在 OCI 上部署 Firewall Threat Defense Virtual

您可以在 Oracle Cloud 基础设施 (OCI) 上部署 Firewall Threat Defense Virtual，前者是一种公共云计算服务，使您能够在 Oracle 提供的高可用性托管环境中运行应用程序。

以下程序介绍了如何准备 OCI 环境并启动 Firewall Threat Defense Virtual实例。您可以登录 OCI 门户，在 OCI 市场中搜索 Cisco Firepower NGFW 虚拟防火墙 (NGFWv) 产品，然后启动计算实例。启动 Firewall Threat Defense Virtual后，您必须配置路由表，以便根据流量的源和目标将流量定向到防火墙。

概述

Cisco Cisco Secure Firewall Threat Defense Virtual 运行与物理 Cisco 防火墙威胁防御 相同的软件，以虚拟形式提供成熟的安全功能。Firewall Threat Defense Virtual 可以部署在公共 OCI 中。然后，可以对其进行配置，以保护在一段时间内扩展、收缩或转换其位置的虚拟和物理数据中心工作负载。

OCI 计算资源大小

形状是确定分配给实例的 CPU 数量、内存量和其他资源的模板。Firewall Threat Defense Virtual 支持以下 OCI 形状类型：

表 *1:* 支持 *x86* 部署的计算资源大小

OCI 形状	支持的 Threat Defense Virtual 版本	属性		接口
		oCPU	随机存取存储器 (GB)	
Intel VM.DenseIO2.8	7.3.x 及更高版本	8	120	最小值 4，最大值 8
Intel VM.StandardB1.4	7.3.x 及更高版本	4	48	最小值 4，最大值 4
Intel VM.StandardB1.8	7.3.x 及更高版本	4	96	最小值 4，最大值 8
Intel VM.Standard1.4	7.3.x 及更高版本	4	28	最小值 4，最大值 4
Intel VM.Standard1.8	7.3.x 及更高版本	8	56	最小值 4，最大值 8
Intel VM.Standard2.4	7.1、7.2.x 和 7.3.x	4	60	最小值 4，最大值 4
Intel VM.Standard2.8	7.1、7.2.x 和 7.3.x	8	120	最小值 4，最大值 8
Intel VM.Standard3.Flex	7.3.x 及更高版本	4	16	最小值 4，最大值 4
	7.3.x 及更高版本	6	24	最小值 4，最大值 6
	7.3.x 及更高版本	8	32	最小值 4，最大值 8
Intel VM.Optimized3.Flex	7.3.x 及更高版本	4	16	最小值 4，最大值 8
	7.3.x 及更高版本	6	24	最小值 4，最大值 10
	7.3.x 及更高版本	8	32	最小值 4，最大值 10

OCI 形状	支持的 Threat Defense Virtual 版本	属性		接口
		oCPU	随机存取存储器 (GB)	
AMD VM.Standard.E4.Flex	7.3.x 及更高版本	4	16	最小值 4，最大值 4
	7.3.x 及更高版本	6	24	最小值 4，最大值 6
	7.3.x 及更高版本	8	32	最小值 4，最大值 8
AMD VM.Standard.E5.Flex	仅限 7.6.4	4	16	最小值 4，最大值 4
	仅限 7.6.4	6	24	最小值 4，最大值 6
	仅限 7.6.4	8	32	最小值 4，最大值 8
AMD VM.Standard.E6.Flex	仅限 7.6.4	4	16	最小值 4，最大值 4
	仅限 7.6.4	6	24	最小值 4，最大值 6
	仅限 7.6.4	8	32	最小值 4，最大值 8

表 *2:* 支持 ***ARM*** 部署的计算资源大小

OCI 形状	支持的 Threat Defense Virtual 版本	属性		接口
		oCPU	随机存取存储器 (GB)	
Ampere VM.Standard.A1.Flex 的 Altra 处理器	10.0.0 及更高版本	4	8	最小值 4，最大值 4
	10.0.0 及更高版本	8	16	最小值 4，最大值 8
	10.0.0 及更高版本	12	24	最小值 4，最大值 10
	10.0.0 及更高版本	16	32	最小值 4，最大值 10

OCI 形状	支持的 Threat Defense Virtual 版本	属性		接口
		oCPU	随机存取存储器 (GB)	
Ampere VM.Standard.A2.Flex 的 AmpereOne 处理器	10.0.0 及更高版本	2	8	最小值 4，最大值 4
	10.0.0 及更高版本	4	16	最小值 4，最大值 8
	10.0.0 及更高版本	6	24	最小值 4，最大值 10
	10.0.0 及更高版本	8	32	最小值 4，最大值 10

注释 我们建议使用 Flex 计算资源大小。

注释 对于 VM.Standard.A1.Flex 资源大小，1 个 oCPU 相当于 1 个 vCPU。

对于其余计算资源大小，1 个 oCPU 相当于 2 个 vCPUs。

- *7.4.x 及更高版本中的 Flex 形状支持 SR-IOV 模式。
- Firewall Threat Defense Virtual 至少需要 4 个接口。

有关使用 Firewall Threat Defense Virtual 7.3 及更高版本支持的 OCI 计算形状的建议。

- OCI 市场映像版本 **7.3.0-69-v2** 及更高版本仅与 Firewall Threat Defense Virtual 7.3 及更高版本的 OCI 计算形状兼容。
- 您只能将 Firewall Threat Defense Virtual 7.3 及更高版本支持的 OCI 计算形状用于新部署。
- OCI 计算配置版本 **7.3.0-69-v3** 及更高版本与使用 Firewall Threat Defense Virtual 7.3 之前的 OCI 计算配置版本升级与 Firewall Threat Defense Virtual 一起部署的虚拟机不兼容。
- **VM.DenseIO2.8** 计算形态订用将继续计费，即使在您关闭实例后也是如此。有关详细信息，请参阅 OCI 文档。

