

Application Note

Cisco Router and Security Device Manager **Firewall Policy Management**

Introduction

Security administrators can easily and quickly manage access control lists (ACLs) and packet-inspection rules through a graphical and intuitive Firewall Wizard and Firewall Policy table available with Cisco® Router and Security Device Manager (SDM).

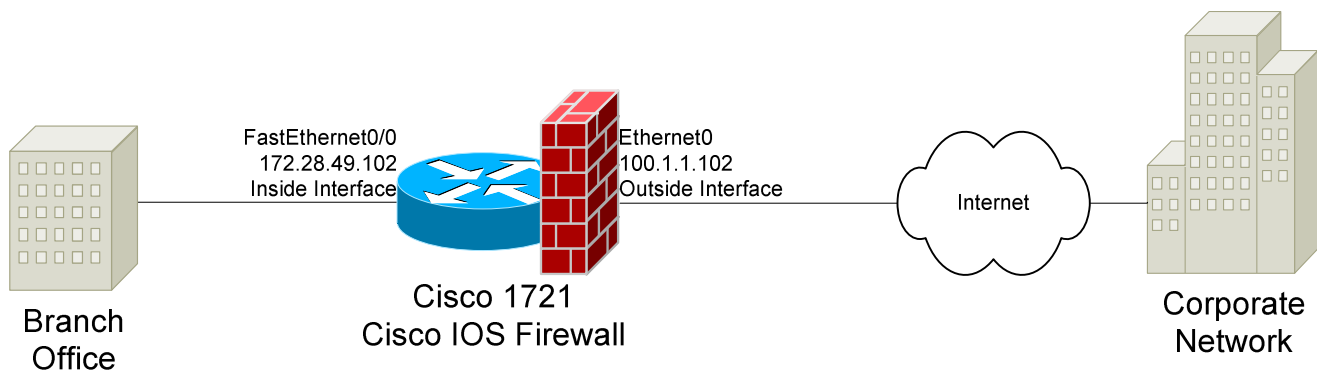
Cisco IOS Firewall

Cisco IOS® Firewall applies access lists and inspection rules to a traffic flow at inbound or outbound router interfaces.

Deployment Scenario

Figure 1 shows the deployment of a branch-office Internet firewall without the Cisco SDM Firewall Wizard and Firewall Policy support. The Cisco IOS Firewall resides in a branch office, with the outside (Ethernet0) interface connected to the corporate network via the Internet, and the inside (Fast Ethernet0/0) interface connected to the branch-office subnet.

Figure 1 Branch Office Internet Firewall Deployment Scenario



The deployment involves two steps: basic firewall configuration and branch office-specific configuration.

Branch Office Internet Firewall Sample Configuration

Basic Firewall Configuration

The basic firewall configuration is generic to all Cisco IOS firewalls. The Cisco IOS Firewall is configured to protect the branch office by denying local loopback traffic and broadcast traffic, and by denying spoofing packets on both inside and outside interfaces. The inspection rules are applied to the outbound packets of the outside interface.

The following are the Cisco IOS Software commands necessary to configure a basic firewall for this deployment scenario.

!



```
! acl 101 for outside interface
! turn on unicast reverse path forwarding check
! permit IPSec tunnel traffic
! permit GRE tunnel traffic
! deny spoofing traffic
! deny broadcast, local loopback and private address
!
access-list 101 deny ip 172.28.49.96 0.0.0.31 any
access-list 101 permit icmp any host 100.1.1.102 echo-reply
access-list 101 permit icmp any host 100.1.1.102 time-exceeded
access-list 101 permit icmp any host 100.1.1.102 unreachable
access-list 101 deny ip 10.0.0.0 0.255.255.255 any
access-list 101 deny ip 172.16.0.0 0.15.255.255 any
access-list 101 deny ip 192.168.0.0 0.0.255.255 any
access-list 101 deny ip 127.0.0.0 0.255.255.255 any
access-list 101 deny ip host 255.255.255.255 any
access-list 101 deny ip host 0.0.0.0 any
access-list 101 deny ip any any log
!
! acl 100 for inside interface
! deny spoofing traffic
! deny broadcast and local loopback addresses
! permit all other traffic
!
access-list 100 deny ip 10.1.0.0 0.0.255.255 any
access-list 100 deny ip host 255.255.255.255 any
access-list 100 deny ip 127.0.0.0 0.255.255.255 any
access-list 100 permit ip any any
!
! CBAC inspection rules for outbound packets on outside interface
!
ip inspect name DEFAULT100 cuseeme
```



```
ip inspect name DEFAULT100 ftp
ip inspect name DEFAULT100 h323
ip inspect name DEFAULT100 netshow
ip inspect name DEFAULT100 rcmd
ip inspect name DEFAULT100 realaudio
ip inspect name DEFAULT100 rtsp
ip inspect name DEFAULT100 smtp
ip inspect name DEFAULT100 sqlnet
ip inspect name DEFAULT100 streamworks
ip inspect name DEFAULT100 tftp
ip inspect name DEFAULT100 tcp
ip inspect name DEFAULT100 udp
ip inspect name DEFAULT100 vdolive
ip inspect name DEFAULT100 icmp
!
!  acl 101 is applied to outside interface E0 inbound traffic
!
interface Ethernet0
  description Outside Interface
  ip access-group 101 in
  ip inspect DEFAULT100 out
  ip verify unicast reverse-path
  exit
!
!  acl 100 is applied to inside interface FE0 inbound traffic
!
interface FastEthernet0
  description Inside Interface
  ip access-group 100 in
!
```

