Protezione della sicurezza della rete e concessione dell'accesso a terze parti

Sommario

Introduzione

Nel corso di questa richiesta di assistenza, è possibile che si desideri che i tecnici Cisco accedano alla rete dell'organizzazione. La concessione di tale accesso consente spesso di risolvere la richiesta di assistenza in modo più rapido. In questi casi, Cisco può accedere alla rete, e lo farà solo, con la tua autorizzazione.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Procedure ottimali

Cisco consiglia di attenersi a queste linee guida per proteggere la sicurezza della rete quando si concede l'accesso a un tecnico o a una persona esterna all'azienda o all'organizzazione.

- Se possibile, utilizzare Cisco Unified MeetingPlace per condividere le informazioni con i

tecnici dell'assistenza. Cisco consiglia di utilizzare Cisco Unified MeetingPlace per i seguenti motivi:Cisco Unified MeetingPlace utilizza il protocollo SSL (Secure Socket Layer), che in alcuni casi è più sicuro rispetto al protocollo SSH (Secure Shell) o Telnet.Cisco Unified MeetingPlace non richiede l'immissione di password a utenti esterni alla società o all'organizzazione.**Nota:** ogni volta che si concede l'accesso alla rete a persone esterne alla società o all'organizzazione, le password specificate devono essere temporanee e valide solo se richieste da terzi.In genere, Cisco Unified MeetingPlace non richiede la modifica dei criteri del firewall perché la maggior parte dei firewall aziendali consente l'accesso HTTPS in uscita.Per ulteriori informazioni, visitare Cisco Unified MeetingPlace.

- Se non è possibile utilizzare Cisco Unified MeetingPlace e si sceglie di consentire l'accesso di terze parti tramite un'altra applicazione, ad esempio SSH, verificare che la password sia temporanea e disponibile solo per un utilizzo unico. Inoltre, è necessario modificare o invalidare immediatamente la password quando l'accesso di terze parti non è più necessario. Se si utilizza un'applicazione diversa da Cisco Unified MeetingPlace, è possibile seguire le seguenti procedure e linee guida:Per creare un account temporaneo sui router Cisco IOS, utilizzare questo comando:
  ```
  Router(config)#username tempaccount secret QWE!@#
  ```

  Per creare un account temporaneo su PIX/ASA, usare questo comando:
  ```
  PIX(config)#username tempaccount password QWE!@#
  ```

  Per rimuovere l'account temporaneo, utilizzare questo comando:
  ```
  Router (config)#no username tempaccount
  ```

  Generare la password temporanea in modo casuale. La password temporanea non deve essere correlata alla richiesta di servizio o al provider di servizi di supporto specifico. Ad esempio, non utilizzare password come *cisco*, *cisco123* o *ciscotac*.Non fornire mai il proprio nome utente o password.Non utilizzare Telnet su Internet. Non è sicuro.
- Se il dispositivo Cisco che richiede supporto si trova dietro un firewall aziendale e se un tecnico dell'assistenza deve modificare le policy del firewall per introdurlo nel dispositivo Cisco, verificare che la modifica apportata alla policy sia specifica del tecnico dell'assistenza assegnato al problema. Non aprire mai l'eccezione al criterio all'intero Internet o a un intervallo di host più ampio del necessario.Per modificare un criterio firewall su un firewall Cisco IOS, aggiungere queste righe all'elenco degli accessi in entrata in Interfaccia con connessione Internet:
  ```
  Router(config)#ip access-list ext inbound
  Router(config-ext-nacl)#1 permit tcp host
      <IP address for TAC engineer> host <Cisco device address> eq 22
  ```

  Nota: nell'esempio, la configurazione `Router(config-ext-nacl)#` viene visualizzata su due righe per preservare spazio. Tuttavia, quando si aggiunge questo comando all'elenco degli accessi in entrata, la configurazione deve essere visualizzata su una riga.Per modificare un criterio firewall su un firewall Cisco PIX/ASA, aggiungere questa riga al gruppo di accesso in entrata:
  ```
  ASA(config)#access-list inbound line 1 permit tcp host
      <IP address for TAC engineer> host <Cisco device address> eq 22
  ```

  Nota: nell'esempio, la configurazione `ASA(config)#` viene visualizzata su due righe per preservare spazio. Tuttavia, quando si aggiunge questo comando al gruppo di accesso in entrata, la configurazione deve essere visualizzata su una sola riga.Per consentire l'accesso SSH sui router Cisco IOS, aggiungere questa riga alla classe access-class:

```
Router(config)#access-list 2 permit host <IP address for TAC engineer>
Router(config)#line vty 0 4
Router(config-line)#access-class 2
```

Per consentire l'accesso SSH su Cisco PIX/ASA, aggiungere questa configurazione:

```
ASA(config)#ssh <IP address for TAC engineer> 255.255.255.255 outside
```

Per domande o ulteriore assistenza sulle informazioni descritte in questo documento, contattare il Technical Assistance Center (TAC) di Cisco.

Questa pagina Web ha solo scopo informativo e viene fornita "così com'è" senza alcuna garanzia o concessione. Le procedure ottimali sopra descritte non sono concepite per essere complete, ma sono consigliate per integrare le procedure di sicurezza correnti dei clienti. L'efficacia di qualsiasi prassi di sicurezza dipende dalla situazione specifica di ciascun cliente; e i clienti sono incoraggiati a considerare tutti i fattori rilevanti nella determinazione delle procedure di sicurezza più appropriate per le loro reti.

Informazioni correlate

- Cisco Unified MeetingPlace
- Software Cisco PIX Firewall
- Riferimenti per i comandi di Cisco Secure PIX Firewall
- Avvisi sui prodotti per la sicurezza (inclusi PIX)
- Cisco Technical Assistance Center (TAC)
- RFC (Requests for Comments)
- Documentazione e supporto tecnico – Cisco Systems