Inzicht in de toegangspunten voor veilige webapparaten

Inhoud

Inleiding

Dit document beschrijft de structuur van Secure Web Appliance (SWA) Accesslog.

Voorwaarden

Vereisten

Cisco raadt kennis van deze onderwerpen aan:

- Toegang tot de Command Line Interface (CLI) van SWA.

- Administratieve toegang tot de SWA.
- Basiskennis van de SWA-werkstroom.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

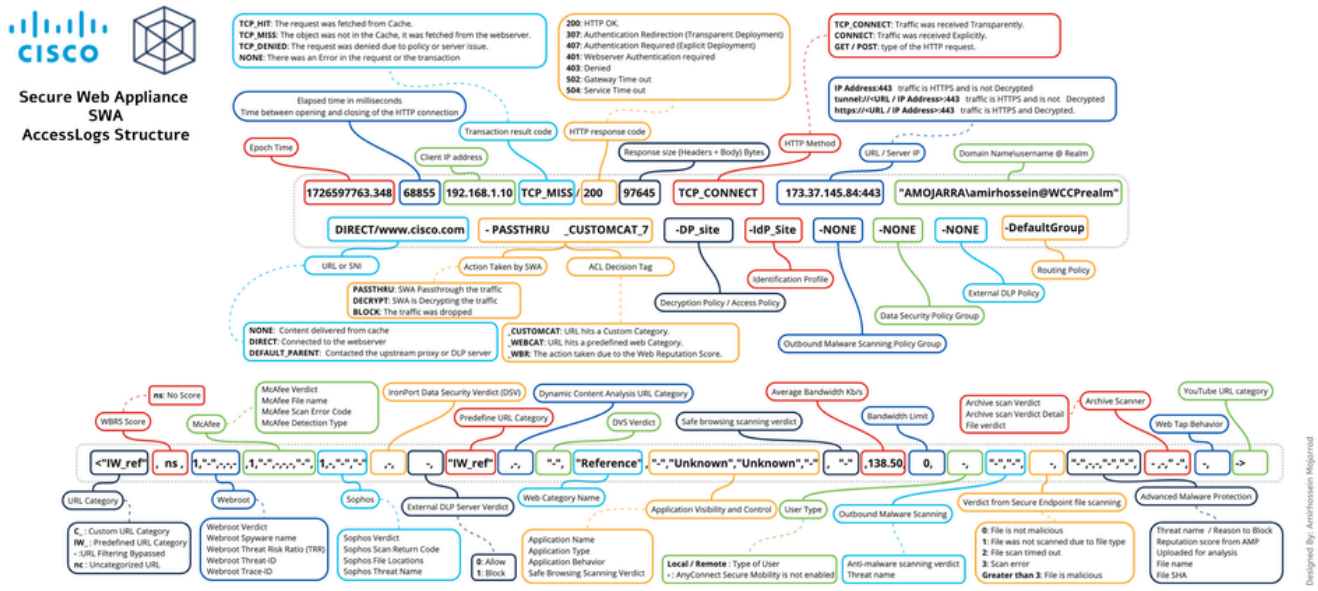
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële

impact van elke opdracht begrijpt.

Accessoire structuur

In dit artikel wordt de Accesslog structuur uitgelegd door dit voorbeeld:

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



Afbeelding - Accessoirestructuur

Opmerking: de structuur van toegangslogboeken is afhankelijk van de versie van SWA. Aan het begin van elk AccessLog-bestand bevindt zich een regel die de structuur en de volgorde van de formaatspecificatie weergeeft.

