BGP

本节介绍如何配置 威胁防御，以使用边界网关协议 (BGP) 来路由数据、执行身份验证以及重新分发路由信息。

关于 BGP

BGP 是一种外部和内部自主系统路由协议。自治系统是一个或一组接受共同管理并采用共同路由策略的网络。BGP 用于交换互联网的路由信息，并且是互联网运营商 (ISP) 之间所使用的协议。

路由表更改

在 BGP 邻居之间首次建立 TCP 连接时，BGP 邻居会交换完整路由信息。当检测到对路由表所做的更改时，BGP 路由器仅会向其邻居发送已更改的路由。BGP 路由器不会发送定期路由更新，并且 BGP 路由更新仅对到达目标网络的最佳路径进行通告。

注释 系统通过扫描完整的 AS 路径（在 AS_PATH 属性中指定）并检查本地系统的 AS 编号是否未出现在 AS 路径中来完成 AS 环路检测。默认情况下，EBGP 将获知的路由通告给同一对等体，以防止在执行环路检查时 ASA 上出现额外的 CPU 周期，并避免现有传出更新任务中出现延迟。

当存在多个到达某个特定目标的路由时，通过BGP获悉的路由的属性可用于确定到达该目标的最佳路径。这些属性称为 BGP 属性，可在路由选择过程中使用：

- 权重 - 这是思科定义的路由器本地属性。权重属性不会向相邻路由器进行通告。如果路由器获悉有多个到达同一目标的路由，则首选权重最高的路由。

- 本地首选项 - 本地首选项属性用于从本地 AS 中选择出口点。与权重属性不同，本地优先属性在整个本地 AS 中传播。如果有多个来自 AS 的出口点，则使用具有最高本地优先属性的出口点作为特定路由的出口点。
- 多出口鉴别器 - 多出口鉴别器 (MED) 或度量属性可用作对外部 AS 关于进入正在通告此度量的 AS 的首选路径的建议。因为正在接收 MED 的外部 AS 也可能正在使用其他 BGP 属性选择路由，所以它仅作为建议。首选 MED 指标较低的路由。
- 源 - 源属性指示 BGP 获悉某个特定路由的方式。源属性可能具有下面三个可能值中的一个，用于路由选择。
  - IGP - 此路由是源 AS 的内部路由。当使用网络路由器配置命令向 BGP 注入路由时，会设置该值。
  - EGP - 此路由通过外部边界网关协议 (EBGP) 获悉。
  - 不完整 - 路由源未知或通过其他方式获悉。当路由重新分发到 BGP 时，可能会出现源不完整的情况。
- AS_path - 当路由通告通过一个自治系统时，会在按顺序排列的 AS 编号列表中添加 AS 编号，标识路由通告已经穿越的 AS。仅将拥有最短 AS_path 列表的路由添加至 IP 路由表中。
- 下一跳 - EBGP 下一跳属性是用于到达通告路由器的 IP 地址。对于 EBGP 对等体，下一跳地址是对等体之间的连接 IP 地址。对于 IBGP，EBGP 下一跳地址会携带至本地 AS 中。

  在将 VPN 通告的路由重新分发到 iBGP 对等体时，请使用 **next-hop-self** 命令，以确保使用正确的下一跳 IP 重新分发路由。
- 社区 - 社区属性提供一种目标（称为社区）的分组方式，可对社区应用路由决策（例如，接受、首选项和重新分发）。路由映射用于设置社区属性。预定义的社区属性如下：
  - no-export - 不向 EBGP 对等体通告相应路由。
  - no-advertise - 不向任何对等体进行通告。
  - internet - 此路由向互联网社区进行通告；网络中的所有路由器均属于此类型。

何时使用 BGP

客户网络（例如，大学和公司）通常使用 OSPF 等内部网关协议 (IGP) 在其网络内交换路由信息。客户连接到 ISP，然后 ISP 使用 BGP 交换客户路由和 ISP 路由。在自治系统 (AS) 之间使用 BGP 时，该协议称为外部 BGP (EBGP)。如果运营商使用 BGP 在 AS 内交换路由，则此协议称为内部 BGP (IBGP)。

BGP 也可用于通过 IPv6 网络承载有关 IPv6 前缀的路由信息。

BGP 路径选择

BGP 可能会从不同来源接收同一路由的多个通告。BGP 仅选择一个路径作为最佳路径。选择此路径后，BGP 将选定的路径放在 IP 路由表中，并将此路径传播给其邻居。BGP 按显示的顺序使用以下条件为目标选择路径：

- 如果路径指定的下一跳不可访问，则放弃更新。
- 首选权重最高的路径。
- 如果权重相同，则首选具有最高本地优先值的路径。
- 如果本地优先值相同，则首选 BGP 在此路由器上运行所发起的路径。
- 如果未发起路由，则首选 AS_path 最短的路由。
- 如果所有路径的 AS_path 长度相同，则首选源类型最低的路径（其中，IGP 低于 EGP，EGP 低于不完整路径）。
- 如果源代码相同，则首选 MED 属性最低的路径。
- 如果路由的 MED 相同，则首选外部路径而非内部路径。
- 如果路径依然相同，则首选穿过最近的 IGP 邻居的路径。
- 在 BGP 多路径，第 3 页的路由表中确定是否需要安装多个路径。
- 如果两个路径都是外部路径，则首选第一个接收的路径（最早的路径）。
- 首选具有由 BGP 路由器 ID 指定的最低 IP 地址的路径。
- 如果多个路径的发起方或路由器 ID 相同，则首选集群列表长度最短的路径。
- 首选来自最低邻居地址的路径。

