ASA/PIX 8.x: Esempio di configurazione MPF per consentire/bloccare siti FTP utilizzando espressioni regolari

Sommario

Introduzione

In questo documento viene descritto come configurare Cisco Security Appliance ASA/PIX 8.x che utilizza espressioni regolari con Modular Policy Framework (MPF) per bloccare o consentire alcuni siti FTP in base al nome del server.

Prerequisiti

Requisiti

in questo documento si presume che Cisco Security Appliance sia configurato e funzioni correttamente.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco serie 5500 Adaptive Security Appliance (ASA) con software versione 8.0(x) e successive
- Cisco Adaptive Security Device Manager (ASDM) versione 6.x per ASA 8.x

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Premesse

Panoramica del framework di criteri modulari

MPF offre un modo coerente e flessibile per configurare le funzionalità delle appliance di sicurezza. Ad esempio, è possibile utilizzare MPF per creare una configurazione di timeout specifica per una particolare applicazione TCP, a differenza di una configurazione che si applica a tutte le applicazioni TCP.

MPF supporta le seguenti funzionalità:

- normalizzazione TCP, limiti e timeout delle connessioni TCP e UDP e randomizzazione dei numeri di sequenza TCP
- CSC
- Ispezione delle applicazioni
- IPS
- Policy di input QoS
- Policy di output QoS
- Coda priorità QoS

La configurazione dell'MPF prevede quattro attività:

1. Identificare il traffico di layer 3 e layer 4 a cui si desidera applicare le azioni. per ulteriori informazioni, fare riferimento a Identificazione del traffico con una mappa delle classi del layer 3/4.
2. (Solo ispezione dell'applicazione). Definire azioni speciali per il traffico di ispezione delle applicazioni. per ulteriori informazioni, fare riferimento a Configurazione delle azioni speciali per le ispezioni delle applicazioni.
3. Applicare azioni al traffico di layer 3 e layer 4. per ulteriori informazioni, fare riferimento a Definizione delle azioni mediante una mappa dei criteri di layer 3/4.
4. Attivare le azioni su un'interfaccia. Per ulteriori informazioni, fare riferimento a Applicazione di un criterio di layer 3/4 a un'interfaccia tramite un criterio di servizio.

Espressione regolare

Un'espressione regolare corrisponde alle stringhe di testo letteralmente come una stringa esatta o

mediante l'utilizzo di metacaratteri, pertanto è possibile trovare più varianti di una stringa di testo. È possibile utilizzare un'espressione regolare per far corrispondere il contenuto di un determinato traffico dell'applicazione. Ad esempio, è possibile trovare una stringa URL all'interno di un pacchetto HTTP.

Nota: utilizzare **Ctrl+V** per eseguire l'escape di tutti i caratteri speciali nella CLI, ad esempio i punti interrogativi (?) o le tabulazioni. Ad esempio, digitare **d[Ctrl+V]g** per immettere **d?g** nella configurazione.

Per creare un'espressione regolare, utilizzare il comando **regex**. Inoltre, il comando **regex** può essere utilizzato per varie funzioni che richiedono la corrispondenza del testo. Ad esempio, è possibile configurare azioni speciali per l'ispezione delle applicazioni utilizzando l'utilità MPF che utilizza una mappa dei criteri di ispezione. Per ulteriori informazioni, fare riferimento al comando policy-map type inspect.

Nella mappa dei criteri di ispezione è possibile identificare il traffico su cui si desidera intervenire se si crea una mappa della classe di ispezione contenente uno o più comandi di **corrispondenza** oppure è possibile utilizzare i comandi di **corrispondenza** direttamente nella mappa dei criteri di ispezione. Alcuni comandi di **corrispondenza** consentono di identificare il testo in un pacchetto utilizzando un'espressione regolare. Ad esempio, è possibile trovare le stringhe URL all'interno dei pacchetti HTTP. È possibile raggruppare le espressioni regolari in una mappa di classe delle espressioni regolari. Per ulteriori informazioni, fare riferimento al comando class-map type regex.

In questa tabella vengono elencati i metacaratteri con significati speciali.

Carattere	Descrizione	Note
.	Punto	Corrisponde a qualsiasi carattere singolo. Ad esempio, **d.g** corrisponde a dog, dag, dtg e a qualsiasi parola che contenga tali caratteri, ad esempio doggonnit.
(espr)	Sottoespressione	Una sottoespressione separa i caratteri dai caratteri circostanti, in modo che sia possibile utilizzare altri metacaratteri nella sottoespressione. Ad esempio, **d(o|a)g** corrisponde a cane e cane, mentre **do|ag** corrisponde a do e ag. Una sottoespressione può essere utilizzata anche con i quantificatori di ripetizione per differenziare i caratteri destinati alla ripetizione. Ad esempio, **ab(xy){3}z** corrisponde ad abxyxyxyxyz.
|	Alternanza	Corrisponde all'espressione che separa. Ad esempio, **cane|gatto** corrisponde a cane o gatto.
?	Punto interrogativo	Quantificatore che indica che l'espressione precedente contiene 0 o 1. Ad esempio, **lo?se** corrisponde a lse o lose. **Nota: è** necessario immettere **Ctrl+V**,