您可以在 OCI 上创建账户，使用 Oracle 云市场上的思科 Firepower NGFW 虚拟防火墙（NGFWv）产品来启动计算实例，然后选择 OCI 形状。

固件支持：

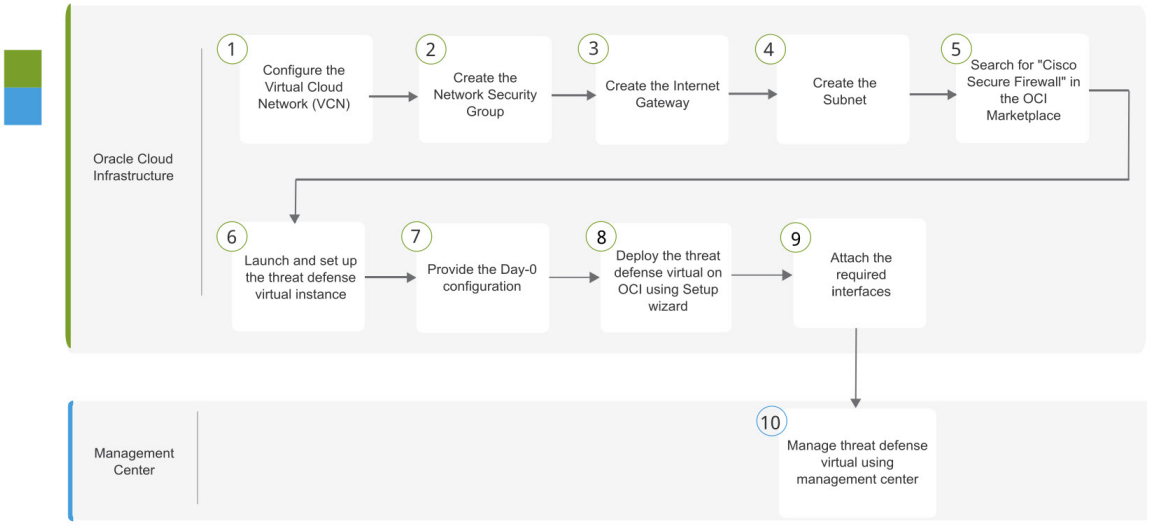
默认情况下，使用 UEFI 模式部署 Threat Defense Virtual 实例。

注释 OCI 不支持安全启动功能。

现有的棕色地带部署可以升级到版本 10.0.0，而不会受到影响。不支持在部署后更改启动模式。

端到端程序

以下流程图说明了在 Oracle Cloud 基础设施上部署 Threat Defense Virtual 的工作流程。



	工作空间	步骤
1	Oracle Cloud 基础设施	在 OCI 上部署 Threat Defense Virtual：配置虚拟云网络 (VCN)（**网络 (Networking)** > **虚拟云网络 (Virtual Cloud Networks)** > **CIDR 块 (CIDR block)** > **创建 VCN (Create VCN)**。
2	Oracle Cloud 基础设施	在 OCI 上部署 Threat Defense Virtual：创建网络安全组。依次选择**网络 (Networking)** > **虚拟云网络 (Virtual Cloud Networks)** > **虚拟云网络详细信息 (Virtual Cloud Network Details)** > **网络安全组 (Network Security Groups)**，然后点击**创建网络安全组 (Create Network Security Group)**。
3	Oracle Cloud 基础设施	在 OCI 上部署 Threat Defense Virtual：创建互联网网关。**网络 (Networking)** > **虚拟云网络 (Virtual Cloud Networks)** > **虚拟云网络详细信息 (Virtual Cloud Network Details)** > **互联网网关 (Internet Gateways)** > **创建互联网网关 (Create Internet Gateway)**。
4	Oracle Cloud 基础设施	在 OCI 上部署 Threat Defense Virtual：创建子网。**网络 (Networking)** > **虚拟云网络 (Virtual Cloud Networks)** > **虚拟云网络详细信息 (Virtual Cloud Network Details)** > **子网 (Subnets)** > **创建子网 (Create Subnet)**。

	工作空间	步骤
5	Oracle Cloud 基础设施	在 OCI 上部署 Threat Defense Virtual，第 16 页：在 OCI 市场中搜索“Cisco Secure Firewall”。
6	Oracle Cloud 基础设施	在 OCI 上部署 Threat Defense Virtual，第 16 页：启动并设置 Threat Defense Virtual 实例。
7	Oracle Cloud 基础设施	在 OCI 上部署 Threat Defense Virtual，第 16 页：提供 Day-0 配置。
8	Oracle Cloud 基础设施	在 OCI 上部署 Threat Defense Virtual，第 16 页：使用设置向导在 OCI 上部署 Threat Defense Virtual。
9	Oracle Cloud 基础设施	在 OCI 上部署 Threat Defense Virtual：连接接口。**计算 (Compute)** > **实例 (Instances)** > **实例详细信息 (Instance Details)** > **连接的 VNIC (Attached VNICs)**。
10	管理中心	使用管理中心管理 Firewall Threat Defense Virtual

前提条件

- 在 https://www.oracle.com/cloud/ 上创建一个 OCI 账户。
- 思科智能账户。可以在思科软件中心 (https://software.cisco.com/) 创建一个账户。
- 许可 Firewall Threat Defense Virtual。
  - 所有安全服务的许可证授权均在 防火墙管理中心中配置。
  - 有关如何管理许可证的详细信息，请参阅《*Cisco Secure Firewall Management Center* 管理员指南》中的“许可”。

注释 思科提供的所有默认许可证授权（以前用于 Firewall Threat Defense Virtual 虚拟设备）都将支持 IPv6 配置。

- 接口要求：
  - 管理接口 (2) - 一个用于将 Firewall Threat Defense Virtual 连接到 防火墙管理中心，另一个用于诊断；无法用于直通流量。
  - 流量接口 (2) - 用于将 Firewall Threat Defense Virtual 连接到内部主机和公共网络。
- 通信路径：
  - 用于访问 Firewall Threat Defense Virtual的公共 IP。

