Configurar o recurso Cisco ASA Shun para isentar o dispositivo virtual

Contents

[Introdução](#)

[Recurso "Shun" de detecção de ameaças](#)

[Isentar o dispositivo virtual](#)

[Determine se o equipamento foi "desativado"](#)

Introdução

Este documento descreve como configurar o Cisco ASA para isentar o Virtual Appliance do componente de detecção de ameaças. O componente de detecção de ameaças do Cisco ASA executa a inspeção de pacotes no DNS e em outros protocolos. O suporte abrangente recomenda essas alterações de configuração do ASA para evitar que esse recurso entre em conflito com nosso dispositivo virtual:

- Isente o Virtual Appliance do recurso de "shun" da Threat Detection, conforme descrito neste artigo.
- Isente o Virtual Appliance da inspeção de pacotes DNS para permitir nossa criptografia DNS (DNScrypt), que é abordada neste artigo: O firewall Cisco ASA bloqueia o DNScrypt.

Recurso "Shun" de detecção de ameaças

Quando o recurso 'Shun' está habilitado, o ASA pode bloquear completamente um endereço IP de origem que aciona regras de detecção de ameaças. Mais detalhes estão no artigo da Cisco: Funcionalidade e configuração de detecção de ameaças do ASA.

O Virtual Appliance normalmente envia um número muito alto de consultas de DNS para os resolvedores de DNS Umbrella. Nos casos em que há um problema local na conexão com os resolvedores (como uma interrupção/latência temporária da rede), essas consultas podem falhar. Devido ao grande volume de consultas enviadas, mesmo uma pequena porcentagem de falhas faz com que o ASA evite o dispositivo virtual; o que leva a uma interrupção completa do DNS por um período.

Isentar o dispositivo virtual

Note: Os comandos neste artigo são indicados apenas como orientação e é recomendável consultar um especialista da Cisco antes de fazer qualquer alteração em um ambiente de produção.

Usando a CLI:

- Para isentar o IP do equipamento de ser evitado, execute este comando: **no shun**

Através da interface ASDM:

- Escolha o painel Configuration > Firewall > Threat Detection.
- Para impedir que o endereço IP do equipamento seja rejeitado, insira um endereço no campo 'Redes excluídas do bloqueio'. Você pode inserir vários endereços ou sub-redes separados por vírgulas.

Determine se o equipamento foi "desativado"

Se essas etapas não tiverem sido seguidas, o dispositivo pode se tornar "desconectado" em algumas circunstâncias, o que leva a uma interrupção de DNS.

Quando o Virtual Appliance não tem conectividade externa, o console do Cisco ASA registra o evento da seguinte maneira:

4|06 de junho de 2014 14:00:42|401004: Pacote rejeitado: 192.168.1.3 ==> 208.67.222.222 na interface interna
4|06 de junho de 2014 14:00:42|401004: Pacote perdido: 192.168.1.3 ==> 208.67.222.222 na interface interna

Para ver uma lista de endereços IP atualmente rejeitados, execute este comando no ASA: **show shun**

Para limpar imediatamente os endereços IP atualmente bloqueados, execute este comando no ASA: **clear shun**

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.