		quindi il punto interrogativo, altrimenti viene richiamata la funzione della guida.
*	Asterisco	Un quantificatore che indica la presenza di 0, 1 o qualsiasi numero dell'espressione precedente. Ad esempio, **lo*se** corrisponde a lse, lose, loose e così via.
{x}	Ripeti quantificatore	Ripetere esattamente x volte. Ad esempio, **ab(xy){3}z** corrisponde ad abxyxyxyxyz.
{x}	Quantificatore a ripetizione minimo	Ripetere almeno x volte. Ad esempio, **ab(xy){2,}z** corrisponde ad abxyxyz, abxyxyxyxyz e così via.
[abc]	Classe Character	Corrisponde a qualsiasi carattere tra parentesi. Ad esempio, **[abc]** corrisponde a, b o c.
[^abc]	Classe di caratteri negata	Corrisponde a un singolo carattere non contenuto tra parentesi. Ad esempio, **[^abc]** corrisponde a qualsiasi carattere diverso da a, b o c. **[^A-Z]** corrisponde a qualsiasi carattere singolo diverso da una lettera maiuscola.
[a-c]	Classe intervallo caratteri	Trova tutti i caratteri compresi nell'intervallo. **[a-z]** corrisponde a qualsiasi lettera minuscola. È possibile combinare caratteri e intervalli: **[abcq-z]** corrisponde a, b, c, q, r, s, t, u, v, w, x, y, z e così **[a-cq-z]**. Il carattere trattino (-) è letterale solo se è l'ultimo o il primo carattere tra parentesi: **[abc-]** o **[-abc]**.
""	Virgolette	Mantiene gli spazi finali o iniziali nella stringa. Ad esempio, **" test"** mantiene lo spazio iniziale quando cerca una corrispondenza.
^	Accento circonflesso	Specifica l'inizio di una riga.
\	Carattere di escape	Se utilizzato con un metacarattere, corrisponde a un carattere letterale. Ad esempio, **\[** corrisponde alla parentesi quadra sinistra.
carattere	Carattere	Quando il carattere non è un metacarattere, corrisponde al carattere letterale.
\r	Ritorno a capo	Trova/sostituisce un ritorno a capo: 0x0d
\n	Nuova riga	Trova/sostituisce una nuova riga: 0x0a

\t	Tabulazione	Corrisponde a una scheda: 0x09.
\f	Alimentazione	Corrisponde a un feed di modulo: 0x0c
\xNN	Numero esadecimale con escape	Corrisponde a un carattere ASCII che utilizza un carattere esadecimale costituito esattamente da due cifre.
\NNN	Numero ottale scappato	Trova/sostituisce un carattere ASCII come ottale che è costituito esattamente da tre cifre. Ad esempio, il carattere 040 rappresenta uno spazio.

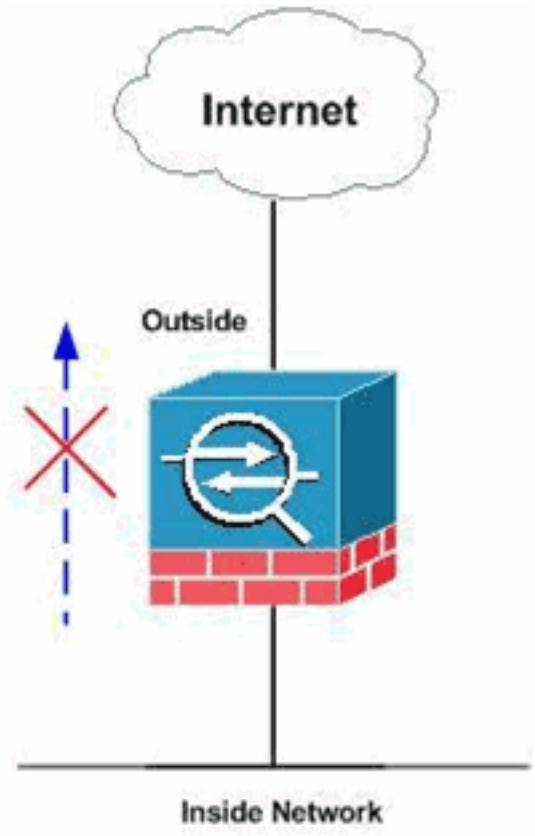
Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Nota: i siti FTP selezionati sono consentiti o bloccati tramite espressioni regolari.

Configurazioni

Nel documento vengono usate queste configurazioni:

- Configurazione ASA CLI
- ASA Configuration 8.x con ASDM 6.x

Configurazione ASA CLI

Configurazione ASA CLI

```
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
```

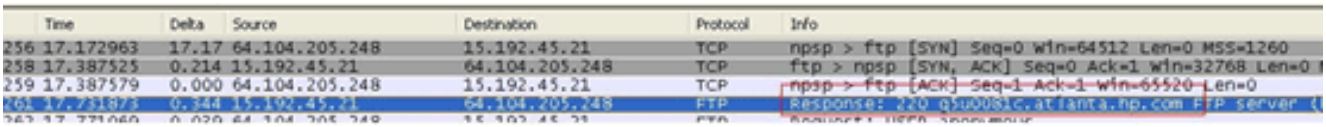
```
logging enable
logging timestamp
logging buffered debugging
mtu outside 1500
mtu inside 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-61557.bin
no asdm history enable
arp timeout 14400

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
```

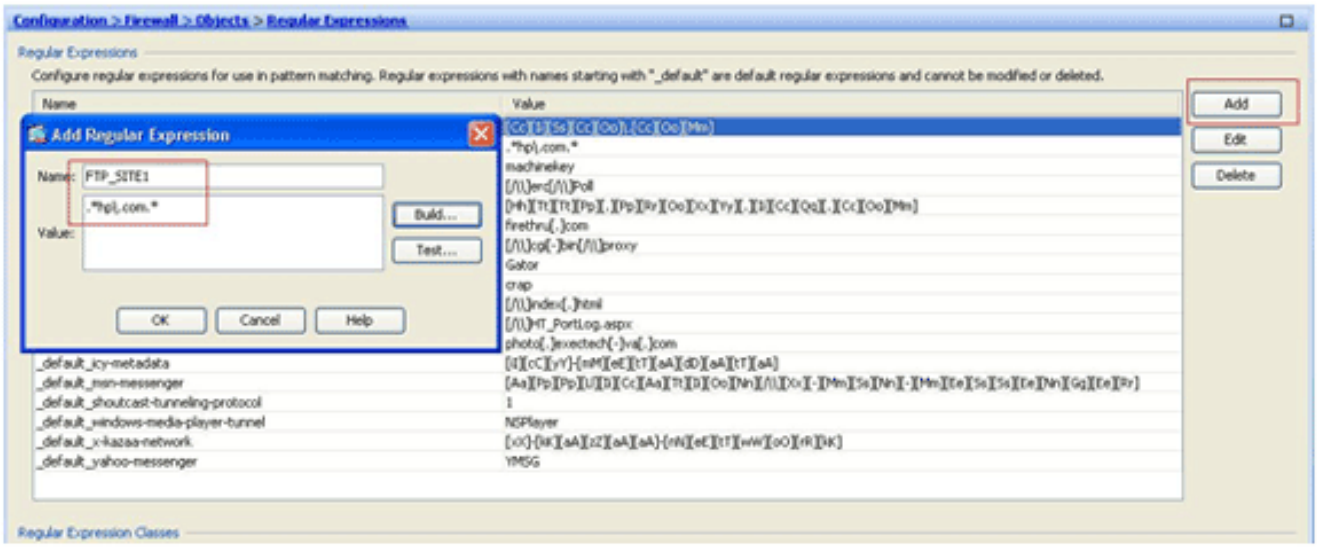
ASA Configuration 8.x con ASDM 6.x

Completare questa procedura per configurare le espressioni regolari e applicarle a MPF per bloccare i siti FTP specifici:

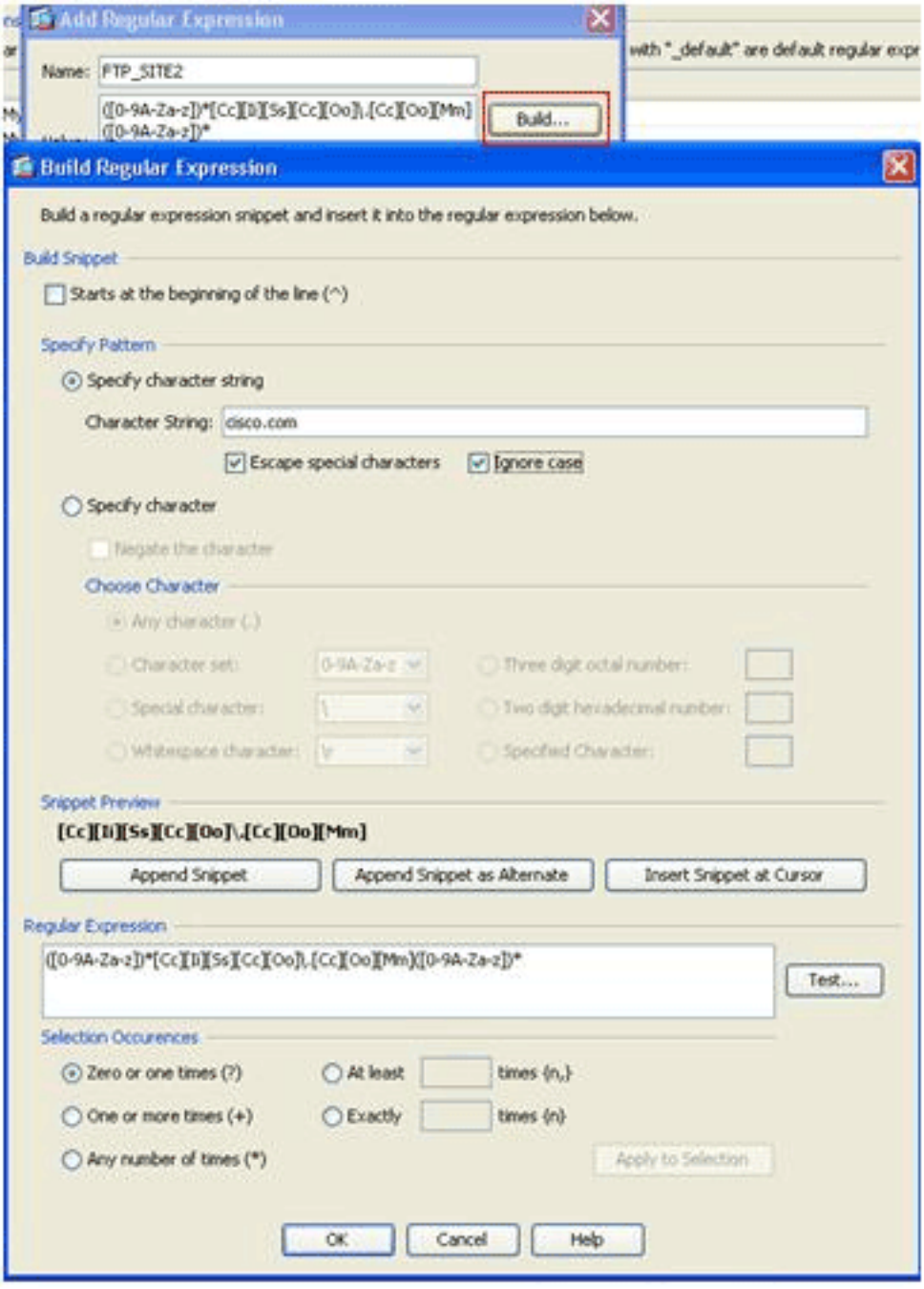
1. **Determinare il nome del server FTP.**Il motore di ispezione FTP può fornire l'ispezione utilizzando diversi criteri, quali comando, nome file, tipo di file, server e nome utente. In questa procedura viene utilizzato il server come criterio. Il motore di ispezione FTP utilizza la risposta 220 del server inviata dal sito FTP come valore del server. Questo valore può essere diverso dal nome di dominio utilizzato dal sito. In questo esempio viene usato Wireshark per catturare i pacchetti FTP sul sito ispezionato in modo da ottenere il valore di risposta 220 da usare nell'espressione regolare usata nel passaggio 2.



