O ESA com AMP recebe o " O serviço da reputação do arquivo não é reachable" Erro

Índice

Introdução

Este original descreve o alerta atribuído à ferramenta de segurança do email de Cisco (ESA) com a proteção avançada do malware (AMP) permitida, onde o serviço é incapaz de se comunicar sobre a porta 32137 ou 443 para a reputação do arquivo.

Corrija “o serviço da reputação do arquivo não é” erro alcançável recebido para o AMP

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

```
The Warning message is:

The File Reputation service is not reachable.

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

Version: 12.5.0-066
Serial Number: 123A82F6780XXX9E1E10-XXX5DBEFCXXX
Timestamp: 07 Oct 2019 14:25:13 -0400
```

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

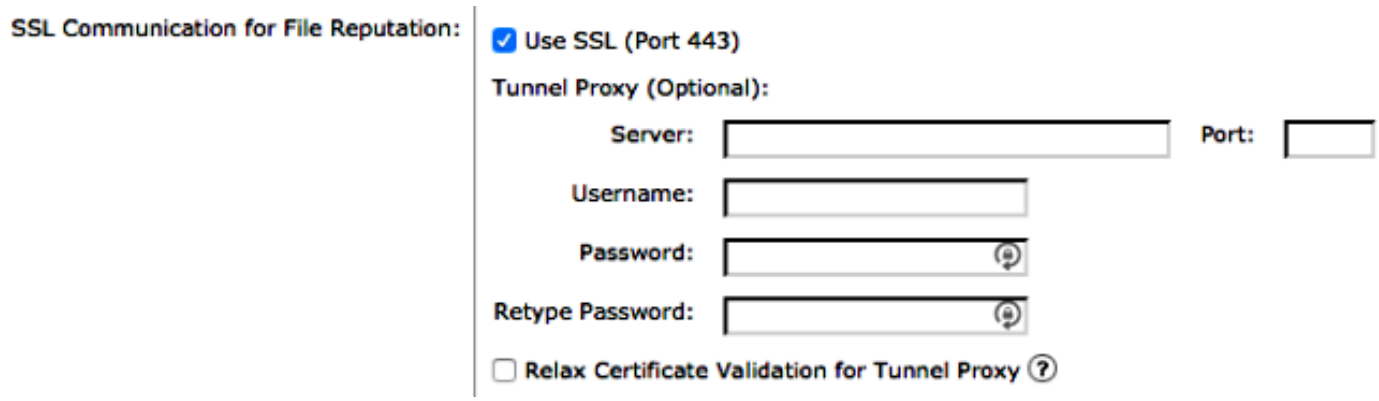
Se aquele é o caso, o administrador ESA pode escolher mandar a reputação do arquivo comunicar-se sobre a porta 443.

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] >*:

```
(Cluster example.com)> ampconfig

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.
- CACHESETTINGS - Configure the cache settings for AMP.
```

```
- CLUSTERSET - Set how advanced malware protection is configured in a cluster.
- CLUSTERSHOW - Display how advanced malware protection is configured in a cluster.
[]> advanced

Enter cloud query timeout?
[15]>

Choose a file reputation server:
1. AMERICAS (cloud-sa.amp.cisco.com)
2. AMERICAS(Legacy) (cloud-sa.amp.sourcefire.com)
3. EUROPE (cloud-sa.eu.amp.cisco.com)
4. APJC (cloud-sa.apjc.amp.cisco.com)
5. Private reputation cloud
[1]>

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

Enter heartbeat interval?
[15]>

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

Proxy server detail:
Server :
Port :
User :

Do you want to change proxy detail [N]>

Do you want to suppress the verdict update alerts for all messages that are not delivered to the
recipient? [N]>

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

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 seleção 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 AMP 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 AMP:

```
Mon Jan 26 10:11:16 2015 Warning: amp The File Reputation service in the cloud
is unreachable.
Mon Jan 26 10:12:15 2015 Warning: amp The File Reputation service in the cloud
is unreachable.
Mon Jan 26 10:13:15 2015 Warning: amp The File Reputation service in the cloud
is unreachable.
```

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

```
Mon Jan 26 10:19:19 2015 Info: amp stunnel process started pid [3725]
Mon Jan 26 10:19:22 2015 Info: amp The File Reputation service in the cloud
is reachable.
Mon Jan 26 10:19:22 2015 Info: amp File reputation service initialized
successfully
Mon Jan 26 10:19:22 2015 Info: amp File Analysis service initialized
successfully
Mon Jan 26 10:19:23 2015 Info: amp The File Analysis server is reachable
Mon Jan 26 10:20:24 2015 Info: amp File reputation query initiating. File Name =
'amp_watchdog.txt', MID = 0, File Size = 12 bytes, File Type = text/plain
Mon Jan 26 10:20:24 2015 Info: amp Response received for file reputation query
from Cloud. File Name = 'amp_watchdog.txt', MID = 0, Disposition = file unknown,
Malware = None, Reputation Score = 0, sha256 = a5f28f1fed7c2fe88bcdf403710098977
fa12c32d13bfbd78bbe27e95b245f82, upload_action = 1
```

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

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

```
Wed Jan 14 15:33:01 2015 Info: File reputation query initiating. File Name =
'securedoc_20150112T114401.html', MID = 703, File Size = 108769 bytes, File
Type = text/html
Wed Jan 14 15:33:02 2015 Info: Response received for file reputation query from
Cloud. File Name = 'securedoc_20150112T114401.html', MID = 703, Disposition = file
unknown, Malware = None, Reputation Score = 0, sha256 = c1afd8efe4eeb4e04551a8a0f5
533d80d4bec0205553465e997f9c672983346f, upload_action = 1
```

Com esta informação do log, 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 AMP, 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)**.

> Nota: Se utilizando um proxy do túnel entre o ESA e os server da reputação do arquivo, você pode ser exigido permitir a opção de relaxar a validação certificada para o proxy do túnel. Esta opção está fornecida para saltar a validação certificada padrão se o certificado do servidor proxy do túnel não é assinado por uma autoridade da raiz confiada pelo ESA. Por exemplo, selecione esta opção se usando um certificado auto-assinado em um servidor proxy interno confiado do túnel.

Arquive o exemplo da reputação:

```
10.0.0-125.local> telnet cloud-sa.amp.sourcefire.com 443

Trying 23.21.199.158...
Connected to ec2-23-21-199-158.compute-1.amazonaws.com.
Escape character is '^]'.
^]
telnet> quit
Connection closed.
```

Arquive o exemplo da análise:

```
10.0.0-125.local> telnet panacea.threatgrid.com 443

Trying 69.55.5.244...
Connected to 69.55.5.244.
Escape character is '^]'.
^]
telnet> quit
Connection closed.
```

Informações Relacionadas

- Teste avançado da proteção do malware ESA (AMP)
- 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