

ASA 8.3 以降：内部ネットワーク上のメール (SMTP) サーバ アクセスの設定例

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[設定](#)

[ネットワーク図](#)

[設定](#)

[ESMTP TLS の設定](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

概要

この設定例は、内部ネットワークに配置されたメール (SMTP) サーバにアクセスするために ASA セキュリティ アプライアンスを設定する方法を示します。

バージョン 8.3 以降の Cisco Adaptive Security Appliance (ASA) での ASDM を使用した同等な設定の詳細について『[ASA 8.3.x 以降：DMZ でのメール \(SMTP\) サーバ アクセスの設定例](#)』には、ASA セキュリティ アプライアンスをセットアップして、DMZ ネットワークにあるメール /SMTP サーバにアクセスする方法についての詳細が記載されています。

バージョン 8.3 以降の Cisco Adaptive Security Appliance (ASA) での ASDM を使用した同等な設定の詳細について『[ASA 8.3.x 以降：外部ネットワーク上のメール \(SMTP\) サーバ アクセスの設定例](#)』には、ASA セキュリティ アプライアンスをセットアップして、外部ネットワークにあるメール /SMTP サーバにアクセスする方法が記載されています。

Cisco PIX セキュリティ アプライアンス ソフトウェア バージョン 7.x または Cisco 適応型セキュリティ アプライアンス (ASA) で、Open Shortest Path First (OSPF) を使用して GRE トンネルのない VPN/IPsec を設定する方法の詳細については、[PIX/ASA 7.x 以降：内部ネットワーク上のメール \(SMTP\) サーバ アクセスの設定例](#)』には、バージョン 8.2 以前が稼働する Cisco 適応型セキュリティ アプライアンス (ASA) での同等の設定の詳細が記載されています。

前提条件

要件

このドキュメントに関する固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くものです。

- バージョン 8.3 以降が稼働する Cisco 適応型セキュリティ アプライアンス (ASA)
- Cisco 1841 ルータ (Cisco IOS[®] Software Release 12.4(20)T 搭載)

