ASA configuré en tant que serveur DHCP ne permet pas aux hôtes d'acquérir une adresse IP

Contenu

Introduction

Ce document décrit un problème de configuration spécifique qui peut empêcher les hôtes d'obtenir une adresse IP de l'appliance de sécurité adaptative (ASA) Cisco avec DHCP.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Problème

Avec l'ASA configuré en tant que serveur DHCP, les hôtes ne peuvent pas acquérir d'adresse IP.

L'ASA est configuré en tant que serveur DHCP sur deux interfaces : VLAN 6 (interface interne) et VLAN 10 (interface DMZ2). Les PC de ces VLAN ne peuvent pas obtenir d'adresse IP de l'ASA

via DHCP.

- La configuration DHCP est correcte.
- Aucun syslog n'est généré par l'ASA qui indique la cause du problème.
- Les captures de paquets prises sur l'ASA indiquent uniquement l'arrivée du paquet DHCP DISCOVER. L'ASA ne répond pas avec un paquet OFFER.

Les paquets sont abandonnés par le chemin de sécurité accéléré (ASP), et une capture appliquée à l'ASP indique que les paquets DHCP DISCOVER sont abandonnés en raison de l'échec des vérifications de sécurité du chemin lent :

```
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 instruction NAT (Network Address Translation) statique étendue qui englobe tout le trafic IP sur ce sous-réseau. Les paquets de diffusion DHCP DISCOVER (destinés à 255.255.255.255) correspondent à cette instruction NAT qui provoque l'échec :

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

Si vous supprimez l'instruction NAT mal configurée, elle résout le problème.

Additional Information

Si vous utilisez l'utilitaire packet-tracer sur l'ASA pour simuler le paquet DHCP DISCOVER qui entre dans l'interface DMZ2, le problème peut être identifié comme étant dû à 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
```