Informazioni sui log degli accessi di Secure Web Appliance

Sommario

Introduzione

In questo documento viene descritta la struttura del log degli accessi di Secure Web Appliance (SWA).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Accesso all'interfaccia della riga di comando (CLI) dell'SWA.

- Accesso amministrativo all'SWA.
- Conoscenza di base del flusso di lavoro SWA.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata

ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Struttura del log degli accessi

In questo articolo, la struttura del log degli accessi viene spiegata da questo esempio:

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

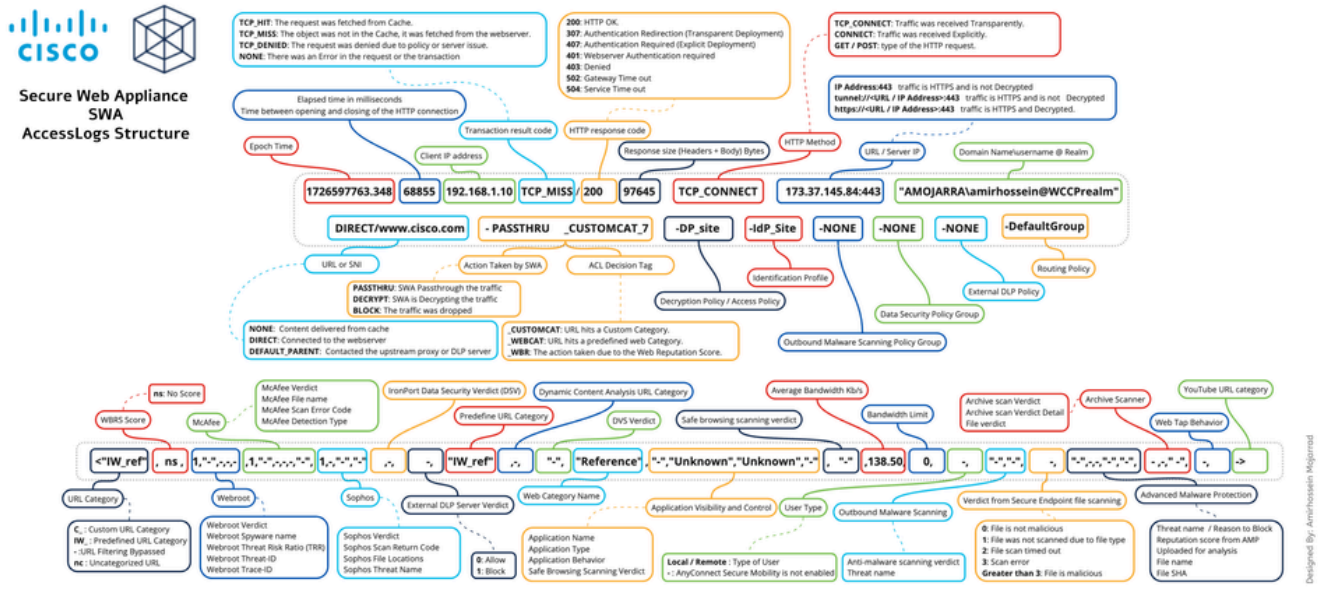

Immagine - Struttura del log degli accessi

Nota: La struttura dei log degli accessi dipende dalla versione di SWA. All'inizio di ogni file di AccessLog è presente una riga che ne mostra la struttura e l'ordine di specificazione del formato.

Sezione	Esempio da Accesslog	Specifica formato	Dettagli
Tempo di attesa	1726597763.348	%t	Il tempo Epoch (spesso chiamato sistema per il tracciamento del te secondi (o millisecondi/microsecc 00:00:00 UTC

			Ora dell'epoca in cui la transazion È possibile convertire questo valo Epoch in linea o qualsiasi sistema
Tempo trascorso	68855	%d	Quantità di millisecondi impiegati dell'interruzione della richiesta e c
Source IP address	192.168.1.10	%d	Indirizzo IP client/origine.
Codice risultato transazione	TCP_MISS	%s	Il codice risultato transazione indi client. Di seguito è riportato l'elenco dei RISP_TA TCP TCP_IMS_HIT RISCONTRI TCP TCP_MISS TCP_REFRESH_HIT

			MANCATO AGGIORNAMENTO TCP_CLIENT TCP_NEGATO HTTPS TCP_DENIED_SSL TCP_CLIENT_REFRESH_MISS_ HTTPS TCP_MISS_SSL
Codice di risposta HTTP	/200	%h	Il codice di risposta HTTP rappres server Web in risposta alla richies Di seguito è riportato l'elenco del Per ulteriori informazioni, vedere questo articolo. Codice di stato | Significato

			000	000 è un codice verificata un'int la fase TLS o ir trasferimento d
			2xx completate	
			200	OK
			204	Nessun conten
			206	Contenuto parz intervallo)
			Reindirizzamento 3xx	
			301	Reindirizzamen
			302	Reindirizzamen
			304	Non modificato
			307	Reindirizzamen (di solito visibile SWA autentica
			Errore client 4xx	
			400	Richiesta non v
			401	È richiesta l'aut (generalmente trasparente me
			403	Non consentito
			404	Non trovato
			407	Necessaria aut
			Errore server 5xx	
			500	Errore interno d
			502	Gateway non v
			503	Servizio non dis
			504	Timeout gatewa

