

# Cisco IOS ファイアウォールを使用して SMTP および ESMTP 接続を検査するための設定例

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[設定](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

## 概要

このドキュメントは、Cisco IOS で Cisco IOS® ファイアウォールを着信シンプル メール転送プロトコル (SMTP) 接続または拡張 SMTP (ESMTP) を検査するための設定例を示します。この検査は、Cisco PIX 500 シリーズ セキュリティ アプライアンスの MailGuard 機能に似ています。

## 前提条件

### 要件

このドキュメントに特有の要件はありません。

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco IOS ソフトウェア リリース 12.3(4)T 以降
- Cisco 3640 ルータ

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ました。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。対象のネットワークが稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

## 表記法

ドキュメント表記の詳細については、『[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

SMTP 検査では、SMTP コマンドが違法なコマンドであるかどうか調べられます。違法なコマンドが含まれているパケットはパターン「xxxx」に変換され、サーバに転送されます。このプロセスによりサーバは否定応答を送信し、この否定応答によりクライアントは有効なコマンドを発行するようになります。無効な SMTP コマンドとは、次に示すコマンドを除くすべてのコマンドです。

• データ	• RCPT
• HELO	• RSET
• HELP	• SAML
• MAIL	• SEND
• NOOP	• SOML
• QUIT	• VRFY

ESMTP 検査は、SMTP 検査と同様の方法で行われます。違法なコマンドが含まれているパケットはパターン「xxxx」に変換され、サーバに転送されます。これにより、否定応答が返されます。無効な ESMTP コマンドとは、次に示すコマンドを除くすべてのコマンドです。

• AUTH	• NOOP
• データ	• QUIT
• EHLO	• RCPT
• ETRN	• RSET
• HELO	• SAML
• HELP	• SEND
• HELP	• SOML
• MAIL	• VRFY

ESMTP 検査では、より詳細なコマンド検査により次の拡張も調べられます。

- メッセージ サイズ宣言 ( SIZE )
- リモート キュー処理宣言 ( ETRN )
- バイナリ MIME ( BINARYMIME )
- コマンド パイプライン
- [Authentication]
- 配信ステータス通知 ( DSN )
- 拡張ステータスコード ( ENHANCEDSTATUSCODE )
- 8 ビット MIMTransport ( 8BITMIME )

注： SMTP 検査と ESMTP 検査は同時に設定できません。両方を設定しようとする、エラーメッセージが出されます。

注： Cisco IOSソフトウェアリリース12.3(4)T以降では、Cisco IOS Firewallはトラフィックを許可するためのダイナミックアクセスリストエントリを作成しません。Cisco IOS ファイアウォールは、検査された接続のセキュリティを制御するため、セッション状態テーブルを維持します。

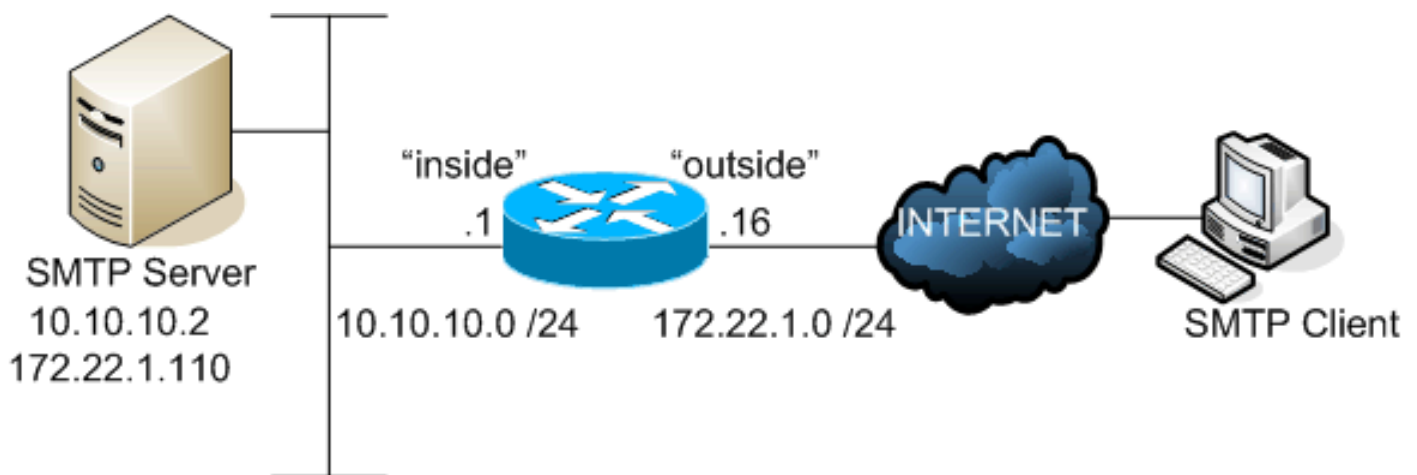
## 設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