- 有关 Firewall Threat Defense Virtual 系统要求，请参阅《Cisco Secure Firewall Threat Defense 兼容性指南》。

准则和限制

支持的功能

- 在 OCI 虚拟云网络 (VCN) 中部署
- 路由模式（默认）
- 许可 - 仅支持 BYOL
- IPv6
- 仅 防火墙管理中心 支持。
- 支持单根 I/O 虚拟化 (SR-IOV)。

FTDv 智能许可的性能级别

Firewall Threat Defense Virtual 支持性能层许可，该级别许可可基于部署要求提供不同的吞吐量级别和 VPN 连接限制。

表 *3:* 基于授权的 *Firewall Threat Defense Virtual* 许可功能限制

性能层	设备规格（核心/RAM）	速率限制	RA VPN 会话限制
FTDv5，100Mbps	4 核/8 GB	100Mbps	50
FTDv10，1Gbps	4 核/8 GB	1Gbps	250
FTDv20，3Gbps	4 核/8 GB	3 Gbps	250
FTDv30，5Gbps	8 核/16 GB	5Gbps	250
FTDv50，10Gbps	12 核/24 GB	10Gbps	750
FTDv100，16Gbps	16 核/32 GB	16Gbps	10,000

请参阅《*Cisco Secure Firewall Management Center* 管理员指南》中的“许可”一章，了解在许可 Firewall Threat Defense Virtual 设备时的准则。

注释 要更改 vCPU/内存值，必须先关闭 Firewall Threat Defense Virtual 设备的电源。

性能优化

为实现 Firewall Threat Defense Virtual的最佳性能，您可以对 VM 和主机进行调整。有关详细信息，请参阅 OCI 上的虚拟化调整和优化。

接收端扩展 - Firewall Threat Defense Virtual 支持接收端扩展 (RSS)，网络适配器利用这项技术将网络接收流量分发给多个处理器内核。在 7.0 及更高版本上受支持。有关详细信息，请参阅用于接收端扩展 (RSS) 的多个 RX 队列。

部署

运行版本 7.4.3 或更高版本的 Threat Defense Virtual 实例会在首次启动期间执行多项初始化任务，这会导致控制台在大约五分钟后可用。这种延迟是正常的。如果设备在首次启动后大约两分钟内关闭，重要的初始化步骤可能会中断，从而可能导致设置不完整和意外行为。

要解决此问题，必须使用新映像重新安装虚拟平台。

Snort

- 如果您观察到异常行为，例如 Snort 需要很长时间才能关闭，或者 VM 通常缓慢，或者在执行某个进程时，请从 Firewall Threat Defense Virtual 和 VM 主机收集日志。收集总体 CPU 使用情况、内存、I/O 使用情况和读/写速度日志将有助于对问题进行故障排除。
- 当 Snort 关闭时，观察到高 CPU 和 I/O 使用率。如果在内存不足且没有专用 CPU 的单个主机上创建了大量 Firewall Threat Defense Virtual 实例，则 Snort 将需要很长时间才能关闭，这将导致创建 Snort 核心。

不支持的功能

- 通过 防火墙设备管理器 提供本地管理支持。
- Firewall Threat Defense Virtual 本地 HA
- 透明/内联/被动模式
- 通过 DHCP 配置数据接口

限制

- OCI 上的 Firewall Threat Defense Virtual部署不支持将 Mellanox 5 作为 SR-IOV 模式下的 vNIC。
- IPv6 仅适用于根据 OCI 标准（VCN IPv4 和 IPv6）配置的　双堆栈。
- Firewall Threat Defense Virtual（ASAv 静态和 DHCP 配置）所需的单独路由规则。

OCI Ampere A1 (ARM) 实例注意事项

- 当部署在传统虚拟机监控程序上时，OCI Ampere A1 (ARM) 实例可能会遇到吞吐量降低的情况，尤其是在启用 SR-IOV 时。如果在此类部署中发现性能下降，请通过打开服务请求来联系 Oracle Cloud Infrastructure (OCI) 支持。

- OCI 团队已记录 Ampere A1 实例启用 SR-IOV 的网络的已知限制。有关其他详细信息，请参阅 Oracle Cloud Infrastructure 已知问题文档：

  https://docs.oracle.com/en-us/iaas/Content/Compute/known-issues.htm

- **VM.Standard.A1.Flex 实例网络限制**
  - VM.Standard.A1.Flex 规格仅支持半虚拟化网络启动选项。
  - 通过硬件辅助 (SR-IOV) 网络启动的实例可能会性能下降，在极少数情况下会出现数据损坏。为防止这些问题，适用于 Ampere A1 计算 (aarch64) 的 OCI 平台映像已被预配置为仅使用半虚拟化网络。如果在创建实例期间选择了硬件辅助网络，则启动将失败，并显示类似未能验证实例启动选项的错误消息。
  - 与 OCI Ampere A1 计算兼容的自定义映像在启用 SR-IOV 的情况下可以成功启动；但是，思科强烈建议避免使用硬件辅助网络，以防止出现潜在的性能和数据完整性问题。

解决办法

使用平台映像创建 VM.Standard.A1.Flex 实例时，允许 Oracle 自动选择推荐的半虚拟化网络启动类型。对于自定义映像，请勿选择硬件辅助 (SR-IOV) 网络。

升级限制和局限性

恢复升级限制

⚠

注意 不支持恢复升级。

确保在升级前进行备份。升级到 Threat Defense Virtual 10.0.0 后，您无法回滚到以前的软件版本。要返回到较早的版本，必须重新部署管理中心。

网络拓扑示例

下图显示了在路由防火墙模式下建议用于 Firewall Threat Defense Virtual 的拓扑，在 OCI 中为 Firewall Threat Defense Virtual 配置了 4 个子网（管理、诊断、内部和外部）。

