

PIX/ASA 7.x and Later: VPN Filter (Permit Specific Port or Protocol) Configuration Example for L2L and Remote Access

Document ID: 99103

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Related Products
- Conventions

Background Information

Configure

- L2L Network Diagram
- L2L VPN Filter Configuration
- L2L VPN Filter Configuration through ASDM
- Bidirectional VPN Filter Configuration
- Bidirectional VPN Filter Configuration through ASDM
- Remote Access Network Diagram
- Remote Access VPN Filter Configuration
- Remote Access VPN Filter Configuration through ASDM

Related Information

Introduction

This document describes the procedure to use Cisco ASA to configure VPN filter in L2L and Remote Access with Cisco VPN Client.

Filters consist of rules that determine whether to allow or reject tunneled data packets that come through the security appliance, based on criteria such as source address, destination address, and protocol. You configure ACLs to permit or deny various types of traffic for this **group policy**. You can also configure this attribute in username mode, in which case, the value configured under **username** supersedes the group-policy value.

Note: In order for tunnel configuration changes to take effect, you must log off the VPN tunnel and reestablish the tunnel.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- For an L2L VPN filter, the L2L IPSec configuration must be configured. Refer to PIX/ASA 7.x: Simple PIX-to-PIX VPN Tunnel Configuration Example for more information on how to configure Site to Site IPSec VPN in the Cisco Security Appliance that runs software version 7.x.
- For a Remote Access VPN filter, the Remote Access IPSec configuration must be configured. Refer to PIX/ASA 7.x and Cisco VPN Client 4.x for Windows with Microsoft Windows 2003 IAS RADIUS

Components Used

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

- Cisco 5500 Series Adaptive Security Appliance (ASA) software that runs version 8.2(1)
- Cisco Adaptive Security Device Manager version 6.3(5)
- Cisco VPN Client version 4.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.

Related Products

This configuration can also be used with Cisco PIX 500 Series Security Appliance that runs version 7.x and later.

Conventions

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

Background Information

The **sysopt connection permit-ipsec** command allows all the traffic that enters the security appliance through a VPN tunnel to bypass interface access lists. Group policy and per-user authorization access lists still apply to the traffic. In PIX/ASA 7.1 and later, the **sysopt connection permit-ipsec** command is changed to **sysopt connection permit-vpn**. The **vpn-filter** is applied to post-decrypted traffic after it exits a tunnel and pre-encrypted traffic before it enters a tunnel.

An ACL that is used for a **vpn-filter** must **not** also be used for an interface access-group. When a **vpn-filter** is applied to a group-policy/user name mode that governs Remote Access VPN Client connections, the ACL must be configured with the client assigned IP addresses in the **src_ip** position of the ACL and the local network in the **dest_ip** position of the ACL. When a **vpn-filter** is applied to a group-policy that governs an L2L VPN connection, the ACL must be configured with the remote network in the **src_ip** position of the ACL and the local network in the **dest_ip** position of the ACL.

```
access-list <acl-no> <permit/deny> ip <remote network> <local network>
```

Exercise caution when you construct the ACLs for use with the **vpn-filter** feature. The ACLs are constructed with the post-decrypted traffic (inbound VPN traffic) in mind. However, they are also applied to the traffic originated in the opposite direction.

Note: At the end of each ACL, there is an implicit, unwritten rule that denies all traffic that is not permitted. If the traffic is not explicitly permitted by an access control entry (ACE), it is denied. ACEs are referred to as rules in this topic. In this scenario, refer to the access list 103 configured in the L2L VPN Filter Configuration.

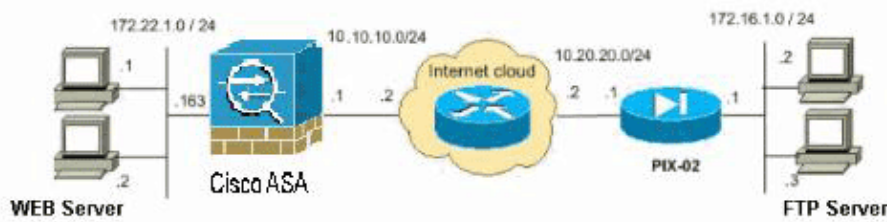
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

L2L Network Diagram

This document uses this network setup for **L2L VPN Filter**:



L2L VPN Filter Configuration

This document uses these configurations:

CiscoASA

```
CiscoASA# show running-config
!
!--- Output suppressed

access-list 103 extended deny tcp host 172.16.1.2 host 172.22.1.2 eq 80

!--- Access list 103 is created for the VPN Filter.
!--- This access list 103 filters/denies the request from the remote host(172.16.1.2)
!--- to the local WEB Server (172.22.1.2).

access-list 103 extended permit ip any any

!
!--- Output suppressed

group-policy filter internal
group-policy filter attributes
  vpn-filter value 103

!--- Create the group policy (filter)and specify the access list
!--- number in the vpn filter command.

!
!--- Output suppressed

tunnel-group 10.20.20.1 general-attributes
  default-group-policy filter

!--- Associate the group policy (filter) with the tunnel group.
```

!
!

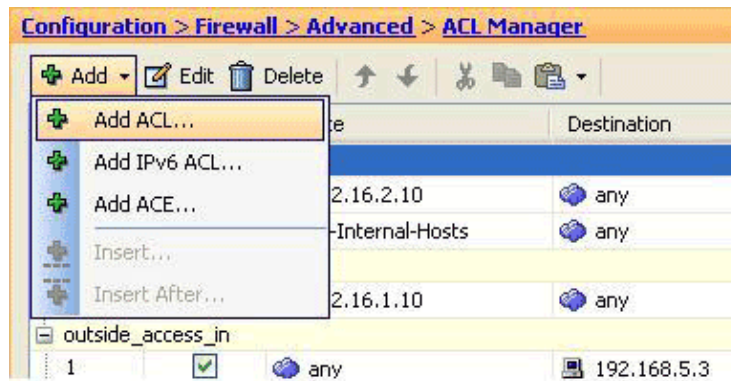
!--- Output suppressed

L2L VPN Filter Configuration through ASDM

Complete these steps in order to configure an L2L VPN filter through the Cisco Adaptive Security Device Manager (ASDM):

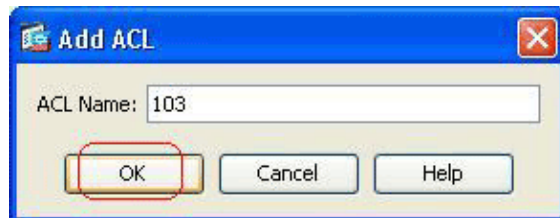
1. Add an access list:

a. In the ASDM, choose **Configuration > Firewall > Advanced > ACL Manager**.



b. Click **Add**, and choose **Add ACL**.

The Add ACL dialog box appears.

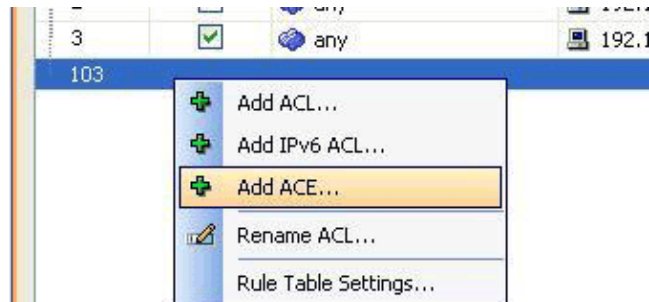


c. Enter **103** in the ACL Name field, and click **OK**.

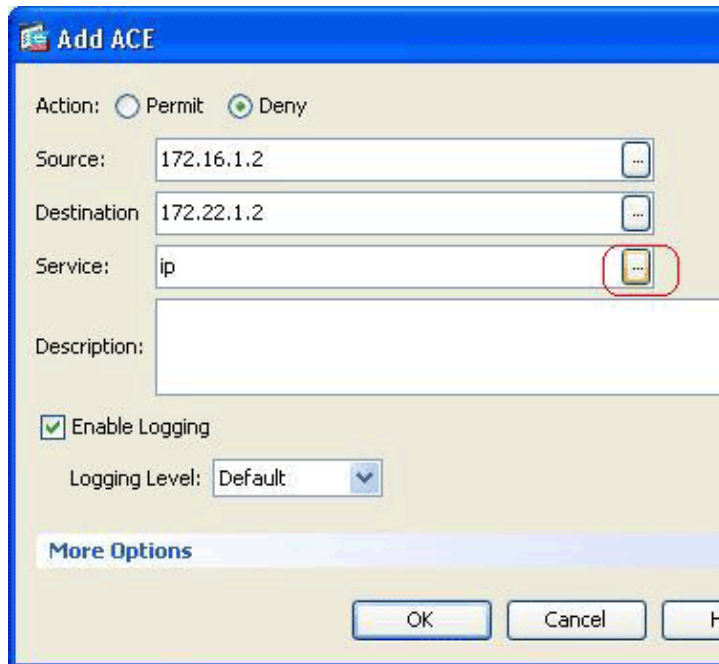
The new ACL appears in the ACL list.

2. Add an ACE:

a. Right-click the new ACL, and choose **Add ACE**.

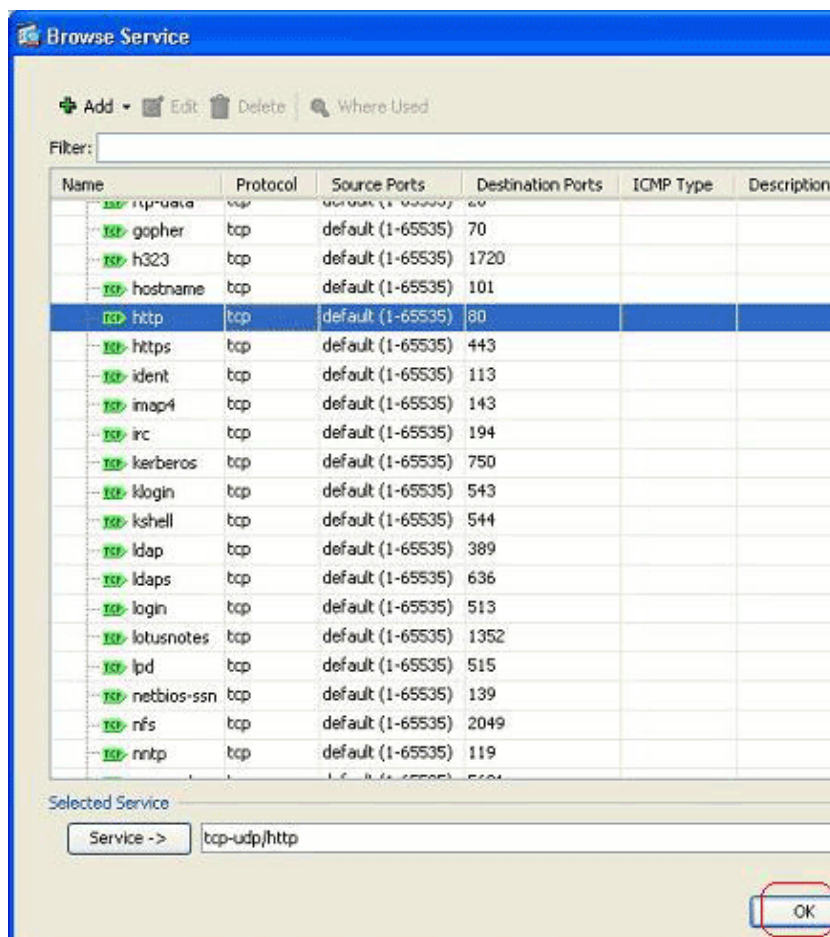


The Add ACE dialog box appears.

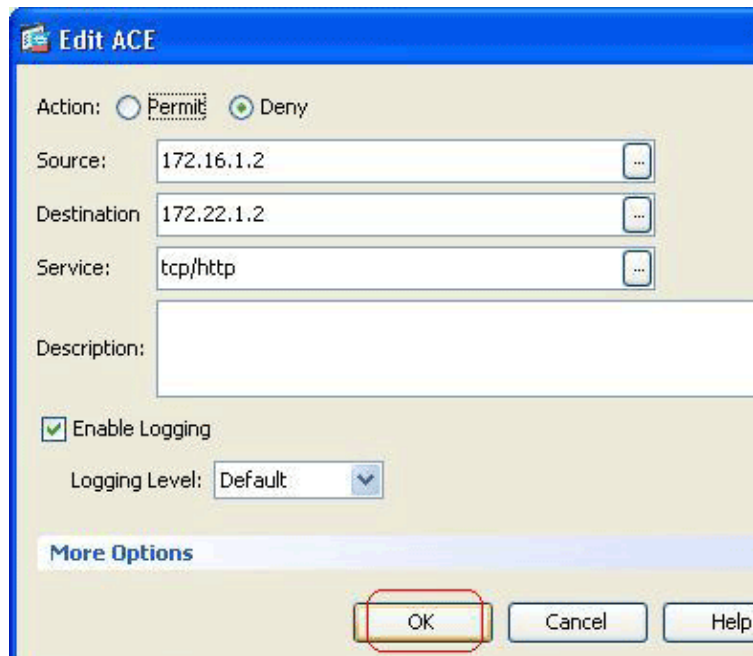


- b. Click the **Deny** option button, enter the source IP address and the destination IP address, and then click the browse button (...) located next to the Service field.

The Browse Service dialog box appears.



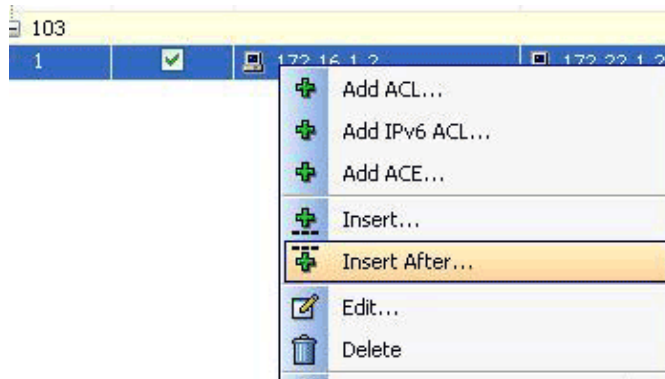
- c. Choose **TCP port 80**, and click **OK** to return to the Edit ACE dialog box.



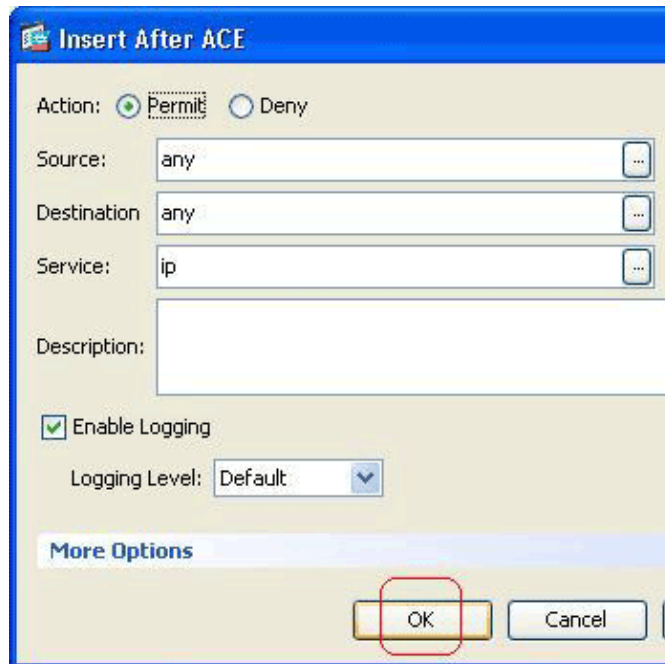
d. Click **OK**.

