最佳实践： 威胁防御的使用案例

以下主题介绍了您可能希望使用 设备管理器，通过 威胁防御 完成的一些常见任务。这些使用案例假定您已完成设备配置向导，并保留了此初始配置。即使修改了初始配置，也应该能够使用这些示例了解产品的使用方法。

- 如何在设备管理器上配置设备 ， 第 1 页
- 如何深入了解您的网络流量， 第 6 页
- 如何阻止威胁， 第 13 页
- 如何阻止恶意软件， 第 17 页
- 如何实施可接受使用策略（URL 过滤），第 20 页
- 如何控制应用的使用， 第 25 页
- 如何添加子网， 第 28 页
- 如何被动监控网络上的流量， 第 33 页
- 更多示例， 第 38 页

如何在设备管理器上配置设备

完成设置向导后，您的设备应该会正常工作并应部署了下列基本策略：

- 外部接口和内部接口。其他数据接口则未配置。
- (Firepower 4100/9300) 未预配置任何数据接口。
- (ISA 3000) 网桥组包含 2 个内部接口和 2 个外部接口。要完成设置，需要手动设置 BVI1 IP 地址。
- （除了 Firepower 4100/9300）内部和外部接口的安全区。
- （除了Firepower 4100/9300）信任所有内部到外部流量的访问规则。 对于 ISA 3000，存在允许从内部到外部的所有流量以及从外部到内部的所有流量的访问规则。
- （除了 Firepower 4100/9300 和 ISA 3000） 接口 NAT 规则，用于将所有内部到外部流量转换到外部接口 IP 地址上的唯一端口。
- （除了 Firepower 4100/9300 和 ISA 3000） 在内部接口上运行的 DHCP 服务器。

以下步骤概述了可能需要配置的其他功能。请点击页面上的帮助按钮 (**?**)，获取有关每个步骤的详细信息。

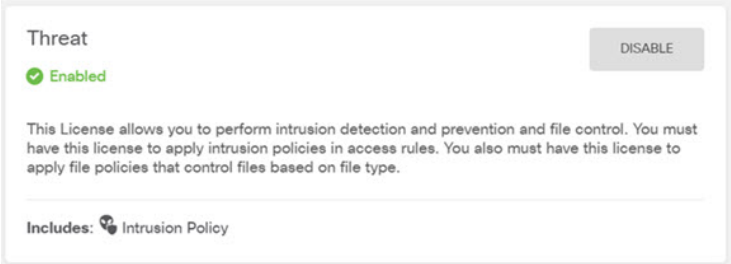
过程

步骤 1 选择**设备**，然后点击**智能许可证**组中的**查看配置**。

对于您想要使用的可选许可证（ 威胁、恶意软件、URL），点击**启用 (Enable)**。如果在安装过程中注册设备，还可启用所需的 RA VPN 许可证。如果不确定是否需要使用某个许可证，请参阅该许可证的说明。

如果尚未注册，可以从该页面执行该操作。点击**注册设备**，并按照说明执行操作。请在评估版许可证到期前进行注册。

例如，以下是启用的Cisco Secure Firewall IPS 许可证：



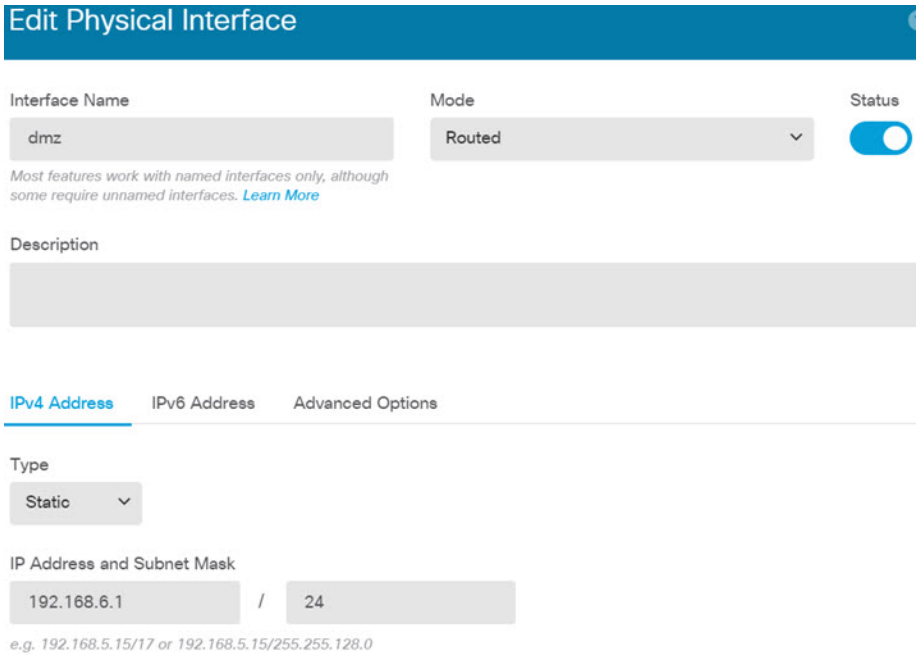
步骤 2 如果连接其他接口，请选择**设备**，然后点击**接口**摘要中的链接，然后点击接口类型以查看接口列表。

- 对于 Firepower 4100/9300，未对任何数据接口进行名称、IP 地址或安全区预配置，因此，您需要启用和配置要使用的任何接口。
- 由于ISA 3000 预先配置了包含所有数据接口的网桥组，因此无需配置这些接口。 但是，必须手动配置 BVI IP 地址。如果要拆分该网桥组，可以对其进行编辑，删除要单独处理的接口。然后，可以将这些接口配置为承载单独的网络。

  对于其他型号，可以为其他接口创建网桥组或配置单独的网络，或同时采用这两种方法。
- 对于 Firepower 1010，除 Ethernet1/1（外部）以外的所有接口均分配给 VLAN1（内部）的访问模式交换机端口。可以将交换机端口更改为防火墙端口；添加新的 VLAN 接口，并为其分配交换机端口；或配置中继模式交换机端口。

点击每个接口的编辑图标 ( )，定义 IP 地址和其他设置。

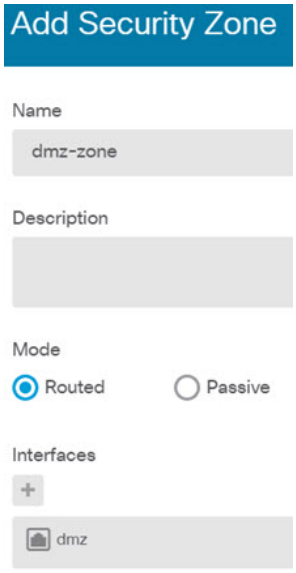
以下示例将一个接口配置为“隔离区”(DMZ)，可以将可公开访问的资产（例如 Web 服务器）放在该区域中。完成后点击**保存 (Save)**。



步骤 3 如果已配置新接口，请选择**对象 (Objects)**，然后从目录中选择**安全区域 (Security Zones)**。

根据需要编辑或创建新区域。每个接口都必须属于一个区域，因为需要根据安全区域而不是接口来配置策略。配置接口时不能将其放在区域中，因此每当创建新接口或更改现有接口的用途之后，都必须编辑区域对象。

以下示例显示如何为 DMZ 接口创建一个新的 DMZ 区域。

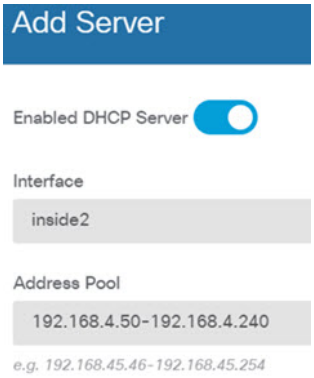


步骤 4 如果希望内部客户端使用DHCP从设备中获取IP地址，请选择**设备**，然后依次选择**系统设置**>**DHCP服务器**。选择 **DHCP 服务器**选项卡。

内部接口已配置了 DHCP 服务器，但可以编辑地址池或甚至将其删除。如果配置了其他内部接口，则在这些接口上设置 DHCP 服务器是非常典型的做法。点击 +，为每个内部接口配置服务器和地址池。

此外，还可以在**配置**选项卡中对为客户端提供的 WINS 和 DNS 列表进行微调。

以下示例显示如何在 inside2 接口（地址池为 192.168.4.50-192.168.4.240）上设置 DHCP 服务器。



步骤 5 选择**设备**，然后点击**路由**组中的**查看配置**，并配置默认路由。

默认路由通常指向位于外部接口之外的上游或 ISP 路由器。默认的 IPv4 路由适用于 any-ipv4 (0.0.0.0/0)，而默认的 IPv6 路由适用于 any-ipv6 (::0/0)。为所使用的每个 IP 版本创建路由。如果使用 DHCP 获取外部接口的地址，则可能已经拥有所需的默认路由。

此页面上定义的路由仅适用于数据接口，而不会影响管理接口。在**系统设置** > **管理接口**上设置管理网关。

以下示例显示 IPv4 的默认路由。在此示例中，isp-gateway 是用于标识 ISP 网关 IP 地址的网络对象（必须从 ISP 中获取地址）。可以通过点击**网关 (Gateway)** 下拉菜单底部的**创建新网络 (Create New Network)**，来创建该对象。

步骤 6 选择**策略 (Policies)**，并为网络配置安全策略。

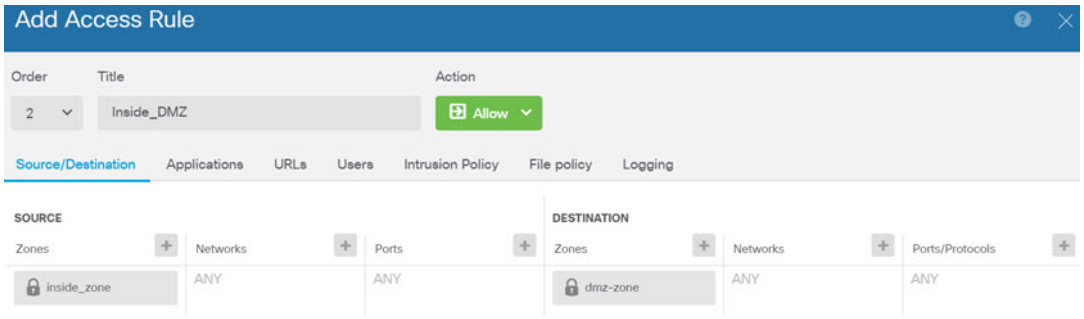
设备安装向导设置允许内部区域与外部区域之间存在流量流动，并对所有接口上流向外部接口的流量启用网络地址转换 (NAT)。即使配置了新接口，如果将其添加到内部区域对象中，访问控制规则也将自动应用于这些接口。

但是，如果有多个内部接口，则需要一条访问控制规则来允许内部区域之间的流量。如要添加其他安全区域，则需要规则来允许这些区域之间的流量。这是您需要进行的最低限度的更改。

此外，您还可配置其他策略以提供附加服务，并对NAT和访问规则进行精细调整，以实现组织需要的结果。您可以配置以下策略：

- **SSL 解密 (SSL Decryption)** - 如果要检查加密连接（例如HTTPS）是否存在入侵、恶意软件等，则必须解密连接。使用 SSL 解密策略确定需要解密的连接。系统检查连接后，会将其重新加密。
- **身份 (Identity)** - 如果要将网络活动与各个用户相关联，或根据用户或用户组成员身份控制网络访问，请使用身份策略确定与给定源 IP 地址关联的用户。
- **安全智能** - 使用安全智能策略快速丢弃进出选定 IP 地址或URL 的连接。阻止已知恶意站点后，在访问控制策略中便无需考虑这些站点。思科提供定期更新的已知恶意地址和URL源，可使安全智能阻止列表实现动态更新。使用智能源，无需通过编辑策略来添加或删除阻止列表中的项目。
- **NAT**（网络地址转换）- 使用 NAT 策略将内部 IP 地址转换为外部可路由地址。
- **访问控制 (Access Control)** - 使用访问控制策略确定网络上允许的连接。您可以按安全区域、IP 地址、协议、端口、应用、URL、用户或用户组进行过滤。您还可以使用访问控制规则来应用入侵策略和文件（恶意软件）策略。使用此策略实施 URL 过滤。
- **入侵 (Intrusion)** - 使用入侵策略检测已知威胁。即使使用访问控制规则应用入侵策略，也仍可以编辑入侵策略，以选择性地启用或禁用特定的入侵规则。

以下示例显示如何在访问控制策略中允许内部区域与 DMZ 区域之间的流量。在此示例中，任何其他选项卡上均未设置任何选项，**日志记录 (Logging)** 除外，其中**在连接结束时 (At End of Connection)** 选项已被选中。



步骤 7 确认您的更改。

a) 点击网页右上角的**部署更改**图标。

b) 点击**立即部署**按钮。

您可以等待部署完成，也可以点击**确定**，稍后再检查任务列表或部署历史记录。

如何深入了解您的网络流量

在完成初始设备设置后，您会获得一项访问控制策略，该策略允许所有内部流量访问互联网或其他上游网络，以及一项会阻止所有其他流量的默认操作。在创建其他访问控制规则之前，您可能会发现深入了解网络中实际发生的流量非常有益。

