

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

Document ID: 99103

Introduction

Prerequisites

- Requirements
- Components Used
- Related Products
- Conventions

Background Information

Configure

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

Related Information

Introduction

This document describes the procedure to use PIX/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.

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 Authentication Configuration Example for more information on how to configure Remote Access IPsec VPN in PIX/ASA 7.0 with Cisco VPN Client 4.x.

Components Used

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

- Cisco PIX 500 Series Security Appliance that runs version 7.x and later
- 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 5500 Series Adaptive Security Appliance (ASA) software 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 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.

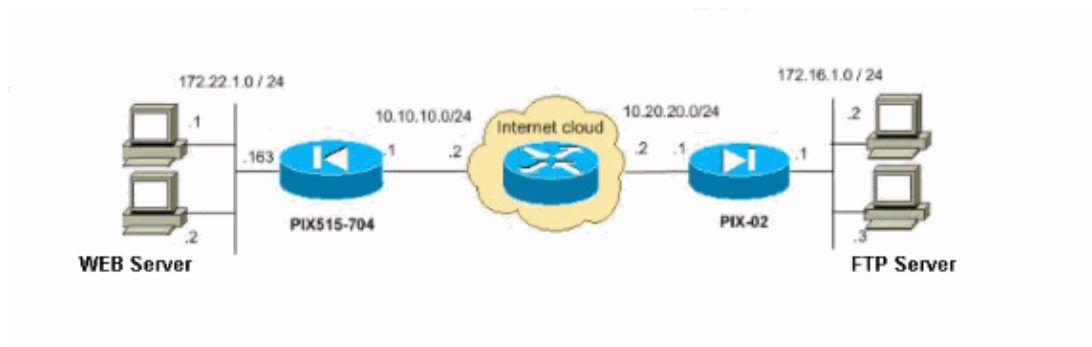
Configure

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:

| PIX515-704 |
|---|
| <pre> PIX515-704# show running-config 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 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. tunnel-group 10.20.20.1 general-attributes default-group-policy filter !--- Associate the group policy (filter) with the tunnel group. </pre> |

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 is illustrated 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.

```
PIX515-704# show running-config
```

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

```
access-list 103 permit tcp 172.16.1.0 255.255.255.0 host 172.22.1.1 eq 80
```

```
!--- 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 103 permit tcp host 172.16.1.3 eq 21 172.22.1.0 255.255.255.0
```

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

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

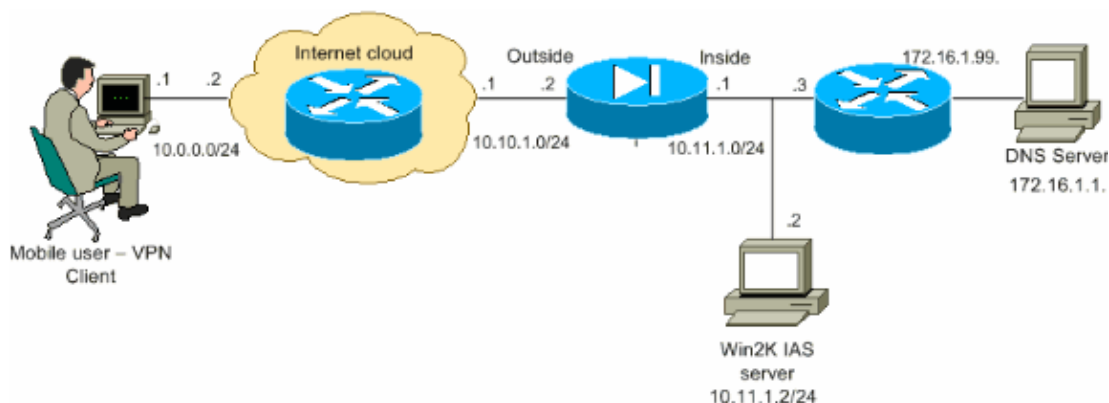
```
!--- Create the group policy (filter) and specify the access list number  
!--- in the vpn filter command.
```

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

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

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:

PIX

```
PIX# show running-config
```

```
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 netowrk 172.16.1.0/24
```

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

```
username vpn3000 password nPtKy7KDCerzhKeX 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.
```

```
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.
```

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

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

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](#)

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

Updated: Oct 10, 2008

Document ID: 99103
