使用 Cisco Defense Orchestrator 管理 ASA

使用 Cisco Defense Orchestrator 管理 ASA

Cisco Defense Orchestrator (CDO) 是一种基于云的多设备管理器，可提供一种简单、一致且安全的方式来管理所有 ASA 设备上的安全策略。

本文档的目标是为 Cisco Defense Orchestrator (CDO) 的新客户提供可用于标准化对象和策略、升级受管设备以及管理 VPN 策略和监控远程工作人员的活动大纲。本文档假设如下：

- 您已开设 30 天试用账户，或者您已购买 CDO，并且思科已为您创建 CDO 租户。
- 您已为超级管理员用户设置了 新 CDO 租户的初始登录。
- 您的 ASA 已配置，您正在企业中使用它。
- 如果您希望 CDO 管理的 ASA 无法直接从互联网访问，则需要在网络中部署安全设备连接器 (SDC)。SDC 管理 CDO 和 ASA 之间的通信。有关详细信息，请参阅使用 CDO 的 VM 映像部署安全设备连接器或在您自己的虚拟机上部署安全设备连接器。

立即行动

安全设备连接器

使用设备凭证将 CDO 连接到 ASA 时，最佳实践是在网络中下载并部署安全设备连接器 (SDC)，以管理 CDO 与 ASA 之间的通信。ASA 都可以使用设备凭证载入到 CDO。如果您不希望 SDC 管理 ASA 和 CDO 之间的通信，并且可以直接从互联网访问您的设备，则无需在网络中安装 SDC。可以使用云连接器将 ASA 载入 CDO。

通过为租户部署多个SDC，您可以通过CDO租户来管理更多设备，而不会出现性能下降。单个SDC可以管理的设备数量取决于这些设备上实施的功能及其配置文件的大小。但是，出于规划部署的目的，我们预计一个 SDC 可支持大约 500 台设备。

查看 SDC：

1. 登录 CDO。

使用 Cisco Defense Orchestrator 管理 ASA

2. 从 CDO 菜单中选择**管理 (Admin)** > **安全连接器 (Secure Connectors)**。

载入设备

您可以批量或一次一个地将 ASA 载入 CDO。有关 CDO 支持的 ASA 软件和硬件的讨论，请参阅ASA 支持详情。

在租户上创建其他 CDO 用户

Cisco Defense Orchestrator (CDO) 中有多种用户角色：只读、仅编辑、仅部署、管理员和超级管理员。为每个租户上的每个用户配置用户角色。如果 CDO 用户可以访问多个租户，则他们可能具有相同的用户 ID，但在不同的租户中具有不同的角色。当接口或文档提及只读用户、管理员用户或超级管理员用户时，我们描述的是该用户对特定租户的权限级别。请参阅CDO中的用户角色，了解授予不同类型用户的权限。

创建租户时，系统会自动为您分配超级管理员用户。超级管理员能够在您的租户上创建其他用户。对于要连接到租户的新用户，他们需要拥有或创建一个使用与其在 CDO 中的用户记录相同的电子邮件地址的 Cisco Secure Sign-On 帐户。请参阅将用户帐户添加到 CDO，在 CDO 中创建用户记录。

策略编排

策略协调涉及查看对象和策略。请记住，使用 ASA 策略时，CDO 将“访问组”称为“访问策略”。当您查找 ASA 访问策略时，您可以从 CDO 菜单栏策略 > ASA 访问策略进行导航。

解决网络对象问题

多年来，您的安全设备上可能有不再使用的对象，这些对象与其他对象重复，或者其值在设备之间不一致。通过修复这些对象问题开始您的协调任务。

按以下顺序处理对象问题。您在早期步骤中所做的工作可能会解决您在后续步骤中必须解决的许多问题：

1. 解决未使用的对象。未使用的对象 是设备中存在但未被其他对象、访问列表或 NAT 规则引用的对象。

2. 解决重复对象对象。重复对象 是指同一设备上具有不同名称但值相同的两个或多个对象。这些对象通常是意外创建的，可用于类似的目的，并供不同的策略使用。解决重复对象问题后，CDO 会使用保留的对象名称来更新所有受影响的对象引用。

3. 解决不一致的对象。不一致对象 是指两台或多台设备上具有相同名称但值不同的对象。有时，用户会在不同的配置中创建具有相同名称和内容的对象，但随着时间的推移，这些对象的值会出现分歧，从而造成不一致。这可能是一个安全问题。您可能有一条保护过时资源的规则。

