Pratiques recommandées pour la stratégie centralisée, quarantaines de virus et d'épidémie installées et transfert d'ESA à SMA

Contenu

Introduction

Les quarantaines suivantes peuvent être maintenant collectivement centralisées sur une appliance de Gestion de sécurité Cisco (SMA) :

- Antivirus
- Épidémie
- Quarantaines de stratégie utilisées pour les messages par lesquels sont attrapés : Filtres de messageFiltres satisfaitsStratégies de prévention de perte de données

La centralisation de ces quarantaines offre les avantages suivants :

- Les administrateurs peuvent gérer les messages mis en quarantaine des plusieurs appliances de sécurité du courrier électronique (ESA) dans un emplacement.
- Des messages mis en quarantaine sont enregistrés derrière le Pare-feu au lieu de dans le DMZ, réduisant le risque de sécurité.
- Des quarantaines centralisées peuvent être sauvegardées en tant qu'élément de la fonctionnalité de sauvegarde standard sur le SMA.

Conditions préalables

- SMA exécutant 8.1 (guide utilisateur SMA, chapitre 8, stratégie centralisée, virus, et quarantaines d'épidémie)
- ESA exécutant 8.0.1 (le guide utilisateur ESA, le chapitre 27, met en quarantaine)
- Pare-feu - port 7025/TCP (dans et)/utilisation d'adresse Internet : AsyncOS IPS/description : Passez la stratégie, le virus, et les données de quarantaine d'épidémie entre les appliances de sécurité du courrier électronique et l'appliance de Gestion de la sécurité quand cette caractéristique est centralisée

Configurez

Commencent par l'ESA, dans une quarantaine de stratégie existante, là les messages actifs dans la quarantaine de stratégie :

Afin de migrer ces messages et puis compter sur le SMA pour être l'appliance active possédant la quarantaine de stratégie, terminez-vous les directions suivantes.

Sur le SMA, naviguez vers l'**appliance de Gestion > des services > des quarantaines centralisés de stratégie, de virus et d'épidémie**. Sinon activé déjà, **enable de** clic **:**

Sélectionnez l'interface, si c'est approprié, qui est destinée pour traiter le trafic de l'ESA au SMA.

> **Note**: Le port de quarantaine peut être changé, mais ceci devra être ouvert s'il y a un Pare-feu/d'ACL de réseau en place.

Cliquez sur **Submit**. L'écran régénérera pour afficher ? Service activé ? message, vu ci-dessous :

Naviguez vers l'**appliance de Gestion > des services > des dispositifs de sécurité centralisés** et ajoutez la transmission ESA au SMA :

Cliquez sur Add l'**appliance d'email**.

> **Note**: Vous devez seulement ajouter l'adresse IP que le SMA l'utilisera pour communiquer avec l'ESA. Le nom d'appareils est utilisé seulement comme référence administrative.

Soyez sûr **d'établir la connexion** et la **connexion de test**. Lors d'établir la connexion du SMA à l'ESA, le nom d'utilisateur et le mot de passe d'administrateur seront demandés. C'est l'utilisateur et le mot de passe administratifs de l'ESA qui est ajouté. Basé sur ce qui est déjà en activité contre ce qu'est ajouté, les résultats du test peuvent varier, mais devraient être semblables à :

Soyez sûr **de soumettre** et **commettre des modifications** en ce moment sur le SMA.

À ce moment, si vous deviez revisiter l'ESA et la tentative de configurer la section centralisée de services de la quarantaine de stratégie, il serait semblable à ce qui suit :

Les étapes de transfert doivent encore être terminées sur le SMA. Revenez au SMA et continuez la section suivante.

Une fois les **modifications de validation** est terminées, l'**assistant de transfert de lancement ?** de l'étape 2 deviendront actifs :

Sélectionnez l'**assistant de transfert de lancement** et continuez comme suit :

Si seulement une quarantaine particulière doit être migrée, choisissez la **coutume**. Dans cet exemple, nous continuerons **automatique**, qui migrera des quarantaines de stratégie ANY/ALL de l'ESA vers SMA. Veuillez noter que vous verrez le nom spécifié choisi pendant l'ESA pour ajouter

précédemment cité, suivi de l'adresse IP utilisée dans la transmission :

Cliquez sur Next, et continuez :

En conclusion, cliquez sur Submit, et la notification de « succès » est présentée :

Commettez vos modifications sur le SMA.

En retournant à l'ESA, naviguez vers des **Services de sécurité > des quarantaines de stratégie, de virus et d'épidémie**. Les étapes nécessaires sur le SMA sont maintenant identifiées :

Enable de clic ? , et continuez :

L'avis, cela ici de nouveau le port approprié utilisé pour la transmission est noté. Ceux-ci **doivent** s'assortir, et si l'ACL de Pare-feu/réseau est en service, doivent être ouverts afin de permettre le transfert approprié entre l'ESA et le SMA.

> **Note**: Si vous avez la stratégie, le virus, et les quarantaines d'épidémie configurées sur un ESA, le transfert des quarantaines et de tous leurs messages commence dès que vous commettrez cette modification.

> **Note**: Seulement un transfert de processus peut être en cours à tout moment. N'activez pas la stratégie centralisée, le virus, et les quarantaines d'épidémie sur une autre appliance de sécurité du courrier électronique jusqu'à ce que le transfert précédent soit complet.

Cliquez sur Submit, et cliquez sur finalement la **validation**. La notification de l'information devrait être semblable. S'il y a un grand nombre de messages déjà dans la quarantaine locale, ceux-ci peuvent prendre du temps de traiter de l'ESA à SMA :

Revisitez le SMA, et naviguez vers l'**appliance de Gestion > des services > des quarantaines centralisés de stratégie, de virus et d'épidémie**. Les étapes de transfert seront maintenant terminées :

Vérification

À ce moment, le transfert de la quarantaine de stratégie de l'ESA au SMA est complet. Pour la vérification finale, vérifiez la quarantaine de stratégie sur le SMA :

Vous devriez voir les mêmes messages qui ont été initialement répertoriés sur l'ESA. Sélectionnez # hyperlien dans la colonne de messages, et le vérifiez :

Si vous regardez les mail_logs sur l'ESA, le transfert des messages réels sera présenté :

> **Note**: Notez l'utilisation de transmission entre l'ESA (XX.X.XX.XX X) et SMA (YY.Y.YY.YY Y) par l'intermédiaire de port 7025.

```
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
```

Revisitez l'ESA, et ce qui suit est maintenant présenté en visualisant la stratégie, le virus, épidémie met en quarantaine :

L'étape suivante de la vérification envoie un nouveau message-test par l'ESA qui sera attrapé pour la quarantaine de stratégie. En regardant des mail_logs sur l'ESA, notez la ligne mise en surbrillance indiquer le transfert à partir de l'ESA à SMA par l'intermédiaire de 7025, en indiquant la quarantaine de stratégie :

```
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
```

Revisitez la quarantaine précédemment mentionnée de stratégie sur le SMA, le nouveau message-test est maintenant dedans quarantaine aussi bien :

Informations connexes

- La stratégie de centralisation ESA, le virus, et la quarantaine d'épidémie (PVO) ne peuvent pas être activés
- Appliance de sécurité du courrier électronique de Cisco - Guides d'utilisateur
- Support et documentation techniques - Cisco Systems