Compreender os registros de acesso do dispositivo da Web seguro

Contents

Introdução

Este documento descreve a estrutura do Access Log do Secure Web Appliance (SWA).

Pré-requisitos

Requisitos

A Cisco recomenda o conhecimento destes tópicos:

- Acesso à interface de linha de comando (CLI) do SWA.

- Acesso administrativo ao SWA.
- Entendimento básico do fluxo de trabalho do SWA.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto

potencial de qualquer comando.

Estrutura do log de acesso

Neste artigo, a estrutura do Accesslog é explicada por este exemplo:

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

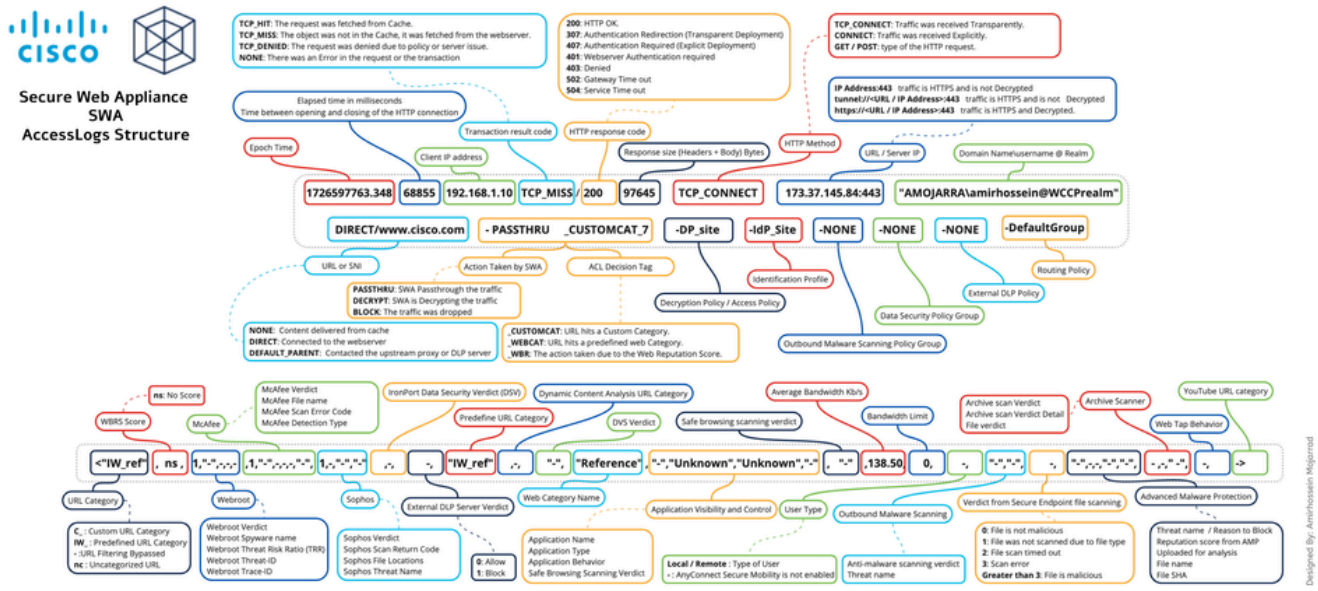

Imagem - Estrutura do registro de acessos

Note: A estrutura dos logs de acesso depende da versão do SWA. No início de cada arquivo Accesslog, há uma linha que mostra sua estrutura e a ordem do Especificador de Formato.

Seção	Exemplo do registro de acessos	Especificador de Formato	Detalhes
Tempo de época	1726597763.348	% t	O tempo de época (geralmente c é um sistema para rastrear o tem (ou milissegundos/microssegund 1970, às 00:00:00 UTC

			O tempo de Época em que a tran Você pode converter este valor p qualquer sistema operacional linu
Tempo decorrido	68855	% e	A quantidade de milissegundos d concluída/anulada e a conexão s
Endereço IP origem	192.168.1.10	% a	Endereço IP do cliente/origem.
Código do Resultado da Transação	TCP_MISS	% w	O Código de resultado da transa solicitações do cliente. Aqui está a lista dos Códigos de TCP_HIT TCP_IMS_HIT TCP_MEM_HIT TCP_MISS TCP_REFRESH_HIT

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td></td></tr>
<tr><td>TCP_CLIENT_REFRESH_MISS</td></tr>
<tr><td>TCP_DENIED</td></tr>
<tr><td>HTTPS TCP_DENIED_SSL</td></tr>
<tr><td>TCP_CLIENT_REFRESH_MISS</td></tr>
<tr><td>HTTPS TCP_MISS_SSL</td></tr>
</table>
</td></tr>
<tr><td>Código de Resposta HTTP</td><td>/200</td><td>% h</td><td>O Código de Resposta HTTP rep
servidor Web em resposta à soli

Aqui está a lista dos códigos de
obter mais informações visite a s
artigo)
<table>
<tr><td>Código de status</td><td>Significado</td></tr>
<tr><td>000</td><td>000 é um cód
uma interrupç
mais tarde du</td></tr>
<tr><td>2xx Bem-sucedido</td><td></td></tr>
<tr><td>200</td><td>OK</td></tr>
</table>
</td></tr>
</table>

			204	Sem conteúdo
			206	Conteúdo par de intervalo)
			Redirecionamento 3xx	
			301	Redirecionam
			302	Redirecionam
			304	Não Modificad
			307	Redirecionam (Geralmente v enquanto o S
			Erro do cliente 4xx	
			400	Solicitação In
			401	Autenticação vista na impla está autentica
			403	Proibido
			404	Not found
			407	Autenticação
			Erro de servidor 5xx	
			500	Erro interno d
			502	Gateway inco
			503	Serviço indisp
			504	Tempo limite
Tamanho Total Transferido	97645	%s	Total de bytes transferidos para a	

<table>
<tr>
<td>Método de HTTP</td>
<td>TCP_CONNECT</td>
<td>% 1r</td>
<td>Um método HTTP é uma forma p
ação desejada a ser executada e
recuperar dados com GET ou en
<table>
<tr><td>GET</td><td>O m
dad
excl
não
term</td></tr>
<tr><td>POST</td><td>O m
dad
corp
para
envi
serv</td></tr>
<tr><td>CONNECT</td><td>O m
esta
prox
con
dest
tráfe
cript

Indi
expl
o cli
dire</td></tr>
<tr><td>TCP_CONNECT</td><td>Indi
tran
WC</td></tr>
</table>
</td>
</tr>
<tr>
<td>Destino</td>
<td>10.37.145.84:443</td>
<td>% 2r</td>
<td>Esta seção mostra o URL do ser

No redirecionamento transparent
descriptografado, o SWA mostra
porta.

Se a URL começar com tunnel://
descriptografou o tráfego.

Se o URL começar com https:// s</td>
</tr>
</table>

<table>
<tr><td></td><td></td><td></td><td>tráfego.</td></tr>
<tr><td>Nome de usuário e território de autenticação</td><td>"AMOJARRA\amirhossein@WCCPrealm"</td><td>%A</td><td>Credenciais usadas para esta co

Se a solicitação for autenticada, territórios de autenticação como:

<Nome do domínio> \ <Nome do autenticação>

Se a solicitação ainda não tiver s autenticação, você verá no regis</td></tr>
<tr><td>Tipo de acesso</td><td>DIRECT/</td><td>% H</td><td>Código que descreve qual servid conteúdo da solicitação.

Os valores mais comuns incluem

<table><tr><td>NENHUM</td><td>O Web Pro contatou n conteúdo.</td></tr><tr><td>DIRECT</td><td>O Web Pro solicitação</td></tr><tr><td>DEFAULT_PARENT</td><td>O Web Pro servidor DL</td></tr></table></td></tr>
<tr><td>Endereço do servidor</td><td>www.cisco.com</td><td>%d</td><td>Endereço IP da fonte de dados c</td></tr>
<tr><td>Tipo/subtipo de conteúdo MIME</td><td>-</td><td>% c</td><td>MIME Indica a natureza e o form sortimento de bytes. Os tipos MI RFC 6838

Dois tipos MIME principais são ir

• text/plain é o valor padrão deve ser legível e não deve
• application/octet-stream é Um tipo de arquivo descon navegadores têm um cuida</td></tr>
</table>

<table>
<tr><td></td><td></td><td></td><td>para proteger os usuários d
possíveis comportamentos

Para obter uma lista completa de</td></tr>
<tr><td>Marca de decisão da ACL</td><td>PASSTHRU_CUSTOMCAT_7-</td><td>%D</td><td>Uma marca de decisão da ACL é
acesso que indica como o Web F
informações dos filtros do Web F
mecanismos de varredura.

Observação: o final da marc
gerado dinamicamente que
aumentar o desempenho. V

Esta é uma lista das Marcas de d
obter mais informações, visite a s
artigo)
<table><tr><td>Marca de decisão da 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
			DECRYPT_ADMIN
			DECRYPT_EUN_CUSTOMCAT
			DECRYPT_EUN_WBRS
			DECRYPT_EUN_WEBCAT

			DESCRIPTOGRAFAR_WEBCAT
			DESCRIPTOGRAFAR_WBRS
			DROP_ADMIN
			DROP_WEBCAT
			DROP_WBRS
			PASSTHRU_ADMIN
			PASSTHRU_WEBCAT
			PASSTHRU_WBRS
			OUTROS

Nome da política	DP_site-	N/A	Depende do tipo de tráfego, isso • Nome da Política de Descr não estiver descriptografad • Nome da Política de Acess descriptografado.
Política de identidade	IdP_Site-	N/A	Mostra o nome do perfil de identi
Grupo de Políticas de Verificação de Malware de Saída	NENHUM-	N/A	Nome do grupo de Política de Ve Qualquer espaço no nome do gr sublinhado (_)
Grupo de Políticas de Segurança de Dados	NENHUM-	N/A	Nome do grupo de Política de Se transação corresponde à Política esse valor é DefaultGroup. Esse somente quando os Filtros de Se ativados. "NONE" aparece quand dados foi aplicada. Qualquer espaço no nome do gr sublinhado (_)
Grupo de Política DLP Externo	NENHUM-	N/A	Quando a transação corresponde é DefaultGroup. "NONE" aparece foi aplicada. Qualquer espaço no nome do gr sublinhado (_).
Grupo de Política de Roteamento	GrupoPadrão-	N/A	Nome do grupo de Política de Ro asProxyGroupName/ProxyServe Quando a transação corresponde valor é DefaultRouting. Quando n

<table>
<tr><td></td><td></td><td></td><td>esse valor é DIRECT
Qualquer espaço no nome do gr
sublinhado (_).</td></tr>
<tr><td>Toque no tráfego da Web</td><td>NENHUM</td><td>N/A</td><td>Nome da Política de Toque de T</td></tr>
<tr><td>Abreviação da categoria de URL</td><td><"C_Cisco",</td><td>%XC</td><td>Categoria de URL que correspor<table><tr><td>-</td><td>Filtragem de URL Ig</td></tr><tr><td>nc</td><td>URLs não categoriz</td></tr><tr><td>err</td><td>Filtragem de URL Ig</td></tr><tr><td>imp</td><td>Impossível</td></tr><tr><td>IW_</td><td>Se o nome da categ com IW_, isso signif solicitação estava a Categoria de URL p Cisco</td></tr><tr><td>C_</td><td>Se o nome da categ com IC_, significa q estava atingindo Ca personalizada</td></tr></table></td></tr>
<tr><td>Pontuação do Web Reputation</td><td>-,</td><td>% XW</td><td>Esse campo mostra a pontuaçã
ns significa que o URL não tem p</td></tr>
<tr><td>Varredura do Webroot</td><td>-,"-",-,-,-,</td><td></td><td>Esses 5 campos estão relaciona<table><tr><td>Veredito do Webroot,</td><td>% Xv</td></tr></table></td></tr>
</table>

			Webroot Spyname	"%Xn"
			Webroot TRR	% Xt
			ID de ameaça do Webroot,	%Xs
			Webroot TraceID	%Xi
Varredura McAfee	-,"-",-,-,-,"-",		Esses 6 campos estão relaciona	
			Veredito da McAfee,	%Xd

			Nome de arquivo da McAfee,	"%Xe"
			Código de erro de varredura da McAfee,	% Xf
			Tipo de detecção McAfee,	% Xg
			Tipo de vírus da McAfee,	% Xh
			Nome de vírus da McAfee,	"%Xj"
Verificação Sophos	-,-,"-","-",		Esses 4 campos estão relaciona	
			Resultado do Sophos,	% XY

			Código de retorno de verificação Sophos,	% Xx
			Locais de arquivos do Sophos,	"%Xy"
			Nome da ameaça Sophos,	"%Xz"
Veredito da verificação de segurança de dados da Cisco	-,	% Xl	O veredito de verificação do Cisc coluna Conteúdo da Política de s Esta lista descreve os valores po 0.Permitir 1.Bloquear - (hífen).Nenhuma verificação foi Dados da Cisco. Esse valor apar dados da Cisco estão desabilitad está definida como Permitir.	
Veredito de verificação de DLP externo	-,	% Xp	O veredito de verificação de DLP na resposta de ICAP. Esta lista descreve os valores po 0.Permitir	

			1.Bloquear - (hífen).Nenhuma verificação foi valor aparece quando a verificaç quando o conteúdo não foi verifi isenta na página Políticas de DL
Veredito de categoria de URL predefinido	"-",	%XQ	O veredito predefinido da catego verificação do lado da solicitaçã Esse campo lista um hífen (-) q Se a solicitação atingir uma Cate poderá ver o nome da categoria mas a decisão foi tomada pela c Para obter uma lista de abreviaç consulteDescrições de categoria
Veredito de categoria de URL	-,	%XA	O veredito da categoria de URL (Dynamic Content Analysis, anál verificação do lado da resposta, Aplica-se somente ao mecanism uso da Web da Cisco. nc: Esse valor aparece no veredi quando o mecanismo de análise nenhuma categoria de URL é atr indicando que a URL é descateg inicial antes que a verificação do
Veredito de Unified Inbound DVS	"-",	%XZ	Veredito de verificação antimalw fornece a categoria de malware i verificação estão habilitados. Ap monitoradas devido à verificaçã
Tipo de Ameaça do Filtro do Web Reputation	"-",	% Xk	O Nome da categoria ou o Tipo Web Reputation. O nome da cat Web é alta e o tipo de ameaça é Normalmente, esse campo é pre abaixo.

<table>
<tr><td>URL encapsulada do Google Translate</td><td>"-",</td><td>%X#10#</td><td>O URL que é encapsulado dentr
Se não houver um URL encapsu</td></tr>
<tr><td>Controle de aplicativos (AVC/ADC)</td><td>"-","-","-",</td><td></td><td>Nesses três campos, são registra
and Control (AVC) e Application
<table><tr><td>Nome do aplicativo AVC/ADC</td><td>"%XO"</td><td>C
p
a
n</td></tr><tr><td>Tipo de aplicativo AVC/ADC</td><td>"%Xu"</td><td>C
n
s
A</td></tr><tr><td>Comportamento do aplicativo AVC/ADC</td><td>"%Xb"</td><td>C
p
a
n

E
A</td></tr></table></td></tr>
<tr><td>Veredito de Navegação Segura</td><td>"-",</td><td>%XS</td><td>Esse valor indica se o recurso de
conteúdo de site foi aplicado à tr
<table><tr><td>ensrch</td><td>A solicitação original do
pesquisa segura foi aplic</td></tr><tr><td>encrt</td><td>A solicitação original do
classificações de conteú</td></tr><tr><td>unsupp</td><td>A solicitação original do
pesquisa sem suporte.</td></tr><tr><td>err</td><td>A solicitação original do</td></tr></table></td></tr>
</table>

<table>
<tr><td></td><td></td><td></td><td><table>
<tr><td></td><td>segura e o recurso de cl
puderam ser aplicados d</td></tr>
<tr><td>-</td><td>A pesquisa segura e o re
site não foram aplicados
recursos foram ignorado
em uma categoria de UR
de um aplicativo sem su</td></tr>
</table></td></tr>
<tr><td>Largura de Banda Média</td><td>11.35,</td><td>%XB</td><td>A largura de banda média consu</td></tr>
<tr><td>Controle de limite de largura de banda</td><td>0,</td><td>% XT</td><td>Um valor que indica se a solicita
controle de limite de largura de b
"1" indica que a solicitação foi lim
"0" indica que a solicitação não f</td></tr>
<tr><td>Tipo de usuário</td><td>-,</td><td>% I</td><td>O tipo de usuário que faz a solici
Aplica-se somente quando o Any
Quando não está habilitado, o va</td></tr>
<tr><td>Varredura de malware de saída</td><td>"-","-",</td><td></td><td>Esses 2 campos se aplicam a tra
devido à verificação de solicitaçã
verificação de malware de saída
<table>
<tr><td>Veredito do Unified Outbound DVS</td><td>"%X3"</td></tr>
<tr><td>Nome da ameaça de saída</td><td>"%X4"</td></tr>
</table></td></tr>
</table>

Proteção avançada contra malware	-,"-",-,-,"-","-",		Esses 6 campos estão relaciona conhecido como Proteção avanç Veredito do arquivo %X# Nome da ameaça %X# Pontuação de reputação %X#

			Ação de carregamento para análise	%X#
			Nome do arquivo	%X#5
			Arquivo SHA	%X#6
Varredura de arquivos	-,-,"-",		Estes 3 campos indicam o status	
			Veredito de verificação de arquivo morto	%X#8# Veredito da v ARCHIVESC ARCHIVESC

					ARCHIVESC
					ARCHIVESC
					ARCHIVESC

					ARCHIVESC
			Detalhe do veredito da varredura de arquivo morto	% Xo	Detalhe do ve um arquivo de bloqueado (A com base na configuraçõe Detalhes do v e o nome do a "Arquivo não que o arquivo bloqueado.
			Veredito do arquivo	% Xm	Veredito do a arquivos
Toque na Web	-,	%XU	Comportamento de Toque na We		
Categoria de URL do YouTube	->	%X#29#	A categoria de URL do YouTube campo mostra "nc" quando nenh		

Código de Resposta HTTP

Esta é a lista completa de Códigos de Resposta HTTP

Código de status	Significado
Informações 1xx	
100	Continuar
101	Protocolos de comutação
102	Processamento
103	Dicas iniciais
2xx Bem-sucedido	
200	OK
201	Criado
202	Aceito
203	Informações Não Autoritativas
204	Sem conteúdo
205	Redefinir conteúdo
206	Conteúdo parcial
207	Status múltiplo
208	Já Relatado
226	Mensagem Instantânea Usada
Redirecionamento 3xx	
300	Várias opções
301	Movido Permanentemente
302	Encontrado (Anteriormente "Movido Temporariamente")
303	Consulte Outro
304	Não Modificado
305	Usar proxy

306	Proxy do Switch
307	Redirecionamento Temporário para Autenticação (Geralmente visto na implantação transparente enquanto o SWA está autenticando o usuário)
308	Redirecionamento permanente
Erro do cliente 4xx	
400	Solicitação Incorreta
401	Autenticação do servidor Web necessária (normalmente vista na implantação transparente enquanto o SWA está autenticando o usuário)
402	Pagamento necessário
403	Proibido
404	Not found
405	Método Não Permitido
406	Não aceitável
407	Autenticação de Proxy Explícita Necessária
408	Tempo Limite da Solicitação
409	Conflito
410	Sumiu
411	Comprimento necessário
412	Falha na pré-condição
413	Carga Muito Grande
414	URI muito longo
415	Tipo de mídia sem suporte
416	Intervalo não satisfatório
417	Falha na expectativa
418	Eu sou um bule
421	Solicitação mal direcionada
422	Entidade Não Processável
423	Bloqueado
424	Dependência com Falha

425	Muito cedo
426	Atualização Necessária
428	Pré-condição Necessária
429	Muitas Solicitações
431	Campos do Cabeçalho da Solicitação Muito Grandes
451	Indisponível Por Motivos Legais
Erro de servidor 5xx	
500	Erro interno do servidor
501	Não implementado
502	Gateway incorreto
503	Serviço indisponível
504	Tempo limite do gateway
505	Versão HTTP Não Suportada
506	A Variante Também Negocia
507	Armazenamento Insuficiente
508	Loop detectado
510	Não Estendido
511	Autenticação de Rede Necessária

Marca de decisão da ACL

Esta é a lista completa das marcas de decisão da ACL:

Marca de decisão da ACL	Descrição
ALLOW_ADMIN_ERROR_PAGE	O Web Proxy permitiu a transação para uma página de notificação e para qualquer logotipo usado nessa página.
ALLOW_CUSTOMCAT	O Web Proxy permitiu a transação com base em configurações personalizadas de filtragem de categoria de URL para o grupo de Diretiva de Acesso.
ALLOW_REFERER	O Web Proxy permitiu a transação com base em uma isenção de conteúdo

	inserido/referenciado.
ALLOW_WBRS	O Web Proxy permitiu a transação com base nas configurações do filtro do Web Reputation para o grupo de Diretiva de Acesso.
AMP_FILE_VERDICT	Valor que representa um veredito do servidor de reputação da AMP para o arquivo:
	1 - Desconhecido
	2 - Limpar
	3 - Mal-intencionado
	4 - Não verificável
ARCHIVESCAN_ALLCLEAR	Veredito de verificação de arquivo morto
ARCHIVESCAN_BLOCKEDFILETYPE	ARCHIVESCAN_ALLCLEAR - Não há tipos de arquivos bloqueados no arquivo inspecionado.
ARCHIVESCAN_NESTEDTOODEEP	ARCHIVESCAN_BLOCKEDFILETYPE - Há um tipo de arquivo bloqueado no arquivo inspecionado. O próximo campo na entrada do log (Detalhe do veredito) fornece detalhes, especificamente o tipo de arquivo bloqueado e o nome do arquivo bloqueado.
ARCHIVESCAN_UNKNOWNFMT	ARCHIVESCAN_NESTEDTOODEEP - O arquivo está bloqueado porque contém mais arquivos "encapsulados" ou aninhados do que o máximo configurado. O campo Detalhes do veredito contém "Arquivo não verificável bloqueado".
ARCHIVESCAN_UNSCANABLE	ARCHIVESCAN_UNKNOWNFMT - O arquivo morto está bloqueado porque contém um tipo de arquivo de formato desconhecido. Os detalhes do veredito são "Arquivo não digitalizável bloqueado".
ARCHIVESCAN_FILETOOBIG	ARCHIVESCAN_UNSCANABLE - O arquivo morto está bloqueado porque contém um arquivo que não pode ser examinado. Os detalhes do veredito são "Arquivo não digitalizável bloqueado".

	ARCHIVESCAN_FILETOOBIG - O arquivo está bloqueado porque o tamanho do arquivo é maior que o máximo configurado. Os detalhes do veredito são "Arquivo não digitalizável bloqueado".
	Detalhe do veredito da varredura de arquivo morto
	O campo e o campo Veredito na entrada do log fornecem informações adicionais sobre o Veredito, como o tipo de arquivo bloqueado e o nome do arquivo bloqueado, "Não-digitalizável - Arquivo bloqueado" ou "-" para indicar que o arquivo não contém nenhum tipo de arquivo bloqueado.
	Por exemplo, se um arquivo de Arquivo Inspecionável for bloqueado (ARCHIVESCAN_BLOCKEDFILETYPE) com base na Política de Acesso: Configurações de bloqueio de objetos personalizados, a entrada Detalhes do veredito inclui o tipo de arquivo bloqueado e o nome do arquivo bloqueado.
	Consulte Políticas de Acesso: Bloqueando Objetos e Definições de Inspeção de Arquivo para obter mais informações sobre a Inspeção de Arquivo.
BLOCK_ADMIN	Transação bloqueada com base em algumas configurações padrão do grupo de Diretiva de Acesso.
BLOCK_ADMIN_CONNECT	Transação bloqueada com base na porta TCP de destino, conforme definido na configuração HTTP CONNECT Ports para o grupo Access Policy.
BLOCK_ADMIN_CUSTOM_USER_AGENT	Transação bloqueada com base no agente de usuário definido na configuração Bloquear agentes de usuário personalizados para o grupo de política de acesso.
BLOCK_ADMIN_TUNNELING	O Web Proxy bloqueou a transação com base no túnel do tráfego não HTTP nas portas HTTP do Grupo de Políticas

	de Acesso.
BLOCK_ADMIN_HTTPS_NonLocalDestination	Operação bloqueada; o cliente tentou ignorar a autenticação usando a porta SSL como um proxy explícito. Para evitar isso, se uma conexão SSL for estabelecida com o próprio WSA, somente as solicitações para o nome de host de redirecionamento WSA real serão permitidas.
BLOCK_ADMIN_IDS	Transação bloqueada com base no tipo MIME do conteúdo do corpo da solicitação, conforme definido no grupo de Política de Segurança de Dados.
BLOCK_ADMIN_FILE_TYPE	Transação bloqueada com base no tipo de arquivo conforme definido no grupo Política de acesso.
BLOCK_ADMIN_PROTOCOL	Transação bloqueada com base no protocolo conforme definido na configuração Bloquear protocolos do grupo de política de acesso.
BLOCK_ADMIN_SIZE	Transação bloqueada com base no tamanho da resposta, conforme definido nas configurações de Tamanho do Objeto para o grupo de Diretiva de Acesso.
BLOCK_ADMIN_SIZE_IDS	Transação bloqueada com base no tamanho do conteúdo do corpo da solicitação, conforme definido no grupo de Política de Segurança de Dados.
BLOCK_AMP_RESP	O Web Proxy bloqueou a resposta com base nas configurações de Proteção avançada contra malware para o grupo de Política de acesso.
BLOCK_AMW_REQ	O Web Proxy bloqueou a solicitação com base nas configurações do Anti-Malware para o grupo de Política de verificação de malware de saída. O corpo da solicitação produziu um veredito de Malware positivo.
BLOCK_AMW_RESP	O Web Proxy bloqueou a resposta com base nas configurações de antimalware do grupo de política de acesso.
BLOCK_AMW_REQ_URL	O Web Proxy suspeita que a URL na solicitação HTTP não pode ser segura, portanto, ele bloqueou a transação no momento da solicitação com base nas

	configurações Anti-Malware do grupo de Política de Acesso.
BLOCK_AVC	Transação bloqueada com base nas configurações de Aplicativo definidas para o grupo de Política de Acesso.
BLOCK_CONTENT_UNSAFE	Transação bloqueada com base nas configurações de classificação de conteúdo do site para o grupo de Política de Acesso. A solicitação do cliente era para conteúdo adulto e a política está configurada para bloquear esse tipo de conteúdo.
BLOCK_CONTINUE_CONTENT_UNSAFE	A transação foi bloqueada e exibiu a página Avisar e continuar com base nas configurações de classificação de conteúdo do site no grupo Política de acesso. A solicitação do cliente era para conteúdo para adultos e a política está configurada para fornecer um aviso aos usuários que acessam conteúdo para adultos.
BLOCK_CONTINUE_CUSTOMCAT	A transação foi bloqueada e exibiu a página Avisar e continuar com base em uma categoria de URL personalizada no grupo de política de acesso configurado para "Avisar".
BLOCK_CONTINUE_WEBCAT	A transação bloqueou e exibiu a página Avisar e continuar com base em uma categoria de URL predefinida no grupo de política de acesso configurado para "Avisar".
BLOCK_CUSTOMCAT	Transação bloqueada com base em configurações personalizadas de filtragem de categoria de URL para o grupo de Diretiva de Acesso.
BLOCK_ICAP	O Web Proxy bloqueou a solicitação com base no veredito do sistema DLP externo, conforme definido no grupo de Política DLP Externo.
BLOCK_SEARCH_UNSAFE	A solicitação do cliente incluiu uma consulta de pesquisa não segura e a Política de Acesso está configurada para impor pesquisas seguras, portanto, a solicitação original do cliente foi bloqueada.
BLOCK_SUSPECT_USER_AGENT	Transação bloqueada com base na

	configuração Agente de Usuário Suspeito para o grupo de Política de Acesso.
BLOCK_UNSUPPORTED_SEARCH_APP	Transação bloqueada com base nas configurações de pesquisa segura do grupo de Política de Acesso. A transação era para um mecanismo de pesquisa sem suporte, e a política está configurada para bloquear mecanismos de pesquisa sem suporte.
BLOCK_WBRS	Transação bloqueada com base nas configurações do filtro do Web Reputation para o grupo de Diretiva de Acesso.
BLOCK_WBRS_IDS	O Web Proxy bloqueou a solicitação de carregamento com base nas configurações do filtro do Web Reputation para o grupo de Diretiva de Segurança de Dados.
BLOCK_WEBCAT	Transação bloqueada com base nas configurações de filtragem de categoria de URL para o grupo de Diretiva de Acesso.
BLOCK_WEBCAT_IDS	O Web Proxy bloqueou a solicitação de carregamento com base nas configurações de filtragem de categoria de URL para o grupo de Diretiva de Segurança de Dados.
BLOCK_YTCAT	O Web Proxy bloqueou a transação com base nas configurações de filtragem de categoria predefinidas do YouTube para o grupo de Diretiva de Acesso.
BLOCK_CONTINUE_YTCAT	O Web Proxy bloqueou a transação e exibiu a página Avisar e continuar com base em uma categoria predefinida do YouTube no grupo de Política de acesso configurado para 'Avisar'.
DECRYPT_ADMIN	O Web Proxy descriptografou a transação com base em algumas configurações padrão do grupo de Diretiva de Descriptografia.
DECRYPT_ADMIN_EXPIRED_CERT	O Web Proxy descriptografou a transação, embora o certificado do servidor tenha expirado.
DECRYPT_EUN_ADMIN_DEFAULT_ACTION	O Web Proxy descriptografou a

	transação com base nas configurações padrão como conexão de remoção para o grupo de políticas de descriptografia quando EUN está habilitado.
DECRYPT_EUN_ADMIN_EXPIRED_CERT	O Web Proxy descriptografou a transação quando as configurações de proxy HTTPS descartam um certificado expirado com EUN habilitado.
DECRYPT_EUN_ADMIN_INVALID_LEAF_CERT	O Web Proxy descriptografou a transação quando as configurações de proxy HTTPS descartam um certificado folha inválido com EUN habilitado.
DECRYPT_EUN_ADMIN_MISMATCHED_HOSTNAME	O Web Proxy descriptografou a transação quando as configurações de proxy HTTPS descartam o nome de host incompatível com EUN habilitado.
DECRYPT_EUN_ADMIN_OCSP_OTHER_ERROR	O Web Proxy descriptografou a transação quando as configurações de proxy HTTPS descartam um OCSP com outros erros com EUN habilitado.
DECRYPT_EUN_ADMIN_OCSP_REVOKED_CERT	O Web Proxy descriptografou a transação quando as configurações de proxy HTTPS descartam um certificado revogado OCSP com EUN habilitado.
DECRYPT_EUN_ADMIN_UNRECOGNIZED_ROOT_CERT	O Web Proxy descriptografou a transação quando as configurações de proxy HTTPS removem uma autoridade raiz não reconhecida ou um certificado do emissor com EUN habilitado.
DECRYPT_EUN_CUSTOMCAT	O Web Proxy descriptografou a transação com base nas configurações personalizadas de filtragem de categoria de URL para o grupo de políticas de descriptografia. Se EUN estiver habilitado, o tráfego será descartado.
DECRYPT_EUN_WBRS	O Web Proxy descriptografou a transação com base nas configurações do filtro de reputação da Web para o grupo de políticas de descriptografia. Se EUN estiver habilitado, o tráfego será descartado.
DECRYPT_EUN_WBRS_NO_SCORE	O Web Proxy descriptografou a transação com base nas configurações do filtro de reputação da Web para URL sem pontuação no grupo de políticas de

	descriptografia. Se EUN estiver habilitado, o tráfego será descartado.
DECRYPT_EUN_WEBCAT	O Web Proxy descriptografou a transação com base nas configurações de filtragem de categoria de URL para o grupo de políticas de descriptografia. Se EUN estiver habilitado, o tráfego será descartado.
DESCRIPTOGRAFAR_WEBCAT	O Web Proxy descriptografou a transação com base nas configurações de filtragem de categoria de URL para o grupo de Diretiva de Descriptografia.
DESCRIPTOGRAFAR_WBRS	O Web Proxy descriptografou a transação com base nas configurações do filtro do Web Reputation para o grupo de Diretiva de Descriptografia.
DEFAULT_CASE	O Web Proxy permitiu que o cliente acessasse o servidor porque nenhum dos serviços AsyncOS, como Web Reputation ou verificação Anti-Malware, executou qualquer ação na transação.
DENY_ADMIN	O Web Proxy negou a transação. Isso ocorre para solicitações HTTPS quando a autenticação é necessária e Decrypt for Authentication está desabilitado nas configurações de proxy HTTPS.
DROP_ADMIN	O Web Proxy descartou a transação com base em algumas configurações padrão do grupo de Diretiva de Descriptografia.
DROP_ADMIN_EXPIRED_CERT	O Web Proxy descartou a transação porque o certificado do servidor expirou.
DROP_WEBCAT	O Web Proxy descartou a transação com base nas configurações de filtragem de categoria de URL para o grupo de Diretiva de Descriptografia.
DROP_WBRS	O Web Proxy descartou a transação com base nas configurações do filtro do Web Reputation para o grupo de Diretiva de Descriptografia.
MONITOR_ADMIN_EXPIRED_CERT	O Web Proxy monitorou a resposta do servidor porque o certificado do servidor expirou.
MONITOR_AMP_RESP	O Web Proxy monitorou a resposta do servidor com base nas configurações de Proteção avançada contra malware

	para o grupo de Política de acesso.
MONITOR_AMW_RESP	O Web Proxy monitorou a resposta do servidor com base nas configurações antimalware do grupo de política de acesso.
MONITOR_AMW_RESP_URL	O Web Proxy suspeita que a URL na solicitação HTTP não pode ser segura, mas monitorou a transação com base nas configurações Anti-Malware do grupo de Política de Acesso.
MONITOR_AVC	O Web Proxy monitorou a transação com base nas configurações do Aplicativo para o grupo de Diretiva de Acesso.
MONITOR_CONTINUE_CONTENT_UNSAFE	Originalmente, o Web Proxy bloqueou a transação e exibiu a página Avisar e continuar com base nas configurações de classificação de conteúdo do site no grupo Política de acesso. A solicitação do cliente era para conteúdo para adultos e a política está configurada para fornecer um aviso aos usuários que acessam conteúdo para adultos. O usuário aceitou o aviso e continuou até o site originalmente solicitado, e nenhum outro mecanismo de varredura bloqueou subsequentemente a solicitação.
MONITOR_CONTINUE_CUSTOMCAT	Originalmente, o Web Proxy bloqueou a transação e exibiu a página Avisar e continuar com base em uma categoria de URL personalizada no grupo de política de acesso configurado para "Avisar". O usuário aceitou o aviso e continuou até o site originalmente solicitado, e nenhum outro mecanismo de varredura bloqueou subsequentemente a solicitação.
MONITOR_CONTINUE_WEBCAT	Originalmente, o Web Proxy bloqueou a transação e exibiu a página Avisar e continuar com base em uma categoria de URL predefinida no grupo de política de acesso configurado para "Avisar". O usuário aceitou o aviso e continuou até o site originalmente solicitado, e nenhum outro mecanismo de varredura

	bloqueou subsequentemente a solicitação.
MONITOR_CONTINUE_YTCAT	Originalmente, o Web Proxy bloqueou a transação e exibiu a página Avisar e continuar com base em uma categoria predefinida do YouTube no grupo de Política de acesso configurado para 'Avisar'. O usuário aceitou o aviso e continuou até o site originalmente solicitado, e nenhum outro mecanismo de varredura bloqueou subsequentemente a solicitação.
MONITOR_IDS	O Web Proxy verificou a solicitação de carregamento usando uma Política de Segurança de Dados ou uma Política de DLP Externo, mas não bloqueou a solicitação. Ele avaliou a solicitação em relação às Políticas de acesso.
MONITOR_SUSPECT_USER_AGENT	O Web Proxy monitorou a transação com base na configuração do Agente de Usuário Suspeito para o grupo de Política de Acesso.
MONITOR_WBRS	O Web Proxy monitorou a transação com base nas configurações do filtro do Web Reputation para o grupo de Diretiva de Acesso.
NO_AUTHORIZATION	O Web Proxy não permitiu que o usuário acessasse o aplicativo porque o usuário já estava autenticado em um território de autenticação, mas não em nenhum território de autenticação configurado na Política de Autenticação de Aplicativo.
NO_PASSWORD	Falha na autenticação do usuário.
PASSTHRU_ADMIN	O Web Proxy passou pela transação com base em algumas configurações padrão do grupo de Diretiva de Descriptografia.
PASSTHRU_ADMIN_EXPIRED_CERT	O Web Proxy passou pela transação, embora o certificado do servidor tenha expirado.
PASSTHRU_WEBCAT	O Web Proxy passou pela transação com base nas configurações de filtragem de categoria de URL para o grupo de Política de Descriptografia.

PASSTHRU_WBRS	O Web Proxy passou pela transação com base nas configurações do filtro do Web Reputation para o grupo de Diretiva de Descriptografia.
REDIRECT_CUSTOMCAT	O Web Proxy redirecionou a transação para uma URL diferente com base em uma categoria de URL personalizada no grupo de Política de Acesso configurado para "Redirecionar".
SAAS_AUTH	O Web Proxy permitiu que o usuário acessasse o aplicativo porque o usuário foi autenticado de forma transparente no território de autenticação configurado na Política de Autenticação de Aplicativo.
OUTROS	O Web Proxy não concluiu a solicitação devido a um erro, como uma falha de autorização, uma desconexão do servidor ou uma anulação do cliente.

Valores do veredito da verificação de malware

Um veredito de verificação de malware é um valor atribuído a uma solicitação de URL ou resposta do servidor que determina a probabilidade de que ele contenha malware. Os mecanismos de varredura Webroot, McAfee e Sophos retornam o veredito de varredura de malware ao mecanismo DVS para que o mecanismo DVS possa determinar se o objeto examinado deve ser monitorado ou bloqueado. Cada veredito de verificação de malware corresponde a uma categoria de malware listada na página Políticas de acesso > Reputação e Configurações antimalware quando você edita as configurações de antimalware de uma Política de acesso específica.

Esta lista apresenta os diferentes valores de veredito de verificação de malware e cada categoria de malware correspondente:

Valor do veredito da verificação de malware	Categoria de malware
-	não definido
0	Desconhecido
1	Não verificado

Valor do veredito da verificação de malware	Categoria de malware
2	Timeout
3	Erro
4	Não verificável
10	Spyware genérico
12	Objeto Auxiliar de Navegador
13	Adware
14	Monitor do sistema
18	Monitor de sistema comercial
19	Discador
20	Sequestrador
21	URL de phishing
22	Trojan Downloader
23	Cavalo de Troia
24	Phisher de Cavalo de Troia
25	Worm
26	Arquivo criptografado

Valor do veredito da verificação de malware	Categoria de malware
27	Vírus
33	Outro malware
34	PUA
35	Anulado
36	Heurística de Epidemia
37	Arquivos mal-intencionados conhecidos e de alto risco

Informações Relacionadas

- Manual do usuário do AsyncOS 15.2 para Cisco Secure Web Appliance
- Use as práticas recomendadas de dispositivos da Web seguros
- Garanta a funcionalidade adequada do grupo HA do Virtual WSA em um ambiente VMware
- Configurar Parâmetro de Desempenho em Logs de Acesso
- Entender o formato do registro de acesso HTTPS no Secure Web Appliance
- Acessar logs do dispositivo da Web seguro

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.