   In base all'acquisizione, il valore 220 della risposta per ftp://hp.com è (ad esempio) *q5u0081c.atlanta.hp.com*.
2. **Creare espressioni regolari.**Scegliere **Configurazione > Firewall > Oggetti > Espressioni regolari**, quindi fare clic su **Aggiungi** nella scheda Espressione regolare per creare le espressioni regolari come descritto nella procedura seguente:Creare un'espressione regolare, *FTP_SITE1*, in modo che corrisponda alla risposta 220 (come mostrato nell'acquisizione del pacchetto in Wireshark o in qualsiasi altro strumento utilizzato) ricevuta dal sito ftp (ad esempio, ".* hp\.com.*") e fare clic su **OK**.

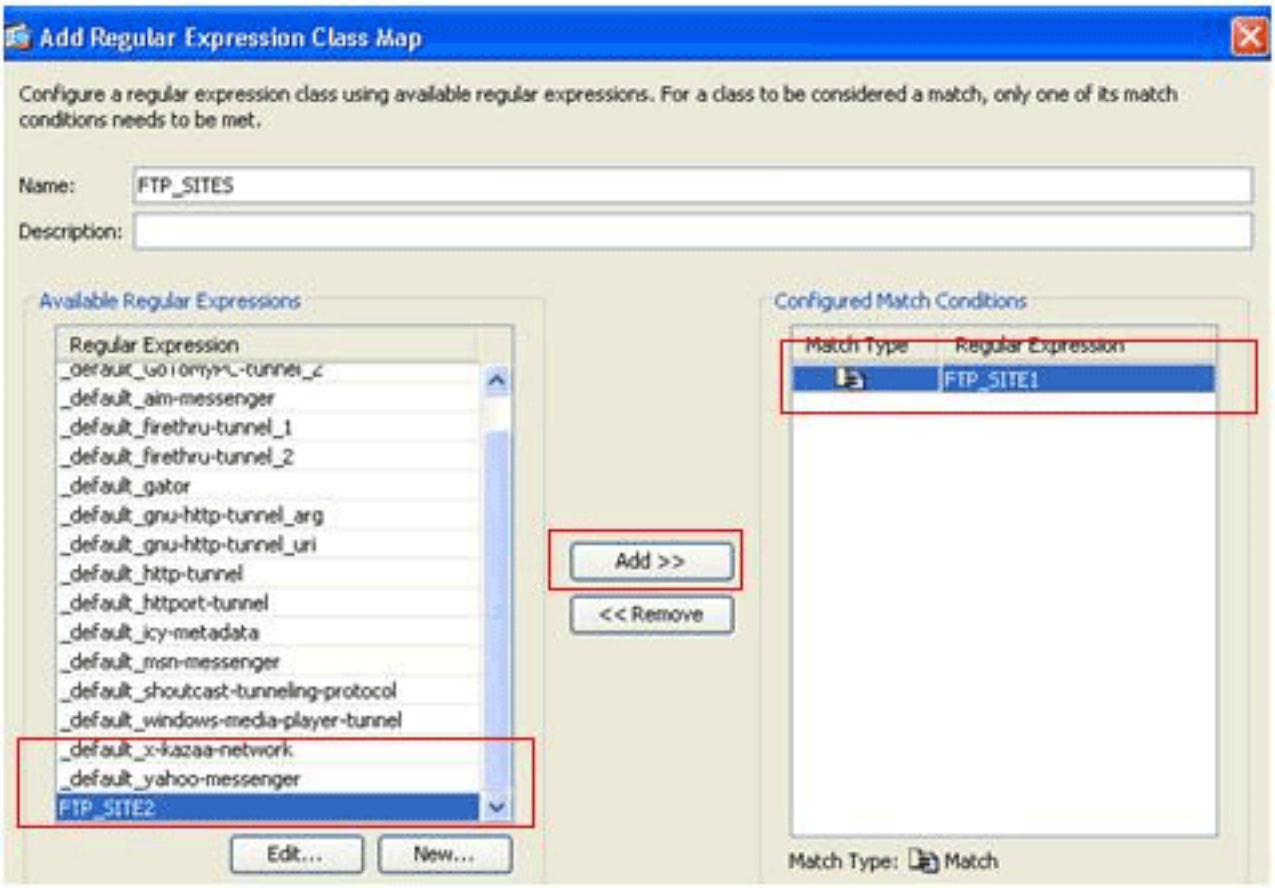


Nota: è possibile fare clic su **Genera** per visualizzare le informazioni della Guida sulla creazione di espressioni regolari più



