Melhores prática para a política centralizada, quarentena do vírus e da manifestação Setup e migração do ESA ao S A

Índice

Introdução

As seguintes quarentena podem agora coletivamente ser centralizadas em um dispositivo do Gerenciamento do Cisco Security (S A):

- Anti-vírus
- Manifestação
- Quarentena da política usadas para as mensagens por que são travados:
  Filtros da mensagemFiltros satisfeitosPolíticas de prevenção da perda de dados

Centralizar estas quarentena oferece os seguintes benefícios:

- Os administradores podem controlar mensagens quarantined das ferramentas de segurança múltiplas do email (ESA) em um lugar.
- As mensagens Quarantined são armazenadas atrás do Firewall em vez no DMZ, reduzindo o risco de segurança.
- As quarentena centralizadas podem ser suportadas como parte do backup de funcionalidade padrão no S A.

Pré-requisitos

- S A que executa 8.1 (Guia do Usuário S A, capítulo 8, política centralizada, vírus, e quarentena da manifestação)
- ESA que executa 8.0.1 (Guia do Usuário ESA, capítulo 27, quarentena)
- Porta de firewall 7025 /TCP (em e para fora)/uso do hostname: AsyncOS
  IPs/descrição: Passe a política, o vírus, e os dados da quarentena da manifestação entre ferramentas de segurança do email e o dispositivo do Gerenciamento de segurança quando esta característica é centralizada

Configurar

Está começando com o ESA, em uma quarentena da política existente, uns mensagens ativa na quarentena da política:

A fim migrar estas mensagens e confiar então no S A para ser o dispositivo ativo que possui a quarentena da política, termine os seguintes sentidos.

No S A, navegue ao **dispositivo do Gerenciamento > serviços > quarentena centralizados da política, do vírus e da manifestação**. Se não permitido já, o clique **permite:**

Selecione a relação, se aplicável, que é pretendida segurar o tráfego do ESA ao S A.

> Nota: A porta da quarentena pode ser mudada, mas esta deverá ser aberta se há um Firewall/rede ACL no lugar.

Clique em Submit. A tela refrescará para mostrar? Serviço permitido? mensagem, vista abaixo:

Navegue ao **dispositivo do Gerenciamento > dispositivos centralizados do > segurança dos serviços** e adicionar a comunicação ESA ao S A:

O clique **adiciona o dispositivo do email**.

> Nota: Você precisa somente de adicionar o endereço IP de Um ou Mais Servidores Cisco ICM NT que o S A se usará para comunicar com o ESA. O nome do dispositivo é usado somente como uma referência administrativa.

Seja certo **estabelecer a conexão** e a **conexão de teste**. Em cima de estabelecer a conexão do S A ao ESA, o nome e a senha de usuário do administrador serão pedidos. Esta é o usuário e a senha administrativos do ESA que está sendo adicionado. Baseado no que é já ativo contra o que está sendo adicionado, os resultados do teste podem variar, mas devem ser similares a:

Seja certo **submeter** neste momento e **comprometer mudanças no** S A.

Neste tempo, se você devia revisitar o ESA e tentar configurar a seção centralizada dos serviços da quarentena da política, seria similar ao seguinte:

As etapas da migração devem ainda ser terminadas no S A. Retorne ao S A e continue com a seguinte seção.

As mudanças comprometer são terminadas uma vez, o **assistente da migração do lançamento?** da etapa 2 tornar-se-ão ativos:

Selecione o **assistente da migração do lançamento** e continue como segue:

Se somente uma quarentena particular deve ser migrada, escolha o **costume**. Neste exemplo, nós continuaremos com **automático**, que migrará quarentena da política ANY/ALL do ESA ao S

A. Note por favor que você verá o nome especificado escolhido durante o ESA adicionar mencionado mais cedo, seguido pelo endereço IP de Um ou Mais Servidores Cisco ICM NT usado em uma comunicação:

Clique **em seguida**, e continue:

Finalmente, o clique **submete-se**, e a notificação do “sucesso” é apresentada:

Comprometa suas mudanças no S A.

Retornando ao ESA, navegue aos **Serviços de segurança > às quarentena da política, do vírus e da manifestação**. As etapas necessárias no S A são reconhecidas agora:

O clique **permite?** , e continue:

A observação, isso aqui a porta adequada usada para uma comunicação é notada outra vez. Estes **devem** combinar, e se o Firewall/rede ACL está no uso, devem ser abertos a fim permitir a migração apropriada entre o ESA e o S A.

> Nota: Se você tem a política, o vírus, e as quarentena da manifestação configuradas em um ESA, a migração das quarentena e das todas suas mensagens começa assim que você comprometer esta mudança.

> Nota: Somente um processo de migração pode ser em andamento a qualquer hora. Não permita a política centralizada, o vírus, e as quarentena da manifestação em uma outra ferramenta de segurança do email até que a migração precedente esteja completa.

O clique **submete-se**, e finalmente o clique **compromete**. A notificação de informação deve ser similar. Se há um grande número mensagens já na quarentena local, estes podem tomar o tempo processar do ESA ao S A:

Revisite o S A, e navegue ao **dispositivo do Gerenciamento > serviços > quarentena centralizados da política, do vírus e da manifestação**. As etapas da migração serão terminadas agora:

Verificação

Neste tempo, a migração da quarentena da política do ESA ao S A está completa. Para a verificação final, verifique a quarentena da política no S A:

Você deve ver as mesmas mensagens que foram alistadas originalmente no ESA. Selecione # hiperlink na coluna das mensagens, e verifique-o:

Se você olha os mail_logs no ESA, a migração dos mensagens reais estará apresentada:

> Nota: Note o uso de uma comunicação entre o ESA (XX.X.XX.XX X) e S A (YY.Y.YY.YY Y) através da porta 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
```

Revisite o ESA, e o seguinte é apresentado agora ao ver a política, o vírus, manifestação Quarantines:

A próxima etapa da verificação está enviando um mensagem de teste novo com o ESA que será travado para a quarentena da política. Olhando mail_logs no ESA, observe a linha destacada indicar transferência do ESA ao S A através de 7025, indicando a quarentena da política:

```
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
```

Revisite a quarentena previamente mencionada da política no S A, o mensagem de teste novo está agora na quarentena também:

Informações Relacionadas

- A política de centralização ESA, o vírus, e a quarentena da manifestação (PVO) não podem ser permitidos
- Cisco envia por correio eletrónico a ferramenta de segurança - Guias do utilizador final
- Suporte Técnico e Documentação - Cisco Systems