通过Firepower威胁防御(FTD)允许Traceroute通过威胁服务策略

目录

简介

本文描述配置通过Firepower威胁防御(FTD)允许traceroute

先决条件

要求

Cisco 建议您了解以下主题：

- Firepower管理中心(FMC)
- Firepower威胁防御(FTD)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 此条款是可适用的对所有Firepower平台
- Cisco Firepower运行软件版本6.4.0的威胁防御(FTD)
- 运行软件版本6.4.0虚拟的Cisco Firepower的管理中心(FMC)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

帮助您的Traceroute确定数据包上对他们的目的地的路由。traceroute工作在发送UDP数据包旁边对目的地在无效的端口。由于端口无效，路由器目的地的回应ICMP超时消息并且汇报该错误对ASA。

traceroute显示被发送的每台探测器结果。输出每条线路对应于在增加命令的一个TTL值。此表解释输出符号。

输出符号	说明
*	无响应为在超时周期的探测器接收。
nn毫秒	每个节点，往返时间(以毫秒)探测器指定的编号的。
!! *n*	ICMP网络是不可得到的。
!! H	ICMP主机是不可得到的。
!! P	ICMP是不可得到的。
!! A	禁止的ICMP管理性。
?	未知ICMP错误。

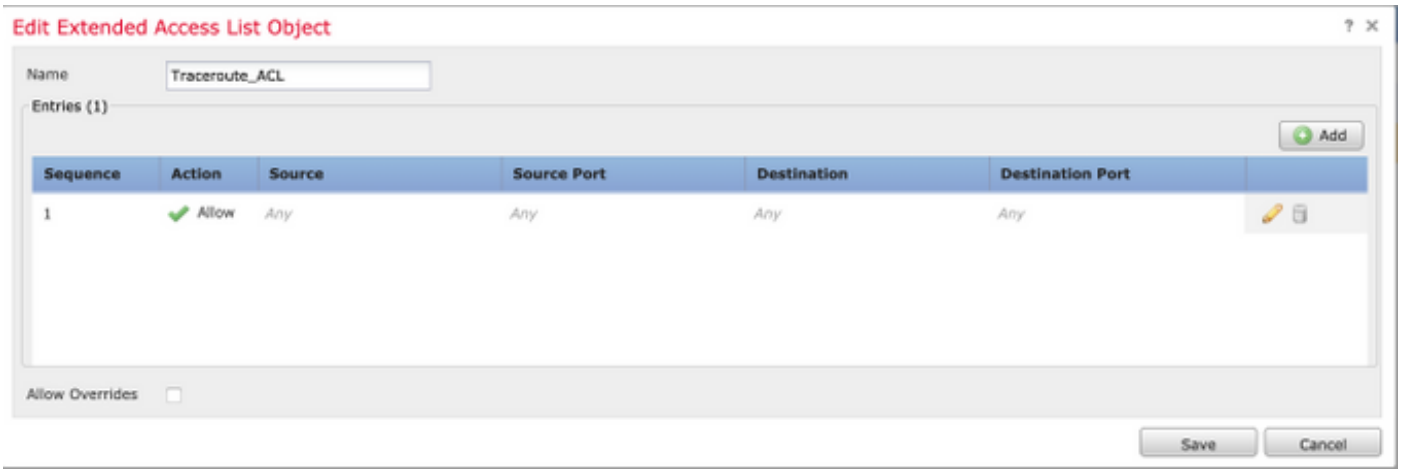
默认情况下， ASA不出现在追踪途径作为跳。要做它出现，您需要减少在穿过ASA并且增加在ICMP不可达信息的速率限制的数据包的time-to-live。

> **警告：**如果减少生存时间，数据包与TTL 1丢弃，但是连接为假定的会话打开连接也许包含数据包与更加极大的TTL。注意一些数据包，例如OSPF Hello数据包，发送与TTL=1，因此减少生存时间能有意外的结果。当定义您的数据流类别时，请记住这些考虑事项。

配置

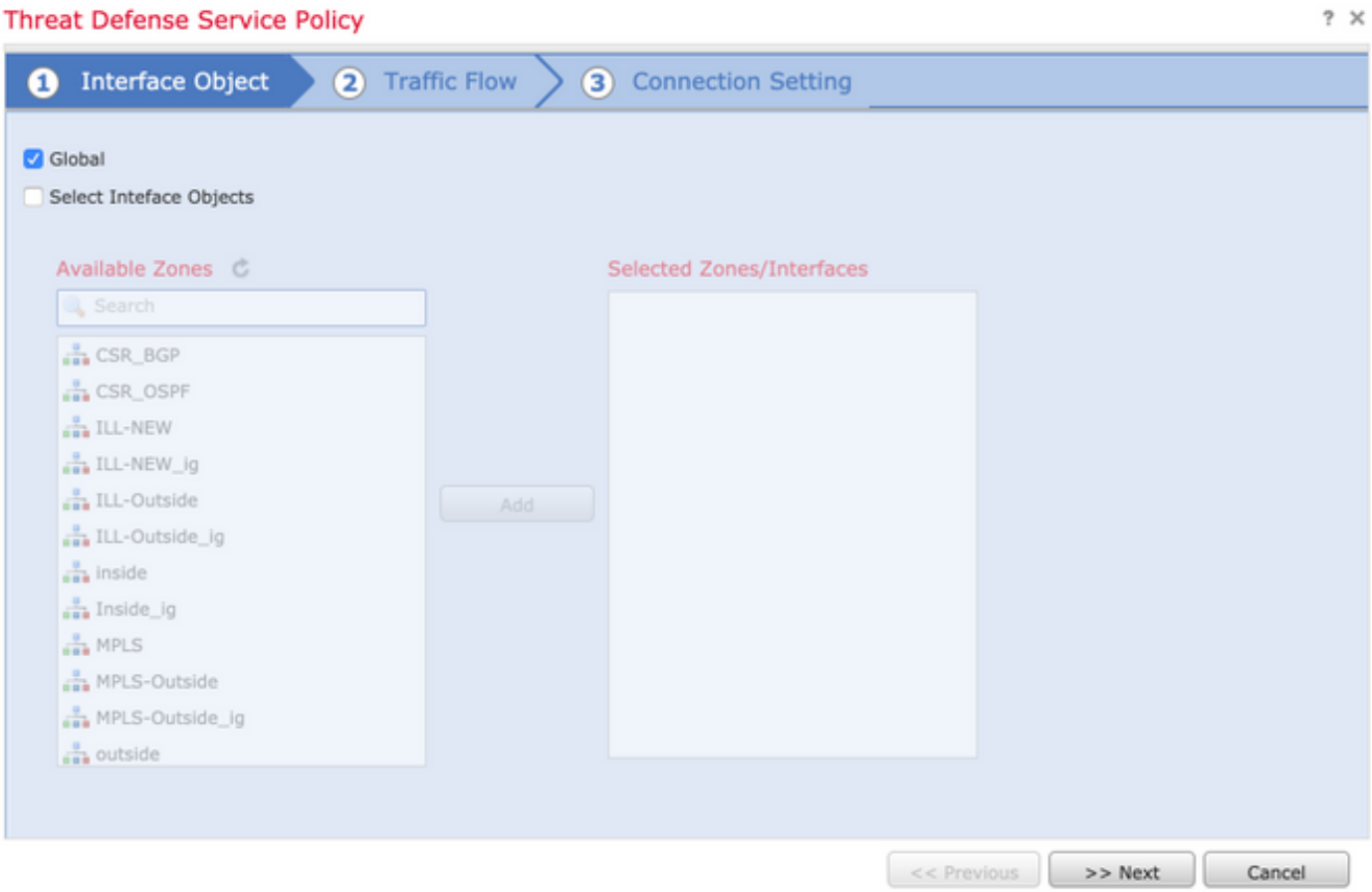
步骤1.创建定义了数据流类别报告需要的traceroute启用的扩展ACL。

登陆对**FMC GUI**并且导航对**对象>对象Management>访问列表**。 选择**延长**从目录表并且**添加**一新的扩展访问列表。如镜像所显示，输入一名称对于对象，例如，在Traceroute_ACL下，**增加**规则允许感兴趣流量和**保存**它， ：

