

# ASA 8.3 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

## 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

この設定例は方法で情報を外部ネットワークにあるメールサーバにアクセスのための ( ASA ) 適応型セキュリティ アプライアンス ( ASA ) ソフトウェア設定する提供します。

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：内部ネットワークにある mail/SMTP サーバにアクセスのための ASA セキュリティ アプライアンス モデルを設定するために \( 内部ネットワーク 設定例の SMTP \) サーバアクセスを郵送して下さい](#)』。

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： \( バージョン 8.2 および それ 以前との同一の構成のための外部ネットワーク 設定例の SMTP \) サーバアクセスを \( ASA \) 適応型セキュリティ アプライアンス \( ASA \) ソフトウェア on Cisco 郵送して下さい](#)。

## 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。

- Cisco 適応型セキュリティ アプライアンス (ASA) ソフトウェア (ASA) そのバージョン 8.3 および それ 以降を実行します
- Cisco 1841 ルータ (Cisco IOS<sup>®</sup> 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。

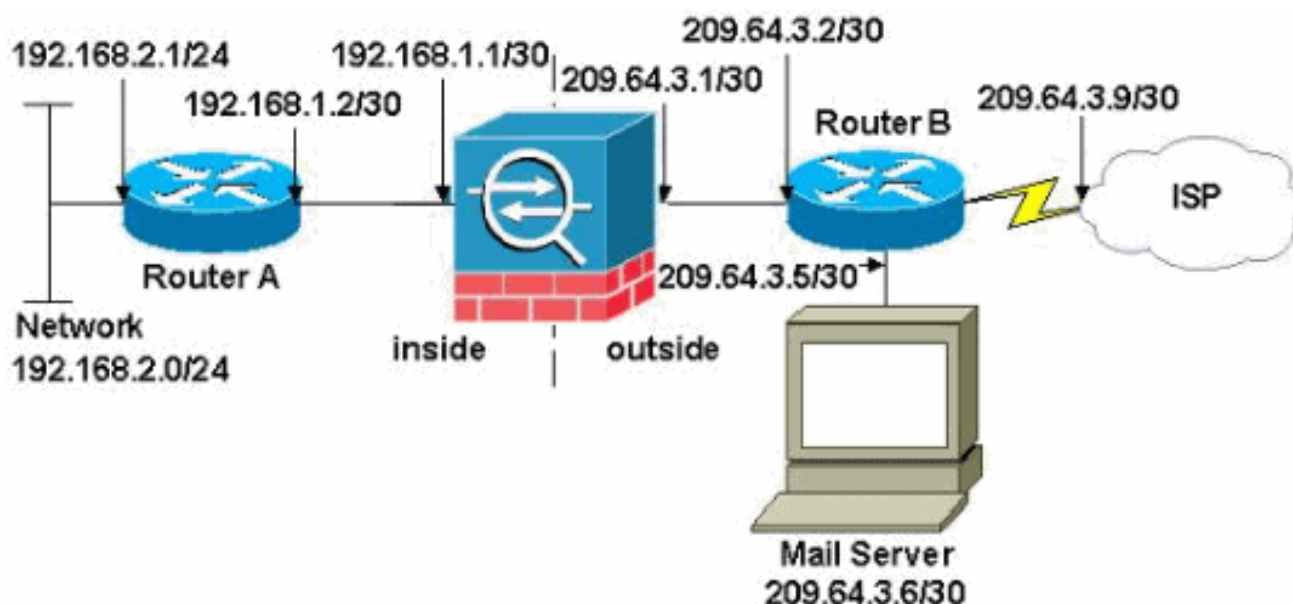
## 設定

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。

この例で使用されるネットワーク セットアップに内部ネットワーク ( 192.168.1.0/30 ) および外

部ネットワーク ( 209.64.3.0/30 ) が付いている ASA があります。IP アドレス 209.64.3.6 を持つメールサーバは外部ネットワークにいます。NAT 文をように内部インターフェイス ( Ethernet0 ) から outside インターフェイスに通じる 192.168.2.x ネットワークからのあらゆるトラフィック設定して下さい ( イーサネットは 209.64.3.253 によって 209.64.3.129 の範囲でアドレスに 1 ) 変換します。最後の利用可能なアドレス ( 209.64.3.254 ) ポートアドレス変換 ( PAT ) のために予約済みです。

