Fase 3 de Troubleshooting de Trayectoria de Datos de Firepower: Inteligencia de seguridad

Contenido

Introducción

Este artículo forma parte de una serie de artículos que explican cómo resolver sistemáticamente los problemas de la ruta de datos en sistemas Firepower para determinar si los componentes de Firepower pueden estar afectando al tráfico. Consulte el artículo Descripción general para obtener información sobre la arquitectura de las plataformas Firepower y los enlaces a otros artículos de Troubleshooting de Trayectoria de Datos.

En este artículo se describe la tercera etapa de la solución de problemas de la ruta de datos de Firepower, la función de inteligencia de seguridad.

Prerequisites

- Este artículo pertenece a todas las plataformas Firepower soportadas actualmente
- La inteligencia de seguridad para URL y DNS se introdujo en la versión 6.0.0

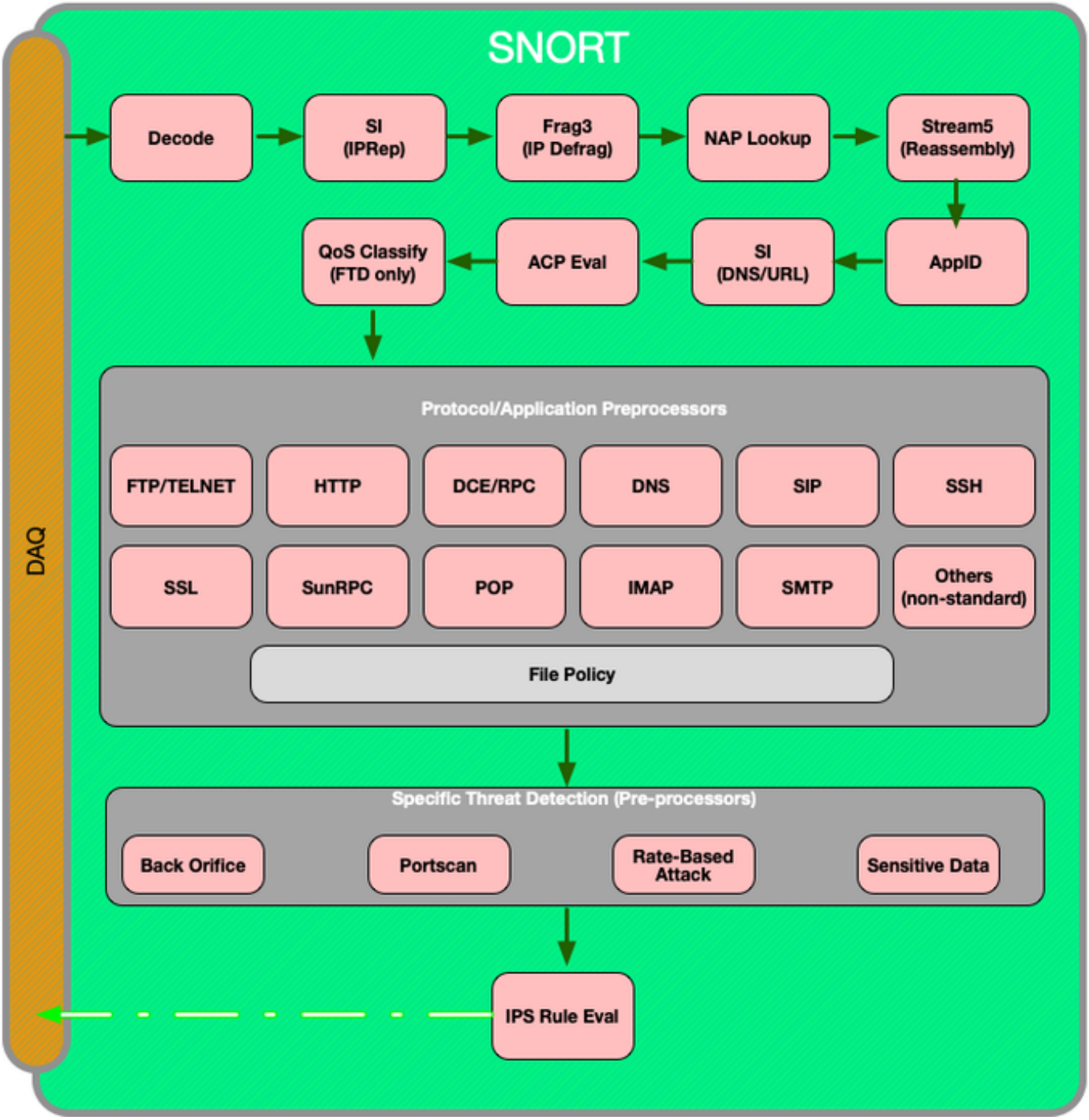
Solución de problemas de la fase de inteligencia de seguridad Firepower