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) を参照してください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことをご了承ください。

## 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 セットアップを使用します。



## 設定

このドキュメントでは、次の設定を使用しています。

### 3640 Router

```
3640-123#show running-config
Building configuration...

Current configuration : 1432 bytes
!
version 12.3
service config
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname 3640-123
!
boot-start-marker
boot-end-marker
!
enable password 7 02050D4808095E731F
!
no aaa new-model
!
resource policy
!
voice-card 3
```

```

!
ip subnet-zero
!
!
ip cef
no ip dhcp use vrf connected
!
!
!--- This is the Cisco IOS Firewall configuration. !---
IN-OUT is the inspection rule for traffic that flows !--
- from the inside interface of the router to the outside
interface. ip inspect name IN-OUT tcp ip inspect name
IN-OUT udp ip inspect name IN-OUT ftp ip inspect name
IN-OUT http ip inspect name IN-OUT icmp !--- OUT-IN is
the inspection rule for traffic that flows !--- from the
outside interface of the router to the inside interface.
!--- This rule is where SMTP/ESMTP inspection is
specified. ip inspect name OUT-IN smtp ! no ip ips deny-
action ips-interface ! no ftp-server write-enable ! ! !
! controller T1 3/0 framing sf linecode ami ! ! ! ! ! !-
-- The outside interface. interface Ethernet2/0 ip
address 172.22.1.16 255.255.255.0 !--- Apply the access
list to permit SMTP/ESMTP connections !--- to the mail
server. This also allows Cisco IOS Firewall !--- to
inspect SMTP or ESMTP commands. ip access-group 101 in
ip nat outside !--- Apply the inspection rule OUT-IN
inbound on this interface. This is !--- the rule that
defines SMTP/ESMTP inspection. ip inspect OUT-IN in ip
virtual-reassembly half-duplex ! interface Serial2/0 no
ip address shutdown ! !--- The inside interface.
interface Ethernet2/1 ip address 10.10.10.1
255.255.255.0 ip nat inside !--- Apply the inspection
rule IN-OUT inbound on this interface. ip inspect IN-OUT
in ip virtual-reassembly half-duplex ! ip http server no
ip http secure-server ip classless ip route 0.0.0.0
0.0.0.0 172.22.1.1 ! ! !--- The static translation for
the mail server. ip nat inside source static 10.10.10.2
172.22.1.110 ip nat inside source static 10.10.10.5
172.22.1.111 ! !--- The access list to permit SMTP and
ESMTP to the mail server. !--- Cisco IOS Firewall
inspects permitted traffic. access-list 101 permit tcp
any host 172.22.1.110 eq smtp ! ! ! control-plane ! ! !
voice-port 1/0/0 ! voice-port 1/0/1 ! voice-port 1/1/0 !
voice-port 1/1/1 ! ! ! ! ! ! ! ! line con 0 line aux 0
line vty 0 4 password 7 121A0C0411045D5679 login ! ! end

```

## 確認

ここでは、設定が正常に機能しているかどうかを確認します。

[アウトプット インタープリタ ツール \( 登録ユーザ専用 \) \( OIT \)](#) は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

- **show ip inspect all** : Cisco IOS ファイアウォール検査ルールとインターフェイスへのこのルールの適用の設定を検証します。

```

3640-123#show ip inspect all
Session audit trail is disabled
Session alert is enabled
one-minute (sampling period) thresholds are [400:500] connections
max-incomplete sessions thresholds are [400:500]