Deel	Voorbeeld uit Accesslog	Formatteringsspecificatie	Detail
Tijdsperiode	1726597763.348	%t	Epoch bijhou millise 00: 00 Het tij

			U kun Linux-
verstreken tijd	68855	%e	Het aa voltoo
Bron-IP-adres	192.168.1.10	%a	IP-ad
Code transactieresultaat	TCP_MISS	%w	Trans Dit is TCP_ TCP_ TCP_ TCP_ TCP_

			TCP_ TCP_ TCP_ TCP_ TCP_
HTTP-antwoordcode	/200	%h	De HT webse client. Hier is inform Statu 000 2xx gesla 200 204 206

			3xx Omle 301 302 304 307 4xx-client 400 401 403 404 407 5xx-serve 500 502 503 504
Totale overgedragen grootte	97645	%s	Totaa
HTTP-methode	TCP_CONNECT	%1r	Een H gewe worde van g KRIJ

			POST CONN TCP_
Bestemming	10.37.145.84:443	%2r	In dez poortn In tran toont Als de heeft Als de
Gebruikersnaam en	"AMOJARRA\amirhossein@WCCPrealm"	%A	De re

verificatiereeks			Als he verific <Dom Als he in het
toegangstype	DIRECT/	%H	Code van d De m NONE DIRE DEFA
Serveradres	www.cisco.com	%d	IP-adr
MIME-inhoudstype/subtype	-	%c	MIME assor IETF Twee • • Voor

ACL-beslissingstag	PASSTHRU_CUSTOMCAT_7-	%D	Een A aange inform scane Hier is inform ACL- ALLC ALLC AMP_ BLOC BLOC BLOC

			BLOC
			BLOC
			BLOC
			BLOC
			BLOC
			BLOC
			BLOC
			BLOC
			BLOC

			BLOC
			BLOC
			DECR
			DECR
			DECR
			DECR
			DECR
			DECR

			DROI DROI DROI PASS PASS PASS Other
Naam beleid	DP_site-	N.v.t.	Afhan • •
identiteitsbeleid	IdP_Site-	N.v.t.	Toont
beleidsgroep Uitgaand	NONE-	N.v.t.	Naam

scannen op malware			Elke s onder
beleidsgroep Gegevensbeveiliging	NONE-	N.v.t.	Groep overe waard weerg wordt toege Elke s onder
externe DLP-beleidsgroep	NONE-	N.v.t.	Wann is dez DLP-b Elke s onder
Routeringsbeleidsgroep	Standaardgroep-	N.v.t.	Naam Proxy Wann deze gebru Elke s onder
Tik op Webverkeer	NONE	N.v.t.	Tik op
Afkorting van URL-rubriek	<"C_CISC",	%XC	URL-r - NC vergis imp

			IW_ C_
Webreputatiescore	-	%XW	Dit ve ns be
Webroot-scanning	-,"-",-,-,-,		Deze Webr Webr Web Webr

			Webr
McAfee Scanning	-,"-",-,-,-,"-",		Deze
			McAf
			McAf Besta
			McAf foutc
			McAf

			McAf
			McAf
Sophos Scanning	-,-,"-","-",		Deze
			Soph
			Soph retou
			Soph besta
			Soph

Cisco Data Security Scan-oordeel	-	%XL	Het C Inhou In dez 0.Toe 1.Blok - (kop Filters gegev categ
Uitspraak externe DLP-scan	-	%XP	Het ex respo In dez 0.Toe 1.Blok - (kop Deze uitges vrijges
Vooraf gedefinieerde URL-categorieuitspraak	"-",	%XQ	Het vo scann In dit uitges Als de voora beslis Zie Ru rubrie
Verdict in URL-rubriek	-	%XA	Het U Analy Is alle URL.

			nc: De wanne URL-c URL t aan d
Unified Inbound DVS Verdict	"-",	%XZ	Unifie Malwa van to scann
Webreputatiefilter, type bedreiging	"-",	%Xk	De ca Webre webre reputa Doorg lager.
Google Translate ingekapselde URL	"-",	%X#10#	De UF ingeka
Toepassingscontrole (AVC/ADC)	"-","-","-",		In dez (AVC) AVC/ toepa AVC/ toepa AVC/ toepa

Veilig browsen	"-",	%XS	Deze inhou verrijk encod niet onder vergis -
gemiddelde bandbreedte	11.35,	%XB	De ge
bandbreedtelimietregeling	0,	%XT	Een w instell "1" ge "0" ge
Type gebruiker	-	%I	Het ty

			Dit is Als de
Uitgaand scannen op malware	"-","-",		Deze gecor voor h Unifie Verdi Naam bedre
Geavanceerde bescherming tegen malware	-,"-",-,-,"-","-",		Deze Advar Besta

