ASA/PIX 7.2： MPF を使用した正規表現による特定 Web サイト（URL）のブロック

目次

概要

このドキュメントでは、特定の Web サイト（URL）をブロックするために 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 7.2 を設定する方法について説明します。

注: この設定は、すべてのアプリケーション ダウンロードをブロックしません。 信頼できるファイル ブロック、専用 機器に関しては、ASA のための CSC モジュールのような Websense、等、またはモジュールのような、使用されなければなりません。

HTTPS フィルタリングは、ASA ではサポートされません。 ASA は、HTTPS で、パケットのコンテンツが暗号化されるので HTTPS トラフィックのための正規表現に基づいて強度 の パケット インスペクションかインスペクションをすることができません（ssl）。

前提条件

要件

このドキュメントは、Cisco セキュリティ アプライアンスが設定されていて、正常に動作してい

ることを前提としています。

使用するコンポーネント

- ソフトウェア バージョン 7.2(2) を実行する Cisco 5500 シリーズ適応型セキュリティ アプライアンス（ASA）
- ASA のための Cisco Adaptive Security Device Manager （ASDM）バージョン 5.2(2) 7.2(2)

このドキュメントの情報は、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、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

関連製品

この設定はまたと PIX ソフトウェア バージョン 7.2(2) を実行する Cisco 500 シリーズ使用することができます。

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. アクションを適用するレイヤ 3 およびレイヤ 4 トラフィックを特定します。 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. （アプリケーション検査のみ）アプリケーション検査トラフィックの特別なアクションを定義します。 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 トラフィックにアクションを適用します。 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は正確に正確なストリングとして、またはメタ文字、従ってあなたと文字列の複数のバリアントを一致することができます。 特定のアプリケーション トラフィックの内容を照合するため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 のすべての特殊文字を、エスケープするのに **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、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る **regex** コマンドを使用して下さい。 たとえば、インスペクション ポリシーマップが付いているモジュラ 政策の枠組でアプリケーション インスペクション用の特別なアクションを設定できます（ポリシーマップが inspect コマンドをタイプするのを参照して下さい）。 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**正規表現の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 マップの正規表現をグループ化できます（class-map 型 regex コマンドを参照して下さい）。

表 1 は特別な意味があるメタ文字をリストしたものです。

文字	説明	注意事項
. 。	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	直前の表現が 0、1、または任意の個数存在することを示す修飾子。 たとえば、**lo*se は** lse と、失います、緩い、等一致します。
{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 と、abxyxyxyz、等一致します。
[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。 それが角カッコ内の最後または最初文字であるときだけダッシュ（-）文字はリテラルです: **[[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 0x0d と一致します。
\n	改行	復帰改行文字 0x0a と一致します。
\t	Tab	タブ 0x09 と一致します。
\f	改ページ	書式送り文字 0x0c と一致します。
\xNN	エスケープされた 16 進数	16 進法（丁度 2 ディジット）に ASCII文字をマッチさせます。
\	エスケー	8 ように ASCII文字と一致します（丁度 3

NNN	プされた 8 進数	ディジット）。 たとえば、文字 040 はスペースを表します。

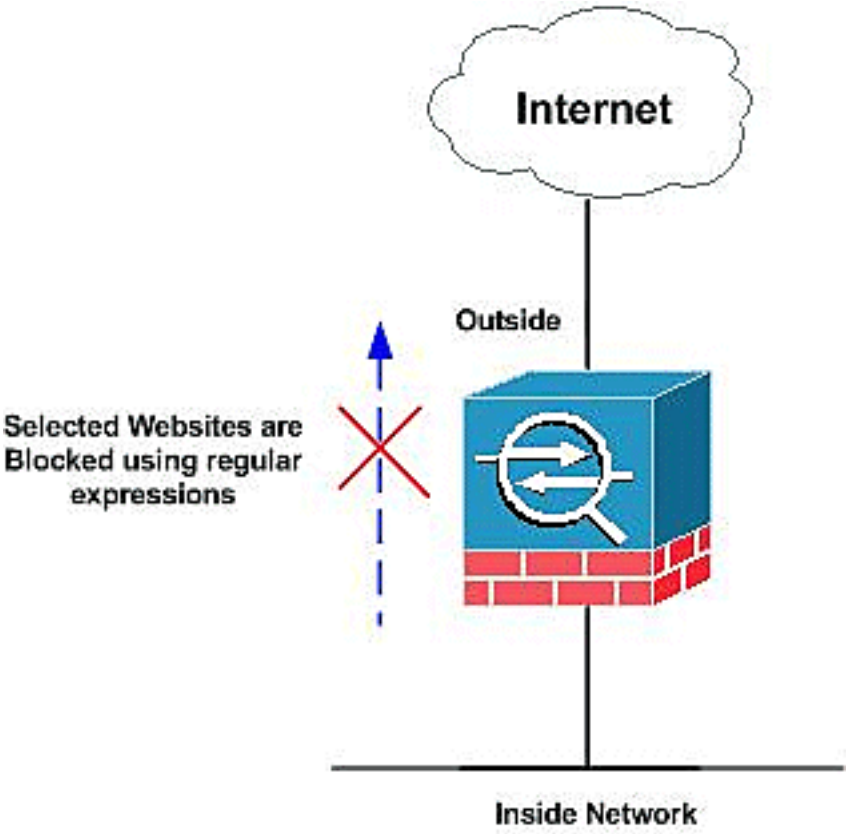
設定

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。



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 5.2 の ASA 設定 7.2(x)

ASA CLI 設定

ASA CLI の設定
ciscoasa#**show running-config** : Saved : ASA Version 7.2(2) ! hostname ciscoasa domain-name default.domain.invalid enable password 8Ry2YjIyt7RRXU24

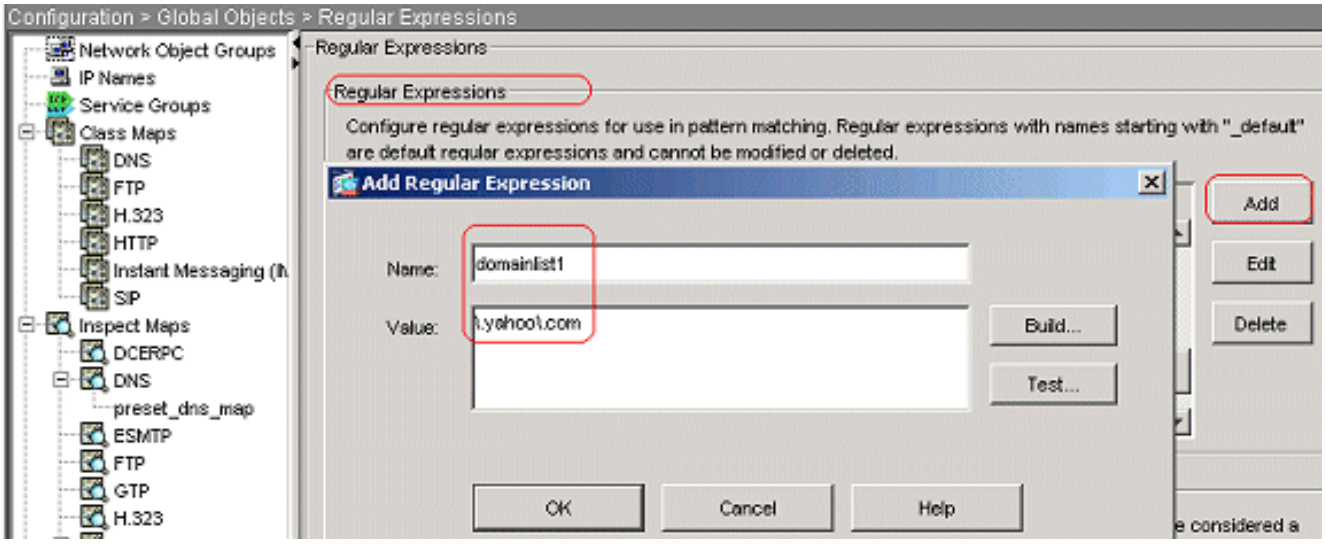
```
encrypted names ! interface Ethernet0/0 nameif inside
security-level 100 ip address 10.1.1.1 255.255.255.0 !
interface Ethernet0/1 nameif outside security-level 0 ip
address 192.168.1.5 255.255.255.0 ! interface
Ethernet0/2 nameif DMZ security-level 90 ip address
10.77.241.142 255.255.255.192 ! interface Ethernet0/3
shutdown no nameif no security-level no ip address !
interface Management0/0 shutdown no nameif no security-
level no ip address ! passwd 2KFQnbNIdI.2KYOU encrypted
regex urllist1
".*\.([Ee][Xx][Ee]|[Cc][Oo][Mm]|[Bb][Aa][Tt])
HTTP/1.[01]" !--- Extensions such as .exe, .com, .bat to
be captured and !--- provided the http version being
used by web browser must be either 1.0 or 1.1 regex
urllist2 ".*\.([Pp][Ii][Ff]|[Vv][Bb][Ss]|[Ww][Ss][Hh])
HTTP/1.[01]" !--- Extensions such as .pif, .vbs, .wsh to
be captured !--- and provided the http version being
used by web browser must be either !--- 1.0 or 1.1 regex
urllist3 ".*\.([Dd][Oo][Cc]|[Xx][Ll][Ss]|[Pp][Pp][Tt])
HTTP/1.[01]" !--- Extensions such as .doc(word),
.xls(ms-excel), .ppt to be captured and provided !---
the http version being used by web browser must be
either 1.0 or 1.1 regex urllist4
".*\.([Zz][Ii][Pp]|[Tt][Aa][Rr]|[Tt][Gg][Zz])
HTTP/1.[01]" !--- Extensions such as .zip, .tar, .tgz to
be captured and provided !--- the http version being
used by web browser must be either 1.0 or 1.1 regex
domainlist1 "\.yahoo\.com" regex domainlist2
"\.myspace\.com" regex domainlist3 "\.youtube\.com" !---
Captures the URLs with domain name like yahoo.com, !---
youtube.com and myspace.com regex contenttype "Content-
Type" regex applicationheader "application/.*" !---
Captures the application header and type of !--- content
in order for analysis boot system disk0:/asa802-k8.bin
ftp mode passive dns server-group DefaultDNS domain-name
default.domain.invalid access-list inside_mpc extended
permit tcp any any eq www access-list inside_mpc
extended permit tcp any any eq 8080 !--- Filters the
http and port 8080 !--- traffic in order to block the
specific traffic with regular !--- expressions pager
lines 24 mtu inside 1500 mtu outside 1500 mtu DMZ 1500
no failover icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-602.bin no asdm history enable
arp timeout 14400 route DMZ 0.0.0.0 0.0.0.0
10.77.241.129 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 uauth 0:05:00 absolute dynamic-access-policy-
record DfltAccessPolicy http server enable http 0.0.0.0
0.0.0.0 DMZ no snmp-server location no snmp-server
contact snmp-server enable traps snmp authentication
linkup linkdown coldstart no crypto isakmp nat-traversal
telnet timeout 5 ssh timeout 5 console timeout 0 threat-
detection basic-threat threat-detection statistics
access-list ! class-map type regex match-any
DomainBlockList match regex domainlist1 match regex
domainlist2 match regex domainlist3 !--- Class map
created in order to match the domain names !--- to be
blocked class-map type inspect http match-all
BlockDomainsClass match request header host regex class
DomainBlockList !--- Inspect the identified traffic by
class !--- "DomainBlockList" class-map type regex match-
```

```
any URLBlockList match regex urllist1 match regex
urllist2 match regex urllist3 match regex urllist4 !---
Class map created in order to match the URLs !--- to be
blocked class-map inspection_default match default-
inspection-traffic class-map type inspect http match-all
AppHeaderClass match response header regex contenttype
regex applicationheader !--- Inspect the captured
traffic by regular !--- expressions "content-type" and
"applicationheader" class-map httptraffic match access-
list inside_mpc !--- Class map created in order to match
the !--- filtered traffic by ACL class-map type inspect
http match-all BlockURLsClass match request uri regex
class URLBlockList ! !--- Inspect the identified traffic
by class !--- "URLBlockList" ! policy-map type inspect
dns preset_dns_map parameters message-length maximum 512
policy-map type inspect http http_inspection_policy
parameters protocol-violation action drop-connection
class AppHeaderClass drop-connection log match request
method connect drop-connection log class
BlockDomainsClass reset log class BlockURLsClass reset
log !--- Define the actions such as drop, reset or log
!--- in the inspection policy map policy-map
global_policy class inspection_default inspect dns
preset_dns_map inspect ftp 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 policy-map
inside-policy class httptraffic inspect http
http_inspection_policy !--- Map the inspection policy
map to the class !--- "httptraffic" under the policy map
created for the !--- inside network traffic ! service-
policy global_policy global service-policy inside-policy
interface inside !--- Apply the policy to the interface
inside where the websites will be blocked prompt
hostname context
Cryptochecksum:e629251a7c37af205c289cf78629fc11 : end
ciscoasa#
```

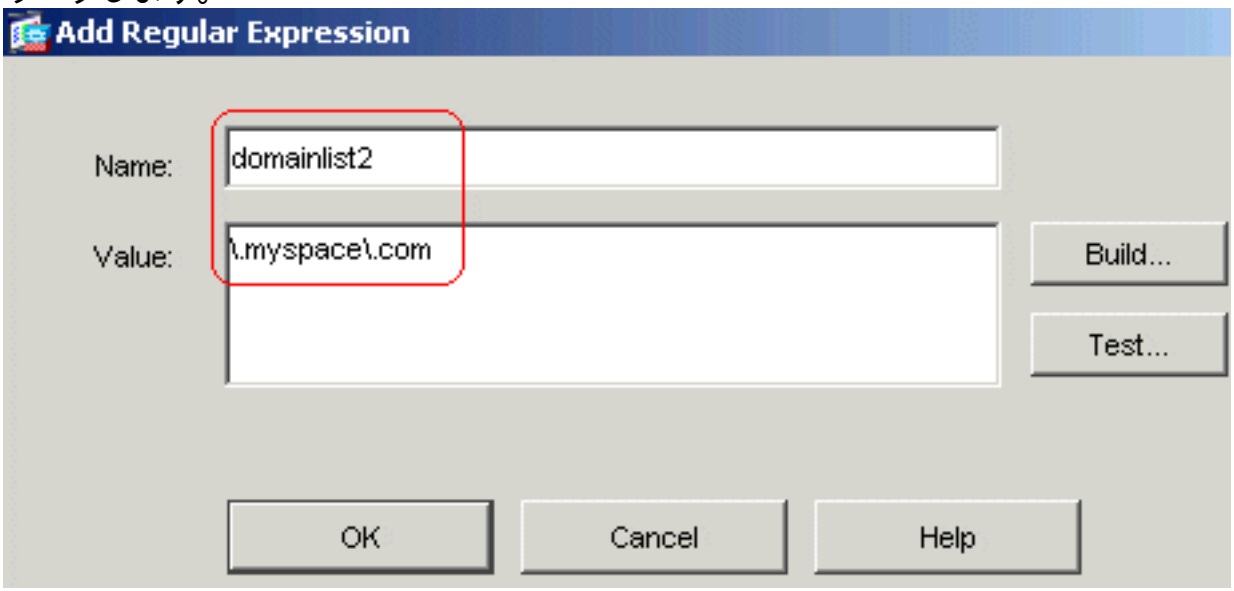
ASDM 5.2 の ASA 設定 7.2(x)

正規表現を設定し、特定の Web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:

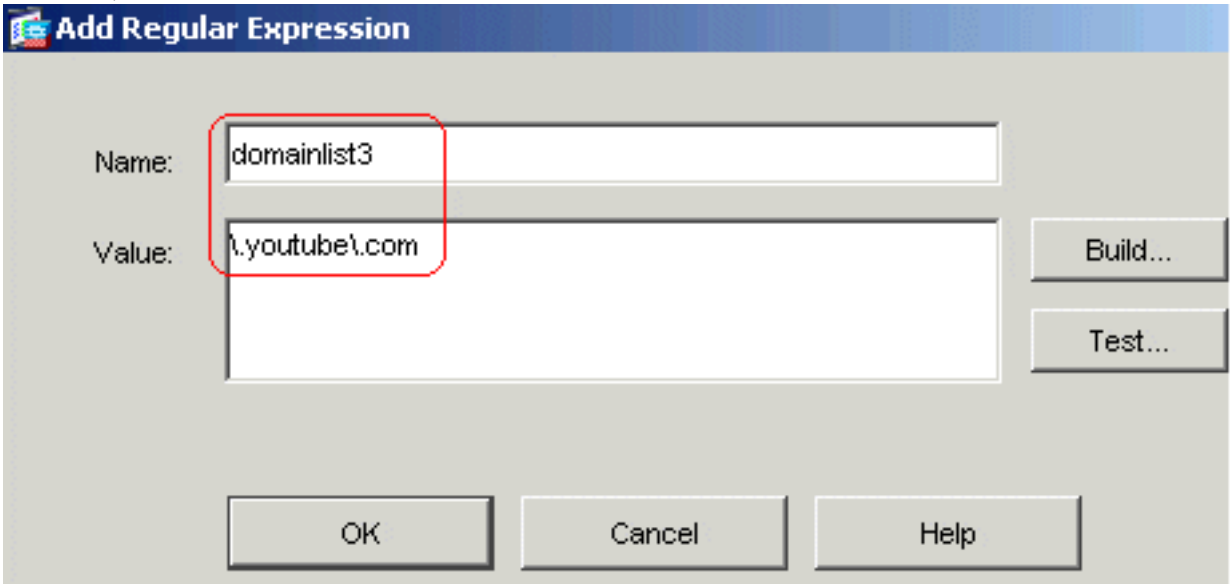
1. **正規表現の作成> グローバル オブジェクト > 正規表現** 『Configuration』 を選択 し、正規表現タブの下で正規表現を作成するために『Add』 をクリック して下さい。ドメイン名 **yahoo.com** をキャプチャする正規表現 **domainlist1** を作成します。 [OK] をクリックします。



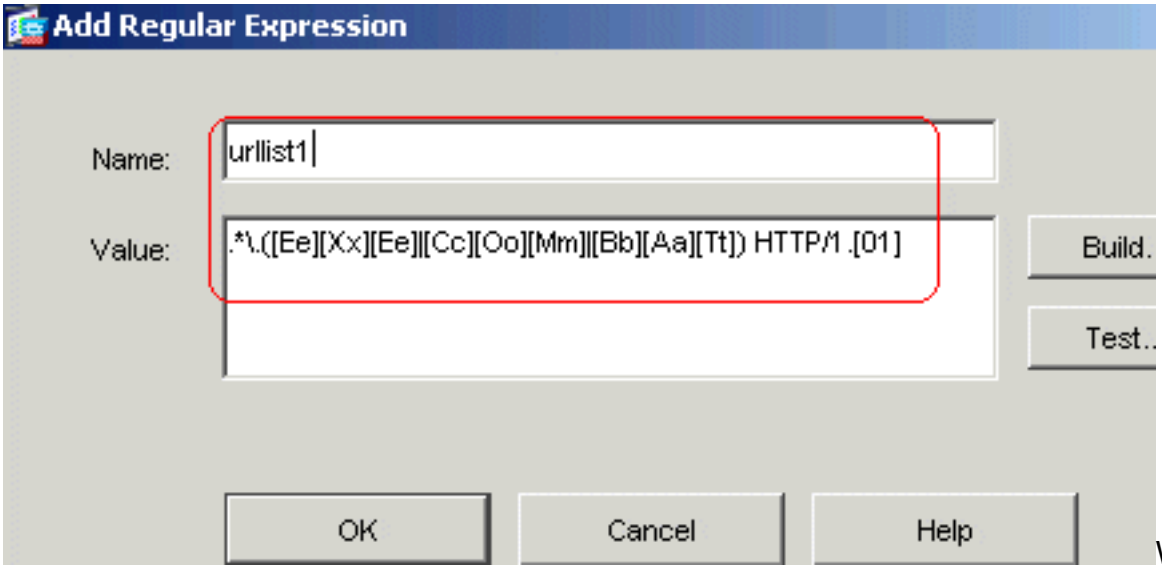
ドメイン名 **myspace.com** をキャプチャする正規表現 **domainlist2** を作成します。 [OK] をクリックします。



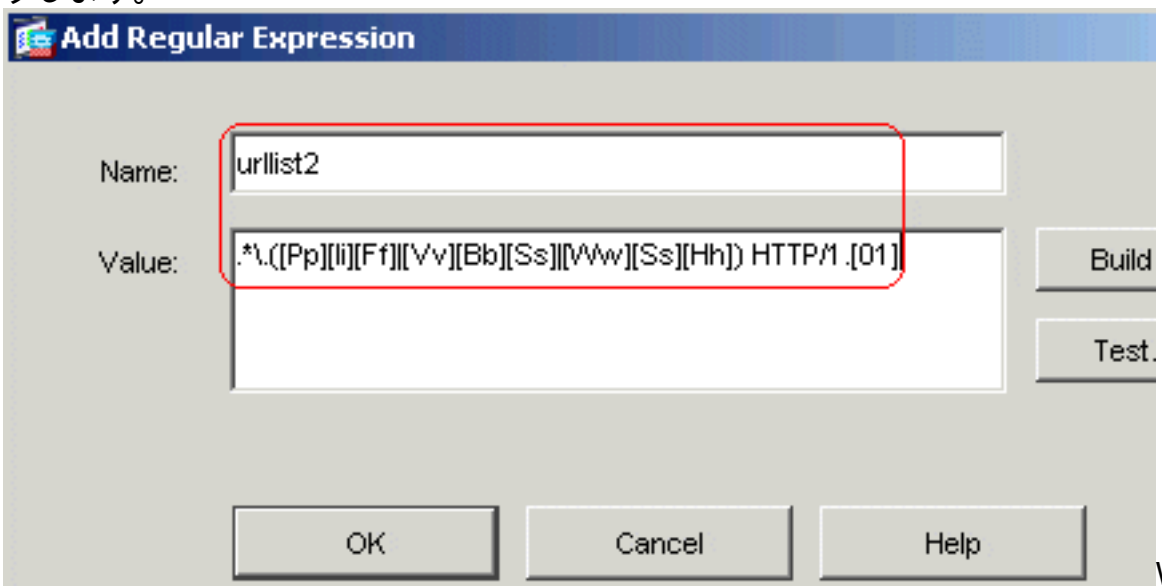
ドメイン名 **youtube.com** をキャプチャする正規表現 **domainlist3** を作成します。 [OK] をクリックします。



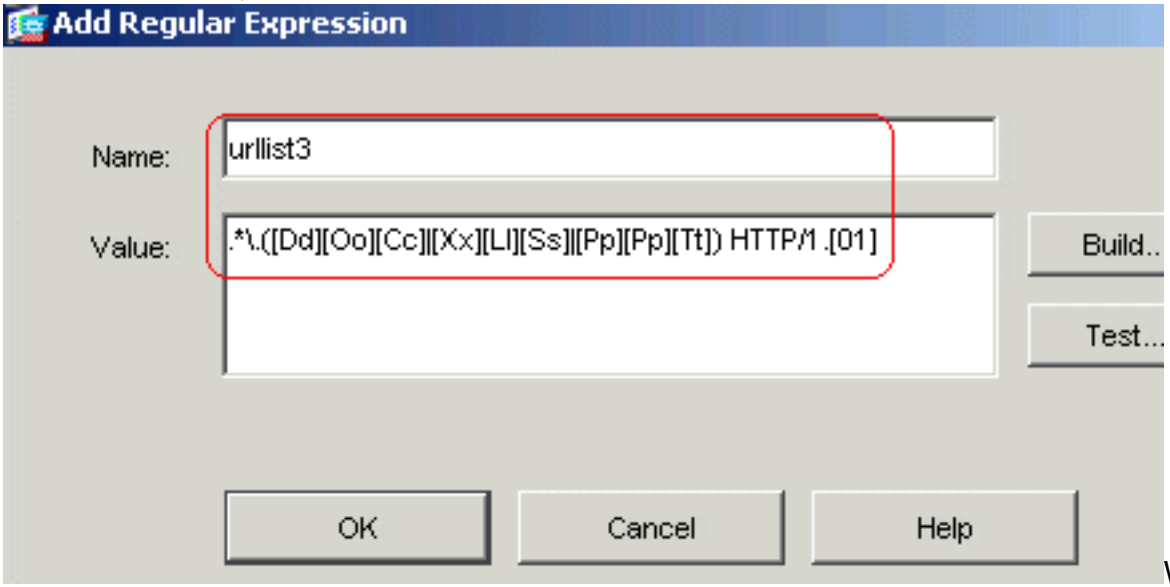
Web ブラウザによって使用される http バージョンが 1.0 または 1.1 である必要があったら **exe**、**com** および**バット**のようなファイル拡張子をキャプチャ するために正規表現 **urllist1 を**作成して下さい。 [OK] をクリックします。



Webブラウザによって使用する HTTP バージョンが 1.0 または 1.1 **PIF**、**vbs** および **wsh** のようなファイル拡張子を、キャプチャ するために正規表現 **urllist2 を**作成して下さい。 [OK] をクリックします。

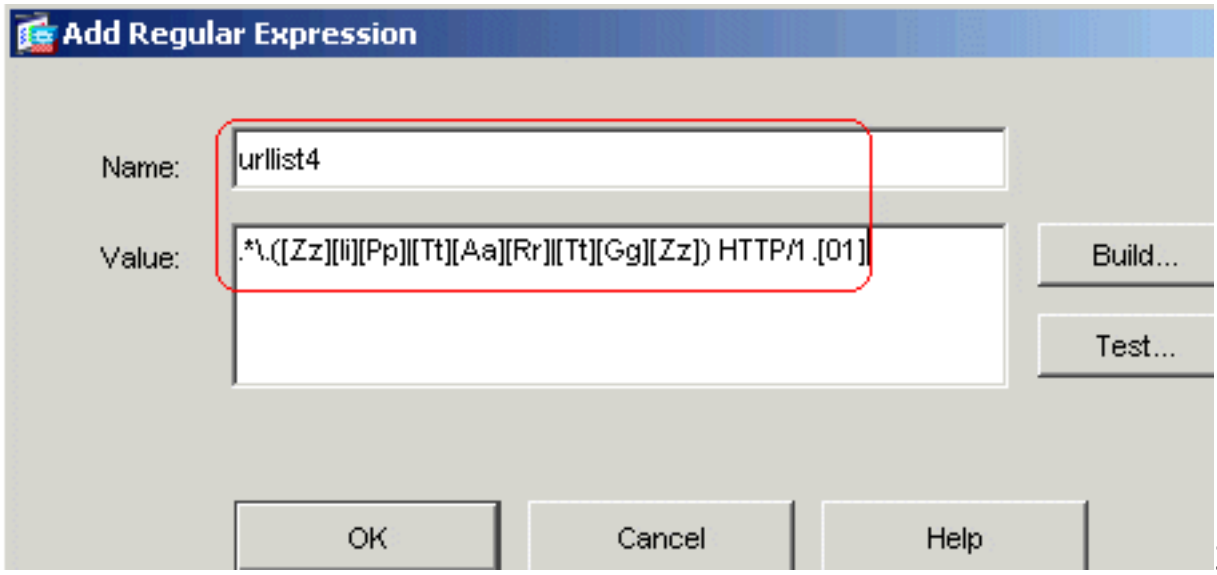


Webブラウザによって使用する HTTP バージョンが 1.0 または 1.1 **ドキュメント**、**xls** および **ppt** のようなファイル拡張子を、キャプチャ するために正規表現 **urllist3 を**作成して下さい。 [OK] をクリックします。

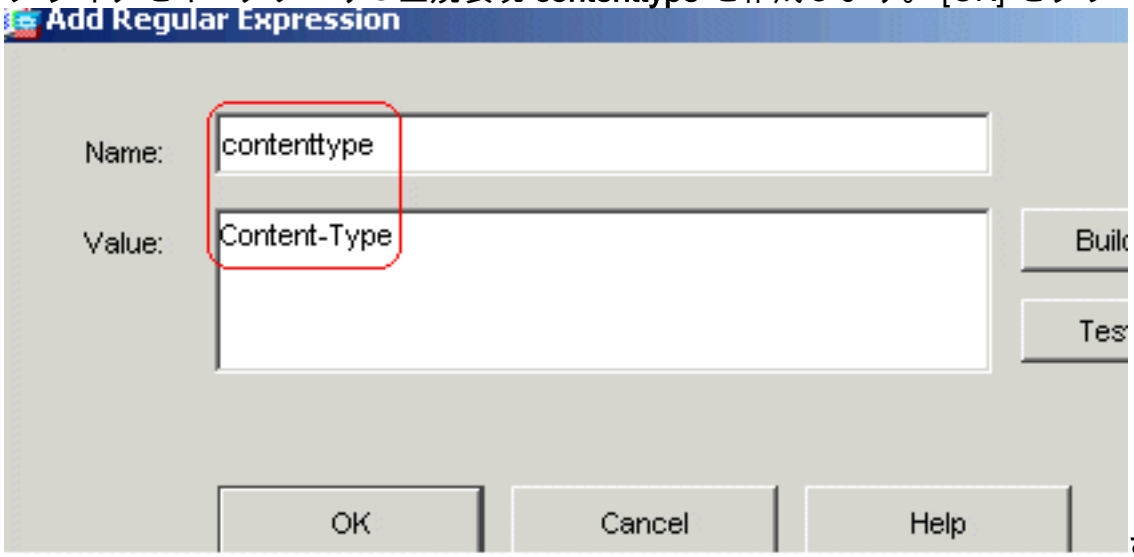


Webブラウザによって使用する HTTP バージョンが 1.0 または 1.1 **zip**、**tar** および **tgz** のようなファ

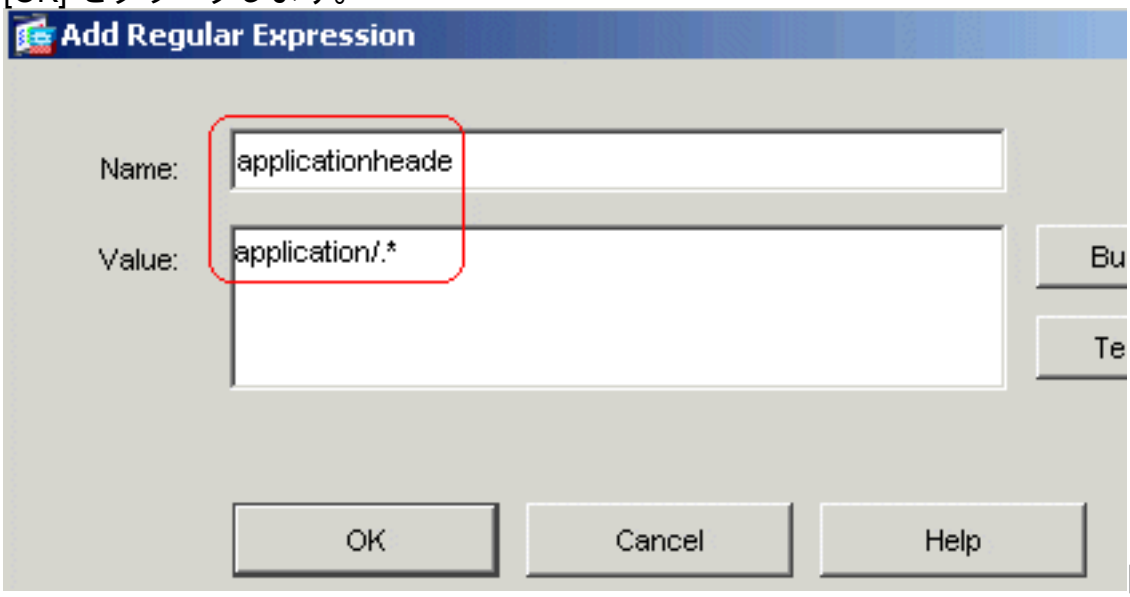
イル拡張子を、キャプチャ するために正規表現 **urllist4 を**作成して下さい。 [OK] をクリックします。



コンテンツ タイプをキャプチャする正規表現 **contenttype** を作成します。 [OK] をクリックします。



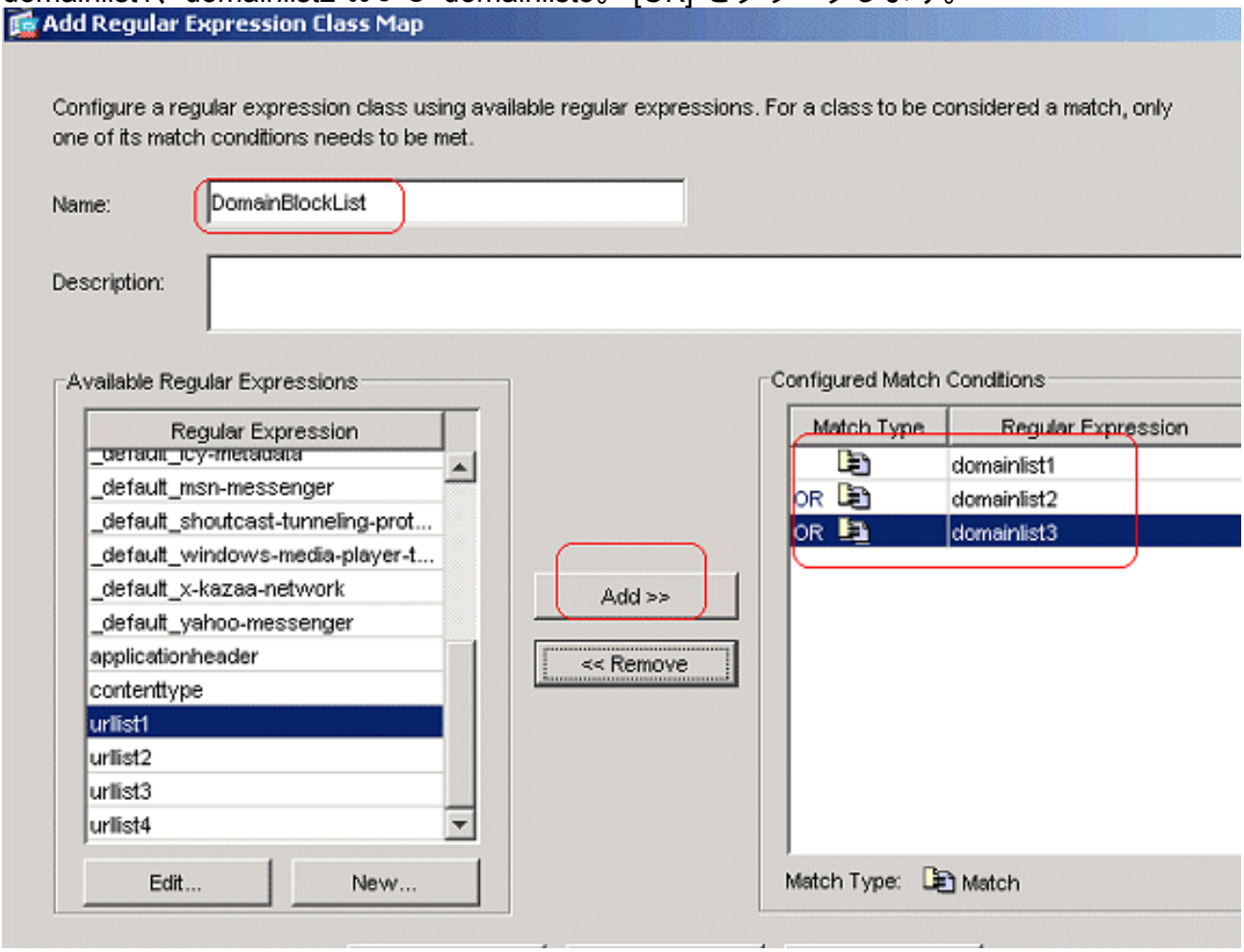
さまざまなアプリケーション ヘッダーをキャプチャする正規表現 **applicationheader** を作成します。 [OK] をクリックします。



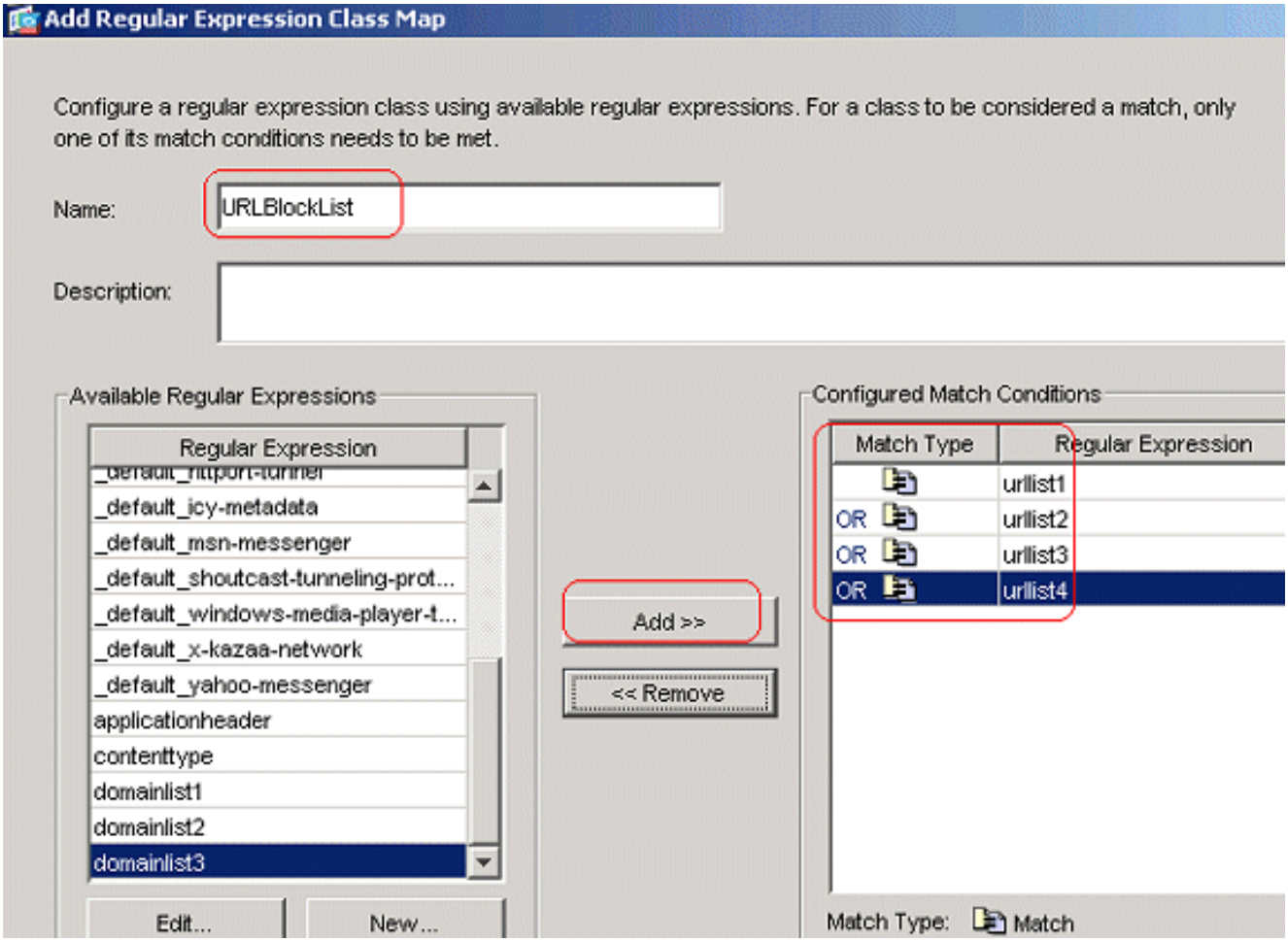
同等の CLI 設定

2. **正規表現クラスの作成> グローバル オブジェクト > 正規表現** 『Configuration』 を選択 し、

正規表現クラス タブの下でさまざまなクラスを作成するために『Add』 をクリック して下さい。正規表現の一致するために正規表現クラス **DomainBlockList を**作成して下さい: domainlist1、domainlist2 および domainlist3。 [OK] をクリックします。

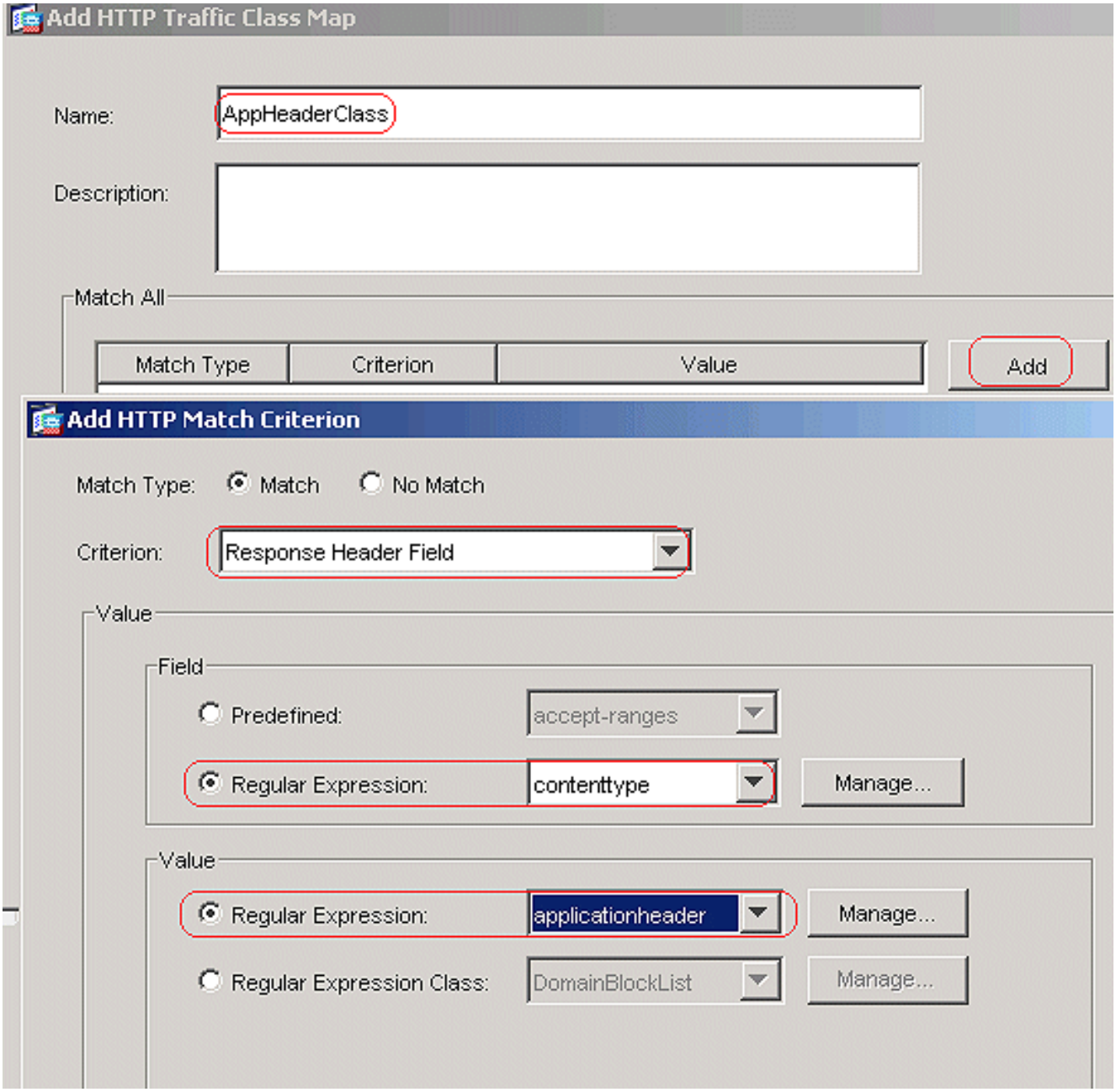


正規表現の一致するために正規表現クラス **URLBlockList を**作成して下さい: urllist1、urllist2、urllist3 および urllist4。 [OK] をクリックします。

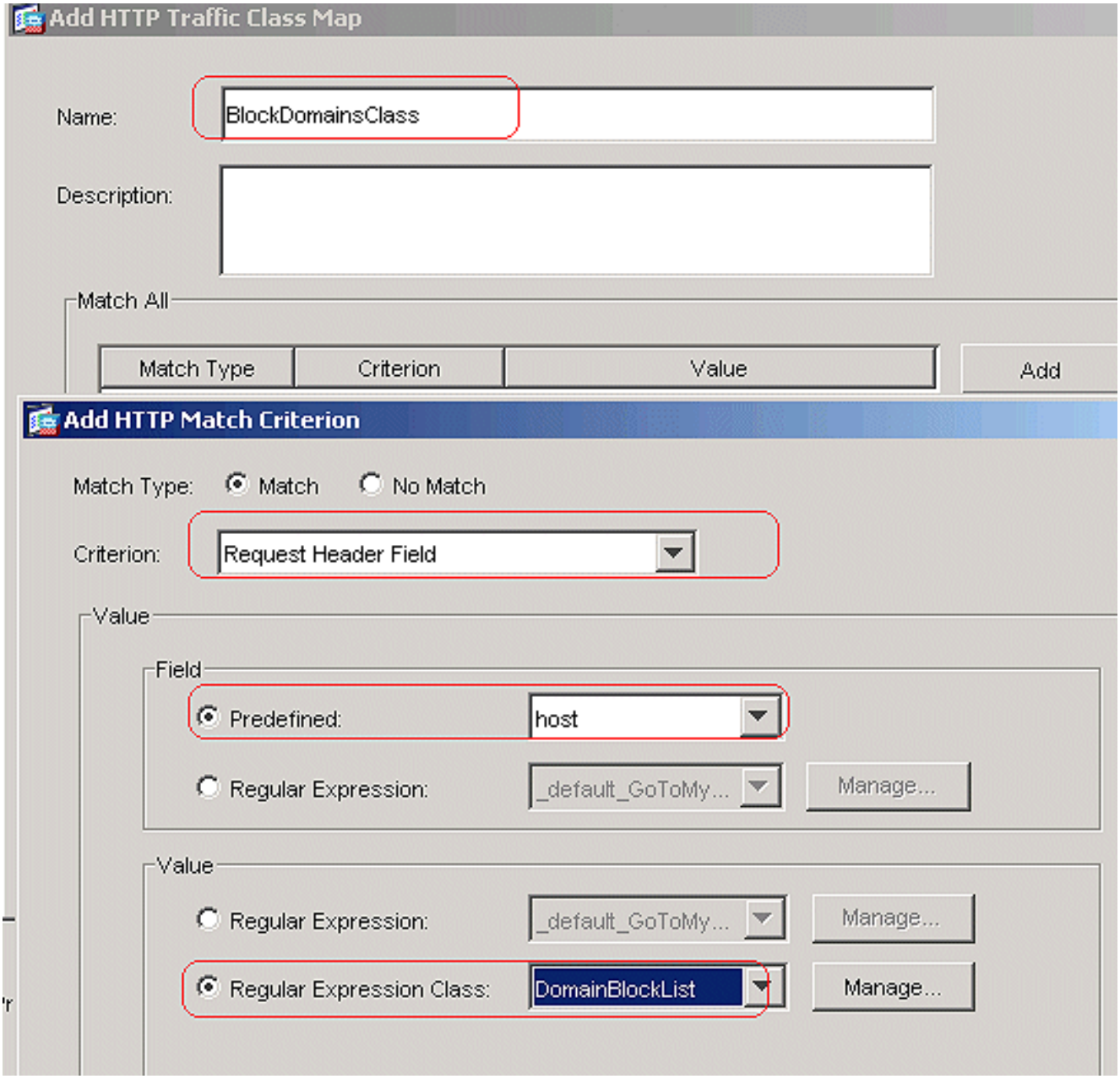


同等の CLI 設定

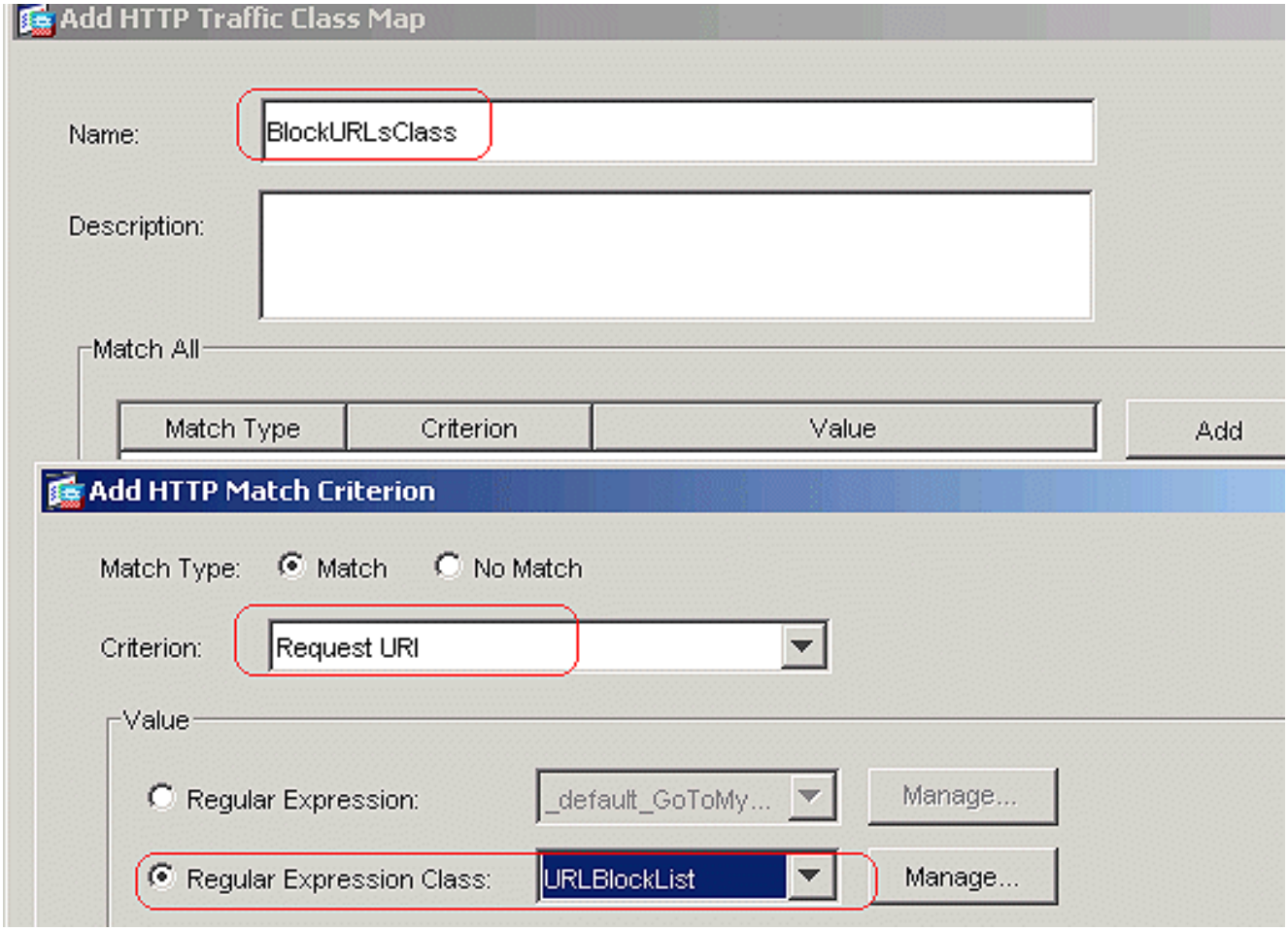
3. **クラス マップによる特定されたトラフィックの検査> グローバル オブジェクト > クラスマップ > HTTP > Add** クラスマップをさまざまな正規表現によって識別される HTTPトラフィックを点検するために作成するために『Configuration』 を選択 して下さい。正規表現キャプチャが付いている応答 ヘッダーを一致するためにクラスマップ **AppHeaderClass を**作成して下さい。



[OK] をクリックします。正規表現キャプチャが付いている要求ヘッダーを一致するために クラスマップ **BlockDomainsClass** を作成して下さい。

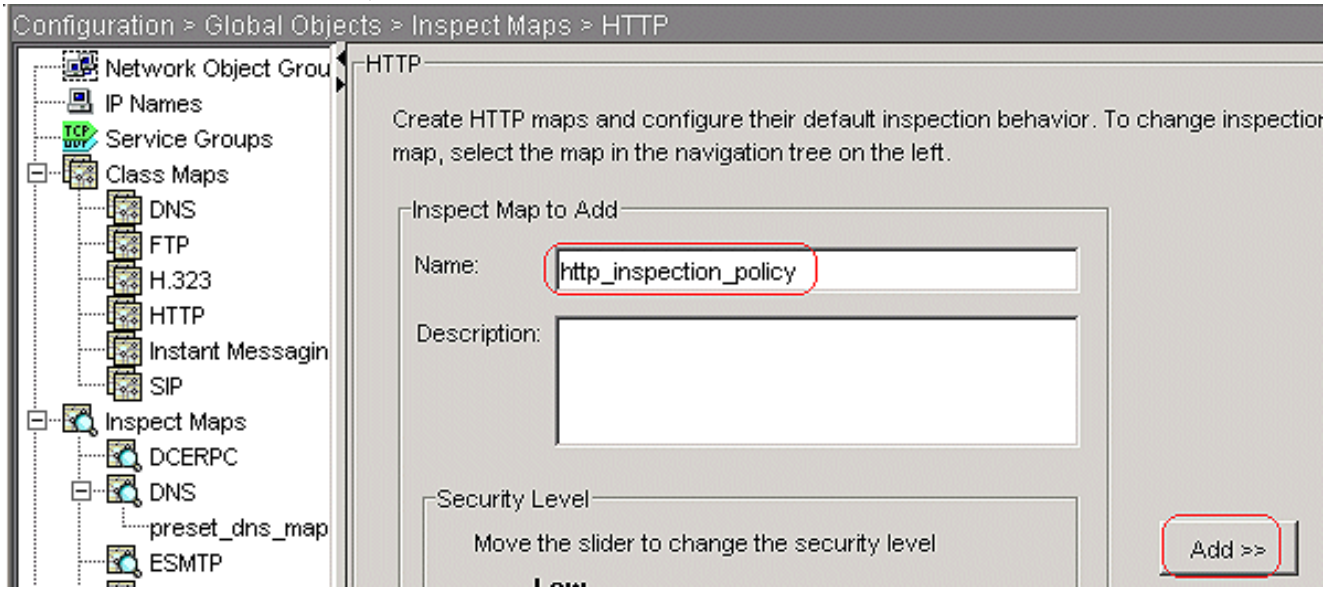


[OK] をクリックします。正規表現キャプチャとの要求 URI を一致するためにクラスマップ **BlockURLsClass を**作成して下さい。

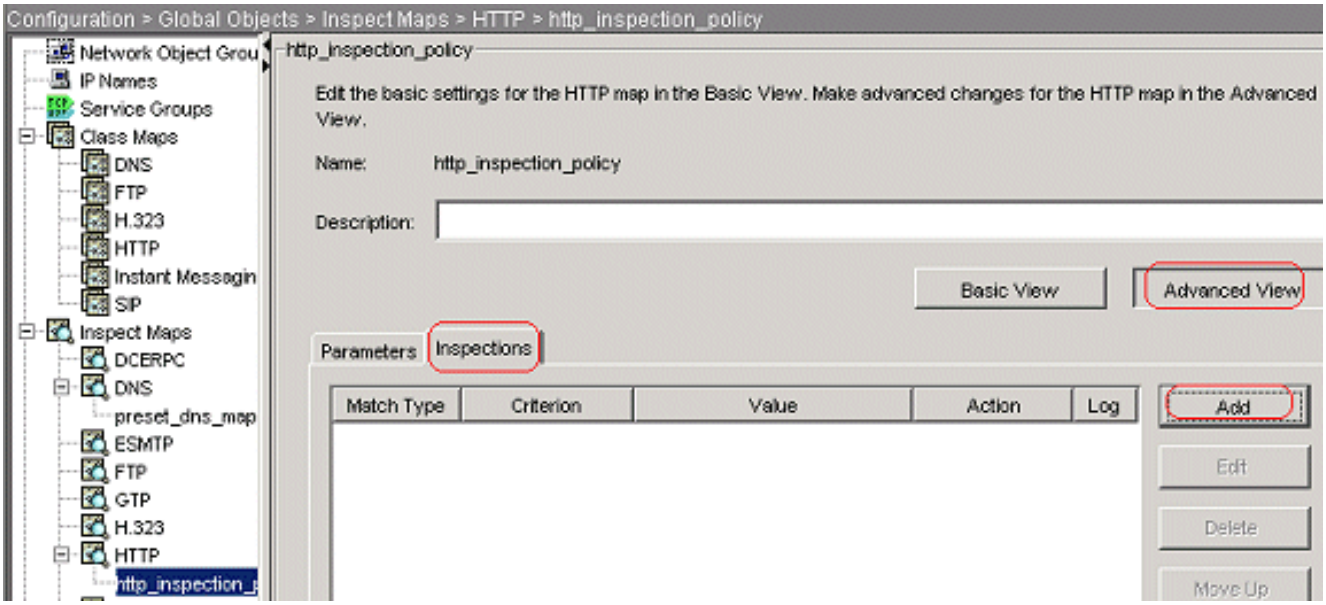


[OK] をクリックします。**同等の CLI 設定**

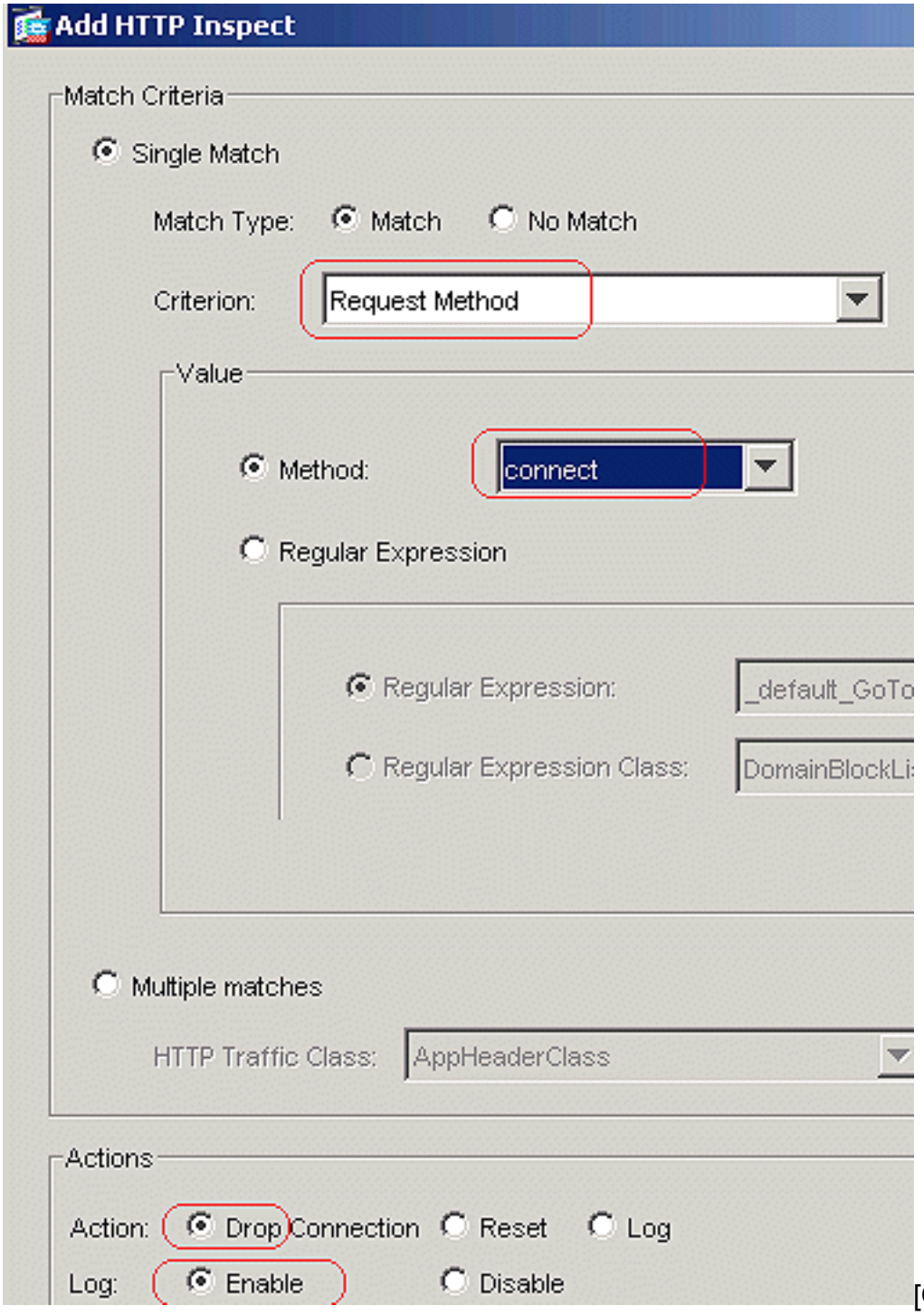
4. **検査ポリシーで一致するトラフィックに対するアクションを設定する> グローバル オブジェクト > Inspect マッピング します > HTTP http_inspection_policy を**一致されたトラフィックのための操作を設定 するために作成するために『Configuration』 を選択 して下さい。 『Add』 をクリック し、**適用して下さい。**



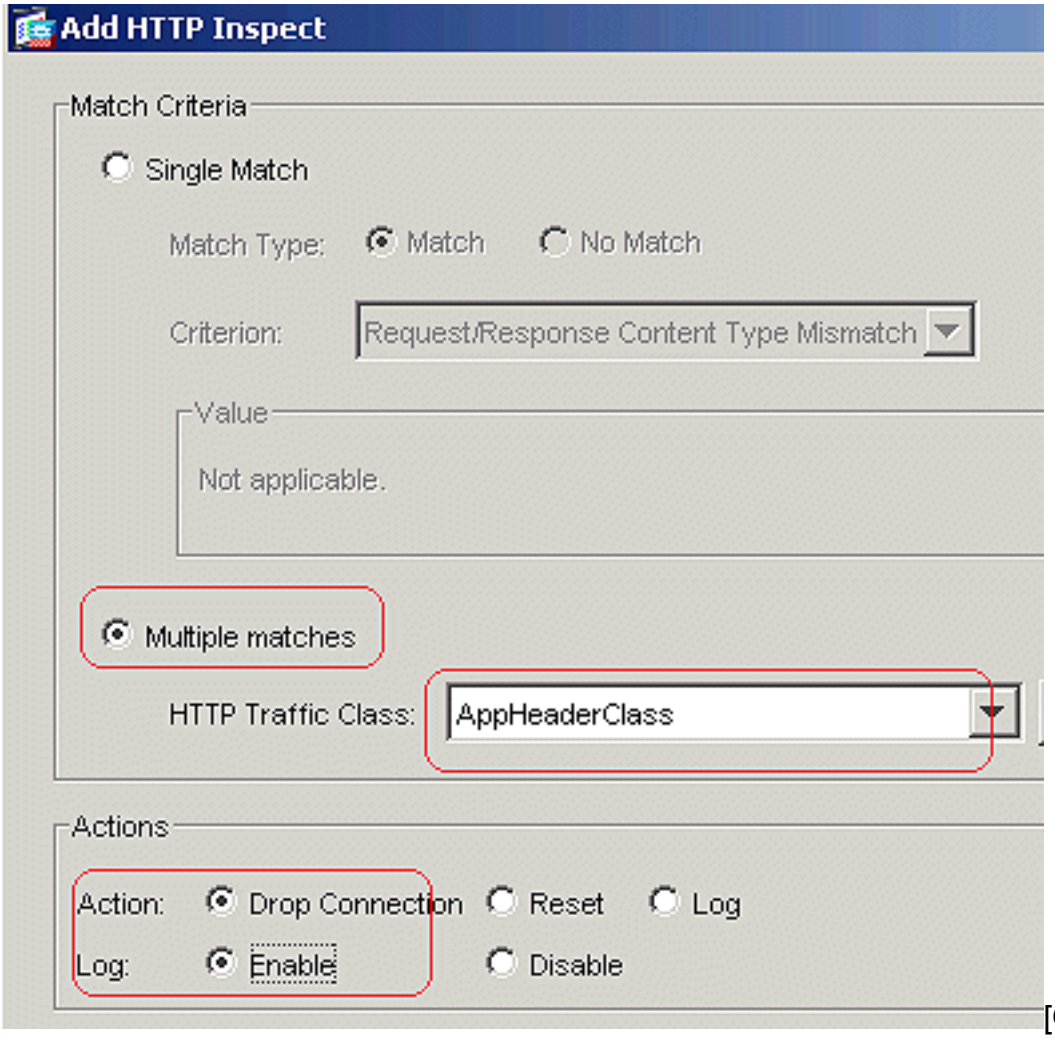
> グローバル オブジェクト > Inspect マッピング し、> HTTP > http_inspection_policy 『Advanced』 をクリック します **View > インスペクション > Add を**これまでのところ作成されるさまざまなクラスのための操作を設定 するために『Configuration』 を選択 して下さい。



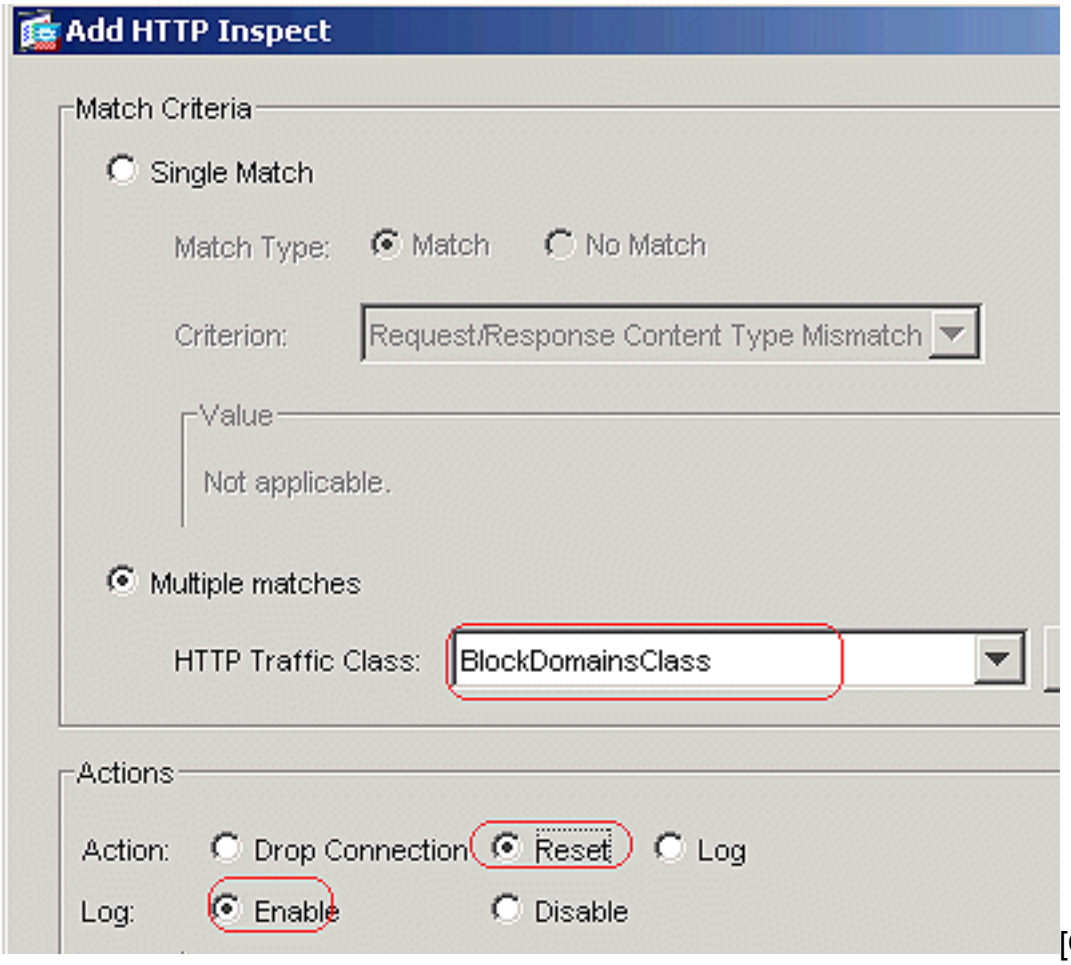
[OK] をクリックします。**ドロップする接続**として操作を設定 して下さい; 基準のための口ギングを要求 方式として**有効に し、**ように**接続します**評価して下さい。



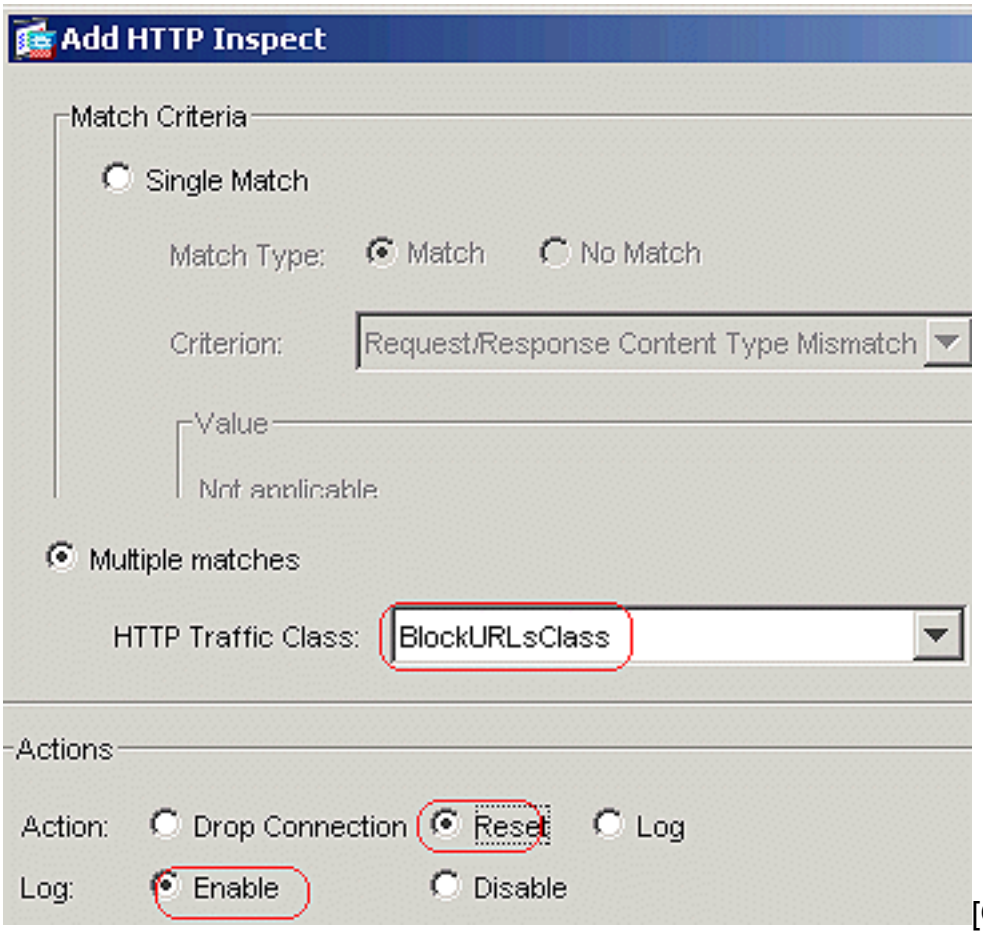
[OK] をクリックします。操作を**ドロップする接続**として設定 し、クラス **AppHeaderClass** のための**ロギングを有効に して下さい。**



[OK] をクリックします。操作を**リセット**として設定 し、クラス **BlockDomainsClass** のための口ギングを**有効に して下さい**。



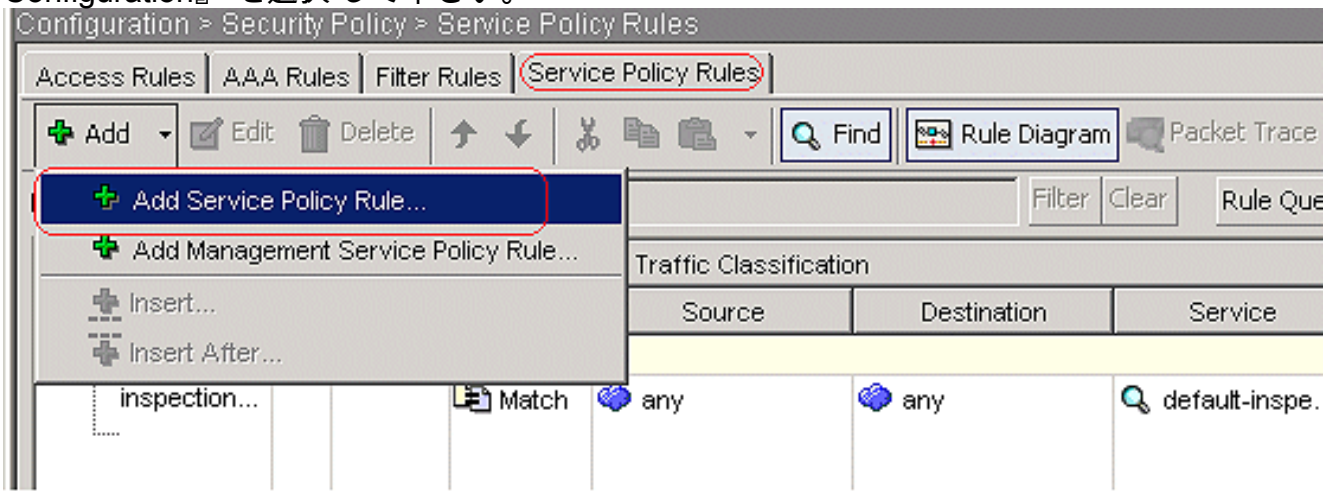
[OK] をクリックします。操作を**リセット**として設定 し、クラス **BlockURLsClass** のための**ロギングを有効**



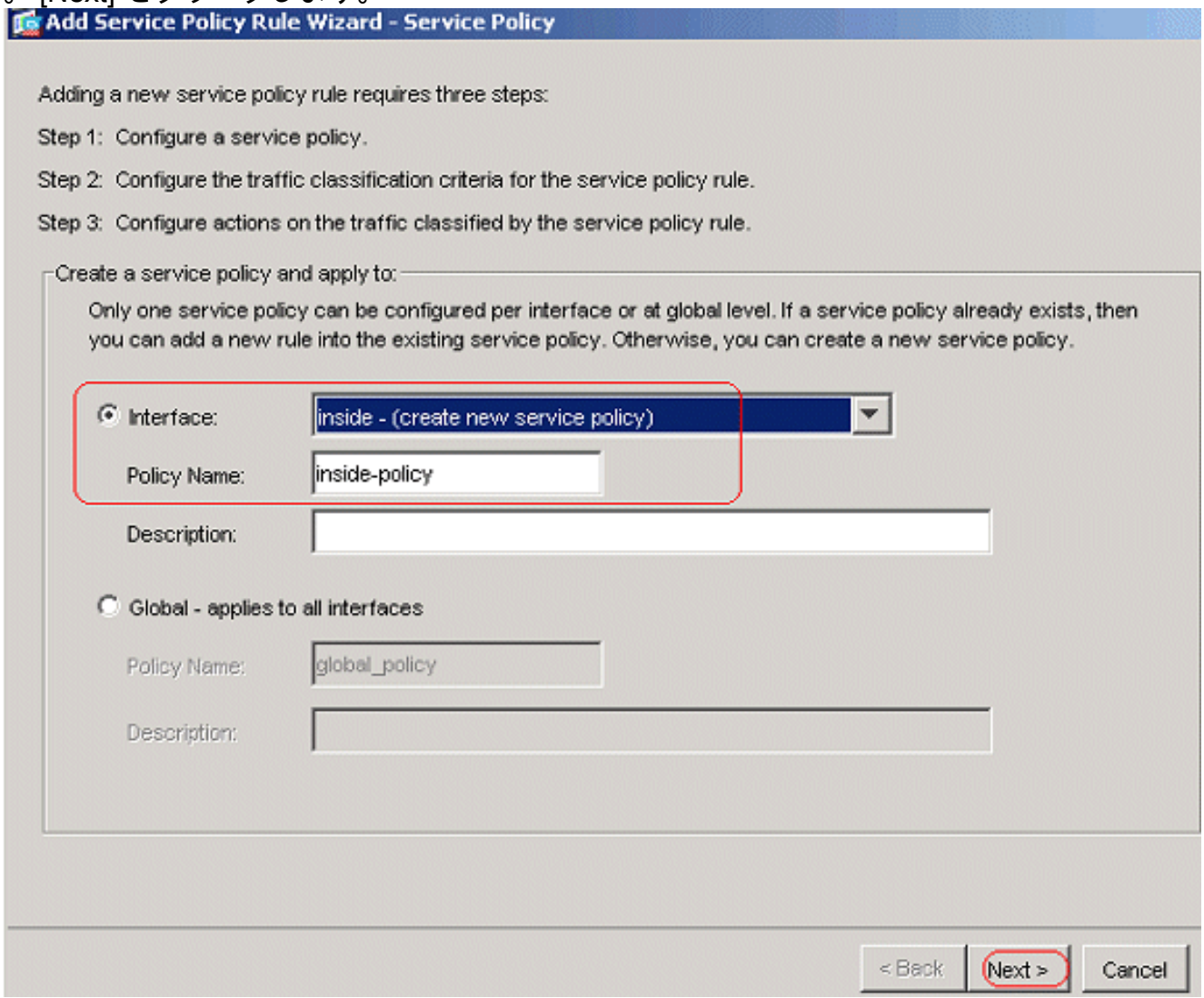
に して下さい。[OK] をクリックします。[Apply] をクリックします。**同等の CLI 設定**

5. **検査の HTTP ポリシーをインターフェイスに適用する**サービス ポリシー Rules タブの下で **> Security ポリシー > サービス ポリシー ルール > Add > Add サービス ポリシー ルールを『**

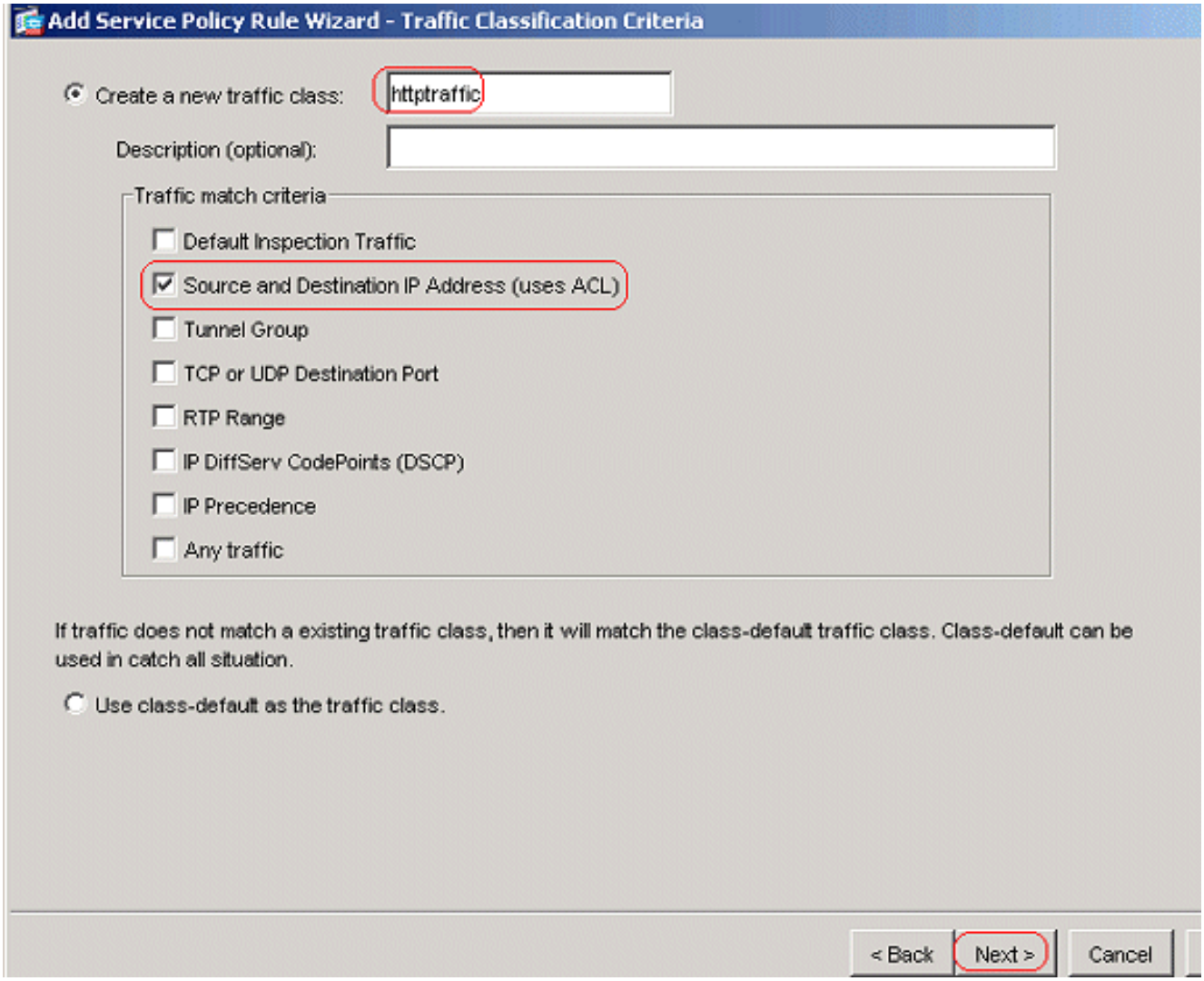
Configuration』 を選択 して下さい。



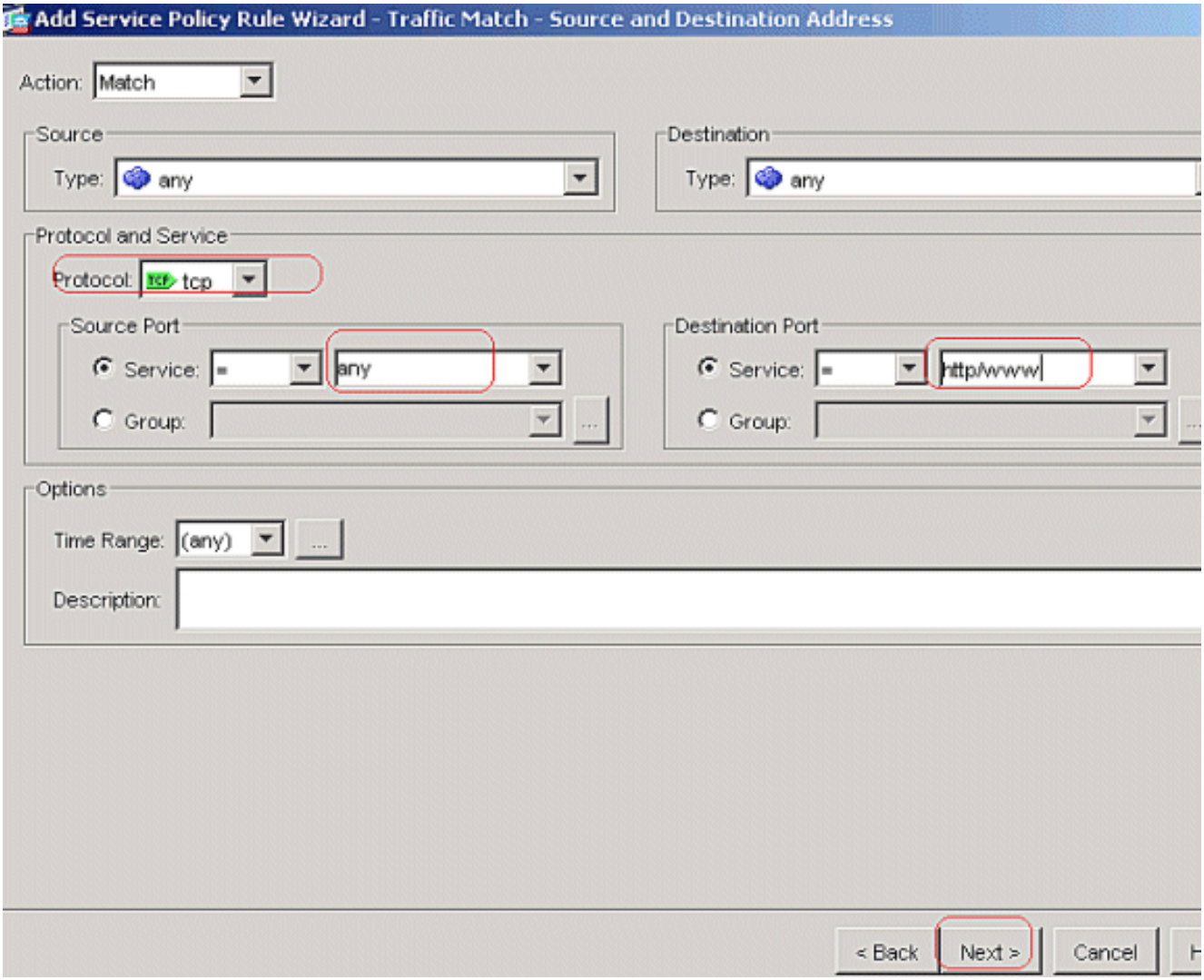
HTTP トラフィックの中ポリシーとしてドロップダウン・メニューおよびポリシー名前から**内部インターフェイス**が付いている**インターフェイス** オプション ボタンを選択して下さい。 [Next] をクリックします。



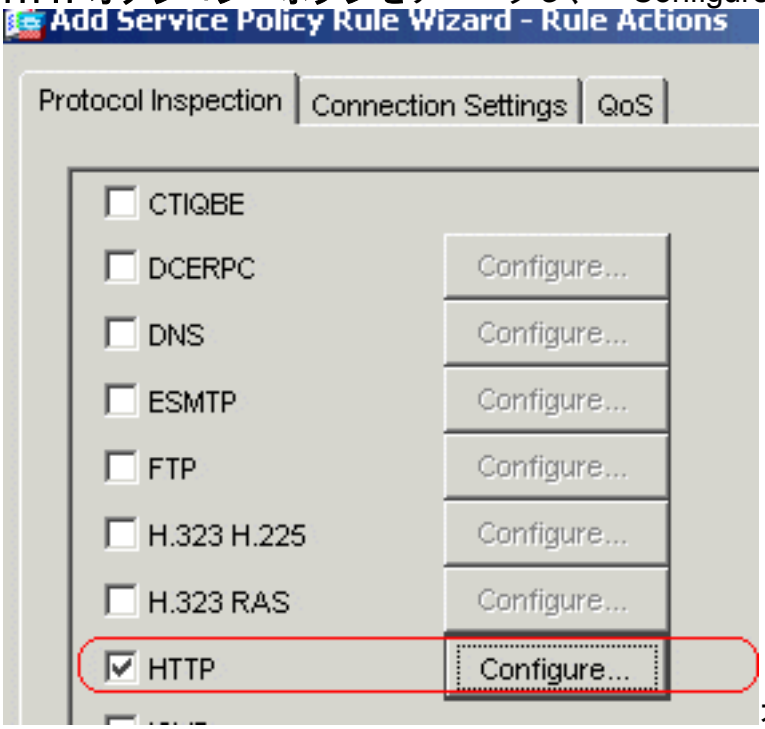
httptraffic クラスマップを作成し**送信元 および 宛先 IPアドレス (使用 ACL) を**チェックして下さい。 [Next] をクリックします。



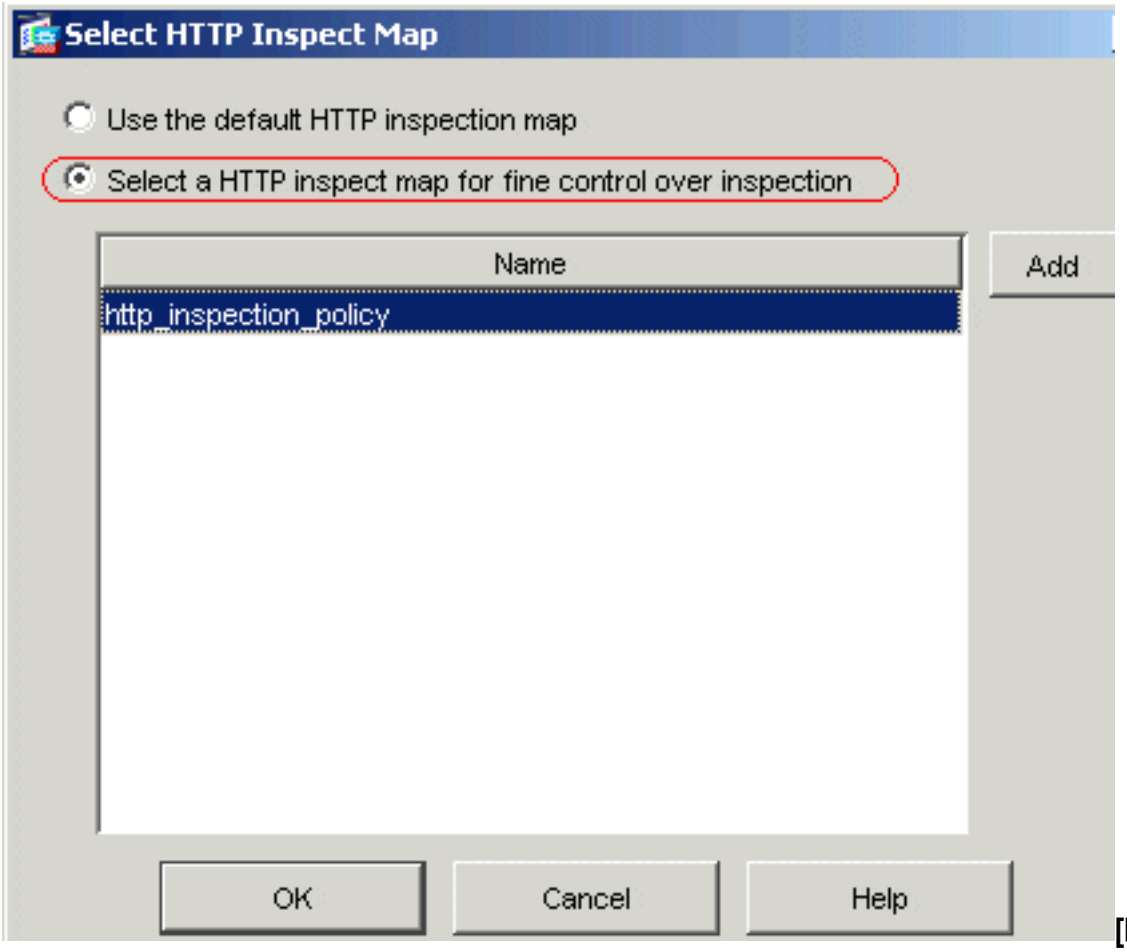
HTTP TCPポートの送信元および宛先を同様に選択して下さい。 [Next] をクリックします。



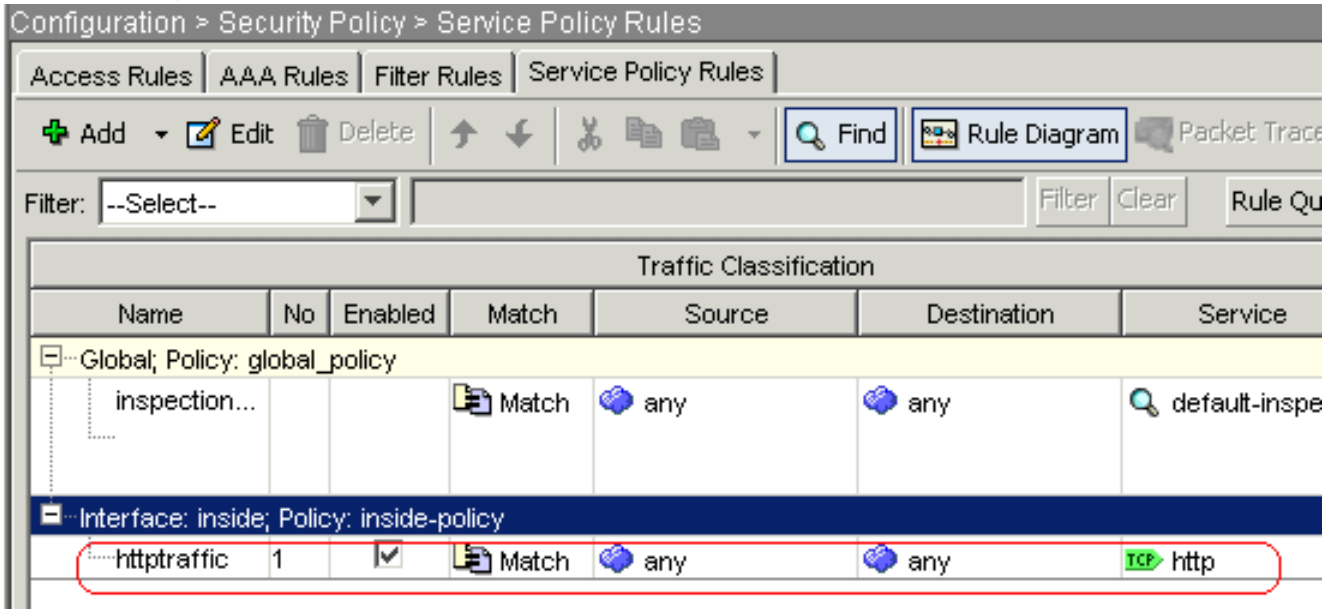
HTTPオプション・ボタンをチェックし、『Configure』 をクリック して下さい。



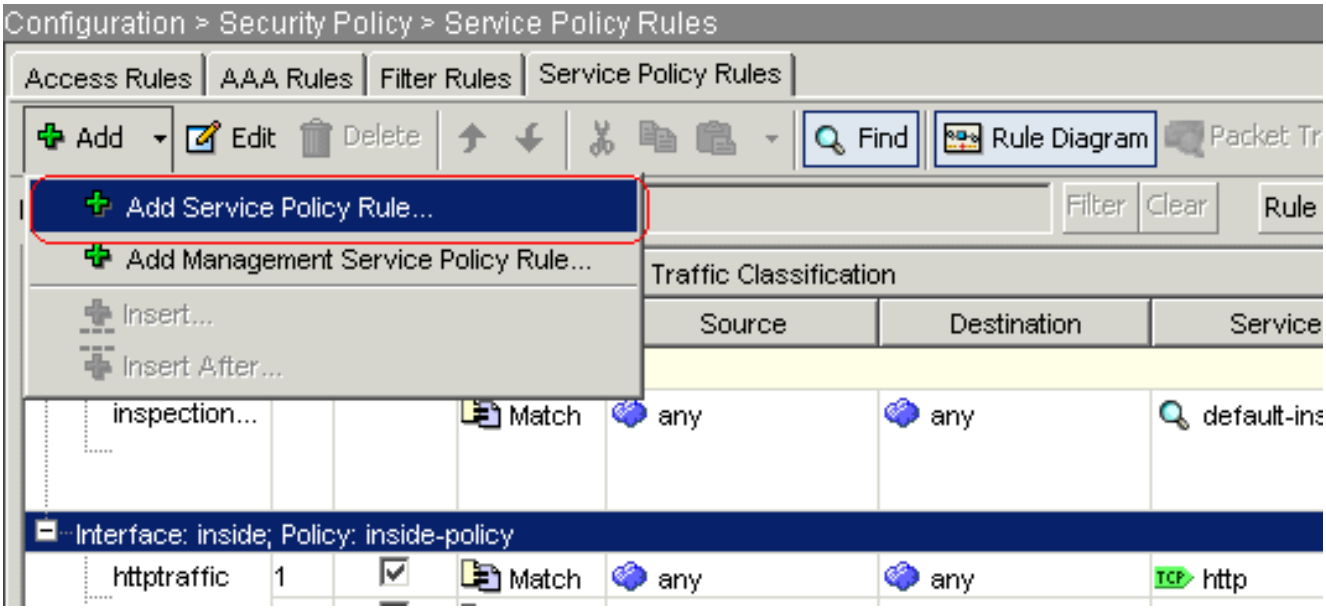
オプション ボタンを**選択しますインスペクションの制御に HTTP Inspect マップを**チェックして下さい。 [OK] をクリックします。



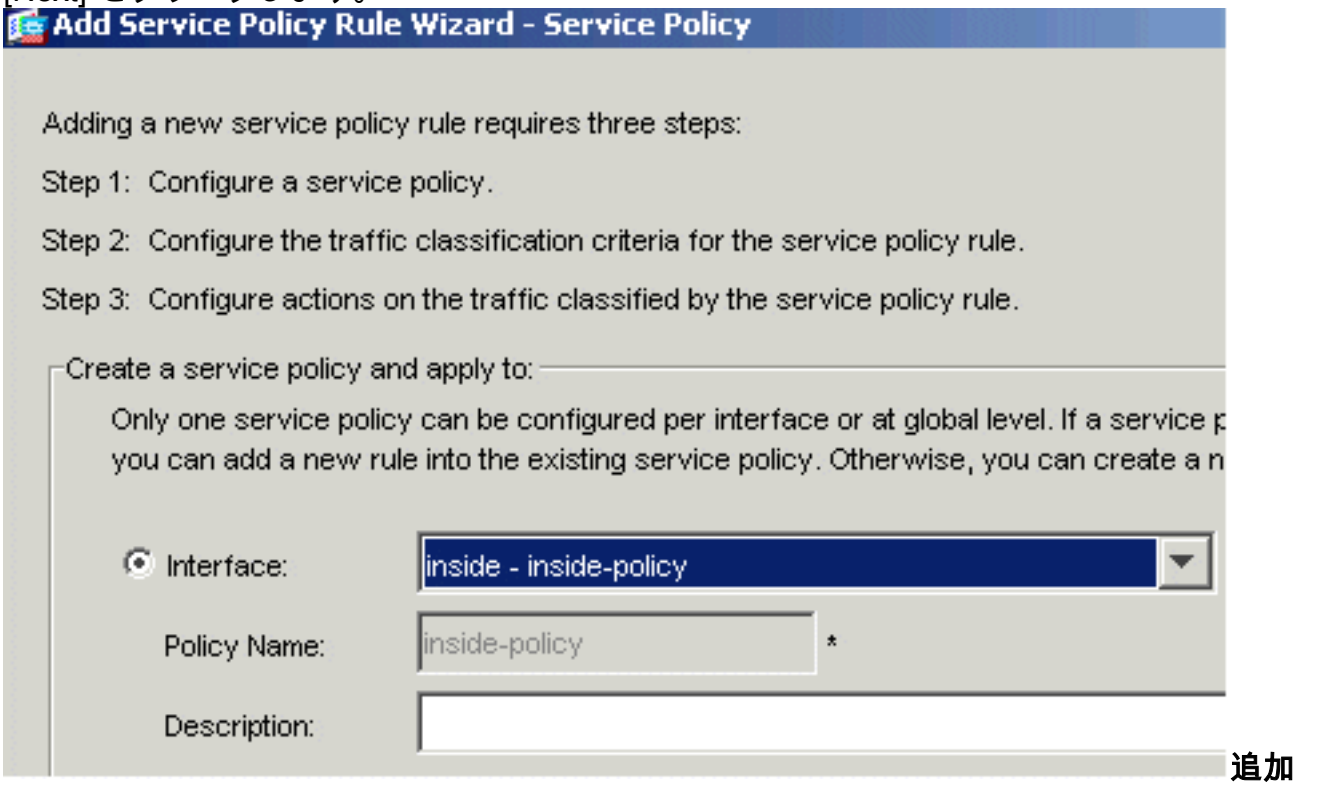
[Finish] をクリックします。



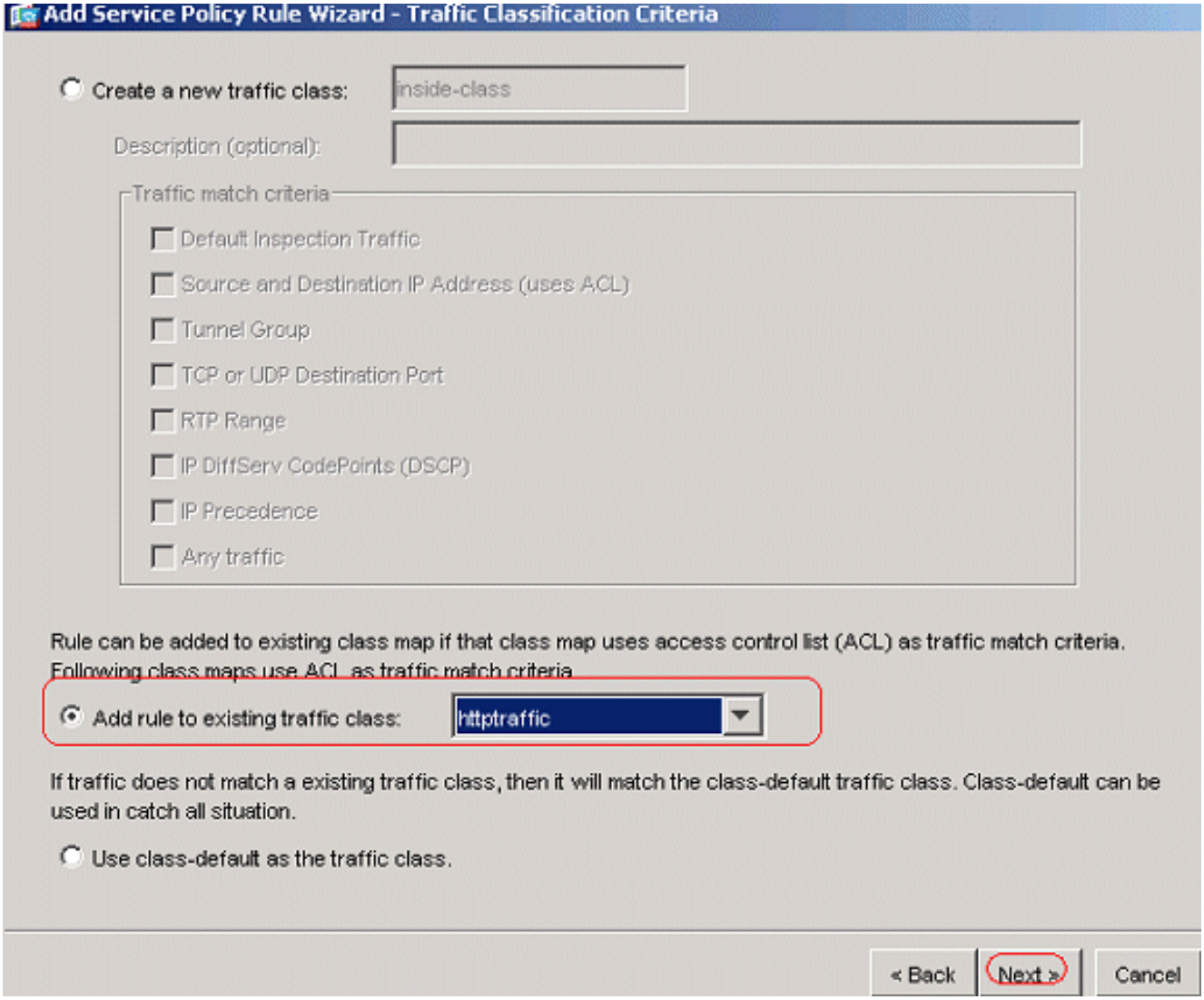
ポート 8080 のトラフィック再度、> Add サービス ポリシー ルールを『Add』 をクリックして下さい。



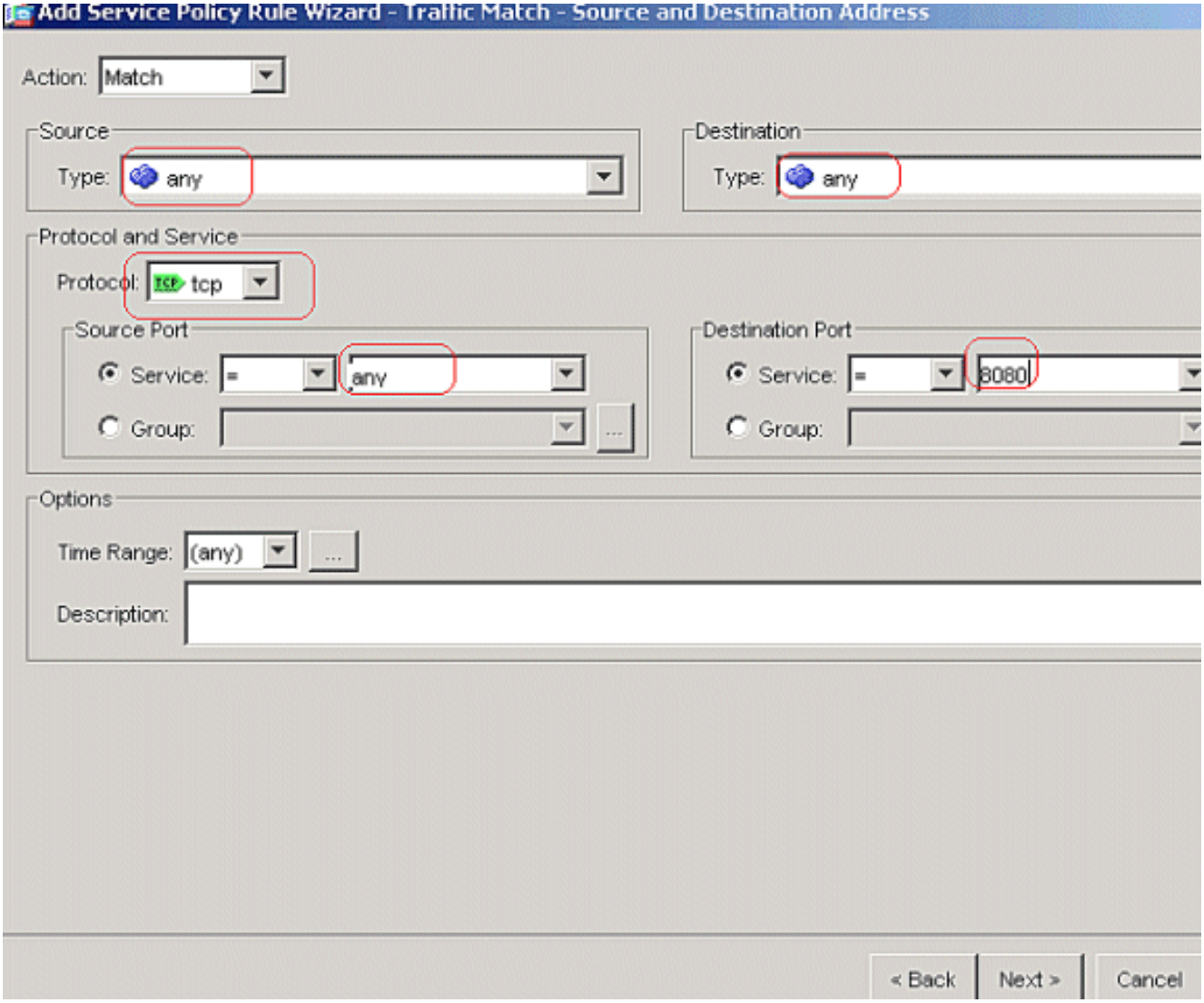
[Next] をクリックします。



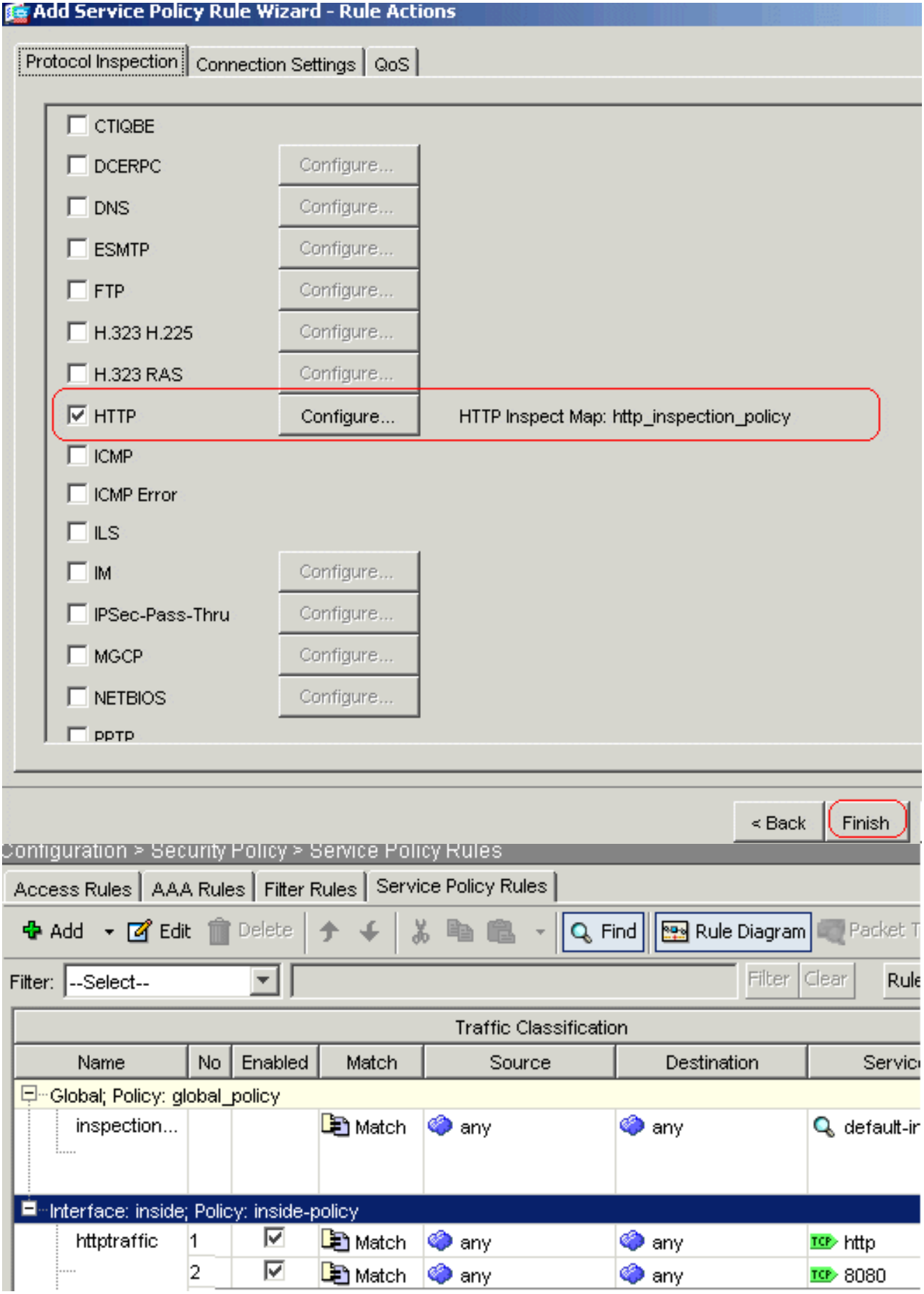
追加ルールを既存のトラフィック クラス オプション ボタンに選択し、ドロップダウン・メニューから **httptraffic** 選択して下さい。 [Next] をクリックします。



8080 TCPポートの送信元および宛先を同様に選択して下さい。 [Next] をクリックします。



[Finish] をクリックします。



[Apply] をクリックします。**同等の CLI 設定**

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の表示`ciscoasa#show running-config regex regex urllist1 ".*\.([Ee][Xx][Ee]|[Cc][Oo][Mm]|[Bb][Aa][Tt]) HTTP/1.[01]" regex urllist2 ".*\.([Pp][Ii][Ff]|[Vv][Bb][Ss]|[Ww][Ss][Hh]) HTTP/1.[01]" regex urllist3 ".*\.([Dd][Oo][Cc]|[Xx][Ll][Ss]|[Pp][Pp][Tt]) HTTP/1.[01]" regex urllist4 ".*\.([Zz][Ii][Pp]|[Tt][Aa][Rr]|[Tt][Gg][Zz]) HTTP/1.[01]" regex domainlist1 "\.yahoo\.com" regex domainlist2 "\.myspace\.com" regex domainlist3 "\.youtube\.com" regex contenttype "Content-Type" regex applicationheader "application/.*" ciscoasa#`
- **show running-config class-map**：設定されたクラス マップの表示`ciscoasa#show running-config class-map ! class-map type regex match-any DomainBlockList match regex domainlist1 match regex domainlist2 match regex domainlist3 class-map type inspect http match-all BlockDomainsClass match request header host regex class DomainBlockList class-map type regex match-any URLBlockList match regex urllist1 match regex urllist2 match regex urllist3 match regex urllist4 class-map inspection_default match default-inspection-traffic class-map type inspect http match-all AppHeaderClass match response header regex contenttype regex applicationheader class-map httptraffic match access-list inside_mpc class-map type inspect http match-all BlockURLsClass match request uri regex class URLBlockList ! ciscoasa#`
- **show running-config policy-map type inspect http**：設定された HTTP トラフィックを検査するポリシー マップの表示`ciscoasa#show running-config policy-map type inspect http ! policy-map type inspect http http_inspection_policy parameters protocol-violation action drop-connection class AppHeaderClass drop-connection log match request method connect drop-connection log class BlockDomainsClass reset log class BlockURLsClass reset log ! ciscoasa#`
- **show running-config policy-map**：デフォルトの policy-map コンフィギュレーションおよびすべての policy-map コンフィギュレーションの表示`ciscoasa#show running-config policy-map ! policy-map type inspect dns preset_dns_map parameters message-length maximum 512 policy-map type inspect http http_inspection_policy parameters protocol-violation action drop-connection class AppHeaderClass drop-connection log match request method connect drop-connection log class BlockDomainsClass reset log class BlockURLsClass reset log policy-map global_policy class inspection_default inspect dns preset_dns_map inspect ftp 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 policy-map inside-policy class httptraffic inspect http http_inspection_policy ! ciscoasa#`
- **show running-config service-policy**：現在実行中のすべてのサービス ポリシー設定の表示`ciscoasa#show running-config service-policy service-policy global_policy global service-policy inside-policy interface inside`
- **show running-config access-list**：セキュリティ アプライアンスで実行されている access-list コンフィギュレーションの表示`ciscoasa#show running-config access-list access-list inside_mpc extended permit tcp any any eq www access-list inside_mpc extended permit tcp any any eq 8080 ciscoasa#`

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。

注: debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

- **デバッグ http** — HTTPトラフィックのためのデバッグ メッセージを表示します。

関連情報

- Cisco 適応型セキュリティ アプライアンスに関するサポート ページ（英語）

- Cisco Adaptive Security Device Manager (ASDM) に関するサポート ページ
- Cisco 500 シリーズ PIX に関するサポート ページ
- テクニカルサポートとドキュメント - Cisco Systems