Schutz der Netzwerksicherheit bei der Gewährung des Zugriffs an Dritte

Inhalt

Einleitung

Im Verlauf dieser Serviceanfrage können Sie möchten, dass Cisco Techniker auf das Netzwerk Ihres Unternehmens zugreifen. Wenn Sie einen solchen Zugriff gewähren, kann Ihre Serviceanfrage häufig schneller bearbeitet werden. In solchen Fällen kann und wird Cisco nur mit Ihrer Erlaubnis auf Ihr Netzwerk zugreifen.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Konventionen

Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Best Practices

Cisco empfiehlt, diese Richtlinien zu befolgen, um die Sicherheit Ihres Netzwerks zu gewährleisten, wenn Sie Support-Technikern oder Personen außerhalb Ihres Unternehmens oder Unternehmens Zugang gewähren.

- Verwenden Sie Cisco Unified MeetingPlace, wenn möglich, um Informationen mit Support-Technikern auszutauschen. Cisco empfiehlt die Verwendung von Cisco Unified MeetingPlace aus folgenden Gründen:Cisco Unified MeetingPlace verwendet das Secure Socket Layer (SSL)-Protokoll, das in einigen Fällen sicherer ist als Secure Shell (SSH) oder Telnet.Bei Cisco Unified MeetingPlace müssen Sie niemandem außerhalb Ihres Unternehmens Passwörter zuweisen.**Hinweis:** Wenn Sie Personen außerhalb Ihres Unternehmens oder Ihrer Organisation Netzwerkzugriff gewähren, müssen alle von Ihnen bereitgestellten Kennwörter temporäre Kennwörter sein, die nur gültig sind, solange der Drittanbieter Zugriff auf Ihr Netzwerk benötigt.In der Regel müssen Sie für Cisco Unified MeetingPlace keine Firewall-Richtlinien ändern, da die meisten Firewalls der Enterprise-Klasse ausgehenden HTTPS-Zugriff zulassen.Weitere Informationen finden Sie unter Cisco Unified MeetingPlace.
- Wenn Sie Cisco Unified MeetingPlace nicht verwenden können und den Zugriff von Drittanbietern über eine andere Anwendung, z. B. SSH, zulassen möchten, stellen Sie sicher, dass das Kennwort temporär und nur für die einmalige Verwendung verfügbar ist. Darüber hinaus müssen Sie das Passwort sofort ändern oder ungültig machen, wenn kein Drittanbieterzugriff mehr erforderlich ist. Wenn Sie eine andere Anwendung als Cisco Unified MeetingPlace verwenden, können Sie die folgenden Verfahren und Richtlinien befolgen:Verwenden Sie den folgenden Befehl, um ein temporäres Konto auf Cisco IOS-Routern zu erstellen:
  ```
  Router(config)#username tempaccount secret QWE!@#
  ```

  Um ein temporäres Konto auf PIX/ASA zu erstellen, verwenden Sie den folgenden Befehl:
  ```
  PIX(config)#username tempaccount password QWE!@#
  ```

  Um das temporäre Konto zu entfernen, verwenden Sie den folgenden Befehl:
  ```
  Router (config)#no username tempaccount
  ```

  Generieren Sie das temporäre Kennwort zufällig. Das temporäre Kennwort darf nicht mit dem jeweiligen Service Request oder Anbieter von Support Services in Zusammenhang stehen. Verwenden Sie beispielsweise keine Kennwörter wie *cisco*, *cisco123* oder *ciscotac*.Geben Sie niemals Ihren eigenen Benutzernamen oder Ihr eigenes Kennwort an.Verwenden Sie Telnet nicht über das Internet. Es ist nicht sicher.
- Wenn sich das Cisco Gerät, für das Support erforderlich ist, hinter einer Firewall des Unternehmens befindet und ein Support-Techniker eine Änderung der Firewall-Richtlinien für SSH auf dem Cisco Gerät vornehmen muss, stellen Sie sicher, dass die Richtlinienänderung auf den Support-Techniker abgestimmt ist, der dem Problem zugewiesen ist. Machen Sie die Richtlinienausnahme niemals für das gesamte Internet oder für eine größere Bandbreite von Hosts offen als erforderlich.Um eine Firewall-Richtlinie auf einer Cisco IOS-Firewall zu ändern, fügen Sie diese Zeilen unter "Internetschnittstelle" zur Liste für eingehende Zugriffe hinzu:
  ```
  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
  ```

  Hinweis: In diesem Beispiel wird die `Router(config-ext-nacl)#`-Konfiguration in zwei Zeilen angezeigt, um Platz zu sparen. Wenn Sie diesen Befehl jedoch der Liste für eingehende Zugriffe hinzufügen, muss die Konfiguration in einer Zeile angezeigt werden.Um eine Firewall-Richtlinie auf einer Cisco PIX/ASA-Firewall zu ändern, fügen Sie diese Zeile der eingehenden Zugriffsgruppe hinzu:

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

Hinweis: In diesem Beispiel wird die `ASA(config)#`-Konfiguration in zwei Zeilen angezeigt, um Platz zu sparen. Wenn Sie diesen Befehl jedoch der eingehenden Zugriffsgruppe hinzufügen, muss die Konfiguration in einer Zeile angezeigt werden.Um den SSH-Zugriff auf Cisco IOS-Router zuzulassen, fügen Sie diese Zeile der Zugriffsklasse hinzu:

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

Fügen Sie folgende Konfiguration hinzu, um den SSH-Zugriff auf Cisco PIX/ASA zuzulassen:

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

Wenn Sie Fragen zu den in diesem Dokument beschriebenen Informationen haben oder weitere Unterstützung benötigen, wenden Sie sich an das Cisco Technical Assistance Center (TAC).

Diese Webseite dient lediglich zu Informationszwecken und wird "wie besehen" ohne Garantie oder Garantie bereitgestellt. Die oben genannten Best Practices sind nicht vollständig, sondern sollen die aktuellen Sicherheitsverfahren der Kunden ergänzen. Die Effektivität von Sicherheitspraktiken hängt von der spezifischen Situation des jeweiligen Kunden ab. und Kunden wird empfohlen, bei der Festlegung der für ihre Netzwerke am besten geeigneten Sicherheitsverfahren alle relevanten Faktoren zu berücksichtigen.

Zugehörige Informationen

- Cisco Unified MeetingPlace
- Cisco PIX Firewall-Software
- Cisco Secure PIX Firewall - Befehlsreferenzen
- Problemhinweise zu Sicherheitsprodukten (einschließlich PIX)
- Cisco Technical Assistance Center (TAC)
- Anforderungen für Kommentare (RFCs)
- Technischer Support und Dokumentation für Cisco Systeme