O centro de gerenciamento da potência de fogo indica alguns eventos da conexão de TCP na direção errada

Índice

Introdução

Este documento descreve as razões e as etapas da mitigação para o Gerenciamento Center(FMC) da potência de fogo que indica eventos da conexão de TCP no sentido reverso onde o IP do iniciador é o IP de servidor da conexão de TCP e IP do que responde é o IP de cliente da conexão de TCP.

> Nota: Há umas razões múltiplas para a ocorrência de tais eventos. Isto documenta explica a maioria de causa comum deste sintoma.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Tecnologia da potência de fogo
- Conhecimento básico da ferramenta de segurança adaptável (ASA)
- Compreensão do mecanismo do sincronismo de Transmission Control Protocol(TCP)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- A defesa da ameaça da potência de fogo ASA (5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) essa executa a versão de software 6.0.1 e mais atrasado
- A defesa da ameaça da potência de fogo ASA (5512-X,5515-X, ASA 5525-X, ASA 5545-X,

ASA 5555-X,FP9300,FP4100) essa executa a versão de software 6.0.1 e mais atrasado
- O ASA com os módulos da potência de fogo (5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X,5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X) esses executa as versões de software 6.0.0 e mais atrasado
- Versão 6.0.0 e mais recente do centro de gerenciamento da potência de fogo (FMC)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos usados neste documento começaram com uma configuração clara (do padrão). Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Background

Em uma conexão de TCP, o **cliente** refere o IP que envia o pacote inicial. O centro de gerenciamento da potência de fogo gerencie um evento de conexão quando o dispositivo gerenciado (sensor ou FTD) vê o pacote de TCP inicial de uma conexão.

Os dispositivos que seguem o estado de uma conexão de TCP têm um **idle timeout** definido para certificar-se de que as conexões que não são fechadas erroneamente por valores-limite não consomem a memória disponível por períodos longos de tempo. O default idle timeout para conexões de TCP estabelecidas na potência de fogo é **três minutos**. Uma conexão de TCP que fique inativa por três minutos ou mais, não é seguida pelo sensor IPS da potência de fogo.

O pacote subsequente depois que o intervalo é tratado enquanto um fluxo de TCP novo e a decisão de encaminhamento estão tomados conforme a regra que combina este pacote. Quando o pacote é do server, o IP do server está gravado como o iniciador deste fluxo novo. Quando registrar é permitido para a regra, um evento de conexão está gerado no centro de gerenciamento da potência de fogo.

> Nota: Conforme políticas configuradas, a decisão de encaminhamento para o pacote que vem depois que o intervalo é diferente da decisão para o pacote de TCP inicial. Se a ação padrão configurada é “bloco”, o pacote está deixado cair.

Um exemplo deste sintoma é conforme o tiro de tela abaixo:

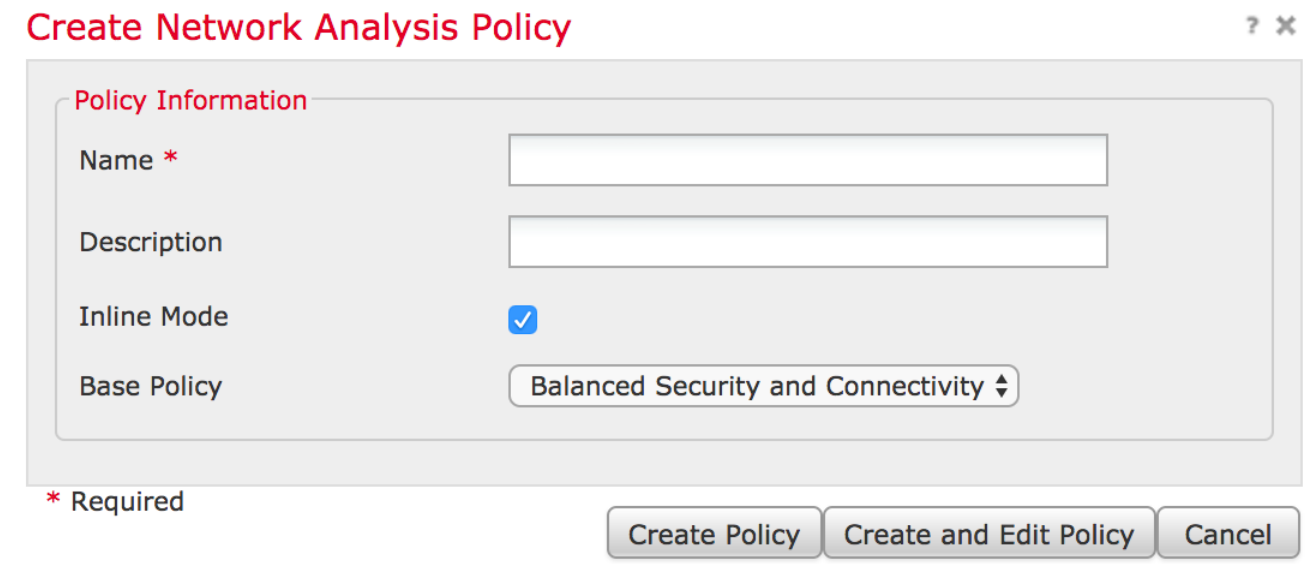
First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code
2017-05-12 17:48:05		Block		10.32.38.30		192.168.38.30				443 (https) / tcp	44705 / tcp
2017-05-12 17:39:13		Allow		192.168.38.30		10.32.38.30				44705 / tcp	443 (https) / tcp

Solução

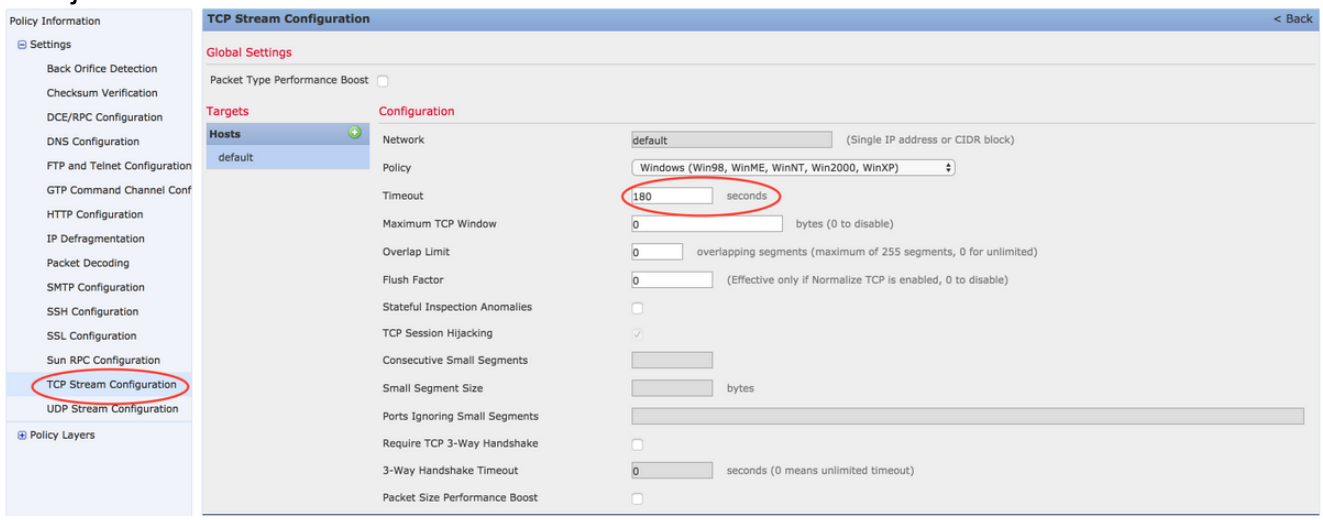
O problema acima mencionado é abrandado aumentando o **intervalo das** conexões de TCP. Em ordem mude o intervalo,

1. Navegue às **políticas > ao controle de acesso > à intrusão**.
2. Navegue ao canto superior direito e selecione a **política do acesso de rede**.