BGP 多路径

BGP 多路径允许将多个等成本 BGP 路径的 IP 路由表安装到相同的目标前缀。然后，跨安装的所有路径共享到目标前缀的流量。

这些路径连同最佳路径一起安装在表中，以实现负载共享。BGP 多路径不影响最佳路径选择。例如，路由器仍会根据算法将其中一个路径指定为最佳路径，并将此最佳路径通知其 BGP 对等体。

要想成为多路径的候选对象，指向同一目标的路径需要具有与最佳路径特性相同的以下特性：

- 重量
- 本地优先级
- AS-PATH 长度
- 源代码
- 多出口鉴别器 (MED)

- 以下选项之一：
  - 相邻的 AS 或子 AS（在添加 BGP 多路径之前）
  - AS 路径（在添加 BGP 多路径之后）

某些 BGP 多路径功能对多路径候选对象有一些额外要求：

- 此路径应从外部或联盟外部邻居 (eBGP) 获悉。
- BGP 下一跳的 IGP 指标应等于最佳路径 IGP 指标。

这些是内部 BGP (iBGP) 多路径候选对象的额外要求：

- 此路径应从内部邻居 (eBGP) 获悉。
- BGP 下一跳的 IGP 指标应等于最佳路径 IGP 指标，除非路由器是面向非等成本 iBGP 多路径配置的。

BGP 可将最多 *n* 个最近收到的路径从多路候选对象插入到 IP 路由表中，其中 *n* 是要安装到路由表的路由数，如配置 BGP 多路径时所指定的那样。禁用多路径时的默认值为 1。

对于非等成本的负载平衡，您还可以使用 BGP 链路带宽。

注释 等效的下一自跳将在从 eBGP 中选择的最佳路径上执行，并且是在最佳路径转发至内部对等体之前执行。

BGP 的要求和必备条件

型号支持

威胁防御

Threat Defense Virtual

支持的域

任意

用户角色

管理员

网络管理员

BGP 准则

防火墙模式准则

不支持透明防火墙模式。仅在路由模式下支持 BGP。

IPv6 准则

支持 IPv6。

其他准则

- 系统不会在 CP 路由表中为通过 PPPoE 接收的 IP 地址添加路由条目。BGP 始终查看用于发起 TCP 会话的 CP 路由表，因此 BGP 不会形成 TCP 会话。

  因此，不支持通过 PPPoE 发送 BGP。

- 要避免在路由更新大于链路上的最小 MTU 时丢弃由于路由更新而导致的邻接摆动，请确保在链路两端的接口上配置相同的 MTU。
- 成员设备的 BGP 表未与控制设备表同步。仅其路由表与控制单元路由表同步。
- 使用静态或动态 VTI 接口配置基于路由的站点间 VPN 时，如果使用 BGP 作为路由协议，请确保 TTL 跳的值大于 1。

配置 BGP

要配置 BGP，请参阅下列主题：

过程

步骤 1 配置 BGP 基本设置， 第 6 页
步骤 2 配置 BGP 常规设置， 第 8 页
步骤 3 配置 BGP 邻居设置， 第 9 页
步骤 4 配置 BGP 汇聚地址设置， 第 13 页
步骤 5 配置 BGPv4 过滤设置， 第 13 页

注释 “过滤”部分仅适用于 IPv4 设置

步骤 6 配置 BGP 网络设置， 第 14 页
步骤 7 配置 BGP 重新分发设置， 第 15 页
步骤 8 配置 BGP 路由注入设置， 第 15 页

步骤 9 配置 BGP 路由导入/导出设置，第 16 页

配置 BGP 基本设置

可为 BGP 设置很多基本设置。

对于使用虚拟路由的设备，必须在 **BGP** 页面的**常规设置 (General Settings)** 下配置此部分中描述的基本设置。有关详细信息，请参阅管理中心 Web 界面 - 路由页面修改。

过程

步骤 1 依次选择**设备(Devices)** > **设备管理(Device Management)**，并且编辑 威胁防御 设备。

步骤 2 选择**路由**。

步骤 3 （对于虚拟路由器感知设备）在**常规设置**下，点击 **BGP**。

步骤 4 选中**启用 BGP (Enable BGP)** 复选框以启用 BGP 路由进程。

步骤 5 在 **AS 编号**字段中，输入 BGP 进程的自治系统 (AS) 编号。AS 编号内部包含多个自主编号。AS 编号范围为从 1 至 4294967295，或从 1.0 至 65535.65535。AS 编号是一个唯一分配的值，用于在互联网上标识各个网络。

步骤 6 在**路由器 ID** 下拉列表中，选择“自动”或“手动”。如果选择了“自动”，则会将 威胁防御设备上的最高级别的 IP 地址用作路由器 ID。

步骤 7 要使用固定路由器 ID，请选择“手动”，然后在 **IP 地址** 字段中输入一个 IPv4 地址。默认值是自动。对于虚拟路由器感知设备，您可以覆盖**虚拟路由器 (Virtual Routers)** > **BGP** 页面中的路由器 ID 设置。

步骤 8 （可选）从**常规**开始，编辑各项 BGP 设置。这些设置的默认值适用于大多数情况，但也可以调整它们，以适应您的网络的需求。点击 **编辑**（ ） 以编辑组中的设置：

a) 为下一跳验证输入 BGP 路由器的**扫描间隔**。有效值范围为 5 至 60 秒。默认值为 60。

b) 输入 **AS_PATH 属性中 AS 编号的数量**。AS_PATH 属性是形成供数据包传播的定向路由的源和目标路由器之间的中间 AS 编号序列。有效值介于 1 与 254 之间。默认值为“无”。

c) 选中**记录邻居更改**复选框，启用对 BGP 邻居更改（向上或向下）和重置的日志记录。这有助于解决网络连接问题并衡量网络稳定性。默认情况下，此选项已启用。

d) 选中**使用 TCP 路径 MTU 发现**复选框，使用路径 MTU 确定方法确定两个 IP 主机之间网络路径上的最大传输单位 (MTU) 大小。这可以避免 IP 分片。默认情况下，此选项已启用。

e) 选中**在故障转移时重置会话**复选框，在出现链路故障后立即重置外部 BGP 会话。默认情况下，此选项已启用。

f) 选中**执行第一个 AS 作为对等体的 AS 用于 EBGP 路由**复选框，放弃从未在 AS_PATH 属性中将其 AS 编号列为首个分段的外部 BGP 对等体接收的传入更新。这可以防止错误配置或未经授权的对等体通过通告路由（如同其源自另一个自治系统）来错误定向流量。默认情况下，此选项已启用。

g) 选中**将点分表示法用于 AS 编号**复选框，将完整的二进制 4 字节 AS 编号拆分为两个单词，每个单词 16 位，以点分隔。0-65553 的 AS 编号以十进制数字表示，大于 65535 的 AS 编号使用点分表示法来表示。默认情况下将禁用此复选框。

h) 点击**确定**。

步骤 9 （可选）编辑**最佳路径选择**部分：

a) 为 **默认本地首选项** 输入一个介于 0 与 4294967295 之间的值。默认值为 100。值越大，表示优先级越高。此首选项会发送到本地自治系统中的所有路由器和接入服务器。

b) 选中**允许比较来自不同邻居的MED**复选框，允许比较来自不同自治系统中不同邻居的路径的多出口鉴别器 (MED)。默认情况下将禁用此复选框。

c) 选中**比较相同 EBGP 路径的路由器 ID** 复选框，在最佳路径选择过程中，比较从外部 BGP 对等体接收的类似路径，并将最佳路径切换到路由器 ID 最低的路由。默认情况下将禁用此复选框。

d) 选中**在邻居 AS 通告的路径之间选择最佳 MED 路径**复选框，启用从联盟对等体获悉的路径之间的MED比较。仅当路径中没有外部自治系统时，才会比较MED。默认情况下将禁用此复选框。

e) 选中**将缺失 MED 的路径视为最不推荐的路径**复选框，将缺失 MED 的属性视为具有无穷值，从而使此路径成为最不需要使用的路径；因此，缺失 MED 的路径最不优先考虑。默认情况下将禁用此复选框。

f) 点击**确定**。

步骤 10 （可选）编辑**邻居计时器**部分：

a) 在**保持连接时间间隔 (Keep alive interval)** 字段中，输入 BGP 邻居在不发送保持连接消息后保持活动状态的时间间隔。在此 keepalive 时间间隔结束时，如果未发送消息，则声明 BGP 对等体处于失效状态。默认值为 60 秒。

b) 在**保持时间**字段中，输入在发起和配置 BGP 连接期间 BGP 邻居保持活动状态的时间间隔。默认值为 180 秒。指定一个从 0 至 65535 的值。

c) （可选）在**最小保持时间**字段中，输入在发起和配置 BGP 连接期间 BGP 邻居保持活动状态的最小时间间隔。指定一个从 3 至 65535 的值。

注释 保持时间小于 20 秒会增加对等体振荡的可能性。

d) 点击**确定**。

步骤 11 在**下一跃点**部分中，选择地选中**启用地址跟踪**复选框，以启用BGP下一跃点地址跟踪，并输入检查路由表中所安装的更新后下一跃点路由的**延迟间隔**。点击**确定**。

注释 **下一跃点**部分仅适用于 IPv4 设置。

步骤 12 （可选）编辑**无中断重启**部分：

注释 仅当威胁防御设备处于故障转移或跨集群模式下时，此部分才可用。此操作已经完成，以便在处于故障转移设置中的某一设备发生故障时，流量中的数据包不会被丢弃。

a) 选中 **启用无中断重启** 复选框，使 威胁防御 对等体能在状态切换后避免路由抖动。

b) 在**重启时间**字段中，指定在收到BGP开放消息之前，威胁防御对等体删除过时路由的持续时间。默认值为 120 秒。有效值介于 1 至 3600 秒之间。

c) 在 **过时路径时间** 字段中，输入 威胁防御 在从重启 威胁防御 收到记录终止 (EOR) 消息之后，删除过时路由之前等待的持续时间。默认值为 360 秒。有效值介于 1 至 3600 秒之间。

d) 点击**确定 (OK)**。

步骤 13 点击**保存 (Save)**。

步骤 14 要查看 BGP 基本设置，请从虚拟路由器下拉列表中选择所需的路由器，然后点击 **BGP**。

此页面显示在**设置 (Settings)** 页面中配置的基本设置。您可以在此页面上编辑路由器 ID 设置。

步骤 15 要编辑路由器ID设置，请修改 **IP 地址**字段中的 IP 地址。修改后的值会覆盖在 **BGP** 页面中**常规设置 (General Settings)** 下配置的路由器 ID 设置。