La inteligencia de seguridad es una función que realiza una inspección tanto de listas negras como de listas blancas para:

- Direcciones IP (también conocidas como "Redes" en determinadas partes de la interfaz de usuario)
- Localizadores uniformes de recursos (URL)
- Consultas del sistema de nombres de dominio (DNS)

Las listas de la inteligencia de seguridad se pueden rellenar con fuentes proporcionadas por Cisco o con listas y fuentes configuradas por el usuario.

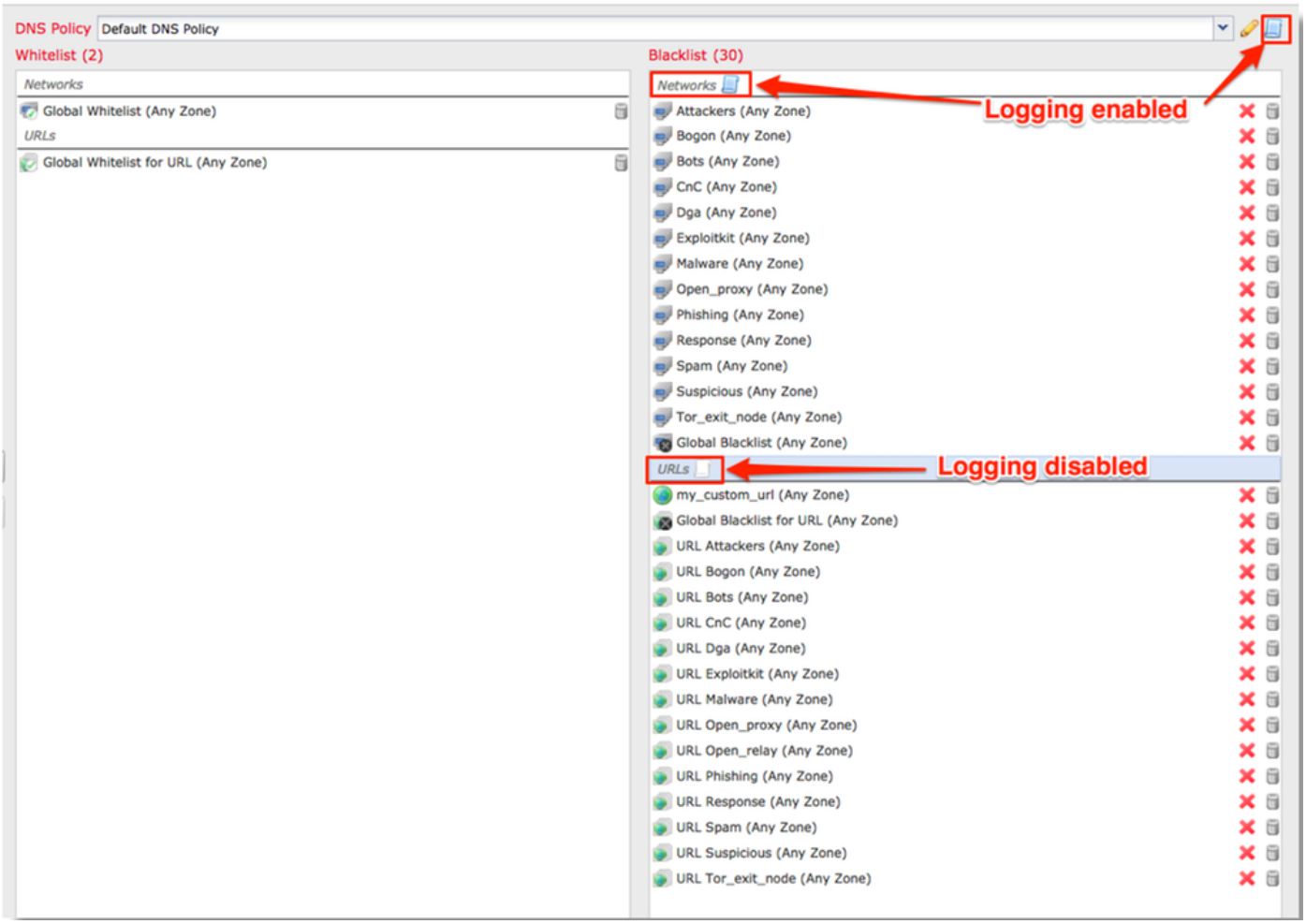
La reputación de la inteligencia de seguridad basada en direcciones IP es el primer componente de Firepower que inspecciona el tráfico. La inteligencia de seguridad de DNS y URL se realiza tan pronto como se detecta el protocolo de aplicación relevante. A continuación se muestra un diagrama que describe el flujo de trabajo de inspección del software Firepower.



