ASA/PIX 8.x:MPF 구성과 함께 정규식을 사용하여 FTP 사이트 허용/차단 예

목차

소개

이 문서에서는 서버 이름별로 특정 FTP 사이트를 차단하거나 허용하기 위해 MPF(Modular Policy Framework)와 함께 정규식을 사용하는 Cisco Security Appliances ASA/PIX 8.x를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에서는 Cisco Security Appliance가 구성되어 제대로 작동한다고 가정합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 소프트웨어 버전 8.0(x) 이상을 실행하는 Cisco 5500 Series ASA(Adaptive Security Appliance)
- ASA 8.x용 Cisco ASDM(Adaptive Security Device Manager) 버전 6.x

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

배경 정보

모듈식 정책 프레임워크 개요

MPF는 보안 어플라이언스 기능을 구성할 수 있는 일관되고 유연한 방법을 제공합니다.예를 들어, 모든 TCP 애플리케이션에 적용되는 것과 달리 MPF를 사용하여 특정 TCP 애플리케이션에 특정한 시간 제한 컨피그레이션을 생성할 수 있습니다.

MPF는 다음 기능을 지원합니다.

- TCP 정규화, TCP 및 UDP 연결 제한 및 시간 제한, TCP 시퀀스 번호 임의 설정
- CSC
- 애플리케이션 검사
- IPS
- QoS 입력 폴리싱
- QoS 출력 폴리싱
- QoS 우선순위 큐

MPF 컨피그레이션은 다음 네 가지 작업으로 구성됩니다.

1. 작업을 적용할 레이어 3 및 레이어 4 트래픽을 식별합니다.자세한 내용은 레이어 3/4 클래스 맵을 사용하여 트래픽 식별을 참조하십시오.
2. (애플리케이션 검사만 해당) 애플리케이션 검사 트래픽에 대한 특별 작업을 정의합니다.자세한 내용은 애플리케이션 검사를 위한 특별 작업 구성을 참조하십시오.
3. 레이어 3 및 레이어 4 트래픽에 작업을 적용합니다.자세한 내용은 레이어 3/4 정책 맵을 사용하여 작업 정의를 참조하십시오.
4. 인터페이스에서 작업을 활성화합니다.자세한 내용은 서비스 정책을 사용하여 인터페이스에 레이어 3/4 정책 적용을 참조하십시오.

정규식

정규식은 문자 그대로 정확한 문자열이나 메타 문자를 사용하여 텍스트 문자열을 일치하므로 텍스트 문자열의 여러 변형을 일치시킬 수 있습니다.특정 애플리케이션 트래픽의 내용을 매칭하려면 정규식을 사용할 수 있습니다.예를 들어, HTTP 패킷 내에서 URL 문자열을 매칭할 수 있습니다.

참고: Ctrl+V를 사용하여 물음표(?) 또는 탭과 같은 CLI의 모든 특수 문자를 이스케이프합니다.예를 들어 **d[Ctrl+V]g를** 입력하여 컨피그레이션**에 d?g**를 입력합니다.

정규식을 만들려면 regex 명령을 **사용합니다**.또한 **regex** 명령은 텍스트 일치를 필요로 하는 다양한 기능에 사용할 수 있습니다.예를 들어 검사 정책 맵을 사용하는 MPF를 사용하여 애플리케이션 검사에 대한 특수 작업을 구성할 수 있습니다.자세한 내용은 **policy-map type inspect** 명령을 참조하십시오.

검사 정책 맵에서 하나 이상의 **match** 명령이 포함된 검사 클래스 맵을 만들거나 검사 정책 맵에서 직접 **match** 명령을 사용할 수 있는 경우 수행할 트래픽을 식별할 수 있습니다.일부 **match** 명령을 사용하면 정규식을 사용하여 패킷의 텍스트를 식별할 수 있습니다.예를 들어, HTTP 패킷 내에서 URL 문자열을 매칭할 수 있습니다.정규식 클래스 맵에서 정규식을 그룹화할 수 있습니다.자세한 내용은 class-map type regex 명령을 참조하십시오.

이 표에는 특별한 의미가 있는 메타 문자가 나열되어 있습니다.

문자	설명	참고
.	점	단일 문자와 일치합니다 .예를 들어 **d.g는** dog, dag, dtg 및 이러한 문자가 포함된 단어(예: doggonnit)와 일치합니다.
(exp)	하위 식	하위 식은 문자를 주변 문자와 분리하므로 하위 식에서 다른 메타 문자를 사용할 수 있습니다.예를 들어 **d(o|a)g는** dog 및 dag와 일치하지만 **do|ag**는 do 및 ag와 일치합니다.하위 식을 반복 한정자와 함께 사용하여 반복에 사용되는 문자를 구분할 수도 있습니다.예를 들어 **ab(xy){3}z는 abxyxyxyz**와 일치합니다.
|	대체	분리되는 식 중 하나와 일치합니다.예를 들어 **dog|cat은** dog 또는 cat과 일치합니다.
?	물음표	이전 식의 0 또는 1이 있음을 나타내는 한정자입니다.예를 들어 lo?**se는 lse 또는 lose**와 일치합니다. **참고:** Ctrl+V를 입력한 다음 물음표를 입력하거나 도움말 기능을 호출해야 합니다.
*	별표	이전 식이 0, 1 또는 임의의 숫자임을 나타내는 한정자입니다.예를 들어 **lo*se는 lse**, lose, loose 등과 일치합니다.
{x}	반복 한정자	정확히 x번 반복합니다 .예를 들어 **ab(xy){3}z는 abxyxyxyz**와 일치합니다.
{x,}	최소 반복 한정	최소 x번 반복합니다.예를 들어 **ab(xy){2,}z는 abxyxyz**, abxyxyxyz 등과

