Mejores prácticas de la configuración para CES ESA

Contenido

Introducción

Este documento proporciona un resumen de recomendaciones para los administradores que usan la Seguridad del correo electrónico de la nube de Cisco (CES) para configurar su dispositivo de seguridad del correo electrónico de Cisco (ESA).

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- La administración ESA, la administración del nivel CLI y GUI

Componentes Utilizados

La información en este documento se basa en las mejores prácticas y las recomendaciones para los clientes y los administradores CES.

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.

Productos Relacionados

Este documento se puede también utilizar con estas versiones de software y hardware:

- Hardware y dispositivos virtuales (NON-CES) de las en-premisas ESA que funcionan con cualquier versión de AsyncOS para la Seguridad del correo electrónico

Mejores prácticas de la configuración para CES ESA

> Advertencia: Cualquier cambio a las configuraciones basadas en las mejores prácticas como está previsto en este documento se debe revisar y entender antes de confiar sus cambios de configuración en un entorno de producción. Consulte por favor con su ingeniero en sistemas o el equipo de cuenta CES antes de realizar los cambios de configuración con los cuales usted el 100% no entiende ni tiene comodidad al administrar.

Servicios de seguridad

Anti-Spam de IronPort (IPA)

- Siempre el 1.5 MB de la exploración y nunca analiza el 2 MB

Filtrado de URL

- Clasificación y reputación del permiso URL
- Seguimiento de la interacción de la red del permiso

Detección de Graymail

- Talla 1 MB de los mensajes del permiso y del máximo

Filtros del brote

- Habilite las reglas adaptantes, la talla 1 máxima MB de la exploración
- Habilite el seguimiento de la interacción de la red

Protección avanzada de Malware

- Tipos de archivo adicionales del permiso después de habilitar la característica

Seguimiento de mensajes

- Registro rechazado permiso de la conexión (si procede)

Administración del sistema

Usuarios

- Fije las políticas de contraseña
- Si Lightweight Directory Access Protocol (LDAP) posible de la palancada para la autenticación

Suscripciones del registro

- Registros del historial de configuración del permiso
- Registros del Filtrado de URL del permiso
- Encabezado adicional del registro “de”

Cambios de nivel CLI

Filtrado de URL de la Seguridad SD de la red

- **websecurityadvancedconfig**

```
Do you want to disable DNS lookups? [N]> y

Enter the maximum number of URLs that should be scanned:
[100]> 20

Enter the threshold value for outstanding requests:
[50]> 5

Enter the default time-to-live value (seconds):
[30]> 600

Do you want to rewrite all URLs with secure proxy URLs? [Y]> n
```

Registro URL

- ESA habilitando el Filtrado de URL y las mejores prácticas
- **outbreakconfig**

```
Logging of URLs is currently disabled.

Do you wish to enable logging of URL's? [N]> y

Logging of URLs has been enabled.
```

Filtro del Anti-spoof

- Detección forjada del correo electrónico (FED) con la Seguridad del correo electrónico de Cisco

Encabezado que sella el filtro

- escriba y habilite

```
Logging of URLs is currently disabled.

Do you wish to enable logging of URL's? [N]> y

Logging of URLs has been enabled.
```

Tabla del acceso del host

Grupos adicionales del remitente

- Guía del usuario ESA: Crear un grupo del remitente para el manejo de mensajes SKIP_SBRS – Coloque más arriba para las fuentes que saltan la reputaciónSPOOF_ALLOW – Filtro del spoofing de la parte dePARTNER – Para TLS forzó las conexiones

En el grupo predefinido del remitente SUSPECTLIST

- Guía del usuario ESA: Verificación del remitente: Host permiso “calificaciones SBR en ninguno”Opcionalmente, el permiso “conexión de operaciones de búsqueda del expediente PTR del host falla debido al error de DNS temporal”

Muestra agresiva del SOMBRERO

- LISTA NEGRA [-10 a la DIRECTIVA -2]: BLOQUEADO
- SUSPECTLIST [-2 a la DIRECTIVA -1]: HEAVYTHROTTLED
- GRAYLIST[-1 a 2 y NINGUNO] DIRECTIVA: LIGHTTHROTTLED
- ACCEPTLIST [2 a la DIRECTIVA 10]: ACEPTADO

> **Note**: Los ejemplos antedichos del SOMBRERO muestran las directivas además configuradas del flujo de correo. Para toda la información sobre MFP, refiera por favor al guía del usuario de la versión apropiada de AsyncOS para la Seguridad del correo electrónico que se ejecuta en su ESA. Ejemplo, AsyncOS 10.0: Tabla del acceso del host (SOMBRERO), grupos del remitente, y directivas del flujo de correo