您可以使用 设备管理器 的监控功能来分析网络流量。 设备管理器 报告可帮助您回答以下问题：

- 我的网络的用途是什么？
- 哪些用户使用的网络流量最多？
- 我的用户会访问哪些站点？
- 他们使用的是什么设备？
- 哪些访问控制规则（策略）的使用次数最多？

初始访问规则可提供一些信息帮助您深入了解流量，包括策略、目的和安全区。但要获取用户信息，您需要配置一项要求用户验证自己（身份）的身份策略。要获取网络中所使用应用的信息，您需要进行一些其他调整。

以下步骤程序介绍了如何设置 威胁防御设备以监控流量，并概述了配置和监控策略的端到端流程。

注释 通过此步骤程序无法了解用户所访问站点的网站类别和信誉，因此在URL类别控制面板中看不到有用的信息。只有实施基于类别的 URL 过滤并启用 URL 许可证，才能获取类别和信誉数据。如果只想获取这些信息，可以添加一个新访问控制规则，以允许访问可接受的类别（例如财务），并将其设为访问控制策略的第一个规则。有关实施URL过滤的详细信息，请参阅如何实施可接受使用策略（URL 过滤），第 20 页。

过程

步骤 1 要了解用户行为，您需要配置身份策略以确保可以识别与连接关联的用户。

通过启用身份策略，可以收集有关网络用户以及他们所使用资源的信息。在用户监控控制面板中可获取这些信息。另外，也可以获取事件查看器中所示的连接事件的用户信息。

在本示例中，我们将实施主动身份验证以获取用户身份。使用主动身份验证时，设备将提示用户输入用户名和密码。只有用户使用支持 HTTP 连接的网络浏览器时，才会对他们进行身份验证。

如果用户未通过身份验证，其仍可进行 Web 连接。这仅仅意味着，您不会获取连接的用户身份信息。如果需要，可以创建一项访问控制规则，以丢弃身份验证失败的用户的流量。

a) 在主菜单中点击**策略**，然后点击**身份**。

身份策略最初处于禁用状态。使用主动身份验证时，身份策略使用您的 Active Directory 服务器对用户进行身份验证，并将他们与其使用的工作站的 IP 地址关联。随后，系统会将该 IP 地址的流量标识为该用户的流量。

b) 点击**启用身份策略**。

c) 点击**创建身份规则**按钮或 + 按钮，创建规则以要求进行主动身份验证。

在本示例中，我们假设您要对每个用户都执行身份验证。

d) 为规则输入**名称**，可以是您选择的任何内容，例如 Require_Authentication。

e) 在**源/目标**选项卡上，保留默认设置，此设置应用于任何条件。

您可以根据需要将该策略限制为更具体的流量集。但是，主动身份验证仅适用于 HTTP 流量，因此非 HTTP 流量与源/目标条件匹配并不重要。有关身份策略属性的详细信息，请参阅配置身份规则

f) 对于**操作**，请选择**主动身份验证**。

假设您尚未配置身份策略设置，由于存在一些未定义的设置，系统将打开“身份策略配置”对话框。

g) 配置主动身份验证所需的强制网络门户和 SSL 解密设置。

如果身份规则要求对用户进行主动身份验证，则该用户将被重定向到强制网络门户端口，然后系统会提示他们进行身份验证。强制网络门户需要使用 SSL 解密规则，系统将自动生成这些规则，但您必须选择要用于 SSL 解密规则的证书。

- **服务器证书** - 选择在主动身份验证期间提供给用户的内部证书。您可以选择预定义的自签名 DefaultInternalCertificate，也可以点击**创建新的内部证书**并上传您的浏览器已信任的证书。

  如果用户不上传其浏览器已经信任的证书，则必须接受该证书。

- **重定向到主机名** - 选择定义接口的完全限定主机名的网络对象，该接口应用作主动身份验证请求的强制网络门户。如果该对象尚不存在，请点击**创建新网络**。

  FQDN 必须解析为设备上接口之一的 IP 地址。通过使用 FQDN，您可以为客户端将识别的主动身份验证分配证书，从而避免用户在被重定向到 IP 地址时收到不受信任证书警告。证书可以在证书的使用者备选名称 (SAN) 中指定 FQDN、通配符 FQDN 或多个 FQDN。

  如果身份规则要求对用户进行主动身份验证，但您未指定重定向 FQDN，则用户将被重定向到他们连接的接口上的强制网络门户端口。

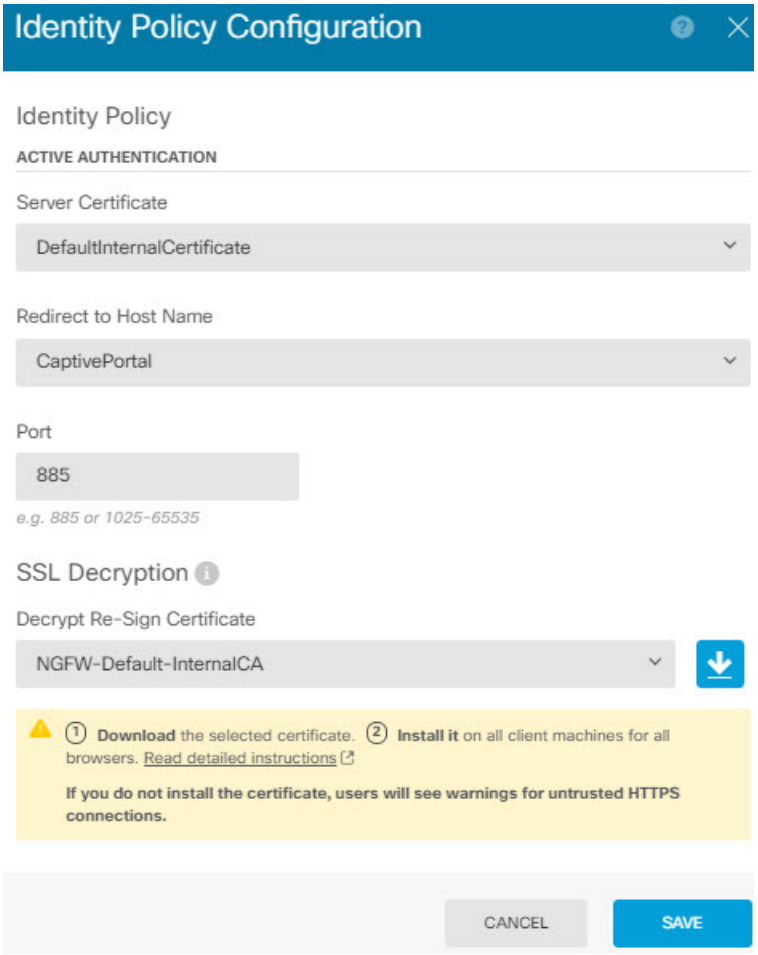
- **端口** - 强制网络门户端口。默认端口是 885 (TCP)。如果配置了其他端口，则该端口必须在 1025-65535 的范围内。

- **解密重签名证书** - 选择内部 CA 证书，以用于使用重签名证书实施解密的规则。您可以使用预定义的 NGFW-Default-InternalCA 证书（默认证书），也可以使用创建或上传的证书。如果尚无证书，请点击**创建内部 CA** 进行创建。（仅当您尚未启用 SSL 解密策略时，系统才会提示您提供解密重签名证书。）

  如果尚未在客户端浏览器中安装证书，请点击下载按钮( )获取副本。有关如何安装证书的信息，请参阅各浏览器文档。另请参阅为解密重签名规则下载 CA 证书。

示例：

“身份策略配置”对话框现在应如下所示。



h) 点击**保存**以保存主动身份验证设置。

“主动身份验证”选项卡现在显示在“操作”设置下方。

i) 在**主动身份验证**选项卡上，选择 **HTTP 协商**。

此选项允许浏览器和目录服务器按顺序协商最安全的身份验证协议，先是NTLM，然后是HTTP基本验证。

注释 如果您不提供**重定向到主机名** FQDN，HTTP Basic、HTTP 响应页面和 NTLM 身份验证方法会使用接口的 IP 地址将用户重定向到强制网络门户。但对于 HTTP 协商，用户将使用完全限定 DNS 名称 *firewall-hostname.AD-domain-name* 进行重定向。如果您想在不提供**重定向到主机名** FQDN 的情况下使用 HTTP 协商，还必须更新 DNS 服务器以将此名称映射到您需要进行主动身份验证的所有内部接口的 IP 地址。否则，将无法进行重定向，用户也无法进行身份验证。建议您始终提供**重定向到主机名** FQDN 以确保行为一致，而无论采用哪种身份验证方法。 如果无法或不想更新 DNS 服务器，请选择其他某种身份验证方法。

j) 对于 **AD 身份源**，请点击**创建新身份领域**。

如果您已创建领域服务器对象，只需选中它并跳过配置服务器的步骤。

填写以下字段，然后点击**确定 (OK)**。

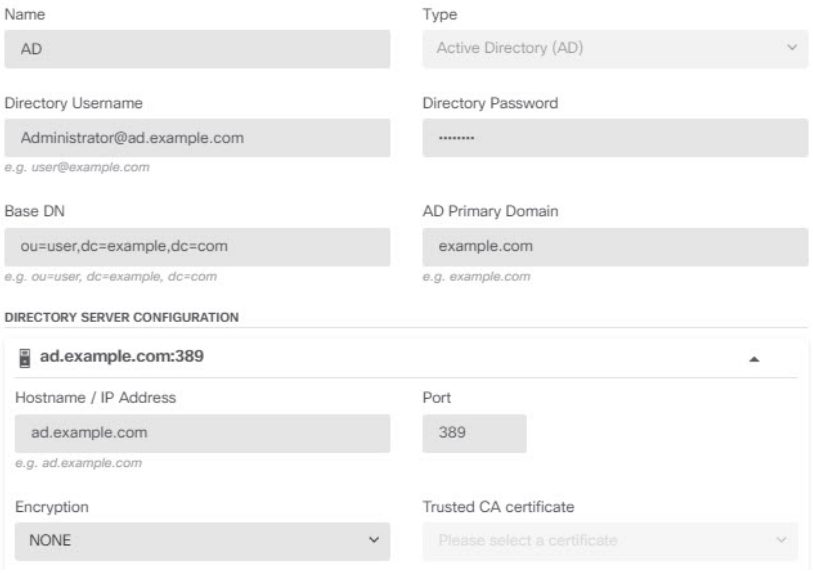
- **名称** - 目录领域的名称。
- **类型** - 目录服务器的类型。Active Directory 是唯一支持的类型，所以无法更改此字段。
- **目录用户名、目录密码** - 用户的标识名称和密码，该用户具备访问您要检索的用户信息的适当权限。对于 Active Directory，用户不需要更高的权限。您可以在域中指定任何用户。用户名必须是完全限定的；例如，Administrator@example.com（而不仅仅是 Administrator）。

  注释 系统使用此信息生成 ldap-login-dn 和 ldap-login-password。例如，Administrator@example.com 被转换为 cn=adminisntrator、cn=users、dc=example、dc=com。请注意，cn = users 始终是此转换的一部分，因此您必须在公用名“users”文件夹下配置此处指定的用户。

- **基准 DN** - 用于搜索或查询用户和组信息的目录树，即用户和组的公共父项。例如 dc=example,dc=com。有关查找基准 DN 的信息，请参阅确定目录基准标识名。
- **AD 主域** - 设备应加入的 Active Directory 完全限定域名。例如 example.com。
- **主机名/IP 地址** - 目录服务器的主机名或 IP 地址。如果以加密方式连接到服务器，则必须输入完全限定域名，而非 IP 地址。
- **端口** - 用于与服务器通信的端口号。默认值为 389。如果选择 LDAPS 作为加密方法，请使用端口 636。
- **加密** - 要使用加密连接下载用户和组信息，请选择所需的方法 **STARTTLS** 或 **LDAPS**。系统默认为**无**，也就是说以明文形式下载用户和组信息。
  - **STARTTLS** 将会协商加密方法，并使用目录服务器支持的最强方法。使用端口 389。如果将领域用于远程访问 VPN，则不支持此选项。
  - **LDAPS** 需要基于 SSL 的 LDAP。使用端口 636。
- **受信任的 CA 证书** - 如果选择加密方法，请上传证书颁发机构 (CA) 证书以便在系统和目录服务器之间启用受信任的连接。如果要使用证书进行身份验证，则证书中的服务器名称必须与服务器主机名/IP 地址匹配。例如，如果使用 10.10.10.250 作为 IP 地址，但证书中的地址为 ad.example.com，则连接失败。

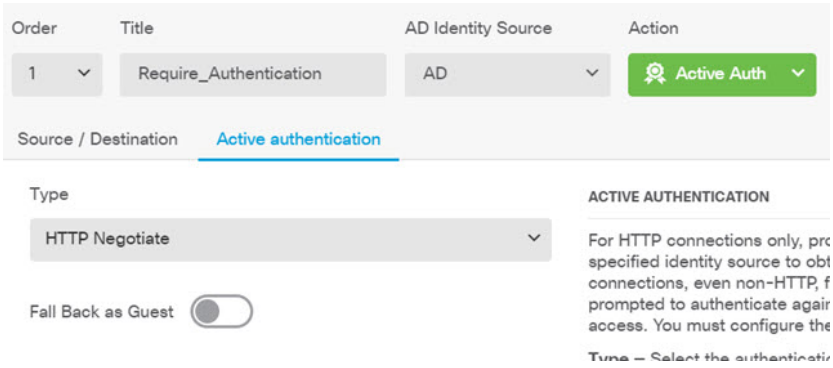
示例：

例如，下图显示了如何为 ad.example.com 服务器创建未加密的连接。主域为 example.com，目录用户名为 Administrator@ad.example.com。所有用户和组信息均位于标识名 (DN) ou=user,dc=example,dc=com 的下方。



k) 对于 **AD 身份源**，请选择您刚刚创建的对象。

规则应类似于以下内容：



l) 点击**确定**以添加规则。

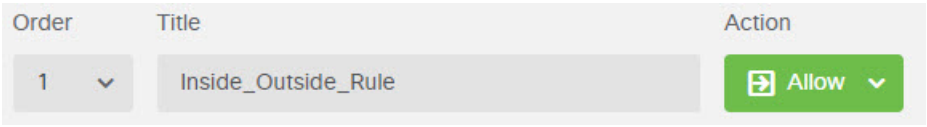
如果查看窗口的右上角，可以看到**部署**图标现在带有一个圆点，表示存在未部署的更改。在用户界面进行更改还不足以获取在设备上配置的更改，还必须部署更改。因此，您可以执行一组相关更改，然后再部署它们，这样就不会出现仅在设备上配置了部分更改的情况。部署更改在此程序的后面步骤执行。

步骤 2 将 Inside_Outside_Rule 访问控制规则上的操作更改为**允许**。

Inside_Outside_Rule访问规则创建为信任规则。但由于不检测受信任的流量，所以在流量匹配条件不含除区域、IP 地址和端口之外的应用或其他条件时，系统无法了解受信任流量（例如应用）的某些特征。如果将该规则更改为允许非受信任的流量，系统会全面检测流量。

注释 （ ISA 3000。）还要考虑将 Outside_Inside_Rule、Inside_Inside_Rule 和 Outside_Outside_Rule 从“信任”更改为“允许”。

a) 点击**策略 (Policies)**页面上的**访问控制 (Access Control)**。
b) 将鼠标悬停在Inside_Outside_Rule行右侧的**操作**单元格上将显示编辑和删除图标，然后点击编辑图标 ( ) 以打开该规则。
c) 在**操作**下选择**允许**。

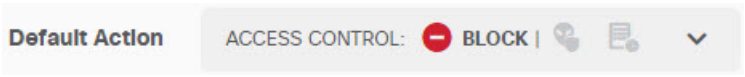


d) 点击**确定**以保存更改。

步骤 3 基于访问控制策略默认操作启用日志记录。

控制面板仅包含与启用连接日志记录的访问控制规则匹配的连接的信息。Inside_Outside_Rule规则启用日志记录，但默认操作为禁用日志记录。因此，控制面板仅显示 Inside_Outside_Rule 的信息，而不反映与任何规则皆不匹配的连接。

a) 点击访问控制策略页面底部默认操作的任意位置。

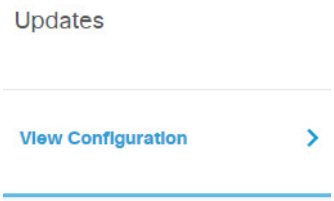


b) 选择**选择日志操作 > 连接开始和结束时**。
c) 点击**确定 (OK)**。

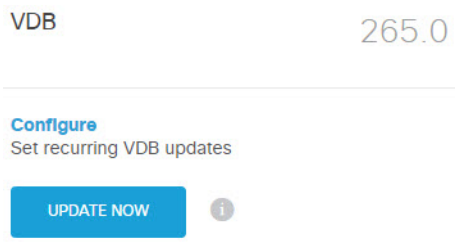
步骤 4 设置漏洞数据库 (VDB) 的更新计划。

思科会定期发布 VDB 更新，其中包括可识别连接中所用应用的应用检测器。您应定期更新 VDB。您可以手动下载更新，也可以设置定期更新计划。以下步骤程序介绍了如何设置计划。默认情况下，VDB 更新处于禁用状态，所以您需要采取措施来获取 VDB 更新。

a) 点击**设备**。
b) 点击“更新”组中的**查看配置**。



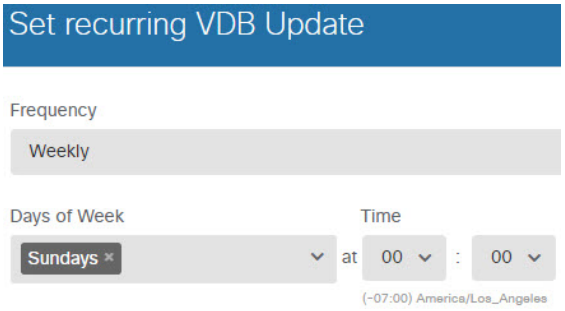
c) 点击 VDB 组中的**配置**。



d) 定义更新计划。

选择不会影响网络的时间和频率。另外，请注意系统在下载更新后会自动执行部署。激活新的检测器需要执行此操作。因此，也会部署您已进行和保存，但尚未部署的任何配置更改。

例如，以下计划会在每周星期日上午 12:00（使用 24 小时制表示法）更新一次 VDB。



e) 点击**保存 (Save)**。

步骤 5 确认您的更改。

a) 点击网页右上角的**部署更改**图标。

b) 点击**立即部署**按钮。

您可以等待部署完成，也可以点击**确定**，稍后再检查任务列表或部署历史记录。

下一步做什么

这时，监控控制面板和事件应开始显示用户和应用的相关信息。您可以评估这些信息是否存在不需要的模式，并制定新的访问规则来限制不可接受的用途。

如果要开始收集入侵和恶意软件的相关信息，您需要针对一个或多个访问规则启用入侵和文件策略。另外，您还需要对这些功能启用许可证。

如果要开始收集 URL 类别的相关信息，则必须实施 URL 过滤。

如何阻止威胁

通过将入侵策略添加到访问控制规则中，可以实施下一代入侵防御系统 (IPS) 过滤。入侵策略可分析网络流量，根据已知威胁比较流量内容。如果某个连接与您正在监控的威胁匹配，系统将丢弃该连接，从而阻止攻击。

处理所有其他流量后，才会检验网络流量中是否存在入侵。通过将入侵策略与访问控制规则相关联，您是在告诉系统：在其传递符合访问控制规则条件的流量之前，您首先想要使用入侵策略检测流量。

您只能对**允许**流量的规则配置入侵策略。对于设置为**信任**或**阻止**流量的规则，系统不会执行检测。另外，如果默认操作是**允许**，您可以将入侵策略配置为默认操作的一部分。

这些入侵策略由 思科 Talos 情报小组 (Talos) 设计，其设定了入侵和预处理器规则的状态和高级设置。 如果您使用 Snort 3 作为检测引擎，则可以根据 Talos 策略创建自己的自定义策略。

除了检查允许的流量是否存在潜在入侵之外，您还可以使用安全智能策略来预先阻止所有传送至或来自已知不良 IP 地址，或传送至已知不良 URL 的流量。

过程

步骤 1 如果尚未启用，请启用 威胁许可证。

必须启用 威胁许可证，才能使用入侵策略和安全智能。如果您当前使用的是评估许可证，将启用该许可证的评估版本。如果已注册设备，则必须购买所需的许可证，并将其添加到您在 Cisco.com 的智能软件管理器账户。

a) 点击**设备**。

b) 点击“智能许可证”(Smart License) 组中的**查看配置 (View Configuration)**。

c) 点击 **威胁**组中的**启用 (Enable)**。

系统会将该许可证注册到您的账户，或激活相应的评估许可证。该组应指示许可证已启用，且按钮将改为显示“禁用”。

步骤 2 针对一个或多个访问规则选择入侵策略。

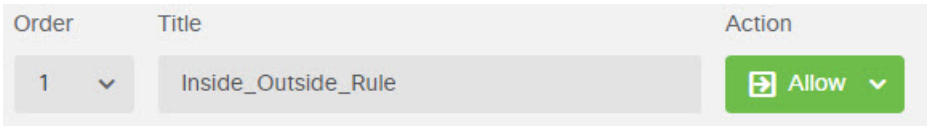
确定哪些规则包括应该扫描威胁的流量。在本示例中，我们会将入侵检测添加到Inside_Outside_Rule中。

a) 在主菜单中点击**策略 (Policies)**。

确保系统显示**访问控制**策略。

b) 将鼠标悬停在Inside_Outside_Rule行右侧的**操作**单元格上将显示编辑和删除图标，然后点击编辑图标 ( ) 以打开该规则。

c) 如果尚未针对**操作**选择**允许**，请进行此选择。

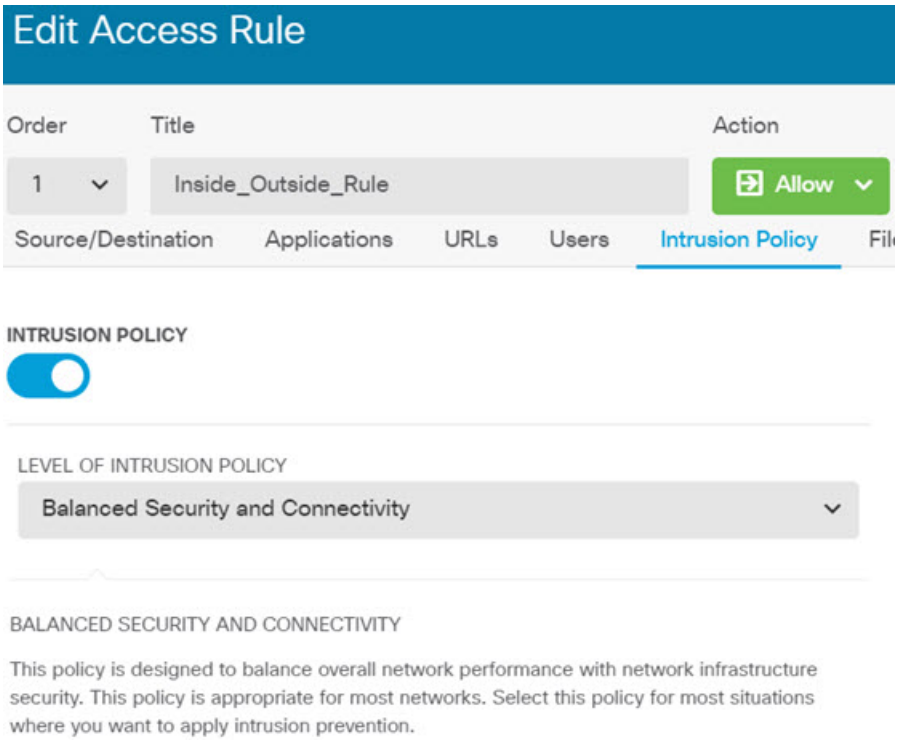


d) 点击**入侵策略 (Intrusion Policy)** 选项卡。

e) 点击**入侵策略 (Intrusion Policy)** 开关启用该选项，然后选择入侵策略。

对于大多数网络，合适的策略是**平衡安全和连接**策略。它提供良好的入侵防御，而不会过度激进，有可能会丢弃可能不想被丢弃的流量。如果您确定要丢弃很多流量，可以选择**连接优先于安全**以放宽策略。

