Sicherer Zugriff auf Web-Appliances

Inhalt

Einleitung

In diesem Dokument wird die Struktur des Zugriffsprotokolls für sichere Web-Appliances (SWA) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:

- Zugriff auf die Kommandozeile von SWA

- Administratorzugriff auf die SWA.
- Grundlegendes Verständnis des SWA-Workflows

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Zugriffsstruktur

In diesem Artikel wird die Accesslog-Struktur durch dieses Beispiel erläutert:

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

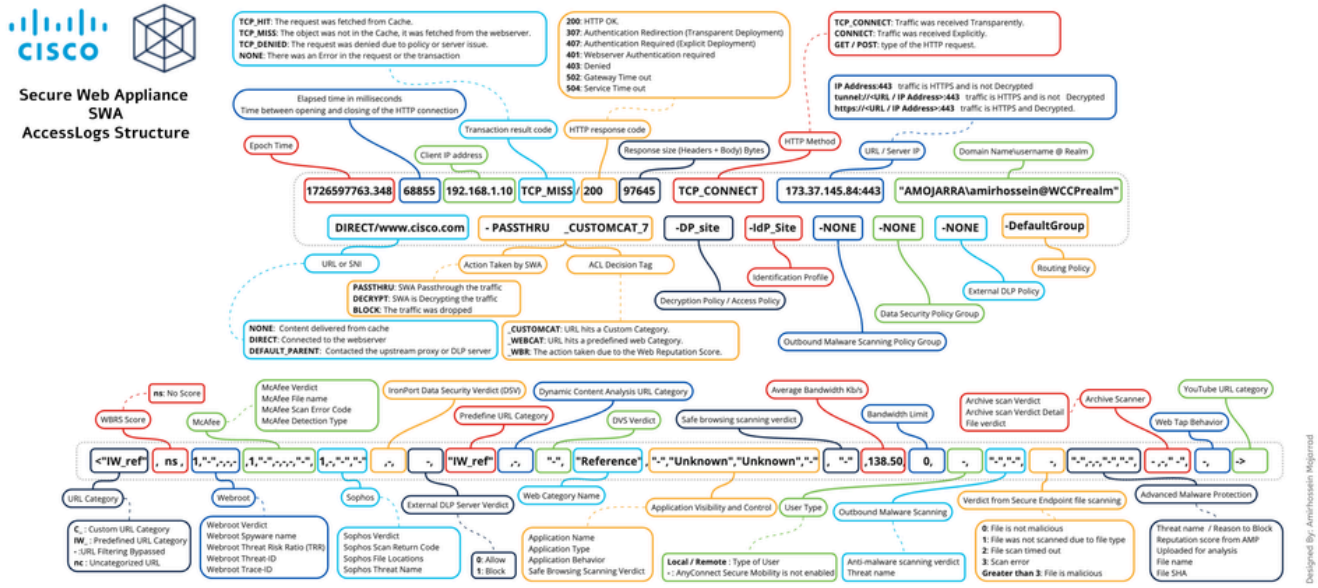

Bild - Zugriffsstruktur

Anmerkung: Die Struktur der Zugriffsprotokolle hängt von der SWA-Version ab. Am Anfang jeder Accesslog-Datei befindet sich eine Zeile, die die Struktur und die Reihenfolge des Formatbezeichners anzeigt.

Abschnitt	Beispiel aus AccessLog	Formatangabe	Details
Epochenzeit	1726597763.348	%t	Die Epochenzei Zeitverfolgung, Millisekunden/M 00:00 UTC verg Die Epochenzei Sie können dies beliebiges Linux

Verstrichene Zeit	68855	%e	Die Dauer in Mi abgeschlossen/
IP-Quelladresse	192.168.1.10	%a	Client/Source-I
Transaktionsergebniscode	TCP verpasst	%w	Der Transaktion auflöst. Hier sehen Sie TCP_HIT TCP_IMS_HIT TCP_MEM_HIT TCP verpasst TCP_AKTUALI

<table>
<tr><td></td><td></td><td></td><td>TCP_CLIENT_R
TCP ABGELEH
TCP_DENIED_
TCP_CLIENT_R
TCP_MISS_SS</td></tr>
<tr><td>HTTP-Antwortcode</td><td>/200</td><td>%h</td><td>Der HTTP-Antw
Antwort auf die
Hier ist die Liste
Informationen b
Artikel)<table><tr><td>Statuscode</td><td>B</td></tr><tr><td>000</td><td>0
d
e</td></tr><tr><td>2xx erfolgreich</td><td></td></tr><tr><td>200</td><td>C</td></tr><tr><td>204</td><td>K</td></tr><tr><td>206</td><td>T</td></tr><tr><td></td><td></td></tr></table></td></tr>
</table>

			3xx-Weiterleitung
			301 P
			302 T
			304 N
			307 T (W g
			4xx-Client-Fehler
			400 U
			401 W d B
			403 V
			404 N
			407 E
			5xx Serverfehler
			500 In
			502 U
			503 D
			504 G
Gesamtgröße übertragen	97645	%s	Gesamtzahl der
HTTP-Methode	TCP_VERBINDEN	%1r	Eine HTTP-Met gewünschte Akt Ressource ausg das Senden von HOLEN

