Neusoft

东软云安全系统 V1.0

用户使用指南

2019 年 9 月

联系信息

网站：http://www.neusoft.com

电子信箱：servicedesk@neusoft.com

服务电话：400 655 6789

目录

前言

本手册介绍东软云安全系统（Neusoft Cloud Security System，简称 NCSS）的功能及其操作方法，旨在帮助管理员了解 NCSS 的各项功能并根据实际需求正确配置 NCSS。

本手册由以下章节构成：

- 第 1 章，NCSS 概述，介绍 NCSS 的部署要求、部署场景以及 WebUI 整体布局和主页信息。
- 第 2 章，系统管理，介绍如何设置 NCSS 系统和 DHCP 服务器信息、更新 NCSS 和虚拟防火墙系统、管理 License 以及如何查看版权信息。
- 第 3 章，虚机中心，介绍如何为数据中心的网络、ESXi 主机和虚拟机部署虚拟防火墙以保护资源安全。
- 第 4 章，网络，介绍被保护虚拟机所属的虚拟交换机和安全域的相关信息。
- 第 5 章，策略，介绍如何配置访问策略、DoS 攻击防御策略、应用安全和控制策略以及防病毒策略。
- 第 6 章，监控，介绍如何监控虚拟防火墙的运行状态和流量情况。
- 第 7 章，报警，介绍如何为被管理虚拟防火墙配置报警功能。
- 第 8 章，日志，介绍如何查看和删除 NCSS 日志以及虚拟防火墙的日志信息。
- 第 9 章，报表，介绍如何添加报表生成计划以及查看报表文件。
- 第 10 章，任务管理，介绍如何查看当前系统操作任务。

第1章 NCSS 概述

NCSS 是用于保护 VMware vSphere 私有云环境数据中心资源的安全防护产品。NCSS 由两部分组成：

- vSMC：虚拟安全管理模块（virtual Security Management Center），以虚拟机的形式部署在 VMware vSphere 中，用于部署和管理 vSPM 安全防护模块。
- vSPM：虚拟安全防护模块（virtual Security Protection Module），即分布式虚拟
- 防火墙（以下简称虚拟防火墙），可以通过 vSMC 自动部署，为受保护的虚拟机提供微隔离和安全防护。

通过先进的引流技术以及虚拟机微隔离技术，NCSS 能够将进出虚拟机的所有流量都牵引到虚拟防火墙，以使虚拟防火墙对流量进行过滤与控制，从而能够防范内部和外部的网络攻击。因此，可以为用户的私有云资源提供有效的安全防护。此外，NCSS 提供可视化的监控功能，帮助管理员了解系统和被管理虚拟防火墙的运行状态及安全状态，以便采取进一步的安全措施。

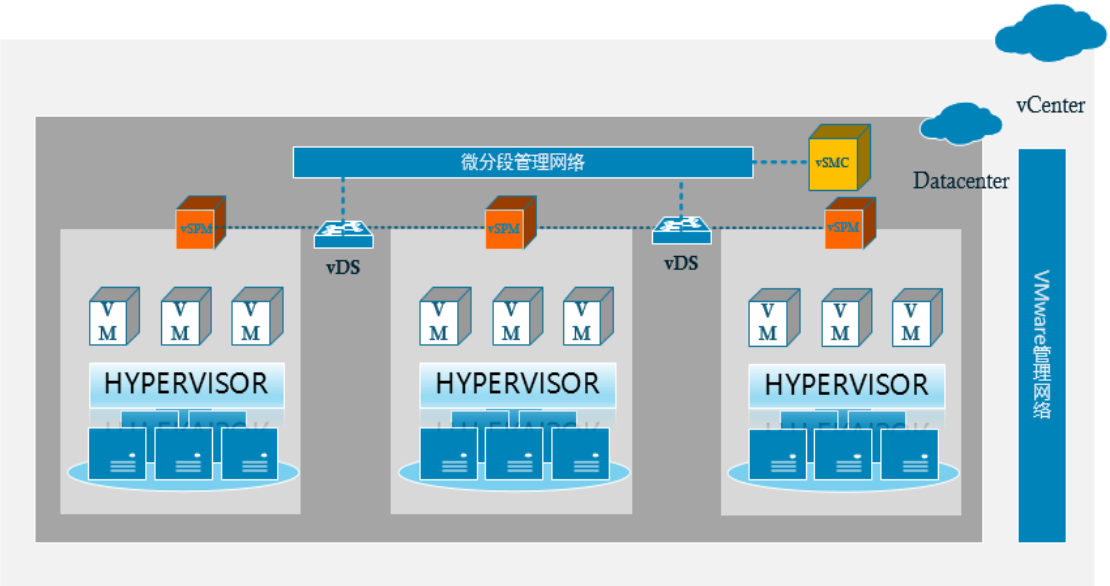
在 NCSS 上，管理员可以为数据中心的网络、主机和虚拟机部署虚拟防火墙，向虚拟防火墙统一下发安全防护策略，并对虚拟防火墙进行统一监控和管理。

本章包含以下内容：

提示：NCSS可以部署在VMware vSphere 5.1、5.5、6.X 等版本的环境中。部署vSMC虚拟机时，系统最低配置要求为2个vCPU、4G 内存和20G 硬盘。

1.1.NCSS 部署场景

下图为 NCSS 的部署场景：



用户网络为一个 VMware vSphere 数据中心，通过 vCenter 对 ESXi 主机进行管理。为了全方位防护内网虚拟机的安全，需要在 VMware 管理网络中部署一台 vSMC 虚拟机，通过 vSMC 为指定的 ESXi 主机按需部署 vSPM 分布式虚拟防火墙，为指定虚拟机或网络启用安全防护。

部署方式如下：

1. 创建 vSMC 虚拟机，并为 vSMC 虚拟机配置管理接口 IP，用于管理 NCSS。

   提示：也可以在VMware vSphere数据中心外部搭建vSMC主机，但是必须与VMware管理网络和微分段管理网络互通。

2. 登录 NCSS 管理界面：

   a) 添加 vCenter 服务器地址（即添加要保护的数据中心网络）。

   b) 配置 DHCP 服务器接口，设置接口 IP 地址，指定 vSMC 要为 vSPM 自动分配的 IP 地址范围。

   c) 选择管理网络和内部业务网络。

   d) 为指定的 ESXi 主机部署 vSPM 分布式虚拟防火墙。

   e) 为指定的虚拟机开启 vSPM 防护，或为指定网络中的虚拟机批量开启安全防护。

提示：一个vCenter可以管理多个数据中心。但是，一套NCSS系统只能保护一个数据中心，所以要基于数据中心部署分布式虚拟交换机和vSMC虚拟机。

1.2.登录

在产品部署完成之后，可通过浏览器登录并进行相关配置。

1. 使用浏览器访问 vSMC 的管理接口 IP 地址。
2. 点击**继续浏览此网站（不推荐）**，信任产品使用的证书。

3. 输入缺省用户名 admin 和密码 neteye，并选择语言。

提示：如果连续使用错误密码登录达三次，则当前访问者的IP地址会被锁定20分钟。建议您使用缺省密码进行初次登录后，对此密码进行更改。

1.3.WebUI 布局和主页信息

登录 NCSS 后，可以查看 NCSS Web 用户界面（WebUI）的整体布局和主页信息。

WebUI 的快捷按钮包括：

- ：点击查看最近报警。
- ：点击查看系统当前操作任务。
- ：点击修改密码。密码长度为 6～127 字节，任意 UTF-8 字符串（空格和问号除外）。
- ：点击退出 NCSS 系统。

主页直观展示 NCSS 管理的虚拟防火墙状态和流量信息：

- 防火墙情况

  防火墙情况区域自动显示已部署的虚拟防火墙的信息。在**查看方式**下拉框中，可以选择拓扑图或平铺图的方式查看虚拟防火墙概况。

  虚拟防火墙状态分为：在线（ ）、在线且报警（ ）、未授权（ ）和离线（ ）。点击一个在线虚拟防火墙，可以查看其基本信息和报警信息。

  点击 更新虚拟防火墙信息。系统自动刷新功能缺省是关闭的，可以选择系统自动刷新的时间间隔。

- 应用/IP 排行

可以在**选择防火墙**下拉框中选择一个、多个或全部虚拟防火墙，在**排行**下拉框中选择 3、5、10，系统自动显示产生流量最多的 Top 3/5/10 IP 地址或应用。点击 更新数据信息。自动刷新时间间隔缺省为 1 分钟，可以根据需要选择其他时间间隔或关闭自动刷新功能。

第2章 系统管理

本章介绍 NCSS 系统的配置和维护，包括以下内容：

2.1.管理员

管理员可以对 NCSS 系统进行管理。NCSS 系统支持以下类型的管理员：

根管理员

用于创建、修改和删除超级管理员、审计管理员和配置管理员，配置 NCSS 系统和 DHCP 服务信息，查看、上传和下载 License 以及查看版权信息。NCSS 系统仅有一个根管理员（用户名 root，密码 neteye）。

超级管理员

超级管理员可以使用 NCSS 系统内的所有功能。系统缺省提供一个超级管理员（用户名 admin，密码 neteye），不可删除。

审计管理员

仅可以查看系统、报警、监控和日志信息。

配置管理员

仅可以配置 NCSS 系统的功能，不能查看报警、监控和日志信息。

2.1.1. 添加管理员

1. 以根管理员身份登录到 NCSS，选择**系统管理>管理员**。
2. 点击**添加**添加管理员。

- **名称**：管理员的登录名称，不可修改。名称不可重复。名称为 1～63 字节，由字母、数字和下列字符组成：_-.@
- **描述**：管理员的描述信息。0～255 字节，UTF-8 字符。不能包括以下字符：？”’ \<>&
- **密码/确认密码**：管理员的登录密码。6～127 字节，UTF-8 字符，不能包括空格和问号。

- 用户类型：包括管理员（即超级管理员）、审计管理员和配置管理员。

3. 点击**确定**。

2.1.2. 编辑/删除管理员

1. 以根管理员身份登录到 NCSS，选择**系统管理>管理员**。

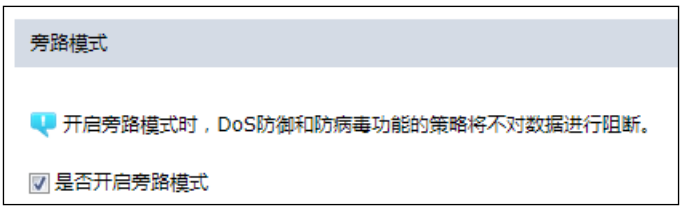
2. 在**管理员**列表中：

- 双击某个条目，对管理员信息进行编辑。
- 勾选**名称**左侧的复选框选中所有管理员（admin 除外），或者勾选条目对应的复选框选中一个或多个条目，点击**删除**。在弹出的对话框中点击**确定**，删除管理员。

2.2.系统设置

系统相关配置步骤为如下：

1. 选择**系统管理>系统设置。**
2. 配置是否开启旁路模式。

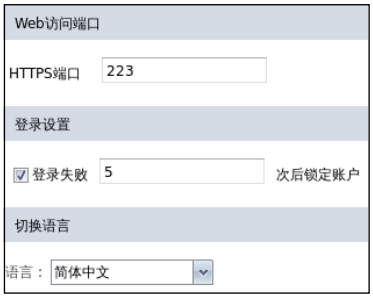


系统部署模式分为旁路模式和在线模式。缺省情况下，系统为旁路模式部署。两种模式对功能策略缺省配置的具体影响请见**错误!未找到引用源。**。

表 1——旁路模式与在线模式缺省策略差异

策略	**旁路模式**	**在线模式**
访问策略	开启日志记录功能。	关闭日志记录功能。
DoS 防御	报警，但不阻断数据。	报警且阻断数据。
应用安全	开启日志记录功能。	关闭日志记录功能。
应用控制	开启日志记录功能。	关闭日志记录功能。
防病毒	发现病毒后不对文件进行阻断。	发现病毒后对文件进行阻断。

3. 配置 Web 访问端口、登录失败次数限制和系统语言。



- **HTTPS 端口：**通过 HTTPS 连接的方式进行管理，即通过 HTTPS 端口登录 NCSS。端口取值范围为 1～65535，默认端口是 443。

- **登录失败次数**：可对登录失败次数进行设置。取值范围为 1～10，默认值为 3。多次登录失败锁定访问者 IP 地址的功能默认为启用。如果连续登录 NCSS 失败的次数达到最大值，该访问者的 IP 地址在后续 20 分钟内会被系统锁定。

登录系统后，如果 30 分钟内没有任何操作，管理员将因为超时而退出，需要重新登录才可以进入系统。

- **语言**：NCSS 提供简体中文和英文两种系统语言，默认为简体中文。

4. 配置 SMTP 报警服务器信息。

此处可以配置发件人和邮件服务器等信息。NCSS 可以通过邮件为用户发送报警信息和报表文件。

- **服务器地址**：SMTP 服务器的地址。可以是域名或 IP 地址。
- **端口**：SMTP 服务器的端口号，取值范围为 1～65535。
- **SSL 安全连接**：用于启用或禁用 SSL 加密。
- **发件人地址**：发件人邮箱地址。
- **身份认证**：设置是否启用身份认证。
- **用户名**：发件人邮件的用户名。
- **密码**：发件人邮件的密码。

2.3.DHCP 服务器设置

管理员可以在 NCSS 上开启 DHCP 服务。完成 DHCP 配置后，系统可以自动为被管理的虚拟防火墙分配 IP 地址。

提示：如果使用非DHCP方式部署虚拟防火墙，请关闭DHCP服务，以免引起网络问题。

配置步骤为如下：

1. 选择**系统管理>DHCP 服务**。
2. 点击**开启**，启用 DHCP 服务并设置 DHCP 服务器信息。

- **DHCP 操作**：开启或关闭 DHCP 服务。
- **接口**：NCSS 提供 DHCP 服务的接口。
- **IP 地址**：DHCP 服务接口的 IP 地址。
- **租期**：IP 地址租期时间。时间范围为 1～1440000 分钟。
- **开始 IPv4 地址**：待分配 IP 地址段的起始 IPv4 地址。
- **结束 IPv4 地址**：待分配 IP 地址段的结束 IPv4 地址。
- **掩码**：待分配 IP 地址段的掩码。

3. 点击**确定**。

提示：DHCP配置确定后不可编辑，需点击解锁按钮后才可修改配置。

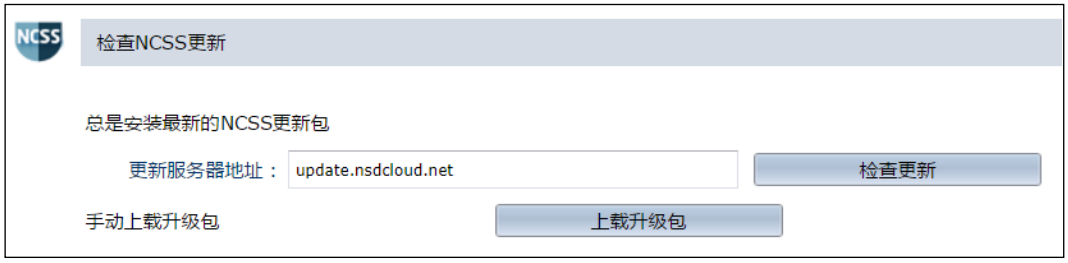
2.4.更新设置

管理员可以对 NCSS 系统以及虚拟防火墙进行升级。配置步骤为如下：

1. 选择**系统管理>更新设置**。
2. 在**检查 NCSS 更新**区域，进行如下设置：
   - 填写更新服务器的 URL 地址，点击**检查更新**进行在线更新。

如果有可用更新，NCSS 在下载更新包之后，页面会自动退出到登录页面，正在进行但未完成的任务将被终止，之后 NCSS 系统将进行更新操作。NCSS 不提供升级回退机制，所有更新立即生效。

- 点击**上载升级包**，上载本地升级包文件以完成更新。



3. 在**检查防火墙更新**区域，可以通过以下两种方式对虚拟防火墙系统、IPS 攻击签名规则、防病毒规则进行更新；应用知识库规则更新仅支持手动上载升级包的更新方式。
   - 通过 Internet 自动更新
     - 更新类型：包括系统、IPS 更新、防病毒更新、应用控制。
     - **更新服务器地址**：填写升级服务器的 URL 地址，点击**立即更新**进行在线更新。
     - **更新模式**：选择升级的模式，包括**自动安装更新**和**从不检测更新**。当模式为自动安装更新时，可以设置升级时间周期。
   - **手动上载升级包**：点击**上载升级包**，上载本地升级包文件以完成更新。

4. 点击**确定**。

2.5.License

NCSS 的 License 用于控制 NCSS 可防护的 ESXi 主机的 CPU 数量。可在 **ESXi 主机>配置>已获许可的功能**中查看各主机 CPU 的数量，并据此申请 NCSS 的 License。

管理员可以上载和下载 License，配置步骤如下所示：

1. 选择**系统管理>License**。
2. 在 **License** 页面中，查看 License 信息。

- 点击**下载**将 License 保存到本地。
- 点击**上传**，在弹出的**上传**对话框中选择要上传的 License 所在的路径。License 上传成功后，可保护 CPU 数量自动更新。

NCSS License 信息：

- **序列号**：NCSS 的序列号。
- **状态**：License 的状态，分为有效和无效两种状态。
- **发行商**：License 发行商。
- **有效期**：指 License 最后生效的日期，格式为 YYYY-MM-DD。如果无限制使用，则在此处指定为“永远”（perpetual）。例如，有效期 2018-01-01，其含义为 License 从 2018 年 1 月 2 日 00:00:00 起失效（此限制允许误差范围：±1 小时）。失效时间以 NCSS 所在系统时间为准。
- **CPU 数量**：允许 NCSS 保护的最大物理 CPU 数量。

vSPM 虚拟防火墙 License 信息：

- **规则**：虚拟防火墙支持的规则总数。
- **会话**：虚拟防火墙支持的会话总数。
- **IPS 更新有效期**：IPS 规则更新的最后期限。
- **防病毒更新有效期**：病毒库更新的最后期限。
- **应用更新有效期**：应用规则更新的最后期限。

2.6.版权信息

可以查看 NCSS 使用开源组织源码所遵循的开源组织协议及开源组织的专有版权信息。

选择**系统管理>版权信息**，进入**版权信息**页面查看版权信息。

第3章 虚机中心

NCSS 能够自动探测并获取其所在数据中心内的资源信息，包括虚拟网络、主机和虚拟机的信息。本章介绍如何为数据中心资源部署虚拟防火墙安全防护以及查看数据中心网络的拓扑视图，章节内容如下所示：

在 NCSS 上，请根据以下配置顺序为数据中心的资源部署虚拟防火墙防护：

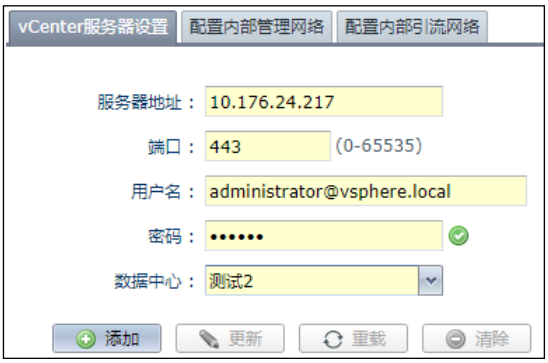
1. **选择虚机中心>全局配置**，选取需保护的数据中心。
2. 选择**系统管理>DHCP 服务**，配置 DHCP 服务。
3. **选择虚机中心>主机**，为 ESXi 主机部署虚拟防火墙。
4. **选择虚机中心>虚拟机或虚机中心>虚拟网络**，为 ESXi 主机中的虚拟机或虚拟网络添加虚拟防火墙保护功能。

3.1.全局配置

管理员需在此处设置 vCenter 服务器的信息，选取需要防护的数据中心，并对 NCSS 所使用的网络进行配置。

- **添加 vCenter 服务器**

1. 选择**虚机中心>全局配置**。
2. 在 **vCenter 服务器设置**页签中添加 vCenter 服务器并设置相应的信息。



- 服务器地址：vCenter 服务器的 IP 地址。
- 端口：vCenter 服务器的端口号。
- 用户名：vCenter 服务器的用户名。
- 密码：vCenter 服务器的密码。
- 数据中心：选取需要保护的数据中心。只有在填完用户名和密码且验证通过后，数据中心栏才会显示选项。当用户名和密码填写完成后，光标移开密码区域，系统自动开始认证，认证成功后，密码栏后方会出现 。

3. 点击**添加**。

提示：当数据中心的账号或端口有变化时，可以使用“更新”功能以同步数据中心的资源信息。选择虚机中心 > 全局设置，点击更新按钮，编辑用户名、密码和端口，编辑完成后点击确定。

- **配置内部管理网络**

管理网络为 vSMC 模块和 vSPM 模块间通信使用，可根据网络环境选择交换机类型和管理接口。

4. 在**配置内部管理网络**页签中选择交换机类型和接口，为接口配置 IP 地址。

- 所属主机:vSMC 所在的主机名称。
- 交换机类型：可根据原有网络情况，选择**标准交换机**或者**分布式交换机**。
- 接口：选择用于内部通信的接口。
- IP 地址：接口通信的 IP 地址。当在接口中选择 eth0 时，此处配置的 IP 地址为从 IP 地址，不影响 eth0 通过原有 IP 地址进行通信。
- 掩码：接口 IP 地址对应的掩码。
- 网关：接口的网关，仅跨网段通信时需要配置。
- 目的地址：目的网络或主机地址，仅跨网段通信时需要配置。

