ESA 上の静的ファイル レピュテーション ホストまたは代替ファイル レピュテーション クラウド サーバ プールの設定

目次

概要

このドキュメントでは、Cisco E メール セキュリティ アプライアンス (ESA) を静的ホストまたは代替レピュテーション クラウド サーバプールと通信し、高度なマルウェア防御 (AMP) を利用してこれらをファイル レピュテーションに使用するように設定する方法を説明します。

背景説明

ファイル レピュテーション クエリは、ESA 上の AMP の 2 つのレイヤの最初のレイヤです。 ファイル レピュテーションは、各ファイルのフィンガープリントを ESA を通過する際に取得し、AMP のクラウドベースのインテリジェンス ネットワークに送信してレピュテーションを判定します。 これらの結果から、ESA の管理者は悪意のあるファイルを自動的にブロックし、管理者が定義したポリシーを適用できます。 ファイル レピュテーション クラウド サービスは Amazon Web Services (AWS) でホストされます。 このドキュメントに記載されているホスト名に対して DNS クエリを実行すると、「.amazonaws.com」が表示されています。

ESA 上の AMP の 2 番目のレイヤはファイル分析です。 これについての説明は、このドキュメントの対象外です。

ファイル レピュテーション トラフィックの SSL 通信では、デフォルトでポート 32137 を使用します。 サービスの設定時には、ポート 443 を代わりに使用できます。 詳細については、『ESA User Guide』の「File Reputation Filtering and File Analysis」の項を参照してください。 ESA およびネットワークの管理者は、設定を開始する前に、IP アドレスのプールへの接続、IP ロケーション、およびポート通信（32137 と 443）を確認する必要がある場合があります。

デフォルト AMERICAS（Legacy）評判クラウド サーバ プール（クラウド sa.amp.sourcefire.com）

ファイル レピュテーションのライセンスを取得し、有効にして ESA で設定すると、デフォルトで次のレピュテーション クラウド サーバプールに対して設定されます。

- AMERICAS（Legacy）（クラウドsa.amp.sourcefire.com）

ホスト名の「cloud-sa.amp.sourcefire.com」は DNS 正規名レコード（CNAME）です。 CNAME は、ドメイン名が別の「正規の」ドメイン名のエイリアスであることを指定するために使用される DNS のリソース レコードのタイプです。 プール内のこの CNAME に関連付けられたホスト名は次のようになります。

- ec2-107-22-180-78.compute-1.amazonaws.com (107.22.180.78)
- ec2-54-225-142-100.compute-1.amazonaws.com (54.225.142.100)
- ec2-23-21-208-4.compute-1.amazonaws.com (23.21.208.4)
- ec2-54-83-195-228.compute-1.amazonaws.com (54.83.195.228)

選択されるかもしれない 2 つの追加ファイル評判サーバ選択があります:

- 南 北 中央アメリカ（クラウドsa.amp.cisco.com）
- ヨーロッパ（cloud-sa.eu.am p.cisco.com）

両方のサーバはこの資料の「静的ファイル評判サーバ ホスト名（.cisco.com）」セクションでカバーされます。

この dig または nslookup クエリを実行すると、南・北・中央アメリカの cloud-sa-amp.sourcefire.com CNAME に関連付けられたホストをネットワークからいつでも確認できます。

```
$ dig cloud-sa.amp.sourcefire.com +short
cloud-sa-589592150.us-east-1.elb.amazonaws.com.
107.22.180.78
54.225.208.214
23.21.208.4
54.83.195.228

$ nslookup cloud-sa.amp.sourcefire.com
Server: 208.67.222.222
Address: 208.67.222.222#53

Non-authoritative answer:
cloud-sa.amp.sourcefire.com canonical name = cloud-sa-589592150.us-east-1.elb.amazonaws.com.
Name: cloud-sa-589592150.us-east-1.elb.amazonaws.com
Address: 54.225.208.214
Name: cloud-sa-589592150.us-east-1.elb.amazonaws.com
Address: 54.83.195.228
Name: cloud-sa-589592150.us-east-1.elb.amazonaws.com
Address: 107.22.180.78
Name: cloud-sa-589592150.us-east-1.elb.amazonaws.com
```

```
Address: 23.21.208.4
```