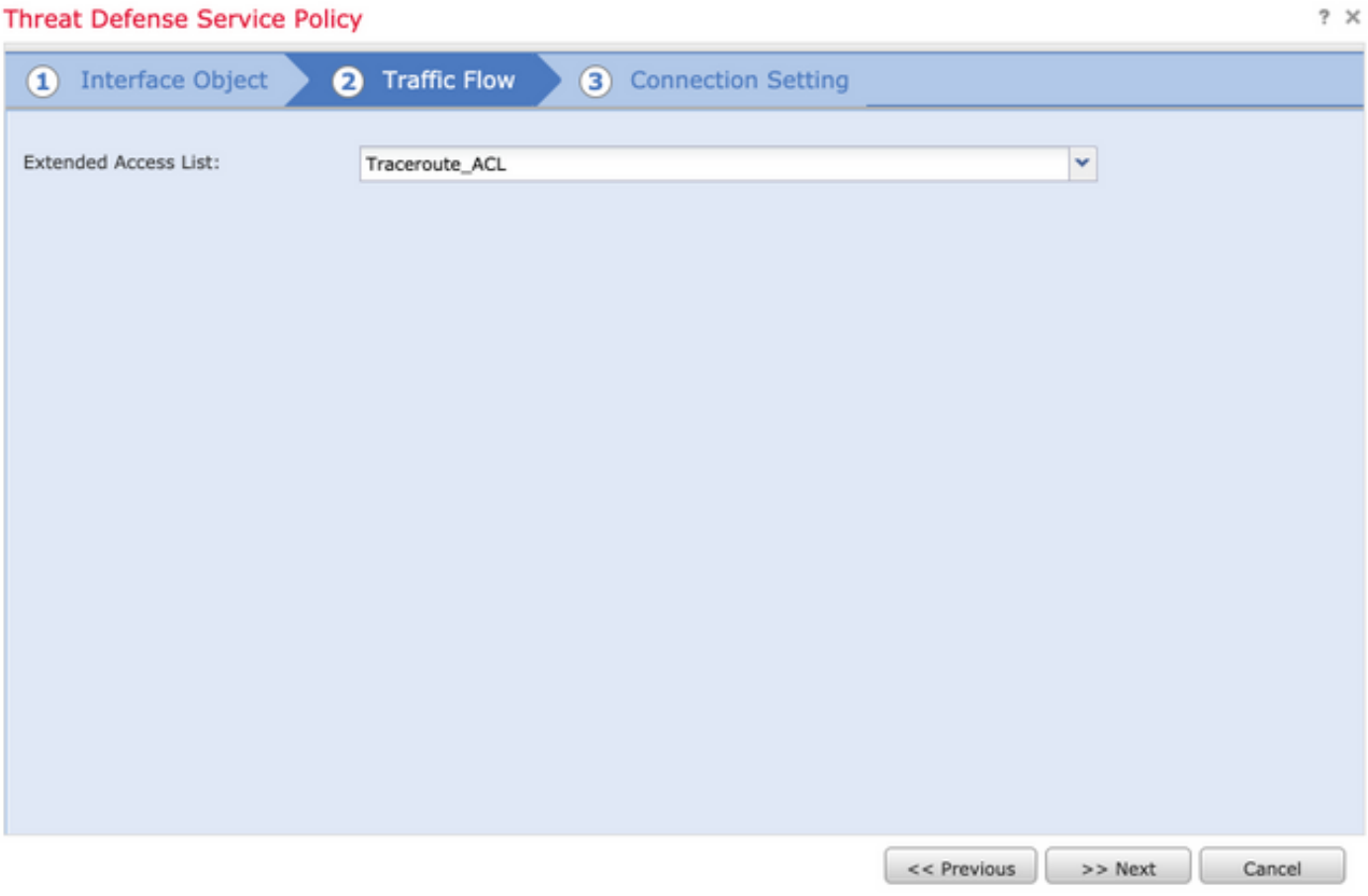


步骤2.配置服务策略裁决消耗time-to-live值。

导航到**策略>访问控制**然后**编辑**策略分配到设备。如镜像所显示，在**高级选项卡。下**，请**编辑威胁防御服务策略**然后添加新规则从**添加规则**选项卡然后选择**全局**复选框应用它全局并且**其次**单击， ：