The new ACE entry appears in the ACL list.

e. Right-click the new ACE entry, and choose **Insert After**.



The Insert After ACE dialog box appears.



f. Add an ACE that permits any-to-any traffic:

- a. Click the **Permit** option.
- b. Choose **any** in the Source and Destination fields, and choose **ip** in the Service field.
- c. Click **OK**.

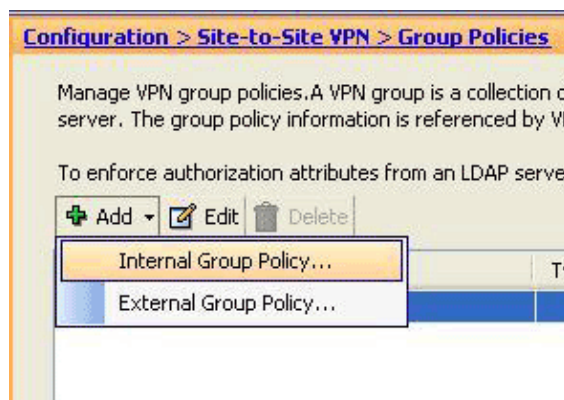
Note: Adding an ACE that permits any-to-any traffic prevents the Implicit Deny rule at the end of the access list.

This image shows the 103 access list with the two access control entries:

| ACE | Order | Source | Destination | Service | Action |
|-----|-------|------------|-------------|----------|--------|
| 103 | 1 | 172.16.1.2 | 172.22.1.2 | tcp http | Deny |
| 103 | 2 | any | any | IP ip | Permit |

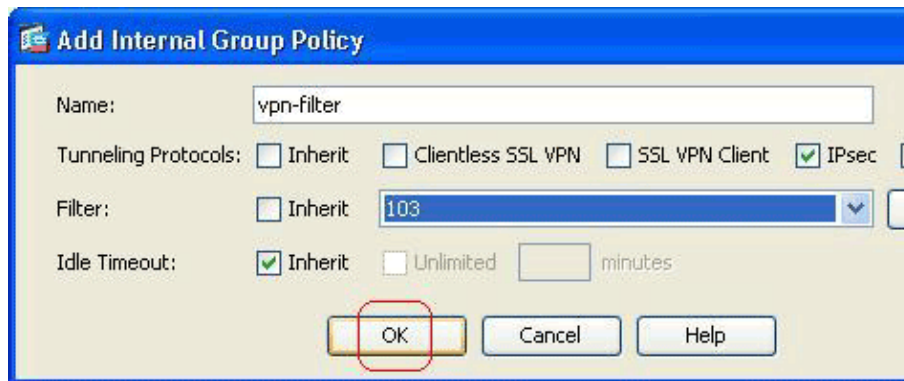
3. Configure the group policy:

- a. In the ASDM, choose **Configuration > Site-to-Site VPN > Group Policies** in order to configure the group policy.



- b. Click **Add**, and choose **Internal Group Policy**.

The Add Internal Group Policy dialog box appears.



- c. Enter a name for the group policy in the Name field, and choose **103** from the Filter drop-down list.

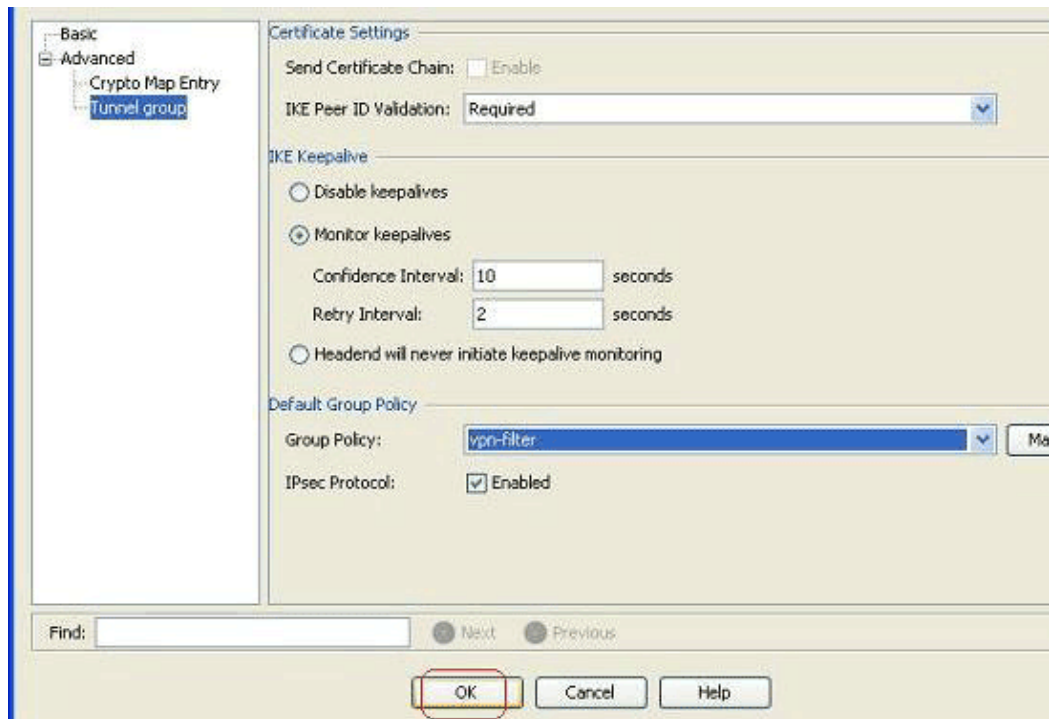
Tip: You can also use the **Manage** button located next to the Filter drop-down list in order to select the filter.

- d. Click **OK**.

4. Add the internal group policy to the site-to-site tunnel group.

- a. In the ASDM, choose **Configuration > Site-to-Site VPN > Connection Profiles**.

- b. Choose the required tunnel group, and click **Edit** button in order to modify the tunnel group parameters.



- c. Choose **vpn-filter** from the Group Policy drop-down list.

Tip: You can also use the **Manage** button located next to the Group Policy drop-down list in order to select the filter.

Bidirectional VPN Filter Configuration

The VPN Filter works bi-directionally with a single ACL. The remote host/network is always defined at the beginning of the ACE, regardless of the direction of the ACE (inbound or outbound).

This configuration is described in this sample configuration.

As ACL is stateful, if the traffic is allowed in one direction, then the return traffic for that flow is automatically allowed.

Note: If TCP/UDP ports are not used with the access list, both sides can access each other. For example:

```
access-list 103 permit ip 172.16.1.2 host 172.22.1.1
```

Note: This ACL allows the traffic to be originated from 172.16.1.2 to 172.22.1.1 and also from 172.22.1.1 to 172.16.1.2, as the ACL is applied bi-directionally.

```
CiscoASA# show running-config

CiscoASA
!
!--- Output suppressed

!--- This access list allows the traffic for the remote network 172.16.1.0
!--- to the local web server on port 80.

access-list 105 extended permit tcp 172.16.1.0 255.255.255.0 host 172.22.1.1 eq www

!--- This access list allows the traffic in the reverse direction,
!--- from 172.22.1.0 to 172.16.1.3 (ftp server). The remote host/network
!--- is always defined as the first entry in
!--- the ACE regardless of the direction.

access-list 105 extended permit tcp host 172.16.1.3 eq ftp 172.22.1.0 255.255.255.0

!--- Implicit deny.
!--- Denies all other traffic other than permitted traffic.

!
!--- Output suppressed

group-policy filter internal
group-policy filter attributes
  vpn-filter value 105

!--- Create the group policy (filter)and specify the access list number
!--- in the vpn filter command.

!
!--- Output suppressed

tunnel-group 10.20.20.1 general-attributes
  default-group-policy filter

!--- Associate the group policy (filter) with the tunnel group.

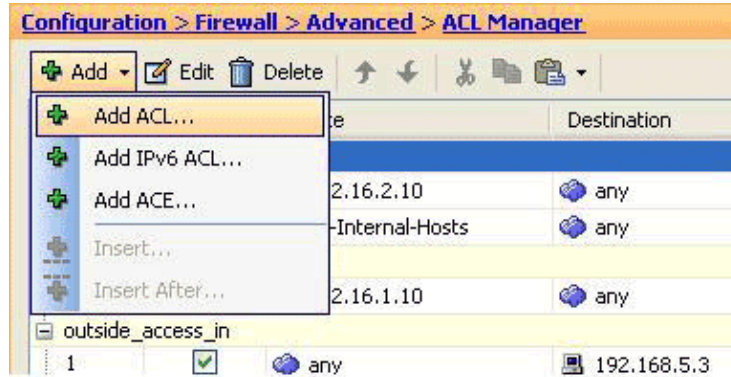
!
!--- Output suppressed
```

Bidirectional VPN Filter Configuration through ASDM

Complete these steps in order to configure a bidirectional VPN filter through the ASDM:

1. Add an access list:

a. In the ASDM, choose **Configuration > Firewall > Advanced > ACL Manager**.



