O ESA com ampère recebe “o serviço da reputação do arquivo na nuvem é” erro inacessível

Índice

Introdução

Este documento descreve o alerta atribuído à ferramenta de segurança do email de Cisco (ESA) com a proteção avançada do malware (ampère) permitida, onde o serviço não se comunica sobre a porta 32137 para a reputação do arquivo.

Corrija “o serviço da reputação do arquivo na nuvem é” erro inacessível recebido para o ampère

O ampère foi liberado para o uso no ESA na versão 8.5.5 de AsyncOS para a Segurança do email. Com o ampère licenciado e permitido no ESA, os administradores recebem esta mensagem:

```
The Warning message is:

amp The File Reputation service in the cloud is unreachable.

Last message occurred 2 times between Tue Jul 26 10:17:15 2015 and Tue Jul 26 10:18:16 2016.

Version: 10.0.0-125
Serial Number: 123A82F6780EEE9E1E10-AAA5DBEFCEEE
Timestamp: 26 Jul 2016 10:56:28 -0600
```

O serviço ampère pôde ser permitido, mas provavelmente não se comunica na rede através da porta 32137 para a reputação do arquivo.

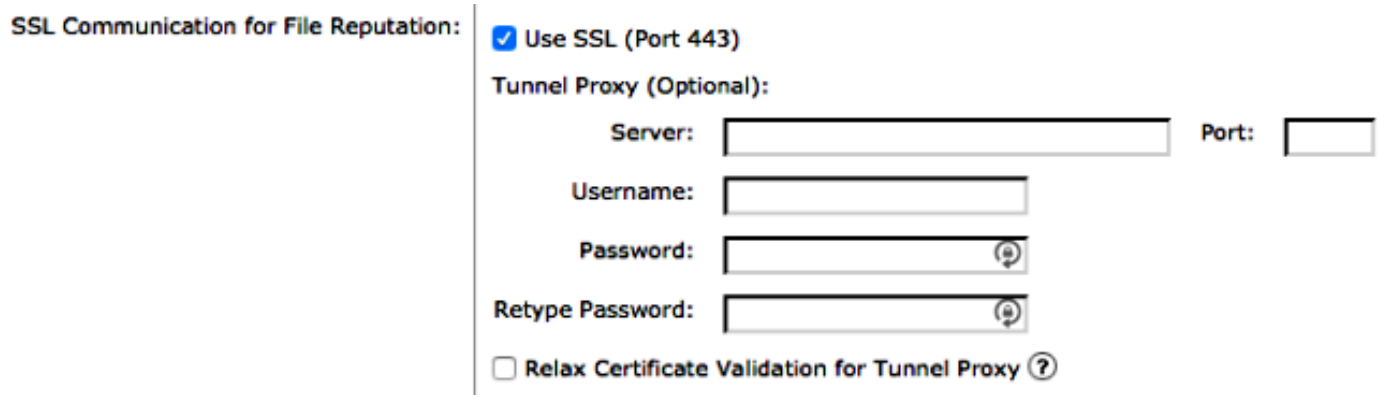
Se aquele é o caso, o administrador ESA pode escolher mandar a reputação do arquivo comunicar-se sobre a porta 443.

A fim fazer assim, execute o **ampconfig > avançado do** CLI e seja certo que **Y** está selecionado para *você quer permitir uma comunicação SSL (porta 443) para a reputação do arquivo? [N] >*:

```
10.0.0-125.local> ampconfig

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Microsoft Windows / DOS Executable
Appliance Group ID/Name: Not part of any group yet
```

```
Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File Analysis
reporting details.
- CLEARCACHE - Clears the local File Reputation cache.
[]> advanced

Enter cloud query timeout?
[15]>

Choose a file reputation server:
1. AMERICAS (cloud-sa.amp.sourcefire.com)
2. Private reputation cloud
[1]>

Enter cloud domain?
[a.immunet.com]>

Do you want use the recommended reputation threshold from cloud service? [Y]>

Enter heartbeat interval?
[15]>

Do you want to enable SSL communication (port 443) for file reputation? [N]> Y

Choose a file analysis server:
1. AMERICAS (https://panacea.threatgrid.com)
2. Private analysis cloud
[1]>

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Microsoft Windows / DOS Executable
Appliance Group ID/Name: Not part of any group yet
```