```

```
max-incomplete tcp connections per host is 50. Block-time 0 minute.
tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec
tcp idle-time is 3600 sec -- udp idle-time is 30 sec
dns-timeout is 5 sec
```

#### Inspection Rule Configuration

```
Inspection name IN-OUT
```

```
tcp alert is on audit-trail is off timeout 3600
udp alert is on audit-trail is off timeout 30
ftp alert is on audit-trail is off timeout 3600
http alert is on audit-trail is off timeout 3600
icmp alert is on audit-trail is off timeout 10
```

```
Inspection name OUT-IN
```

```
smtp max-data 20000000 alert is on audit-trail is off timeout 3600
```

#### Interface Configuration

```
Interface Ethernet2/1
```

```
Inbound inspection rule is IN-OUT
```

```
tcp alert is on audit-trail is off timeout 3600
udp alert is on audit-trail is off timeout 30
ftp alert is on audit-trail is off timeout 3600
http alert is on audit-trail is off timeout 3600
icmp alert is on audit-trail is off timeout 10
```

```
Outgoing inspection rule is not set
```

```
Inbound access list is not set
```

```
Outgoing access list is not set
```

```
Interface Ethernet2/0
```

```
Inbound inspection rule is OUT-IN
```

```
smtp max-data 20000000 alert is on audit-trail is off timeout 3600
```

```
Outgoing inspection rule is not set
```

```
Inbound access list is 101
```

```
Outgoing access list is not set
```

- **debug ip inspect smtp** : Cisco IOS ファイアウォール SMTP 検査イベントに関するメッセージを表示します。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。

```
ausnml-3600-02#debug ip inspect smtp
```

```
INSPECT SMTP Inspection debugging is on
```

```
ausnml-3600-02#
```

```
*Oct 18 21:51:35.886: CBAC SMTP: reply_type OTHERS
```

```
*Oct 18 21:51:35.886: CBAC SMTP: OTHER REPLY - Reply len: 64, match_len:64,
```

```
reply_re_state:18
```

```
*Oct 18 21:51:35.886: CBAC SMTP: OTHER REPLY match id:13
```

```
*Oct 18 21:51:35.886: CBAC SMTP: OTHER REPLY match id:10
```

```
*Oct 18 21:51:35.886: CBAC SMTP: End Of Reply Line - index:0 ,len:64
```

```
!--- The client issues a command. *Oct 18 21:51:40.810: CBAC SMTP: VERB - Cmd len:1,
match_len:1, cmd_re_state:9 *Oct 18 21:51:40.994: CBAC SMTP: VERB - Cmd len:2, match_len:1,
cmd_re_state:24 *Oct 18 21:51:41.190: CBAC SMTP: VERB - Cmd len:3, match_len:1,
cmd_re_state:40 *Oct 18 21:51:41.390: CBAC SMTP: VERB - Cmd len:4, match_len:1,
cmd_re_state:56 *Oct 18 21:51:41.390: CBAC SMTP: VERB - match id:5 *Oct 18 21:51:42.046:
CBAC SMTP: CMD PARAM - Cmd len:5, match_len:1, cmd_re_state:7 *Oct 18 21:51:43.462: CBAC
SMTP: CMD PARAM - Cmd len:6, match_len:1, cmd_re_state:2 *Oct 18 21:51:43.594: CBAC SMTP:
CMD PARAM - Cmd len:7, match_len:1, cmd_re_state:2 *Oct 18 21:51:43.794: CBAC SMTP: CMD
PARAM - Cmd len:9, match_len:2, cmd_re_state:2 *Oct 18 21:51:43.994: CBAC SMTP: CMD PARAM -
Cmd len:10, match_len:1, cmd_re_state:2 *Oct 18 21:51:44.194: CBAC SMTP: CMD PARAM - Cmd
len:12, match_len:2, cmd_re_state:3 *Oct 18 21:51:44.194: CBAC SMTP: CMD PARAM - match id:6
*Oct 18 21:51:44.194: CBAC SMTP: End Of Command Line - index:1, len:12 !--- The server
replies. *Oct 18 21:51:44.198: CBAC SMTP: reply_type OTHERS *Oct 18 21:51:44.198: CBAC SMTP:
OTHER REPLY - Reply len: 11, match_len:11, reply_re_state:18 *Oct 18 21:51:44.198: CBAC
SMTP: OTHER REPLY match id:13 *Oct 18 21:51:44.198: CBAC SMTP: OTHER REPLY match id:10 *Oct
18 21:51:44.198: CBAC SMTP: End Of Reply Line - index:1 ,len:11 !--- The client issues a
command. *Oct 18 21:51:49.482: CBAC SMTP: VERB - Cmd len:1, match_len:1, cmd_re_state:3 *Oct
18 21:51:50.222: CBAC SMTP: VERB - Cmd len:2, match_len:1, cmd_re_state:15 *Oct 18
21:51:50.618: CBAC SMTP: VERB - Cmd len:3, match_len:1, cmd_re_state:31 *Oct 18
```

