集約ポリシー、ウイルス、アウトブレイク隔離のセットアップと ESA から SMA への移行に関するベスト プラクティス

目次

概要

次の検疫を Cisco セキュリティ管理アプライアンス (SMA) にまとめて集約できるようになりました。

- ウイルス対策
- アウトブレーク
- 以下で捕捉されるメッセージに使用するポリシー隔離
  メッセージ フィルタコンテンツ フィルタデータ損失防止ポリシー

これらの隔離の中央集中化には次の利点があります。

- 管理者は複数の E メール セキュリティ アプライアンス (ESA) で隔離されたメッセージを 1 か所で管理できます。
- 隔離されたメッセージは、セキュリティ リスクを減らすために、DMZ の代わりに、ファイアウォールの内側に保存されます。
- SMA の標準のバックアップ機能の一部として、集約隔離をバック アップできます。

前提条件

- 8.1 を実行する SMA (SMA ユーザ ガイド、第 8 章、一元化されたポリシー、ウイルスおよびアウトブレイク隔離)
- 8.0.1 を実行する ESA (ESA ユーザ ガイド、第 27 章、検疫)
- ファイアウォール：ポート 7025/TCP (入出力) /ホスト名の使用： AsyncOS IP/説明： この機能を一元化する場合、E メール セキュリティ アプライアンスとセキュリティ管理アプライアンス間のポリシー、ウイルス、アウトブレイク検疫データを通過させます。

設定

ESA から、既存のポリシー隔離では、アクティブ メッセージがポリシー隔離に存在します。

これらのメッセージを移行し、ポリシー隔離を所有するアクティブ アプライアンスとして SMA に依存するには、次の手順を実行します。

SMA で、[Management Appliance] > [Centralized Services] > [Policy, Virus and Outbreak Quarantines] の順に移動します。 まだ有効になっていない場合は、[Enable] をクリックします。

ESA から SMA へのトラフィックを処理することを目的としているインターフェイスを必要に応じて選択します。

> **注:** 隔離ポートが変更される可能性がありますが、指定されたファイアウォール/ネットワーク ACL がある場合は、これを開く必要があります。

[Submit] をクリックします。 画面が更新され、「Service enabled」 メッセージが次のように表示されます。

[Management Appliance] > [Centralized Services] > [Security Appliances] の順に移動して、ESA 通信を SMA に追加します。

[Add Email Appliance] をクリックします。

> **注:** SMA が ESA との通信に使用する IP アドレスのみを追加する必要があります。 アプライアンス名は、管理目的でのみ使用されます。

接続を確立し、接続をテストします。 SMA の ESA への接続を確立すると、管理者のユーザ名とパスワードが要求されます。 これは、追加される ESA の管理者ユーザとパスワードです。 すでにアクティブなものと追加されているものに基づいてテストの結果は異なりますが、次のようになります。

この時点で SMA で必ず [Submit] と [Commit Changes] を実行します。

この時点で ESA を再度開いて、ポリシー隔離の集中型サービス セクションを設定しようとすると、次のようになります。

移行手順は、SMA で実行する必要があります。 SMA に戻り、次のセクションに進みます。

[Commit Changes] が完了すると、[Launch Migration Wizard]（Step 2）がアクティブになります。

[Launch Migration Wizard] を選択して次のように続行します。

特定の隔離だけを移行する場合は、[Custom] を選択します。 この例では、[Automatic] を使用して続行し、ANY/ALL ポリシー隔離を ESA から SMA. に移行します。 前述の ESA の追加中に選択した特定の名前が表示され、その後に通信で使用される IP アドレスが表示されます。

[Next] をクリックして続行します。

最後に、[Submit] をクリックすると、「成功」通知が表示されます。

SMA の変更をコミットします。

ESA に戻り、**[Security Services] > [Policy, Virus and Outbreak Quarantines] に移動します**。 これで、SMA の前提条件の手順が認識されます。

[Enable] をクリックして,続行します。

ここでもまた、通信に使用される適切なポートが示されます。 これらは一致している**必要があり**、ファイアウォールおよびネットワーク ACL が使用されている場合は、ESA と SMA 間の適切な移行を可能にするために開く必要があります。

