



配置基本策略

使用以下设置配置基本安全策略：

- 内部和外部接口 - 为内部接口分配静态 IP 地址，并将 DHCP 用作外部接口。
- DHCP 服务器 - 在内部接口上为客户端使用 DHCP 服务器。
- 默认路由 - 通过外部接口添加默认路由。
- NAT - 在外部接口上使用接口 PAT。
- 访问控制 - 允许流量从内部传到外部。

您还可以自定义安全策略，以包括更高级的检查。

- [配置接口，第 1 页](#)
- [配置 DHCP 服务器，第 7 页](#)
- [添加默认路由，第 8 页](#)
- [配置 NAT，第 11 页](#)
- [配置访问控制规则，第 14 页](#)
- [部署配置，第 17 页](#)

配置接口

使用 防火墙设备管理器 进行初始设置时，系统会预配置以下接口：

- 以太网 1/1 - **outside**，IP 地址来自 DHCP、IPv6 自动配置
- 以太网 1/2 - **inside**，192.168.95.1/24
- 默认路由 - 通过外部接口上的 DHCP 获取

如果在向 Firewall Management Center 注册之前在 防火墙设备管理器 中执行其他特定于接口的配置，则会保留该配置。

以下示例使用 DHCP 在接口内部配置了一个路由模式（含静态地址），并在接口外部配置了一个路由模式。它还会为内部 Web 服务器添加一个 DMZ 接口。

过程

步骤 1 选择设备 (Devices) > 设备管理 (Device Management)，然后点击防火墙的 编辑 (🔗)。

步骤 2 点击接口 (Interfaces)。

图 1: 接口

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router	
Management0/0	management	Physical				Disabled	Global	🔍 ↩
GigabitEthernet0/0		Physical				Disabled		✎
GigabitEthernet0/1		Physical				Disabled		✎
GigabitEthernet0/2		Physical				Disabled		✎
GigabitEthernet0/3		Physical				Disabled		✎
GigabitEthernet0/4		Physical				Disabled		✎
GigabitEthernet0/5		Physical				Disabled		✎
GigabitEthernet0/6		Physical				Disabled		✎
GigabitEthernet0/7		Physical				Disabled		✎

步骤 3 要从 40-Gb 或更大的接口创建分支端口，请点击该接口的 中断 图标。

如果您已经在配置中使用了全接口，则必须在继续创建分支之前删除该配置。

步骤 4 点击要用于内部的接口的 编辑 (🔗)。

图 2: “常规”选项卡

Edit Physical Interface

General IPv4 IPv6 Path Monitoring

Name:
inside

Enabled
 Management Only

Description:

Mode:
None

Security Zone:
inside_zone

Interface ID:
GigabitEthernet0/1

MTU:
1500
(64 - 9000)

Priority:
0 (0 - 65535)

Propagate Security Group Tag:

NVE Only:

- a) 从安全区域 (Security Zone) 下拉列表中选择一个现有的内部安全区域，或者点击**新建 (New)**添加一个新的安全区域。

例如，添加一个名为 **inside_zone** 的区域。您可以根据区域或组应用安全策略。例如，配置访问控制策略，使流量可以从内部区域进入外部区域，但不能从外部进入内部区域。

如果预配置了内部接口，则其余字段为可选。

- b) 输入长度最大为 48 个字符的名称 (Name)。

例如，将接口命名为 **inside**。

- c) 选中启用 (Enabled) 复选框。

- d) 将模式 (Mode) 保留为无 (None)。

- e) 点击 **IPv4** 和/或 **IPv6** 选项卡。

- **IPv4** - 从下拉列表中选择使用**静态 IP (Use Static IP)**，然后以斜杠表示法输入 IP 地址和子网掩码。

例如，输入 **192.168.1.1/24**

图 3: IPv4 选项卡

The screenshot shows the 'Edit Physical Interface' window with the 'IPv4' tab selected. The 'IP Type' dropdown is set to 'Use Static IP'. The 'IP Address' field contains '192.168.1.1/24'. Below the field, there is a note: 'eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25'.

