Comprensión de los registros de acceso de Secure Web Appliance

Contenido

Introducción

Este documento describe la estructura del registro de acceso de Secure Web Appliance (SWA).

Prerequisites

Requirements

Cisco recomienda conocer estos temas:

- Acceso a la interfaz de línea de comandos (CLI) de SWA.

- Acceso administrativo al SWA.
- Comprensión básica del flujo de trabajo SWA.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Estructura de AccessLog

En este artículo, la estructura de AccessLog se explica con este ejemplo:

```
1726597763.348 68855 192.168.1.10 TCP_MISS/200 97645 TCP_CONNECT 10.37.145.84:443 "AMOJARRA\amirhossein
```

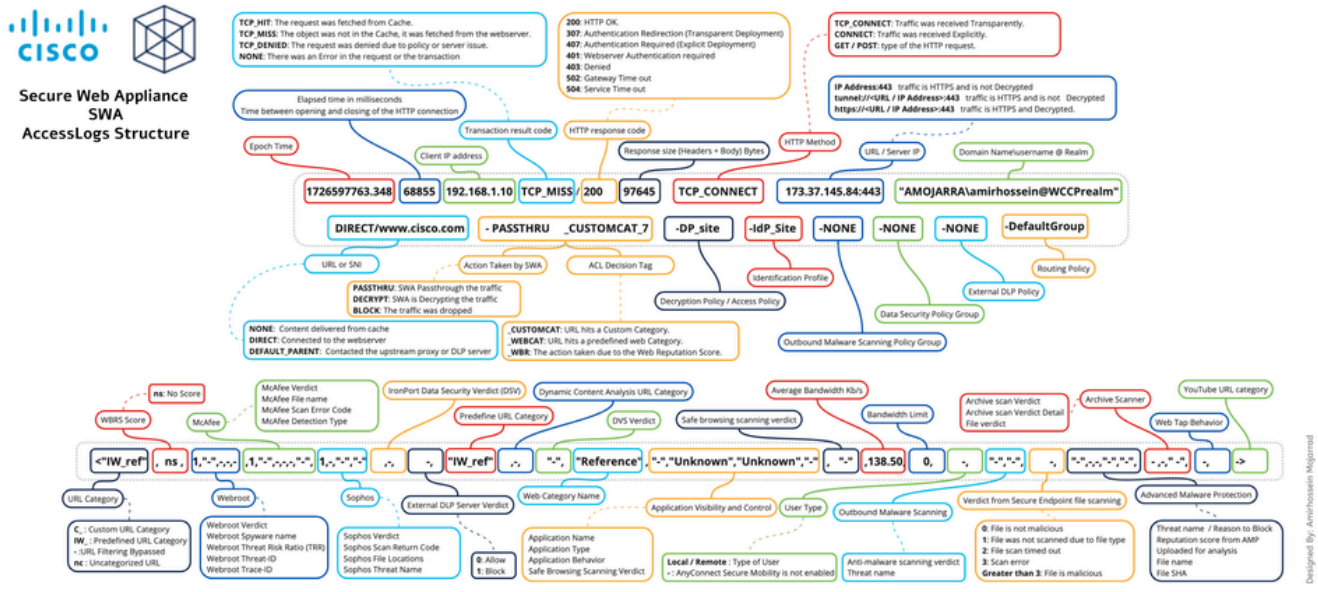

Imagen - Estructura de AccessLog

Nota: La estructura de los registros de acceso depende de la versión de SWA. Al principio de cada archivo de AccessLog hay una línea que muestra su estructura y el orden del especificador de formato.

Sección	Ejemplo de AccessLog	Especificador de formato	Detalles
Tiempo de época	1726597763.348	%t	El tiempo Epoch (a menudo llam sistema para realizar un seguim de segundos (o milisegundos/mi el 1 de enero de 1970, a las 00:(

			La hora de Epoch en la que fina Puede convertir este valor media línea o cualquier sistema operat
Tiempo transcurrido	68855	%e	La cantidad de milisegundos qu completarse/anularse y de que s
Dirección IP de origen	192.168.1.10	%a	Dirección IP de origen/cliente.
Código de resultado de transacción	TCP_MISS	%w	El código de resultado de la tran solicitudes de los clientes. A continuación se muestra la list

TCP_HIT
TCP_IMS_HIT
TCP_MEM_HIT
TCP_MISS
TCP_REFRESH_HIT

			TCP_CLIENT_REFRESH_MISS TCP_DENIED HTTPS de TCP_DENIED_SSL TCP_CLIENT_REFRESH_MISS HTTPS DE TCP_MISS_SSL
Código de respuesta HTTP	/200	%h	El código de respuesta HTTP re el servidor Web en respuesta a A continuación se muestra la list importantes (para obtener más i respuesta HTTP de este artículo Código de estado: Significado 000: 000 es un código de interrupción en la co tarde durante la tra