图 *1:* 包含四个 ***VCN*** 中的子网的 ***OCI*** 部署示例 ***Firewall Threat Defense Virtual***

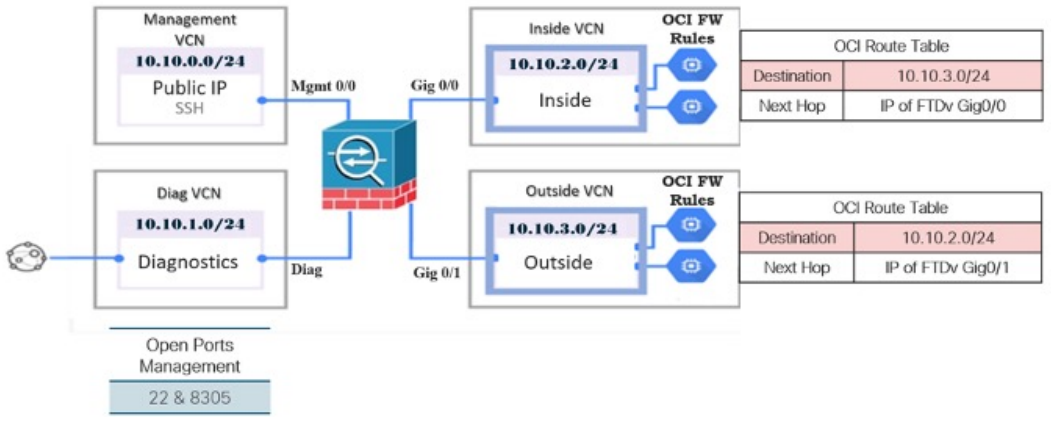
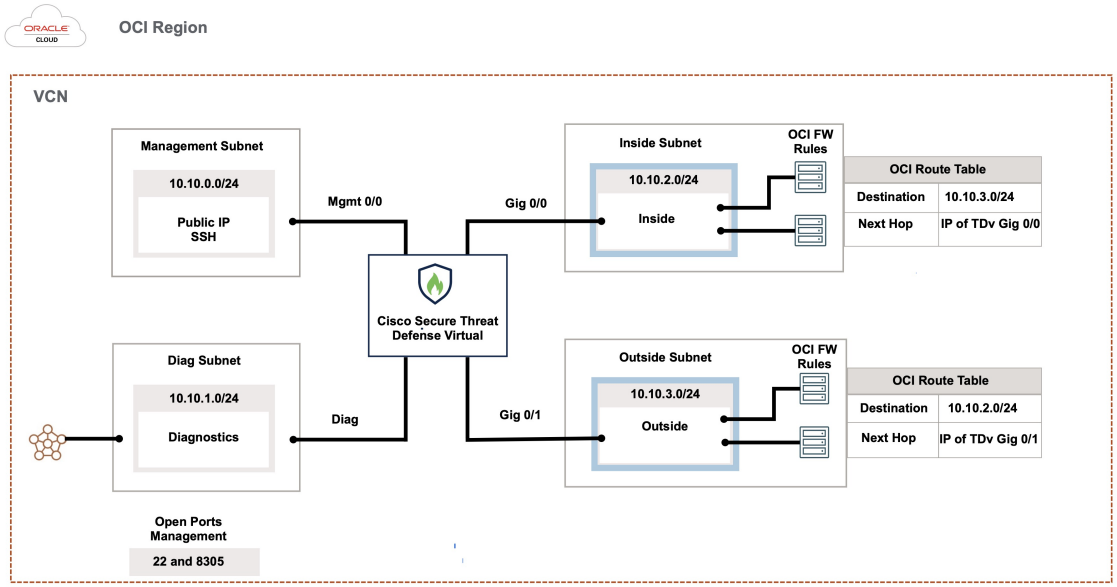
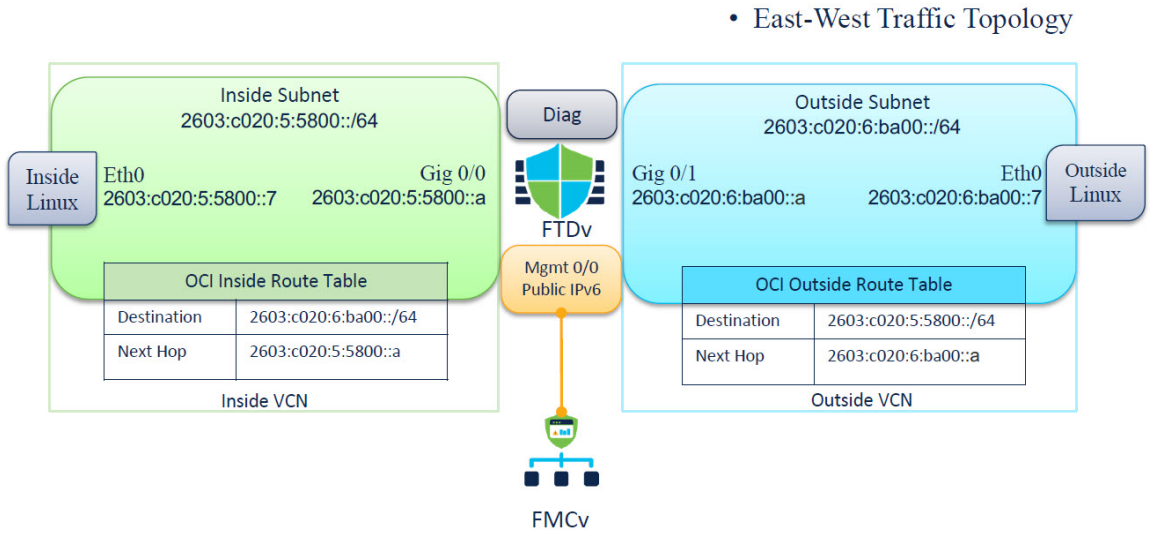


