

DHCP مداخلك هنيوكت مت يذلا ASA حمسي ال IP ناووع باستكاب ني في ضم لل

المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [المشكلة](#)
- [الحل](#)
- [معلومات إضافية](#)

المقدمة

يصف هذا المستند مشكلة تكوين معينة يمكن أن تسبب في عدم قدرة الأجهزة المضيفة على تكوين عنوان IP من جهاز الأمان القابل للتكيف (ASA) من Cisco باستخدام DHCP.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى برنامج ASA، الإصدار 8.2.5.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

المشكلة

مع تكوين ASA كخادم DHCP، لا يمكن للمضيفين الحصول على عنوان IP.

تم تكوين ASA كخادم DHCP على واجهتين: VLAN 6 (داخل الواجهة) و VLAN 10 (واجهة DMZ2). لا يمكن لأجهزة الكمبيوتر الموجودة على شبكات VLAN هذه الحصول على عنوان IP بنجاح من ASA عبر DHCP.

- تكوين DHCP صحيح.
- لا يتم إنشاء أي syslogs بواسطة ASA الذي يشير إلى سبب المشكلة.
- تظهر التقاط الحزم التي تم التقاطها على ASA فقط وصول حزمة اكتشاف DHCP. لا يرد ASA مع حزمة عرض.
- يتم إسقاط الحزم من خلال مسار الأمان السريع (ASP)، ويشير التقاط يتم تطبيقه على ASP إلى إسقاط حزم اكتشاف DHCP بسبب "فشل عمليات التحقق من أمان المسار البطيء".

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

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

الحل

يحتوي التكوين على عبارة ترجمة عنوان الشبكة (NAT) الثابتة الواسعة التي تشمل جميع حركة مرور IP على هذه الشبكة الفرعية. البث DHCP اكتشاف الحزم (الموجهة إلى 255.255.255.255) تطابق عبارة NAT هذه التي تتسبب في الفشل:

```
static (DMZ1,DMZ2) 0.0.0.0 0.0.0.0 netmask 0.0.0.0
إن يزيل أنت ال nat تشكيل غير صحيح، هو يحل المشكلة.
```

معلومات إضافية

إذا كنت تستخدم الأداة المساعدة Packet-tracer على ASA لمحاكاة حزمة اكتشاف DHCP التي تدخل واجهة DMZ2، يمكن تحديد المشكلة كما هو بسبب تكوين 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