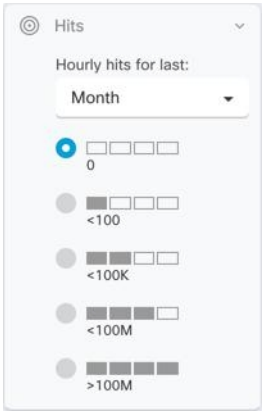
使用 Cisco Defense Orchestrator 管理 ASA

修复影子规则

现在，您已解决网络对象问题，请查看影子规则的网络策略并进行修复。影子规则**影子规则**在 ASA 访问策略页面上用半月形标记 ◑ 进行标记。访问策略中的规则在列表中进行配置，并从上到下一次评估一个。策略中的影子规则永远不会匹配，因为网络流量与策略中的影子规则上方的规则相匹配。如果存在永远不会命中的影子规则，请将其删除，或编辑策略以使规则生效。

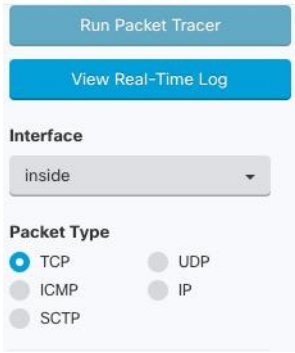
评估策略命中率

确定策略中的规则是否实际评估网络流量。CDO 每小时收集一次有关策略中规则的命中率数据。您的设备由 CDO 管理的时间越长，特定规则的命中率数据就越有意义。按您感兴趣的时间段内的命中计数过滤 ASA 访问策略，以查看其是否受到命中。如果不是，请考虑重写策略或将其删除。



策略故障排除

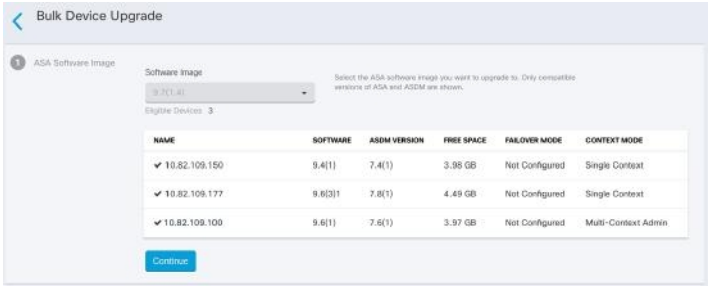
您可以使用 ASA Packet Tracer 通过策略测试合成数据包的路径，并确定规则是否无意中阻止或允许访问。



升级 ASA 和 ASDM

接下来，升级到最新版本的 ASA 和 ASDM。客户报告称，使用 CDO 升级其 ASA 可节省 75%-90% 的时间。

使用 Cisco Defense Orchestrator 管理 ASA



CDO 提供的向导让您能够在单情景或多情景模式下升级单个 ASA 或多个 ASA 上安装的 ASA 和 ASDM 映像。CDO 维护 ASA 和 ASDM 映像的数据库。

CDO 在后台执行必要的升级兼容性检查。该向导将指导您选择兼容的 ASA 和 ASDM 映像，安装这些映像并重新启动设备以完成升级。CDO 会验证您在 CDO 上选择的映像是否是复制到并安装在 ASA 上的映像，从而确保升级过程的安全。

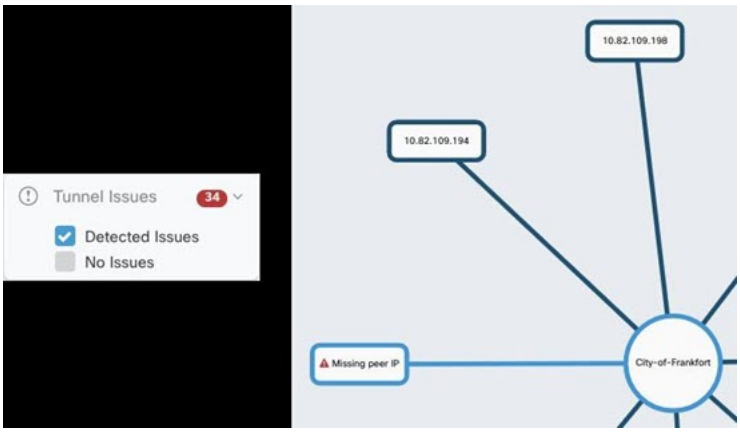
CDO 会定期查看其数据库并向其添加最新的 ASA 和 ASDM 映像。CDO 仅支持正式发布 (GA) 映像，不会将自定义映像添加到其数据库。如果您在列表中没有看到特定的 GA 映像，请通过**联系支持人员 (Contact Support)** 页面联系思科 TAC。我们将使用已建立的支持请求 SLA 处理请求，并上传缺少的 GA 映像。

