Transferências, atualizações ou elevações satisfeitas da ferramenta de segurança usando um host estático

Índice

Introdução

Este documento descreve o endereço IP de Um ou Mais Servidores Cisco ICM NT e hospeda-o necessário para configurar sua ferramenta de segurança do índice de Cisco para o uso com um host estático para transferências, atualizações, e elevações. Estas configurações devem ser usada para ou o hardware ou Cisco virtual envia por correio eletrónico a ferramenta de segurança (ESA), a ferramenta de segurança da Web (WSA), ou o dispositivo do Gerenciamento de segurança (S A).

Transferências, atualizações ou elevações satisfeitas da ferramenta de segurança usando um host estático

Cisco oferece host estáticos para os clientes que têm exigências restritas do Firewall ou do proxy. É importante notar que se você configura seu dispositivo para usar os host estáticos para transferências e atualizações, os mesmos host estáticos para transferências e as atualizações devem ser permitidas no Firewall e no proxy na rede também.

Estão aqui os hostname, os endereços IP de Um ou Mais Servidores Cisco ICM NT, e as portas estáticos que são envolvidas na transferência, na atualização, e nos processos de upgrade:

- downloads-static.ironport.com 208.90.58.105 (porta 80)
- updates-static.ironport.com 208.90.58.25 (porta 80)184.94.240.106 (porta 80)

Preste serviços de manutenção à configuração da atualização

através do GUI

Termine estas etapas a fim mudar a transferência, a atualização, ou a configuração da elevação em AsyncOS do GUI:

1. Navegue à página de configuração dos ajustes da atualização WSA: **Ajustes da administração do sistema > da elevação e da atualização**ESA: **Serviços de segurança > atualizações do serviço**S A: **Ajustes da administração do sistema > da atualização**
2. O clique **edita ajustes da atualização….**
3. *Nos server da atualização (imagens)* secione, selecione “os server locais da atualização (lugar de arquivos de imagem da atualização)”.
4. Para o campo *URL da base*, entre em http://downloads-static.ironport.com e para o campo de *porta*, grupo para a porta **80**.
5. Saa dos campos *(opcionais) da autenticação* vazios.
6. (*) ESA somente - Para o *host (as definições anti-vírus da McAfee, as atualizações do motor PXE, as definições anti-vírus de Sophos, as regras do Anti-Spam de IronPort, as regras dos filtros da manifestação, as atualizações DLP, as regras da zona de hora (fuso horário) e o cliente do registro (usados para buscar Certificados para a Filtragem URL)* colocam, entram em **updates-static.ironport.com**. (A porta 80 é opcional.)
7. Deixe a seção dos *server da atualização (lista)* e coloque-a ajustado toda aos server da atualização de Cisco IronPort do padrão.
8. Assegure-se de que você tenha a relação selecionada como necessária para uma comunicação externa, se for necessário para comunicar-se sobre uma relação específica. A configuração padrão será ajustada ao **automóvel seleta**.
9. Verifique e atualize os servidores proxy configurados, se for necessário.
10. Clique em Submit.
11. No canto superior direito, o clique **compromete mudanças**.
12. Finalmente, clique sobre **mudanças Commit** outra vez a fim confirmar todas as alterações de configuração.

Continue à seção da verificação deste documento.

Configuração do updateconfig através do CLI

As mesmas mudanças podem ser aplicadas através do CLI no dispositivo. Termine estas etapas a fim mudar a transferência, a atualização, ou a configuração da elevação em AsyncOS do CLI:

1. Execute o **updateconfig do** comando CLI.
2. Entre no comando setup.
3. A primeira seção apresentada para configurar é “chave de recurso atualiza”. Uso “**2. Use para possuir o server**” e para entrar em http://downloads-static.ironport.com:80/.
4. (*) ESA somente - A segunda seção apresentada para configurar é “serviço (imagens)”. Uso “**2. Use para possuir o server**” e para entrar em **updates-static.ironport.com**.
5. Todos prompts de configuração restantes podem ser deixados ajustados para optar.
6. Assegure-se de que você tenha a relação selecionada como necessária para uma comunicação externa, se for necessário para comunicar-se sobre uma relação específica. A configuração padrão será ajustada ao **automóvel**.
7. Verifique e atualize o servidor proxy configurado, se for necessário.

8. Bata o retorno para ir para trás à alerta principal CLI.
9. Execute o comando CLI **COMPROMETEM** para salvar todas as alterações de configuração.

Continue à seção da verificação deste documento.

Verificação

Atualizações

Para a verificação das atualizações no dispositivo é o melhor validar do CLI.

Do CLI:

1. Execute o **updatenow**. (*) ESA somente - você pode executar a **força do updatenow** para ter todos os serviços e a regra ajusta a atualização.
2. Execute **updater_logs da cauda**.

Você quererá pagar a toda atenção às seguintes linhas "http://updates-static.ironport.com/.." Isto deve sinalizar uma comunicação e a transferência com o server estático do updater.

