Cisco Secure Firewall Threat Defense 兼容性指南

上次修改日期: 2025 年 1 月 17 日

Cisco Cisco Secure Firewall Threat Defense 兼容性指南

本指南介绍适用于思科 Cisco Secure Firewall Threat Defense 的软件和硬件兼容性。有关相关兼容性指南，请参阅下表。

注释 并非所有软件版本（尤其是补丁）都适用于所有平台。判断是否支持某个版本的一种快速方法是在思科支持和下载站点上发布其升级/安装软件包。如果站点“缺少”升级或安装软件包，则表示不支持该版本。您还可以查看版本说明和寿命终止通知，第 37 页。如果您认为遗漏了某个版本，请联系思科 TAC。

表 *1:* 其他资源

说明	资源
支持公告 提供思科下一代防火墙产品系列（包括管理平台和操作系统）的支持时间安排。	思科 NGFW 产品系列软件版本和支持公告
兼容性指南 提供支持的硬件型号和软件版本的详细兼容性信息，包括捆绑的组件和集成产品。	Cisco Secure Firewall Management Center 兼容性指南 思科 Firepower 4100/9300 FXOS 兼容性
发行说明 提供了至关重要和版本特定的信息，包括升级警告和行为更改。版本说明还包含升级和安装说明的快速链接。	Cisco Secure Firewall Threat Defense 版本说明 思科 Firepower 4100/9300 FXOS 发行说明
新功能指南 按版本提供新功能和弃用功能的信息。	Cisco Secure Firewall Management Center 各版本的新增功能 Cisco Secure Firewall 设备管理器各版本的新增功能
文档路线图 提供指向当前可用和旧版文档的链接。如果您要查找的内容未在上面列出，请尝试使用规划图。	浏览 Cisco Secure Firewall Threat Defense 文档 浏览思科 FXOS 文档

建议的版本：版本 7.4.2

要利用新功能和已解决的问题，我们建议您将所有符合条件的设备至少升级到建议的版本，包括最新的补丁。在 思科支持和下载站点 上，建议的版本标有金色星号。在版本 7.2.6+/7.4.1+ 中，管理中心会在有新的建议发布版本时通知您，并在产品升级页面上显示建议发布版本。

较旧设备的建议版本

如果设备太旧，无法运行建议的版本，而且现在不打算更新硬件，则应选择一个主要版本，然后尽可能安装补丁。一些主要版本被指定为长期或超长期，因此请考虑其中一个版本。有关这些术语的解释，请参阅思科 NGFW 产品系列软件版本和支持公告。

如果您对硬件刷新感兴趣，请联系思科代表或合作伙伴联系人。

威胁防御平台摘要

这些表总结了 威胁防御支持的设备和本地（客户部署）管理方法。

注释 云交付的防火墙管理中心 可以管理威胁防御 7.0.3 至 7.6.0（7.1 除外）。对于带有设备管理器的 CDO，必须至少运行威胁防御 6.4。

威胁防御 硬件

表 *2: Cisco Secure Firewall Threat Defense* 按管理器和版本划分的硬件

设备平台	设备版本：使用本地部署管理中心	设备版本：使用设备管理器
Firepower 1010、1120 和 1140	6.4+	6.4+
Firepower 1010E	7.2.3+ 7.3 中不支持	7.2.3+ 7.3 中不支持
Firepower 1150	6.5+	6.5+
Cisco Secure Firewall 1210、1220	7.6+	7.6+
Firepower 2110、2120、2130、2140	6.2.1 至 7.4	6.2.1 至 7.4
Secure Firewall 3105	7.3.1+	7.3.1+
安全防火墙 3110, 3120, 3130, 3140	7.1+	7.1+
Firepower 4110, 4120, 4140	6.0.1 至 7.2	6.5 到 7.2
Firepower 4150	6.1 到 7.2	6.5 到 7.2
Firepower 4115、4125、4145	6.4+	6.5+

设备平台	设备版本：使用本地部署管理中心	设备版本：使用设备管理器
Firepower 4112	6.6+	6.6+
Cisco Secure Firewall 4215、4225、4245	7.4.0+	—
Firepower 9300: SM-24, SM-36, SM-44	6.0.1 至 7.2	6.5 到 7.2
Firepower 9300: SM-40, SM-48, SM-56	6.4+	6.5+
ISA 3000	6.2.3+	6.2.3+
ASA 5506-X、5506H-X、5506W-X	6.0.1 至 6.2.3	6.1 至 6.2.3
ASA 5508-X、5516-X	6.0.1 至 7.0	6.1 至 7.0
ASA 5512-X	6.0.1 至 6.2.3	6.1 至 6.2.3
ASA 5515-X	6.0.1 至 6.4	6.1 至 6.4
ASA 5525-X、5545-X、5555-X	6.0.1 至 6.6	6.1 至 6.6

Threat Defense Virtual

表 *3:* 按管理器和版本*Threat Defense Virtual*

设备平台	设备版本：使用本地部署管理中心	设备版本：使用设备管理器
公共云		
AWS	6.0.1+	6.6+
Azure	6.2+	6.5+
GCP	6.7+	7.2+
OCI	6.7+	—
Megaport	7.2.8+	7.2.8+
本地/私有云		
HyperFlex	7.0+	7.0+
KVM	6.1+	6.2.3+
Nutanix	7.0+	7.0+
OpenStack	7.0+	-

设备平台	设备版本：使用本地部署管理中心	设备版本：使用设备管理器
VMware 8.0	7.6+	7.6+
VMware 7.0	7.0+	7.0+
VMware 6.7	6.5+	6.5+
VMware 6.5	6.2.3+	6.2.3+
VMware 6.0	6.0 至 6.7	6.2.2 至 6.7
VMware 5.5	6.0.1 至 6.2.3	6.2.2 至 6.2.3
VMware 5.1	仅 6.0.1	-

威胁防御硬件

Firepower 1000/2100 系列

Firepower 1000/2100 系列设备使用 FXOS 操作系统。升级威胁防御会自动升级 FXOS。有关捆绑的 FXOS 版本的信息，请参阅捆绑组件，第 18 页。这些设备还可以运行 ASA 而非威胁防御；请参阅 Cisco Secure Firewall ASA 兼容性。

表 *4: Firepower 1000/2100* 系列兼容性

威胁防御	**Firepower 1150**	**Firepower 1010E**	**Firepower 1010** **Firepower 1120** **Firepower 1140**	**Firepower 2110** **Firepower 2120** **Firepower 2130** **Firepower 2140**
7.6	是	是	是	-
7.4.1 – 7.4.x	是	是	是	是
7.4.0	-	—	—	—
7.3	是	-	是	是
7.2	是	是 需要 7.2.3+	是	是
7.1	是	-	是	是
7.0	是	-	是	是
6.7	是	-	是	是

威胁防御	Firepower 1150	Firepower 1010E	Firepower 1010 Firepower 1120 Firepower 1140	Firepower 2110 Firepower 2120 Firepower 2130 Firepower 2140
6.6	是	-	是	是
6.5	是	-	是	是
6.4	-	—	是	是
6.3	-	—	—	是
6.2.3	-	—	—	是
6.2.2	-	—	—	是
6.2.1	-	—	—	是

Cisco Secure Firewall 1200 系列

Cisco Secure Firewall 1200 系列设备使用 FXOS 操作系统。升级威胁防御会自动升级 FXOS。有关捆绑的 FXOS 版本的信息，请参阅捆绑组件，第 18 页。这些设备还可以运行 ASA 而非威胁防御；请参阅Cisco Secure Firewall ASA 兼容性。

表 *5: Cisco Secure Firewall 1200* 系列兼容性

威胁防御	Cisco Secure Firewall 1210 Cisco Secure Firewall 1220
7.6	是

Cisco Secure Firewall 3100/4200 系列

Cisco Secure Firewall 3100/4200 系列设备使用 FXOS 操作系统。FXOS 如何升级取决于设备是处于应用模式还是多实例模式。这些设备还可以运行 ASA 而非威胁防御；请参阅Cisco Secure Firewall ASA 兼容性。

应用模式

在设备模式下，升级 威胁防御 时会自动升级 FXOS。有关捆绑的 FXOS 版本的信息，请参阅捆绑组件，第 18 页。

表 *6: Cisco Secure Firewall 3100/4200* 系列应用模式兼容性

威胁防御	**Cisco Secure Firewall 4215** **Cisco Secure Firewall 4225** **Cisco Secure Firewall 4245**	**Cisco Secure Firewall 3105**	**Cisco Secure Firewall 3110** **Cisco Secure Firewall 3120** **Cisco Secure Firewall 3130** **Cisco Secure Firewall 3140**
7.6	是	是	是
7.4.1 – 7.4.x	是	是	是
7.4.0	是	-	—
7.3	-	是	是
7.2	-	—	是
7.1	-	—	是

多实例模式

在多实例模式下，可分别升级机箱（FXOS 和固件）和威胁防御。但是，一个软件包同时包含了这两个组件。可以只进行机箱升级，也可以只进行威胁防御升级。有关捆绑的 FXOS 版本的信息，请参阅捆绑组件，第 18 页。

虽然您可以在较新的 FXOS 上运行较旧的威胁防御实例，但新功能和已解决的问题通常需要完全升级。

表 *7: Cisco Secure Firewall 3100/4200* 系列多实例模式兼容性

威胁防御	**Cisco Secure Firewall 4215** **Cisco Secure Firewall 4225** **Cisco Secure Firewall 4245**	**Cisco Secure Firewall 3110** **Cisco Secure Firewall 3120** **Cisco Secure Firewall 3130** **Cisco Secure Firewall 3140**
7.6	是	是
7.4.1 – 7.4.x	-	是

Firepower 4100/9300

对于 Firepower 4100/9300，主要 威胁防御 版本具有一个特别限定和推荐的配套 FXOS 版本，下文以**粗体**列出。请尽可能使用这些组合，因为我们会对其执行增强测试。请注意，该表列出了每个FXOS

版本的最低内部版本，但在大多数情况下，我们建议使用最新版本。有关详细信息，请参阅思科 Firepower 4100/9300 FXOS 发行说明。

注释 虽然我们记录了威胁防御 7.4.x 需要 FXOS 2.14.1.163+，但这适用于重新映像到 7.4.2+。如果您已在运行早期的 FXOS 2.14.1 版本，则可以成功升级到 7.4.2+，而无需升级 FXOS (CSCwf64429)。

这些设备也可以运行 ASA，而不是 威胁防御。在 ASA 9.12+ 和 威胁防御 6.4.0+ 中，您可以在同一 Firepower 9300 机箱中的不同模块上运行 ASA 和 威胁防御。有关详细信息，请参阅思科 Firepower 4100/9300 FXOS 兼容性。

表 *8: Firepower 4100/9300* 兼容性

威胁防御	FXOS	Firepower 9300		Firepower 4100 系列			
		SM-24 SM-36 SM-44	SM-40 SM-48 SM-56	4110 4120 4140	4150	4112	4115 4125 4145
7.6	**2.16.0.128+**	-	是	-	—	是	是
7.4.1 – 7.4.x	**2.14.1.163+** 2.16.0.128+	-	是	-	—	是	是
7.4.0	-	—	—	—	—	—	—
7.3	**2.13.0.198+** 2.14.1.163+ 2.16.0.128+	-	是	-	—	是	是
7.2	**2.12.0.31+** 2.13.0.198+ 2.14.1.163+ 2.16.0.128+	是 无 2.13+	是	是 无 2.13+	是 无 2.13+	是	是
7.1	**2.11.1.154+** 2.12.0.31+ 2.13.0.198+ 2.14.1.163+ 2.16.0.128+	是 无 2.13+	是	是 无 2.13+	是 无 2.13+	是	是

威胁防御	FXOS	Firepower 9300		Firepower 4100 系列			
		SM-24 **SM-36** **SM-44**	**SM-40** **SM-48** **SM-56**	**4110** **4120** **4140**	**4150**	**4112**	**4115** **4125** **4145**
7.0	**2.10.1.159+** 2.11.1.154+ 2.12.0.31+ 2.13.0.198+ 2.14.1.163+	是 无 2.13+	是	是 无 2.13+	是 无 2.13+	是	是
6.7	**2.9.1.131+** 2.10.1.159+ 2.11.1.154+ 2.12.0.31+ 2.13.0.198+ 2.14.1.163+	是 无 2.13+	是	是 无 2.13+	是 无 2.13+	是	是
6.6	**2.8.1.105+** 2.9.1.131+ 2.10.1.159+ 2.11.1.154+ 2.12.0.31+ 2.13.0.198+ 2.14.1.163+	是 无 2.13+	是	是 无 2.13+	是 无 2.13+	是	是
6.5	**2.7.1.92+** 2.8.1.105+ 2.9.1.131+ 2.10.1.159+ 2.11.1.154+ 2.12.0.31+	是	是	是	是	-	是

威胁防御	FXOS	Firepower 9300		Firepower 4100 系列			
		SM-24 SM-36 SM-44	SM-40 SM-48 SM-56	4110 4120 4140	4150	4112	4115 4125 4145
6.4	**2.6.1.157+** 2.7.1.92+ 2.8.1.105+ 2.9.1.131+ 2.10.1.159+ 2.11.1.154+ 2.12.0.31+	是	是	是	是	-	是
6.3	**2.4.1.214+** 2.6.1.157+ 2.7.1.92+ 2.8.1.105+ 2.9.1.131+ 2.10.1.159+ 2.11.1.154+ 2.12.0.31+	是	-	是	是	-	—
6.2.3	**2.3.1.73 及更高版本** 2.4.1.214+ 2.6.1.157+ 2.7.1.92+ 2.8.1.105+ 注释 Firepower 6.2.3.16+ 需要 FXOS 2.3.1.157+。	是	-	是	是	-	—

威胁防御	FXOS	Firepower 9300		Firepower 4100 系列			
		SM-24 SM-36 SM-44	SM-40 SM-48 SM-56	4110 4120 4140	4150	4112	4115 4125 4145
6.2.2	**2.2.2.x** 2.3.1.73 及更高版本 2.4.1.214+ 2.6.1.157+ 2.7.1.92+	是	-	是	是	-	—
6.2.1	-	—	—	—	—	—	—
6.2.0	**2.1.1.x**、**2.2.1.x**、**2.2.2.x** 2.3.1.73 及更高版本 2.4.1.214+ 2.6.1.157+	是	-	是	是	-	—
6.1	**2.0.1.x** 2.1.1.x 2.3.1.73 及更高版本	是	-	是	是	-	—
6.0.1	**1.1.4.x** 2.0.1.x	是	-	是	-	—	—

ASA 5500-X 系列和 ISA 3000

ASA 5500-X 系列和 ISA 3000 设备使用 ASA 操作系统。升级 威胁防御 时会自动升级 ASA。有关捆绑的 ASA 版本的信息，请参阅捆绑组件，第 18 页。

版本 7.0 是支持 ASA 5500-X 系列设备的最后一个主要 威胁防御 版本。

表 *9: ASA 5500-X* 系列和 *ISA 3000* 兼容性

威胁防御	ISA 3000	ASA 5508-X ASA 5516-X	ASA 5525-X ASA 5545-X ASA 5555-X	ASA 5515-X	ASA 5506-X ASA 5506H-X ASA 5506W-X ASA 5512-X
7.6	是	-	—	—	—
7.4.1 – 7.4.x	是	-	—	—	—
7.4.0	-	—	—	—	—
7.3	是	-	—	—	—
7.2	是	-	—	—	—
7.1	是	-	—	—	—
7.0	是	是	-	—	—
6.7	是	是	-	—	—
6.6	是	是	是	-	—
6.5	是	是	是	-	—
6.4	是	是	是	是	-
6.3	是	是	是	是	-
6.2.3	是	是	是	是	是
6.2.2	-	是	是	是	是
6.2.1	-	—	—	—	—
6.2.0	-	是	是	是	是
6.1	-	是	是	是	是
6.0.1	-	是	是	是	是

Threat Defense Virtual

表 *10: Threat Defense Virtual* 兼容性：公共云

Threat Defense Virtual	Amazon Web Services (AWS)	Microsoft Azure (Azure)	Google 云平台 (GCP)	兆端口虚拟边缘（兆端口）	Oracle 云基础设施 (OCI)
7.6	是	是	是	是	是
7.4.1 – 7.4.x	是	是	是	是	是
7.4.0	-	—	—	—	—
7.3	是	是	是	是	是
7.2	是	是	是	是 需要 7.2.8+	是
7.1	是	是	是	-	是
7.0	是	是	是	-	是
6.7	是	是	是	-	是
6.6	是	是	-	—	—
6.6	是	是	-	—	—
6.4	是	是	-	—	—
6.3	是	是	-	—	—
6.2.3	是	是	-	—	—
6.2.2	是	是	-	—	—
6.2.1	-	—	—	—	—
6.2	是	是	-	—	—
6.1	是	-	—	—	—
6.0.1	是	-	—	—	—

表 *11: Threat Defense Virtual* 兼容性：本地/私有云

Threat Defense Virtual	VMware vSphere/VMware ESXi	思科 HyperFlex (HyperFlex)	基于内核的虚拟机 (KVM)	Nutanix 企业云 (Nutanix)	OpenStack
7.6	是 VMware 6.5、6.7、7.0、8.0	是	是	是	是
7.4.2 – 7.4.x	是 VMware 6.5、6.7、7.0、8.0	是	是	是	是
7.4.1	是 VMware 6.5、6.7、7.0	是	是	是	是
7.4.0	-	—	—	—	—
7.3	是 VMware 6.5、6.7、7.0	是	是	是	是
7.2	是 VMware 6.5、6.7、7.0	是	是	是	是
7.1	是 VMware 6.5、6.7、7.0	是	是	是	是
7.0	是 VMware 6.5、6.7、7.0	是	是	是	是
6.7	是 VMware 6.0、6.5、6.7	-	是	-	—
6.6	是 VMware 6.0、6.5、6.7	-	是	-	—
6.5	是 VMware 6.0、6.5、6.7	-	是	-	—
6.4	是 VMware 6.0、6.5	-	是	-	—

Threat Defense Virtual	VMware vSphere/VMware ESXi	思科 HyperFlex (HyperFlex)	基于内核的虚拟机 (KVM)	Nutanix 企业云 (Nutanix)	OpenStack
6.3	是 VMware 6.0、6.5	-	是	-	—
6.2.3	是 VMware 5.5、6.0、6.5	-	是	-	—
6.2.2	是 VMware 5.5、6.0	-	是	-	—
6.2.1	-	—	—	—	—
6.2.0	是 VMware 5.5、6.0	-	是	-	—
6.1	是 VMware 5.5、6.0	-	是	-	—
6.0.1	是 VMware 5.1、5.5	-	—	—	—

威胁防御高可用性和群集

这些表格列出了对高可用性和集群的威胁防御支持。对于威胁防御硬件，支持的不同取决于您使用的是独立设备（也称为本机实例或应用模式）还是容器实例（也称为多实例模式）。虚拟威胁防御不支持容器实例。

独立设备

下表列出了威胁防御硬件对独立设备高可用性和集群的支持。在管理中心部署中，所有威胁防御硬件都支持高可用性。对于设备管理器，从版本 6.3 开始支持高可用性，但不支持群集。

表 *12:* 硬件独立设备：高可用性和集群支持

平台	高可用性	集群
Firepower 1000	是	-
Cisco Secure Firewall 1200	是	-
Firepower 2100	是	-

平台	高可用性	集群
Cisco Secure Firewall 3100	是	7.6+（16 节点） 7.1+（8 节点）
Cisco Secure Firewall 4200	是	7.6+（16 节点） 7.4+（8 节点）
Firepower 4100	是	7.2+（16 节点） 6.2+（6 节点）
Firepower 9300	是	7.2+（16 节点） 6.2+（6 节点） 所有版本还支持机箱内集群（3 节点）。
ASA 5500-X	是	-
ISA 3000	是	-

下表列出了对高可用性（使用管理中心或设备管理器）和集群（仅使用管理中心）的 Threat Defense Virtual 支持。

表 *13:* 虚拟独立设备：高可用性和集群支持

平台	高可用性	集群
公共云		
AWS	-	7.2+（16 节点）
Azure	—	7.3+（16 节点）
GCP	—	7.3+（16 节点）
Megaport	7.2.8+	—
OCI	-	—
本地/私有云		
HyperFlex	-	—
KVM	7.3+	7.4.1+（16 节点） 7.2+（4 节点）
Nutanix	-	—

平台	高可用性	集群
OpenStack	-	—
VMware	6.7+	7.4.1+（16 节点） 7.2+（4 节点）

容器实例

下表列出了对容器实例高可用性和集群的支持，仅在管理中心部署的特定威胁防御硬件上提供。

表 *14:* 容器实例：高可用性和集群支持

平台	高可用性	集群
Cisco Secure Firewall 3100 系列	7.4.1+	-
Secure Firewall 4200 系列	7.6+	-
Firepower 4100 系列	6.3+	7.2+（16 节点） 6.6+（6 节点）
Firepower 9300	6.3+	7.2+（16 节点） 6.6+（6 节点） 版本 6.6+ 还支持机箱内集群（3 节点）。

威胁防御管理

本地管理中心

所有设备均支持通过客户部署的（本地）管理中心 来进行远程管理，但其必须运行与其受管设备相同或更高的版本。这意味着：

- 您可以使用较新的 管理中心（通常有几个主要版本）来管理较旧的设备。但是，我们建议您始终更新整个部署。新功能和已解决的问题通常同时需要 管理中心 及其托管设备上的最新版本。
- 您不能将设备升级超过 管理中心。即使对于维护（第三位数）版本，您也必须首先升级 管理中心。

请注意，在大多数情况下，您可以将较早的设备直接升级到 管理中心 的主要或维护版本。但有时您可以管理无法直接升级的旧设备，即使该设备支持目标版本。在极少数情况下，特定 管理中心 设备组合会出现问题。有关版本特定的要求，请参阅版本说明。

表 *15:* 本地 管理中心 设备兼容性

管理中心 版本	您可以管理的最旧设备版本
7.6	7.1
7.4 对 NGIPS 设备管理的最新支持。	7.0
7.3	6.7
7.2	6.6
7.1	6.5
7.0	6.4
6.7	6.3
6.6	6.2.3
6.5	6.2.3
6.4	6.1
6.3	6.1
6.2.3	6.1
6.2.2	6.1
6.2.1	6.1
6.2	6.1
6.1	5.4.0.2/5.4.1.1
6.0.1	5.4.0.2/5.4.1.1
6.0	5.4.0.2/5.4.1.1
5.4.1	适用于 ASA-5506-X 系列、ASA5508-X 和 ASA5516-X 上的 ASA FirePOWER 的 5.4.1。 适用于 ASA5512-X、ASA5515-X、ASA5525-X、ASA5545-X、ASA5555-X 和 ASA-5585-X 系列上的 ASA FirePOWER 的 5.3.1。 适用于 Firepower 7000/8000 系列和传统设备的 5.3.0。

云交付的防火墙管理中心

云交付的防火墙管理中心 可以管理运行**版本 7.0.3 至 7.6.0**（**版本 7.1 除外**）的 威胁防御 设备。

您可以通过版本7.2+本地管理中心来统一管理云托管设备，以便仅用于事件日志记录和分析目的。或者，您可以通过 Security Analytics and Logging (SaaS)将事件发送至思科云。

通过分析管理中心统一管理设备

云交付的防火墙管理中心支持比本地管理中心更广泛的托管设备版本。如果使用内部管理中心进行分析，这可能会造成问题，因为设备可能“太旧”或“太新”，无法统一管理。

您可能无法：

- 向分析管理中心注册较新的设备，因为较旧的设备阻止所需的管理中心升级。
- 将共同管理的设备升级到最新版本，因为分析管理中心“卡住”在较旧的版本上。
- 恢复设备升级，如果恢复会使设备与分析管理中心不兼容。

例如，假设您想将 7.6.0 版统一管理设备添加到当前包含 7.0.x 版统一管理设备的部署中。云交付的防火墙管理中心可以管理所有这些设备，但本地分析管理中心无法管理。

按偏好顺序，您可以：

- 将 7.0.x 版设备至少升级到 7.2.0 版，将分析管理中心升级到 7.6.0 版，然后将 7.6.0 版设备添加到两个管理中心。
- 从分析管理中心删除 7.0.x 版设备，将分析管理中心升级到 7.6.0 版，然后将 7.6.0 版设备添加到两个管理中心。
- 将分析管理中心保持原样，不添加 7.6.0 版设备。

也就是说，您的选择包括：

- 要从所有设备获取事件，请升级（或更换）分析管理中心和旧设备。
- 要放弃来自旧设备的事件，只需升级（或更换）分析管理中心。
- 要放弃来自较新设备的事件，可将分析管理中心保留为较旧的版本。

设备管理器

您可以使用 设备管理器 在本地管理单个 威胁防御 设备。大多数型号都支持本地管理。

或者，添加 思科防御协调器 以远程管理多个 威胁防御 设备，作为 管理中心 的替代方案。虽然某些配置仍需要 设备管理器，但 CDO 允许您在 威胁防御 部署中建立和维护一致的安全策略。

捆绑组件

这些表格列出了与威胁防御捆绑的各种组件的版本。可使用这些信息来确定捆绑组件中可能影响您的部署的未解决或已解决的漏洞。

请注意，有时我们会针对特定版本发布更新版本。如果捆绑的组件在内部版本之间发生变化，我们会列出最新版本中的组件。（在大多数情况下，只有最新版本可供下载。）有关新版本及其解决的问题的详细信息，请参阅适用于您的版本的发行说明。

操作系统

ASA 5500-X 系列和 ISA 3000 设备使用 ASA 操作系统。Firepower 1000/2100、Cisco Secure Firewall 1200 和 Cisco Secure Firewall 3100/4200 系列设备使用 FXOS 操作系统。对于 Firepower 4100/9300，请参阅Firepower 4100/9300 ， 第 6 页。

表 *16:*

威胁防御	ASA	FXOS
7.6.0	9.22(1.1)	2.16.0.128
7.4.2.1	9.20.2.36	2.14.1.176
7.4.2	9.20(2.32)	2.14.1.167
7.4.1.1	9.20(2.201)	2.14.1.131
7.4.1	9.20(2.2)	2.14.1.131
7.4.0	9.20(1.84)	2.14.0.475
7.3.1.1	9.19(1.202)	2.13.0.1022
7.3.1	9.19(1.200)	2.13.0.1022
7.3.0	9.19(1)	2.13.0.198
7.2.9	9.18(4.47)	2.12.1.86
7.2.8.1	9.18(4.212)	2.12.1.1703
7.2.8	9.18(4.210)	2.12.1.73
7.2.7	9.18(4.201)	2.12.1.73
7.2.6	9.18(4.22)	2.12.1.73
7.2.5.2	9.18(3.61)	2.12.0.530
7.2.5.1	9.18(3.60)	2.12.0.530
7.2.5	9.18(3.53)	2.12.0.519
7.2.4.1	9.18(3.53)	2.12.0.519
7.2.4	9.18(3.39)	2.12.0.499
7.2.3.1	-	—
7.2.3	9.18(2.219)	2.12.0.1030
7.2.2	9.18(2.200)	2.12.0.1104
7.2.1	9.18(2.4)	2.12.0.442

威胁防御	ASA	FXOS
7.2.0.1	9.18(1.200)	2.12.0.31
7.2.0	9.18(1)	2.12.0.31
7.1.0.3	9.17(1.24)	2.11.1.191
7.1.0.2	9.17(1.201)	2.11.1.1300
7.1.0.1	9.17(1.150)	2.11.1.154
7.1.0	9.17(1.0)	2.11.1.154
7.0.6.3	9.16(4.70)	2.10.1.1633
7.0.6.2	9.16(4.57)	2.10.1.1625
7.0.6.1	9.16(4.45)	2.10.1.1614
7.0.6	9.16(4.35)	2.10.1.1603
7.0.5.1	-	—
7.0.5	9.16(4.200)	2.10.1.1400
7.0.4	9.16(3.18)	2.10.1.208
7.0.3	9.16(3.201)	2.10.1.1200
7.0.2.1	9.16(3.200)	2.10.1.192
7.0.2	9.16(3.11)	2.10.1.192
7.0.1.1	9.16(2.5)	2.10.1.175
7.0.1	9.16(2.5)	2.10.1.175
7.0.0.1	9.16(1.25)	2.10.1.159
7.0.0	9.16(1)	2.10.1.159
6.7.0.3	9.15(1.19)	2.9.1.138
6.7.0.2	9.15(1.15)	2.9.1.138
6.7.0.1	9.15(1.8)	2.9.1.135
6.7.0	9.15(1)	2.9.1.131
6.6.7.2	9.14(4.201)	2.8.1.192
6.6.7.1	9.14(4.21)	2.8.1.192
6.6.7	9.14(4.13)	2.8.1.186
6.6.5.2	9.14(3.22)	2.8.1.172

威胁防御	ASA	FXOS
6.6.5.1	9.14(3.15)	2.8.1.172
6.6.5	9.14(3.6)	2.8.1.165
6.6.4	9.14(2.155)	2.8.1.1148
6.6.3	9.14(2.151)	2.8.1.1146
6.6.1	9.14(1.150)	2.8.1.129
6.6.0.1	9.14(1.216)	2.8.1.105
6.6.0	9.14(1.1)	2.8.1.105
6.5.0.5	9.13(1.18)	2.7.1.129
6.5.0.4	9.13(1.5)	2.7.1.117
6.5.0.3	9.13(1.4)	2.7.1.117
6.5.0.2	9.13(1.151)	2.7.1.115
6.5.0.1	9.13(1.2)	2.7.1.115
6.5.0	9.13(1)	2.7.1.107
6.4.0.18	9.12(4.68)	2.6.1.272
6.4.0.17	9.12(4.62)	2.6.1.265
6.4.0.16	9.12(4.54)	2.6.1.260
6.4.0.15	9.12(4.41)	2.6.1.254
6.4.0.14	9.12(4.37)	2.6.1.239
6.4.0.13	9.12(4.37)	2.6.1.239
6.4.0.12	9.12(4.152)	2.6.1.230
6.4.0.11	9.12(2.40)	2.6.1.214
6.4.0.10	9.12(2.38)	2.6.1.214
6.4.0.9	9.12(2.33)	2.6.1.201
6.4.0.8	9.12(2.18)	2.6.1.166
6.4.0.7	9.12(2.151)	2.6.1.156
6.4.0.6	9.12(2.12)	2.6.1.156
6.4.0.5	9.12(2.4)	2.6.1.144
6.4.0.4	9.12(2.4)	2.6.1.144

威胁防御	ASA	FXOS
6.4.0.3	9.12(1.12)	2.6.1.133
6.4.0.2	9.12(1.10)	2.6.1.133
6.4.0.1	9.12(1.7)	2.6.1.133
6.4.0	9.12(1.6)	2.6.1.133
6.3.0.5	9.10(1.31)	2.4.1.255
6.3.0.4	9.10(1.28)	2.4.1.248
6.3.0.3	9.10(1.18)	2.4.1.237
6.3.0.2	9.10(1.12)	2.4.1.237
6.3.0.1	9.10(1.8)	2.4.1.222
6.3.0	9.10(1.3)	2.4.1.216
6.2.3.18	9.9(2.91)	2.3.1.219
6.2.3.17	9.9(2.88)	2.3.1.217
6.2.3.16	9.9(2.74)	2.3.1.180
6.2.3.15	9.9(2.60)	2.3.1.167
6.2.3.14	9.9(2.55)	2.3.1.151
6.2.3.13	9.9(2.51)	2.3.1.144
6.2.3.12	9.9(2.48)	2.3.1.144
6.2.3.11	9.9(2.43)	2.3.1.132
6.2.3.10	9.9(2.41)	2.3.1.131
6.2.3.9	9.9(2.37)	2.3.1.122
6.2.3.8	9.9(2.37)	2.3.1.122
6.2.3.7	9.9(2.32)	2.3.1.118
6.2.3.6	9.9(2.26)	2.3.1.115
6.2.3.5	9.9(2.245)	2.3.1.108
6.2.3.4	9.9(2.15)	2.3.1.108
6.2.3.3	9.9(2.13)	2.3.1.104
6.2.3.2	9.9(2.8)	2.3.1.85
6.2.3.1	9.9(2.4)	2.3.1.84

威胁防御	ASA	FXOS
6.2.3	9.9(2)	2.3.1.84
6.2.2.5	9.8(2.44)	2.2.2.107
6.2.2.4	9.8(2.36)	2.2.2.86
6.2.2.3	9.8(2.30)	2.2.2.79
6.2.2.2	9.8(2.22)	2.2.2.75
6.2.2.1	9.8(2.10)	2.2.2.63
6.2.2	9.8(2.3)	2.2.2.52
6.2.1	9.8(1)	2.2.1.49
6.2.0.6	9.7(1.25)	—
6.2.0.5	9.7(1.23)	—
6.2.0.4	9.7(1.19)	—
6.2.0.3	9.7(1.15)	—
6.2.0.2	9.7(1.10)	—
6.2.0.1	9.7(1.7)	-
6.2.0	9.7(1.4)	—
6.1.0.7	9.6(4.12)	—
6.1.0.6	9.6(3.23)	—
6.1.0.5	9.6(2.21)	—
6.1.0.4	9.6(2.16)	—
6.1.0.3	9.6(2.16)	—
6.1.0.2	9.6(2.4)	—
6.1.0.1	9.6(2.4)	-
6.1.0	9.6(2)	—
6.0.1.4	9.6(1.19)	—
6.0.1.3	9.6(1.12)	—
6.0.1.2	9.6(1.11)	—

威胁防御	ASA	FXOS
6.0.1.1	9.6(1)	-
6.0.1	9.6(1)	—
6.0.0.1	9.6(1)	-
6.0.0	9.6(1)	—

Snort

Snort 是主要的检测引擎。Snort 3 在带有 设备管理器 的版本 6.7+ 和带有 管理中心 的版本 7.0+ 中可用。

表 *17:*

威胁防御	Snort 2	Snort 3
7.6.0	2.9.23-227	3.1.79.1-121
7.4.2.1	2.9.22-2000	3.1.53.201-112
7.4.2	2.9.22-2000	3.1.53.200-107
7.4.1.1	2.9.22-1103	3.1.53.100-56
7.4.1	2.9.22-1009	3.1.53.100-56
7.4.0	2.9.22-181	3.1.53.1-40
7.3.1.1	2.9.21-1109	3.1.36.101-2
7.3.1	2.9.21-1000	3.1.36.100-2
7.3.0	2.9.21-105	3.1.36.1-101
7.2.9	2.9.20-9000	3.1.21.900-7
7.2.8.1	2.9.20-8101	3.1.21.800-2
7.2.8	2.9.20-8005	3.1.21.800-2
7.2.7	2.9.20-6102	3.1.21.600-26
7.2.6	2.9.20-6102	3.1.21.600-26
7.2.5.2	2.9.20-5201	3.1.21.501-27
7.2.5.1	2.9.20-5100	3.1.21.501-26
7.2.5	2.9.20-5002	3.1.21.500-21
7.2.4.1	2.9.20-4103	3.1.21.401-6

威胁防御	**Snort 2**	**Snort 3**
7.2.4	2.9.20-4004	3.1.21.400-24
7.2.3.1	2.9.20-3100	3.1.21.100-7
7.2.3	2.9.20-3010	3.1.21.100-7
7.2.2	2.9.20-2001	3.1.21.100-7
7.2.1	2.9.20-1000	3.1.21.100-7
7.2.0.1	2.9.20-108	3.1.21.1-126
7.2.0	2.9.20-107	3.1.21.1-126
7.1.0.3	2.9.19-3000	3.1.7.3-210
7.1.0.2	2.9.19-2000	3.1.7.2-200
7.1.0.1	2.9.19-1013	3.1.7.2-200
7.1.0	2.9.19-92	3.1.7.1-108
7.0.6.3	2.9.18-6306	3.1.0.603-31
7.0.6.2	2.9.18-6201	3.1.0.602-26
7.0.6.1	2.9.18-6008	3.1.0.600-20
7.0.6	2.9.18-6008	3.1.0.600-20
7.0.5.1	2.9.18-5100	—
7.0.5	2.9.18-5002	3.1.0.500-7
7.0.4	2.9.18-4002	3.1.0.400-12
7.0.3	2.9.18-3005	3.1.0.300-3
7.0.2.1	2.9.18-2101	3.1.0.200-16
7.0.2	2.9.18-2022	3.1.0.200-16
7.0.1.1	2.9.18-1026	3.1.0.100-11
7.0.1	2.9.18-1026	3.1.0.100-11
7.0.0.1	2.9.18-1001	3.1.0.1-174
7.0.0	2.9.18-174	3.1.0.1-174
6.7.0.3	2.9.17-3014	3.0.1.4-129
6.7.0.2	2.9.17-2003	3.0.1.4-129
6.7.0.1	2.9.17-1006	3.0.1.4-129

威胁防御	Snort 2	Snort 3
6.7.0	2.9.17-200	3.0.1.4-129
6.6.7.2	2.9.16-7101	—
6.6.7.1	2.9.16-7100	—
6.6.7	2.9.16-7017	—
6.6.5.2	2.9.16-5204	—
6.6.5.1	2.9.16-5107	—
6.6.5	2.9.16-5034	—
6.6.4	2.9.16-4022	—
6.6.3	2.9.16-3033	—
6.6.1	2.9.16-1025	—
6.6.0.1	2.9.16-140	—
6.6.0	2.9.16-140	—
6.5.0.5	2.9.15-15510	—
6.5.0.4	2.9.15-15201	—
6.5.0.3	2.9.15-15201	—
6.5.0.2	2.9.15-15101	—
6.5.0.1	2.9.15-15101	-
6.5.0	2.9.15-7	—
6.4.0.18	2.9.14-28000	—
6.4.0.17	2.9.14-27005	—
6.4.0.16	2.9.14-26002	—
6.4.0.15	2.9.14-25006	—
6.4.0.14	2.9.14-24000	—
6.4.0.13	2.9.14-19008	—
6.4.0.12	2.9.14-18011	—
6.4.0.11	2.9.14-17005	—

威胁防御	Snort 2	Snort 3
6.4.0.10	2.9.14-16023	—
6.4.0.9	2.9.14-15906	—
6.4.0.8	2.9.14-15707	—
6.4.0.7	2.9.14-15605	—
6.4.0.6	2.9.14-15605	—
6.4.0.5	2.9.14-15507	—
6.4.0.4	2.9.12-15301	-
6.4.0.3	2.9.14-15301	-
6.4.0.2	2.9.14-15209	-
6.4.0.1	2.9.14-15100	-
6.4.0	2.9.14-15003	—
6.3.0.5	2.9.13-15503	—
6.3.0.4	2.9.13-15409	—
6.3.0.3	2.9.13-15307	—
6.3.0.2	2.9.13-15211	—
6.3.0.1	2.9.13-15101	-
6.3.0	2.9.13-15013	—
6.2.3.18	2.9.12-1813	—
6.2.3.17	2.9.12-1605	—
6.2.3.16	2.9.12-1605	—
6.2.3.15	2.9.12-1513	—
6.2.3.14	2.9.12-1401	—
6.2.3.13	2.9.12-1306	—
6.2.3.12	2.9.12-1207	—
6.2.3.11	2.9.12-1102	—
6.2.3.10	2.9.12-902	—

威胁防御	Snort 2	Snort 3
6.2.3.9	2.9.12-806	—
6.2.3.8	2.9.12-804	—
6.2.3.7	2.9.12-704	—
6.2.3.6	2.9.12-607	—
6.2.3.5	2.9.12-506	—
6.2.3.4	2.9.12-383	—
6.2.3.3	2.9.12-325	—
6.2.3.2	2.9.12-270	—
6.2.3.1	2.9.12-204	-
6.2.3	2.9.12-136	—
6.2.2.5	2.9.11-430	—
6.2.2.4	2.9.11-371	—
6.2.2.3	2.9.11-303	—
6.2.2.2	2.9.11-273	-
6.2.2.1	2.9.11-207	-
6.2.2	2.9.11-125	-
6.2.1	2.9.11-101	—
6.2.0.6	2.9.10-301	—
6.2.0.5	2.9.10-255	—
6.2.0.4	2.9.10-205	—
6.2.0.3	2.9.10-160	—
6.2.0.2	2.9.10-126	—
6.2.0.1	2.9.10-98	-
6.2.0	2.9.10-42	—
6.1.0.7	2.9.9-312	—
6.1.0.6	2.9.9-258	—

威胁防御	Snort 2	Snort 3
6.1.0.5	2.9.9-225	—
6.1.0.4	2.9.9-191	—
6.1.0.3	2.9.9-159	—
6.1.0.2	2.9.9-125	—
6.1.0.1	2.9.9-92	-
6.1.0	2.9.9-330	—
6.0.1.4	2.9.8-490	—
6.0.1.3	2.9.8-461	—
6.0.1.2	2.9.8-426	—
6.0.1.1	2.9.8-383	-
6.0.1	2.9.8-224	—

