Domande frequenti sulla sicurezza dei contenuti: Come si accede alla CLI su un'appliance di sicurezza dei contenuti?

Sommario

Introduzione

In questo documento viene descritto come accedere alla CLI tramite un client Telnet o Secure Shell (SSH) su un'appliance Cisco Content Security.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Email Security Appliance (ESA)
- Cisco Web Security Appliance (WSA)
- Cisco Security Management Appliance (SMA)
- AsyncOS

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco ESA AsyncOS, tutte le versioni
- Cisco WSA AsyncOS, tutte le versioni
- Cisco SMA versioni AsyncOS, tutte le versioni

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali

conseguenze derivanti dall'uso dei comandi.

> **Nota:** Il presente documento fa riferimento a software non gestito o supportato da Cisco. Le informazioni sono fornite a titolo di cortesia. Per ulteriore assistenza, contattare il fornitore del software.

Come si accede alla CLI su un'appliance di sicurezza dei contenuti?

Èpossibile accedere alla CLI dell'accessorio tramite un client Telnet o SSH. Poiché il protocollo Telnet non è crittografato, quando si accede all'accessorio tramite Telnet è più facile che le credenziali vengano rubate.

Cisco consiglia a tutti i computer di produzione di utilizzare un client SSH. Inoltre, il client Microsoft Windows Telnet standard è difficile da utilizzare. Per impostazione predefinita, Telnet è configurato sulla porta di gestione.

Completare questa procedura per disabilitare Telnet:

1. Accedere alla GUI Web.
2. Selezionare **Rete > Interfacce IP**.
3. Fare clic sul nome dell'interfaccia che si desidera modificare.
4. Deselezionare la casella di controllo **Telnet** nel campo Servizi.

Per accedere all'accessorio tramite SSH (porta 22), completare la procedura seguente:

1. Installare un client SSH in Microsoft Windows, ad esempio PuTTY.
2. Avviare il client SSH:

   Aggiungere le informazioni sull'host relative all'accessorio (ad esempio **c650.example.com**).

   Fare clic su **Carica**.

   Immettere il nome utente.

   Immettere la password.
3. Aprire un prompt dei comandi con ***nix**.
4. Immettere il comando **$ ssh exampleC650.com**.
5. Per specificare un utente diverso, immettere il comando **$ ssh <user>@exampleC650.com**.

Se il nome utente è **admin**, immettere il comando **$ ssh admin@C650.example.com**.

Per accedere all'accessorio in modalità Telnet, effettuare le seguenti operazioni:

Nota: Cisco consiglia di utilizzare un client SSH per l'accesso; si sconsiglia di utilizzare Telnet.

1. Aprire un prompt dei comandi.
2. Immettere il comando **telnet c650.example.com**.
3. Immettere il nome utente.
4. Immettere la password.