配置 BGP 常规设置

配置路由映射、管理路由距离、同步、下一跃点和数据包转发。在大多数情况下，这些设置的默认值都是适当的，但您可以进行调整以适应网络的需要。

过程

步骤 1 在**设备管理 (Device Management)** 页面中，点击**路由 (Routing)**。

步骤 2 （对于虚拟路由器感知设备）在虚拟路由器下拉列表中，选择要为其配置 BGP 的虚拟路由器。

步骤 3 选择 **BGP** > **IPv4**或 **IPv6**。

步骤 4 点击 **General**。

步骤 5 在**常规**选项卡中，更新以下部分：

a) 在**设置 (Settings)** 部分中，输入或选择**路由映射 (Route Map)** 对象，然后点击**确定 (OK)**。

注释 **路由映射**字段仅适用于 IPv4 设置

b) 在 **管理路由距离** 部分，根据需要更新以下内容，然后点击 **确定**：

- **外部** - 输入外部 BGP 路由的管理距离。从外部自治系统获悉的路由是外部路由。此参数值的范围为 1 至 255。默认值为 20。
- **内部** - 输入内部 BGP 路由的管理距离。从本地自治系统中的对等体获悉的路由是内部路由。此参数值的范围为 1 至 255。默认值为 200。
- **本地** - 输入本地 BGP 路由的管理距离。本地路由是指通过网络路由器显示命令列出的网络，通常作为正在从其他进程重新分发的路由器或网络的后门。此参数值的范围为 1 至 255。默认值为 200。

c) 在 **路由和同步** 部分中，根据需要更新以下内容，然后点击 **确定**：

- （可选） **生成默认路由 (Generate default routes)** - 选择此选项的复选框以配置默认信息来源。
- （可选） **汇总子网路由至网络级路由 (Summarize subnet routes into network-level routes)** - 选中该复选框，以将子网路由配置为自动汇总到网络级路由中。此复选框仅适用于 IPv4 设置。
- （可选） **通告非活动路由 (Advertise inactive routes)** - 选中该复选框，以通告未装载至路由信息库 (RIB) 中的路由。

- （可选） **在 BGP 和 IGP 系统之间同步 (Synchronise between BGP and IGP system)** - 选择该复选框，以启用 BGP 和内部网关协议 (IGP) 系统之间的同步。通常，BGP 发言方不会向外部邻居通告路由，除非路由是本地路由或存在于IGP中。使用此功能，自治主系统中的路由器和接入服务器可在 BGP 将某个路由分配给其他自治系统之前获得该路由。
- （可选） **将 iBGP 重新分发到 IGP 中 (Redistribute IBGP into IGP)** - 选中该复选框，以将 iBGP 配置为重新分发到内部网关协议 (IGP) 中，例如 OSPF。

d) 在**在多个路径上转发数据包**部分中，根据需要更新以下内容，并点击**确定**：

- （可选）**路径数 (Number of Paths)** - 输入可以安装在路由表中的边界网关协议路由的最大数量。值的范围是从 1 到 8。默认值为 1。
- （可选）**IBGP 路径数 (IBGP Number of Paths)** - 输入可以安装在路由表中的并行内部边界网关协议 (iBGP) 路由的最大数目。值的范围是从 1 到 8。默认值为 1。

步骤 6 点击**保存 (Save)**。

配置 BGP 邻居设置

在交换更新之前，BGP路由器必须与其每个对等体连接。这些对等体称为BGP邻居。使用“邻居”可以定义 BGP IPv4 或 IPv6 邻居及邻居设置。

过程

步骤 1 在“设备管理”页面中，点击**路由 (Routing)**。

步骤 2 （对于虚拟路由器感知设备）在虚拟路由器下拉列表中，选择要为其配置 BGP 的虚拟路由器。

步骤 3 选择 **BGP** > **IPv4**或 **IPv6**。

步骤 4 点击 **Neighbor**。

步骤 5 点击**添加**以定义 BGP 邻居及邻居设置。

步骤 6 输入 BGP 邻居的 **IP 地址**。此 IP 地址会添加到 BGP 邻居表。在静态 VTI 上配置 BGP IPv6 时，请输入邻居的虚拟隧道 IP 地址。

步骤 7 选择 BGP 邻居**接口**。

注释 **接口**字段仅适用于 IPv6 设置。

步骤 8 在**远程 AS** 字段中，输入 BGP 邻居所属的自治系统。

步骤 9 选中**启用地址 (Enabled address)** 复选框以启用与此BGP邻居的通信。仅当选中“已启用地址”复选框时，才会配置进一步的邻居设置。

步骤 10 （可选）选中**以管理员身份关闭 (Shutdown administratively)** 复选框，以禁用邻居或对等体组。

步骤 11 （可选）选中**配置平稳重启（故障转移 / 跨区模式）(Configure graceful restart [failover / spanned mode])** 复选框，以为此邻居启用 BGP 平稳重启功能的配置。选择此选项后，必须选中 **启用平稳重启 (Enable graceful restart)** 复选框来指定对此邻居启用还是禁用平稳重启。

注释
- 仅当设备处于 HA 模式或配置了 L2 集群（来自同一网络的所有节点）时，才会启用平稳重启。
- BGPv6 的平稳重启选项仅在 Cisco Secure Firewall Threat Defense 7.3 或更高版本上启用。
- 如果仅在常规设置而不是 BGP IPv6 中配置平稳重启，则全局常规设置配置仍然存在。
- 如果在常规设置和 BGP IPv6 中配置平稳重启，则全局常规设置配置将被 BGP IPv6 配置设置覆盖。

步骤 12 （可选）要为 BGP 启用 BFD 支持配置，请从 **BFD 故障转移 (BFD Fallover)** 下拉列表中选择 BFD 类型 - 单跳、多跳或自动检测跳。该选择会注册 BGP 邻居以接收来自 BFD 的转发路径检测失败消息。如果您不想获得 BFD 支持，请选择“无”(None)。