Branch Office-Specific Firewall Configuration



The next step is to allow specific protocols that will be used in this deployment scenario. The protocols allowed on the branch office Internet firewall are telnet, FTP, and HTTP for both outside and inside traffic. Inspect the traffic from the branch-office subnet and the traffic from the corporate network.

```
!  
!  
! Firewall inspection is setup for bi-directionally for traffic to/from  
!  
! the Corporate and Branch network.  
!  
ip inspect name BranchFIRE ftp  
ip inspect name BranchFIRE tcp  
!  
! FE0 the inside interface to the Branch Office subnet  
!  
interface FastEthernet0  
    ip address 172.28.49.102 255.255.255.0  
    ip access-group 111 in      ! allows specific traffic  
                               from the Branch Office subnet  
                               Also denies unwanted traffic  
                               to the Corporate Network  
    ip inspect BranchFIRE in ! FW inspect traffic from the  
                               Branch Office subnet  
!  
! E0 the outside interface to the Cooperate Network  
!  
interface Ethernet0  
    ip address 100.1.1.102 255.255.255.0  
    ip access-group 121 in      ! allows specific traffic from the  
                               Cooperate Network.  
                               Also denies unwanted traffic to  
                               the Branch Office  
    ip inspect BranchFIRE in ! Fw inspect traffic from the  
                               Corporate Network  
!  
!  
! acl 111 allows the initial packets sourced from the Branch Office.
```



```
! Packets are then inspected by the firewall rules.
!
access-list 111 permit tcp 172.28.49.0 0.0.0.255 any eq telnet
access-list 111 permit tcp 172.28.49.0 0.0.0.255 any eq ftp
access-list 111 permit tcp 172.28.49.0 0.0.0.255 any eq www
!
! similar to ael 111, ael 121 allows the initial packets sourced from
! the Corporate Network to be inspected.
!
access-list 121 permit tcp 100.1.1.0 0.0.0.255 any eq telnet
access-list 121 permit tcp 100.1.1.0 0.0.0.255 any eq ftp
access-list 121 permit tcp 100.1.1.0 0.0.0.255 any eq www
!
! Last, the user must merge the Basic Firewall configuration and the Branch Office
! Specific Firewall configuration manually.
!
ip inspect name DEFAULT100 cuseeme
ip inspect name DEFAULT100 ftp
ip inspect name DEFAULT100 h323
ip inspect name DEFAULT100 netshow
ip inspect name DEFAULT100 rcmd
ip inspect name DEFAULT100 realaudio
ip inspect name DEFAULT100 rtsp
ip inspect name DEFAULT100 smtp
ip inspect name DEFAULT100 sqlnet
ip inspect name DEFAULT100 streamworks
ip inspect name DEFAULT100 tftp
ip inspect name DEFAULT100 tcp
ip inspect name DEFAULT100 udp
ip inspect name DEFAULT100 vdolive
ip inspect name DEFAULT100 icmp
ip inspect name BranchFIRE ftp
```



```
ip inspect name BranchFIRE tcp
ip audit notify log
ip audit po max-events 100
no ftp-server write-enable
!
interface Ethernet0
  description $FW_OUTSIDE$$ETH-LAN$
  ip address 100.1.1.102 255.255.255.0
  ip access-group 101 in
  ip verify unicast reverse-path
  ip inspect BranchFIRE in
  ip inspect DEFAULT100 out
  half-duplex
!
interface FastEthernet0
  description $FW_INSIDE$$ETH-LAN$$ETH-SW-LAUNCH$
  ip address 172.28.49.102 255.255.255.224
  ip access-group 100 in
  speed auto
!
!
access-list 100 remark auto generated by SDM firewall configuration
access-list 100 remark SDM_ACL Category=1
access-list 100 remark Allow www from Branch Office to outside network
access-list 100 permit tcp 0.0.0.102 255.255.255.0 any eq www
access-list 100 remark allow ftp from Branch Office to outside network
access-list 100 permit tcp 0.0.0.102 255.255.255.0 any eq ftp
access-list 100 remark allow telnet from Branch Office to outside network
access-list 100 permit tcp 0.0.0.102 255.255.255.0 any eq telnet
access-list 100 deny ip 100.1.1.0 0.0.0.255 any
access-list 100 deny ip host 255.255.255.255 any
access-list 100 deny ip 127.0.0.0 0.255.255.255 any
```



```
access-list 100 permit ip any any
access-list 101 remark auto generated by SDM firewall configuration
access-list 101 remark SDM_ACL Category=1
access-list 101 permit tcp 0.0.0.0 255.255.255.0 any eq www
access-list 101 permit tcp 0.0.0.0 255.255.255.0 any eq ftp
access-list 101 permit tcp 0.0.0.0 255.255.255.0 any eq telnet
access-list 101 deny ip 172.28.49.96 0.0.0.31 any
access-list 101 permit icmp any host 100.1.1.102 echo-reply
access-list 101 permit icmp any host 100.1.1.102 time-exceeded
access-list 101 permit icmp any host 100.1.1.102 unreachable
access-list 101 deny ip 10.0.0.0 0.255.255.255 any
access-list 101 deny ip 172.16.0.0 0.15.255.255 any
access-list 101 deny ip 192.168.0.0 0.0.255.255 any
access-list 101 deny ip 127.0.0.0 0.255.255.255 any
access-list 101 deny ip host 255.255.255.255 any
access-list 101 deny ip host 0.0.0.0 any
access-list 101 deny ip any any log
!
```