> **注:** これらのホストは静的ではなく、これらのホストのみに基づいて ESA のファイル レピュテーション トラフィックを制限しないことを推奨します。 プール内のホストは予告なく変更されるため、クエリの結果は異なる場合があります。

次のサードパーティ ツールから IP 地理的位置を確認できます。

- http://geoiplookup.net/ip/107.22.180.78
- http://geoiplookup.net/ip/54.225.208.214
- http://geoiplookup.net/ip/23.21.208.4
- http://geoiplookup.net/ip/54.83.195.228

静的ファイル レピュテーション サーバのホスト名（.cisco.com）

シスコは、2016 年に AMP のファイル レピュテーション サービスに「.cisco.com」ベースのホスト名の提供を開始しました。 ファイル レピュテーションに使用できる次の静的ホスト名と IP アドレスがあります。

- cloud-sa.amp.cisco.com（北米 - 米国）
- cloud-sa.eu.amp.cisco.com（欧州 – アイルランド共和国）
- cloud-sa.apjc.amp.cisco.com（アジア太平洋地域 – 日本）

ネットワークからのホストおよび関連する IP アドレスを確認し、**発掘**または **nslookup** クエリを実行するかもしれません:

北米（US）：

```
$ dig cloud-sa.amp.cisco.com +short
52.21.117.50
```

ヨーロッパ（アイルランド共和国）：

```
$ nslookup cloud-sa.eu.amp.cisco.com
Server: 208.67.222.222
Address: 208.67.222.222#53

Non-authoritative answer:
Name: cloud-sa.eu.amp.cisco.com
Address: 52.30.124.82
```

アジア太平洋地域（日本）：

```
 $ dig cloud-sa.apjc.amp.cisco.com +short
52.69.39.127
```

次のサードパーティ ツールから IP 地理的位置を確認できます。

- http://geoiplookup.net/ip/52.21.117.50
- http://geoiplookup.net/ip/52.30.124.82
- http://geoiplookup.net/ip/52.69.39.127

現時点では、「.sourcefire.com」のホスト名を廃止する予定はありません。

代替ヨーロッパ評判クラウド サーバ プール（cloud-sa.eu.am p.sourcefire.com）

EU ベースのサーバおよびデータセンターのみに固有のトラフィックを送信する必要がある欧州連合（EU）を拠点とする顧客の場合、管理者は ESA を次の EU の静的ホストまたは EU のレピュテーション クラウド サーバプールを指すように設定できます。

- cloud-sa-eu.amp.cisco.com
- cloud-sa.eu.am p.sourcefire.com

デフォルトホスト名「クラウドsa.amp.sourcefire.com のように」、ホスト名「cloud-sa.eu.am p.sourcefire.com」はまた CNAME です。 プール内のこの CNAME に関連付けられたホスト名は次のようになります。

- ec2-54-217-245-97.eu-west-1.compute.amazonaws.com (54.217.245.97)
- ec2-54-247-186-153.eu-west-1.compute.amazonaws.com (54.247.186.153)
- ec2-176-34-122-245.eu-west-1.compute.amazonaws.com (176.34.122.245)

ネットワークからのヨーロッパ cloud-sa.eu.amp.sourcefire.com CNAME に関連付けられ、**発掘または nslookup** クエリを実行するホストを確認するかもしれません::

```
$ dig cloud-sa.eu.amp.sourcefire.com +short
cloud-sa-162723281.eu-west-1.elb.amazonaws.com.
54.217.245.97
54.247.186.153
176.34.122.245

$ nslookup cloud-sa.eu.amp.sourcefire.com
Server: 208.67.222.222
Address: 208.67.222.222#53

Non-authoritative answer:
cloud-sa.eu.amp.sourcefire.com canonical name = cloud-sa-162723281.eu-west-1.elb.amazonaws.com.
Name: cloud-sa-162723281.eu-west-1.elb.amazonaws.com
Address: 54.247.182.97
Name: cloud-sa-162723281.eu-west-1.elb.amazonaws.com
Address: 176.34.122.245
Name: cloud-sa-162723281.eu-west-1.elb.amazonaws.com
Address: 54.247.186.153
```

