ASA/PIX 8.x： MPF と正規表現を使用した FTP サイトの許可/ブロックの設定例

目次

はじめに
前提条件
要件
使用するコンポーネント
表記法
背景説明
モジュラ ポリシー フレームワークの概要
正規表現
設定
ネットワーク図
設定
ASA CLI 設定
ASDM 6.x を使用した ASA コンフィギュレーション 8.x
確認
トラブルシューティング
関連情報

はじめに

このドキュメントでは、サーバ名によって特定の FTP サイトをブロックまたは許可するために Modular Policy Framework（MPF）で正規表現を使用する Cisco セキュリティ アプライアンス ASA/PIX 8.x を設定する方法について説明します。

前提条件

要件

この資料は Ciscoセキュリティ アプライアンスが設定される仮定し、ときちんとはたらきます。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- ソフトウェア バージョン 8.0(x) 以降が稼働する Cisco 5500 シリーズ適応型セキュリティ アプライアンス（ASA）
- ASA 8.x 用の Cisco Adaptive Security Device Manager（ASDM）バージョン 6.x

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

モジュラ ポリシー フレームワークの概要

MPF を使用すると、一貫した柔軟な方法でセキュリティ アプライアンスの機能を設定できるようになります。 たとえば、MPF を使用してタイムアウトを設定すると、すべての TCP アプリケーションにではなく、特定の TCP アプリケーションに固有に適用できます。

MPF は次の機能をサポートします。

- TCP 正規化、TCP 接続と UDP 接続の制限およびタイムアウト、TCP シーケンス番号のランダム化
- CSC
- アプリケーション検査
- IPS
- QoS 入力ポリシング
- QoS 出力ポリシング
- QoS プライオリティ キュー

MPF の設定は、次の 4 つの作業で構成されます。

1. 操作を適用したいと思うレイヤ3 およびレイヤ4 トラフィックを識別して下さい。 詳細は、『レイヤ 3/4 クラス マップによるトラフィックの特定』を参照してください。
2. （アプリケーション インスペクションだけ。）アプリケーション インスペクション トラフィックのための特別な操作を定義して下さい。 詳細は、『アプリケーション検査のための特別なアクションの設定』を参照してください。
3. レイヤ3 およびレイヤ4 トラフィックに操作を適用して下さい。 詳細は、『レイヤ 3/4 ポリシー マップによるアクションの定義』を参照してください。
4. インターフェイスでアクションをアクティブにします。 詳細については、『サービス ポリシーによるインターフェイスへのレイヤ 3/4 ポリシーの適用』を参照してください。

正規表現

正規表現一致文字列正確に正確なストリングとしてまたはメタ文字の使用によって、従って文字列の複数のバリアントを一致することができます。 ある特定のアプリケーショントラフィックのコンテンツを一致するのに正規表現を使用できます。 たとえば、HTTP パケット内の URL ストリングを照合できます。

注: 疑問符（か。）またはタブのような CLI の特殊文字すべてを、エスケープするために **Ctrl+V** を使用して下さい。 たとえば、**d** を入力するために **d [Ctrl+V] g** を入力して下さいか。**g** を入力します。

正規表現を作成するために、**regex** コマンドを使用して下さい。 さらに、**regex** コマンドはテキスト一致を必要とするさまざまな機能に使用することができます。 たとえば、インスペクション ポリシーマップを使用する MPF の使用でアプリケーション インスペクション用の特別な操作を設定できます。 詳細については **policy-map タイプ inspect コマンドを**参照して下さい。

インスペクション ポリシーマップでは、1つ以上の **match コマンドが**含まれている、またはインスペクション ポリシーマップで **match コマンドを**直接使用できますインスペクション クラスマップを作成する場合行動したいと思うトラフィックを識別できます。 いくつかの **match コマンドは**正規表現を使用してパケットのテキストを識別することを可能にしました。 たとえば、HTTP パケット内の URL ストリングを照合できます。 正規表現クラス マップで正規表現をグループ化できます。 詳細については、**class-map type regex** コマンドを参照してください。

次の表に、特殊な意味を持つメタ文字を示します。

文字	説明	注意事項
を探します。	ドット	任意の単一の文字と照合されます。 たとえば、**d.g** は dog、dag、dtg、doggonnit など、これらの文字が含まれているすべての単語と一致します。
(exp)	サブ表現	サブ表現は、文字を周囲の文字から分離して、サブ表現に他のメタ文字を使用できるようにします。 たとえば、**d(o|a)g** は dog および dag に一致しますが、**do|ag** は do および ag に一致します。 また、サブ表現を繰り返し限定作用素とともに使用して、繰り返す文字を区別できます。 たとえば、**ab(xy){3}z** は、abxyxyxyz に一致します。
|	代替	このメタ文字によって区切られている複数の表現のいずれかと一致します。 たとえば、**dog|cat** は dog または cat に一致します。
?	疑問符	直前の表現が 0 または 1 個存在することを示す修飾子。 たとえば、**lo?se** は lse または lose に一致します。 **注: Ctrl+V** を入力してから疑問符を入力しないと、ヘルプ機能が呼び出されます。
*	アスタリスク	0 が、1 あることを、または前の式のいくつも示す量指定子。 たとえば、**lo*se** は、lse、lose、loose などに一致します。
{x}	繰り返し限定作用素	厳密に x 回繰り返します。 たとえば、**ab(xy){3}z** は、abxyxyxyz に一致します。
{x,}	最小繰り返し限定作用素	少なくとも x 回繰り返します。 たとえば、**ab(xy){2,}z** は、abxyxyz や abxyxyxyz などに一致します。
[abc]	文字クラス	カッコ内の任意の文字と一致します。 たとえば、**[abc]** は a、b、または c と一致します。

[^abc]	否定文字クラス	角カッコに含まれていない単一文字と一致します。 たとえば、**[^abc]** は a、b、c 以外の文字に一致します。**[^A-Z]** は、大文字でない単一文字と一致します。
[a-c]	文字範囲クラス	範囲内の任意の文字と一致します。 **[[a-z]** は、任意の小文字と一致します。 これらの文字と範囲を組み合わせて使用することもできます。 **[[abcq-z]** および **[a-cq-z]** は、a、b、c、q、r、s、t、u、v、w、x、y、z に一致します。 ダッシュ（-）文字は、角カッコ内の最初の文字または最後の文字である場合にのみリテラルとなります。 **[[abc-]** または **[-abc]**。
""	引用符	文字列の末尾または先頭のスペースを保持します。 たとえば、**" test"** は、一致を検索する場合に先頭のスペースを保持します。
^	キャレット	行の始まりを規定 します。
\	エスケープ文字	メタ文字とともに使用すると、リテラル文字と一致します。 たとえば、**\[** は左の角カッコと一致します。
char	文字	文字がメタ文字のとき、リテラル文字と一致します。
\r	復帰	キャリッジリターンと一致します: 0x0d.
\n	改行	復帰改行文字と一致します: 0x0a.
\t	Tab	タブと一致します: 0x09.
\f	改ページ	書式送り文字と一致します: 0x0c.
\xNN	エスケープされた 16 進数	丁度 2 ディジットである 16 進法を使用する ASCII文字と一致します。
\NNN	エスケープされた 8 進数	厳密に 3 桁の 8 進数としての ASCII 文字と一致します。 たとえば、文字 040 はスペースを表します。

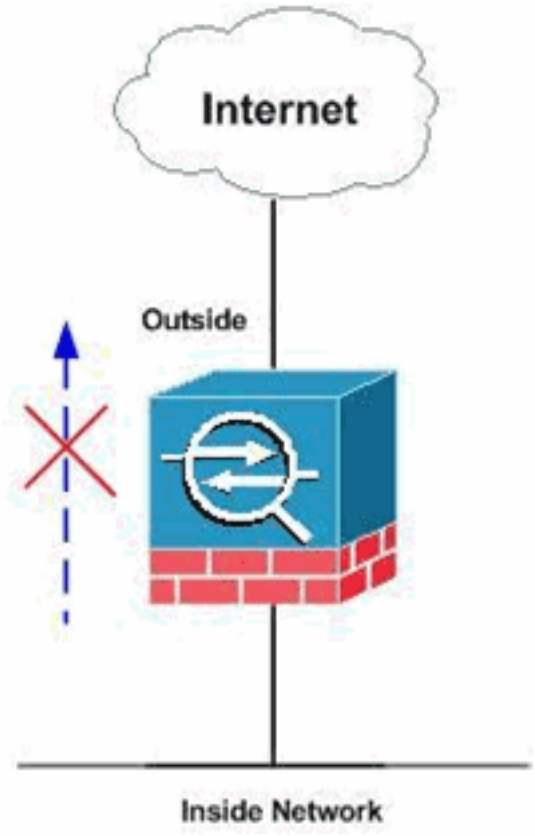
設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。



注: FTP 指定サイトは正規表現を使用して許可されるか、またはブロックされます。

設定

このドキュメントでは、次の設定を使用します。

- ASA CLI 設定
- ASDM 6.x を使用した ASA コンフィギュレーション 8.x

ASA CLI 設定

ASA CLI の設定

```
ciscoasa#show run
: Saved
:
ASA Version 8.0(4)
!
hostname ciscoasa
domain-name cisco.com
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 10.66.79.86 255.255.255.224
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
```

```
 ip address 10.238.26.129 255.255.255.248
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
!--- Write regular expression (regex) to match the FTP
site you want !--- to access. NOTE: The regular
expression written below must match !--- the response
220 received from the server. This can be different !---
than the URL entered into the browser. For example, !---
FTP Response: 220 g1u0103c.austin.hp.com


regex FTP_SITE1 "([0-9A-Za-z])*[Hh][Pp]\.[Cc][Oo][Mm]"
regex FTP_SITE2 "([0-9A-Za-z])* CISCO SYSTEMS ([0-9A-Za-
z])*"

!--- NOTE: The regular expression will be checked
against every line !--- in the Response 220 statement
(which means if the FTP server !--- responds with
multiple lines, the connection will be denied if !---
there is no match on any one line).


boot system disk0:/asa804-k8.bin
ftp mode passive
pager lines 24
logging enable
logging timestamp
logging buffered debugging
mtu outside 1500
mtu inside 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-61557.bin
no asdm history enable
arp timeout 14400

global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0
route outside 0.0.0.0 0.0.0.0 10.66.79.65 1

timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00
absolute
dynamic-access-policy-record DfltAccessPolicy

http server enable
http 0.0.0.0 0.0.0.0 inside
http 0.0.0.0 0.0.0.0 outside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart
```

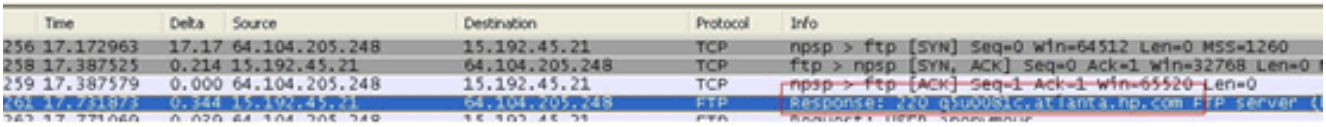
```
telnet timeout 5
ssh scopy enable
ssh timeout 5
console timeout 0
management-access inside
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept


class-map type regex match-any FTP_SITES
 match regex FTP_SITE1
 match regex FTP_SITE2

! Class map created in order to match the server names !
of FTP sites to be blocked by regex. class-map type
inspect ftp match-all FTP_class_map
 match not server regex class FTP_SITES

! Write an FTP inspect class map and match based on
server !--- names, user name, FTP commands, and so on.
Note that this !--- example allows the sites specified
with the regex command !--- since it uses the match not
command. If you need to block !--- specific FTP sites,
use the match command without the  not  option.


class-map inspection_default
 match default-inspection-traffic

policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512

policy-map type inspect ftp FTP_INSPECT_POLICY
 parameters
 class FTP_class_map
  reset log

! Policy map created in order to define the actions !---
such as drop, reset, or log. policy-map global_policy
class inspection_default inspect dns preset_dns_map
inspect h323 h225 inspect h323 ras inspect netbios
inspect rsh inspect rtsp inspect skinny inspect esmtp
inspect sqlnet inspect sunrpc inspect tftp inspect sip
inspect xdmcp inspect icmp inspect ftp strict
FTP_INSPECT_POLICY

!--- The FTP inspection is specified with strict option
!--- followed by the name of policy. service-policy
global_policy global prompt hostname context
Cryptochecksum:40cefb1189e8c9492ed7129c7577c477 : end
```

ASDM 6.x を使用した ASA コンフィギュレーション 8.x

正規表現を設定し、FTP 特定のサイトをブロックするために MPF に適用するためにこれらのステップを完了して下さい:

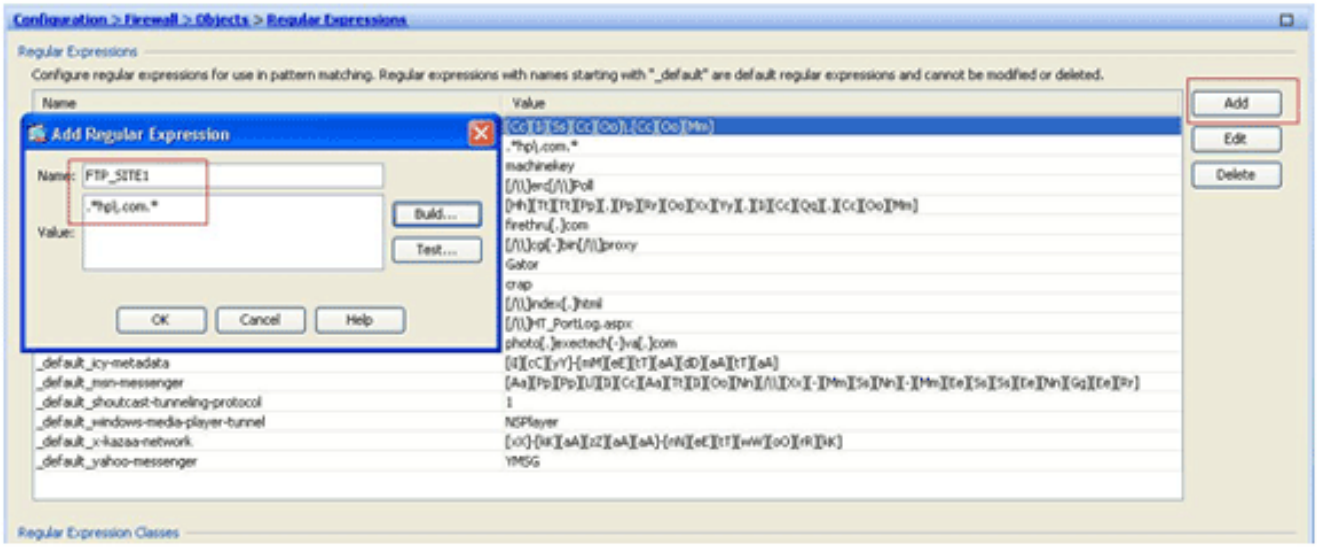
1. **FTP サーバ名前を判別して下さい。** FTP インスペクション エンジンはコマンド、ファイル名、ファイルタイプ、サーバおよびユーザネームのような別の基準を使用してインスペクションを、提供できます。 このプロシージャは基準としてサーバを使用します。 FTP インス

ペクション エンジンは Server 値として FTP サイトによって返されるサーバ 220 応答を使用します。 この値はサイトによって使用されるドメイン名と異なります。 この例は Wireshark をステップ 2.の正規表現で使用されるの応答 220 値を取得するために点検されるサイトに FTP パケットをキャプチャ するのに使用します。

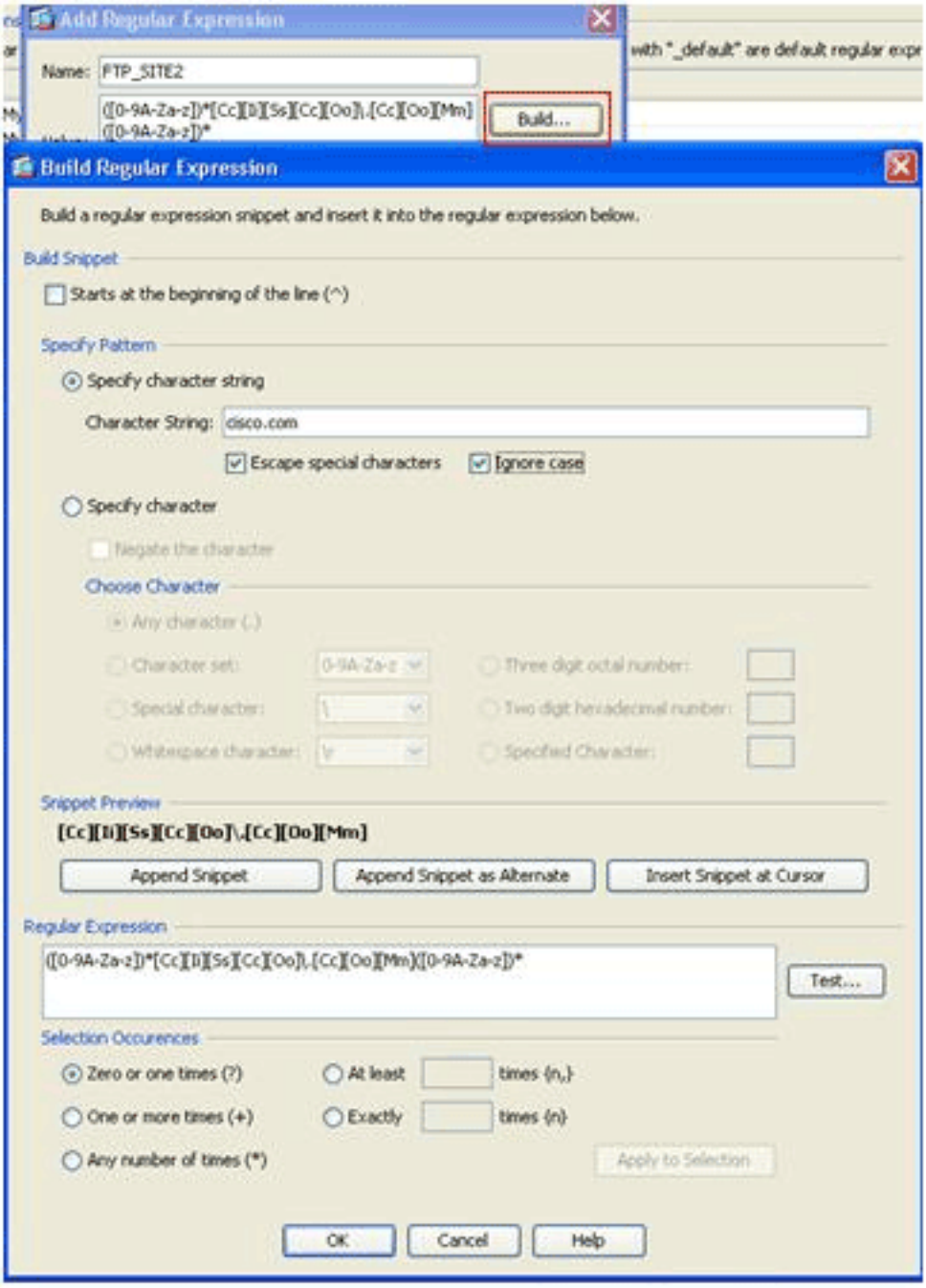


キャプチャに基づいて ftp://hp.com の応答 220 値は（ たとえば ） *q5u0081c.atlanta.hp.com* です。

2. **正規表現を作成して下さい。> ファイアウォール > オブジェクト > 正規表現** 『Configuration』 を選択 し、正規表現タブの下でこのプロシージャに記述されているように正規表現を作成するために『Add』 をクリック して下さい:FTP サイトから届く応答 220 を（ Wireshark のパケットキャプチャか使用される他のどのツールに見られるように ）一致するために正規表現を、*FTP_SITE1*、作成して下さい（ たとえば、「。* HP \ .com.* は」 ）、および『OK』 をクリック します。

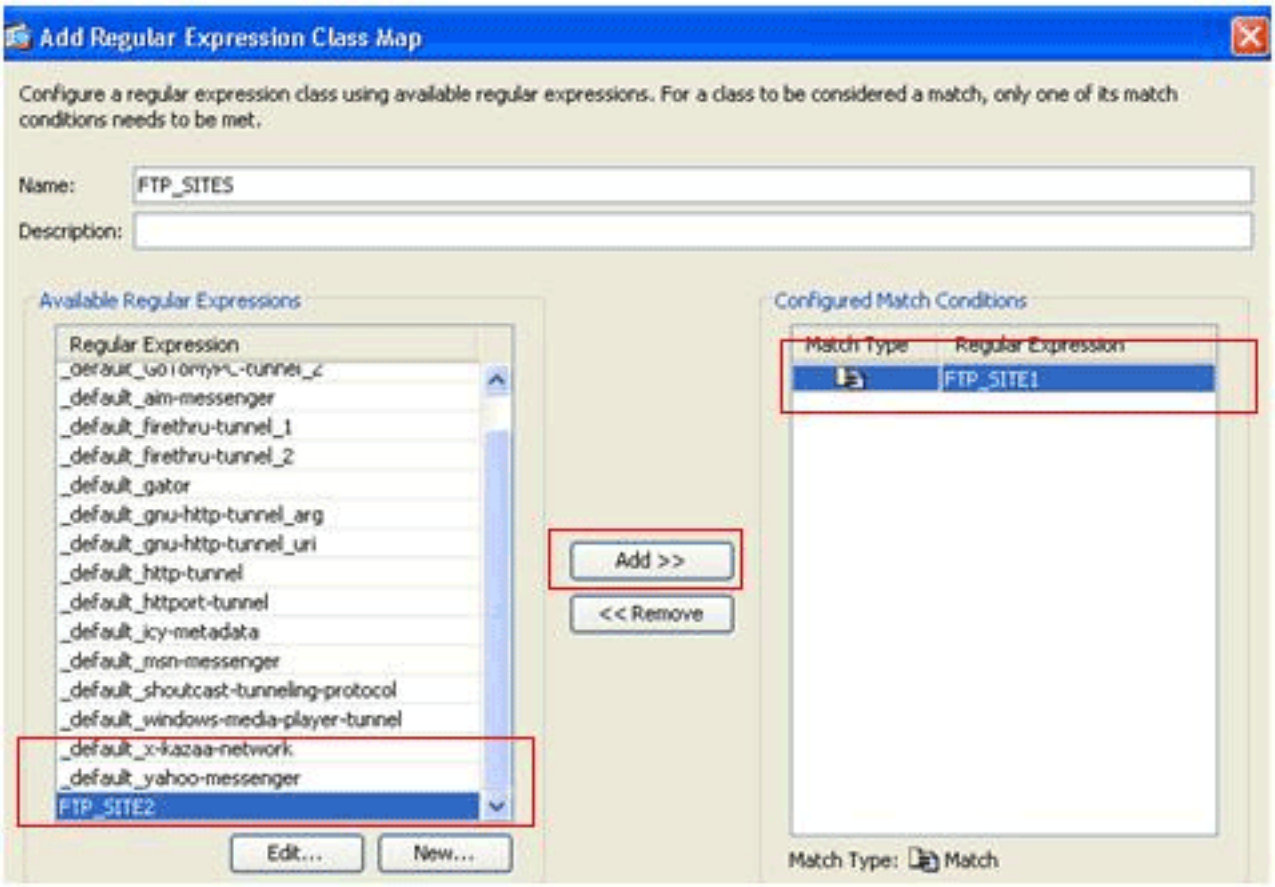


注: 高度正規表現を作成する方法のヘルプのための**ビルドを**クリックできます。

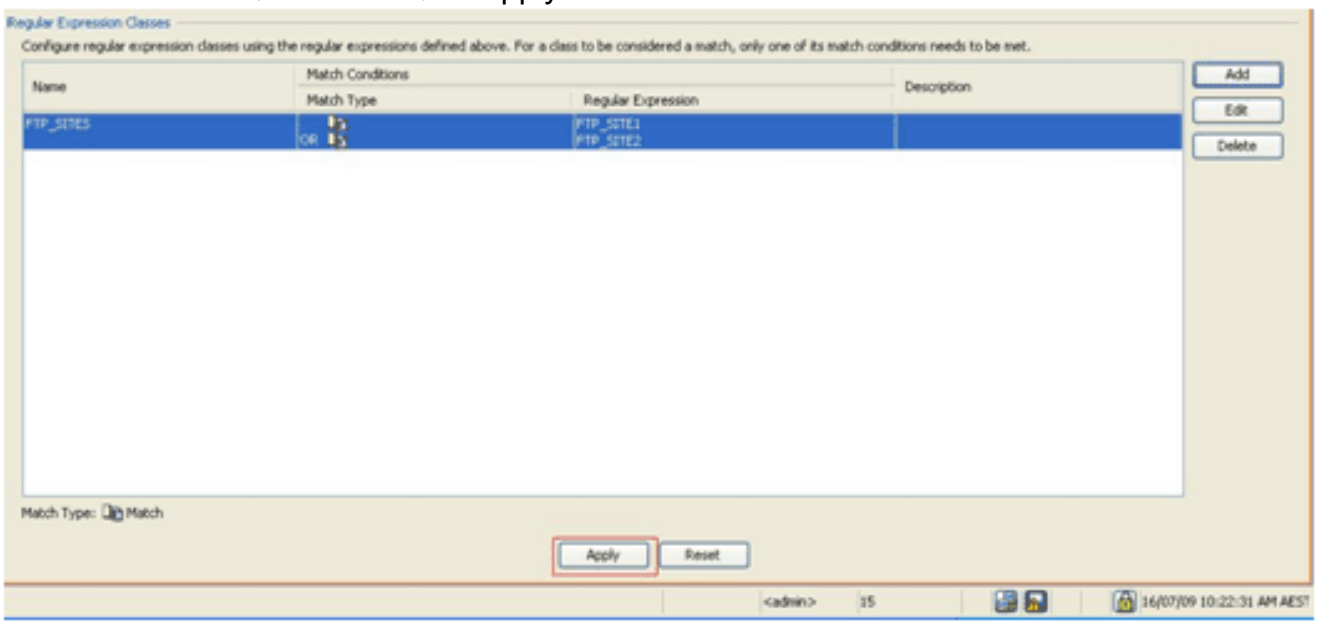


正規表現が作成されたら、『Apply』 をクリック して下さい。

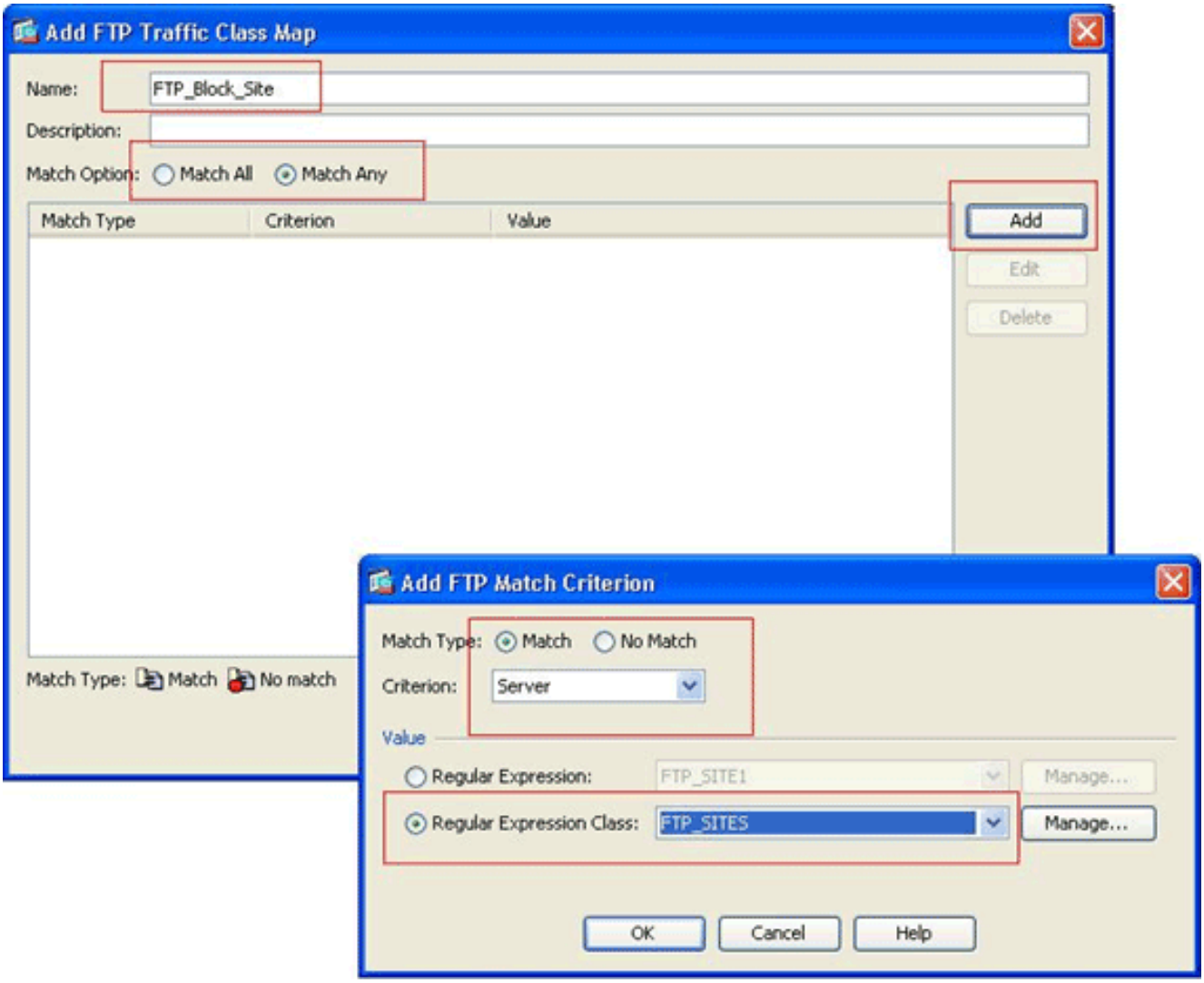
3. **正規表現クラスを作成して下さい。> ファイアウォール > オブジェクト > 正規表現** 『Configuration』 を選択 し、正規表現クラス セクションの下でこのプロシージャに記述されているようにクラスを作成するために『Add』 をクリック して下さい:正規表現 *FTP_SITE1* および *FTP_SITE2* の一致するために正規表現クラスを、*FTP_SITES*、作成し『OK』 をクリック して下さい。



クラスマップが作成されたら、『Apply』 をクリック して下さい。

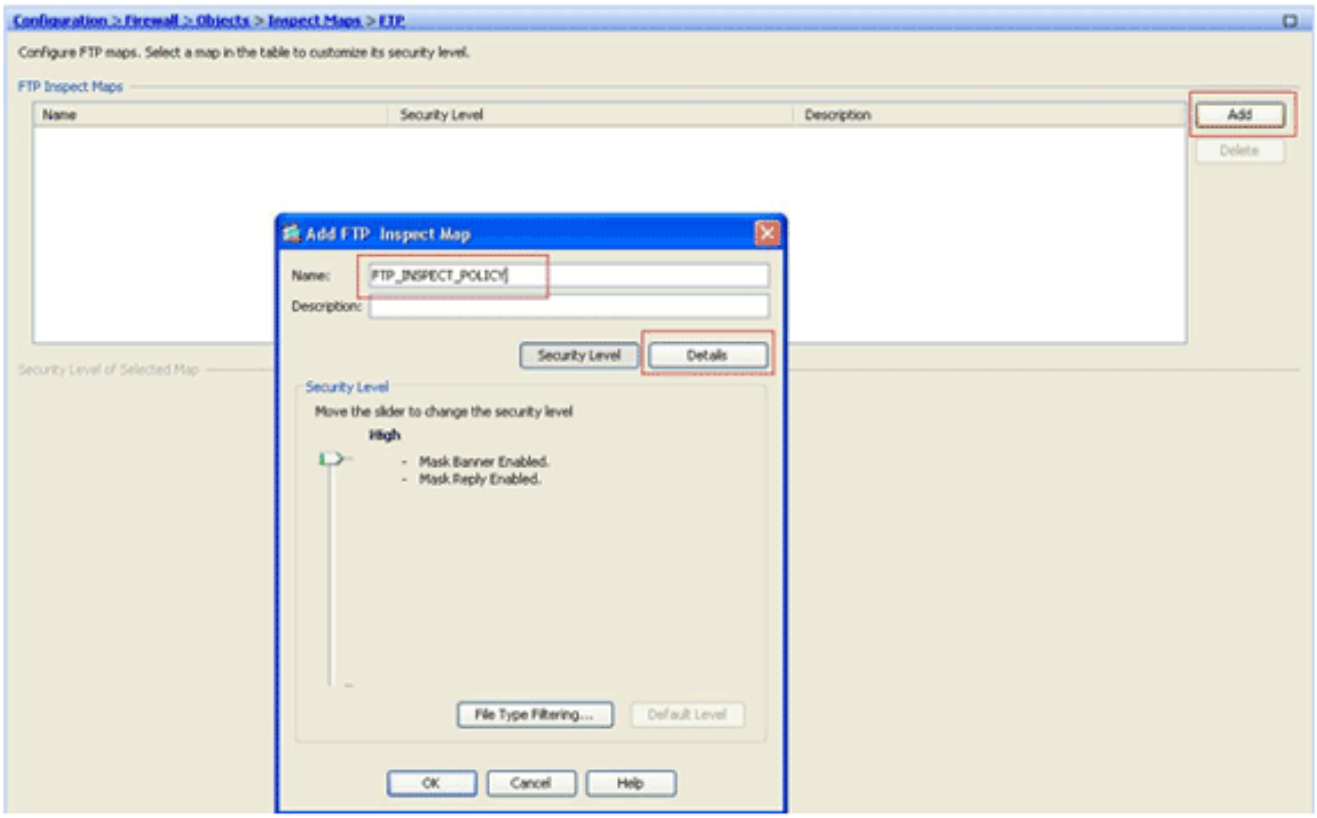


4. **クラスマップとの識別されたトラフィックを検査して下さい。> ファイアウォール > オブジェクト > クラスマップ > FTP > Add** 『Configuration』 を選択 し、右クリックし、クラスマップをこのプロシージャに記述されているようにさまざまな正規表現によって識別される FTP トラフィックを検査するために作成するために『Add』 を選択 して下さい:作成した正規表現の FTP 応答 220 を一致するためにクラスマップを、*FTP_Block_Site*、作成して下さい。

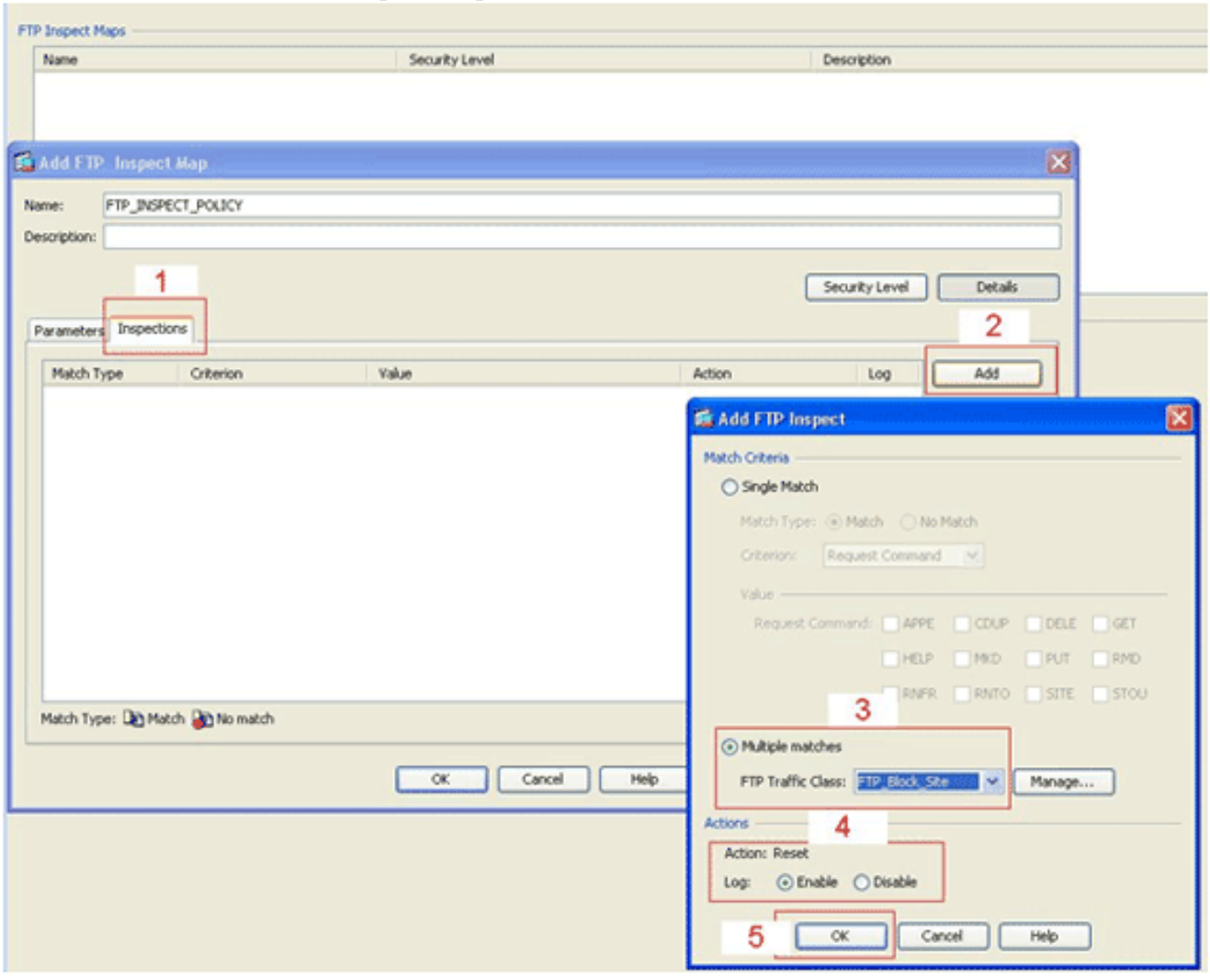


正規表現で規定 される サイトを除きたいと思う場合**マッチ** Radio ボタンをクリックしないで下さい。値 セクションで、正規表現か正規表現クラスを選択して下さい。 このプロシージャに関しては、先に作成されたクラスを選択して下さい。[Apply] をクリックします。

5. **インスペクション ポリシーの一致されたトラフィックのための操作を設定 して下さい。> ファイアウォール > オブジェクト > Inspect マッピング します > FTP>** インスペクション ポリシーを作成するために**追加し**要求に応じて設定 しました一致されたトラフィックのための操作を『Configuration』 を選択 して下さい。



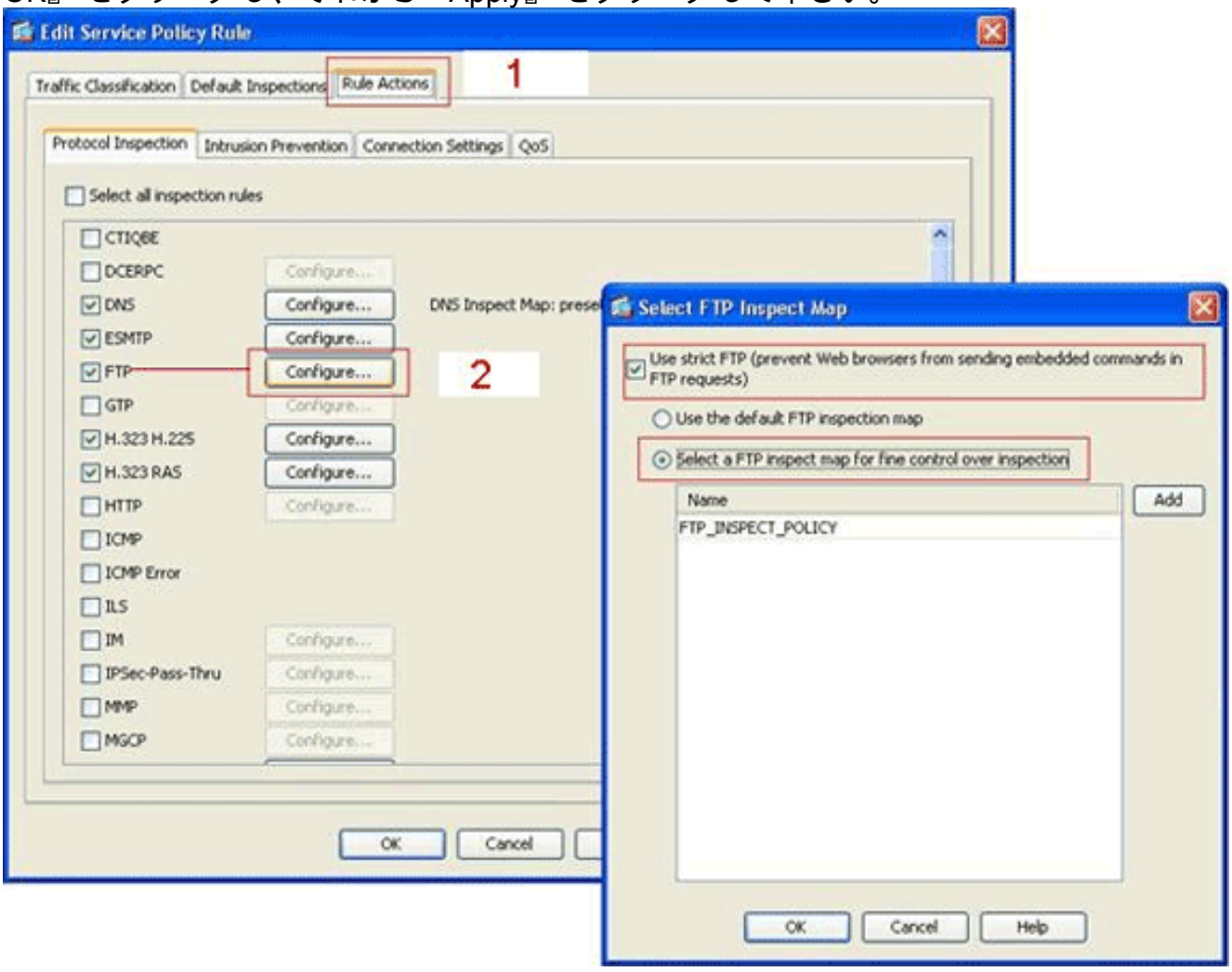
インスペクション ポリシーのための名前および説明を入力して下さい。（たとえば、*FTP_INSPECT_POLICY*。）**[Details]** をクリックします。



インスペクション タブをクリックして下さい。（1）[Add] をクリックします。（2）**倍数**

マッチ Radio ボタンをクリックし、ドロップダウン リストからトラフィック クラスを選択して下さい。（3）有効に なるか、または無効に なる望ましいリセット操作を選択して下さい。 この例は指定されたサイトと*一致しない* FTP すべてのサイトのためにリセットされる FTP接続を有効に します。（4）再度『OK』 をクリック し、『OK』 をクリック し、それから『Apply』 をクリック して下さい。（5）

6. **グローバル な インスペクション リストにインスペクション FTP ポリシーを適用して下さい。> ファイアウォール > サービス ポリシー ルール**『Configuration』 を選択 して下さい。右側で、**inspection_default** ポリシーを選択し、『Edit』 をクリック して下さい。ルール アクションの下で（1）を、クリックします FTP のための **Configure ボタンを**記録して下さい。（2）選定された FTP Inspect Map ダイアログボックスでは、**使用厳密な FTP** チェック ボックスをチェックし、次に**インスペクション** Radio ボタン**の良い制御のための FTP Inspect マップを**クリックして下さい。新しい FTP インスペクション ポリシーは、*FTP_INSPECT_POLICY*、リストで目に見えるはずです。再度『OK』 をクリック し、『OK』 をクリック し、それから『Apply』 をクリック して下さい。



確認

ここでは、設定が正常に動作していることを確認します。

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

- **show running-config regex** —設定された正規表現を示します。

```
ciscoasa#show running-configregex
```

```
regex FTP_SITE1 "[Cc][Ii][Ss][Cc][Oo]\.[Cc][Oo][Mm]"
regex FTP_SITE2 ".*hp\.com.*"
```

- **show running-config class-map** —設定されたクラスマップを示します。

```
ciscoasa#show running-config class-map
class-map type regex match-any FTP_SITES
 match regex FTP_SITE1
 match regex FTP_SITE2
class-map type inspect ftp match-all FTP_Block_Site
 match not server regex class FTP_SITES
class-map inspection_default
 match default-inspection-traffic
!
```

- **show running-config policy-map 型 Inspect http** — HTTPトラフィックを点検するポリシーマップを示します設定された。

```
ciscoasa#show running-config policy-map type inspect ftp
!
policy-map type inspect ftp FTP_INSPECT_POLICY
 parameters
  mask-banner
  mask-syst-reply
 class FTP_Block_Site
  reset log
 !
```

- **Show running-config は policy-map** —すべてのポリシーマップ設定、またデフォルトポリシー マップ設定を表示します。

```
ciscoasa#show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map type inspect ftp FTP_INSPECT_POLICY
 parameters
  mask-banner
  mask-syst-reply
 class FTP_Block_Site
  reset log
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
  inspect ftp strict FTP_INSPECT_POLICY
!
```

- **show running-config は service-policy** —すべてに現在 サービス ポリシー コンフィギュレーションの実行を表示する。

```
ciscoasa#show running-config service-policy
service-policy global_policy global
```

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

インスペクション エンジンがトラフィックを検査し、正しくそれらを可能にするか、または廃棄することを確認するために **show service policy コマンドを**使用できます。

```
ciscoasa#show service-policy

Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: dns preset_dns_map, packet 0, drop 0, reset-drop 0
      Inspect: h323 h225 _default_h323_map, packet 0, drop 0, reset-drop 0
      Inspect: h323 ras _default_h323_map, packet 0, drop 0, reset-drop 0
      Inspect: netbios, packet 0, drop 0, reset-drop 0
      Inspect: rsh, packet 0, drop 0, reset-drop 0
      Inspect: rtsp, packet 0, drop 0, reset-drop 0
      Inspect: skinny , packet 0, drop 0, reset-drop 0
      Inspect: esmtp _default_esmtp_map, packet 0, drop 0, reset-drop 0
      Inspect: sqlnet, packet 0, drop 0, reset-drop 0
      Inspect: sunrpc, packet 0, drop 0, reset-drop 0
      Inspect: tftp, packet 0, drop 0, reset-drop 0
      Inspect: sip , packet 0, drop 0, reset-drop 0
      Inspect: xdmcp, packet 0, drop 0, reset-drop 0
      Inspect: ftp strict FTP_INSPECT_POLICY, packet 40, drop 0, reset-drop 2
```

関連情報

- ASA/PIX 8.x： MPF と正規表現を使用した特定の Web サイト（URL）のブロックの設定例
- PIX/ASA 7.x 以降： MPF を使用したピアツーピア（P2P）およびインスタント メッセージング（IM）トラフィックのブロックの設定例
- PIX/ASA 7.x： FTP/TFTP サービスの有効化の設定例
- アプリケーション層プロトコル検査の適用
- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス–サポート
- Cisco Adaptive Security Device Manager（ASDM）
- Cisco PIX 500 シリーズ セキュリティ アプライアンス–サポート
- Cisco PIX ファイアウォール ソフトウェア–サポート
- Cisco PIX ファイアウォール ソフトウェア コマンド リファレンス