- IPv6 - 为无状态自动配置选中自动配置 (Autoconfiguration) 复选框。

图 4: IPv6 选项卡

The screenshot shows the 'Edit Physical Interface' window with the 'IPv6' tab selected. The 'Basic' sub-tab is active. The 'Enable IPV6' checkbox is unchecked. The 'Enforce EUI 64' checkbox is unchecked. The 'Link-Local address' field is empty. The 'Autoconfiguration' checkbox is checked. The 'Obtain Default Route' checkbox is unchecked.

f) 点击确定 (OK)。

步骤 5 点击要用于外部的接口的 编辑 (🔗)。

图 5: “常规”选项卡

Edit Physical Interface

General IPv4 IPv6 Path Monitoring Hardware

Name:

Enabled
 Management Only

Description:

Mode:

Security Zone:

Interface ID:
GigabitEthernet0/0

MTU:

(64 - 9000)

Priority:
 (0 - 65535)

Propagate Security Group Tag:

NVE Only:

- a) 从安全区域 (Security Zone) 下拉列表中选择一个现有的外部安全区域，或者点击新建 (New) 添加一个新的安全区域。

例如，添加一个名为 **outside_zone** 的区域。

如果预配置了外部接口，则其余字段为可选。

- b) 输入长度最大为 48 个字符的 **Name**。

例如，将接口命名为 **outside**。

- c) 选中启用 (Enabled) 复选框。

- d) 将模式 (Mode) 保留为无 (None)。

- e) 点击 IPv4 和/或 IPv6 选项卡。

• **IPv4** - 选择使用 DHCP (Use DHCP)，然后配置以下选填参数：

• 使用 DHCP 获取默认路由 (Obtain default route using DHCP) - 从 DHCP 服务器获取默认路由。

• DHCP 路由指标 (DHCP route metric) - 分配到所获悉路由的管理距离，介于 1 和 255 之间。获悉的路由的默认管理距离为 1。

图 6: IPv4 选项卡

Edit Physical Interface

General IPv4 IPv6 Path M

IP Type:
Use DHCP

Obtain default route using DHCP:

DHCP route metric:
1
(1 - 255)

- **IPv6** - 为无状态自动配置选中**自动配置 (Autoconfiguration)** 复选框。

图 7: IPv6 选项卡

Edit Physical Interface

General IPv4 IPv6 Path Monitoring Hardware Configu

Basic Address Prefixes Settings DHCP

Enable IPv6:

Enforce EUI 64:

Link-Local address:

Autoconfiguration:

Obtain Default Route:

f) 点击**确定 (OK)**。

步骤 6 例如，配置 DMZ 接口以托管 Web 服务器。

- 点击您要使用的接口的**编辑** (🔗)。
- 从**安全区域 (Security Zone)** 下拉列表中选择一个现有的 DMZ 安全区域，或者点击**新建 (New)** 添加一个新的安全区域。

例如，添加一个名为 **dmz_zone** 的区域。

- 输入长度最大为 48 个字符的**名称 (Name)**。

例如，将接口命名为 **dmz**。

- 选中**启用 (Enabled)** 复选框。
- 将**模式 (Mode)** 保留为**无 (None)**。
- 点击 **IPv4** 和/或 **IPv6** 选项卡并配置所需的 IP 地址。
- 点击**确定 (OK)**。

步骤 7 点击**保存 (Save)**。

配置 DHCP 服务器

如果希望客户端使用 DHCP 从防火墙获取 IP 地址，请启用 DHCP 服务器。

过程

步骤 1 选择设备 (Devices) > 设备管理 (Device Management)，然后单击设备的编辑 (🔗)。

步骤 2 选择 DHCP > DHCP 服务器 (DHCP Server)。

图 8: DHCP 服务器

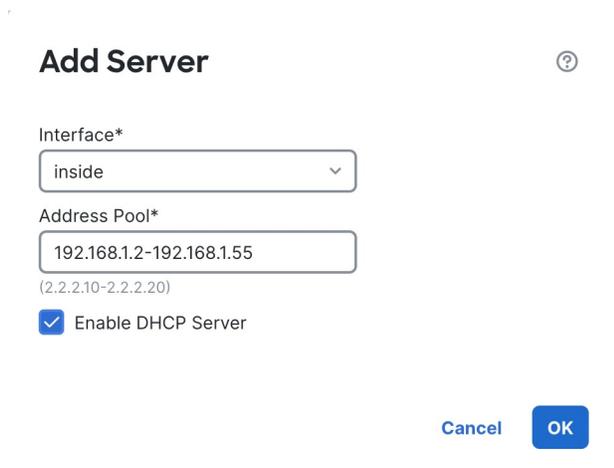
The screenshot displays the configuration interface for a DHCP server. The top navigation bar includes tabs for Device, Routing, Interfaces, Inline Sets, DHCP (selected), VTEP, and SNMP. On the left, a sidebar lists 'DHCP Server', 'DHCP Relay', and 'DDNS'. The main configuration area includes:

- Ping Timeout:** A text input field containing '50' with a range '(10 - 10000 ms)'.
- Lease Length:** A text input field containing '3600' with a range '(300 - 10,48,575 sec)'.
- Auto-Configuration:** An unchecked checkbox.
- Interface:** A dropdown menu.
- Override Auto Configured Settings:**
 - Domain Name:** A text input field.
 - Primary DNS Server:** A dropdown menu.
 - Secondary DNS Server:** A dropdown menu.
 - Primary WINS Server:** A dropdown menu.
 - Secondary WINS Server:** A dropdown menu.

At the bottom, there is a 'Server' tab (highlighted with a red box) and an 'Advanced' section. A '+ Add' button (also highlighted with a red box) is located in the bottom right corner. Below the configuration fields, there is a table with columns for 'Interface', 'Address Pool', and 'Enable DHCP Server', which currently shows 'No records to display'.

步骤 3 在服务器 (Server) 区域中，单击添加 (Add) 并配置以下选项。

图 9: 添加服务器



Add Server ⓘ

Interface*

inside

Address Pool*

192.168.1.2-192.168.1.55

(2.2.2.10-2.2.2.20)

Enable DHCP Server

Cancel OK

- 接口 (**Interface**) - 从下拉列表中选择接口名称。
- 地址池 (**Address Pool**) - 设置 IP 地址的范围。IP 地址必须与选定接口位于相同的子网上，且不能包括接口自身的 IP 地址。
- 启用 DHCP 服务器 (**Enable DHCP Server**) - 在所选接口上启用 DHCP 服务器。

步骤 4 点击确定 (OK)。

步骤 5 点击保存 (Save)。

添加默认路由

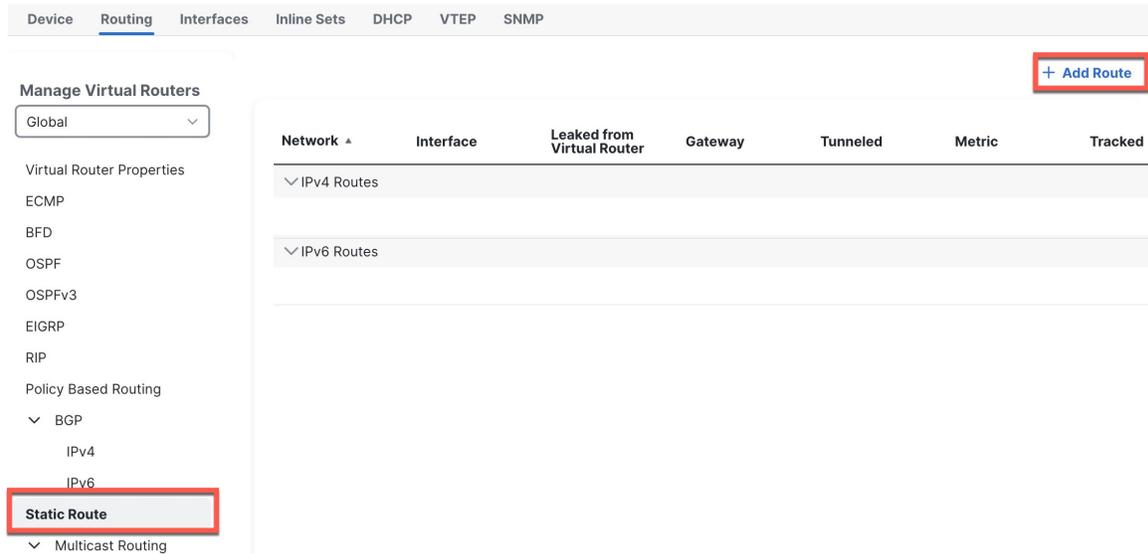
默认路由通常指向可从外部接口访问的上游路由器。如果您从 DHCP 获取外部地址，则设备可能已经收到了默认路由。如果需要手动添加路由，则遵照此程序执行。