Dimensione totale trasferita	97645	%s	Totale byte trasferiti per la richies
Metodo HTTP	CONNESSIONE TCP	%1r	Un metodo HTTP è un metodo st di specificare l'azione che deve es server Web, ad esempio il recupe con POST. OTTIENI: Il met richie esclus inform del m signifi POST: Il met inviar nel co utiliz di file del se CONNETTI: Il met per st proxy conne destin utiliz comu Indica esplic il clier diretta CONNESSIONE TCP: Indica traspa Windo reindi
Destinazione	10.37.145.84:443	%2r	Questa sezione mostra l'URL del

<table>
<tr><td></td><td></td><td></td><td>porta TCP.

Nel reindirizzamento trasparente,
SWA mostra l'indirizzo IP di desti

Se l'URL inizia con tunnel:// , il pr
decrittografato il traffico.

Se l'URL inizia con https://, il prot</td></tr>
<tr><td>Nome utente e realm di autenticazione</td><td>"AMOJARRA\amirhossein@WCCPrealm"</td><td>%A</td><td>Credenziali utilizzate per la conne

Se la richiesta viene autenticata,
autenticazione come:

<Nome dominio> \ <Nome utente

Se la richiesta non è ancora auter
viene visualizzato il trattino "-"</td></tr>
<tr><td>Tipo di accesso</td><td>DIRECT/</td><td>%H</td><td>Codice che descrive il server con
della richiesta.

I valori più comuni includono:

<table><tr><td>NESSUNA</td><td>Poiché il
non ha c
recupera</td></tr><tr><td>DIRETTO</td><td>Il proxy V
nella rich</td></tr><tr><td>PADRE_PREDEFINITO</td><td>Il proxy V
un serve
contenut</td></tr></table></td></tr>
<tr><td>Indirizzo server</td><td>www.cisco.com</td><td>%d</td><td>Origine dati o indirizzo IP del serv</td></tr>
<tr><td>tipo/sottotipo di contenuto MIME</td><td>-</td><td>%c</td><td>MIME Indica la natura e il format
di byte. I tipi MIME sono definiti e

Due tipi MIME primari sono impor</td></tr>
</table>

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

text/plain è il valore predefin
deve essere leggibile e non
application/octet-stream è il
Questo tipo deve essere uti
browser prestano particolar
questi file, per proteggere gl
e da possibili comportamen

Per ottenere un elenco completo
(Lana)
</td>
</tr>
<tr>
<td>Tag di decisione ACL</td>
<td>PASSTHRU_CUSTOMCAT_7-</td>
<td>%D</td>
<td>
Un tag di decisione ACL è un can
che indica il modo in cui il proxy W
informazioni provenienti dai filtri W
dai motori di scansione.

Nota: la fine del tag di decisi
in modo dinamico e utilizzato
migliorare le prestazioni. Puo

Di seguito è riportato un elenco d
(Per ulteriori informazioni, consult
decisione negli ACL in questo arti
<table>
<tr><td>Tag di decisione ACL</td></tr>
<tr><td>ALLOW_CUSTOMCAT</td></tr>
<tr><td>CONSENTI_WBRS</td></tr>
<tr><td>AMP_FILE_VERDICT</td></tr>
</table>
</td>
</tr>
</table>

			BLOCK_ADMIN
			BLOCK_ADMIN_CONNECT
			BLOCK_ADMIN_CUSTOM_USE
			BLOCK_ADMIN_TUNNELING
			TIPO_FILE_AMMINISTRATORE_
			PROTOCOLLO_AMMINISTRAZI

			BLOCK_AMP_RESP
			BLOCCO_AVC
			BLOCK_CONTENT_UNSAFE
			BLOCK_CUSTOMCAT
			BLOCCO_ICAP
			BLOCK_WBRS

			BLOCK_WEBCAT
			TIPO_BLOCCO
			DECRYPT_ADMIN
			DECRITTOGRAFARE
			DECRITTOGRAFIA_EUN_WBRS
			DECRIPT_EUN_WEBCAT

			DECRITTOGRAFA_WEBCAT
			DECRITTOGRAFIA_WBRS
			DROP_ADMIN
			DROP_WEBCAT
			DROP_WBRS
			PASSTHRU_ADMIN

			PASSTHRU_WEBCAT PASSTHRU_WBRS Other (Altro)
Nome criterio	Sito_DP-	N/D	A seconda del tipo di traffico, vien • Nome criterio di decrittograf ancora stato decrittografato • Nome criterio di accesso: Il
Criteri di identità	IdP_Site-	N/D	Mostra il nome del profilo di identi
Gruppo di criteri di analisi malware in uscita	NESSUNA-	N/D	Nome del gruppo di criteri di anali Qualsiasi spazio nel nome del gru carattere di sottolineatura (_)
Gruppo di criteri di sicurezza dati	NESSUNA-	N/D	Nome del gruppo di criteri di sicur transazione corrisponde ai criteri questo valore è DefaultGroup. Qu visualizzato solo quando i filtri di s Quando non è stato applicato alcu visualizzato "NONE".

<table>
<tr><td></td><td></td><td></td><td>Qualsiasi spazio nel nome del gru
carattere di sottolineatura (_)</td></tr>
<tr><td>Gruppo di criteri di prevenzione della perdita dei dati esterno</td><td>NESSUNA-</td><td>N/D</td><td>Quando la transazione corrisponc
dei dati esterni globali, questo val
applicati criteri di prevenzione del
visualizzato "NONE".

Qualsiasi spazio nel nome del gru
carattere di sottolineatura (_).</td></tr>
<tr><td>Gruppo di criteri di routing</td><td>GruppoPredefinito</td><td>N/D</td><td>Nome del gruppo di criteri di routi
NomeGruppoProxy/NomeServerF

Quando la transazione corrisponc
valore è DefaultRouting. Quando
upstream, questo valore è DIREC

Qualsiasi spazio nel nome del gru
carattere di sottolineatura (_).</td></tr>
<tr><td>Traffic Tap Web</td><td>NESSUNA</td><td>N/D</td><td>Nome del criterio Traffic Tap sul V</td></tr>
<tr><td>Abbreviazione categoria URL</td><td><"C_Cisco",</td><td>%XC</td><td>Categoria URL corrispondente all
<table><tr><td>-</td><td>Filtro URL ignorato</td></tr><tr><td>nc</td><td>URL non classificati</td></tr><tr><td>errore</td><td>Filtro URL ignorato</td></tr><tr><td>imp</td><td>Impossibile</td></tr><tr><td>IW</td><td>Se il nome della cate
con IW_, significa ch
stava raggiungendo
Predefine URL Categ</td></tr><tr><td>C_</td><td>Se il nome della cate
con IC_, significa che</td></tr></table></td></tr>
</table>

			stava raggiungendo Category
Punteggio reputazione Web	-,	%XW	Questo campo mostra il punteggi ns indica che l'URL non ha un pu
Analisi Webroot	-,"-",-,-,-		Questi 5 campi sono correlati alla

Webroot Verdict	%Xv
Webroot Spyname	"%Xn"
Webroot TRR,	%Xt
ID minaccia Webroot,	%Xs
Webroot TraceID	%Xi

Scansione McAfee	-,"-",-,-,-"-",		Questi 6 campi sono correlati alla	
			Verdetto McAfee	%Xd
			Nome file McAfee,	"%Xe"
			Codice errore analisi McAfee,	%Xf
			Tipo di rilevamento McAfee,	%Xg
			Tipo di virus McAfee,	%Xh

			Nome virus McAfee,	"%Xj"
Scansione Sophos	-,-,"-","-",		Questi 4 campi sono correlati a sc	
			Sophos Verdict	%XY
			Codice di ritorno Sophos Scan,	%Xx
			Percorsi dei file Sophos,	"%Xy"
			Sophos Threat Name	"%Xz"
Verdetto analisi sicurezza dati Cisco	-,	%Xl	Il verdetto della scansione di Cisc nella colonna Contenuto della pol In questo elenco vengono descrit 0.Consenti 1.Blocco	

			- (trattino).Nessuna scansione av Cisco. Questo valore viene visual Security sono disabilitati o quand impostata su Consenti.
Verdetto scansione DLP esterna	-,	%Xp	Il verdetto di scansione del DLP e risposta ICAP. In questo elenco vengono descrit 0.Consenti 1.Blocco - (trattino).Nessuna scansione av valore viene visualizzato quando quando il contenuto non è stato a URL esente nella pagina Criteri D
Verdetto categoria URL predefinito	"-"	%XQ	Verdetto predefinito della categor lato richiesta, abbreviato. In questo campo viene visualizza disabilitato. Se la richiesta raggiunge una cat visualizzare il nome della categor ma la decisione è stata presa dall Per un elenco delle abbreviazioni Descrizioni delle categorie URL.
Verdetto categoria URL	-,	%XA	Verdetto della categoria URL dete Content Analysis) durante la scar Si applica solo al motore di filtro U Cisco. nc: Questo valore viene visualizza richiesta quando il motore di anal non è assegnata alcuna categoria indicando che l'URL non è stato c iniziale prima che venga classifica
Verdict Unified	"-"	%XZ	Verdetto di scansione antimalwar categoria Malware indipendente d

Inbound DVS			applica alle transazioni bloccate c risposte del server.
Tipo di minaccia filtro reputazione Web	"-"	%Xk	Il nome della categoria o il tipo di Reputazione Web. Il nome della c reputazione Web è alta e il tipo di reputazione è bassa. In genere, questo campo viene co inferiore.
Google Translate Encapsulated URL	"-"	%X#10#	L'URL incapsulato nel motore di t presente alcun URL incapsulato,
Controllo applicazioni (AVC/ADC)	"-","-","-",		In questi tre campi vengono regis Visibility and Control (AVC) e di A (ADC). Nome applicazione AVC/ADC — "%XO" — Nc m Ap AD Tipo di applicazione AVC/ADC — "%Xu" — Tip AV so ab Comportamento dell'applicazione AVC/ADC — "%Xb" — Co re ap m È
Verdetto sull'esplorazione sicura	"-"	%XS	Questo valore indica se alla trans di ricerca sicura o le classificazion