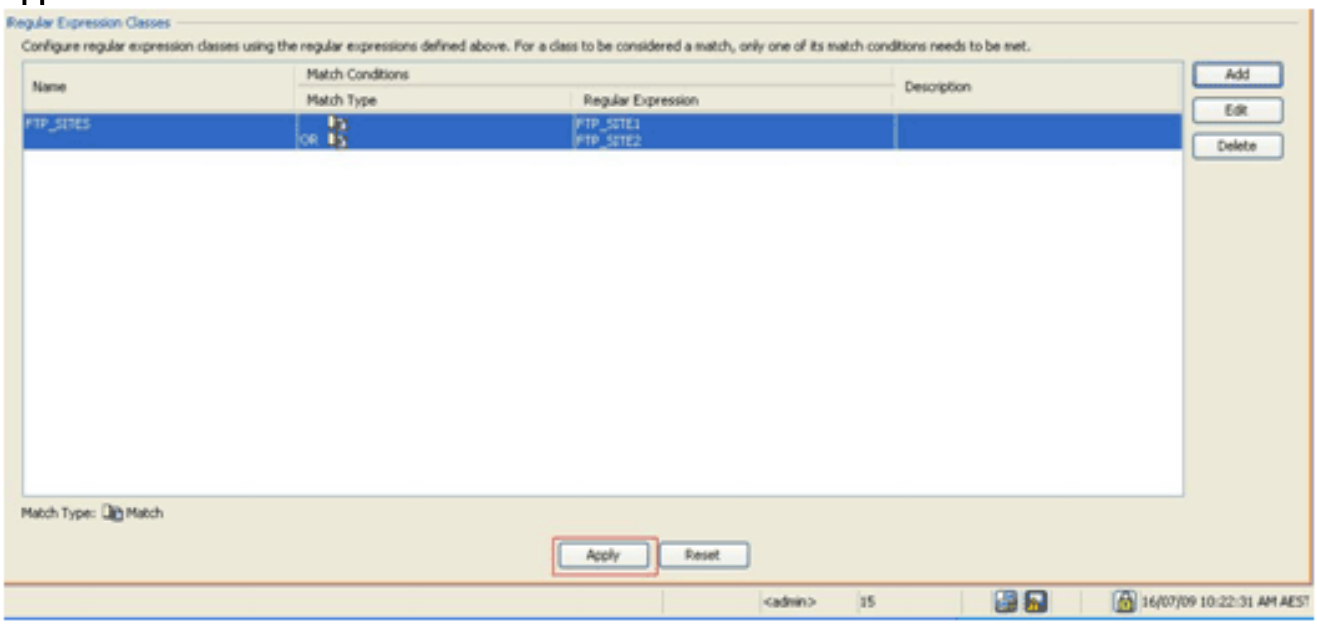
avanzate. Una volta creata l'espressione regolare, fare clic su **Applica.**

3. **Creare classi di espressioni regolari.**Scegliere **Configurazione > Firewall > Oggetti > Espressioni regolari**, quindi fare clic su **Aggiungi** nella sezione Classi di espressioni regolari per creare la classe come descritto in questa procedura:Creare una classe di espressioni regolari, *FTP_SITES*, in modo che corrisponda a una qualsiasi delle espressioni regolari *FTP_SITE1* e *FTP_SITE2*, quindi fare clic su **OK**.



