

How to Manage the VPN 3000 Concentrator from the Public Network

Document ID: 14107

Introduction

Prerequisites

Requirements

Components Used

Conventions

Cisco VPN 3000 Concentrator Releases Before 4.1

Cisco VPN 3000 Concentrator Release 4.1 and Later

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

For optimal security, the filters on the public interface allow only tunneled and Internet Control Message Protocol (ICMP) traffic by default. However, there are cases when an administrator needs to manage the VPN Concentrator from a computer on the public network. The procedures in this document shows you how to configure this.

Note: The information in this document is based on all Cisco VPN 3000 Concentrator releases. With the introduction of WebVPN (SSL VPN) functionality in the 4.1 code release, a new way to configure management access to the Public interface is defined. Follow these links for your version of the VPN 3000 Concentrator software.

- [Cisco VPN 3000 Concentrator Releases Before 4.1](#)
- [Cisco VPN 3000 Concentrator Release 4.1 and Later](#)

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on all releases of the Cisco VPN 3000 Concentrator.

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.

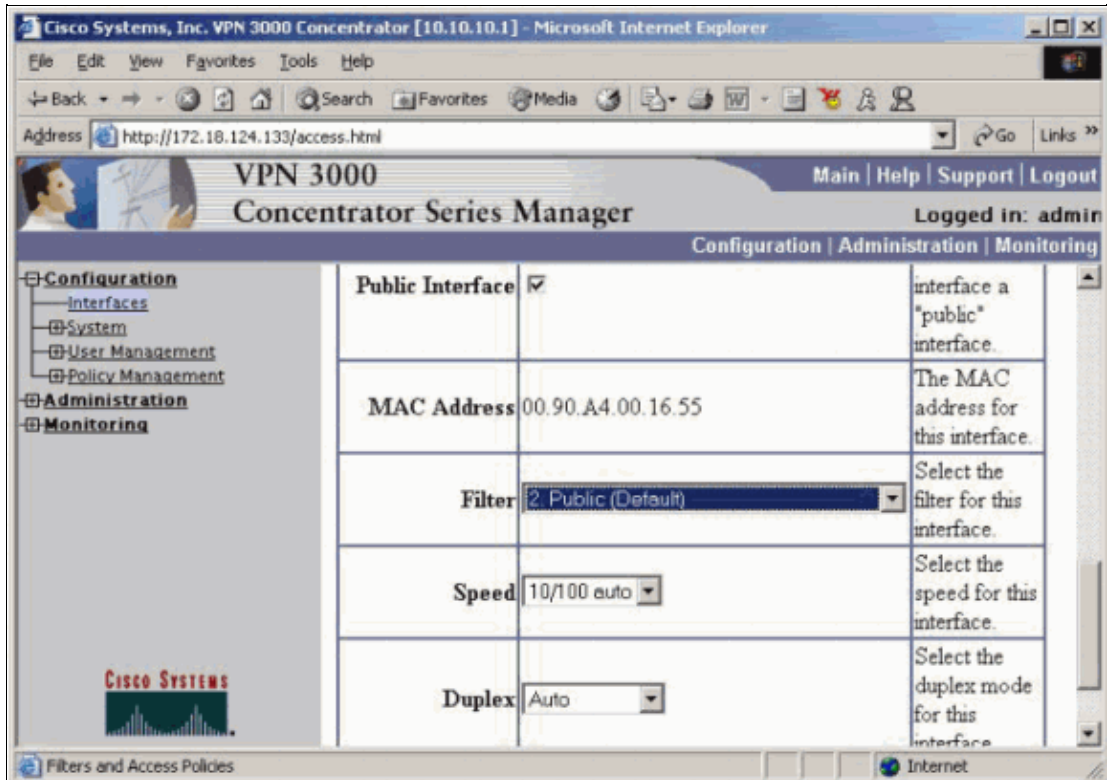
Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Cisco VPN 3000 Concentrator Releases Before 4.1

Use this procedure in order to configure the VPN Concentrator so that you can manage it from the public network for releases before 4.1.

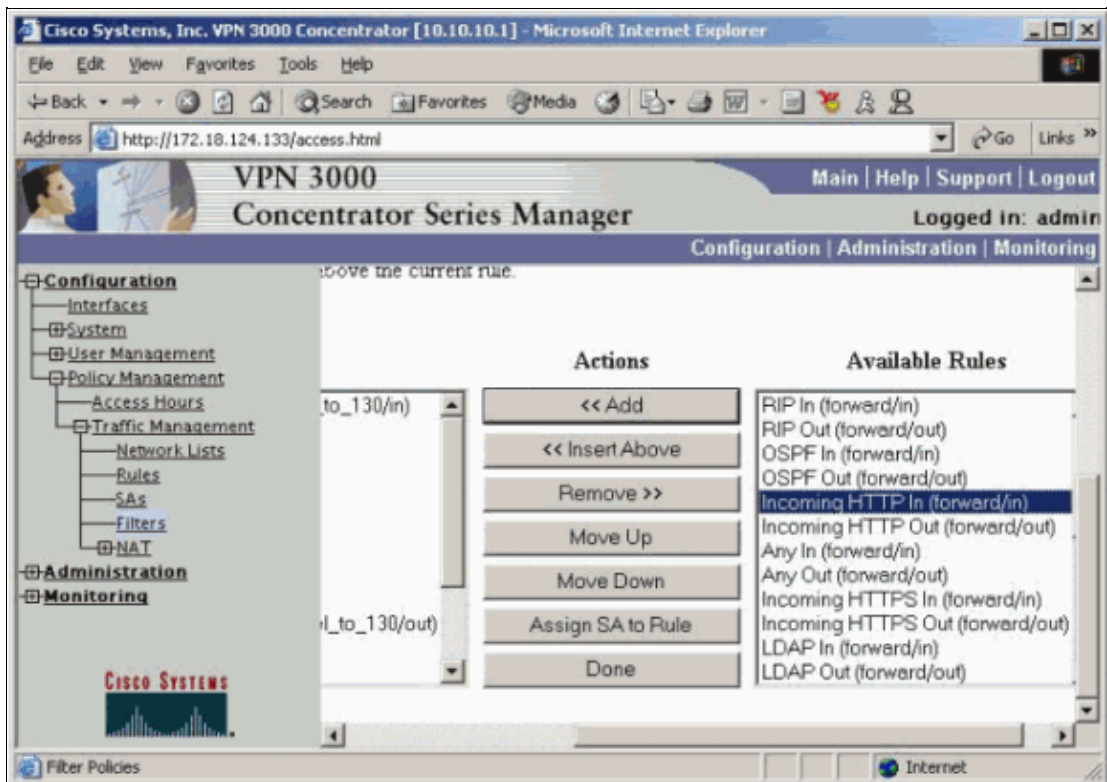
1. Select **Configuration > Interfaces > Ethernet**.
2. Check to see what filter is applied to the Public Interface (the default is "Public (default)").



3. Select **Configuration > Policy Management > Traffic Management > Filters**.
4. Highlight **Public Filter**, and click **Assign Rules to Filter**.



5. Under the Available Rules option, select **Incoming HTTP In (forward/in)**, then click on the << Add button.



6. Repeat step 5 for **Incoming HTTP Out (forward/out)**.
7. Click **Done**.

Note: If the rules were not configured earlier, use these configuration parameters.

- a. Select **Configuration > Policy Management > Traffic Management > Rules**.
- b. Click **Add** and change these fields from their default settings:

- ◇ **Rule Name:** Create a unique name for this rule (for example, "Public HTTP In")
- ◇ **Action:** Forward
- ◇ **Protocol:** TCP
- ◇ **Source IP Address:** IP address of the workstation that you manage
- ◇ **Wildcard Mask:** 0.0.0.0
- ◇ **Destination IP Address:** IP address of the public interface of the VPN Concentrator
- ◇ **Wildcard Mask:** 0.0.0.0
- ◇ **TCP/UDP Destination Port:** HTTP

c. Click **Add**.

d. Repeat steps a through c in order to add a second rule with this new configuration:

- ◇ **Rule Name:** Create a unique name for this rule (for example, "Public HTTP Out")
- ◇ **Action:** Forward
- ◇ **Protocol:** TCP
- ◇ **Source IP address:** IP address of the public interface of the VPN Concentrator
- ◇ **Wildcard Mask:** 0.0.0.0
- ◇ **Destination IP address:** IP address of the workstation
- ◇ **Wildcard Mask:** 0.0.0.0
- ◇ **TCP/UDP Source Port:** HTTP