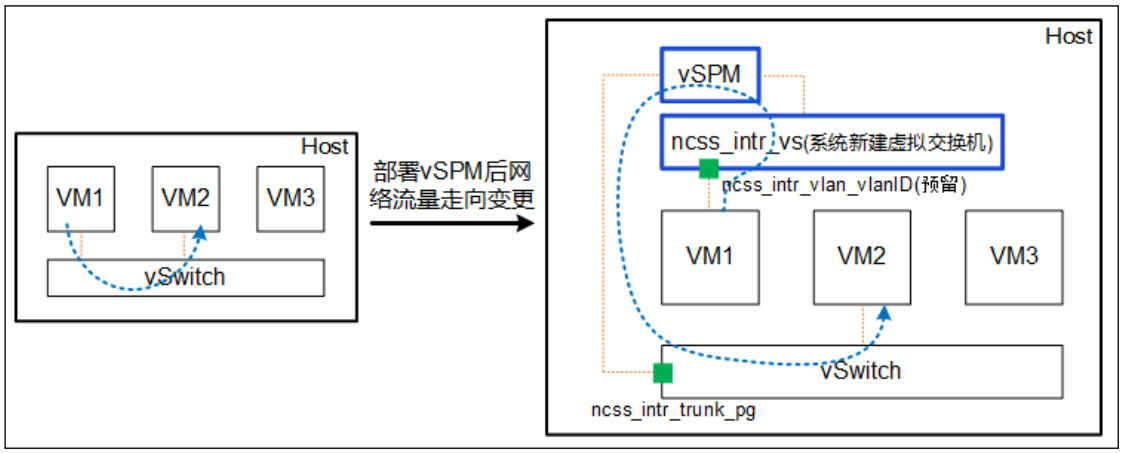
提示：此处的“接口”需要根据实际环境的拓扑来选择，原则上需要保证vSMC同vCenter以及各个ESXi主机之间是网络联通的，vSMC需要通过“内部管理网络”来向各ESXi主机部署vSPM。实际部署时，需要根据网络情况确定是否要增加eth1接口。通常，环境中区分管理网络和业务网络，则需要增加eth1接口用于连接各ESXi主机。

5. 点击**保存**。

- **配置内部引流网络**

内部网络为被保护虚拟机流量引向的网络，在这个网络中，虚拟机间不再直接通信，虚拟机间的流量都需要经过 vSPM 模块的检测。在未部署 vSPM 时，VM1 到 VM2 流量如左侧 Host 中所示，从 VM1 经 vSwitch 到 VM2。当部署 vSPM 后，VM1 的流量会被引导到系统新建的虚拟交换机上，

然后经过 vSPM 检测，再回到 vSwitch 中，最后到达 VM2。



6. 在**配置内部引流网络**页签，选择创建的虚拟交换机的类型，并指定系统预留 VLAN。

- 交换机类型：要创建的交换机类型，可选**标准交换机**或者**分布式交换机**。
- 系统预留 VLAN：在创建交换机时预留的 VLAN ID，缺省 100，最多支持 500 个。
- 交换机文件夹：创建的交换机文件夹名称，不可更改。
- 交换机名称：创建的交换机名称，不可更改。
- 端口组名称：创建的端口组名称，不可更改。
- INT 端口组名称：系统预留 VLAN 对应的端口组名称。

7. 点击**保存**。

8. （可选）需要更改预留 VLAN 时，可向右延伸，扩展预留 VLAN，点击**保存 VLAN**。

提示：点击“重载”将重新加载vCenter的相关信息。点击“清除”，将清除NCSS上所有配置，包括清除虚机保护、清除vSPM模块、相关的安全配置等。

3.2.主机

NCSS 可以识别其所在数据中心的 ESXi 主机。如需保护指定主机下的虚拟网络和虚拟机，管理员需要先在主机上部署虚拟防火墙，然后再为虚拟网络和虚拟机添加安全防护功能。当不再需要虚拟防火墙时，也可以将其从主机上移除。

3.2.1. 部署虚拟防火墙（DHCP 方式）

因为使用 eth0 提供 DHCP 服务，将造成内部网络 IP 地址分配问题，所以只有当 vSMC 具备两块及两块以上网卡，且在**错误!未找到引用源。**的**配置内部管理网络**中所选网卡不为 eth0 时，才可以使用此种方式进行虚拟防火墙部署。

3.2.1.1.启用 DHCP 服务

1. 选择**系统管理>DHCP 服务**。
2. 点击**开启**，启用 DHCP 服务并设置 DHCP 服务器信息。

- DHCP 操作：开启或关闭 DHCP 服务。
- 接口：NCSS 提供 DHCP 服务的接口。
- IP 地址：DHCP 服务接口的 IP 地址。
- 租期：IP 地址租期时间。时间范围为 1～1440000 分钟。
- 开始 IPv4 地址：待分配 IP 地址段的起始 IPv4 地址。
- 结束 IPv4 地址：待分配 IP 地址段的结束 IPv4 地址。
- 掩码：待分配 IP 地址段的掩码。

3. 点击**确定**。

3.2.1.2.为主机部署虚拟防火墙

1. 选择**虚机中心>主机**。
2. 在**主机**列表中，勾选指定主机名称对应的复选框，选中一个或多个需要保护的主机，也可以勾选**主机名称**左侧的复选框选中所有主机，点击**部署虚拟防火墙**为主机部署虚拟防火墙。

- **主机名称：**vCenter 中主机的名称。
- **数据存储：**主机数据的存储位置。
- **CPU 数量：**主机的物理 CPU 数量。
- **连接状态：**主机的链路状态。
  - 表示已连接。
  - 表示已断开。
  - 表示该主机已被从数据中心移除。
- **开机状态：**主机是否处于开机状态。
  - 表示处于开机状态。
  - 表示处于关机状态。
- **部署状态：**主机是否处于虚拟防火墙的保护中。
  - 空白表示未受保护状态。
  - 表示处于保护状态。
  - 表示处于保护异常状态。
- **虚拟交换机：**主机所属的虚拟交换机。
- **保护虚机数量：**主机中被保护的虚拟机数量。
- **虚拟防火墙：**部署在主机上的虚拟防火墙的名称。
- **虚拟防火墙状态：**请参照**错误!未找到引用源。**所描述的防火墙状态信息。

3. 根据实际需求选择管理交换机和需要保护的虚拟交换机、数据存储位置以及 CPU 和内存大小。

推荐勾选**资源预留**，以使虚拟防火墙独占主机 CPU 和内存资源。如果不勾选，虚拟防火墙会与主机上的其他虚拟机共享 CPU 和内存资源。

此处需根据网络环境选择管理交换机和管理交换机端口组，确保与**错误!未找到引用源。**中所配置的内部管理网络能够通信。如所选主机为 vSMC 所在主机，且 vSMC 为单网卡，需在此处选择与 vSMC 相同的管理交换机及端口组，避免部署时 vSMC 的内部管理网卡被接入选择的不同的管理端口组中，这有可能带来 vSMC 通信中断等问题。

4. 点击**确定**。

虚拟防火墙部署成功后，主机的保护状态显示为 。

3.2.2. 部署虚拟防火墙（非 DHCP 方式）

3.2.2.1.禁用 DHCP 服务

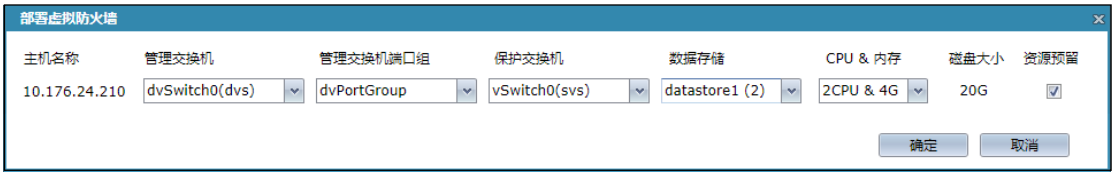
1. 选择**系统管理>DHCP 服务器设置**。
2. 点击**关闭**，禁用 DHCP 服务。

3. 点击**确定**。

3.2.2.2.为主机部署虚拟防火墙

1. 选择**虚机中心>主机**。
2. 在**主机**列表中，勾选指定主机名称对应的复选框，选中需要保护的主机，点击**部署虚拟防火墙**为主机部署虚拟防火墙。

3. 根据实际需求选择管理交换机和需要保护的虚拟交换机、数据存储位置以及 CPU 和内存大小。



推荐勾选**资源预留**，以使虚拟防火墙独占主机 CPU 和内存资源。如果不勾选，虚拟防火墙会与主机上的其他虚拟机共享 CPU 和内存资源。

此处需根据网络环境选择管理交换机和管理交换机端口组，确保与**错误!未找到引用源。**中所配置的管理网络能够通信。如 vSMC 为单网卡情况，且所选主机为 vSMC 所在主机，需先理清主机内部网络结构，然后在此处选择与 vSMC 相同的管理交换机及端口组，避免部署时 vSMC 的内部管理网卡被接入选择的不同的管理端口组中，这有可能带来 vSMC 通信中断等问题。

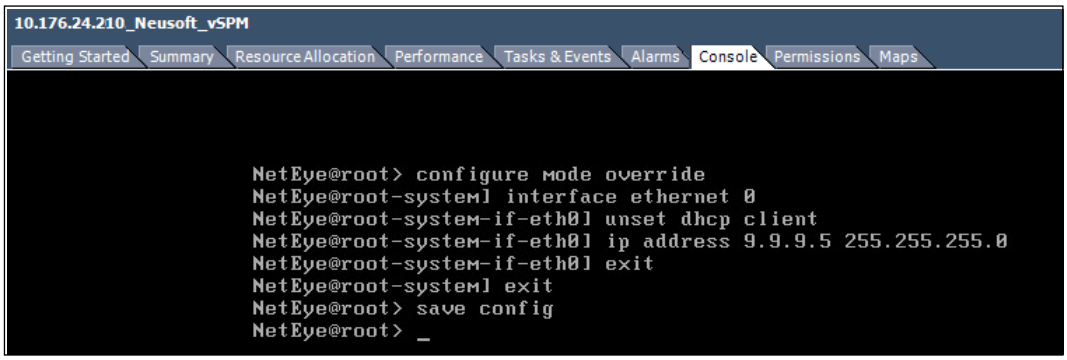
4. 点击**确定**。

提示：点击确定之后，经过一段时间，UI会显示部署防火墙异常状态，需要手动添加vSPM。在出现提示之后，方可执行**错误!未找到引用源。**中相关步骤。

3.2.2.3.在 VMware 中配置虚拟防火墙

在 VMware 中，找到主机，其节点下的“10.176.24.210_Neusoft_vSPM”即是刚刚部署的虚拟防火墙。点击“**10.176.24.210_Neusoft_vSPM**”并点击 **Console**，为虚拟防火墙的接口 eth0 添加 IP 地址并禁用此接口的 DHCP 客户端功能。

虚拟防火墙的初始用户名和密码都是“Neusoft”。具体配置如下：



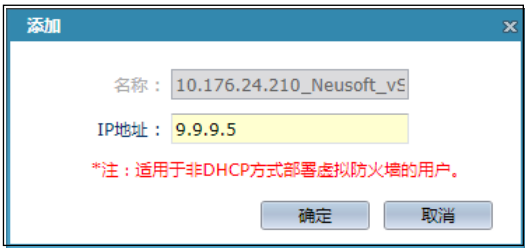
操作步骤：打开防火墙虚拟机终端，进入防火墙全局配置模式>进入 eht0 接口配置模式>将接口切换为静态 IP 配置>配置静态 IP 地址>返回到特权配置模式>保存设置。

配置好 IP 地址后，请先在虚拟防火墙的 Console 下使用 Ping 命令 Ping NCSS 管理接口的 IP 地址，如果可以 Ping 通，说明虚拟防火墙的 IP 地址是有效的。可以返回 NCSS 界面继续为主机部署虚拟防火墙。

3.2.2.4.连接虚拟防火墙

1. 选择**虚机中心>主机**。
2. 在**主机**列表中，可以看到 10.176.24.210 的虚拟防火墙部署状态为 。点击**连接虚拟防火墙**手动添加虚拟防火墙。

3. 输入在 VMware 上为虚拟防火墙配置的 IP 地址。点击**确定**继续部署虚拟防火墙。



4. 部署成功后，主机的保护状态显示为 。同时可以在**近期任务**列表中查看操作的任务以及任务的状态。

3.2.3. 移除虚拟防火墙

1. 选择**虚机中心>主机**。
2. 在**主机**列表中，选中需要移除保护的主机，点击**移除虚拟防火墙**。

3. 在弹出的对话框中点击**确定**。

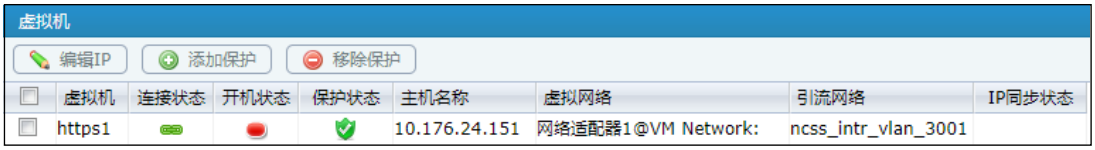
3.3.虚拟机

虚拟防火墙可以保护数据中心的服务虚机（即提供服务的虚拟机）。在为主机部署虚拟防火墙之后，管理员可以为指定的虚拟机添加或移除虚拟防火墙安全保护，同时也可以编辑虚拟机的 IP 地址。

3.3.1. 添加保护

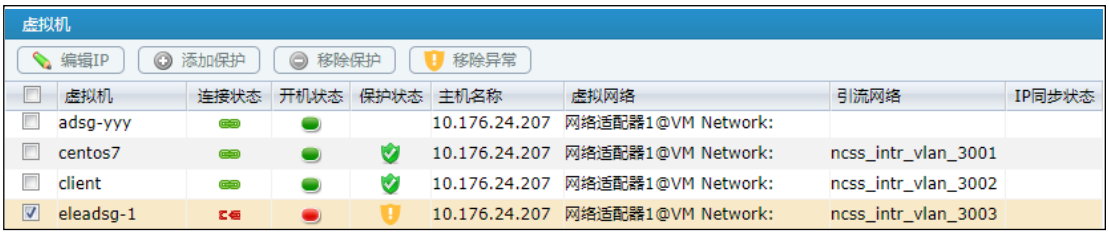
1. 选择**虚机中心>虚拟机**。
2. 在**虚拟机**列表中，勾选虚拟机名称对应的复选框，选中一个或多个（最多 5 个）需要保护的虚拟机，点击**添加保护**,指定需要进行引流的网卡。

3. 点击**确定**，为虚拟机部署虚拟防火墙安全防护。



- 虚拟机：虚拟机的名称。
- 连接状态：虚拟机的连接状态。
  - 表示已连接。
  - 表示已断开。
  - 表示该虚拟机所在主机已被从数据中心移除。
- 开机状态：虚拟机的开关机状态。
  - 表示主机处于开机状态。
  - 表示主机处于关机状态。
- 保护状态：虚拟机是否处于虚拟防火墙的保护中。
  - 表示处于保护状态。

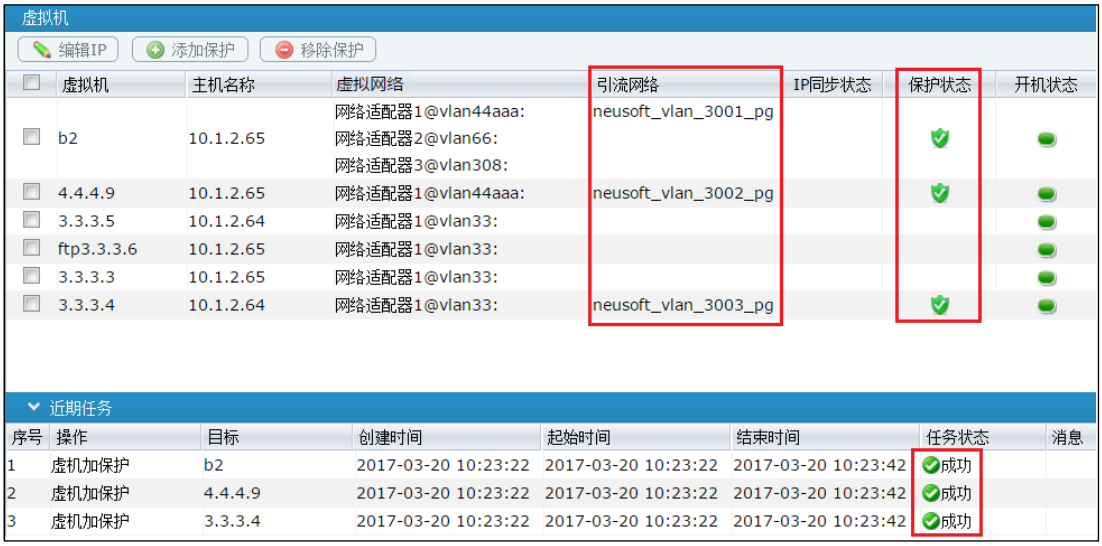
- 表示为虚拟机添加保护的时候出现异常，如网络中断。此时，需要勾选该项，点击**移除异常**按钮，将虚拟机恢复到未保护状态。



- 表示已处于保护状态，但由于虚拟防火墙出现异常情况而无法继续保护虚拟机。

- 主机名称：虚拟机所属 ESXi 主机的名称。
- 虚拟网络：虚拟机所属的虚拟网络（端口组）。
- 引流网络：添加保护之后，虚拟机所在的新端口组和虚拟交换机。
- IP 同步状态：虚拟机 IP 地址的同步状态。
  - 表示系统自动读取到了虚拟机的 IP 地址。
  - 表示虚拟机的 IP 地址是手动添加的。

安全防护添加成功后，虚拟机的保护状态显示为 并被引流到新的网络。同时可以在**近期任务**列表中查看操作的任务以及任务的状态。



3.3.2. 移除保护

1. 选择**虚机中心>虚拟机**。
2. 在**虚拟机**列表中，选中已被保护的虚拟机（最多 5 个）后，点击**移除保护**。

3.3.3. 编辑虚拟机 IP 地址

如果虚拟机没有安装 VMware Tools 或者 VMware Tools 未正常工作，NCSS 便无法自动同步虚拟机的 IP 地址，此时需要手动添加虚拟机网络适配器的 IP 地址。该 IP 地址用于安全策略的实现和流量监控等，但不会应用到虚拟机的网络适配器上，因此不会影响用户环境中虚拟机 IP 地址的部署。

1. 选择**虚机中心>虚拟机**。
2. 在**虚拟机**列表中，选中虚拟机条目，点击**编辑 IP**。

3. 点击**确定**。

3.4.虚拟网络

管理员可以为虚拟网络（端口组）中的虚拟机添加/移除虚拟防火墙安全保护。

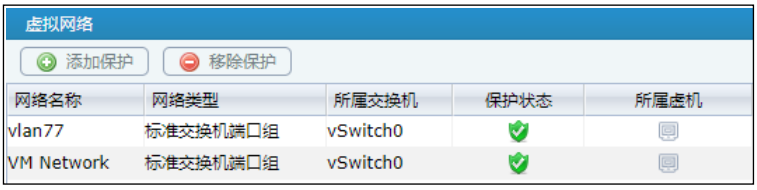
3.4.1. 添加保护

1. 选择**虚机中心>虚拟网络**。
2. 在**虚拟网络**列表中，选中需要保护的虚拟网络，点击**添加保护**。如需查看某虚拟网络包含的虚拟机，点击此虚拟网络条目对应的 。

   - 网络名称：虚拟网络的名称。
   - 网络类型：虚拟网络的类型。
   - 所属交换机：虚拟网络所属的交换机。
   - 保护状态：虚拟网络是否处于保护状态。
     - 空白表示未添加保护。
     - 表示处于保护状态。
     - 表示为虚拟网络添加保护的时候出现异常，如网络中断。当问题解决后，可以继续添加保护。
   - 所属虚机：虚拟网络包含的虚拟机。
3. 勾选**虚拟机名称**前面的复选框选中所有虚拟机。勾选虚拟机对应的复选框选中指定虚拟机并选择该虚拟机的网卡。

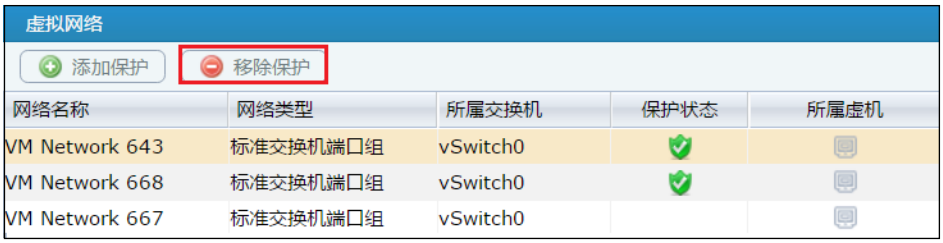
4. 点击**确定**。

安全防护添加成功后，虚拟网络的保护状态显示为 。同时可以在**近期任务**列表中查看操作的任务以及任务的状态。



3.4.2. 移除保护

1. 选择**虚机中心>虚拟网络**。
2. 在**虚拟网络**列表中，选中需要移除保护的虚拟网络，点击**移除保护**。



3. 如需移除对所有虚拟机的保护，勾选**虚拟机名称**前面的复选框。如需移除指定虚拟机的保护，勾选其对应的复选框。

4. 点击**确定**。

3.5.虚拟防火墙

分布式虚拟防火墙用于为需要保护的虚拟网络、主机和虚拟机提供微隔离和安全防护。管理员可以重启或关闭被管理的虚拟防火墙，配置步骤如下所示：

1. 选择**虚机中心>虚拟防火墙**。
2. 在**虚拟防火墙**列表中，点击虚拟防火墙对应的 连接到防火墙管理页面， 重启防火墙，点击 关闭防火墙,点击 来恢复防火墙连接。

   按钮只在状态栏中出现 状态时使用。

- 名称：虚拟防火墙的名称。
- 状态：虚拟防火墙的状态信息，包括：
  - ：表示虚拟防火墙处于正常工作状态。
  - ：表示虚拟防火墙处于异常工作状态，vSMC 管理模块将持续探测其状态，如期间虚拟防火墙恢复正常，则变为正常状态。
  - ：表示虚拟防火墙处于宕机状态，vSMC 管理模块将不再对其进行探测，系统将认为此防火墙不可用。
- IP 地址：虚拟防火墙的 IP 地址或域名。
- 平台：虚拟防火墙型号。
- 创建日期：虚拟防火墙添加到 NCSS 的时间。
- 版本：虚拟防火墙的软件版本信息。
- 上次心跳时间：NCSS 最后一次收到被管理虚拟防火墙发送的心跳包的时间与当前系统时间的差值。
- 描述：虚拟防火墙的描述信息。