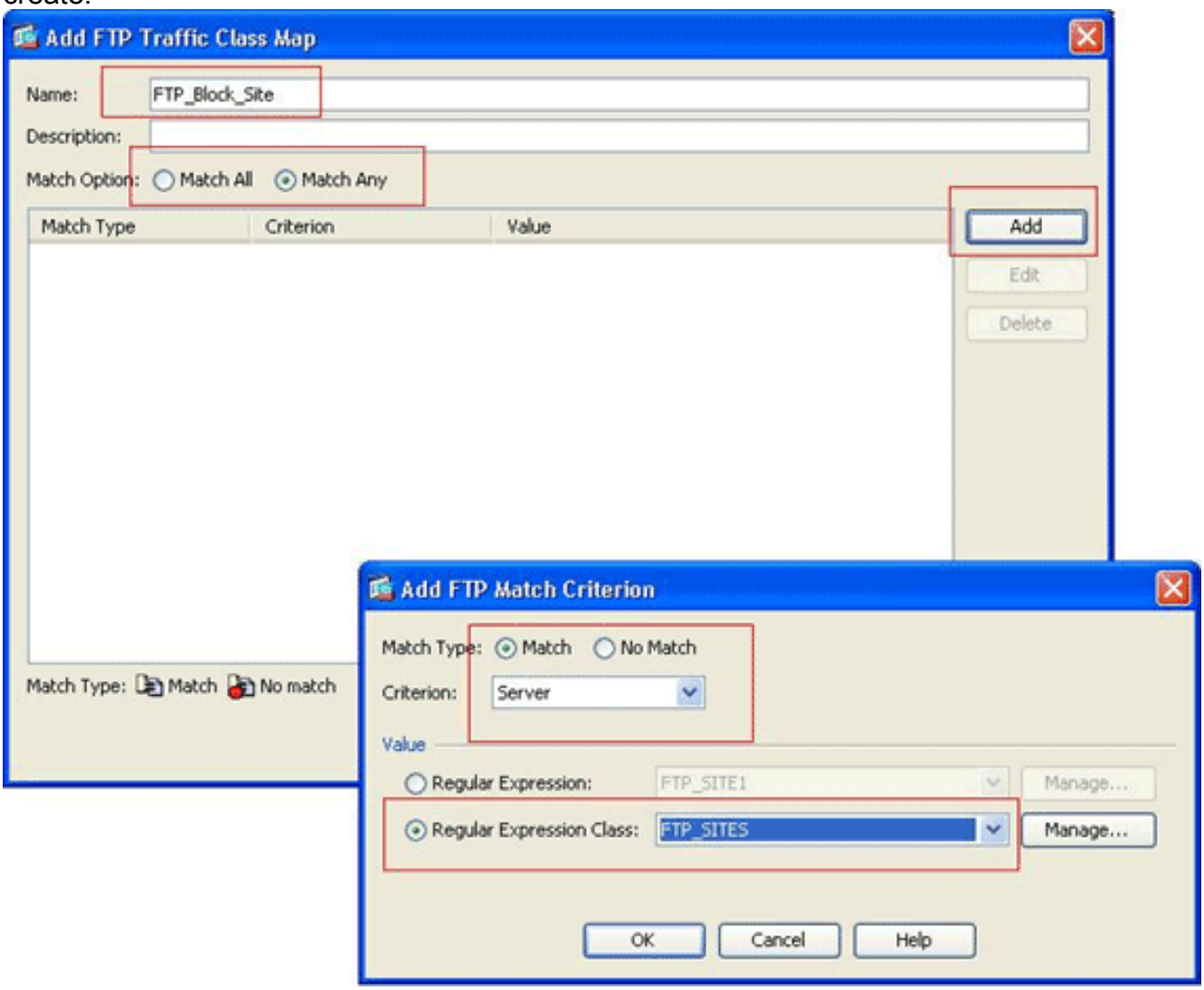
U

na volta creata la mappa della classe, fare clic su **Applica**.



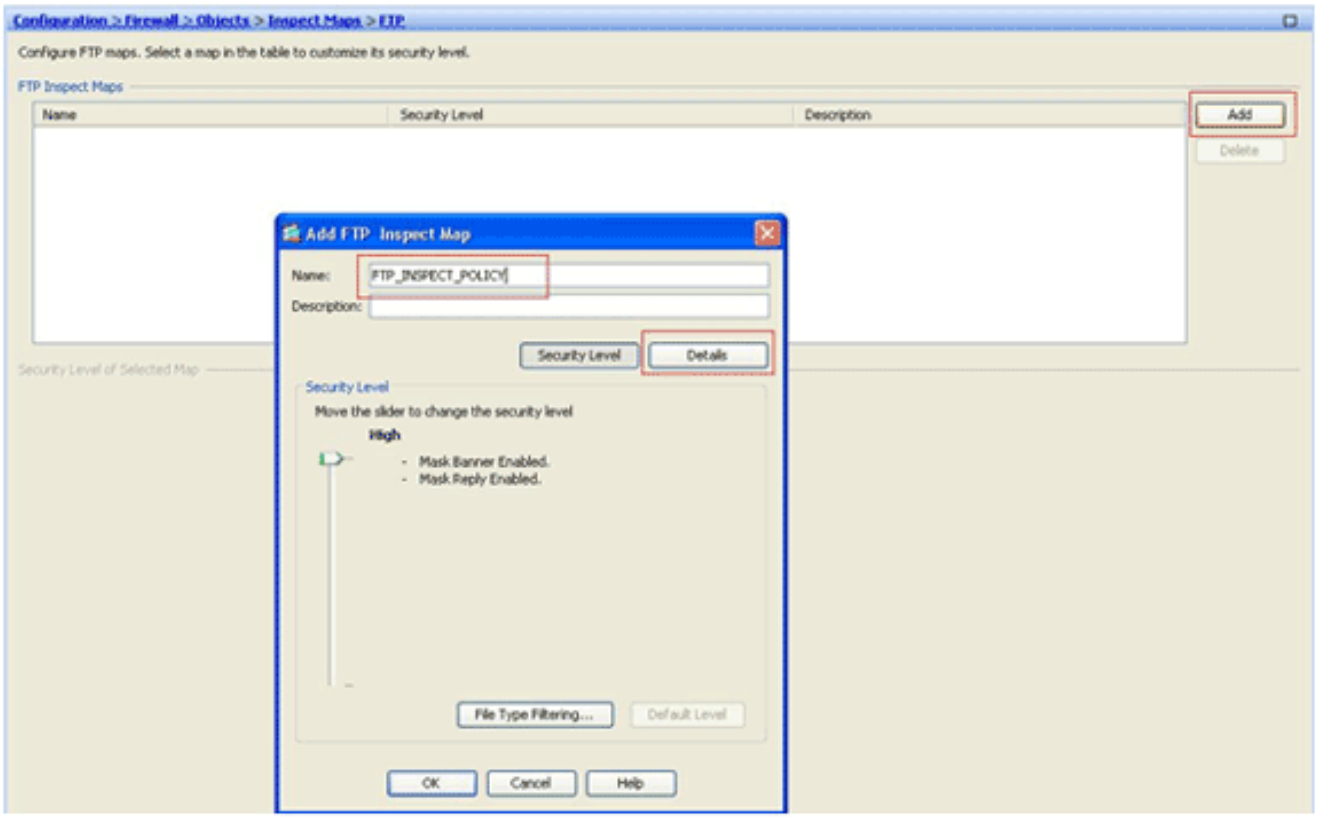
4. **Esaminare il traffico identificato con le mappe di classe.**Scegliere **Configurazione > Firewall > Oggetti > Mappe classi > FTP > Aggiungi**, fare clic con il pulsante destro del mouse e scegliere **Aggiungi** per creare una mappa di classe per ispezionare il traffico FTP identificato da varie espressioni regolari, come descritto in questa procedura:Creare una mappa di

classe, *FTP_Block_Site*, in modo che corrisponda alla risposta FTP 220 con le espressioni regolari
create.

