Ivan Castillo

S5: Laboratorio: Malware de firewall

Protección contra malware usando un AWS Network Firewall

Información general sobre el laboratorio

Malware, que significa software malicioso, se refiere a cualquier software intrusivo desarrollado por cibercriminales (a los que se suele llamar hackers) para robar datos o destruir equipos y sistemas. Los ejemplos de malware común incluyen virus, gusanos, troyanos, spyware, adware y ransomware.

Los firewalls son como muros de seguridad físicos que se encuentran entre la red interna de una organización y cualquier red pública externa, como la Internet. El firewall protege a una red interna del acceso por usuarios no autorizados en una red externa.

Los usuarios necesitan acceso a Internet por motivos de negocios, pero pueden descargar malware accidentalmente, el que puede afectar la seguridad de la red y de los datos.

Las amenazas de malware pueden estar presentes, y las organizaciones pueden usar varias técnicas y servicios para mitigar estas amenazas (por ejemplo, firewalls, software antivirus y prácticas recomendadas de control de usuarios). Este laboratorio se enfoca en técnicas de contramedidas usando un firewall.

ESCENARIO

AnyCompany lo contrató como un nuevo ingeniero de seguridad y la empresa le confió la tarea de reforzar el periodo de seguridad de la empresa. Existen informes de usuarios que descargaron malware accidentalmente después de acceder a sitios web específicos. El equipo de TI de AnyCompany le proporcionó las URL de los sitios que alojan el malware. Su trabajo es encontrar una solución para mitigar el acceso a estos archivos de actores maliciosos.

OBJETIVOS

Después de completar este laboratorio, podrá realizar lo siguiente:

- Actualizar un firewall de red de AWS
- Crear un grupo de reglas de firewall
- Verificar y probar que el acceso a los sitios maliciosos esté bloqueado

ENTORNO DE LABORATORIO

En este laboratorio, tiene una instancia de **TestInstance** (Amazon Elastic Compute Cloud [Amazon EC2]) preconfigurada para usar en las pruebas de acceso al sitio que aloja los archivos maliciosos. Esto está contenido en una zona de perímetro y está separado del resto de los servidores importantes de AnyCompany. Actualiza el firewall de la red de AnyCompany, crea un grupo de reglas y luego adjunta el grupo de reglas a una política de firewall y el firewall de red en sí. Luego inicia sesión en TestInstance y prueba la corrección.

Todos los componentes de backend, como Amazon EC2, los roles de AWS Identity y Access Management (IAM) y algunos servicios de AWS, ya están construidos en el laboratorio.

Tarea 1: Confirmar accesibilidad

En esta tarea, inicia sesión en la instancia **TestInstance** de EC2 que se preconfiguró durante la preparación del laboratorio. Desde ahí, emite un comando **wget** a los archivos del actor malicioso que el equipo de TI le proporcionó para confirmar la accesibilidad.

wget es una herramienta de línea de comando gratis y programa de descarga de archivos de red.

1. Desde la página de la consola de Vocareum, seleccione el botón **AWS Details** (Detalles de AWS).
2. Junto a **TestInstanceURL**, hay un enlace. Copie y pegue el enlace en un nuevo laboratorio en su navegador web.

Este enlace inicia su sesión en el servidor TestInstance de EC2 mediante AWS Systems Manager Session Manager.

3. Para cambiar directorios y ver el directorio de trabajo actual, ejecute los siguientes comandos:
   cd ~
   pwd

El siguiente paso replica cómo un usuario final descargaría un archivo malicioso usando un navegador web. La acción se simula usando el comando **wget** en los archivos maliciosos en la línea de comandos.