> **注:** これらのホストは静的ではなく、これらのホストのみに基づいて ESA のファイル レピュテーション トラフィックを制限しないことを推奨します。 プール内のホストは予告なく変更されるため、クエリの結果は異なる場合があります。

次のサードパーティ ツールから IP 地理的位置を確認できます。

- http://geoiplookup.net/ip/176.34.122.245
- http://geoiplookup.net/ip/54.247.186.153
- http://geoiplookup.net/ip/54.217.245.97

ESA 上の静的ファイル レピュテーション ホストまたは代替ファイル レピュテーション クラウド サーバ プールの設定

ファイル レピュテーションは、ESA の GUI または CLI から設定できます。 このドキュメントに記載されている設定手順は、CLI 設定を示しています。 ただし、GUI で同じ手順および情報を適

用できます（ [Security Services] > [File Reputation and Analysis] > [Edit Global Settings...] > [Advanced Settings for File Reputation] ）。

AsyncOS 10.x 以降

AsyncOS 10.x の新機能により、ESA をプライベート レピュテーション クラウド（ オンプレミス ファイル レピュテーション サーバ ）またはクラウドベースのファイル レピュテーション サーバを使用するように設定できます。 この変更により、AMP の設定では「レピュテーション クラウド サーバプールの入力」の手順でホスト名を要求されなくなりました。 追加のファイル レピュテーション サーバをプライベート レピュテーション クラウドとして設定することを選択し、そのホスト名に公開キーを提供する必要があります。

10.0.x 以降では、代替 AMP レピュテーション サーバを設定する際に、そのホスト名に関連付けられた公開キーを入力する必要がある場合があります。

すべての AMP レピュテーション サーバは同じ公開キーを使用します。

```
-----BEGIN PUBLIC KEY-----
MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEchIap1VqPuGibM2n3wjfhqQZdzC9
WI1Z7QZ2Q7VesLe+A53TxYujeo7fCDKJEQKrPjU6kI36PSZusObr9Cur/g==
-----END PUBLIC KEY-----
```

次の例は代替ファイル レピュテーション サーバを cloud-sa.eu.amp.sourcefirce.com に設定する場合に役立ちます。

```
my11esa.local > ampconfig

NOTICE: This configuration command has not yet been configured for the current cluster mode
(Machine 122.local).

What would you like to do?
1. Switch modes to edit at mode "Cluster Test_cluster".
2. Start a new, empty configuration at the current mode (Machine 122.local).
3. Copy settings from another cluster mode to the current mode (Machine 122.local).
[1]>

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Adobe Portable Document Format (PDF)
Microsoft Office 2007+ (Open XML)
Microsoft Office 97-2004 (OLE)
Microsoft Windows / DOS Executable
Other potentially malicious file types
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.
- 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.sourcefire.com)
2. Private reputation cloud
[2]>

Enter AMP reputation server hostname or IP address?
[]> cloud-sa.eu.amp.sourcefire.com

Do you want to input new public key? [N]> y

Paste the public key followed by a . on a new line
-----BEGIN PUBLIC KEY-----
MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEchIap1VqPuGibM2n3wjfhqQZdzC9
WI1Z7QZ2Q7VesLe+A53TxYujeo7fCDKJEQKrPjU6kI36PSZusObr9Cur/g==
-----END PUBLIC KEY-----
.
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? [Y]>

Please make sure you have added the Amp onprem reputation server CA certificate in certconfig-
>CERTAUTHOROTIES->CUSTOM
Proxy server detail:
Server :
Port :
User :

Do you want to change proxy detail [N]>

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

設定変更を確定します。

AsyncOS 9.7.x 以前

次の AsyncOS 9.7.2-065 for Email Security の例は、代替レピュテーション クラウド サーバプールを cloud-sa.eu.amp.sourcefirce.com に設定する場合に役立ちます。