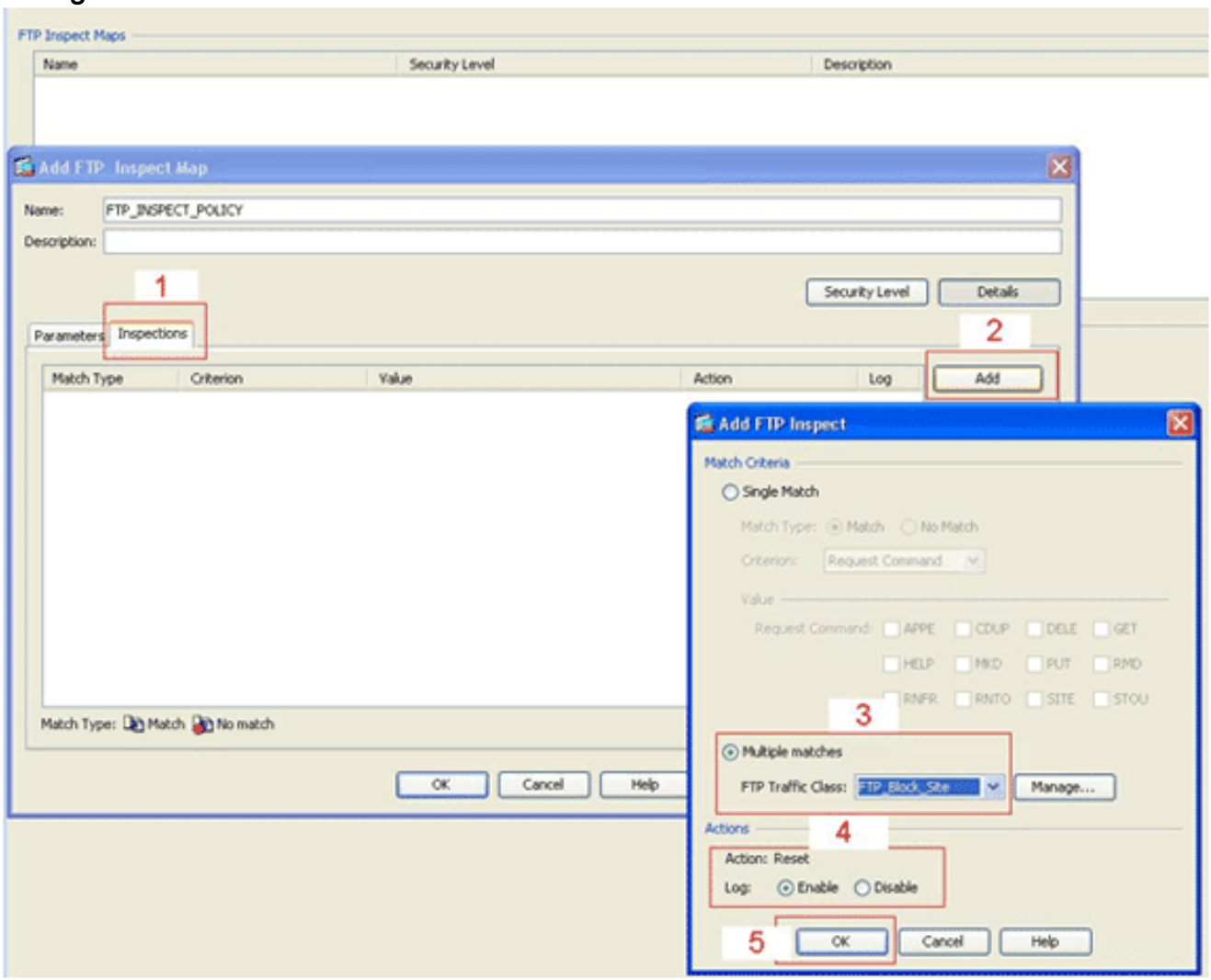


Se si desidera escludere i siti specificati nell'espressione regolare, fare clic sul pulsante di opzione **Nessuna corrispondenza**.Nella sezione Valore scegliere un'espressione regolare o una classe di espressioni regolari. Per questa procedura, scegliere la classe creata in precedenza.Fare clic su **Apply** (Applica).

5. **Impostare le azioni per il traffico corrispondente nei criteri di ispezione.**Scegliere **Configurazione > Firewall > Oggetti > Ispeziona mappe > FTP> Aggiungi** per creare un criterio di ispezione e impostare l'azione per il traffico corrispondente come richiesto.

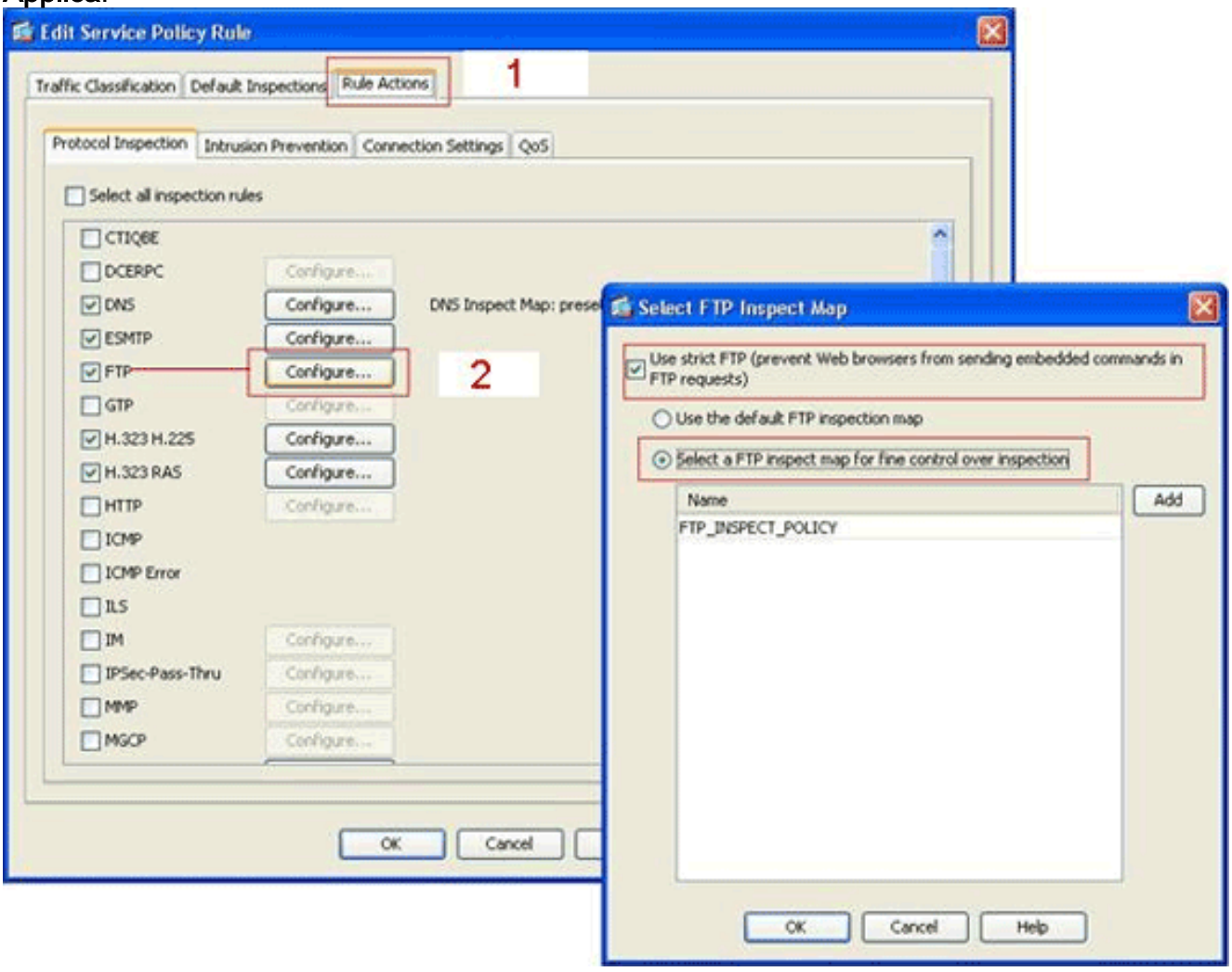


Immettere il nome e una descrizione per il criterio di ispezione. Ad esempio, *FTP_INSPECT_POLICY*.Fare clic su **Dettagli.**



Fare clic sulla scheda **Ispezioni**. (1)Fare clic su **Add**. (2)Fare clic sul pulsante di opzione **Più corrispondenze** e scegliere la classe di traffico dall'elenco a discesa. (3)Scegliere l'azione di ripristino desiderata da abilitare o disabilitare. In questo esempio viene attivata la reimpostazione della connessione FTP per tutti i siti FTP *non corrispondenti ai* siti specificati. (4)Fare clic su **OK**, fare di nuovo clic su **OK** e quindi su **Applica**. (5)

6. **Applicare il criterio FTP di ispezione all'elenco di ispezione globale.**Scegliere **Configurazione > Firewall > Regole dei criteri di servizio**.Sul lato destro, selezionare il criterio **selection_default** e fare clic su **Modifica**.Nella scheda Azioni regola (1), fare clic sul pulsante **Configura** per FTP. (2)Nella finestra di dialogo Seleziona mappa di ispezione FTP, selezionare la casella di controllo **Usa FTP rigido**, quindi fare clic sul pulsante di opzione **FTP inspect map per un controllo preciso sull'ispezione**.Il nuovo criterio di ispezione FTP, *FTP_INSPECT_POLICY*, dovrebbe essere visibile nell'elenco.Fare clic su **OK**, fare di nuovo clic su **OK** e quindi su **Applica**.



Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

- **show running-config regex**: visualizza le espressioni regolari configurate.
  ```
  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**: visualizza le mappe di classe configurate.

```
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**: visualizza le mappe dei criteri che ispezionano il traffico HTTP configurato.

```
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**: visualizza tutte le configurazioni della mappa dei criteri e la configurazione predefinita.

```
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**: visualizza tutte le configurazioni dei criteri del servizio attualmente in esecuzione.

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

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Èpossibile utilizzare il comando **show service-policy** per verificare che il motore di ispezione controlli il traffico e li autorizzi o li scarti correttamente.

```
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
```

Informazioni correlate

- ASA/PIX 8.x: Esempio di blocco di determinati siti Web (URL) mediante espressioni regolari con configurazione MPF
- PIX/ASA 7.x e versioni successive: Blocca il traffico peer-to-peer (P2P) e di messaggistica immediata (IM) utilizzando un esempio di configurazione MPF
- PIX/ASA 7.x: Esempio di configurazione dell'abilitazione dei servizi FTP/TFTP
- Applicazione dell'ispezione del protocollo a livello di applicazione
- Appliance Cisco ASA serie 5500 Adaptive Security - Supporto
- Cisco Adaptive Security Device Manager (ASDM)
- Cisco PIX serie 500 Security Appliance - Supporto
- Software Cisco PIX Firewall - Supporto
- Riferimenti per i comandi di Cisco PIX Firewall