Sicurezza porta sugli switch Cisco Business 220

Obiettivo

In questo articolo vengono illustrate le opzioni per la sicurezza delle porte sugli switch Cisco Business serie 220.

Dispositivi interessati | Versione firmware

- Serie CBS220 (DataSheet) | 2.0.0.17

Introduzione

Èpossibile aumentare la sicurezza di rete limitando l'accesso su una porta a utenti con indirizzi MAC specifici. Gli indirizzi MAC possono essere appresi in modo dinamico o configurati in modo statico. I monitor di sicurezza delle porte hanno ricevuto e appreso pacchetti. L'accesso alle porte bloccate è limitato agli utenti con indirizzi MAC specifici.

Non è possibile abilitare la sicurezza delle porte sulle porte su cui è abilitato 802.1X o sulle porte definite come destinazione SPAN.

Port Security può funzionare in due modalità:

- **Classic Lock**: tutti gli indirizzi MAC appresi sulla porta sono bloccati e la porta non rileva nuovi indirizzi MAC. Gli indirizzi appresi non sono soggetti ad invecchiamento o riapprendimento.
- **Blocco dinamico limitato**: il dispositivo apprende gli indirizzi MAC fino al limite configurato di indirizzi consentiti. Una volta raggiunto il limite, il dispositivo non impara altri indirizzi. In questa modalità, gli indirizzi sono soggetti a aging e riprogrammazione.

Quando viene rilevato un frame da un nuovo indirizzo MAC su una porta non autorizzata (la porta è bloccata in modo classico ed è presente un nuovo indirizzo MAC oppure la porta è bloccata in modo dinamico ed è stato superato il numero massimo di indirizzi consentiti), viene richiamato il meccanismo di protezione ed è possibile eseguire una delle azioni seguenti:

- Frame scartato.
- Frame inoltrato.
- Il frame viene scartato e viene generato un messaggio SYSLOG.
- La porta è chiusa.

Quando l'indirizzo MAC sicuro viene visualizzato su un'altra porta, il frame viene inoltrato, ma l'indirizzo MAC non viene appreso su quella porta.

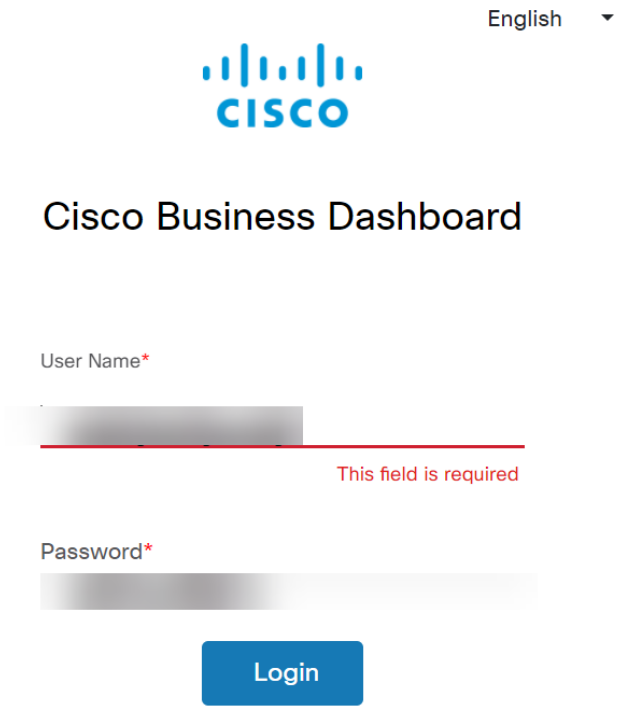
Oltre a una di queste azioni, è possibile generare trap e limitarne la frequenza e il

numero per evitare di sovraccaricare i dispositivi.

Configura sicurezza porta

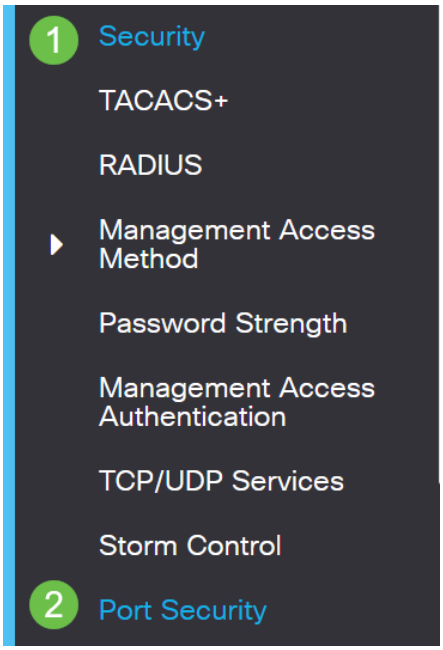
Passaggio 1

Accedere all'interfaccia utente Web.



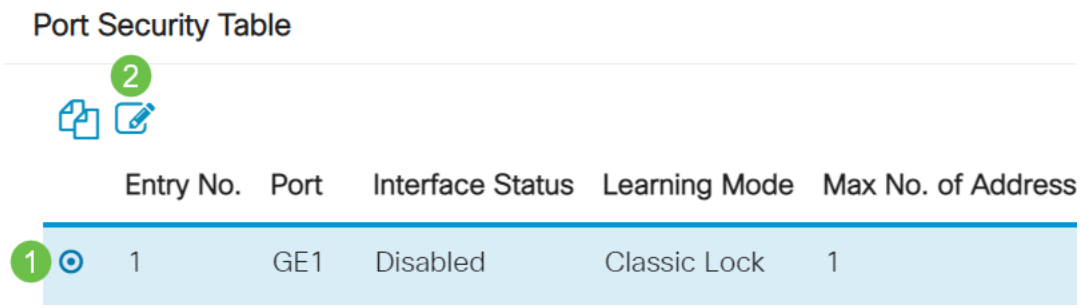
Passaggio 2

Dal menu a sinistra, selezionare **Sicurezza > Sicurezza porta**.



Passaggio 3

Selezionare l'interfaccia da modificare, quindi fare clic sull'**icona Modifica**.

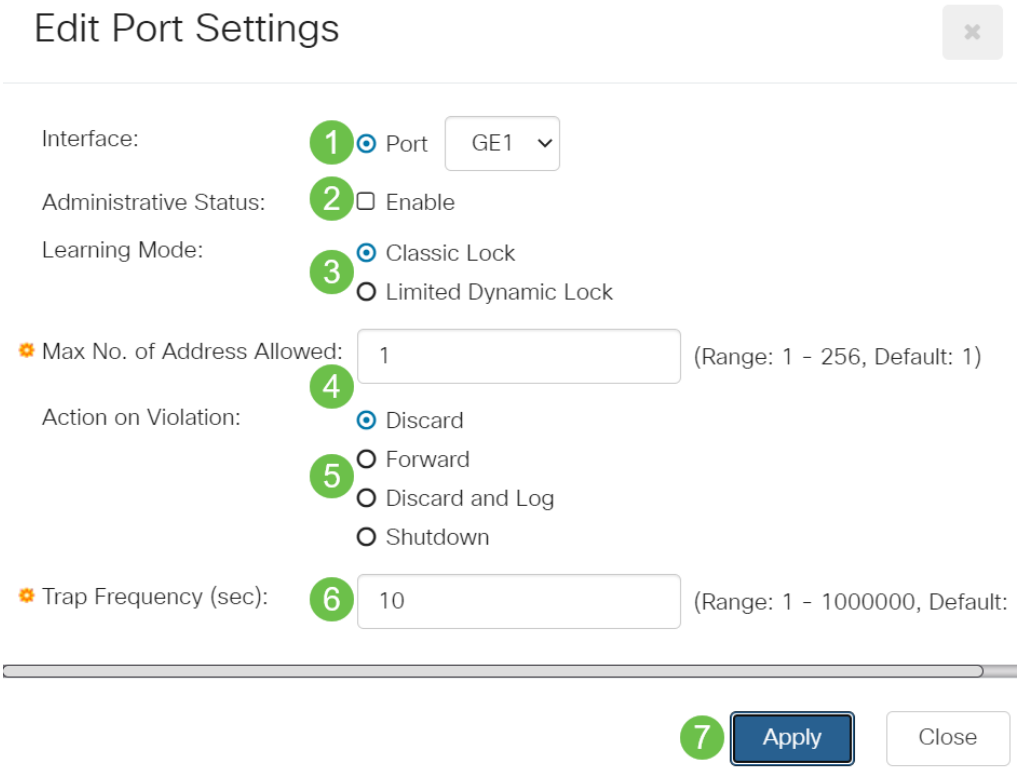


Passaggio 4

Immettere i parametri.

- **Interfaccia (Interface)** - Selezionate il nome dell'interfaccia.
- **Stato amministrativo (Administrative Status)** - Selezionate questa opzione per bloccare la porta.
- **Modalità apprendimento (Learning Mode)** - Consente di selezionare il tipo di blocco delle porte. Per configurare questo campo, è necessario sbloccare lo stato dell'interfaccia. Il campo Modalità di apprendimento è abilitato solo se il campo Stato interfaccia è bloccato. Per modificare la modalità di apprendimento, è necessario deselezionare l'opzione Blocca interfaccia. Una volta modificata la modalità, è possibile ripristinare l'interfaccia Lock. Le opzioni sono:
    - **Classic Lock**: blocca la porta immediatamente, indipendentemente dal numero di indirizzi che sono già stati appresi.
    - **Blocco dinamico limitato (Limited Dynamic Lock)** - Blocca la porta eliminando gli indirizzi MAC dinamici correnti associati alla porta. La porta apprende fino al numero massimo di indirizzi consentiti sulla porta. Sono abilitati sia il riapprendimento che la misurazione della durata degli indirizzi MAC.
- **N. max indirizzi consentiti**: immettere il numero massimo di indirizzi MAC che è possibile apprendere sulla porta se è selezionata la modalità di apprendimento Blocco dinamico limitato. Il numero 0 indica che l'interfaccia supporta solo indirizzi statici.
- **Azione in caso di violazione**: selezionare un'azione da applicare ai pacchetti in arrivo su una porta bloccata. Le opzioni sono:
    - **Discard**: scarta i pacchetti da qualsiasi origine non individuata ·
    - **Forward**: inoltra i pacchetti da un'origine sconosciuta senza conoscere l'indirizzo MAC
    - **Discard and Log** - Elimina i pacchetti da qualsiasi origine non riconosciuta, chiude l'interfaccia, registra gli eventi e invia trap ai ricevitori trap specificati. Shutdown - Elimina i pacchetti da qualsiasi origine non identificata e chiude la porta. La porta rimane chiusa finché non viene riattivata o finché il dispositivo non viene riavviato.
    - **Frequenza trap**: immettere il tempo minimo (in secondi) che deve trascorrere tra le trap

Fare clic su **Apply** (Applica).



Se si desidera visualizzare un esempio del comportamento predefinito per la sicurezza delle porte sul CBS220, selezionare Comportamento di sicurezza porta.

Conclusioni

Èsemplice come quello. Una rete sicura!

Per ulteriori configurazioni, fare riferimento al Cisco Business serie 220 Switch Administration Guide.

Per visualizzare altri articoli, consultare la pagina di supporto degli switch Cisco Business serie 220.