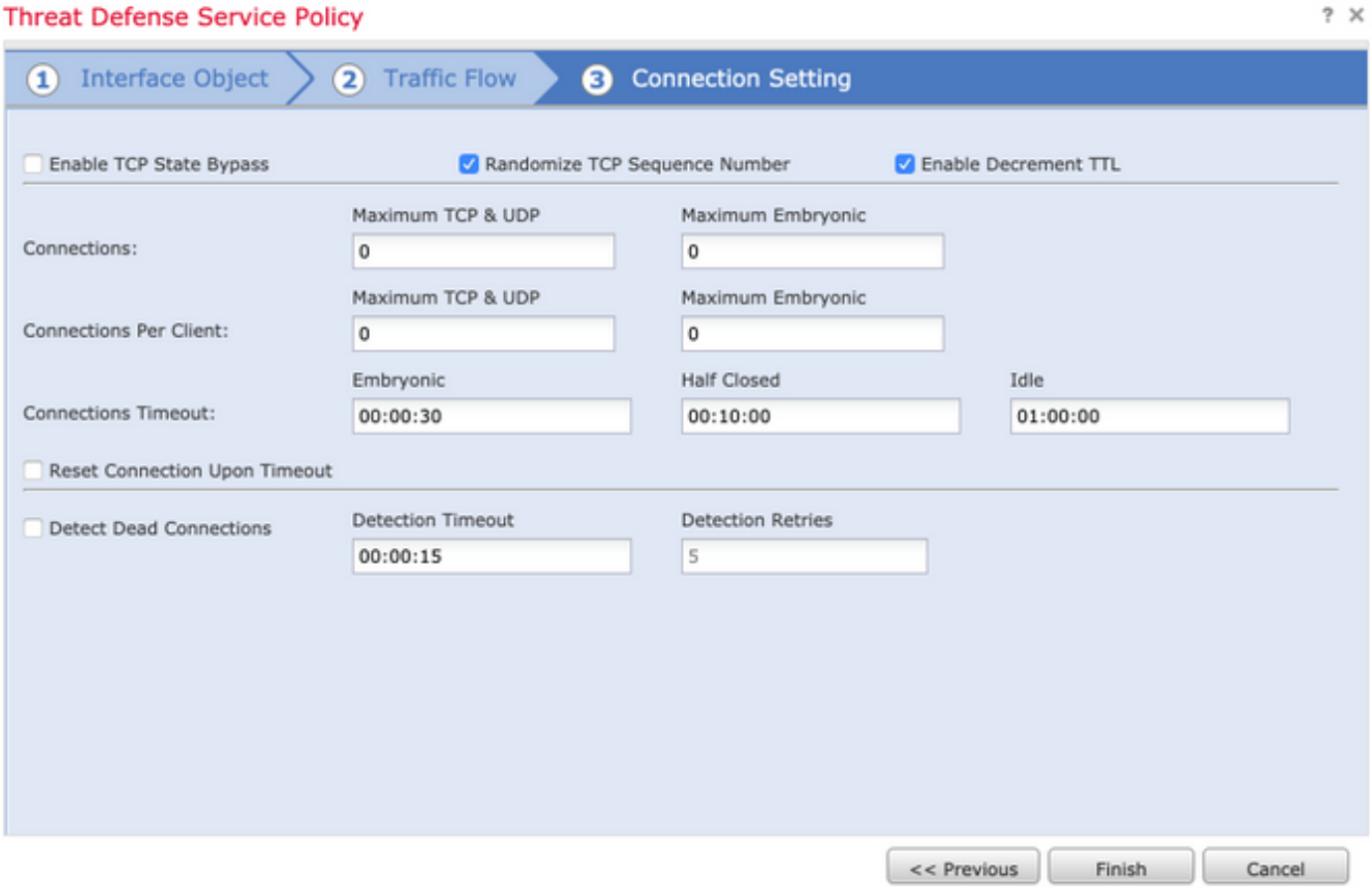


导航对**通信流>扩展访问列表**从在上一个步骤创建的下拉菜单然后选择**扩展访问列表对象。**如镜像所显示，现在请单击**其次，**：



选择**Enable (event)减少量TTL**复选框并且修改其他连接选项(可选)。如镜像所显示，现在请单击**芬通社**添

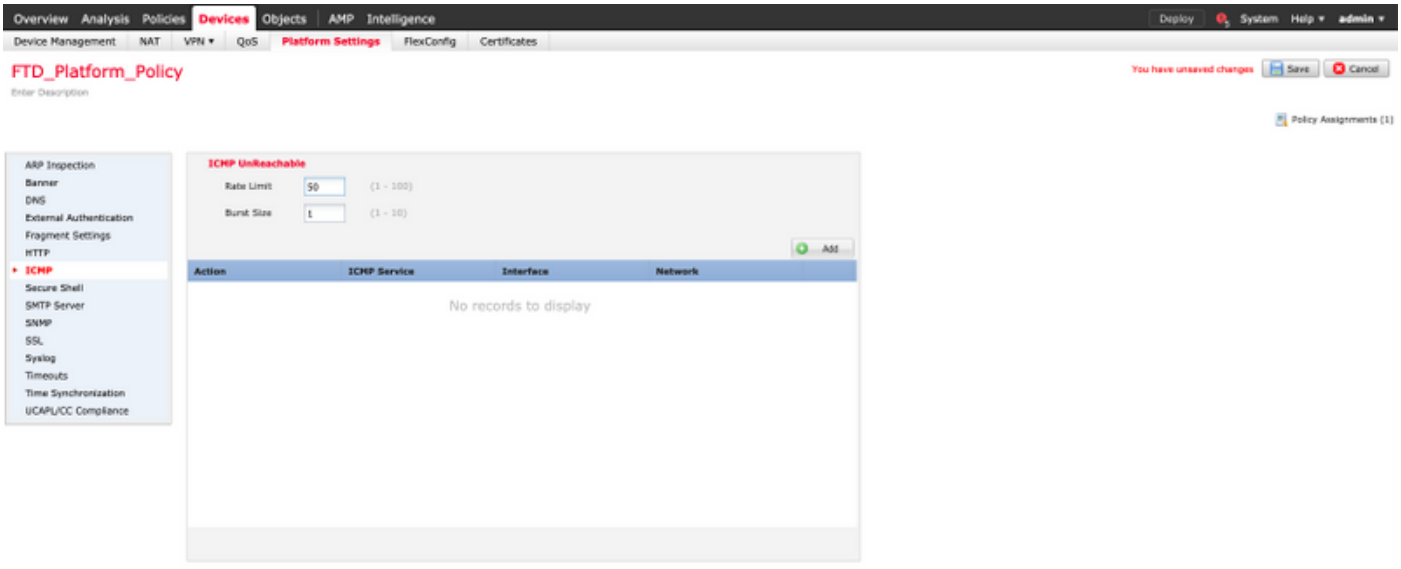
加规则然后点击OK键并且**保存**对威胁防御服务策略的更改，：



一旦上一个步骤完成，请保证**保存**访问控制策略。

步骤3.增加在ICMP不可达信息的速率限制(可选)。

导航对**设备>平台设置**然后**编辑**或者**创建**一项新的Firepower威胁防御平台设置策略并且关联它到设备。例如，现在请选择从目录的**ICMP**并且增加**速率限制**到50 (您能忽略突发流量大小)如镜像所显示，然后单击**"Save"**并且继续**实施**策略到设备，：



警告：保证**ICMP目的地不可达的(类型3)和ICMP Time exceeded (类型11)**在ACL策略或Fastpath'ed允许从外向里在PRE过滤器策略。

验证

一旦策略部署完成，请检查从FTD CLI的配置：

```
FTD# show run policy-map
!
policy-map type inspect dns preset_dns_map
---Output omitted---

class class_map_Traceroute_ACL
set connection timeout idle 1:00:00
set connection decrement-ttl
class class-default
!

FTD# show run class-map
!
class-map inspection_default

---Output omitted---

class-map class_map_Traceroute_ACL
match access-list Traceroute_ACL
!

FTD# show run access-l Traceroute_ACL
access-list Traceroute_ACL extended permit object-group ProxySG_ExtendedACL_30064773500 any any
log
FTD#
```

故障排除

您能采取在FTD入口和出口接口的捕获关注数据流的能进一步排除故障问题。

提示：CSCvq79913，为空pdts_info丢弃的ICMP错误信息包，保证最好是使用prefilter ICMP type3和11回程数据流。