			stringere: La richiesta client or applicata la funziona cifrare: La richiesta client or applicata la caratter del sito. interrompere: La richiesta originale di ricerca non suppo errore: La richiesta client or possibile applicare l funzionalità di classi causa di un errore. -: Alla richiesta client r ricerca sicura né la contenuto del sito p ignorate (ad esempi una categoria URL stata effettuata da u
Larghezza di banda media	11.35,	%XB	Larghezza di banda media utilizza Kb/sec.
Controllo Limite Larghezza Di Banda	0,	%XT	Valore che indica se la richiesta è impostazioni di controllo del limite "1" indica che la richiesta è stata "0" indica che la richiesta non è s
Tipo utente	-,	%I	Tipo di utente che effettua la richi Si applica solo quando AnyConne Se non è attivata, il valore è un tra
Scansione malware in	"-","-",		Questi due campi si applicano all causa dell'analisi delle richieste c di analisi malware in uscita.

<table>
<tr>
<td>uscita</td>
<td></td>
<td></td>
<td>
<table>
<tr><td>Unified Outbound DVS Verdict</td><td>"%X3"</td></tr>
<tr><td>Nome minaccia in uscita</td><td>"%X4"</td></tr>
</table>
</td>
</tr>
<tr>
<td>Protezione avanzata da malware</td>
<td>-,"-",-,-,"-","-",</td>
<td></td>
<td>
Questi 6 campi sono correlati a S
Advanced Malware Protection):
<table>
<tr><td>Invia verdetto</td><td>%X#1#</td></tr>
<tr><td>Nome minaccia</td><td>%X#2#</td></tr>
<tr><td>Punteggio reputazione</td><td>%X#3#</td></tr>
</table>
</td>
</tr>
</table>

			Carica azione per analisi %X#4#
			Nome file %X#5#
			Agente integrità sistema file %X#6#
Scansione dell'archivio	-,-,"-",		Questi 3 campi indicano lo stato d Verdetto scansione archivio %X#8# Verdetto della s ARCHIVESCA ARCHIVESCA

					ARCHIVESCA
					ARCHIVESCA

					ARCHIVESCA
					ARCHIVESCA
			Dettaglio verdetto scansione archivio	%Xo	Dettaglio verde archivio invisib (ARCHIVESCA criteri di acces personalizzati, il tipo di file blo "Unscanable A l'archivio non c
			Invia verdetto	%Xm	Verdetto file pe
Tap Web	-,	%XU	Comportamento Web Tap.		

Categoria URL di YouTube	->	%X#29#	La categoria dell'URL di YouTube abbreviata. Questo campo visuali alcuna categoria.

Codice di risposta HTTP

Di seguito è riportato l'elenco completo dei codici di risposta HTTP

Codice di stato	Significato
Informazioni 1xx	
100	Continua
101	Protocolli di switching
102	Elaborazione
103	Suggerimenti iniziali
2xx completate	
200	OK
201	Creato
202	Accettato
203	Informazioni non autorevoli
204	Nessun contenuto
205	Reimposta contenuto
206	Contenuto parziale
207	Multi-Status
208	Già segnalato
226	Messaggistica istantanea utilizzata
Reindirizzamento 3xx	
300	Opzioni multiple
301	Spostato in modo permanente
302	Trovato (in precedenza "Spostato temporaneamente")
303	Vedere Altro

304	Non modificato
305	Usa proxy
306	Cambia proxy
307	Reindirizzamento temporaneo per autenticazione (di solito visibile nella distribuzione trasparente mentre SWA autentica l'utente)
308	Reindirizzamento permanente
Errore client 4xx	
400	Richiesta non valida
401	È richiesta l'autenticazione del server Web (generalmente visualizzata nella distribuzione trasparente mentre SWA autentica l'utente)
402	Pagamento necessario
403	Non consentito
404	Non trovato
405	Metodo non consentito
406	Non accettabile
407	Necessaria autenticazione proxy esplicita
408	Timeout richiesta
409	Conflitto
410	Non più
411	Lunghezza richiesta
412	Precondizione non riuscita
413	Payload troppo grande
414	URI troppo lungo
415	Tipo di supporto non supportato
416	Intervallo non soddisfatto
417	Previsione non riuscita
418	Io sono una teiera
421	Richiesta indirizzata in modo errato
422	Entità non elaborabile

423	Bloccato
424	Dipendenza non riuscita
425	Troppo presto
426	Aggiornamento necessario
428	Precondizione obbligatoria
429	Troppe richieste
431	Campi intestazione richiesta troppo grandi
451	Non disponibile per motivi legali
Errore server 5xx	
500	Errore interno del server
501	Non implementato
502	Gateway non valido
503	Servizio non disponibile
504	Timeout gateway
505	Versione HTTP non supportata
506	Negoziazione anche con Variant
507	Spazio di archiviazione insufficiente
508	Rilevato loop
510	Non esteso
511	Autenticazione di rete richiesta

Tag di decisione ACL

Di seguito è riportato l'elenco completo dei tag di decisione degli ACL:

Tag di decisione ACL	Descrizione
PAGINA_ERRORE_ALLOW_ADMIN	Il proxy Web ha consentito la transazione a una pagina di notifica e a qualsiasi logo utilizzato in tale pagina.
ALLOW_CUSTOMCAT	Il proxy Web ha consentito la transazione in base alle impostazioni di filtro delle categorie di URL personalizzate per il gruppo di criteri di

	accesso.
RIFERIMENTO_CONSENTI	Il proxy Web ha consentito la transazione in base a un'esenzione del contenuto incorporata/referenziata.
CONSENTI_WBRS	Il proxy Web ha consentito la transazione in base alle impostazioni del filtro Reputazione Web per il gruppo di criteri di accesso.
AMP_FILE_VERDICT	Valore che rappresenta un verdetto del server della reputazione AMP per il file:
	1 - Sconosciuto
	2 - Pulito
	3 - Dannoso
	4 - Non scansionabile
ARCHIVESCAN_ALLCLEAR	Verdetto scansione archivio
ARCHIVESCAN_BLOCKEDFILETYPE	ARCHIVESCAN_ALLCLEAR: nessun tipo di file bloccato nell'archivio ispezionato.
ARCHIVESCAN_NESTEDTOODEEP	ARCHIVESCAN_BLOCKEDFILETYPE: è presente un tipo di file bloccato nell'archivio ispezionato. Il campo successivo nella voce di registro (Dettaglio verdetto) fornisce i dettagli, in particolare il tipo di file bloccato e il nome del file bloccato.
ARCHIVESCAN_UNKNOWNFMT	ARCHIVESCAN_NESTEDTOODEEP - L'archivio è bloccato perché contiene un numero di archivi "incapsulati" o nidificati superiore al massimo configurato. Il campo Dettaglio verdetto contiene "Archiviazione non scansionabile bloccata".
ARCHIVESCAN_UNSCANABLE	ARCHIVESCAN_UNKNOWNFMT: l'archivio è bloccato perché contiene un tipo di file di formato sconosciuto. Il dettaglio del verdetto è "Archiviazione non scansionabile bloccata".
ARCHIVESCAN_FILETOOBIG	ARCHIVESCAN_UNSCANABLE - L'archivio è bloccato perché contiene un file che non può essere analizzato. Il dettaglio del verdetto è "Archiviazione non scansionabile bloccata".
	ARCHIVESCAN_FILETOOBIG:

	l'archivio è bloccato perché le sue dimensioni superano il valore massimo configurato. Il dettaglio del verdetto è "Archiviazione non scansionabile bloccata".
	Dettaglio verdetto scansione archivio
	Il campo e il campo Verdict nella voce di registro forniscono ulteriori informazioni sul verdetto, ad esempio il tipo di file bloccato e il nome del file bloccato, "Non analizzabile archivio bloccato" o "-" per indicare che l'archivio non contiene alcun tipo di file bloccato.
	Ad esempio, se un file di archivio Inspectable è bloccato (ARCHIVESCAN_BLOCKEDFILETYPE) in base ai criteri di accesso: Impostazioni blocco oggetti personalizzati, la voce Dettaglio verdetto include il tipo di file bloccato e il nome del file bloccato.
	Per ulteriori informazioni, fare riferimento al documento Criteri di accesso: Blocco di oggetti e impostazioni di ispezione dell'archivio per ulteriori informazioni sull'ispezione dell'archivio.
BLOCK_ADMIN	Transazione bloccata in base ad alcune impostazioni predefinite per il gruppo di criteri di accesso.
BLOCK_ADMIN_CONNECT	Transazione bloccata in base alla porta TCP della destinazione definita nell'impostazione Porte CONNECT HTTP per il gruppo di criteri di accesso.
BLOCK_ADMIN_CUSTOM_USER_AGENT	Transazione bloccata in base all'agente utente definito nell'impostazione Blocca agenti utente personalizzati per il gruppo di criteri di accesso.
BLOCK_ADMIN_TUNNELING	Il proxy Web ha bloccato la transazione in base al tunneling del traffico non HTTP sulle porte HTTP per il gruppo di criteri di accesso.
BLOCK_ADMIN_HTTPS_NonLocalDestination	Transazione bloccata; il client ha tentato di ignorare l'autenticazione utilizzando la porta SSL come proxy esplicito. Per evitare questo problema, se una