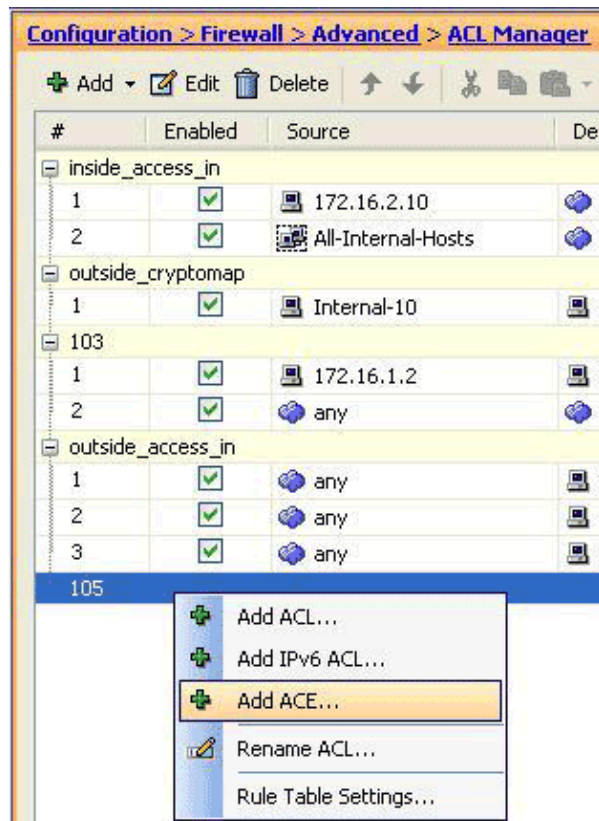
b. Click **Add**, and choose **Add ACL**.

c. Enter **105** in the ACL Name field, and click **OK**.

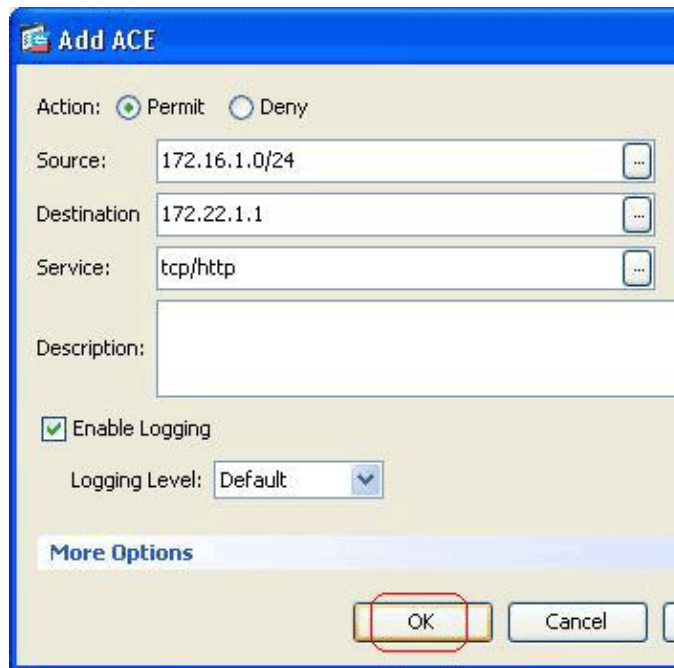
The new ACL appears in the ACL list.

2. Add an ACE:

a. In the ACL list, right-click the 105 entry, and choose **Add ACE**.

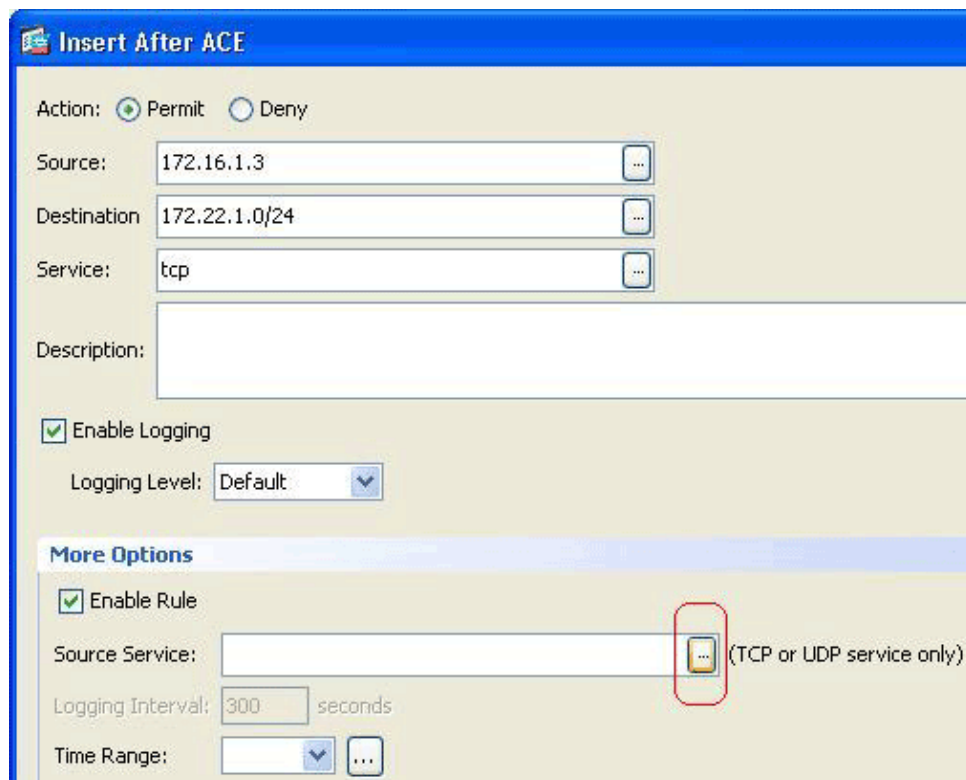


The Add ACE dialog box appears.

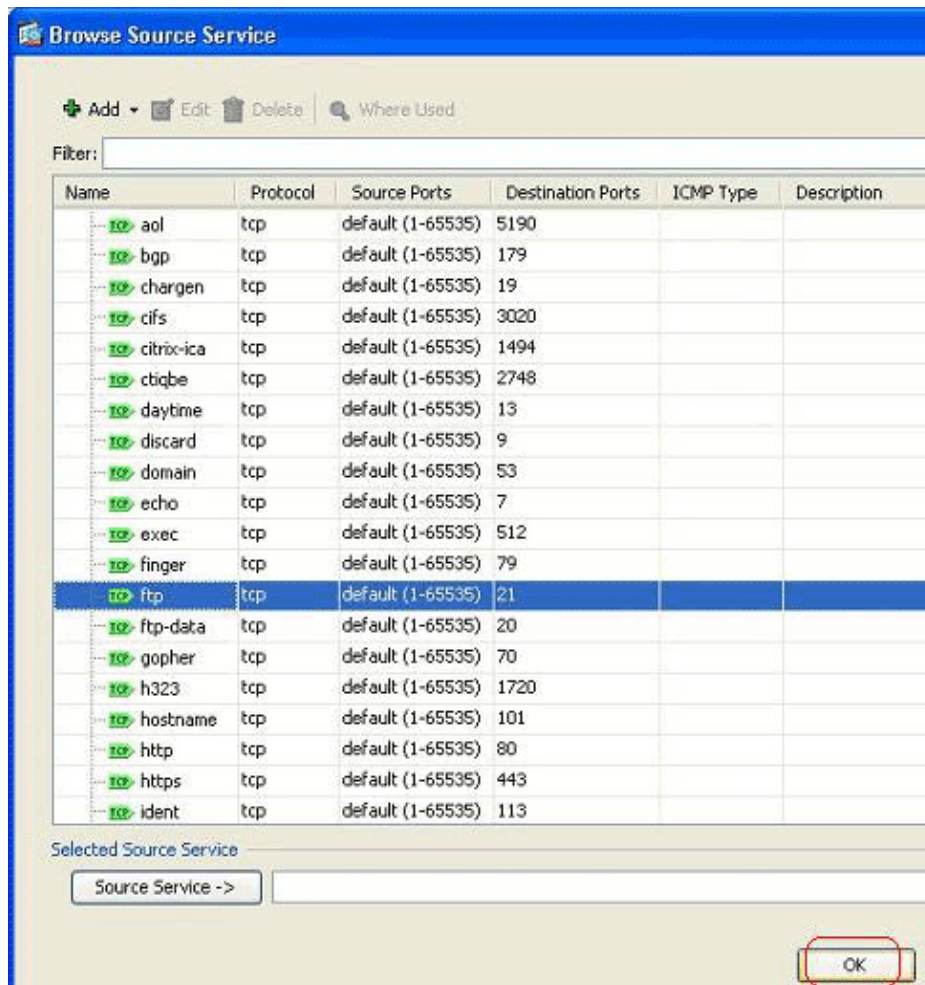


- b. Click the **Permit** option button.
- c. Enter the **172.16.1.0** network in the Source field, and enter **172.22.1.1** in the Destination field.
- d. Click the Service browse button (...), and choose **tcp/http**.
- e. Click **OK**.
- f. In the ACL list, right-click the new ACE entry, and choose **Insert After ACE**.

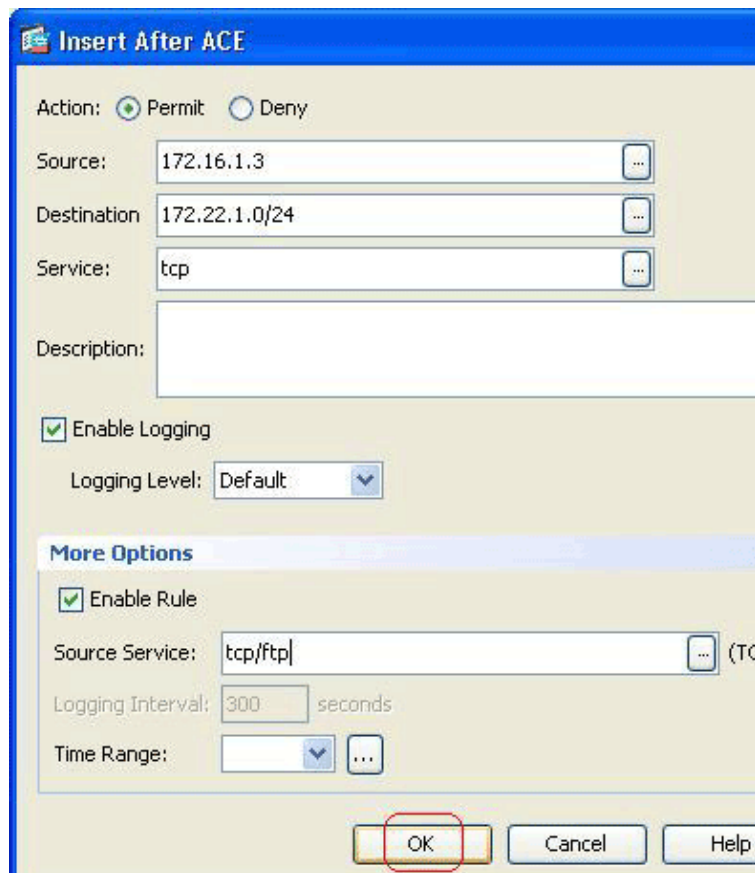
The Insert After ACE dialog box appears.



- g. Click the **Permit** option.
- h. Enter **172.16.1.3** in the Source field, and choose **172.22.1.0/24** for the Destination.
- i. In the More Options area, click the **Enable Rule** check box, and then click the browse button (...) located next to the Source Service field.
- j. The Browse Source Service dialog box appears.

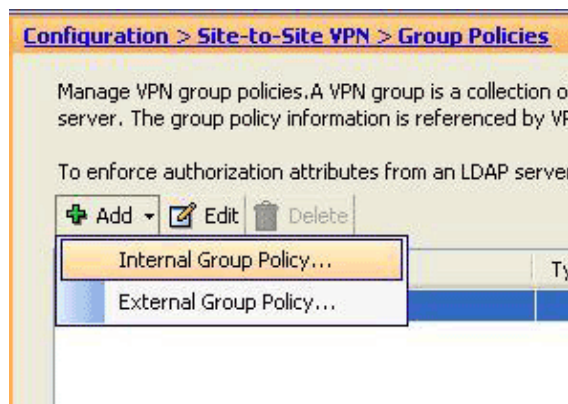


k. Select **ftp**, and click **OK** to return to the Insert After ACE dialog box.



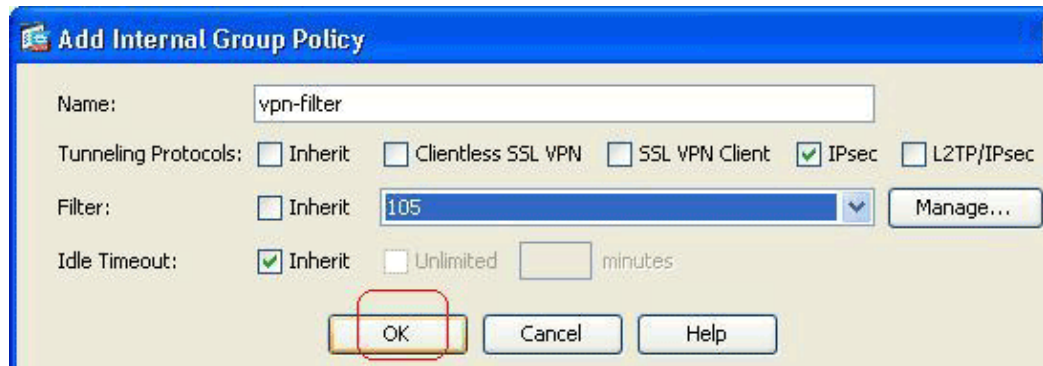
3. Add an internal group policy:

- a. In the ASDM, choose **Configuration > Site-to-Site VPN > Group Policies** in order to configure the group policy.



- b. Click **Add**, and choose **Internal Group Policy**.

The Add Internal Group Policy dialog box appears.



- c. Enter a name for the group policy in the Name field, and choose **105** from the Filter drop-down list.