			Naam
			Repu
			Actie analy
			Besta
			Besta
Archiefscan	-,-,"-",		Deze
			Scan archiv

			Archi Verdi Detai

			Besta vonni
Webtap	-	%XU	Web-t
YouTube URL categorie	->	%X#29#	De aa toont

HTTP-antwoordcode

Hier is de volledige lijst van HTTP-responscodes

Statuscode	Betekenis
1xx Informatie	
100	doorgaan
101	Switchprotocollen
102	verwerking
103	Vroege hints
2xx geslaagd	
200	OK
201	gemaakt
202	aanvaard
203	niet-gezaghebbende informatie
204	Geen inhoud
205	Inhoud opnieuw instellen
206	Gedeeltelijke inhoud
207	multi-status
208	Al gemeld

226	IM Gebruikt
3xx Omleiding	
300	Meerdere keuzes
301	Permanent verplaatst
302	Gevonden (voorheen "tijdelijk verplaatst")
303	Zie andere
304	Niet gewijzigd
305	Proxy gebruiken
306	Switch-proxy
307	Tijdelijke omleiding voor authenticatie (Meestal te zien in de transparante implementatie terwijl SWA de gebruiker verifieert)
308	permanente omleiding
4xx-clientfout	
400	Ongeldige aanvraag
401	Vereiste webserververificatie (meestal te zien in de transparante implementatie terwijl SWA de gebruiker verifieert)
402	Betaling vereist
403	verboden
404	Niet gevonden
405	Methode niet toegestaan
406	ontoelaatbaar
407	Expliciete proxyverificatie vereist
408	Time-out voor aanvraag
409	conflict
410	Verdwenen
411	Vereiste lengte
412	Voorwaarde mislukt
413	Te grote lading

414	URI te lang
415	Niet-ondersteund mediatype
416	Bereik niet bevredigend
417	Verwachting mislukt
418	Ik ben een theepot
421	verkeerd gericht verzoek
422	niet-verwerkbare entiteit
423	vergrendeld
424	Mislukte afhankelijkheid
425	te vroeg
426	Upgrade vereist
428	Voorwaarde vereist
429	Te veel verzoeken
431	Te grote kopvelden aanvragen
451	Niet beschikbaar om juridische redenen
5xx-serverfout	
500	Fout interne server
501	Niet uitgevoerd
502	Slechte gateway
503	Service niet beschikbaar
504	Time-out gateway
505	HTTP-versie niet ondersteund
506	Variant onderhandelt ook
507	Onvoldoende opslag
508	lus gedetecteerd
510	Niet uitgebreid
511	Netwerkverificatie vereist

ACL-beslissingstag

Hier is de volledige lijst van de ACL beslissing tags:

ACL-beslissingstag	Beschrijving
ALLOW_ADMIN_ERROR_PAGE	De webproxy stond de transactie toe om een meldingspagina en een logo dat op die pagina werd gebruikt, te openen.
ALLOW_CUSTOMCAT	De webproxy stond de transactie toe op basis van aangepaste filterinstellingen voor URL-categorieën voor de groep Toegangsbeleid.
ALLOW_REFERER	De Web Proxy stond de transactie toe op basis van een vrijstelling voor ingesloten/verwezen inhoud.
ALLOW_WBRS	De Web Proxy stond de transactie toe op basis van de instellingen van het Web Reputation-filter voor de groep Toegangsbeleid.
AMP_FILE_VERDICT	Waarde die een oordeel weergeeft van de AMP-reputatieserver voor het bestand:
	1 – Onbekend
	2 – Schoon
	3 – Kwaadaardig
	4 – Niet-scanbaar
ARCHIVESCAN_ALLCLEAR	Scanoordeel archiveren
ARCHIVESCAN_BLOCKEDFILETYPE	ARCHIVESCAN_ALLCLEAR – Er zijn geen geblokkeerde bestandstypen in het geïnspecteerde archief.
ARCHIVESCAN_NESTEDTOODEEP	ARCHIVESCAN_BLOCKEDFILETYPE – Er is een geblokkeerd bestandstype in het geïnspecteerde archief. Het volgende veld in het logboekitem (Verdict Detail) bevat details, met name het type bestand dat is geblokkeerd en de naam van het geblokkeerde bestand.
ARCHIVESCAN_UNKNOWNMT	ARCHIVESCAN_NESTEDTOODEEP – Het archief is geblokkeerd omdat het meer "ingekapselde" of geneste archieven bevat dan het geconfigureerde maximum. Het veld Verdict Detail bevat "Niet-scanbaar archief geblokkeerd".