步骤 13 （可选）输入 BGP 邻居的**说明**。

步骤 14 （可选）从 **更新源 (Update Source)**下拉列表中选择 BGP 数据包源接口。

您可以选择环回地址作为此接口，以克服路径故障。您还可以选择任何物理接口、端口通道或子接口。

步骤 15 （可选）在**过滤路由**中，根据需要使用访问列表、路由映射、前缀列表和 AS 路径过滤器来分发 BGP 邻居信息。更新以下部分：

a) 选择适当的传入或传出**访问列表**以分发 BGP 邻居信息。

注释 访问列表仅适用于 IPv4 设置。

b) 选择适当的传入或传出**路由映射**以将路由映射应用到传入或传出路由。

c) 选择适当的传入或传出**前缀列表**以分发 BGP 邻居信息。

d) 选择适当的传入或传出**AS 路径过滤器**以分发 BGP 邻居信息。

e) 选中**限制允许从邻居接收的前缀数量 (Limit the number of prefixes allowed from the neighbor)** 复选框，以控制可以从邻居接收的前缀的数量。

- 在**最大前缀数**字段中，输入允许从特定邻居接收的前缀的最大数量。
- 在**阈值级别**字段中，输入路由器开始生成警告消息时所处的（最大值的）百分比。有效值是介于 1 和 100 之间的整数。默认值为 75。

f) 选中**控制从对等体接收的前缀 (Control prefixes received from the peer)** 复选框，以指定对从对等体接收的前缀的额外控制。执行以下操作之一：

- 选中**超出前缀限制时终止对等 (Terminate peering when prefix limit is exceeded)** 复选框，以在达到前缀限制时停止 BGP 邻居。在 **Restart interval** 字段中，指定 BGP 邻居重新启动前的间隔。
- 选中**仅在超出前缀限制时发出警报消息 (Give only warning message when prefix limit is exceeded)** 复选框，以在达到最大前缀限制时生成日志消息。此时将不会终止 BGP 邻居。

g) 点击**确定**。

步骤 16 （可选）在**路由**中，指定其他邻居路由参数。继续更新以下内容：

a) 在**Advertisement Interval**字段中，输入前后两次发送BGP路由更新的最小间隔（以秒为单位）。有效值介于 1 与 600 之间。

b) 选中**删除传出路由更新中的专用 AS 编号 (Remove private AS numbers from outbound routing updates)** 复选框，以阻止在出站路由上通告专用 AS 编号。

c) 选中**生成默认路由 (Generate default routes)** 复选框，以允许本地路由器将默认路由 0.0.0.0 发送到邻居，以用作该邻居的默认路由。在**路由映射**字段中输入或选择允许有条件地注入路由0.0.0.0的路由映射。

d) 要添加有条件通告的路由，请点击“添加行”+。在“添加通告路由”对话框中，执行以下操作：

1. 在**通告映射 (Advertise Map)** 字段中添加或选择路由映射，如果满足现有映射或非现有映射的条件，则会通告该映射。
2. 点击**现有映射 (Exist Map)**，然后从“路由映射对象选择器”(Route Map Object Selector) 中选择路由映射。此路由映射与 BGP 表中的路由进行比较，以确定是否对通告映射路由进行通告。
3. 点击**非现有映射 (Non-Exist Map)**，然后从“路由映射对象选择器”(Route Map Object Selector) 中选择路由映射。此路由映射与BGP表中的路由进行比较，以确定是否对通告映射路由进行通告。
4. 点击**确定**。

步骤 17 在**计时器 (Timers)** 中，选中**设置 BGP 对等体的计时器 (Set timers for the BGP peer)** 复选框，以设置保持连接频率、保持时间和最小保持时间。

- **保持连接间隔 (Keep alive interval)** - 输入 威胁防御 设备向邻居发送保持连接消息的频率（以秒为单位）。有效值介于 0 与 65535 之间。默认值为 60 秒。
- **保持时间**- 威胁防御 设备在未接收到保持连接消息后声明对等体处于失效状态的间隔（以秒为单位）。有效值介于 0 与 65535 之间。默认值为 180 秒。
- **最小保持时间**-（可选）威胁防御设备在未接收到保持连接消息后声明对等体处于失效状态的最小间隔（以秒为单位）。有效值介于 3 与 65535 之间。默认值为 3 秒。

  注释 保持时间小于 20 秒会增加对等体振荡的可能性。

步骤 18 在**高级**中，更新以下内容：

a) （可选）选中 **Enable Authentication** 复选框，以在两个 BGP 对等体之间的 TCP 连接上启用 MD5 身份验证。

1. 从**启用加密类型**下拉列表中选择加密类型。
2. 在 **Password** 字段中输入密码。在 **Confirm Password** 字段中重新输入密码。密码区分大小写，当启用 service password-encryption 命令时，长度最大为 25 个字符；未启用 service password-encryption 命令时，长度最大为 81 个字符。此字符串包含任意字母数字字符，包括空格。