如果您需要积极关注安全性，请尝试**安全优先于连接**策略。**最大检测**策略更加重视网络基础设施的安全性，有可能对操作造成更大的影响。



f) 点击**确定 (OK)** 以保存更改。

步骤 3 （可选。）转到**策略 (Policies)** > **入侵 (Intrusion)**，点击齿轮图标，然后为入侵策略配置系统日志服务器。

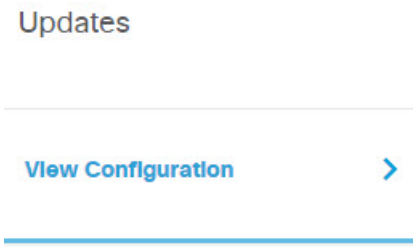
入侵事件不使用为访问控制规则配置的系统日志服务器。

步骤 4 设置入侵规则数据库的更新计划。

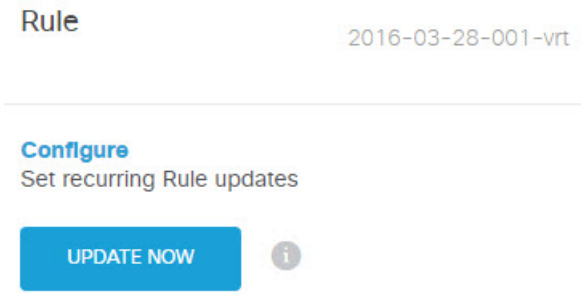
思科会定期发布入侵规则数据库更新，入侵策略使用入侵规则数据库来确定是否应丢弃连接。您应定期更新规则数据库。您可以手动下载更新，也可以设置定期更新计划。以下步骤程序介绍了如何设置计划。默认情况下，数据库更新处于禁用状态，所以您需要采取措施来获取更新的规则。

a) 点击**设备**。

b) 点击“更新”(Updates) 组中的**查看配置 (View Configuration)**。



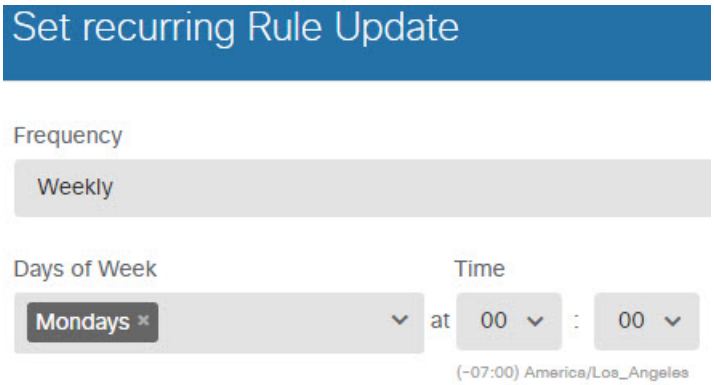
c) 点击“规则”(Rule) 组中的**配置 (Configure)**。



d) 定义更新计划。

选择不会影响网络的时间和频率。另外，请注意系统在下载更新后会自动执行部署。激活新规则需要执行此操作。因此，也会部署您已进行和保存，但尚未部署的任何配置更改。

例如，以下计划会在每周星期一上午 12:00（使用 24 小时制表示法）更新一次规则数据库。



e) 点击**保存 (Save)**。

步骤 5 配置安全智能策略预先丢弃主机和站点已知不良的连接。

通过使用安全智能阻止连接属于已知威胁的主机或站点，为系统节省执行深度数据包检测，以识别每个连接中的威胁所需的时间。安全智能可提早阻止不必要的流量，为系统留出更多的时间来处理您真正关心的流量。

a) 点击**设备 (Device)**，然后点击**更新 (Updates)** 组中的**查看配置 (View Configuration)**。

b) 点击安全智能源组中的**立即更新 (Update Now)**。

c) 此外，点击**配置 (Configure)** 并为源设置定期更新。默认情况下，**每小时**适合大多数网络，但如有必要，可以降低频率。

d) 点击**策略 (Policies)**，然后点击**安全智能 (Security Intelligence)** 策略。

e) 点击**启用安全智能 (Enable Security Intelligence)**（如果尚未启用该策略）。

f) 在**网络 (Network)**选项卡上，点击阻止/丢弃列表下的 **+**，并选择**网络源 (Network Feeds)** 选项卡上的所有源。您可以点击源旁边的 **i** 按钮，阅读每个源的说明。

如果您看到指出尚不存在任何源的消息，请稍后重试。源下载尚未完成。如果此问题仍然存在，请确保管理 IP 地址和互联网之间存在路径。

g) 点击**确定 (OK)** 添加选定的源。

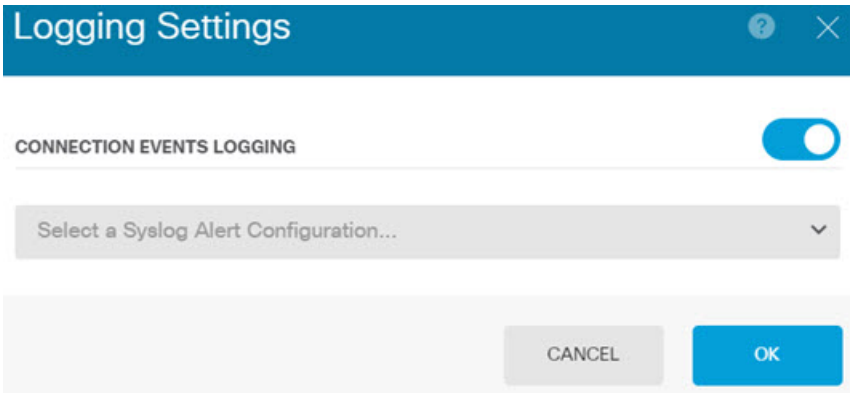
如果您知道存在其他不良 IP 地址，可以依次点击 **+** > **网络对象 (Network Objects)**，添加包含这些地址的对象。您可以点击列表底部的**创建新网络对象 (Create New Network Object)** 立即添加这些对象。

h) 点击 **URL** 选项卡，然后依次点击阻止/丢弃列表中的 **+** > **URL 源 (URL Feeds)**，选择所有 URL 源。点击**确定 (OK)** 以将其添加到列表中。

与网络列表类似，您可以将自己的URL对象添加到该列表中，以阻止源中不存在的其他站点。依次点击 **+** > **URL 对象 (URL Objects)**。您可以通过点击列表末尾的**创建新 URL 对象 (Create New URL Object)**添加新对象。

i) 点击齿轮图标，并启用**连接事件日志记录 (Connection Events Logging)**，以便策略能够为匹配的连接生成安全智能事件。点击**确定 (OK)**，保存更改。

如果您不启用连接日志记录，您将没有数据来评估策略的表现是否达到预期。如果定义了外部系统日志服务器，现在即可选择此服务器，以便将事件同时发送到该服务器上。



j) 根据需要，您可以在每个选项卡的**不阻止**列表中添加网络或 URL 对象，创建阻止列表例外。

不阻止列表不是真正的“允许”列表。它们是例外列表。如果例外列表中的地址或 URL 也出现在阻止列表中，系统允许该地址或 URL 的连接传递到访问控制策略。通过这种方式，您可以阻止源，但如果您后期发现所需的地址或站点被阻止，可以使用例外列表来覆盖阻止，而不需要彻底删除源。注意，这些连接随后由访问控制和入侵策略（如果已配置）评估。因此，如果任何连接包含威胁，这些连接将在入侵检查过程中被识别和阻止。

使用“访问和 SI 规则”控制面板和事件查看器中的“安全智能”视图，判断哪些流量实际上被策略丢弃，以及您是否需要在**不阻止**列表中添加地址或 URL。

步骤 6 确认您的更改。

a) 点击网页右上角的**部署更改**图标。

b) 点击**立即部署**按钮。

您可以等待部署完成，也可以点击**确定**，稍后再检查任务列表或部署历史记录。

下一步做什么

如果已识别任何入侵，这时监控控制面板和事件应开始显示攻击者、目标和威胁的相关信息。您可以评估这些信息来确定，您的网络是否需要更多安全预防措施，或是否需要降低使用的入侵策略级别。

对于安全智能，您可以在“访问和SI规则”控制面板上查看策略使用情况。您还可以在事件查看器中查看安全智能事件。安全智能数据块不反映在入侵威胁信息中，因为流量在可检测之前已被阻止。

如何阻止恶意软件

用户不断面临着经由互联网站点或其他通信方法（例如邮件）而感染恶意软件的风险。即使受信任的网站，也可能遭受劫持，让信任该网站的用户遭受恶意软件的肆意攻击。网页可能包含来自不同

来源的对象。这些对象可能包含图像、可执行文件、JavaScript、广告等等。受感染的网站通常会植入外部源中托管的对象。真正的安全性意味着，逐个查看每个对象，而不只是初始请求。

使用文件策略检测使用恶意软件防御的恶意软件。另外，您还可以使用文件策略执行文件控制，以允许控制特定类型的所有文件，而不考虑文件中是否包含恶意软件。

恶意软件防御使用Cisco Secure Malware Analytics 云为网络流量中检测到的恶意软件检索处置。管理接口必须可连接互联网，以便访问 Cisco Secure Malware Analytics 云 并搜索恶意软件。当设备检测到符合条件的文件时，它将使用该文件的 SHA-256 散列值来查询 Cisco Secure Malware Analytics 云中是否存在该文件的处置。可能的处置可以是**正常**、**恶意软件**或**未知**（没有明确判定）。如果无法连接 Cisco Secure Malware Analytics 云，则处置为**未知**。

通过将文件策略与访问控制规则相关联，您是在告诉系统：在其传递符合访问控制规则条件的流量之前，您首先想要检测连接中的任何文件。

您只能对**允许**流量的规则配置文件策略。对于设置为**信任**或**阻止**流量的规则，系统不会执行检测。

过程

步骤 1 如果尚未启用，请启用恶意软件和 威胁许可证。

除入侵策略所需的 威胁许可证之外，您还必须启用恶意软件许可证才能使用文件策略。如果您当前使用的是评估许可证，将启用该许可证的评估版本。如果已注册设备，则必须购买所需的许可证，并将它们添加到您在 Cisco.com 的智能软件管理器账户。

a) 点击**设备**。

b) 点击“智能许可证”组中的**查看配置**。

c) 如果尚未启用，请在**恶意软件**组中点击**启用 (Enable)**，如果已经启用，则在 **威胁**组中点击。

系统会将该许可证注册到您的账户，或激活相应的评估许可证。该组应指示许可证已启用，且按钮将改为显示“禁用”。

步骤 2 针对一个或多个访问规则选择文件策略。

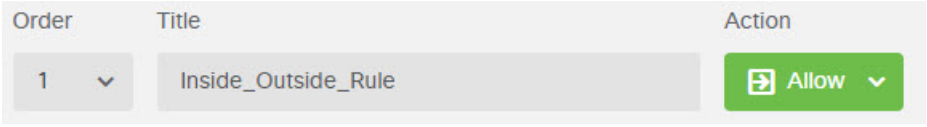
确定哪些规则包括应该扫描恶意软件的流量。在本示例中，我们会将文件检测添加到 Inside_Outside_Rule 中。

a) 在主菜单中点击**策略**。

确保系统显示**访问控制**策略。

b) 将鼠标悬停在 Inside_Outside_Rule 行右侧的**操作**单元格上将显示编辑和删除图标，然后点击编辑图标 ( ) 以打开该规则。

c) 如果尚未针对**操作**选择**允许**，请进行此选择。



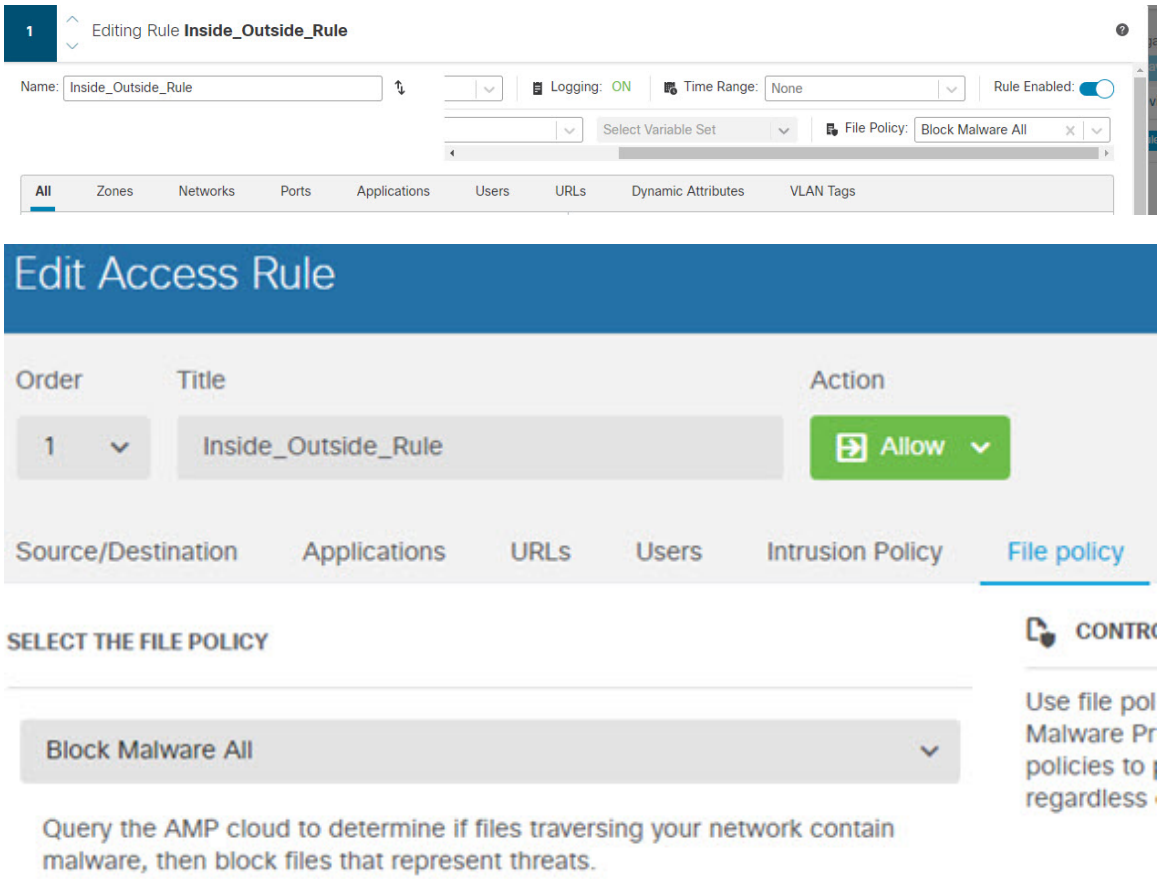
d) 点击**文件策略**选项卡。

e) 点击要使用的文件策略。

您的主要选择为**阻止所有恶意软件**或**全部执行云查找**，前者将丢弃被视为恶意软件的任何文件，后者将查询 Cisco Secure Malware Analytics 云 以确定文件处置，但不执行阻止。如果您想先查看文件评估的方式，请使用云查找。如果对文件的评估方式感到满意，稍后可以切换到阻止策略。