图 *2:* ***VCN*** 中具有四个子网的 ***OCI*** 部署示例 ***Firewall Threat Defense Virtual***



注释 在单个 VCN 中使用四个子网时，必须将特定于子网的路由添加到与该子网关联的路由表中。

Firewall Threat Defense Virtual IPv6 部署拓扑



如何管理 Secure Firewall Threat Defense Virtual 设备

您有两个选择来管理您的 Secure Firewall Threat Defense Virtual。

Secure Firewall Management Center

如果要管理大量设备或要使用 Firewall Threat Defense 支持的更复杂的功能和配置，请使用 防火墙管理中心（而不是集成的 防火墙设备管理器）来配置您的设备。有关详细信息，请参阅使用 Secure Firewall Management Center 来管理 Secure Firewall Threat Defense Virtual

重要事项 您不能同时使用 防火墙设备管理器 和 防火墙管理中心 来管理 Firewall Threat Defense 设备。在启用 防火墙设备管理器 集成管理功能后，将无法使用 防火墙管理中心 来管理 Firewall Threat Defense 设备，除非您禁用本地管理功能并重新配置管理功能以使用防火墙管理中心。另一方面，当您向Firewall Threat Defense 注册 防火墙管理中心 设备时，防火墙设备管理器 载入管理服务会被禁用。

注意 目前，思科不提供将 防火墙设备管理器 配置迁移到 防火墙管理中心 的选项，反之亦然。选择为 Firewall Threat Defense 设备配置的管理类型时，请考虑这一点。

Cisco Secure Firewall 设备管理器

防火墙设备管理器 是大多数 Firewall Threat Defense 设备上都包含的 Web界面。它可以配置小型网络最常用的软件基本功能。此产品专为仅包含一台或几台设备的网络而设计，在这种网络中，无需使用高性能多设备管理器来控制包含大量设备的大型网络。有关详细信息，请参阅使用 Cisco Secure Firewall 设备管理器 来管理 Secure Firewall Threat Defense Virtual

注释 有关支持的 防火墙设备管理器 设备的列表，请参阅*Cisco Secure Firewall Threat Defense* 兼容性指南。

云交付的防火墙管理中心

云交付的防火墙管理中心是一个基于云的管理平台，让您可以集中管理 Secure Firewall Threat Defense Virtual 设备。云交付的防火墙管理中心支持 Secure Firewall Threat Defense Virtual 7.0.3、7.2.0 及更高版本。有关详细信息，请参阅使用 云交付的防火墙管理中心 来管理 Secure Firewall Threat Defense Virtual。

重要事项 您不能将云交付的防火墙管理中心与 防火墙设备管理器 配合使用来管理同一台 Secure Firewall Threat Defense Virtual 设备。

配置 OCI 环境

您可以为 Threat Defense Virtual 部署配置虚拟云网络 (VCN)，具体如下：

- **多个 VCN (Multiple VCNs)** - 至少需要四个 VCN，每个 Firewall Threat Defense Virtual 接口各一个。这允许在不同网络之间进行隔离的流量检测。
- **带子网的单个 VCN (Single VCN with Subnets)** - 或者，您可以配置带四个子网的单个 VCN，每个 Threat Defense Virtual 接口各一个。在此配置中，防火墙可以使用关联的路由表检查和控制同一 VCN 中子网之间的流量。这使您可以在使用单个 VCN 时有效地管理子网间流量。

您可以继续执行以下程序来完成管理 VCN。然后返回到**网络 (Networking)**，为诊断接口、内部接口和外部接口创建 VCN。

过程

步骤 1 登录 OCI 并选择您的区域。

OCI 划分为彼此隔离的多个区域。区域显示在屏幕的右上角。一个区域中的资源不会出现在另一个区域中。请定期检查以确保您在预期的区域内。

步骤 2 依次选择**网络 (Networking)** > **虚拟云网络 (Virtual Cloud Networks)**，然后点击**创建 VCN (Create VCN)**。

步骤 3 输入 VCN 的描述性**名称**，例如 *FTDv-Management*。

步骤 4 输入 VCN 的 **CIDR 块**。

a) IP 地址的 IPv4 CIDR 块。CIDR（无类别域间路由）是 IP 地址及其关联路由前缀的紧凑表示。例如，10.0.0.0/24。

注释
在此 VCN 中使用 DNS 主机名。

b) IP 地址的 IPv6 CIDR 块。CIDR（无类别域间路由） 是 IP 地址及其关联路由前缀的紧凑表示。例如，[::/0]。
c) 选择 IPv6 CIDR 块作为 Oracle 为虚拟云网络分配的 IPv6/56 前缀。

步骤 5 点击**添加 IPv6 CIDR 块 (Add IPv6 CIDR Block)** 以添加新的 IPv6 块。

步骤 6 添加 VCN 的 IPv6 前缀，例如 */54*。

步骤 7 点击**创建 VCN (Create VCN)**。

下一步做什么

继续执行以下程序以完成管理 VCN。完成管理 VCN 后，您将为诊断接口、内部接口和外部接口创建 VCN。

注释 从导航菜单中选择服务后，左侧的菜单包括隔间列表。隔间可帮助您组织资源，以便更轻松地控制对资源的访问。您的根隔间由Oracle在调配租用时为您创建。管理员可以在根隔间中创建更多隔间，然后添加访问规则以控制哪些用户可以在其中查看和执行操作。有关详细信息，请参阅 Oracle 文档管理隔间。

创建网络安全组

网络安全组由一组 vNIC 和一组应用于这些 vNIC 的安全规则组成。

过程

步骤 1 依次选择**网络 (Networking)** > **虚拟云网络 (Virtual Cloud Networks)** > **虚拟云网络详细信息 (Virtual Cloud Network Details)** > **网络安全组 (Network Security Groups)**，然后点击**创建网络安全组 (Create Network Security Group)**。