	connessione SSL è al WSA stesso, sono consentite solo le richieste al nome host di reindirizzamento WSA effettivo.
ID_AMMINISTRATORE_BLOCCO	Transazione bloccata in base al tipo MIME del contenuto del corpo della richiesta definito nel gruppo di criteri di sicurezza dei dati.
TIPO_FILE_AMMINISTRATORE_BLOCCO	Transazione bloccata in base al tipo di file definito nel gruppo di criteri di accesso.
PROTOCOLLO_AMMINISTRAZIONE_BLOCCO	Transazione bloccata in base al protocollo definito nell'impostazione Blocca protocolli per il gruppo di criteri di accesso.
DIM_AMMIN_BLOCCO	Transazione bloccata in base alle dimensioni della risposta definite nelle impostazioni Dimensioni oggetto per il gruppo di criteri di accesso.
BLOCK_ADMIN_SIZE_IDS	Transazione bloccata in base alle dimensioni del contenuto del corpo della richiesta definito nel gruppo di criteri di sicurezza dei dati.
BLOCK_AMP_RESP	Il proxy Web ha bloccato la risposta in base alle impostazioni di Protezione avanzata da malware per il gruppo di criteri di accesso.
BLOCK_AMW_REQ	Il proxy Web ha bloccato la richiesta in base alle impostazioni antimalware per il gruppo di criteri Analisi malware in uscita. Il corpo della richiesta ha prodotto un verdetto Malware positivo.
BLOCK_AMW_RESP	Il proxy Web ha bloccato la risposta in base alle impostazioni antimalware per il gruppo di criteri di accesso.
URL_BLOCK_AMW_REQ	Il proxy Web sospetta che l'URL nella richiesta HTTP non possa essere sicuro, quindi ha bloccato la transazione al momento della richiesta in base alle impostazioni antimalware per il gruppo di criteri di accesso.
BLOCCO_AVC	Transazione bloccata in base alle impostazioni dell'applicazione configurate per il gruppo di criteri di accesso.
BLOCK_CONTENT_UNSAFE	Transazione bloccata in base alle

	impostazioni delle classificazioni del contenuto del sito per il gruppo di criteri di accesso. La richiesta client era per contenuto per adulti e il criterio è configurato per bloccare il contenuto per adulti.
BLOCK_CONTINUE_CONTENT_UNSAFE	La transazione è stata bloccata e viene visualizzata la pagina Avvisa e continua in base alle impostazioni delle classificazioni del contenuto del sito nel gruppo di criteri di accesso. La richiesta client era per contenuti per adulti e il criterio è configurato per inviare un avviso agli utenti che accedono a contenuti per adulti.
BLOCK_CONTINUE_CUSTOMCAT	La transazione è stata bloccata e viene visualizzata la pagina Avvisa e continua in base a una categoria URL personalizzata nel gruppo di criteri di accesso configurato su "Avvisa".
BLOCK_CONTINUE_WEBCAT	La transazione è stata bloccata e viene visualizzata la pagina Avvisa e continua in base a una categoria URL predefinita nel gruppo di criteri di accesso configurato su "Avvisa".
BLOCK_CUSTOMCAT	Transazione bloccata in base alle impostazioni personalizzate del filtro delle categorie URL per il gruppo di criteri di accesso.
BLOCCO_ICAP	Il proxy Web ha bloccato la richiesta in base al verdetto del sistema di prevenzione della perdita dei dati esterno definito nel gruppo di criteri di prevenzione della perdita dei dati esterni.
BLOCK_SEARCH_UNSAFE	La richiesta client include una query di ricerca non sicura e i criteri di accesso sono configurati per applicare le ricerche sicure, pertanto la richiesta client originale è stata bloccata.
BLOCK_SUSPECT_USER_AGENT	Transazione bloccata in base all'impostazione dell'agente utente sospetto per il gruppo di criteri di accesso.
BLOCK_UNSUPPORTED_SEARCH_APP	Transazione bloccata in base alle impostazioni di ricerca sicura per il

	gruppo di criteri di accesso. La transazione è stata eseguita per un motore di ricerca non supportato e il criterio è configurato per bloccare i motori di ricerca non supportati.
BLOCK_WBRS	Transazione bloccata in base alle impostazioni del filtro Reputazione Web per il gruppo di criteri di accesso.
BLOCK_WBRS_IDS	Il proxy Web ha bloccato la richiesta di caricamento in base alle impostazioni del filtro Reputazione Web per il gruppo di criteri di sicurezza dati.
BLOCK_WEBCAT	Transazione bloccata in base alle impostazioni del filtro della categoria URL per il gruppo di criteri di accesso.
BLOCK_WEBCAT_IDS	Il proxy Web ha bloccato la richiesta di caricamento in base alle impostazioni del filtro della categoria URL per il gruppo di criteri di sicurezza dati.
TIPO_BLOCCO	Il proxy Web ha bloccato la transazione in base alle impostazioni predefinite del filtro di categoria YouTube per il gruppo di criteri di accesso.
BLOCK_CONTINUE_TYPE	Il proxy Web ha bloccato la transazione e ha visualizzato la pagina Avvisa e continua in base a una categoria predefinita di YouTube nel gruppo di criteri di accesso configurato su 'Avvisa'.
DECRYPT_ADMIN	Il proxy Web ha decrittografato la transazione in base ad alcune impostazioni predefinite per il gruppo di criteri di decrittografia.
DECRYPT_ADMIN_EXPIRED_CERT	Il proxy Web ha decrittografato la transazione anche se il certificato del server è scaduto.
DECRYPT_EUN_ADMIN_DEFAULT_ACTION	Il proxy Web ha decrittografato la transazione in base alle impostazioni predefinite come connessione di ricezione per il gruppo di criteri di decrittografia quando EUN è abilitato.
DECRYPT_EUN_ADMIN_EXPIRED_CERT	Il proxy Web ha decrittografato la transazione quando le impostazioni del proxy HTTPS rilasciano un certificato scaduto con EUN abilitato.
DECRYPT_EUN_ADMIN_INVALID_LEAF_CERT	Il proxy Web ha decrittografato la

	transazione quando le impostazioni del proxy HTTPS rilasciano un certificato foglia non valido con EUN abilitato.
DECRYPT_EUN_ADMIN_MISMATCHED_HOSTNAME	Il proxy Web ha decrittografato la transazione quando le impostazioni del proxy HTTPS eliminano il nome host non corrispondente con EUN abilitato.
DECRYPT_EUN_ADMIN_OCSP_OTHER_ERROR	Il proxy Web ha decrittografato la transazione quando le impostazioni del proxy HTTPS rilasciano un OCSP con altri errori con EUN abilitato.
DECRYPT_EUN_ADMIN_OCSP_REVOKED_CERT	Il proxy Web ha decrittografato la transazione quando le impostazioni del proxy HTTPS rilasciano un certificato OCSP revocato con EUN abilitato.
DECRYPT_EUN_ADMIN_UNRECOGNITION_ROOT_CERT	Il proxy Web ha decrittografato la transazione quando le impostazioni del proxy HTTPS rilasciano un'autorità radice o un certificato di autorità emittente non riconosciuto con EUN abilitato.
DECRITTOGRAFARE	Il proxy Web ha decrittografato la transazione in base alle impostazioni di filtro delle categorie URL personalizzate per il gruppo di criteri di decrittografia. Se EUN è abilitato, il traffico viene interrotto.
DECRITTOGRAFIA_EUN_WBRS	Il proxy Web ha decrittografato la transazione in base alle impostazioni del filtro della reputazione Web per il gruppo di criteri di decrittografia. Se EUN è abilitato, il traffico viene interrotto.
DECRYPT_EUN_WBRS_NO_SCORE	Il proxy Web ha decrittografato la transazione in base alle impostazioni del filtro reputazione Web per l'URL senza punteggio nel gruppo di criteri di decrittografia. Se EUN è abilitato, il traffico viene interrotto.
DECRIPT_EUN_WEBCAT	Il proxy Web ha decrittografato la transazione in base alle impostazioni del filtro della categoria URL per il gruppo di criteri di decrittografia. Se EUN è abilitato, il traffico viene interrotto.
DECRITTOGRAFA_WEBCAT	Il proxy Web ha decrittografato la

	transazione in base alle impostazioni del filtro della categoria URL per il gruppo di criteri di decrittografia.
DECRITTOGRAFIA_WBRS	Il proxy Web ha decrittografato la transazione in base alle impostazioni del filtro Reputazione Web per il gruppo di criteri di decrittografia.
MAIUSCOLE_PREDEFINITE	Il proxy Web ha consentito al client di accedere al server perché nessuno dei servizi AsyncOS, ad esempio la reputazione Web o l'analisi antimalware, ha eseguito alcuna azione sulla transazione.
NEGA_AMMIN	Il proxy Web ha negato la transazione. Questo si verifica per le richieste HTTPS quando è necessaria l'autenticazione e Decrittografa per autenticazione è disabilitato nelle impostazioni proxy HTTPS.
DROP_ADMIN	Il proxy Web ha eliminato la transazione in base ad alcune impostazioni predefinite per il gruppo di criteri di decrittografia.
DROP_ADMIN_EXPIRED_CERT	Il proxy Web ha interrotto la transazione perché il certificato del server è scaduto.
DROP_WEBCAT	Il proxy Web ha eliminato la transazione in base alle impostazioni di filtro delle categorie URL per il gruppo di criteri di decrittografia.
DROP_WBRS	Il proxy Web ha eliminato la transazione in base alle impostazioni del filtro Reputazione Web per il gruppo di criteri di decrittografia.
MONITOR_ADMIN_EXPIRED_CERT	Il proxy Web ha monitorato la risposta del server perché il certificato del server è scaduto.
MONITOR_AMP_RESP	Il proxy Web ha monitorato la risposta del server in base alle impostazioni di Protezione avanzata da malware per il gruppo di criteri di accesso.
MONITOR_AMW_RESP	Il proxy Web ha monitorato la risposta del server in base alle impostazioni antimalware per il gruppo di criteri di accesso.
URL_MONITOR_AMW_RESP	Il proxy Web sospetta che l'URL nella

	richiesta HTTP non possa essere sicuro, ma ha monitorato la transazione in base alle impostazioni antimalware per il gruppo di criteri di accesso.
AVC_MONITOR	Il proxy Web ha monitorato la transazione in base alle impostazioni dell'applicazione per il gruppo di criteri di accesso.
MONITOR_CONTINUE_CONTENT_UNSAFE	In origine, il proxy Web ha bloccato la transazione e ha visualizzato la pagina Avvisa e continua in base alle impostazioni delle classificazioni del contenuto del sito nel gruppo Criteri di accesso. La richiesta client era per contenuti per adulti e il criterio è configurato per inviare un avviso agli utenti che accedono a contenuti per adulti. L'utente ha accettato l'avviso e ha proseguito con il sito richiesto in origine e nessun altro motore di scansione ha successivamente bloccato la richiesta.
MONITOR_CONTINUE_CUSTOMCAT	In origine, il proxy Web ha bloccato la transazione e ha visualizzato la pagina Avvisa e continua basata su una categoria URL personalizzata nel gruppo di criteri di accesso configurato su "Avvisa". L'utente ha accettato l'avviso e ha proseguito con il sito richiesto in origine e nessun altro motore di scansione ha successivamente bloccato la richiesta.
MONITOR_CONTINUE_WEBCAT	In origine, il proxy Web ha bloccato la transazione e ha visualizzato la pagina Avvisa e continua in base a una categoria URL predefinita nel gruppo di criteri di accesso configurato su "Avvisa". L'utente ha accettato l'avviso e ha proseguito con il sito richiesto in origine e nessun altro motore di scansione ha successivamente bloccato la richiesta.
MONITOR_CONTINUE_YTCAT	In origine, il proxy Web ha bloccato la transazione e ha visualizzato la pagina Avvisa e continua basata su una categoria predefinita di YouTube nel gruppo di criteri di accesso configurato

