 80%，在安装客户端时不需要增加配置；
- 未装客户端的情况下，如果资源（CPU/内存/硬盘使用量）使用量高于 80%，在安装客户端时添加 1CPU/512M 内存/500M 硬盘；

3 安装与升级

3.1 安装建议

无代理产品各组件之间有连通性要求，请确保客户环境内对应的网络环境满足以下要求：



3.1.1 管理中心

对于控制中心的安装需要注意以下几点：

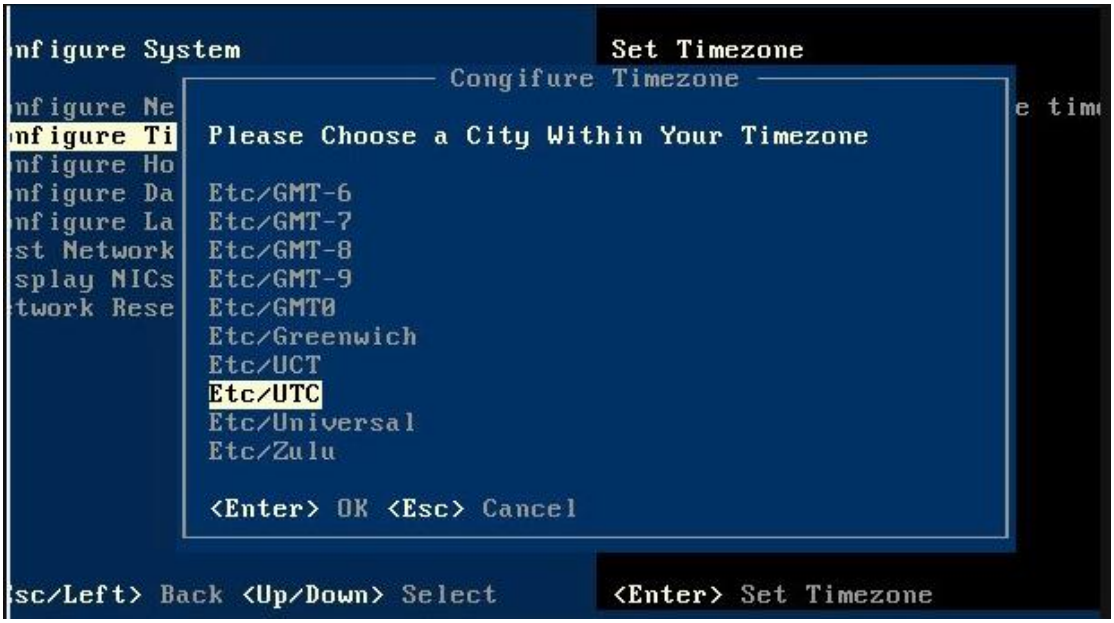
a. FQDN 和 IP 地址

由于管理中心不支持双向通讯，因此不要变更控制中心的 FQDN 或者 IP 地址。如果管理中心发生什么意外（比如被删除），用户可以重新安装管理中心，并依然指定之前的 IP 地址。所有之前的有代理端会自动注册到新的管理中心。不要更改系统后台时间。

