Mejores prácticas para la directiva centralizada, cuarentenas del virus y del brote puestas y migración del ESA al S A

Contenido

Introducción

Las cuarentenas siguientes se pueden ahora centralizar colectivamente en un dispositivo de la Administración del Cisco Security (S A):

- Contra virus
- Brote
- Cuarentenas de la directiva usadas para los mensajes por los cuales son cogidos: Filtros del mensajeFiltros contentosDirectivas de prevención de la pérdida de datos

La centralización de estas cuarentenas ofrece las siguientes ventajas:

- Los administradores pueden manejar los mensajes quarantined de los dispositivos de seguridad múltiples del correo electrónico (ESA) en una ubicación.
- Los mensajes Quarantined se salvan detrás del Firewall en vez en del DMZ, reduciendo el riesgo de seguridad.
- Las cuarentenas centralizadas se pueden sostener como parte de la funcionalidad de backup estándar en el S A.

Prerrequisitos

- S A que ejecuta 8.1 (guía del usuario S A, capítulo 8, directiva centralizada, virus, y cuarentenas del brote)
- ESA que ejecuta 8.0.1 (guía del usuario ESA, capítulo 27, cuarentenas)
- Puerto de firewall 7025 /TCP (en y hacia fuera)/uso del nombre de host: AsyncOS IP/descripción: Pase la directiva, el virus, y los datos de la cuarentena del brote entre los dispositivos de seguridad del correo electrónico y el dispositivo de la Administración de seguridad cuando se centraliza esta característica

Configurar

Están comenzando con el ESA, en una cuarentena de la política existente, mensajes activos en la cuarentena de la directiva:

Para emigrar estos mensajes y después confiar en el S A para ser el dispositivo activo que posee la cuarentena de la directiva, complete las direcciones siguientes.

En el S A, navegue al **dispositivo de la Administración > los servicios > las cuarentenas centralizados de la directiva, del virus y del brote**. Si no habilitado ya, **permiso del** tecleo**:**

Seleccione la interfaz, si procede, que se piensa para manejar el tráfico del ESA al S A.

> Nota: El puerto de la cuarentena puede ser cambiado, pero éste necesitará ser abierto si hay un Firewall/una red ACL en el lugar.

Haga clic en Submit (Enviar). ¿La pantalla restaurará para mostrar? ¿Servicio habilitado? mensaje, visto abajo:

Navegue al **dispositivo de la Administración > los dispositivos centralizados del > Security (Seguridad) de los servicios** y agregue la comunicación ESA al S A:

El tecleo **agrega el dispositivo del correo electrónico**.

> Nota: Usted necesita solamente agregar la dirección IP que el S A utilizará para comunicar con el ESA. El nombre del dispositivo se utiliza solamente como referencia administrativa.

Esté seguro **de establecer la conexión** y la **conexión de prueba**. Sobre el establecimiento de la conexión del S A al ESA, el nombre y la contraseña de usuario administrador serán pedidos. Ésta es el usuario administrador y la contraseña del ESA se está agregando que. De acuerdo con cuál es ya activo contra lo que se está agregando, los resultados de la prueba pueden variar, pero deben ser similares a:

Esté seguro **de someter** y **de confiar los cambios** en este momento en el S A.

Ahora, si usted revisitara el ESA e intentara configurar la sección centralizada de los servicios de la cuarentena de la directiva, sería similar al siguiente:

Los pasos de la migración se deben todavía completar en el S A. Vuelva al S A y continúe con la sección siguiente.

¿Los cambios del cometer se completan una vez, el **Asisitente de la migración del lanzamiento?** del paso 2 llegarán a ser activos:

Seleccione al **Asisitente de la migración del lanzamiento** y continúe como sigue:

Si solamente se va una cuarentena determinada a ser emigrada, elija la **aduana**. En este ejemplo,

continuaremos con **automático**, que emigrará las cuarentenas de la directiva ANY/ALL del ESA al S A. Observe por favor que usted verá el nombre especificado elegido durante el ESA para agregar mencionado anterior, seguido por la dirección IP usada en la comunicación:

Haga clic **después**, y continúe:

Finalmente, el tecleo **somete**, y se presenta la notificación del “éxito”:

Confíe sus cambios en el S A.

Volviendo al ESA, navegue a los **Servicios de seguridad > a las cuarentenas de la directiva, del virus y del brote**. Los pasos necesarios de antemano en el S A ahora se reconocen:

¿Permiso del tecleo**?** , y continúe:

El aviso, eso aquí el puerto apropiado usado para la comunicación se observa otra vez. Éstos **deben** hacer juego, y si el Firewall/la red ACL es funcionando, se deben abrir para permitir la migración apropiada entre el ESA y el S A.

> Nota: Si usted tiene la directiva, el virus, y cuarentenas del brote configuradas en un ESA, la migración de las cuarentenas y de todos sus mensajes comienza tan pronto como usted confíe este cambio.

> Nota: Solamente un proceso de migración puede estar en curso en cualquier momento. No habilite la directiva centralizada, el virus, y las cuarentenas del brote en otras dispositivo de seguridad del correo electrónico hasta que la migración anterior sea completa.

El tecleo **somete**, y finalmente hace clic el **cometer**. La notificación de información debe ser similar. Si hay un gran número de mensajes ya en la cuarentena local, éstos pueden tomar tiempo para procesar del ESA al S A:

Revisite el S A, y navegue al **dispositivo de la Administración > los servicios > las cuarentenas centralizados de la directiva, del virus y del brote**. Los pasos de la migración ahora serán completados:

Verificación

Ahora, la migración de la cuarentena de la directiva del ESA al S A es completa. Para la verificación final, marque la cuarentena de la directiva en el S A:

Usted debe ver los mismos mensajes que fueron enumerados originalmente en el ESA. Seleccione # enlace hipertexto en la columna de los mensajes, y verifiquelo:

Si usted mira los mail_logs en el ESA, la migración de los mensajes actuales será presentada:

> Nota: Observe el uso de la comunicación entre el ESA (XX.X.XX.XX X) y S A (YY.Y.YY.YY Y) vía el puerto 7025.

```
Wed Mar  5 02:48:40 2014 Info: New SMTP DCID 2 interface XX.X.XX.XXX address
```

```
YY.Y.YY.YYY port 7025
Wed Mar  5 02:48:40 2014 Info: DCID 2 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:49:52 2014 Info: New SMTP DCID 3 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:49:52 2014 Info: DCID 3 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:50:22 2014 Info: New SMTP DCID 4 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:50:22 2014 Info: DCID 4 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:50:23 2014 Info: New SMTP DCID 5 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:50:23 2014 Info: DCID 5 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:50:40 2014 Info: New SMTP DCID 6 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:50:40 2014 Info: DCID 6 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:50:41 2014 Info: New SMTP DCID 7 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:50:41 2014 Info: DCID 7 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:50:42 2014 Info: New SMTP DCID 8 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:50:42 2014 Info: DCID 8 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:51:01 2014 Info: New SMTP DCID 9 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:51:01 2014 Info: DCID 9 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:51:01 2014 Info: CPQ listener cpq_listener starting
Wed Mar  5 02:51:01 2014 Info: New SMTP DCID 10 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:51:01 2014 Info: DCID 10 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:51:02 2014 Info: New SMTP DCID 11 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:51:02 2014 Info: DCID 11 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:51:02 2014 Info: MID 1 enqueued for transfer to centralized quarantine
"Policy" (content filter _policy_q_in_)
Wed Mar  5 02:51:02 2014 Info: MID 1 queued for delivery
Wed Mar  5 02:51:02 2014 Info: New SMTP DCID 12 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:51:02 2014 Info: DCID 12 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:51:02 2014 Info: Delivery start DCID 12 MID 1 to RID [0] to Centralized
Policy Quarantine
Wed Mar  5 02:51:02 2014 Info: MID 2 enqueued for transfer to centralized quarantine
"Policy" (content filter _policy_q_in_)
Wed Mar  5 02:51:02 2014 Info: MID 2 queued for delivery
Wed Mar  5 02:51:02 2014 Info: MID 3 enqueued for transfer to centralized quarantine
"Policy" (content filter _policy_q_in_)
Wed Mar  5 02:51:02 2014 Info: MID 3 queued for delivery
Wed Mar  5 02:51:02 2014 Info: Message done DCID 12 MID 1 to RID [0] (centralized
policy quarantine)
Wed Mar  5 02:51:02 2014 Info: MID 1 RID [0] Response 'ok:  Message 1 accepted'
Wed Mar  5 02:51:02 2014 Info: Message finished MID 1 done
Wed Mar  5 02:51:02 2014 Info: MID 1 migrated from all quarantines
Wed Mar  5 02:51:02 2014 Info: Delivery start DCID 12 MID 2 to RID [0] to Centralized
Policy Quarantine
Wed Mar  5 02:51:02 2014 Info: New SMTP DCID 13 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
```

```
Wed Mar  5 02:51:02 2014 Info: DCID 13 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:51:02 2014 Info: New SMTP DCID 14 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:51:02 2014 Info: DCID 14 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:51:02 2014 Info: Message done DCID 12 MID 2 to RID [0] (centralized
policy quarantine)
Wed Mar  5 02:51:02 2014 Info: MID 2 RID [0] Response 'ok:  Message 2 accepted'
Wed Mar  5 02:51:02 2014 Info: Message finished MID 2 done
Wed Mar  5 02:51:02 2014 Info: MID 2 migrated from all quarantines
Wed Mar  5 02:51:02 2014 Info: Delivery start DCID 12 MID 3 to RID [0] to Centralized
Policy Quarantine
Wed Mar  5 02:51:02 2014 Info: Message done DCID 12 MID 3 to RID [0] (centralized
policy quarantine)
Wed Mar  5 02:51:02 2014 Info: MID 3 RID [0] Response 'ok:  Message 3 accepted'
Wed Mar  5 02:51:02 2014 Info: Message finished MID 3 done
Wed Mar  5 02:51:02 2014 Info: MID 3 migrated from all quarantines
Wed Mar  5 02:51:02 2014 Info: New SMTP DCID 15 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:51:02 2014 Info: DCID 15 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:51:07 2014 Info: DCID 12 close
```