ARCHIVESCAN_UNSCANABLE	ARCHIVESCAN_UNKNOWNFMT – Het archief is geblokkeerd omdat het een bestandstype met onbekende indeling bevat. Het vonnis detail is "Unscanable Archive-Blocked."
ARCHIVESCAN_FILETOOBIG	ARCHIVESCAN_UNSCANABLE – Het archief is geblokkeerd omdat het een bestand bevat dat niet kan worden gescand. Het vonnis detail is "Unscanable Archive-Blocked."
	ARCHIVESCAN_FILETOOBIG – Het archief is geblokkeerd omdat de grootte van het archief groter is dan het geconfigureerde maximum. Het vonnis detail is "Unscanable Archive-Blocked."
	Archiefscan Verdict Detail
	Het veld en het veld Verdict in de logboekvermelding bevatten aanvullende informatie over het vonnis, zoals het type bestand dat is geblokkeerd en de naam van het geblokkeerde bestand, "Unscannable Archive-Blocked" of "-" om aan te geven dat het archief geen geblokkeerde bestandstypen bevat.
	Als een bestand met een controleerbaar archief bijvoorbeeld is geblokkeerd (ARCHIVESCAN_BLOCKEDFILETYPE) op basis van de instellingen voor toegangsbeleid: aangepaste objecten blokkeren, bevat het veld Verdict Detail het type bestand dat is geblokkeerd en de naam van het geblokkeerde bestand.
	Raadpleeg Toegangsbeleid: Objecten blokkeren en Instellingen archiefinspectie voor meer informatie over archiefinspectie.
BLOCK_ADMIN	Transactie geblokkeerd op basis van enkele standaardinstellingen voor de groep Toegangsbeleid.
BLOCK_ADMIN_CONNECT	Transactie geblokkeerd op basis van de TCP-poort van de bestemming zoals gedefinieerd in de instelling HTTP CONNECT Ports voor de groep Toegangsbeleid.
BLOCK_ADMIN_CUSTOM_USER_AGENT	Transactie geblokkeerd op basis van de

	gebruikersagent zoals gedefinieerd in de instelling Aangepaste gebruikersagenten blokkeren voor de groep Toegangsbeleid.
BLOCK_ADMIN_TUNNELING	De Web Proxy blokkeerde de transactie op basis van tunneling van het niet-HTTP-verkeer op de HTTP-poorten voor de Access Policy Group.
BLOCK_ADMIN_HTTPS_NonLocalDestination	Transactie geblokkeerd; client probeerde verificatie te omzeilen met behulp van de SSL-poort als een expliciete proxy. Om dit te voorkomen, als er een SSL-verbinding is met de WSA zelf, zijn alleen verzoeken om de eigenlijke WSA-redirect-hostnaam toegestaan.
BLOCK_ADMIN_IDS	Transactie geblokkeerd op basis van het MIME-type van de inhoud van de aanvraaginstantie zoals gedefinieerd in de groep Beleid voor gegevensbeveiliging.
BLOCK_ADMIN_FILE_TYPE	Transactie geblokkeerd op basis van het bestandstype zoals gedefinieerd in de groep Toegangsbeleid.
BLOCK_ADMIN_PROTOCOL	Transactie geblokkeerd op basis van het protocol zoals gedefinieerd in de instelling Blokprotocollen voor de groep Toegangsbeleid.
BLOCK_ADMIN_SIZE	Transactie geblokkeerd op basis van de grootte van het antwoord zoals gedefinieerd in de instellingen Objectgrootte voor de groep Toegangsbeleid.
BLOCK_ADMIN_SIZE_IDS	Transactie geblokkeerd op basis van de grootte van de inhoud van de aanvraaginstantie zoals gedefinieerd in de beleidsgroep Gegevensbeveiliging.
BLOCK_AMP_RESP	De Web Proxy blokkeerde de respons op basis van de Advanced Malware Protection-instellingen voor de groep Toegangsbeleid.
BLOCK_AMW_REQ	De webproxy blokkeerde het verzoek op basis van de instellingen voor anti-malware voor de beleidsgroep Uitgaand scannen van malware. De verzoekende instantie heeft een positief Malware-

