

# Restrict Certain Cisco VPN Client Versions from Connecting to the VPN Concentrator/ASA/PIX

Document ID: 100347

---

## Introduction

### Prerequisites

Requirements

Components Used

Conventions

### Restrict VPN Client Version

Cisco VPN 3000 Concentrator Configuration

ASA/PIX Configuration

### Related Information

---

## Introduction

This document provides a sample configuration for how to restrict certain versions of the Cisco VPN Client from connecting to the VPN Concentrator or Security Appliances such as PIX and ASA.

## Prerequisites

## Requirements

There are no specific requirements for this document.

## Components Used

The information in this document is based on these software and hardware versions:

- Cisco VPN – 3000 Series Concentrator with 4.x Version
- Cisco VPN Client with 4.x Version and later
- Cisco ASA 5500 Series with Version 7.x and later
- Cisco PIX 500 Series with Version 7.x and later

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Conventions

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

## Restrict VPN Client Version

### Cisco VPN 3000 Concentrator Configuration

The VPN Concentrator can permit or deny VPN Clients by their type and software version.

In order to use this feature, login to the VPN Concentrator and choose **Configuration > User Management > Groups**. Then choose the group and go to the IPsec tab.

Construct the rules in this way:

```
p[ermit]/d[eny] :
```

Examples:

- deny \*:3.6\* Denies all VPN Clients that run Software Version 3.6x
- d VPN CLIENT : 4.6\* Prevents users with VPN Client Version 4.6 to be able to establish the VPN connection to the VPN Concentrator
- p windows : 4.8\* Allows only Version 4.8 to connect
- p \* : 4.8\* Permits any platform that runs any Version of 4.8

If the administrator does not wish to specify the platform, use this rule instead:

```
p * : 4.8*
```

**Note:** The \* character is a wildcard. You can use it multiple times in each rule.

Use a separate line for each rule.

Order rules by priority. The first rule that matches is the rule that applies. If a later rule contradicts it, the system ignores it. If you do not define any rules, all connections are permitted.

When a client matches none of the rules, the connection is denied. This means that, if you define a deny rule, you must also define at least one permit rule, or all connections are denied.

For both software and hardware clients, the client type and software version must match (case sensitive) in their appearance in the Monitoring | Sessions window, which includes spaces. It is recommended that you copy and paste from that window to this one.

Use n/a for either the type or version to identify information that the client does not send. For example, permit n/a:n/a allows you to permit any client that does not send the client type and version.

You can use a total of 255 characters for rules. The newline between rules uses two characters. In order to conserve characters, use p for permit and d for deny. Eliminate spaces except as required for the client type and version. You do not need a space before or after the colon (:).

## ASA/PIX Configuration

In order to configure rules that limit the remote access client types and versions that can connect through IPsec and the security appliance, issue the **client-access-rule** command in group-policy configuration mode. In order to delete a rule, issue the **no** form of this command.

This example shows how to create client access rules for the group policy named FirstGroup. These rules permit VPN Clients that run Software Version 4.1, while deny all VPN 3002 hardware clients:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# client-access-rule 1 d t VPN3002 v *
hostname(config-group-policy)# client-access-rule 2 p * v 4.1
```

When you construct rules, refer to these guidelines:

- If you do not define any rules, the security appliance permits all connection types.
- When a client matches none of the rules, the security appliance denies the connection. If you define a deny rule, you must also define at least one permit rule, or the security appliance denies all connections.
- For both software and hardware clients, type and version must match their appearance exactly in the show vpn-sessiondb remote display.
- The \* character is a wildcard, which you can use multiple times in each rule. For example, client-access-rule 3 deny type \* version 3.\* creates a priority 3 client access rule that denies all client types that run Version 3.x Software.
- You can construct a maximum of 25 rules per group policy.
- There is a limit of 255 characters for an entire set of rules.
- You can use n/a for clients that do not send client type or version.

**Note:** In order to restrict MAC OS VPN Client, use the syntax "**Mac OS X**" for the platform type to match Mac connections.

---

## Related Information

- [Cisco ASA 5500 Series Security Appliances](#)
- [Cisco PIX 500 Series Security Appliances](#)
- [IPsec Negotiation/IKE Protocols](#)
- [Cisco VPN 3000 Series Concentrators](#)
- [Technical Support & Documentation – Cisco Systems](#)

---

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Sep 30, 2008

Document ID: 100347

---