ASA: El acceso entrante a los direccionamientos NAT falla después de la actualización a 8.4(3)

Contenido

Introducción

Este documento proporciona información sobre las direcciones NAT que fallan después de actualizar Adaptive Security Appliance (ASA) a la versión 8.4(3). Este documento también proporciona una resolución a este problema.

prerrequisitos

Requisitos

Los Quien lea este documento deben tener conocimiento de estos temas.

- Comprensión básica del concepto de Address Resolution Protocol (ARP) y de proxy ARP

Componentes Utilizados

La información en este documento se basa en estas versiones de software y hardware.

- Cualquier dispositivo de seguridad adaptante de las 5500 Series de Cisco ASA
- Versión 8.4(3) o posterior adaptante del dispositivo de seguridad

Convenciones

Para obtener más información sobre las convenciones del documento, consulte Convenciones de Consejos Técnicos de Cisco.

Síntomas

Comenzando con la Versión de ASA 8.4(3), el ASA no responde a los pedidos ARP recibidos en una interfaz, para los IP Addresses que no son la subred IP parte de una esa interfaz. Antes de la versión 8.4(3), el ASA respondería a los pedidos ARP que no estaban en la subred IP de la interfaz ASA.

Este cambio puede manifestarse inmediatamente después de actualizar el ASA a la versión 8.4(3). En algunos casos, los usuarios de Internet no pueden conectar con la dirección global de un servidor traducido con el ASA.

Se visualiza este mensaje si se encuentra esta situación, y el “debug arp” se habilita en el CLI ASA:

```
arp-in: Arp packet received from 192.168.10.1 which is in different subnet
than the connected interface 192.168.11.1/255.255.255.0
```

La causa raíz de este problema no es un bug. Vea la información abajo para aprender más sobre las causas y las soluciones potenciales al problema.

Condiciones/entorno

Para encontrar esta situación, el ASA debe recibir un pedido ARP para una dirección IP que haga juego a una dirección global en una traducción de NAT configurada. El IP Address global debe residir en una subred IP que sea diferente de la subred IP configurada en la interfaz ASA.

Causa/descripción de problemas

Para entender las ramificaciones completas de este problema, es importante conseguir una comprensión completa de cómo este problema puede aparecer y la mejor manera de atenuar el problema.

Éstos son algunos casos donde esta situación puede ser encontrada:

El dispositivo ascendente tiene rutas de IP configuradas sin el IP Address de Next Hop

Ésta es probablemente la mayoría de la causa común de esta situación. Es debido a una configuración no óptima de un dispositivo ascendente. Se prefiere para configurar las rutas de IP tales que el salto siguiente de la ruta de IP es una dirección IP en la misma subred como direccionamiento de esa interfaz:

```
ip route 10.1.2.0 255.255.255.0 192.168.1.2
```

Sin embargo, los administradores de la red configuran a veces una interfaz en vez de una dirección IP como el salto siguiente:

```
ip route 10.1.2.0 255.255.255.0 FastEthernet0/1
```

Esto hace al router rutear el tráfico destinado a la red 10.1.2.0/24 a la interfaz del FastEthernet0/1, y envía un pedido ARP para el IP Address de destino en el paquete del IP. Se asume que un poco de dispositivo responderá al pedido ARP, y el router entonces adelante el paquete a la dirección MAC que era resuelto debido al proceso ARP. Las ventajas de los este tipos de configuración son que es muy fácil configurar y administrar. El administrador no tiene que

explícitamente configurar un IP Address de Next Hop para la ruta, y asumen que un dispositivo adyacente tendrá Proxy-arp habilitado y responderá al pedido ARP si es capaz de la encaminamiento los paquetes al IP Address de destino.

Sin embargo, hay problemas graves con este tipo de configuración de la ruta de IP:

- Enviando un pedido ARP de determinar el salto siguiente para el tráfico IP, exponen al router a los problemas causados por los otros dispositivos que pudieron responder incorrectamente a ese pedido ARP. El resultado es tráfico puede negro-ser agujereado cuando está enviado a un dispositivo incorrecto.
- La ruta hará el dispositivo enviar un pedido ARP para cada dirección destino única en los paquetes que hacen juego la ruta. Esto puede causar una gran cantidad de tráfico ARP en la subred y afectar negativamente al funcionamiento así como al espacio de memoria requerido para llevar a cabo potencialmente una gran cantidad de entradas ARP.
- Porque el espacio de la tabla ARP es un recurso encuadernado de la memoria, una cantidad excesiva de entradas puede afectar negativamente el funcionamiento del router y stabilty.

Por lo tanto, la mejor práctica es configurar todas las rutas con IP explícita las direcciones del salto siguiente y no utilizar las rutas que tienen un nombre de la interfaz en sí mismo para identificar la interfaz saliente. Si la interfaz es necesaria atar la ruta a la interfaz de egreso para la Conmutación por falla, ingrese el nombre de la interfaz de egreso y el salto siguiente en la Static ruta.

Dado las implicaciones administrativas para algunos clientes de Cisco, un pedido de mejora se ha abierto para hacer el nuevo comportamiento seguro configurable: Id. de bug Cisco CSCty95468 (clientes registrados solamente) (ENH: Comando Add de permitir las entradas de memoria caché ARP de las subredes NON-conectadas).

Máscaras unidas mal de la subred IP en los dispositivos adyacentes

Las máscaras unidas mal de la subred IP configuradas en la interfaz ASA y la interfaz de dispositivo adyacente pueden causar una situación similar. Si el dispositivo adyacente tenía una máscara de subred que era un supernet (255.255.240.0) de la máscara de subred IP de la interfaz ASA (255.255.255.0), el dispositivo adyacente ARP para los IP Addresses que no está en la subred IP de la interfaz ASA. Asegúrese de que las máscaras de subred estén correctas.

Implicaciones del modo transparente

Otro efecto secundario de este cambio es la incapacidad para aprender las direcciones MAC de las subredes NON-directo-conectadas en el modo transparente. Esto afecta a la comunicación en estos escenarios:

- El ASA transparente no tiene un IP Address de administración configurado o la configuración es incorrecta.
- El ASA transparente está utilizando las subredes secundarias en el mismo segmento.

No hay solución alternativa para este problema en el modo transparente con excepción del downgrade. Sin embargo, este pedido de mejora se ha abierto para hacer que el ASA interopera con las subredes secundarias en el modo transparente: Id. de bug Cisco CSCty49855 (clientes registrados solamente) (ENH: Host conectados del soporte no directamente en el mecanismo de detección MAC).

Resolución

La solución a este problema (en caso de que la dirección IP en la pregunta no está en la misma subred de la capa 3 que el IP de la interfaz ASA) es realizar los cambios necesarios asegurarse de que los dispositivos adyacente al tráfico de la ruta ASA directamente a la dirección IP de la interfaz ASA como el dispositivo de Next Hop, en vez de la confianza en un dispositivo al Proxy-arp en nombre de la dirección IP.

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems