Resuelva problemas la cuarentena centralizada PVO en el ESA y el S A

Contenido

Introducción

Este documento describe cómo resolver problemas la salida y los Problemas de conexión cuando se habilita el quarnatine policiy, del virus y del brote centralizado.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Envíe por correo electrónico el dispositivo de seguridad (ESA) con AsyncOS 8.1 o más adelante
- Dispositivo de la Administración de seguridad (S A) con AsyncOS 8.0 o más adelante

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). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

Centralizado directiva, virus y brote (PVO) cuarentena característica era introducido en AsyncOS 8.0 ()/8.1 ESA (S A). Esta característica tiene requisitos adicionales de la conectividad de red, y plantea algunos nuevos desafíos para resolver problemas.

Entienda la comunicación

- La comunicación CPQ utiliza el S TP, pero con algunos comandos adicionales para los meta datos de transferencia

- El S A estará atentas las conexiones en la interfaz y virará hacia el lado de babor definido bajo servicios centralizados - > las cuarentenas de la directiva, del virus y del brote. ¡Por abandono, el puerto es 7025, pero esto se pudo haber cambiado por el Usuario administrador!
- El ESA estará atentas las conexiones en la interfaz y virará hacia el lado de babor definido bajo Servicios de seguridad - > las cuarentenas de la directiva, del virus y del brote. ¡Una vez más por abandono, el puerto es 7025, pero esto se pudo haber cambiado por el Usuario administrador!
- El S A también utiliza SSH (vía el comando client) para conseguir la información de la configuración de los ESA. Particularmente, se utiliza esto cuando el S A entrega los correos electrónicos liberados al ESA. El S A utilizará el SSH para preguntar la configuración ESA y para determinarla a que interconecte el /port para entregar el email liberado.

Módulos de escucha

- El ESA y el S A tendrán un módulo de escucha ocultado llamado el “cpq_listener” que escuchará en el puerto especificado.
- Estos módulos de escucha pueden ser vistos en el archivo de configuración. Por ejemplo:

```
<listener>
     <listener_name>cpq_listener</listener_name>
     <protocol>CPQ</protocol>
     <interface_name>Incoming Mail</interface_name>
     <port>7025</port>
     <listen_queue_size>50</listen_queue_size>
     <type>private</type>
     <hat>
$RELAYED
   RELAY {}
$BLOCKED
   REJECT {}
RELAYLIST:
   10.1.2.3
       $RELAYED (Only select hosts can relay from this box)
ALL
   $BLOCKED (Everyone else)
     </hat>
     <rat>
       <rat_entry>
         <rat_address>ALL</rat_address>
         <access>ACCEPT</access>
       </rat_entry>
     </rat>
```

- Suspenderán a estos módulos de escucha si el Usuario administrador utiliza los “suspendlisteners todos” o “suspenda”. Si el puerto no está validando las conexiones, usted debe marcar si el estado del sistema es “offline” y curriculum vitae si es necesario.

Salida del Troubleshooting del ESA al S A

- Marque que el ESA puede conectar con el S A en el puerto configurado e interconectar. Esto se puede hacer usando el telnet. Usted debe conseguir un banner 220 si la comunicación es acertada.

- El ESA tendrá un objeto de destino llamado “the.cpq.host”, que contiene los mensajes mientras que él se hace cola para la salida al S A. Usted puede ver esto usando los “tophosts” o monitorear - > estatus de la salida. Usted no puede utilizar el “hoststatus” con él, sino que usted puede utilizar los “showrecipients” y los “deleterecipients” en caso necesario.

