Configurações seguras de implementação e uso

Proteja todo o acesso físico, local e remoto aos servidores que hospedam o Archer. Restrinja todos os métodos de acesso ao mínimo absoluto necessário para manter o Archer.

Não configure ambientes de teste do Archer para conter cópias exatas de dados do ambiente de produção completo ou para usar o mesmo sistema ou informações de autenticação. Se o ambiente de teste contiver quaisquer informações confidenciais do ambiente de produção, tome as mesmas precauções do ambiente de produção para proteger o ambiente de teste.

Nesta página

- Lista de IPs confiáveis

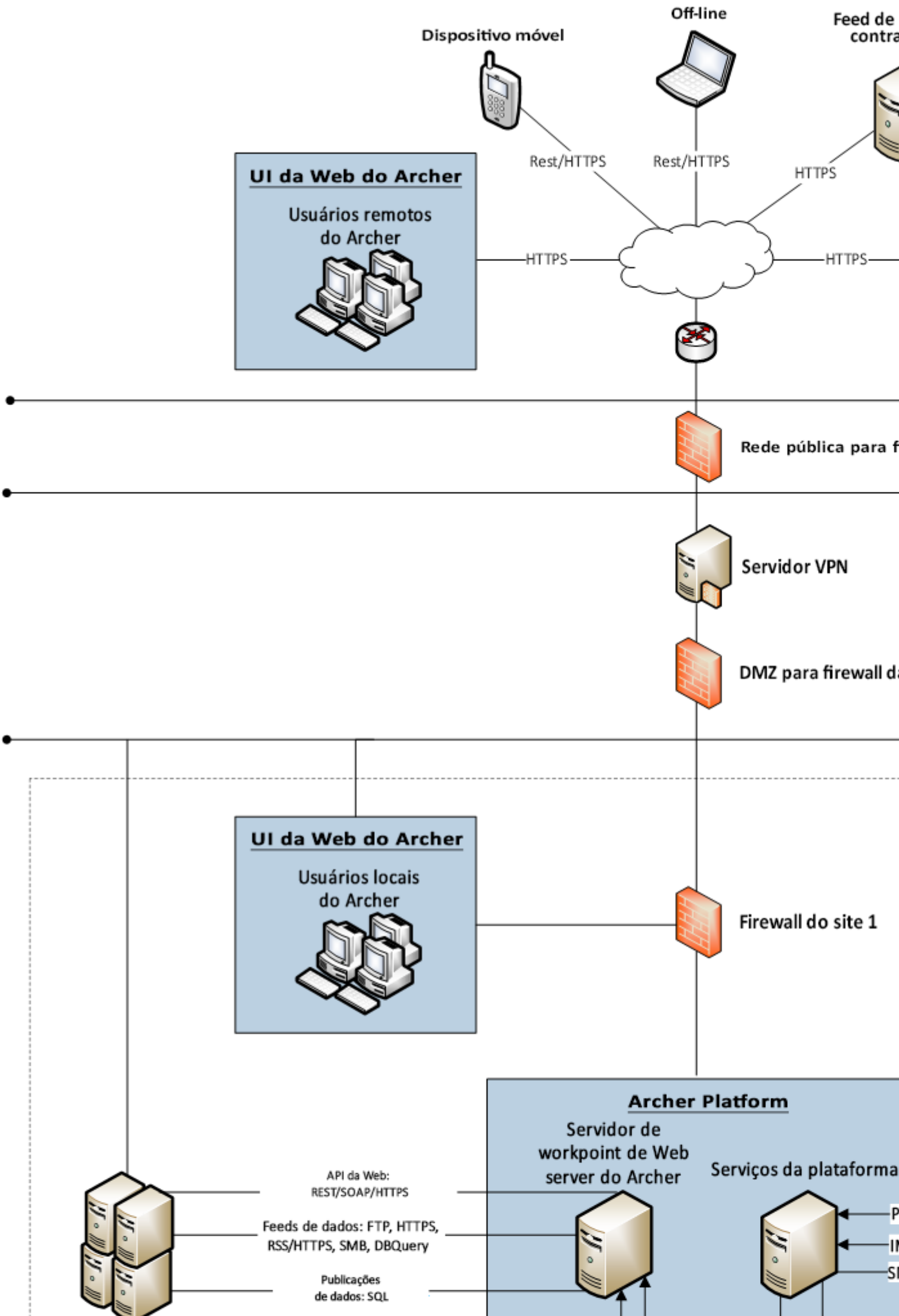
Mapa de Controles de Segurança

Uma implementação do Archer consiste em 3 camadas físicas: uma camada da Web, uma camada de serviços e uma camada de banco de dados. Uma organização pode implementar o Archer em uma configuração de host único ou de vários hosts.

Ao implementar o Archer em uma rede corporativa, faça o seguinte: Implemente os hosts do Archer dentro da rede corporativa. O firewall DMZ para rede corporativa intercepta toda a comunicação entre o host único e os outros componentes na rede. Garanta que os usuários estejam acessando Archer de dentro da rede corporativa. Se os usuários precisarem acessar Archer pela Internet, é recomendável que eles se conectem à rede corporativa por meio de uma conexão VPN segura. Permita apenas acesso remoto a Archer hosts para manutenção segura usando o Protocolo de Área de Trabalho Remota (RDP) por meio de uma conexão VPN segura. Configure regras de firewall para garantir uma comunicação segura entre Archer e outros componentes na rede.

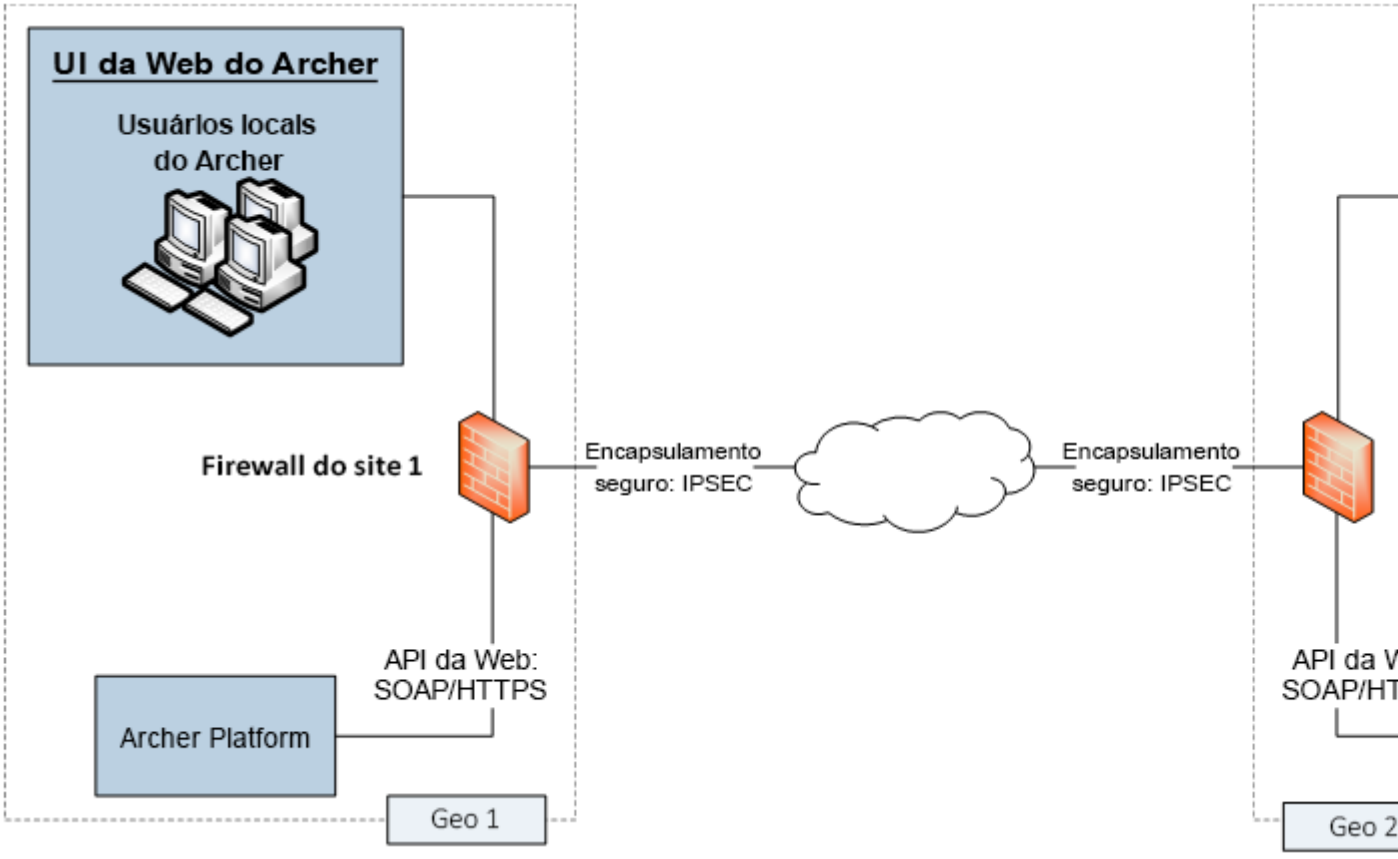
Importante: Implemente os serviços do Archer em um local seguro, cujo acesso físico aos servidores é restrito apenas à equipe que gerencia os servidores.

A figura a seguir mostra um exemplo de uma configuração de vários hosts.


Off-line
Dispositivo móvel
Feed de
contra
Rest/HTTPS
Rest/HTTPS
HTTPS
UI da Web do Archer
Usuários remotos
do Archer
HTTPS
HTTPS
Rede pública para f
Servidor VPN
DMZ para firewall d
UI da Web do Archer
Usuários locais
do Archer
Firewall do site 1
Archer Platform
Servidor de
workpoint de Web
server do Archer
Serviços da plataforma
API da Web:
REST/SOAP/HTTPS
Feeds de dados: FTP, HTTPS,
RSS/HTTPS, SMB, DBQuery
Publicações
de dados: SQL

Para configurações de vários hosts, faça o seguinte: Implante Archer servidores web, de serviços e de banco de dados na rede corporativa. Implante servidores de feed de dados na rede corporativa, exceto aqueles que fornecem informações usando HTTPS, como serviços RSS e Threat Intelligence. Implante um Web Application Firewall entre a DMZ e a rede pública. Garanta que todos Archer os servidores em um site estejam conectados à mesma sub-rede. Implante firewalls em cada site para garantir a transferência segura de dados de uma instância de Archer em um site para outra instância de Archer localizada em um site diferente. Configure regras de firewall para interceptar toda a comunicação entre Archer componentes na rede, conforme mostrado na figura anterior. Para obter mais informações, consulte Regras de Firewall.

Embora a figura anterior mostre vários tipos de feeds de dados, a figura a seguir expande o tipo de feed de dados Archer-to-Archer usando o exemplo de 1 local geográfico para outro.



Ao implementar o Archer em vários locais geograficamente dispersos e configurar uma instância do Archer em 1 local a fim de alimentar dados para outra instância do Archer em outro local, faça o seguinte: Configure regras de firewall para interceptar toda a comunicação entre os Archer componentes na rede e entre diferentes sites, conforme ilustrado pelos firewalls na figura anterior. Implemente a transferência de dados entre sites usando um túnel seguro, conforme mostrado na figura anterior.

Regras de firewall

Use firewalls para restringir o tráfego de rede entre o Archer e sistemas externos.

Todas as recomendações de firewall são baseadas nos seguintes pressupostos: Você tem um firewall com monitoramento, indicando que apenas o estabelecimento de portas TCP é considerado. Você especifica a direção da comunicação para as portas UDP porque as conexões não têm sessões. O firewall processa as regras de cima para baixo, terminando com a remoção genérica de todos os pacotes. Você implementará o Archer como mostrado em uma das figuras do Mapa de controles de segurança.

DMZ para rede corporativa

Configurar a comunicação confiável do servidor VPN na DMZ (DeMilitarized Zone, rede de perímetro) para as máquinas client em que a interface de usuário da Web do Archer é executada.

Crie regras de firewall para todas as máquinas a partir da quais você pretende acessar remotamente a rede corporativa através de RDP.

Rede corporativa para sub-rede do site

A RSA recomenda que o firewall de cada site permita o acesso somente a partir de máquinas client do Archer designadas por meio de um endereço IP e uma porta confiáveis.

Defina regras de firewall para remover tudo, exceto o que estiver explicitamente permitido.

Configuração de host único

Proteja as portas padrão a seguir para garantir uma comunicação segura entre máquinas clients em que a interface de usuário da Web da Archer é executada e o servidor da Web da Archer: TCP 80TCP 443

A tabela a seguir mostra as regras de firewall para uma configuração de host único.

Objetivo	**REGRA | DIREÇÃO**	**Endereço IP de origem –> Endereço IP de destino**	**Protocolo**	**Porta**
Web do client Conectividade	PERMITIR | ENTRADA	ArcherWebUI_IPAddr –> ArcherWebServer_IPaddr	TCP	443
	PERMITIR | SAÍDA	ArcherWebServer_IPaddr –> ArcherWebUI_IPAddr	TCP	443
<Default>	BLOQUEAR | ENTRADA	All_* –> All_*	*	*
	BLOQUEAR | SAÍDA	All_* –> All_*	*	*

Configuração de vários hosts

Proteja as portas padrão a seguir para garantir uma comunicação segura entre máquinas clients em que a interface de usuário da Web da Archer é executada e o servidor da Web da Archer: TCP 80TCP 443

A tabela a seguir mostra as regras de firewall para uma configuração de vários hosts que inclui um proxy inverso/balanceador de carga.

Objetivo	**REGRA | DIREÇÃO**	**Endereço IP de origem –> Endereço IP de destino**	**Protocolo**	**Porta**
Web do client Conectividade	PERMITIR | ENTRADA	ArcherWebUI_IPAddr –> ArcherWebServer_IPaddr	TCP	443

Objetivo	REGRA | DIREÇÃO	Endereço IP de origem –> Endereço IP de destino	Protocolo	Porta
	PERMITIR | SAÍDA	ArcherWebServer_IPaddr –> ArcherWebUI_IPAddr	TCP	443
Feeds RSS	PERMITIR | ENTRADA	RSSServer_IPAddr –> ArcherWebServer_IPaddr	TCP	443
	PERMITIR | SAÍDA	ArcherWebServer_IPaddr –> RSSServer_IPAddr	TCP	443
Feeds de ameaças	PERMITIR | ENTRADA	ThreatFeedServer_IPAddr –> ArcherWebServer_IPaddr	TCP	443
	PERMITIR | SAÍDA	ArcherWebServer_IPaddr –> ThreatFeedServer_IPAddr	TCP	443
<Default>	BLOQUEAR | ENTRADA	All_* –> All_*	*	*
	BLOQUEAR | SAÍDA	All_* –> All_*	*	*

Feeds de dados de Archer para Archer

O Archer pode ser executado em várias sub-redes dentro da rede corporativa, na qual cada sub-rede é chamada de local. Você pode configurar o Archer para permitir que o Archer localizado em 1 site

alimente dados no Archer em outro site. Para obter mais informações, consulte Feed de dados Archer-to-Archer.

Para este cenário, faça o seguinte: Certifique-se de que o firewall em cada extremidade da transferência de dados permita a comunicação somente por meio de um endereço IP e porta confiáveis. Proteja as seguintes portas padrão para garantir uma comunicação segura entre 2 instâncias localizadas em sites diferentes: TCP 80 TCP 443 Archer

A tabela a seguir mostra como configurar as regras de firewall do site.

Objetivo	**REGRA | DIREÇÃO**	**Endereço IP de origem –> Endereço IP de destino**	**Protocolo**	**Porta**
Feed de dados do Archer	PERMITIR | ENTRADA	ArcherDataFeed_IPAddr –> ArcherWebServer_IPaddr	TCP	443
<Default>	BLOQUEAR | ENTRADA	All_* –> All_*	*	*
	BLOQUEAR | SAÍDA	All_* –> All_*	*	*

Configurações de implementação de segurança

A tabela a seguir mostra os controles de segurança que devem estar em vigor para ga
implementação do Archer.

Configurações de implementação	**Configuração de implementação de segurança**	**Prós da Configuração de implementação de segurança**	**Contras da Configuração de implementação de segurança**	**Instruçõ sobre co configur Configu de implem de segu**
HTTPS está habilitado em uma nova instalação de 6.x, por padrão, entre client e servidor. Remova qualquer vinculação HTTP existente (porta 80) por meio do IIS Manager.	Para a melhor segurança possível entre o client e o servidor, habilite o HTTPS e desabilite o HTTP no Microsoft IIS.	Fornece um alto nível de proteção para a comunicação entre client e servidor, evitando os tipos de ataque de adulteração, falsificação e man-in-the-middle.	Pode afetar o desempenho.	Consulte "Comuni com o se da Web" Ajuda do Platform
Comunicação criptografada do banco de dados	Criptografar a comunicação entre o servidor da Web do Archer e o banco de dados da instância aumenta a segurança.	Oferece mais segurança com a implementação da comunicação segura entre o servidor da Web e o banco de dados da instância.	Pode afetar o desempenho.	Consulte "Manten segurança Ajuda do Archer Pl

Configurações de implementação	**Configuração de implementação de segurança**	**Prós da Configuração de implementação de segurança**	**Contras da Configuração de implementação de segurança**	**Instruçõ sobre co configur Configu de implem de segu**
Configuração de cookie de sessão persistente	Excluir o cookie que mantém o token de sessão quando o client é encerrado aumenta a segurança.	Fornece maior segurança exigindo nova autenticação depois do log-out ou do fechamento do navegador.	O usuário tem de autenticar novamente.	Consulte "Habilita armazen do token sessão e cookie persister Ajuda do de contro Archer.
Configuração de segurança do Windows Server	Fortalecer o servidor da Web com base nas práticas recomendadas do setor reduz a probabilidade de vulnerabilidades.	Fornece segurança avançada e menos risco para os servidores implementados para o Archer.	Pode fazer com que alguns recursos sem proteção do Windows Server se tornem indisponíveis.	Siga as recomen de config de segur Microsoft versão a do IIS.

Configurações de implementação	Configuração de implementação de segurança	Prós da Configuração de implementação de segurança	Contras da Configuração de implementação de segurança	Instruç sobre co configu Configu de implem de segu
Configuração de segurança do SQL Server	Fortalecer a instalação do SQL Server hospedado no servidor de banco de dados com base nas práticas recomendadas do setor reduz a probabilidade de vulnerabilidades nos servidores.	Fornece maior segurança e menor risco para o servidor de banco de dados implementado na instalação da Plataforma.	Pode fazer com que alguns recursos sem proteção do SQL Server se tornem indisponíveis.	Siga as recomen de config de segur Microsoft versão a do SQL s

Configuração de segurança do servidor da Web

Para obter recomendações sobre a configuração de segurança do IIS, consulte a base de conhecimento da Microsoft.

Além das recomendações da Microsoft, configure o Microsoft IIS para fazer o seguinte: Habilitar comunicações SSL. Consulte Comunicação do servidor da Web.Proíba extensões de arquivo arbitrárias. Remova Informações sobre versão do IIS e ASP.Net dos cabeçalhos HTTP.

Proibir extensões de arquivo arbitrárias do IIS.

A Filtragem de solicitações é um recurso de segurança integrado do IIS (Internet Information Services, serviços de informações da Internet). As configurações desse recurso estão localizadas no elemento <requestFiltering>, que contém um elemento filho para <FileExtensions>. Esse elemento pode conter um conjunto de extensões

de nome de arquivo que o IIS nega ou permite. Por exemplo, você pode bloquear todas as solicitações de arquivos Web.config.

Para obter mais informações, visite as extensões de nome de arquivo de páginas da Web da Microsoft em https://docs.microsoft.com/en-us/iis/configuration/system.webServer/security/requestFiltering/fileextensions/index e Filtragem de solicitações em https://docs.microsoft.com/en-us/iis/configuration/system.webServer/security/requestFiltering/.

Ao usar o elemento <file Extensions> do IIS, não impeça o upload das seguintes extensões de arquivo do IIS, pois isso fará com que o Archer funcione incorretamente.

.
.ASPX
.AXD
.BAT
.BMP
.CAB
.CONFIG
.CSHTML
.CSS
.DAT
.DLL
.EJS
.FPJ
.GIF
.HTC
.HTM
.HTML
.ICO
.JPG
.JPEG
.JS
.MASTER
.MCWEBHELP
.PNG
.SETTINGS
.SVC
.TDF
.TXT
.WOFF
.WOFF2
.XAP
.XML
.ZIP

Negar upload de arquivos arbitrários

O Archer permite aos usuários fazer upload de arquivos com qualquer tipo de extensão. É recomendável treinar seus usuários quanto às boas práticas de segurança, inclusive não fazer upload de nenhum arquivo de fontes que não sejam as originais para impedir a introdução de arquivos possivelmente mal-intencionados na plataforma Archer.

Para aumentar a segurança, você pode impedir que os usuários façam upload de arquivos com extensões específicas. Para obter mais informações sobre as restrições de criação de arquivos, consulte "Configurando uma instância para arquivos confiáveis e não confiáveis" na Ajuda do ACP.

Dependendo do que os usuários fazem com o Archer, evite certos tipos de arquivo. Por exemplo, impeça o upload de arquivos executáveis .exe para o Archer. Porém, se os seus usuários investigam incidentes de segurança, convém permitir o upload de arquivos executáveis que contenham vírus e malware para uso em investigações.

A tabela a seguir fornece uma lista de extensões de arquivo usadas pelas operações normais do Archer. Não impeça uploads de arquivos com estas extensões.

.AI
.BMP
.CSS
.DOC
.DOCM
.DOCX
.DOT
.DOTM
.EMF
.EPS
.EXIF
.GIF
.ICO
.JPEG
.JPG
.PDF
.PNG
.POT
.POTM
.POTX
.PPA
.PPAM
.PPS
.PPSM

.PPSX
.PPT
.PPTM
.PPTX
.PS
.RTF
.TIF
.TIFF
.TXT
.WMF
.XLA
.XLAM
.XLS
.XLSB
.XLSM
.XLSX
.XLT
.XLTM
.XLTX
.XML

Remover informações de versão do IIS e ASP.Net dos cabeçalhos HTTP

Para dificultar que invasores identifiquem vulnerabilidades no software que está alimentando o servidor da Web, não divulgue os tipos de aplicativo e seus respectivos números de versão em cabeçalhos HTTP. Embora certos cabeçalhos HTTP sejam necessários, aqueles que identificam o servidor da Web não são necessários, inclusive: Servidor: Microsoft-IIS/<número_da_versão>X-Powered-By: ASP.NETX-AspNet-Versão: <version_ number>

Remover Cabeçalho HTTP AspNet-Version

É recomendável que você faça o seguinte: Remova os cabeçalhos HTTP que identificam o servidor web. Certifique-se de que <httpRuntime enableVersionHeader="false"/> esteja definido no arquivo Archer web.config, localizado em:IIS\DefaultWebSite\RSAArcher\web.configIIS\DefaultWebSite\RSAArcher\api\web.

Remover o cabeçalho HTTP X-Powered-By

1. Inicie o Microsoft IIS Manager.
2. Expanda a pasta Sites.

3. No agrupamento IIS, selecione o site que você deseja modificar e clique duas vezes na seção Cabeçalhos de Resposta HTTP.
4. Se "X-Powered-By: ASP.NET" for exibido na caixa de lista Cabeçalho personalizado, clique no link Remover na coluna à direita.

Observação: para garantir que o cabeçalho do servidor não seja adicionado automaticamente à resposta HTTP de saída pelo Microsoft IIS, use o utilitário UrlScan gratuito da Microsoft.

Remover cabeçalho de Versão do IIS

É recomendável que você garanta que<requestFiltering removeServerHeader ="true"/> está definido no Archer arquivo web.config, localizado em:

- IIS\DefaultWebSite\RSAArcher\web.config
- IIS\DefaultWebSite\RSAArcher\api\web.config

1. Abra o arquivo web.config.
2. No nó web.config system.webServer, use as seguintes configurações para configurar requestFiltering.
3. <security>

   <requestFiltering removeServerHeader ="true"/>

   </security>
4. Salve o arquivo.

(Opcional) Remover gerenciadores do IIS

Para melhorar a segurança e o desempenho do sistema, remova os gerenciadores IIS não utilizados e não exigidos pelo Archer.

aspq-ISAPI-4.0_32bit	PageHandlerFactory-ISAPI-4.0_32bit	WebServiceHandlerFactory-ISAPI-4.0_32bit
aspq-ISAPI-4.0_64bit	regras-ISAPI-4.0_32bit	xamlx-ISAPI-4.0_32bit
AXD-ISAPI-4.0_32bit	regras-ISAPI-4.0_64bit	xamlx-ISAPI-4.0_64bit
AXD-ISAPI-4.0_64bit	SimpleHandlerFactory-ISAPI-4.0_32bit	xoml-ISAPI-4.0_32bit

cshtm-ISAPI-4.0_32bit	svc-ISAPI-4.0_32bit	xoml-ISAPI-4.0_64bit
cshtm-ISAPI-4.0_64bit	svc-ISAPI-4.0_64bit	ASP Clássico
cshtml-ISAPI-4.0_32bit	vbhtm-ISAPI-4.0_32bit	TraceHandler-Integrado-4.0
cshtml-ISAPI-4.0_64bit	vbhtm-ISAPI-4.0_64bit	
HttpRemotingHandlerFactory-rem-ISAPI-4.0_32bit	vbhtml-ISAPI-4.0_32bit	
HttpRemotingHandlerFactory-soap-ISAPI-4.0_32bit	vbhtml-ISAPI-4.0_64bit	

Configurações de segurança HTTP

Uma parte fundamental da segurança do site inclui definir as configurações de segurança HTTP. Essas configurações protegem contra ataques, incluindo XSS, injeção de código e clickjacking, que têm maior probabilidade de afetar seu site.

Além das 3 configurações de segurança mencionadas abaixo, para obter mais configurações de segurança HTTP, consulte os 2 tópicos a seguir:

- Configurar IIS para o protocolo HTTPS/SSL
- Configurar o arquivo web.config da plataforma para o protocolo HTTPS/SSL

Cabeçalho HTTP Content-Security-Policy

O Archer usa o cabeçalho HTTP Content-Security-Policy, com o atributo frame-ancestors definido como `Self`, para evitar ataques de script entre quadros. Esse cabeçalho impede que hosts fora do servidor do Archer enquadrem páginas do Archer, semelhante ao que faz o cabeçalho X-Frame-Options. No entanto, o Internet Explorer não é compatível com o cabeçalho Content-Security-Policy.

É possível remover o cabeçalho HTTP Content-Security-Policy e adicionar cabeçalhos HTTP personalizados ao IIS. Se você remover o cabeçalho HTTP Content-Security-Policy e instalar uma versão mais recente do Archer, o instalador adicionará o cabeçalho novamente ao IIS.

O Archer também usa o cabeçalho HTTP X-Frame-Options. Os principais navegadores, como Google Chrome, Mozilla Firefox e Internet Explorer,

são compatíveis com esse cabeçalho. Defina o valor desse cabeçalho na lista do IIS como `SameOrigin` para impedir que os usuários carreguem um host do Archer em um iframe de outro host.

Cabeçalho X-Content-Type-Options

O Archer usa o cabeçalho X-Content-Type-Options, definido como `nosniff`, para evitar ataques de detecção de MIME. Este cabeçalho impede que os navegadores reconfigurem os tipos MIME nos hosts do Archer. `nosniff` evita que os navegadores assumam o tipo de conteúdo da página e renderiza as páginas com o tipo MIME correto.

É possível remover o cabeçalho HTTP X-Content-Type-Options e adicionar cabeçalhos HTTP personalizados ao IIS. Se você remover o cabeçalho HTTP X-Content-Type-Options e instalar uma versão mais recente do Archer, o instalador adicionará o cabeçalho novamente ao IIS.

Os seguintes navegadores são compatíveis com esse cabeçalho: Google Chrome, Mozilla Firefox, Microsoft Edge, Internet Explorer e Opera. Não há suporte no Safari para esse cabeçalho.

Cabeçalho Access-Control-Allow-Origin

O Archer usa o cabeçalho Access-Control-Allow-Origin para configurar quais hosts podem acessar as respostas enviadas da API do Archer. O valor padrão deste cabeçalho é `*`, que permite que qualquer host acesse as respostas da API.

Para restringir o acesso às respostas da API apenas ao host de origem da solicitação, defina `<add key="RestrictCORSDomains" value = "true"/>` no arquivo web.config do Archer, localizado em IIS\DefaultWebSite\RSAArcher\api\web.config.

Os principais navegadores, como Google Chrome, Mozilla Firefox e Internet Explorer, são compatíveis com esse cabeçalho.

Lista de IPs confiáveis

A Lista de IPs confiáveis permite definir um intervalo de endereços IP que podem acessar o Archer. A Lista de IPs confiáveis restringe apenas as conexões de entrada e deve incluir os seguintes itens: Servidores de aplicativos da Web Servidores de serviços Máquinas clientes acessando o aplicativo da Web

Opcionalmente, os seguintes itens também podem ser incluídos: Servidores de origem de feed de dados Servidores LDAP

Implemente a Lista de IPs confiáveis para limitar a disponibilidade da plataforma como um possível vetor de ataque.