			2xx correcto	
			200	OK
			204	Sin contenido
			206	Contenido parcial (t intervalo)
			Redirección 3xx	
			301	Redirección perma
			302	Redirección tempor
			304	No modificado
			307	Redirección tempor (Normalmente se ob mientras SWA aute
			Error de cliente 4xx	
			400	Solicitud incorrecta
			401	Se requiere autenti observa en la imple autentica al usuario
			403	Prohibido
			404	Not found
			407	Se requiere autenti
			5xx Error de servidor	
			500	Error interno del se
			502	Gateway incorrecto
			503	Servicio no disponib
			504	Tiempo de espera c
Tamaño total	97645	%s	Total de bytes transferidos para	

transferido			
Método HTTP	TCP_CONNECT	%1r	Un método HTTP es un método especifique la acción que un ser como recuperar datos con GET GET — El m dato únic deb térm POST — El m dato el cu envi dato CONNECT(conectar) — El m esta prox con dest tráfi cifra Indi expl está dire TCP_CONNECT — Indi tran WC
Destino	10.37.145.84:443	%2r	En esta sección se muestra la U puerto TCP. En la redirección transparente, a muestra la dirección IP de destin Si la URL comienza con tunnel:/

<table>
<tr><td></td><td></td><td></td><td>tráfico.

Si la URL comienza con https://</td></tr>
<tr><td>Nombre de usuario y rango de autenticación</td><td>"AMOJARRA\amirhossein@WCCPrealm"</td><td>%A</td><td>Credenciales utilizadas para est

Si la solicitud se autentica, SWA rangos de autenticación como:

<Domain Name> \ <User Name>

Si la solicitud aún no se ha aute el registro verá el guión "-"</td></tr>
<tr><td>Tipo de acceso</td><td>DIRECT/</td><td>%H</td><td>Código que describe el servidor contenido de la solicitud.

Los valores más comunes incluy
<table><tr><td>NINGUNO</td><td>El proxy w puso en co recuperar</td></tr><tr><td>DIRECT</td><td>El proxy w solicitud pa</td></tr><tr><td>DEFAULT_PARENT</td><td>El proxy w servidor D</td></tr></table></td></tr>
<tr><td>Dirección del servidor</td><td>www.cisco.com</td><td>%d</td><td>Dirección IP del servidor o del o</td></tr>
<tr><td>MIME content-type/subtype</td><td>-</td><td>%c</td><td>MIME Indica la naturaleza y el f surtido de bytes. Los tipos MIME 6838

Dos tipos MIME principales son predeterminados:

• text/plain es el valor prede archivo de texto debe ser l contener datos binarios.</td></tr>
</table>

<table>
<tr>
<td></td>
<td></td>
<td></td>
<td>

application/octet-stream es
demás casos. Un tipo de a
Los navegadores prestan
archivos, para proteger a l
software y de posibles com

Para obtener una lista completa
(iana)
</td>
</tr>
<tr>
<td>Etiqueta de decisión de ACL</td>
<td>PASSTHRU_CUSTOMCAT_7-</td>
<td>%D</td>
<td>
Una etiqueta de decisión ACL es
acceso que indica cómo el proxy
información de los filtros de Web
motores de análisis.

Nota: El final de la etiqueta
generado dinámicamente q
aumentar el rendimiento. P

Esta es una lista de las etiquetas
(Para obtener más información,
ACL en este artículo)
<table>
<tr><td>Etiqueta de decisión de ACL</td></tr>
<tr><td>ALLOW_CUSTOMCAT</td></tr>
<tr><td>ALLOW_WBRS</td></tr>
<tr><td>AMP_FILE_VERDICT</td></tr>
<tr><td>BLOCK_ADMIN</td></tr>
</table>
</td>
</tr>
</table>

			BLOCK_ADMIN_CONNECT
			BLOCK_ADMIN_CUSTOM_USE
			BLOCK_ADMIN_TUNNELING
			BLOCK_ADMIN_FILE_TYPE
			BLOCK_ADMIN_PROTOCOL
			BLOCK_AMP_RESP
			BLOCK_AVC
			BLOCK_CONTENT_UNSAFE

			BLOCK_CUSTOMCAT
			BLOCK_ICAP
			BLOCK_WBRS
			BLOCK_WEBCAT
			BLOCK_YTCAT
			DESCIFRAR_ADMIN
			DECRYPT_EUN_CUSTOMCAT
			DECRYPT_EUN_WBRS

			DESCIFRAR_EUN_WEBCAT
			DESCIFRAR_WEBCAT
			DESCIFRAR_WBRS
			DROP_ADMIN
			DROP_WEBCAT
			DROP_WBRS
			PASSTHRU_ADMIN

			PASSTHRU_WEBCAT PASSTHRU_WBRS OTRO
Nombre de política	DP_site-	N/A	Dependiendo del tipo de tráfico, • Nombre de la política de d está descifrado • Nombre de política de acc descifrado.
Política de identidad	IdP_Site-	N/A	Muestra el nombre del perfil de i
Grupo de políticas de escaneo de malware saliente	NINGUNO-	N/A	Nombre del grupo de políticas d Cualquier espacio en el nombre guión bajo (_)
Grupo de políticas de seguridad de datos	NINGUNO-	N/A	Nombre del grupo de políticas d transacción coincide con la polít este valor es DefaultGroup. Este aparece cuando los filtros de se habilitados. "NONE" aparece cu de seguridad de datos. Cualquier espacio en el nombre guión bajo (_)

<table>
<tr><td>Grupo de políticas DLP externas</td><td>NINGUNO-</td><td>N/A</td><td>Cuando la transacción coincide
valor es DefaultGroup. Aparece
ninguna política DLP externa.