Determine que el registro está habilitado para eventos de

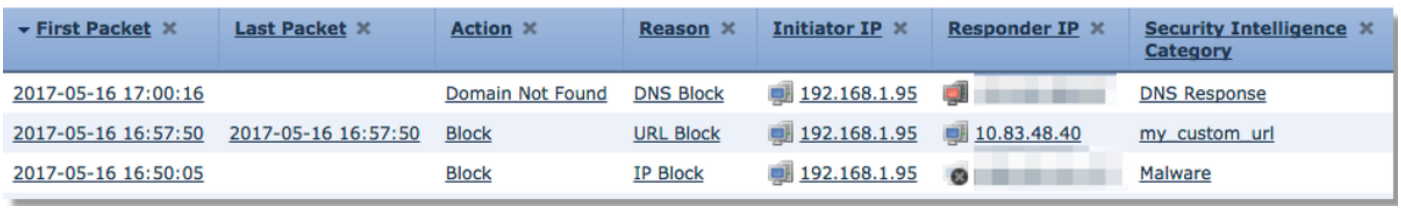
inteligencia de seguridad

Los bloques en el nivel de inteligencia de seguridad son muy fáciles de determinar mientras esté habilitado el registro. Esto se puede determinar en la interfaz de usuario (IU) de Firepower Management Center (FMC) mediante la navegación en **Políticas > Control de acceso > Directiva de control de acceso**. Después de hacer clic en el icono de edición junto a la política en cuestión, navegue hasta la pestaña **Seguridad Inteligente**.



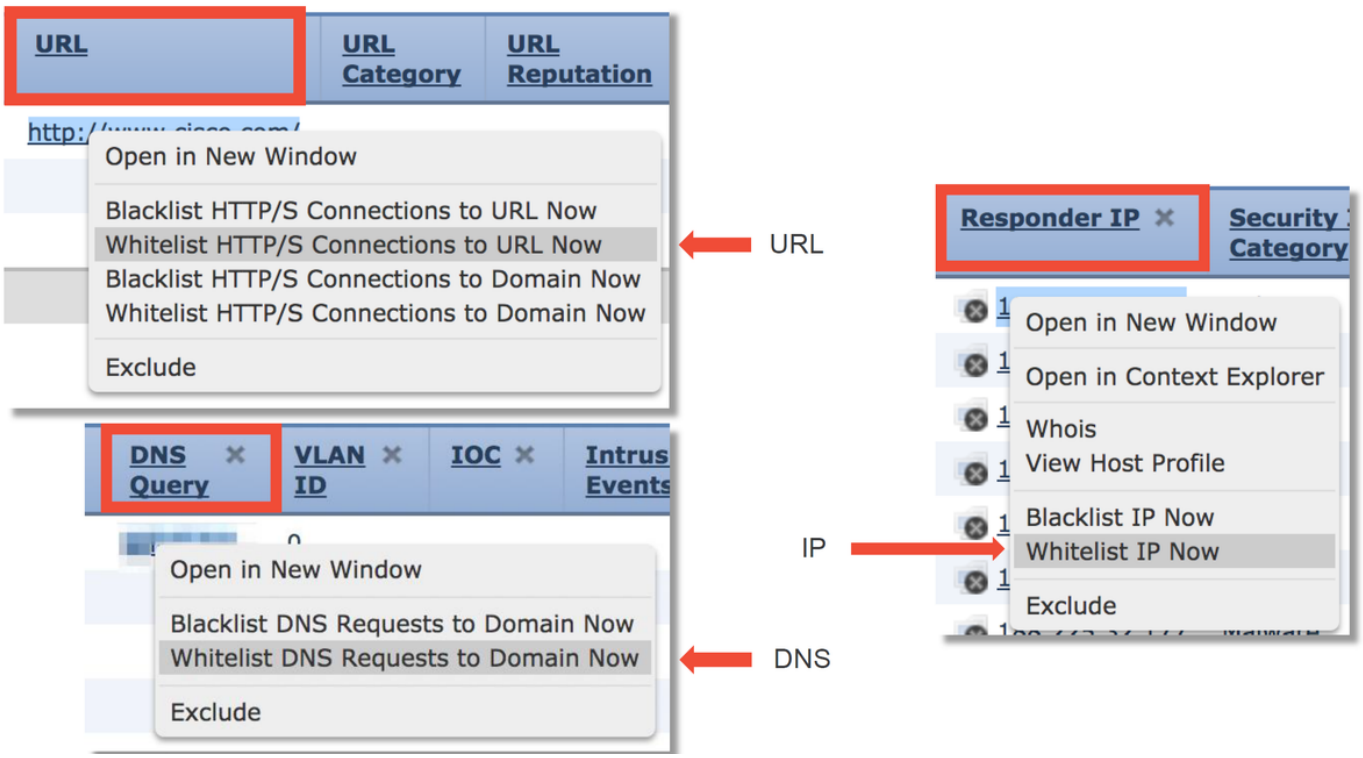
Revisar los eventos de inteligencia de seguridad