过程

步骤 1 选择设备 (**Devices**) > 设备管理 (**Device Management**)，然后点击设备的编辑 (✎)。

步骤 2 选择 路由 > 静态路由。

图 10: 静态路由



如果从 DHCP 服务器收到默认路由，它将显示在此表中。

步骤 3 点击添加路由 (**Add Route**)，然后设置以下选项。

图 11: 添加静态路由配置

Add Static Route Configuration

Type: IPv4 IPv6

Interface*
outside

(Interface starting with this icon signifies it is available for route leak)

Available Network +

Search

- any-ipv4
- gateway
- IPv4-Benchmark-Tests
- IPv4-Link-Local
- IPv4-Multicast
- IPv4-Private-10.0.0.0-8

Selected Network

- any-ipv4

Gateway*
gateway +

Metric:
1
(1 - 254)

Tunneled: (Used only for default Route)

Route Tracking:
 +

- **类型 (Intrusion)** - 根据要添加静态路由的类型，点击 **IPv4** 或 **IPv6** 单选按钮。
- **接口 (Interface)** - 选择出口接口；通常是外部接口。
- **可用网络 (Available Network)** - 为 IPv4 默认路由选择 **any-ipv4**，为 IPv6 默认路由选择 **any-ipv6**，然后点击添加 (**Add**) 将其移至选定网络 (**Selected Network**) 列表。
- **网关 (Gateway) 或 IPv6 网关 (IPv6 Gateway)** - 输入或选择作为此路由的下一个跃点的网关路由器。您可以提供 IP 地址或网络/主机对象。

步骤 4 点击确定 (**OK**)。

路由即已添加至静态路由表。

步骤 5 点击保存。

配置 NAT

此步骤将为内部客户端创建一条 NAT 规则，以便将内部地址转换为外部接口 IP 地址上的端口。这类 NAT 规则称为接口端口地址转换 (PAT)。

过程

步骤 1 选择设备 (Devices) > NAT，然后点击新建策略 (New Policy)。

步骤 2 为策略命名，选择要使用策略的设备，然后点击保存 (Save)。

图 12: 新建策略

New Policy

Name:

Description:

Targeted Devices
Select devices to which you want to apply this policy.