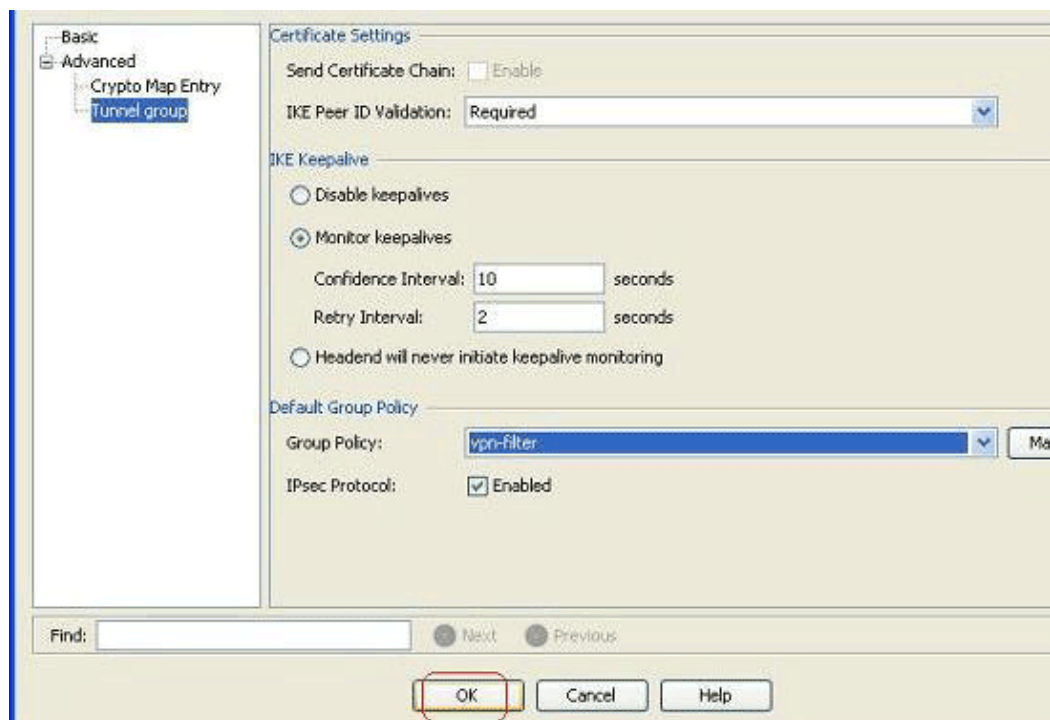
Tip: You can also use the Manage button located next to the Filter drop-down list in order to select the filter.

- d. Click **OK**.

4. Add the internal group policy to the site-to-site tunnel group:

- a. In the ASDM, choose **Configuration > Site-to-Site VPN > Connection Profiles**.

- b. Choose the required tunnel group, and click **Edit** button in order to modify the tunnel group parameters.

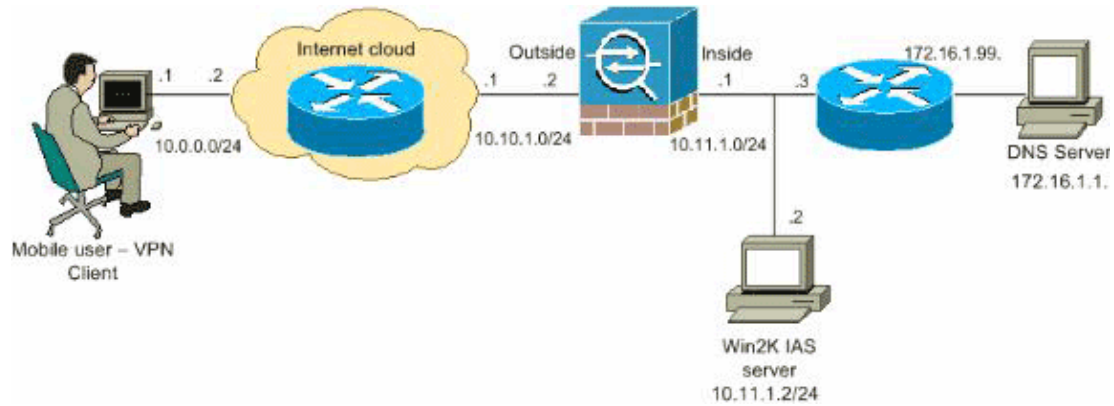


- c. Choose **vpn-filter** from the Group Policy drop-down list.

Tip: You can also use the **Manage** button located next to the Group Policy drop-down list in order to select the filter.

Remote Access Network Diagram

This document uses this network setup for Remote Access VPN Filter:



Remote Access VPN Filter Configuration

This document uses this configuration:

```

CiscoASA
CiscoASA# show running-config

!
!--- Output suppressed

ip local pool vpnclient 10.16.20.1-10.16.20.5

!--- Create a pool of addresses from which IP addresses are assigned
!--- dynamically to the remote VPN Clients.

access-list 103 extended permit udp 10.16.20.0 255.0.0.0 host 172.16.1.1 eq 53

!--- Access list 103 is created for the VPN Filter for the group policy(filter).
!--- Access list 103 allows the access for the DNS Server(172.16.1.1)

!--- Implicit deny. Denies all traffic other than permitted traffic.

access-list 104 extended permit ip 10.16.20.0 255.0.0.0 172.16.1.0 255.255.255.0

!--- Access list 104 is created for the VPN Filter for the user(vpn3000).
!--- This access list 103 allows the access for the network 172.16.1.0/24

!--- Implicit deny. Denies all traffic other than permitted traffic.

!
!--- Output suppressed

username vpn3000 password xaI3t+nY5wjYQ2thSKJfoQ== nt-encrypted

!--- In order to identify remote access users to the Security
!--- Appliance, you can also configure usernames and passwords
!--- on the device in addition to the use of AAA.

```

```

username vpn3000 attributes
  vpn-filter value 104

!--- Apply the VPN Filter ACL 104 in the username mode.
!--- This filter is applicable to a particular user (vpn3000) only.
!--- The username mode VPN Filter (acl 104) overrides
!--- the vpn filter policy (acl 103) applied in the group
!--- policy(filter) mode for this user(vpn3000) alone.

!
!--- Output suppressed

group-policy vpn-filter internal
group-policy vpn-filter attributes
  vpn-filter value 103

!--- Create the group policy (filter) and specify the access list number
!--- in the vpn-filter command.

!
!--- Output suppressed

tunnel-group vpn3000 general-attributes
  default-group-policy vpn-filter

!--- Associate the group policy (filter) with the tunnel group(vpn3000).

```

Note: Certain configuration changes take effect only during the negotiation of subsequent SAs. If you want the new settings to take effect immediately, clear the existing SAs in order to reestablish them with the changed configuration. If the security appliance is actively processing IPsec traffic, it is desirable to clear only the portion of the SA database that the configuration changes would affect. Reserve clearing the full SA database for large-scale changes, or when the security appliance processes a small amount of IPsec traffic.

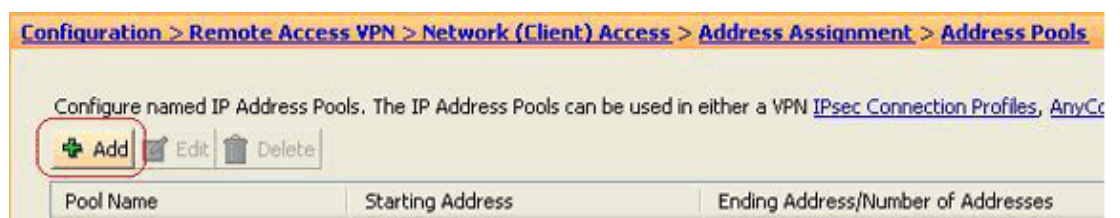
Note: You can use these given commands in order to clear and re-initialize the SAs.

- **clear ipsec sa** Removes all of the IPsec SAs from the security appliance.
- **clear ipsec peer 10.1.1.1** Deletes IPsec SAs with a peer IP address of 10.1.1.1.
- **clear isakmp sa** Removes all of the IKE runtime SA database.