系统数据库

漏洞数据库 (VDB) 是可能影响主机的已知漏洞以及操作系统指纹、客户端指纹和应用指纹的数据库。系统借助 VDB 来确定某个特定主机是否会增加遭受危害的风险。

地理位置数据库 (GeoDB) 是可用于根据地理位置查看和过滤流量的数据库。

表 *18:*

威胁防御	VDB	GeoDB
7.6.0	4.5.0-392	2022-07-04-101
7.4.1 至 7.4.x	4.5.0-376	2022-07-04-101
7.4.0	4.5.0-365	2022-07-04-101
7.3.0 至 7.3.x	4.5.0-358	2022-07-04-101
7.2.0 至 7.2.x	4.5.0-353	2022-05-11-103
7.1.0	4.5.0-346	2020-04-28-002
6.7.0 至 7.0.x	4.5.0-338	2020-04-28-002
6.6.1 至 6.6.x	4.5.0-336	2019-06-03-002
6.6.0	4.5.0-328	2019-06-03-002

威胁防御	VDB	GeoDB
6.5.0	4.5.0-309	2019-06-03-002
6.4.0	4.5.0-309	2018-07-09-002
6.3.0	4.5.0-299	2018-07-09-002
6.2.3	4.5.0-290	2017-12-12-002
6.0.1 至 6.2.2	4.5.0-271	2015-10-12-001

集成的产品

下列思科产品可能有其他兼容性要求，例如，它们可能需要在特定硬件或特定操作系统上运行。有关信息，请参阅相应产品的文档。

注释 只要有可能，我们建议您使用每个集成产品的最新兼容版本。这样可确保您拥有最新的功能、漏洞修复和安全补丁。

身份服务和用户控制

请注意：

- 使用思科 ISE 和 ISE-PIC：我们列出了我们为其提供增强兼容性测试的 ISE 和 ISE-PIC 版本，但其他组合也可能适用。
- 使用 Cisco Firepower 用户代理：6.6 版是支持用户代理软件作为身份源的最后一个 管理中心 版本；这将阻止升级到版本 6.7+。

  您可以改为将 被动身份代理 与 Microsoft Active Directory 配合使用。有关详细信息，请参阅使用 被动身份代理 进行用户控制。
- 思科 TS 代理：版本 1.0 和 1.1 不再可用。

表 *19:* 集成式产品：身份服务/用户控制

管理中心/威胁防御	思科身份服务引擎 (ISE)		思科 Firepower 用户代理	思科终端服务 (TS) 代理	被动身份代理
	ISE	ISE-PIC			
支持...	管理中心 设备管理器	管理中心 设备管理器	仅限管理中心	仅限管理中心	仅限管理中心

管理中心/威胁防御	思科身份服务引擎 (ISE)		思科 Firepower 用户代理	思科终端服务 (TS) 代理	被动身份代理
	ISE	ISE-PIC			
云交付的防火墙管理中心（无版本）	3.3 3.2 3.1 补丁 2+ 3.0 补丁 6+ 2.7 补丁 2+ pxGrid 云身份源 需要 ISE 3.1 补丁 3 或更高版本。	3.2 3.1 2.7 补丁 2+	—	1.4	1.0
7.6	3.3 补丁 2 3.2 补丁 5 3.1 补丁 2+	3.2 3.1	—	1.4	1.0
7.4	3.3 3.2 3.1 补丁 2+ 3.0 补丁 6+	3.2 3.1	—	1.4	-
7.3	3.2 3.1 3.0 2.7 补丁 2+	3.2 3.1 2.7 补丁 2+	—	1.4 1.3	—
7.2.4 – 7.2.x	3.3 3.2 3.1 3.0 2.7 补丁 2+	3.2 3.1 2.7 补丁 2+	—	1.4 1.3	—
7.2.0 – 7.2.3	3.2 3.1 3.0 2.7 补丁 2+	3.2 3.1 2.7 补丁 2+	—	1.4 1.3	-

管理中心/威胁防御	思科身份服务引擎 (ISE)		思科 Firepower 用户代理	思科终端服务 (TS) 代理	被动身份代理
	ISE	ISE-PIC			
7.1	3.2 3.1 3.0 2.7 补丁 2+	3.2 3.1 2.7 补丁 2+	—	1.4 1.3	-
7.0	3.2 3.1 3.0 2.7 补丁 2+ 2.6 补丁 6+	3.2 3.1 2.7 补丁 2+ 2.6 补丁 6+	—	1.4 1.3	-
6.7	3.0 2.7 补丁 2+ 2.6 补丁 6+	2.7 补丁 2+ 2.6 补丁 6+	—	1.4 1.3	-
6.6	3.0 2.7，任何补丁 2.6，任何补丁 2.4	2.7，任何补丁 2.6，任何补丁 2.4	2.5 2.4	1.4 1.3 1.2	-
6.5	2.6 2.4	2.6 2.4	2.5 2.4	1.4 1.3 1.2 1.1	-
6.4	2.4 2.3 补丁 2 2.3	2.4 2.2 补丁 1	2.5 2.4 2.3，无 ASA FirePOWER	1.4 1.3 1.2 1.1	-
6.3	2.4 2.3 补丁 2 2.3	2.4 2.2 补丁 1 2.4	2.4 2.3，无 ASA FirePOWER	1.2 1.1	-

管理中心/威胁防御	思科身份服务引擎 (ISE)		思科 Firepower 用户代理	思科终端服务 (TS) 代理	被动身份代理
	ISE	ISE-PIC			
6.2.3	2.3 补丁 2 2.3 2.2 补丁 5 2.2 补丁 1 2.2	2.2 补丁 1	2.4 2.3	1.2 1.1	-
6.2.2	2.3 2.2 补丁 1 2.2 2.1	2.2 补丁 1	2.3	1.2 1.1 1.0	-
6.2.1	2.1 2.0.1 2.0	2.2 补丁 1	2.3	1.1 1.0	-
6.2.0	2.1 2.0.1 2.0 1.3	—	2.3	-	—
6.1	2.1 2.0.1 2.0 1.3	—	2.3	-	—
6.0.1	1.3	—	2.3	-	—

Cisco Secure Dynamic Attributes Connector

Cisco Secure Dynamic Attributes Connector 是一款轻量级应用，可根据云/虚拟工作负载变化在 管理中心 上快速无缝地更新防火墙策略。有关详细信息，请参阅以下之一：

- 本地连接器：《Cisco Secure Dynamic Attributes Connector 配置指南》
- 云交付的连接器：使用 思科防御协调器 中的云交付的防火墙管理中心来管理 Cisco Secure Firewall Threat Defense 中的通过 思科防御协调器来管理思科安全动态属性连接器 一章
- 与 Cisco Secure Firewall Management Center 捆绑：《Cisco Secure Firewall Management Center 设备配置指南》

表 *20:* 集成式产品：*Cisco Secure Dynamic Attributes Connector*

管理中心	Cisco Secure Dynamic Attributes Connector	
	本地部署	云交付（通过 CDO）
云交付的管理中心（无版本）	3.0 2.2 2.0	是
7.1+	3.0 2.2 2.0 1.1	是
7.0	3.0 2.2 2.0 1.1	—

Cisco Secure Dynamic Attributes Connector 让您能够在安全规则中使用来自各种云服务平台的服务标签和类别。

下表显示了 Cisco Secure Firewall Management Center 随附的 Cisco Secure Dynamic Attributes Connector (CSDAC) 支持的连接器。有关本地 CSDAC 支持的连接器列表，请参阅《Cisco Secure Dynamic Attributes Connector 配置指南》。

表 *21:* 按 *Cisco Secure Dynamic Attributes Connector* 版本和 平台列出的受支持连接器列表

CSDAC 版本/平台	AWS	AWS 安全组	AWS 服务标记	Azure	Azure 服务标签	Cisco Cyber Vision	思科多云防御	通用文本	GitHub	Google Cloud	Microsoft Office 365	vCenter	Webex	Zoom
版本 1.1（本地）	是	否	不兼容	兼容	是	否	不兼容	不兼容	不兼容	不兼容	兼容	是	否	不兼容
版本 2.0（本地）	是	否	不兼容	兼容	是	否	不兼容	不兼容	不兼容	兼容	兼容	是	否	不兼容
版本 2.2（本地）	是	否	不兼容	兼容	是	否	不兼容	不兼容	兼容	兼容	兼容	是	否	不兼容
版本 2.3（本地）	是	否	不兼容	兼容	是	否	不兼容	不兼容	兼容	兼容	兼容	兼容	兼容	兼容
版本 3.0（本地）	兼容	兼容	兼容	兼容	兼容	是	否	兼容	兼容	兼容	兼容	兼容	兼容	兼容
云交付(思科防御协调器)	是	否	不兼容	兼容	是	否	是	否	兼容	兼容	是	否	不兼容	不兼容