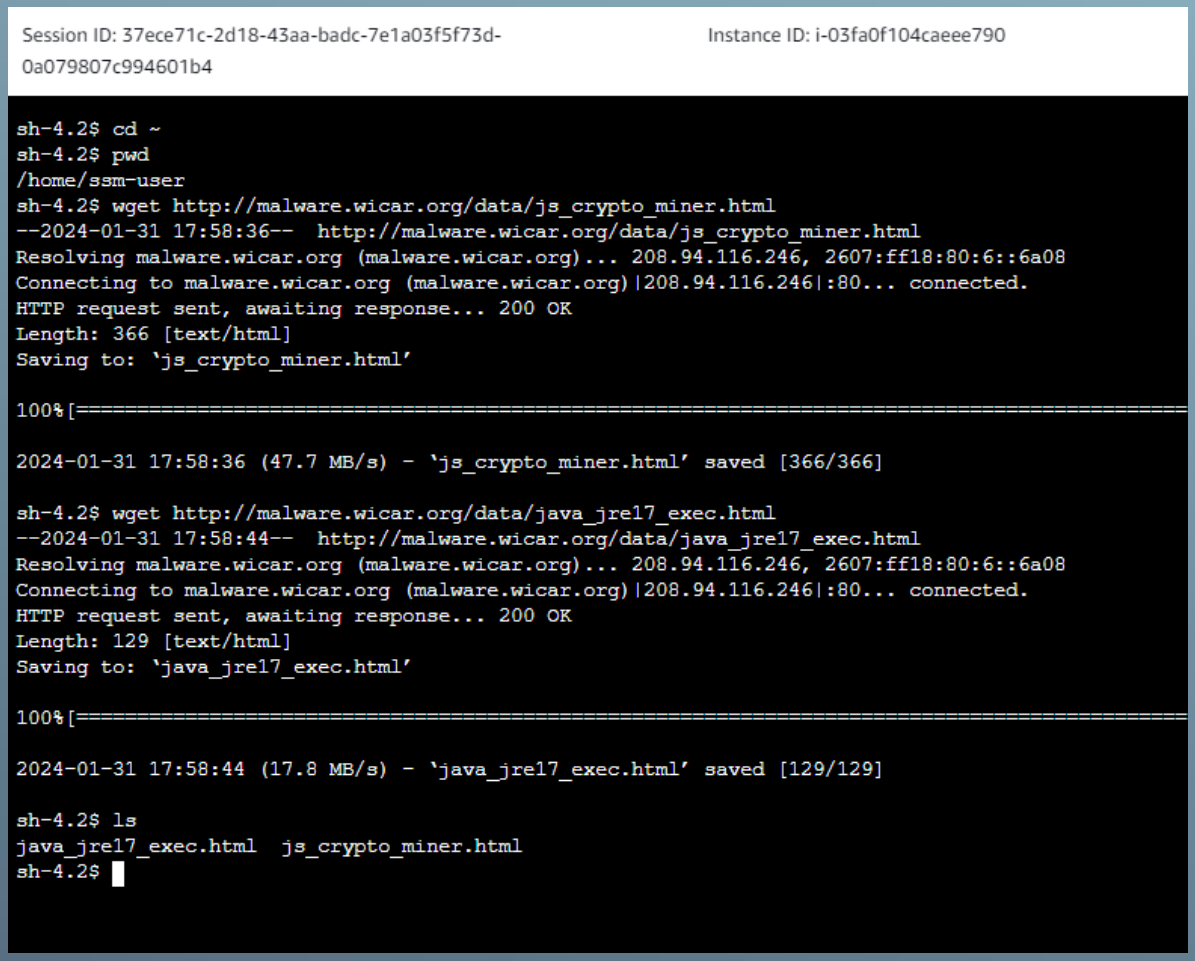
4. En este entorno de laboratorio protegido, ingrese el siguiente código y presione Intro para descargar parte del malware:

   wget http://malware.wicar.org/data/js_crypto_miner.html

5. En este entorno de laboratorio protegido, ingrese el siguiente código y presione Intro para descargar el resto del malware:

   wget http://malware.wicar.org/data/java_jre17_exec.html

6. Debería ver un resultado similar al que se muestra a continuación:



7. Para ver los archivos descargados, ejecute el siguiente comando:

   Ls

RESUMEN DE LA TAREA 1

En esta tarea, confirmó que la URL que aloja los archivos de malware es accesible mediante la siguiente red y el firewall de red que usa AnyCompany. Usó una instancia TestInstance de EC2 aislada para ejecutar los comandos y descargar los mismos archivos maliciosos que descargaron los usuarios. Ahora debe corregir el firewall de red de AnyCompany para detener el acceso a este sitio.

Tarea 2: Inspeccionar el firewall de red

En esta tarea, inspeccionará el **firewall** de AWS Network Firewall que se configuró durante la preparación del laboratorio. Actualizar este firewall es la prioridad principal que le asignó AnyCompany como el nuevo ingeniero de seguridad.

8. En la consola de administración de AWS, ingrese **VPC** en la barra de búsqueda y luego seleccione **VPC**.
9. En el panel de navegación izquierdo, en **NETWORK FIREWALL** (Firewall de red), seleccione **Firewalls**.
10. Seleccione **LabFirewall** y lea los tres pasos en la sección **Overview** (Información general).
11. En el **Paso 2: Configurar la política de firewall**, seleccione el enlace de **LabFirewallPolicy** para abrir la política asociada.

Una política de firewall define el comportamiento del firewall en una colección de grupos de reglas con y sin estado y otras configuraciones.

12. En la sección **Stateless default actions** (Acciones predeterminadas sin estado), seleccione **Edit** (Editar).
13. Para **Stateless default actions** (Acciones predeterminadas sin estado), configure las siguientes opciones:

    - **Choose how to treat fragmented packets** (Seleccionar cómo tratar paquetes fragmentados): Seleccione **Use the same actions for all packets** (Usar las mismas acciones para todos los paquetes).
    - **Action** (Acción): Seleccione **Forward to stateful rule groups** (Reenviar a grupos de reglas con estado).

14. Seleccione **Save **(Guardar).

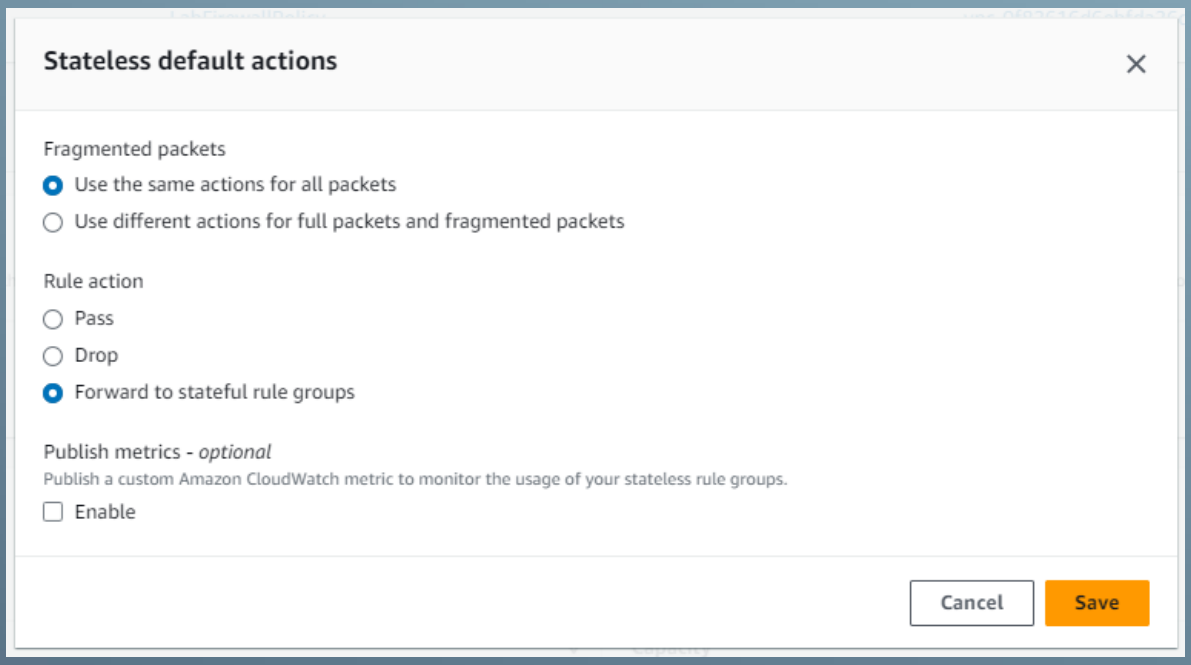
Estas configuraciones ahora reenvían todos los paquetes a un grupo de reglas con estado para una mayor inspección.