注释　不能指定 number-space-anything 格式的密码。数字后的空格会导致身份验证失败。

b) （可选）选中 **将社区属性发送到此邻居** 复选框，以指定应将社区属性发送到 BGP 邻居
c) （可选）选中**使用 FTD 作为此邻居的下一跳**复选框，将路由器配置为 BGP 发言邻居或对等体组的下一跳。
d) 选中**禁用连接验证**复选框可为可通过单跳访问但在环回接口上配置或通过非直接连接 IP 地址配置的 eBGP 对等会话禁用连接验证过程。取消选中（默认设置）时，BGP 路由过程将验证单跳 eBGP 对等会话 (TTL=254) 的连接，以确定 eBGP 对等体在默认情况下是否直接连接到相同的网段。如果对等体没有直连到同一网段，连接验证将阻止建立对等会话。
e) 选择**允许连接未直接连接的邻居**，以接受并尝试建立与未直接连接的网络上的外部对等体的BGP连接。（可选）在 **TTL 跳**字段中输入生存时间。有效值介于 1 与 255 之间。或者，选择**到邻居的有限 TTL 跳数**，以确保 BGP 对等会话的安全。在 **TTL hops** 字段中，输入用于分隔 eBGP 对等体的最大跳数。有效值介于 1 与 254 之间。
f) （可选）选中**使用 TCP MTU 路径发现**复选框，为 BGP 会话启用 TCP 传输会话。
g) 从 **TCP 传输模式** 下拉列表中选择 TCP 连接模式。选项包括“默认”、“主动”或“被动”。
h) （可选）输入 BGP 邻居连接的**权重**。
i) 从下拉列表中选择 威胁防御设备将接受的 **BGP 版本**。版本可以设置为“仅限 4”，以强制软件仅对指定邻居使用版本 4。默认使用版本 4，如有要求，可以动态地协商降至版本 2。

步骤 19 仅当考虑进行 AS 迁移时，才更新**迁移**。

注释　在过渡完成后，应删除 AS 迁移自定义。

a) （可选）选中 **Customize the AS number for routes received from the neighbor** 复选框，为从 eBGP 邻居接收的路由自定义 AS_PATH 属性。
b) 在**本地 AS 编号**字段中输入本地自治系统编号。有效值是从 1 到 4294967295 或 1.0 到 65535.65535 之间的任何有效自治系统编号。
c) （可选）选中**不将本地 AS 编号附加到从邻居接收的路由前 (Do not prepend local AS number to routes received from neighbor)** 复选框，以防止将本地 AS 编号附加到从 eBGP 对等体接收的任何路由前。
d) （可选）选中**将实际 AS 编号替换为从邻居接收的路由中的本地 AS 编号 (Replace real AS number with local AS number in routes received from neighbor)** 复选框，将实际自治系统编号替换为 eBGP 更新中的本地自治系统编号。来自本地 BGP 路由过程的自主系统编号不会预置到前面。
e) （可选）选中 **接受实际 AS 编号或从邻居接收的路由中的本地 AS 编号 (Accept either real AS number or local AS number in routesreceived from neighbor)** 复选框，将 eBGP 邻居配置为使用实际自治系统号（来自本地 BGP 路由过程）或使用本地自治系统编号建立对等会话。

步骤 20 点击**确定 (OK)**。

步骤 21 点击**保存 (Save)**。

配置 BGP 汇聚地址设置

BGP邻居存储和交换路由信息，随着配置的BGP发言方的增加，路由信息的量也随之增加。路由聚合是将多个不同路由的属性组合在一起的过程，以便仅通告一个路由。聚合前缀使用无类别域内路由 (CIDR) 原则将相邻的网络合并成一个可在路由表中汇总的无类别 IP 地址集。因此，通告的路由更少。使用“添加/编辑汇聚地址”对话框可将特定路由的聚合定义到一个路由中。

过程

步骤 1 编辑 威胁防御 设备时，点击 **路由 (Routing)**。

步骤 2 （对于虚拟路由器感知设备）在虚拟路由器下拉列表中，选择要为其配置 BGP 的虚拟路由器。

步骤 3 选择 **BGP** > **IPv4**或 **IPv6**。

步骤 4 点击**添加汇聚地址 (Add Aggregate Address)**。

步骤 5 在**聚合计时器**字段中，为聚合计时器指定一个值（以秒为单位）。有效值为 0 或介于 6 与 60 之间的任意值。默认值为 30。

步骤 6 点击 （＋）**添加 (Add)** 并更新 **添加聚合地址 (Add Aggregate Address)** 对话框：

a) **网络** - 输入 IPv4 地址或选择所需的网络/主机对象。
b) **属性映射** -（可选）输入或选择用于设置聚合路由属性的路由映射。
c) **通告映射** -（可选）输入或选择用于选择路由的路由映射，以创建 AS_SET 源社区。
d) **隐含映射** -（可选）输入或选择用于选择要隐含的路由的路由映射。
e) **生成 AS 设置路径信息** -（可选）选中该复选框以生成自动系统设置路径信息。
f) **从更新中过滤所有路由** -（可选）选中该复选框可从更新中过滤所有更加特定的路由。
g) 点击**确定 (OK)**。

