네트워크 보안 보호 및 제3자에 대한 액세스 권한 부여

목차

소개

이 서비스 요청 과정에서 Cisco 엔지니어가 조직의 네트워크에 액세스하도록 할 수 있습니다. 이러한 액세스 권한을 부여하면 서비스 요청을 더 신속하게 해결할 수 있습니다. 이러한 경우 Cisco는 사용자의 허가를 받아 네트워크에 액세스할 수 있으며, 이 경우에만 액세스할 수 있습니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

모범 사례

회사 또는 조직 외부의 지원 엔지니어 또는 직원에게 액세스 권한을 부여할 때 네트워크의 보안을 보호하기 위해 이러한 지침을 따르는 것이 좋습니다.

- 가능하면 Cisco Unified MeetingPlace를 사용하여 지원 엔지니어와 정보를 공유합니다. 다음과 같은 이유로 Cisco Unified MeetingPlace를 사용하는 것이 좋습니다.Cisco Unified MeetingPlace는 경우에 따라 SSH(Secure Shell) 또는 텔넷보다 더 안전한 SSL(Secure Socket

Layer) 프로토콜을 사용합니다.Cisco Unified MeetingPlace에서는 회사 또는 조직 외부의 사용자에게 비밀번호를 제공할 필요가 없습니다.**참고:** 회사 또는 조직 외부의 사람에게 네트워크 액세스 권한을 부여할 때마다 서드파티가 네트워크에 액세스해야 하는 경우에만 유효한 임시 비밀번호가 되어야 합니다.일반적으로 대부분의 엔터프라이즈 방화벽은 아웃바운드 HTTPS 액세스를 허용하므로 Cisco Unified MeetingPlace에서 방화벽 정책을 변경할 필요가 없습니다.자세한 내용은 Cisco Unified MeetingPlace를 참조하십시오.

- Cisco Unified MeetingPlace를 사용할 수 없고 SSH와 같은 다른 애플리케이션을 통해 서드파티 액세스를 허용하도록 선택한 경우 비밀번호가 일시적이며 일회용으로만 사용할 수 있는지 확인합니다. 또한 서드파티 액세스가 더 이상 필요하지 않은 경우 즉시 비밀번호를 변경하거나 무효화해야 합니다. Cisco Unified MeetingPlace 이외의 애플리케이션을 사용하는 경우 다음 절차 및 지침을 따를 수 있습니다.Cisco IOS 라우터에서 임시 계정을 생성하려면 다음 명령을 사용합니다.

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

PIX/ASA에서 임시 계정을 생성하려면 다음 명령을 사용합니다.

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

임시 계정을 제거하려면 다음 명령을 사용합니다.

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

임시 비밀번호를 임의로 생성합니다. 임시 비밀번호는 특정 서비스 요청 또는 지원 서비스 제공자와 관련되어서는 안 됩니다. 예를 들어, *cisco*, *cisco123* 또는 *ciscotac*와 같은 비밀번호를 사용하지 *마십시오*.사용자 이름 또는 암호를 지정하지 마십시오.인터넷을 통해 텔넷을 사용하지 마십시오. 안전하지 않습니다.

- 지원이 필요한 Cisco 디바이스가 기업 방화벽 뒤에 있고 지원 엔지니어가 Cisco 디바이스에 SSH를 구현하기 위해 방화벽 정책을 변경해야 하는 경우, 해당 문제에 할당된 지원 엔지니어와 관련된 정책 변경이 있는지 확인하십시오. 정책 예외를 전체 인터넷 또는 필요 이상으로 광범위한 호스트에 개방하지 마십시오.Cisco IOS 방화벽에서 방화벽 정책을 수정하려면 인터넷 연결 인터페이스 아래의 인바운드 액세스 목록에 다음 행을 추가합니다.

```
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
```

참고: 이 예에서 공간 절약하기 위해 `(config-ext-nacl)#` 컨피그레이션이 두 행에 표시됩니다. 그러나 이 명령을 인바운드 access-list에 추가할 경우 컨피그레이션이 한 줄에 나타나야 합니다.Cisco PIX/ASA 방화벽에서 방화벽 정책을 수정하려면 이 행을 인바운드 액세스 그룹에 추가합니다.

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

참고: 이 예에서 공간을 절약하기 위해 `ASA(config)#` 컨피그레이션이 두 행에 표시됩니다. 그러나 인바운드 액세스 그룹에 이 명령을 추가할 때 컨피그레이션이 한 줄에 나타나야 합니다.Cisco IOS 라우터에서 SSH 액세스를 허용하려면 이 행을 access-class에 추가합니다.

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

Cisco PIX/ASA에서 SSH 액세스를 허용하려면 다음 컨피그레이션을 추가합니다.

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

이 문서에 설명된 정보에 대해 질문이 있거나 추가 지원이 필요한 경우 Cisco TAC(Technical

Assistance Center)에 문의하십시오.

이 웹 페이지는 정보 제공용으로만 제공되며 보증 또는 보증 없이 "있는 그대로" 제공됩니다. 위의 모범 사례는 포괄적이지는 않지만 고객의 현재 보안 절차를 보완하기 위해 제안됩니다. 모든 보안 방식의 효율성은 각 고객의 상황에 따라 달라집니다. 그리고 고객은 네트워크에 가장 적합한 보안 절차를 결정할 때 모든 관련 요소를 고려해야 합니다.

관련 정보

- Cisco Unified MeetingPlace
- Cisco PIX 방화벽 소프트웨어
- Cisco Secure PIX Firewall 명령 참조
- 보안 제품 필드 알림(PIX 포함)
- Cisco TAC(Technical Assistance Center)
- RFC(Request for Comments)
- 기술 지원 및 문서 – Cisco Systems