Filtra il traffico destinato ai dispositivi Cisco IOS XE WebUI utilizzando un elenco degli accessi

Sommario

Introduzione

Prerequisiti

- Requisiti
- Componenti usati
- Introduzione

Configurazione

- Configurazione classe di accesso al servizio HTTP
- Esempio di IPv4
- Esempio di IPv6

Verifica

D: Dopo aver applicato l'elenco degli accessi, riceverò una risposta 403 anziché nessuna risposta. Perché?

Introduzione

In questo documento viene descritto come configurare un elenco degli accessi (ACL) su un dispositivo Cisco IOS XE per filtrare il traffico destinato ai servizi Web.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Questo documento è destinato ai dispositivi aziendali con software Cisco IOS® XE.

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.

Introduzione

Quando i servizi Web HTTP devono essere abilitati per disporre dell'accesso webUI per gestire il dispositivo IOS XE o per l'accesso utente webauth/guest, è possibile implementare le funzionalità di filtro del traffico per garantire che solo gli indirizzi IP necessari possano accedere a WebUI e

che gli utenti guest possano continuare a essere collegati alla rete.

Configurazione

Configurazione classe di accesso al servizio HTTP

Il metodo più semplice per definire l'accesso può essere eseguito tramite il supporto della classe di accesso IP sul server Web HTTP. In questo esempio di configurazione, la subnet ipv4 192.168.10.0/24 è consentita, la subnet ipv6 fd00::/64 è consentita e tutti gli altri elementi sono negati. Alla fine dell'elenco degli accessi è presente un'istruzione implicita di rifiuto, ma è possibile aggiungere un'istruzione esplicita di rifiuto, anche se lo si desidera. Nel caso del controller LAN wireless C9800, considerare sempre l'accesso HTTP/HTTPS a WMI (Wireless Management Interface) e alla porta di gestione/servizio fuori banda.

Esempio di IPv4

Passaggio 1. Configurare un ACL standard e includere i dispositivi/subnet attendibili a cui è consentito accedere al dispositivo Cisco IOS XE tramite HTTP/HTTPS

```
ip access-list standard restrict_ipv4_webui
permit 192.168.10.0 0.0.0.255
```

Nota: questo ACL deve includere solo subnet sicure per poter accedere come amministratore Web al dispositivo IOS XE. Vale a dire, tutte le subnet guest non devono essere incluse in questo ACL. L'esclusione delle subnet guest non compromette l'autenticazione, l'accesso guest o il reindirizzamento Web.

Passaggio 2. Assegnare l'ACL standard alla classe di accesso del servizio Web HTTP.

```
ip http access-class ipv4 restrict_ipv4_webui
```

Esempio di IPv6

Passaggio 1. Configurare un ACL IPv6 per includere i dispositivi/le subnet attendibili a cui è consentito accedere al dispositivo Cisco IOS XE tramite HTTP/HTTPS

```
ipv6 access-list restrict_ipv6_webui
permit fd00::/64 any
```

Passaggio 2. Assegnare l'ACL standard alla funzionalità del servizio Web HTTP.

```
ip http access-class ipv6 restrict_ipv6_webui
```

Verifica

Controllare le voci dell'ACL IPv4

```
show ip access-list restrict_ipv4_webui
Standard IP access list restrict_ipv4_webui
10 permit 192.168.10.0 0.0.0.255
```

Controllare le voci ACL IPv6

```
show ipv6 access restrict_ipv4_webui
IPv6 access list restrict_ipv6_webui
permit ipv6 FD00::/64 any sequence 10
```

D: Dopo aver applicato l'elenco degli accessi, riceverò una risposta 403 anziché nessuna risposta. Perché?

R: Questo è il comportamento previsto. L'elenco ACL è progettato per limitare gli utenti autorizzati ad accedere al processo http/https. Una risposta 403 indica che l'accesso a questa risorsa non è consentito e rappresenta la risposta corretta in questo scenario, in quanto l'elenco degli accessi viene applicato al processo HTTP/HTTPS anziché a un elenco degli accessi a livello di interfaccia. Se l'elenco degli accessi è stato applicato a un'interfaccia invece che al processo HTTP/HTTPS, la risposta appropriata non è nessuna

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).