下一步做什么

- 对于 BGPv4 设置，请继续 配置 BGPv4 过滤设置， 第 13 页
- 对于 BGPv6 设置，请继续 配置 BGP 网络设置， 第 14 页

配置 BGPv4 过滤设置

过滤设置用于过滤传入的BGP更新中接收的路由或网络。过滤用于限制路由器所获悉或通告的路由信息。

开始之前

过滤仅适用于 BGP IPv4 路由策略。

过程

步骤 1 在“设备管理”页面中，点击**路由 (Routing)**。

步骤 2 （对于虚拟路由器感知设备）在虚拟路由器下拉列表中，选择要为其配置 BGP 的虚拟路由器。

步骤 3 选择 **BGP** > **IPv4**。

步骤 4 点击 **Filtering**。

注释 **过滤 (Filtering)** 字段仅适用于 IPv4 设置。

步骤 5 点击 （＋）**添加 (Add)** 并更新**添加过滤器 (Add Filter)** 对话框：

a) **访问列表 (Access List)** - 选择定义在路由更新中要接收和抑制哪些网络的访问控制列表。

b) **方向 (Direction)** -（可选）选择指定是否应将过滤器应用于入站更新或出站更新的方向。

c) **协议 (Protocol)** -（可选）选择要过滤的路由进程：“无”、“BGP”、“已连接”、“OSPF”、“RIP”或“静态”。

d) **进程 ID** -（可选）输入 OSPF 路由协议的进程 ID。

e) 点击**确定 (OK)**。

步骤 6 点击**保存 (Save)**。

配置 BGP 网络设置

网络设置用于添加将由BGP路由过程通告的网络，以及将被检查以过滤要通告的网络的路由映射。

过程

步骤 1 在**设备管理 (Device Management)** 页面中，点击**路由 (Routing)**。

步骤 2 （对于虚拟路由器感知设备）在虚拟路由器下拉列表中，选择要为其配置 BGP 的虚拟路由器。

步骤 3 选择 **BGP** > **IPv4**或 **IPv6**。

步骤 4 点击 **Networks**。

步骤 5 点击**添加 (Add)** 并更新**添加网络 (Add Networks)** 对话框：

a) **网络 (Network)** - 选择将由 BGP 路由过程通告的网络：

注释 要通告网络前缀，路由表中必须存在通往设备的路由。

要添加新的网络对象，请请参阅创建网络对象。

b) （可选） **路由映射 (Route Map)** - 输入或选择应被检查以过滤要通告的网络的路由映射。如果未指定，则重新分发所有网络。要添加新的路由映射对象，请参阅路由映射

c) 点击**确定 (OK)**。

步骤 6 点击**保存 (Save)**。

配置 BGP 重新分发设置

重新分发设置可定义将其他路由域中的路由重新分发到 BGP 的条件。

过程

步骤 1 在**设备管理 (Device Management)** 页面中，点击**路由 (Routing)**。

步骤 2 （对于虚拟路由器感知设备）在虚拟路由器下拉列表中，选择要为其配置 BGP 的虚拟路由器。

步骤 3 选择 **BGP** > **IPv4**或 **IPv6**。

步骤 4 点击 **Redistribution**。

步骤 5 点击**添加**并更新**添加重新分发**对话框：

a) **源协议** - 从“源协议”下拉列表中选择要将路由重新分发到 BGP 域所使用的协议。

注释　用户定义的虚拟路由器不支持从 RIP 重新分发流量。

b) **进程 ID** - 输入所选源协议的标识符。应用至 OSPF 协议。对于使用虚拟路由的设备，此下拉列表列出了为您为其配置 BGP 设置的虚拟路由器分配的进程 ID。

c) **指标** -（可选）为重新分配的路由输入一个指标。

d) **路由映射** - 输入或选择应检查的路由映射，以便过滤要重新分发的网络。如果未指定，则重新分发所有网络。要创建新的路由映射对象，请点击 **添加**（+）。请参阅程序的配置路由映射条目以添加新的路由映射。

e) **匹配** - 用于将路由从一个路由协议重新分发到另一个路由协议的条件。路由必须与要重新分发的所选条件相匹配。您可以选择以下一个或多个匹配条件。只有在选择OSPF 作为源协议时，才会启用这些选项。

- 内部
- 外部 1
- 外部 2
- NSSA 外部 1
- NSSA 外部 2

f) 点击**确定**。

配置 BGP 路由注入设置

路由注入设置使您可以定义有条件地注入 BGP 路由表中的路由。

过程

步骤 1 在**设备管理 (Device Management)** 页面中，点击**路由 (Routing)**。

步骤 2 （对于虚拟路由器感知设备）在虚拟路由器下拉列表中，选择要为其配置 BGP 的虚拟路由器。

步骤 3 选择 **BGP** > **IPv4**或 **IPv6**。

步骤 4 点击**路由注入 (Route Injection)**。

步骤 5 点击**添加 (Add)** 并更新**添加路由注入 (Add Route Injection)** 对话框：

a) **注入映射** - 输入或选择指定要注入本地 BGP 路由表的前缀的路由映射。要创建新的路由映射对象，请点击 **添加**（＋）。有关添加新的路由映射的程序，请参阅配置路由映射条目。

b) **现有映射** - 输入或选择包含 BGP 发言者将跟踪的前缀的路由映射。

c) **已注入的路由将继承聚合路由的属性 (Injected routes will inherit the attributes of the aggregate route)** - 选中复选框可将已注入的路由配置为继承聚合路由的属性。

d) 点击**确定 (OK)**。

步骤 6 点击**保存 (Save)**。

配置 BGP 路由导入/导出设置

在BGP中，可以通过分别使用目的和源虚拟路由器的路由目标扩展社区导入或导出路由来实现虚拟路由器间路由泄漏。您可以使用路由映射来过滤所需的路由目标，而不是泄漏整个路由表。您还可以将全局虚拟路由器的路由泄漏到用户定义的虚拟路由器，反之亦然。

- 您可以将 BGP 配置为使用路由目标扩展社区在两个用户定义的虚拟路由器之间泄漏路由：
  - 使用路由目标导出，使用来自源虚拟路由器的路由目标标记路由。
  - 使用路由目标导入，将与路由目标匹配的路由导入到目的虚拟路由器。
  - 或者，您可以分别使用导出或导入路由映射来过滤来自源虚拟路由器或到目的虚拟路由器的路由。您可以通过匹配扩展社区列表来配置路由映射，以过滤路由。同样，您可以通过设置扩展社区路由目标来配置路由映射，以使用路由目标扩展社区标记路由。
- 要将路由从全局虚拟路由器导入到用户定义的虚拟路由器，需要在全局虚拟路由器导入路由映射中指定 IPv4/IPv6 路由映射，以导入到用户定义的虚拟路由器。
- 要将路由从用户定义的虚拟路由器导出到全局虚拟路由器，除了导出路由目标外，还可以指定全局虚拟路由器导出路由映射，以从用户定义的虚拟路由器导出。