Available Devices and Templates

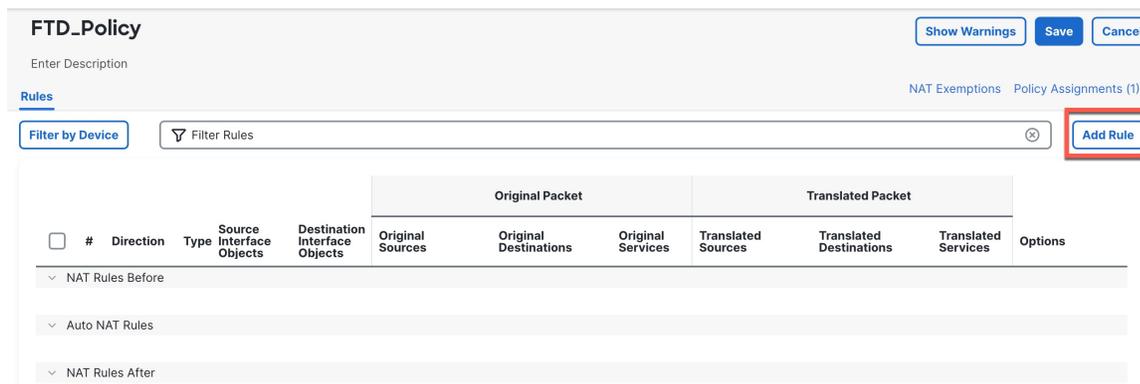
192.168.0.124
192.168.0.155

Selected Devices and Templates

192.168.0.124
192.168.0.155

策略即已添加 Firewall Management Center。您仍然需要为策略添加规则。

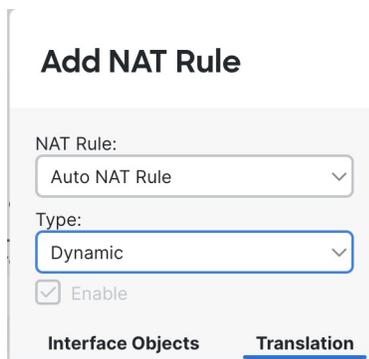
图 13: NAT 策略



步骤 3 点击添加规则 (Add Rule)。

步骤 4 配置基本规则选项：

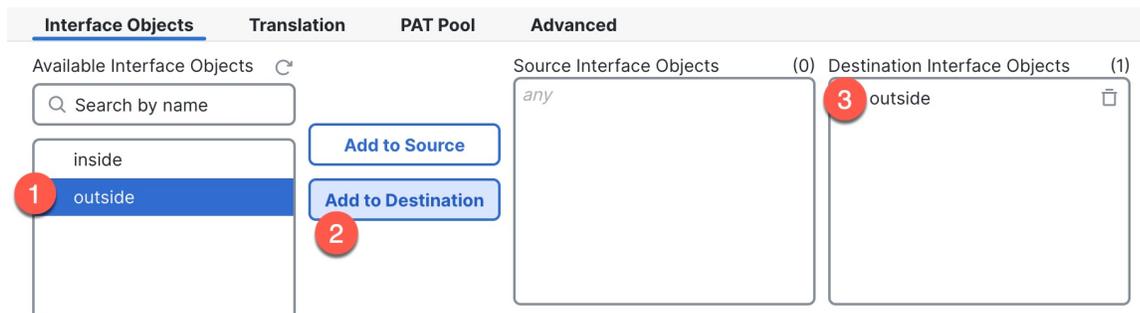
图 14: 基本规则选项



- NAT 规则 (NAT Rule) - 选择自动 NAT 规则 (Auto NAT Rule)。
- 类型 (Type) - 选择动态 (Dynamic)。

步骤 5 在 **Interface Objects** 页面，将 **Available Interface Objects** 区域中的外部区域添加到 **Destination Interface Objects** 区域。

图 15: 接口对象



步骤 6 在转换 (Translation) 页面上配置以下选项:

图 16: 转换

The screenshot shows the 'Translation' tab in a configuration interface. It is divided into two main sections: 'Original Packet' and 'Translated Packet'.
 In the 'Original Packet' section:
 - 'Original Source:*' is a dropdown menu with 'all-ipv4' selected and a '+' icon to its right.
 - 'Original Port:' is a dropdown menu with 'TCP' selected.
 In the 'Translated Packet' section:
 - 'Translated Source:' is a dropdown menu with 'Destination Interface IP' selected.
 - Below it is a blue information icon and a note: 'The values selected for Destination Interface Objects in 'Interface Objects' tab will be used'.
 - 'Translated Port:' is an empty text input field.

- 原始源-点击 添加 (+) 为所有 IPv4 流量添加网络对象 (0.0.0.0/0)。

图 17: 新的网络对象

The screenshot shows a 'New Network Object' dialog box. It has the following fields and options:
 - 'Name': Text input field containing 'all-ipv4'.
 - 'Description': Empty text input field.
 - 'Network': Three radio buttons: 'Host', 'Range', and 'Network' (which is selected). There is also an 'FQDN' radio button.
 - Below the radio buttons is a text input field containing '0.0.0.0/0'.
 - A checkbox labeled 'Allow Overrides' is unchecked.
 - At the bottom right are 'Cancel' and 'Save' buttons.