Se você usa o GUI, escolha **Serviços de segurança > reputação do arquivo e a análise > edita configurações globais > avançou (gota-para baixo)** e assegura-se de que a caixa de verificação do **uso SSL** esteja verificada como mostrado aqui:



Comprometa alguns e todas as mudanças à configuração.

Finalmente, reveja a ordem atual do início de uma sessão ampère para ver o serviço e o sucesso ou a falha da Conectividade. Você pode realizar este do CLI com **cauda ampère**.

Antes das mudanças feitas ao **ampconfig > avançou**, você veria isto nos logs ampère:

```
10.0.0-125.local> ampconfig

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Microsoft Windows / DOS Executable
Appliance Group ID/Name: Not part of any group yet


Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File Analysis
reporting details.
- CLEARCACHE - Clears the local File Reputation cache.
[]> advanced

Enter cloud query timeout?
[15]>

Choose a file reputation server:
1. AMERICAS (cloud-sa.amp.sourcefire.com)
2. Private reputation cloud
[1]>

Enter cloud domain?
[a.immunet.com]>

Do you want use the recommended reputation threshold from cloud service? [Y]>

Enter heartbeat interval?
[15]>

Do you want to enable SSL communication (port 443) for file reputation? [N]> Y

Choose a file analysis server:
1. AMERICAS (https://panacea.threatgrid.com)
2. Private analysis cloud
[1]>

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Microsoft Windows / DOS Executable
Appliance Group ID/Name: Not part of any group yet
```

Depois que a mudança é feita ao **ampconfig > avançado**, você vê este nos logs ampère:

```
10.0.0-125.local> ampconfig

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Microsoft Windows / DOS Executable
Appliance Group ID/Name: Not part of any group yet


Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File Analysis
reporting details.
- CLEARCACHE - Clears the local File Reputation cache.
[]> advanced
```

```
Enter cloud query timeout?
[15]>

Choose a file reputation server:
1. AMERICAS (cloud-sa.amp.sourcefire.com)
2. Private reputation cloud
[1]>

Enter cloud domain?
[a.immunet.com]>

Do you want use the recommended reputation threshold from cloud service? [Y]>

Enter heartbeat interval?
[15]>

Do you want to enable SSL communication (port 443) for file reputation? [N]> Y

Choose a file analysis server:
1. AMERICAS (https://panacea.threatgrid.com)
2. Private analysis cloud
[1]>

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Microsoft Windows / DOS Executable
Appliance Group ID/Name: Not part of any group yet
```

O arquivo de amp_watchdog.txt segundo as indicações do exemplo anterior executará os minutos cada 10 e será seguido no log ampère. Este arquivo é parte da manutenção de atividade para o ampère.

Uma pergunta normal no log ampère contra uma mensagem com tipo de arquivo configurado para a reputação do arquivo e a análise do arquivo seria similar a esta:

```
10.0.0-125.local> ampconfig

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Microsoft Windows / DOS Executable
Appliance Group ID/Name: Not part of any group yet


Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File Analysis
reporting details.
- CLEARCACHE - Clears the local File Reputation cache.
[]> advanced

Enter cloud query timeout?
[15]>

Choose a file reputation server:
1. AMERICAS (cloud-sa.amp.sourcefire.com)
2. Private reputation cloud
[1]>

Enter cloud domain?
```

```
[a.immunet.com]>

Do you want use the recommended reputation threshold from cloud service? [Y]>

Enter heartbeat interval?
[15]>

Do you want to enable SSL communication (port 443) for file reputation? [N]> Y

Choose a file analysis server:
1. AMERICAS (https://panacea.threatgrid.com)
2. Private analysis cloud
[1]>

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Microsoft Windows / DOS Executable
Appliance Group ID/Name: Not part of any group yet
```

Com esta informação de registro, o administrador deve poder correlacionar o ID de mensagem (MEADOS DE) nos logs do correio.