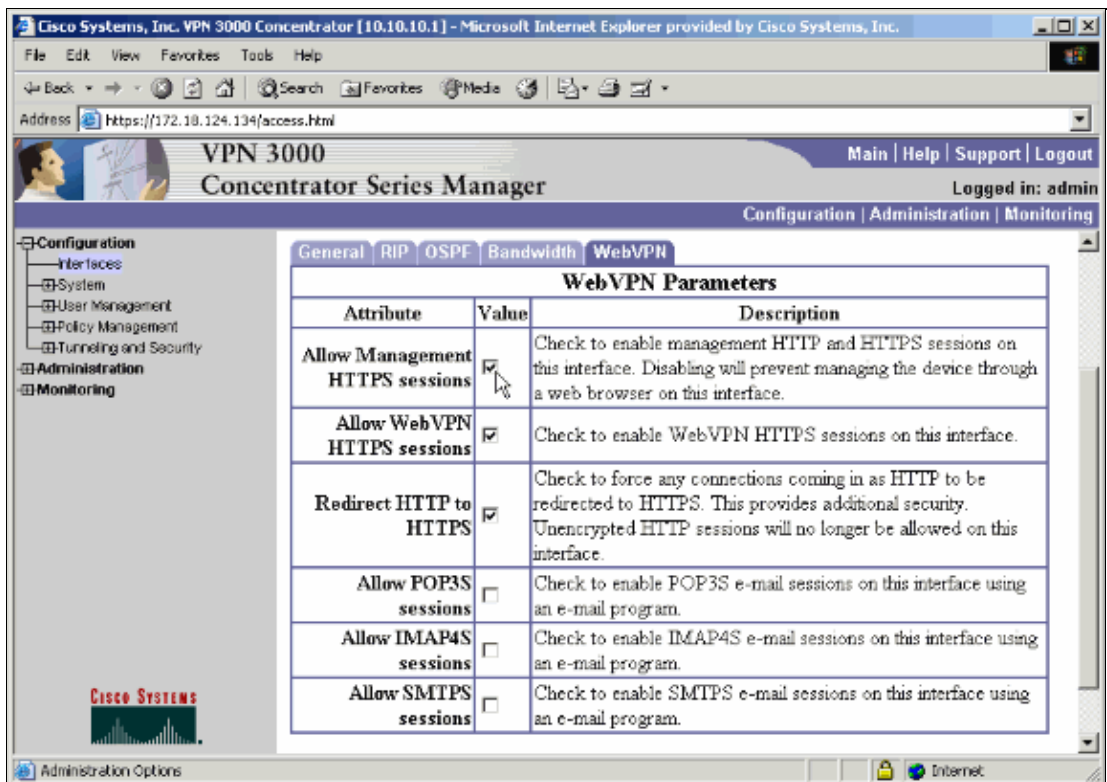
8. Click **Save** in order to save the configuration changes.

Cisco VPN 3000 Concentrator Release 4.1 and Later

With the introduction of SSL VPN functionality, HTTP/HTTPS access to the Public interface became a necessity. The default configuration however, is to allow SSL VPN access while disallowing management access to the same Public interface.

Use this procedure in order to configure the VPN Concentrator so that you can manage it from the public network for releases 4.1 and later.

1. Select **Configuration > Interfaces > Ethernet 2 (Public)**, then choose the WebVPN tab.
2. Check the **Allow Management HTTPS sessions** check box.



3. Check the **Redirect HTTP to HTTPS** checkbox for enhanced security.
4. Click the **Apply** button and save the configuration.

Note: This checkbox setting overrides the rules that the Public filter defines (or whatever filter is applied to the Public interface). You do not need to add rules to filters in WebVPN supported code.

In order to access the management screen from the Public interface, the URL now becomes **http[s]://<concentrator public IP address>/admin.html**.

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 VPN
Service Providers: VPN Service Architectures
Service Providers: Network Management
Virtual Private Networks: General

Related Information

- [Cisco VPN 3000 Series Concentrator Support Page](#)
- [Cisco VPN 3000 Series Client Support Page](#)
- [IPSec Support Page](#)
- [Technical Support – Cisco Systems](#)