3.6.虚拟机网关设置

如果 vCenter 网络不存在 VLAN，管理员应手动将虚拟机网关的 MAC 地址添加到 NCSS 上，以保证网络的畅通。

管理员可以进行如下操作，操作结果会同步到所有被管理的虚拟防火墙上：

- 3.6.1 添加虚拟机网关
- 3.6.2 删除虚拟机网关

当 vCenter 中没有可用的虚拟防火墙时，操作结果会保存在 NCSS 系统中。当成功部署了虚拟防火墙后，操作结果会直接同步到虚拟防火墙上。

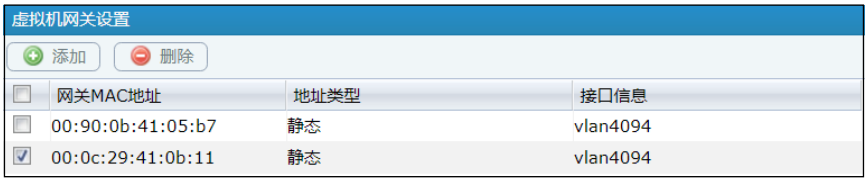
3.6.1. 添加虚拟机网关

1. 选择**虚机中心>虚拟机网关设置**。
2. 点击**添加**，添加虚拟机网关。
3. 在**网关 MAC 地址**文本框中输入虚拟机网关的 MAC 地址。

4. 点击**确定**。

3.6.2. 删除虚拟机网关

1. 选择**虚机中心>虚拟机网关设置**。

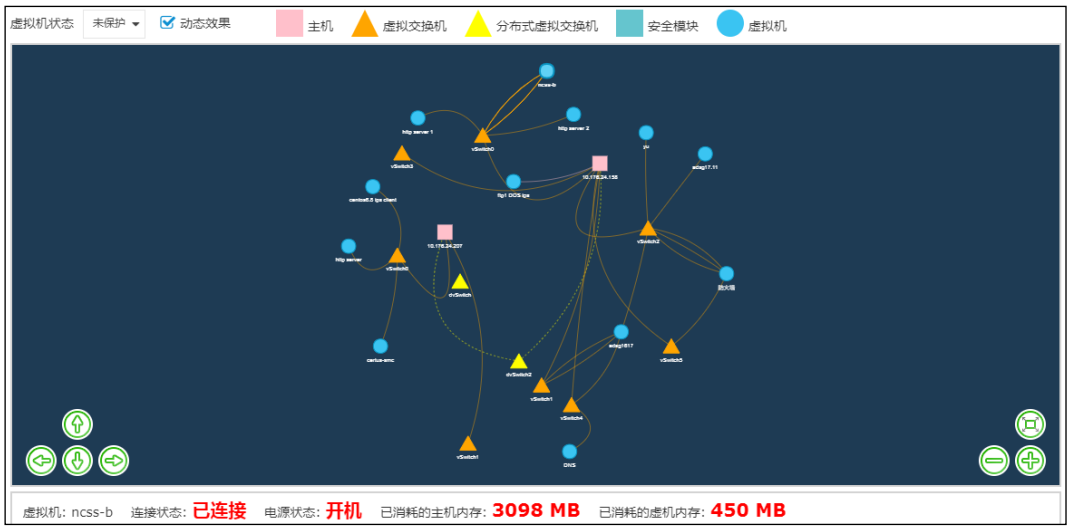


2. 在**虚拟网关设置**列表中，勾选**网关 MAC 地址**左侧的复选框选中所有网关 MAC 地址条目，或者勾选条目对应的复选框选中一个或多个条目，点击**删除**。在弹出的对话框中点击**确定**，删除网关 MAC 地址。

3.7.拓扑视图

NCSS 提供数据中心拓扑可视化功能，帮助管理员了解数据中心内部虚拟机、虚拟交换机、虚拟防火墙（vSPM 安全模块）和主机的分布和连接情况。

1. 选择**虚机中心>拓扑视图**。
2. 在**虚拟机拓扑下拉框**中，选择**未保护**（缺省）或**已保护**查看未受虚拟防火墙保护和已受保护的虚拟机的分布情况。勾选**动态效果**（缺省）或者去勾选**动态效果**，选择是否使图标在拓扑图中浮动。
   - 将鼠标置于虚拟交换机或 vSPM 图标上，查看其所属的主机。
   - 将鼠标置于虚拟机图标上，查看虚拟机的网络适配器及 IP 和 MAC 地址。点击虚拟机图标，在拓扑图下方查看连接状态、电源状态、已消耗的主机内存、已消耗的虚机内存及流量和威胁统计。
   - 将鼠标置于连线上，查看虚拟交换机和虚拟机所属的端口组。
   - 点击 vSPM 图标，查看接收和发送的流量信息。



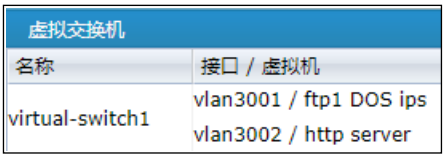
第4章 网络

管理员为虚拟机添加虚拟防火墙保护之后，系统会自动创建与虚拟机对应的虚拟交换机和安全域。本章包括以下内容：

4.1.虚拟交换机

管理员可以查看虚拟交换机信息。

1. 选择**网络 >虚拟交换机**。
2. 在**虚拟交换机**列表中，查看被保护的虚拟机所属的虚拟交换机和端口组信息。



虚拟交换机	
名称	接口 / 虚拟机
virtual-switch1	vlan3001 / ftp1 DOS ips vlan3002 / http server

- 名称：虚拟交换机的名称。
- 接口/虚拟机：虚拟交换机中包含的接口及接口连接的虚拟机。

4.2.安全域

虚拟防火墙基于安全域对数据流进行控制。管理员可以在访问策略、DoS 防御策略、应用安全策略和应用控制策略中引用安全域。在为虚拟机添加防护之后，这里会显示系统自动生成的安全域，该安全域可以直接使用。另外，在此处可以配置安全域的域内缺省安全策略，包括**允许**和**禁止**。

步骤如下所示：

1. 选择**网络>安全域**。
2. 勾选需要更改缺省域内策略的条目，点击**允许**或**禁止**。

第5章 策略

管理员可以在 NCSS 上配置访问控制策略、DoS 攻击防御策略、应用安全策略、应用控制策略以及防病毒策略。NCSS 可以将配置好的策略统一下发到被管理虚拟防火墙上。虚拟防火墙被部署到需保护的网络、主机和虚拟机后，便可以对流经的数据流进行检测和控制，因此可以有效保护数据中心资源的安全。

本章包括以下内容：

5.1.访问策略

访问策略用于控制从特定源发往特定目的数据流。通过访问策略，虚拟防火墙可以对同一网络内部的访问进行控制，从而防止数据中心敏感资源被非法访问和使用。缺省情况下，NCSS 中没有访问策略。管理员可以根据实际需要添加访问策略。

管理员可以对访问策略进行如下操作，操作结果会同步到所有被管理虚拟防火墙上：

5.1.1. 添加访问策略

1. 选择**策略 >访问策略**。
2. 在**访问策略**区域中，点击**添加**。
3. 填写名称和描述信息，启用或禁用策略以及记录日志功能并设置虚拟防火墙的动作。

- 名称：访问策略的名称。长度 1～63 字节，UTF-8 字符。不能包含空格和以下字符：?,"'\ < > & #
- 描述：访问策略的描述信息。长度 0～255 个字节，UTF-8 字符。不能包含以下字符：?"'\ < > &
- 启用：勾选复选框启用策略或取消勾选禁用策略。策略的状态缺省为启用。
- 记录日志：勾选复选框启用记录日志功能或取消勾选禁用此功能。此功能在旁路模式下，缺省为开启；在线模式下，缺省为禁用。
- 动作：虚拟防火墙如何处理匹配访问策略的数据包。
  - 允许（缺省动作）：转发数据包并更新其所属会话的状态。
  - 禁止：丢弃数据包并取消其会话。

4. 设置安全域、源 IP 地址以及目的 IP 地址。

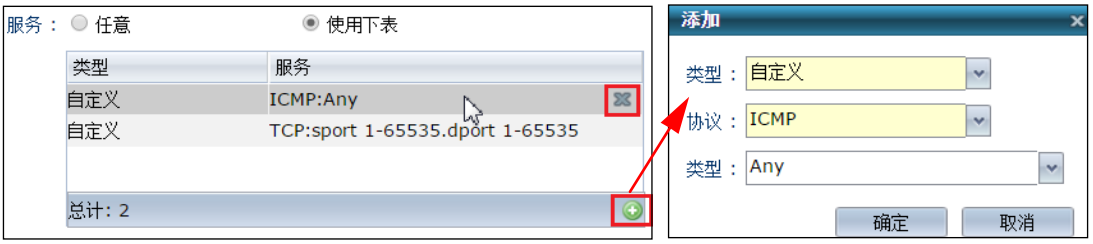
- 安全域：对通过哪个安全域内的访问进行控制。缺省为**任意**，即任意安全域的通信。
- 源 IP 和目的 IP：发送数据包的 IP 地址和数据包要到达的 IP 地址。
  - 任意（缺省值）：包括所有 IPv4 地址。
  - 使用下表：使用表中的地址条目。

点击添加 IP 地址条目，包括 IPv4 地址、地址范围、IPv4 地址/掩码。

管理员最多可以为每条策略配置 4096 个源 IP 地址条目和 4096 个目的 IP 地址条目。IP 地址条目不允许出现完全相同的情况。

如需删除已添加的地址条目，选中条目后点击 。

5. 设置数据包使用的服务。



- 任意（缺省值）：包括所有协议类型。
- 使用下表：使用表中的服务条目。

点击添加服务条目。自定义协议包括 ICMP、TCP、UDP 和 Other。TCP 和 UDP 协议的源和目的端口号范围为 1～65535。其它协议号范围为 1～255。

管理员最多可以配置 32 个服务条目（共 4096 个端口号）。服务列表内的条目不允许出现完全相同的情况。

如需删除已添加的服务条目，选中条目后点击 。

6. 点击**确定**以使策略生效。

5.1.2. 编辑/删除/移动访问策略

1. 选择**策略>访问策略**。

2. 在**访问策略**列表中：
   - 双击某个条目或者点击条目对应的，对其进行编辑。
   - 勾选**序号**左侧的复选框选中所有策略，或者勾选策略条目对应的复选框选中一个或多个条目，点击**删除**。在弹出的对话框中点击**确定**，删除策略。
   - 点击条目对应的，修改策略的序号以提升或降低策略的优先级（1~80000），在弹出的对话框中设置序号并点击**是**。策略的序号越小，与数据包进行匹配时优先级越高。

5.1.3. 启用/禁用访问策略

1. 选择**策略>访问策略**。
2. 在**访问策略**列表中，勾选序号左侧的复选框选中所有策略，或者勾选策略条目对应的复选框选中一个或多个条目，点击**启用**或**禁用**，启用或禁用访问策略。

5.2.攻击防御

管理员可以配置 DoS 攻击防御策略并将策略应用于指定安全域中，以防止安全域中的资源遭受 DoS/DDoS 攻击。DoS 攻击的类型、方式及虚拟防火墙的解决措施如下表所示：

攻击类型	攻击方式	虚拟防火墙解决措施
ICMP 泛滥	在短时间内向受害主机发送大量 ICMP Echo 请求包，耗尽主机资源。	限制每秒钟允许通过的 ICMP Echo 请求数据包个数。 **阈值**：1～1000000 pps。
TCP SYN 泛滥	在短时间内向受害主机发送带有虚假源 IP 地址的 TCP SYN 数据包，使受害主机系统中堆积大量的半连接，直至资源耗尽。	限制每秒钟允许通过的 TCP SYN 请求数据包数。 **阈值**：1～1000000 pps。
UDP 泛滥	在短时间内向受害主机发送大量 UDP 数据包，耗尽主机资源。	限制每秒钟允许通过的 UDP 数据包个数。 **阈值**：1～1000000 pps。
DNS 泛滥	在短时间内向受害主机发送大量 DNS 请求，耗尽主机资源。	限制每秒钟允许通过的来自某安全域的（基于 UDP 的）DNS 查询请求数量。 **阈值**：1～1000000 pps。 同时启用 UDP 泛滥防御和 DNS 泛滥防御时： ▪ 如果 DNS 泛滥的阈值大于 UDP 泛滥阈值，则以 UDP 泛滥的阈值和动作为准。 ▪ 如果 DNS 泛滥阈值小于或等于 UDP 泛滥阈值，则以 DNS 泛滥的阈值和动作为准。
TCP RST 扫描	向目标主机发送大量带有虚假源 IP 的 TCP RST 数据包，使该主机中正常的连接被恶意关闭，服务也因此被迫中断。	接收到 TCP RST 数据包时，会检查此数据包是否属于虚拟防火墙中已存在的任何一个会话，如果不属于任何会话，将认定此数据包具有 TCP RST 扫描行为，并按照管理员设置的动作对其进行处理。

WinNuke	向使用 Windows 操作系统的主机的 139、138、137、113 或 53 端口发送 TCP URG 数据包，造成 NetBIOS 碎片重叠，并导致系统崩溃。	当虚拟防火墙中存在目的端口为 139、138、137、113 或 53 的 TCP 会话时，如果接收到属于这个会话的 TCP URG 数据包，将认定此数据包具有 WinNuke 攻击的特征，并按照管理员设置的动作对其进行处理。
LAND	在短时间内向受害主机发送大量源、目的 IP 相同的 TCP SYN 数据包，使受害者系统中存在大量的无用连接，耗尽受害主机的资源，导致拒绝服务。	当接收到 TCP SYN 数据包时，会验证此数据包的源 IP 地址和目的 IP 地址是否相同。如果相同，会按照管理员设置的动作对其进行处理。
Smurf	伪造大量的源 IP 地址为受害主机 IP 且目的 IP 地址为广播地址的 ICMP Echo 请求包，使网络中的所有主机都不断地向受害主机发送应答数据包，导致受害主机被淹没乃至整个网络发生拥塞。	接收到 ICMP Echo 数据包时，会检查此数据包的目的 IP 地址是否为广播地址。如果是，将认定此数据包具有 Smurf 攻击行为，并按照管理员设置的动作对其进行处理。
TCP SYN Cookie	通过 TCP 源探测+首包丢弃的方法防御 TCP SYN Flood 攻击的一种方式，对 IP 地址源只做一次验证，通过后就加入白名单，占用很少的系统资源。 同时，为了防止出现 SYN Flood 攻击时，有可能对所有的攻击报文都回复错误序列号的 SYN-ACK 报文，还可以通过增加黑名单降低系统资源占用率。	虚拟防火墙接收到 IP 发送的第一个 SYN 报文后，将其丢弃。收到同一 IP 发送的第二个 SYN 报文后，伪造一个带有错误序列号的 SYN+ACK 报文回应给 IP 源所在的客户端： ▪ 如果客户端回复了 RST 应答，则将这个源 IP 加入白名单。 ▪ 如果未收到客户端的 RST 应答，则针对同一 IP 后续发送的每个 SYN 报文都回复一个带有错误序列号的伪造 SYN+ACK 报文。 ▪ 如果在针对同一 IP 发出 10 个伪造 SYN+ACK 报文后仍未收到客户端回应，则将这个源 IP 加入黑名单；否则将这个源 IP 加入白名单。 白名单和黑名单一共支持最多 2000 个 IPv4 地址。

管理员可以根据实际需求对攻击防御进行配置，配置步骤如下所示：

1. 选择**策略>攻击防御>DoS 防御**。

2. 选择需保护的安全域。
3. 勾选攻击类型左侧的复选框，启用相应的攻击防御功能，配置阈值以及数据包数量达到阈值时虚拟防火墙对后续数据包的处理动作。如需禁用功能，取消勾选复选框。
   - **报警**：产生一个报警事件，通知管理员检测到攻击行为。
   - **丢弃**：丢弃数据包。
   - **丢弃并报警**：丢弃数据包，并且产生一个报警事件。

4. 点击**确定**以使配置生效。

5.3.应用安全

虚拟防火墙能够针对应用层数据进行解析并对其内容进行安全性检测和控制。应用安全防护功能包括：

- 入侵防御

  通过攻击签名检测和各应用层协议的协议限制，NCSS 能够识别应用层的恶意行为，检测和阻断潜在的攻击，保护用户的网络环境。攻击签名规则可进行实时升级。

- 防病毒

  主要基于文件类型，对匹配策略的数据流进行病毒扫描。防病毒规则可进行实时升级。

虚拟防火墙通过以下策略对指定的流量进行检测：

- 5.3.1 入站策略：检测向指定安全域内的服务器上传文件和发送邮件的流量，检测和阻断到服务器的非法流量，以保护内网中服务器（Web、邮件、FTP、DNS、Telnet 和 Other 服务器）的安全。
- 5.3.2 出站策略：检测从服务器端下载文件和接收邮件的流量，检测和阻断到指定安全域内客户端的非法流量，以保护内网中客户端的安全。

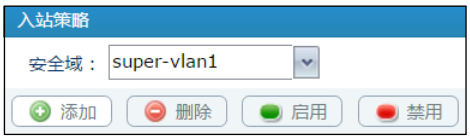
5.3.1. 入站策略

入站策略用于对指定安全域内的服务器进行防护。管理员可以对入站策略进行如下操作，操作结果会同步到所有被管理的虚拟防火墙上：

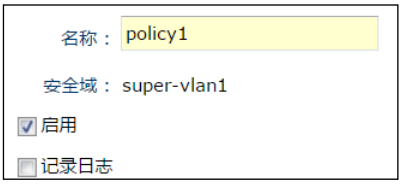
- 5.3.1.1 添加入站策略
- 5.3.1.2 编辑/删除/移动入站策略
- 5.3.1.3 启用/禁用入站策略

5.3.1.1.添加入站策略

1. 选择**策略 >应用安全>入站策略**。
2. 在**安全域**下拉框中，选择要保护的服务器所在的安全域。



3. 点击**添加**，添加策略。填写名称，启用或禁用策略以及记录日志功能。



- 名称：策略的名称。长度 1～63 字节，UTF-8 字符。不能包含空格和以下字符：?,"'\<>&#
- 启用：勾选复选框启用策略或取消勾选禁用策略。策略的状态缺省为启用。

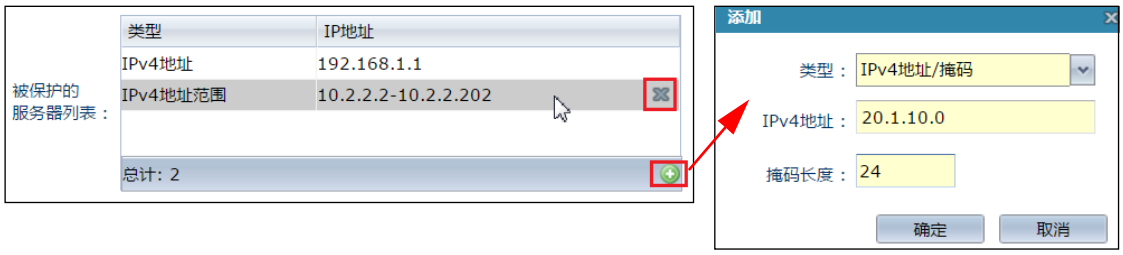
- 记录日志：勾选复选框启用记录日志功能或取消勾选禁用此功能。此功能在旁路模式下，缺省为开启；在线模式下，缺省为禁用。

4. 设置被保护的服务器的 IP 地址。

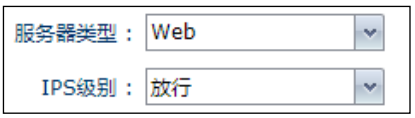
- 点击添加 IP 地址条目，包括 IPv4 地址、地址范围、IPv4 地址/掩码。

管理员最多可以配置 4096 个 IP 地址条目。IP 地址条目不允许出现完全相同的情况。

- 如需删除已添加的地址条目，选中条目后点击 。



5. 设置要保护的服务器类型并为服务器设置 IPS 功能。

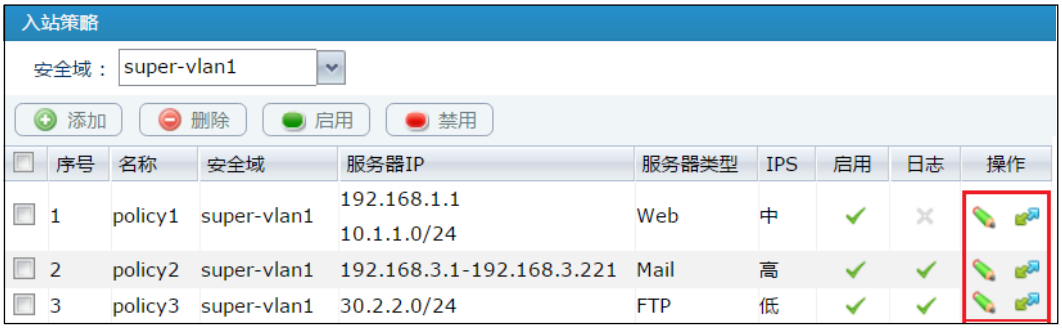


- 服务器类型：包括 Web、Mail、FTP、DNS、Telnet 和 Other。
- IPS 级别：
  - 关闭：不启用 IPS 防护。
  - 低：仅防御严重级别为高的攻击。
  - 中：防御级别为高和中的攻击。
  - 高：防御所有攻击。
  - 放行（缺省）：进行入侵检测，但不阻断威胁流量。

6. 点击**确定**以使策略生效。

5.3.1.2.编辑/删除/移动入站策略

1. 选择**策略>应用安全>入站策略**。



2. 在**入站策略**列表中：

- 双击某个条目或者点击条目对应的，对其进行编辑。
- 勾选**序号**左侧的复选框选中所有策略，或者勾选策略条目对应的复选框选中一个或多个条目，点击**删除**。在弹出的对话框中点击**确定**，删除策略。
- 点击条目对应的，修改策略的序号以提升或降低策略的优先级（1~80000），在弹出的对话框中设置序号并点击**是**。策略的序号越小，与数据包进行匹配时优先级越高。

5.3.1.3.启用/禁用入站策略

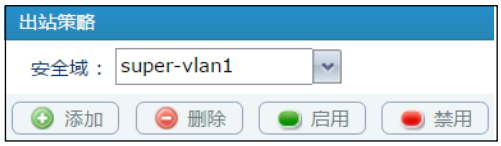
1. 选择**策略>应用安全>入站策略**。
2. 在**入站策略**列表中，勾选序号左侧的复选框选中所有策略，或者勾选策略条目对应的复选框选中一个或多个条目，点击**启用**或**禁用**，启用或禁用策略。

5.3.2. 出站策略

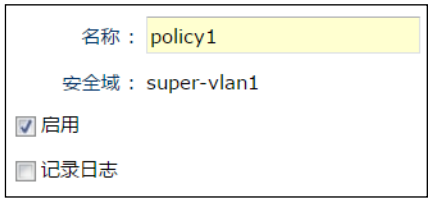
出站策略用于对指定安全域内的客户端进行防护。管理员可以对出站策略进行如下操作，操作结果会同步到所有被管理的虚拟防火墙上：