Cualquier espacio en el nombre
guión bajo (_).</td></tr>
<tr><td>Grupo de políticas de enrutamiento</td><td>DefaultGroup-</td><td>N/A</td><td>Nombre del grupo de directivas
ProxyGroupName/ProxyServerN

Cuando la transacción coincide
este valor es DefaultRouting. Cu
upstream, este valor es DIRECT

Cualquier espacio en el nombre
guión bajo (_).</td></tr>
<tr><td>Toque Tráfico web</td><td>NINGUNO</td><td>N/A</td><td>Tráfico web Toque el nombre de</td></tr>
<tr><td>Abreviatura de categoría de URL</td><td><"C_Cisco",</td><td>%XC</td><td>Categoría de URL con la que co
<table><tr><td>-</td><td>Filtrado de URL om</td></tr><tr><td>nc</td><td>URL no categorizad</td></tr><tr><td>error</td><td>Filtrado de URL om</td></tr><tr><td>imp</td><td>Imposible</td></tr><tr><td>IW_</td><td>Si el nombre de la c
comienza por IW_,
solicitud estaba lleg
categoría de URL d
Predefine</td></tr><tr><td>C_</td><td>Si el nombre de la c
comienza por IC_, s
solicitud estaba alc
categoría de URL p</td></tr></table></td></tr>
</table>

<table>
<tr><td>Puntuación de reputación en la Web</td><td>-,</td><td>%XW</td><td>Este campo muestra la puntuaci
ns significa que la URL no tiene</td></tr>
<tr><td>Exploración de Webroot</td><td>-,"-",-,-,-,</td><td></td><td>Estos 5 campos están relaciona
<table>
<tr><td>Veredicto de Webroot,</td><td>%Xv</td></tr>
<tr><td>Spyname De Webroot,</td><td>"%Xn"</td></tr>
<tr><td>Webroot TRR,</td><td>%Xt</td></tr>
<tr><td>ThreatID de Webroot</td><td>%Xs</td></tr>
<tr><td>ID de seguimiento de Webroot,</td><td>%Xi</td></tr>
</table></td></tr>
</table>

Escaneo de McAfee	-,"-",-,-,-,"-",		Estos 6 campos están relaciona	
			Veredicto de McAfee,	%Xd
			Nombre de archivo de McAfee,	"%Xe"
			Código de error de análisis de McAfee,	%Xf
			Tipo de detección de McAfee,	%Xg
			Tipo de virus de McAfee,	%Xh

			Nombre de virus de McAfee,	"%Xj"
Escaneo de Sophos	-,-,"-","-",		Estos 4 campos están relaciona	
			Veredicto de Sophos,	%XY
			Código de retorno de Sophos Scan,	%Xx
			Ubicaciones de archivos de Sophos,	"%Xy"
			Nombre de la amenaza de Sophos,	"%Xz"
Veredicto del análisis de	-,	%Xl	El veredicto del análisis de Cisc columna Contenido de la política	

Cisco Data Security			Esta lista describe los valores po 0.Permitir 1.Bloqueo - (guión).Los filtros de seguridad análisis. Este valor aparece cua Cisco están desactivados o cua establece en Permitir.
Veredicto de exploración de DLP externa	-,	%Xp	El veredicto de la exploración de proporcionado en la respuesta I Esta lista describe los valores po 0.Permitir 1.Bloqueo - (guión).El servidor DLP externo aparece cuando el análisis de D contenido no se ha analizado de página Políticas de DLP externa
Veredicto de categoría de URL predefinida	"-",	%XQ	El veredicto predefinido de la ca análisis de la solicitud, abreviad Este campo muestra un guión (desactivado. Si la solicitud llega a una catego nombre de la categoría de URL la decisión la tomó la categoría Para obtener una lista de abrevi consulteDescripciones de categ
Veredicto de categoría de URL	-,	%XA	El veredicto de la categoría de U de contenido dinámico (DCA) du abreviado. Se aplica únicamente al motor d web de Cisco. nc: Este valor aparece en el vere cuando el motor de análisis de c

			ha asignado ninguna categoría d que indica que la URL no se ha inicial antes de que el análisis de
Veredicto de Unified Inbound DVS	"-",	%XZ	Veredicto de escaneo anti-malw proporciona la categoría de malw de escaneo que estén habilitado bloqueadas o supervisadas debi
Tipo de amenaza de Web Reputation Filter	"-",	%Xk	Los filtros de Web Reputation de de amenaza. El nombre de cate la Web es alta y el tipo de amen Normalmente, este campo se re -4 o inferior.
URL encapsulada de Google Translate	"-",	%X#10#	La URL que se encapsula dentro hay una URL encapsulada, el va
Control de aplicaciones (AVC/ADC)	"-","-","-",		En estos 3 campos se registran aplicaciones (AVC) y de descub

Nombre de la aplicación AVC/ADC	"%XO"	
Tipo de aplicación de AVC/ADC	"%Xu"	
Comportamiento de la aplicación AVC/ADC	"%Xb"	

<table>
<tr><td>Veredicto de navegación segura</td><td>"-",</td><td>%XS</td><td>Este valor indica si se aplicó a la segura o la función de clasificac<table><tr><td>atracar</td><td>La solicitud original del de búsqueda segura.</td></tr><tr><td>cifrar</td><td>La solicitud original del característica de clasific</td></tr><tr><td>unsupp</td><td>La solicitud original del no compatible.</td></tr><tr><td>error</td><td>La solicitud original del aplicar la función de bús contenido del sitio debid</td></tr><tr><td>-</td><td>Ni la función de búsque contenido del sitio se ap omitieron las caracterís permitió en una categor realizó desde una aplica</td></tr></table></td></tr>
<tr><td>Ancho de banda medio</td><td>11.35,</td><td>%XB</td><td>El ancho de banda medio consu</td></tr>
<tr><td>Control de límite de ancho de banda</td><td>0,</td><td>%XT</td><td>Valor que indica si la solicitud se control de límite de ancho de ba
"1" indica que la solicitud se ha
"0" indica que la solicitud no se</td></tr>
<tr><td>Tipo de usuario</td><td>-,</td><td>%I</td><td>El tipo de usuario que realiza la
Solo se aplica cuando AnyConn
Cuando no está habilitado, el va</td></tr>
<tr><td>Escaneo de malware</td><td>"-","-",</td><td></td><td>Estos 2 campos se aplican a las supervisadas debido al análisis</td></tr>
</table>

<table>
<tr>
<td>saliente</td>
<td></td>
<td></td>
<td>una directiva de escaneo de ma
<table>
<tr><td>Veredicto DVS de salida de Unified</td><td>"%X3"</td></tr>
<tr><td>Nombre de amenaza saliente</td><td>"%X4"</td></tr>
</table>
</td>
</tr>
<tr>
<td>Protección frente a malware avanzado</td>
<td>-,"-",-,-,"-","-",</td>
<td></td>
<td>Estos 6 campos están relaciona
conocido como protección frente
<table>
<tr><td>Veredicto de archivo</td><td>%X#</td></tr>
</table>
</td>
</tr>
</table>

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td>Nombre de amenaza</td><td>%X#</td></tr>
<tr><td>Puntuación de reputación</td><td>%X#</td></tr>
<tr><td>Cargar acción para análisis</td><td>%X#</td></tr>
<tr><td>Nombre del archivo</td><td>%X#</td></tr>
<tr><td>Archivo SHA</td><td>%X#</td></tr>
</table>
</td></tr>
<tr><td>Análisis de archivo</td><td>-,-,"-",</td><td></td><td>
Estos 3 campos indican el estad
almacenamiento:
<table>
<tr><td>Veredicto de análisis de archivo</td><td>%X#8#</td><td>Veredicto de a
ARCHIVESCA</td></tr>
</table>
</td></tr>
</table>

					ARCHIVESCA
					ARCHIVESCA
					ARCHIVESCA

					ARCHIVESCA
					ARCHIVESCA
			Detalle de veredicto de análisis de archivo	%Xo	Detalle de ver archivo de alm bloqueado (AR función de la p personalizada detalles de ver bloqueado y e "Archivo no es que el archivo

					bloqueado.
			Veredicto de archivo	%Xm	Veredicto de a
Toque Web	-,	%XU	Comportamiento de Web Tap.		
Categoría de URL de YouTube	- >	%X#29#	La categoría de URL de YouTub Este campo muestra "nc" cuand		

Código de respuesta HTTP

Esta es la lista completa de código de respuesta HTTP

Código de estado	Significado
Información 1xx	
100	Continúe
101	Protocolos de switching
102	Procesamiento
103	Sugerencias tempranas
2xx correcto	
200	OK
201	Creado
202	Aceptado
203	Información no autorizada
204	Sin contenido
205	Restablecer contenido
206	Contenido parcial
207	Estado múltiple

208	Ya informado
226	IM utilizada
Redirección 3xx	
300	Varias opciones
301	Movido permanentemente
302	Encontrado (previamente "movido temporalmente")
303	Ver otros
304	No modificado
305	Utilizar proxy
306	Switch Proxy
307	Redirección temporal para autenticación (Normalmente se observa en la implementación transparente mientras SWA autentica al usuario)
308	Redireccionamiento permanente
Error de cliente 4xx	
400	Solicitud incorrecta
401	Se requiere autenticación de servidor web (normalmente se observa en la implementación transparente mientras SWA autentica al usuario)
402	Pago requerido
403	Prohibido
404	Not found
405	Método no permitido
406	No aceptable
407	Se requiere autenticación de proxy explícita
408	Tiempo de espera de solicitud
409	Conflicto
410	Desaparecido
411	Longitud requerida

412	Error de condición previa
413	Carga útil demasiado grande
414	URI demasiado largo
415	Tipo de medio no compatible
416	Rango no satisfecho
417	Error de expectativa
418	Soy una tetera
421	Solicitud mal dirigida
422	Entidad no procesable
423	Bloqueado
424	Dependencia fallida
425	Demasiado pronto
426	Actualización necesaria
428	Requisito previo necesario
429	Demasiadas solicitudes
431	Campos de encabezado de solicitud demasiado grandes
451	No disponible por motivos legales
5xx Error de servidor	
500	Error interno del servidor
501	No implementado
502	Gateway incorrecto
503	Servicio no disponible
504	Tiempo de espera de gateway
505	Versión HTTP no admitida
506	Variant también negocia
507	Almacenamiento insuficiente
508	Bucle detectado
510	No extendido
511	Se requiere autenticación de red

Etiqueta de decisión de ACL

Esta es la lista completa de las etiquetas de decisión de ACL:

Etiqueta de decisión de ACL	Descripción
ALLOW_ADMIN_ERROR_PAGE	El proxy web permitió la transacción a una página de notificación y a cualquier logotipo utilizado en esa página.
ALLOW_CUSTOMCAT	El proxy web permitió la transacción basándose en la configuración de filtrado de categoría de URL personalizada para el grupo de políticas de acceso.
ALLOW_REFERER	El proxy web permitió la transacción basándose en una exención de contenido integrado/referido.
ALLOW_WBRS	El proxy de web permitió la transacción basándose en la configuración del filtro de reputación web para el grupo de políticas de acceso.
AMP_FILE_VERDICT	Valor que representa un veredicto del servidor de reputación de AMP para el archivo:
	1 - Desconocido
	2 - Limpio
	3 - Malintencionado
	4 - No escaneable
ARCHIVESCAN_ALLCLEAR	Veredicto de análisis de archivo
ARCHIVESCAN_BLOCKEDFILETYPE	ARCHIVESCAN_ALLCLEAR - No hay tipos de archivo bloqueados en el archivo inspeccionado.
ARCHIVESCAN_NESTEDTOODEEP	ARCHIVESCAN_BLOCKEDFILETYPE - Hay un tipo de archivo bloqueado en el archivo inspeccionado. El siguiente campo de la entrada del registro (Detalle del veredicto) proporciona detalles, en concreto el tipo de archivo bloqueado y el nombre del archivo bloqueado.
ARCHIVESCAN_UNKNOWNFMT	ARCHIVESCAN_NESTEDTOODEEP - El archivo está bloqueado porque

	contiene más archivos "encapsulados" o anidados que el máximo configurado. El campo Detalle de veredicto contiene "Archivo no escaneable bloqueado".
ARCHIVESCAN_UNSCANABLE	ARCHIVESCAN_UNKNOWNFMT - El archivo está bloqueado porque contiene un tipo de archivo de formato desconocido. El detalle del veredicto es "Archivo no escaneable bloqueado".
ARCHIVESCAN_FILETOOBIG	ARCHIVESCAN_UNSCANABLE - El archivo está bloqueado porque contiene un archivo que no se puede analizar. El detalle del veredicto es "Archivo no escaneable bloqueado".
	ARCHIVESCAN_FILETOOBIG - El archivo está bloqueado porque el tamaño del archivo es mayor que el máximo configurado. El detalle del veredicto es "Archivo no escaneable bloqueado".
	Detalle de veredicto de análisis de archivo
	El campo Veredicto y el campo Veredicto de la entrada del registro proporcionan información adicional sobre el veredicto, como el tipo de archivo bloqueado y el nombre del archivo bloqueado, "Archivo no escaneable bloqueado" o "-" para indicar que el archivo no contiene ningún tipo de archivo bloqueado.
	Por ejemplo, si un archivo de almacenamiento inspeccionable está bloqueado (ARCHIVESCAN_BLOCKEDFILETYPE) en función de la política de acceso: Configuración personalizada de bloqueo de objetos, la entrada Detalles del veredicto incluye el tipo de archivo bloqueado y el nombre del archivo bloqueado.
	Consulte Políticas de acceso: Bloquear objetos y Configuración de inspección de archivo para obtener más información sobre la inspección de archivo.