Una vez que se habilita el registro, puede ver los Eventos de Seguridad Inteligente en **Análisis > Conexiones > Eventos de Seguridad Inteligente**. Debe estar claro por qué se bloquea el tráfico.



First Packet	Last Packet	Action	Reason	Initiator IP	Responder IP	Security Intelligence Category
2017-05-16 17:00:16		Domain Not Found	DNS Block	192.168.1.95		DNS Response
2017-05-16 16:57:50	2017-05-16 16:57:50	Block	URL Block	192.168.1.95	10.83.48.40	my_custom_url
2017-05-16 16:50:05		Block	IP Block	192.168.1.95		Malware

Como paso de mitigación rápida, puede hacer clic con el botón derecho del ratón en la IP, URL o consulta DNS bloqueada por la función Security Intelligence y elegir una opción de lista blanca.



Si sospecha que algo se ha incluido incorrectamente en la lista negra o desea solicitar un cambio de reputación, puede abrir un ticket directamente con Cisco Talos en el siguiente enlace:

https://www.talosintelligence.com/reputation_center/support

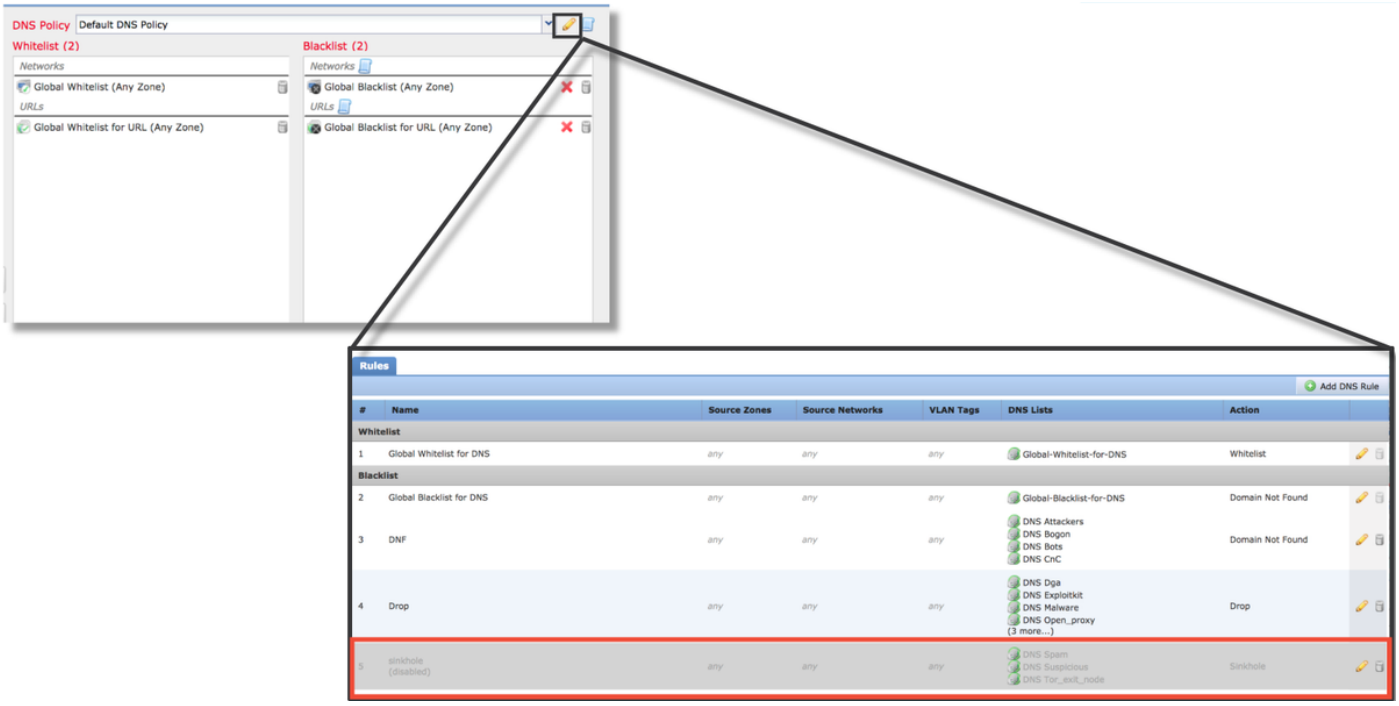
También puede proporcionar los datos al centro de asistencia técnica Cisco Technical Assistance Center (TAC) para investigar si un elemento debe eliminarse de la lista negra.