Cisco SDM Firewall Support

Cisco SDM allows users to easily configure Cisco IOS Firewall security features. The following steps are used to configure the same deployment scenario, this time using Cisco SDM as opposed to the Cisco IOS Software CLI.

Basic Firewall Configuration

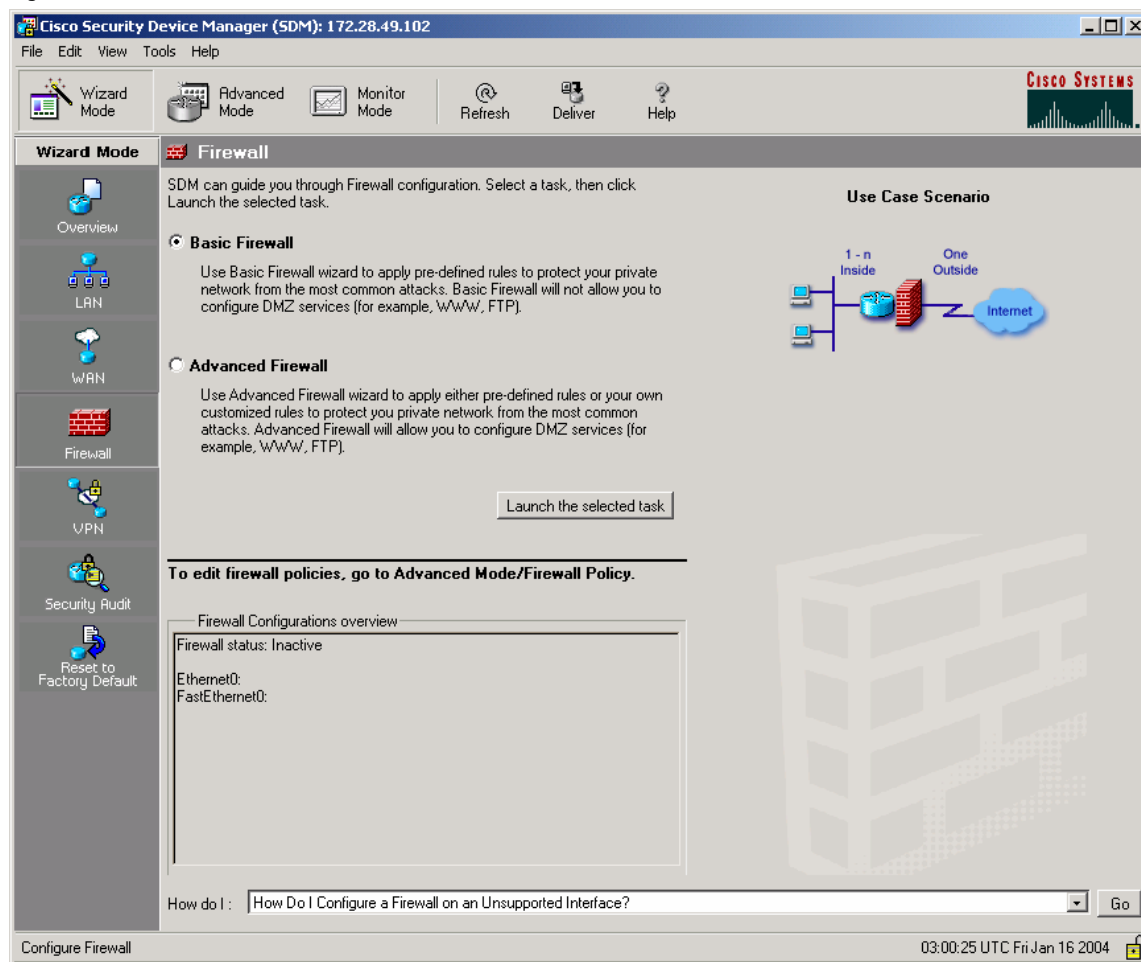
The Cisco SDM Firewall Wizard can secure the branch-office firewall by using predefined rules to allow private-network users to access the Internet, and protect the private network from the most common outside attacks. The Firewall Wizard is capable of the following:

- Applying default access rules to inside and outside interfaces
- Applying default inspection rules to outside interface
- Enabling IP Unicast Reverse Path Forwarding (RPF) on the outside interface

Users invoke the Cisco SDM Firewall Wizard from Wizard mode and launch the Basic Firewall wizard assuming that no demilitarized zone (DMZ) is required, as in this example. If a DMZ is to be used, use the Advanced Firewall wizard instead. The Firewall Wizard (Figure 2) guides you through the basic firewall configuration.



Figure 2 Cisco SDM Firewall Wizard



Once the basic firewall is configured using the wizard, use the Cisco SDM Firewall Policy view to display and alter the firewall configuration further if desired.

Cisco SDM Firewall Policy

The Cisco SDM Firewall Policy is composed of the Firewall Policy views. A view displays the access rights for a particular traffic flow and the inspection rules on a particular interface.

Take a look at Access List 100, which is applied to the inbound traffic at the inside interface. The Cisco IOS Software CLI commands are scattered throughout the running configuration, requiring users to examine the entire configuration to understand the access rights of a traffic flow at an interface. Now with the Cisco SDM Firewall Policy Table, it is simple and easy to relate the traffic flow and interfaces where the access lists are applied using the graphical interface.



Figure 3 depicts the traffic originating from the branch-office subnet filtered by Access List 100. The traffic is inspected by the inspection rule DEFAULT100 (created by the Basic Firewall Wizard).

Figure 3 Inbound Traffic at Inside Interface (FastEthernet0)

Wizard mode firewall status: Active 03:35:52 UTC Fri Jan 16 2004

Action	Source	Destination	Service	Log	Option	Description
Deny	100.1.1.0/0.0.0.255	any	IP	ip		
Deny	255.255.255.255	any	IP	ip		
Deny	127.0.0.0/0.255.2	any	IP	ip		
Permit	any	any	IP	ip		

Application Protocol	Description
cuseeme	CUSeeMe Protocol
ftp	File Transfer Protocol
h323	H.323 Protocol (e.g., MS NetMeeting, Intel Video Phone)
netshow	Microsoft NetShow Protocol
rcmd	UNIX R commands (rlogin, rexec, rsh)

The Cisco SDM Firewall Policy Table also can show the returning traffic via the **Returning traffic** radio button.



Figure 4 shows the returned traffic from the corporate network that enters the Cisco IOS Firewall outside (Ethernet0) interface. Access List 101 is used to filter the traffic.

Figure 4 Inbound Traffic at Outside Interface (Ethernet0)

The screenshot displays the Cisco IOS Firewall Policy View in Advanced Mode. The configuration is for the FastEthernet0 to Ethernet0 interface. The traffic direction is set to 'Returning traffic'. The Firewall Feature Availability is 'Available', the Access Rule is '101', and the Inspection Rule is 'DEFAULT100'. The Services section shows a list of rules for 'Ethernet0 - inbound' traffic.