			POST VERBINDEN TCP_VERBIND
Ziel	10.37.145.84:443	%2r	In diesem Absc Portnummer an Bei der transpar Datenverkehrs Wenn die URL Datenverkehr n Wenn die URL Datenverkehr e
Benutzername und	"AMOJARRA\amirhossein@WCCPrealm"	%A	Für diese Verbi

Authentifizierungsbereich			Wenn die Anfor Benutzernamen <Domänennam Authentifizierun Wenn die Anfor Authentifizierun
Zugriffstyp	DIRECT/	%H	Code, der besc kontaktiert wurd Die gängigsten NONE DIREKT DEFAULT_PAR
Serveradresse	www.cisco.com	%d	IP-Adresse der
MIME-Inhaltstyp/-Untertyp	-	%c	MIME Gibt die Reihe von Bytes standardisiert. Für die Rolle de • text/plain i lesbar sei • applicatio unbekann besonder vor Softwa Verhalten Eine vollständig

ACL-Entscheidungs-Tag	PASSTHRU_CUSTOMCAT_7-	%D	Ein ACL-Entsch Zugriffsprotokol behandelt hat. S URL-Kategorien Hinweis: D generierte Leistung zu Nachfolgend fin Entscheidungsn zum ACL Decis ACL-Entscheidu ZULASSEN_BE WBRS_ZULAS AMP_DATEI_V BLOCK_ADMIN BLOCK_ADMIN BLOCK_ADMIN

			BLOCK_ADMIN
			BLOCK_ADMIN
			BLOCK_ADMIN
			SPERRE_AMP
			BLOCKIEREN_
			BLOCK_INHAL
			BLOCKIEREN_
			BLOCK_ICAP

			BLOCK_WBRS
			BLOCKIEREN_
			BLOCK_YTCAT
			ENTSCHLÜSS
			DECRYPT_EU
			DECRYPT_EU
			DECRYPT_EU

			ENTSCHLÜSS
			ENTSCHLÜSS
			DROP_ADMIN
			DROP_WEBCA
			DROP_WBRS
			PASSTHRU_AD
			PASSTHRU_W
			PASSTHRU_W

			ANDERE
Richtlinienname	DP_Standort-	–	Je nach Art des • Name der und noch • Name der entschlüss
Identitätsrichtlinie	IDp_Standort-	–	Zeigt den Name
Richtliniengruppe für Scanning ausgehender Malware	NONE-	–	Gruppenname d Jedes Leerzeich (_) ersetzt.
Gruppe für Datensicherheitsrichtlinien	NONE-	–	Name der Cisco globalen Cisco DefaultGroup. D Datensicherheit keine Datensich Jedes Leerzeich (_) ersetzt.
Policy-Gruppe für externen SvD	NONE-	–	Wenn die Trans übereinstimmt, keine Richtlinie Jedes Leerzeich (_) ersetzt.
Routingrichtliniengruppe	Standardgruppe-	–	Routing-Richtlin Wenn die Trans dieser Wert Def ist dieser Wert D

<table>
<tr><td></td><td></td><td></td><td>Jedes Leerzeich
(_) ersetzt.</td></tr>
<tr><td>Anzapfen des Webverkehrs</td><td>NONE</td><td>–</td><td>Name der Web</td></tr>
<tr><td>URL-Kategorie Abkürzung</td><td><"C_Cisco",</td><td>%XC</td><td>URL-Kategorie,<table><tr><td>-</td><td>UR</td></tr><tr><td>nc</td><td>Nic</td></tr><tr><td>Fehler</td><td>UR</td></tr><tr><td>Imp</td><td>Un</td></tr><tr><td>IW_</td><td>We
beg
An
Ca</td></tr><tr><td>C_</td><td>We
beg
An
ber
trif</td></tr></table></td></tr>
<tr><td>Webreputations-Bewertung</td><td>-,</td><td>%XW</td><td>In diesem Feld
ns bedeutet, da</td></tr>
<tr><td>Webroot-Scanning</td><td>-",-",-,-,-,</td><td></td><td>Diese fünf Felde<table><tr><td>Webroot-Verdic</td></tr></table></td></tr>
</table>

			Webroot Spyna
			Webroot-TRR,
			Webroot-Bedro ID,
			Webroot-Tracel
McAfee-Scanning	-",-",-,-,-",-",		Diese sechs Fe
			McAfee-Verdict

			McAfee-Datein
			McAfee Scan-Fehlercode,
			McAfee-Erkennungstyp,
			McAfee-Virenty
			McAfee-Virusna
Sophos-Scanning	-,-,"-","-",		Diese vier Felde
			Sophos-Verdict

			Rückgabecode Sophos-Scans, Sophos- Dateispeicheror Sophos- Bedrohungsnar
Cisco Data Security-Scan	-,	%xl	Das Cisco Data "Inhalt" der Cisc Diese Liste bes 0.Zulassen 1.Block - (Bindestrich).V initiiert. Dieser W deaktiviert oder
Scan-Verdict für externen SvD	-,	%xp	Das Ergebnis d ICAP-Antwort. Diese Liste bes 0.Zulassen 1.Block - (Bindestrich).E initiiert. Dieser W deaktiviert ist od ausgenommene

			nicht gescannt v
Verdict der vordefinierten URL-Kategorie	"-",	%XQ	Die vordefinierte anforderungsse In diesem Feld v deaktiviert ist. Wenn die Anfor der vordefinierte Entscheidung w getroffen. Eine Liste der U Kategoriebesch
URL-Kategoriebeurteilung	-,	%XA	Das vom DCA-M Antwortseite fes Gilt nur für die U nc: Dieser Wert das Dynamic Co Anforderungsze darauf hin, dass kategorisiert wir
Verdict für Unified Inbound DVS	"-",	%XZ	Einheitliches An Malware-Kategc aktiviert sind. G blockiert oder üb
Bedrohungstyp des Webreputations-Filters	"-",	%xk	Der Kategoriena Filtern zurückge Webreputation I die Reputation g Normalerweise darunter ausgef
Gekapselte URL von Google Translate	"-",	%X#10#	Die URL, die in gekapselte URL

<table>
<tr>
<td>Anwendungskontrolle (AVC/ADC)</td>
<td>"-","-","-",</td>
<td></td>
<td>In diesen drei F
(AVC) und Appl
<table>
<tr><td>AVC-/ADC-Anwendungsna</td></tr>
<tr><td>AVC/ADC-Anwendungstyp</td></tr>
<tr><td>AVC/ADC-Anwendungsve</td></tr>
</table>
</td>
</tr>
<tr>
<td>Verdict für sicheres Surfen</td>
<td>"-",</td>
<td>%XS</td>
<td>Dieser Wert gib
für die Bewertur
<table>
<tr><td>eingraben</td><td>Die u
Funk</td></tr>
<tr><td>verführen</td><td>Die u
Bewe</td></tr>
<tr><td>abstützen</td><td>Die u
unter</td></tr>
<tr><td>Fehler</td><td>Die u
eines
noch
werd</td></tr>
<tr><td>-</td><td>Wede
Bewe</td></tr>
</table>
</td>
</tr>
</table>

			ange Trans oder Anwe
Durchschnittliche Bandbreite	11.35,	%XB	Die durchschnit benötigt wird, in
Kontrolle des Bandbreitenlimits	0,	%XT	Ein Wert, der an Bandbreitengren "1" gibt an, dass "0" gibt an, dass
Benutzertyp	-,	%I	Der Benutzertyp "[Remote]". Gilt nur, wenn A Wenn sie nicht a
Scannen auf ausgehende Malware	"-","-",		Diese beiden Fe Clientanforderun Richtlinie für da Verdict für Unifi Outbound DVS Name der ausg Bedrohung

Advanced Malware Protection	-,"-",-,-,"-","-",		Diese 6 Felder l Malware Protec Datei-Verdict Bedrohungsnar Reputationsbev Aktion zur Anal hochladen

			Dateiname Datei SHA
Archivsuche	-,-,"-",		Diese drei Felde Archiv-Scan-Verdict %

			Archivscan-Verdict-Detail Datei-Verdict
Web-Tap	-,	%XU	Web-Tap-Verha
YouTube-URL-Kategorie	->	%X#29#	Die der Transak diesem Feld wir

HTTP-Antwortcode

Hier finden Sie die vollständige Liste des HTTP-Antwortcodes.

Statuscode	Bedeutung
1xx Informationen	
100	Fortfahren
101	Switching-Protokolle
102	Verarbeitung
103	Erste Hinweise

2xx erfolgreich	
200	OK
201	Erstellt
202	Akzeptiert
203	Nicht autorisierende Informationen
204	Kein Inhalt
205	Inhalt zurücksetzen
206	Teilweise
207	Multistatus
208	Bereits gemeldet
226	Verwendete IM
3xx-Weiterleitung	
300	Mehrere Optionen
301	Dauerhaft verschoben
302	Gefunden (zuvor "Vorübergehend verschoben")
303	Weitere Informationen
304	Nicht geändert
305	Proxy verwenden
306	Switch-Proxy
307	Temporäre Umleitung zur Authentifizierung (Wird in der Regel bei der transparenten Bereitstellung gesehen, während SWA den Benutzer authentifiziert)
308	Permanente Umleitung
4xx-Client-Fehler	
400	Ungültige Anforderung
401	Webserver-Authentifizierung erforderlich (wird in der Regel bei der transparenten Bereitstellung verwendet, während der Benutzer von SWA authentifiziert wird)

402	Zahlung erforderlich
403	Verboten
404	Nicht gefunden
405	Methode nicht zulässig
406	Nicht akzeptabel
407	Explizite Proxy-Authentifizierung erforderlich
408	Anforderungs-Timeout
409	Konflikt
410	vorbei
411	Erforderliche Länge
412	Vorbedingung fehlgeschlagen
413	Nutzlast zu groß
414	URI zu lang
415	Nicht unterstützter Medientyp
416	Bereich nicht zufriedenstellend
417	Erwartung fehlgeschlagen
418	Ich bin ein Teekessel
421	Fehlgeleitete Anforderung
422	Nicht verarbeitbare Einheit
423	Gesperrt
424	Fehlgeschlagene Abhängigkeit
425	Zu früh
426	Upgrade erforderlich
428	Voraussetzung erforderlich
429	Zu viele Anfragen
431	Headerfelder für Anforderungen zu groß
451	Aus rechtlichen Gründen nicht verfügbar
5xx Serverfehler	
500	Interner Serverfehler

501	Nicht implementiert
502	Ungültiges Gateway
503	Dienst nicht verfügbar
504	Gateway-Zeitüberschreitung
505	HTTP-Version nicht unterstützt
506	Variante handelt auch aus
507	Unzureichender Speicher
508	Schleife erkannt
510	Nicht verlängert
511	Netzwerkauthentifizierung erforderlich

ACL-Entscheidungs-Tag

Nachfolgend finden Sie eine vollständige Liste der ACL-Entscheidungsmarkierungen:

ACL-Entscheidungs-Tag	Beschreibung
ALLOW_ADMIN_ERROR_PAGE	Der Webproxy hat die Transaktion zu einer Benachrichtigungsseite und zu einem beliebigen Logo zugelassen, das auf dieser Seite verwendet wird.
ZULASSEN_BENUTZERDEFINIERT	Der Webproxy hat die Transaktion basierend auf benutzerdefinierten URL-Kategoriefiltereinstellungen für die Zugriffsrichtliniengruppe zugelassen.
ALLOW_REFERER	Der Webproxy hat die Transaktion basierend auf einer Ausnahme für eingebettete/referenzierte Inhalte zugelassen.
WBRS_ZULASSEN	Der Webproxy hat die Transaktion basierend auf den Webreputations-Filtereinstellungen für die Zugriffsrichtliniengruppe zugelassen.
AMP_DATEI_VERDICT	Wert, der ein Verdict vom AMP-Reputationsserver für die Datei darstellt:
	1 - Unbekannt
	2 - Sauber
	3 - Schädlich
	4 - Nicht scanbar

ARCHIVESCAN_ALLCLEAR	Archiv-Scan-Verdict
ARCHIVESCAN_BLOCKEDFILETYP	ARCHIVESCAN_ALLCLEAR - Im inspizierten Archiv befinden sich keine blockierten Dateitypen.
ARCHIVESCAN_NESTEDTOODEE	ARCHIVESCAN_BLOCKEDFILETYPE - Im inspizierten Archiv befindet sich ein blockierter Dateityp. Das nächste Feld im Protokolleintrag (Verdict Detail) enthält Details, insbesondere den Typ der blockierten Datei und den Namen der blockierten Datei.
ARCHIVESCAN_UNKNOWNFMT	ARCHIVESCAN_NESTEDTOODEEP - Das Archiv wird blockiert, da es mehr "gekapselte" oder geschachtelte Archive enthält als der konfigurierte Maximalwert. Das Feld "Verdict Detail" enthält "Nicht scanbares Archiv blockiert".
ARCHIVESCAN_UNSCANABLE	ARCHIVESCAN_UNKNOWNFMT - Das Archiv wird blockiert, weil es einen Dateityp mit unbekanntem Format enthält. Das Verdict-Detail lautet "Nicht scannbares Archiv blockiert".
ARCHIVESCAN_FILETOOBIG	ARCHIVESCAN_UNSCANABLE - Das Archiv wird blockiert, weil es eine Datei enthält, die nicht gescannt werden kann. Das Verdict-Detail lautet "Nicht scannbares Archiv blockiert".
	ARCHIVESCAN_FILETOOBIG - Das Archiv wird blockiert, da die Größe des Archivs den konfigurierten Maximalwert übersteigt. Das Verdict-Detail lautet "Nicht scannbares Archiv blockiert".
	Archivscan-Verdict-Detail
	Das Feld und das Verdict-Feld im Protokolleintrag enthalten zusätzliche Informationen zum Verdict, z. B. den Typ der blockierten Datei und den Namen der blockierten Datei, "Nicht scannbares Archiv blockiert" oder "-", um anzugeben, dass das Archiv keine blockierten Dateitypen enthält.
	Wenn z. B. eine inspizierbare Archivdatei (ARCHIVESCAN_BLOCKEDFILETYPE)

	auf Basis der Zugriffsrichtlinie blockiert wird: Benutzerdefinierte Einstellungen für Objektsperrung. Der Eintrag Verdict Detail enthält den Typ der gesperrten Datei und den Namen der gesperrten Datei.
	Weitere Informationen finden Sie unter Zugriffsrichtlinien: Blockieren von Objekten und Archivinspektionseinstellungen für weitere Informationen zur Archivinspektion.
BLOCK_ADMIN	Die Transaktion wird aufgrund einiger Standardeinstellungen für die Zugriffsrichtliniengruppe blockiert.
BLOCK_ADMIN_VERBINDEN	Die Transaktion wird auf Basis des TCP-Ports des Ziels blockiert, wie in der Einstellung für HTTP CONNECT-Ports für die Zugriffsrichtliniengruppe definiert.
BLOCK_ADMIN_CUSTOM_USER_AGENT	Die Transaktion wird auf Basis des Benutzer-Agents blockiert, wie in der Einstellung Benutzerdefinierte Benutzer-Agents blockieren für die Zugriffsrichtlinien-Gruppe definiert.
BLOCK_ADMIN_TUNNELING	Der Webproxy blockierte die Transaktion basierend auf dem Tunneling des Nicht-HTTP-Verkehrs auf den HTTP-Ports für die Zugriffsrichtliniengruppe.
BLOCK_ADMIN_HTTPS_NichtLokalesZiel	Transaktion blockiert; -Client hat versucht, die Authentifizierung mithilfe des SSL-Ports als explizitem Proxy zu umgehen. Um dies zu verhindern, sind bei einer SSL-Verbindung mit der WSA selbst nur Anfragen an den tatsächlichen WSA-Umleitungshostnamen zulässig.
BLOCK_ADMIN_IDS	Die Transaktion wird aufgrund des MIME-Typs des Inhalts des Anforderungstexts blockiert, wie in der Gruppe "Datensicherheitsrichtlinie" definiert.
BLOCK_ADMIN_DATEITYP	Transaktion aufgrund des in der Zugriffsrichtliniengruppe definierten Dateityps blockiert.
BLOCK_ADMIN_PROTOKOLL	Die Transaktion wird auf Grundlage des

	Protokolls blockiert, das in der Einstellung "Protokolle blockieren" für die Zugriffsrichtliniengruppe definiert ist.
BLOCK_ADMIN_GRÖSSE	Die Transaktion wird aufgrund der Größe der Antwort blockiert, die in den Objektgrößeneinstellungen für die Zugriffsrichtliniengruppe definiert ist.
BLOCK_ADMIN_SIZE_IDS	Die Transaktion wird aufgrund der Größe des Inhalts des Anforderungstexts blockiert, wie in der Gruppe "Datensicherheitsrichtlinie" definiert.
SPERRE_AMP_RESP	Der Webproxy blockierte die Antwort basierend auf den Einstellungen für den erweiterten Malwareschutz für die Zugriffsrichtliniengruppe.
BLOCKIEREN_AMW_REQ	Der Webproxy blockierte die Anforderung basierend auf den Anti-Malware-Einstellungen für die Gruppe der Scanning-Richtlinie für ausgehende Malware. Der Anforderungstext enthält ein positives Malware-Urteil.
BLOCKIEREN_AMW_RESP	Der Webproxy blockierte die Antwort basierend auf den Anti-Malware-Einstellungen für die Zugriffsrichtlinien-Gruppe.
BLOCK_AMW_REQ_URL	Der Webproxy vermutet, dass die URL in der HTTP-Anforderung nicht sicher sein kann. Daher blockierte er die Transaktion zum Zeitpunkt der Anforderung auf Basis der Anti-Malware-Einstellungen für die Zugriffsrichtliniengruppe.
BLOCKIEREN_AVC	Die Transaktion wird aufgrund der konfigurierten Anwendungseinstellungen für die Zugriffsrichtliniengruppe blockiert.
BLOCK_INHALT_UNSICHER	Die Transaktion wird aufgrund der Einstellungen für die Inhaltsbewertung der Website für die Zugriffsrichtliniengruppe blockiert. Die Client-Anforderung galt für nicht jugendfreie Inhalte, und die Richtlinie ist so konfiguriert, dass nicht jugendfreie Inhalte blockiert werden.
BLOCK_CONTINUE_CONTENT_UNSAFE	Die Transaktion wurde blockiert, und die

	Seite "Warnen und fortfahren" wird auf Basis der Einstellungen für die Bewertung des Website-Inhalts in der Gruppe "Zugriffsrichtlinie" angezeigt. Die Client-Anforderung galt für nicht jugendfreie Inhalte, und die Richtlinie ist so konfiguriert, dass Benutzer, die auf nicht jugendfreie Inhalte zugreifen, gewarnt werden.
BLOCKIEREN_FORTFAHREN_ANPASSEN	Die Transaktion wurde blockiert, und die Seite "Warnen und fortfahren" wird auf Basis einer benutzerdefinierten URL-Kategorie in der Zugriffsrichtlinien-Gruppe angezeigt, die auf "Warnen" konfiguriert ist.
BLOCK_CONTINUE_WEBCAT	Die Transaktion wurde blockiert, und die Seite "Warnen und fortfahren" wird auf Basis einer vordefinierten URL-Kategorie in der Zugriffsrichtlinien-Gruppe angezeigt, die auf "Warnen" konfiguriert ist.
BLOCKIEREN_ANPASSEN	Die Transaktion wird aufgrund von benutzerdefinierten Einstellungen für die URL-Kategoriefilterung für die Zugriffsrichtliniengruppe blockiert.
BLOCK_ICAP	Der Webproxy blockierte die Anforderung basierend auf der Beurteilung des externen SvD-Systems, wie in der Gruppe Richtlinien für externen SvD definiert.
BLOCKSUCHE_UNSICHER	Die Clientanforderung enthielt eine unsichere Suchabfrage, und die Zugriffsrichtlinie wurde so konfiguriert, dass sichere Suchvorgänge durchgesetzt werden, sodass die ursprüngliche Clientanforderung blockiert wurde.
BLOCK_VERDÄCHTIG_BENUTZER_AGENT	Die Transaktion wird aufgrund der Einstellung des verdächtigen Benutzer-Agents für die Zugriffsrichtliniengruppe blockiert.
BLOCK_UNSUPPORTED_SEARCH_APP	Transaktion aufgrund der Einstellungen für die sichere Suche für die Zugriffsrichtliniengruppe blockiert. Die Transaktion betrifft eine nicht unterstützte Suchmaschine, und die