```
my97esa.local> ampconfig

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Adobe Portable Document Format (PDF)
Microsoft Office 2007+ (Open XML)
Microsoft Office 97-2004 (OLE)
Microsoft Windows / DOS Executable
Other potentially malicious file types
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]>

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

Enter reputation cloud server pool?
[cloud-sa.amp.sourcefire.com]> cloud-sa.eu.amp.sourcefire.com

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

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

Enter heartbeat interval?
[15]>

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

Proxy server detail:
Server :
Port :
User :

Do you want to change proxy detail [N]>
```

設定変更を確定します。

オンプレミス ファイル レピュテーション サーバ (FireAMP プライベート クラウド)

オンプレミス ファイル レピュテーション サーバ (FireAMP プライベート クラウドとも呼ばれる) の使用は、AsyncOS 10.x for Email Security から導入されました。

ネットワークに Cisco AMP 仮想プライベート クラウド アプライアンスを導入すると、パブリック レピュテーション クラウドに送信せずに、メッセージ添付ファイルのファイル レピュテーションを問い合わせることができます。 オンプレミス ファイル レピュテーション サーバを使用するようにアプライアンスを設定するには、『ESA User Guide』の「File Reputation Filtering and File Analysis」の章またはオンライン ヘルプを参照してください。

確認

このセクションでは、設定が正常に機能していることを確認します。

ファイル レピュテーション トラフィックが設定されている静的ホストまたはレピュテーション クラウド サーバプールにつながっていることを確認するには、指定されたフィルタを使用して ESA からパケット キャプチャを実行し、ポート 32137 またはポート 443 のトラフィックを取得します。

この例では、ポート 443 を使用して cloud-sa.eu.amp.sourcefire.com クラウド サーバプールと SSL 通信を使用します。

これは AMP ログで ESA に記録されます。

```
my97esa.local> ampconfig

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Adobe Portable Document Format (PDF)
Microsoft Office 2007+ (Open XML)
Microsoft Office 97-2004 (OLE)
Microsoft Windows / DOS Executable
Other potentially malicious file types
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]>

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

Enter reputation cloud server pool?
[cloud-sa.amp.sourcefire.com]> cloud-sa.eu.amp.sourcefire.com

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

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

Enter heartbeat interval?
[15]>

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

Proxy server detail:
Server :
Port :
User :

Do you want to change proxy detail [N]>
```

ESA パケット トレースの実行は次のメッセージ交換を取得しました。

```
my97esa.local> ampconfig

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Adobe Portable Document Format (PDF)
Microsoft Office 2007+ (Open XML)
Microsoft Office 97-2004 (OLE)
Microsoft Windows / DOS Executable
Other potentially malicious file types
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]>

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

Enter reputation cloud server pool?
[cloud-sa.amp.sourcefire.com]> cloud-sa.eu.amp.sourcefire.com

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

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

Enter heartbeat interval?
[15]>

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

Proxy server detail:
Server :
Port :
User :

Do you want to change proxy detail [N]>
```

トラフィックがポート 443 に通信することがわかります。 ESA (my11esa.local) から、トラフィックはホスト名 ec2-176-34-122-245.eu-west-1.compute.amazonaws.com と通信します。 このホスト名は、IP アドレス 176.34.122.245 に関連付けられています。

```
my97esa.local> ampconfig

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Adobe Portable Document Format (PDF)
Microsoft Office 2007+ (Open XML)
Microsoft Office 97-2004 (OLE)
```

```
Microsoft Windows / DOS Executable
Other potentially malicious file types
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]>

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

Enter reputation cloud server pool?
[cloud-sa.amp.sourcefire.com]> cloud-sa.eu.amp.sourcefire.com

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

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

Enter heartbeat interval?
[15]>

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

Proxy server detail:
Server :
Port :
User :

Do you want to change proxy detail [N]>
```

176.34.122.245 の IP アドレスは、cloud-sa.eu.amp.sourcefire.com の CNAME のプール メンバーです。

```
my97esa.local> ampconfig

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Adobe Portable Document Format (PDF)
Microsoft Office 2007+ (Open XML)
Microsoft Office 97-2004 (OLE)
Microsoft Windows / DOS Executable
Other potentially malicious file types
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]>