Action	Source	Destination	Service	Log	Option	Description
Deny	172.28.49.96/0.0	any	ip			ip
Permit	any	100.1.1.102	echo-reply			echo-reply
Permit	any	100.1.1.102	time-exceed			time-exceed
Permit	any	100.1.1.102	unreachable			unreachable
Deny	10.0.0.0/0.255.25	any	ip			ip
Deny	172.16.0.0/0.15.2	any	ip			ip
Deny	192.168.0.0/0.0.2	any	ip			ip
Deny	127.0.0.0/0.255.2	any	ip			ip
Deny	255.255.255.255	any	ip			ip
Deny	0.0.0.0	any	ip			ip
Deny	any	any	ip		Log	ip

The Applications section shows a list of protocols and their descriptions:

Application Protocol	Description
cuseeme	CUseeMe Protocol
ftp	File Transfer Protocol
h323	H.323 Protocol (e.g., MS NetMeeting, Intel Video Phone)
netshow	Microsoft NetShow Protocol
rcmd	UNIX R commands (rlogin, rexec, rsh)

Wizard mode firewall status: Active 03:37:52 UTC Fri Jan 16 2004



Figure 5 shows the traffic originating from the Internet enter the Cisco IOS Firewall outside (Ethernet0) interface. Access List 101 is used to filter the traffic.

Figure 5 Access List 101—Inbound Traffic at Outside Interface

The screenshot displays the Cisco Firewall Policy View interface. At the top, it shows the direction of traffic: From: Ethernet0, To: FastEthernet0. Below this, a diagram illustrates the traffic flow from the Internet through the Ethernet0 interface, through the Cisco IOS Firewall, and then through the FastEthernet0 interface. The status of the firewall is shown as 'IOS Firewall : Inactive (from Ethernet0 to FastEthernet0)'.

The main configuration area shows the 'Access Rule: 101' and 'Inspection Rule: Ethernet0 - inbound'. The 'Services' section includes a list of rules:

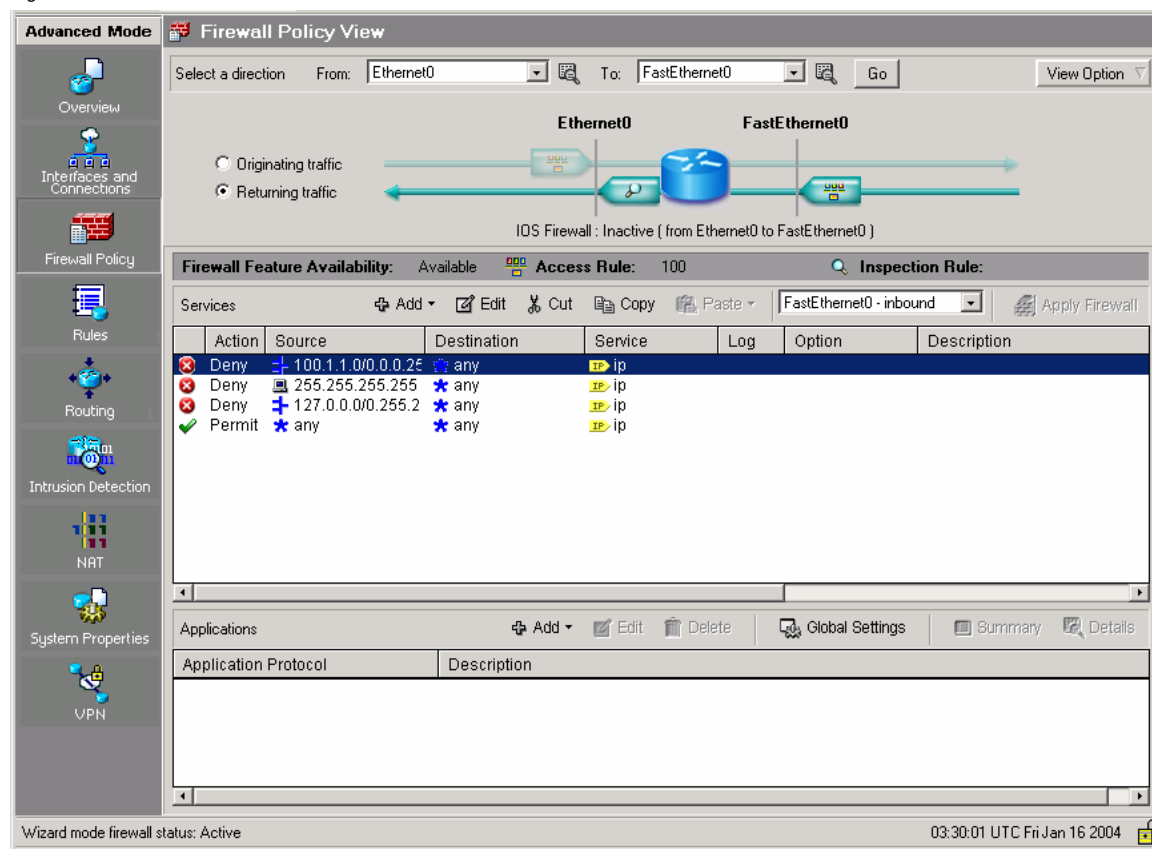
Action	Source	Destination	Service	Log	Option	Description
Deny	172.28.49.96/0.0	any	ip			
Permit	any	100.1.1.102	echo-reply			
Permit	any	100.1.1.102	time-exceede			
Permit	any	100.1.1.102	unreachable			
Deny	10.0.0.0/0.255.25	any	ip			
Deny	172.16.0.0/0.15.2	any	ip			
Deny	192.168.0.0/0.0.2	any	ip			
Deny	127.0.0.0/0.255.2	any	ip			
Deny	255.255.255.255	any	ip			
Deny	0.0.0.0	any	ip			
Deny	any	any	ip	Log		

The 'Applications' section is currently empty. The status bar at the bottom indicates 'Wizard mode firewall status: Active' and the time '03:26:46 UTC Fri Jan 16 2004'.



The returned traffic from the branch-office subnet enters the Cisco IOS Firewall inside (FastEthernet0) interface (Figure 6). Access list 100 is used to filter the traffic.

Figure 6 Access List 100—Inbound Traffic at Inside Interface



Branch Office-Specific Firewall Configuration

Look at Access List 111, which is applied to the inbound traffic to allow telnet, FTP, and HTTP traffic to enter the inside (FastEthernet0) interface. The user must merge the basic firewall configuration and the branch office-specific firewall together. To do this, merge the entries of Access List 111 to Access List 100.

Access List 111

```
!  
access-list 111 permit tcp 172.28.49.0 0.0.0.255 any eq telnet  
access-list 111 permit tcp 172.28.49.0 0.0.0.255 any eq ftp  
access-list 111 permit tcp 172.28.49.0 0.0.0.255 any eq www  
!
```

Now, with the Cisco SDM Firewall Policy Table, it is simple and easy to add and merge the access entries to the Access List 100.

BranchFIRE inspection rule will inspect the inbound traffic at the outside (Ethernet0) interface.



Merging Access Lists

To use Cisco SDM Firewall Policy Table to merge access lists, take the following steps:

- At **Advanced Mode**, select **Firewall Policy**
- Select a Direction from **FastEthernet0** to **Ethernet0**
- Go to Firewall Feature/Service panel
- Click **Add**, select **Insert Before**
- Fill in the information, click **OK**
- Action: **Permit**
- Source Host/Network:
 - Type: **A Network/172.28.49.102/24**
- Destination Host/Network:
 - Type: **Any IP Address**
- Protocol and service:
 - **TCP**/Source Port Service = **any**/Destination Port Service = **telnet**

Figure 7 shows the Add an Extended Rule Entry screen.



Figure 7 Add an Extended Rule Entry

Add an Extended Rule Entry [X]

Action
Select an action:

Description

Source Host/Network
Type:

Destination Host/Network
Type:

Protocol and Service
 TCP UDP ICMP IP

IP Protocol
IP protocol: ...

Log matches against this entry

OK Cancel Help



Currently the configuration changes performed using Cisco SDM have not been delivered to the router. To do so, on the Cisco SDM Menu Bar, click **Deliver**. If the preview command option is selected, you can see the actual commands that will be delivered to the router (Figure 8).

Figure 8 Cisco IOS Software CLI Commands Generated by Cisco SDM Firewall Policy Table

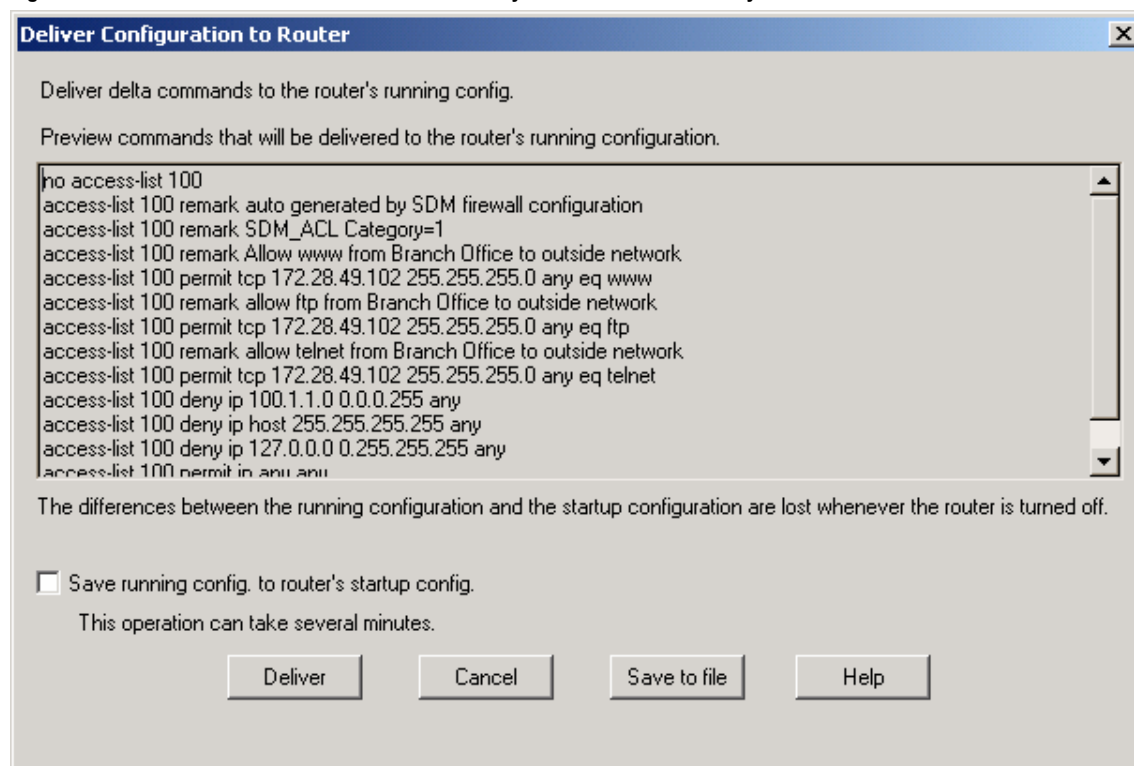


Figure 9 shows merged Access List 100.



Figure 9 Merged Access List 100

Cisco Security Device Manager (SDM): 172.28.49.102

File Edit View Tools Help

Wizard Mode Advanced Mode Monitor Mode Refresh Deliver Help

Advanced Mode Firewall Policy View

Select a direction From: FastEthernet0 To: Ethernet0 Go View Option

FastEthernet0 Ethernet0

Originating traffic
 Returning traffic

IOS Firewall: Active (from FastEthernet0 to Ethernet0)

Firewall Feature Availability: Available Access Rule: 100 Inspection Rule: DEFAULT100

Services Add Edit Cut Copy Paste FastEthernet0 - inbound Apply Firewall

Action	Source	Destination	Service	Log	Option	Description
✓ Permit	172.28.49.102/25	any	tcp dest: www/tcp			Allow www from Branch Office t
✓ Permit	172.28.49.102/25	any	tcp dest: ftp/tcp			allow ftp from Branch Office to d
✓ Permit	172.28.49.102/25	any	tcp dest: telnet/tcp			allow telnet from Branch Office
✗ Deny	100.1.1.0/0.0.0.255	any	ip ip			
✗ Deny	255.255.255.255	any	ip ip			
✗ Deny	127.0.0.0/0.0.0.255	any	ip ip			
✓ Permit	any	any	ip ip			

Applications Add Edit Delete Global Settings Summary Details

Application Protocol	Description
cuseeme	CUSeeMe Protocol
ftp	File Transfer Protocol
h323	H.323 Protocol (e.g. MS NetMeeting, Intel Video Phone)
netshow	Microsoft NetShow Protocol
rcmd	UNIX R commands (rlogin, rexec, rsh)

Wizard mode firewall status: Active 04:02:13 UTC Fri Jan 16 2004



Using the Firewall Policy Table to Create Inspection Rules

To create inspection rules, apply BranchFIRE inspection rule to the inbound traffic at the outside (Ethernet0) interface. Then take the following steps:

- At **Advanced Mode**, select **Firewall Policy**
- Select a Direction from **Ethernet0 to FastEthernet0**
- Go to **Application** panel
- Click **Add**, select **Add...**
- Fill in the information, click **OK**

In the Inspection Rule Editor (Figure 10), the Inspection Rule Name is **BranchFIRE**. Check Protocols **tcp** and **udp**.

Figure 10 Inspection Rule Editor

Protocol	Alert	Audit Trail	Timeout(sec):
<input type="checkbox"/> icmp	default(on) ▾	default(off) ▾	10
<input type="checkbox"/> netshow	default(on) ▾	default(off) ▾	3600
<input type="checkbox"/> rcmd	default(on) ▾	default(off) ▾	3600
<input type="checkbox"/> realaudio	default(on) ▾	default(off) ▾	3600
<input type="checkbox"/> rpc	default(on) ▾	default(off) ▾	30
<input type="checkbox"/> rtsp	default(on) ▾	default(off) ▾	3600
<input type="checkbox"/> sip	default(on) ▾	default(off) ▾	30
<input type="checkbox"/> skinny	default(on) ▾	default(off) ▾	3600
<input type="checkbox"/> smtp	default(on) ▾	default(off) ▾	3600
<input type="checkbox"/> sqlnet	default(on) ▾	default(off) ▾	3600
<input type="checkbox"/> streamworks	default(on) ▾	default(off) ▾	30
<input checked="" type="checkbox"/> tcp	default(on) ▾	default(off) ▾	3600
<input type="checkbox"/> tftp	default(on) ▾	default(off) ▾	30
<input checked="" type="checkbox"/> udp	default(on) ▾	default(off) ▾	30
<input type="checkbox"/> vdolive	default(on) ▾	default(off) ▾	3600

Option...

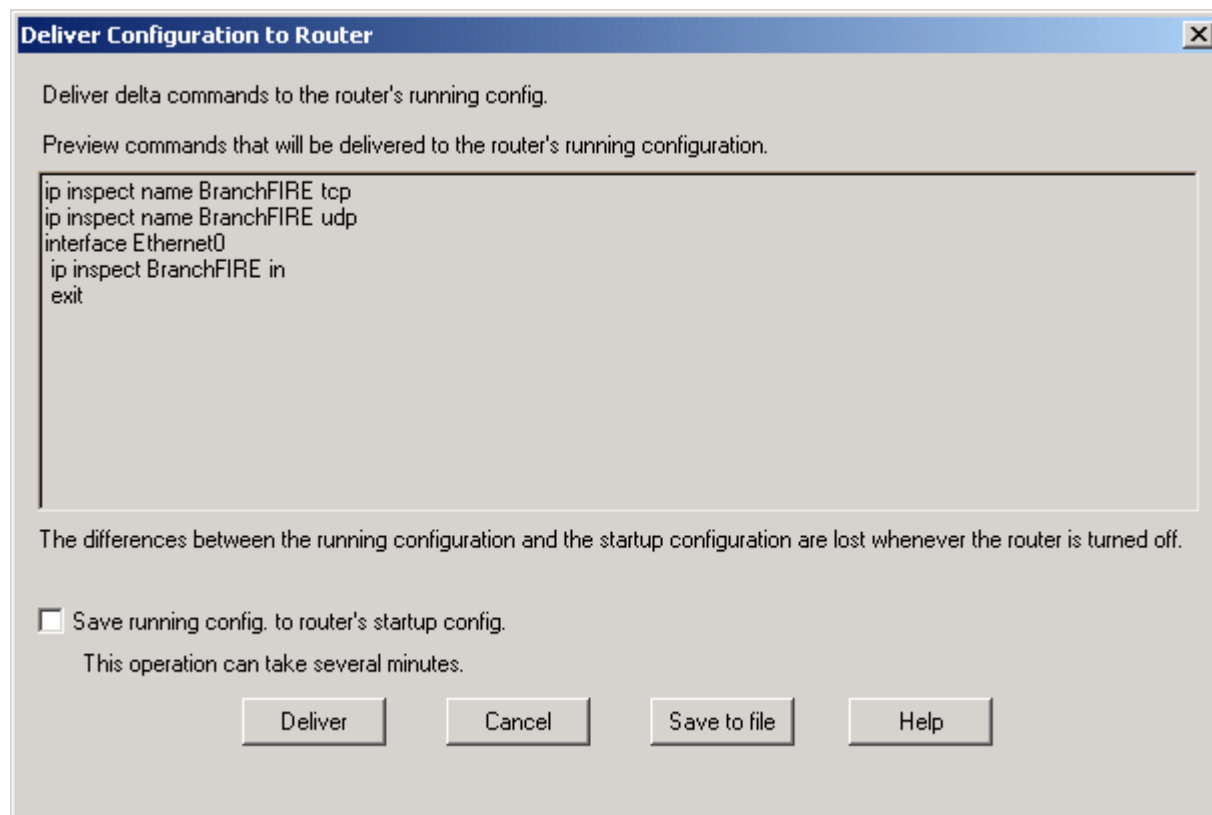
Insert additional RPC protocol entries

OK Cancel Help



Deliver the changes to the router (Figure 11). At the Menu Bar, click **Deliver**.

Figure 11 Cisco IOS Software CLI Commands Generated by Cisco SDM Firewall Policy Table



In summary, by using Cisco SDM Firewall Wizard and Firewall Policy Table, users can generate the same complex firewall configuration easily and quickly with minimum knowledge of Cisco IOS Software commands and minimal security knowledge. In addition, the Policy View provides users with a graphical interface to view the details of the firewall policies with access rights, traffic flows, and interfaces.

**Corporate Headquarters**

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters

Cisco Systems International
BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Web site at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2004 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, the Cisco Systems logo, and Cisco IOS are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0402R)