注释

您不能使用系统定义的 **any-ipv4** 对象，因为自动 NAT 规则在对象定义过程中添加 NAT，并且您无法编辑系统定义的对象。

- 转换的源 (Translated Source) - 选择目标接口 IP (Destination Interface IP)。

步骤 7 点击保存 (Save) 以添加规则。

规则即已保存至 **Rules** 表。

步骤 8 点击 NAT 页面上的保存 (Save) 以保存更改。

配置访问控制规则

如果您在注册防火墙时创建了基本的阻止所有流量访问控制策略，则需要向该策略添加规则以允许流量通过防火墙。访问控制策略可包括按顺序评估的多个规则。

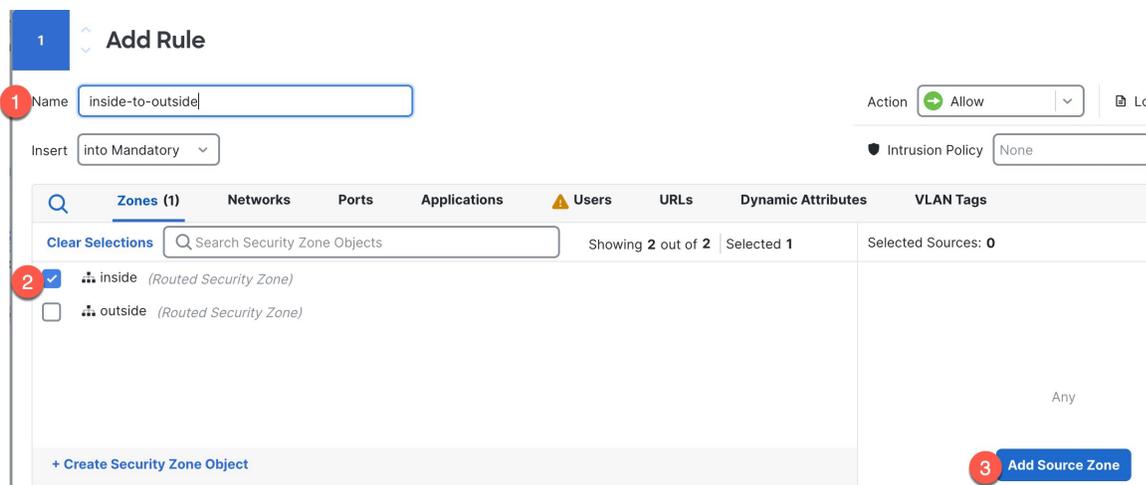
此过程将创建一个访问控制规则，以允许从内部区域到外部区域的所有流量。

过程

步骤 1 选择 策略 > 安全策略 > 访问控制，然后点击分配给设备的访问控制策略对应的 编辑 (✎)。

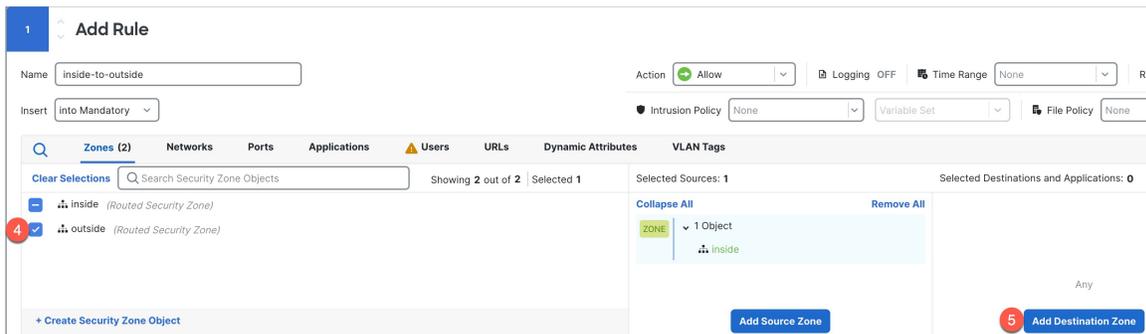
步骤 2 点击添加规则 (Add Rule) 并设置以下参数。

图 18: 源区域



1. 为此规则命名，例如 **inside-to-outside**。
2. 从区域 (Zones) 中选择内部区域
3. 点击添加源区域 (Add Source Zone)。

图 19: 目标区域



4. 从区域 (Zones) 中选择外部区域。

5. 点击添加目标区域 (Add Destination Zone)。

其他设置保留原样。

步骤 3 (可选) 点击数据包流程图中的策略类型，以便自定义相关策略。

预过滤器、解密、安全智能和身份策略在访问控制规则之前应用。不需要自定义这些策略，但在了解网络需求后，这些策略可通过快速路由受信任流量（绕过处理）或阻止流量以避免进一步处理，从而提高网络性能。

图 20: 在访问控制之前应用政策



- **预过滤器规则** - 默认预过滤器策略通过所有流量，以便其他规则执行操作（分析）。您可以对默认策略进行的唯一更改是阻止隧道流量。否则，您可以创建新的预过滤器策略，以便与可以分析（传递）、快速路径（绕过进一步检查）或阻止的访问控制策略关联。

预过滤功能可在流量到达更远的地方之前，通过拦截或快速路径来处理流量，从而提高性能。在新策略中，您可以添加隧道规则和预过滤器规则。通过隧道规则，您可以对明文（非加密）直通隧道进行快速路由、阻止或重新分区。预过滤器规则可让您快速路由或阻止通过 IP 地址、端口和协议识别的非隧道流量。

