Configurar uma Regra de Controle de Acesso com Limite de Tempo no FDM com API Rest

Contents

Introdução

Este documento descreve como configurar e validar uma regra de controle de acesso com base no tempo com API Rest no FTD gerenciado pelo FDM.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Firepower Threat Defense (FTD)
- FDM (Firepower Device Management, Gerenciamento de dispositivos do Firepower)
- Conhecimento da interface de programação de aplicativo de transferência de estado representacional (REST API)
- Lista de controle de acesso (ACL)

Componentes Utilizados

As informações neste documento são baseadas no FTD versão 7.1.0.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

A API do FTD versão 6.6.0 e posterior suporta regras de controle de acesso que são limitadas com base no tempo.

Usando a API do FTD, você pode criar objetos de intervalo de tempo, que especificam intervalos de tempo únicos ou recorrentes, e aplicar esses objetos às regras de controle de acesso. Usando intervalos de tempo, você pode aplicar uma regra de controle de acesso ao tráfego durante determinados horários do dia ou por determinados períodos de tempo, a fim de fornecer flexibilidade ao uso da rede. Não é possível usar o FDM para criar ou aplicar intervalos de tempo, nem o FDM mostrará se uma regra de controle de acesso tem um

intervalo de tempo aplicado a ela.

Configurar

Etapa 1. Clique nas opções avançadas (menu Kebab) para abrir o FDM API explorer.

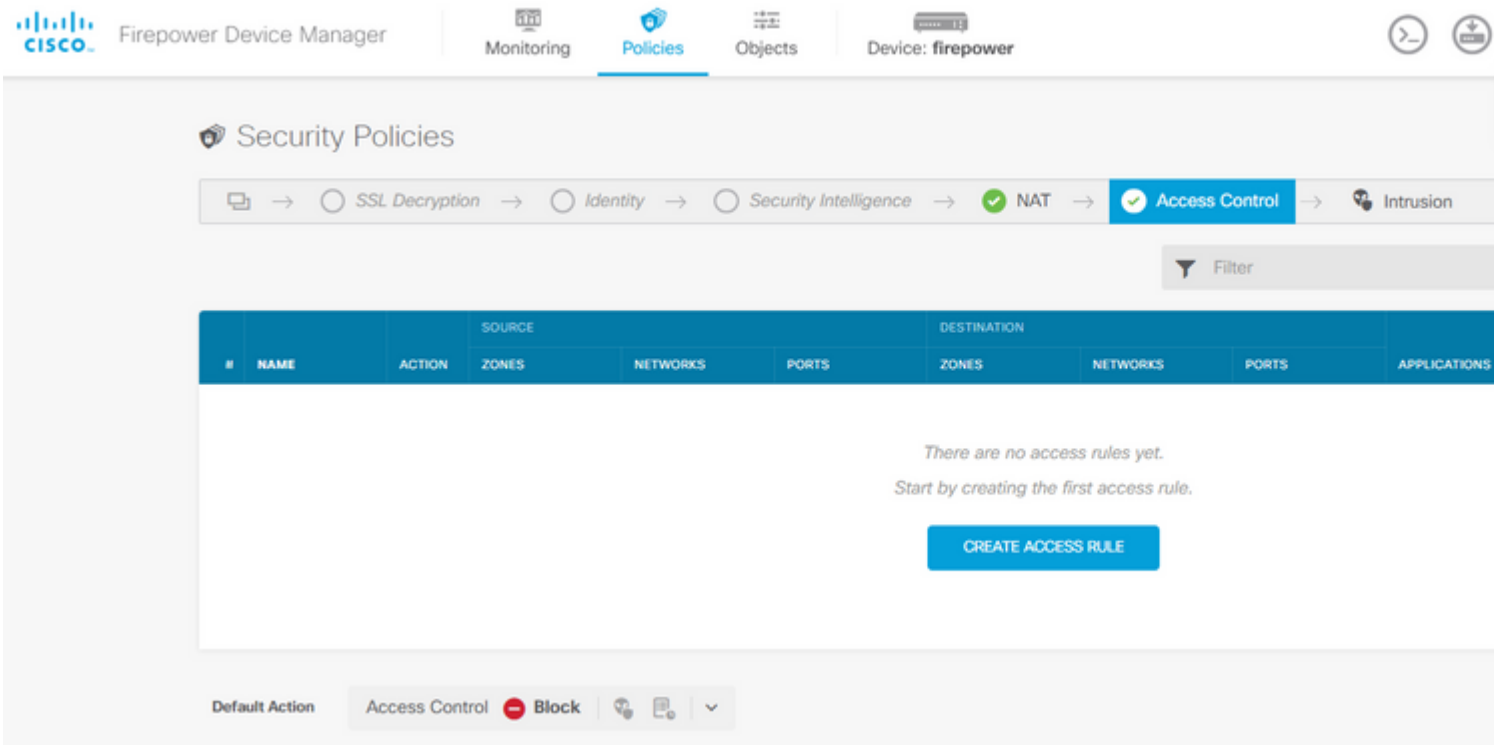


Imagem 1. Interface do usuário da Web do FDM.

