Ejemplo de Configuración de DNS Doctoring en ASA

Contenido

Introducción

Este documento muestra cómo se utiliza el Doctorado DNS en el Dispositivo de seguridad adaptable (ASA) para cambiar las direcciones IP incrustadas en las respuestas del Sistema de nombres de dominio (DNS) para que los clientes puedan conectarse a la dirección IP correcta de los servidores.

Prerequisites

Requirements

El Doctorado de DNS requiere la configuración de la traducción de direcciones de red (NAT) en el ASA, así como la habilitación de la inspección de DNS.

Componentes Utilizados

La información de este documento se basa en Adaptive Security Appliance.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). If your network is live, make sure that you understand the potential impact of any command.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las

convenciones del documento.

Ejemplos de DNS Doctoring

Servidor DNS en el interior de ASA

Figure 1

```
nat (inside,outside) source static 10.1.1.100 198.51.100.100 dns
!
policy-map global_policy
  class inspection_default
    inspect dns
```

En la Figura 1, el administrador local controla el servidor DNS. El servidor DNS debe entregar una dirección IP privada, que es la dirección IP real asignada al servidor de aplicaciones. Esto permite que el cliente local se conecte directamente al servidor de aplicaciones.

Desafortunadamente, el cliente remoto no puede acceder al servidor de aplicaciones con la dirección privada. Como resultado, el Doctorado DNS se configura en el ASA para cambiar la dirección IP integrada dentro del paquete de respuesta DNS. Esto garantiza que cuando el cliente remoto realiza una solicitud DNS para www.abc.com, la respuesta que obtiene es para la dirección traducida del servidor de aplicaciones. Sin la palabra clave DNS en la instrucción NAT, el cliente remoto intenta conectarse a 10.1.1.100, lo que no funciona porque esa dirección no se puede enrutar en Internet.

Servidor DNS en el exterior del ASA

Figure 2

```
nat (inside,outside) source static 10.1.1.100 198.51.100.100 dns
!
policy-map global_policy
  class inspection_default
    inspect dns
```

En la Figura 2, el servidor DNS es controlado por el ISP o un proveedor de servicios similar. El servidor DNS debe distribuir la dirección IP pública, es decir, la dirección IP traducida del servidor de aplicaciones. Esto permite a todos los usuarios de Internet acceder al servidor de aplicaciones a través de Internet.

Desafortunadamente, el cliente local no puede acceder al servidor de aplicaciones con la dirección pública. Como resultado, el Doctorado DNS se configura en el ASA para cambiar la

dirección IP integrada dentro del paquete de respuesta DNS. Esto garantiza que cuando el cliente local realice una solicitud DNS para www.abc.com, la respuesta recibida sea la dirección real del servidor de aplicaciones. Sin la palabra clave DNS en la instrucción NAT, el cliente local intenta conectarse a 198.51.100.100. Esto no funciona porque este paquete se envía al ASA, que descarta el paquete.

VPN NAT y DNS Doctoring

Figure 3

Piense en una situación en la que hay redes que se solapan. En esta condición, la dirección 10.1.1.100 vive tanto en el lado remoto como en el lado local. Como resultado, debe realizar NAT en el servidor local para que el cliente remoto pueda seguir accediendo a él con la dirección IP 192.1.1.100. Para que esto funcione correctamente, es necesario el Doctorado DNS.

No se puede realizar el Doctorado DNS en esta función. La palabra clave DNS sólo se puede agregar al final de un objeto NAT o NAT de origen. La NAT de dos veces no admite la palabra clave DNS. Hay dos configuraciones posibles y ambas fallan.

Error de configuración 1: Si configura la línea de fondo, traduce 10.1.1.1 a 192.1.1.1, no sólo para el cliente remoto, sino para todos los usuarios de Internet. Dado que 192.1.1.1 no es enrutable a Internet, nadie en Internet puede acceder al servidor local.

```
nat (inside,outside) source static 10.1.1.100 192.168.1.100 dns
nat (inside,outside) source static 10.1.1.100 192.168.1.100 destination
   REMOTE_CLIENT REMOTE_CLIENT
```

Error de configuración 2: Si configura la línea NAT de DNS Doctoring después de la línea NAT doble necesaria, esto provoca una situación en la que el DNS Doctoring nunca funciona. Como resultado, el cliente remoto intenta acceder a www.abc.com con la dirección IP 10.1.1.100, que no funciona.

```
nat (inside,outside) source static 10.1.1.100 192.168.1.100 destination
   REMOTE_CLIENT REMOTE_CLIENT
nat (inside,outside) source static 10.1.1.100 64.1.1.100 dns
```

Información Relacionada

- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco ASA 5500 Series Adaptive Security Appliances > Descargas de software
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).