Directiva del flujo de correo (parámetros de la política predeterminada)

Ajustes de seguridad

- Fije Transport Layer Security (TLS) a preferido
- Habilite el Marco de políticas del remitente (el SPF)
- Habilite los DomainKeys Identified Mail (el DKIM)
- Habilite la autenticación del mensaje basada en el dominio, la información y la verificación de la conformidad (DMARC) y envíe los informes globales del feedback

> **Note**: DMARC requiere ajustar adicional a configurar. Para toda la información sobre DMARC, refiera por favor al guía del usuario de la versión apropiada de AsyncOS para la Seguridad del correo electrónico que se ejecuta en su ESA. Ejemplo, AsyncOS 10.0: Verificación DMARC

Directivas del correo entrante

Umbrales del Anti-Spam

- Los umbrales se deben dejar en los umbrales predeterminados. La modificación de anotar podía dar lugar a un aumento del falso positivo.

Contra virus

- Exploración del mensaje: Exploración para los virus solamente
- Los mensajes de Unscannable, virus infectaron los mensajes: fije el “mensaje original del archivo” a ningún

AMP

- Agregue el “AMP” para sujetar Prepend para Unscannable, neutralización “mensaje del archivo”

Graymail

- El analizar habilitado para cada veredicto, Prepend el tema y lo entrega
- Agregue la x-encabezado para el correo electrónico a granel, encabezado = “X-BulkMail”, valor = “verdad”

Filtros del brote

- El nivel predeterminado de la amenaza es 3, ajusta por favor según sus requerimientos de seguridad Si la amenaza llana para un mensaje iguala o excede este umbral, el mensaje será enviado a la cuarentena del brote. (amenaza 1=lowest, amenaza 5=highest)
- Modificación del mensaje del permiso. Reescritura URL para el mensaje sin signo
- El tema del cambio prepend a: [Possible $threat_category Fraud]

Directivas salientes del correo

Contra virus

- Exploración del mensaje
- Exploración para los virus solamenteel O.N.U-control incluye una X-encabezado con los resultados de la exploración AV en el mensaje
- Para todos los mensajes: Avanzado > la otra notificación, permiso “otras” e incluye la dirección de correo electrónico del contacto admin/SOC

Cuarentenas de la directiva

PRE-cree las cuarentenas siguientes:

- Entrante inadecuado
- Saliente inadecuado
- Entrante malévolo URL
- Saliente malévolo URL
- Spoof sospechado
- Malware

Otras configuraciones

Diccionarios

- Blasfemia del permiso/del estudio y diccionario sexual de los términos
- Cree el diccionario forjado del correo electrónico con los nombres ejecutivos
- Cree el diccionario para las palabras claves restrictas u otras

Controles del destino

- Permiso TLS para el destino predeterminado
- Fije los umbrales inferiores para los dominios del webmail
- Límite de velocidad su propio correo saliente con las configuraciones del control del destino

Filtros contentos

> **Note**: Para toda la información sobre los filtros contentos, refiera por favor al guía del usuario de la versión apropiada de AsyncOS para la Seguridad del correo electrónico que se ejecuta en su ESA. Ejemplo, AsyncOS 10.0: Filtros contentos

Filtro contento inadecuado

- La blasfemia de las condiciones O sexuales diccionario hace coincidir, envía una copia a la cuarentena inadecuada

Filtro malévolo del contenido de la reputación URL

- Envíe una copia al URL malévolo (-10 a -6) para quarantine

Filtro del contenido de la categoría URL con éstos seleccionados

- Adulto, pornografía, pederastia, jugando
- Envíe una copia a la cuarentena inadecuada

Detección forjada del correo electrónico

- “Executives_FED nombrado diccionario”
- Cuarentena del umbral 90 FED() una copia

Filtro contento habilitado macro de los documentos

- si una o más conexiones contienen una macro
- Condición opcional - > de los SBR untrusted extiéndase
- Envíe una copia para quarantine

Protección de la conexión

- si se protegen una o más conexiones
- Condición opcional - > de los SBR untrusted extiéndase
- Envíe una copia para quarantine

Información Relacionada

- BRKSEC-2131 - Seguridad del correo electrónico de Cisco: Mejores prácticas y ajuste fino (2016 Las Vegas)
- BRKSEC-2131 - Seguridad del email para la gente del NON-E-correo (2015 San Diego)
- BRKSEC-3770 - (DMARC) - no son phish: buceo de profundidad en las técnicas de autenticación del email (2014 San Francisco)
- Acuerdo de licencia de usuario final CES
- Descripción de servicio CES
- Términos de la nube del Cisco Universal
- Soporte Técnico y Documentación - Cisco Systems