Etapa 2. Escolha a categoria **AccessPolicy** para exibir as diferentes chamadas de API.

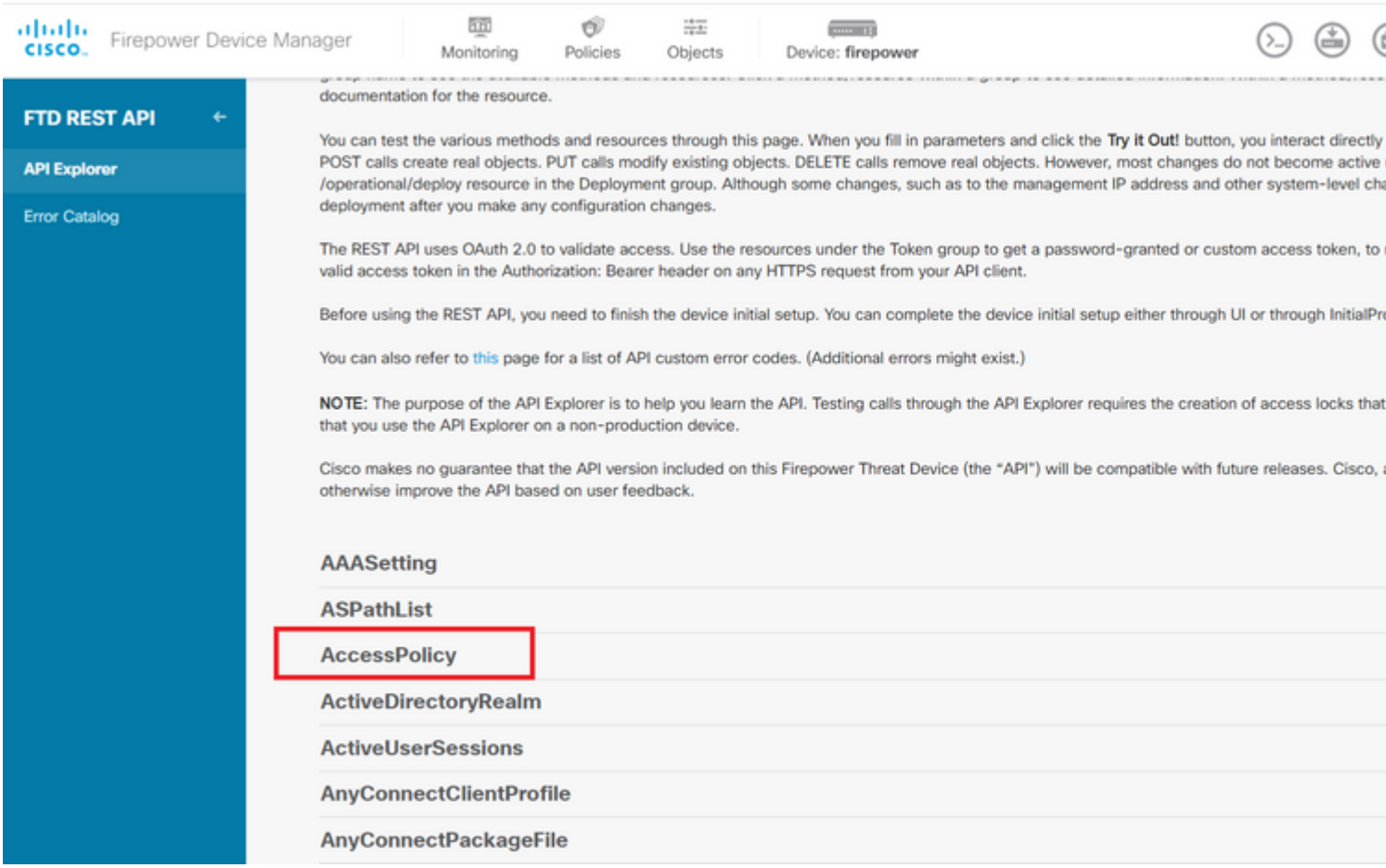
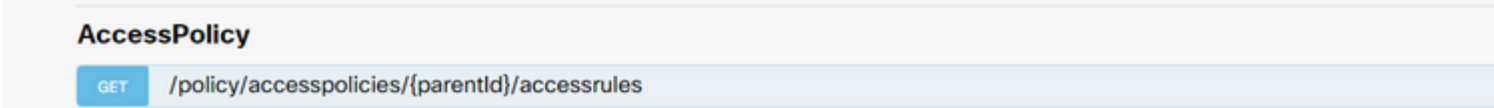


Imagem 2. Interface de usuário da Web do API Explorer.