CSDAC 版本/平台	AWS	AWS 安全组	AWS 服务标记	Azure	Azure 服务标签	Cisco Cyber Vision	思科多云防御	通用文本	GitHub	Google Cloud	Microsoft Office 365	vCenter	Webex	Zoom
Cisco Secure Firewall Management Center 7.4.1	是	否	不兼容	兼容	是	否	不兼容	兼容	兼容	兼容	兼容	兼容	兼容	兼容
Cisco Secure Firewall Management Center 7.6	兼容	兼容	兼容	兼容	兼容	是	否	兼容	兼容	兼容	兼容	兼容	兼容	兼容

威胁检测

请注意：

- 思科安全分析和日志记录（本地）需要 Stealthwatch 管理控制台 (SMC) 的安全分析和日志记录本地应用程序。有关 SMC 的 Stealthwatch 企业版 (SWE) 要求的信息，请参阅Cisco Security Analytics and Logging（本地部署）：Firepower 事件集成指南。
- 现已对版本 6.4 – 7.4 中提供的思科 SecureX 集成终止支持。关于更换技术，请联系思科代表或合作伙伴联系人。

表 *22:* 集成产品：威胁检测

管理中心/威胁防御	Cisco Security Analytics and Logging (SaaS)	思科安全分析和日志记录（本地部署）	Cisco Secure Malware Analytics	思科安全数据包分析器
支持...	管理中心 设备管理器	仅限管理中心	仅限管理中心	仅限管理中心
6.5+	是	是	是	-
6.4	是 需要配备威胁防御 6.4 的管理中心。	是	是	是
6.3	-	—	是	是
6.1 – 6.2.3	-	—	是	-

威胁防御 远程访问 VPN

远程访问虚拟专用网络 (RA VPN) 允许个人用户使用计算机或支持的移动设备从远程位置连接到您的网络。请记住，更新的威胁防御功能可能需要更新版本的客户端。

有关详细信息，请参阅《Cisco Secure Client/AnyConnect 安全移动客户端配置指南》。

表 *23:* 集成产品：威胁防御 ***RA VPN***

威胁防御	**Cisco Secure Client/Cisco AnyConnect** 安全移动客户端
6.2.2+	4.0+

浏览器要求

浏览器

我们使用这些常用浏览器的最新版本进行测试，这些浏览器在当前支持的 macOS 和 Microsoft Windows 版本上运行：

表 *24:* 浏览器

浏览器	设备管理器版本
Google Chrome	任意
Mozilla Firefox	任意
Microsoft Edge（仅限 Windows）	版本 6.7+
Apple Safari	未经广泛测试。欢迎提供反馈。

如果您在使用任何其他浏览器时遇到问题，或者正在运行的操作系统已达到使用年限，我们建议您更换或升级。如果您继续遇到问题或有反馈意见，请联系思科 TAC。

浏览器设置和扩展

无论使用哪种浏览器，请保持启用 JavaScript 和 Cookie。如果您使用的是 Microsoft Edge，请不要启用 IE 模式。

请注意，某些浏览器扩展可能会阻止您保存 PKI 对象中证书和密钥等字段的值。这些扩展包括（但不限于）Grammarly 和 Whatfix Editor。出现这种情况是因为这些扩展程序在字段中插入了字符（如 HTML），导致系统认为这些字符无效。我们建议您在登录我们的产品时禁用这些扩展。

屏幕分辨率

表 *25:* 屏幕分辨率

接口	最小分辨率
设备管理器	1024 x 768
Firepower 4100/9300 的机箱管理器	1024 x 768

保护通信安全

首次登录时，系统会使用自签名数字证书来确保网络通信的安全。浏览器应显示不受信任的颁发机构警告，但也应允许您将证书添加到信任存储区中。虽然这样可以继续使用，但我们还是建议您用全球知名或内部信任的证书颁发机构 (CA) 签发的证书替换自签证书。

要开始替换设备管理器上的自签名证书，请依次点击**设备 (Device)**、**系统设置 (System Settings)** > 、**管理访问 (Management Access)** 链接和**管理 Web 服务器 (Management Web Server)** 选项卡。有关详细步骤，请参阅在线帮助或《Cisco Secure Firewall 设备管理器配置指南》。

注释 如果不替换自签名证书：

- Google Chrome 不会缓存静态内容，例如图像、CSS 或 JavaScript。特别是在低带宽环境中，这会使得页面加载时间延长。
- Mozilla Firefox 可在浏览器更新时停止信任自签名证书。如果发生这种情况，您可以刷新 Firefox，但请记住，这样会丢失一些设置；请参阅 Mozilla 的刷新 Firefox 支持页面。

从监控网络浏览

许多浏览器默认使用传输层安全 (TLS) v1.3。如果您使用 SSL 策略来处理加密流量，并且受监控网络中的人员使用启用了 TLS v1.3 的浏览器，则系统可能无法加载支持 TLS v1.3 的网站。

注释 在 6.2.3 及更早版本中，支持 TLS v1.3 的网站总是无法加载。解决方法是，您可以将托管 设备配置为从 ClientHello 协商中删除扩展 43 (TLS 1.3)；请参阅标题为在启用 *SSL* 检测的情况下使用 *TLS 1.3* 加载网站失败的软件公告。在版本 6.2.3.7+ 中，您可以指定何时降级；在咨询 思科 TAC 后，请参阅 Cisco Secure Firewall Threat Defense 命令参考 中的 **system support** 命令。

寿命终止通知

下表将提供寿命终止详细信息。已过的日期以**粗体**显示。

Snort

如果您仍在使用 Snort 2 检测引擎进行威胁防御，请立即切换到 Snort 3，以提高检测能力和性能。从威胁防御版本 6.7+（带设备管理器）和版本 7.0+（带管理中心）开始提供。Snort 2 将在未来的版本中弃用。您最终将无法升级 Snort 2 设备。

在管理中心部署中，升级到威胁防御版本 7.2+ 还会将符合条件的 Snort 2 设备升级到 Snort 3。对于因使用自定义入侵或网络分析策略而不符合条件的设备，可手动升级 Snort。请参阅《Cisco Secure Firewall Management Center Snort 3 配置指南》中的从 *Snort 2* 迁移到 *Snort 3*。

在设备管理器部署中，手动升级 Snort。请参阅《Cisco Secure Firewall 设备管理器配置指南》中的入侵策略。

软件

这些主要软件版本已达到销售终止和/或支持终止。已停止支持的版本将从 思科支持和下载站点 中删除。

表 *26:* 软件 *EOL* 公告

版本	停售日期	更新结束	支持终止	通告
7.1	**2023-12-22**	2024-12-21	2025-12-31	Cisco Firepower Threat Defense (FTD) 7.1.(x)、Firepower Management Center (FMC) 7.1.(x)、自适应安全设备 (ASA) 9.17.(x) 和 Firepower eXtensible Operating System (FXOS) 2.11.(x) 的销售终止和寿命终止公告
6.7	**2021-07-09**	**2022-07-09**	**2024-07-31**	思科 Firepower 威胁防御 (FTD) 6.7、Firepower 管理中心 (FMC) 6.7 和 Firepower 可扩展操作系统 (FXOS) 2.9(x) 的销售终止和寿命终止公告
6.6	**2022-03-02**	**2023-03-02**	2025-03-31	Cisco Firepower Threat Defense (FTD/FTDv) 6.6(x)、Firepower 管理中心 (FMC/FMCv) 6.6(x) 和 Firepower eXtensible Operating System (FXOS) 2.8(x) 的销售终止和寿命终止公告
6.5	**2020-06-22**	**2021-06-22**	**2023-06-30**	思科 Firepower 威胁防御 (FTD) 6.5(x)、Firepower 管理中心 (FMC) 6.5(x) 和 Firepower 可扩展操作系统 (FXOS) 2.7(x) 的销售终止和寿命终止公告
6.4	**2023-02-27**	**2024-02-27**	2026-02-28	Cisco Firepower Threat Defense (FTD) 6.4(X)、Firepower Management Center (FMC) 6.4(X) 和 Firepower eXtensible Operating System (FXOS) 2.6(x) 的销售终止和寿命终止公告
6.3	**2020-04-30**	**2021-04-30**	**2023-04-30**	思科 Firepower 威胁防御 (FTD) 6.2.2, 6.3(x)、Firepower 可扩展操作系统 (FXOS) 2.4.1 和 Firepower 管理中心 (FMC) 6.2.2 和 6.3(x) 的销售终止和寿命终止公告
6.2.3	**2022-02-04**	**2023-02-04**	2025-02-28	思科 Firepower 威胁防御 (FTD) 6.2.3、Firepower 管理中心 (FMC) 6.2.3 和 Firepower 可扩展操作系统 (FXOS) 2.2(x) 的销售终止和寿命终止公告
6.2.2	**2020-04-30**	**2021-04-30**	**2023-04-30**	思科 Firepower 威胁防御 (FTD) 6.2.2, 6.3(x)、Firepower 可扩展操作系统 (FXOS) 2.4.1 和 Firepower 管理中心 (FMC) 6.2.2 和 6.3(x) 的销售终止和寿命终止公告
6.2.1	**2019-03-05**	**2020-03-04**	**2022-03-31**	思科 Firepower 威胁防御版本 6.2.0 和 6.2.1 的销售终止和寿命终止公告

