Bloquear download de arquivo executável em SWA

Contents

Introdução

Este documento descreve o processo de configuração do Secure Web Appliance (SWA) para bloquear o download de arquivos executáveis.

Pré-requisitos

Requisitos

A Cisco recomenda o conhecimento destes tópicos:

- Acesso à interface gráfica do usuário (GUI) do SWA
- Acesso administrativo ao 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.

Antes de Começar

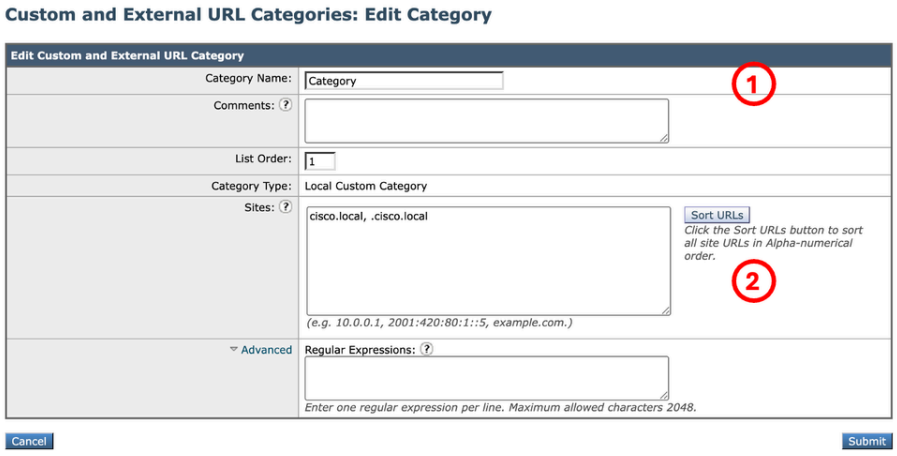
O Cisco SWA pode efetivamente bloquear o download de arquivos executáveis inspecionando o tipo MIME (Multipurpose Internet Mail Extensions) do conteúdo da Web. Ao identificar tipos de arquivos, como application/x-msdownload, application/x-msi e outros tipos MIME relacionados, o

SWA aplica políticas que impedem que o executável seja entregue aos usuários. Além da detecção de tipo MIME, o SWA pode aproveitar a filtragem de extensão de arquivo, a análise baseada em reputação e as regras de política personalizadas para fortalecer ainda mais a proteção contra downloads indesejados ou arriscados. Esses recursos ajudam as empresas a manter um ambiente de navegação seguro e reduzir o risco de infecções por malware.

Tip: O SWA não pode identificar o tipo MIME do arquivo, a menos que o tráfego seja descriptografado.

application/octet-stream é um tipo MIME genérico usado para indicar que um arquivo contém dados binários. Ele não especifica a natureza do arquivo, portanto, pode ser usado para qualquer arquivo que não se ajuste a um tipo MIME mais específico. Esse tipo é geralmente atribuído a arquivos executáveis, instaladores e outros arquivos não texto quando o servidor Web não pode determinar um tipo mais preciso.

Configuration Steps

Etapa 1.Crie uma categoria de URL personalizada para o site.	Etapa 1.1.Na GUI, navegue até Web Security Manager e escolhaCustom and External URL Categories. Etapa 1.2.Clique em Adicionar categoria para criar uma nova Categoria de URL personalizada. Etapa 1.3.Digite o nome da nova categoria. Etapa 1.4.Defina o domínio e/ou subdomínios do site que você está tentando bloquear o tráfego de upload (Neste exemplo, cisco.local e todos os seus subdomínios). Etapa 1.5.Envie as alterações.  Imagem - Criar categoria de URL personalizada

	Tip: Para obter mais informações sobre como configurar categorias de URL personalizadas, acesse: https://www.cisco.com/c/en/us/support/docs/security/secure-web-appliance-virtual/220557-configure-cu...
Etapa 2.Descriptografar o tráfego do URL	Caution: A descriptografia de um grande número de URLs pode prejudicar o desempenho. Etapa 2.1. Na GUI, navegue até Web Security Manager e escolhaPolíticas de descriptografia Etapa 2.2.Clique em Add Policy. Etapa 2.3.EnterName para a nova política. Etapa 2.4.(Opcional) Selecione oPerfil de identificação ao qual essa política se aplica. Tip: (Opcional) Se quiser aplicar a diretiva a todos os usuários, mesmo que eles não estejam autenticados, escolha Todos os usuários (usuários autenticados e não autenticados). Etapa 2.5.Na seção Definição de membro de política, clique nos links URL Categoriespara adicionar a Categoria de URL personalizada. Etapa 2.6.Selecione a Categoria de URL que foi criada na Etapa 1. Etapa 2.7.Clique em Submit.

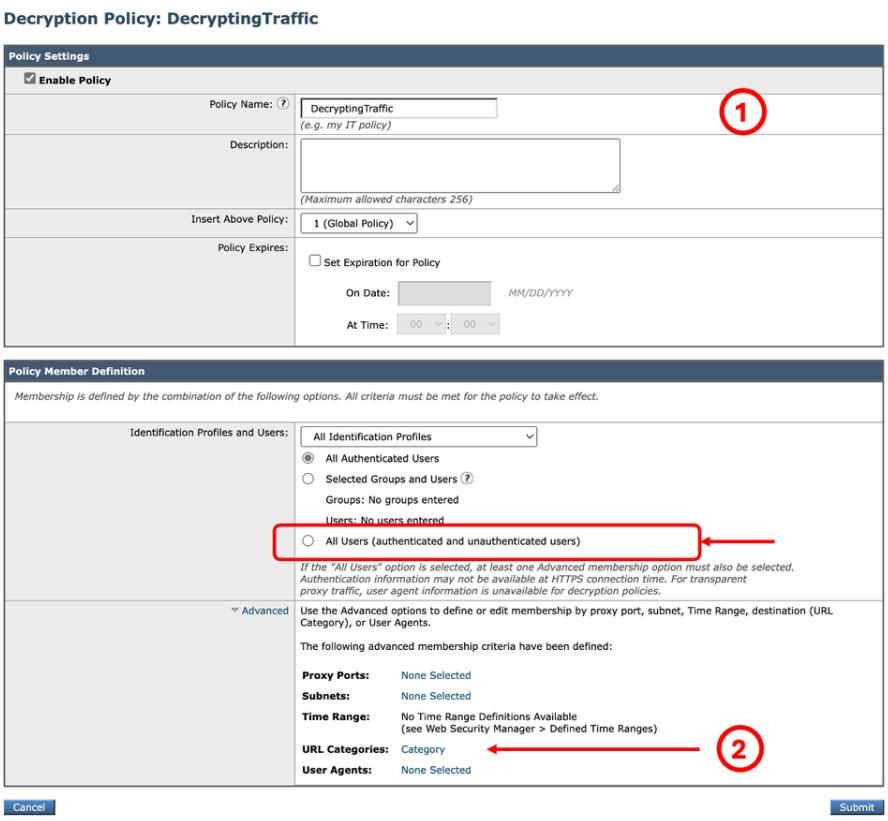


Imagem - Criar uma política de descriptografia

Etapa 2.8.Na página Políticas de descriptografia, clique no link daFiltragem de URL para obter a nova política.

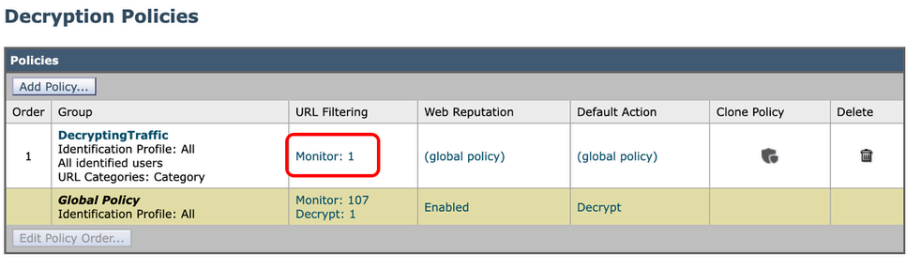


Imagem - Selecione a filtragem de URL

Etapa 2.9.Escolha Descriptografar como a ação para Categoria de URL Personalizada.

Etapa 2.10.Clique em Enviar.

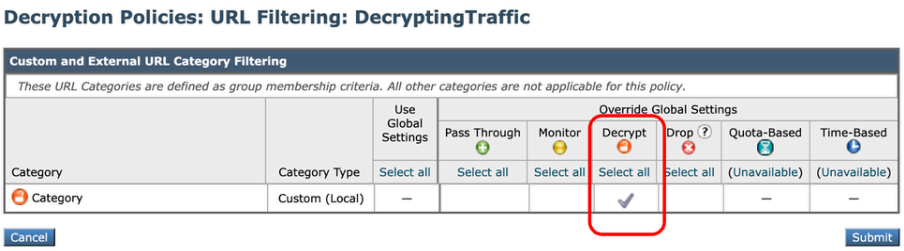


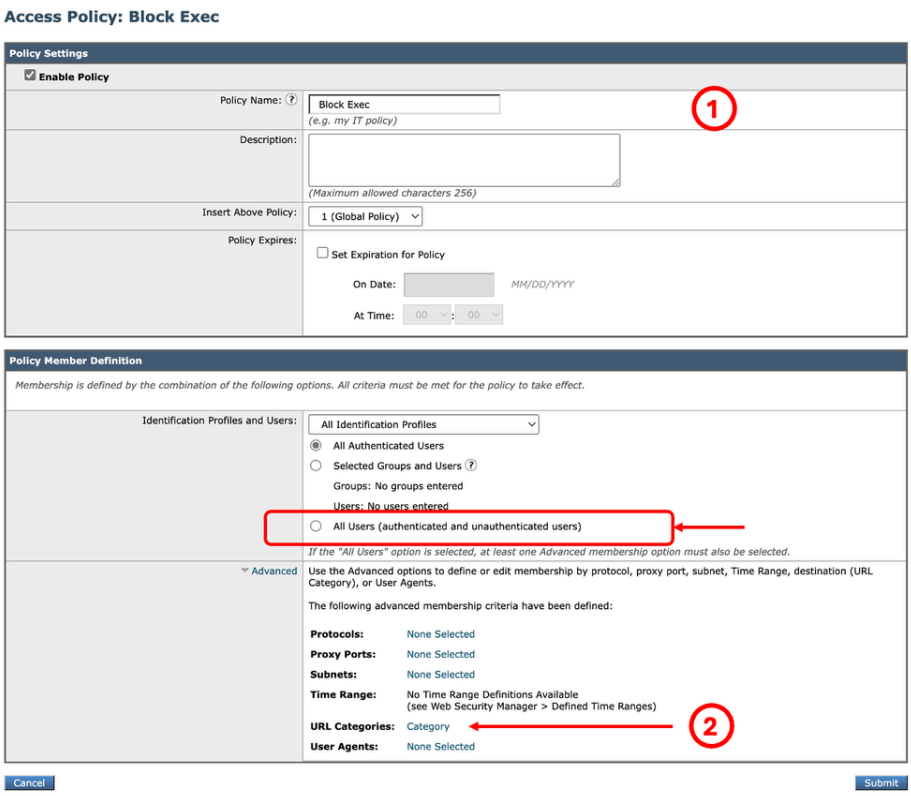
	Imagem - Definir descriptografia como ação
Etapa 3.Bloquear os arquivos executáveis	Etapa 3.1.Na GUI, navegue até Web Security Manager e escolhaAccess Policies. Etapa 3.2.Clique em Add Policy. Etapa 3.3.EnterName para a nova política. Etapa 3.4.(Opcional) Selecione oPerfil de identificação ao qual você precisa que essa política se aplique. Tip: (Opcional) Se quiser aplicar a diretiva a todos os usuários, mesmo que eles não estejam autenticados, escolha Todos os usuários (usuários autenticados e não autenticados). Etapa 3.5.Na seção Definição de membro de política, clique nos links Categorias de URL para adicionar a Categoria de URL personalizada. Etapa 3.6.Selecione a Categoria de URL que foi criada na Etapa 1. Etapa 3.7.Clique em Enviar. 

Imagem - Política de acesso

Tip: Para fins de geração de relatórios, é melhor escolher um nome que não seja igual a nenhuma outra política de acesso/descriptografia.

Etapa 3.8.Na página Políticas do InAccess, verifique se a ação de filtragem de URL está definida como Monitorar.

Etapa 3.9. Na página Políticas do InAccess, clique no link de Objetos para a nova política.

Imagem - Selecionar os Objetos

Imagem - Selecione a filtragem de URL

Etapa 3.10. No menu suspenso, escolha Definir configurações de bloqueio de objetos personalizados.

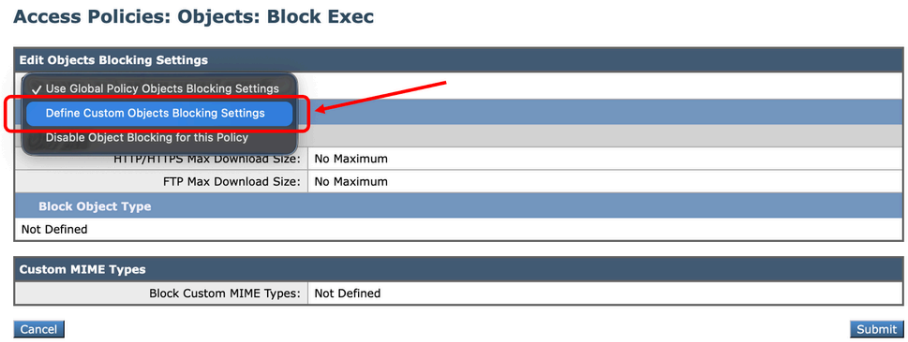


Imagem - Definir objetos personalizados

Etapa 3.11.Clique em Código Executável para selecionar os tipos de Objetos que deseja bloquear.

Etapa 3.12.Clique em Installers para selecionar os tipos de Objetos que deseja bloquear.

Etapa 3.13. Além disso, você pode inserir os tipos MIME dos

arquivos que deseja bloquear na seção Tipos MIME Personalizados.

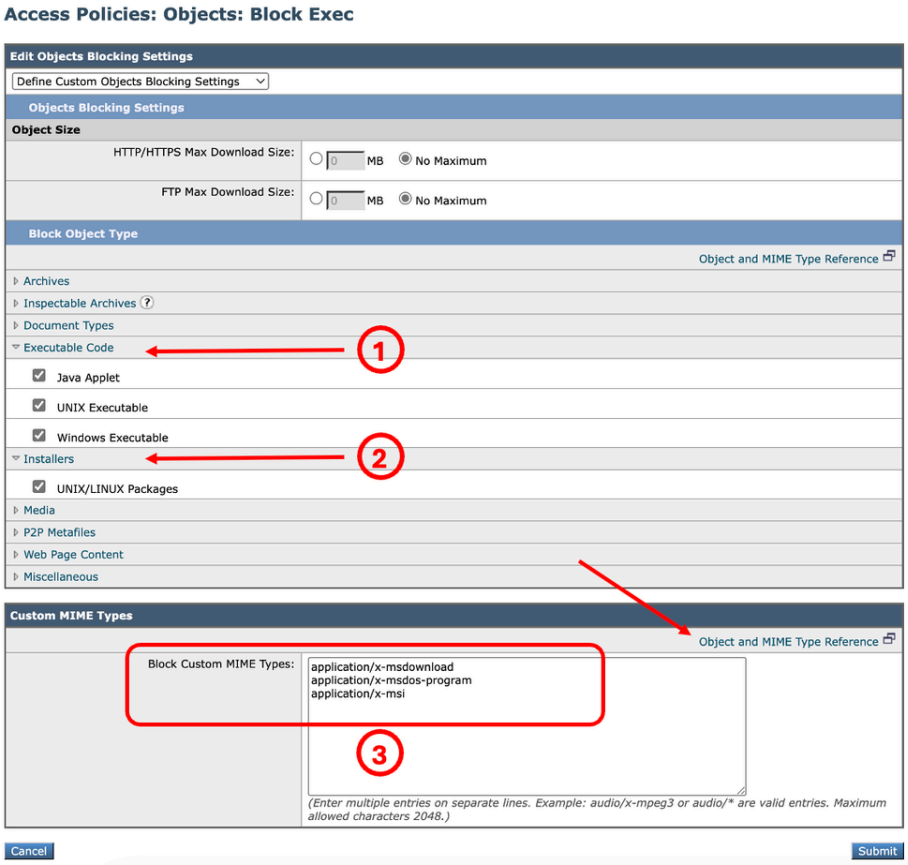


Imagem - Configurando Objetos a Serem Bloqueados

Tip: Para exibir a lista de tipos de MIME, clique em Referência de Tipo de Objeto e MIME.

Etapa 3.14.Enviar.

Etapa 3.15.Confirmar alterações.

Validação do bloqueio de extensão de arquivo

Neste exemplo, quando um usuário tenta fazer download de um arquivo executável, esta página de aviso é exibida:

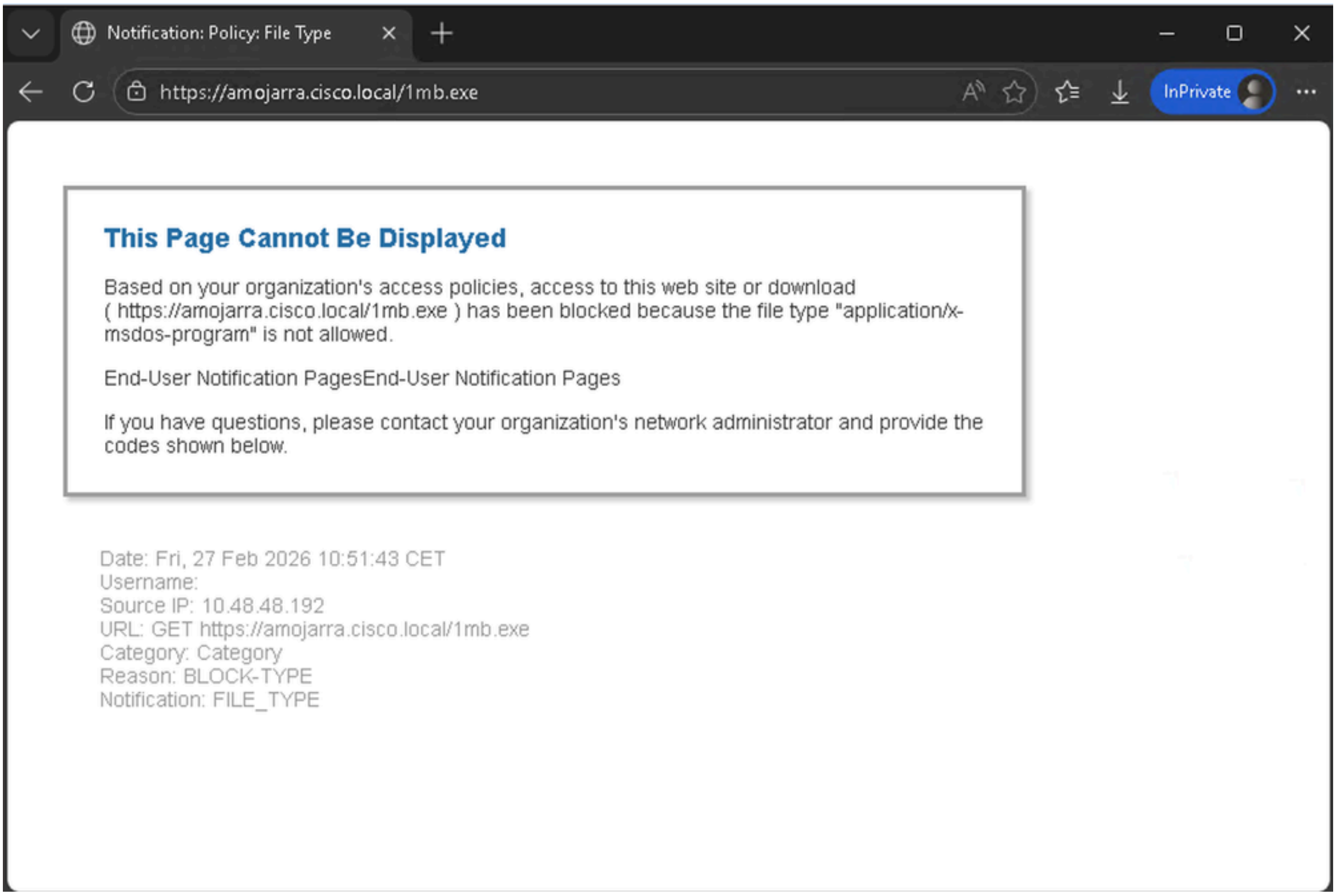


Imagem - Página de Notificação de Bloqueio

Tip: Para configurar a página EUN (Notificação de usuário final), na GUI, navegue para Serviços de segurança, clique em Notificação de usuário final e modifique a seção Páginas de notificação de usuário final.

Nos logs de acesso, você pode ver duas linhas de log relacionadas ao tráfego.

A primeira linha de log está relacionada à política de descriptografia (Nome: DecryptingTraffic) que está descriptografando o tráfego. A ação é DECRYPT_CUSTOMCAT

A segunda linha do Log de acesso está relacionada à Política de acesso (Nome: Block_Exec) que criamos na Etapa 2.3. A ação é BLOCK_ADMIN_FILE_TYPE

Política	Log de acesso
Política de descriptografia	1772186569.823 182 10.48.48.192 TCP_MISS_SSL/200 39 CONNECT tunnel://amojarra.cisco.local:443/ - DIRECT/amojarra.cisco.local - DECRYPT_CUSTOMCAT_7-DecryptingTraffic-DefaultGroup-NONE-NONE-NONE-LAB_Access-NONE <"C_Cate",-,-,-,"-,-,-,-,-,"-,-,-,-,"-,-,-,"-","-",-,-,-,"-,-,"-,"-,"-,"-","-,"-","-","-","-","-,"-,"-,"-,"-",-,-,-,-,-,-,"-,"-,-,-,-,-,-,-,-",-,-,-,-,-> -

Política de acesso	1772186576.735 2242 10.48.48.192 TCP_DENIED_SSL/403 0 GET https://amojarra.cisco.local:443/1mb.exe - DIRECT/amojarra.cisco.local application/x-msdos-program BLOCK_ADMIN_FILE_TYPE_12-Block_Exec-DefaultGroup-NONE-NONE-NONE-LAB_Access-NONE <"C_Cate",ns,0,"-",0,0,0,-,"-,-,-,-,"-,-,-,"-,"-,"-,-,-,"nc",-,"-,"-,"-","-","Desconhecido","Desconhecido","-","-",0.00,0,-,"Desconhecido","-,-,"-,-,-,-,-,"-,"-,"-",-,-,-,-,-,-"-",-,-,-,-

Informações Relacionadas

- Manual do usuário do AsyncOS 15.2 para Cisco Secure Web Appliance
- Guia de instalação do Cisco Secure Email and Web Virtual Appliance
- Configurar categorias de URL personalizadas no Secure Web Appliance - Cisco
- Use as práticas recomendadas de dispositivos da Web seguros
- Configurar firewall para dispositivo seguro da Web
- Configurar certificado de descriptografia no aplicativo da Web seguro
- Configurar e solucionar problemas de SNMP em SWA
- Configurar logs de envio de SCP no Secure Web Appliance com o Microsoft Server
- Habilitar canal/vídeo específico do YouTube e bloquear o restante do YouTube no SWA
- Entender o formato do registro de acesso HTTPS no Secure Web Appliance
- Acessar logs do dispositivo da Web seguro
- Ignorar autenticação no Secure Web Appliance
- Bloquear o tráfego no Secure Web Appliance
- Ignorar o tráfego de atualizações da Microsoft no Secure Web Appliance

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.