	vonnis uitgesproken.
BLOCK_AMW_RESP	De Web Proxy blokkeerde de reactie op basis van de instellingen voor Anti-Malware voor de groep Toegangsbeleid.
BLOCK_AMW_REQ_URL	De Web Proxy vermoedt dat de URL in het HTTP-verzoek niet veilig kan zijn, dus blokkeerde het de transactie op het aanvraagmoment op basis van de Anti-Malware-instellingen voor de Access Policy-groep.
BLOCK_AVC	Transactie geblokkeerd op basis van de geconfigureerde toepassingsinstellingen voor de groep Toegangsbeleid.
BLOCK_CONTENT_UNSAFE	Transactie geblokkeerd op basis van de instellingen voor inhoudsbeoordelingen van de site voor de groep Toegangsbeleid. Het clientverzoek was voor inhoud voor volwassenen en het beleid is geconfigureerd om inhoud voor volwassenen te blokkeren.
BLOCK_CONTINUE_CONTENT_UNSAFE	Transactie geblokkeerd en weergegeven op de pagina Waarschuwen en doorgaan op basis van de instellingen voor de beoordeling van de inhoud van de site in de groep Toegangsbeleid. Het clientverzoek was voor inhoud voor volwassenen en het beleid is geconfigureerd om gebruikers een waarschuwing te geven voor toegang tot inhoud voor volwassenen.
BLOCK_CONTINUE_CUSTOMCAT	Transactie geblokkeerd en weergegeven op de pagina Waarschuwen en doorgaan op basis van een aangepaste URL-categorie in de groep Toegangsbeleid geconfigureerd als Waarschuwen.
BLOCK_CONTINUE_WEBCAT	Transactie geblokkeerd en weergegeven op de pagina Waarschuwen en doorgaan op basis van een vooraf gedefinieerde URL-categorie in de groep Toegangsbeleid geconfigureerd als Waarschuwen.
BLOCK_CUSTOMCAT	Transactie geblokkeerd op basis van aangepaste filterinstellingen voor URL-rubrieken voor de groep

	Toegangsbeleid.
BLOCK_ICAP	De Web Proxy blokkeerde het verzoek op basis van het oordeel van het externe DLP-systeem zoals gedefinieerd in de groep Extern DLP-beleid.
BLOCK_SEARCH_UNSAFE	Het clientverzoek bevatte een onveilige zoekopdracht en het toegangsbeleid is geconfigureerd om veilige zoekopdrachten af te dwingen, zodat het oorspronkelijke clientverzoek is geblokkeerd.
BLOCK_SUSPECT_USER_AGENT	Transactie geblokkeerd op basis van de instelling Verdachte User Agent voor de groep Toegangsbeleid.
BLOCK_UNSUPPORTED_SEARCH_APP	Transactie geblokkeerd op basis van de instellingen voor veilig zoeken in de groep Toegangsbeleid. De transactie was voor een niet-ondersteunde zoekmachine en het beleid is geconfigureerd om niet-ondersteunde zoekmachines te blokkeren.
BLOCK_WBRS	Transactie geblokkeerd op basis van de instellingen van het filter Webreputatie voor de groep Toegangsbeleid.
BLOCK_WBRS_IDS	De Web Proxy blokkeerde het uploadverzoek op basis van de instellingen van het Web Reputation-filter voor de beleidsgroep Gegevensbeveiliging.
BLOCK_WEBCAT	Transactie geblokkeerd op basis van filterinstellingen voor URL-rubrieken voor de groep Toegangsbeleid.
BLOCK_WEBCAT_IDS	De webproxy heeft het uploadverzoek geblokkeerd op basis van de filterinstellingen voor de URL-categorie voor de beleidsgroep Gegevensbeveiliging.
BLOCK_YTCAT	De webproxy heeft de transactie geblokkeerd op basis van de vooraf gedefinieerde filterinstellingen voor de categorie YouTube voor de groep Toegangsbeleid.
BLOCK_CONTINUE_YTCAT	De webproxy blokkeerde de transactie en gaf de pagina Waarschuwen en doorgaan weer op basis van een vooraf