步骤 2 输入网络安全组的描述性**名称**，例如 *FTDv-Mgmt-Allow-22-8305*。

步骤 3 点击**下一步**。

步骤 4 添加安全规则：

a) 添加规则以允许 TCP 端口 22 用于 SSH 访问。
b) 添加规则以允许 TCP 端口 8305 用于 HTTPS 访问。

可以通过 防火墙管理中心 管理 Firewall Threat Defense Virtual，这需要为 HTTPS 连接打开端口 8305。

注释
您可以将这些安全规则应用于管理接口/VCN。

步骤 5 点击**创建 (Create)**。

创建互联网网关

要使管理子网可公开访问，则需要互联网网关。

过程

步骤 1 依次选择**网络 (Networking)** > **虚拟云网络 (Virtual Cloud Networks)** > **虚拟云网络详细信息 (Virtual Cloud Network Details)** > **互联网网关 (Internet Gateways)**，然后点击**创建互联网网关 (Create Internet Gateway)**。

步骤 2 输入您的互联网网关的描述性**名称**，例如 *FTDv-IG*。

步骤 3 点击**创建互联网网关 (Create Internet Gateway)**。

步骤 4 将路由添加至互联网网关：

a) 依次选择**网络 (Networking)** > **虚拟云网络 (Virtual Cloud Networks)** > **虚拟云网络详细信息 (Virtual Cloud Network Details)** > **路由表 (Route Tables)**。
b) 点击默认路由表的链接以添加路由规则。
c) 点击**添加路由规则 (Add Route Rules)**。
d) 从**目标类型 (Target Type)** 下拉列表中，选择**互联网网关 (Internet Gateway)**。
e) 输入目标 IPv4 CIDR 块，例如 0.0.0.0/0。
f) 输入目标 IPv6 CIDR 块，例如 [::/0]。
g) 从**目标互联网网关 (Target Internet Gateway)** 下拉列表中选择您创建的网关。
h) 点击**添加路由规则 (Add Route Rules)**。

创建子网

每个 VCN 至少有一个子网。您将为管理 VCN 创建一个管理子网。诊断 VCN 还需要一个诊断子网，内部 VCN 需要一个内部子网，外部 VCN 需要一个外部子网。

如果使用一个 VCN，则要在 VCN 内创建管理子网、诊断子网、内部子网和外部子网。

过程

步骤 1 依次选择**网络 (Networking)** > **虚拟云网络 (Virtual Cloud Networks)** > **虚拟云网络详细信息 (Virtual Cloud Network Details)** > **子网 (Subnets)**，然后点击**创建子网 (Create Subnet)**。

步骤 2 输入子网的描述性**名称**，例如管理。

步骤 3 选择**子网类型 (Subnet Type)**（保留建议的默认值**区域 (Regional)**）。

步骤 4 输入 **CIDR 块 (CIDR Block)**，例如 10.10.0.0/24。子网的内部（非公共）IP 地址可从此 CIDR 块获取。

a) 如果要启用 IPv6，则选中**启用 IPv6 CIDR 块 (ENABLE IPv6 CIDR BLOCK)** 复选框。
b) 在 **IPv6 CIDR 块 (IPv6 CIDR Block)** 中，输入 IPv6 前缀范围。

步骤 5 从**路由表 (Route Table)** 下拉列表中选择您之前创建的路由表之一。

步骤 6 为您的子网选择**子网访问 (Subnet Access)**。

对于“管理”(Management) 子网，这必须是**公共子网 (Public Subnet)**。

步骤 7 选择 **DHCP 选项 (DHCP Option)**。

步骤 8 选择您之前创建的**安全列表**。

步骤 9 点击**创建子网 (Create Subnet)**。

下一步做什么

配置管理 VCN（管理、诊断、内部、外部）后，您便可以启动 Firewall Threat Defense Virtual。有关 Firewall Threat Defense Virtual VCN 配置的示例，请参见下图。

图 ***3: Firewall Threat Defense Virtual*** 虚拟云网络

使用 Cloud Shell 配置 IPv6 网关地址

在 OCI 中，每个子网都有一个唯一的 IPv6 网关地址，您必须在 Firewall Threat Defense Virtual 中配置该地址，IPv6 流量才会正常工作。此网关地址可从在 Cloud Shell 中运行 OCI 命令的子网详细信息进行检索。

过程

步骤 1 转至 **OCI > 打开 CloudShell（OCI 云终端）(Open CloudShell [OCI Cloud Terminal])** 。

步骤 2 执行以下命令以便从子网获取 IPv6 详细信息：

```
oci network subnet get  -subnet_id <subnet_OCID>
```

步骤 3 从命令结果中查找 `ipv6-virtual-router-ip` 键。

步骤 4 复制该键的值并根据需要使用它。

在 OCI 上部署 Threat Defense Virtual

使用 Oracle Cloud 市场中的 Cisco Firepower NGFW 虚拟防火墙 (NGFWv) 产品通过计算实例在 OCI 上部署 Firewall Threat Defense Virtual。根据 CPU 数量、内存量和网络资源等特征来选择最合适的计算机形状。

过程

步骤 1 登录 OCI 门户。

区域显示在屏幕的右上角。确保您在预期的区域内。

步骤 2 选择**市场 (Marketplace)** > **应用程序 (Applications)**。

步骤 3 在市场中搜索“Cisco Firepower NGFW virtual firewall (NGFWv)”，然后选择产品。

步骤 4 查看条款和条件，然后选中**我已阅读并接受的Oracle使用条款和合作伙伴条款和条件 (I have reviewed and accept the Oracle Terms of Use and the Partner terms and conditions)** 复选框。

步骤 5 点击**启动实例 (Launch Instance)**。

步骤 6 输入您的实例的描述性**名称**，例如 *FTDv-6-7*。

步骤 7 点击**更改形状 (Change Shape)**，然后选择包含 Firewall Threat Defense Virtual 所需 CPU 数量、RAM 量和所需接口数量的形状，例如 VM.Standard2.4（请参阅概述，第 1 页）。

