

# Protecting Network Security When Granting Access to Third Parties

Document ID: 72884

---

**Introduction**

**Prerequisites**

Requirements

Components Used

Conventions

**Best Practices**

**NetPro Discussion Forums – Featured Conversations**

**Related Information**

---

## Introduction

During the course of this service request, you may want Cisco engineers to access your organization's network. Granting such access will often allow your service request to be resolved more quickly. In such cases, Cisco can, and will only, access your network with your permission.

## Prerequisites

### Requirements

There are no specific requirements for this document.

### Components Used

This document is not restricted to specific software and hardware versions.

### Conventions

Refer to Cisco Technical Tips Conventions for information on document conventions.

## Best Practices

Cisco recommends that you follow these guidelines in order to help you protect the security of your network when you grant access to any support engineer or person outside of your company or organization.

- If possible, use Cisco Unified MeetingPlace in order to share information with support engineers. Cisco recommends that you use Cisco Unified MeetingPlace for these reasons:
  - ◆ Cisco Unified MeetingPlace uses the Secure Socket Layer (SSL) protocol, which is more secure than secure shell (SSH) or Telnet in some cases.
  - ◆ Cisco Unified MeetingPlace does not require you to provide passwords to anyone outside of your company or organization.

**Note:** Whenever you grant network access to persons outside your company or organization, any passwords that you provide must be temporary passwords that are valid only as long as the third party requires access to your network.

- ◆ Typically, Cisco Unified MeetingPlace does not require you to change your firewall policy because most enterprise firewalls allow outbound HTTPS access.

Visit Cisco Unified MeetingPlace for more information.

- If you cannot use Cisco Unified MeetingPlace and if you choose to allow third-party access through another application, such as SSH, ensure the password is temporary and available for one-time use only. In addition, you must immediately change or invalidate the password after third-party access is no longer necessary. If you use an application other than Cisco Unified MeetingPlace, you may follow these procedures and guidelines:

- ◆ In order to create a temporary account on Cisco IOS routers, use this command:

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

- ◆ In order to create a temporary account on PIX/ASA, use this command:

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

- ◆ In order to remove the temporary account, use this command:

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

- ◆ Randomly generate the temporary password. The temporary password must not be related to the particular service request or provider of support services. For example, do not use passwords such as *cisco*, *cisco123*, or *ciscotac*.
  - ◆ Never give your own user name or password.
  - ◆ Do not use Telnet over the Internet. It is not secure.
- If the Cisco device that requires support is located behind a corporate firewall and a change to firewall policies is required for a support engineer to SSH into the Cisco device, ensure that the policy change is specific to the support engineer assigned to the issue. Never make the policy exception open to the entire Internet or to a wider range of hosts than necessary.

- ◆ To modify a firewall policy on a Cisco IOS Firewall, add these lines to the inbound access-list under Internet facing interface:

```
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
```

**Note:** In this example, the Router ( config-ext-nacl ) # configuration is displayed on two lines in order to conserve space. However, when you add this command to the inbound access-list, the configuration must appear on one line.

- ◆ To modify a firewall policy on a Cisco PIX/ASA firewall, add this line to the inbound access-group:

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

**Note:** In this example, the ASA ( config ) # configuration is displayed on two lines in order to conserve space. However, when you add this command to the inbound access-group, the configuration must appear on one line.

- ◆ To allow SSH access on Cisco IOS routers, add this line to the 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
```

- ◆ To allow SSH access on Cisco PIX/ASA, add this configuration:

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

If have questions about or require additional assistance with the information described in this document, contact the Cisco Technical Assistance Center (TAC).

This web page is for informational purposes only and is provided on an "as is" basis without any guarantee or warranty. The best practices above are not intended to be comprehensive, but are suggested to complement customers' current security procedures. The effectiveness of any security practice is dependent on each customer's specific situation; and customers are encouraged to consider all relevant factors when determining security procedures most appropriate for their networks.

## NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Security
Security: Intrusion Detection [Systems]
Security: AAA
Security: General
Security: Firewalling

## Related Information

- [Cisco Unified MeetingPlace](#)
- [Cisco PIX Firewall Software](#)
- [Cisco Secure PIX Firewall Command References](#)
- [Security Product Field Notices \(including PIX\)](#)
- [Cisco Technical Assistance Center \(TAC\)](#)
- [Requests for Comments \(RFCs\)](#)
- [Technical Support & Documentation – Cisco Systems](#)

---

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

---

Updated: Jul 23, 2007

Document ID: 72884

---