例如，如果知道要阻止网络上的所有 FTP 流量，但不阻止来自管理员的快速 SSH 流量，则可以添加一个新的预过滤器策略。

- **解密** - 默认情况下不应用解密。解密是让网络流量接受深度检查的一种方法。大多数情况下都不要对流量进行解密，只有在法律允许的情况下才能这样做。为了最大限度地保护网络，对于前往关键服务器或来自不信任网段的流量，解密策略可能是一个好主意。
- **安全智能** - (需要 IPS 许可证) 默认启用安全智能。安全智能是在将连接传递到访问控制策略进行进一步处理之前应用的另一项针对恶意活动的早期防御措施。安全智能使用信誉智能快速阻止与思科威胁智能组织 Talos 提供的 IP 地址、URL 和域名之间的连接。您可以根据需要添加或删除其他 IP 地址、URL 或域。

注释

如果没有 IPS 许可证，即使访问控制策略中显示该策略已启用，也不会部署该策略。

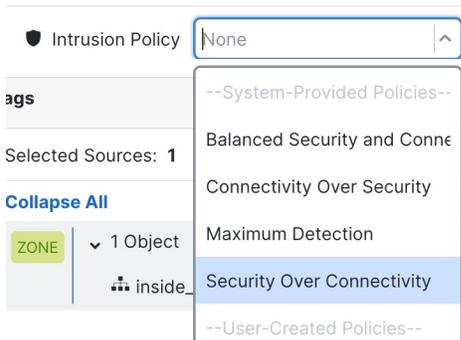
- **身份** - 默认情况下不应用身份。在允许访问控制策略处理流量之前，可以要求用户进行身份验证。

步骤 4（可选）添加在访问控制规则之后应用的入侵策略。

入侵策略是一组已定义的入侵检测和防御配置，用于检查流量是否违反安全规定。Firewall Management Center 包括许多系统提供的策略，您可以按原样启用或自定义这些策略。此步骤可启用系统提供的策略。

- a) 点击入侵策略 (**Intrusion Policy**) 下拉列表。

图 21: 系统提供的入侵策略



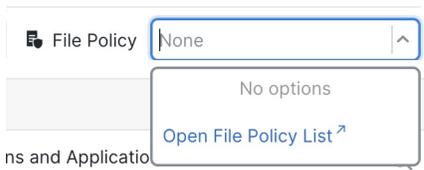
- b) 从列表中选择一个系统提供的策略。

对于大多数使用场景，我们建议选择平衡安全与连接。

步骤 5（可选）添加在访问控制规则之后应用的文件策略。

- a) 点击文件策略 (**File Policy**) 下拉列表，然后选择现有策略或通过选择打开文件策略列表 (**Open File Policy List**) 添加一个策略。

图 22: 文件策略



对于新策略，系统将在单独的选项卡中打开策略 > 安全策略 > 恶意软件和文件 页面。

- b) 有关创建策略的详细信息，请参阅 [Cisco Secure Firewall 设备管理器配置指南](#)。
- c) 返回添加规则 (**Add Rule**) 页面，从下拉列表中选择新创建的策略。