Etapa 3. Execute o comando **GET** para obter a ID da política de acesso.



dados do corpo da resposta para um bloco de notas. Posteriormente, você deverá usar a ID da Política de Controle de Acesso.

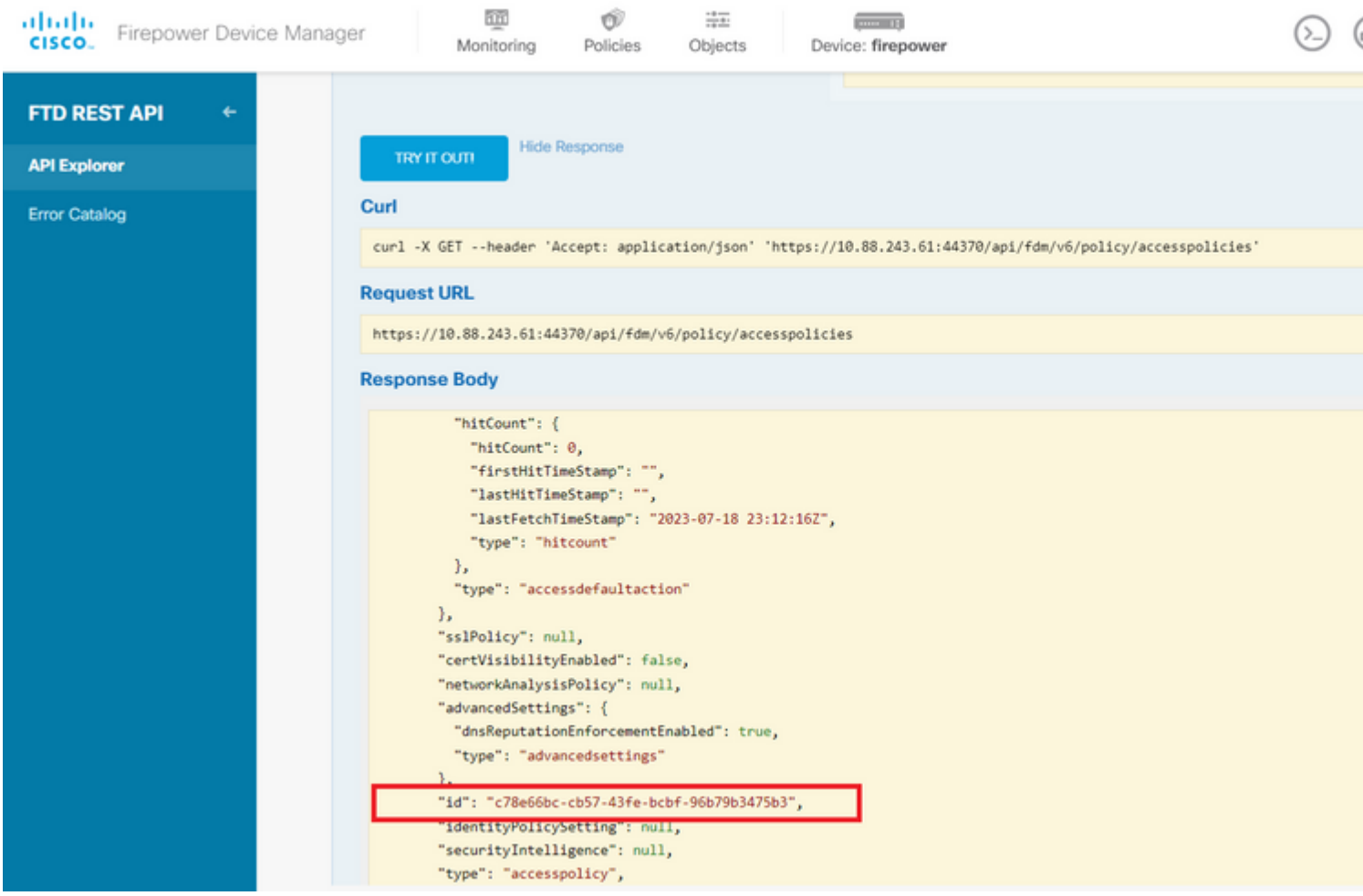


Imagem 5. Resposta GET da Política de Acesso.