Exemplo, de um ESA que atualiza o motor de Cisco Antispam (CASO) e regras associadas:

```
Wed Aug 2 09:22:05 2017 Info: case was signalled to start a new update
Wed Aug 2 09:22:05 2017 Info: case processing files from the server manifest
Wed Aug 2 09:22:05 2017 Info: case started downloading files
Wed Aug 2 09:22:05 2017 Info: case waiting on download lock
Wed Aug 2 09:22:05 2017 Info: case acquired download lock
Wed Aug 2 09:22:05 2017 Info: case beginning download of remote file "http://updates-
static.ironport.com/case/2.0/case/default/1480513074538790"
Wed Aug 2 09:22:07 2017 Info: case released download lock
Wed Aug 2 09:22:07 2017 Info: case successfully downloaded file
"case/2.0/case/default/1480513074538790"
Wed Aug 2 09:22:07 2017 Info: case waiting on download lock
Wed Aug 2 09:22:07 2017 Info: case acquired download lock
Wed Aug 2 09:22:07 2017 Info: case beginning download of remote file "http://updates-
static.ironport.com/case/2.0/case_rules/default/1501673364679194"
Wed Aug 2 09:22:10 2017 Info: case released download lock
<<<SNIP FOR BREVITY>>>
```

Enquanto o serviço se comunica, transferências, e então com sucesso atualizações, você está ajustado.

Uma vez que a atualização do serviço é terminada, os updater_logs mostrarão:

```
Wed Aug 2 09:22:50 2017 Info: case started applying files
Wed Aug 2 09:23:04 2017 Info: case cleaning up base dir [bindir]
Wed Aug 2 09:23:04 2017 Info: case verifying applied files
Wed Aug 2 09:23:04 2017 Info: case updating the client manifest
Wed Aug 2 09:23:04 2017 Info: case update completed
Wed Aug 2 09:23:04 2017 Info: case waiting for new updates
```

Atualizações

A fim verificar que a comunicação da elevação é bem sucedida e termina, navegue à página da **elevação do sistema** e clique **elevações disponíveis**. Se a lista de indicadores disponíveis das versões, então sua instalação está completa.

Do CLI, você pode simplesmente executar o **comando upgrade**. Escolha a opção da

transferência ver a elevação manifesta, se há umas elevações disponíveis.

```
myesa.local> upgrade


Choose the operation you want to perform:
- DOWNLOADINSTALL - Downloads and installs the upgrade image (needs reboot).
- DOWNLOAD - Downloads the upgrade image.
[]> download

Upgrades available.
1. AsyncOS 9.6.0 build 051 upgrade For Email, 2015-09-02 this release is for General Deployment
2. AsyncOS 9.7.0 build 125 upgrade For Email, 2015-10-15. This release is for General Deployment
3. AsyncOS 9.7.1 build 066 upgrade For Email, 2016-02-16. This release is for General
Deployment.
4. cisco-sa-20150625-ironport SSH Keys Vulnerability Fix
[4]>
```

Troubleshooting

Atualizações

O dispositivo envia alertas da notificação quando as atualizações falham. Está aqui um exemplo da notificação de Email o mais geralmente recebida:

```
The updater has been unable to communicate with the update server for at least 1h.

Last message occurred 4 times between Tue Mar 1 18:02:01 2016 and Tue Mar 1 18:32:03 2016.

Version: 9.7.1-066
Serial Number: 888869DFCCCC-3##CV##
Timestamp: 01 Mar 2016 18:52:01 -0500
```

Você quererá testar uma comunicação do dispositivo ao server especificado do updater. Nesta instância, nós somos estados relacionados com downloads-static.ironport.com. Usando o telnet, o dispositivo deve ter uma comunicação aberta sobre a porta 80:

```
myesa.local> telnet downloads-static.ironport.com 80

Trying 208.90.58.105...
Connected to downloads-static.ironport.com.
Escape character is '^]'.
```

Igualmente, o mesmos devem ser vistos para updates-static.ironport.com:

```
> telnet updates-static.ironport.com 80

Trying 208.90.58.25...
Connected to origin-updates.ironport.com.
Escape character is '^]'.
```

Se seu dispositivo tem interfaces múltiplas, você pode desejar executar o **telnet do** CLI, e especifica a relação, a fim validar que a interface adequada está selecionada:

```
> telnet

Please select which interface you want to telnet from.
1. Auto
2. Management (172.18.249.120/24: myesa.local)
[1]>

Enter the remote hostname or IP address.
```

```
[]> downloads-static.ironport.com

Enter the remote port.
[25]> 80

Trying 208.90.58.105...
Connected to downloads-static.ironport.com.
Escape character is '^]'.
```

Atualizações

Ao tentar promover, você pode ver a seguinte resposta:

```
No available upgrades. If the image has already been downloaded it has been de-provisioned from the upgrade server. Delete the downloaded image, if any and run upgrade.
```

Você quererá rever a versão de AsyncOS que está sendo executado no dispositivo e rever igualmente os Release Note da versão de AsyncOS a que você está promovendo. É possível que não há um caminho de upgrade da versão que você está executando à versão você está tentando promover a.

Se você está promovendo a uma correção de programa quente (HP), ao Early Deployment (ED), ou à versão de AsyncOS da distribuição limitada (LD), você pode precisar de abrir um caso de suporte a fim pedir o abastecimento apropriado é terminado, para que seu dispositivo ver o caminho de upgrade como necessário.

Informações Relacionadas

- Cisco envia por correio eletrónico a ferramenta de segurança - Release Note
- Ferramenta de segurança da Web de Cisco - Release Note
- Dispositivo do Gerenciamento do Cisco Security - Release Note
- Suporte Técnico e Documentação - Cisco Systems