Remote Access VPN Filter Configuration through ASDM

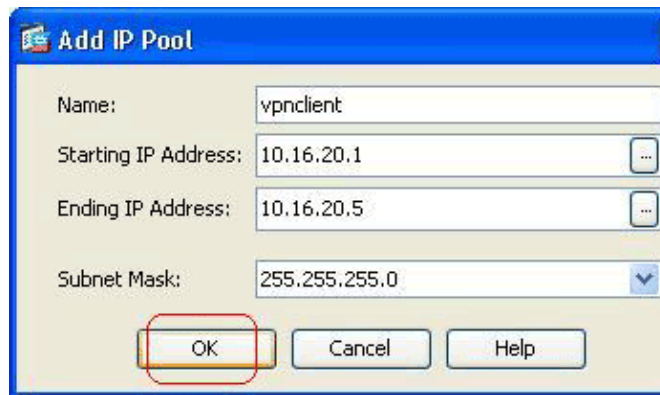
Complete these steps in order to configure a remote access VPN filter through the ASDM:

1. Create an address pool:
 - a. In the ASDM, choose **Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools**.



- b. Click **Add**.

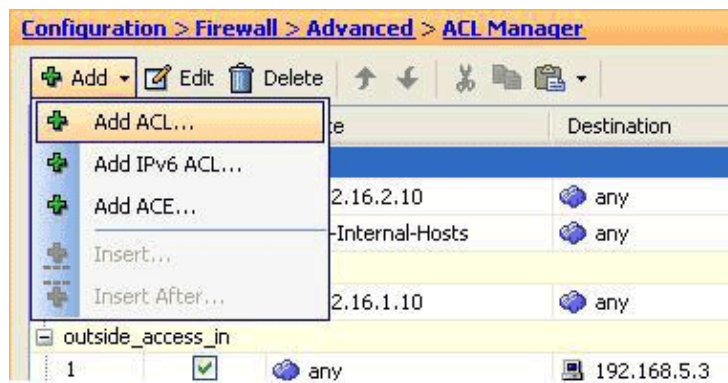
The Add IP Pool dialog box appears.



- c. Enter a name for the IP pool. This example uses *vpnclient*.
- d. Enter the starting and ending IP addresses, and then choose the subnet mask.
- e. Click **OK**.

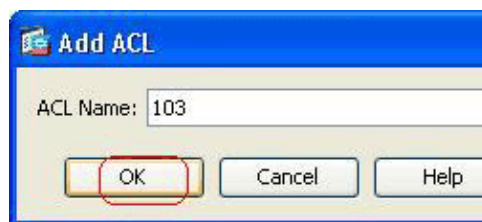
2. Add an access list to allow access to the domain server:

- a. In the ASDM, choose **Configuration > Firewall > Advanced > ACL Manager**.



- b. Click **Add**, and choose **Add ACL**.

The Add ACL dialog box appears.



- c. Enter **103** in the ACL Name field, and click **OK**.

3. Add an ACE:

- a. In the ACL list, right-click the 103 entry, and choose **Add ACE**.

The Add ACE dialog box appears.

Add ACE

Action: Permit Deny

Source: 10.16.20.0/24

Destination: 172.16.1.1

Service: ip

Description:

Enable Logging

Logging Level: Default

- b. Click the **Permit** option button.
- c. Enter the **10.16.20.0/24** network in the Source field, and enter **172.16.1.1** in the Destination field.
- d. Click the browse button (...) located next to the Service field.

The Browse Service dialog box appears.

Browse Service

+ Add Edit Delete Where Used

Filter:

| Name | Protocol | Source Ports | Destination Ports |
|--------------|----------|-------------------|-------------------|
| UDF cifs | udp | default (0-65535) | 3020 |
| UDF discard | udp | default (0-65535) | 9 |
| UDF dnstcp | tcp | default (0-65535) | 53 |
| UDF domain | udp | default (0-65535) | 53 |
| UDF echo | udp | default (0-65535) | 7 |
| UDF http | tcp | default (0-65535) | 80 |
| UDF isakmp | udp | default (0-65535) | 500 |
| UDF kerberos | udp | default (0-65535) | 750 |

- e. Select the *udp* protocol named *domain*, and click **OK** to return to the Add ACE dialog box.

Add ACE

Action: Permit Deny

Source: 10.16.20.0/24

Destination: 172.16.1.1

Service: udp/domain

Description:

Enable Logging

Logging Level: Default

More Options

OK Cancel

f. Click **OK**.

4. Add a new user:

a. In the ASDM, choose **Configuration > Remote Access VPN > AAA/Local Users > Local Users**.

Configuration > Remote Access VPN > AAA/Local Users > Local Users

Create entries in the ASA local user database.

Command authorization must be enabled in order for the user account privileges to be enforced. To enable command authorization, go to [Authorization](#).

AAA authentication console commands must be enabled in order for certain access restrictions to be enforced. To enable AAA authentication command go to [Authentication](#).

| Username | Privilege Level (Role) | Access Restrictions | VPN Group Policy | VPN Group Lock |
|-----------|------------------------|---------------------|----------------------------|----------------------------|
| test | 15 | Full | -- Inherit Group Policy -- | -- Inherit Group Policy -- |
| cisco | 15 | Full | -- Inherit Group Policy -- | -- Inherit Group Policy -- |
| enable_15 | 15 | Full | N/A | N/A |

Add Edit Delete

b. Click the **Add** button.

The Add User Account dialog box appears.

Add User Account

Identity

- VPN Policy

Username: vpn3000

Password: *****

Confirm Password: *****

User authenticated using MSCHAP

Access Restriction

Select one of the options below to restrict ASDM, SSH, Telnet

Note: All users have network access, regardless of these set

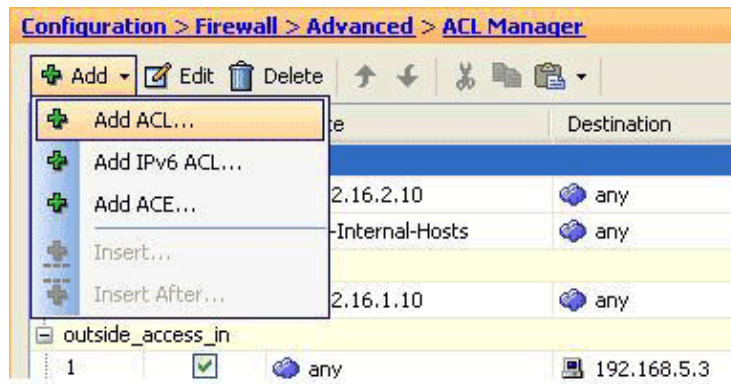
Full access(ASDM, SSH, Telnet and Console)

c. Enter a user name and password. This example uses *vpn3000* as the user name.

d. Click **OK**.

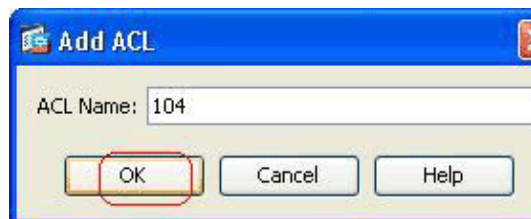
5. Create an access list to restrict access for the vpn3000 user:

- a. In the ASDM, choose **Configuration > Firewall > Advanced > ACL Manager**.



- b. Click **Add**, and choose **Add ACL**.

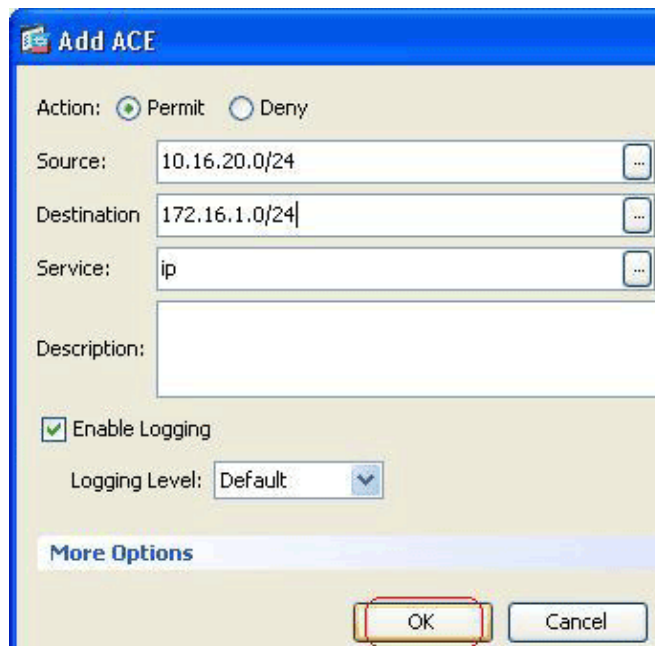
The Add ACL dialog box appears.