版本	停售日期	更新结束	支持终止	通告
6.2	**2019-03-05**	**2020-03-04**	**2022-03-31**	思科 Firepower 威胁防御版本 6.2.0 和 6.2.1 的销售终止和寿命终止公告
6.1	**2019-11-22**	**2021-05-22**	**2023-05-31**	思科 Firepower 威胁防御版本 6.1、NGIPSv 和 NGFWv 版本 6.1、Firepower 管理中心 6.1 和 Firepower 可扩展操作系统 (FXOS) 2.0(x) 的销售终止和寿命终止公告
6.0.1	**2017-11-10**	**2018-11-10**	**2020-11-30**	思科 Firepower 软件版本 5.4、6.0 和 6.0.1 以及 Firepower 管理中心软件版本 5.4、6.0 和 6.0.1 的销售终止和寿命终止公告

这些仍受支持的分支上的软件版本已从 思科支持和下载站点 中删除。

注释 在版本 6.2.3+ 中，卸载修补程序（四位数发行版）会导致设备运行您升级之前的版本。这意味着您只需卸载更高版本的补丁即可运行已弃用的版本。除非另有说明，否则不要保留已弃用的版本。相反，我们建议您升级。如果无法升级，请卸载已弃用的补丁。

表 *27:* 软件删除的版本

版本	删除日期	相关漏洞和其他详细信息
7.2.6	**2024-04-29**	CSCwi63113：重新加载/升级后启用 SNMP 的 FTD 引导循环
6.4.0.6	**2019-12-19**	CSCvr52109：部署到多个设备后，FTD 可能不会匹配正确的访问控制规则
6.2.3.8	**2019-01-07**	CSCvn82378：在将 FMC 升级到 6.2.3.8-51 时，通过 ASA/FTD 的流量可能会停止传输

硬件和虚拟平台

这些平台已达到销售终止和/或支持终止。

表 *28:* 威胁防御 硬件 *EOL* 公告

平台	上一个设备版本	上一个要管理的管理中心	停售日期	支持终止	通告
Firepower 2110、2120、2130、2140	7.4	待定	待定	待定	-

平台	上一个设备版本	上一个要管理的管理中心	停售日期	支持终止	通告
Firepower 4110	7.2	待定	**2024-07-31**	2027-01-31	Cisco Firepower 4110 系列安全设备和 3 年订用的销售终止和寿命终止公告
			2022-01-31	2027-01-31	思科 Firepower 4110 系列安全设备和 5 年订用的销售终止和寿命终止公告
ASA 5508-X、5516-X	7.0	7.4	**2021-08-02**	2026-08-31	思科 ASA5508 和 ASA5516 系列安全设备及 5 年订用的销售终止和寿命终止公告
ASA 5525-X、5545-X、5555-X	6.6	7.2	**2020-09-04**	2025-09-30	思科 ASA5525、ASA5545 和 ASA5555 系列安全设备及 5 年订用的销售终止和寿命终止公告
Firepower 4120, 4140, 4150	7.2	待定	**2024-08-31**	2025-08-31	Cisco Firepower 4120/40/50 和 FPR 9300 SM24/36/44 系列安全设备 1 年订用的销售终止和寿命终止公告
			2022-08-31	2025-08-31	Cisco Firepower 4120/40/50 和 FPR 9300 SM24/36/44 系列安全设备 3 年订用的销售终止和寿命终止公告
			2020-08-31	2025-08-31	思科 Firepower 4120/40/50 和 FPR 9300 SM24/36/44 系列安全设备/模块和 5 年订用的销售终止和寿命终止公告
Firepower 9300：SM-24、SM-36、SM-44 模块	7.2	待定	**2024-08-31**	2025-08-31	Cisco Firepower 4120/40/50 和 FPR 9300 SM24/36/44 系列安全设备 1 年订用的销售终止和寿命终止公告
			2022-08-31	2025-08-31	Cisco Firepower 4120/40/50 和 FPR 9300 SM24/36/44 系列安全设备 3 年订用的销售终止和寿命终止公告
			2020-08-31	2025-08-31	思科 Firepower 4120/40/50 和 FPR 9300 SM24/36/44 系列安全设备/模块和 5 年订用的销售终止和寿命终止公告
ASA 5515-X	6.4	7.0	**2017-08-25**	**2022-08-31**	思科 ASA 5512-X 和 ASA 5515-X 销售终止和寿命终止公告

平台	上一个设备版本	上一个要管理的管理中心	停售日期	支持终止	通告
ASA 5506-X、5506H-X、5506W-X	6.2.3	6.6	**2021-08-02**	2026-08-31	配备 ASA 软件的思科 ASA5506 系列安全设备的销售终止和寿命终止公告
			2021-07-31	**2022-07-31**	思科 ASA5506 系列安全设备 1 年订用的销售终止和寿命终止公告
			2020-05-05	**2022-07-31**	思科 ASA5506 系列安全设备 3 年订用的销售终止和寿命终止公告
			2018-09-30	**2022-07-31**	思科 ASA5506 系列安全设备 5 年订用的销售终止和寿命终止公告
ASA 5512-X	6.2.3	6.6	**2017-08-25**	**2022-08-31**	思科 ASA 5512-X 和 ASA 5515-X 销售终止和寿命终止公告

术语和品牌

表 *29:* 产品线

当前名称	较早名称
Secure Firewall Threat Defense	FirePower Firepower 系统 FireSIGHT 系统 Sourcefire 3D 系统

表 *30:* 设备

当前名称		较早名称
威胁防御	Secure Firewall Threat Defense	Firepower 威胁防御 (FTD)
	Secure Firewall Threat Defense Virtual	Firepower Threat Defense Virtual (FTDv)
传统 NGIPS	ASA FirePOWER ASA FirePOWER 模块 具备 FirePOWER 服务的 ASA	—
	7000/8000 系列	系列3
	NGIPSv	虚拟受管设备

当前名称		较早名称
传统	系列2	—
	适用于 Blue Coat X 系列的思科 NGIPS	用于 X 系列的 FireSIGHT 软件 用于 X 系列的 Sourcefire 软件

表 *31:* 设备管理

当前名称	较早名称
Secure Firewall Management Center	Firepower 管理中心 (FMC) FireSIGHT 管理中心 FireSIGHT Defense Center Defense Center
Cisco Secure Firewall Management Center Virtual	Firepower Management Center Virtual (FMCv) FireFIGHT Virtual 管理中心 FireSIGHT Virtual 防御中心 虚拟防御中心
云交付的防火墙管理中心	—
Cisco Secure Firewall 设备管理器	Firepower 设备管理器 (FDM)
Cisco Secure Firewall 自适应安全设备管理器 (ASDM)	自适应安全设备管理器 (ASDM)
Cisco Secure Firewall 机箱管理器	Firepower 机箱管理器
思科防御协调器 (CDO)	—

表 *32:* 操作系统

当前名称	较早名称
Cisco Secure Firewall eXtensible Operating System (FXOS)	Firepower eXtensible Operating System (FXOS)
Cisco Secure Firewall 自适应安全设备 (ASA) 软件	自适应安全设备 (ASA) 软件

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。