将 Fortinet 迁移到 Threat Defense 2100 - 示例

- 将 迁移到防火墙威胁防御 2100 - 示例， 第 1 页

将 迁移到防火墙威胁防御 2100 - 示例

注释 创建迁移完成后可在目标设备上运行的测试计划。

- 在维护窗口之前执行以下任务， 第 1 页
- 在维护窗口期间执行以下任务， 第 2 页

在维护窗口之前执行以下任务

开始之前

确保已安装并部署了 管理中心。有关详细信息，请参阅相应的管理中心硬件安装指南和相应的管理中心入门指南。

步骤 1 从要迁移的源 Fortinet 保存全局或每 VDOM 配置的副本。

步骤 2 在网络中部署 Firepower 2100 系列 设备，连接接口并打开设备电源。

有关详细信息，请参阅《适用于使用管理中心的 2100 系列的思科威胁防御快速入门指南》。

步骤 3 注册 Firepower 2100 系列 设备以接受 管理中心 的管理。

有关详细信息，请参阅将设备添加到管理中心。

步骤 4 （可选）如果源 Fortinet 配置具有汇聚接口，请在目标 Firepower 2100 系列 设备上创建端口通道 (EtherChannel)。

有关详细信息，请参阅配置 EtherChannel 和冗余接口。

步骤 5 从 https://software.cisco.com/download/home/286306503/type 下载并运行最新版本的 防火墙迁移工具。

有关详细信息，请参阅 从 Cisco.com 下载防火墙迁移工具。

步骤 6 启动 防火墙迁移工具 并指定目标参数时，请确保选择注册到 管理中心 的 Firepower 2100 系列 设备。

有关详细信息，请参阅 指定防火墙迁移工具的目标参数。

步骤 7 将 Fortinet 接口与 威胁防御 接口映射。

注释 防火墙迁移工具 允许您将 Fortinet 接口类型映射到 威胁防御 接口类型。

例如，您可以将 Fortinet 中的汇聚接口映射到 威胁防御 中的物理接口。

有关详细信息，请参阅映射 Fortinet 接口与威胁防御接口。

步骤 8 将逻辑接口映射到安全区时，点击**自动创建 (Auto-Create)** 以允许 防火墙迁移工具 创建新的安全区。要使用现有安全区，请手动将 Fortinet 逻辑接口映射到安全区。

有关详细信息，请参阅将 ASA Fortinet 逻辑接口映射到安全区和接口组。

步骤 9 按照本指南的说明依次检查和验证要迁移的配置，然后将配置推送到 管理中心。

步骤 10 查看迁移后报告，手动设置其他配置并部署到 威胁防御，完成迁移。

有关详细信息，请参阅查看迁移后报告并完成迁移。

步骤 11 使用您在计划迁移时创建的测试计划测试 Firepower 2100 系列 设备。

在维护窗口期间执行以下任务

开始之前

确保您已完成所有必须在维护窗口之前执行的任务。请参阅在维护窗口之前执行以下任务，第 1 页。

步骤 1 清除周围交换基础设施上的地址解析协议 (ARP) 缓存。

步骤 2 执行从周围交换基础设施到 Firepower 2100 系列 设备接口 IP 地址的基本 ping 测试，确保它们可访问。

步骤 3 执行从需要第 3 层路由的设备到 Firepower 2100 系列 设备接口 IP 地址的基本 ping 测试。

步骤 4 如果要为 Firepower 2100 系列 设备分配新的 IP 地址，而不是重新使用分配给 设备的 IP 地址，请执行以下步骤：

1. 更新指向该 IP 地址的任何静态路由，以使其现在指向 Firepower 2100 系列 设备 IP 地址。
2. 如果使用路由协议，请确保邻居将 Firepower 2100 系列 设备 IP 地址视为预期的下一跳目标。

步骤 5 运行全面的测试计划并监控管理 Firepower 2100 设备的 管理中心。

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。