	자	일치합니다.
[abc]	문자 클래스	대괄호의 모든 문자와 일치합니다.예를 들어 **[abc]는** a, b 또는 c와 일치합니다.
[^abc]	부정 문자 클래스	대괄호 안에 포함되지 않은 단일 문자와 일치합니다.예를 들어 **[^abc]는** a, b 또는 c 이외의 문자와 일치합니다.**[^A-Z]**는 대문자가 아닌 단일 문자와 일치합니다.
[a-c]	문자 범위 클래스	범위의 모든 문자와 일치합니다.**[a-z]는** 소문자와 일치합니다.문자 및 범위를 혼합할 수 있습니다 .**[abcq-z]**는 a, b, c, q, r, s, t, u, v, w, x, y, z 등과 **[a-cq-z]** 일치합니다.대시(-) 문자는 대괄호 안의 마지막 또는 첫 번째 문자인 경우에만 리터럴입니다 .**[abc-]** 또는 **[-abc]**.
""	따옴표	문자열의 후행 또는 선행 공백을 유지합니다.예를 들어 " **test**"는 일치 항목을 찾을 때 선행 공백을 유지합니다.
^	캐럿	줄의 시작을 지정합니다.
\ \ \ \ \ \ \ \\ \ \\ \ \\ \\ \\\ \ \\\ \\\ \\ \\\ \\\\ \\\ \\\\ \\ \\\ \\\\\ \\\\\\ \\\\\ \\\\ \\\ \\\\ \\\ \\\\ \\\\\ \\\ \\ \\ \\ \\ \\\ \\ \\ \\ \\\\\\ \\\\\\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\\ \\ \\\\\\\ \\ \\ \\ \\ \\ \\\\ \	이스케이프 문자	메타 문자와 함께 사용하면 리터럴 문자와 일치합니다.예를 들어, **\[**왼쪽 대괄호와 일치합니다.
문자	문자	문자가 메타 문자가 아닌 경우 는 리터럴 문자와 일치합니다.
\r	캐리지 리턴	캐리지 리턴과 일치:0x0d
\n	새 줄	새 줄 일치:0x0a
\t	탭	탭을 확인합니다.0x09
\f	서식	양식 피드와 일치시킵니다.0x0c입니다.
\xNN	이스	정확히 두 자릿수의 16진

	케이프된 16진수 숫자	수를 사용하는 ASCII 문자와 일치합니다.
\NNN	이스케이프된 8진수 번호	정확히 3자리의 8진수로 ASCII 문자와 일치합니다 .예를 들어 문자 040은 공백을 나타냅니다.

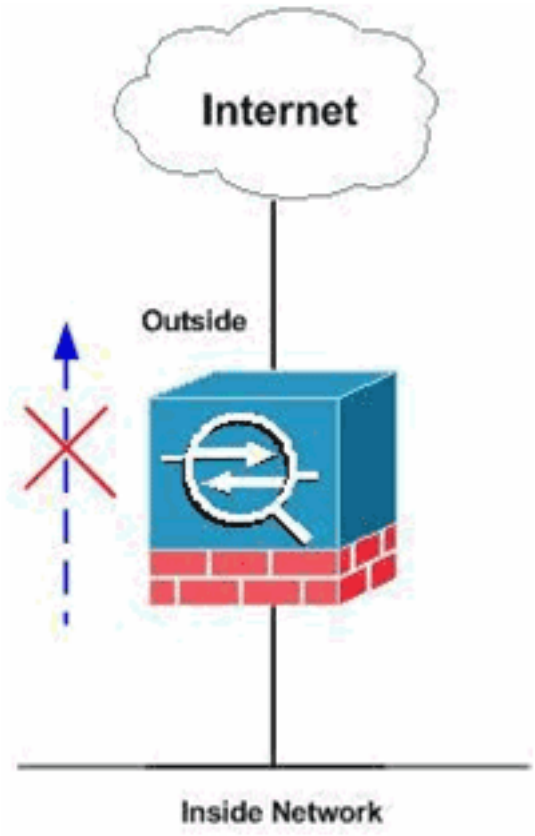
구성

이 섹션에서는 이 문서에 설명된 기능을 구성하는 정보를 제공합니다.

참고: 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 섹션에 사용된 명령에 대한 자세한 내용을 확인하십시오.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



참고: 선택한 FTP 사이트는 정규식을 사용하여 허용되거나 차단됩니다.

구성

이 문서에서는 다음 구성을 사용합니다.

ASA CLI 컨피그레이션

ASA CLI 컨피그레이션

```
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
```

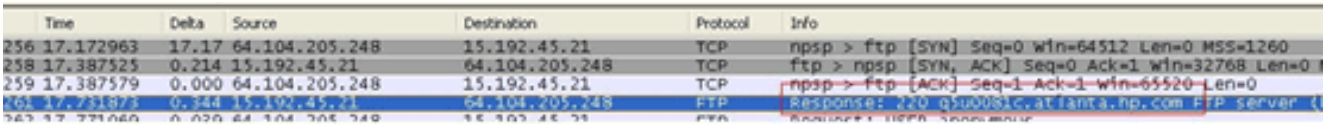
```
 parameters
 class FTP_class_map
  reset log

! 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
```

ASA Configuration 8.x with ASDM 6.x

특정 FTP 사이트를 차단하기 위해 정규식을 구성하고 MPF에 적용하려면 다음 단계를 완료합니다.