	gedefinieerde YouTube-categorie in de groep Toegangsbeleid die is geconfigureerd voor 'Waarschuwen'.
DECRYPT_ADMIN	De Web Proxy heeft de transactie gedecodeerd op basis van enkele standaardinstellingen voor de groep Decryptiebeleid.
DECRYPT_ADMIN_EXPIRED_CERT	De Web Proxy heeft de transactie gedecodeerd, hoewel het servercertificaat is verlopen.
DECRYPT_EUN_ADMIN_DEFAULT_ACTION	De Web Proxy heeft de transactie gedecodeerd op basis van standaardinstellingen als dropverbinding voor de beleidsgroep voor decodering wanneer EUN is ingeschakeld.
DECRYPT_EUN_ADMIN_EXPIRED_CERT	De Web Proxy decodeerde de transactie toen HTTPS-proxy-instellingen een verlopen certificaat dropten met EUN ingeschakeld.
DECRYPT_EUN_ADMIN_INVALID_LEAF_CERT	De Web Proxy decodeerde de transactie toen HTTPS-proxy-instellingen een ongeldig leafcertificaat dropten met EUN ingeschakeld.
DECRYPT_EUN_ADMIN_MISMATCHED_HOSTNAME	De Web Proxy decodeerde de transactie toen HTTPS-proxy-instellingen de niet-overeenkomende hostnaam dropten met EUN ingeschakeld.
DECRYPT_EUN_ADMIN_OCSP_OTHER_ERROR	De Web Proxy decodeerde de transactie wanneer HTTPS-proxy-instellingen een OCSP dropten met andere fouten met EUN ingeschakeld.
DECRYPT_EUN_ADMIN_OCSP_REVOKED_CERT	De Web Proxy decodeerde de transactie toen HTTPS-proxy-instellingen een OCSP ingetrokken certificaat dropten met EUN ingeschakeld.
DECRYPT_EUN_ADMIN_UNRECOGNITED_ROOT_CERT	De Web Proxy decodeerde de transactie wanneer HTTPS-proxy-instellingen een niet-herkende rootautoriteit of uitgeverscertificaat dropten met EUN ingeschakeld.
DECRYPT_EUN_CUSTOMCAT	De webproxy heeft de transactie gedecodeerd op basis van aangepaste filterinstellingen voor URL-categorieën

	voor de beleidsgroep voor decodering. Als EUN is ingeschakeld, wordt het verkeer verwijderd.
DECRYPT_EUN_WBRS	De Web Proxy heeft de transactie gedecodeerd op basis van de instellingen van het webreputatiefilter voor de beleidsgroep voor decodering. Als EUN is ingeschakeld, wordt het verkeer verwijderd.
DECRYPT_EUN_WBRS_NO_SCORE	De Web Proxy heeft de transactie gedecodeerd op basis van de instellingen van het webreputatiefilter voor geen score-URL in de beleidsgroep voor decodering. Als EUN is ingeschakeld, wordt het verkeer verwijderd.
DECRYPT_EUN_WEBCAT	De webproxy heeft de transactie gedecodeerd op basis van de filterinstellingen voor de URL-categorie voor de beleidsgroep voor decodering. Als EUN is ingeschakeld, wordt het verkeer verwijderd.
DECRYPT_WEBCAT	De webproxy heeft de transactie gedecodeerd op basis van de filterinstellingen voor de URL-categorie voor de groep Decryptiebeleid.
DECRYPT_WBRS	De Web Proxy heeft de transactie gedecodeerd op basis van de instellingen van het filter Webreputatie voor de groep Decryptiebeleid.
DEFAULT_CASE	Met de Web Proxy kon de client toegang krijgen tot de server omdat geen van de AsyncOS-services, zoals Web Reputation of Anti-Malware-scanning, enige actie ondernam op de transactie.
DENY_ADMIN	De Web Proxy heeft de transactie geweigerd. Dit gebeurt voor HTTPS-verzoeken wanneer verificatie vereist is en Decrypt for Authentication is uitgeschakeld in de HTTPS-proxy-instellingen.
DROP_ADMIN	De webproxy heeft de transactie laten vallen op basis van enkele standaardinstellingen voor de groep Decryptiebeleid.