使用其他策略也可以阻止恶意软件。这些策略搭配文件控制，可阻止上传 Microsoft Office（或 Office）和 PDF 文档。也就是说，除了阻止恶意软件，这些策略还可阻止用户向其他网络发送这些类型的文件。如果它们符合您的需求，您可以选择这些策略。

对于本示例，请选择**阻止所有恶意软件**。



f) 点击**日志记录**选项卡，并确认是否已选中“文件事件”下的**日志文件**。

默认情况下，无论何时选择文件策略，文件日志记录均已启用。只有启用文件日志记录，才能获得事件和控制面板中的文件和恶意软件信息。

g) 点击**确定**以保存更改。

步骤 3 确认您的更改。

a) 点击网页右上角的**部署更改**图标。

b) 点击**立即部署**按钮。

您可以等待部署完成，也可以点击**确定**，稍后再检查任务列表或部署历史记录。

下一步做什么

如果已传输任何文件或恶意软件，这时监控控制面板和事件应开始显示文件类型、文件和恶意软件的相关信息。您可以评估这些信息，以确定您的网络在文件传输方面是否需要更多安全预防措施。

如何实施可接受使用策略（URL 过滤）

您的网络可能设有可接受使用策略。可接受使用策略可区分适合您所在组织的网络活动和认为不合适的活动。这些策略通常专注于互联网使用情况，旨在保持工作效率，避免法律责任（例如，维护非敌对工作空间）以及总体控制 Web 网络流量。

您可以使用URL过滤来定义访问策略的可接受使用策略。您可以基于各种类别（例如赌博）过滤，这样就无需识别应阻止的每个单独的网站。对于类别匹配，您还可以指定要允许或阻止的站点的相对信誉。如果用户尝试浏览至任何包含该类别和信誉组合的 URL，会话将被阻止。

使用类别和信誉数据还会简化策略创建和管理。此方法可保证系统将按预期控制网络流量。最后，由于思科的威胁智能会不断更新有关新 URL 以及现有 URL 的新类别和新风险的信息，因此可以确保系统使用最新信息来过滤所请求的 URL。代表安全威胁（如恶意软件、垃圾邮件、僵尸网络和网络钓鱼）的恶意站点出现和消失的速度可能比您更新和部署新策略的速度要快。

以下程序介绍了如何使用URL过滤实施可接受使用策略。在本例中，我们将阻止某些类别的任何信誉的站点、存在风险的社交网站和未分类站点 badsite.example.com。

过程

步骤 1 如果尚未执行此操作，请启用 **URL** 许可证。

只有启用 URL 许可证，才能使用 URL 类别和信誉信息，或查看控制面板和事件中的信息。如果您当前使用的是评估许可证，将启用该许可证的评估版本。如果已注册设备，则必须购买所需的许可证，并将其添加到您在 Cisco.com 的智能软件管理器账户。

a) 点击**设备**。

b) 点击“智能许可证”组中的**查看配置**。

c) 点击 **URL 许可证 (URL License)** 组中的**启用 (Enable)**。

系统会将该许可证注册到您的账户，或激活相应的评估许可证。该组应指示许可证已启用，且按钮将改为显示“禁用”。

步骤 2 创建 URL 过滤访问控制规则。

您可能想要先查看用户访问的站点的类别，再实施阻止规则。对于这种情况，您可以创建一项规则，对可接受的类别（例如财务）执行“允许”操作。由于必须检测所有网络连接来确定URL是否属于此类别，所以即便是非财务站点，您也会收到相关的类别信息。

但是，可能存在您已知要阻止的URL类别。阻止策略还会强制执行检测，所以您会获得非阻止类别连接的类别信息，而不只是受阻止的类别。

a) 在主菜单中点击**策略**。

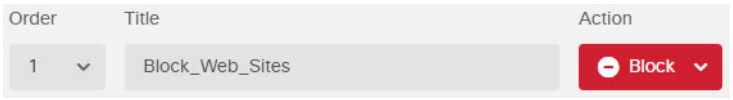
确保系统显示**访问控制**策略。

b) 点击 + 可添加新规则。

c) 配置顺序、标题和操作。

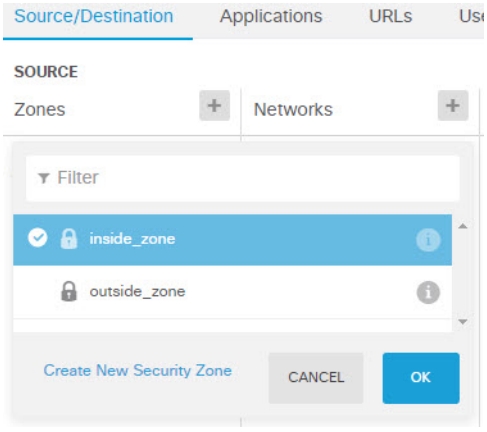
- **顺序** - 默认将新规则添加到访问控制策略的末尾。但是，您必须将此规则放在符合相同源/目的及其他条件的任何规则之前（上方），否则该规则将无法获得匹配（一个连接仅匹配一条规则，即该规则是连接在表中匹配的第一条规则）。对于该规则，我们将使用与初始设备配置期间创建的 Inside_Outside_Rule 相同的源/目的。您可能也已经创建了其他规则。为了最大限度地提高访问控制效率，最好是尽早设置特定规则，以确保快速决定允许还是丢弃某个连接。对于此示例，请选择 **1** 作为规则顺序。
- **标题** - 为该规则指定一个有意义的名称，例如 Block_Web_Sites。

- **操作** - 选择**阻止**。

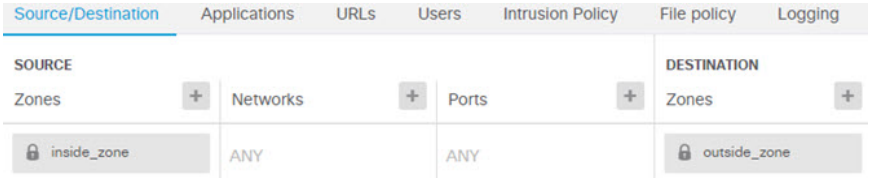


d) 在**源/目的 (Source/Destination)** 选项卡上，点击 **+** 以打开**源 (Source)** > **区域 (Zones)**，然后选择 **inside_zone**，再在区域对话框中点击**确定 (OK)**。

添加任何标准的方式与此相同。点击**+**打开一个小对话框，从中点击您要添加的项目。可以点击多个项目，点击已选项目将取消选择该项目（选中标记表示所选项目）。选择项目后，点击**确定**按钮才能将它们添加到策略中，只是选中项目并不能将项目添加到策略中。



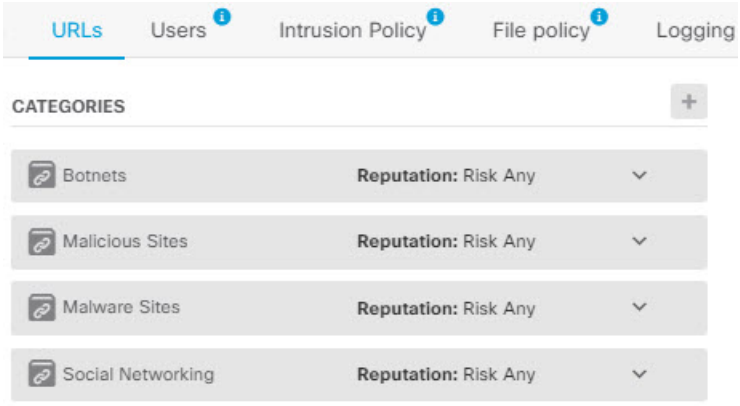
e) 按照相同的方法，为**目的** > **区域**选择 **outside_zone**。



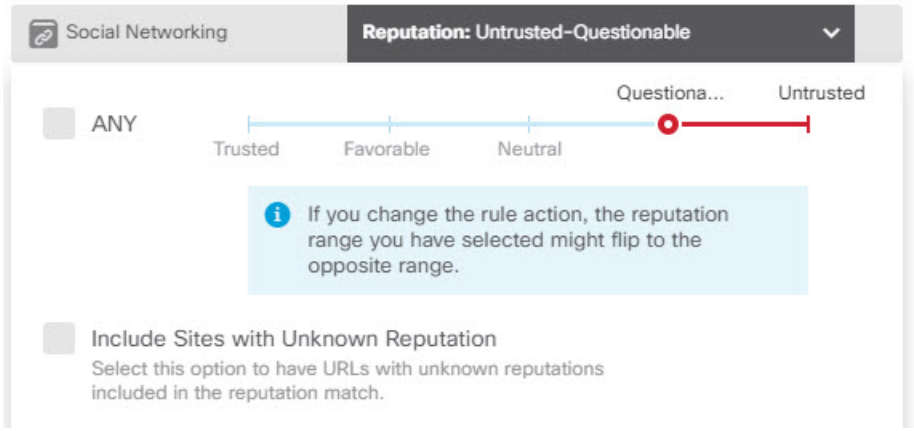
f) 点击 **URL** 选项卡。

g) 点击**类别**的 **+**，然后选择要完全或部分阻止的类别。

在本示例中，请选择僵尸网络、恶意网站、恶意软件站点和社交网络。您可能还希望阻止其他类别。如果您知道要阻止的站点，但不确定类别，请在**待检查 URL** 字段输入 URL，然后点击**前往**。您将转至显示查询结果的网站。



h) 要对“社交网络”类别按信誉敏感性实施阻止，请点击该类别的**信誉：任何风险**，取消选择**任何**，然后将滑块移到**可疑**。点击远离滑块的位置将其关闭。



信誉滑块的左侧指示要允许的站点，右侧是要阻止的站点。在这种情况下，只会阻止信誉属于“可疑”和“不受信任”范围的社交网站。因此，您的用户应该能够访问风险较低的常用社交网站。

选择**包含信誉未知的站点**选项，可使具有未知信誉的 URL 包括在信誉匹配项中。新站点通常未评级，并且站点的信誉可能会由于其他原因而未知或无法确定。

使用信誉，您可以选择性地阻止要允许的某个类别内的某些站点。

i) 点击类别列表左侧 **URL** 列表旁边的 **+**。

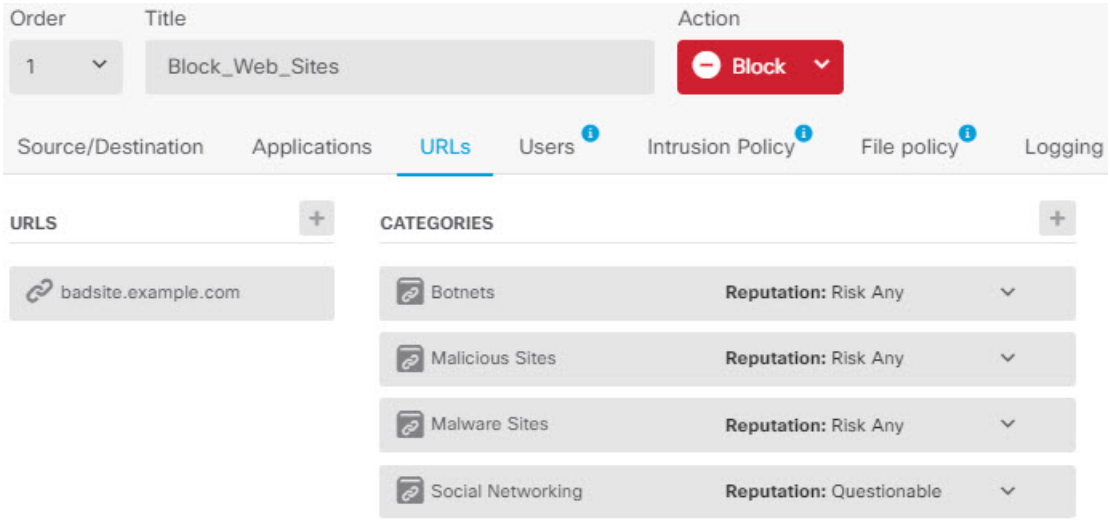
j) 在弹出对话框的底部，点击**创建新 URL** 链接。

k) 对于名称和 URL，请输入 **badsite.example.com**，然后点击**确定**以创建对象。

您可以为该对象指定与 URL 相同的名称，也可以为其指定不同的名称。对于 URL，请勿包含 URL 的协议部分，只添加服务器名称。

l) 选择该新对象，然后点击**确定 (OK)**。

在编辑策略时添加该新对象，即可方便地将该对象添加到列表中。新对象不会自动选中。



m) 点击**日志记录**选项卡，然后依次选择**选择日志操作** > **连接开始和结束时**。

只有启用日志记录才能将类别和信誉信息记入 Web 类别控制面板和连接事件。

n) 点击**确定**以保存该规则。

步骤 3 （可选。）设置 URL 过滤的首选项。

在启用 URL 许可证时，系统会自动启用对 Web 类别数据库的更新。系统每 30 分钟检查一次更新，不过数据通常每天更新一次。如果您由于某种原因不想更新，可以关闭这些更新。

