L'ASA configurée comme serveur DHCP ne permet pas à des hôtes pour saisir une adresse IP

Contenu

Introduction

Ce document décrit un problème spécifique de configuration qui peut rendre des hôtes saisir une adresse IP de l'appliance de sécurité adaptable Cisco (ASA) avec le DHCP.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur la version de logiciel 8.2.5 ASA.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Problème

L'ASA étant configuré comme serveur DHCP, les hôtes ne peuvent pas saisir une adresse IP.

L'ASA est configurée comme serveur DHCP sur deux interfaces : VLAN 6 (interface interne) et VLAN 10 (interface DMZ2). Les PC sur ces VLAN ne peuvent pas avec succès obtenir une adresse IP de l'ASA par l'intermédiaire du DHCP.

- La configuration DHCP est correcte.
- Aucun Syslog n'est généré par l'ASA qui indiquent la cause du problème.
- Les captures de paquet prises sur l'exposition ASA seulement l'arrivée du DHCP DÉCOUVRENT le paquet. L'ASA ne répond pas de retour avec un paquet d'OFFRE.

Les paquets sont lâchés par le chemin accéléré de Sécurité (ASP), et une capture appliquée à l'ASP indique que le DHCP DÉCOUVRENT des paquets sont dû abandonné « aux contrôles de Sécurité de Slowpath a manqué : "

```
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
```

Solution

La configuration contient une large déclaration (NAT) de traduction d'adresses de réseau statique qui entoure tout le trafic IP sur ce sous-réseau. Le DHCP d'émission DÉCOUVRENT la correspondance de paquets (destinés à 255.255.255.255) cette déclaration NAT qui entraîne la panne :

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

Si vous retirez la déclaration NAT inexactement configurée, elle résout le problème.

Informations supplémentaires

Si vous employez l'utilitaire de traceur de paquets sur l'ASA pour simuler le DHCP DÉCOUVREZ le paquet qui écrit l'interface DMZ2, le problème peut être identifié comme provoqué par la configuration 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
```