O ASA configurado como um servidor DHCP não permite que os anfitriões adquiram um endereço IP de Um ou Mais Servidores Cisco ICM NT

Índice

Introdução

Este documento descreve um problema de configuração específico que possa fazer com que os anfitriões sejam incapazes de adquirir um endereço IP de Um ou Mais Servidores Cisco ICM NT da ferramenta de segurança adaptável de Cisco (ASA) com DHCP.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada na versão de software 8.2.5 ASA.

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.

Problema

Com o ASA configurado como um servidor DHCP, os anfitriões são incapazes de adquirir um endereço IP de Um ou Mais Servidores Cisco ICM NT.

O ASA é configurado como um servidor DHCP em duas relações: VLAN 6 (interface interna) e VLAN10 (relação DMZ2). Os PC naqueles VLAN não podem com sucesso obter um endereço IP de Um ou Mais Servidores Cisco ICM NT do ASA através do DHCP.

- A configuração de DHCP está correta.
- Nenhum Syslog é gerado pelo ASA que indica a causa do problema.
- As capturas de pacote de informação tomadas no ASA mostram somente a chegada do pacote DHCP DISCOVER. O ASA não responde para trás com um pacote da OFERTA.

Os pacotes são deixados cair pelo trajeto acelerado da Segurança (ASP), e uma captação aplicada ao ASP indica que os pacotes DHCP DISCOVER são deixados cair devido de “às verificações de segurança Slowpath falhadas: ”

```
ASA# capture asp type asp-drop all
ASA# show capture asp

3 packets captured
1: 14:57:05.627241 802.1Q VLAN#10 P0 0.0.0.0.68 > 255.255.255.255.67:
udp 300 Drop-reason: (sp-security-failed) Slowpath security checks failed
2: 14:57:08.627286 802.1Q VLAN#10 P0 0.0.0.0.68 > 255.255.255.255.67:
udp 300 Drop-reason: (sp-security-failed) Slowpath security checks failed
3: 14:57:16.626966 802.1Q VLAN#10 P0 0.0.0.0.68 > 255.255.255.255.67:
udp 300 Drop-reason: (sp-security-failed) Slowpath security checks failed
```

Solução

A configuração contém uma indicação larga da tradução de endereço da rede estática (NAT) que abranja todo o tráfego IP nessa sub-rede. Os pacotes DHCP DISCOVER da transmissão (destinados a 255.255.255.255) combinam esta declaração NAT que causa a falha:

```
static (DMZ1,DMZ2) 0.0.0.0 0.0.0.0 netmask 0.0.0.0
```

Se você remove a declaração NAT incorretamente configurada, resolve o problema.

Informações adicionais

Se você usa a utilidade do pacote-projétil luminoso no ASA para simular o pacote DHCP DISCOVER que incorpora a relação DMZ2, o problema pode ser identificado como causado pela configuração de NAT:

```
tutera-firewall#packet-tracer input DMZ2 udp 0.0.0.0 68 255.255.255.255 67 detail
.....
Phase: 2
Type: UN-NAT
Subtype: static
Result: ALLOW
Configuration:
static (DMZ1,DMZ2) 0.0.0.0 0.0.0.0 netmask 0.0.0.0
match ip DMZ1 any DMZ2 any
```

```
static translation to 0.0.0.0
translate_hits = 0, untranslate_hits = 641
Additional Information:
NAT divert to egress interface DMZ1
Untranslate 0.0.0.0/0 to 0.0.0.0/0 using netmask 0.0.0.0
Result:
input-interface: DMZ2
input-status: up
input-line-status: up
output-interface: DMZ1
output-status: up
output-line-status: up
Action: drop
Drop-reason: (sp-security-failed) Slowpath security checks failed
```