查看在单个 ASA 上升级 ASA 和 ASDM 映像并继续使用您自己的存储库中的映像升级多个 ASA以了解有关升级 ASA 的更多信息。

监控和管理 VPN 连接

查看站点间 VPN 问题

CDO 报告网络中 ASA 设备上存在的 VPN 问题。您可以通过两种方式查看您的环境，即显示 VPN 对等体列表的表或显示中心辐射型拓扑中的VPN连接的映射。使用过滤器边栏搜索需要注意的VPN隧道。



使用 CDO 评估您的 VPN 隧道：

- 检查站点间 VPN 隧道连接
- 查找缺少对等体的 VPN 隧道

使用 Cisco Defense Orchestrator 管理 ASA

- 查找存在加密密钥问题的 VPN 对等体
- 查找为隧道定义的不完整或配置错误的访问列表
- 查找隧道配置中的问题

板载非托管站点间 VPN 对等体

CDO 还标识非托管 VPN 对等体。识别这些设备后，请使用载入非托管站点间 VPN 对等体载入设备并使用 CDO 对其进行管理。

ASA 远程访问 VPN 支持

CDO 允许创建远程访问虚拟专用网络 (RA VPN) 配置，以允许用户在通过 ASA 连接时安全地访问企业资源。当您的 ASA 载入 CDO 时，CDO 会识别已使用 ASDM 或思科安全管理器 (CSM) 配置的任何 RA VPN 设置，以便您可以使用 CDO 对其进行管理。

AnyConnect 是终端设备上通过 RA VPN 连接的唯一受支持客户端。

CDO 支持 ASA 设备上的 RA VPN 功能的以下方面：

- 基于 SSL 客户端的远程访问
- IPv4 和 IPv6 寻址
- 跨多台 ASA 设备共享 RA VPN 配置

有关详细信息，请参阅 为 ASA 配置远程访问虚拟专用网络。

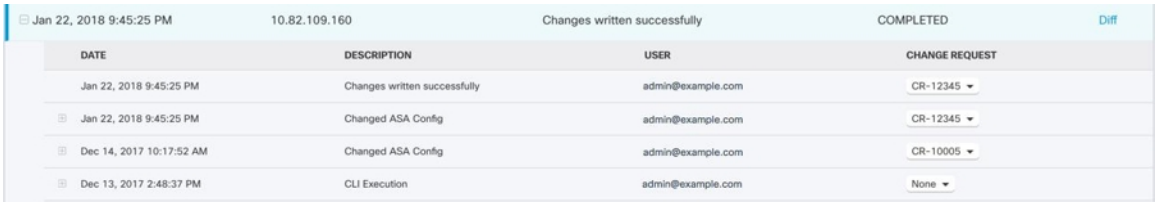
监控设备配置同步

CDO 会定期将其数据库中存储的设备配置与 ASA 上安装的设备配置进行比较。您载入 CDO 的 ASA 仍可载入 ASA 仍可由设备的自适应安全设备管理器 (ASDM) 管理，因此 CDO 会确保其配置与设备上的配置相同，并会提醒您注意差异。有关“已同步”、“未同步”或“检测到冲突”设备状态的详细信息，请参阅冲突检测。

跟踪更改日志中的更改

您对设备配置所做的更改会记录在 中。变更日志更改日志显示的信息包括从 CDO 部署到设备的更改、从设备导入到CDO的更改、更改内容以及查看更改“差异”的功能、更改发生的时间以及执行者。

您还可以创建自定义标签，并将其应用到您所做的更改。更改请求管理在更改日志中，您可以按该自定义标签、日期范围、按特定用户或按更改类型过滤更改列表，以查找您要查找的内容。