5.3.2.1.添加出站策略

1. 选择**策略>应用安全>出站策略**。
2. 在**安全域**下拉框中，选择要保护的客户端所在的安全域。



3. 点击**添加**，添加策略。
4. 填写名称，启用或禁用策略以及记录日志功能。



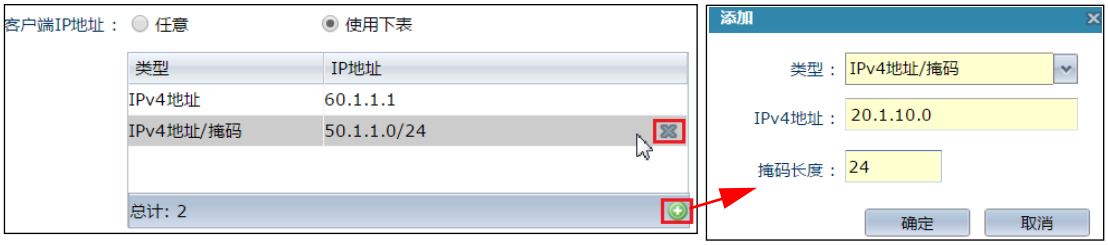
- 名称：策略的名称。长度 1～63 字节，UTF-8 字符。不能包含空格和以下字符：?,"' \ < > & #
- 启用：勾选复选框启用策略或取消勾选禁用策略。策略的状态缺省为启用。

- 记录日志：勾选复选框启用记录日志功能或取消勾选禁用此功能。此功能在旁路模式下，缺省为开启；在线模式下，缺省为禁用。

5. 设置被保护客户端的 IP 地址。
   - 任意（缺省值）：包括所有 IPv4 地址。
   - 使用下表：使用表中的地址条目。

点击添加 IP 地址条目，包括 IPv4 地址、地址范围、IPv4 地址/掩码。管理员最多可以配置 4096 个 IP 地址条目。IP 地址条目不允许出现完全相同的情况。

如需删除已添加的地址条目，选中条目后点击 。



6. 设置 IPS 功能。

- IPS 级别：
  - 关闭：关闭 IPS 功能。
  - 低：仅防御严重级别为高的攻击。
  - 中：防御级别为高和中的攻击。
  - 高：防御所有攻击。
  - 放行（缺省）：进行入侵检测，但不阻断威胁流量。
- 防病毒设置：防病毒功能缺省为关闭。可以为 FTP 下载、HTTP 下载、POP3 和 IMAP 流量开启相应的防病毒检测功能并设置检测级别。
  - 低：对易被感染的可执行二进制文件进行病毒检测。
  - 中：对易被感染的文件进行病毒检测。
  - 高：对所有文件进行病毒检测。

可以为 POP3 或 IMAP 协议邮件设置最大受保护邮件大小限制。取值范围为 1~10MB，缺省为 10MB。如果邮件超出此限制，虚拟防火墙不再进行后续的防病毒检测。

7. 点击**确定**以使策略生效。

5.3.2.2.编辑/删除/移动出站策略

1. 选择**策略>应用安全>出站策略**。

2. 在**出站策略**列表中：
   - 双击某个条目或者点击条目对应的，对其进行编辑。
   - 勾选**序号**左侧的复选框选中所有策略，或者勾选策略条目对应的复选框选中一个或多个条目，点击**删除**。在弹出的对话框中点击**确定**，删除策略。
   - 点击条目对应的，修改策略的序号以提升或降低策略的优先级（1~80000），在弹出的对话框中设置序号并点击**是**。策略的序号越小，与数据包进行匹配时优先级越高。

5.3.2.3.启用/禁用出站策略

1. 选择**策略 >应用安全>出站策略**。
2. 在**出站策略**列表中，勾选序号左侧的复选框选中所有策略，或者勾选策略条目对应的复选框选中一个或多个条目，点击**启用或禁用**，启用或禁用策略。

5.4.应用控制

管理员可以在指定的安全域上配置应用控制策略，虚拟防火墙对匹配到策略的用户流量进行应用控制，限制指定的用户可以访问及不能访问哪些应用。

应用控制配置步骤如下：

1. 创建应用控制防护配置，设置用户可以访问及不能访问的应用。
2. 创建策略，设置要限定的用户的匹配条件（用户流量的源安全域和源 IP 地址），并引用已创建的应用控制防护配置。

当用户的信息匹配策略中设置的限定条件，同时用户要访问的应用也匹配应用控制防护配置中设置的应用条目，虚拟防火墙会根据条目中的动作（阻断/放行）对应用及其所属会话进行处理。

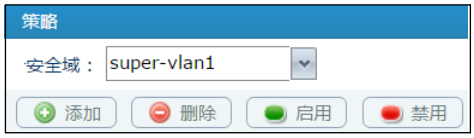
本节包含以下内容：

5.4.1. 策略

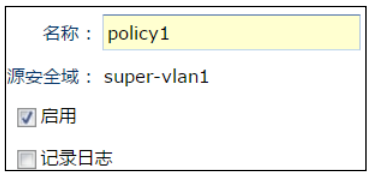
管理员可以对策略进行如下操作，操作结果会同步到所有被管理的虚拟防火墙上：

5.4.1.1.添加应用控制策略

1. 选择**策略 >应用控制>策略**。
2. 在**安全域**下拉框中，选择发起应用访问的内网用户所在的安全域。



3. 点击**添加**，添加策略。填写名称，启用或禁用策略以及记录日志功能。



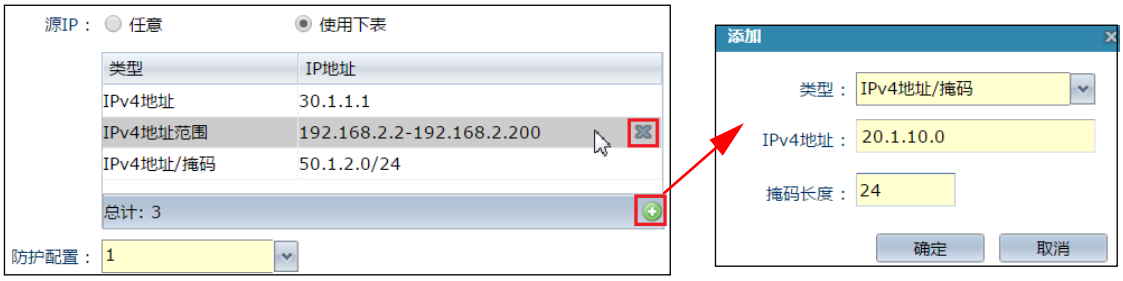
- 名称：策略的名称。长度 1～63 字节，UTF-8 字符。不能包含空格和以下字符：?,"' \ < > & #
- 启用：勾选复选框启用策略或取消勾选禁用策略。策略的状态缺省为启用。

- 记录日志：勾选复选框启用记录日志功能或取消勾选禁用此功能。此功能在旁路模式下，缺省为开启；在线模式下，缺省为禁用。

4. 设置用户的源 IP 地址。
   - 任意（缺省值）：包括所有 IPv4 地址。
   - 使用下表：使用表中的地址条目。

点击添加 IP 地址条目，包括 IPv4 地址、地址范围、IPv4 地址/掩码。管理员最多可以配置 4096 个 IP 地址条目。IP 地址条目不允许出现完全相同的情况。

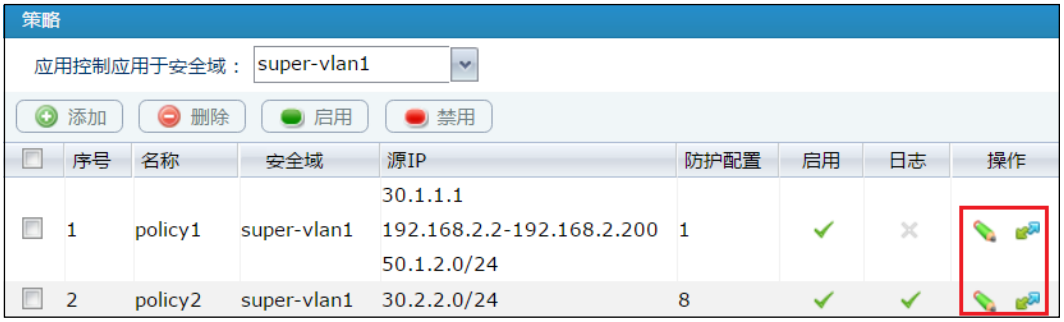
如需删除已添加的地址条目，选中条目后点击 。



5. 从**防护配置**下拉框中选取已创建好的应用控制防护配置。更多信息，请参见**错误!未找到引用源。**。
6. 点击**确定**以使策略生效。

5.4.1.2.编辑/删除/移动应用控制策略

1. 选择**策略>应用控制>策略**。



2. 在**策略**列表中：
   - 双击某个条目或者点击条目对应的，对其进行编辑。
   - 勾选**序号**左侧的复选框选中所有策略，或者勾选策略条目对应的复选框选中一个或多个条目，点击**删除**。在弹出的对话框中点击**确定**，删除策略。
   - 点击条目对应的，修改策略的序号以提升或降低策略的优先级（1~80000），在弹出的对话框中设置序号并点击**是**。策略的序号越小，与数据包进行匹配时优先级越高。

5.4.1.3.启用/禁用应用控制策略

1. 选择**策略 >应用控制>策略**。
2. 在**策略**列表中，勾选序号左侧的复选框选中所有策略，或者勾选策略条目对应的复选框选中一个或多个条目，点击**启用或禁用**，启用或禁用策略。

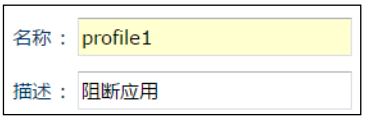
5.4.2. 防护配置

应用控制防护配置用于设置要进行控制的应用及对应用的处理动作。防护配置需要被应用控制策略引用才会生效。NCSS 最多支持 1024 个防护配置，每个防护配置最多支持 4096 个应用或应用分类。

管理员可以对防护配置进行如下操作，操作结果会同步到所有被管理的虚拟防火墙上：

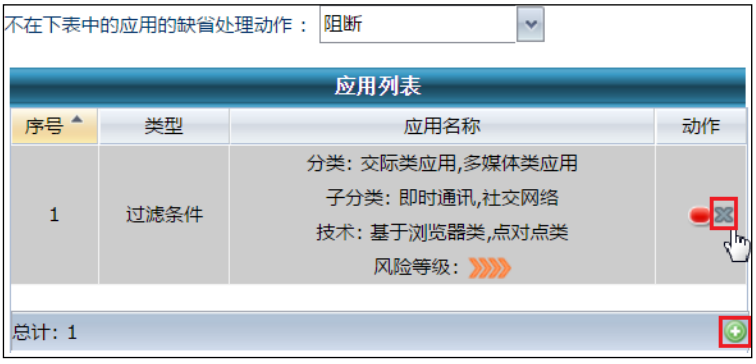
5.4.2.1.添加防护配置

1. 选择**策略 >应用控制>防护配置**。
2. 点击**添加**，添加防护配置。
3. 填写名称和描述信息。



   - 名称：防护配置的名称。长度 1～63 字节，UTF-8 字符。不能包含空格和以下字符：?,"'\ < > & #
   - 描述：防护配置的描述信息。长度 0～255 字节，UTF-8 字符。不能包含以下字符：? " ′ \ < > &。

4. 设置当应用不在应用列表中时对应用的处理动作，可以为**阻断**或**放行**。



应用条目的匹配流程为如下：

- 如果用户发起的应用匹配到应用列表中的应用条目，虚拟防火墙将按照指定的动作对应用及其所属会话进行处理。
- 如果未匹配到应用条目，虚拟防火墙将按照不在应用列表中的应用的缺省处理动作对应用进行处理。当虚拟防火墙无法识别某项应用（即应用不在应用知识库中）时，将放行应用及其所属会话。

5. 在**应用列表**中，点击 添加应用控制规则，如需删除已添加的条目，选中条目后点击 。
   - 序号：应用控制规则的匹配顺序，序号越小，越先匹配。
   - 选择类型：可通过指定过滤条件批量添加应用或指定应用名称添加单个应用。
     - 当选择**过滤条件**时，需选择应用分类、子分类、技术类型和风险等级，可以点击**查看**查看详细信息；点击**确定**。缺省为 **Any**，表示所有应用。
     - 选择**应用**时，在**应用列表**中点击 添加应用，点击**确定**。如需删除已添加的条目，选中条目后点击 。
   - 动作：对匹配到应用列表的应用的处理动作，包括**阻断**和**放行**。

6. 点击**确定**以使防护配置生效。

5.4.2.2.编辑/删除防护配置

1. 选择**策略>应用控制>防护配置**。

2. 在**防护配置**列表中：
   - 双击某个条目或者点击条目对应的 ，对其进行编辑。
   - 点击 查看引用防护配置的应用控制策略。
   - 勾选**名称**左侧的复选框选中所有防护配置，或者勾选防护配置条目对应的复选框选中一个或多个条目，点击**删除**。在弹出的对话框中点击**确定**，删除防护配置。已被应用控制策略引用的防护配置不能被删除。

5.4.3. 应用知识库

应用知识库列出虚拟防火墙能够识别的所有 RFC 标准应用，包括应用的名称、分类、子分类、所用技术及风险等级。管理员可查看应用知识库中的所有应用或查找特定应用。

1. 选择**策略>应用控制>应用知识库**。
2. 可以通过以下方式查找相关应用的信息：
   - 在**选择应用**区域中，分别点击应用的分类、子分类、技术和风险等级，每项可以选择一个、多个或选择 **Any**（即所有）。然后点击**确定**。
   - 在**应用名称**文本框中，输入应用的名称，点击**确定**。

当鼠标指向应用名称时，系统会显示此应用的描述信息。可以点击**清空过滤条件**，重置过滤条件并清空查询结果。

5.5.防病毒引擎

防病毒功能基于文件类型对数据流进行病毒扫描。如果未检测到病毒则直接放行；如果检测到病毒则根据管理员配置的处理动作进行处理（包括阻断或放行），并通过隔离文件记录相关信息。如果数据流同时匹配了多个防病毒属性，只要这些属性中的任何一个动作设置为阻断，该数据流将被阻断。防病毒规则可以进行实时升级，为用户网络提供即时保护。

当启用防病毒功能时，虚拟防火墙缺省对如下内容进行病毒扫描：

- 基于应用层协议（包括 HTTP、SMTP、FTP、POP3 和 IMAP）的数据流
- 网络中传输的特定类型的文件
- 网络中传输的压缩文件

如果检测到病毒，虚拟防火墙会根据管理员配置的动作对文件进行处理（包括阻断或放行），并产生报警日志。

本节包含以下内容：

5.5.1. 基本设置

只有在出站策略中启用了防病毒扫描功能，防病毒引擎的基本设置功能才会生效。

基本设置是防病毒功能的全局配置，包括以下内容：

- 启发式扫描

  检测潜在的威胁，包括针对钓鱼（Phishing）网站进行的病毒检测和基于算法进行的病毒检测。

- 压缩文档扫描

  对压缩文件进行病毒扫描。

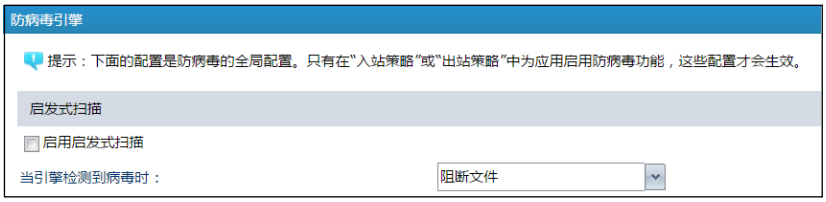
- 扫描设置

  虚拟防火墙缺省对基于应用层协议（包括 HTTP、FTP、SMTP、POP3 和 IMAP）的数据流进行病毒扫描。当管理员为上述协议数据流开启了滴流（持续下载）功能时，虚拟防火墙每隔一段时间将一部分已下载缓存的未扫描数据传给客户端，以避免扫描文件过大导致文件传输中断。

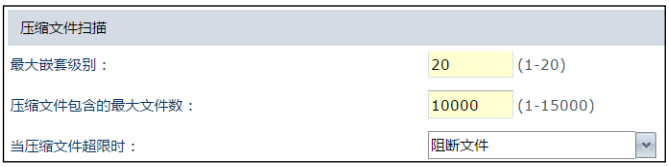
防病毒引擎基本设置的配置如下：

1. 选择**策略>防病毒引擎>基本设置**。
2. 勾选**启用启发式扫描**，启用此功能；取消勾选禁用此功能（缺省为禁用）。设置当引擎检测到病毒时对文件的处理动作，包括**阻断文件**和**放行文件**。在旁路模式下，缺省为**放行文件**；在线模式

下，缺省为**阻断文件**。



3. 设置压缩文件扫描功能。



- 最大嵌套级别：一个压缩文档中的最大嵌套层数。
- 压缩文件包含的最大文件数：一个压缩文档中的最大文件数目。
- 当压缩文件超限时：处理动作包括**阻断文件**和**不经扫描，放行所有文件**。在旁路模式下，缺省为**不经扫描，放行所有文件**；在线模式下，缺省为**阻断文件**。

4. 设置**滴流和防病毒引擎的处理动作。**

- 设置是否在 HTTP、FTP、SMTP、POP3 及 IMAP 上启用滴流功能，缺省为全部启用（勾选）。
  - 时间间隔：向客户端传送数据的时间间隔。
  - 数据大小：虚拟防火墙每次向客户端发送的数据大小。
- 当引擎检测到病毒时：处理动作包括**阻断文件**和**放行文件**。在旁路模式下，缺省为**放行文件**；在线模式下，缺省为**阻断文件**。
- 当引擎过载或扫描失败时：处理动作包括**阻断所有文件**和**不经扫描，放行所有文件**。
- 当引擎初始化失败时：处理动作包括**阻断所有文件**和**不经扫描，放行所有文件**。

5. 点击**确定**以使配置生效。

5.5.2. 信任的 URL

如果用户要访问的 URL 与信任 URL 列表中的条目匹配，那么不对其进行病毒扫描。每个信任 URL 列表最多支持 512 个 URL 条目。

管理员可以对信任 URL 进行如下操作，操作结果会同步到所有被管理的虚拟防火墙上：

- 5.5.2.1 添加信任的 URL
- 5.5.2.1 删除信任的 URL
- 5.5.2.3 启用/禁用信任的 URL

5.5.2.1.添加信任的 URL

1. 选择**策略 >防病毒引擎>信任的 URL**。
2. 点击**添加**，添加被信任的 URL。

   - URL：不进行防病毒扫描的 URL 地址；可以输入 IPv4 地址或域名。
   - 启用：勾选复选框启用此信任 URL（缺省为启用），或取消勾选禁用 URL。

3. 点击**确定**以使配置生效。

5.5.2.2.删除信任的 URL

1. 选择**策略>防病毒引擎>信任的 URL**。

2. 在**信任的 URL** 列表中，勾选 **URL** 左侧的复选框选中所有 URL，或者勾选 URL 条目对应的复选框选中一个或多个条目，点击**删除**。在弹出的对话框中点击**确定**，删除 URL。

5.5.2.3.启用/禁用信任的 URL

1. 选择**策略 >防病毒引擎>信任的 URL**。
2. 在**信任的 URL** 列表中，勾选 **URL** 左侧的复选框选中所有 URL，或者勾选 URL 条目对应的复选框选中一个或多个条目，点击**启用或禁用**，启用或禁用 URL。

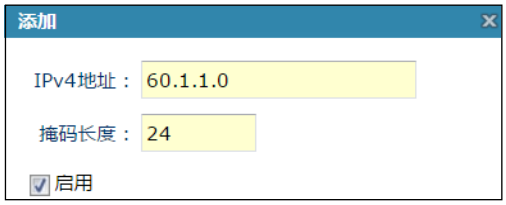
5.5.3. 信任的 IP 地址

如果客户端的源 IP 地址与信任 IP 地址列表中的条目匹配，则虚拟防火墙不对其进行病毒扫描。每个信任 IP 地址列表最多支持 512 个条目。

管理员可以对信任 IP 地址进行如下操作，操作结果会同步到所有被管理的虚拟防火墙上：

5.5.3.1.添加信任的 IP 地址

1. 选择**策略 >防病毒引擎>信任的 IP 地址**。
2. 点击**添加**，添加被信任的 IP 地址。



   - IPv4 地址/掩码长度：信任客户端的地址/掩码长度，即不进行防病毒扫描的地址。
   - 启用：勾选复选框启用此信任地址（缺省为启用），或取消勾选禁用地址。

3. 点击**确定**以使配置生效。

5.5.3.2.删除信任的 IP 地址

1. 选择**策略>防病毒引擎>信任的 IP 地址**。

2. 在**信任的 IP 地址**列表中，勾选 **IP 地址**左侧的复选框选中所有地址，或者勾选地址条目对应的复选框选中一个或多个条目，点击**删除**。在弹出的对话框中点击**确定**，删除地址。

5.5.3.3.启用/禁用信任的 IP 地址

1. 选择**策略 >防病毒引擎>信任的 IP 地址**。
2. 在**信任的 IP 地址**列表中，勾选 **IP 地址**左侧的复选框选中所有地址，或者勾选地址条目对应的复选框选中一个或多个条目，点击**启用或禁用**，启用或禁用地址。

第6章 监控

NCSS 的监控功能用来实时监控被管理虚拟防火墙的状态和全网流量信息，以帮助管理员了解系统运行状态和安全状态。本章包括以下内容：

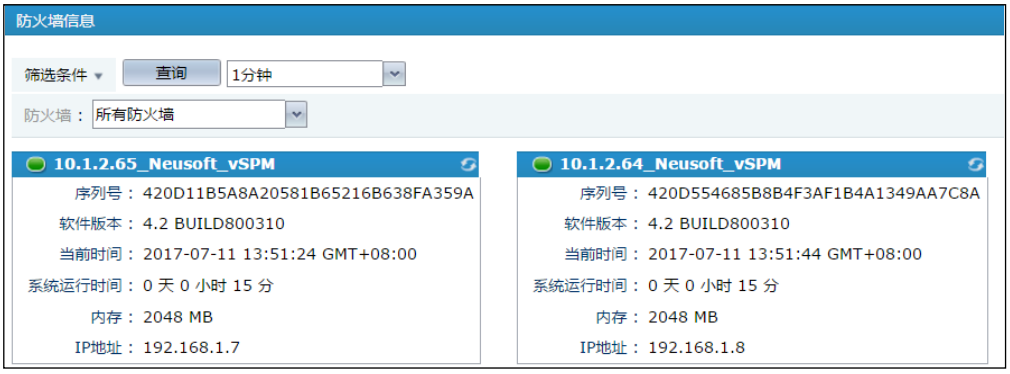
6.1.防火墙状态

管理员可以查看每台被管理虚拟防火墙的以下信息：

6.1.1. 防火墙信息

防火墙信息包括序列号、软件版本信息、当前时间、系统运行时间、内存及 IP 地址。

1. 选择**监控>防火墙状态>防火墙信息**。
2. 选择要查看的虚拟防火墙，点击**查询**查看对应虚拟防火墙的详细信息。可以设置系统自动刷新时间间隔。

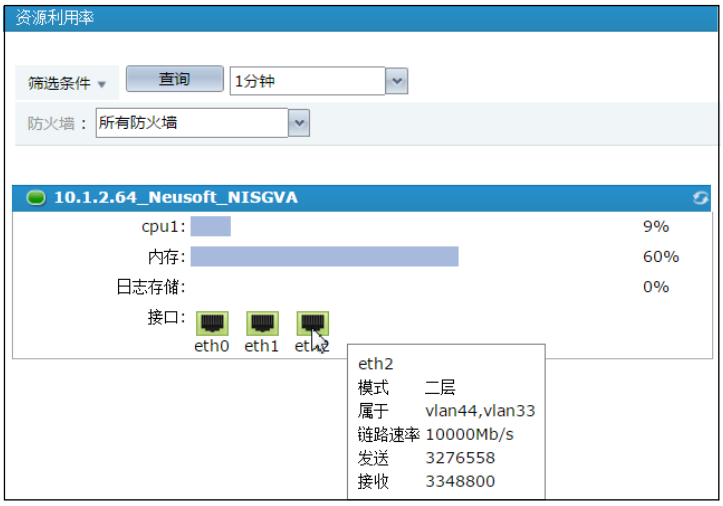


6.1.2. 资源利用率

资源利用率包括 CPU 利用率、内存利用率、日志存储空间利用率以及接口状态。接口状态包括接口名称、模式、IP 地址、链路速率以及接口流量统计等。

1. 选择**监控>防火墙状态>资源利用率**。

2. 选择要查看的虚拟防火墙，点击**查询**，即可查看具体信息。可以设置系统自动刷新时间间隔。



3. 如需查看某个接口的状态，将鼠标悬停在该接口上，接口的详细信息就会显示在弹出的窗口里。

6.1.3. ARP

ARP 表记录 IP 地址和 MAC 地址的一一对应关系。

1. 选择**监控>防火墙状态>ARP**。在 ARP 列表中可以查看 ARP 的条目信息。
2. 在**筛选条件**区域中，设置一项或多项 ARP 条目筛选条件。
   a) 从**防火墙**下拉框中，选择虚拟防火墙。
   b) 在 **IP 地址**和 **MAC 地址**文本中输入地址信息。
   c) 在**类型**下拉框中选取 ARP 类型。
3. 点击**查询**。也可以点击**清空所有过滤**清空所有过滤条件。

- IP 地址：目的主机 IP 地址。
- MAC 地址：与 IP 地址相对应的 MAC 地址。
- 类型：ARP 表项类型，包括静态、动态和消亡。
- 状态：ARP 表项状态。
  - INCOMPLETE：已发送 ARP 请求但还没有应答。

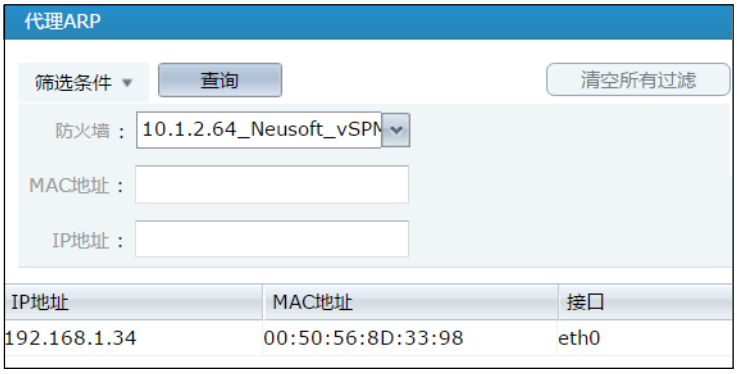
- REACHABLE：可用。
- STALE：可用，但生存时间过长，应再次查询学习。
- FAILED：不可用，该状态不可见。

- 生存时间（秒）：动态 ARP 表项存活时间。
- 接口：表项所属的的三层接口。

6.1.4. 代理 ARP

代理 ARP 用于不在同一网段的设备之间的通讯。

1. 选择**监控>防火墙状态>代理 ARP**。在代理 ARP 列表中可以查看条目信息。
2. 在**筛选条件**区域中，设置一项或多项条目筛选条件。
   a) 从**防火墙**下拉框中，选择虚拟防火墙。
   b) 在 **IP 地址**和 **MAC 地址**文本中输入地址信息。
3. 点击**查询**。也可以点击**清空所有过滤**清空所有过滤条件。



- IP 地址：目的主机 IP 地址。
- MAC 地址：与 IP 地址对应的 MAC 地址。
- 接口：表项所属的三层接口。

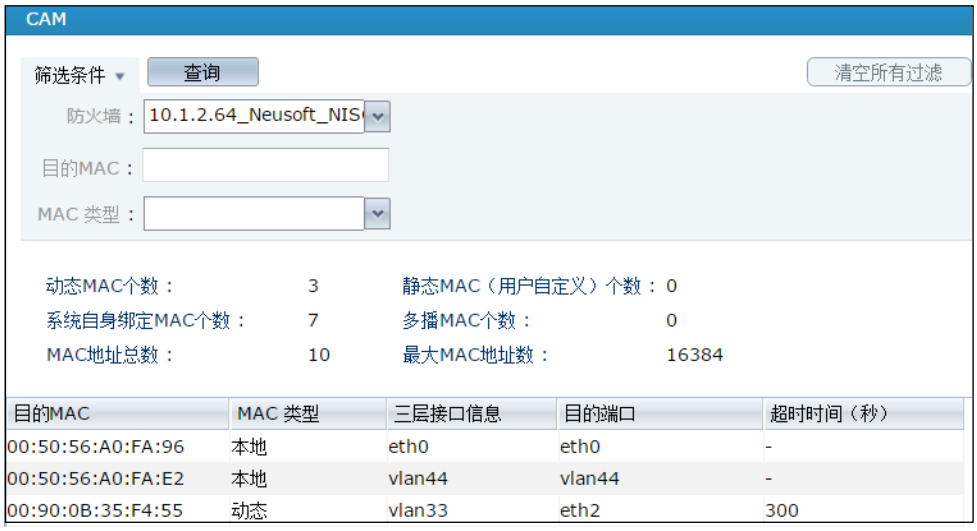
6.1.5. CAM

通过 CAM 表，虚拟防火墙可以为数据包选择相应的出口接口，从而提高系统带宽的利用率。管理员可以监控 CAM 表的信息。

1. 选择**监控>防火墙状态>CAM**。可以在 CAM 列表中查看 CAM 的条目信息。
2. 在**筛选条件**区域中，设置查看数据的筛选条件。
   a) 从**防火墙**下拉框中，选择虚拟防火墙。
   b) 在**目的 MAC** 文本中输入地址信息。

c) 在 **MAC 类型**下拉框中选取 MAC 类型。

3. 点击**查询**。也可以点击**清空所有过滤**清空所有过滤条件。



- 目的 MAC：数据包的目的 MAC 地址。
- MAC 类型：CAM 表项类型，包括动态、静态、本地和多播。
- 三层接口信息：表项所属三层接口的信息。
- 目的端口：接收数据包的目的端口。
- 超时时间（秒）：动态 CAM 表项的超时时间。

6.1.6. 路由

管理员可以监控被管理虚拟防火墙的 IPv4 路由、IPv6 路由、策略路由以及多播路由的实时信息。

1. 选择**监控>防火墙状态>路由**。
2. 在**筛选条件**区域中，从**防火墙**下拉框中，选择虚拟防火墙。

3. 点击**查询**。

- IPv4/IPv6 路由列表
  - 类型：路由类型，包括直连路由（Connected）和静态路由（Static）。
  - 目的 IP：数据包被发往的目的主机/网络的 IPv4 或 IPv6 地址。
  - 路由信息：路由过程的详细信息。
- 策略路由列表
  - 名称：策略路由的策略名称。
  - 目的 IP：数据包被发往的目的主机/网络的 IPv4 或 IPv6 地址。
  - 路由信息：路由过程的详细信息。
- 多播路由列表
  - 源 IP：多播数据包的源 IP 地址。
  - 多播组 IP：目的多播组的 IP 地址。
  - 入口接口：接收多播数据包的 DVMRP 接口。
  - 转发接口：将多播数据包转发出去的 DVMRP 接口。
  - 生存时间：多播数据包所能经过的最大路由设备数目。

6.2.流量

NCSS 监控被保护网络的流量信息，其中包括：

6.2.1. 被保护虚机

被保护虚机流量统计信息可以使管理员更好地了解受保护虚拟机的流量信息，及时发现异常。

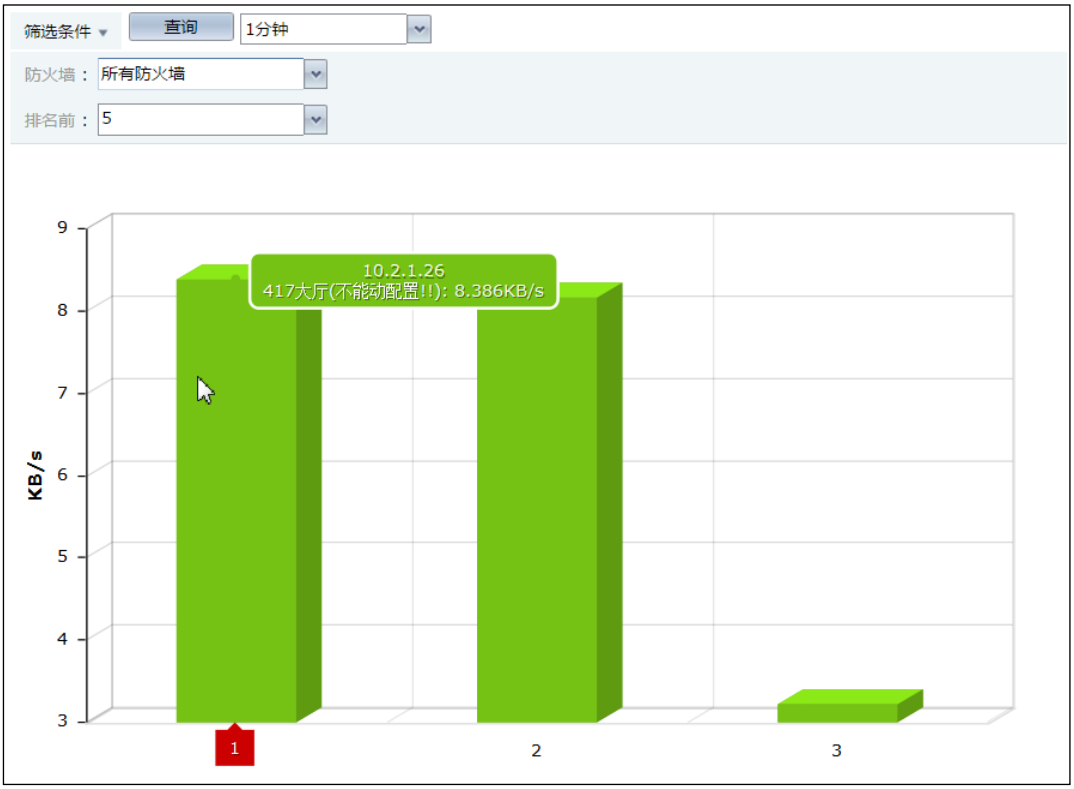
1. 选择**监控>流量>被保护虚机**。可以查看虚拟机实时的收发流量信息。
2. 在**筛选条件**区域中，设置查看数据的筛选条件。
   a) 从**主机**下拉框中选择主机。
   b) 从**虚拟机**下拉框中选择虚拟机。
3. 点击**查询**。管理员也可以选择系统自动刷新时间间隔。

6.2.2. IP 地址排名

可以查看 IP 地址的实时流量排名。

1. 选择**监控>流量>IP 地址排名**。
2. 在**筛选条件**区域中，设置查看数据的筛选条件。
   a) 从**防火墙**下拉框中，选择虚拟防火墙。
   b) 在**排名前**下拉框中设置排名前 N 名，可以设置前 3 名、前 5 名和前 10 名。

3. 点击**查询**。



4. 将鼠标置于某个 IP 地址对应的柱状图上，将显示该 IP 地址的实时流量值（单位 B/s、KB/s 或 MB/s）。

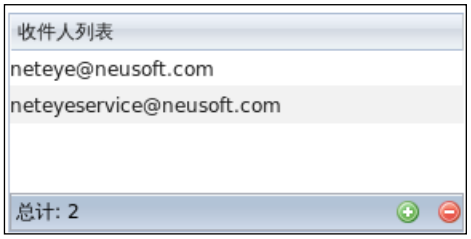
第7章 报警

NCSS 的报警功能用来报告被管理虚拟防火墙的异常情况。本章包括如下内容：

7.1.收件人设置

在 NCSS 上可以定义接收报警信息的收件人名单列表（最多 32 个人员）。当虚拟防火墙上产生报警时，报警信息将通过邮件发送给相应的人员。

1. 选择**报警>收件人设置**。
2. 点击  ，添加新的收件人邮件地址。如需删除收件人地址，选择相应的条目，点击  将其从列表中删除。



3. 点击**确定**。

7.2.报警信息

当发生报警事件时，NCSS 会生成报警信息提示管理员关注此事件。在首页和报警页面均可查看报警信息。

1. 选择**报警>报警信息**，查看报警信息。

- 图标 表明报警信息未读； 表示报警信息已读。点击**序号**左侧的 ，可以将所有报警信息置为已读；点击某个信息所对应 ，将单个信息置为已读。
- 序号：报警信息条目的编号。最新生成的排在列表最上端。
- 时间：报警产生的时间。
- 报警信息：报警信息的内容。
- 报警级别：报警的严重级别，分为高、中、低三种。
- 防火墙名称：产生报警的虚拟防火墙。
- 操作：删除报警信息。选中某条信息并点击对应的 ，删除此信息。

2. 点击**筛选条件**对应的 ，设置信息过滤条件。

a) 从**防火墙**下拉框中选择 NCSS、所有或部分虚拟防火墙。

b) 设置日期和时间范围。可以手动输入日期或者点击 选择日期。

3. 点击**查询**，满足上述条件的报警信息将会显示出来。

点击**清除设备的报警信息**，清除所选设备上的所有报警信息。

点击**清空所有过滤**，清除当前设置的过滤条件。

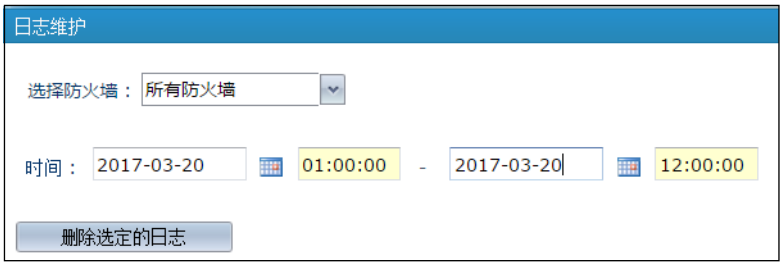
第8章 日志

NCSS 系统自身可以生成日志并且能够收集被管理虚拟防火墙的日志信息。本章包括如下内容：

8.1. 日志维护

管理员可以查看并删除 NCSS 的日志和虚拟防火墙的日志。

1. 选择**日志 > 日志维护**。
2. 在**选择防火墙**下拉列表中，选择 NCSS 或虚拟防火墙。
3. 指定要删除日志的时间范围。可以手动输入日期或者点击 选择日期。如果不指定时间，则删除所有日志。
4. 点击**删除选定的日志**。

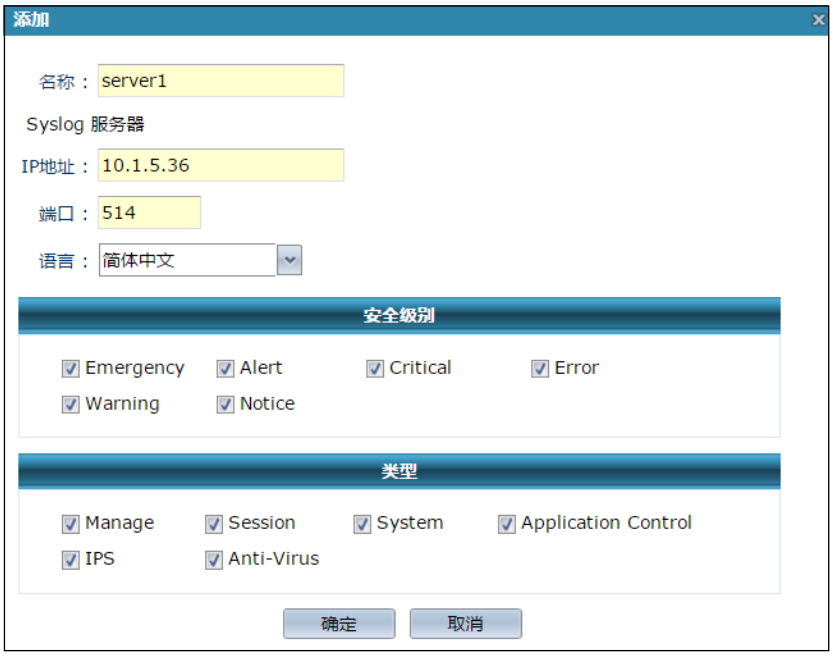


8.2. Syslog 配置

管理员可以在 NCSS 上添加 Syslog 服务器，NCSS 能够将日志信息发送到指定的 Syslog 服务器上。

8.2.1. 添加 Syslog 服务器

1. 选择**日志 >Syslog 配置**。
2. 点击**添加**，添加 Syslog 服务器。

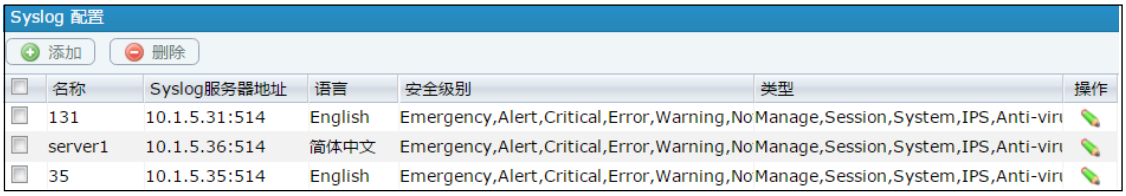


- 名称：Syslog 服务器名称。
- IP 地址：Syslog 服务器 IP 地址。
- 端口：Syslog 服务器端口。
- 语言：日志输出语言，简体中文或英语。
- 安全级别：日志输出事件的安全级别。
- 类型：日志的来源类型。

3. 点击**确定**。

8.2.2. 编辑/删除 Syslog 服务器

4. 选择**日志**>**Syslog 配置**。



5. 在 **Syslog 配置**列表中：

   - 双击某个条目或者点击条目对应的，对其进行编辑。
   - 勾选**名称**左侧的复选框选中所有服务器，或者勾选条目对应的复选框选中一个或多个条目，点击**删除**。在弹出的对话框中点击**确定**，删除服务器。

8.3.NCSS 日志

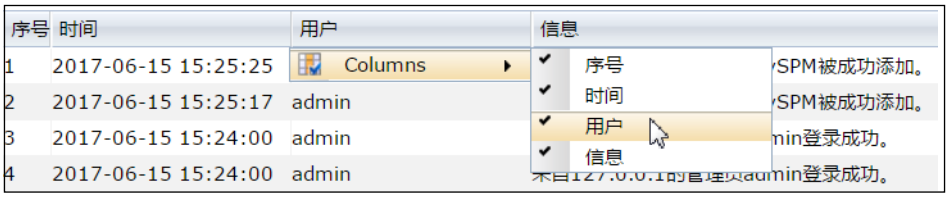
NCSS 日志记录的是管理员在 NCSS 系统上进行管理操作引发的事件。管理员可以进行如下操作：

8.3.1. 查看日志

1. 选择**日志 >NCSS 日志**。查看 NCSS 日志信息。

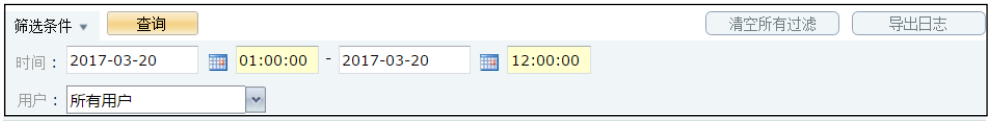
   - 序号：日志的编号。最新生成的日志排在列表最上端。
   - 时间：日志记录的 NCSS 事件发生的时间。格式为：YYYY-MM-DD HH:MM:SS。
   - 用户：触发 NCSS 日志事件产生的管理员。
   - 信息：NCSS 日志的实际内容。

2. 如果要隐藏列表中的某个字段信息，单击参数字段右侧向下箭头，在出现的 **Columns** 下拉表中，取消勾选要隐藏的字段，如**用户**。



8.3.2. 筛选日志

1. 选择**日志 >NCSS 日志**。
2. 点击**筛选条件**，设置一项或多项日志筛选条件。
   a) 设置日期和时间范围。可以手动输入日期或者点击 选择日期。
   b) 选择一个用户或所有用户。
3. 点击**查询**。如果要取消所有过滤设置，点击**清空所有过滤**。



8.3.3. 导出日志

最多能够导出最新的 2 万条日志。

1. 选择**日志 >NCSS 日志**。
2. 点击**导出日志**。

8.4.防火墙日志

防火墙日志记录的是在被管理虚拟防火墙上产生的安全事件。

8.4.1. 系统日志

系统日志记录的是在被管理虚拟防火墙上产生的与系统相关的事件。

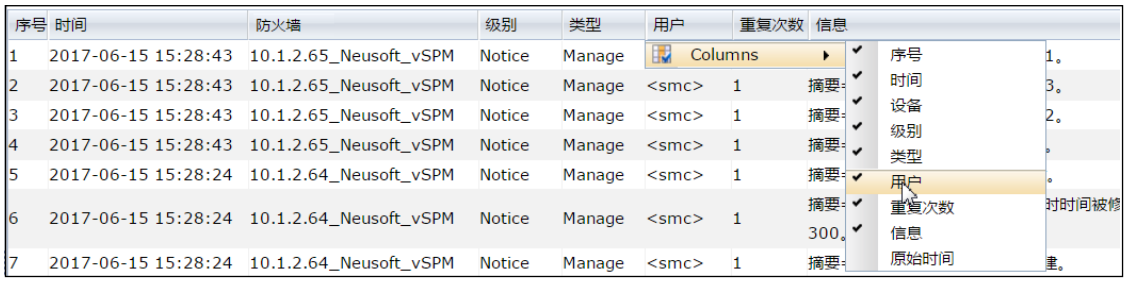
8.4.1.1.查看日志

1. 选择**日志>防火墙日志>系统日志**。
2. 查看被管理虚拟防火墙的日志信息。

序号	时间	防火墙	级别	类型	用户	重复次数	信息
1	2017-04-16 16:45:35	10.1.2.67_Neusoft_NISGVA	Warnning	System	N/A	1	摘要=在上一个小时内，通过SMTP发送了0封邮件，通过IMAP接收了0封邮件，通过POP3接收了0封邮件。
2	2017-04-16 16:32:00	10.1.2.65_Neusoft_NISGVA	Warnning	System	N/A	1	摘要=在上一个小时内，通过SMTP发送了0封邮件，通过IMAP接收了0封邮件，通过POP3接收了0封邮件。
3	2017-04-16 16:31:57	10.1.2.64_Neusoft_NISGVA	Warnning	System	N/A	1	摘要=在上一个小时内，通过SMTP发送了0封邮件，通过IMAP接收了0封邮件，通过POP3接收了0封邮件。

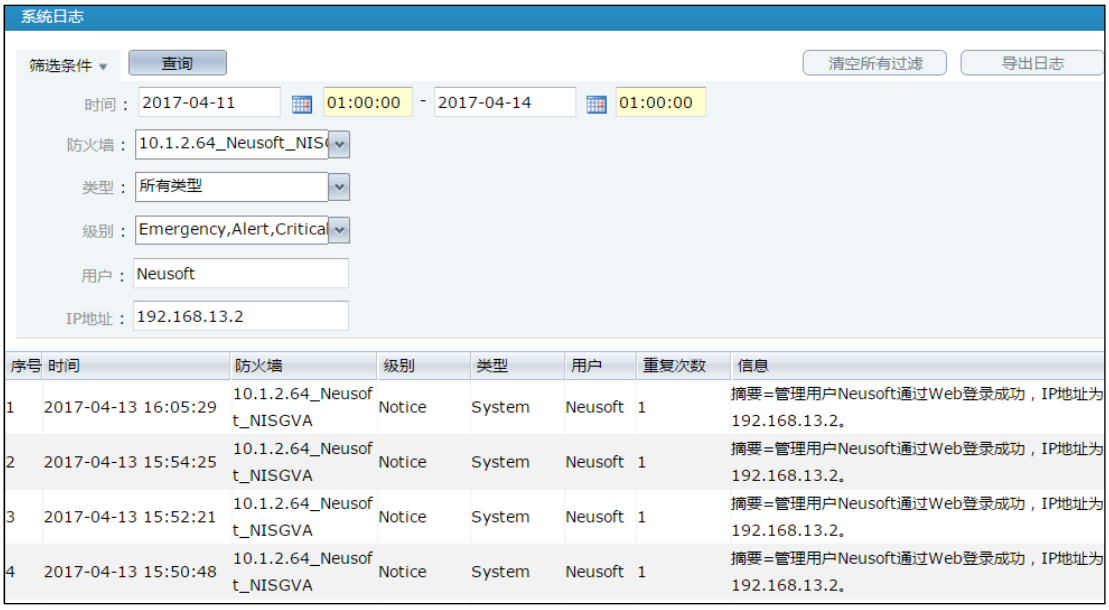
- 序号：日志的编号。最新生成的日志排在列表最上端。
- 时间：NCSS 接收到系统日志的时间。
- 防火墙：生成系统日志的虚拟防火墙。
- 级别：系统日志的安全等级，包括 Emergency、Alert、Critical、Error、Waring、和 Notice。
- 类型：产生系统日志的模块类型。
- 用户：触发系统日志产生的用户。
- 重复次数：系统日志重复出现的次数。
- 信息：系统日志的实际内容。
- 原始时间：在被管理虚拟防火墙上生成日志的时间。

3. 如果要隐藏列表中的某个字段信息，单击参数字段右侧向下箭头，在出现的 **Columns** 下拉表中，取消勾选要隐藏的字段，如**用户**。



8.4.1.2.筛选日志

1. 选择**日志>防火墙日志>系统日志**。
2. 点击**筛选条件**，设置一项或多项日志筛选条件。



a) 设置日期和时间范围。可以手动输入日期或者点击 选择日期。

b) 选择被管理的虚拟防火墙。

c) 选择日志类型和级别。

d) 填写被管理虚拟防火墙的用户名称和 IP 地址。

3. 点击**查询**。如果要取消所有过滤设置，点击**清空所有过滤**。

8.4.1.3.导出日志

1. 选择**日志>防火墙日志>系统日志**。
2. 点击**导出日志**。

8.4.2. 防病毒日志

防病毒日志记录的是在被管理虚拟防火墙上产生的与防病毒相关的事件。

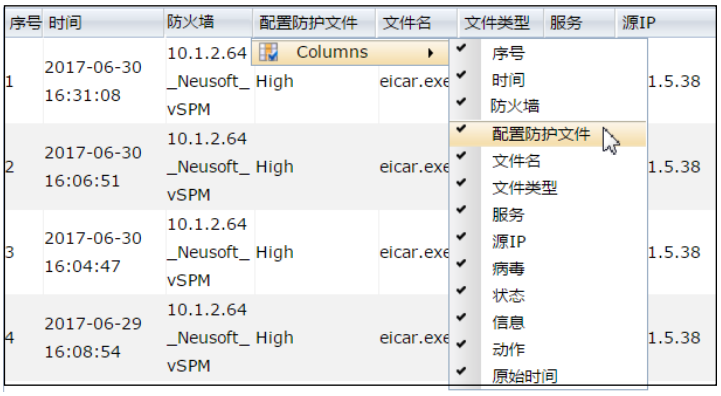
8.4.2.1.查看日志

1. 选择**日志>防火墙日志>防病毒日志**。
2. 查看被管理虚拟防火墙的日志信息。

序号	时间	防火墙	配置防护文件	文件名	文件类型	服务	源IP	病毒	状态	信息	动作	原始时间
1	2017-06-30 16:31:08	10.1.2.64_Neusoft_vSPM	High	eicar.exe	Unknown	HTTP	10.1.5.38	Eicar-Test-Signature.UNOFFICIAL	Virus_Signature_Scan	摘要=文件被病毒感染。	阻断	2017-06-30 16:30:54
2	2017-06-30 16:06:51	10.1.2.64_Neusoft_vSPM	High	eicar.exe	Unknown	HTTP	10.1.5.38	Eicar-Test-Signature.UNOFFICIAL	Virus_Signature_Scan	摘要=文件被病毒感染。	阻断	2017-06-30 16:06:24
3	2017-06-30 16:04:47	10.1.2.64_Neusoft_vSPM	High	eicar.exe	Unknown	HTTP	10.1.5.38	Eicar-Test-Signature.UNOFFICIAL	Virus_Signature_Scan	摘要=文件被病毒感染。	阻断	2017-06-30 16:04:21
4	2017-06-29 16:08:54	10.1.2.64_Neusoft_vSPM	High	eicar.exe	Unknown	HTTP	10.1.5.38	Eicar-Test-Signature.UNOFFICIAL	Virus_Signature_Scan	摘要=文件被病毒感染。	阻断	2017-06-29 16:08:22

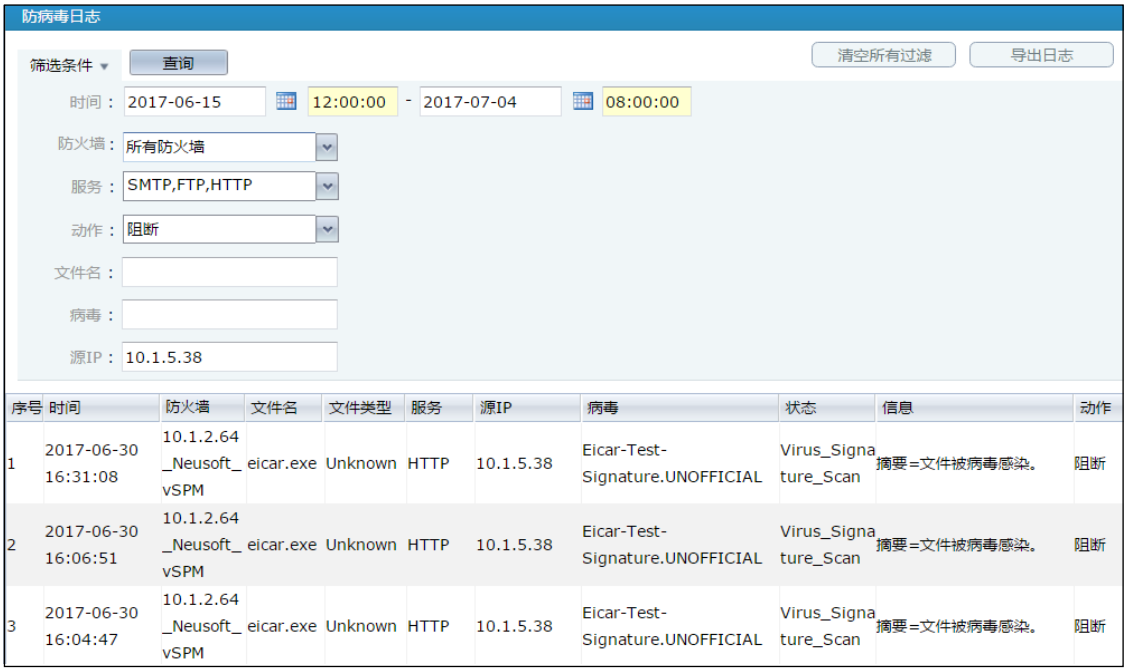
- 序号：日志的编号。最新生成的日志排在列表最上端。
- 时间：NCSS 接收到虚拟防火墙防病毒日志的时间。
- 防火墙：生成日志的虚拟防火墙。
- 配置防护：文件匹配的防病毒策略所引用的防护配置。
- 文件名：检测出病毒的文件的名称。
- 文件类型：文件的类型。
- 服务：文件传输的类型。
- 源 IP：文件发送的源 IP 地址。
- 病毒：检测到的病毒的名称。
- 状态：文件被认定为病毒的原因。
- 信息：日志的实际内容。
- 动作：对文件的处理动作，包括**阻断**和**放行**。
- 原始时间：在被管理虚拟防火墙上生成日志的时间。

3. 如果要隐藏列表中的某个字段信息，单击参数字段右侧向下箭头，在出现的 **Columns** 下拉表中，取消勾选要隐藏的字段，如**配置防护文件**。



8.4.2.2.筛选日志

1. 选择**日志>防火墙日志>防病毒日志**。
2. 点击**筛选条件**，设置一项或多项日志筛选条件。



a) 设置日期和时间范围。可以手动输入日期或者点击 选择日期。

b) 选择被管理的虚拟防火墙。

c) 选择服务类型。

d) 选择对文件的处理动作。

e) 填写文件的名称。

f) 填写病毒的名称。

g) 填写文件发送的源 IP 地址。

3. 点击**查询**。如果要取消所有过滤设置，点击**清空所有过滤**。

8.4.2.3.导出日志

1. 选择**日志>防火墙日志>防病毒日志**。
2. 点击**导出日志**。

8.4.3. IPS 日志

IPS 日志记录的是在被管理虚拟防火墙上产生的与 IPS 相关的事件。

8.4.3.1.查看日志

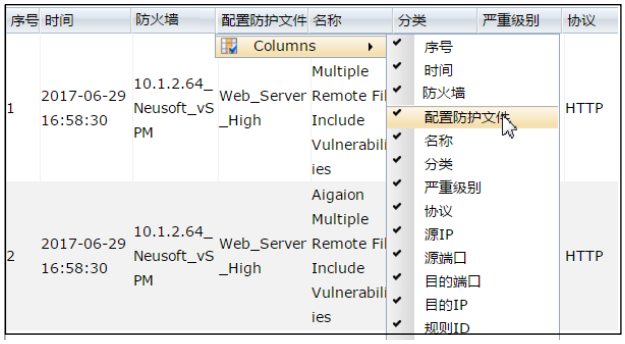
1. 选择**日志>防火墙日志>IPS 日志**。
2. 查看被管理虚拟防火墙的日志信息。

序号	时间	防火墙	名称	分类	严重级别	协议	源IP	源端口	目的端口	目的IP	规则ID	信息	动作
1	2017-06-29 16:58:30	10.1.2.64_N eusoft_vSPM	Aigaion Multiple Remote File Include Vulnerabilities	INPUT VALIDATE FAILED	高	HTTP	0.0.0.0	8233	80	10.1.5.40	21876	摘要=系统检测到攻击。	阻断
2	2017-06-29 16:58:30	10.1.2.64_N eusoft_vSPM	Aigaion Multiple Remote File Include Vulnerabilities	INPUT VALIDATE FAILED	高	HTTP	0.0.0.0	8233	80	10.1.5.40	21876	摘要=系统检测到攻击。	阻断

- 序号：日志的编号。最新生成的日志排在列表最上端。
- 时间：NCSS 接收到 IPS 日志的时间。
- 防火墙：被检测到 IPS 攻击事件的虚拟防火墙。
- 配置防护：IPS 攻击匹配的攻击签名规则所引用的防护配置。缺省不显示。
- 名称：攻击匹配的攻击签名规则集名称。
- 分类：攻击匹配的攻击签名规则类别。
- 严重级别：攻击的严重程度，包括**高**、**中**、**低**和**警示信息**。
- 协议：匹配攻击签名规则的应用层协议。
- 源 IP：发起攻击的源 IP 地址。
- 源端口：发起攻击的源端口。
- 目的端口：攻击目标的端口。

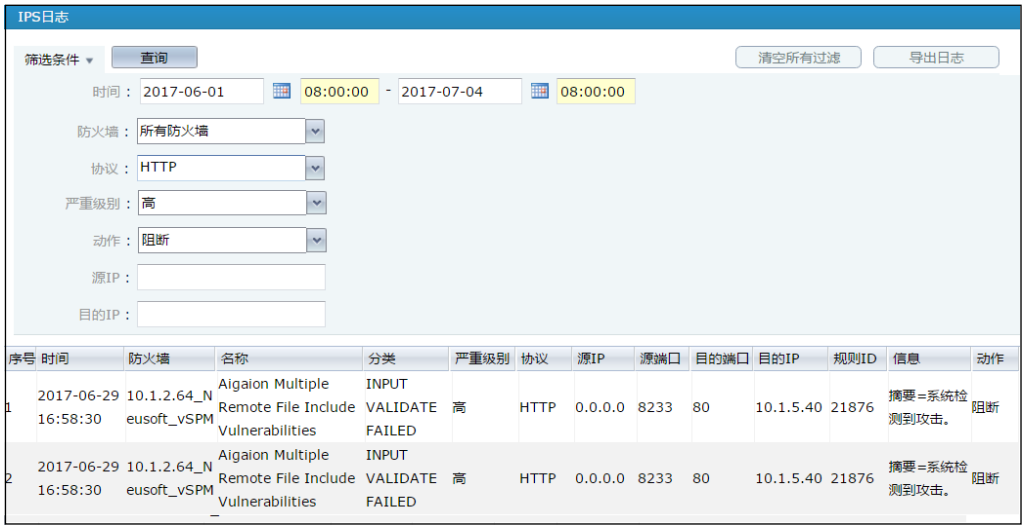
- 目的 IP：攻击的目标 IP 地址。
- 规则 ID：攻击匹配的攻击签名规则的标识。
- 信息：日志记录的事件的实际内容。
- 动作：对匹配攻击行为的数据包处理所执行的动作，包括**放行**和**阻断**。
- 原始时间：在被管理虚拟防火墙上检测出 IPS 攻击的时间。缺省不显示。

3. 如果要隐藏列表中的某个字段信息，单击参数字段，在出现的 **Columns** 下拉表中，取消勾选要隐藏的字段，如**配置防护文件**。



8.4.3.2.筛选日志

1. 选择**日志>防火墙日志>IPS 日志**。
2. 点击**筛选条件**，设置一项或多项日志筛选条件。



a) 设置日期和时间范围。可以手动输入日期或者点击 选择日期。
b) 选择被管理的虚拟防火墙。
c) 选择匹配攻击签名规则的应用层协议。
d) 选择攻击的严重程度。
e) 选择对匹配攻击行为的数据包处理所执行的动作。
f) 填写发起攻击的源 IP 地址。

g) 填写攻击目标的 IP 地址。

3. 点击**查询**。如果要取消所有过滤设置，点击**清空所有过滤**。

8.4.3.3.导出日志

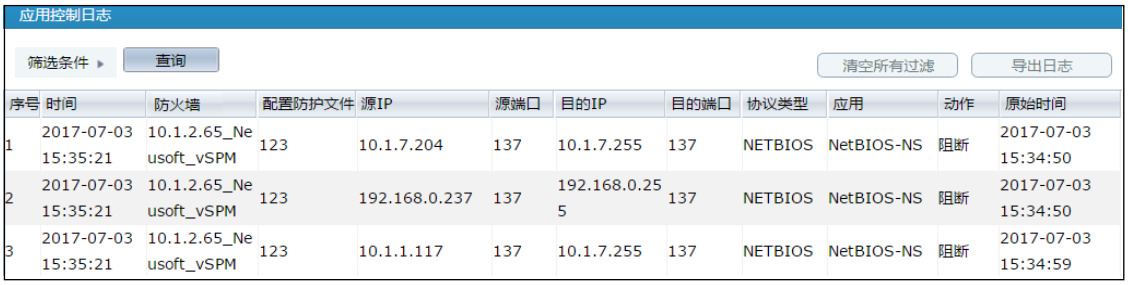
1. 选择**日志>防火墙日志>IPS 日志**。
2. 点击**导出日志**。

8.4.4. 应用控制日志

应用控制日志记录的是在被管理虚拟防火墙上产生的与应用控制相关的事件。

8.4.4.1.查看日志

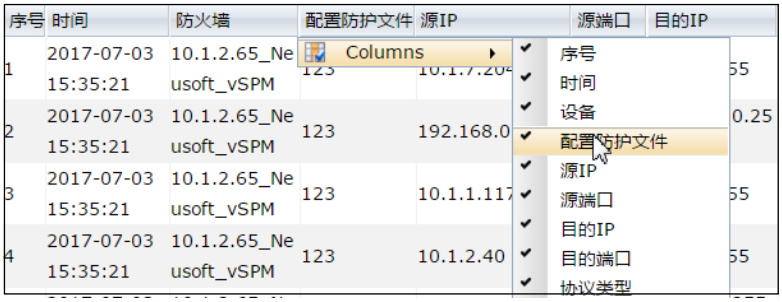
1. 选择**日志>防火墙日志>应用控制日志**。
2. 查看被管理虚拟防火墙的日志信息。



序号	时间	防火墙	配置防护文件	源IP	源端口	目的IP	目的端口	协议类型	应用	动作	原始时间
1	2017-07-03 15:35:21	10.1.2.65_Nesoft_vSPM	123	10.1.7.204	137	10.1.7.255	137	NETBIOS	NetBIOS-NS	阻断	2017-07-03 15:34:50
2	2017-07-03 15:35:21	10.1.2.65_Nesoft_vSPM	123	192.168.0.237	137	192.168.0.255	137	NETBIOS	NetBIOS-NS	阻断	2017-07-03 15:34:50
3	2017-07-03 15:35:21	10.1.2.65_Nesoft_vSPM	123	10.1.1.117	137	10.1.7.255	137	NETBIOS	NetBIOS-NS	阻断	2017-07-03 15:34:59

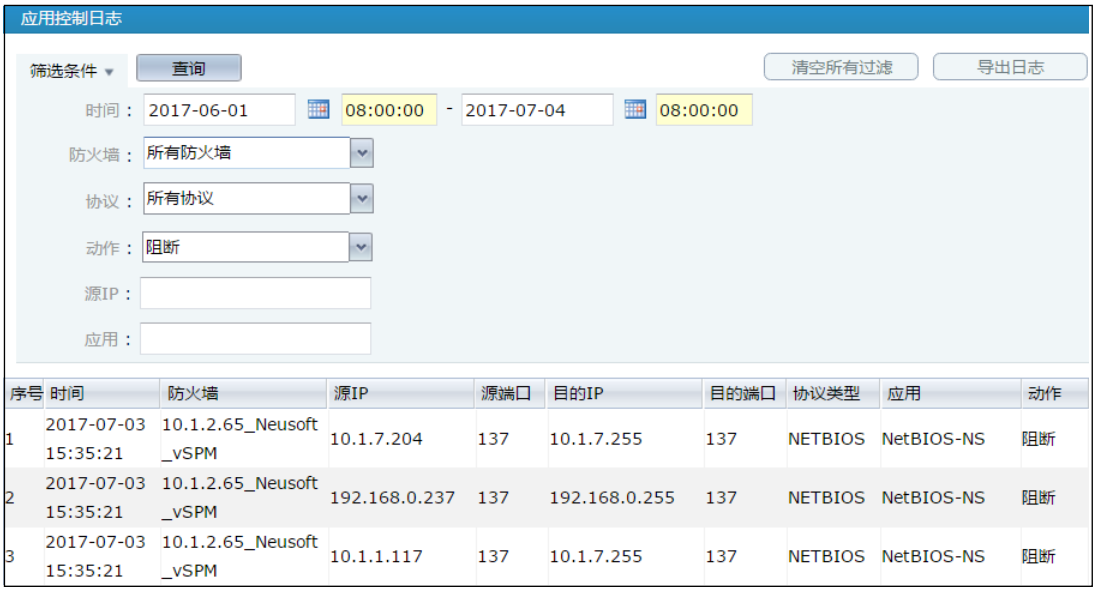
- 序号：日志的编号。最新生成的日志排在列表最上端。
- 时间：NCSS 接收到应用控制日志的时间。
- 防火墙：生成应用控制日志的虚拟防火墙。
- 配置防护：应用请求匹配的应用控制策略所引用的防护配置。缺省不显示。
- 源 IP：匹配应用控制规则的应用的源 IP 地址。
- 源端口：匹配应用控制规则的应用的源端口。
- 目的 IP：匹配应用控制规则的应用的目的 IP 地址。
- 目的端口：匹配应用控制规则的应用的目的端口。
- 协议类型：匹配应用控制规则的应用使用的协议类型。
- 应用：匹配应用控制规则的应用名称。
- 动作：对匹配应用控制规则的应用的处理动作，包括**放行**和**阻断**。
- 原始时间：在被管理虚拟防火墙上生成应用控制日志的时间。缺省不显示。