DROP_ADMIN_EXPIRED_CERT	De webproxy heeft de transactie laten vallen omdat het servercertificaat is verlopen.
DROP_WEBCAT	De webproxy heeft de transactie laten vallen op basis van de filterinstellingen voor de URL-categorie voor de groep Decryptiebeleid.
DROP_WBRS	De webproxy heeft de transactie laten vallen op basis van de instellingen van het filter Webreputatie voor de groep Decryptiebeleid.
MONITOR_ADMIN_EXPIRED_CERT	De Web Proxy bewaakte de serverrespons omdat het servercertificaat is verlopen.
MONITOR_AMP_RESP	De Web Proxy bewaakte de serverrespons op basis van de Advanced Malware Protection-instellingen voor de Access Policy-groep.
MONITOR_AMW_RESP	De Web Proxy bewaakte de serverrespons op basis van de instellingen voor Anti-Malware voor de groep Toegangsbeleid.
MONITOR_AMW_RESP_URL	De Web Proxy vermoedt dat de URL in het HTTP-verzoek niet veilig kan zijn, maar het bewaakte de transactie op basis van de Anti-Malware-instellingen voor de Access Policy-groep.
MONITOR_AVC	De webproxy bewaakte de transactie op basis van de toepassingsinstellingen voor de groep Toegangsbeleid.
MONITOR_CONTINUE_CONTENT_UNSAFE	Oorspronkelijk blokkeerde de webproxy de transactie en werd de pagina Waarschuwen en doorgaan weergegeven op basis van de instellingen voor inhoudsbeoordelingen van de site in de groep Toegangsbeleid. Het clientverzoek was voor inhoud voor volwassenen en het beleid is geconfigureerd om gebruikers een waarschuwing te geven voor toegang tot inhoud voor volwassenen. De gebruiker accepteerde de waarschuwing en ging verder naar de oorspronkelijk gevraagde site, en geen andere scanengine blokkeerde

	vervolgens het verzoek.
MONITOR_CONTINUE_CUSTOMCAT	Oorspronkelijk blokkeerde de webproxy de transactie en gaf de pagina Waarschuwen en doorgaan weer op basis van een aangepaste URL-categorie in de groep Toegangsbeleid die is geconfigureerd als Waarschuwen. De gebruiker accepteerde de waarschuwing en ging verder naar de oorspronkelijk gevraagde site, en geen andere scanengine blokkeerde vervolgens het verzoek.
MONITOR_CONTINUE_WEBCAT	Oorspronkelijk blokkeerde de webproxy de transactie en gaf de pagina Waarschuwen en doorgaan weer op basis van een vooraf gedefinieerde URL-categorie in de groep Toegangsbeleid die is geconfigureerd voor 'Waarschuwen'. De gebruiker accepteerde de waarschuwing en ging verder naar de oorspronkelijk gevraagde site, en geen andere scanengine blokkeerde vervolgens het verzoek.
MONITOR_CONTINUE_YTCAT	Oorspronkelijk blokkeerde de webproxy de transactie en gaf de pagina Waarschuwen en doorgaan weer op basis van een vooraf gedefinieerde YouTube-categorie in de groep Toegangsbeleid die is geconfigureerd voor 'Waarschuwen'. De gebruiker accepteerde de waarschuwing en ging verder naar de oorspronkelijk gevraagde site, en geen andere scanengine blokkeerde vervolgens het verzoek.
MONITOR_IDS	De webproxy heeft het uploadverzoek gescand met behulp van een gegevensbeveiligingsbeleid of een extern DLP-beleid, maar heeft het verzoek niet geblokkeerd. Het evalueerde het verzoek aan de hand van het toegangsbeleid.
MONITOR_SUSPECT_USER_AGENT	De Web Proxy bewaakte de transactie op basis van de instelling Suspect User Agent voor de groep Toegangsbeleid.