使用 Cisco Defense Orchestrator 管理 ASA

恢复之前的配置

如果您对要“撤消”的ASA进行了更改，可以使用CDO将设备恢复为以前的配置。有关详细信息，请参阅 恢复 ASA 配置。

使用命令行接口和命令宏管理设备

CDO 是一种基于 Web 的管理产品，为您提供图形用户界面 (GUI) 和命令行接口 (CLI)，以便一次管理一个或多个设备。

ASA CLI 用户会喜欢我们的 CLI 工具的额外功能。以下是使用 CDO 的 CLI 工具而不是通过 SSH 会话连接到设备的一些原因：

- CDO知道命令所需的用户模式。您不需要提升或降低您的权限级别来执行命令，也不需要输入特定的命令上下文来执行命令。
- CDO保留了的命令历史记录需求链接，因此您可以通过从列表中选择命令来轻松地重新运行该命令。
- CLI 操作记录在更改日志中，因此您可以查看发送的命令和执行的操作。
- 命令可以在批量模式下运行，允许您同时将对象或策略部署到多个设备。
- CDO 用品 CLI 宏。CLI 宏是存储的即用命令，您可以按原样运行，或者可以完成并运行“填空”CLI 命令。您可以在一台设备上运行这些命令，也可以同时将命令发送到多个 ASA。
- CLI 为您提供完整的 ASA 配置文件。您可以查看它，或者如果您是高级用户，可以直接编辑它并保存更改，而不是发出 CLI 命令来更改它。

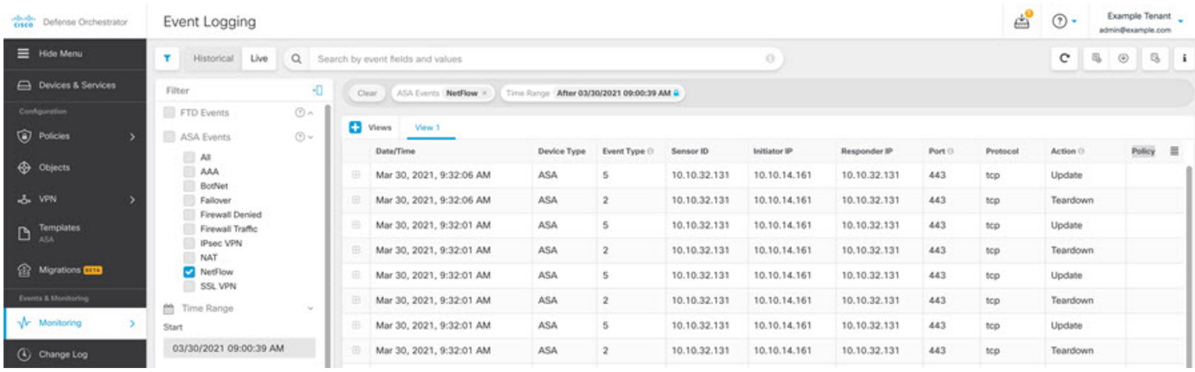
将 CDO 与 SecureX 集成

Cisco SecureX 平台思科 SecureX 结合了思科的集成安全产品组合以及客户基础设施的优势，旨在提供可统一可视性、实现自动化并增强网络、终端、云和应用安全性的一致体验。通过集成平台中的连接技术，SecureX提供了可衡量的洞察力、预期成果以及无与伦比的跨团队协作。您可以阅读有关以及如何操作的更多信息。SecureX和CDO将 CDO 添加到 SecureX

思科安全分析和日志记录

通过额外许可，思科安全分析和日志记录让您可以将系统日志事件和 Netflow 安全事件日志记录 (NSEL) 事件从 ASA 定向到 安全事件连接器 (SEC)，然后由 SEC 将其转发到思科云。进入云后，您可以在 CDO 的“事件日志记录”(Event Logging) 页面中查看这些事件。您可以在其中过滤和查看事件，以便清楚地了解在网络中触发的安全规则。

使用 Cisco Defense Orchestrator 管理 ASA



除了监控事件，您还可以从 CDO 启动 Secure Cloud Analytics 门户，以对记录的事件执行行为分析。

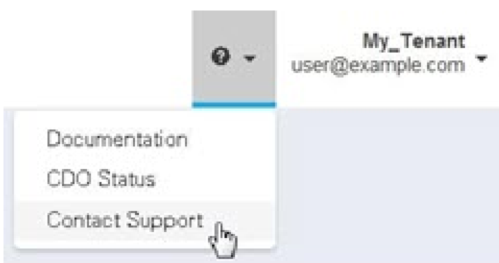
有关如何实施思科安全分析和日志记录的完整说明，请参阅为 ASA 设备实施安全日志记录分析 (SaaS)。

后续操作

现在，您可以开始载入 ASA 并协调策略。

如果您需要帮助

您可以通过点击 CDO GUI 中的支持菜单联系支持人员、提出问题或阅读我们的产品文档。



使用 Cisco Defense Orchestrator 管理 ASA

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。