3. 如果要隐藏列表中的某个字段信息，单击参数字段右侧的向下箭头，在出现的 **Columns** 下拉表中，取消勾选要隐藏的字段，如**配置防护文件**。



8.4.4.2.筛选日志

1. 选择**日志>防火墙日志>应用控制日志**。
2. 点击**筛选条件**，设置一项或多项日志筛选条件。



a) 设置日期和时间范围。可以手动输入日期或者点击 选择日期。

b) 选择被管理的虚拟防火墙。

c) 选择匹配应用控制规则的应用使用的协议类型。

d) 选择对匹配应用控制规则的应用的处理动作，包括**放行**和**阻断**。

e) 填写匹配应用控制规则的应用的源 IP 地址。

f) 填写匹配应用控制规则的应用名称。

3. 点击**查询**。如果要取消所有过滤设置，点击**清空所有过滤**。

8.4.4.3.导出日志

1. 选择**日志 >防火墙日志>应用控制日志**。
2. 点击**导出日志**。

第9章 报表

NCSS 的报表功能是基于 WebUI 的一种应用，可以定期生成关于以下主题的统计信息并以图表的形式显示出来：系统、流量、防病毒、攻击、应用和用户。

NCSS 报表有标准的格式，包括封面、目录以及数据三部分，其中数据是以图表的形式呈现的。生成的报表可供下载并保存到本地或者根据需要通过邮件发送给指定的用户。

本章包括如下内容：

9.1. 常规设置

常规设置应用于所有的报表中。

1. 选择**报表>常规设置**。

2. 在**主题**文本框中，输入邮件的主题信息，不可以输入?\'。
3. 设置报表标识。
   - 点击**使用默认标识**，使用 NCSS 提供的缺省标识。
   - 点击**导入**，点击**上传**，上传其他标识。请根据 WebUI 提示导入合适的图片。
4. 点击**确定**。

9.2.任务

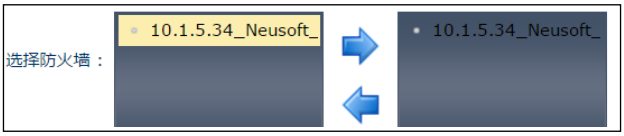
NCSS 可以根据不同的需要生成报表，其中包括报表标题、显示语言、报表格式、被监控的虚拟防火墙、报表内容、报表生成频率以及接收人清单。

9.2.1. 添加报表任务

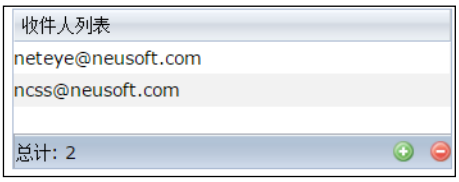
1. 选择**报表>任务**。
2. 点击**添加**，添加报表任务。

- 报表标题：长度 1～63 字节，UTF-8 字符。
- 描述：长度 0～255 个字节，UTF-8 字符。不能包含以下字符：?"'\<>& 。
- 语言：报表以何种语言显示出来。NCSS 支持英文（缺省）和简体中文。
- 格式：报表的输出格式。NCSS 支持 PDF（缺省）和 HTML 两种格式。
- 立即生成报表：在当前系统时间立即生成报表。
  - 日报：统计最近一天产生的数据信息。
  - 周报：统计最近一周产生的数据信息。
  - 月报：统计最近一个月产生的数据信息。
- 按计划时间生成报表：根据设置的时间自动生成报表。

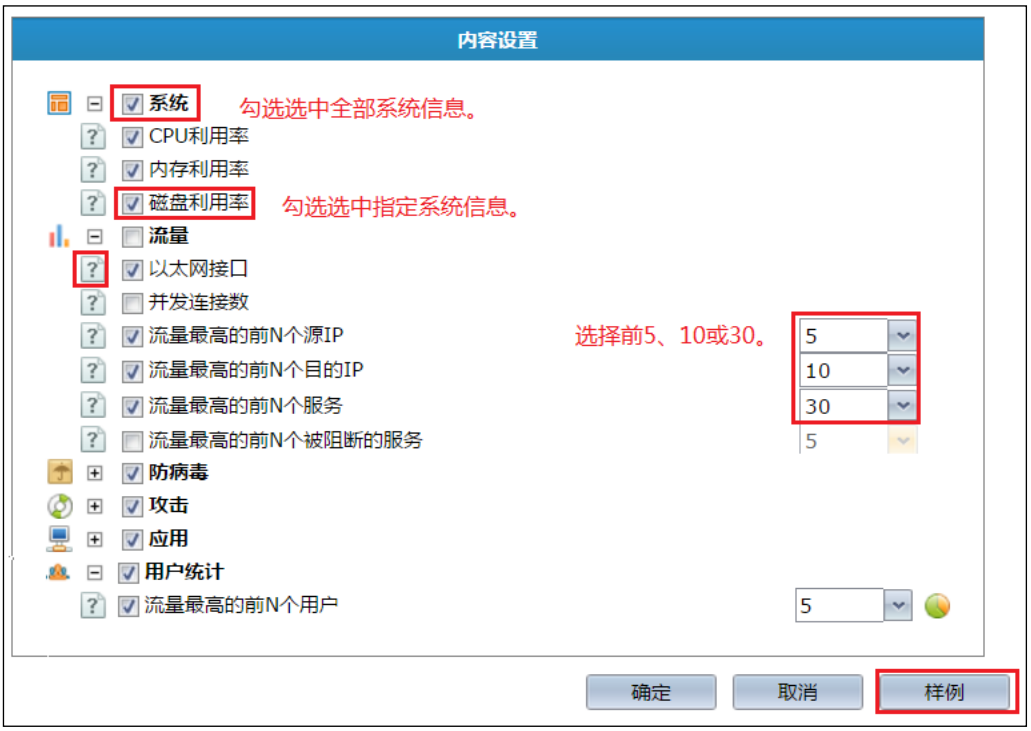
3. 从左侧的列表框中选择需要生成报表的虚拟防火墙，点击 。



4. 在**收件人列表**中，点击 ，添加收件人的 e-mail 地址（最多 32 个）。如需删除收件人地址，选择相应的条目，点击 将其从列表中删除。

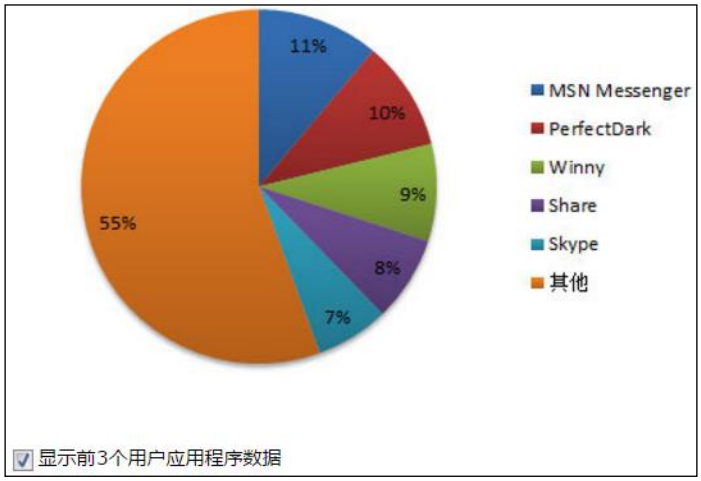


5. 选择报表生成的内容，包括系统、流量、防病毒、攻击、应用和用户统计。



- 点击 图标，查看相应的报表统计信息的示例图。点击页面底部的**样例**按钮查看报表样例。

- 对于用户统计信息，如需额外为用户显示前 3 个用户的前 5 个应用信息，点击 ，在弹出的窗口中，勾选**显示前 3 个用户应用统计**复选框。然后点击**确定**。



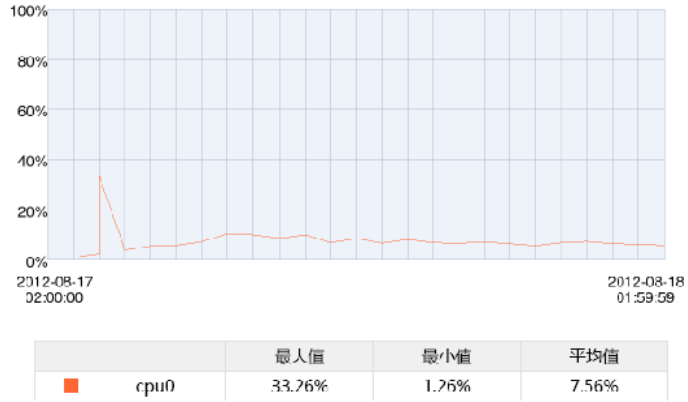
6. 点击**确定**。

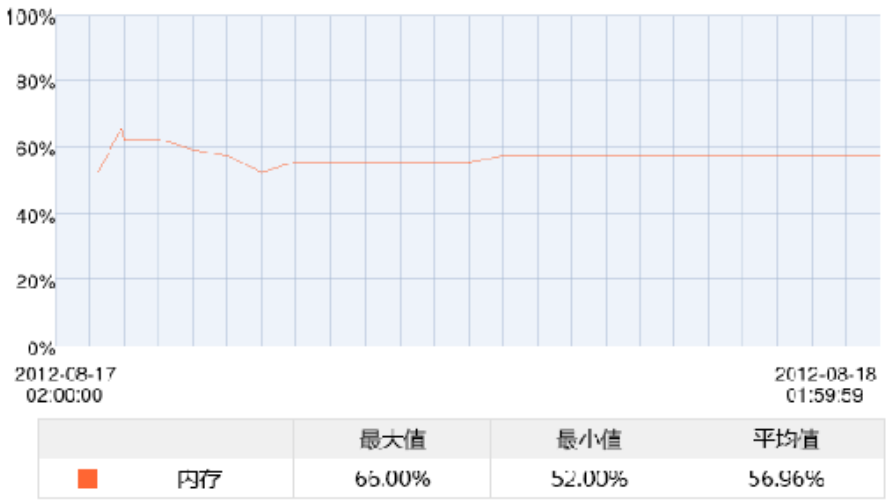
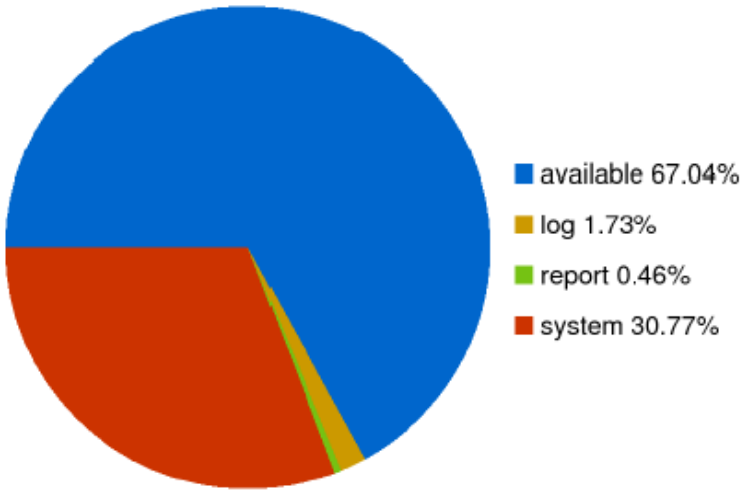
以下为详细的报表信息及其样例：

9.2.1.1.系统

错误!未找到引用源。给出系统信息类型及示例图：

表 1——系统信息

类型	**描述**
CPU 利用率	NCSS 每 5 分钟统计一次 CPU 利用率并显示平均值。如果系统有多个内核或多个 CPU，那么每个核或 CPU 会单独显示。  图中纵坐标为 CPU 利用率百分比。 图中绘制图的点为 5 分钟内的均值。

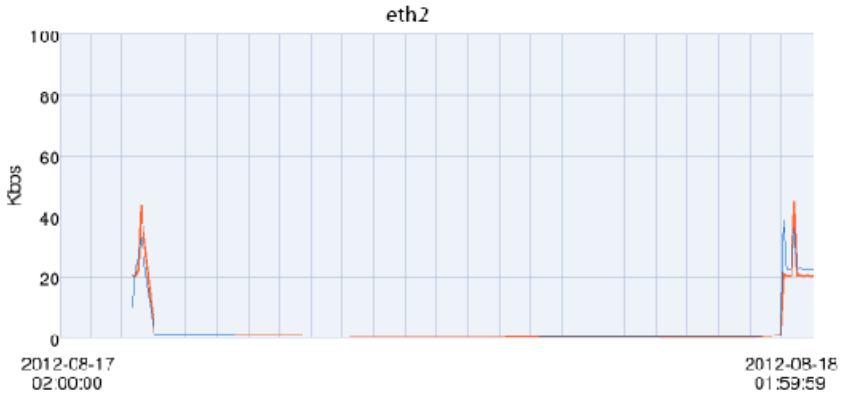
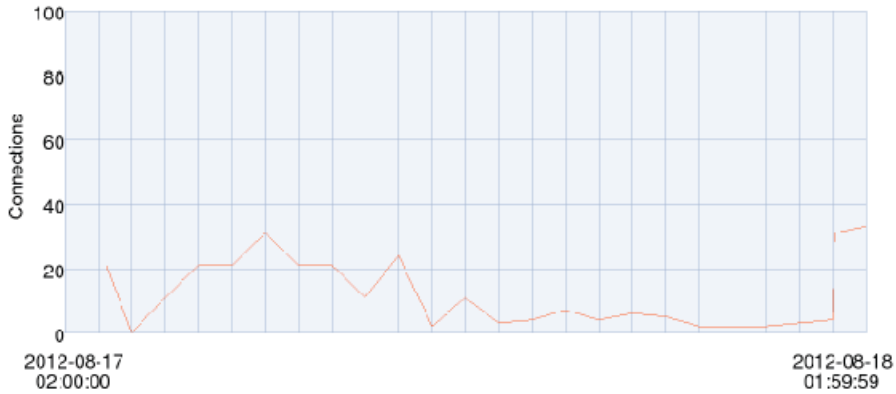
内存利用率	NCSS 每 5 分钟统计一次系统内存利用率并显示平均值。  最大值 最小值 平均值 内存 65.00% 52.00% 56.96% 图中纵坐标为内存利用率百分比。 图中绘制图的点为 5 分钟内的均值。
磁盘利用率	NCSS 统计生成报表时的磁盘使用情况。 

9.2.1.2.流量统计

错误!未找到引用源。给出流量信息类型及示例图:

表 2——流量信息

类型	**描述**

以太网接口	NCSS 每 5 分钟统计一次入口和出口以太网接口的流量信息。  最大值 最小值 平均值 入口 44.91Kbps 0.06Kbps 19.76Kbps 出口 38.55Kbps 0.14Kbps 20.76Kbps 图中绘制图的点为 5 分钟内的均值。
并发连接数	NCSS 每 5 分钟统计一次并发连接总数。  最大值 最小值 平均值 连接数 33.00 0.00 12.04 图中绘制图的点为 5 分钟内的总值。
流量最高的前 N 个源 IP	NCSS 统计流量最高的前 N 个源 IP 地址的信息。 序列 源IP地址 流量(KB) 百分比 1 192.168.111.2 1902 8.34% 2 192.168.111.3 1706 7.48% 3 192.168.111.4 1560 6.84% 4 192.168.111.5 1329 5.83% 5 192.168.111.6 1290 5.66% 说明： ▪ 流量（KB）：来自某一特定源 IP 地址的总流量。

	▪ 百分比：来自某一特定源 IP 地址的总流量占系统总流量的比例。
流量最高的前 N 个目的 IP	NCSS 统计流量最高的前 N 个目的 IP 地址的信息。 序列 | 目地IP地址 | 流量(KB) | 百分比 1 | 192.168.101.2 | 1902 | 8.34% 2 | 192.168.101.3 | 1706 | 7.48% 3 | 192.168.101.4 | 1560 | 6.84% 4 | 192.168.101.5 | 1329 | 5.83% 5 | 192.168.101.6 | 1290 | 5.66% 说明： ▪ 流量（KB）：发往某一特定目的 IP 地址的总流量。 ▪ 百分比：发往某一特定目的 IP 地址的总流量占系统总流量的比例。
流量最高的前 N 个服务	NCSS 统计流量最高的前 N 种服务的信息。 序列 | 端口 | 服务名称 | 流量(KB) | 百分比 1 | UDP:12 | UDP_ANY | 1840 | 8.07% 2 | TCP:13 | TCP_ANY | 1577 | 6.91% 3 | UDP:14 | UDP_ANY | 1376 | 6.03% 4 | TCP:15 | TCP_ANY | 1157 | 5.07% 5 | UDP:16 | UDP_ANY | 1104 | 4.84% 说明： ▪ 端口：目的端口号。如果无端口则显示协议号，如 Other：44。 ▪ 服务名称：使用特定目的端口的服务对象的名称。 ▪ 流量（KB）：发往某一特定目的端口的总流量。 ▪ 百分比：发往某一特定目的端口的总流量占系统总流量的比例。

流量最高的前 N 个被阻断的服务	NCSS 统计被访问策略阻断次数最多的前 N 个服务。 序列 | 端口 | 服务 | 阻断次数 | 百分比 1 | OTHER:1231 | | 23 | 10.95% 2 | OTHER:1232 | | 19 | 9.05% 3 | OTHER:1235 | | 16 | 7.62% 4 | OTHER:1240 | | 12 | 5.71% 5 | OTHER:1247 | | 11 | 5.24% 说明： ▪ 阻断次数：某一特定目的端口被访问策略阻断的总次数。 ▪ 百分比：某一特定目的端口被访问策略阻断的总次数占所有端口被访问策略阻断的总次数的比例。

9.2.1.3.防病毒

错误!未找到引用源。给出防病毒信息类型及示例图：

表 3——防病毒信息

类型	**描述**
被检测到的前 N 个病毒	被检测出次数最多的前 N 个病毒的信息。 序列 | 病毒名称 | 检测到的病毒数量 | 百分比 1 | Eicar-Signature_1.UNOFFICIAL | 23 | 10.09% 2 | Eicar-Signature_2.UNOFFICIAL | 19 | 8.33% 3 | Eicar-Signature_3.UNOFFICIAL | 17 | 7.46% 4 | Eicar-Signature_4.UNOFFICIAL | 14 | 6.14% 5 | Eicar-Signature_5.UNOFFICIAL | 13 | 5.70% 说明： ▪ 检测到的病毒数量：某一特定病毒被检测出的总次数。 ▪ 百分比：在某一特定病毒被检测出的总次数占检测出病毒总次数的比例。

<table>
<tr><td>被检测到的前 N 种病毒文件类型</td><td>被检测出病毒次数最多的前 N 种文件类型的信息。

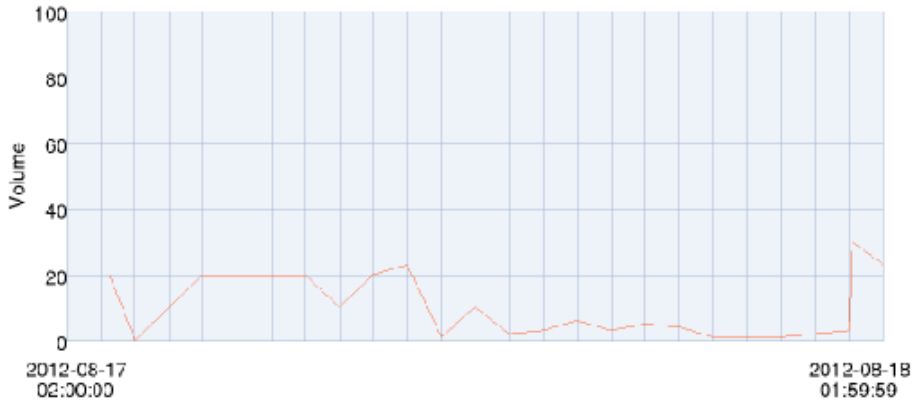
<table>
<tr><th>序列</th><th>文件类型</th><th>检测到的病毒数量</th><th colspan="2">百分比</th></tr>
<tr><td>1</td><td>rar</td><td>50</td><td></td><td>21.93%</td></tr>
<tr><td>2</td><td>zip</td><td>46</td><td></td><td>20.18%</td></tr>
<tr><td>3</td><td>txt</td><td>38</td><td></td><td>16.67%</td></tr>
<tr><td>4</td><td>dat</td><td>35</td><td></td><td>15.35%</td></tr>
<tr><td>5</td><td>jpg</td><td>31</td><td></td><td>13.60%</td></tr>
</table>
</td></tr>
<tr><td>被检测到病毒最多的前 N 个服务器</td><td>被服务器保护检测出病毒次数最多的前 N 个服务器的信息。

<table>
<tr><th>序列</th><th>服务器IP/域名</th><th>服务器类型</th><th>检测到的病毒数量</th><th colspan="2">百分比</th></tr>
<tr><td>1</td><td>hmail_2.com</td><td>POP3</td><td>21</td><td></td><td>19.27%</td></tr>
<tr><td>2</td><td>hmail_0.com</td><td>HTTP</td><td>14</td><td></td><td>12.84%</td></tr>
<tr><td>3</td><td>hmail_2.com</td><td>SMTP</td><td>12</td><td></td><td>11.01%</td></tr>
<tr><td>4</td><td>hmail_2.com</td><td>FTP</td><td>11</td><td></td><td>10.09%</td></tr>
<tr><td>5</td><td>hmail_0.com</td><td>IMAP</td><td>11</td><td></td><td>10.09%</td></tr>
</table>

说明：
▪ 检测到的病毒数量：某一特定服务器被服务器保护检测出病毒的总次数。
▪ 百分比：某一特定服务器被服务器保护检测出病毒的总次数占服务器保护检测出病毒的总次数的比例。</td></tr>
<tr><td>被检测到病毒最多的前 N 个客户端</td><td>被客户端保护检测出病毒次数最多的前 N 个客户端的信息。