步骤 8 从**虚拟云网络 (Virtual Cloud Network)** 下拉列表中选择管理 VCN。

步骤 9 从**子网 (Subnet)** 下拉列表中选择管理子网（如果未自动填充）。

步骤 10 选中**使用网络安全组控制流量 (Use Network Security Groups to Control Traffic)**，然后选择为管理 VCN 配置的安全组。

步骤 11 点击**分配公共 IP 地址 (Assign a Public Ip Address)** 单选按钮。

步骤 12 在**添加 SSH 密钥 (Add SSH keys)** 下，点击**粘贴公共密钥 (Paste Public Keys)** 单选按钮并粘贴 SSH 密钥。

基于 Linux 的实例使用 SSH 密钥对而不是密码来对远程用户进行身份验证。密钥对包括私钥和公共密钥。您可以在创建实例时将私钥保留在计算机上并提供公共密钥。有关准则，请参阅管理 Linux 实例上的密钥对。

步骤 13 点击**显示高级选项 (Show Advanced Options)** 链接以展开选项。

步骤 14 在**初始化脚本 (Initialization Script)** 下，点击**粘贴云初始化脚本 (Paste Cloud-Init Script)** 单选按钮来为 Firewall Threat Defense Virtual 提供 day0 配置。day0 配置会在首次引导 Firewall Threat Defense Virtual 期间应用。

以下示例显示您可以在**云初始化脚本 (Cloud-Init Script)** 字段中复制和粘贴的示例 day0 配置：

```
{
"Hostname": "ftdv-oci",
"AdminPassword": "myPassword@123456",
"FirewallMode": "routed",
"IPv4Mode": "dhcp",
"IPv6Mode": "dhcp",
"ManageLocally":"No",
"FmcIp": "1.2.3.4",
"FmcRegKey": "cisco123reg",
```

```
"FmcNatId": "cisco123nat"
}
```

- **FmcRegKey** - 这是一次性使用的注册密钥，用于将设备注册到 防火墙管理中心。该注册密钥是任何用户定义的字母数字值，最长 37 个字符。
- **FmcNatId** - 这是一个唯一的一次性字符串（用户定义）。如果设备和 防火墙管理中心 之间被 NAT 设备分开，则必须输入唯一的 NAT ID 和唯一的注册密钥。

步骤 15 点击**创建 (Create)**。

下一步做什么

监控 Firewall Threat Defense Virtual 实例，点击**创建 (Create)** 按钮后，状态会显示为“正在调配”(Provisioning)。

重要事项 监控状态非常重要。一旦 Firewall Threat Defense Virtual实例从调配变为运行状态，您需要在 Firewall Threat Defense Virtual启动完成之前根据需要连接 VNIC。

连接接口

Firewall Threat Defense Virtual会进入运行状态并连接一个 VNIC（请参阅**计算 (Compute)** > **实例 (Instances)** > **实例详细信息 (Instance Details)** > **连接的 VNIC (Attached VNICs)**）。这称为主 VNIC，并会映射到管理 VCN。在 Firewall Threat Defense Virtual 完成首次启动之前，您需要为之前创建的其他 VCN 子网（诊断、内部、外部）连接 VNIC，以便在 Firewall Threat Defense Virtual 上正确检测 VNIC。

过程

步骤 1 选择新启动的 Firewall Threat Defense Virtual实例。

步骤 2 依次选择**连接的 VNIC (Attached VNICs)** > **创建 VNIC (Create VNIC)**。

步骤 3 输入 VNIC 的描述性**名称 (Name)**，例如 *Inside*。

步骤 4 从**虚拟云网络 (Virtual Cloud Network)** 下拉列表中选择 VCN。

步骤 5 从**子网 (Subnet)** 下拉列表选择您的子网。

步骤 6 选中**使用网络安全组控制流量 (Use Network Security Groups to Control Traffic)**，然后选择为所选 VCN 配置的安全组。

步骤 7 选中**跳过源目标 选中**使用网络安全组控制流量 (Use Network Security Groups to Control Traffic)。

步骤 8 （可选）指定**专用 IP 地址**。仅当您要为 VNIC 选择特定 IP 时，才需要执行此操作。

如果未指定 IP，OCI 将从您分配给子网的 CIDR 块分配 IP 地址。

步骤 9 点击**保存更改 (Save Changes)** 以创建 VNIC。

步骤 10 对部署所需的每个 VNIC 重复此程序。

为连接的 VNIC 添加路由规则

将路由表规则添加到诊断、内部和外部路由表。

过程

步骤 1 依次选择**网络 (Networking)** > **虚拟云网络 (Virtual Cloud Networks)**，然后点击与 VCN 关联的默认路由表（内部或外部）。

步骤 2 点击**添加路由规则 (Add Route Rules)**。

步骤 3 从**目标类型 (Target Type)** 下拉列表中，选择**专用 IP (Private IP)**。

步骤 4 从**目的类型 (Destination Type)** 下拉列表中选择**CIDR 块 (CIDR Block)**。

步骤 5 输入**目标 CIDR 块**，例如 0.0.0.0/0。

步骤 6 在**目标选择 (Target Selection)** 字段中输入 VNIC 的私有 IP 地址。

如果未向 VNIC 明确分配 IP 地址，则可以从 VNIC 详细信息（**计算 (Compute)** > **实例 (Instances)** > **实例详细信息 (Instance Details)** > **连接的 VNIC (Attached VNICs)**）中查找自动分配的 IP 地址。

步骤 7 点击**添加路由规则 (Add Route Rules)**。

如果要通过互联网网关配置 IPv6 互联网访问，请执行以下操作：

a) 从**目标类型 (Target Type)** 下拉列表中，选择**互联网网关 (Internet Gateway)**。
b) 在**目标 CIDR 块**中，指定 IP 地址
c) 从**目标互联网网关 (Target Internet Gateway)** 下拉列表中，选择现有互联网网关隔间或创建新的互联网网关隔间。

步骤 8 对部署所需的每个 VNIC 重复此程序。

注释
如果使用通过 DHCP 的路由规则或 IPv6 地址前缀配置的 IPv6 地址为 /128，则必须在 Firewall Threat Defense Virtual 路由表中添加以下路由。

ipv6 route <interface_name> <interface_subnet_CIDR> <ipv6_virtual_router_ip>

示例：

- `ipv6 route inside 2603:c020:5:5800::/64 fe80::200:17ff:fe96:921b`
- `ipv6 route outside 2603:c020:6:ba00::/64 fe80::200:17ff:fe21:748c`

使用 SSH 连接到 Firewall Threat Defense Virtual实例

要从 Unix 风格的系统连接到 Firewall Threat Defense Virtual 实例，请使用 SSH 登录实例。

过程

步骤 1 使用以下命令设置文件权限，以便只有您可以读取文件：

```
$ chmod 400 <private_key>
```

其中：

<private_key> 是文件的完整路径和名称，该文件包含与要访问的实例关联的私钥。

步骤 2 使用以下 SSH 命令访问实例：

```
$ ssh -i <private_key> <username>@<public-ip-address>
```

<private_key> 是文件的完整路径和名称，该文件包含与要访问的实例关联的私钥。

<username> 是 Firewall Threat Defense Virtual 实例的用户名。

<public-ip-address> 是您从控制台检索的实例 IP 地址。

使用 OpenSSH 连接到 Firewall Threat Defense Virtual实例

要从 Windows 系统连接到 Firewall Threat Defense Virtual 实例，请使用 OpenSSH 登录实例。

过程

步骤 1 如果这是您首次使用此密钥对，则必须设置文件权限，以便只有您能读取文件。

执行以下操作：

a) 在 Windows 资源管理器中，导航至私钥文件，右键点击该文件，然后点击**属性 (Properties)**。
b) 在**安全**选项卡上，点击**高级**。
c) 确保**所有者 (Owner)** 是您的用户帐户。
d) 点击**禁用继承 (Disable Inheritance)**，然后选择**将此对象的继承权限转换为显式权限 (Convert inherited permissions into explicit permissions on this object)**。
e) 选择不是您的用户帐户的每个权限条目，然后点击**删除 (Remove)**。
f) 确保您的用户帐户的访问权限为**完全控制 (Full control)**。
g) 保存更改。

步骤 2 要连接到实例，请打开 Windows PowerShell 并运行以下命令：

```
$ ssh -i <private_key> <username>@<public-ip-address>
```

其中：

<private_key> 是文件的完整路径和名称，该文件包含与要访问的实例关联的私钥。

<username> 是 Firewall Threat Defense Virtual 实例的用户名。

<public-ip-address> 是您从控制台检索的实例 IP 地址。

使用 PuTTY 连接到 Firewall Threat Defense Virtual实例

要使用 PuTTY 从 Windows 系统连接到 Firewall Threat Defense Virtual 实例，请执行以下操作：

过程

步骤 1 打开 PuTTY。

步骤 2 在**类别 (Category)** 窗格中，选择**会话 (Session)** 并输入以下内容：

- **主机名（或 IP 地址）：**

  <username>@<public-ip-address>

  其中：

  <username> 是 Firewall Threat Defense Virtual 实例的用户名。

  <public-ip-address> 是您从控制台检索的实例公共 IP 地址。

- **端口：** 22
- **连接类型：** SSH

步骤 3 在**类别 (Category)** 窗格中，展开**窗口 (Window)**，然后选择**转换 (Translation)**。

步骤 4 在**远程字符集 (Remote character set)** 下拉列表中，选择 **UTF-8**。

基于 Linux 的实例的默认区域设置为 UTF-8，这样会将 PuTTY 配置为使用相同的区域设置。

步骤 5 在**类别 (Category)** 窗格中，依次展开**连接 (Connection)** 和 **SSH**，然后点击**身份验证 (Auth)**。

步骤 6 点击**浏览 (Browse)**，然后选择您的私钥。

步骤 7 点击**打开 (Open)** 以启动会话。

如果这是第一次连接到实例，您可能会看到一条消息，表明服务器的主机密钥未缓存在注册表中。点击**是**以继续连接。

IPv6 故障排除

问题 SSH - 使用 IPv6 的 Firewall Threat Defense Virtual 不工作

- 解决方法 确保已添加通过互联网网关进行 IPv6 公共访问的路由。
- 解决方法 Firewall Threat Defense Virtual 管理配置中存在启用 IPv6。
- 解决方法 验证已将 IPv6 相关访问列表添加到已部署的 Firewall Threat Defense Virtual。
- 解决方法 验证是否使用“ipv6 address dhcp default”在管理接口上配置 IPv6。如果仅使用“ipv6 address dhcp”，则单独添加以下路由“ipv6 route management ::/0<IPv6_Gateway_address>”。
- 解决方法 验证是否允许正确的 ssh 入口。使用以下命令为所有“ssh ::/0 management”设置 ssh access allow。

问题 无法将 IPv6 地址分配给现有子网。

- 解决方法 验证子网所属的 VCN 是否已启用 IPv6。
- 解决方法 确保使用的是正确的 IPv6 CIDR。
- 解决方法 子网只能包含“/64”IPv6 CIDR 前缀。

问题 东西向流量不起作用。

- 解决方法 验证是否已正确添加以下路由。

  解决方法 ipv6 route <interface_name> <interface_subnet_CIDR> <ipv6_virtual_router_ip>

  解决方法 示例：ipv6 route inside 2603:c020:5:5800::/56 fe80::200:17ff:fe96:921b

- 解决方法 确保使用的是正确的 IPv6 CIDR。
- 解决方法 确保是否为 IPv6 配置了正确的访问列表。

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。

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。

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。