BGP 虚拟路由器间路由泄漏支持 IPv4 和 IPv6 前缀。

开始之前

- 创建虚拟路由器。
- 配置 BGP 基本设置。

- 配置 BGP， 第 5 页

过程

步骤 1 在“设备管理”页面中，点击**路由 (Routing)**。

步骤 2 （对于虚拟路由器感知设备）在虚拟路由器下拉列表中，选择要为其配置 BGP 的虚拟路由器。

步骤 3 选择 **BGP** > **IPv4** 或 **IPv6**。

步骤 4 （仅虚拟路由器支持）点击**路由导入/导出 (Route Import/Export)**。

步骤 5 在**路由目标导入**字段中，输入要与待导入的路由匹配的路由目标扩展社区。在部署时，与此值匹配的目标虚拟路由器的路由将导入到源虚拟路由器的 BGP 表中。

注释
- 路由目标必须采用 **ASN:nn** 格式。
- 您可以以逗号分隔值的形式输入多个路由目标。
- 此值的范围为 0:1 到 65534:65535。

步骤 6 在**路由目标导出**字段中，输入路由目标扩展社区，以使用路由目标值标记源虚拟路由器的路由。部署时，源虚拟路由器的路由使用此值进行标记。

注释
- 路由目标必须采用 **ASN:nn** 格式。
- 您可以以逗号分隔值的形式输入多个路由目标。
- 此值的范围为 0:1 到 65534:65535。

步骤 7 路由映射可帮助您缩小要共享的路由的范围，而不是泄漏整个路由表。路由映射过滤应用于使用指定路由目标值获取的路由列表：

a) （可选）在**用户虚拟路由器**下，从**导入路由映射**下拉列表中选择路由映射，以过滤目的虚拟路由器上的路由。

注释 用户虚拟路由器导入路由映射只有在配置了路由目标导入时才有效。

b) （可选）在 **用户虚拟路由器**下，从 **导出路由映射** 下拉列表中选择路由映射，以在将路由导出到其他虚拟路由器之前过滤源虚拟路由器上的路由。

注释 您可以将路由映射中的 match 和 set 子句与路由目标扩展社区列表一起使用，以根据其他条件进行过滤或使用路由目标社区值标记路由。有关详细信息，请参阅路由映射

步骤 8 要在用户定义的虚拟路由器和全局虚拟路由器之间共享路由，请在**全局虚拟路由器**下指定路由映射：

a) 要将全局虚拟路由器路由泄漏到用户定义的虚拟路由器，请从**导入路由映射**下拉列表中选择路由映射。将 IPv4 或 IPv6 路由映射导入用户定义的虚拟路由器。

b) 要将用户定义的虚拟路由器路由泄漏到全局虚拟路由器，请从**导出路由映射**下拉列表中选择路由映射。将 IPv4 或 IPv6 路由映射导出到全局虚拟路由器。

注释 除了指定路由映射之外，您还必须指定导出的路由目标。

注释 您可以使用路由映射对象的 match 子句过滤路由以进行泄漏。有关详细信息，请参阅路由映射。

步骤 9 按照步骤（步骤 3 到步骤 8）为其他虚拟路由器配置相关的 BGP 路由导入和导出设置。

步骤 10 点击**保存**，然后点击**部署**。

当数据包流入入口虚拟路由器时，BGP 会从具有匹配路由目标值的目的虚拟路由器导入路由，如果还配置了路由映射，则会进一步过滤路由并使用这些路由来识别用于路由数据包的最佳路径路由。

Cisco Secure Firewall Threat Defense中 BGP 历史记录

特性	Version	最低 威胁防御	详细信息
BGPv6 上的平稳重启支持	7.4	任意	您可以在 BGPv6 上为 Cisco Secure Firewall Threat Defense 7.3 及更高版本配置平稳重启。 新增/修改的屏幕： **路由** > **BGP** > **IPv6** > **添加/编辑邻居**。
BGP 的环回接口支持	7.4	任意	您可以将环回接口用于 BGP。 新增/修改的屏幕： **路由** > **BGP** > **IPv4 或 IPv6** > **添加/编辑邻居** 。
用于互连虚拟路由器的 BGP 配置	7.1	任意	可以将 BGP 设置配置为在用户定义的虚拟路由器之间以及全局虚拟路由器和用户定义的虚拟路由器之间动态泄漏路由。引入和导出路由功能是为了在虚拟路由器之间交换路由，方法是为它们标记路由目标，并选择性地使用路由映射过滤匹配的路由。仅当您选择用户定义的虚拟路由器时，才能访问此 BGP 功能。 新增/修改的屏幕：对于选定的用户定义的虚拟路由器， **设备 (Devices)** > **设备管理 (Device Management)** > **路由 (Routing)** > **BGPv4/v6** > **路由导入/导出 (Route Import/Export)** 选项卡。
BGPv6 支持用户定义的虚拟路由器	7.1	任意	Cisco Secure Firewall Threat Defense 现在支持在用户定义的虚拟路由器上配置 BGPv6。 新增/修改的屏幕：对于选定的用户定义的虚拟路由器， **设备 (Devices)** > **设备管理 (Device Management)** > **路由 (Routing)** > **BGPv6** 页面。

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。