Configuración del acceso a recursos internos para usuarios de VPN en FTD con tráfico HairPin

Contenido

Problema

El objetivo es permitir el acceso completo de los usuarios de VPN a los recursos de la red interna después de la autenticación VPN correcta mediante RADIUS (en un servidor unido a un dominio de Windows) en Cisco Secure Firewall FTD.

La configuración de VPN ya está operativa; los usuarios pueden descargar e instalar el cliente VPN y autenticarse correctamente. El problema se centra en configurar el control de acceso necesario y las reglas NAT para permitir el acceso de recursos internos necesario a través de VPN.

Entorno

- Producto: Cisco Secure Firewall Firepower (FTD), versión 7.6.0 (como un dispositivo CSF1220CX)
- Gestión: FirePOWER Management Center (FMC), FMC en la nube (cdFMC) o Firepower Device Manager (FDM)
- VPN: se configura con autenticación RADIUS en un servidor conectado a un dominio (NPS) de Windows
- Grupo de direcciones VPN: 192.168.250.1 - 192.168.250.200
- Ejemplo de subred interna de destino: 192.168.95.0/24
- Versión del software: 9.2.1 (como se indica en el flujo de trabajo)
- Interfaces relevantes: interfaz 'externa' para entrada de VPN
- Se requiere acceso a RDP y Active Directory a través de una conexión VPN

Resolución

Estos pasos detallan la configuración necesaria para permitir que los usuarios de VPN accedan a los recursos internos (como RDP y Active Directory) en Cisco FTD. Esto incluye la creación de reglas de política de acceso, la configuración de exenciones de NAT y conexiones entre nodos NAT para el tráfico VPN, y el uso de comandos de solución de problemas para validar la configuración.

Paso 1: Agregue una entrada de lista de acceso para permitir que el conjunto de direcciones VPN

acceda a los recursos internos.

```
access-list CSM_FW_ACL_ advanced permit ip object VPN_Pool any rule-id 268438528
access-list CSM_FW_ACL_ remark rule-id 268438528: ACCESS POLICY: Default Access Control Policy - Mandat
access-list CSM_FW_ACL_ remark rule-id 268438528: L7 RULE: Permit_VPN_Pool
```

Paso 2: Agregue una regla de lista de acceso para permitir que los recursos internos envíen tráfico de retorno al grupo VPN:

```
access-list CSM_FW_ACL_ advanced permit ip any object VPN_Pool
```

Estas reglas se pueden endurecer posteriormente para restringir fuentes y destinos específicos según sea necesario.

Paso 3: Configure NAT Exemption o Hairpin NAT para el Tráfico VPN

Existen dos enfoques comunes:

- ◦ Opción A: exención de NAT para el grupo VPN a la subred interna

```
nat (outside,inside) source static VPN_Pool VPN_Pool destination static Net_192.168.95.1-24 Net_192.168
```

- ◦ Opción B: Hairpin NAT for VPN Pool on Same Interface (no-proxy-arp)

```
nat (any,any) source static VPN_Pool VPN_Pool no-proxy-arp
```

- ◦ Opción C: NAT de horquilla dinámica para grupo VPN en interfaz externa

```
nat (outside,outside) dynamic VPN_Pool interface
```

El método correcto depende de si los recursos internos están en la misma interfaz física (requiere NAT de horquilla) o en interfaces diferentes (exención de NAT).

Paso 4: Utilice el comando `packet-tracer` para simular los flujos de tráfico del grupo VPN a los recursos internos y validar si el tráfico está permitido por la regla, NAT y ruta deseada.

```
packet-tracer input outside icmp 192.168.250.1 8 0 192.168.95.1
packet-tracer input outside tcp 192.168.250.1 12345 192.168.95.1 80
packet-tracer input inside icmp 192.168.95.1 8 0 192.168.250.1
packet-tracer input inside tcp 192.168.250.1 54321 192.168.95.1 443
--
Phase 5
ID: 5
Type: ACCESS-LIST
Result: ALLOW
Config: access-group CSM_FW_ACL_ globalaccess-list CSM_FW_ACL_ advanced permit ip object VPN_Pool any r
Additional Information:  This packet will be sent to snort for additional processing where a verdict wi
Elapsed Time: 0 ns
--
Phase 7
ID: 7
Type: NAT
Result: ALLOW
Config: nat (outside,outside) dynamic VPN_Pool interface
Additional Information: Static translate 192.168.250.1/12345 to 192.168.250.1/12345 Forward Flow based
Elapsed Time: 0 ns
```

Nota: El resultado del rastreador de paquetes para la fase WebVPN podría mostrar un "DROP" para el tráfico VPN en la interfaz externa. Este comportamiento se espera para el tráfico de texto sin formato en la interfaz externa y todavía se puede utilizar para validar NAT.

Notas complementarias

- Es posible que las capturas de paquetes en la interfaz de usuario de Threat Defence solo muestren las solicitudes entrantes. Si no se observan caídas, pero el tráfico no llega al recurso interno, verifique las reglas de la lista de acceso y NAT.
- Cuando SSH no está disponible, toda la resolución de problemas se puede realizar a través de las funciones de la interfaz de usuario de Threat Defence en cdFMC, pero el uso del comando es limitado.
- Es posible que se necesiten algunas modificaciones en los dispositivos adyacentes para la conectividad de extremo a extremo.

Causa

La causa raíz fue una política de acceso y una configuración de NAT insuficientes para el tráfico del conjunto VPN a interno y entre interno y VPN. La configuración predeterminada no permitía una comunicación bidireccional completa desde el grupo VPN a los recursos internos y hacia atrás, ni manejaba los requisitos de NAT de horquilla para la entrada y salida del tráfico en la misma interfaz.

Contenido relacionado

- Configuración de la exención de NAT en FTD
- Soporte técnico y descargas de Cisco

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).