Troubleshooting

Reveja o Firewall e as configurações de rede a fim assegurar-se de que uma comunicação SSL esteja aberta para estes:

Porta	Protocolo	Entrada/saída	Hostname	Descrição
443	TCP	Para fora	Como configurado em Serviços de segurança > em reputação e em análise do arquivo, seção avançada.	Alcance para nublar-s serviços para a anális arquivo.
32137	TCP	Para fora	Como configurado em Serviços de segurança > em reputação e em análise do arquivo, seção avançada, seção avançada, parâmetro do pool do server da nuvem.	Alcance para nublar-s serviços a fim obter a reputação do arquivo.

Você pode testar a conectividade básica de seu ESA ao serviço da nuvem sobre 443 através do telnet a fim assegurar-se de que seu dispositivo possa com sucesso alcançar os serviços ampère, arquivar a reputação, e arquivar a análise.

> Nota: Os endereços para a reputação do arquivo e a análise do arquivo são configurados no CLI com **ampconfig > avançado**, ou do GUI com **Serviços de segurança > reputação e análise do arquivo > edite configurações globais > avançado (gota-para baixo)**.

Arquive o exemplo da reputação:

```
10.0.0-125.local> ampconfig

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Microsoft Windows / DOS Executable
Appliance Group ID/Name: Not part of any group yet


Choose the operation you want to perform:
```

```
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File Analysis
reporting details.
- CLEARCACHE - Clears the local File Reputation cache.
[]> advanced

Enter cloud query timeout?
[15]>

Choose a file reputation server:
1. AMERICAS (cloud-sa.amp.sourcefire.com)
2. Private reputation cloud
[1]>

Enter cloud domain?
[a.immunet.com]>

Do you want use the recommended reputation threshold from cloud service? [Y]>

Enter heartbeat interval?
[15]>

Do you want to enable SSL communication (port 443) for file reputation? [N]> Y

Choose a file analysis server:
1. AMERICAS (https://panacea.threatgrid.com)
2. Private analysis cloud
[1]>

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Microsoft Windows / DOS Executable
Appliance Group ID/Name: Not part of any group yet
```

Arquive o exemplo da análise:

```
10.0.0-125.local> ampconfig

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Microsoft Windows / DOS Executable
Appliance Group ID/Name: Not part of any group yet


Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File Analysis
reporting details.
- CLEARCACHE - Clears the local File Reputation cache.
[]> advanced

Enter cloud query timeout?
[15]>

Choose a file reputation server:
1. AMERICAS (cloud-sa.amp.sourcefire.com)
2. Private reputation cloud
[1]>

Enter cloud domain?
```

```
[a.immunet.com]>

Do you want use the recommended reputation threshold from cloud service? [Y]>

Enter heartbeat interval?
[15]>

Do you want to enable SSL communication (port 443) for file reputation? [N]> Y

Choose a file analysis server:
1. AMERICAS (https://panacea.threatgrid.com)
2. Private analysis cloud
[1]>

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Microsoft Windows / DOS Executable
Appliance Group ID/Name: Not part of any group yet
```

Informações Relacionadas

- Teste avançado da proteção do malware ESA (ampère)
- Guias do Usuário ESA
- ESA FAQ: Que é um ID de mensagem (MEADOS DE), o identificador de conexão da injeção (ICID), ou o identificador de conexão da entrega (DCID)?
- Como eu procuro e para ver o correio entra o ESA?
- Suporte Técnico e Documentação - Cisco Systems