Impeça negociações para cifras nulas ou anônimas no ESA e no S A

Índice

Introdução

Este documento descreve como alterar Cisco envia por correio eletrónico ajustes da cifra da ferramenta de segurança (ESA) e do dispositivo do Gerenciamento do Cisco Security (S A) a fim impedir negociações para cifras nulas ou anônimas. Este documento aplica-se aos dispositivos baseados baseados e virtuais do hardware.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco ESA
- Cisco S A

Componentes Utilizados

A informação neste documento é baseada em todas as versões de Cisco ESA e de Cisco S A.

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 sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Impeça negociações para cifras nulas ou anônimas

Esta seção descreve como impedir negociações para cifras nulas ou anônimas em Cisco ESA

que executa AsyncOS para versões 9.1 e mais recente da Segurança do email, e igualmente em Cisco S A.

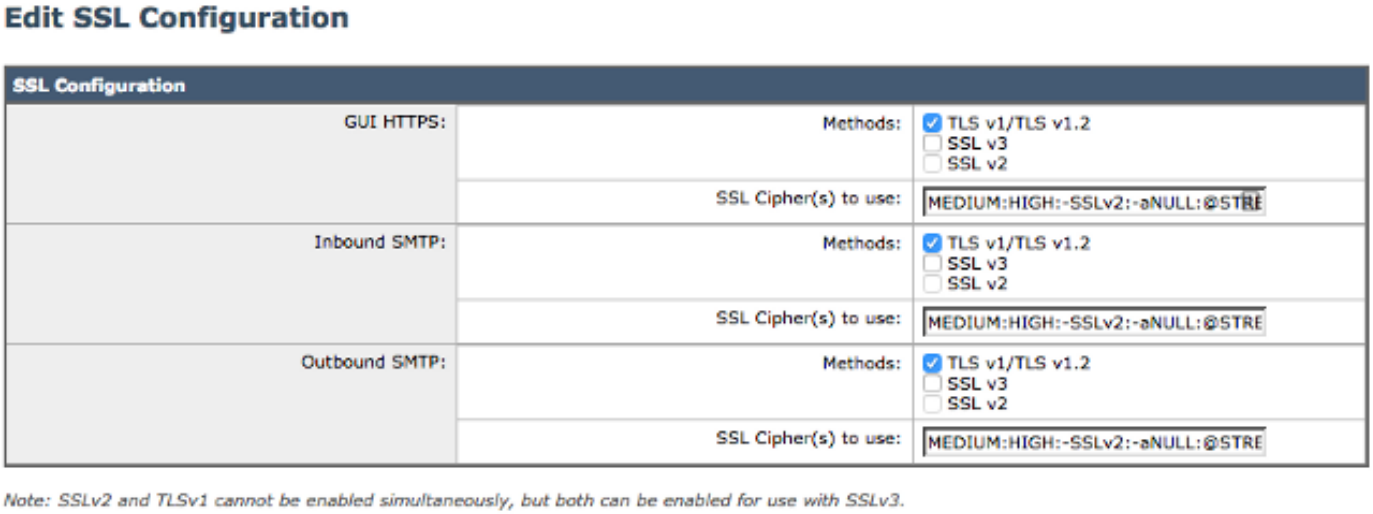
ESA que executam AsyncOS para a versão 9.5 mais recente da Segurança do email

Com a introdução de AsyncOS para a versão 9.5 da Segurança do email, o v1.2 TLS é apoiado agora. Os comandos que são descritos na seção anterior ainda trabalham; contudo, você verá as atualizações para o v1.2 TLS incluído nas saídas.

Estão aqui umas saídas de exemplo do CLI:

```
> sslconfig

sslconfig settings:
GUI HTTPS method: tlsv1/tlsv1.2
GUI HTTPS ciphers:
MEDIUM
HIGH
-SSLv2
-aNULL
@STRENGTH
Inbound SMTP method: tlsv1/tlsv1.2
Inbound SMTP ciphers:
MEDIUM
HIGH
-SSLv2
-aNULL
@STRENGTH
Outbound SMTP method: tlsv1/tlsv1.2
Outbound SMTP ciphers:
MEDIUM
HIGH
-SSLv2
-aNULL
@STRENGTH

Choose the operation you want to perform:
- GUI - Edit GUI HTTPS ssl settings.
- INBOUND - Edit Inbound SMTP ssl settings.
- OUTBOUND - Edit Outbound SMTP ssl settings.
- VERIFY - Verify and show ssl cipher list.
[]> inbound

Enter the inbound SMTP ssl method you want to use.
1. SSL v2
2. SSL v3
3. TLS v1/TLS v1.2
4. SSL v2 and v3
5. SSL v3 and TLS v1/TLS v1.2
6. SSL v2, v3 and TLS v1/TLS v1.2
[3]>
```

A fim alcançar estes ajustes do GUI, navegue à **administração do sistema > à configuração de SSL > editam ajustes…**:



> Dica: Para a informação completa, refira o guia apropriado do utilizador final ESA para a versão 9.5 ou mais recente.

ESA que executam AsyncOS para a versão 9.1 da Segurança do email ou mais velho

Você pode alterar as cifras que são usadas no ESA com o comando do **sslconfig**. A fim impedir as negociações ESA para cifras nulas ou anônimas, incorpore o comando do **sslconfig no** ESA CLI e aplique estes ajustes:

- Método de entrada do Simple Mail Transfer Protocol (SMTP): **sslv3tlsv1**
- Cifras de entrada S TP: **MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH**
- Método de partida S TP: **sslv3tlsv1**
- Cifras de partida S TP: **MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH**

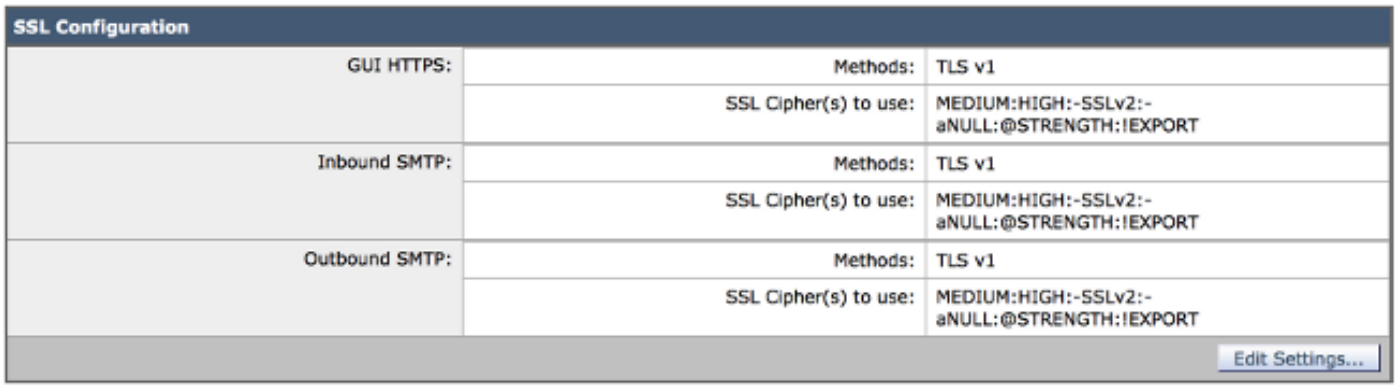
Está aqui um exemplo de configuração para cifras de entrada:

```
CLI: > sslconfig

sslconfig settings:
  GUI HTTPS method:  sslv3tlsv1
  GUI HTTPS ciphers: RC4-SHA:RC4-MD5:ALL
  Inbound SMTP method:  sslv3tlsv1
  Inbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL
  Outbound SMTP method:  sslv3tlsv1
  Outbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL

Choose the operation you want to perform:
- GUI - Edit GUI HTTPS ssl settings.
- INBOUND - Edit inbound SMTP ssl settings.
- OUTBOUND - Edit outbound SMTP ssl settings.
- VERIFY - Verify and show ssl cipher list.
[]> inbound

Enter the inbound SMTP ssl method you want to use.
1. SSL v2.
2. SSL v3
```

```
3. TLS v1
4. SSL v2 and v3
5. SSL v3 and TLS v1
6. SSL v2, v3 and TLS v1
[5]> 3

Enter the inbound SMTP ssl cipher you want to use.
[RC4-SHA:RC4-MD5:ALL]> MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH
```

Nota: Ajuste o **GUI**, **DE ENTRADA**, e **DE PARTIDA** como necessário para cada cifra.

Até à data de AsyncOS para a versão 8.5 da Segurança do email, o comando do **sslconfig** está igualmente disponível através do GUI. A fim alcançar estes ajustes do GUI, navegue à **administração do sistema > às configurações de SSL > editam ajustes**:



Dica: Fixe os soquetes o 3.0 da versão que da alga (SSL) (RFC-6101) é um Obsoleto e um protocolo inseguro. Há uma vulnerabilidade em SSLv3 CVE-2014-3566 conhecido como o *Oracle do estofamento no ataque da criptografia do legado Downgraded (CANICHE)*, que é seguido pela identificação de bug Cisco CSCur27131. Cisco recomenda que você desabilita SSLv3 quando você mudar as cifras, usa o Transport Layer Security (TLS) somente, e seleciona o *option 3* (TLS v1). Refira a identificação de bug Cisco CSCur27131 para detalhes completos.

S A que executam AsycnOS para o Gerenciamento de segurança satisfeito 9.6 ou mais novo

Similar ao ESA, execute o comando do **sslconfig no** CLI.

S A que executam AsyncOS para o Gerenciamento de segurança satisfeito 9.5 ou mais atrasado

O comando do **sslconfig** não está disponível para versões velhas do S A.

Nota: Umas versões mais velhas de AsyncOS para o S A apoiaram somente TLS v1. Promova por favor a 9.6 ou mais novo em seu S A para o Gerenciamento atualizado SSL.

Você deve terminar estas etapas do S A CLI a fim alterar as cifras SSL:

1. Salvar o arquivo de configuração S à seu computador local.

2. Abra o arquivo XML.

3. Procure pela seção do *<ssl> no* XML:

```
CLI: > sslconfig

sslconfig settings:
  GUI HTTPS method:  sslv3tlsv1
  GUI HTTPS ciphers: RC4-SHA:RC4-MD5:ALL
  Inbound SMTP method:  sslv3tlsv1
  Inbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL
  Outbound SMTP method:  sslv3tlsv1
  Outbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL

Choose the operation you want to perform:
- GUI - Edit GUI HTTPS ssl settings.
- INBOUND - Edit inbound SMTP ssl settings.
- OUTBOUND - Edit outbound SMTP ssl settings.
- VERIFY - Verify and show ssl cipher list.
[]> inbound

Enter the inbound SMTP ssl method you want to use.
1. SSL v2.
2. SSL v3
3. TLS v1
4. SSL v2 and v3
5. SSL v3 and TLS v1
6. SSL v2, v3 and TLS v1
[5]> 3

Enter the inbound SMTP ssl cipher you want to use.
[RC4-SHA:RC4-MD5:ALL]> MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH
```

4. Altere as cifras como desejado e salvar o XML:

```
CLI: > sslconfig

sslconfig settings:
  GUI HTTPS method:  sslv3tlsv1
  GUI HTTPS ciphers: RC4-SHA:RC4-MD5:ALL
  Inbound SMTP method:  sslv3tlsv1
  Inbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL
  Outbound SMTP method:  sslv3tlsv1
  Outbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL

Choose the operation you want to perform:
- GUI - Edit GUI HTTPS ssl settings.
- INBOUND - Edit inbound SMTP ssl settings.
- OUTBOUND - Edit outbound SMTP ssl settings.
- VERIFY - Verify and show ssl cipher list.
[]> inbound

Enter the inbound SMTP ssl method you want to use.
1. SSL v2.
2. SSL v3
3. TLS v1
4. SSL v2 and v3
5. SSL v3 and TLS v1
6. SSL v2, v3 and TLS v1
[5]> 3

Enter the inbound SMTP ssl cipher you want to use.
[RC4-SHA:RC4-MD5:ALL]> MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH
```

5. Carregue o arquivo de configuração novo no S A.

6. **Submeta** e **comprometa** todas as mudanças.

Informações Relacionadas

- Cisco ESA - Release Note
- Cisco ESA - Guias do Usuário
- Cisco S A - Release Note
- Cisco S A - Guias do Usuário
- Suporte Técnico e Documentação - Cisco Systems