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

Enter reputation cloud server pool?
[cloud-sa.amp.sourcefire.com]> cloud-sa.eu.amp.sourcefire.com

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

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

Enter heartbeat interval?
[15]>

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

Proxy server detail:
Server :
Port :
User :

Do you want to change proxy detail [N]>
```

この例では、通信は設定されたレピュテーション クラウド サーバプール cloud-sa.eu.amp.sourcefire.com によって送られ、受け入れられました。

トラブルシューティング

このセクションでは、設定のトラブルシューティングに役立つ情報を提供します。

Telnet を使用した接続のテスト

ファイル レピュテーション クラウドへのポート レベルの接続を確認するには、設定されたレピュテーション クラウド サーバプールのホスト名を使用し、設定されたポート 32137 またはポート 443 への Telnet を使用してテストします。

```
my97esa.local> telnet cloud-sa.amp.sourcefire.com 443

Trying 23.21.208.4...
Connected to ec2-23-21-208-4.compute-1.amazonaws.com.
Escape character is '^]'.
^]
telnet> quit
Connection closed.
```

EU への接続を検証し、ポート 443 で成功しました。

```
my97esa.local> telnet cloud-sa.eu.amp.sourcefire.com 443

Trying 176.34.113.72...
Connected to ec2-176-34-113-72.eu-west-1.compute.amazonaws.com.
```

```
Escape character is '^]'.
^]
telnet> quit
Connection closed.
```
EU への接続を検証し、ポート 32137 で接続できませんでした。

```
my97esa.local> telnet cloud-sa.eu.amp.sourcefire.com 32137

Trying 176.34.113.72...
telnet: connect to address 176.34.113.72: Operation timed out
telnet: Unable to connect to remote host
```
同じ Telnet のテスト方法で、ポート 32137 またはポート 443 を使用して、レピュテーション クラウド サーバプールの CNAME の背後の直接 IP またはホスト名への Telnet をテストできます。 ホスト名およびポートへの Telnet を正常に実行できない場合は、ESA の外部のネットワーク接続とファイアウォール設定を確認する必要があります。

オンプレミス ファイル レピュテーション サーバへの Telnet の成功の検証は、示されているものと同じプロセスで行われます。

公開キーの入力

AsyncOS 10.x 以降を実行する ESA で公開キーを入力する場合は、公開キーが正常に貼り付けられていること、またはロードされていることを保証します。 公開キーのエラーは設定出力に表示されます。

```
my97esa.local> telnet cloud-sa.eu.amp.sourcefire.com 32137

Trying 176.34.113.72...
telnet: connect to address 176.34.113.72: Operation timed out
telnet: Unable to connect to remote host
```
エラーが表示された場合は、設定をもう一度行ってください。 永続的なエラーについては、シスコ サポートにお問い合わせください。

AMP ログの確認

ESA で AMP のログを表示する場合は、ファイル レピュテーション クエリ時に指定した「クラウドからのファイル レピュテーション クエリ」が表示されることを確認します。

```
my97esa.local> telnet cloud-sa.eu.amp.sourcefire.com 32137

Trying 176.34.113.72...
telnet: connect to address 176.34.113.72: Operation timed out
telnet: Unable to connect to remote host
```
これが表示される場合、クエリは設定されたレピュテーション クラウド サーバプールからではなく、ローカル ESA キャッシュから応答を取り込みました。

```
my97esa.local> telnet cloud-sa.eu.amp.sourcefire.com 32137

Trying 176.34.113.72...
telnet: connect to address 176.34.113.72: Operation timed out
telnet: Unable to connect to remote host
```

その他のエラーとアラート

ESA の管理者は次の通知を受けることがあります。 この通知を受け取った場合は、設定および検証プロセスを再度手順に従って行ってください。

```
my97esa.local> telnet cloud-sa.eu.amp.sourcefire.com 32137

Trying 176.34.113.72...
telnet: connect to address 176.34.113.72: Operation timed out
telnet: Unable to connect to remote host
```

関連情報

- 適切な AMP 操作に必要なサーバ アドレス
- テクニカル サポートとドキュメント – Cisco Systems