21:51:50.954: CBAC SMTP: VERB - Cmd len:4, match\_len:1, cmd\_re\_state:46 \*Oct 18  
21:51:50.954: CBAC SMTP: VERB - match id:15 \*Oct 18 21:51:51.642: CBAC SMTP: CMD PARAM - Cmd  
len:5, match\_len:1, cmd\_re\_state:7 \*Oct 18 21:51:51.914: CBAC SMTP: CMD PARAM - Cmd len:6,  
match\_len:1, cmd\_re\_state:2 \*Oct 18 21:51:52.106: CBAC SMTP: CMD PARAM - Cmd len:7,  
match\_len:1, cmd\_re\_state:2 \*Oct 18 21:51:54.754: CBAC SMTP: CMD PARAM - Cmd len:8,  
match\_len:1, cmd\_re\_state:4 \*Oct 18 21:51:55.098: CBAC SMTP: CMD PARAM - Cmd len:9,  
match\_len:1, cmd\_re\_state:2 \*Oct 18 21:51:55.322: CBAC SMTP: CMD PARAM - Cmd len:11,  
match\_len:2, cmd\_re\_state:3 \*Oct 18 21:51:55.322: CBAC SMTP: CMD PARAM - match id:6 \*Oct 18  
21:51:55.322: CBAC SMTP: End Of Command Line - index:2, len:11 *!--- The server replies.* \*Oct  
18 21:51:55.326: CBAC SMTP: reply\_type OTHERS \*Oct 18 21:51:55.326: CBAC SMTP: OTHER REPLY -  
Reply len: 19, match\_len:19, reply\_re\_state:3 \*Oct 18 21:51:55.326: CBAC SMTP: OTHER REPLY  
match id:13 \*Oct 18 21:51:55.326: CBAC SMTP: End Of Reply Line - index:2 ,len:19 \*Oct 18  
21:51:57.070: CBAC SMTP: VERB - Cmd len:1, match\_len:1, cmd\_re\_state:3 \*Oct 18 21:51:57.402:  
CBAC SMTP: VERB - Cmd len:2, match\_len:1, cmd\_re\_state:15 \*Oct 18 21:51:58.162: CBAC SMTP:  
VERB - Cmd len:3, match\_len:1, cmd\_re\_state:31 \*Oct 18 21:51:58.462: CBAC SMTP: VERB - Cmd  
len:4, match\_len:1, cmd\_re\_state:46 \*Oct 18 21:51:58.466: CBAC SMTP: VERB - match id:15 \*Oct  
18 21:51:58.746: CBAC SMTP: CMD PARAM - Cmd len:5, match\_len:1, cmd\_re\_state:7 \*Oct 18  
21:51:59.006: CBAC SMTP: CMD PARAM - Cmd len:6, match\_len:1, cmd\_re\_state:2 \*Oct 18  
21:51:59.234: CBAC SMTP: CMD PARAM - Cmd len:7, match\_len:1, cmd\_re\_state:2 \*Oct 18  
21:51:59.418: CBAC SMTP: CMD PARAM - Cmd len:9, match\_len:2, cmd\_re\_state:2 \*Oct 18  
21:51:59.618: CBAC SMTP: CMD PARAM - Cmd len:10, match\_len:1, cmd\_re\_state:2 \*Oct 18  
21:51:59.818: CBAC SMTP: CMD PARAM - Cmd len:12, match\_len:2, cmd\_re\_state:3 \*Oct 18  
21:51:59.818: CBAC SMTP: CMD PARAM - match id:6 \*Oct 18 21:51:59.818: CBAC SMTP: End Of  
Command Line - index:3, len:12 \*Oct 18 21:51:59.818: CBAC SMTP: reply\_type OTHERS \*Oct 18  
21:51:59.818: CBAC SMTP: OTHER REPLY - Reply len: 19, match\_len:19, reply\_re\_state:3 \*Oct 18  
21:51:59.822: CBAC SMTP: OTHER REPLY match id:13 \*Oct 18 21:51:59.822: CBAC SMTP: End Of  
Reply Line - index:3 ,len:19 \*Oct 18 21:52:04.974: CBAC SMTP: VERB - Cmd len:1, match\_len:1,  
cmd\_re\_state:9 \*Oct 18 21:52:05.170: CBAC SMTP: VERB - Cmd len:2, match\_len:1,  
cmd\_re\_state:24 \*Oct 18 21:52:05.326: CBAC SMTP: VERB - Cmd len:3, match\_len:1,  
cmd\_re\_state:40 \*Oct 18 21:52:05.526: CBAC SMTP: VERB - Cmd len:4, match\_len:1,  
cmd\_re\_state:55 \*Oct 18 21:52:05.526: CBAC SMTP: VERB - match id:6 \*Oct 18 21:52:05.742:  
CBAC SMTP: CMD PARAM - Cmd len:6, match\_len:2, cmd\_re\_state:3 \*Oct 18 21:52:05.742: CBAC  
SMTP: CMD PARAM - match id:6 \*Oct 18 21:52:05.742: CBAC SMTP: End Of Command Line - index:4,  
len:6 \*Oct 18 21:52:05.746: CBAC SMTP: reply\_type OTHERS \*Oct 18 21:52:05.746: CBAC SMTP:  
OTHER REPLY - Reply len: 54, match\_len:54, reply\_re\_state:3 \*Oct 18 21:52:05.746: CBAC SMTP:  
OTHER REPLY match id:13 \*Oct 18 21:52:05.746: CBAC SMTP: End Of Reply Line - index:4 ,len:54  
\*Oct 18 21:52:05.746: CBAC SMTP: reply\_type OTHERS \*Oct 18 21:52:05.746: CBAC SMTP: OTHER  
REPLY - Reply len: 15, match\_len:15, reply\_re\_state:3 \*Oct 18 21:52:05.746: CBAC SMTP: OTHER  
REPLY match id:13 \*Oct 18 21:52:05.746: CBAC SMTP: End Of Reply Line - index:5 ,len:15 \*Oct  
18 21:52:05.746: CBAC SMTP: reply\_type OTHERS \*Oct 18 21:52:05.746: CBAC SMTP: OTHER REPLY -  
Reply len: 15, match\_len:15, reply\_re\_state:3 \*Oct 18 21:52:05.746: CBAC SMTP: OTHER REPLY  
match id:13 \*Oct 18 21:52:05.746: CBAC SMTP: End Of Reply Line - index:6 ,len:15 \*Oct 18  
21:52:05.746: CBAC SMTP: reply\_type OTHERS \*Oct 18 21:52:05.750: CBAC SMTP: OTHER REPLY -  
Reply len: 6, match\_len:6, reply\_re\_state:3 \*Oct 18 21:52:05.750: CBAC SMTP: OTHER REPLY  
match id:13 \*Oct 18 21:52:05.750: CBAC SMTP: End Of Reply Line - index:7 ,len:6 \*Oct 18  
21:52:05.750: CBAC SMTP: reply\_type OTHERS \*Oct 18 21:52:05.750: CBAC SMTP: OTHER REPLY -  
Reply len: 19, match\_len:19, reply\_re\_state:3 \*Oct 18 21:52:05.750: CBAC SMTP: OTHER REPLY  
match id:13 \*Oct 18 21:52:05.750: CBAC SMTP: End Of Reply Line - index:8 ,len:19 \*Oct 18  
21:52:05.750: CBAC SMTP: reply\_type OTHERS \*Oct 18 21:52:05.750: CBAC SMTP: OTHER REPLY -  