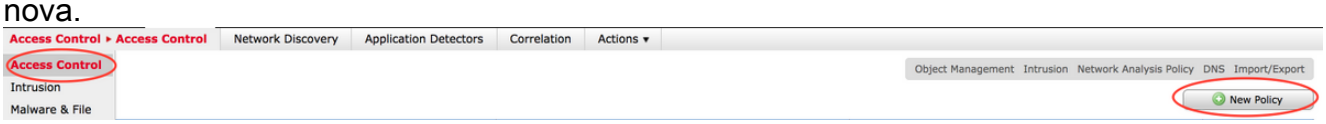
3. Seleto **crie a política**, escolha um nome e clique sobre **Create e edite a política**. Não altere a **política**
baixa.



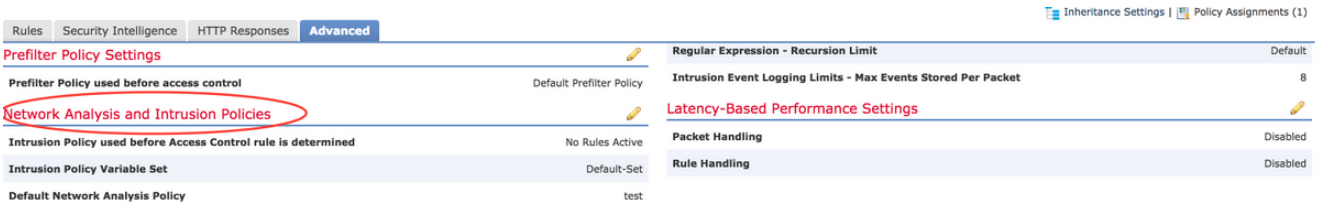
4. Expanda a **opção de configuração** e escolha a **configuração do córrego TCP**.
5. Navegue à seção de configuração e mude o valor do **intervalo** como desejado.



6. Navegue às **políticas > ao controle de acesso > ao controle de acesso**.
7. Selecione a opção **editam** para editar o a política aplicada ao dispositivo gerenciado relevante ou para criar uma política
nova.



8. Selecione o **guia avançada na** política de acesso.
9. Encontre a seção das **políticas da análise de rede e da intrusão** e clique sobre o ícone **Edit**.



10. Do menu suspenso da **política da análise de rede padrão**, escolha a política criada em etapa 2.
11. Clique a **APROVAÇÃO** e **salvar as** mudanças.
12. Clique sobre a opção **Deploy** para distribuir policia aos dispositivos manged relevantes.

Cuidado: O intervalo crescente é esperado causar uma utilização de memória mais alta, potência de fogo tem que seguir os fluxos que não são fechados por valores-limite por um tempo mais longo. O aumento real na utilização de memória é diferente para cada rede exclusiva porque depende de quanto tempo os aplicativos de rede mantêm a quietude das conexões de TCP.

Conclusão

A avaliação de desempenho de cada rede para o idle timeout das conexões de TCP é diferente. Depende completamente em cima dos aplicativos que estão no uso. Um valor ótimo deve ser estabelecido observando quanto tempo os aplicativos de rede mantêm a quietude das conexões de TCP. Para as edições que se referem o módulo de serviço da potência de fogo em Cisco ASA, quando um valor ótimo não pode ser deduzido, o intervalo pode ser ajustado aumentando o intensifica dentro ao valor de timeout do ASA.

Informações Relacionadas

- Guia de início rápido da defesa da ameaça da potência de fogo de Cisco para o ASA
- Suporte Técnico e Documentação - Cisco Systems
- Guia de início rápido da potência de fogo ASA