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。

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。

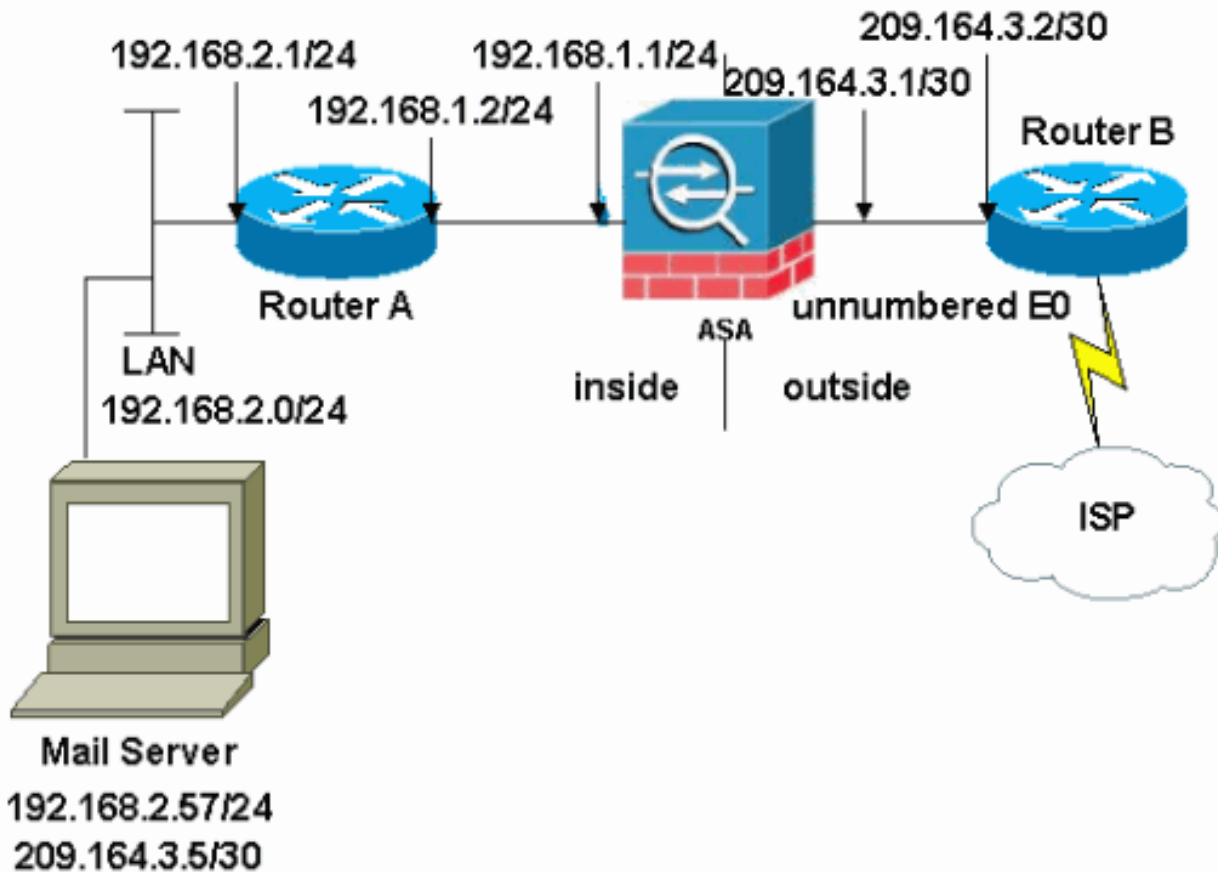
設定

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。



注: この設定で使用している IP アドレススキームは、インターネット上で正式にルーティング可能なものではありません。これらは [RFC 1918](#) で、ラボ環境で使用されたアドレスです。

この例で使用しているネットワーク構成の ASA には、内部ネットワーク (192.168.1.0/24) と外部ネットワーク (209.164.3.0/30) があります。IP アドレス 209.64.3.5 のメールサーバは内部ネットワークに配置されています。

設定

このドキュメントでは、次の設定を使用します。

- [ASA](#)
- [ルータ B](#)

```

ASA
ASA#show run : Saved : ASA Version 8.3(1) ! hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted passwd
2KFQnbNIdI.2KYOU encrypted names ! interface Ethernet0
shutdown no nameif no security-level no ip address !
interface Ethernet1 shutdown no nameif no security-level
no ip address ! interface Ethernet2 shutdown no nameif
no security-level no ip address ! !--- Define the IP
address for the inside interface. interface Ethernet3
nameif inside security-level 100 ip address 192.168.1.1
255.255.255.0 ! !--- Define the IP address for the
outside interface. interface Ethernet4 nameif outside
security-level 0 ip address 209.164.3.1 255.255.255.252
! interface Ethernet5 shutdown no nameif no security-
level no ip address ! passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive !--- Create an access list that permits

```

```

Simple !--- Mail Transfer Protocol (SMTP) traffic from
anywhere !--- to the host at 209.164.3.5 (our server).
The name of this list is !--- smtp. Add additional lines
to this access list as required. !--- Note: There is one
and only one access list allowed per !--- interface per
direction, for example, inbound on the outside
interface. !--- Because of limitation, any additional
lines that need placement in !--- the access list need
to be specified here. If the server !--- in question is
not SMTP, replace the occurrences of SMTP with !--- www,
DNS, POP3, or whatever else is required. access-list
smtp extended permit tcp any host 209.164.3.5 eq smtp
pager lines 24 mtu inside 1500 mtu outside 1500 no
failover no asdm history enable arp timeout 14400 !---
Specify that any traffic that originates inside from the
!--- 192.168.2.x network NATs (PAT) to 209.164.3.129 if
!--- such traffic passes through the outside interface.
object network obj-192.168.2.0 subnet 192.168.2.0
255.255.255.0 nat (inside,outside) dynamic 209.164.3.129
!--- Define a static translation between 192.168.2.57 on
the inside and !--- 209.164.3.5 on the outside. These
are the addresses to be used by !--- the server located
inside the ASA. object network obj-192.168.2.57 host
192.168.2.57 nat (inside,outside) static 209.164.3.5 !--
- Apply the access list named smtp inbound on the
outside interface. access-group smtp in interface
outside !--- Instruct the ASA to hand any traffic
destined for 192.168.x.x !--- to the router at
192.168.1.2. route inside 192.168.0.0 255.255.0.0
192.168.1.2 1 !--- Set the default route to 209.164.3.2.
!--- The ASA assumes that this address is a router
address. route outside 0.0.0.0 0.0.0.0 209.164.3.2 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 timeout mgcp-pat
0:05:00 sip 0:30:00 sip_media 0:02:00 timeout uauth
0:05:00 absolute no snmp-server location no snmp-server
contact snmp-server enable traps snmp authentication
linkup linkdown coldstart telnet timeout 5 ssh timeout 5
console timeout 0 ! class-map inspection_default match
default-inspection-traffic ! ! !--- SMTP/ESMTP is
inspected as "inspect esmtp" is included in the map.
policy-map global_policy class inspection_default
inspect dns maximum-length 512 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 !
!--- SMTP/ESMTP is inspected as "inspect esmtp" is
included in the map. service-policy global_policy global
Cryptochecksum:f96eaf0268573bd1af005e1db9391284 : end

```

ルータ B

Current configuration:

```

!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 2522-R5
!
enable secret 5 $1$N0F3$XE2aJhJlCbLWYloDwNvcV.
!
ip subnet-zero

```

```
!  
!  
!  
!  
!  
interface Ethernet0  
  
!--- Sets the IP address of the Ethernet interface to  
209.164.3.2. ip address 209.164.3.2 255.255.255.252 !  
interface Serial0 !--- Instructs the serial interface to  
use !--- the address of the Ethernet interface when the  
need arises. ip unnumbered ethernet 0 ! interface  
Serial11 no ip address no ip directed-broadcast ! ip  
classless !--- Instructs the router to send all traffic  
!--- destined for 209.164.3.x to 209.164.3.1. ip route  
209.164.3.0 255.255.255.0 209.164.3.1 !--- Instructs the  
router to send !--- all other remote traffic out serial  
0. ip route 0.0.0.0 0.0.0.0 serial 0 ! ! line con 0  
transport input none line aux 0 autoselect during-login  
line vty 0 4 exec-timeout 5 0 password ww login ! end
```

注: ルータ A の設定は追加されません。必要な手順は、インターフェイスに IP アドレスを指定し、ASA の内部インターフェイスである 192.168.1.1 にデフォルト ゲートウェイを設定することだけです。

ESMTP TLS の設定

注: 電子メール通信で Transport Layer Security (TLS) 暗号化を使用している場合、ASA の ESMTP 検査機能 (デフォルトで有効) によってパケットが廃棄されます。TLS が有効な電子メールを許可するには、次の出力に示すように ESMTP 検査機能を無効にします。詳細は、Cisco Bug ID [CSCtn08326](#) ([登録ユーザ専用](#)) を参照してください。

```
ciscoasa(config)#policy-map global\_policy ciscoasa(config-pmap)#class inspection\_default  
ciscoasa(config-pmap-c)#no inspect esmtp ciscoasa(config-pmap-c)#exit ciscoasa(config-pmap)#exit
```

注: ASA バージョン 8.0.3 以降では、以下に示すように、**allow-tls** コマンドを使用して、inspect esmtp を有効にした TLS 電子メールを許可することができます。

```
policy-map type inspect esmtp tls-esmtp  
parameters  
allow-tls  
inspect esmtp tls-esmtp
```

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

[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せん。OIT を使用して、**show** コマンド出力の解析を表示できます。

[logging buffered 7](#) コマンドで、メッセージが ASA コンソールに転送されます。メール サーバへの接続に問題がある場合は、コンソール デバッグ メッセージを調べて、送信側と受信側のステーションの IP アドレスを見つけ、問題を特定します。

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](#)
- [Requests for Comments \(RFC \)](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)