Un motor de reglas con estado inspecciona los paquetes en el contexto de su flujo de tráfico, le brinda la capacidad de usar reglas más complejas y le brinda la capacidad de registrar el tráfico de red y las alertas de firewall de AWS Network Firewall sobre el tráfico. Las reglas con estado consideran la dirección del tráfico. El motor de reglas con estado pueden retrasar la entrega de paquetes a los grupos de paquetes para su inspección.

Un motor de reglas sin estado inspecciona cada paquete de forma aislada sin importar factores como la dirección del tráfico o si el paquete es parte de una conexión existente y aprobada. Este motor prioriza la velocidad de la evaluación.

RESUMEN DE LA TAREA 2

En esta tarea, inspeccionó el firewall de red y actualizó la política de firewall. Luego actualizó la política de firewall para reenviar todos los paquetes para una inspección de reglas con estado.



Tarea 3: Crear un grupo de reglas de firewall

En esta tarea, creará un grupo de reglas de firewall de red con reglas que bloquean el acceso a las URL maliciosas. Luego adjuntará esta regla a su política de firewall.

Un grupo de reglas de firewall de red es un conjunto de criterios para inspeccionar y manejar el tráfico de red. Agregará uno o más grupos de reglas a una política de firewall como parte de una configuración de política. Este grupo de reglas bloquea el acceso a las URL del actor malicioso.

15. En el panel de navegación izquierdo, en **NETWORK FIREWALL** (Firewall de red), seleccione **Network Firewall Rule Groups** (Grupos de reglas de firewall de red).
16. Seleccione **Create Network Firewall rule group** (Creare grupo de reglas de firewall de red).
17. En la sección **Create Network Firewall rule group** (Crear grupo de reglas de firewall de red), configure las siguientes opciones:

    - Para **Rule group type** (Tipo de grupo de reglas), seleccione **Stateful rule group** (Grupo de reglas con estado).
    - En la sección **Stateful rule group** (Grupo de reglas con estado), configure las siguientes opciones:
    - **Name** (Nombre): Ingrese StatefulRuleGroup.
    - **Capacity** (Capacidad): Ingrese 100
    - **Stateful rule group options** (Opciones de grupo de reglas con estado): Seleccione **Suricata compatible IPS rules** (Reglas de IPS compatibles con Suricata).

Las reglas del Sistema de prevención de intrusos (IPS) proporciona reglas de firewall avanzadas usando la sintaxis de reglas Suricata. Suricata es un IPS de red de código abierto que incluye un lenguaje basado en reglas estándar para la inspección de tráfico.

18. En la sección **Suricata compatible IPS rules** (Reglas de IPS compatibles con Suricata), ingrese el siguiente código en el cuadro de texto:

    drop http $HOME_NET any -> $EXTERNAL_NET 80 (msg:"MALWARE custom solution"; flow: to_server,established; classtype:trojan-activity; sid:2002001; content:"/data/js_crypto_miner.html";http_uri; rev:1;)

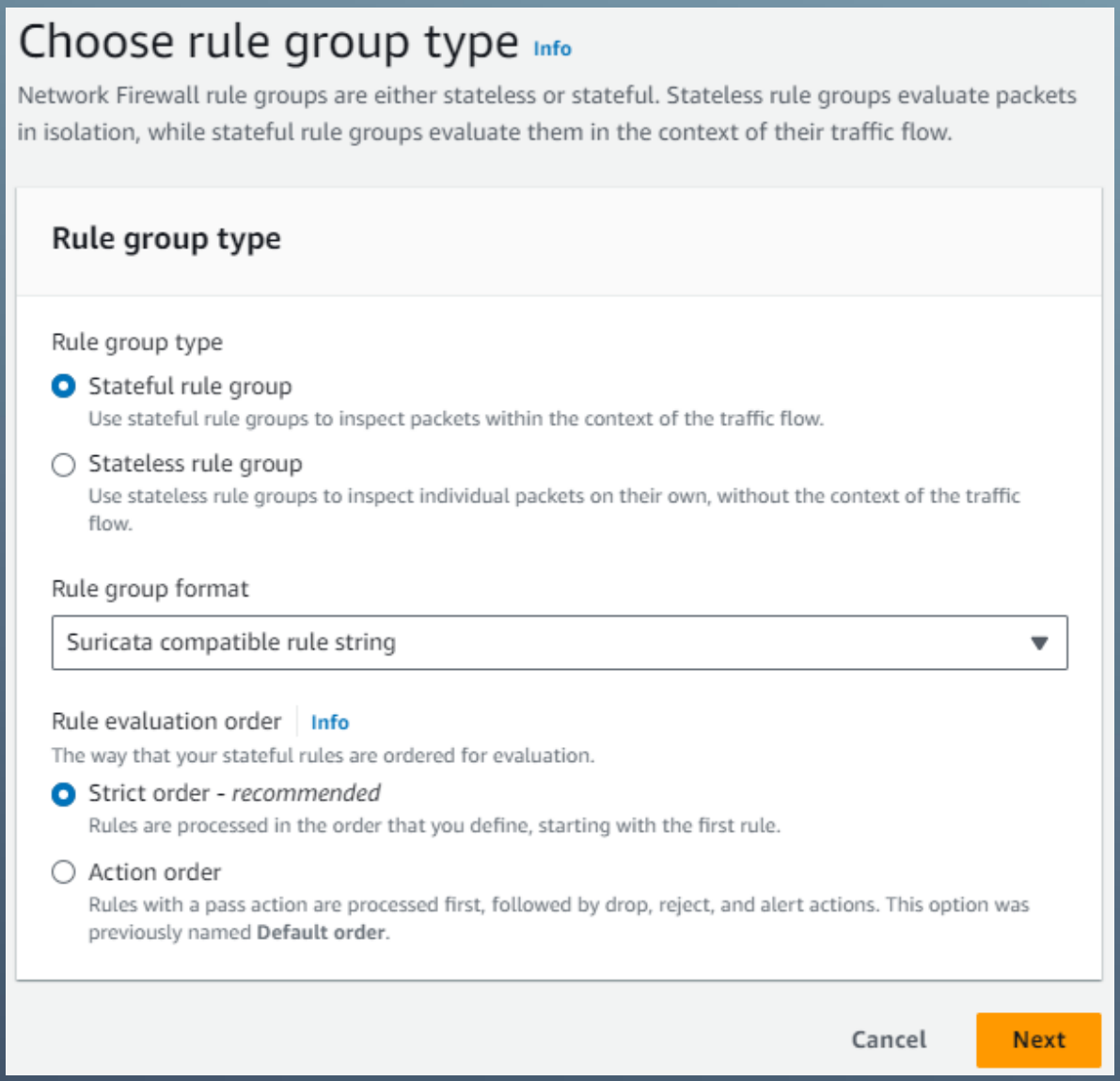
    drop http $HOME_NET any -> $EXTERNAL_NET 80 (msg:"MALWARE custom solution"; flow: to_server,established; classtype:trojan-activity; sid:2002002; content:"/data/java_jre17_exec.html";http_uri; rev:1;)

Las dos reglas de Suricata que agregó ahora bloquean el tráfico que coincide con las URL **http_uri contents /data/js_crypto_miner.html** y **http_uri contents /data/js_crypto_miner.html** cuando el tráfico se inicia desde **LabVPC** a la red pública.

19. Seleccione **Create stateful rule group** (Crear grupo de reglas con estado).

RESUMEN DE LA TAREA 3

En esta tarea, creó un grupo de reglas de firewall de red con estado que usa reglas Suricata. Después de adjuntar este grupo de reglas al firewall de red, este bloquea los sitios web maliciosos a los que accedieron los usuarios de AnyCompany.



Describe rule group Info

Name and describe your rule group so you can easily identify it and distinguish it from other resources.

Rule group details

Name

Enter a name for the rule group that's unique within your stateful rule groups.

StatefulRuleGroup

The name must have 1-128 characters. Valid characters: a-z, A-Z, 0-9 and - (hyphen). The name can't start or end with a hyphen, and it can't contain two consecutive hyphens.

Description - *optional*

This description appears when you view this rule group's details. It can help you quickly identify what your rule group is used for.

Enter rule group description

The description can have 0-256 characters.

Capacity Info

The number of rules you expect to have in this rule group during its lifetime. You can't change capacity after rule group creation, so leave room to grow.

100

The capacity must be greater than or equal to 1 and less than 30,000.

