

Exemple de configuration de l'inspection des connexions SMTP et ESMTP avec le pare-feu Cisco IOS

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Informations générales](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configurations](#)

[Vérification](#)

[Dépannage](#)

[Informations connexes](#)

[Introduction](#)

Ce document propose un exemple de configuration pour l'inspection des connexions entrantes du protocole SMTP ou du protocole ESMTP à l'aide du pare-feu Cisco IOS® dans Cisco IOS. Une telle inspection est semblable à la fonction MailGuard que l'on trouve dans les dispositifs de sécurité de la gamme Cisco PIX 500.

[Conditions préalables](#)

[Conditions requises](#)

Aucune spécification déterminée n'est requise pour ce document.

[Components Used](#)

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Logiciel Cisco IOS Version 12.3(4)T ou ultérieure
- Routeur Cisco 3640

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is

live, make sure that you understand the potential impact of any command.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

Informations générales

L'inspection SMTP entraîne l'inspection des commandes SMTP pour détecter les commandes illégales. Les paquets avec des commandes illégales sont modifiés en un modèle de xxxx et transférés au serveur. Ce processus entraîne l'envoi par le serveur d'une réponse négative, ce qui force le client à émettre une commande valide. Une commande SMTP illégale est une commande, à l'exception de ces commandes :

<ul style="list-style-type: none">• DONNÉES• HELO• AIDE• COURRIER• NOM• QUITTER	<ul style="list-style-type: none">• RCPT• RSET• SAML• ENVOYER• SOMME• VRFY
--	---

L'inspection ESMTP fonctionne de la même manière que l'inspection SMTP. Les paquets avec des commandes illégales sont modifiés en modèle « xxxx » et transférés au serveur, ce qui déclenche une réponse négative. Une commande ESMTP illégale est une commande, à l'exception de ces commandes :

<ul style="list-style-type: none">• AUTORITÉ• DONNÉES• EHLO• ETRN• HELO• AIDE• AIDE• COURRIER	<ul style="list-style-type: none">• NOM• QUITTER• RCPT• RSET• SAML• ENVOYER• SOMME• VRFY
--	---

L'inspection ESMTP examine également ces extensions via une inspection plus approfondie des commandes :

- Déclaration de taille de message (TAILLE)
- Déclaration de traitement de la file d'attente distante (ETRN)
- MIME binaire (BINARYMIME)
- Pipeline de commande
- Authentification
- Notification d'état de livraison (DSN)
- Code d'état amélioré (ENHANCEDSTATUSCODE)
- MIMÉtransport 8 bits (8 BITMIME)

Remarque : l'inspection SMTP et ESMTP ne peut pas être configurée simultanément. Une

tentative de configuration des deux résultats génère un message d'erreur.

Remarque : Dans le logiciel Cisco IOS Version 12.3(4)T et ultérieure, le pare-feu Cisco IOS ne crée plus d'entrées dynamiques de liste d'accès pour autoriser le trafic. Le pare-feu Cisco IOS gère désormais une table d'état de session pour contrôler la sécurité des connexions inspectées.

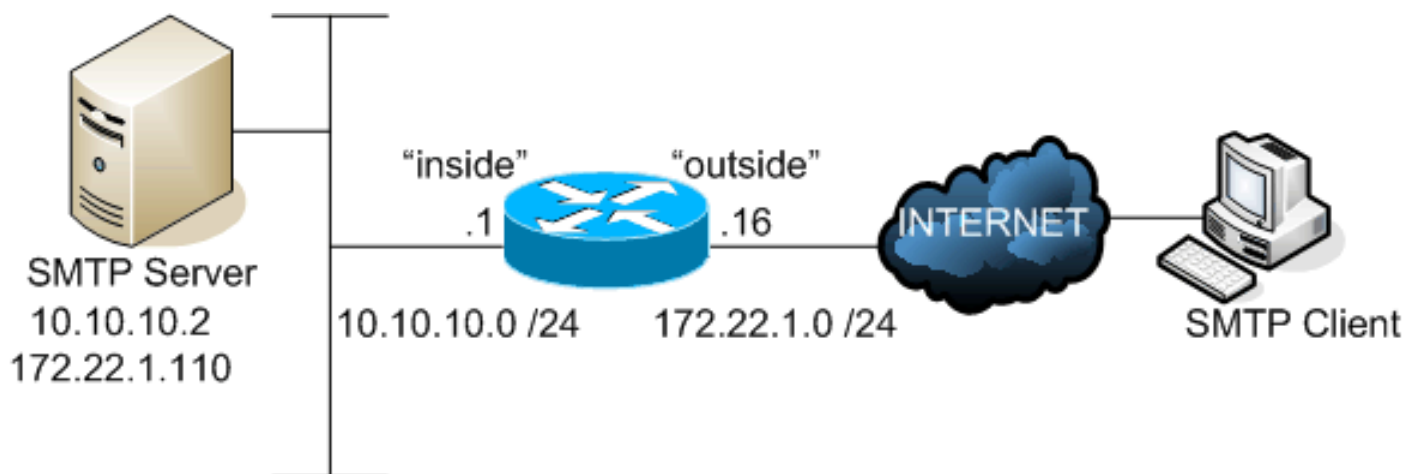
Configuration

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque : utilisez l'[outil de recherche de commandes](#) (clients [enregistrés](#) uniquement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configurations

Ce document utilise la configuration suivante :

Routeur 3640

```
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

```

Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'[Outil Interpréteur de sortie \(clients enregistrés uniquement\) \(OIT\)](#) prend en charge certaines commandes `show`. Utilisez l'OIT pour afficher une analyse de la sortie de la commande `show`.

- **show ip inspect all** - Vérifie la configuration des règles d'inspection du pare-feu Cisco IOS et leur application aux interfaces.

```
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** - Affiche les messages relatifs aux événements d'inspection SMTP du pare-feu Cisco IOS. **Remarque :** Consulter les [renseignements importants sur les commandes de débogage](#) avant d'utiliser les commandes de débogage.

```
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
```

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- [Jeu de fonctions Cisco IOS Firewall - Forum aux questions](#)
- [Page de support pour le pare-feu d'IOS](#)
- [Support et documentation techniques - Cisco Systems](#)