另外，还可以选择将未分类的 URL 发送给思科进行分析。因此，如果安装的 URL 数据库没有进行站点分类，Cisco 云可能会进行分类。云返回类别和信誉，基于类别的规则随后可以正确应用至URL 请求。对因内存限制而安装较小URL 数据库的低端系统而言，选择此选项非常重要。您可以设置查找结果的生存时间：默认值为“从不”，这意味着永远不会刷新查找结果。

a) 点击**设备**。

b) 依次点击**系统设置** > **流量设置** > **URL 过滤首选项**。
c) 选择**针对未知 URL 查询 Cisco CSI**。
d) 选择合理的 **URL 生存时间**，例如 24 小时。
e) 点击**保存 (Save)**。

步骤 4 确认您的更改。

a) 点击网页右上角的**部署更改**图标。

b) 点击**立即部署**按钮。

您可以等待部署完成，也可以点击**确定**，稍后再检查任务列表或部署历史记录。

下一步做什么

此时，监控控制面板和事件应开始显示URL类别和信誉及被丢弃连接的相关信息。您可以评估此信息以确定您的 URL 过滤要丢弃这些不符合条件的站点，还是您需要针对特定类别降低信誉设置。

请考虑事先通知用户，您会基于网站的分类和信誉阻止对网站的访问。

如何控制应用的使用

Web 已成为企业交付应用（无论是基于浏览器的应用平台，还是使用 Web 协议传入和传出企业网络的富媒体应用）普遍使用的平台。

威胁防御通过检查连接确定使用的应用。这样即可写入针对应用的访问控制规则，而不只是针对特定的 TCP/UDP 端口。因此，即使使用相同的端口，也可以选择性地阻止或允许基于 Web 的应用。

虽然可以选择要允许或阻止的特定应用，但也可以基于类型、类别、标记、风险或业务相关性写入规则。例如，您可以创建一条访问控制规则，用于识别并阻止所有业务相关性较低的高风险应用。如果用户尝试使用这些应用中的任何一个，系统会阻止会话。

思科会通过系统和漏洞数据库 (VDB) 更新频繁更改并添加其他应用检测器。因此，阻止高风险应用的规则可自动应用到新应用中，而无需您手动更新规则。

在此使用案例中，我们将阻止属于**匿名程序/代理**类别的任何应用。

开始之前

此使用案例假定您已完成使用案例如何深入了解您的网络流量，第 6 页。该使用案例介绍了如何收集应用使用信息，您可以在“应用”控制面板中分析这些信息。了解实际使用的应用可帮助您基于应用设计有效的规则。另外，该使用案例还介绍了如何安排 VDB 更新，我们在此不再重复。请务必要定期更新 VDB，以便可正确识别应用。

过程

步骤 1 创建基于应用的访问控制规则。

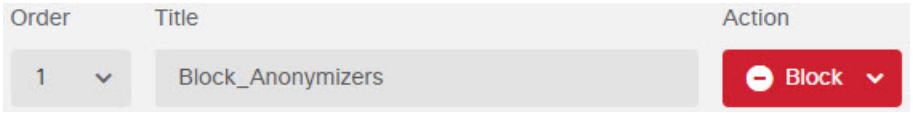
a) 在主菜单中点击**策略**。

确保系统显示**访问控制**策略。

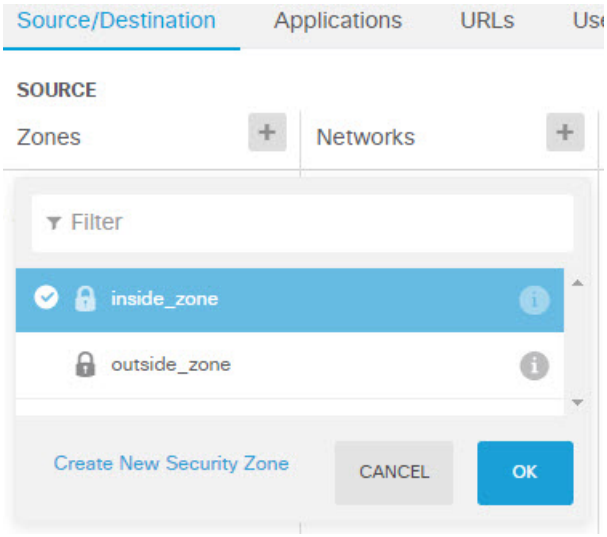
b) 点击 + 可添加新规则。

c) 配置顺序、标题和操作。

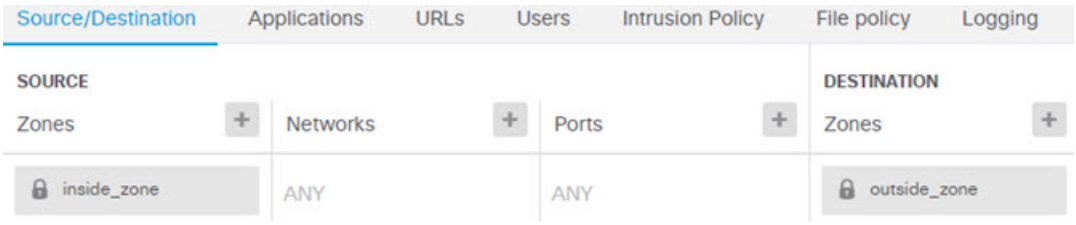
- **顺序** - 默认将新规则添加到访问控制策略的末尾。但是，您必须将此规则放在符合相同源/目的及其他条件的任何规则之前（上方），否则该规则将无法获得匹配（一个连接仅匹配一条规则，即该规则是连接在表中匹配的第一条规则）。对于该规则，我们将使用与初始设备配置期间创建的 Inside_Outside_Rule 相同的源/目的。您可能也已经创建了其他规则。为了最大限度地提高访问控制效率，最好是尽早设置特定规则，以确保快速决定允许还是丢弃某个连接。对于此示例，请选择 **1** 作为规则顺序。
- **标题** - 为该规则指定一个有意义的名称，例如 Block_Anonymizers。
- **操作** - 选择**阻止**。



d) 在**源/目的 (Source/Destination)** 选项卡上，点击 + 以打开**源 (Source)** > **区域 (Zones)**，然后选择 **inside_zone**，再在区域对话框中点击**确定 (OK)**。



e) 按照相同的方法，为**目的** > **区域**选择 **outside_zone**。



f) 点击**应用**选项卡。

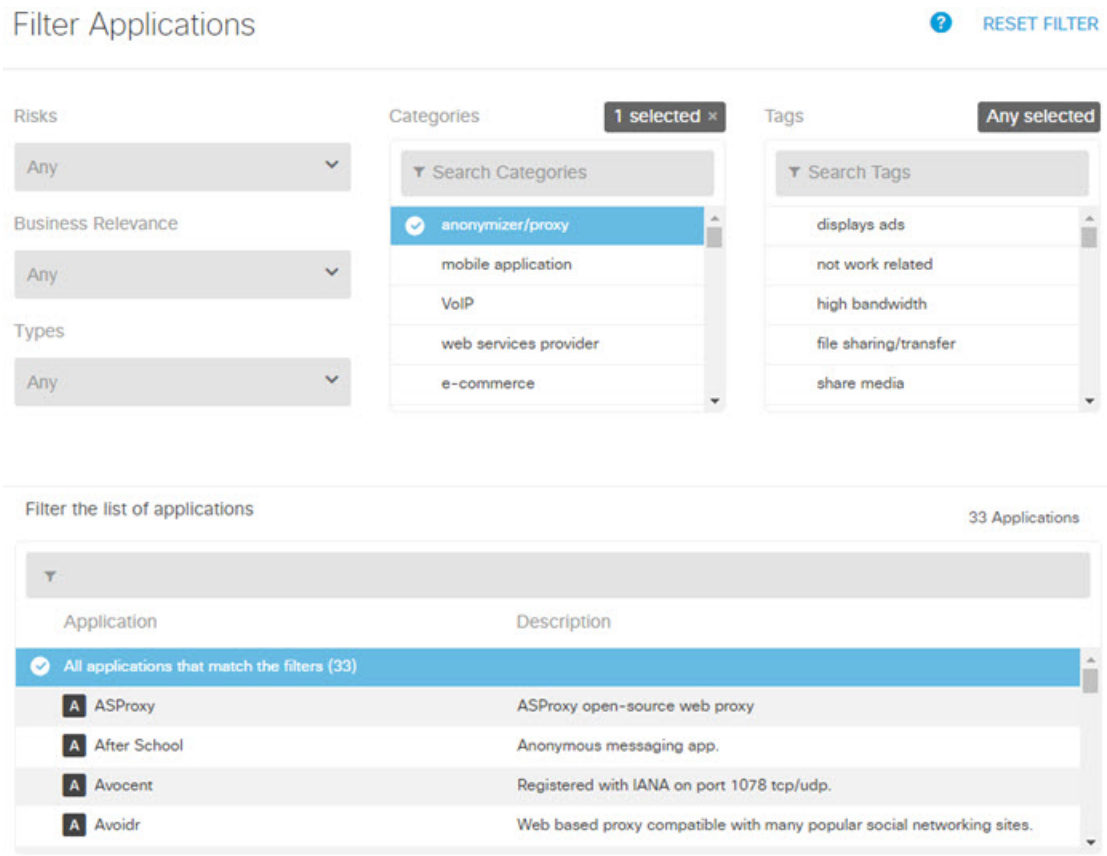
g) 针对**应用**点击 **+**，然后点击弹出对话框底部的**高级过滤器**链接。

虽然可以事先创建应用过滤器对象，再在此处从“应用过滤器”列表中选择它们，但也可以直接在访问控制规则中指定标准，再选择将该标准另存为过滤器对象。除非为单个应用写入规则，否则使用“高级过滤器”对话框查找应用和构建适当的标准更方便。

在选择标准时，对话框底部的“应用”列表将准确显示符合标准的应用。您要编写的规则将应用到这些应用中。

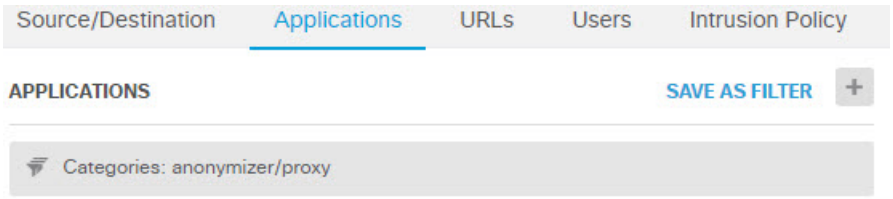
仔细查看此列表。例如，您可能会希望阻止风险极高的所有应用。但是，截至本文撰写之时，TFPT 被归为风险极高类别。而大多数组织不想阻止该应用。请花些时间测试各种过滤条件，以查看哪些应用符合您的选择。请注意，这些列表可能随着每次 VDB 更新而变化。

在本例中，从“类别”列表中选择“匿名程序/代理”。



h) 在“高级过滤器”对话框中点击 **添加 (Add)**。

“应用”选项卡中将添加并显示该过滤器。



i) 点击**日志记录**选项卡，然后依次选择**选择日志操作** > **连接开始和结束时**。

您必须启用日志记录选项卡才能获取与此规则阻止的任何连接相关的信息。

j) 点击**确定**以保存该规则。

步骤 2 确认您的更改。

a) 点击网页右上角的**部署更改**图标。

b) 点击**立即部署**按钮。

您可以等待部署完成，也可以点击**确定**，稍后再检查任务列表或部署历史记录。

步骤 3 点击**监控**并评估结果。

现在，您可能会在**网络概况**控制面板中看到“应用”构件中丢弃的连接。使用**所有/已拒绝/已允许**下拉选项可仅关注被丢弃的应用。

此外，还可以在**Web 应用**控制面板上查找应用的相关信息。**应用**控制面板显示与协议相关的结果。假定您启用了身份策略并要求身份验证，当有人尝试使用这些应用时，您应该能够将应用与尝试连接的用户相关联。

如何添加子网

如果您的设备有一个可用接口，则可以将其连接到交换机（或其他路由器）为其他子网提供服务。

添加子网的潜在原因很多。对于此使用案例，我们将处理以下典型场景。

- 子网是内部网络，使用专用网络 192.168.2.0/24。
- 该网络的接口使用静态地址 192.168.2.1。在本例中，网络使用的是物理接口。另一种选项是使用已连线的接口，并为新网络创建一个子接口。
- 设备将使用 DHCP 为网络中的工作站提供地址，使用的地址池为 192.168.2.2 - 192.168.2.254。
- 允许网络访问其他内部网络和外部网络。传至外部网络的流量将使用 NAT 获取公共地址。