1. **FTP 서버 이름을 확인합니다.**FTP 검사 엔진은 명령, 파일 이름, 파일 유형, 서버 및 사용자 이름과 같은 다른 기준을 사용하여 검사를 제공할 수 있습니다.이 절차에서는 서버를 기준으로 사용합니다.FTP 검사 엔진은 FTP 사이트에서 보낸 서버 220 응답을 서버 값으로 사용합니다.이 값은 사이트에서 사용하는 도메인 이름과 다를 수 있습니다.이 예에서는 Wireshark를 사용하여 2단계에서 정규식에 사용되는 응답 220 값을 얻기 위해 검사 대상 사이트에 FTP 패킷을 캡처합니다

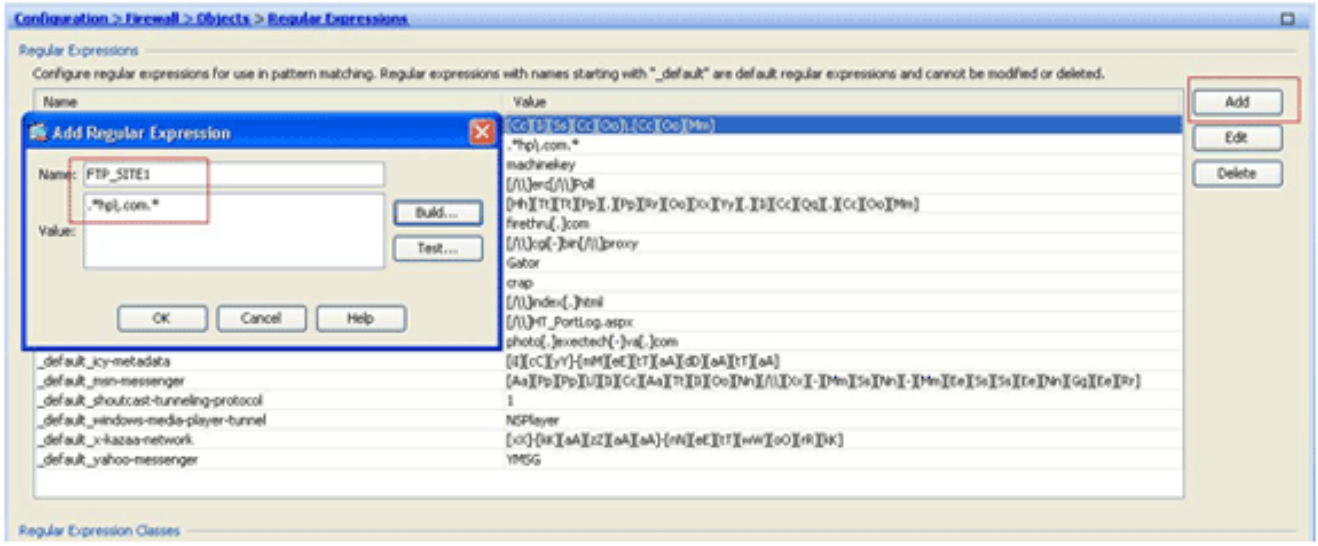
.



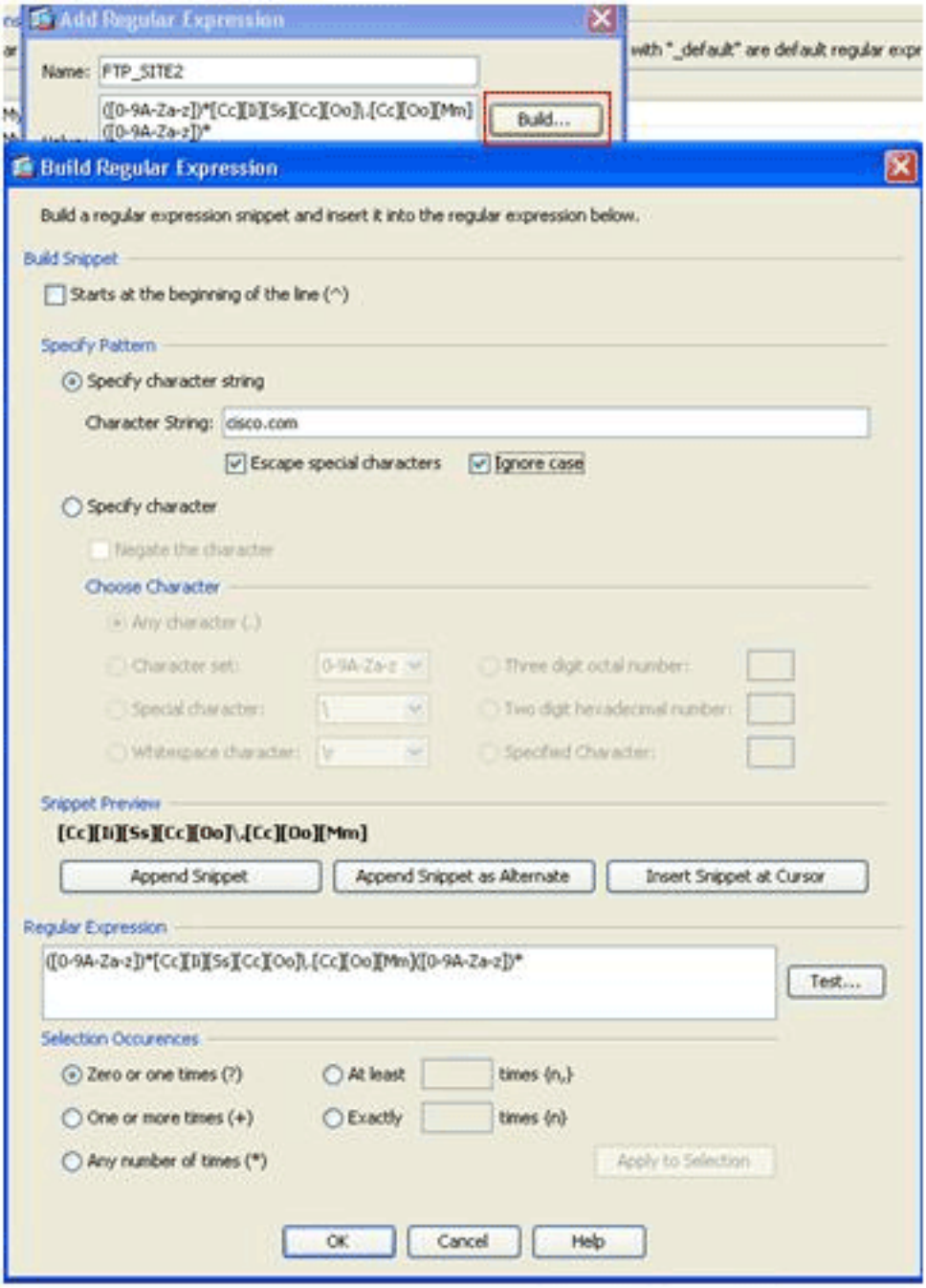
캡처를 기준으로 ftp://hp.com에 대한 응답 220 값은 q5u0081c.atlanta.hp.com입니다.

2. **정규식을 생성합니다.**Configuration **> Firewall > Objects > Regular Expressions**를 선택하고 Regular Expression 탭 아래에서 Add를 클릭하여 다음 절차에 설명된 정규식을 생성합니다.ftp 사이트(예: ".* hp\.com.*")에서 수신한 응답 220(Wireshark의 패킷 캡처나 기타 사용된 모든 툴에서 표시됨)과 일치시키려면 *FTP_SITE1*이라는 정규식을 만들고 **OK**를 클릭합니다

.

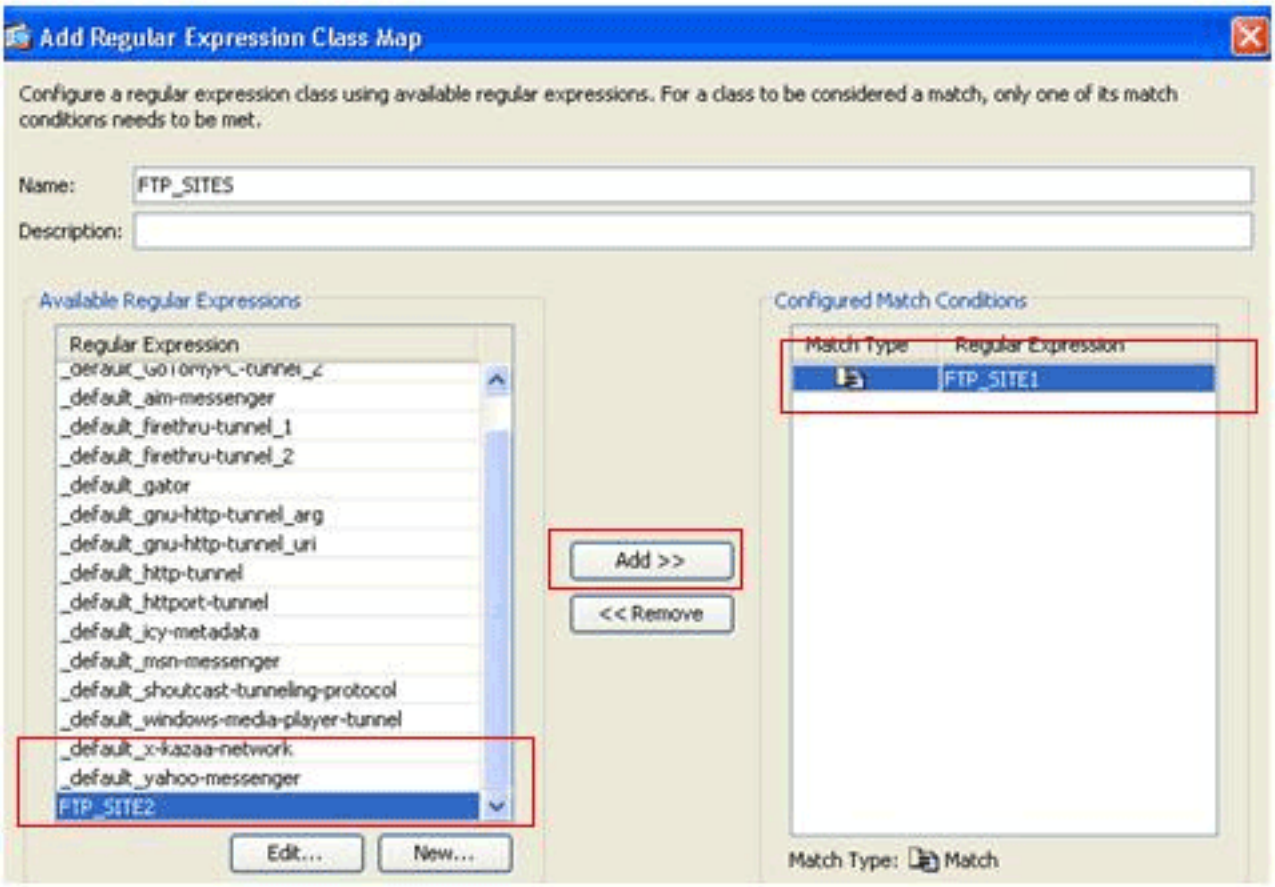


참고: 고급 정규식을 만드는 방법에 대한 도움말을 보려면 빌드를 클릭할 수 있습니다



. 정규식이 생성되면 Apply를 **클릭합니다.**

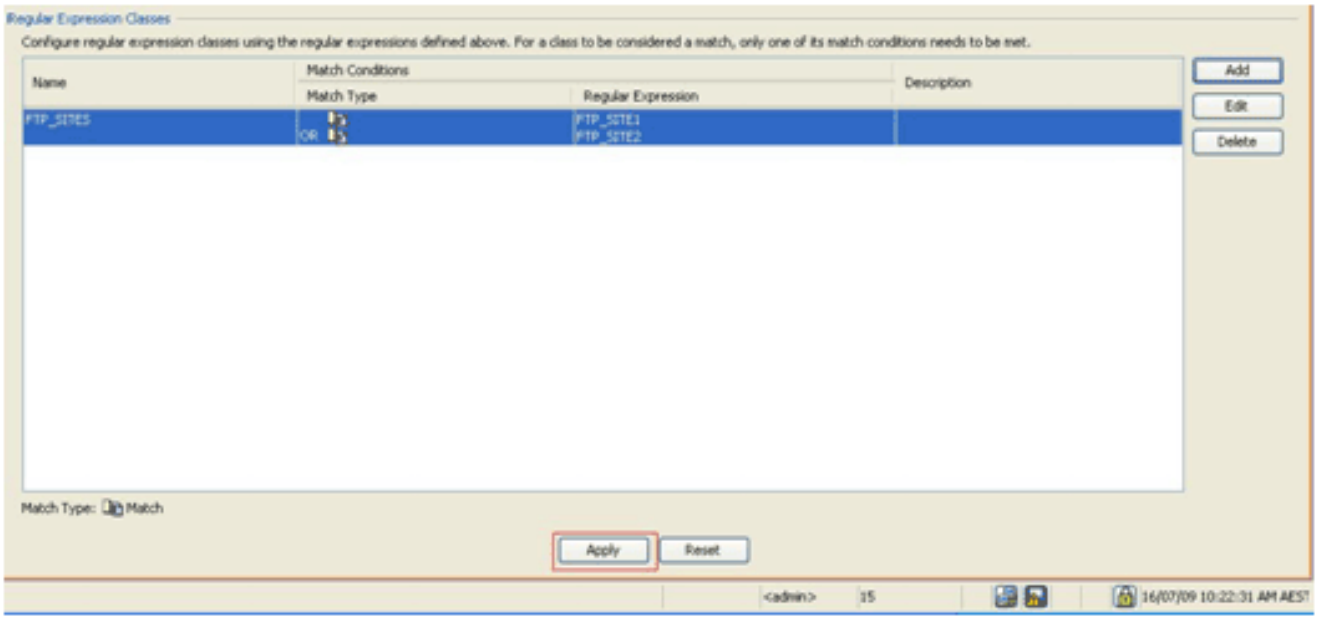
3. **정규식 클래스를 만듭니다.**Configuration **> Firewall > Objects > Regular Expressions를** 선택하고 Regular Expression Classes 섹션 아래에서 Add를 클릭하여 다음 절차에 설명된 대로 클래스를 생성합니다.정규식 FTP_*SITE1* 및 *FTP_SITE2*와 일치시키기 위해 정규식 클래스인 FTP_*SITES*를 만들고 **OK**를 클릭합니다



.

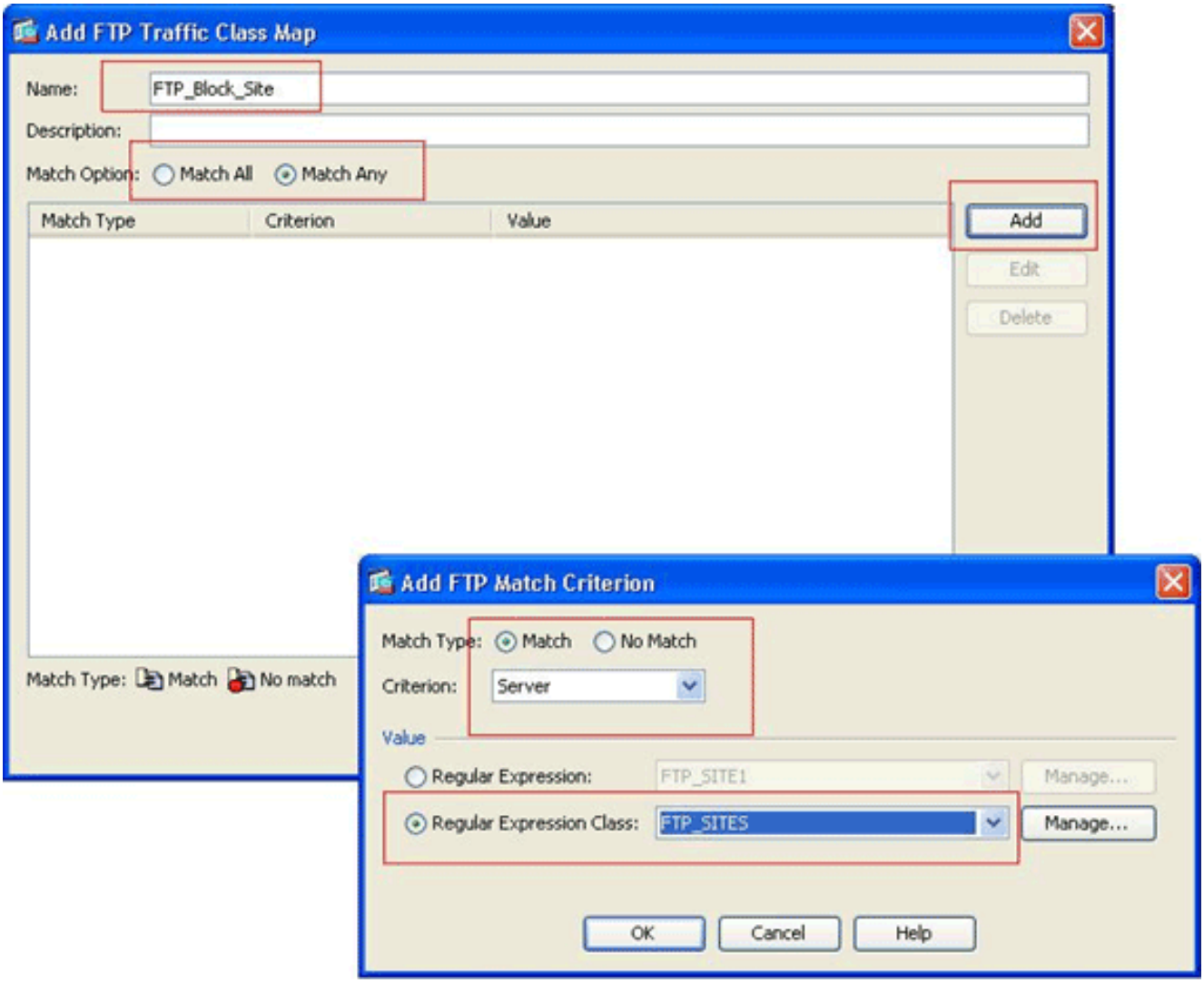
클래스 맵이 생성되면 Apply를 **클릭합니다**

.



4. **식별된 트래픽을 클래스 맵으로 검사합니다.**Configuration **> Firewall > Objects > Class Maps > FTP > Add**를 마우스 오른쪽 버튼으로 클릭하고 **Add를** 선택하여 클래스 맵을 생성하여 이 절차에 설명된 대로 다양한 정규식으로 식별된 FTP 트래픽을 검사하도록 합니다.FTP 응답 220을 생성한 정규식과 일치시키기 위해 클래스 맵인 FTP_Block_Site를 생성합니다

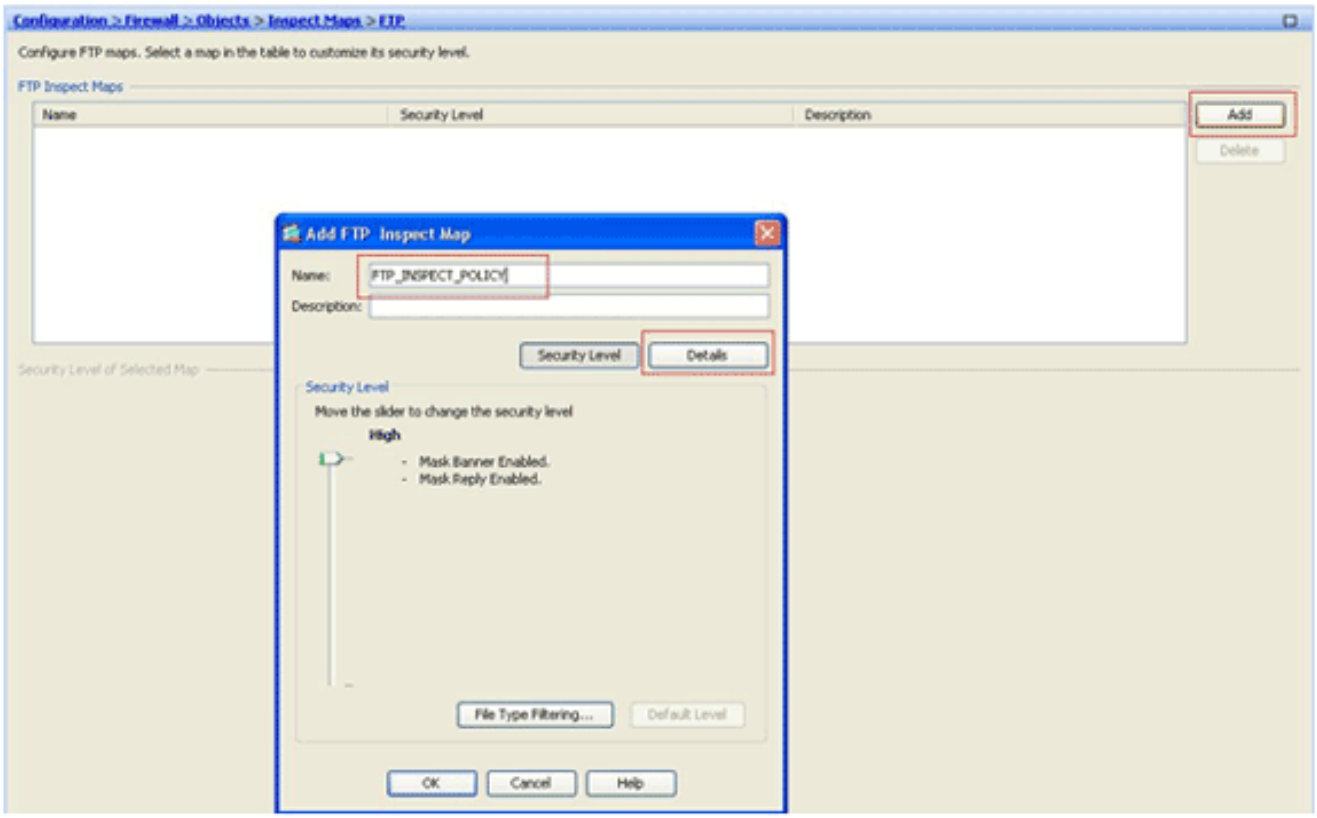
.