Cancel Previous Next

Suricata compatible rule string Info

Suricata is an open source network IPS that includes a standard rule-based language for traffic inspection.

Suricata compatible rule string

```
drop http $HOME_NET any -> $EXTERNAL_NET 80 (msg:"MALWARE custom solution";
flow: to_server,established; classtype:trojan-activity; sid:2002001;
content:"/data/js_crypto_miner.html";http_uri; rev:1;)

drop http $HOME_NET any -> $EXTERNAL_NET 80 (msg:"MALWARE custom solution";
flow: to_server,established; classtype:trojan-activity; sid:2002002;
content:"/data/java_jre17_exec.html";http_uri; rev:1;)
```

Copy rules

Tarea 4: Adjuntar un grupo de reglas al firewall de red

En esta tarea, adjuntará el grupo de reglas de firewall de red que creó al firewall de red.

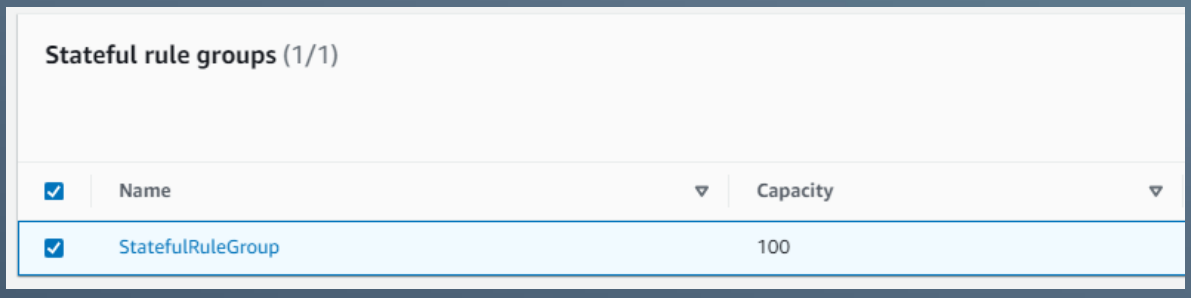
20. En el panel de navegación izquierdo, en **NETWORK FIREWALL** (Firewall de red), seleccione **Firewalls**.
21. Seleccione **LabFirewall**.
22. En **Step 2** (Paso 2), seleccione la lista desplegable **Add rule groups** (Agregar grupos de reglas) y luego seleccione **Add from existing stateful rule groups** (Agregar desde grupos de reglas con estado existentes).
23. Seleccione la casilla para **StatefulRuleGroup** y luego seleccione **Add stateful rule group** (Agregar grupo de reglas con estado).

En la parte superior de la página, debería ver un anuncio verde **You successfully updated FirewallPolicy** (Actualizó correctamente la política de firewall).

24. Desplácese hasta la sección **Stateful rule groups** (Grupos de reglas con estado) para ver el grupo de reglas que se agregó correctamente.

RESUMEN DE LA TAREA 4

Adjuntó el grupo de reglas al firewall, lo que bloquea los intentos de acceder a los archivos del actor malicioso alojados en el sitio web.



Tarea 5: Validar la solución

En esta tarea, volverá a iniciar sesión en TestInstance para probar que el firewall de red bloquee correctamente los intentos de acceder a los archivos del sitio web malicioso.

25. En la consola de administración de AWS, ingrese **EC2** en la barra de búsqueda y luego seleccione **EC2**.
26. En el panel de navegación izquierdo, elija **Instances** (Instancias).
27. Seleccione la casilla junto a **TestInstance**, y luego seleccione **Connect** (Conectar).
28. En la pestaña **Session Manager**, elija **Connect** (Conectar).
29. Para cambiar directorios y ver el directorio de trabajo actual, ejecute los siguientes comandos:

    cd ~
    pwd

30. Para intentar acceder al primer archivo malicioso, ejecute el siguiente comando **wget**.

wget http://malware.wicar.org/data/js_crypto_miner.html

El resultado debería mostrar lo siguiente:

HTTP request sent, awaiting response...

Este resultado muestra que ya no se puede acceder al sitio y al archivo de malware y que el firewall de red los bloqueó correctamente.

