

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

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[関連製品](#)

[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](#)

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 8.x 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 ブロックには、Ironport S シリーズなどの専用の機器または ASA の CSC モジュールなどのモジュールを使用する必要があります。

注: HTTPS フィルタリングは、ASA ではサポートされません。HTTPS ではパケットの内容が暗号化 (SSL) されるため、ASA はディープ パケット インスペクションまたは HTTPS トラフィックの正規表現に基づくインスペクションを実行できません。

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 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

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、ソフトウェア バージョン 8.0(x) 以降が稼働する Cisco 500 シリーズ PIX にも適用できます。

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

正規表現は、ストリングそのものとしてテキスト ストリングと文字どおりに照合することも、メタ文字を使用してテキスト ストリングの複数のバリエーションと照合することもできます。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: Ctrl キーを押した状態で V キーを押すと、CLI において、疑問符 (?) やタブなどの特殊文字をすべてエスケープできます。たとえば、`d[Ctrl+V]?g` と入力し、設定に `d?g` を入力します。

正規表現を作成するには、テキストの照合を必要とするさまざまな機能に使用できる `regex` コマンドを使用します。たとえば、インスペクション ポリシー マップを使用するモジュラ ポリシーフレームワークを使用すると、アプリケーション検査の特別なアクションを設定できます。詳細については、[policy map type inspect](#) コマンドを参照してください。インスペクション ポリシーマップでは、1 つ以上の `match` コマンドを含むインスペクション クラス マップを作成する場合、アクションの実行対象となるトラフィックを識別できます。または、`match` コマンドをインスペクション ポリシー マップ内で直接使用することもできます。一部の `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特定できるようにします。たとえば、HTTP パケット内の URL ストリングを照合できます。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
.	ドット	任意の単一の文字と照合されます。たとえば、 <code>d.g</code> は <code>dog</code> 、 <code>dag</code> 、 <code>dtg</code> 、 <code>doggonnit</code> 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。
(e x p)	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、 <code>d(ol)ag</code> は <code>dog</code> および <code>dag</code> に一致しますが、 <code>do ag</code> は <code>do</code> および <code>ag</code> 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、 <code>ab(xy){3}z</code> は、 <code>abxyxyxyz</code> 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、 <code>dog cat</code> は <code>dog</code> または <code>cat</code> 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、 <code>lo?se</code> は <code>lse</code> または <code>lose</code> 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、lose、loose などに一致しません。
{ 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。
[a b c]	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。
[^ a b c]	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 以外の文字と一致します。 [^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	行の先頭を指定します。
\	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。
c h a r	文字	文字がメタ文字でない場合は、リテラル文字と一致します。
\r	復帰	復帰 0x0d と一致します。
\n	改行	改行 0x0a と一致します。
\t	Tab	タブ 0x09 と一致します。
\f	改ページ	フォーム フィールド 0x0c と一致します。
\x N N	エスケープされた 16 進数	厳密に 2 桁の 16 進数を使用した ASCII 文字と一致します。
\	エスケープ	厳密に 3 桁の 8 進数としての ASCII 文字

N N N	プされた 8 進数	と一致します。たとえば、文字 040 はスペースを表します。
-------------	--------------	--------------------------------

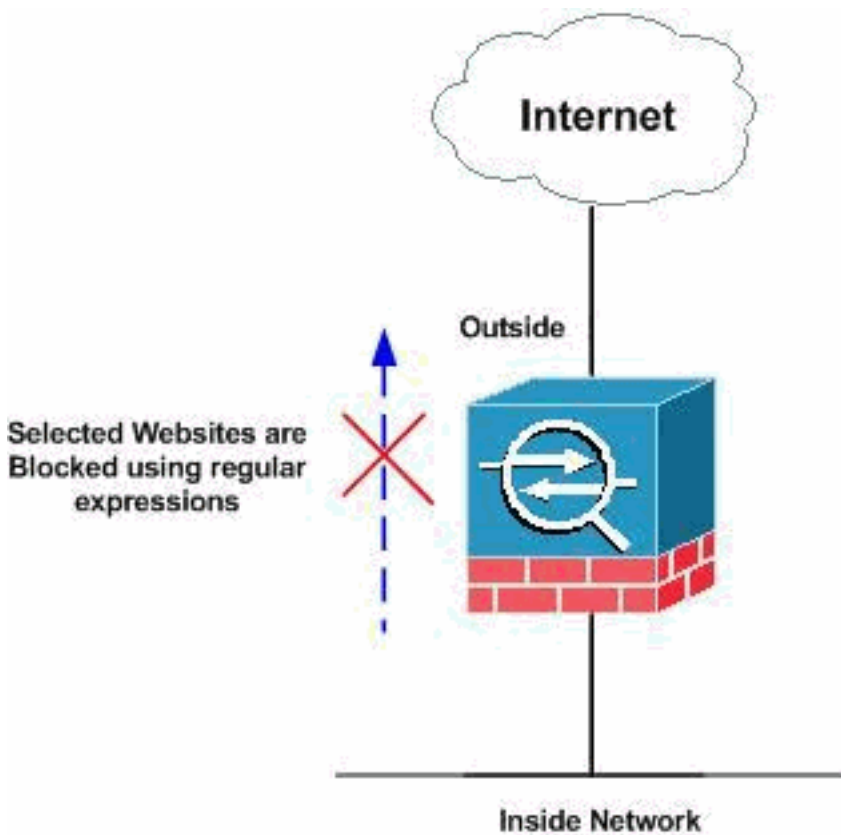
設定

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。



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 running-config : Saved : ASA Version
8.0(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 urlist1
".*\.[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
urlist2 ".*\.[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
urlist3 ".*\.[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 urlist4
".*\.[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

```

```

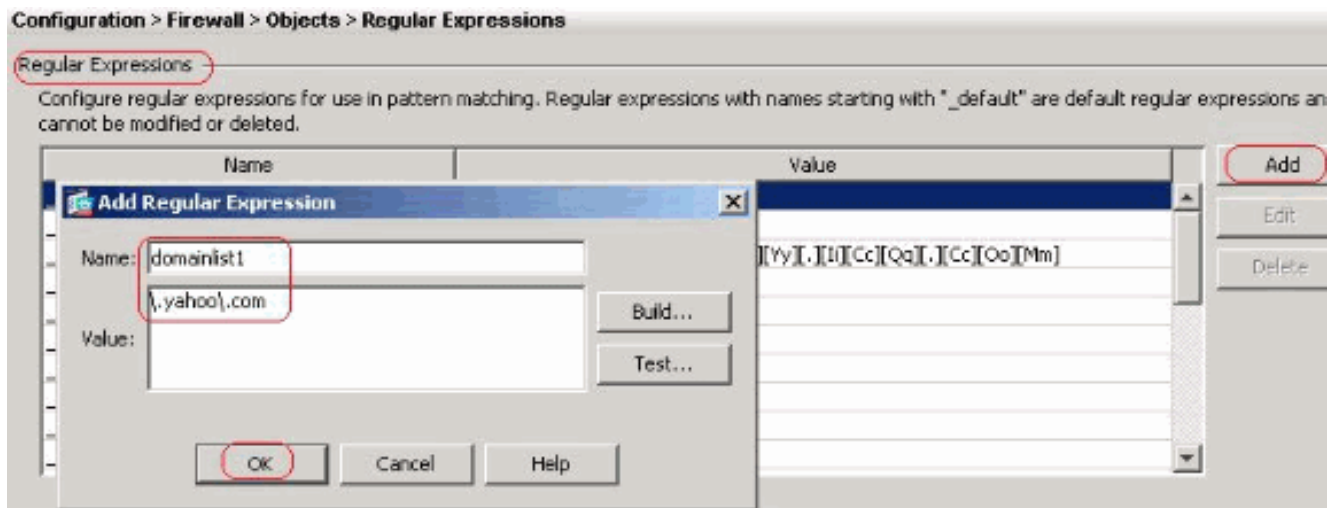
match-any URLBlockList match regex urllist1 match regex
urllist2 match regex urllist3 match regex urllist4 !---
Class map created in order to match the URLs !--- to be
blocked class-map inspection_default match default-
inspection-traffic class-map type inspect http match-all
AppHeaderClass match response 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 are blocked. prompt hostname
context Cryptochecksum:e629251a7c37af205c289cf78629fc11
: end ciscoasa#

```

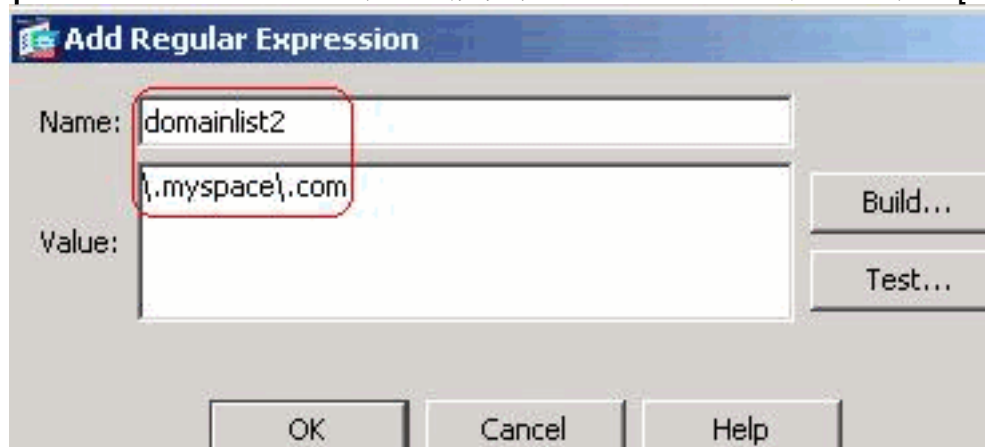
[ASDM 6.x を使用した ASA コンフィギュレーション 8.x](#)

正規表現を設定し、次に示すように、特定の Web サイトをブロックするために MPF に適用するには、次の手順を実行します。

1. **正規表現の作成**[Configuration] > [Firewall] > [Objects] > [Regular Expressions] の順に選択し、[Regular Expression] タブの下にある [Add] をクリックし、次のように正規表現を作成します。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。

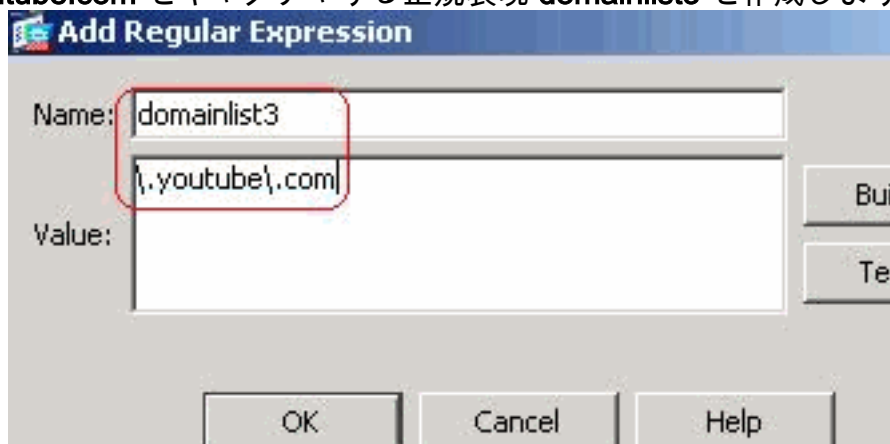


ドメイン名 **myspace.com** をキャプチャする正規表現 **domainlist2** を作成します。[OK] をク

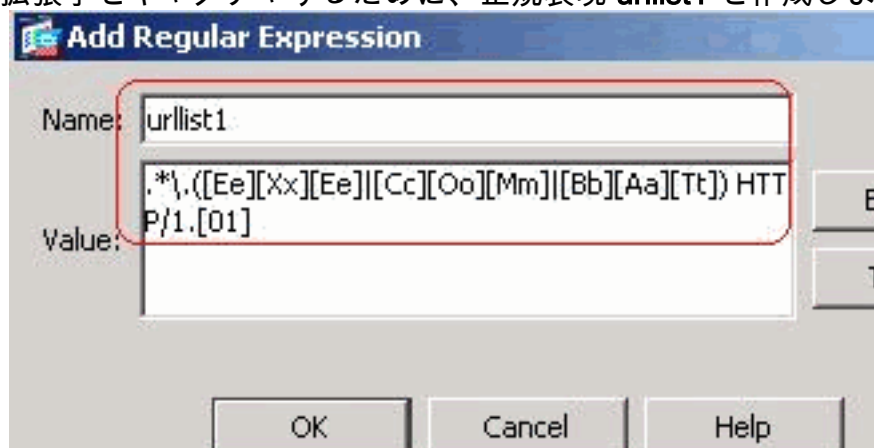


リックします。ドメイン

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 ブラウザで使用されている http のバージョンが 1.0 または 1.1 のどちらかである場合は、**exe**、**com** および **bat** などのファイル拡張子をキャプチャするために、正規表現 **urllist1** を作成します。[OK]



をクリックします。Web ブラ

ウザで使用されている http のバージョンが 1.0 または 1.1 のどちらかである場合は、**pif**、**vbs** および **wsh** などのファイル拡張子をキャプチャするために、正規表現 **urllist2** を作成します。[OK] をクリックします。

The screenshot shows the 'Add Regular Expression' dialog box. The 'Name' field contains 'urllist2'. The 'Value' field contains the regular expression: `.*\.([Pp][Ii][Ff] | [Vv][Bb][Ss] | [Ww][Ss][Hh]) HTTP / 1.[01]`. The dialog has buttons for 'Build..', 'Test..', 'OK', 'Cancel', and 'Help'.

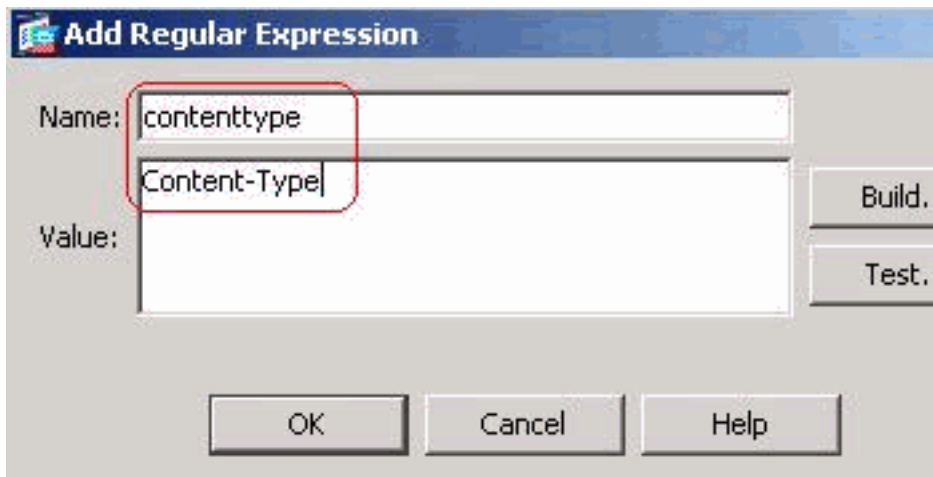
Web ブラウザで使用されている http のバージョンが 1.0 または 1.1 のどちらかである場合は、**doc**、**xls** および **ppt** などのファイル拡張子をキャプチャするために、正規表現 **urllist3** を作成します。[OK] をクリ

The screenshot shows the 'Add Regular Expression' dialog box. The 'Name' field contains 'urllist3'. The 'Value' field contains the regular expression: `.*\.([Dd][Oo][Cc] | [Xx][Ll][Ss] | [Pp][Pp][Tt]) HTTP / 1.[01]`. The dialog has buttons for 'Build..', 'Test..', 'OK', 'Cancel', and 'Help'.

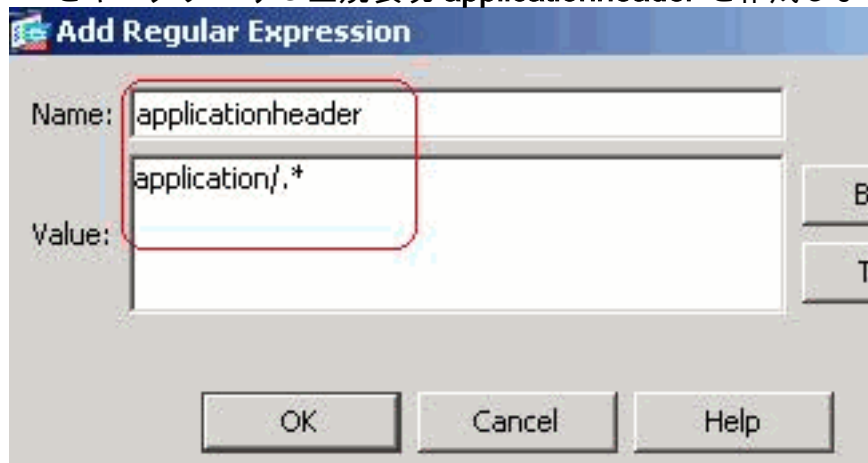
ックします。Web ブラウザで使用されている http のバージョンが 1.0 または 1.1 のどちらかである場合は、**zip**、**tar** および **tgz** などのファイル拡張子をキャプチャするために、正規表現 **urllist4** を作成します。

The screenshot shows the 'Add Regular Expression' dialog box. The 'Name' field contains 'urllist4'. The 'Value' field contains the regular expression: `.*\.([Zz][Ii][Pp] | [Tt][Aa][Rr] | [Tt][Gg][Zz]) HTTP / 1.[01]`. The dialog has buttons for 'OK', 'Cancel', and 'Help'.

[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



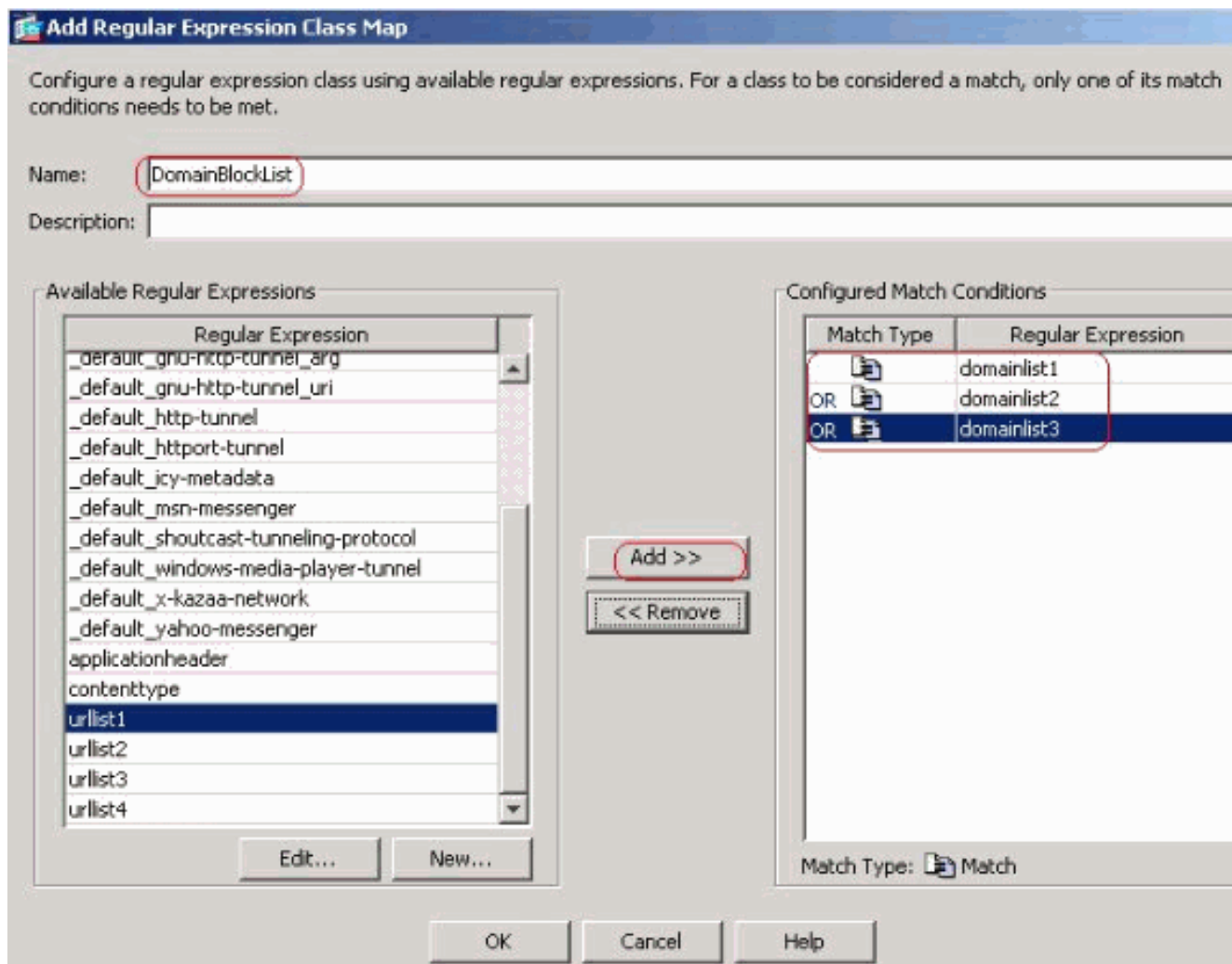
。さまざまなアプリケーションヘッダーをキャプチャする正規表現 `applicationheader` を作成します。[OK] をクリ



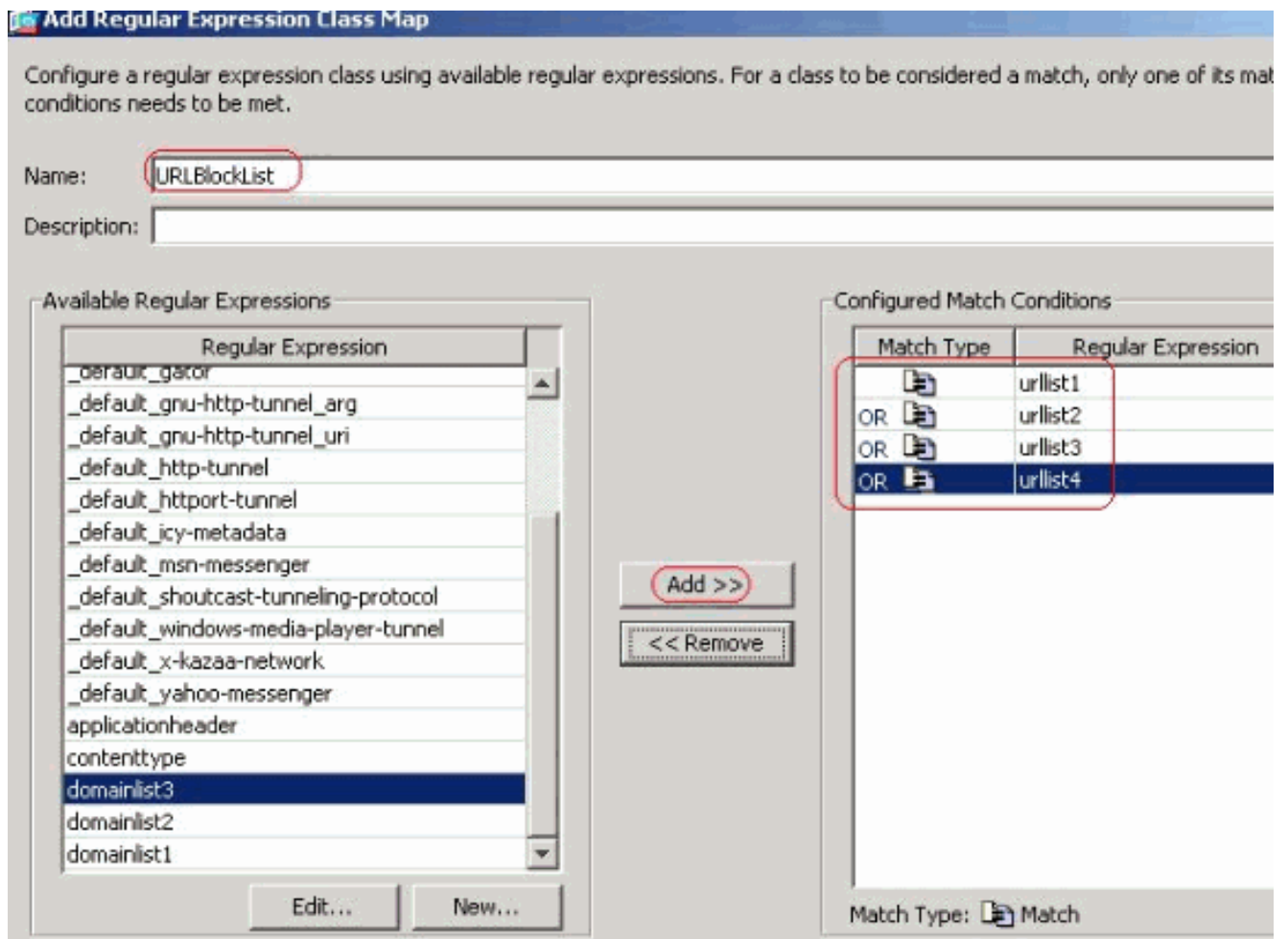
ックします。

同等の CLI 設定

2. 正規表現クラスの作成[Configuration] > [Firewall] > [Objects] > [Regular Expressions] の順に選択し、[Regular Expression Classes] タブの下にある [Add] をクリックし、次のようにさまざまなクラスを作成します。正規表現 `domainlist1`、`domainlist2` と `domainlist3` のいずれかに一致させるため、正規表現クラス `DomainBlockList` を作成します。[OK] をクリックします。

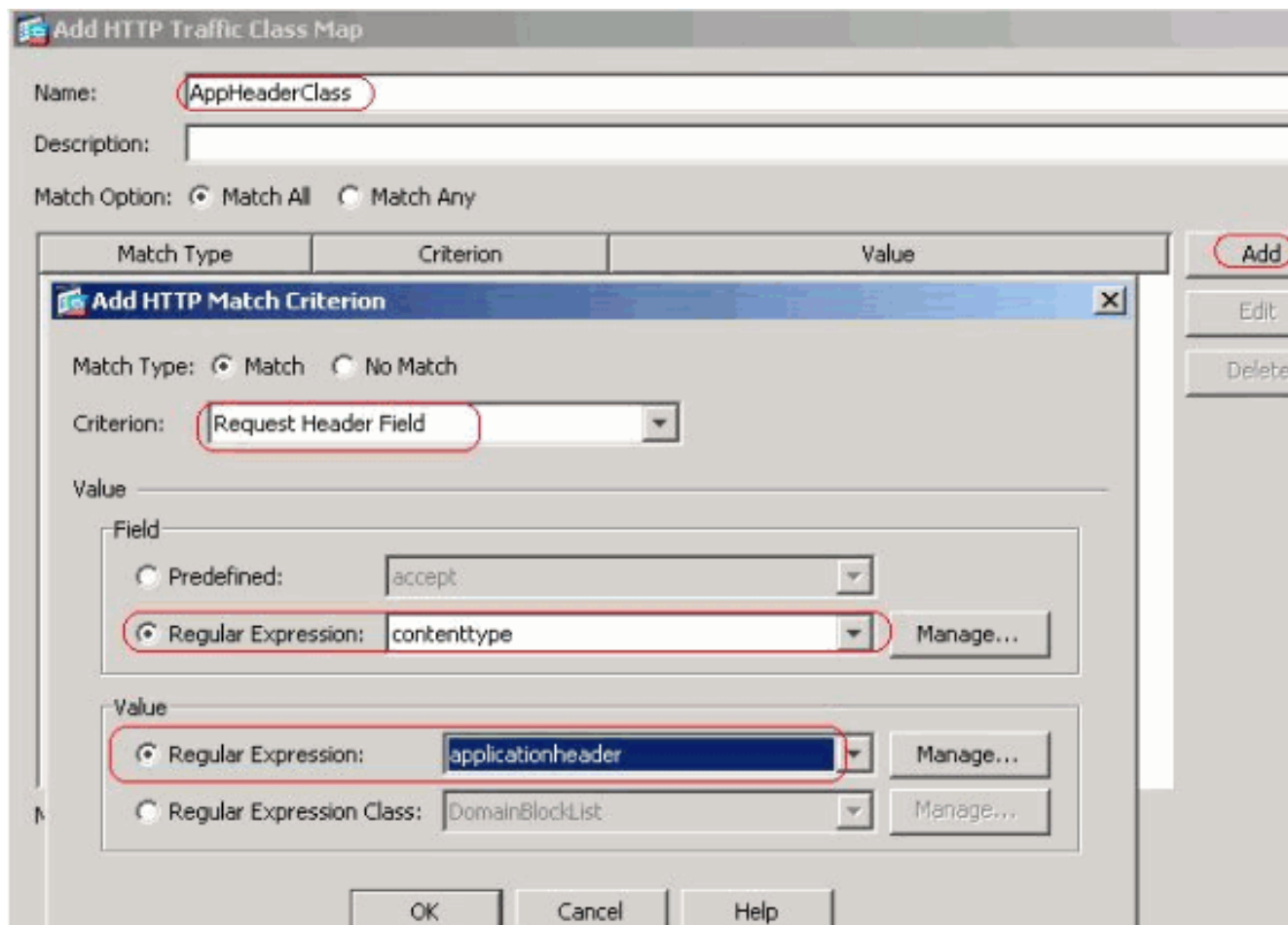


正規表現 urllist1、urllist2、urllist3 と urllist4 のいずれかに一致させるため、正規表現クラス URLBlockList を作成します。[OK] をクリックします。

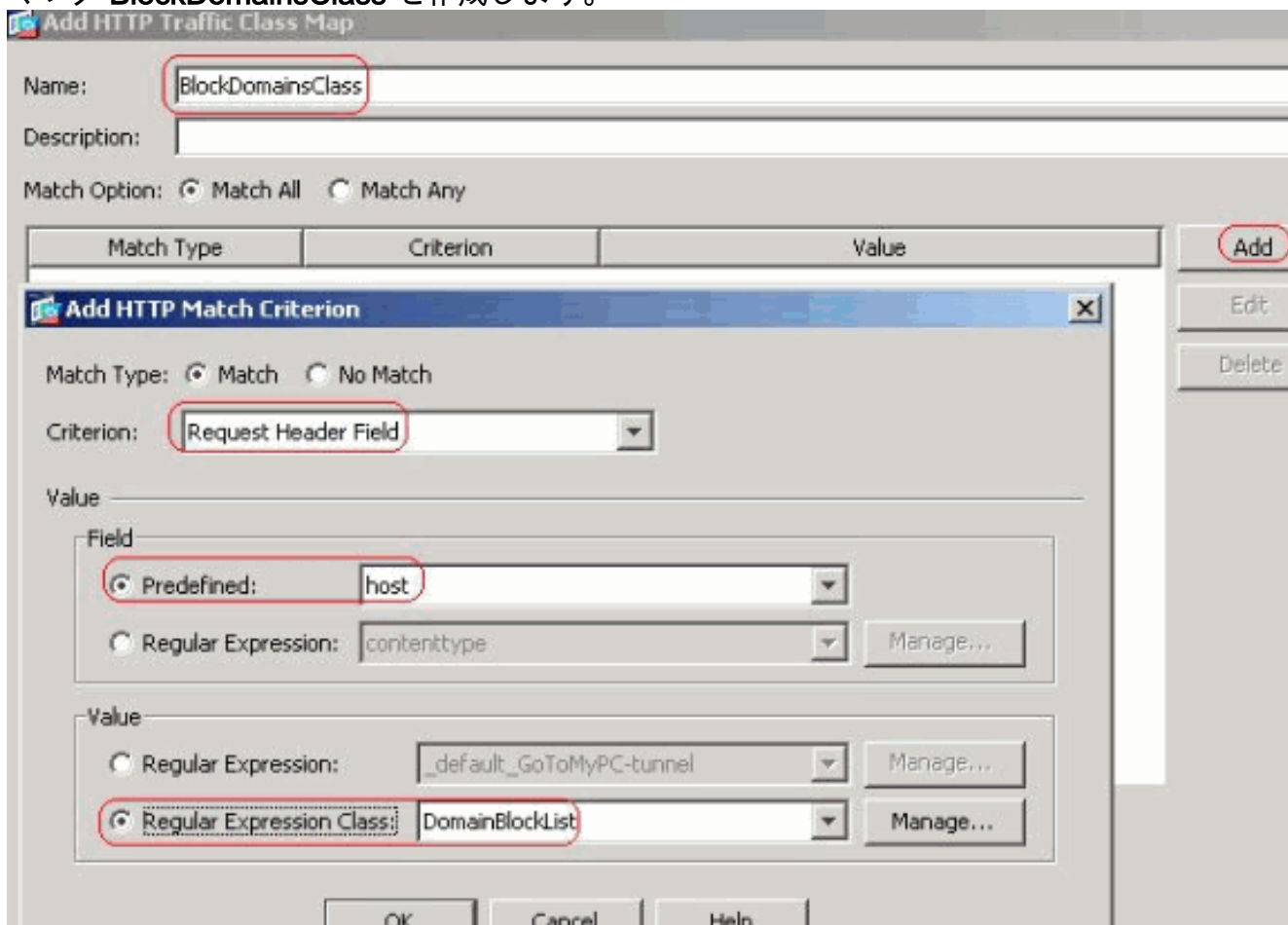


同等の CLI 設定

3. クラス マップによる特定されたトラフィックの検査[Configuration] > [Firewall] > [Objects] > [Class Maps] > [HTTP] > [Add] の順に選択し、さまざまな正規表現で特定された http トラフィックを検査するクラス マップを次のように作成します。正規表現のキャプチャの応答ヘッダーと一致するように、クラス マップ AppHeaderClass を作成します。



[OK] をクリックします。正規表現のキャプチャの要求ヘッダーと一致するように、クラスマップ `BlockDomainsClass` を作成します。



[OK] をクリックします。正規表現のキャプチャの要求 uri と一致するように、クラスマップ

BlockURLsClass を作成します。

The screenshot shows the 'Add HTTP Traffic Class Map' configuration window. The 'Name' field is set to 'BlockURLsClass'. The 'Match Option' is set to 'Match All'. A table with columns 'Match Type', 'Criterion', and 'Value' is shown. An 'Add HTTP Match Criterion' dialog is open, showing 'Match Type' as 'Match', 'Criterion' as 'Request URI', and 'Regular Expression Class' as 'URLBlockList'.

Match Type	Criterion	Value
------------	-----------	-------

Match Type: Match No Match

Criterion: Request URI

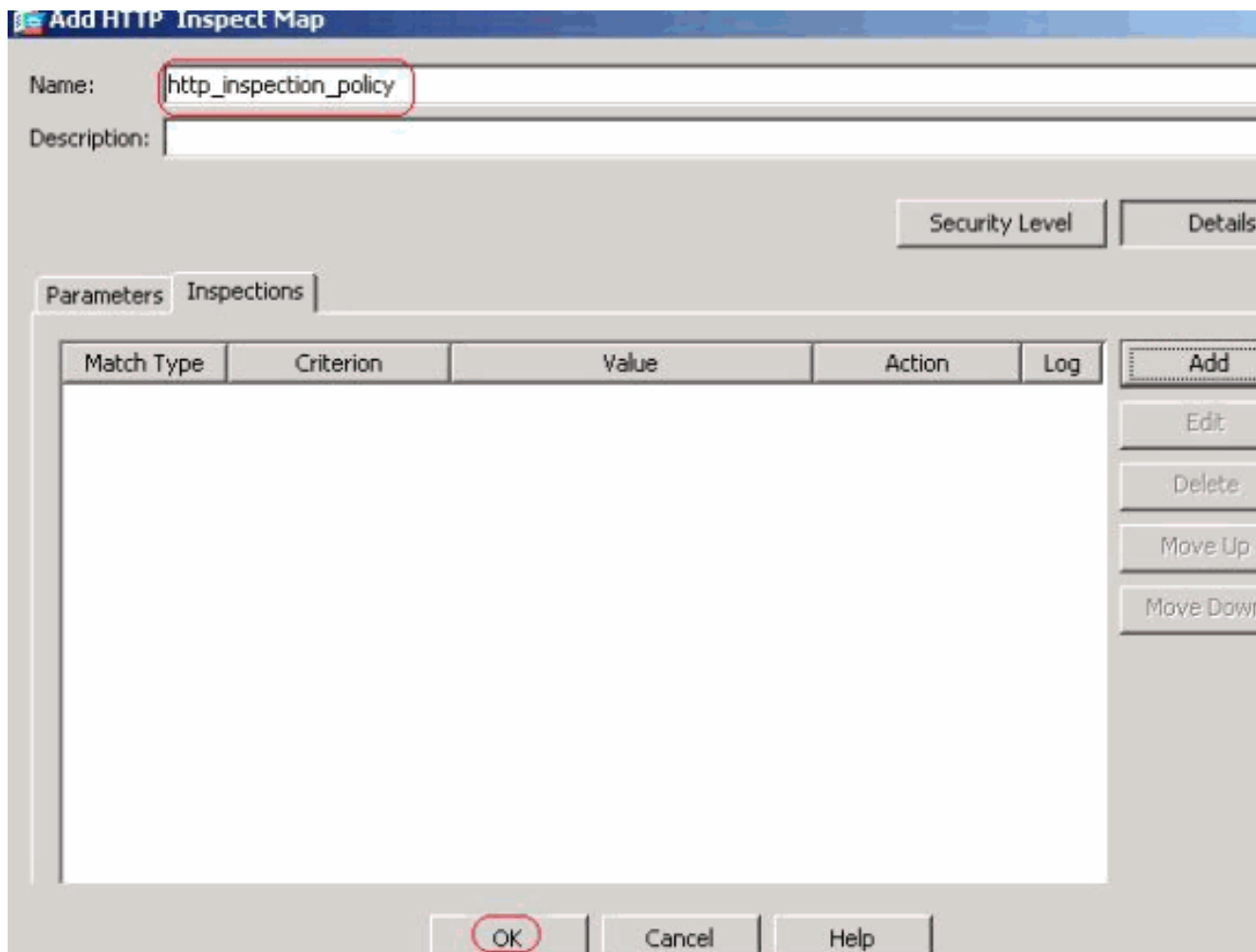
Value

Regular Expression: Manage...

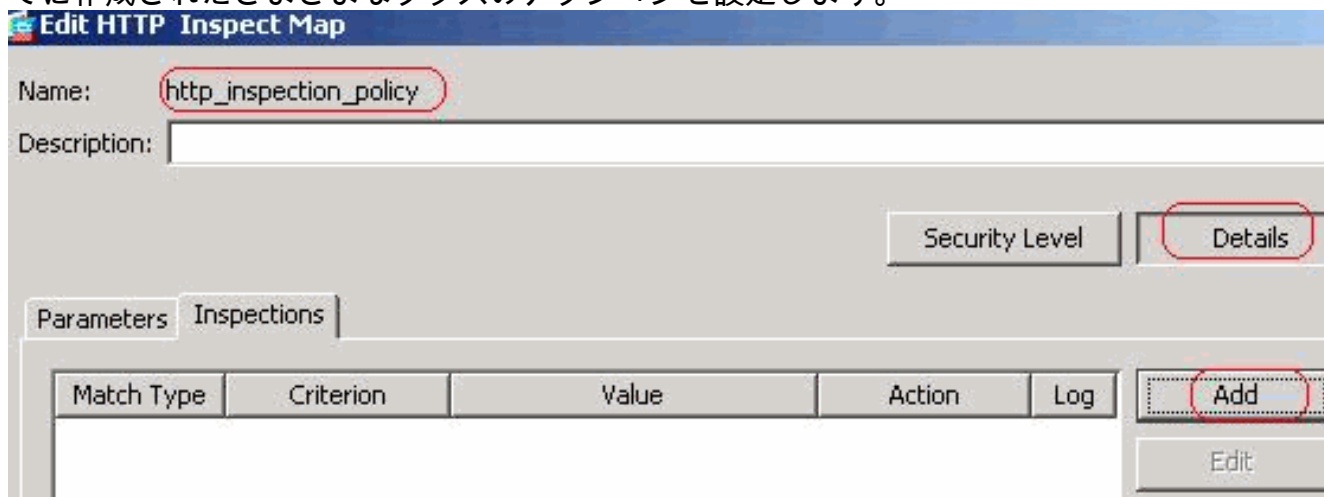
Regular Expression Class: URLBlockList Manage...

[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[Configuration] > [Firewall] > [Objects] > [Inspect Maps] > [HTTP] の順に選択し、一致するトラフィックに対するアクションを設定する http_inspection_policy を作成します。 [OK] をクリックします。



[Configuration] > [Firewall] > [Objects] > [Inspect Maps] > [HTTP] > [http_inspection_policy] (ダブルクリック) を選択し、[Details] > [Add] をクリックし、今までに作成されたさまざまなクラスのアクションを設定します。



アクションを [Drop Connection]、ログ記録を [Enable]、[Criterion] を [Request Method]、[Value] を [connect] に設定します。

Add HTTP Inspect

Match Criteria

Single Match

Match Type: Match No Match

Criterion:

Value

Method:

Regular Expression

Regular Expression:

Regular Expression Class:

Multiple matches

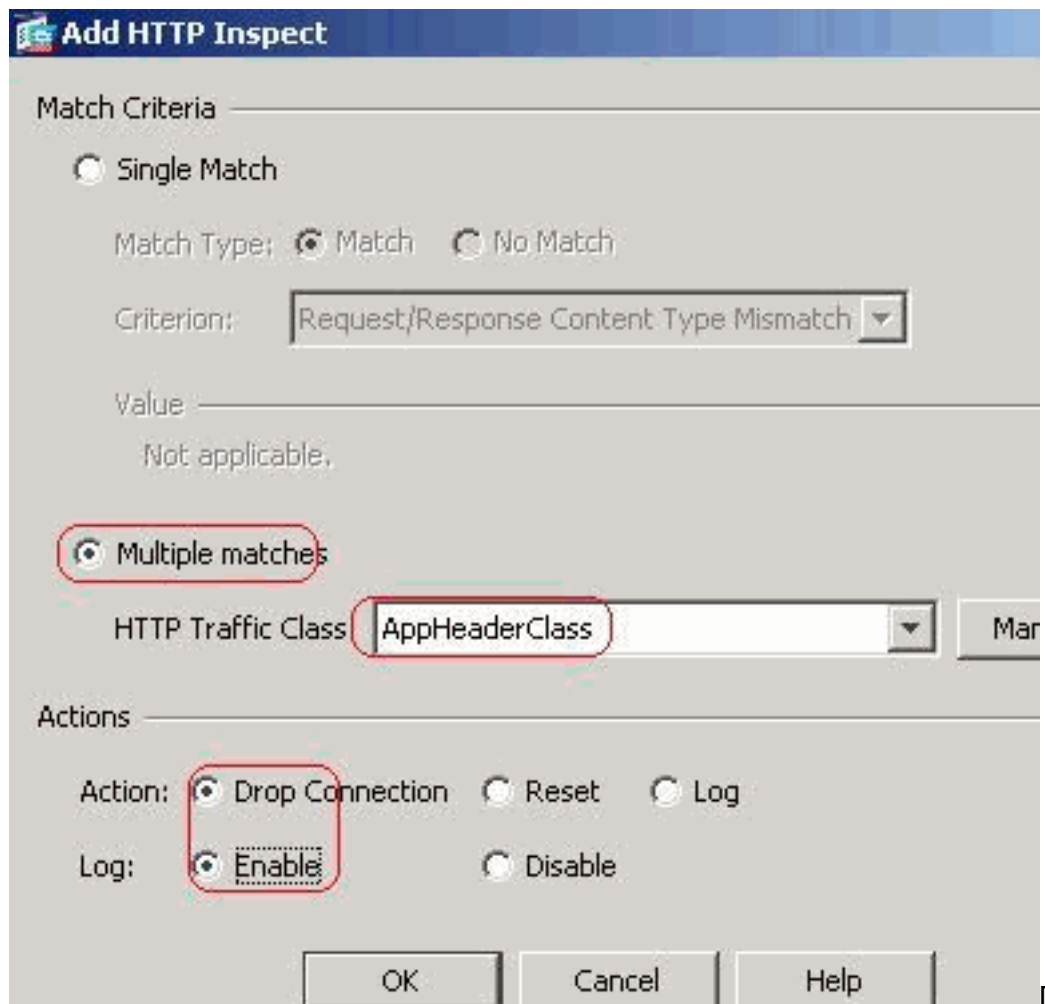
HTTP Traffic Class:

Actions

Action: Drop Connection Reset Log

Log: Enable Disable

[OK] をクリック
します。アクションを [Drop Connection]、クラス **AppHeaderClass** のログ記録を [Enable]



に設定します。

をクリックします。アクションを [Reset]、クラス **BlockDomainsClass** のログ記録を [Enable] に設定します。

[OK]

Add HTTP Inspect

Match Criteria

Single Match

Match Type: Match No Match

Criterion: Request/Response Content Type Mismatch

Value

Not applicable.

Multiple matches

HTTP Traffic Class: BlockDomainsClass

Actions

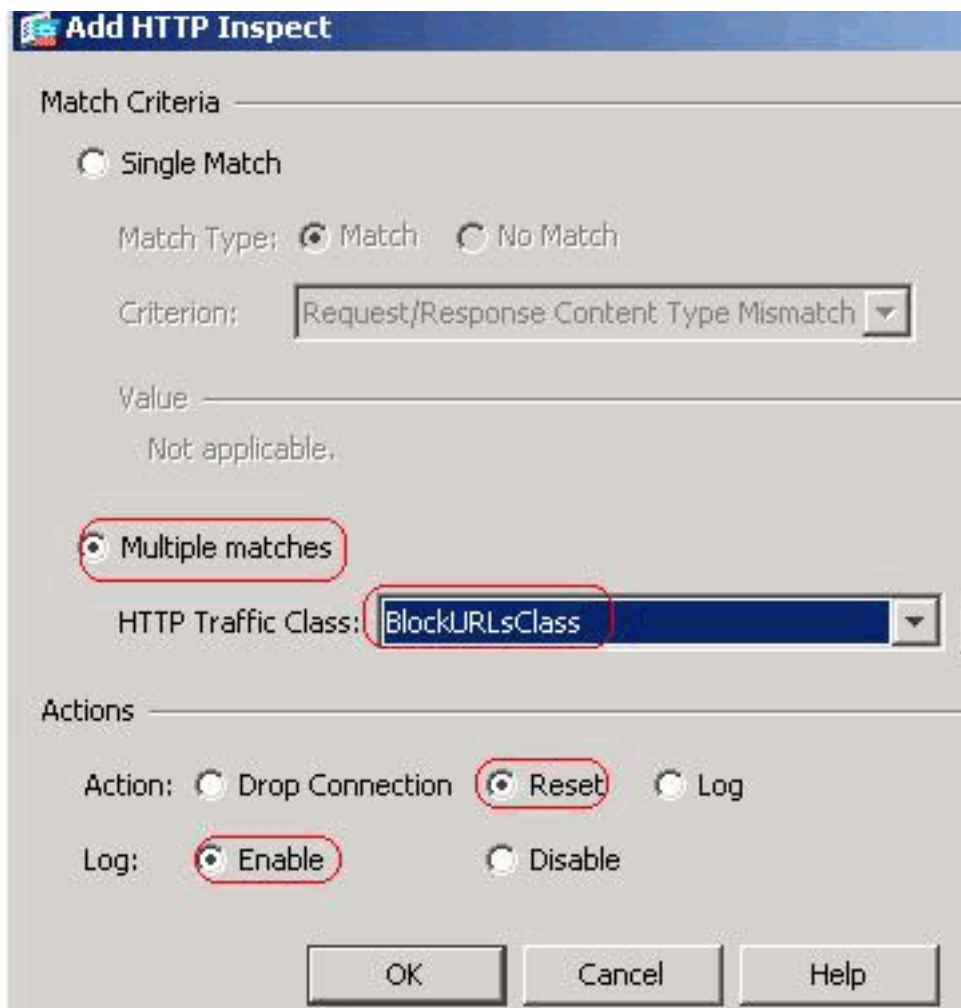
Action: Drop Connection Reset Log

Log: Enable Disable

OK Cancel Help

[OK] をクリックします。

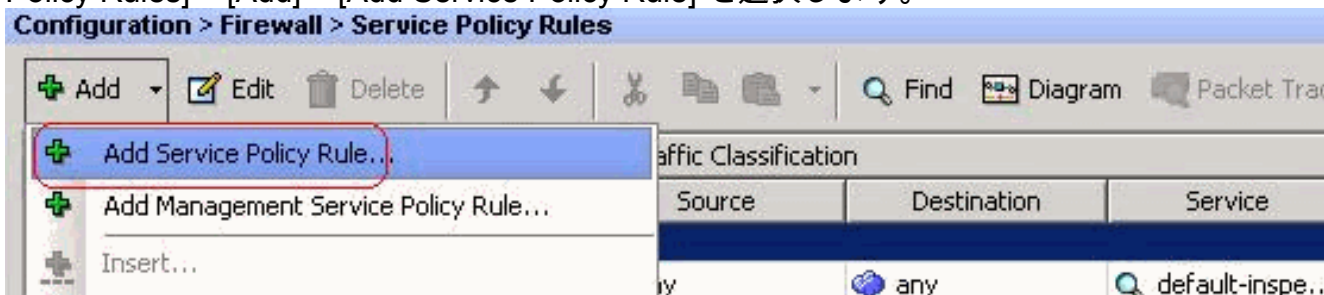
アクションを [Reset]、クラス BlockURLsClass のログ記録を [Enable] に設定します。



[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 [Configuration] > [Firewall] > [Service Policy Rules] > [Add] > [Add Service Policy Rule] を選択します。



HTTP トラフィックドロップダウンメニューの内部インターフェイスと [Interface] オプションボタンを選択し、[Policy Name] として **inside-policy** を選択します。 [Next] をクリックします。

Add Service Policy Rule Wizard - Service Policy

Adding a new service policy rule requires three steps:

Step 1: Configure a service policy.

Step 2: Configure the traffic classification criteria for the service policy rule.

Step 3: Configure actions on the traffic classified by the service policy rule.

Create a Service Policy and Apply To: _____

Only one service policy can be configured per interface or at global level. If a service policy already exists, the new rule into the existing service policy. Otherwise, you can create a new service policy.

Interface: ▼

Policy Name:

Description:

Global - applies to all interfaces

Policy Name:

Description:

≤ Back

Next >

httptraffic のクラス マップを作成し、[Source and Destination IP Address (uses ACL)] にチェックを付けます。[Next] をクリックします。

Add Service Policy Rule Wizard - Traffic Classification Criteria

Create a new traffic class:

Description (optional):

Traffic Match Criteria

Default Inspection Traffic

Source and Destination IP Address (uses ACL)

Tunnel Group

TCP or UDP Destination Port

RTP Range

IP DiffServ CodePoints (DSCP)

IP Precedence

Any traffic

Use an existing traffic class:

Use class-default as the traffic class.

If traffic does not match a existing traffic class, then it will match the class-default traffic class. Class-default all situation.

[Source] および [Destination] として [any]、サービスとして tcp-udp/http を選択します。
[Next] をクリックします。

Add Service Policy Rule Wizard - Traffic Match - Source and Destination Address

Action: Match Do not match

Source: any

Destination: any

Service: tcp-udp/http

Description:

More Options

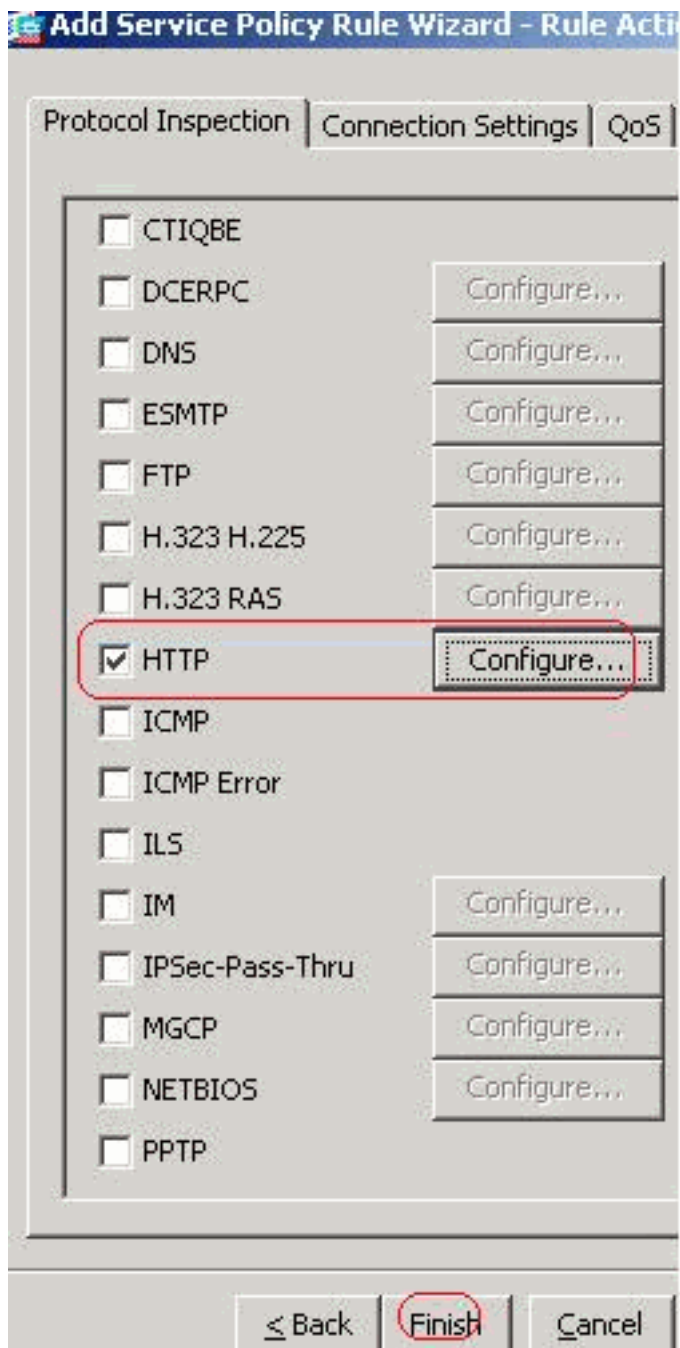
Enable Rule

Source Service: (TCP or UDP service only)

Time Range:

≤ Back **Next >**

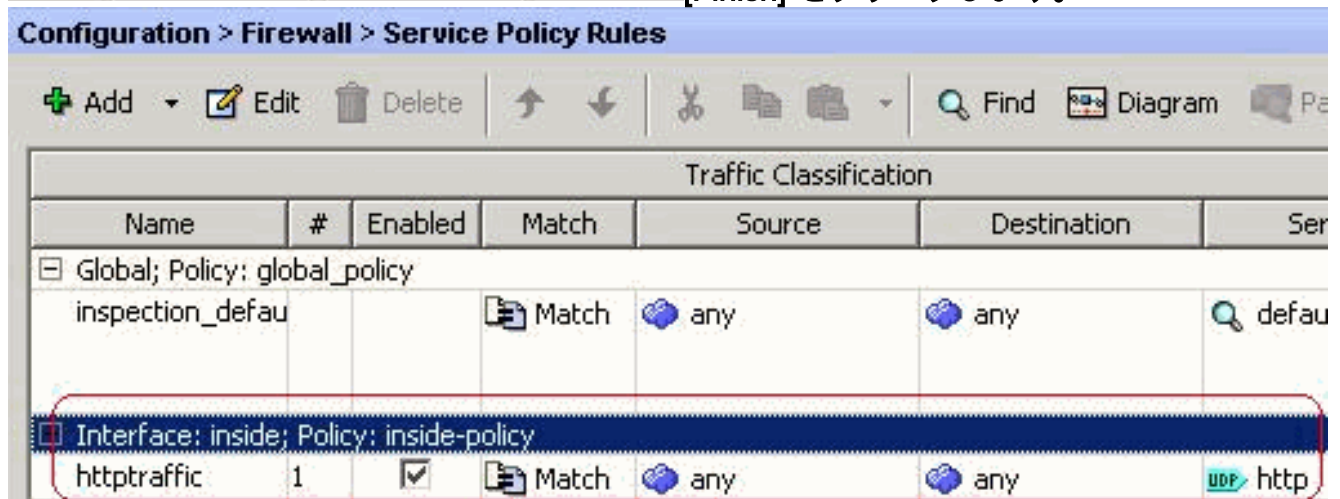
[HTTP] オプション ボタンをチェックし、[Configure] をクリックします。



オプション ボタン [Select a HTTP inspect map for the control over inspection] を図のように選択します。[OK] をクリックします。



[Finish] をクリックします。



ポート 8080 のトラフィック再び、[Add] > [Add Service Policy Rule] を選択します。

Configuration > Firewall > Service Policy Rules

Traffic Classification						
Source	Destination	Service	Action	Match	Priority	Next
any	any	default				
httptraffic	1	<input checked="" type="checkbox"/>	Match	any	any	UDP http

Interface: inside; Policy: inside-policy

[Next] をクリックします。

Add Service Policy Rule Wizard - Service Policy

Adding a new service policy rule requires three steps:

- Step 1: Configure a service policy.
- Step 2: Configure the traffic classification criteria for the service policy rule.
- Step 3: Configure actions on the traffic classified by the service policy rule.

Create a Service Policy and Apply To: _____

Only one service policy can be configured per interface or at global level. If a service policy already exists, then you can add the new rule into the existing service policy. Otherwise, you can create a new service policy.

Interface:

Policy Name: *

Description:

Global - applies to all interfaces

Policy Name:

Description:

*Only one service policy is allowed. Existing service policy names cannot be changed.

オプション ボタン [Add rule to existing traffic class] を選択し、ドロップダウン メニューから httptraffic を選択します。 [Next] をクリックします。

Add Service Policy Rule Wizard - Traffic Classification Criteria

Create a new traffic class:

Description (optional):

Traffic Match Criteria

- Default Inspection Traffic
- Source and Destination IP Address (uses ACL)
- Tunnel Group
- TCP or UDP Destination Port
- RTP Range
- IP DiffServ CodePoints (DSCP)
- IP Precedence
- Any traffic

Add rule to existing traffic class:

Rule can be added to an existing class map if that class map uses access control list (ACL) as its traffic match

Use an existing traffic class:

Use class-default as the traffic class.

If traffic does not match a existing traffic class, then it will match the class-default traffic class. Class-default all situation.

[Source] および [Destination] として [any]、tcp/8080 を選択します。 [Next] をクリックします。

Add Service Policy Rule Wizard - Traffic Match - Source and Destination Address

Action: Match Do not match

Source: ...

Destination: ...

Service: ...

Description:

More Options


Enable Rule

Source Service: ... (TCP or UDP service only)

Time Range: ...

[Finish] をクリックします。

Add Service Policy Rule Wizard - Rule Actions

 The Rule Actions are applied to all the rules grouped in the Traffic Match.

Protocol Inspection | Connection Settings | QoS

- CTIQBE
- DCERPC Configure...
- DNS Configure...
- ESMTTP Configure...
- FTP Configure...
- H.323 H.225 Configure...
- H.323 RAS Configure...
- HTTP Configure... HTTP Inspect Map: http_inspection_policy
- ICMP
- ICMP Error
- ILS
- IM Configure...
- IPsec-Pass-Thru Configure...
- MGCP Configure...
- NETBIOS Configure...

< Back | **Finish** | Cancel

Configuration > Firewall > Service Policy Rules

+ Add | Edit | Delete | ↑ ↓ | ✂ | Find | Diagram | Pac

Traffic Classification						
Name	#	Enabled	Match	Source	Destination	Serv
[-] Global; Policy: global_policy						
inspection_defau			Match	any	any	default
[-] Interface: inside; Policy: inside-policy						
httptraffic	1	<input checked="" type="checkbox"/>	Match	any	any	UDP http
	2	<input checked="" type="checkbox"/>	Match	any	any	TCP 8080

[Apply] をクリックします。同等の CLI 設定

確認

このセクションでは、設定が正常に機能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。

- **debug http** : HTTP トラフィックのデバッグ メッセージの表示

[関連情報](#)

- [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 \(ASDM \) に関するサポート](#)

- [Cisco PIX 500 シリーズ セキュリティ アプライアンスに関するサポート ページ](#)
- [Cisco PIX Firewall ソフトウェア](#)
- [Cisco Secure PIX ファイアウォール コマンド リファレンス](#)
- [セキュリティ製品に関する Field Notice \(PIX を含む \)](#)
- [Requests for Comments \(RFC \)](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)