Content Security Appliance: download, aggiornamenti o upgrade tramite un host statico

Sommario

Introduzione

In questo documento vengono descritti gli indirizzi IP e gli host necessari per configurare l'appliance Cisco Content Security in modo da poterla utilizzare con un host statico per download, aggiornamenti e aggiornamenti. Queste configurazioni devono essere utilizzate per l'hardware o per Cisco Email Security Appliance (ESA), Web Security Appliance (WSA) o Security Management Appliance (SMA) virtuale.

Content Security Appliance: download, aggiornamenti o upgrade tramite un host statico

Cisco offre host statici per i clienti con rigorosi requisiti di firewall o proxy. È importante notare che se si configura l'accessorio per l'utilizzo di host statici per download e aggiornamenti, gli stessi host statici per download e aggiornamenti devono essere consentiti anche nel firewall e nel proxy di rete.

Nomi host statici, indirizzi IP e porte coinvolti nei processi di download, aggiornamento e aggiornamento:

- 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)

Configurazione aggiornamento servizi tramite GUI

Completare questa procedura per modificare la configurazione di download, aggiornamento o aggiornamento su AsyncOS dalla GUI:

1. Passare alla pagina di configurazione delle impostazioni di aggiornamento WSA: **Amministrazione sistema > Impostazioni aggiornamento**ESA: **Servizi di sicurezza > Aggiornamenti dei servizi**SMA: **Amministrazione sistema > Impostazioni aggiornamento**
2. Fare clic su **Modifica impostazioni aggiornamento...**.
3. Nella sezione *Server di aggiornamento (immagini)*, selezionare "Server di aggiornamento locali (percorso dei file immagine di aggiornamento)".
4. Per il campo *URL di base*, immettere in http://downloads-static.ironport.com e per il campo *Porta*, impostare per la porta **80**.
5. Lasciare vuoti i campi *Autenticazione (facoltativo)*.
6. (*) Solo ESA: per il campo *Host (definizioni di McAfee Anti-Virus, aggiornamenti del motore PXE, definizioni di Sophos Anti-Virus, regole di IronPort Anti-Spam, regole dei filtri epidemie, aggiornamenti DLP, regole per il fuso orario e client di registrazione (utilizzato per recuperare i certificati per il filtro URL)*, immettere **updates-static.ironport.com**. (la porta 80 è opzionale).
7. Lasciare la sezione *Update Servers (elenco)* e i campi impostati sui Cisco IronPort Update Servers predefiniti.
8. Accertarsi di aver selezionato l'interfaccia necessaria per la comunicazione esterna, se necessario per comunicare su un'interfaccia specifica. La configurazione predefinita verrà impostata su **Selezione automatica**.
9. Verificare e aggiornare i server proxy configurati, se necessario.
10. Fare clic su **Invia**.
11. Nell'angolo superiore destro fare clic su **Conferma modifiche**.
12. Infine, fare di nuovo clic su **Commit delle modifiche** per confermare tutte le modifiche alla configurazione.

Procedere alla sezione Verifica di questo documento.

Configurazione di updateconfig dalla CLI

Le stesse modifiche possono essere applicate tramite la CLI sull'accessorio. Completare questi passaggi per modificare la configurazione di download, aggiornamento o aggiornamento su AsyncOS dalla CLI:

1. Eseguire il comando CLI **updateconfig**.
2. Immettere il comando **SETUP**.
3. La prima sezione da configurare è "Aggiornamenti chiave funzionalità". Usare '**2. Usare il proprio server**' e immettere http://downloads-static.ironport.com:80/.
4. (*) Solo ESA: la seconda sezione da configurare è "Servizio (immagini)". Utilizzare '**2. Utilizzare un server proprio**' e immettere **updates-static.ironport.com**.
5. Tutti gli altri prompt di configurazione possono essere lasciati impostati sui valori predefiniti.
6. Accertarsi di aver selezionato l'interfaccia necessaria per la comunicazione esterna, se necessario per comunicare su un'interfaccia specifica. La configurazione predefinita sarà impostata su **Auto** (Automatico).
7. Verificare e aggiornare il server proxy configurato, se necessario.
8. Premere INVIO per tornare al prompt della CLI principale.
9. Eseguire il comando **COMMIT** della CLI per salvare tutte le modifiche alla configurazione.

Procedere alla sezione Verifica di questo documento.

Verifica

Aggiornamenti

Per la verifica degli aggiornamenti sull'accessorio è consigliabile eseguire la convalida dalla CLI.

Dalla CLI:

1. Eseguire **updatenow**. (*) Solo ESA: è possibile eseguire **updatenow force** per aggiornare tutti i servizi e i set di regole.
2. Eseguire **tail updater_logs**.

Prestare particolare attenzione alle seguenti righe "http://updates-static.ironport.com/..." Ciò dovrebbe segnalare la comunicazione e il download con il server di aggiornamento statico.

Ad esempio, da un'ESA che aggiorna il Cisco Antispam Engine (CASE) e le regole associate:

```
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>>>
```

L'impostazione è valida a condizione che il servizio comunichi, venga scaricato e quindi venga aggiornato correttamente.

Al termine dell'aggiornamento del servizio, i log_updater visualizzeranno:

```
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
```

Aggiornamenti

Per verificare che la comunicazione relativa all'aggiornamento sia stata completata, passare alla pagina **Aggiornamento sistema** e fare clic su **Aggiornamenti disponibili**. Se viene visualizzato l'elenco delle versioni disponibili, l'installazione è completata.

Dalla CLI, è possibile eseguire semplicemente il comando **upgrade**. Scegliere l'opzione **download** per visualizzare il manifesto di aggiornamento, se sono disponibili aggiornamenti.

```
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]>
```

Risoluzione dei problemi

Aggiornamenti

Quando gli aggiornamenti non vengono completati, l'accessorio invia un messaggio di avviso. Di seguito è riportato un esempio della notifica e-mail ricevuta più di frequente:

```
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
```

Si desidera verificare la comunicazione tra l'accessorio e il server di aggiornamento specificato. In questo caso, siamo interessati a with downloads-static.ironport.com. Se si utilizza telnet, l'accessorio deve avere una comunicazione aperta sulla porta 80:

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

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

Analogamente, lo stesso vale per 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 l'accessorio dispone di più interfacce, è possibile eseguire **telnet** dalla CLI e specificare l'interfaccia per verificare che sia selezionata l'interfaccia corretta:

```
> 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 '^]'.
```

Aggiornamenti

Quando si tenta di eseguire l'aggiornamento, è possibile che venga visualizzata la risposta seguente:

```
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.
```

Si desidera esaminare la versione di AsyncOS in esecuzione sull'accessorio e le note sulla versione di AsyncOS a cui si sta eseguendo l'aggiornamento. È possibile che non esista un percorso di aggiornamento dalla versione in esecuzione alla versione a cui si sta tentando di eseguire l'aggiornamento.

Se si sta eseguendo l'aggiornamento a una versione di AsyncOS Hot Patch (HP), Early Deployment (ED) o Limited Deployment (LD), potrebbe essere necessario aprire una richiesta di assistenza per richiedere il corretto provisioning in modo che l'appliance possa visualizzare il percorso di aggiornamento in base alle esigenze.

Informazioni correlate

- Cisco Email Security Appliance - Note di rilascio
- Cisco Web Security Appliance - Note di rilascio
- Cisco Security Management Appliance - Note sulla release
- Documentazione e supporto tecnico – Cisco Systems