6. Add an ACE:

- a. In the ACL list, right-click the 104 entry, and choose **Add ACE**.

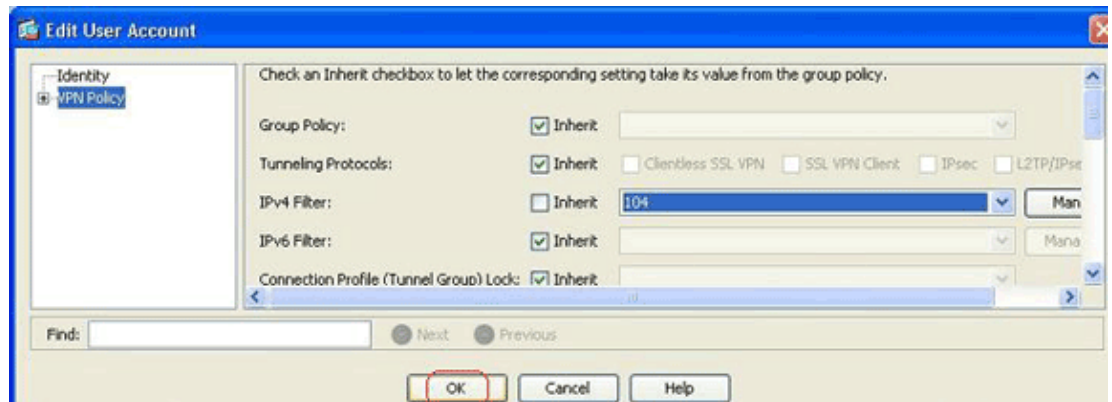
The Add ACE dialog box appears.



- b. Click the **Permit** option button.
c. Enter the **10.16.20.0/24** network in the Source field, and enter **172.16.1.0/24** in the Destination field.
d. Click **OK**.
7. Add the 104 access list as a filtering rule for the vpn3000 user:

- a. In the ASDM, choose **Configuration > Remote Access VPN > AAA/Local Users > Local Users**.
- b. Choose the **vpn3000** user, and click **Edit**.

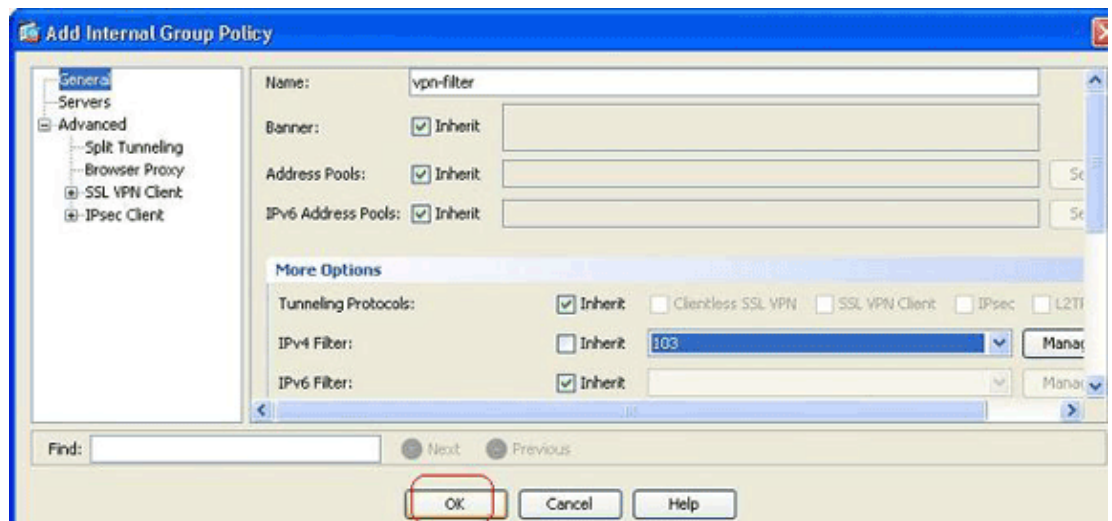
The Edit User Account dialog box appears.



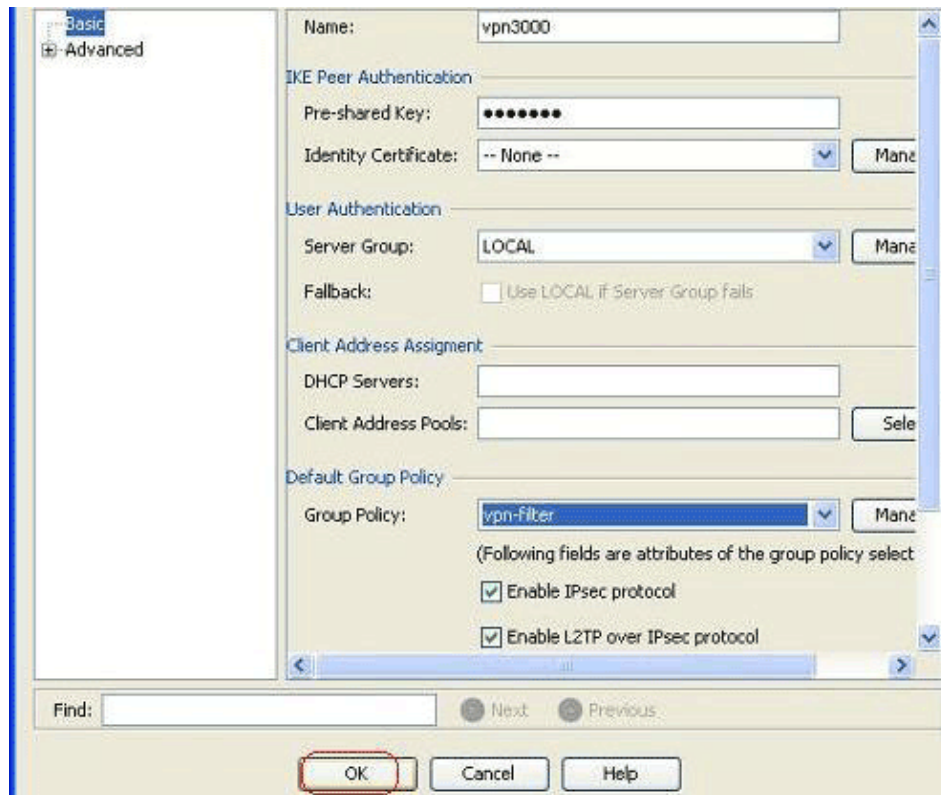
- c. Choose **104** from the IPv4 Filter drop-down list, and click **OK**.
8. Add the 103 access list to the vpn-filter group policy:

- a. In the ASDM, choose **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**, and then click **Add**.

The Add Internal Group Policy dialog box appears.



- b. Enter **vpn-filter** in the Name field, and choose **103** from the IPv4 Filter drop-down list.
 - c. Click **OK**.
9. Add the vpn-filter group policy as the default value for the vpn3000 connection profile:
- a. In the ASDM, choose **Configuration > Remote Access VPN > Network (Client) Access > IPsec Connection Profiles**, select the required tunnel group, and click **Edit**.



b. Choose **vpn-filter** from the Group Policy drop-down list, and click **OK**.

Related Information

- [Cisco PIX 500 Series Security Appliances](#)
- [Cisco ASA 5500 Series Adaptive Security Appliances](#)
- [Most Common L2L and Remote Access IPsec VPN Troubleshooting Solutions](#)
- [Cisco ASA 5500 Series Adaptive Security Appliances Troubleshoot and Alerts](#)
- [Technical Support & Documentation – Cisco Systems](#)

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

© 2010 – 2011 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Feb 21, 2011

Document ID: 99103