注释 此示例假定未使用的接口不是网桥组的一部分。如果它当前是网桥组成员，则必须首先将其从网桥组中删除，然后再执行此步骤过程。

开始之前

将网络电缆物理连接到新子网的接口和交换机。

过程

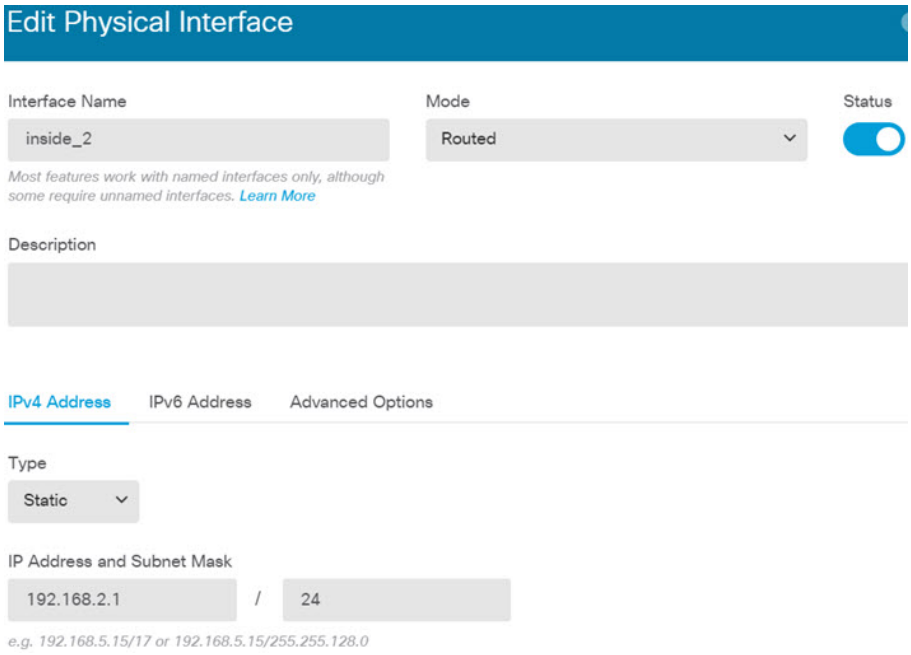
步骤 1 配置接口。

a) 点击**设备 (Device)**，点击**接口 (Interfaces)**摘要中的链接，然后点击接口类型以查看接口列表。

b) 将鼠标悬停在您连线的接口行右侧的**操作 (Actions)** 单元格上方，然后点击编辑图标 ( )。

c) 配置基本接口属性。

- **名称** - 接口的名称。在本例中为 **inside_2**。
- **模式** - 选择**路由**。
- **状态 (Status)** - 点击状态开关启用该接口。
- **IPv4 地址**选项卡 - 针对**类型**选择**静态**，然后输入 **192.168.2.1/24**。



d) 点击**保存 (Save)**。

接口列表将显示更新的接口状态和配置的 IP 地址。

步骤 2 针对该接口配置 DHCP 服务器。

a) 点击**设备**。

b) 点击**系统设置 (System Settings)** > **DHCP 服务器 (DHCP Server)**。

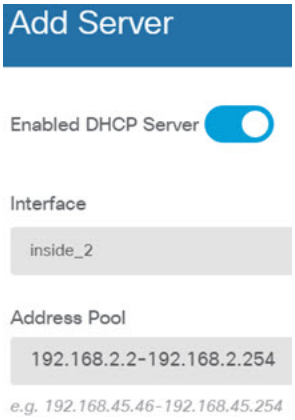
c) 点击 **DHCP 服务器 (DHCP Server)** 选项卡。

下表列出了所有现有 DHCP 服务器。如果使用默认配置，列表中包含内部接口的一个 DHCP 服务器。

d) 点击表格上方的 +。

e) 配置服务器属性。

- **启用 DHCP 服务器 (Enable DHCP Server)** - 点击此旋钮可启用该服务器。
- **接口** - 选择您提供 DHCP 服务所使用的接口。在本例中，选择 inside_2。
- **地址池** - 服务器可以为网络中设备提供的地址。输入 192.168.2.2-192.168.2.254。确保未包含网络地址 (.0)、接口地址 (.1) 或广播地址 (.255)。另外，如果网络中的任何设备需要使用静态地址，请从池中排除这些地址。池必须是一系列连续地址，所以请从该范围的开头或末尾选择静态地址。



f) 点击 **添加 (Add)**。

#	INTERFACE	ENABLED DHCP SERVER	ADDRESS POOL
1	inside	Enabled	192.168.1.5-192.168.1.254
2	inside_2	Enabled	192.168.2.2-192.168.2.254

步骤 3 将该接口添加到内部安全区。

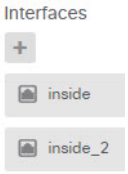
要在接口上编写策略，该接口必须属于安全区。您需要针对安全区编写策略。因此，您在区域中添加和删除接口时，会自动更改应用于接口的策略。

a) 在主菜单中点击**对象 (Objects)**。

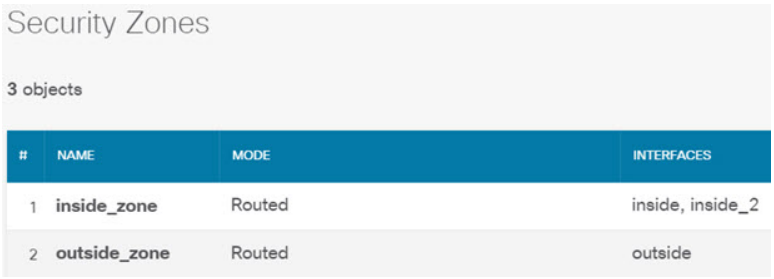
b) 从对象目录中选择**安全区**。

c) 将鼠标悬停在 **inside_zone** 对象行右侧的**操作 (Actions)** 单元格上方，然后点击编辑图标 ( )。

d) 点击**接口 (Interfaces)** 下的 +，选择 inside_2 接口，然后点击接口列表中的**确定 (OK)**。



e) 点击**保存 (Save)**。



步骤 4 创建一条允许在内部网络之间传输流量的访问控制规则。

不会自动允许任何接口之间的流量。必须创建访问控制规则，才能允许所需的流量。唯一例外情况是，允许访问控制规则默认操作中的流量。在本例中，我们假定您保留了设备安装向导配置的阻止默认操作。因此，您需要创建一条规则，以允许内部接口之间的流量。如果已经创建这样的规则，请跳过此步骤。

a) 在主菜单中点击**策略 (Policies)**。

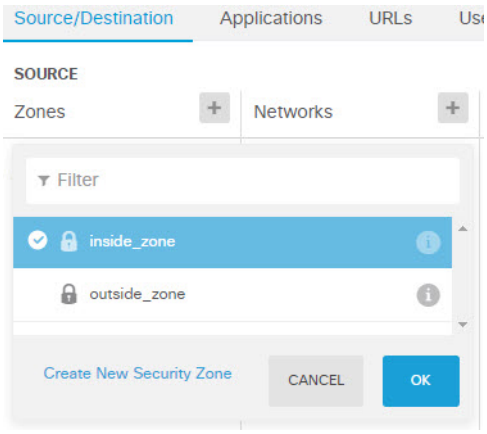
确保系统显示**访问控制**策略。

b) 点击 + 可添加新规则。

c) 配置顺序、标题和操作。

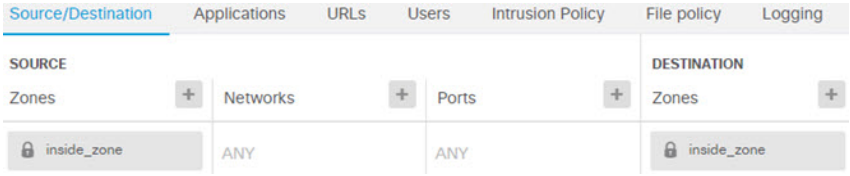
- **顺序**-默认将新规则添加到访问控制策略的末尾。但是，您必须将此规则放在符合相同源/目的及其他条件的任何规则之前（上方），否则该规则将无法获得匹配（一个连接仅匹配一条规则，即该规则是连接在表中匹配的第一条规则）。对于该规则，我们将使用唯一“源/目的”条件，所以可以将该规则添加到列表的末尾。
- **标题** - 为该规则指定一个有意义的名称，例如 Allow_Inside_Inside。
- **操作** - 选择**允许**。

d) 在**源/目的 (Source/Destination)** 选项卡上，点击 + 以打开**源 (Source)** > **区域 (Zones)**，然后选择 **inside_zone**，再在区域对话框中点击**确定 (OK)**。



e) 按照相同的方法，为**目的** > **区域**选择 **inside_zone**。

安全区必须至少包含两个接口，以便为源和目标选择同一区域。



f) （可选。）配置入侵和恶意软件检测。

虽然内部接口位于受信任区域，但用户通常会将笔记本电脑连接到网络。因此，用户可能不知道会将外部网络或 Wi-Fi 热点的威胁带入网络内部。因此，您可能希望扫描内部网络之间的流量中是否存在入侵和恶意软件。

请考虑执行以下操作。

- 点击**入侵策略 (Intrusion Policy)** 选项卡，启用入侵策略，并使用滑块选择“平衡安全和连接”(Balanced Security and Connectivity) 策略。
- 点击**文件策略 (File Policy)** 选项卡，然后选择“阻止所有恶意软件”(Block Malware All) 策略。

g) 点击**日志记录 (Logging)** 选项卡，然后依次选择**选择日志操作 (Select Log Action)** > **连接开始和结束时 (At Beginning and End of Connection)**。

只有启用日志记录，才能获得符合该规则的任何连接的相关信息。日志记录会向控制面板中添加统计信息，并会显示事件查看器中的事件。

h) 点击**确定 (OK)** 以保存该规则。

步骤 5 确认是否已为新子网定义所需的策略。

通过将该接口添加到 inside_zone 安全区，inside_zone 的任何现有策略将自动应用到新子网。但是，请花些时间来检查您的策略，确保未遗漏任何其他策略。

如果已完成初始配置，即可应用以下策略。

- **访问控制** - Inside_Outside_Rule 应允许新子网和外部网络之间的所有流量。如果您按照前面的使用案例执行了操作，该策略还会提供入侵和恶意软件检测。必须有一条规则允许新网络和外部网络之间的某些流量，否则用户将无法访问互联网或其他外部网络。
- **NAT** - InsideOutsideNATrule 适用于传至外部接口的任何接口，并会应用于接口 PAT。如果保留了此规则，则从新网络传至外部网络的流量会将 IP 地址转换为外部接口 IP 地址上的唯一端口。如果在传至外部接口时没有应用于所有接口或 inside_zone 接口的规则，则可能需要立即创建一条规则。
- **身份** - 没有默认的身份策略。但是，如果您按照前面的使用案例执行了操作，则可能已有需要对新网络进行身份验证的身份策略。如果没有适用的身份策略，但希望掌握新网络的用户信息，请立即创建一条策略。

步骤 6 确认您的更改。

a) 点击网页右上角的**部署更改**图标。

b) 点击**立即部署**按钮。

您可以等待部署完成，也可以点击**确定**，稍后再检查任务列表或部署历史记录。

下一步做什么

确认新子网中的工作站是否使用 DHCP 获取 IP 地址，以及它们是否可访问其他内部网络和外部网络。使用监控控制面板和事件查看器评估网络使用情况。

如何被动监控网络上的流量

威胁防御设备通常部署为主动防火墙和 IPS（入侵防御系统）安全设备。设备的核心功能是提供主动网络保护，丢弃不需要的连接和威胁。

但是，您还可以在被动模式下部署系统，使设备只分析受监控交换机端口上的流量。此模式主要用于演示或测试目的，以便您可以在将设备部署为主动防火墙之前熟悉设备。使用被动部署，您可以监控网络上的各种威胁、用户浏览的 URL 类别，等等。

虽然被动模式通常用于演示或测试目的，但也可以在生产环境中使用，前提是它可提供所需的服务，例如 IDS（入侵检测系统，而无需防御）。您可以搭配使用被动接口和主动防火墙路由接口，以提供组织所需的确切服务组合。

以下过程介绍如何被动部署系统来分析通过有限数量的交换机端口传递的流量。

注释 本示例适用于硬件 威胁防御设备。您还可以对 threat defense virtual 使用被动模式，但网络设置是不同的。有关详细信息，请参阅为 Threat Defense Virtual 被动接口配置 VLAN。否则，此程序也适用 threat defense virtual。

开始之前

此过程假定您已连接内部和外部接口，并完成初始设备设置向导。即使在被动部署中，您也需要连接到互联网下载系统数据库更新。您还需要能够连接到管理接口以打开 设备管理器（可通过到内部或管理端口的直接连接实现）。

该示例还假设您已在**策略 (Policies)** > **入侵 (Intrusion)** 页面上为入侵策略启用系统日志。

过程

步骤 1 将交换机端口配置为 SPAN（交换端口分析器）端口，并为源接口配置监控会话。

以下示例为 Cisco Nexus 5000 系列交换机上的两个源接口设置 SPAN 端口和监控会话。如果您使用不同类型的交换机，所需的命令可能会有所不同。

```
switch(config)# interface Ethernet1/48
switch(config-if)# switchport monitor
switch(config-if)# exit
switch(config)# monitor session 1
switch(config-monitor)# source interface ethernet 1/7
switch(config-monitor)# source interface ethernet 1/8
switch(config-monitor)# destination interface ethernet 1/48
switch(config-monitor)# no shut
```