## 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 A](#)
- [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 ! !--- Configure the
inside interface. ? interface Ethernet3 nameif inside
security-level 100 ip address 192.168.1.1
255.255.255.252 ! !--- Configure the outside interface.
interface Ethernet4 nameif outside security-level 0 ip
address 209.64.3.1 255.255.255.252 ! interface Ethernet5
shutdown no nameif no security-level no ip address !
passwd 2KFQnbNIdI.2KYOU encrypted boot system
disk0:/asa831-k8.bin ftp mode passive pager lines 24 mtu
inside 1500 mtu outside 1500 no failover no asdm history
enable arp timeout 14400 !--- This command states that
any traffic !--- from the 192.168.2.x network that
passes from the inside interface (Ethernet0) !--- to the
outside interface (Ethernet 1) translates into an
address !--- in the range of 209.64.3.129 through
209.64.3.253 and contains a subnet !--- mask of
255.255.255.128. object network obj-
209.64.3.129_209.64.3.253 range 209.64.3.129-
209.64.3.253 !--- This command reserves the last
available address (209.64.3.254) for !--- for Port
Address Translation (PAT). In the previous statement, !-
-- each address inside that requests a connection uses
one !--- of the addresses specified. If all of these
addresses are in use, !--- this statement provides a
failsafe to allow additional inside stations !--- to
establish connections. object network obj-209.64.3.254
host 209.64.3.254 !--- This command indicates that all
addresses in the 192.168.2.x range !--- that pass from
the inside (Ethernet0) to a corresponding global !---
designation are done with NAT. !--- As outbound traffic
is permitted by default on the ASA, no !--- static
commands are needed. object-group network nat-pat-group
network-object object obj-209.64.3.129_209.64.3.253
network-object object obj-209.64.3.254 object network
obj-192.168.2.0 subnet 192.168.2.0 255.255.255.0 nat
(inside,outside) dynamic nat-pat-group !--- Creates a
static route for the 192.168.2.x network with
```

```

192.168.1.2. !--- The ASA forwards packets with these
addresses to the router !--- at 192.168.1.2. route
inside 192.168.2.0 255.255.255.0 192.168.1.2 1 !--- Sets
the default route for the ASA Firewall at 209.64.3.2.
route outside 0.0.0.0 0.0.0.0 209.64.3.2 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
since "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 rsh inspect rtsp inspect esmtp inspect
sqlnet inspect skinny inspect sunrpc inspect xdmcp
inspect sip inspect netbios inspect tftp ! service-
policy global_policy global
Cryptochecksum:8a63de5ae2643c541a397c2de7901041 : end

```

## ルータ A

```

Current configuration:
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 2522-R4
!
enable secret 5 $1$N0F3$XE2aJhJlCbLWYloDwNvcV.
!
ip subnet-zero
!
!
!
!
!
interface Ethernet0

!--- Assigns an IP address to the inside Ethernet
interface. ip address 192.168.2.1 255.255.255.0 no ip
directed-broadcast ! interface Ethernet1 !--- Assigns an
IP address to the ASA-facing interface. ip address
192.168.1.2 255.255.255.252 no ip directed-broadcast !
interface Serial0 no ip address no ip directed-broadcast
shutdown ! interface Serial1 no ip address no ip
directed-broadcast shutdown ! ip classless !--- This
route instructs the inside router to forward all !---
non-local packets to the ASA. ip route 0.0.0.0 0.0.0.0
192.168.1.1 !! line con 0 transport input none line aux
0 autoselect during-login line vty 0 4 exec-timeout 5 0
password ww login ! end

```

## ルータ B

```

Current configuration:
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption

```

```
!  
hostname 2522-R4  
!  
enable secret 5 $1$N0F3$XE2aJhJlCbLWYloDwNvcV.  
!  
ip subnet-zero  
!  
!  
!  
!  
interface Ethernet0  
  
!--- Assigns an IP address to the ASA-facing Ethernet  
interface. ip address 209.64.3.2 255.255.255.252 no ip  
directed-broadcast ! interface Ethernet1 !--- Assigns an  
IP address to the server-facing Ethernet interface. ip  
address 209.64.3.5 255.255.255.252 no ip directed-  
broadcast ! interface Serial0 !--- Assigns an IP address  
to the Internet-facing interface. ip address 209.64.3.9  
255.255.255.252 no ip directed-broadcast no ip mroute-  
cache ! interface Serial1 no ip address no ip directed-  
broadcast ! ip classless !--- All non-local packets are  
to be sent out serial 0. In this case, !--- the IP  
address on the other end of the serial interface is not  
known, !--- or you can specify it here. ip route 0.0.0.0  
0.0.0.0 serial 0 ! !--- This statement is required to  
direct traffic destined to the !--- 209.64.3.128 network  
(the ASA global pool) to the ASA to be translated !---  
back to the inside addresses. ip route 209.64.3.128  
255.255.255.128 209.64.3.1 !! line con 0 transport  
input none line aux 0 autoselect during-login line vty 0  
4 exec-timeout 5 0 password ww login ! end
```

## 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
```

## 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す。 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](#)