BLOCK_ADMIN	Transacción bloqueada según algunos valores predeterminados del grupo de políticas de acceso.
BLOCK_ADMIN_CONNECT	Transacción bloqueada basada en el puerto TCP del destino, como se define en la configuración Puertos HTTP CONNECT para el grupo de políticas de acceso.
BLOCK_ADMIN_CUSTOM_USER_AGENT	Transacción bloqueada según el agente de usuario definido en la configuración Bloquear agentes de usuario personalizados para el grupo de directivas de acceso.
BLOCK_ADMIN_TUNNELING	El proxy web bloqueó la transacción basándose en la tunelización del tráfico no HTTP en los puertos HTTP para el grupo de políticas de acceso.
BLOCK_ADMIN_HTTPS_NonLocalDestination	Transacción bloqueada; El cliente intentó omitir la autenticación utilizando el puerto SSL como proxy explícito. Para evitar esto, si una conexión SSL se establece con el propio WSA, solo se permiten las solicitudes al nombre de host de redirección de WSA real.
BLOCK_ADMIN_IDS	Transacción bloqueada en función del tipo MIME del contenido del cuerpo de la solicitud según se define en el grupo de políticas de seguridad de datos.
BLOCK_ADMIN_FILE_TYPE	Transacción bloqueada según el tipo de archivo definido en el grupo de políticas de acceso.
BLOCK_ADMIN_PROTOCOL	Transacción bloqueada según el protocolo definido en la configuración Bloquear protocolos para el grupo de directivas de acceso.
BLOCK_ADMIN_SIZE	Transacción bloqueada en función del tamaño de la respuesta según se define en la configuración Tamaño del objeto para el grupo de políticas de acceso.
BLOCK_ADMIN_SIZE_IDS	Transacción bloqueada en función del tamaño del contenido del cuerpo de la solicitud según se define en el grupo de políticas de seguridad de datos.
BLOCK_AMP_RESP	El proxy web bloqueó la respuesta basándose en la configuración de protección frente a malware avanzado

	del grupo de políticas de acceso.
BLOCK_AMW_REQ	El proxy web bloqueó la solicitud basándose en la configuración anti-malware del grupo de políticas de escaneo de malware saliente. El organismo de solicitud emitió un veredicto positivo de Malware.
BLOCK_AMW_RESP	El proxy web bloqueó la respuesta basándose en la configuración anti-malware del grupo de políticas de acceso.
BLOCK_AMW_REQ_URL	El proxy web sospecha que la URL de la solicitud HTTP no puede ser segura, por lo que bloqueó la transacción a la hora de la solicitud en función de la configuración anti-malware del grupo de políticas de acceso.
BLOCK_AVC	Transacción bloqueada según la configuración de la aplicación para el grupo de políticas de acceso.
BLOCK_CONTENT_UNSAFE	Transacción bloqueada según la configuración de clasificación de contenido del sitio para el grupo de directivas de acceso. La solicitud del cliente era para contenido para adultos y la política está configurada para bloquear contenido para adultos.
BLOCK_CONTINUE_CONTENT_UNSAFE	Transacción bloqueada y mostrada en la página Advertir y continuar según la configuración de clasificación de contenido del sitio en el grupo Directiva de acceso. La solicitud del cliente era para contenido para adultos y la política está configurada para dar una advertencia a los usuarios que acceden a contenido para adultos.
BLOCK_CONTINUE_CUSTOMCAT	La transacción se bloqueó y se mostró en la página Advertir y continuar en función de una categoría de URL personalizada del grupo de políticas de acceso configurado como "Advertir".
BLOCK_CONTINUE_WEBCAT	La transacción se bloqueó y se mostró en la página Advertir y continuar en función de una categoría de URL predefinida en el grupo de políticas de acceso configurado como "Advertir".

BLOCK_CUSTOMCAT	Transacción bloqueada según la configuración de filtrado de categoría de URL personalizado para el grupo de políticas de acceso.
BLOCK_ICAP	El proxy de web bloqueó la solicitud basándose en el veredicto del sistema DLP externo definido en el grupo de políticas DLP externas.
BLOCK_SEARCH_UNSAFE	La solicitud del cliente incluía una consulta de búsqueda no segura y la directiva de acceso está configurada para aplicar búsquedas seguras, por lo que se bloqueó la solicitud del cliente original.
BLOCK_SUSPECT_USER_AGENT	Transacción bloqueada según la configuración del agente de usuario sospechoso para el grupo de políticas de acceso.
BLOCK_UNSUPPORTED_SEARCH_APP	Transacción bloqueada según la configuración de búsqueda segura del grupo de políticas de acceso. La transacción era para un motor de búsqueda no compatible y la política está configurada para bloquear motores de búsqueda no compatibles.
BLOCK_WBRS	Transacción bloqueada en función de la configuración de filtro de Web Reputation para el grupo de políticas de acceso.
BLOCK_WBRS_IDS	El proxy web bloqueó la solicitud de carga basándose en la configuración del filtro de reputación web para el grupo de políticas de seguridad de datos.
BLOCK_WEBCAT	Transacción bloqueada según la configuración de filtrado de categorías de URL para el grupo de políticas de acceso.
BLOCK_WEBCAT_IDS	El proxy web bloqueó la solicitud de carga basándose en la configuración de filtrado de categorías de URL para el grupo de políticas de seguridad de datos.
BLOCK_YTCAT	El proxy web bloqueó la transacción basándose en la configuración de filtrado de categorías de YouTube

	predefinida para el grupo de políticas de acceso.
BLOCK_CONTINUE_YTCAT	El proxy de web bloqueó la transacción y mostró la página Advertir y continuar en función de una categoría de YouTube predefinida en el grupo de políticas de acceso configurado como 'Advertir'.
DESCIFRAR_ADMIN	El proxy web descifró la transacción basándose en algunos valores predeterminados para el grupo de políticas de descifrado.
DECRYPT_ADMIN_EXPIRED_CERT	El proxy web descifró la transacción aunque el certificado del servidor ha caducado.
DECRYPT_EUN_ADMIN_DEFAULT_ACTION	El proxy web descifró la transacción basándose en la configuración predeterminada como conexión de caída para el grupo de políticas de descifrado cuando EUN está habilitado.
DECRYPT_EUN_ADMIN_EXPIRED_CERT	El proxy web descifró la transacción cuando la configuración del proxy HTTPS descarta un certificado caducado con EUN activado.
DECRYPT_EUN_ADMIN_INVALID_LEAF_CERT	El proxy web descifró la transacción cuando la configuración del proxy HTTPS descarta un certificado de hoja no válido con EUN habilitado.
DECRYPT_EUN_ADMIN_MISMATCHED_HOSTNAME	El proxy web descifró la transacción cuando la configuración del proxy HTTPS descarta el nombre de host no coincidente con EUN habilitado.
DECRYPT_EUN_ADMIN_OCSP_OTHER_ERROR	El proxy web descifró la transacción cuando la configuración del proxy HTTPS descarta un OCSP con otros errores con EUN habilitado.
DECRYPT_EUN_ADMIN_OCSP_REVOKED_CERT	El proxy web descifró la transacción cuando la configuración de proxy HTTPS descarta un certificado revocado de OCSP con EUN habilitado.
DECRYPT_EUN_ADMIN_UNRECOGNIZED_ROOT_CERT	El proxy web descifró la transacción cuando la configuración del proxy HTTPS descarta una autoridad raíz no reconocida o un certificado de emisor con EUN habilitado.
DECRYPT_EUN_CUSTOMCAT	El proxy web descifró la transacción

	basándose en la configuración de filtrado de categoría de URL personalizada para el grupo de políticas de descifrado. Si EUN está habilitado, el tráfico se descarta.
DECRYPT_EUN_WBRS	El proxy web descifró la transacción basándose en la configuración del filtro de reputación web para el grupo de políticas de descifrado. Si EUN está habilitado, el tráfico se descarta.
DECRYPT_EUN_WBRS_NO_SCORE	El proxy web descifró la transacción basándose en la configuración del filtro de reputación web para la URL sin puntuación en el grupo de políticas de descifrado. Si EUN está habilitado, el tráfico se descarta.
DESCIFRAR_EUN_WEBCAT	El proxy web descifró la transacción basándose en la configuración de filtrado de categorías de URL para el grupo de políticas de descifrado. Si EUN está habilitado, el tráfico se descarta.
DESCIFRAR_WEBCAT	El proxy web descifró la transacción basándose en la configuración de filtrado de categorías de URL para el grupo de políticas de descifrado.
DESCIFRAR_WBRS	El proxy web descifró la transacción basándose en la configuración del filtro de reputación web para el grupo de políticas de descifrado.
DEFAULT_CASE	El proxy web permitía al cliente acceder al servidor porque ninguno de los servicios AsyncOS, como Web Reputation o el análisis anti-malware, realizó ninguna acción en la transacción.
DENY_ADMIN	El proxy web denegó la transacción. Esto ocurre para las solicitudes HTTPS cuando se requiere autenticación y se inhabilita Descifrar para autenticación en la configuración de proxy HTTPS.
DROP_ADMIN	El proxy web descartó la transacción basándose en algunos valores predeterminados para el grupo de políticas de descifrado.
DROP_ADMIN_EXPIRED_CERT	El proxy web descartó la transacción

	porque el certificado del servidor ha caducado.
DROP_WEBCAT	El proxy web descartó la transacción basándose en la configuración de filtrado de categorías de URL para el grupo de políticas de descifrado.
DROP_WBRS	El proxy de web descartó la transacción basándose en la configuración del filtro de reputación web para el grupo de políticas de descifrado.
MONITOR_ADMIN_EXPIRED_CERT	El proxy web supervisó la respuesta del servidor porque el certificado del servidor ha caducado.
MONITOR_AMP_RESP	El proxy web supervisó la respuesta del servidor en función de la configuración de protección frente a malware avanzado para el grupo de políticas de acceso.
MONITOR_AMW_RESP	El proxy web supervisó la respuesta del servidor en función de la configuración anti-malware del grupo de políticas de acceso.
MONITOR_AMW_RESP_URL	El proxy web sospecha que la URL de la solicitud HTTP no puede ser segura, pero monitoreó la transacción basándose en la configuración Anti-Malware para el grupo de políticas de acceso.
MONITOR_AVC	El proxy web supervisó la transacción basándose en la configuración de la aplicación para el grupo de políticas de acceso.
MONITOR_CONTINUE_CONTENT_UNSAFE	Originalmente, el proxy web bloqueó la transacción y mostró la página Advertir y continuar basándose en la configuración de clasificación de contenido del sitio en el grupo Directiva de acceso. La solicitud del cliente era para contenido para adultos y la política está configurada para dar una advertencia a los usuarios que acceden a contenido para adultos. El usuario aceptó la advertencia y continuó en el sitio solicitado originalmente, y ningún otro motor de análisis bloqueó posteriormente la solicitud.

MONITOR_CONTINUE_CUSTOMCAT	Originalmente, el proxy web bloqueaba la transacción y mostraba la página Advertir y continuar basada en una categoría de URL personalizada del grupo de políticas de acceso configurado como "Advertir". El usuario aceptó la advertencia y continuó en el sitio solicitado originalmente, y ningún otro motor de análisis bloqueó posteriormente la solicitud.
MONITOR_CONTINUE_WEBCAT	Originalmente, el proxy web bloqueaba la transacción y mostraba la página Advertir y continuar en función de una categoría de URL predefinida en el grupo de políticas de acceso configurado como "Advertir". El usuario aceptó la advertencia y continuó en el sitio solicitado originalmente, y ningún otro motor de análisis bloqueó posteriormente la solicitud.
MONITOR_CONTINUE_YTCAT	Originalmente, el proxy web bloqueó la transacción y mostró la página Advertir y continuar basada en una categoría de YouTube predefinida en el grupo de políticas de acceso configurado como 'Advertir'. El usuario aceptó la advertencia y continuó en el sitio solicitado originalmente, y ningún otro motor de análisis bloqueó posteriormente la solicitud.
MONITOR_IDS	El proxy web analizó la solicitud de carga mediante una política de seguridad de datos o una política DLP externa, pero no bloqueó la solicitud. Evaluó la solicitud con las directivas de acceso.
MONITOR_SUSPECT_USER_AGENT	El proxy web supervisó la transacción basándose en la configuración del agente de usuario sospechoso para el grupo de políticas de acceso.
MONITOR_WBRS	El proxy de web supervisó la transacción basándose en la configuración del filtro de Web Reputation para el grupo de políticas de acceso.
NO_AUTHORIZATION	El proxy web no permitió al usuario

	acceder a la aplicación porque el usuario ya estaba autenticado en un rango de autenticación, pero no en ningún rango de autenticación configurado en la directiva de autenticación de la aplicación.
NO_PASSWORD	Error de autenticación del usuario.
PASSTHRU_ADMIN	El proxy web pasó a través de la transacción basándose en algunos valores predeterminados para el grupo de políticas de descifrado.
PASSTHRU_ADMIN_EXPIRED_CERT	El proxy web pasó a través de la transacción aunque el certificado del servidor ha caducado.
PASSTHRU_WEBCAT	El proxy web pasó a través de la transacción basándose en la configuración de filtrado de categorías de URL para el grupo de políticas de descifrado.
PASSTHRU_WBRS	El proxy web pasó a través de la transacción basándose en la configuración de filtro de Web Reputation para el grupo de políticas de descifrado.
REDIRECT_CUSTOMCAT	El proxy web redirigió la transacción a una dirección URL diferente basada en una categoría de URL personalizada del grupo de políticas de acceso configurado en "Redirigir".
SAAS_AUTH	El proxy web permitió al usuario acceder a la aplicación porque el usuario se autenticó de forma transparente en el rango de autenticación configurado en la directiva de autenticación de la aplicación.
OTRO	El proxy web no completó la solicitud debido a un error, como un error de autorización, desconexión del servidor o una anulación del cliente.

Valores de veredicto de escaneo de malware

Un veredicto de escaneo de Malware es un valor asignado a una solicitud de URL o a una respuesta del servidor que determina la probabilidad de que contenga Malware. Los motores de

exploración de Webroot, McAfee y Sophos devuelven el veredicto de exploración de malware al motor DVS, de modo que éste puede determinar si se debe supervisar o bloquear el objeto analizado. Cada veredicto de escaneo de malware corresponde a una categoría de Malware enumerada en la página Access Policies > Reputation and Anti-Malware Settings cuando edita la configuración Anti-Malware para una política de acceso determinada.

Esta lista presenta los diferentes valores de veredicto de escaneo de malware y cada categoría de malware correspondiente:

Valor de veredicto de escaneo de malware	Categoría de malware
-	no establecido
0	Desconocido
1	No analizado
2	Tiempo de espera
3	Error
4	No escaneable
10	Spyware genérico
12	Objeto de ayudante del explorador
13	Adware
14	Monitor del sistema
18	Monitor de sistema comercial
19	Marcador
20	Secuestrador

Valor de veredicto de escaneo de malware	Categoría de malware
21	URL de phishing
22	Descargador troyano
23	Caballo troyano
24	Phisher troyano
25	Gusano
26	Archivo cifrado
27	Virus
33	Otro malware
34	PUA
35	Anulado
36	Heurística de brotes
37	Archivos maliciosos y de alto riesgo conocidos

Información Relacionada

- Guía del usuario de AsyncOS 15.2 para Cisco Secure Web Appliance
- Uso de las prácticas recomendadas de Secure Web Appliance
- Garantizar la correcta funcionalidad del grupo HA de WSA virtual en un entorno VMware
- Configurar el parámetro de rendimiento en registros de acceso
- Comprensión del formato de registro de acceso HTTPS en el dispositivo web seguro
- Acceder a registros de appliances web seguros

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).