Permita o acesso ao Internet para o módulo ips ASA 5500-X

Índice

Introdução

Conforme o projeto, os módulos adaptáveis novos dos sistemas das prevenções de intrusão 5500-X da ferramenta de segurança (ASA) (IPS) não permitem o tráfego da através--caixa na porta do Gerenciamento 0/0. Consequentemente, se o IPS é ajustado para usar o endereço IP de Um ou Mais Servidores Cisco ICM NT da interface de gerenciamento do ASA como o gateway padrão, a seguir o sensor não pode ser controlado ou alcançado dos anfitriões atrás de outras relações. Também, o sensor não poderá alcançar o Internet.

Este documento explica como estabelecer os módulos ips novos ASA 5500-X para alcançar o Internet através do ASA.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Módulos ips ASA 5500-X

Componentes Utilizados

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

- Módulos ips ASA 5500-X

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 sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Caracterize a informação

Os 5512-5555 dispositivos são integrados continuamente com IPS, que é executado como um módulo de software. A relação do Gerenciamento de IPS compartilha da relação do Gerenciamento 0/0 com o ASA. Atualmente, a porta do Gerenciamento 0/0 não permite o tráfego da através--caixa no 5500-X Series ASA dos dispositivos. Esta edição impacta a acessibilidade, especialmente quando a relação do Gerenciamento 0/0 é ajustada como o gateway padrão para o IPS.

Metodologia de Troubleshooting

Pré-requisitos:

Licença de recurso IPS instalada no ASA. Isto é exigido para permitir o módulo ips. Isto pode ser verificado usando o **comando show version no** ASA. Verifique para ver se há o **módulo ips: Permitido nas saídas de versão da mostra**.

```
ASA(config)# show module

            Mod Card Type                                    Model              Serial No.
            --- -------------------------------------------- ------------------ -----------
              0 ASA 5515-X with SW, 6 GE Data, 1 GE Mgmt, AC ASA5515            FCH1549776V
            ips ASA 5515-X IPS Security Services Processor   ASA5515-IPS        FCH1549776V

            Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
            --- --------------------------------- ------------ ------------ ---------------
              0 503d.e59d.90a0 to 503d.e59d.90a7  1.0          2.1(9)8      8.6(1)
            ips 503d.e59d.909e to 503d.e59d.909e  N/A          N/A          7.1(4)E4

            Mod SSM Application Name           Status           SSM Application Version
            --- ------------------------------ ---------------- --------------------------
            ips IPS                            Up               7.1(4)E4

            Mod Status             Data Plane Status     Compatibility
            --- ------------------ --------------------- -------------
              0 Up Sys             Not Applicable
            ips Up                 Up

            Mod License Name   License Status  Time Remaining
            --- -------------- --------------- ---------------
            ips IPS Module     Enabled         perpetual
```

Solução

A fim permitir o módulo ips de alcançar o Internet (por exemplo para atualizações automáticas, a

correlação global, etc.), conecte a porta do Gerenciamento 0/0 no ASA a um dispositivo da camada 3.

Por exemplo, a porta do Gerenciamento 0/0 pode ser conectada a uma porta livre em um roteador interno ou local ao ASA. O roteador, por sua vez, pode ter o gateway padrão que aponta ao interior/interface interna do ASA. Conclua estes passos:

1. Conecte a porta do Gerenciamento 0/0 do ASA ao dispositivo da camada 3. Também, estabeleça a Conectividade entre uma interface interna do ASA e este dispositivo da camada 3.
2. Configurar o endereço IP de gerenciamento para o módulo ips. Certifique-se que este endereço está na mesma sub-rede como o endereço IP de Um ou Mais Servidores Cisco ICM NT da interface de gerenciamento ASA. No exemplo, 10.1.1.1 foi atribuído à relação Management0/0 do ASA e de 10.1.1.2 à relação do Gerenciamento de IPS.
3. Configurar o gateway padrão no módulo ips como o dispositivo da camada 3 mencionado acima. As rotas apropriadas ou o gateway padrão devem ser ajustados em conformidade no dispositivo da camada 3 para enviar o tráfego necessário ao interior/interface interna do ASA.
4. Configurar uma rota estática no ASA de modo que o tráfego de retorno alcance o módulo ips através deste dispositivo da camada 3.

Topologia:

Configuração de exemplo:

Roteador:

```
interface GigabitEthernet0/0
 ip address 192.168.1.2 255.255.255.0
 duplex auto
 speed auto
end
!
interface GigabitEthernet0/1
 ip address 10.1.1.3 255.255.255.0
 duplex auto
 speed auto
end
!
ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

ASA 5515:

```
ASA# show running-config
: Saved
:
ASA Version 8.6(1)2
!
hostname ASA
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface GigabitEthernet0/1
 nameif internet
 security-level 0
```

```
 ip address 172.16.103.73 255.255.255.0
!
interface Management0/0
 nameif management
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!
object network obj-10.0.0.0
 subnet 10.1.0.0 255.255.0.0
!
object network obj-10.0.0.0
 nat (inside,internet) dynamic interface
!
route internet 0.0.0.0 0.0.0.0 172.16.103.64 1
!--- Route configured to reach the ips module through the internal router route inside 10.1.1.2
255.255.255.255 192.168.1.2 1
```

ASA 5515-IPS:

```
sensor#show configuration
! ------------------------------
! Current configuration last modified Sun Sep 18 00:06:25 2012
! ------------------------------
! Version 7.1(4)! Host:
!     Realm Keys          key1.0
! Signature Definition:!     Signature Update    S615.0   2012-01-03
! ------------------------------
service interface
exit
! ------------------------------
service authentication
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service host
network-settings
!--- The management IP address is set. host-ip 10.1.1.2/24,10.1.1.3 !--- The access-list is set
to allow management from the 10.0.0.0/8 network. access-list 10.0.0.0/8 dns-primary-server
enabled !--- The DNS server IP address is set. address 8.8.8.8 exit exit exit
```

Um pedido da característica foi levantado permitir o tráfego da através--caixa na porta do Gerenciamento 0/0 para o IPS.

Os detalhes podem ser encontrados aqui: Identificação de bug Cisco CSCua67798 (clientes registrados somente): ENH ASA 5500-X - Para permitir o tráfego da através--caixa na porta de gerenciamento

FAQ

P: Eu não tenho um dispositivo da camada 3 dentro do ponto da rede o gateway padrão a. Como pode o IPS alcançar o Internet?

R: Refira este documento para outros projetos: /c/en/us/support/docs/security/ips-sensor-software-version-71/113690-ips-config-mod-00.html.

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems