2006 年 4 月（第 1 版）

Cisco Security Device Manager サンプル設定ガイド

SDM 2.1.2 2005/09 リリース版

Cisco IOS Firewall ポリシー設定

I 概　要

Cisco IOS ファイアウォールは、ルータ インターフェイスの送受信トラフィックフローについてアクセスリストとインスペクションルールを適用し、通過させるべきトラフィックかそうでないものかを評価します。セキュリティ管理者は、Cisco Router SDM（Security Device Manager）が提供するグラフィカルで直感的なファイアウォールウィザードとファイアウォールポリシーテーブルを通じて、アクセスコントロールリスト（ACL）やパケットインスペクションルールの管理を行うことができます。

支店に Cisco IOS ファイアウォール機能を搭載したルータをインターネット ファイアウォールとして導入する例を考えます。（図 1）この IOS ファイアウォールは、外部インターフェイス（Fast Ethernet 1）がインターネットを通じて本社ネットワークに接続され、内部インターフェイス（Fast Ethernet 0）が支店/営業所のネットワークに接続されています。

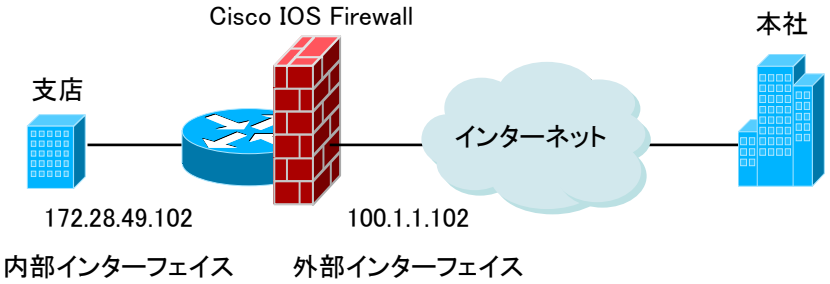

図 1：インターネットファイアウォール構成

この導入例では次の 2 つの手順、(1)基本となるファイアウォール設定、(2)支店/営業所固有の設定が含まれます。Cisco SDM を使用せず、オーソドックスなコマンドラインイン ターフェイス（CLI）で行う設定例を最初に説明します。

1. CLI ベースで行う基本ファイアウォール構成

まず、Cisco IOS Firewall の CLI での設定例をあげます。

基本ファイアウォール設定は、すべての Cisco IOS ファイアウォールに共通しています。この IOS ファイアウォールはブロードキャスト トラフィックやローカルループバックトラフィックを禁止し、また外部/内部インターフェイスの双方で成りすましパケットを禁止することにより支店を守るよう構成されます。インスペクションルールは外部インターフェイスから送信されるパケットに適用されます。以下は本導入シナリオで必要とされる基本的なファイアウォール設定のコマンドです。

(1) 外部インターフェイス向けの ACL101

ユニキャストの逆パス転送チェックの有効化

IPSec トンネルトラフィックの許可

GRE トンネルトラフィックの許可

成りすましトラフィックの禁止

ブロードキャスト、ローカルループバックならびにプライベートアドレスの禁止

```
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
```

(2) 内部インターフェイス向け ACL100

成りすましトラフィックの禁止

ブロードキャスト・ローカルループバックアドレスの禁止

それ例外のすべてのトラフィックを許可

```
!
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
```

(3) 外部インターフェイスからの送信パケットに対する CBAC インスペクションルール

```
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
```

(4) ACL101 を外部インターフェイス（Fast Ethernet 1）の受信トラフィックに適用

```
interface FastEthernet1
description Outside Interface
ip access-group 101 in
ip inspect DEFAULT100 out
ip verify unicast reverse-path
exit
```

(5) ACL100 を内部インターフェイス（Fast Ethernet 0）の受信トラフィックに適用

```
interface FastEthernet0
description Inside Interface
ip access-group 100 in
```

2. 支店側ファイウォール構成

次のステップは、本導入シナリオで使われる特定のプロトコルの許可を行います。支店からのインターネットアクセスで許可されるプロトコルは telnet、FTP、HTTP の送受信です。支店のネットワークからのトラフィック、ならびに本社ネットワークからのトラフィックを検査します。

(1) ファイアウォールによるパケット検査の有効化

```
ip inspect name BranchFIRE ftp
ip inspect name BranchFIRE tcp
```

(2) 支店内部インターフェイス（Fsat Ethernet 0）

支店ネットワークからの特定トラフィックの許可と本社ネットワークへの想定外トラフィックの禁止

```
interface FastEthernet0
ip address 172.28.49.102 255.255.255.0
ip access-group 111 in
```

(3) 本社ネットワークへの外部インターフェイス（Fast Ethernet 1）

ファイアウォールインスペクション：インターネットからのトラフィックの追加

```
interface FastEthernet1
ip address 100.1.1.102 255.255.255.0
ip inspect BranchFIRE in

!
```

(4) ACL111：支店ネットワークを送信元とするパケットの許可

```
!
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
access-list 111 permit ip any host 172.28.49.102

!
```

最後に、ユーザは基本ファイウォール設定と支店/営業所特定のファイアウォール設定を手動で結合する必要があります。

```
!
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
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
ip address 172.28.49.102 255.255.255.224
```

```
ip access-group 100 in
speed auto
!
!
access-list 100 remark Allow www from Branch Office to outside network
access-list 100 permit tcp 172.28.49.0 0.0.0.255 any eq www
access-list 100 remark allow ftp from Branch Office to outside network
access-list 100 permit tcp 172.28.49.0 0.0.0.255 any eq ftp
access-list 100 remark allow telnet from Branch Office to outside network
access-list 100 permit tcp 172.28.49.0 0.0.0.255 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 host 172.28.49.102
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
!
```

II 設 定 手 順

ユーザは Cisco SDM を利用することにより、Cisco IOS ファイアウォール機能を簡単に設定することができます。先に CLI で設定したものを SDM で設定していきます。

1. 基本 Firewall 構成

Cisco SDM ファイアウォールウィザードは、プライベートネットワーク(LAN)のユーザがインターネットへ接続するために必要なルールがあらかじ定義されています。ファイアウォールウィザードでは以下の機能をサポートしています。

(1) 外部/内部インターフェイスへの既定のアクセスルールの適用

(2) 外部インターフェイスへの既定のインスペクションルールの適用

(3) 外部インターフェイスでのユニキャストリバースパス転送の有効化

この例では、Cisco SDM ファイアウォールウィザードを使用して DMZ のない基本的なファイアウォールを構成します。DMZ を使用する場合には、基本ファイアウォール設定ウィザードの代わりに拡張ファイアウォール設定ウィザードを使用します。ファイアウォールと ACL タスク画面の[ファイアウォールの作成]タブで「基本ファイアウォール」を選択し、「選択したタスクを実行する」をクリックして基本ファイアウォール設定ウィザードを起動します。(図 2)

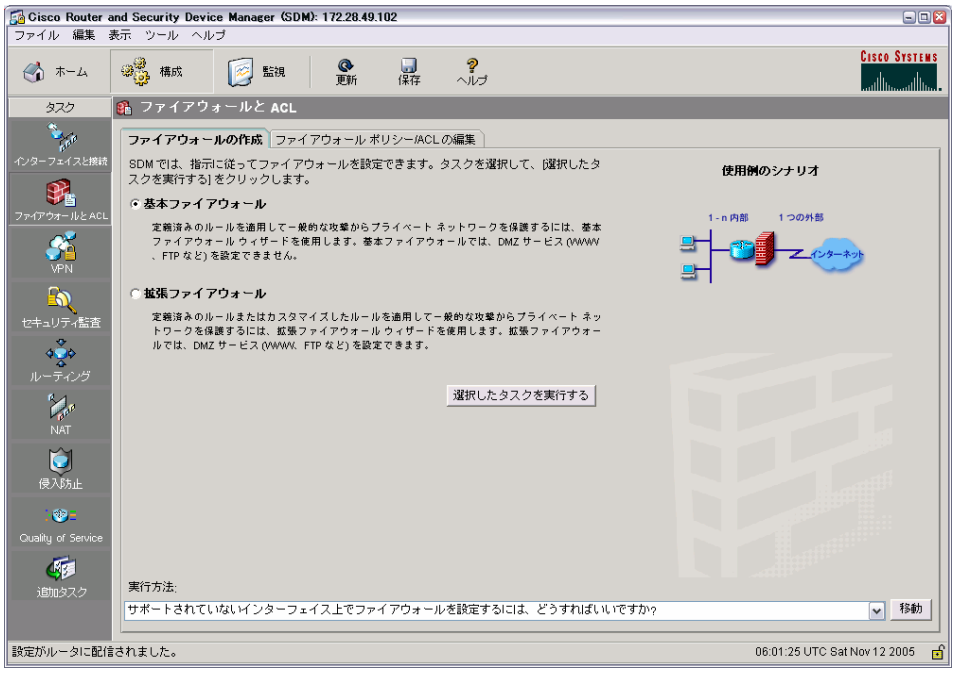

図 2:ファイアウォールと ACL

起動した基本ファイアウォール設定ウィザードに従って、内部ネットワークを外部ネットワークから保護する、安全なインターネットアクセス設定を行います（図 3）。

「次へ」をクリックし、次の画面に進みます。

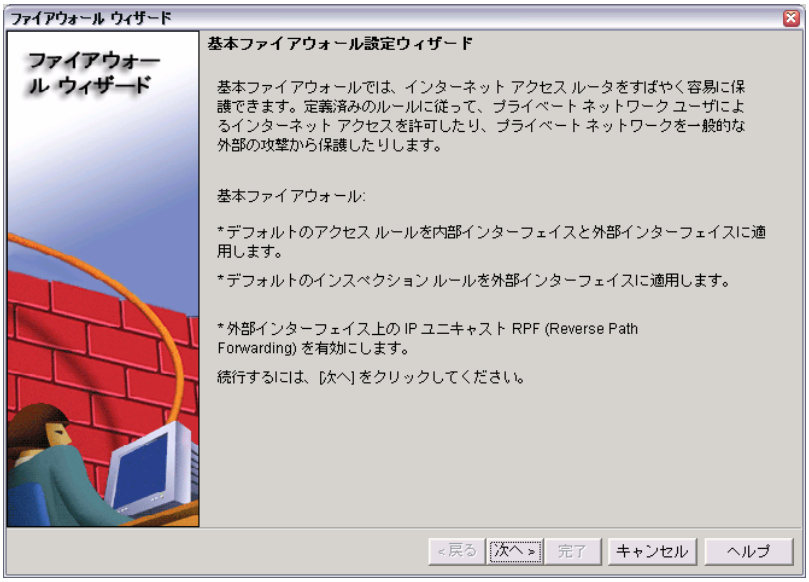

図 3：基本ファイアウォール設定ウィザード

インターネットに接続されている外部インターフェイスと、LAN に接続されている内部インターフェイスを指定します（図 4）。本例では、外部インターフェイスに Fast Ehernet 1、内部インターフェイスに Fast Ethernet 0 を指定し、「次へ」をクリックします。

図 4：基本ファイアウォールのインターフェイス設定

内部および外部インターフェイスを指定すると、ウィザードが設定するセキュリティポリシーによって外部インターフェイスから SDM での接続ができなくなります（図 5）。「OK」をクリックし、処理を進めます。

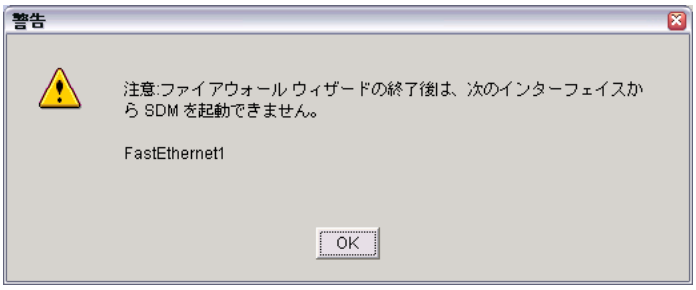

図 5:ファイウォールウィザード警告メッセージ

インターフェイスに設定された IP アドレスなどをもとに、ファイアウォールウィザードは安全なインターネット接続に必要なセキュリティポリシーを作成します（図 6）。「完了」をクリックすると、作成されたセキュリティポリシーがルータに反映され、確認メッセージが表示されます（図 7）。

図 6:ファイアウォールウィザード確認画面

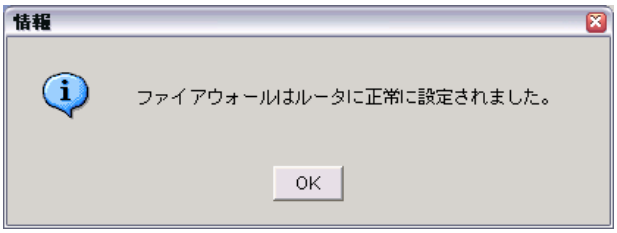

図 7:ファイアウォールウィザード設定完了メッセージ

ウィザードを利用して基本ファイアウォールを構成した後は、設定の表示やファイアウォール設定を変更するためには Cisco SDM ファイアウォールポリシーを使用します。

2. Cisco SDM Firewall ポリシー

Cisco SDM[ファイアウォールポリシー/ACL の編集]タブは、ファイアウォールポリシービューから構成されています。このビューは、特定トラフィックフローのアクセス権限と特定インターフェイス上のインスペクションルールを表示しています。図8でははは企業内ネットワーク(内部インターフェイス、送信元:Fast Ethernet 0)からインターネット(外部インターフェイス、宛先:Fast Ethernet 1)に対するポリシーを示しています。アクセスルールは ACL100、インスペクションルールは DEFAULT100 が定義され、内部インターフェイスに対する受信トラフィック制限およびパケットインスペクションポリシーとして適用されています。

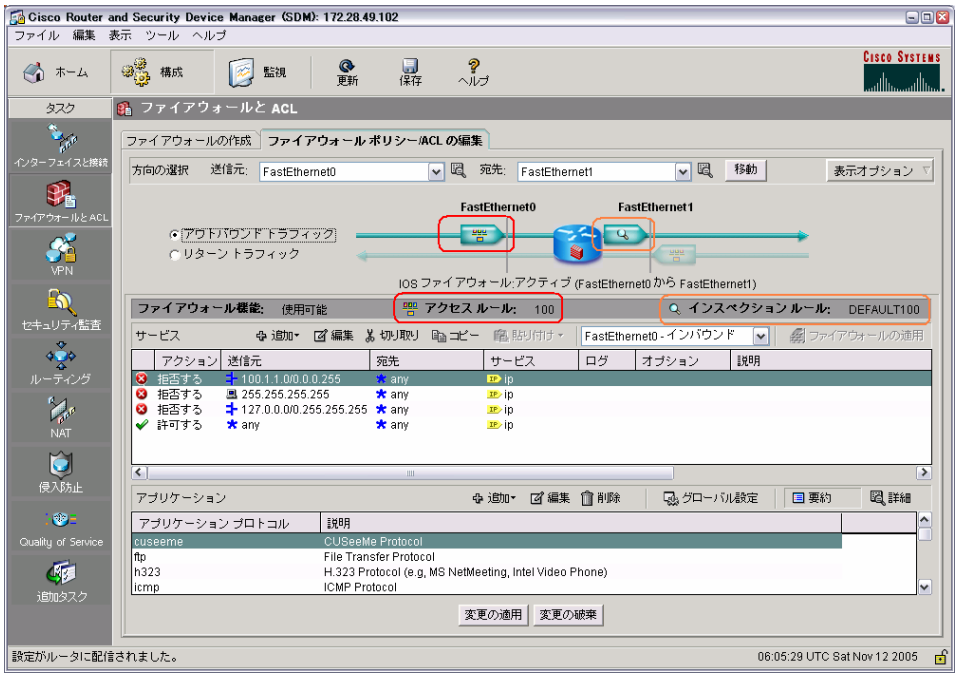

図 8:ファイアウォールポリシービュー(内部→外部)

Cisco の SDM ファイアウォールポリシーテーブルを用いると、グラフィカルなインターフェイスを使ってトラフィックフローとインターフェイスのどこにアクセスリストが適用されているかを簡単かつシンプルに管理できるようになります。

また Cisco SDM ファイアウォールポリシーテーブルでは、リターントラフィックを選択すると、選択した方向（送信元/宛先）に対する戻りのトラフィックポリシーを確認することも出来ます（図 9）。ここでは、アクセスルール ACL101 によって受信制限されていることが確認できます。

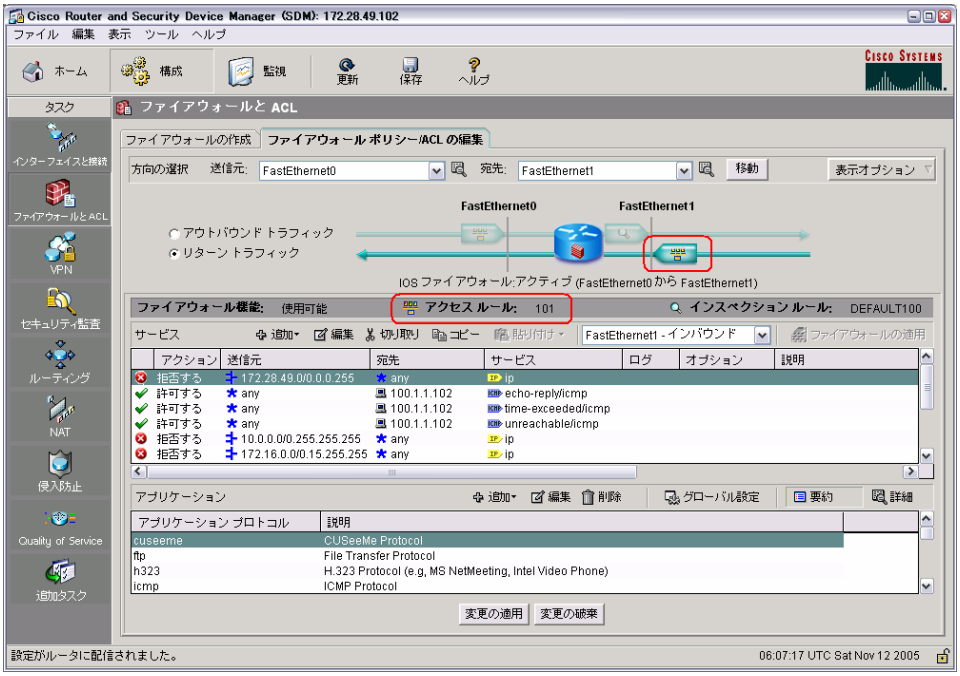

図 9：ファイアウォールポリシービュー（内部→外部）リターントラフィック

図 10 は、インターネット(外部インターフェイス、送信元:FastE thernet 1)から企業内ネットワーク(外部インターフェイス、宛先:Fas tEthernet 1)に対するポリシーを示しています。ここでは ACL101 が受信トラフィック制限として定義されています。

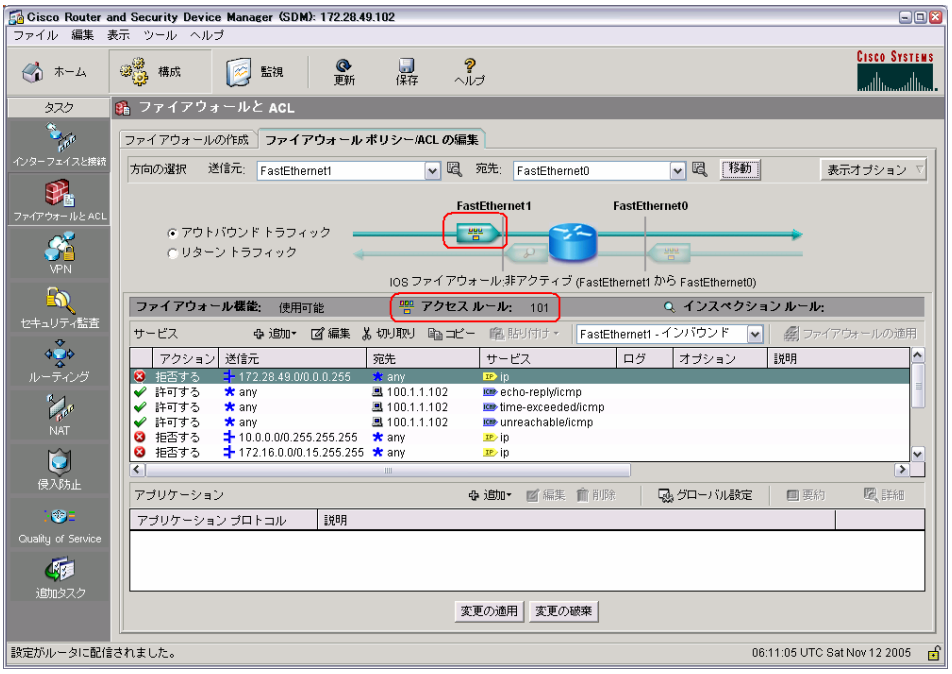

図 10:ファイアウォールポリシービュー(外部→内部)

内部から外部へのポリシーと同様に、リターントラフィックを選択すると、Cisco IOS ファイアウォール内部インターフェイス(Fast Ethernet 0)に受信される、インターネットからのアクセスに対する支店ネットワークからの戻りトラフィックポリシーが表示されます(図 11)。先ほどと同様に、このトラフィックに対するフィルタとして ACL100 が適用されています。

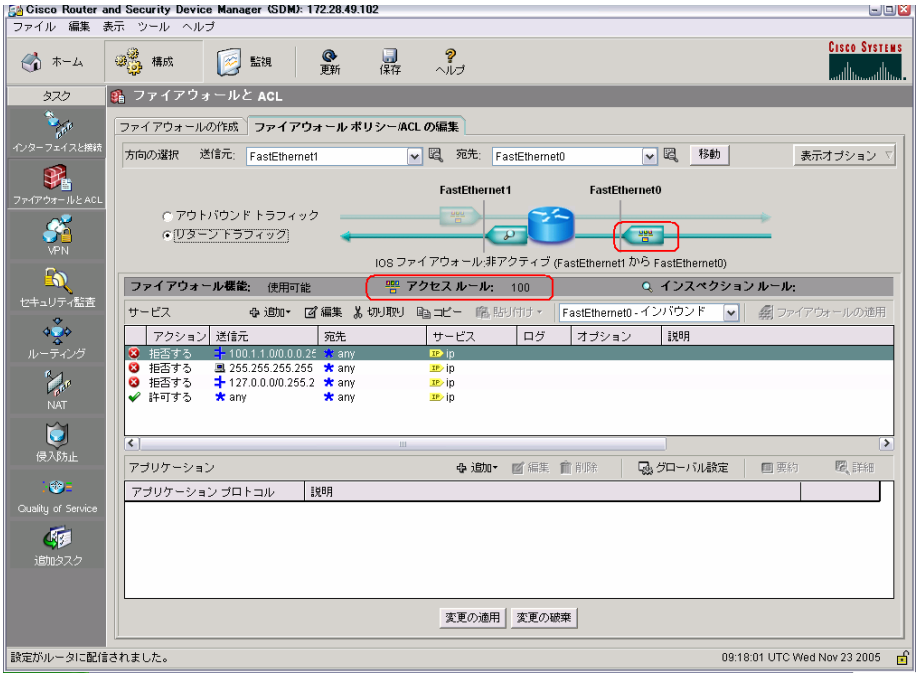

図 11:ファイアウォールポリシービュー(外部→内部)リターントラフィック

3. Cisco SDM によるトラフィックポリシーの追加

コマンドラインベースでのシナリオに沿って、Cisco IOS ファイアウォールを通過する、支店からインターネットへのトラフィックポリシーを追加します。コマンドラインのシナリオでは、ACL111 に定義した telnet、FTP 及び HTTP へのアクセスを許可と基本ファイアウォールルールとして設定された ACL100 の結合にも CLI を利用しなければなりません。

```
ACL111
!
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
access-list 111 permit ip any 172.28.49.102
```

Cisco SDM ファイアウォールポリシーテーブルを用いると、ACL100 への追加と結合をシンプルに、そして簡単に行うことができます。既存のアクセスリストへのポリシーの追加は、サービス欄の「追加」ボタンをクリックして新しいサービスポリシーを定義します。telnet、ftp、http の各サービスポリシーをリストの先頭に追加するため、既存リストの先頭行を選択し、追加ボタンをクリックして「上に挿入」を選択します（図 12）。4 行目のポリシーは、送信元/宛先を any/any で許可しているポリシーを変更します。

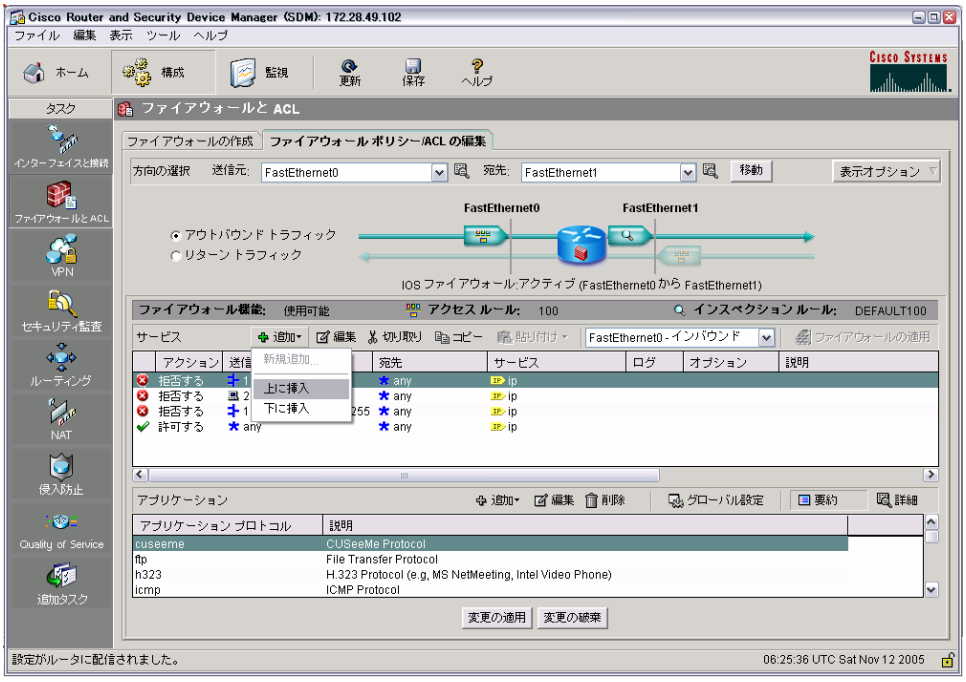

図 12：サービスポリシーの追加

拡張ルールエントリの追加ウィンドウ(図 13)が表示されます。

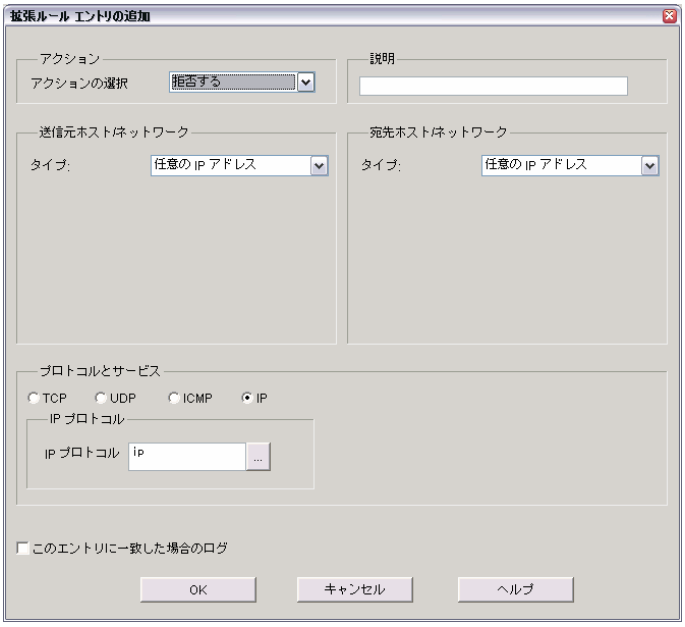

図 13:拡張ルールエントリの追加

最初に、ACL111 に定義されていた telnet の許可を以下の手順で設定します。

アクション:許可する

送信元ホスト/ネットワーク

タイプ:ネットワーク

IP アドレス:172.28.49.0

ワイルドカードマスク:0.0.0.255

宛先ホスト/ネットワーク:any

プロトコルとサービス:TCP

送信元ポート

サービス:=(等しい)

:telnet

ポート番号の指定は、送信元ポート欄のリストボックスボタン(…)をクリックし、表示されるサービスリストボックスから該当するサービス(ポート番号)を選択し、「OK」をクリックします(図 14)。

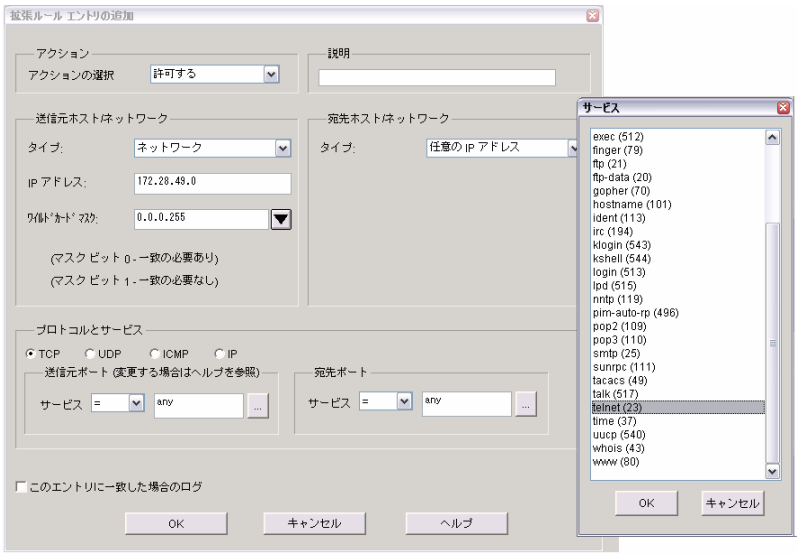

図 14:サービスの追加

必要な設定項目をすべて入力し、拡張ルールエントリの追加画面の「OK」をクリックすると、登録したサービスポリシーがファイアウォールポリシービューに反映されます。引き続き、ACL111 の残りのポリシー(ftp 及び http)についても同様に追加/変更します。すべての登録が完了すると、ファイアウォールポリシービューは図 15 のように表示されます。

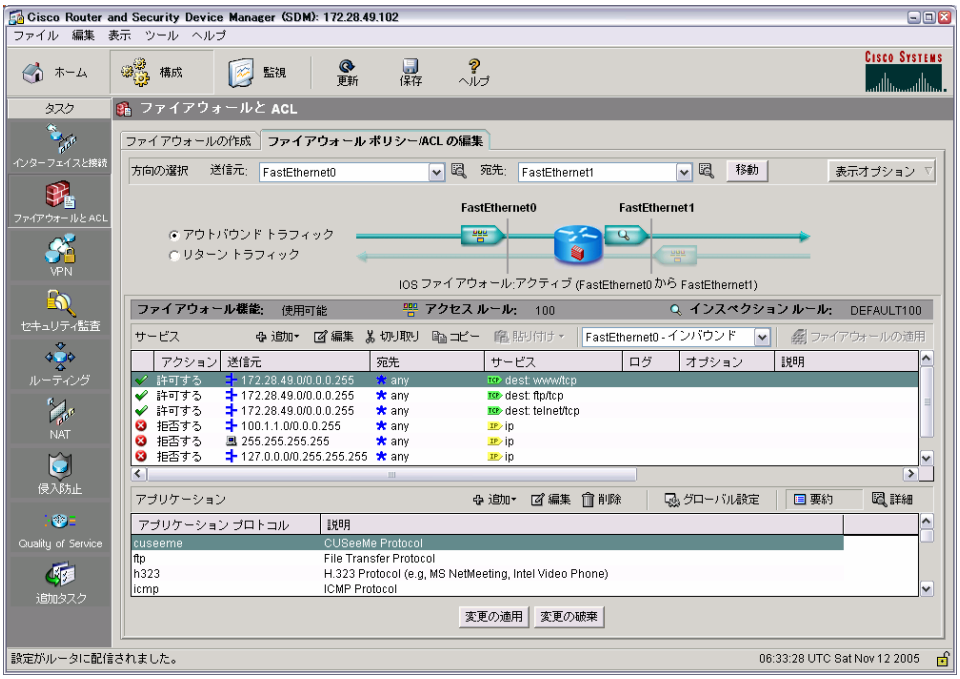

図 15:サービスポリシー追加の完了

この段階では、Cisco SDM のファイアウォールポリシービューにのみ設定が登録されている状態で、これらの設定内容はまだルータに登録されていません。ルータへ設定を反映させるには「変更の適用」をクリックします。また、変更を取り消すには「変更の破棄」をクリックします。本例では次のインスペクションポリシーの追加の後、ルータへ設定を反映します。

4. Cisco SDM によるインスペクションルールの追加

新しいインスペクションルール「BranchFIRE」を作成し、このインスペクションルールを外部インターフェイス（FastEthernet 1）の受信トラフィック（外部→内部）に対して適用します。インスペクションルールの作成するには、アプリケーション欄の「追加」ボタンをクリックし、「追加」を選択してインスペクションルールエディタを起動します（図 16）。

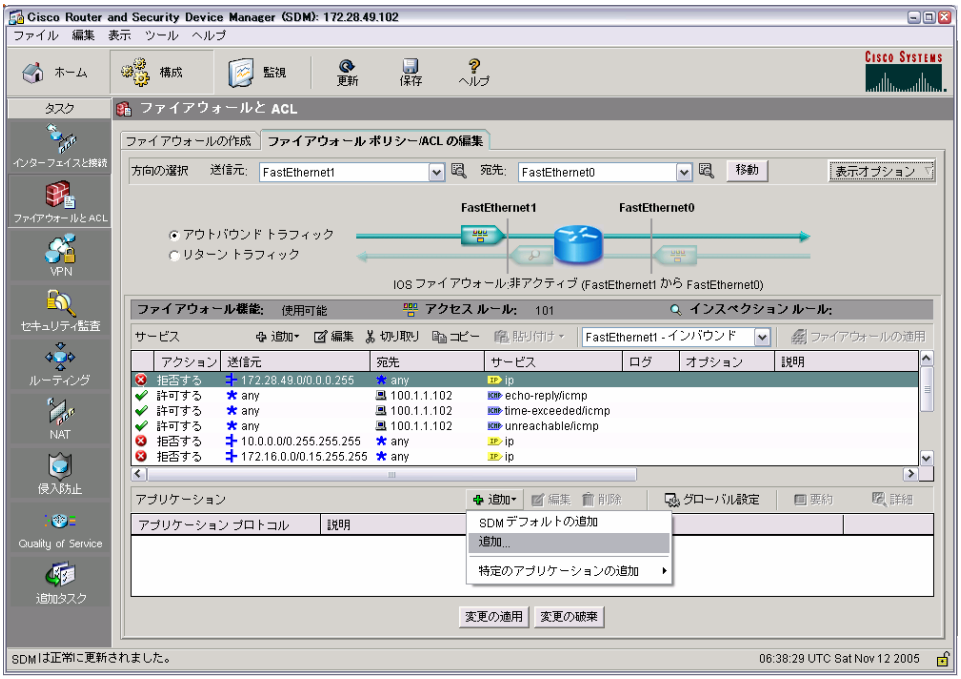

図 16：インスペクションルールの追加

インスペクションルールエディタで、インスペクションルール名「BranchFIRE」、TCP と UDP のインスペクションを有効にし、「OK」をクリックします（図 17）。

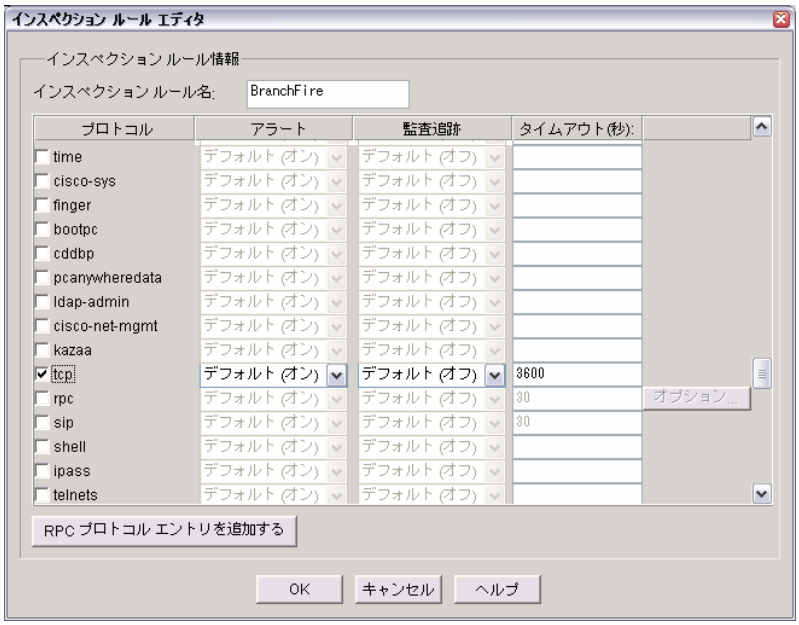

図 17：インスペクションルールエディタ

ファイウォールポリシービューに新しいインスペクションルールが登録されます（図 18）。この設定をルータに反映されるために、「変更の適用」をクリックします。

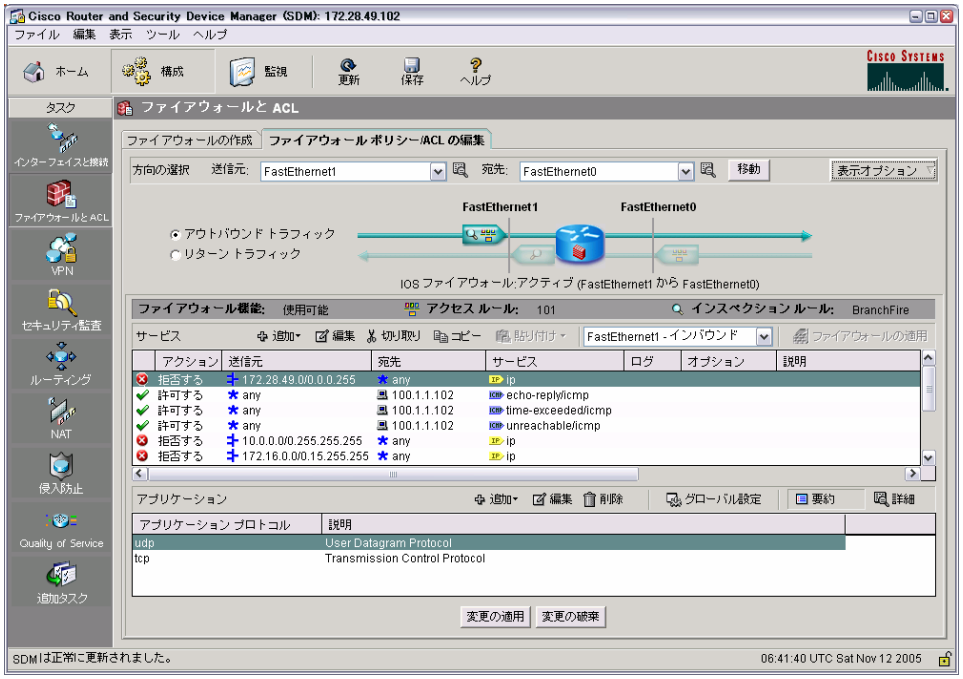

図 18：インスペクションルール追加の完了

以上のように、ユーザは Cisco SDM のファイアウォールウィザードとファイアウォールポリシーテーブルを利用することによって、シスコ IOS Software コマンド及びセキュリティに関する詳細な知識・スキルを持っていなくとも簡単な手順で複雑なファイアウォール構成を生成することができます。さらにポリシービューは、定義されたポリシーのアクセス権、トラフィックの流れ、設定されたインターフェイスの状況など、ユーザがファイアウォールポリシーの詳細を確認する際に有用なグラフィカルインタフェイスを提供します。

Cisco Security Device Manger サンプル設定ガイド
Cisco IOS Firewall ポリシー設定

発行　　2006 年 4 月　第 1 版

発行　　シスコシステムズ株式会社