31. Presione Ctrl+c para detener el comando.
32. Para probar las otras URL maliciosas, ejecute el siguiente comando:

    wget http://malware.wicar.org/data/java_jre17_exec.html

El resultado debería mostrar lo siguiente:

HTTP request sent, awaiting response...

33. A continuación, para eliminar los archivos de malware de prueba, ejecute el siguiente comando:

rm java_jre17_exec.html js_crypto_miner.html

39. Para confirmar que los archivos se eliminaron, ejecute el comando **ls**:

    Ls

Debería ver un resultado en blanco, que confirma que los archivos se eliminaron.

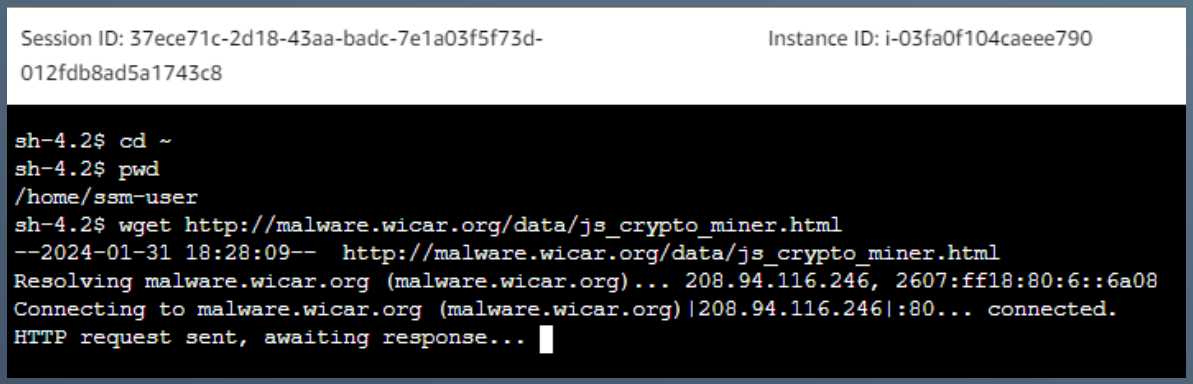
RESUMEN DE LA TAREA 5

En esta tarea, comprobó que el firewall de red se actualizó y se configuró correctamente para bloquear los sitios web maliciosos. Confirmó que el acceso está bloqueado al iniciar sesión en la instancia TestInstance de EC2 y ejecutar comandos wget** para esos archivos. Los usuarios ahora no pueden acceder a esos archivos maliciosos desde este sitio web.

Conclusión

¡Felicitaciones! Aprendió a realizar correctamente las siguientes tareas:

- Actualizar un firewall de red
- Crear un grupo de reglas de firewall
- Verificar y probar que el acceso a los sitios maliciosos esté bloqueado



Session ID: 37ece71c-2d18-43aa-badc-7e1a03f5f73d-012fdb8ad5a1743c8 Instance ID: i-03fa0f104caeee790

```
sh-4.2$ cd ~
sh-4.2$ pwd
/home/ssm-user
sh-4.2$ wget http://malware.wicar.org/data/js_crypto_miner.html
--2024-01-31 18:28:09--  http://malware.wicar.org/data/js_crypto_miner.html
Resolving malware.wicar.org (malware.wicar.org)... 208.94.116.246, 2607:ff18:80:6::6a08
Connecting to malware.wicar.org (malware.wicar.org)|208.94.116.246|:80... connected.
HTTP request sent, awaiting response... ^C
sh-4.2$ wget http://malware.wicar.org/data/java_jre17_exec.html
--2024-01-31 18:29:22--  http://malware.wicar.org/data/java_jre17_exec.html
Resolving malware.wicar.org (malware.wicar.org)... 208.94.116.246, 2607:ff18:80:6::6a08
Connecting to malware.wicar.org (malware.wicar.org)|208.94.116.246|:80... connected.
HTTP request sent, awaiting response...
```

Session ID: 37ece71c-2d18-43aa-badc-7e1a03f5f73d-012fdb8ad5a1743c8 Instance ID: i-03fa0f104caeee790

```
sh-4.2$ rm java_jre17_exec.html js_crypto_miner.html
sh-4.2$ ls
sh-4.2$
```