	Richtlinie ist so konfiguriert, dass nicht unterstützte Suchmaschinen blockiert werden.
BLOCK_WBRS	Die Transaktion wird aufgrund der Webreputations-Filtereinstellungen für die Zugriffsrichtliniengruppe blockiert.
BLOCK_WBRS_IDS	Der Webproxy blockierte die Uploadanfrage basierend auf den Webreputations-Filtereinstellungen für die Datensicherheitsrichtliniengruppe.
BLOCKIEREN_WEBCAT	Die Transaktion wird aufgrund der Einstellungen für die URL-Kategoriefilterung für die Zugriffsrichtliniengruppe gesperrt.
BLOCK_WEBCAT_IDS	Der Webproxy blockierte die Uploadanfrage basierend auf den URL-Kategoriefiltereinstellungen für die Datensicherheitsrichtliniengruppe.
BLOCK_YTCAT	Der Webproxy blockierte die Transaktion auf Grundlage der vordefinierten Einstellungen für die YouTube-Kategoriefilterung für die Zugriffsrichtliniengruppe.
BLOCK_FORTFAHREN_JETZT	Der Webproxy blockierte die Transaktion und zeigte die Seite Warnen und fortfahren an, basierend auf einer vordefinierten YouTube-Kategorie in der Zugriffsrichtlinien-Gruppe, die auf 'Warnen' konfiguriert ist.
ENTSCHLÜSSELN_ADMIN	Der Webproxy hat die Transaktion anhand einiger Standardeinstellungen für die Gruppe Entschlüsselungsrichtlinie entschlüsselt.
DECRYPT_ADMIN_EXPIRED_CERT	Der Webproxy hat die Transaktion entschlüsselt, obwohl das Serverzertifikat abgelaufen ist.
DECRYPT_EUN_ADMIN_DEFAULT_ACTION	Der Webproxy hat die Transaktion anhand der Standardeinstellungen als Verbindung für die Entschlüsselungsrichtliniengruppe entschlüsselt, wenn EUN aktiviert ist.
DECRYPT_EUN_ADMIN_EXPIRED_CERT	Der Webproxy hat die Transaktion entschlüsselt, wenn die HTTPS-Proxyeinstellungen ein abgelaufenes Zertifikat mit aktivierter EUN löschen.
DECRYPT_EUN_ADMIN_INVALID_LEAF_CERT	Der Webproxy hat die Transaktion

	entschlüsselt, wenn die HTTPS-Proxyeinstellungen ein ungültiges Endknoten-Zertifikat mit aktivierter EUN löschen.
DECRYPT_EUN_ADMIN_MISMATCHED_HOSTNAME	Der Webproxy hat die Transaktion entschlüsselt, wenn die HTTPS-Proxyeinstellungen den nicht übereinstimmenden Hostnamen mit aktivierter EUN verwerfen.
DECRYPT_EUN_ADMIN_OCSP_OTHER_ERROR	Der Webproxy hat die Transaktion entschlüsselt, wenn die HTTPS-Proxyeinstellungen einen OCSP mit anderen Fehlern mit aktivierter EUN verwerfen.
DECRYPT_EUN_ADMIN_OCSP_REVOKED_CERT	Der Webproxy hat die Transaktion entschlüsselt, wenn die HTTPS-Proxyeinstellungen ein vom OCSP zurückgenommenes Zertifikat mit aktivierter EUN löschen.
DECRYPT_EUN_ADMIN_UNRECOGNIZED_ROOT_CERT	Der Webproxy hat die Transaktion entschlüsselt, wenn die HTTPS-Proxyeinstellungen ein nicht erkanntes Stammautoritäts- oder Ausstellerzertifikat mit aktivierter EUN löschen.
DECRYPT_EUN_CUSTOMCAT	Der Webproxy hat die Transaktion basierend auf benutzerdefinierten URL-Kategoriefiltereinstellungen für die Entschlüsselungsrichtliniengruppe entschlüsselt. Wenn EUN aktiviert ist, wird der Datenverkehr verworfen.
DECRYPT_EUN_WBRS	Der Webproxy hat die Transaktion basierend auf den Webreputations-Filtereinstellungen für die Gruppe der Entschlüsselungsrichtlinien entschlüsselt. Wenn EUN aktiviert ist, wird der Datenverkehr verworfen.
DECRYPT_EUN_WBRS_NO_SCORE	Der Webproxy hat die Transaktion basierend auf den Webreputations-Filtereinstellungen entschlüsselt, für die in der Gruppe der Entschlüsselungsrichtlinien keine URL für die Bewertung angegeben wurde. Wenn EUN aktiviert ist, wird der Datenverkehr verworfen.
DECRYPT_EUN_WEBCAT	Der Webproxy hat die Transaktion

	basierend auf den Einstellungen für die URL-Kategoriefilterung für die Entschlüsselungsrichtliniengruppe entschlüsselt. Wenn EUN aktiviert ist, wird der Datenverkehr verworfen.
ENTSCHLÜSSELN_WEBCAT	Der Webproxy hat die Transaktion basierend auf den Filtereinstellungen der URL-Kategorie für die Entschlüsselungsrichtliniengruppe entschlüsselt.
ENTSCHLÜSSELN_WBRS	Der Webproxy hat die Transaktion basierend auf den Webreputations-Filtereinstellungen für die Entschlüsselungsrichtliniengruppe entschlüsselt.
STANDARD_FALL	Der Webproxy erlaubte dem Client den Zugriff auf den Server, da keiner der AsyncOS-Dienste, wie z.B. Webreputation oder Anti-Malware-Scanning, eine Aktion für die Transaktion ausgeführt hat.
VERWEIGERN_ADMIN	Der Webproxy hat die Transaktion abgelehnt. Dies tritt bei HTTPS-Anforderungen auf, wenn Authentifizierung erforderlich ist und Entschlüsseln für Authentifizierung in den HTTPS-Proxyeinstellungen deaktiviert ist.
DROP_ADMIN	Der Webproxy hat die Transaktion aufgrund einiger Standardeinstellungen für die Gruppe Entschlüsselungsrichtlinie gelöscht.
DROP_ADMIN_EXPIRED_CERT	Der Webproxy hat die Transaktion abgebrochen, weil das Serverzertifikat abgelaufen ist.
DROP_WEBCAT	Der Webproxy hat die Transaktion basierend auf den Einstellungen für die URL-Kategoriefilterung für die Entschlüsselungsrichtliniengruppe gelöscht.
DROP_WBRS	Der Webproxy hat die Transaktion basierend auf den Webreputations-Filtereinstellungen für die Entschlüsselungsrichtliniengruppe gelöscht.
MONITOR_ADMIN_EXPIRED_CERT	Der Webproxy hat die Serverantwort

	überwacht, da das Serverzertifikat abgelaufen ist.
MONITOR_AMP_RESP	Der Webproxy überwachte die Serverantwort basierend auf den Einstellungen für den erweiterten Malwareschutz für die Zugriffsrichtliniengruppe.
MONITOR_AMW_RESP	Der Webproxy überwachte die Serverantwort basierend auf den Anti-Malware-Einstellungen für die Zugriffsrichtliniengruppe.
MONITOR_AMW_RESP_URL	Der Webproxy vermutet, dass die URL in der HTTP-Anforderung nicht sicher sein kann, aber er hat die Transaktion auf der Basis der Anti-Malware-Einstellungen für die Zugriffsrichtliniengruppe überwacht.
MONITOR_AVC	Der Webproxy überwachte die Transaktion basierend auf den Anwendungseinstellungen für die Zugriffsrichtliniengruppe.
MONITOR_CONTINUE_CONTENT_UNSAFE	Ursprünglich blockierte der Webproxy die Transaktion und zeigte die Seite Warnen und Fortfahren auf der Grundlage der Einstellungen für die Bewertung des Websiteinhalts in der Gruppe Zugriffsrichtlinie an. Die Client-Anforderung galt für nicht jugendfreie Inhalte, und die Richtlinie ist so konfiguriert, dass Benutzer, die auf nicht jugendfreie Inhalte zugreifen, gewarnt werden. Der Benutzer akzeptierte die Warnung und fuhr mit der ursprünglich angeforderten Website fort. Keine andere Scan-Engine blockierte die Anforderung anschließend.
MONITOR_CONTINUE_CUSTOMCAT	Ursprünglich blockierte der Webproxy die Transaktion und zeigte die Seite "Warnen und fortfahren" an, basierend auf einer benutzerdefinierten URL-Kategorie in der Zugriffsrichtlinien-Gruppe, die auf "Warnen" konfiguriert ist. Der Benutzer akzeptierte die Warnung und fuhr mit der ursprünglich angeforderten Website fort. Keine andere Scan-Engine blockierte die

	Anforderung anschließend.
MONITOR_CONTINUE_WEBCAT	Ursprünglich blockierte der Webproxy die Transaktion und zeigte die Seite "Warnen und fortfahren" auf der Grundlage einer vordefinierten URL-Kategorie in der Zugriffsrichtlinien-Gruppe an, die auf "Warnen" konfiguriert wurde. Der Benutzer akzeptierte die Warnung und fuhr mit der ursprünglich angeforderten Website fort. Keine andere Scan-Engine blockierte die Anforderung anschließend.
MONITOR_CONTINUE_YTCAT	Ursprünglich blockierte der Webproxy die Transaktion und zeigte die Seite Warnen und Fortfahren auf der Grundlage einer vordefinierten YouTube-Kategorie in der Zugriffsrichtlinien-Gruppe an, die auf 'Warnen' konfiguriert wurde. Der Benutzer akzeptierte die Warnung und fuhr mit der ursprünglich angeforderten Website fort. Keine andere Scan-Engine blockierte die Anforderung anschließend.
MONITOR_IDS	Der Webproxy hat die Uploadanfrage entweder mithilfe einer Datensicherheitsrichtlinie oder einer Richtlinie für externen SvD gescannt, die Anforderung jedoch nicht blockiert. Die Anfrage wurde anhand der Zugriffsrichtlinien ausgewertet.
MONITOR_SUSPECT_USER_AGENT	Der Webproxy überwachte die Transaktion basierend auf der Einstellung des verdächtigen Benutzer-Agents für die Zugriffsrichtliniengruppe.
MONITOR_WBRS	Der Webproxy überwachte die Transaktion basierend auf den Webreputations-Filtereinstellungen für die Zugriffsrichtliniengruppe.
NO_AUTHORIZATION	Der Webproxy hat dem Benutzer den Zugriff auf die Anwendung nicht erlaubt, da der Benutzer bereits für einen Authentifizierungsbereich authentifiziert wurde, jedoch nicht für einen Authentifizierungsbereich, der in der

	Authentifizierungsrichtlinie für die Anwendung konfiguriert wurde.
KEIN_KENNWORT	Der Benutzer konnte nicht authentifiziert werden.
PASSTHRU_ADMIN	Der Webproxy hat die Transaktion basierend auf einigen Standardeinstellungen für die Gruppe Entschlüsselungsrichtlinie weitergeleitet.
PASSTHRU_ADMIN_EXPIRED_CERT	Der Webproxy hat die Transaktion durchlaufen, obwohl das Serverzertifikat abgelaufen ist.
PASSTHRU_WEBCAT	Der Webproxy hat die Transaktion basierend auf den Einstellungen für die URL-Kategoriefilterung für die Entschlüsselungsrichtliniengruppe weitergeleitet.
PASSTHRU_WBRS	Der Webproxy hat die Transaktion basierend auf den Webreputations-Filtereinstellungen für die Entschlüsselungsrichtliniengruppe weitergeleitet.
REDIRECT_CUSTOMCAT	Der Webproxy hat die Transaktion basierend auf einer benutzerdefinierten URL-Kategorie in der Zugriffsrichtlinien-Gruppe, die für "Redirect" konfiguriert ist, an eine andere URL umgeleitet.
SAAS_AUTH	Der Webproxy gewährte dem Benutzer Zugriff auf die Anwendung, da der Benutzer mithilfe des in der Anwendungsauthentifizierungsrichtlinie konfigurierten Authentifizierungsbereichs transparent authentifiziert wurde.
ANDERE	Der Webproxy hat die Anforderung aufgrund eines Fehlers nicht abgeschlossen, z. B. aufgrund eines Autorisierungsfehlers, einer Servertrennung oder eines Abbruchs vom Client.

Verdict-Werte für Malware-Scanning

Ein Malware-Scan-Verdict ist ein Wert, der einer URL-Anfrage oder einer Serverantwort

zugewiesen wird und die Wahrscheinlichkeit bestimmt, dass Malware darin enthalten ist. Die Webroot-, McAfee- und Sophos-Scanmodule geben das Verdict des Malware-Scans an das DVS-Modul zurück, sodass das DVS-Modul ermitteln kann, ob das gescannte Objekt überwacht oder blockiert werden soll. Jedes Verdict des Malware-Scans entspricht einer Malware-Kategorie, die auf der Seite Zugriffsrichtlinien > Reputation und Anti-Malware-Einstellungen aufgeführt ist, wenn Sie die Anti-Malware-Einstellungen für eine bestimmte Zugriffsrichtlinie bearbeiten.

Diese Liste enthält die verschiedenen Verdict-Werte für das Scannen von Malware und die entsprechenden Malware-Kategorien:

Verdict-Wert für Malware-Scanning	Malware-Kategorie
-	Nicht festgelegt
0	Unbekannt
1	Nicht gescannt
2	Zeitüberschreitung
3	Fehler
4	Nicht scannbar
10	Allgemeine Spyware
12	Browser-Hilfsobjekt
13	Adware
14	Systemüberwachung
18	Commercial System Monitor
19	Dialer

Verdict-Wert für Malware-Scanning	Malware-Kategorie
20	Entführer
21	Phishing-URL
22	Trojaner-Downloader
23	Trojaner
24	Trojanisches Phishingmodul
25	Wurm
26	Verschlüsselte Datei
27	Virus
33	Sonstige Malware
34	PUA
35	Abgebrochen
36	Outbreak-Heuristik
37	Bekannte schädliche und risikoreiche Dateien

Zugehörige Informationen

- Bedienungsanleitung für AsyncOS 15.2 für Cisco Secure Web Appliance
- Best Practices für sichere Web-Appliances
- Gewährleistung der korrekten Funktionalität der virtuellen WSA HA-Gruppe in einer VMware-Umgebung

- Konfigurieren von Leistungsparametern in Zugriffsprotokollen
- HTTPS-Zugriffsformat in sicherer Web-Appliance
- Zugreifen auf Protokolle der sicheren Web-Appliance

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.