> **注:** ESA でポリシー、ウイルス、およびアウトブレイク隔離を設定済みの場合、隔離およびすべてのメッセージの移行は、この変更を確定するとすぐに開始します。

> **注:** 一度に 1 つの移行プロセスだけしか処理できない可能性があります。 前の移行が完了する前に、別の E メール セキュリティ アプライアンスの集約ポリシー、ウイルス、およびアウトブレイク隔離を有効にしないでください。

[Submit] をクリックしてから、[Commit] をクリックします。 情報通知は同じようになります。 ローカルの隔離に多くのメッセージが存在すると、ESA から SMA への処理に時間がかかる可能性があります。

SMA にもう一度戻し、[Management Appliance] > [Centralized Services] > [Policy, Virus and Outbreak Quarantines] の順に移動します。 これで、移行手順は完了します。

確認

この時点で、ESA から SMA へのポリシー隔離の移行が完了しました。 最終確認のために、SMA のポリシー隔離を確認します。

最初に ESA で表示されたのと同じメッセージが表示されます。 メッセージ列の # のハイパーリンクを選択して確認します。

ESA の mail_logs を見ると、実際のメッセージの移行が表示されます。

> **注:** ESA （ XX.X.XX.XX X ）および間の通信の使用に SMA （ Y ）ポート 7025 による YY.Y.YY.YY 注意して下さい。

```
Wed Mar  5 02:48:40 2014 Info: New SMTP DCID 2 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:48:40 2014 Info: DCID 2 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:49:52 2014 Info: New SMTP DCID 3 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:49:52 2014 Info: DCID 3 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:50:22 2014 Info: New SMTP DCID 4 interface XX.X.XX.XXX address
```

```
YY.Y.YY.YYY port 7025
Wed Mar  5 02:50:22 2014 Info: DCID 4 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:50:23 2014 Info: New SMTP DCID 5 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:50:23 2014 Info: DCID 5 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:50:40 2014 Info: New SMTP DCID 6 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:50:40 2014 Info: DCID 6 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:50:41 2014 Info: New SMTP DCID 7 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:50:41 2014 Info: DCID 7 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:50:42 2014 Info: New SMTP DCID 8 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:50:42 2014 Info: DCID 8 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:51:01 2014 Info: New SMTP DCID 9 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:51:01 2014 Info: DCID 9 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:51:01 2014 Info: CPQ listener cpq_listener starting
Wed Mar  5 02:51:01 2014 Info: New SMTP DCID 10 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:51:01 2014 Info: DCID 10 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:51:02 2014 Info: New SMTP DCID 11 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:51:02 2014 Info: DCID 11 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:51:02 2014 Info: MID 1 enqueued for transfer to centralized quarantine
"Policy" (content filter _policy_q_in_)
Wed Mar  5 02:51:02 2014 Info: MID 1 queued for delivery
Wed Mar  5 02:51:02 2014 Info: New SMTP DCID 12 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:51:02 2014 Info: DCID 12 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:51:02 2014 Info: Delivery start DCID 12 MID 1 to RID [0] to Centralized
Policy Quarantine
Wed Mar  5 02:51:02 2014 Info: MID 2 enqueued for transfer to centralized quarantine
"Policy" (content filter _policy_q_in_)
Wed Mar  5 02:51:02 2014 Info: MID 2 queued for delivery
Wed Mar  5 02:51:02 2014 Info: MID 3 enqueued for transfer to centralized quarantine
"Policy" (content filter _policy_q_in_)
Wed Mar  5 02:51:02 2014 Info: MID 3 queued for delivery
Wed Mar  5 02:51:02 2014 Info: Message done DCID 12 MID 1 to RID [0] (centralized
policy quarantine)
Wed Mar  5 02:51:02 2014 Info: MID 1 RID [0] Response 'ok:  Message 1 accepted'
Wed Mar  5 02:51:02 2014 Info: Message finished MID 1 done
Wed Mar  5 02:51:02 2014 Info: MID 1 migrated from all quarantines
Wed Mar  5 02:51:02 2014 Info: Delivery start DCID 12 MID 2 to RID [0] to Centralized
Policy Quarantine
Wed Mar  5 02:51:02 2014 Info: New SMTP DCID 13 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:51:02 2014 Info: DCID 13 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:51:02 2014 Info: New SMTP DCID 14 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:51:02 2014 Info: DCID 14 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:51:02 2014 Info: Message done DCID 12 MID 2 to RID [0] (centralized
policy quarantine)
```

```
Wed Mar  5 02:51:02 2014 Info: MID 2 RID [0] Response 'ok:  Message 2 accepted'
Wed Mar  5 02:51:02 2014 Info: Message finished MID 2 done
Wed Mar  5 02:51:02 2014 Info: MID 2 migrated from all quarantines
Wed Mar  5 02:51:02 2014 Info: Delivery start DCID 12 MID 3 to RID [0] to Centralized
Policy Quarantine
Wed Mar  5 02:51:02 2014 Info: Message done DCID 12 MID 3 to RID [0] (centralized
policy quarantine)
Wed Mar  5 02:51:02 2014 Info: MID 3 RID [0] Response 'ok:  Message 3 accepted'
Wed Mar  5 02:51:02 2014 Info: Message finished MID 3 done
Wed Mar  5 02:51:02 2014 Info: MID 3 migrated from all quarantines
Wed Mar  5 02:51:02 2014 Info: New SMTP DCID 15 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:51:02 2014 Info: DCID 15 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:51:07 2014 Info: DCID 12 close
```

