ASA: O acesso de entrada aos endereços NAT falha após a elevação a 8.4(3)

Índice

Introdução

Este documento fornece a informação sobre os endereços NAT que falham após ter promovido a ferramenta de segurança adaptável (ASA) à versão 8.4(3). Este documento igualmente fornece uma definição a esta edição.

Pré-requisitos

Requisitos

Os leitores deste documento devem ter o conhecimento destes assuntos.

- Compreensão básica do conceito do Address Resolution Protocol (ARP) e do proxy ARP

Componentes Utilizados

A informação neste documento é baseada nestes versão de hardware e software.

- Alguma ferramenta de segurança adaptável do 5500 Series de Cisco ASA
- Versão 8.4(3) ou mais recente adaptável da ferramenta de segurança

Convenções

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Sintomas

Começando com versão ASA 8.4(3), o ASA não responde às requisições ARP recebidas em uma relação, para os endereços IP de Um ou Mais Servidores Cisco ICM NT que não são sub-rede IP parte de uma essa relação. Antes da versão 8.4(3), o ASA responderia às requisições ARP que não estavam na sub-rede IP da relação do ASA.

Esta mudança pode manifestar-se imediatamente depois de promover o ASA à versão 8.4(3). Em alguns casos, os usuários do Internet não podem conectar ao endereço global de um server traduzido com o ASA.

Esta mensagem é indicada se esta situação é encontrada, e “debugar o arp” está permitido no CLI do 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
```

A causa de raiz desta edição não é um erro. Veja a informação abaixo para aprender mais sobre causas e soluções potenciais à edição.

Circunstâncias/ambiente

A fim encontrar esta situação, o ASA deve receber uma requisição ARP para um endereço IP de Um ou Mais Servidores Cisco ICM NT que combine um endereço global em uma tradução NAT configurada. O endereço IP global deve residir em uma sub-rede IP que seja diferente da sub-rede IP configurada na relação do ASA.

Causa/descrição do problema

A fim compreender as ramificação completas desta edição, é importante obter uma compreensão completa de como esta edição pode aparecer e a melhor maneira abrandar o problema.

Estes são alguns exemplos onde esta situação pode ser encontrada:

O dispositivo ascendente tem as rotas IP configuradas sem o endereço IP do próximo salto

Esta é provavelmente a maioria de causa comum desta situação. É devido a uma configuração não-otimizados de um dispositivo ascendente. Prefere-se configurar rotas IP tais que o salto seguinte da rota IP é um endereço IP de Um ou Mais Servidores Cisco ICM NT na mesma sub-rede como o endereço dessa relação:

```
ip route 10.1.2.0 255.255.255.0 192.168.1.2
```

Contudo, às vezes os administradores de rede configuram uma relação em vez de um endereço IP de Um ou Mais Servidores Cisco ICM NT como o salto seguinte:

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

Isto faz com que o roteador distribua o tráfego destinado à rede 10.1.2.0/24 à relação do FastEthernet0/1, e envia uma requisição ARP para o endereço IP de destino no pacote IP. Supõe-se que algum dispositivo responderá à requisição ARP, e o roteador então para a frente o pacote ao MAC address que era resolved devido ao processo ARP. Os benefícios do este tipo de configuração são que é muito fácil configurar e administrar. O administrador não tem que

explicitamente configurar um endereço IP de Um ou Mais Servidores Cisco ICM NT do salto seguinte para a rota, e supõem que um dispositivo adjacente terá o Proxy-arp permitido e responderá à requisição ARP se é capaz do roteamento os pacotes ao endereço IP de destino.

Contudo, há uns problemas graves com este tipo de configuração da rota IP:

- Enviando uma requisição ARP determinar o salto seguinte para o tráfego IP, o roteador é exposto aos problemas causados pelos outros dispositivos que puderam incorretamente responder a essa requisição ARP. O resultado é tráfego pode preto-ser furado quando enviado a um dispositivo incorreto.
- A rota fará com que o dispositivo envie uma requisição ARP para cada endereço de destino original nos pacotes que combinam a rota. Isto pode causar uma grande quantidade de tráfego ARP na sub-rede e negativamente afetar o desempenho assim como o espaço de memória exigido para guardar potencialmente uma grande quantidade de entradas de ARP.
- Porque o espaço da tabela ARP é um recurso encadernado da memória, um número excessivo de entradas pode negativamente impactar o desempenho do roteador e stabilty.

Consequentemente, o melhor prática é configurar todas as rotas com endereços de próximo salto do IP explícito e não usar as rotas que têm um nome da relação por si só para identificar a interface enviada. Se a relação é precisada de amarrar a rota à interface de saída para o Failover, incorpore o nome da interface de saída e o salto seguinte à rota estática.

Dado as implicações administrativas para alguns clientes Cisco, uma requisição de aprimoramento foi aberta a fim fazer o comportamento seguro novo configurável: Identificação de bug Cisco CSCty95468 (clientes registrados somente) (ENH: Comando Add permitir entradas de cache ARP das sub-redes NON-conectadas).

Máscaras de sub-rede combinadas mal IP em dispositivos adjacentes

As máscaras de sub-rede combinadas mal IP configuradas na relação do ASA e na relação de dispositivo adjacente podem causar uma situação similar. Se o dispositivo adjacente teve uma máscara de sub-rede que fosse uns super-rede (255.255.240.0) da máscara de sub-rede IP da relação do ASA (255.255.255.0), o dispositivo adjacente ARP para os endereços IP de Um ou Mais Servidores Cisco ICM NT que não estão na sub-rede IP da relação ASA. Assegure-se de que as máscaras de sub-rede estejam corretas.

Implicações do modo transparente

Um outro efeito secundário desta mudança é a incapacidade aprender endereços MAC das sub-redes NON-direto-conectadas no modo transparente. Isto afeta uma comunicação nestas encenações:

- O ASA transparente não tem um endereço IP de gerenciamento configurado ou a configuração está incorreta.
- O ASA transparente está usando sub-redes secundárias no mesmo segmento.

Não há nenhuma ação alternativa para esta edição no modo transparente a não ser o downgrade. Contudo, esta requisição de aprimoramento foi aberta a fim fazer o interoperam ASA com sub-redes secundárias no modo transparente: Identificação de bug Cisco CSCty49855 (clientes registrados somente) (ENH: Host conectados do apoio não diretamente no mecanismo de descoberta MAC).

Resolução

A solução a este problema (no caso em que o endereço IP de Um ou Mais Servidores Cisco ICM NT na pergunta não está na mesma sub-rede da camada 3 que o IP da relação do ASA) é fazer as mudanças necessárias assegurar-se de que os dispositivos junto ao ASA distribuam o tráfego diretamente ao endereço IP de Um ou Mais Servidores Cisco ICM NT da relação do ASA como o dispositivo do salto seguinte, em vez da confiança em um dispositivo ao Proxy-arp em nome do endereço IP de Um ou Mais Servidores Cisco ICM NT.

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems