Fortalecimento do host

Para garantir a operação segura do Archer, os componentes subjacentes do host devem ser reforçados para que o servidor funcione corretamente e as oportunidades de vulnerabilidades sejam removidas.

O Archer recomenda reforçar o sistema host vinculado a ele para permitir apenas TLS 1.2 em todos os clientes e servidores compatíveis com o Archer.

- Verifique se os servidores SQL, web services e os clients têm os service packs mais recentes usando TLS 1.2.
- Certifique-se de que todas as atualizações de segurança sejam aplicadas antes que o reforço adicional seja executado em todos os componentes subjacentes, inclusive, mas sem limitação, sistema operacional, SQL e IIS.

Nesta página

Recomendações para reforço de codificação TLS/SSL

Quando todos os componentes subjacentes forem atualizados, o reforço por criptografia TLS/SSL poderá ser aplicado. Um conjunto de codificações é um conjunto de algoritmos que ajudam a proteger uma conexão de rede usando TLS (Transport Layer Security). O reforço por codificação impede ataques de codificação conhecidos em TLS/SSL (por exemplo, Sweet32, BEAST, POODLE ou ROBOT). O reforço por codificação também garante que os dados sejam mantidos em segurança e criptografados em trânsito, de acordo com as práticas recomendadas do setor. Para garantir que a configuração da criptografia seja segura para toda a comunicação do Archer, são aplicadas as alterações abaixo nas comunicações do servidor e do client. Como tal, você deve atualizar essas configurações em todo o ambiente de maneira uniforme, caso contrário, podem ocorrer erros de comunicação.

Alterações de configuração

Observação: Para as alterações de registro abaixo, muitos desses caminhos de registro não existirão por padrão. Você precisará criar os caminhos do registro.

Desativar o Multi-Protocol Unified Hello

Caminho do registro
HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\M
HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\M
HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\M

Caminho do registro
HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\M

Desativar PCT 1.0

Caminho do registro	Ke
HKLM: \SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\PCT 1.0\Server	Ati
HKLM: \SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\PCT 1.0\Server	Dis
HKLM: \SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\PCT 1.0\Client	Ati
HKLM: \SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\PCT 1.0\Client	Dis

Desativar SSL 2.0

Caminho do registro	Ke
	Ati

Caminho do registro	Ke
HKLM: \SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server	
HKLM: \SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server	Dis
HKLM: \SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Client	Ati
HKLM: \SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Client	Dis

Desativar SSL 3.0

Caminho do registro	Ke
HKLM: \SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server	Ati
HKLM: \SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server	Dis
	Ati

Caminho do registro	Ke
HKLM: \SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Client	
HKLM: \SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Client	Dis

Observação: Se você desativar o SSL 3.0, poderá bloquear alguns usuários que ainda usam o Windows XP com IE 6 ou IE 7. Sem o SSL 3.0 ativado, não há protocolo disponível para esses usuários retornarem. As certificações de compras mais seguras podem exigir que você desative o SSLv3.

Desativar TLS 1.0

Caminho do registro	Ke
HKLM: \SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server	Ati
HKLM: \SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server	Dis
HKLM: \SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Client	Ati
	Dis

Caminho do registro	Ke
HKLM: \SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Client	

Desativar TLS 1.1

Caminho do registro	Ke
HKLM: \SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server	Ati
HKLM: \SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server	Dis
HKLM: \SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Client	Ati
HKLM: \SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Client	Dis

Ativar TLS 1.2

Caminho do registro	Ke
HKLM: \SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server	Ati
HKLM: \SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server	Dis
HKLM: \SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client	Ati
HKLM: \SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client	Dis

Desativar codificações não seguras

Caminho do registro	Ke
HKLM: \SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\DES 56/56	Ati
HKLM: \SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\NULL	Ati

Caminho do registro	**Ke**
HKLM: \SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 128/128	Ati
HKLM: \SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 40/128	Ati
HKLM: \SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 56/128	Ati
HKLM: \SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 40/128	Ati
HKLM: \SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 56/128	Ati
HKLM: \SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 64/128	Ati
HKLM: \SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 128/128	Ati
HKLM: \SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\Triple DES 168	Ati

Ativar codificações não seguras

Caminho do registro	Key
HKLM: \SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\AES 128/128	Ativ
HKLM: \SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\AES 256/256	Ativ

Desativar algoritmos de hash não seguros

Caminho do registro	Key
HKLM: \SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\MD5	Ativ

Ativar algoritmos de hash seguros

Caminho do registro	
HKLM: \SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\SHA	
HKLM: \SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\SHA256	

Caminho do registro
HKLM: \SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\SHA384
HKLM: \SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\SHA512

Desativar algoritmos de troca de chaves não seguros

Caminho do registro
HKLM: \SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgor Hellman

Ativar algoritmos de troca de chaves seguros

Caminho do registro
HKLM: \SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgor
HKLM: \SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgor

Configurar o pedido do conjunto de codificações para Strength-Preference e Perfect-Forward Secrecy

Caminho do registro	KeyNam
HKLM: \SOFTWARE\Policies\Microsoft\Cryptography\Configuration\SSL\00010002	Funções

Aplicar TLS 1.2 para .NET

Caminho do registro	KeyName
HKLM:\SOFTWARE\Microsoft.NETFramework\v2.0.50727	SystemDefaultTls
HKLM:\SOFTWARE\Microsoft.NETFramework\v2.0.50727	SchUseStrongCry
HKLM:\SOFTWARE\Microsoft.NETFramework\v4.0.30319	SystemDefaultTls
HKLM:\SOFTWARE\Microsoft.NETFramework\v4.0.30319	SchUseStrongCry
HKLM: \SOFTWARE\Wow6432Node\Microsoft.NETFramework\v2.0.50727	SystemDefaultTls

Caminho do registro	KeyName
HKLM: \SOFTWARE\Wow6432Node\Microsoft.NETFramework\v2.0.50727	SchUseStrongCry
HKLM: \SOFTWARE\Wow6432Node\Microsoft.NETFramework\v4.0.30319	SystemDefaultTls
HKLM: \SOFTWARE\Wow6432Node\Microsoft.NETFramework\v4.0.30319	SchUseStrongCry

Definir TLS 1.2 como padrão para comunicações de saída

Caminho do registro	KeyName	Tipo de propried
HKCU: \Software\Microsoft\Windows\CurrentVersion\Internet Settings	SecureProtocols	DWord
HKLM: \SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings	SecureProtocols	DWord

Clients compatíveis

Client	Versão do TLS
Android 4.4.2	TLS 1.2

Client	**Versão do TLS**
Android 5.0.0	TLS 1.2
Android 6.0	TLS 1.2 > http/1.1
Android 7.0	TLS 1.2 > h2
Android 8.0	TLS 1.2 > h2
Android 8.1	TLS 1.2 > h2
Android 9.0	TLS 1.2 > h2
BingPreview, janeiro de 2015	TLS 1.2
Chrome 49/XP SP3	TLS 1.2 > h2
Chrome 69/Windows 7 R	TLS 1.2 > h2
Chrome 70/Windows 10	TLS 1.2 > h2
Chrome 80/Windows 10 R	TLS 1.2 > h2
Firefox 31.3.0 ESR/Windows 7	TLS 1.2

Client	**Versão do TLS**
Firefox 47/Windows 7 R	TLS 1.2 > h2
Firefox 49/XP SP3	TLS 1.2 > h2
Firefox 62/Windows 7 R	TLS 1.2 > h2
Firefox 73/Windows 10 R	TLS 1.2 > h2
Googlebot, fevereiro de 2018	TLS 1.2
IE 11/Windows 10 R	TLS 1.2 > h2
Edge 15/Windows 10 R	TLS 1.2 > h2
Edge 16/Windows 10 R	TLS 1.2 > h2
Edge 18/Windows 10 R	TLS 1.2 > h2
Edge 13/Windows Phone 10 R	TLS 1.2 > h2
Java 8u161	TLS 1.2
Java 11.0.3	TLS 1.2

Client	**Versão do TLS**
Java 12.0.1	TLS 1.2
OpenSSL 1.0.1l R	TLS 1.2
OpenSSL 1.0.2s R	TLS 1.2
OpenSSL 1.1.0k R	TLS 1.2
OpenSSL 1.1.1c R	TLS 1.2
Safari 9/iOS 9 R	TLS 1.2 > h2
Safari 9/OS X 10.11 R	TLS 1.2 > h2
Safari 10/iOS 10 R	TLS 1.2 > h2
Safari 10/OS X 10.12 R	TLS 1.2 > h2
Safari 12.1.2/MacOS 10.14.6 Beta R	TLS 1.2 > h2
Safari 12.1.1/iOS 12.3.1 R	TLS 1.2 > h2
Apple ATS 9/iOS 9 R	TLS 1.2 > h2

Client	Versão do TLS
Yahoo Slurp, janeiro de 2015	TLS 1.2
YandexBot, janeiro de 2015	TLS 1.2

Observação: Você pode obter segurança adicional removendo as codificações de modo CBC listadas na seção "Configurar o pedido do conjunto de codificações para Strength-Preference e Perfect-Forward Secrecy". No entanto, os clients a seguir não teriam mais suporte.

Client	Versão do TLS	Conjunto de codificações
IE 11/ Windows 7 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
IE 11/ Windows 8.1 R	TLS 1.2 > http/ 1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
IE 11/ Windows Phone 8.1 R	TLS 1.2 > http/ 1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
IE 11/ Windows Phone 8.1 Atualização R	TLS 1.2 > http/ 1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

Client	Versão do TLS	Conjunto de codificações
Safari 6/ iOS 6.0.1	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
Safari 7/ iOS 7.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
Safari 7/ OS X 10.9 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
Safari 8/ iOS 8.4 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
Safari 8/ OS X 10.10 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

Verificando a configuração de codificação

Você pode usar várias ferramentas para verificar o reforço do conjunto de codificações que você configurou. O reforço do conjunto de codificações pode levar à conectividade limitada, pois os clients antigos não podem se conectar aos servidores com requisitos de segurança fortes. Algumas ferramentas fornecerão detalhes adicionais sobre essas limitações.

Para servidores públicos, é recomendável testar usando o teste da Qualys SSL Labs: Teste de servidor SSL (desenvolvido pela Qualys SSL Labs).

Para servidores privados, é recomendável testar usando TestSSL: /bin/ SSL baseado em bash/testador TLS: testssl.sh.