MONITOR_WBRS	De Web Proxy bewaakte de transactie op basis van de instellingen van het Web Reputation-filter voor de groep Toegangsbeleid.
NO_AUTORISATIE	De Web Proxy stond de gebruiker geen toegang tot de toepassing toe omdat de gebruiker al was geverifieerd tegen een verificatiereeks, maar niet tegen een verificatiereeks die is geconfigureerd in het toepassingsverificatiebeleid.
NO_PASSWORD	De gebruiker heeft de verificatie mislukt.
PASSTHRU_ADMIN	De webproxy heeft de transactie doorlopen op basis van enkele standaardinstellingen voor de groep Decryptiebeleid.
PASSTHRU_ADMIN_EXPIRED_CERT	De webproxy heeft de transactie doorlopen, hoewel het servercertificaat is verlopen.
PASSTHRU_WEBCAT	De webproxy heeft de transactie doorlopen op basis van de filterinstellingen voor de URL-categorie voor de groep Decryptiebeleid.
PASSTHRU_WBRS	De webproxy heeft de transactie verwerkt op basis van de instellingen van het filter Webreputatie voor de groep Decryptiebeleid.
REDIRECT_CUSTOMCAT	De webproxy heeft de transactie omgeleid naar een andere URL op basis van een aangepaste URL-categorie in de groep toegangsbeleid die is geconfigureerd voor 'Omleiden'.
SAAS_AUTH	De Web Proxy gaf de gebruiker toegang tot de toepassing omdat de gebruiker op transparante wijze werd geverifieerd aan de hand van het verificatiegebied dat is geconfigureerd in het toepassingsverificatiebeleid.
Other (Overig)	De Web Proxy heeft het verzoek niet voltooid als gevolg van een fout, zoals een autorisatiefout, verbreken van de verbinding met de server of een onderbreking van de client.

Verdict-waarden voor scannen op malware

Een Malware scanning verdict is een waarde die wordt toegewezen aan een URL-verzoek of server reactie die de kans dat het Malware bevat bepaalt. De scanengines Webroot, McAfee en Sophos retourneren het scanvonnis voor malware naar de DVS-engine, zodat de DVS-engine kan bepalen of het gescande object moet worden gecontroleerd of geblokkeerd. Elk malwarescanning-vonnis komt overeen met een categorie Malware die wordt vermeld op de pagina Toegangsbeleid > Reputatie- en Anti-Malware-instellingen wanneer u de Anti-Malware-instellingen voor een bepaald toegangsbeleid bewerkt.

Deze lijst bevat de verschillende Malware Scanning Verdict Waarden en elke bijbehorende categorie Malware:

Verdict waarde voor scannen naar malware	categorie Malware
-	Niet ingesteld
0	onbekend
1	Niet gescand
2	Timeout
3	Fout
4	niet scanbaar
10	Generieke spyware
12	Browser Helper Object
13	adware
14	systeemmonitor
18	Commerciële systeemmonitor
19	kiezeres

Verdict waarde voor scannen naar malware	categorie Malware
20	kaper
21	Phishing-URL
22	Trojan Downloader
23	Trojaans paard
24	Trojan Phisher
25	worm
26	gecodeerd bestand
27	virus
33	Andere malware
34	PUA
35	afgebroken
36	uitbraakheuristiek
37	Bekende schadelijke en risicovolle bestanden

Gerelateerde informatie

- Gebruikershandleiding voor AsyncOS 15.2 voor Cisco Secure Web Appliance
- Best practices voor veilige webapparaten gebruiken
- Zorgen voor de juiste functionaliteit van de virtuele WSA HA-groep in een VMware-omgeving

- Prestatieparameter configureren in toegangslogboeken
- Inzicht in HTTPS-toegangslogindeling in Secure Web Appliance
- Toegang tot beveiligde logbestanden van webapparaten

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.