Nota tecnica sulle domande frequenti (FAQ) sull'accesso remoto su Cisco ESA/WSA/SMA

Sommario

Introduzione

Questo documento contiene le risposte alle domande frequenti sull'utilizzo dell'accesso remoto da parte del supporto tecnico Cisco sulle appliance Cisco Content Security. tra cui Cisco Email Security Appliance (ESA), Cisco Web Security Appliance (WSA) e Cisco Security Management Appliance (SMA).

Prerequisiti

Componenti usati

Le informazioni fornite in questo documento si basano sui dispositivi Cisco Content Security che eseguono qualsiasi versione di AsyncOS.

Cos'è l'accesso remoto?

L'accesso remoto è una connessione Secure Shell (SSH) abilitata da un'appliance Cisco Content Security a un host sicuro in Cisco. Solo l'assistenza clienti Cisco può accedere all'accessorio una volta abilitata una sessione remota. L'accesso remoto consente al Supporto Clienti Cisco di analizzare un accessorio. Il supporto consente di accedere all'accessorio tramite un tunnel SSH

creato con questa procedura tra l'accessorio e il server upgrades.ironport.com.

Funzionamento dell'accesso remoto

Quando si avvia una connessione di accesso remoto, l'accessorio apre una porta protetta, casuale e ad alta sorgente tramite una connessione SSH sull'accessorio alla porta configurata/selezionata uno dei seguenti server Cisco Content Security:

Indirizzo IP	Nome host	Utilizzo
63.251.108.107	upgrades.ironport.com	Tutte le appliance di sicurezza dei contenuti
63.251.108.107	c.tunnels.ironport.com	Appliance serie C (ESA)
63.251.108.107	x.tunnels.ironport.com	Appliance serie X (ESA)
63.251.108.107	m.tunnels.ironport.com	Appliance serie M (SMA)
63.251.108.107	s.tunnels.ironport.com	Appliance serie S (WSA)

Èimportante notare che potrebbe essere necessario configurare un firewall del cliente per consentire le connessioni in uscita a uno dei server sopra elencati. Se nel firewall è attivata l'ispezione del protocollo SMTP, il tunnel non verrà stabilito. Le porte che Cisco accetterà di connettere dall'accessorio per l'accesso remoto sono:

- 22
- 25 (Predefinito)
- 53
- 80
- 443
- 4766

La connessione di accesso remoto viene effettuata a un nome host e non a un indirizzo IP hardcoded. Per stabilire la connessione in uscita, è necessario configurare il DNS (Domain Name Server) sull'accessorio.

Su una rete del cliente, alcuni dispositivi di rete compatibili con il protocollo potrebbero bloccare la connessione a causa di una mancata corrispondenza tra il protocollo e la porta. Alcuni dispositivi compatibili con SMTP (Simple Mail Transport Protocol) possono inoltre interrompere la connessione. In caso di dispositivi con riconoscimento del protocollo o connessioni in uscita bloccate, potrebbe essere necessario utilizzare una porta diversa da quella predefinita (25). L'accesso all'estremità remota del tunnel è limitato solo al supporto clienti Cisco. Controllare il firewall o la rete per verificare se sono presenti connessioni in uscita quando si tenta di stabilire o risolvere problemi relativi alle connessioni di accesso remoto per l'accessorio.

> **Nota:** Quando un tecnico dell'assistenza Cisco è collegato all'accessorio tramite accesso remoto, sul prompt del sistema dell'accessorio viene visualizzato *(SERVIZIO)*.

Come abilitare l'accesso remoto

> **Nota:** Consultare il Manuale dell'utente dell'accessorio e della versione di AsyncOS per istruzioni su come abilitare l'accesso remoto per il personale del supporto tecnico Cisco.

> **Nota:** Gli allegati inviati tramite e-mail a attach@cisco.com potrebbero non essere sicuri.

Support Case Manager è l'opzione sicura preferita da Cisco per caricare le informazioni nella richiesta. Per ulteriori informazioni sulla protezione e le limitazioni relative alle dimensioni di altre opzioni di caricamento file: Caricamento di file die clienti su Cisco Technical Assistance Center

Identificare una porta raggiungibile da Internet. Il valore predefinito è la porta 25, che funziona nella maggior parte degli ambienti perché il sistema richiede anche l'accesso generale su quella porta per inviare messaggi e-mail. Le connessioni su questa porta sono consentite nella maggior parte delle configurazioni del firewall.

CLI

Per stabilire una connessione di accesso remoto tramite la CLI, come utente Admin, attenersi alla seguente procedura:

1. Immettere il comando **supporto tecnico**
2. Scegli **TUNNEL**
3. Scegliere di generare o *immettere* una stringa di origine casuale
4. Specificare il numero di porta per la connessione
5. Rispondere "**Y**" per abilitare l'accesso al servizio

L'accesso remoto verrà attivato in questo momento. A questo punto, l'appliance è in grado di stabilire una connessione sicura con l'host secure bastion di Cisco. Fornire il numero di serie dell'accessorio e la stringa iniziale generata al tecnico TAC che supporta la richiesta.

GUI

Per stabilire una connessione di accesso remoto tramite la GUI, come utente Admin, attenersi alla seguente procedura:

1. Selezionare **Guida e supporto tecnico > Accesso remoto** (per ESA, SMA), **Supporto e Guida > Accesso remoto** (per WSA)
2. Fare clic su **Attiva**
3. Scegliere il metodo per la stringa di origine
4. Selezionare la casella di controllo *Avvia connessione tramite tunnel protetto* e specificare il numero di porta per la connessione
5. Fare clic su **Submit (Invia).**

L'accesso remoto verrà attivato in questo momento. A questo punto, l'appliance è in grado di stabilire una connessione sicura con l'host secure bastion di Cisco. Fornire il numero di serie dell'accessorio e la stringa iniziale generata al tecnico TAC che supporta la richiesta.

Come disabilitare l'accesso remoto

CLI

1. Immettere il comando **supporto tecnico**
2. Scegliere **DISABILITA**
3. Rispondere "**S**" quando richiesto "Disabilitare l'accesso al servizio?"

GUI

1. Selezionare **Guida e supporto tecnico > Accesso remoto** (per ESA, SMA), **Supporto e Guida > Accesso remoto** (per WSA).
2. Fare clic su **Disabilita**
3. Nell'output della GUI viene visualizzato "Operazione riuscita — Accesso remoto disabilitato"

Verifica della connettività di accesso remoto

Utilizzare questo esempio per eseguire un test iniziale della connettività tra l'accessorio e Cisco:

```
example.run> > telnet upgrades.ironport.com 25

Trying 63.251.108.107...
Connected to 63.251.108.107.
Escape character is '^]'.
SSH-2.0-OpenSSH_6.2 CiscoTunnels1
```

La connettività può essere verificata per una qualsiasi delle porte elencate sopra: 22, 25, 53, 80, 443 o 4766. Se la connettività non riesce, potrebbe essere necessario eseguire un'acquisizione dei pacchetti per individuare il punto in cui si è verificato un errore di connessione dall'accessorio o dalla rete.

Perché l'accesso remoto non funziona sull'SMA?

L'accesso remoto potrebbe non essere abilitato su uno SMA se lo SMA viene inserito nella rete locale senza accesso diretto a Internet. In questo caso, l'accesso remoto può essere abilitato su un'ESA o un WSA, mentre l'accesso SSH può essere abilitato sull'SMA. In questo modo, il supporto Cisco può connettersi tramite accesso remoto a ESA/WSA e quindi da ESA/WSA all'SMA tramite SSH. Ciò richiede la connettività tra ESA/WSA e SMA sulla porta 22.

> **Nota:** Consultare il Manuale dell'utente dell'accessorio e la versione di AsyncOS per istruzioni su come abilitare l'accesso remoto agli accessori senza una connessione Internet diretta.

CLI

Per stabilire una connessione di accesso remoto tramite la CLI, come utente Admin, attenersi alla seguente procedura:

1. Immettere il comando **supporto tecnico**
2. Scegli **SSHACCESS**
3. Scegliere di generare o *immettere* una stringa di origine casuale
4. Rispondere **"Y"** per abilitare l'accesso al servizio

L'accesso remoto verrà attivato in questo momento. L'output CLI visualizzerà la stringa di inizializzazione. Fornire questa informazione al tecnico di assistenza Cisco. L'output CLI mostra anche lo stato della connessione e i dettagli dell'accesso remoto, incluso il numero di serie dell'accessorio. Fornire questo numero di serie al tecnico di assistenza.

GUI

Per stabilire una connessione di accesso remoto tramite la GUI, come utente Admin, attenersi alla seguente procedura:

1. Selezionare **Guida e supporto tecnico > Accesso remoto** (per ESA, SMA), **Supporto e Guida > Accesso remoto** (per WSA)
2. Fare clic su **Attiva**
3. Scegliere il metodo per la stringa di origine
4. NON selezionare la casella di controllo *Avvia connessione tramite tunnel protetto*
5. Fare clic su **Submit (Invia).**

L'accesso remoto verrà attivato in questo momento. Nell'output della GUI viene visualizzato un messaggio di riuscita e la stringa di inizializzazione dell'accessorio. Fornire questa informazione al tecnico di assistenza Cisco. L'output dell'interfaccia utente mostra anche lo stato della connessione e i dettagli dell'accesso remoto, incluso il numero di serie dell'accessorio. Fornire questo numero di serie al tecnico di assistenza.

Come disabilitare l'accesso remoto quando è abilitato per SSHACCESS

La procedura per disabilitare l'accesso remoto per SSHACCESS è la stessa di quella descritta sopra.

Risoluzione dei problemi

Se l'accessorio non è in grado di abilitare l'accesso remoto e collegarsi a upgrades.ironport.com tramite una delle porte elencate, sarà necessario eseguire un'operazione di acquisizione dei pacchetti direttamente dall'accessorio per verificare la causa dell'errore della connessione in uscita.

> **Nota:** Consultare il Manuale dell'utente dell'accessorio e della versione di AsyncOS per istruzioni su "Esecuzione di un'acquisizione pacchetto".

Il tecnico dell'assistenza Cisco può richiedere che il file .pcap venga fornito per consentire la revisione e la risoluzione dei problemi.

Informazioni correlate

- Domande frequenti ESA: Quali sono i livelli di accesso amministrativo disponibili per l'ESA?
- Cisco Email Security Appliance - Supporto dei prodotti
- Cisco Web Security - Supporto dei prodotti
- Supporto dei prodotti Cisco Content Security Appliance
- Documentazione e supporto tecnico – Cisco Systems