Salida del Troubleshooting del S A al ESA

- Marque que el S A puede conectar con el ESA en el puerto configurado e interconectar. Una vez más usted puede utilizar el telnet y verá el banner 220 si es acertado.
- Al usar los clusteres, es importante que la interfaz definida en los Servicios de seguridad inferiores llanos del cluster - > las cuarentenas de la directiva, del virus y del brote existen para todos los dispositivos en el nivel de equipo. (red del control - > interfaces IP).
- El S A tendrá un objeto de destino llamado “the.cpq.release.host” que contenga los mensajes liberados mientras que él se hace cola para la salida al ESA. Usted puede ver esto usando los “tophosts”. Esto no aparece trabajar con el “hoststatus” o los “showrecipients”, y no he probado los “deleterecipients” con él, pero esto no trabaja probablemente cualquiera.
- Puede también haber problemas con la comunicación de SSH entre el S A y el ESA. Estos problemas no son siempre necesariamente red basada, por ejemplo en CSCus29647 un componente interno del S A sale de la operación. Los problemas tales como éstos aparecerán típicamente como incidentes de la aplicación en los registros del correo, y pueden ser resueltos generalmente reiniciando el S A.

TLS/Certificates

- Todas las conexiones CPQ en cualquier dirección confían en TLS, y como consecuencia la configuración de la cifra sabe desempeñar un papel.
- Para que la conexión TLS tenga éxito, el dispositivo que abre la conexión debe poder verificar que el dispositivo receptor está utilizando nuestro certificado hiddent CPQ. Es posible que esto falle si el dispositivo negocia una cifra anónima. Esto aparecería en los registros como algo similar:

```
Mon Apr  1 12:00:00 2014 Info: New SMTP DCID 123456 interface 10.0.0.2 address 10.0.0.1 port
7025
Mon Apr  1 12:00:00 2014 Info: DCID 123456 TLS failed: verify error: no certificate from
server
Mon Apr  1 12:00:00 2014 Info: DCID 123456 TLS was required but could not be successfully
negotiated
```

- Usted puede reparar estos problemas simplemente quitando las cifras anónimas de la lista saliente de la cifra de la salida, que es hecha agregando “`: - aNULL`” al final de la lista de la cifra. Por ejemplo: `ALTO: MEDIA: - aNULL`

Archivo del registro

- Si el S A tiene una suscripción de los registros del correo (hace por abandono), usted puede revisar los registros del correo para recolectar la penetración adicional.
- CPQ que recibe los eventos parecerá esto para los mensajes quarantined al S A y los mensajes liberados al ESA

```
New CPQ ICID 12345 interface Management (10.10.10.1) address 10.10.20.1 reverse dns host
unknown verified no
```

- Usted puede buscar para estos eventos usando el grep, ejemplo: `grep mail_logs "CPQ ICID"`
- Los eventos, ambos quarantining del ESA y la versión de la salida CPQ de la cuarentena del S A, parecen similares a cualquier otra salida, con excepción del hecho que el puerto de encargo es mencionado y algunas líneas incluyen el verbiage "cuarentena centralizada de la directiva". Ejemplo abajo:

```
Fri Sep 13 15:08:02 2013 Info: New SMTP DCID 12345 interface 10.10.20.1 address 10.10.10.1
port 7025
Fri Sep 13 15:08:02 2013 Info: DCID 12345 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Fri Sep 13 15:08:02 2013 Info: Delivery start DCID 12345 MID 23456 to RID [0] to Centralized
Policy Quarantine
Fri Sep 13 15:08:02 2013 Info: Message done DCID 12345 MID 23456 to RID [0] (centralized
policy quarantine)
Fri Sep 13 15:08:07 2013 Info: DCID 12345 close
```

- Usted puede encontrar estos eventos usando el grep al seach para el puerto, ejemplo: `mail_logs del puerto 7025" del grep el "`

Botón del "enable" ESA inhabilitado

Al intentar habilitar PVO en el ESA, usted puede encontrar que el botón del "enable" es grayed hacia fuera, a pesar de toda la configuración del requisito previó que es completada. Cuando el ESA visualiza la página PVO, comunica con el S A sobre el puerto 7025 para verificar que la configuración está lista para ser habilitado. Si esta comunicación falla, el botón del "enable" será inhabilitado. Usted puede resolver problemas esto apenas como cualquier ESA - > comunicación del puerto 7025 S A grepping para el "puerto el 7025" en el ESA. Para más información refiera a la Nota Técnica enumerada en la información relacionada.

Información Relacionada

- Requisitos para el Asisitente de la migración PVO cuando se agrupa el ESA
- La directiva de centralización ESA, el virus, y la cuarentena del brote (PVO) no pueden ser habilitados