# Netwerkbeveiliging beschermen en toegang aan derden verlenen

## Inhoud



## Inleiding

Tijdens het verloop van deze servicegaanvraag kunt u ervoor kiezen dat Cisco-engineers toegang hebben tot het netwerk van uw organisatie. Door deze toegang te verlenen, kan uw serviceverzoek vaak sneller worden opgelost. In dergelijke gevallen kan en zal Cisco uw netwerk alleen met uw toestemming benaderen.

## Voorwaarden

### Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

### Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

### Conventies

Raadpleeg Cisco Technical Tips Convention voor informatie over documentconventies.

## Beste praktijken

Cisco raadt u aan deze richtlijnen te volgen om u te helpen de veiligheid van uw netwerk te beschermen wanneer u toegang verleent tot een ondersteuningsingenieur of persoon buiten uw bedrijf of organisatie.

- Gebruik indien mogelijk Cisco Unified MeetingPlace om informatie met de steuningenieurs te

delen. Cisco raadt u aan om Cisco Unified MeetingPlace om deze redenen te gebruiken:Cisco Unified MeetingPlace gebruikt het Secure Socket Layer (SSL)-protocol, dat in sommige gevallen veiliger is dan Secure Shell (SSH) of Telnet.Cisco Unified MeetingPlace vereist u niet wachtwoorden aan om het even wie buiten uw bedrijf of organisatie te verstrekken.**N.B.:** Wanneer u netwerktoegang verleent aan personen buiten uw bedrijf of organisatie, moeten wachtwoorden die u verschaft, tijdelijke wachtwoorden zijn die alleen geldig zijn zolang de derde toegang tot uw netwerk vereist.Meestal vereist Cisco Unified MeetingPlace u niet om uw firewallbeleid te veranderen omdat de meeste ondernemingsfirewalls toegang tot HTTPS toestaan.Bezoek Cisco Unified MeetingPlace voor meer informatie.

- Als u geen Cisco Unified MeetingPlace kunt gebruiken en als u ervoor kiest om toegang van derden door een andere toepassing, zoals SSH, toe te staan, zorg dan dat het wachtwoord tijdelijk is en alleen beschikbaar voor eenmalig gebruik. Daarnaast moet u het wachtwoord onmiddellijk wijzigen of ongeldig maken nadat de toegang van derden niet langer nodig is. Als u een andere toepassing dan Cisco Unified MeetingPlace gebruikt, kunt u deze procedures en richtlijnen volgen:Om een tijdelijke account op Cisco IOS-routers te maken, gebruikt u deze opdracht:

  ```
  Router(config)#username tempaccount secret QWE!@#
  ```

  Gebruik deze opdracht om een tijdelijke account op PIX/ASA aan te maken:

  ```
  PIX(config)#username tempaccount password QWE!@#
  ```

  Gebruik deze opdracht om de tijdelijke account te verwijderen:

  ```
  Router (config)#no username tempaccount
  ```

  genereren willekeurig het tijdelijke wachtwoord. Het tijdelijke wachtwoord mag niet gekoppeld zijn aan het specifieke serviceverzoek of de specifieke dienstverlener. Gebruik bijvoorbeeld geen wachtwoorden zoals *cisco*, *cisco123* of *ciscotac*.Geef nooit uw eigen naam of wachtwoord op.Gebruik Telnet niet via het internet. Het is niet zeker.
- Als het Cisco-apparaat dat ondersteuning vereist, zich achter een bedrijfsfirewall bevindt en het firewallbeleid moet worden gewijzigd bij een ondersteuningsingenieur om naar SSH in het Cisco-apparaat te kunnen stappen, zorg er dan voor dat de beleidswijziging specifiek is voor de ondersteuningsingenieur die aan de kwestie is toegewezen. Maak de beleidsuitzondering nooit open voor het hele internet of voor een breder scala aan hosts dan nodig.Als u een firewallbeleid op een Cisco IOS-firewall wilt wijzigen, voegt u deze lijnen toe aan de inkomende toegangslijst onder de interface 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
  ```

  **Opmerking:** In dit voorbeeld wordt de `configuratie` van de `router (-Tekst-Nacl)#` op twee lijnen weergegeven om ruimte te besparen. Wanneer u deze opdracht aan de inkomende toegangslijst toevoegt, moet de configuratie echter op één regel verschijnen.Als u een firewallbeleid op een Cisco PIX/ASA firewall wilt wijzigen, voegt u deze regel toe aan de inkomende toegangsgroep:

  ```
  ASA(config)#access-list inbound line 1 permit tcp host
      <IP address for TAC engineer> host <Cisco device address> eq 22
  ```

  **Opmerking:** In dit voorbeeld wordt de `ASA (configuratie)#` configuratie op twee lijnen weergegeven om ruimte te besparen. Wanneer u deze opdracht aan de inkomende toegangsgroep toevoegt, moet de configuratie echter op één regel verschijnen.Om SSH-

toegang op Cisco IOS-routers toe te staan, voegt u deze regel toe aan de toegangsklasse:

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

U kunt SSH-toegang op Cisco PIX/ASA toestaan door deze configuratie toe te voegen:

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

Als u vragen hebt over of extra assistentie nodig hebt bij de informatie die in dit document wordt beschreven, neem dan contact op met het Cisco Technical Assistance Center (TAC).

Deze webpagina is alleen bedoeld voor informatiedoeleinden en wordt op 'zoals hij is'-basis geleverd zonder garantie of garantie. De hierboven beschreven beste praktijken zijn niet bedoeld om volledig te zijn, maar worden voorgesteld om de huidige beveiligingsprocedures van klanten aan te vullen. De effectiviteit van elke beveiligingspraktijk hangt af van de specifieke situatie van elke klant; en klanten worden aangemoedigd alle relevante factoren in aanmerking te nemen bij het bepalen van beveiligingsprocedures die het meest geschikt zijn voor hun netwerken .

## Gerelateerde informatie

- Cisco Unified MeetingPlace
- Cisco PIX-firewallsoftware
- Opdrachtreferenties van Cisco Secure PIX-firewall
- Security meldingen uit het veld (inclusief PIX)
- Cisco Technical Assistance Center (TAC)
- Verzoeken om opmerkingen (RFC's)
- Technische ondersteuning en documentatie – Cisco Systems