Revisite el ESA, y lo que sigue ahora se presenta al ver la directiva, el virus, brote Quarantines:

El siguiente paso de la verificación está enviando un nuevo mensaje de prueba con el ESA que será cogido para la cuarentena de la directiva. Mirando los mail_logs en el ESA, note la línea resaltada el indicar de la transferencia del ESA al S A vía 7025, indicando la cuarentena de la directiva:

```
Wed Mar  5 02:57:47 2014 Info: Start MID 4 ICID 6
Wed Mar  5 02:57:47 2014 Info: MID 4 ICID 6 From: <robsherw.cisco@gmail.com>
Wed Mar  5 02:57:47 2014 Info: MID 4 ICID 6 RID 0 To: <robsherw@cisco.com>
Wed Mar  5 02:57:47 2014 Info: MID 4 Message-ID
'<7642E61C-4BA2-432E-A524-E163EA0B9753@gmail.com>'
Wed Mar  5 02:57:47 2014 Info: MID 4 Subject 'NEW FUNNY'
Wed Mar  5 02:57:47 2014 Info: MID 4 ready 525 bytes from
<robsherw.cisco@gmail.com>
Wed Mar  5 02:57:47 2014 Info: MID 4 matched all recipients for per-recipient
policy DEFAULT in the inbound table
Wed Mar  5 02:57:47 2014 Info: MID 4 enqueued for transfer to centralized
quarantine "Policy" (content filter _policy_q_in_)
Wed Mar  5 02:57:47 2014 Info: MID 4 queued for delivery
Wed Mar  5 02:57:47 2014 Info: New SMTP DCID 16 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:57:47 2014 Info: DCID 16 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:57:47 2014 Info: Delivery start DCID 16 MID 4 to RID [0] to Centralized
Policy Quarantine
Wed Mar  5 02:57:47 2014 Info: Message done DCID 16 MID 4 to RID [0] (centralized
policy quarantine)
Wed Mar  5 02:57:47 2014 Info: MID 4 RID [0] Response 'ok:  Message 4 accepted'
Wed Mar  5 02:57:47 2014 Info: Message finished MID 4 done
Wed Mar  5 02:57:52 2014 Info: DCID 16 close
```

Revisite la cuarentena previamente mencionada de la directiva en el S A, el nuevo mensaje de prueba ahora está en la cuarentena también:

Información Relacionada

- La directiva de centralización ESA, el virus, y la cuarentena del brote (PVO) no pueden ser habilitados
- Dispositivo de seguridad del correo electrónico de Cisco - Guías del usuario final
- Soporte Técnico y Documentación - Cisco Systems