验证：

```
switch# show monitor session 1 brief
   session 1
---------------
type              : local
state             : up
source intf       :
    rx            : Eth1/7        Eth1/8
    tx            : Eth1/7        Eth1/8
    both          : Eth1/7        Eth1/8
source VSANs      :
destination ports : Eth1/48

Legend: f = forwarding enabled, l = learning enabled
```

步骤 2 将 威胁防御接口连接到交换机的 SPAN 端口。

最好选择 威胁防御设备上当前未使用的端口。根据示例交换机配置，将电缆连接到交换机的以太网 1/48。这是监控会话的目标接口。

步骤 3 将 威胁防御接口配置为被动模式。

a) 点击**设备**，然后点击**接口**摘要中的链接，再点击**接口**或 **EtherChannel**。

b) 点击要编辑的物理接口或 EtherChannel 的编辑图标 ( )。

选择当前未使用的接口。如果您要将使用中的接口转换为被动接口，需要先从任何安全区中删除该接口，并删除使用该接口的所有其他配置。

c) 将**状态**滑块设置为已启用设置 ( )。

d) 进行以下配置：

- **接口名称** - 接口名称，最多 48 个字符。字母字符必须为小写。例如，**monitor**。
- **模式** - 选择**被动**。

e) 点击**确定 (OK)**。

步骤 4 为接口创建被动安全区。

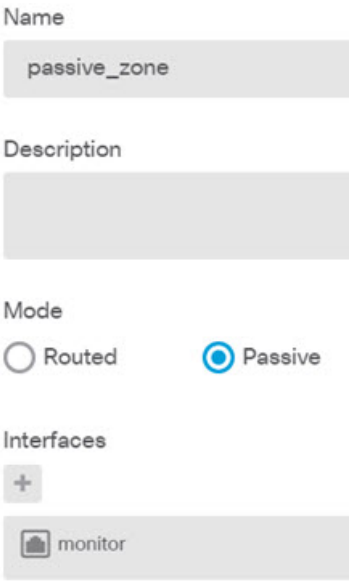
a) 选择**对象**，然后从目录中选择**安全区**。

b) 点击 + 按钮。

c) 输入对象的**名称**和说明（后者为可选项）。例如，**passive_zone**。

d) 对于**模式**，请选择**被动**。

e) 点击 +，然后选择被动接口。



f) 点击**确定 (OK)**。

步骤 5 为被动安全区配置一个或多个访问控制规则。

创建的规则数量和类型取决于您想要收集的信息。例如，如果您要将系统配置为 IDS（入侵检测系统），需要至少一个分配有入侵策略的允许规则。如果您想要收集URL类别数据，需要至少一个具有 URL 类别规范的规则。

您可以创建阻止规则，以确定系统本可阻止主动路由接口上的哪些连接。这些连接实际上并没有被阻止，因为接口是被动接口，但您将清楚地看到系统会如何整理网络上的流量。

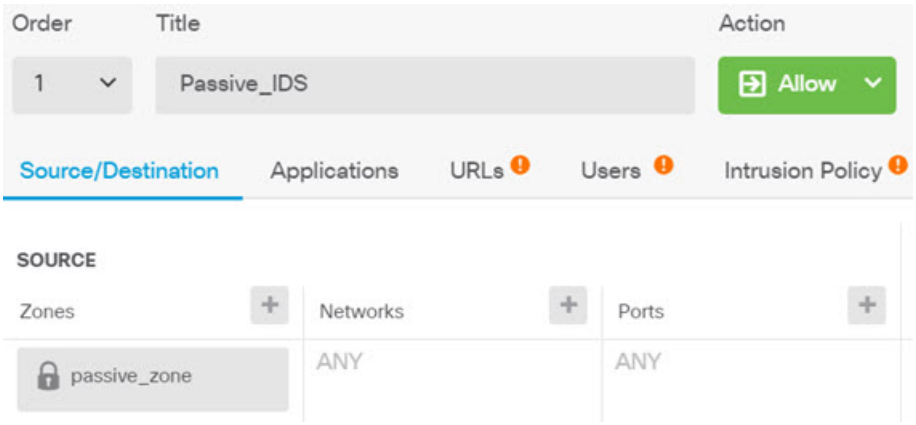
以下使用案例介绍访问控制规则的主要用途。这些规则也适用于被动接口。只需选择被动安全区作为所创建规则的源区域。

- 如何阻止威胁，第 13 页
- 如何阻止恶意软件，第 17 页
- 如何实施可接受使用策略（URL 过滤），第 20 页
- 如何控制应用的使用，第 25 页

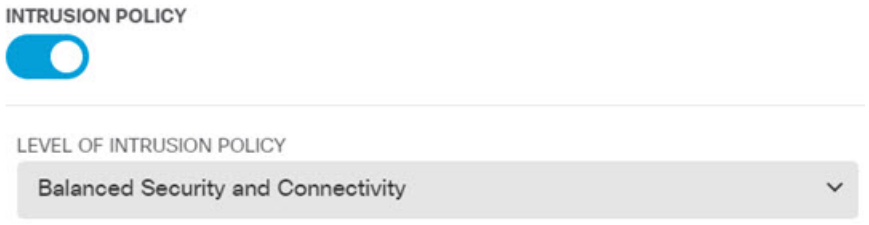
以下过程创建两条允许规则来应用入侵策略并收集 URL 类别数据。

a) 依次选择**策略** > **访问控制**。
b) 点击 + 添加允许所有流量、但应用入侵策略的规则。
c) 选择**1**作为规则顺序。此规则比默认规则更具体，但并不与之重叠。如果您已有自定义规则，请为这些规则选择适当的位置，以便传递到被动接口的流量不匹配这些规则。
d) 输入规则的名称，例如 **Passive_IDS**。
e) 对**操作**选择**允许**。
f) 在**源/目标**选项卡上，选择**源** > **区域**下的被动区。不要配置选项卡上的任何其他选项。

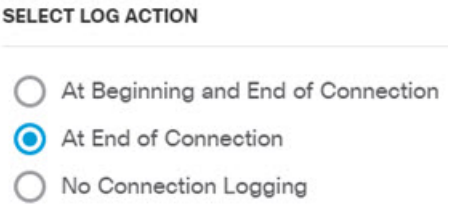
在评估模式运行时，此阶段的规则应为：



g) 点击**入侵策略**选项卡，将滑块滑动至**打开**，并选择**平衡安全和连接**入侵策略（建议将此策略应用于大多数网络）。



h) 点击**日志记录**选项卡，并选择**在连接结束时**作为日志记录选项。



i) 点击**确定 (OK)**。

j) 点击 **+** 添加要求系统执行深度检测以确定所有 HTTP 请求的 URL 和类别的规则。

通过此规则，您可以在控制面板中查看 URL 类别信息。为节省处理时间并提高性能，系统仅在至少有一个指定 URL 类别条件的访问控制规则时确定 URL 类别。

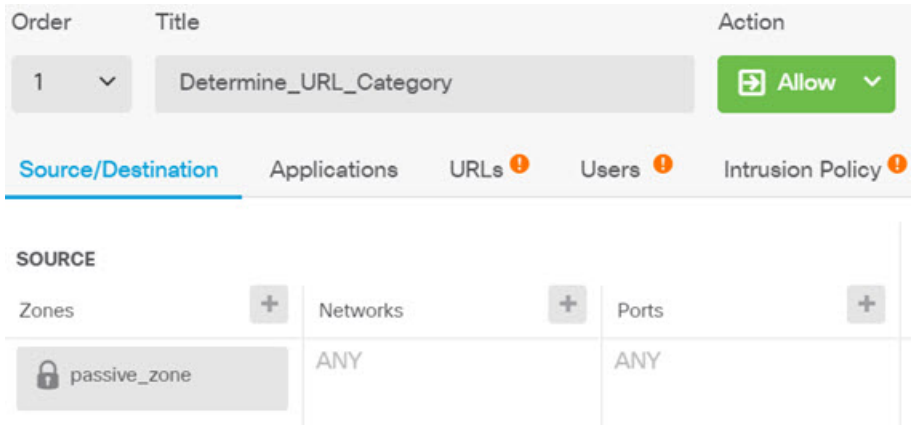
k) 选择**1**作为规则顺序。这样可将规则放置在上一个规则(Passive_IDS)上方。如果您将其放置在该规则（适用于所有流量）后面，流量将永远不会匹配您现在创建的规则。

l) 输入规则的名称，例如 **Determine_URL_Category**。

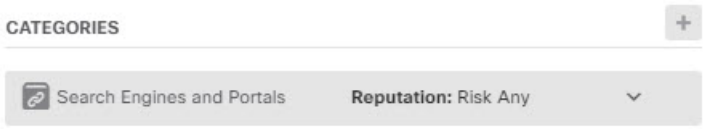
m) 对**操作**选择**允许**。

或者，您可以选择**阻止**。上述任一操作都可以实现此规则的目的。

n) 在**源/目标**选项卡上，选择**源** > **区域**下的被动区。不要配置选项卡上的任何其他选项。



o) 点击 **URL** 选项卡，点击**类别**标题旁边的 **+**，然后选择任何类别。例如，**搜索引擎和门户**。或者，可以选择信誉级别，或保留默认值“任何”。



p) 点击**入侵策略**选项卡，将滑块滑动至**打开**，并选择您为第一个规则选择的同一入侵策略。

q) 点击**日志记录**选项卡，并选择**在连接结束时**作为日志记录选项。

但是，如果您选择**阻止**操作，请选择**在连接开始和结束时**。由于被阻止的连接不会自行终止，只能在连接开始时获取日志信息。

r) 点击**确定 (OK)**。

步骤 6 （可选。）配置其他安全策略。

您还可以配置以下安全策略，了解它们对流量的影响：

- **身份** - 收集用户信息。您可以在身份策略中配置规则，以确保识别与源 IP 地址关联的用户。为被动接口实施身份策略的过程与为路由接口实施身份策略的过程相同。请按照如何深入了解您的网络流量，第 6 页所述的使用案例操作。
- **安全智能** - 阻止已知不良 IP 地址和 URL。有关详细信息，请参阅如何阻止威胁，第 13 页。

注释 被动接口上的所有加密流量均划分为无法解密类别，因此 SSL 解密规则无效，不会应用于被动接口。

步骤 7 确认您的更改。

a) 点击网页右上角的**部署更改**图标。

b) 点击**立即部署**按钮。

您可以等待部署完成，也可以点击**确定**，稍后再检查任务列表或部署历史记录。

步骤 8 使用监控控制面板分析来自整个网络的流量和威胁类型。如果您确定要让 威胁防御设备主动丢弃不需要的连接，请重新部署设备，以便您可以配置用于为监控网络提供防火墙保护的主动路由接口。

更多示例

除了使用案例一章中的示例之外，某些解释特定服务的章节中还包括示例配置。您可能对下面的示例感兴趣。

访问控制

- 如何使用 TrustSec 安全组标记控制网络访问

网络地址转换 (NAT)

IPv4 地址的 NAT

- 提供对内部 Web 服务器的访问权限（静态自动 NAT）
- FTP、HTTP 和 SMTP 的单个地址（具有端口转换的静态自动 NAT）
- 转换因目标而异（动态手动 PAT）
- 转换因目标地址和端口而异（动态手动 PAT）
- DNS 回复修改、外部接口上的 DNS 服务器
- DNS 回复修改、主机网络上的 DNS 服务器
- 使站点间 VPN 流量豁免 NAT

IPv6 地址的 NAT

- NAT64/46 示例：内部 IPv6 网络与外部 IPv4 互联网
- NAT64/46 示例：包含外部 IPv4 互联网和 DNS 转换的内部 IPv6 网络
- NAT66 示例：网络间的静态转换
- NAT66 示例：简单 IPv6 接口 PAT
- DNS 64 回复修改

远程访问虚拟专用网络 (RA VPN)

- 如何实施 RADIUS 授权更改
- 如何使用 Duo LDAP 配置双因素身份验证
- 如何在外部接口上为远程访问 VPN 用户提供互联网访问权限（发夹方法）
- 如何通过远程访问 VPN 使用外部网络上的目录服务器
- 如何通过组控制 RA VPN 访问
- 如何对不同虚拟路由器中的内部网络进行 RA VPN 访问
- 如何自定义 AnyConnect 客户端 图标和徽标

站点间虚拟专用网络 (VPN)

- 使站点间 VPN 流量豁免 NAT
- 如何在外部接口上为外部站点间 VPN 用户提供互联网访问（发夹方法）
- 如何通过站点间 VPN 保护来自多个虚拟路由器的网络流量

SSL/TLS 解密

- 示例：从网络阻止较旧的 SSL/TLS 版本

FlexConfig 策略

- 如何启用和禁用默认全局检测
- 如何撤消 FlexConfig 更改
- 如何启用唯一流量类检测

虚拟路由

- 如何提供对包含重叠地址空间的多个虚拟路由器的互联网访问权限
- 如何通过多个虚拟路由器路由到远程服务器
- 如何对不同虚拟路由器中的内部网络进行 RA VPN 访问
- 如何通过站点间 VPN 保护来自多个虚拟路由器的网络流量

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。