Reply len: 17, match\_len:17, reply\_re\_state:3 \*Oct 18 21:52:05.750: CBAC SMTP: OTHER REPLY  
match id:13 \*Oct 18 21:52:05.750: CBAC SMTP: End Of Reply Line - index:9 ,len:17 \*Oct 18  
21:52:05.750: CBAC SMTP: reply\_type OTHERS \*Oct 18 21:52:05.750: CBAC SMTP: OTHER REPLY -  
Reply len: 6, match\_len:6, reply\_re\_state:3 \*Oct 18 21:52:05.750: CBAC SMTP: OTHER REPLY  
match id:13 \*Oct 18 21:52:05.754: CBAC SMTP: End Of Reply Line - index:10 ,len:6 \*Oct 18  
21:52:05.754: CBAC SMTP: reply\_type OTHERS \*Oct 18 21:52:05.754: CBAC SMTP: OTHER REPLY -  
Reply len: 6, match\_len:6, reply\_re\_state:3 \*Oct 18 21:52:05.754: CBAC SMTP: OTHER REPLY  
match id:13 \*Oct 18 21:52:05.754: CBAC SMTP: End Of Reply Line - index:11 ,len:6 \*Oct 18  
21:52:05.754: CBAC SMTP: reply\_type OTHERS \*Oct 18 21:52:05.754: CBAC SMTP: OTHER REPLY -  
Reply len: 6, match\_len:6, reply\_re\_state:3 \*Oct 18 21:52:05.754: CBAC SMTP: OTHER REPLY  
match id:13 \*Oct 18 21:52:05.754: CBAC SMTP: End Of Reply Line - index:12 ,len:6 \*Oct 18  
21:52:05.754: CBAC SMTP: reply\_type OTHERS \*Oct 18 21:52:05.754: CBAC SMTP: OTHER REPLY -  
Reply len: 3, match\_len:3, reply\_re\_state:3 \*Oct 18 21:52:05.754: CBAC SMTP: OTHER REPLY  
match id:13 \*Oct 18 21:52:05.754: CBAC SMTP: End Of Reply Line - index:13 ,len:3 \*Oct 18  
21:52:15.646: CBAC SMTP: VERB - Cmd len:1, match\_len:1, cmd\_re\_state:6 \*Oct 18 21:52:15.838:

```
CBAC SMTP: VERB - Cmd len:3, match_len:2, cmd_re_state:37 *Oct 18 21:52:16.206: CBAC SMTP:
VERB - Cmd len:4, match_len:1, cmd_re_state:52 *Oct 18 21:52:16.206: CBAC SMTP: VERB - match
id:9 *Oct 18 21:52:18.954: CBAC SMTP: CMD PARAM - Cmd len:6, match_len:2, cmd_re_state:3
*Oct 18 21:52:18.958: CBAC SMTP: CMD PARAM - match id:6 *Oct 18 21:52:18.958: CBAC SMTP: End
Of Command Line - index:5, len:6 *Oct 18 21:52:18.958: CBAC SMTP: reply_type OTHERS *Oct 18
21:52:18.958: CBAC SMTP: OTHER REPLY - Reply len: 21, match_len:21, reply_re_state:18 *Oct
18 21:52:18.958: CBAC SMTP: OTHER REPLY match id:13 *Oct 18 21:52:18.958: CBAC SMTP: OTHER
REPLY match id:10 *Oct 18 21:52:18.958: CBAC SMTP: End Of Reply Line - index:14 ,len:21
```

## トラブルシューティング

現在、この設定に関する特定のトラブルシューティング情報はありません。

## 関連情報

- [Cisco IOS ファイアウォール フィーチャ セットに関する FAQ](#)
- [IOS ファイアウォールのサポート ページ](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)