정규식에 지정된 사이트를 제외하려면 **No Match** 라디오 버튼을 클릭합니다.값 섹션에서 정규식 또는 정규식 클래스를 선택합니다.이 절차의 경우 이전에 만든 클래스를 선택합니다 .Apply를 **클릭합니다**.

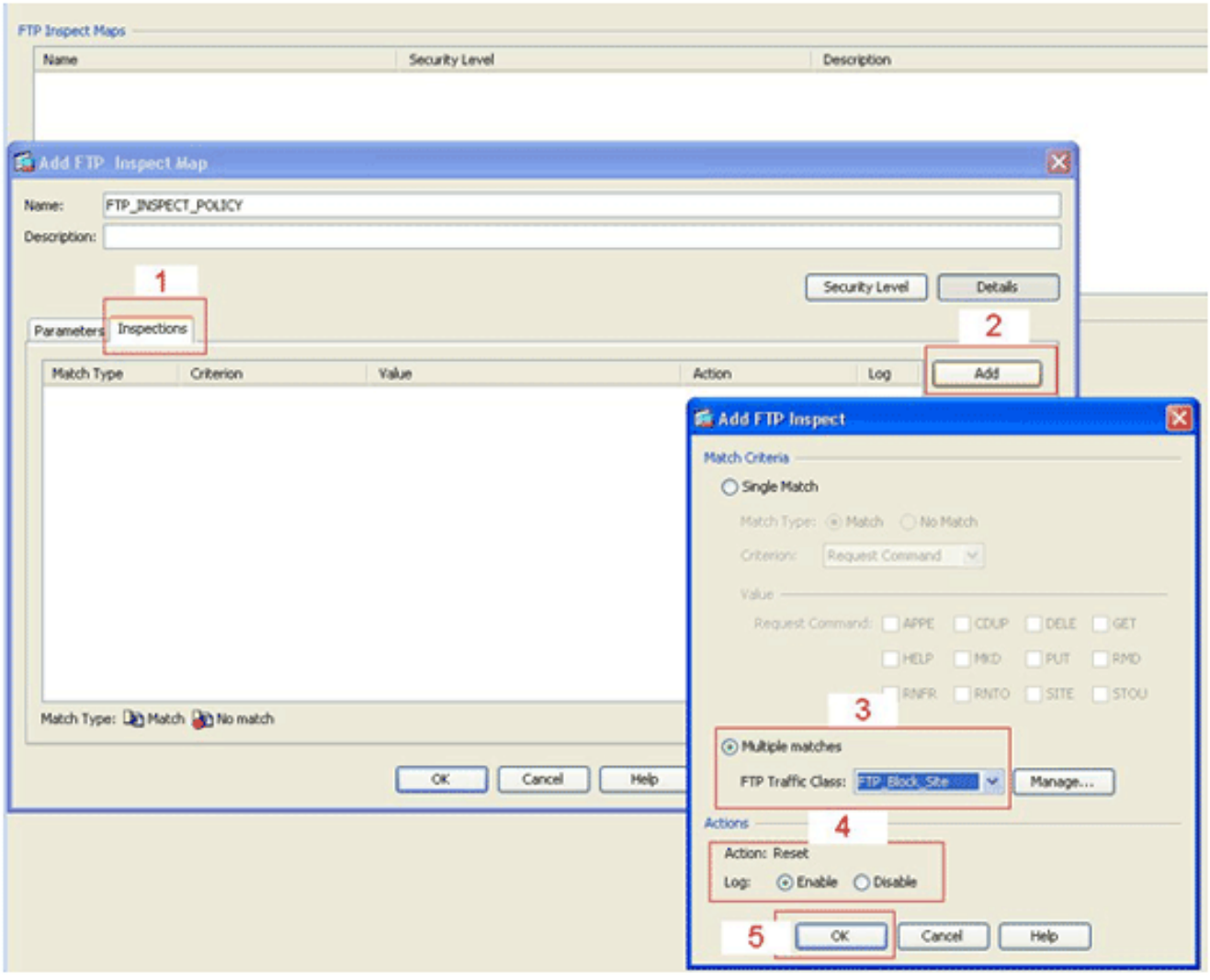
5. **검사 정책에서 일치하는 트래픽에 대한 작업을 설정합니다.**검사 정책을 생성하고 **필요에** 따라 일치하는 트래픽에 대한 작업을 설정하려면 Configuration > Firewall > Objects > Inspect Maps > FTP**> Add**를 선택합니다

.



검사 정책의 이름과 설명을 입력합니다.(예: *FTP_INSPECT_POLICY*)Details를 **클릭합니다**

.

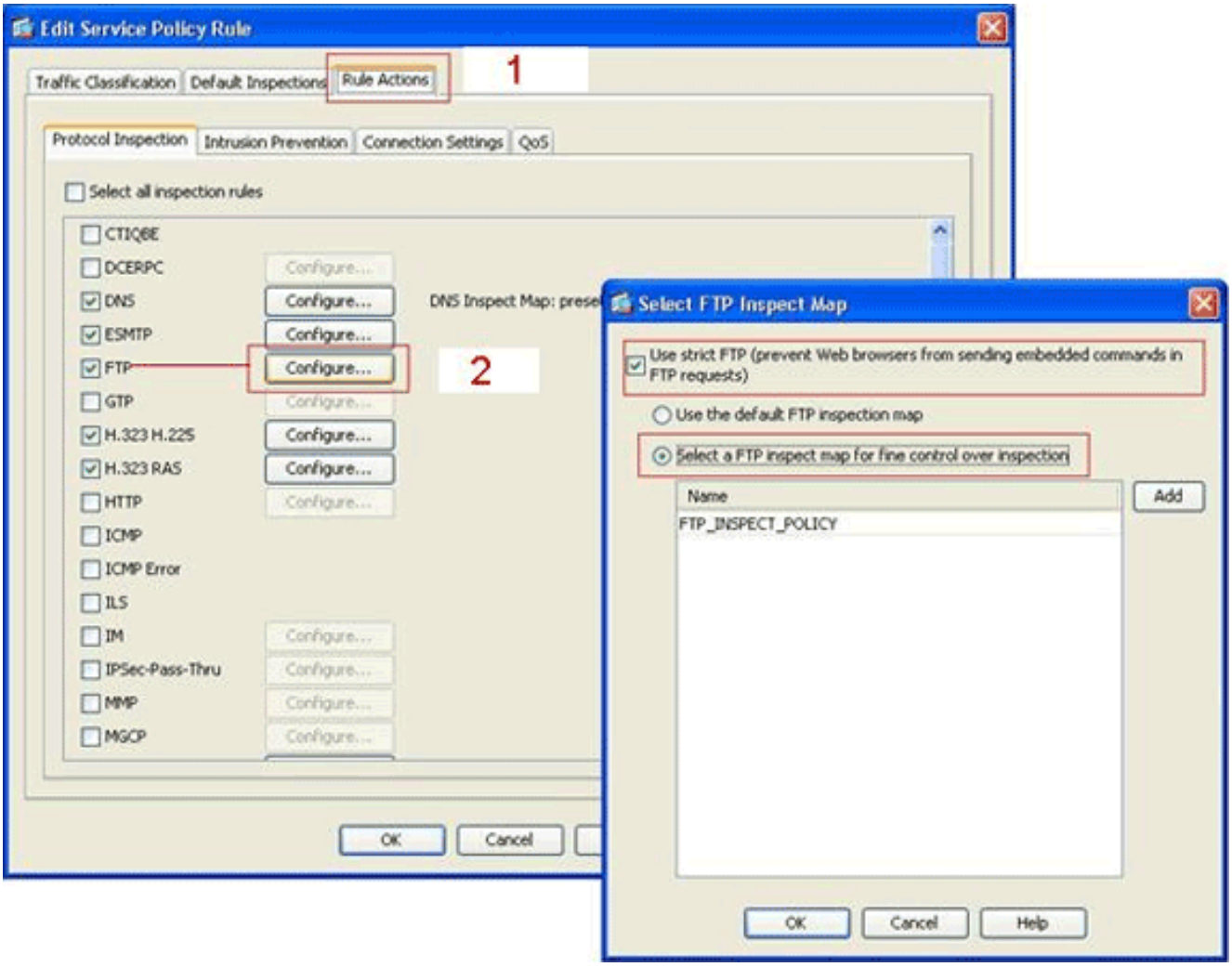


검사 탭을 **클릭합니다**.(1)Add(**추가)를 클릭합니다**.(2)**Multiple matches** 라디오 버튼을 클릭하

고 드롭다운 목록에서 트래픽 클래스를 선택합니다.(3)활성화 또는 비활성화하려면 원하는 재설정 작업을 선택합니다.이 예에서는 지정된 사이트와 *일치하지 않는* 모든 FTP 사이트에 대해 FTP 연결 재설정을 활성화합니다.(4)OK(**확인**)를 클릭하고 **OK(확인)**를 다시 클릭한 다음 Apply(적용)를 **클릭합니다**.(5)

6. **검사 FTP 정책을 전역 검사 목록에 적용합니다.**Configuration **> Firewall > Service Policy Rules를 선택합니다**.오른쪽에서 inspection_**default** 정책을 선택하고 **Edit**를 클릭합니다.Rule Actions(규칙 작업) 탭(1)에서 FTP에 대한 **Configure(구성)** 버튼을 클릭합니다. (2)Select FTP Inspect Map(FTP 검사 맵 선택) 대화 상자에서 **Use strict FTP(엄격한 FTP 사용)** 확인란을 선택한 다음 **FTP inspect map for fine control over inspection** 라디오 버튼**을** 클릭합니다.새 FTP 검사 정책인 *FTP_INSPECT_POLICY*가 목록에 표시되어야 합니다.OK(**확인**)를 클릭하고 **OK(확인)**를 다시 클릭한 다음 Apply(적용)를 **클릭합니다**

.



다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다.OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

- **show running-config regex** - 구성된 정규식을 표시합니다.

```
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** - 구성된 클래스 맵을 표시합니다.

```
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 type inspect http** - 구성된 HTTP 트래픽을 검사하는 정책 맵을 표시합니다.

```
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 policy-map** - 모든 정책 맵 컨피그레이션 및 기본 정책 맵 컨피그레이션을 표시합니다.

```
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 service-policy** - 현재 실행 중인 모든 서비스 정책 컨피그레이션을 표시합니다.

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

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

검사 엔진이 트래픽을 검사하고 올바르게 트래픽을 허용하거나 삭제하는지 확인하기 위해 **show service-policy** 명령을 사용할 수 있습니다.

```
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
```

관련 정보

- ASA/PIX 8.x:MPF 컨피그레이션이 포함된 정규식을 사용하여 특정 웹 사이트(URL) 차단 예
- PIX/ASA 7.x 이상:MPF 컨피그레이션 예를 사용하여 P2P(Peer-to-Peer) 및 IM(Instant Messaging) 트래픽 차단
- PIX/ASA 7.x:Enable FTP/TFTP Services 컨피그레이션 예
- 애플리케이션 레이어 프로토콜 검사 적용
- Cisco ASA 5500 Series Adaptive Security Appliances - 지원
- Cisco ASDM(Adaptive Security Device Manager)
- Cisco PIX 500 Series 보안 어플라이언스 - 지원
- Cisco PIX Firewall Software - 지원
- Cisco PIX Firewall Software 명령 참조