步骤 6 点击应用 (**Apply**)。

规则即已添加至 **Rules** 表。

步骤 7 点击保存。

部署配置

将配置更改部署到设备；在部署之前，您的所有更改都不会在设备上生效。

过程

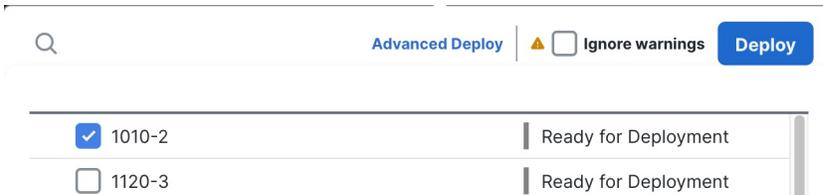
步骤 1 点击右上方的部署 (**Deploy**)。

图 23: 部署



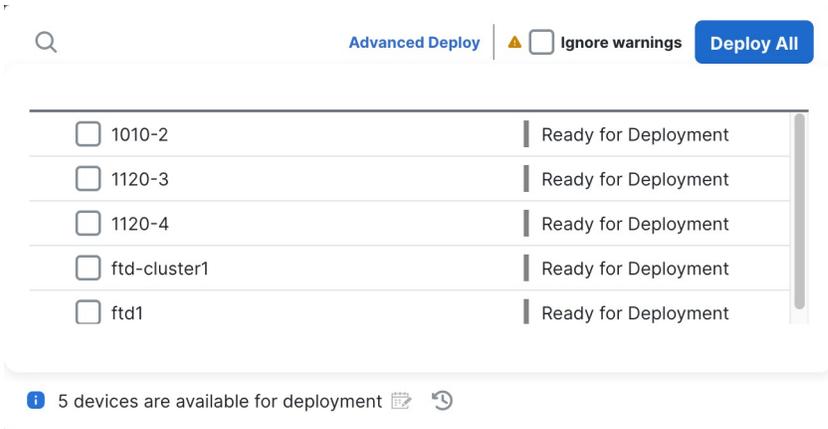
步骤 2 要快速部署，请选中特定设备，然后点击部署 (**Deploy**)。

图 24: 部署所选



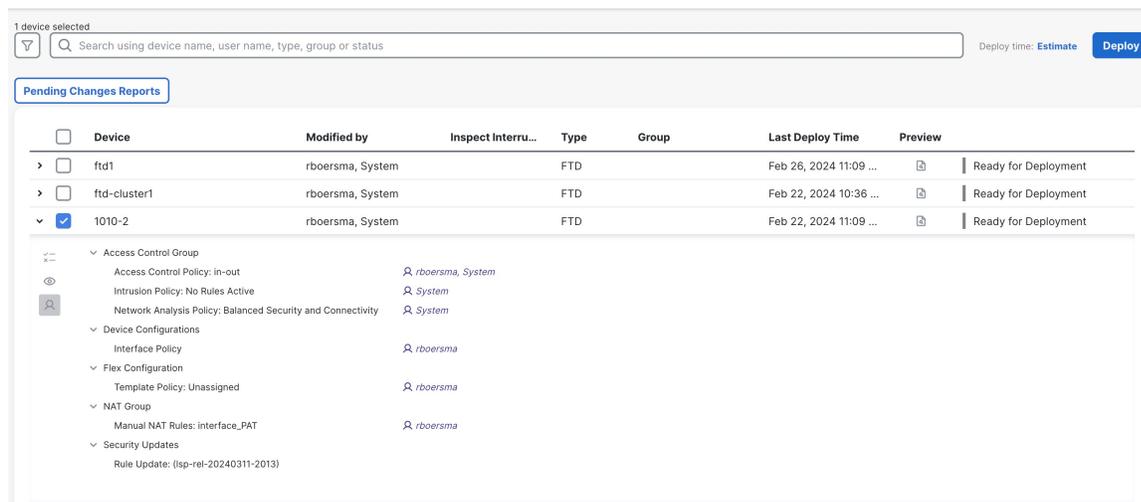
或者，点击全部部署 (**Deploy All**) 以部署到所有设备。

图 25: 全部部署



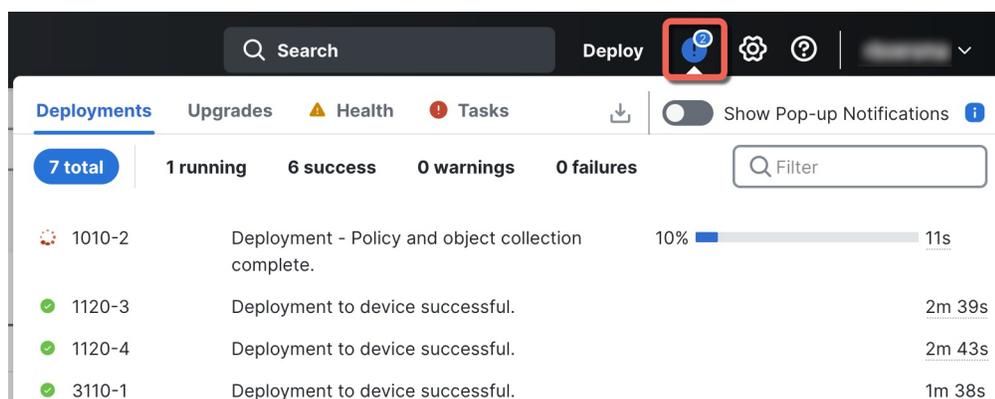
否则，对于其他部署选项，请点击高级部署 (**Advanced Deploy**)。

图 26: 高级部署



步骤 3 确保部署成功。点击菜单栏中部署 (**Deploy**) 按钮右侧的图标可以查看部署状态。

图 27: 部署状态



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。