Etapa 6. Localize e abra a categoria TimeRange no API Explorer para exibir as diferentes chamadas de API.

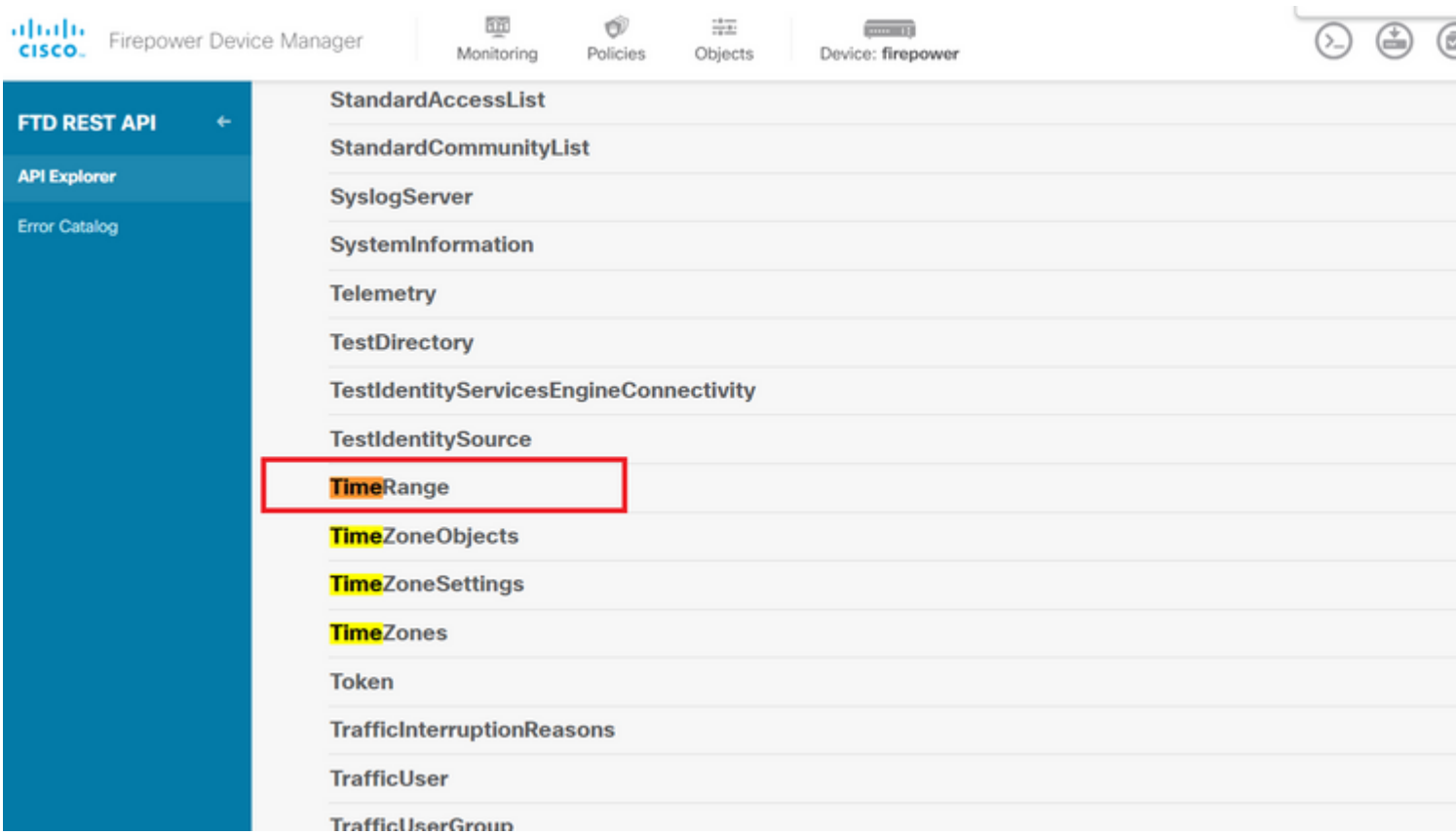


Imagem 6. Categoria de intervalo de tempo.

Passo 7. Crie quantos objetos TimeRange desejar usando a chamada à API **POST**.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.