b. 时间设定

1) 管理中心与各组件之间时间必须同步，管理中心比主机快 1 小时，或者慢 5 分钟，都会导致事件同步异常，建议统一使用 NTP 服务器管理时间。

2) 请勿修改控制台时区



如果访问无代理控制中心的浏览器所在操作系统的时区与无代理控制中心时区不一致，则在管理中心页面上会看到时间不一致。

c. 虚拟机设定

对于承载 ICS 管理中心的虚拟机，建议设定如下：

- 使用 vmxnet3 作为虚拟网卡类型
- 使用 Paravirtual SCSI 作为虚拟磁盘控制器
- 后置归零

3.1.2 安全虚机

a. 主机名

请不要修改安全虚拟机地主机名，另外连通性需要与 VMWare 或者华为相关组件畅通，参见【3.1 安装】。

b. 服务安装 （适用于 VMware）

在 NSX 中安装安全虚机时，需要确保该 NSX 未与其他安全虚机做过集成（如 DS），如果之前有集成，需要手动按照卸载步骤进行清理，否则再次集成会发生报错。

c. 安装包检查 （适用于 VMware）

在安装 NSX 环境时，VCenter 会去获取 NSVM 的 ovf 包，如果无法获取将直接导致无代部署安全虚机。
这种情况下需要确认安全虚机的 ovf 是否存在于:
/opt/nubosh/vmsec-ctrl/tomcat/webapps/ROOT/download/NSVM/

```
[root@localhost NSVM]# ll /opt/nubosh/vmsec-ctrl/tomcat/webapps/ROOT/download/NSVM/
total 1043480
-rw-r--r-- 1 vmsec vmsec 1068499456 Dec 21 18:05 NSVM-1568-disk1.vmdk
-rw-r--r-- 1 vmsec vmsec        133 Dec 21 18:05 NSVM-1568.mf
-rw-r--r-- 1 vmsec vmsec      11094 Dec 21 18:05 NSVM-1568.ovf
```

3.1.3 VMware

a. 兼容性检查

- 参照 VMtool 已知问题列表及兼容矩阵
- 参照 VMware 通告及 vSphere NSX 兼容矩阵

b. 时间设定

所有 VMware 组件均建议配置 NTP 服务器来同步时间。

c. 版本信息

- 对于 vmtool，参照推荐版本信息来进行版本安装
- 对于 NSX，建议使用 NSX 6.3 或更高版本

d. VCenter

- 当 VCenter 部署在 Windows 上，必须安装 Update Manager 组件
- 当 vCenter 文件放在高性能存储上时，vCenter 数据库的性能最佳

> 注意 虚拟化无代理支持添加多个 **vCenter,**但是基于性能考量，不建议添加超过两个 **Vcenter.**
> 另外多个 **vCenter** 里面的虚拟机 **UUID** 不能重复.

e. NSX 组件

- 安装 NSX 组件的主机要求必须满足下列条件

设备	内存	vCPU	磁盘空间
NSX Manager	16 GB（更大的 NSX 部署为 24 GB）	4（更大的 NSX 部署为 8）	60 GB
NSX Controller	4 GB	4	28 GB
NSX Edge	▪ 精简：512 MB ▪ 中型：1 GB ▪ 大型：2 GB ▪ 超大型：8 GB	▪ 精简：1 ▪ 中型：2 ▪ 大型：4 ▪ 超大型：6	▪ 精简、中型、大型：1 个磁盘 584 MB + 1 个磁盘 512 MB ▪ 超大型：1 个磁盘 584 MB + 1 个磁盘 2 GB + 1 个磁盘 256 MB
Guest Introspection	2 GB	2	5 GB（置备的空间为 6.26 GB）

- 另外，推荐使用 VDS (分布式交换机) 而非 VSS（标准交换机）

3.2 升级建议

3.2.1 管理中心

管理中心升级需要严格按照下列次序进行：

1. 管理中心升级：可以上传 iso 包进管理中心进行平滑升级（限 7.0 版本内）。
2. 安全组件升级：可直接上传升级包进行升级。
3. 有代理客户端升级：同安全组件步骤，也可客户端运行安装包覆盖升级。
4. 消息中心：安装时直接运行客户端（需要重启），默认只安装不升级。

3.2.2 vCNs 升级到 NSX

a) 在升级前注意点：

1. 升级 vCNs 到 NSX 之前，需要检查上行链路端口名称，详情参照这里
2. 迁移步骤参照官方指南 vCloud Networking and Security to NSX，详情参照这里
3. 如何判定当前版本是 vCNs 或者是 NSX，详情参照这里

b) 升级失败处理办法：

升级 NSX 失败后可以持回滚到 vCNs，步骤参照这里

4 配置建议

4.1 防恶意软件

首先请确保杀毒引擎，特征库升级到最新版本，配合小红伞，云查同步杀毒。

4.1.1 白名单规则

- 无代理目前不支持通配符设定黑白名单路径，所以在配置黑白名单的时候需要添加完整绝对路径。
- 配置黑白名单的长度有大小要求，总长度的文本大小不能超过 4096 字节。