ESA を再度開いて、ポリシー、ウイルス、アウトブレイク隔離を表示すると、次のように表示されます。

確認の次の手順では、ポリシー隔離によって捕捉される ESA を経由して新しいテスト メッセージを送信します。 ESA の mail_logs を確認して、強調表示されている行に、ポリシー隔離を示す 7025 を経由した ESA から SMA への転送を認識します。

```
Wed Mar  5 02:57:47 2014 Info: Start MID 4 ICID 6
Wed Mar  5 02:57:47 2014 Info: MID 4 ICID 6 From: <robsherw.cisco@gmail.com>
Wed Mar  5 02:57:47 2014 Info: MID 4 ICID 6 RID 0 To: <robsherw@cisco.com>
Wed Mar  5 02:57:47 2014 Info: MID 4 Message-ID
'<7642E61C-4BA2-432E-A524-E163EA0B9753@gmail.com>'
Wed Mar  5 02:57:47 2014 Info: MID 4 Subject 'NEW FUNNY'
Wed Mar  5 02:57:47 2014 Info: MID 4 ready 525 bytes from
<robsherw.cisco@gmail.com>
Wed Mar  5 02:57:47 2014 Info: MID 4 matched all recipients for per-recipient
policy DEFAULT in the inbound table
Wed Mar  5 02:57:47 2014 Info: MID 4 enqueued for transfer to centralized
quarantine "Policy" (content filter _policy_q_in_)
Wed Mar  5 02:57:47 2014 Info: MID 4 queued for delivery
Wed Mar  5 02:57:47 2014 Info: New SMTP DCID 16 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:57:47 2014 Info: DCID 16 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:57:47 2014 Info: Delivery start DCID 16 MID 4 to RID [0] to Centralized
Policy Quarantine
Wed Mar  5 02:57:47 2014 Info: Message done DCID 16 MID 4 to RID [0] (centralized
policy quarantine)
Wed Mar  5 02:57:47 2014 Info: MID 4 RID [0] Response 'ok:  Message 4 accepted'
Wed Mar  5 02:57:47 2014 Info: Message finished MID 4 done
Wed Mar  5 02:57:52 2014 Info: DCID 16 close
```

SMA の前述のポリシー隔離に戻ると、新しいテスト メッセージも存在検疫されています。

関連情報

- ESA の一元化されたポリシー、ウイルスおよびアウトブレイク隔離（PVO）は有効にできません
- Cisco 電子メール セキュリティ アプライアンス - エンド ユーザ ガイド
- テクニカル サポートとドキュメント – Cisco Systems