	su 'Avvisa'. L'utente ha accettato l'avviso e ha proseguito con il sito richiesto in origine e nessun altro motore di scansione ha successivamente bloccato la richiesta.
MONITOR_IDS	Il proxy Web ha analizzato la richiesta di caricamento utilizzando i criteri di sicurezza dei dati o i criteri di prevenzione della perdita dei dati esterni, ma non ha bloccato la richiesta. La richiesta è stata valutata in base ai criteri di accesso.
MONITOR_SUSPECT_USER_AGENT	Il proxy Web ha monitorato la transazione in base all'impostazione dell'agente utente sospetto per il gruppo di criteri di accesso.
MONITOR_WBRS	Il proxy Web ha monitorato la transazione in base alle impostazioni del filtro Reputazione Web per il gruppo di criteri di accesso.
NESSUNA_AUTORIZZAZIONE	Il proxy Web non ha consentito all'utente l'accesso all'applicazione perché l'utente è già stato autenticato in un realm di autenticazione, ma non in alcun realm di autenticazione configurato nei criteri di autenticazione dell'applicazione.
NESSUNA_PASSWORD	Autenticazione non riuscita.
PASSTHRU_ADMIN	Il proxy Web ha passato la transazione in base ad alcune impostazioni predefinite per il gruppo di criteri di decrittografia.
PASSTHRU_ADMIN_EXPIRED_CERT	Il proxy Web ha superato la transazione anche se il certificato del server è scaduto.
PASSTHRU_WEBCAT	Il proxy Web ha passato la transazione in base alle impostazioni di filtro delle categorie URL per il gruppo di criteri di decrittografia.
PASSTHRU_WBRS	Il proxy Web ha passato la transazione in base alle impostazioni del filtro Reputazione Web per il gruppo di criteri di decrittografia.
REINDIRIZZA_PERSONALIZZATO	Il proxy Web ha reindirizzato la transazione a un URL diverso in base a

	una categoria di URL personalizzata nel gruppo di criteri di accesso configurato per il reindirizzamento.
AUTENTICAZIONE_SAAS	Il proxy Web ha consentito all'utente di accedere all'applicazione perché l'utente è stato autenticato in modo trasparente nel realm di autenticazione configurato nei criteri di autenticazione dell'applicazione.
Other (Altro)	Il proxy Web non ha completato la richiesta a causa di un errore, ad esempio un errore di autorizzazione, la disconnessione del server o un'interruzione dal client.

Valori verdetto di analisi malware

Un verdetto di analisi malware è un valore assegnato a una richiesta URL o a una risposta del server che determina la probabilità che contenga malware. I motori di scansione Webroot, McAfee e Sophos restituiscono il verdetto di scansione Malware al motore DVS in modo che il motore DVS possa determinare se monitorare o bloccare l'oggetto digitalizzato. Ogni verdetto di analisi malware corrisponde a una categoria Malware elencata nella pagina Criteri di accesso > Reputazione e impostazioni antimalware quando si modificano le impostazioni antimalware per un determinato criterio di accesso.

In questo elenco sono elencati i diversi valori di verdetto della scansione di malware e ciascuna categoria di malware corrispondente:

Valore verdetto di analisi malware	Categoria malware
-	Non impostato
0	Sconosciuto
1	Non analizzato
2	Timeout
3	Errore

Valore verdetto di analisi malware	Categoria malware
4	Non scansionabile
10	Spyware generico
12	Oggetto helper del browser
13	Adware
14	Monitor di sistema
18	Monitor di sistema commerciale
19	Dialer
20	Hijacker
21	URL di phishing
22	Trojan Downloader
23	Cavallo di Troia
24	Trojan Phisher
25	Worm
26	File crittografato
27	Virus
33	Altro malware
34	PUA

Valore verdetto di analisi malware	Categoria malware
35	Interrotto
36	Euristica epidemie
37	File dannosi e ad alto rischio noti

Informazioni correlate

- Guida per l'utente di AsyncOS 15.2 per Cisco Secure Web Appliance
- Utilizzare le procedure ottimali per Secure Web Appliance
- Garantire la corretta funzionalità del gruppo WSA HA virtuale in un ambiente VMware
- Configura parametro prestazioni nei log degli accessi
- Informazioni sul formato HTTPS Accesslog in Secure Web Appliance
- Accesso ai registri protetti di Web Appliance

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).