白名单配置注意事项:
在基于后缀名的白名单中，请勿添加以下后缀名进白名单:

a. **执行文件类：**

.ini
.exe
.inf
.bat
.sql
.gdcb

b. **文档类：**

doc、docx、xls、xlsx、ppt、pptx、pst、msg、、vsd、vsdx、txt、csv、rtf、123、wks、wk1、pdf、dwg、onetoc2、snt、jpeg、jpg、docb、docm、dot、dotm、dotx、xlsm、xlsb、xlw、xlt、xlm、xlc、xltx、xltm、pptm、pot、pps、ppsm、ppsx、ppam、potx、potm、edb、hwp、602、sxi、sti、sldx、sldm、sldm、vdi、vmdk、vmx、gpg、aes、arc、paq、bz2、tbk、bak、tar、tgz、gz、7z、rar、zip、backup、iso、vcd、bmp、png、gif、raw、cgm、tif、tiff、nef、psd、ai、svg、djvu、m4u、m3u、mid、wma、flv、3g2、mkv、3gp、mp4、mov、avi、asf、mpeg、vob、mpg、wmv、fla、swf、wav、mp3、sh、class、jar、java、rb、asp、php、jsp、brd、sch、dch、dip、pl、vb、vbs、ps1、bat、cmd、js、asm、h、pas、cpp、c、cs、suo、sln、ibd、myi、myd、frm、odb、dbf、db、mdb、accdb、sql、sqlitedb、sqlite3、asc、lay6、lay、mml、sxm、otg、odg、uop、std、sxd、otp、odp、wb2、slk、dif、stc、sxc、ots、ods、3dm、max、3ds、uot、stw、sxw、ott、odt、pem、p12、csr、crt、key、pfx、der

常见的病毒（如驱动人生，永恒之蓝）会伪造或感染此类文件。

4.1.2 恶意软件处理

建议操作设置为“隔离”，对于 VMware 平台的虚拟机，恢复隔离区文件需要手动操作。

4.1.3 预设定扫描

预设定扫描建议分别分配不同的策略，打到对应的机器群，做到分批扫描，避免一次性扫描太多造成的管理中心卡顿问题，或者任务积压。

4.1.5 MD5 手动加黑白

NSVM 支持针对 MD5 进行手动加黑，具体步骤参照这里。

4.1.4 白名单建议

a. Windows update 白名单

pagefile.sys
NTUser.pol
registry.pol
${Windir}\Software Distribution\Datastore\DataStore.edb
${Windir}\Software Distribution\Datastore\Logs\Edb*.log
${Windir}\Software Distribution\Datastore\Logs\Res1.log
${Windir}\Software Distribution\Datastore\Logs\Res2.log
${Windir}\Software Distribution\Datastore\Logs\Edb.chk
${Windir}\Software Distribution\Datastore\Logs\tmp.edb
${Windir}\Software Distribution\Datastore\Logs\hiberfil.sys
${Windir}\Software Distribution\Datastore\Logs\pagefile.sys
${Windir}\Software Distribution\Datastore\Logs\Edbres00001.jrs
${Windir}\Software Distribution\Datastore\Logs\Edbres00002.jrs
${Windir}\Security*.edb
${Windir}\Security*.sdb
${Windir}\Security*.log
${Windir}\Security*.chk

b. Windows Update 白名单 – 目录:

${allusersprofile}\
${Windir}\system32\GroupPolicy\
${Windir}\Cluster\

c. Windows Update 白名单 – 后缀:

*.pst

d. Windows Domain Controllers – **文件：**

TEMP.edb
EDB.chk

e. Windows Domain Controllers – **目录：**

${Windir}\SYSVOL\
${Windir}\NTDS\
${Windir}\ntfrs\
${Windir}\system32\dhcp\
${Windir}\system32\dns\

f. SQL 服务器 – 目录

${ProgramFiles}\Microsoft SQL Server\MSSQL\Data\
${Windir}\WINNT\Cluster\

g. SQL 服务器 – 文件

ldf
mdf

h. 文件服务器

文件服务器对于文件访问的速度，性能很严格，建议配置在整体隔离区外部。

> 注意 🗎 这里给出的建议是基于特殊的服务器角色，对于通用的建议请参照各厂商的具体列表：
> 微软产品 - 参照微软所有产品白名单合集
> 思杰产品 - 参照思杰白名单
> **Linux OS** – 参照 **Linux** 白名单合集

4.1 进程监控

对于信任的进程，可以直接加到信任区，但注意不要把常见的病毒的伪装体加到进程信任区（比如 svchost.exe）。
此处列出一些必须要加入“进程监控”–“阻止”的路径：

a. **驱动人生类派生进程：**

C:\Windows\SysWOW64\svhost.exe
C:\Windows\SysWOW64\svvhost.exe
C:\Windows\SysWOW64\svhhost.exe
C:\Windows\System32\svhost.exe
C:\Windows\System32\svvhost.exe
C:\Windows\System32\svhhost.exe
C:\Windows\System32\wmassrv.dll
C:\vuksntaf.exe

b. **永恒之蓝类派生进程：**

C:WINDOWStasksche.exe
c:\windows\mssecsvc.exe
c:\windows\qeriuwjhrf
c:\windows\tasksche.exe
c:\windows\Taskdl.exe

> 注意 🗎 由于上述病毒变种非常快，此处仅给出基本参考，后续请关注安全实时动态添加新的路径

4.2 防火墙

防火墙的配置需要小心谨慎，对于以下场景建议配置“强制允许”：

- FW 功能出现误报的情况下，可以使用该功能解决误报；
- 对于管理中心管大批量客户端，管理服务器性能无卡扩容然后遇到 CPU 过高响应变慢的情况下，可以使用该功能提升管理中心性能；
- 对于专用网络，比如内部专门用于做 failover 的网卡，可以使用该功能提升客户端性能。

另外对于常见的易被入侵的端口，必需设定拦截规则

- 驱动人生/永恒之蓝/ GandCrab：3389 445[(i)] 135 137 138 139
- 扩展行为（挖矿等）：4040 5555 8220 8088 8090 10255 10250

i: 445 端口一般用于共享文件及共享打印机，封死会影响客户共享服务，需要根据客户情况自己决断。

4.3 入侵检测

- 基于性能考量，对于单台机器的 IPS 规则设定，建议不超过 600 条；
- 对于漏洞扫描出来的规则，请按照“普通”与“严重”进行排序；
- 优先打上严重的 CVE 规则，然后打上普通的规则。

另外对于常见的易被入侵的漏洞，需要打上 IPS 规则：

a. **GandCrab：**

CVE-2017-8570

b. **永恒之蓝 (驱动人生同此)：**

Windows: CVE-2017-0146 CVE-2017-0148

Linux: CVE-2017-7494

> 注意 🗎 对于一些需要本地操作配合的漏洞，入侵检测无法检测。

5 NSX 防火墙与安全组

5.1 NSX 防火墙

在 NSX 里可以创建 NSX 防火墙规则，在将流量重定向 360 安全虚拟（NSVM）前，通过分布式防火墙功能经行第一次过滤。
在使用 NSX 防火墙时有以下注意点：

- VMWare NSX 分布式防火墙（DFW）旨在直接在 VM vNIC 层实施防火墙，该层用于过滤 SDDC 环境中的东西向流量。
- 在大多数情况下，VMWare NSX Edge Firewall 负责处理正在数据中心内移动的南北向流量。
- 虚拟化无代理安全虚拟机是部署在 NSX 上的一个服务，它提供的防火墙和入侵检测功能是定义在 NSX 的安全策略里，该层在 NSX 防火墙规则层之后进行过滤。

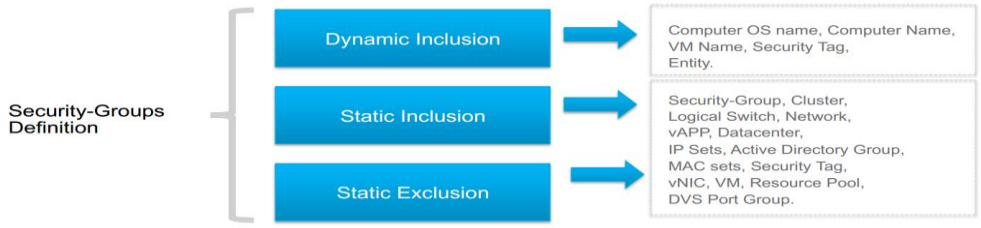
> 注意 **NSX 防火墙的第一层过滤因为是优先于无代理防火墙，因此配置规则需避让无代理安全流量（允许/强制允许）。**

5.1 NSX 安全策略

通常，VMWare 建议使用各种对象分组模型来创建 NSX 安全策略：
- 基于网络的策略：这是基于 L2 或 L3 进行分组的传统方法。

分组可以基于 MAC 地址，IP 地址或两者的组合。
但在动态环境中的不推荐此方法，例如云自动部署，其中 VM 和应用程序拓扑快速更改。
- 基于基础结构的策略：分组基于 SDDC 基础结构，如 vCenter 群集，逻辑交换机和分布式端口组。如果环境里没有物理或逻辑边界，VMWare 建议不要采用此方法。
- 基于应用程序的策略：在此方法中，分组基于应用程序类型。

可以使用多个包含和排除定义 NSX 安全组，如下图所示：



6 其他部署场景

> 注意 下列场景均为无代理模式下的有代理安装。
>
> 支持的平台同无代理模式中有代理 OS 支持列表。

6.1 微软集群服务

群集服务器涉及底层操作系统的两个单独安装，其中共享资源（数据库，磁盘，IP 地址）在群集执行故障转移时来回交换。

如果将虚拟化无代理产品配置为保护群集中的一个节点，请考虑以下事项：

- 将虚拟化无代理所有产品安装到本地磁盘，而不是共享磁盘。
- 对于该环境里的内部封闭环境（如专用网卡，failover 网卡等），不建议打防火墙及入侵检测规则。
- 目前，在 ESXi 5.5 计算机中激活和停用 Microsoft 群集或 SQL 群集时使用无代理保护，在启停安全虚机时有可能会触发集群 failover。

6.2 Hyper-V 环境

在 Hyper-V 环境种部署虚拟化无代理安全产品时，需要考量以下几点：

- 使用无代理防护为每个客户单独配置反恶意软件，IPS 和防火墙策略。
- 在仅有 core 的服务器级别，由于缺少必要组件，不支持安装管理中心镜像。
- 在开启了 Hyper-V 种的”Secure boot”的虚机中，杀毒功能不可用，如果需要杀毒功能，需要禁用”Secure boot”功能。

6.3 敏感集群

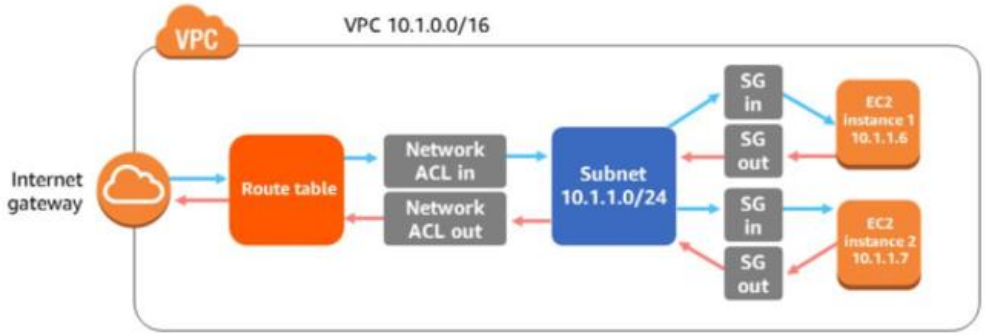
对于 Oracle cluster，该集群为高性能集群，启用防火墙或者入侵检测极度容易引起网络性能问题，请谨慎使用，添加规则遵循：“慢速度加规则”，“快速度减规则”。

6.4 AWS 云平台

对于 AWS 环境里的机器，虚拟化安全无代理只支持有代理模式部署。

在 AWS 上的部署有代理客户端，需要注意以下几点：

1. MTU 的设定，超过 1500 的话将会引起网络通讯异常，客户端无法心跳到管理中心进行同步；
2. AWS 上有多重访问控制功能，如图：



因此在确保通讯能够成功建立的条件下需要注意：

1. 在虚拟机（EC2）级别的安全组（SG），默认拒绝所有流量，需要手动加上允许规则来允许管理中心的网络和端口。
2. 在子网（Subnet）级别有网络 ACL，需要添加对应的管理中心允许规则。
3. 在服务层面，AWS 身份识别与访问控制服务（IAM）里可能会有配置对应的权限控制，需要与客户管理员确认。

> 注意 阿里云注意点同 **AWS** 云。

6.5 Azure 云平台

在使用 Azure 自身的防火墙（FW）或者应用防火墙（WAF）时，请注意规则不要与虚拟化无代理防火墙规则冲突，比如对于同样的五元组做相同的动作的行为将会引发网络性能问题甚至网络瘫痪。