<table>
<tr><th>序列</th><th>客户端IP</th><th>检测到的病毒数量</th><th colspan="2">百分比</th></tr>
<tr><td>1</td><td>192.1.2.2</td><td>33</td><td></td><td>27.73%</td></tr>
<tr><td>2</td><td>192.1.2.4</td><td>27</td><td></td><td>22.69%</td></tr>
<tr><td>3</td><td>192.1.2.6</td><td>21</td><td></td><td>17.65%</td></tr>
<tr><td>4</td><td>192.1.2.10</td><td>19</td><td></td><td>15.97%</td></tr>
<tr><td>5</td><td>192.1.2.8</td><td>19</td><td></td><td>15.97%</td></tr>
</table>

说明：
▪ 检测到的病毒数量：某一特定客户端被客户端保护检测出病毒的总次数。
▪ 百分比：某一特定客户端被客户端保护检测出病毒的总次数占客户端保护检测出病毒的总次数的比例。</td></tr>
</table>

<table>
<tr><td>在邮件中被检测到的前 N 个病毒</td><td>在邮件中被检测到次数最多的前 N 个病毒的信息。
<table><tr><th>序列</th><th>病毒名称</th><th>检测到的病毒数量</th><th colspan="2">百分比</th></tr><tr><td>1</td><td>Eicar-Signature_1.UNOFFICIAL</td><td>23</td><td></td><td>15.65%</td></tr><tr><td>2</td><td>Eicar-Signature_2.UNOFFICIAL</td><td>19</td><td></td><td>12.93%</td></tr><tr><td>3</td><td>Eicar-Signature_3.UNOFFICIAL</td><td>17</td><td></td><td>11.56%</td></tr><tr><td>4</td><td>Eicar-Signature_6.UNOFFICIAL</td><td>12</td><td></td><td>8.16%</td></tr><tr><td>5</td><td>Eicar-Signature_7.UNOFFICIAL</td><td>11</td><td></td><td>7.48%</td></tr></table></td></tr>
<tr><td>在 Web 页面中被检测到的前 N 个病毒</td><td>在 Web 页面中被检测到次数最多的前 N 个病毒的信息。
<table><tr><th>序列</th><th>病毒名称</th><th>检测到的病毒数量</th><th colspan="2">百分比</th></tr><tr><td>1</td><td>Eicar-Signature_4.UNOFFICIAL</td><td>14</td><td></td><td>34.15%</td></tr><tr><td>2</td><td>Eicar-Signature_9.UNOFFICIAL</td><td>11</td><td></td><td>26.83%</td></tr><tr><td>3</td><td>Eicar-Signature_14.UNOFFICIAL</td><td>8</td><td></td><td>19.51%</td></tr><tr><td>4</td><td>Eicar-Signature_19.UNOFFICIAL</td><td>8</td><td></td><td>19.51%</td></tr></table></td></tr>
<tr><td>病毒事件统计</td><td>NCSS 每 5 分钟统计一次检测出的病毒的总数。
 

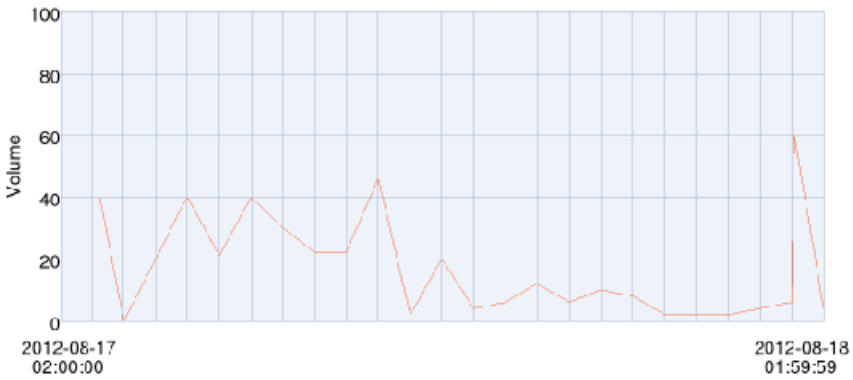
<table><tr><th></th><th>最大值</th><th>最小值</th><th>平均值</th></tr><tr><td>病毒数</td><td>30.00</td><td>0.00</td><td>10.32</td></tr></table>
图中纵坐标为检测出病毒的总次数。 图中绘制图的点为 5 分钟内的总次数。</td></tr>
<tr><td>被检测到病毒最多的前 N 个 Web 站点</td><td>被检测出病毒次数最多的前 N 个网站的信息。
<table><tr><th>序列</th><th>网站名称</th><th>检测到的病毒数量</th><th colspan="2">百分比</th></tr><tr><td>1</td><td>hmail_0.com</td><td>14</td><td></td><td>34.15%</td></tr><tr><td>2</td><td>hmail_1.com</td><td>11</td><td></td><td>26.83%</td></tr><tr><td>3</td><td>hmail_2.com</td><td>8</td><td></td><td>19.51%</td></tr><tr><td>4</td><td>hmail_3.com</td><td>8</td><td></td><td>19.51%</td></tr></table></td></tr>
</table>

<table>
<tr><td>被检测到病毒最多的前 N 个发件人</td><td>在邮件中检测出病毒次数最多的前 N 个发件人的信息。
<table><tr><th>序列</th><th>发件人</th><th>检测到的病毒数量</th><th colspan="2">百分比</th></tr><tr><td>3</td><td>bbbb_3@hmail_3.com</td><td>17</td><td>11.56%</td></tr><tr><td>4</td><td>bbbb_6@hmail_2.com</td><td>12</td><td>8.16%</td></tr><tr><td>5</td><td>bbbb_7@hmail_3.com</td><td>11</td><td>7.48%</td></tr></table></td></tr>
</table>

9.2.1.4.攻击

错误!未找到引用源。给出攻击信息类型及示例图:

表 4——攻击信息

<table>
<tr><th>类型</th><th>描述</th></tr>
<tr><td>攻击事件统计</td><td>NCSS 每 5 分钟统计一次攻击发生的总数。
 

<table><tr><th></th><th>最大值</th><th>最小值</th><th>平均值</th></tr><tr><td>攻击次数</td><td>60.00</td><td>0.00</td><td>17.16</td></tr></table>
图中纵坐标为攻击发生的总次数。 图中绘制图的点为 5 分钟内的总次数。</td></tr>
</table>

<table>
<tr><td>检测到攻击次数最多的前 N 个攻击者</td><td>被检测到攻击次数最多的前 N 个攻击者的信息。

<table>
<tr><th>序列</th><th>攻击者</th><th>检测到的攻击数量</th><th colspan="2">百分比</th></tr>
<tr><td>1</td><td>10.168.1.2</td><td>31</td><td></td><td>8.40%</td></tr>
<tr><td>2</td><td>192.169.3.2</td><td>29</td><td></td><td>7.86%</td></tr>
<tr><td>3</td><td>10.168.1.3</td><td>27</td><td></td><td>7.32%</td></tr>
<tr><td>4</td><td>192.169.2.3</td><td>24</td><td></td><td>6.50%</td></tr>
<tr><td>5</td><td>10.168.1.4</td><td>22</td><td></td><td>5.96%</td></tr>
</table>

说明：
▪ 攻击者：攻击者的 IP 地址。
▪ 检测到的攻击数量：某一特定攻击者发起攻击的总次数。
▪ 百分比：某一特定攻击者发起攻击的总次数占检测到攻击总次数的比例。</td></tr>
<tr><td>检测到攻击次数最多的前 N 个主机</td><td>被攻击次数最多的前 N 个主机的信息。

<table>
<tr><th>序列</th><th>受攻击主机</th><th>检测到的攻击数量</th><th colspan="2">百分比</th></tr>
<tr><td>1</td><td>10.2.1.2</td><td>31</td><td></td><td>8.40%</td></tr>
<tr><td>2</td><td>192.169.2.2</td><td>29</td><td></td><td>7.86%</td></tr>
<tr><td>3</td><td>10.2.1.3</td><td>27</td><td></td><td>7.32%</td></tr>
<tr><td>4</td><td>192.169.3.3</td><td>24</td><td></td><td>6.50%</td></tr>
<tr><td>5</td><td>10.2.1.4</td><td>22</td><td></td><td>5.96%</td></tr>
</table>
</td></tr>
<tr><td>检测到攻击次数最多的前 N 个服务</td><td>被攻击次数最多的前 N 个服务的信息。

<table>
<tr><th>序列</th><th>端口</th><th>服务</th><th>检测到的攻击数量</th><th colspan="2">百分比</th></tr>
<tr><td>1</td><td>TCP:280</td><td>TCP_ANY</td><td>23</td><td></td><td>8.42%</td></tr>
<tr><td>2</td><td>OTHER:1231</td><td></td><td>23</td><td></td><td>8.42%</td></tr>
<tr><td>3</td><td>OTHER:1232</td><td></td><td>19</td><td></td><td>6.96%</td></tr>
<tr><td>4</td><td>UDP:281</td><td>UDP_ANY</td><td>18</td><td></td><td>6.59%</td></tr>
<tr><td>5</td><td>OTHER:1235</td><td></td><td>15</td><td></td><td>5.49%</td></tr>
</table>

说明：
▪ 端口：目的端口号。如果无端口则显示协议号，如 Other：44。
▪ 服务：使用特定目的端口的服务对象的名称。</td></tr>
</table>

<table>
<tr>
<td>被 IPS 检测到次数最多的前 N 个攻击者</td>
<td>被 IPS 检测出发起攻击次数最多的前 N 个攻击者的信息。

<table>
<tr><th>序列</th><th>攻击者</th><th>检测到的攻击数量</th><th colspan="2">百分比</th></tr>
<tr><td>1</td><td>10.168.1.2</td><td>31</td><td>8.40%</td></tr>
<tr><td>2</td><td>192.169.3.2</td><td>29</td><td>7.86%</td></tr>
<tr><td>3</td><td>10.168.1.3</td><td>27</td><td>7.32%</td></tr>
<tr><td>4</td><td>192.169.2.3</td><td>24</td><td>6.50%</td></tr>
<tr><td>5</td><td>10.168.1.4</td><td>22</td><td>5.96%</td></tr>
</table>

说明：
▪ 检测到的攻击数量：IPS 检测出的某一特定攻击者发起攻击的总次数。
▪ 百分比：IPS 检测出的某一特定攻击者发起攻击的总次数占 IPS 检测到攻击总次数的比例。</td>
</tr>
<tr>
<td>被 IPS 检测到次数最多的前 N 个被攻击的主机</td>
<td>被 IPS 检测到被攻击次数最多的前 N 个主机的信息。

<table>
<tr><th>序列</th><th>受攻击主机</th><th>检测到的攻击数量</th><th colspan="2">百分比</th></tr>
<tr><td>1</td><td>192.169.2.2</td><td>29</td><td>16.29%</td></tr>
<tr><td>2</td><td>192.169.3.3</td><td>24</td><td>13.48%</td></tr>
<tr><td>3</td><td>192.169.2.4</td><td>21</td><td>11.80%</td></tr>
<tr><td>4</td><td>192.169.3.5</td><td>17</td><td>9.55%</td></tr>
<tr><td>5</td><td>192.169.2.6</td><td>16</td><td>8.99%</td></tr>
</table>
</td>
</tr>
<tr>
<td>被 IPS 检测到次数最多的前 N 个服务</td>
<td>被 IPS 检测到被攻击次数最多的前 N 个服务的信息。

<table>
<tr><th>序列</th><th>端口</th><th>服务</th><th>检测到的攻击数量</th><th colspan="2">百分比</th></tr>
<tr><td>1</td><td>TCP:280</td><td>TCP_ANY</td><td>23</td><td>28.05%</td></tr>
<tr><td>2</td><td>UDP:281</td><td>UDP_ANY</td><td>18</td><td>21.95%</td></tr>
<tr><td>3</td><td>TCP:285</td><td>TCP_ANY</td><td>10</td><td>12.20%</td></tr>
<tr><td>4</td><td>UDP:286</td><td>UDP_ANY</td><td>9</td><td>10.98%</td></tr>
<tr><td>5</td><td>TCP:290</td><td>TCP_ANY</td><td>5</td><td>6.10%</td></tr>
</table>
</td>
</tr>
<tr>
<td>被 IPS 检测到次数最多的前 N 个攻击类型</td>
<td>被 IPS 检测出发起攻击次数最多的前 N 个攻击类型的信息。

<table>
<tr><th>序列</th><th>攻击类型</th><th>检测到的攻击数量</th><th colspan="2">百分比</th></tr>
<tr><td>1</td><td>未知</td><td>104</td><td>58.43%</td></tr>
<tr><td>2</td><td>输入验证错误</td><td>44</td><td>24.72%</td></tr>
<tr><td>3</td><td>跨站脚本(CSS/XSS)</td><td>30</td><td>16.85%</td></tr>
</table>
</td>
</tr>
</table>

<table>
<tr><td>被 IPS 检测到次数最多的前 N 个客户端</td><td>客户端保护中 IPS 检测到被攻击次数最多的前 N 个客户端的信息。

<table>
<tr><th>序列</th><th>客户端IP</th><th>检测到的攻击数量</th><th colspan="2">百分比</th></tr>
<tr><td>1</td><td>192.169.2.2</td><td>29</td><td></td><td>30.85%</td></tr>
<tr><td>2</td><td>192.169.2.4</td><td>21</td><td></td><td>22.34%</td></tr>
<tr><td>3</td><td>192.169.2.6</td><td>16</td><td></td><td>17.02%</td></tr>
<tr><td>4</td><td>192.169.2.10</td><td>14</td><td></td><td>14.89%</td></tr>
<tr><td>5</td><td>192.169.2.8</td><td>14</td><td></td><td>14.89%</td></tr>
</table>

说明：
▪ 检测到的攻击数量：客户端保护中 IPS 检测出的某一特定主机被攻击的总次数。
▪ 百分比：客户端保护中 IPS 检测出的某一特定主机被攻击的总次数占客户端保护中 IPS 检测出攻击的总次数的比例。</td></tr>
<tr><td>被 IPS 检测到次数最多的前 N 个服务器</td><td>服务器保护中 IPS 检测到被攻击次数最多的前 N 个服务器的信息。

<table>
<tr><th>序列</th><th>服务器IP/域名</th><th>检测到的攻击数量</th><th colspan="2">百分比</th></tr>
<tr><td>1</td><td>192.169.3.3</td><td>24</td><td></td><td>28.57%</td></tr>
<tr><td>2</td><td>192.169.3.5</td><td>17</td><td></td><td>20.24%</td></tr>
<tr><td>3</td><td>192.169.3.7</td><td>15</td><td></td><td>17.86%</td></tr>
<tr><td>4</td><td>192.169.3.1</td><td>14</td><td></td><td>16.67%</td></tr>
<tr><td>5</td><td>192.169.3.9</td><td>14</td><td></td><td>16.67%</td></tr>
</table>

说明：
▪ 检测到的攻击数量：服务器保护中 IPS 检测出的某一特定服务器被攻击的总次数。
▪ 百分比：服务器保护中 IPS 检测出的某一特定服务器被攻击的总次数占服务器保护中 IPS 检测到攻击总次数的比例。</td></tr>
</table>

9.2.1.5.应用

错误!未找到引用源。给出应用信息类型及示例图：

表 5——应用信息

类型	**描述**

<table>
<tr><td>会话最多的前 N 个应用</td><td>会话数最多的应用的信息。

<table>
<tr><th>序列</th><th>应用</th><th>会话数</th><th colspan="2">百分比</th></tr>
<tr><td>1</td><td>魔兽世界</td><td>23</td><td></td><td>10.04%</td></tr>
<tr><td>2</td><td>NNTP</td><td>19</td><td></td><td>8.30%</td></tr>
<tr><td>3</td><td>Daytime</td><td>16</td><td></td><td>6.99%</td></tr>
<tr><td>4</td><td>IMAP</td><td>13</td><td></td><td>5.68%</td></tr>
<tr><td>5</td><td>MSN</td><td>12</td><td></td><td>5.24%</td></tr>
</table>

说明：
▪ 应用：应用的名称。
▪ 会话数：某一特定应用的会话总数。
▪ 百分比：某一特定应用的会话总数占所有应用会话数的比例。</td></tr>
<tr><td>会话最多的前 N 个应用类别</td><td>会话数最多的前 N 种应用类别的信息。

<table>
<tr><th>序列</th><th>应用分类</th><th>会话数</th><th colspan="2">百分比</th></tr>
<tr><td>1</td><td>即时通讯</td><td>39</td><td></td><td>17.03%</td></tr>
<tr><td>2</td><td>游戏</td><td>30</td><td></td><td>13.10%</td></tr>
<tr><td>3</td><td>管理软件</td><td>30</td><td></td><td>13.10%</td></tr>
<tr><td>4</td><td>互联网实用类</td><td>27</td><td></td><td>11.79%</td></tr>
<tr><td>5</td><td>电子邮件</td><td>23</td><td></td><td>10.04%</td></tr>
</table></td></tr>
<tr><td>流量最高的前 N 个应用</td><td>产生流量最高的前 N 个应用的信息。

<table>
<tr><th>序列</th><th>应用</th><th>流量(KB)</th><th colspan="2">百分比</th></tr>
<tr><td>1</td><td>POP2</td><td>2923</td><td></td><td>12.82%</td></tr>
<tr><td>2</td><td>POP3</td><td>2538</td><td></td><td>11.13%</td></tr>
<tr><td>3</td><td>魔兽世界</td><td>2361</td><td></td><td>10.35%</td></tr>
<tr><td>4</td><td>NNTP</td><td>2166</td><td></td><td>9.50%</td></tr>
<tr><td>5</td><td>Daytime</td><td>2137</td><td></td><td>9.37%</td></tr>
</table>

说明：
▪ 流量（KB）：某一特定应用产生的总流量。
▪ 百分比：某一特定应用产生的总流量占所有应用流量的比例。</td></tr>
</table>

流量最高的前 N 个应用类别	产生流量最高的前 N 个应用类别的信息。 序列 | 应用分类 | 流量(KB) | 百分比 1 | 电子邮件 | 8619 | 37.79% 2 | 即时通讯 | 4176 | 18.31% 3 | 游戏 | 2361 | 10.35% 4 | 互联网实用类 | 2166 | 9.50% 5 | 管理软件 | 2137 | 9.37%
被应用控制阻断次数最多的前 N 个应用	被应用控制阻断会话数最多的前 N 个应用的信息。 序列 | 应用 | 会话数 | 百分比 1 | POP2 | 35 | 14.64% 2 | POP3 | 29 | 12.13% 3 | 魔兽世界 | 26 | 10.88% 4 | NNTP | 23 | 9.62% 5 | Daytime | 22 | 9.21% 说明： ▪ 会话数：某一特定应用的会话被应用控制阻断的总数。 ▪ 百分比：某一特定应用的会话被应用控制阻断的总数占所有应用被应用控制阻断的会话总数的比例。
被应用控制阻断次数最多的前 N 个类别	被应用控制阻断会话数最多的前 N 个应用类别的信息。 序列 | 应用分类 | 会话数 | 百分比 1 | 电子邮件 | 97 | 40.59% 2 | 即时通讯 | 38 | 15.90% 3 | 游戏 | 26 | 10.88% 4 | 互联网实用类 | 23 | 9.62% 5 | 管理软件 | 22 | 9.21%

9.2.1.6.用户

错误!未找到引用源。给出用户信息类型及示例图：

表 6——用户信息

类型	**描述**

流量最高的前 N 个用户	产生流量最高的前 N 个用户的信息。 说明： ▪ 流量（KB）：某一特定用户产生的总流量。 ▪ 百分比：某一特定用户产生的总流量占用户总流量的比例。

序列	用户名	流量(KB)	百分比
1	test	1995	8.75%
2	test1	1735	7.61%
3	test2	1537	6.74%
4	test3	1321	5.79%
5	test4	1271	5.57%

9.2.2. 编辑/删除报表任务

1. 选择**报表>任务**。

2. 在**任务**列表中：
   - 双击某个条目对其进行编辑。
   - 勾选**序号**左侧的复选框选中所有任务，或者勾选任务条目对应的复选框选中一个或多个条目，点击**删除**。在弹出的对话框中点击**确定**，删除任务。

9.3.结果

管理员可以查看或删除报表的生成结果，也可以将报表下载到本地 PC。如果已配置 SMTP 服务器，在报表生成后，NCSS 会将报表发送给指定的收件人。

1. 选择**报表>结果**。

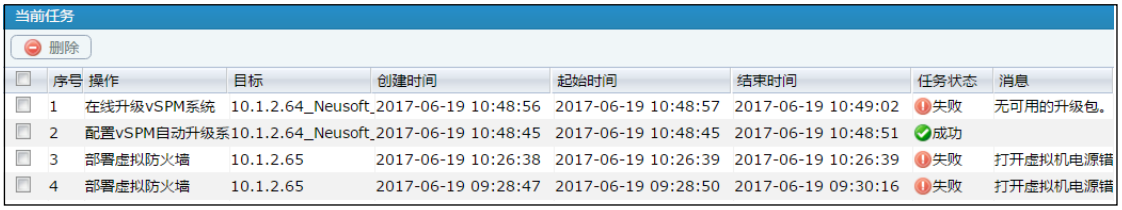
   - 时间：报表生成的时间。
   - 报表标题：报表生成计划中配置的报表名称。
   - 类型：报表计划的类型。
   - 防火墙：生成报表的虚拟防火墙。
   - 报表文件：为管理员提供 PDF 或 HTML 格式报表的下载链接。

2. 点击 PDF 或 HTML，将报表下载为 PDF 或 HTML 格式的文件。
3. 勾选**时间**左侧的复选框选中所有结果，或者勾选结果条目对应的复选框选中一个或多个条目，点击**删除**。在弹出的对话框中点击**确定**，删除报表结果。

第10章 任务管理

本章介绍 NCSS 的任务管理功能。该功能用来查看和删除被管理虚拟防火墙上的任务，包括配置备份、设备更新和策略下发等。

1. 选择**任务管理>任务**。
2. 在当前任务列表中，可以查看当前所有任务。如需删除任务，选中任务后点击**删除**。



- 序号：任务序号。排在列表最前面的任务最近被执行的。
- 操作：查看任务的描述信息。
- 目标：任务是在哪些虚拟防火墙上执行的。
- 创建时间：任务的创建时间。
- 起始时间：任务开始的时间。
- 结束时间：任务结束的时间。
- 任务状态：任务的执行状态，包括成功、失败、等待执行以及正在执行。
- 消息：任务相关的消息。