> **Nota:** Al agregar a la lista blanca sólo se agrega una entrada a la lista blanca de Security Intelligence en cuestión, lo que significa que el objeto puede pasar la comprobación de Security Intelligence. Sin embargo, todos los demás componentes de Firepower aún pueden inspeccionar el tráfico.

Cómo quitar las configuraciones de Security Intelligence

Para quitar las configuraciones de Seguridad Inteligente, navegue a la pestaña **Seguridad Inteligente**, como se mencionó anteriormente. Hay tres secciones; uno para redes, URL y una política para DNS.

Desde allí, las listas y fuentes se pueden eliminar haciendo clic en el símbolo de la papelera.



Observe en la captura de pantalla anterior que todas las listas de inteligencia de seguridad de IP y URL han sido eliminadas excepto para la lista negra global y la lista blanca.

Dentro de la política DNS, que es donde se almacena la configuración de DNS Security Intelligence, una de las reglas se inhabilita.

> **Nota:** Para ver el contenido de las listas negras y blancas globales, navegue hasta **Objetos > Administración de objetos > Inteligencia de seguridad**. A continuación, haga clic en la sección de interés (Red, URL, DNS). Al editar una lista, se mostrará el contenido, aunque la configuración se debe realizar dentro de la política de control de acceso.

Verifique la configuración en el motor

La configuración de Security Intelligence se puede verificar en la CLI mediante el comando **> show access-control-config** , que muestra el contenido de la política de control de acceso activa que se ejecuta en el dispositivo Firepower.

```
> show access-control-config

==================[ My AC Policy ]==================
Description              :
Default Action            : Allow
Default Policy            : SOC
Logging Configuration
   DC                   : Enabled
   Beginning             : Disabled
   End                  : Enabled
Rule Hits                 : 0
Variable Set              : Default-Set

===[ Security Intelligence - Network Whitelist ]====
   Name                 : Global-Whitelist (List)
   IP Count             : 0
   Zone                 : any

===[ Security Intelligence - Network Blacklist ]====
Logging Configuration     : Enabled
   DC                   : Enabled


--------------------[ Block ]---------------------
   Name                 : Attackers (Feed)
   Zone                 : any

   Name                 : Bogon (Feed)
   Zone                 : any
…[omitted for brevity]
```

Observe en el ejemplo anterior que el registro se configura para la lista negra de la red y que se han incluido al menos dos fuentes en la lista negra (Atacantes y Bogon).

Se puede determinar si un elemento individual se encuentra en una lista de Security Intelligence en modo experto. Consulte los siguientes pasos:

Hay un archivo para cada lista de Security Intelligence con un UUID único. El ejemplo anterior

muestra cómo identificar el nombre de la lista, usando el comando **head -n1**.

Datos que se deben proporcionar al TAC

Datos	Instrucciones
Solución de problemas de archivos del FMC y del dispositivo Firepower que inspeccionan el tráfico	http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-techn
Capturas de pantalla de eventos (con marcas de hora incluidas)	Consulte este artículo para obtener instrucciones
Salida de texto de sesiones CLI	Consulte este artículo para obtener instrucciones
Si envía un caso de falso positivo, proporcione el elemento (IP, URL, dominio) a la disputa.	Explicar las razones y pruebas de por qué debe llevarse a cabo la controversia.

Siguiente paso

Si se ha determinado que el componente Security Intelligence no es la causa del problema, el siguiente paso sería resolver los problemas de las reglas de la política de control de acceso.

Haga clic aquí para continuar con el siguiente artículo.