# ASA 8.3 e versioni successive: Esempio di accesso al server di posta (SMTP) nella configurazione DMZ

## Sommario



## Introduzione

In questa configurazione di esempio viene illustrato come configurare l'appliance di sicurezza ASA per l'accesso a un server SMTP (Simple Mail Transfer Protocol) situato nella rete DMZ (Demilitarized Zone).

Fare riferimento alla versione ASA 8.3 e successive: Esempio di configurazione dell'accesso al server di posta (SMTP) sulla rete interna per ulteriori informazioni su come configurare l'appliance di sicurezza ASA per l'accesso a un server di posta/SMTP sulla rete interna.

Fare riferimento alla versione ASA 8.3 e successive: Esempio di configurazione dell'accesso al server di posta (SMTP) sulla rete esterna per ulteriori informazioni su come configurare l'appliance di sicurezza ASA per l'accesso a un server di posta/SMTP sulla rete esterna.

Fare riferimento a PIX/ASA 7.x e versioni successive: Accesso al server di posta (SMTP) sulla DMZ Esempio di configurazione identica su Cisco Adaptive Security Appliance (ASA) con versioni 8.2 e precedenti.

## Prerequisiti

### Requisiti

Nessun requisito specifico previsto per questo documento.

## Componenti usati

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

- Cisco Adaptive Security Appliance (ASA) con versione 8.3 e successive.
- Cisco 1841 Router con software Cisco IOS® versione 12.4(20)T

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.

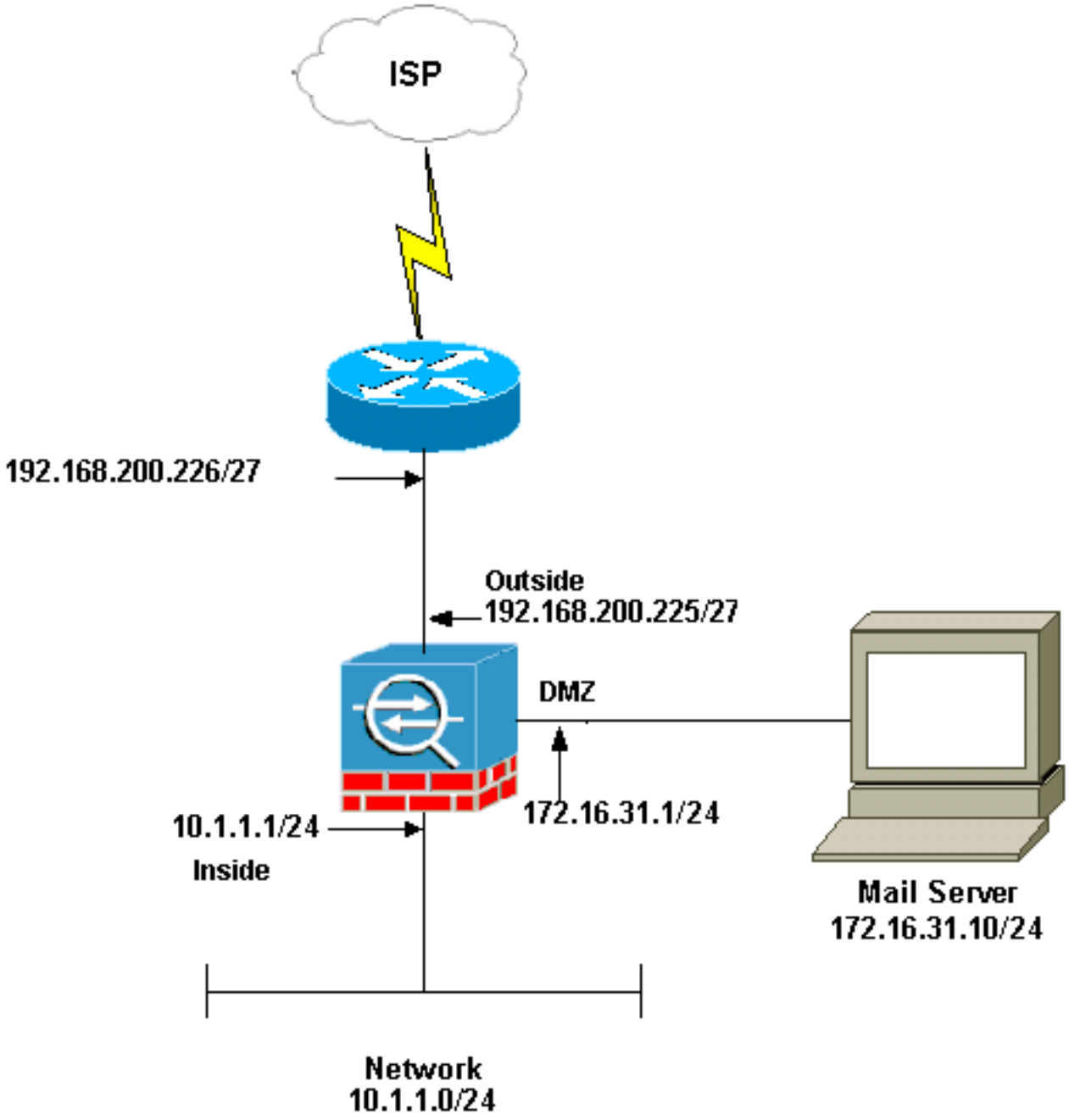
# Configurazione

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:** gli schemi di indirizzamento IP utilizzati in questa configurazione non sono legalmente instradabili su Internet. Si tratta degli indirizzi RFC 1918 utilizzati in un ambiente lab.

La configurazione della rete usata in questo esempio ha un'appliance ASA con rete interna (10.1.1.0/24) e rete esterna (192.168.200.0/27). Il server di posta con indirizzo IP 172.16.31.10 si trova nella rete DMZ (Demilitarized Zone). Per consentire l'accesso interno al server di posta, gli utenti configurano l'identità NAT. Configurare un elenco degli accessi, che in questo esempio è **dmz_int**, per consentire le connessioni SMTP in uscita dal server di posta agli host nella rete interna e associarlo all'interfaccia DMZ.

Analogamente, affinché gli utenti esterni possano accedere al server di posta, configurare un NAT statico e un elenco degli accessi, che nell'esempio riportato è **outside_int**, in modo da consentire agli utenti esterni di accedere al server di posta e associare l'elenco degli accessi all'interfaccia esterna.

## Configurazione ASA

Nel documento viene usata questa configurazione:

## Configurazione 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
 security-level 0
 no ip address
!
interface Ethernet1
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet2
 no nameif
 no security-level
 no ip address
!
!--- Configure the inside interface. interface Ethernet3
nameif inside security-level 100 ip address 10.1.1.1
255.255.255.0 ! !--- Configure the outside interface.
interface Ethernet4 nameif outside security-level 0 ip
address 192.168.200.225 255.255.255.224 ! !--- Configure
dmz interface. interface Ethernet5 nameif dmz security-
level 10 ip address 172.16.31.1 255.255.255.0 ! passwd
2KFQnbNIdI.2KYOU encrypted boot system disk0:/asa831-
k8.bin ftp mode passive !--- This access list allows
hosts to access !--- IP address 192.168.200.227 for the
SMTP port. access-list outside_int extended permit tcp
any host  192.168.200.227 eq smtp
!--- Allows outgoing SMTP connections. !--- This access
list allows host IP 172.16.31.10 !--- sourcing the SMTP
port to access any host. access-list dmz_int extended
permit tcp host 172.16.31.10 eq smtp any

pager lines 24
mtu BB 1500
mtu inside 1500
mtu outside 1500
mtu dmz 1500
no failover
no asdm history enable
arp timeout 14400


  object network obj-192.168.200.228-192.168.200.253
   range 192.168.200.228-192.168.200.253
 object network obj-192.168.200.254
   host 192.168.200.254
```

```
 object-group network nat-pat-group
   network-object object obj-192.168.200.228-
192.168.200.253
   network-object object obj-192.168.200.254

 object network obj-10.1.1.0
   subnet 10.1.1.0 255.255.255.0
   nat (inside,outside) dynamic nat-pat-group

!--- This network static does not use address
translation. !--- Inside hosts appear on the DMZ with
their own addresses. object network obj-10.1.1.0
   subnet 10.1.1.0 255.255.255.0
   nat (inside,dmz) static obj-10.1.1.0

!--- This network static uses address translation. !---
Hosts that access the mail server from the outside !---
use the 192.168.200.227 address. object network obj-
172.16.31.10
   host 172.16.31.10
   nat (dmz,outside) static 192.168.200.227
access-group outside_int in interface outside
access-group dmz_int in interface dmz
route outside 0.0.0.0 0.0.0.0  192.168.200.226 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
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
!
!--- The inspect esmtp command (included in the map)
allows !--- SMTP/ESMTP to inspect the application.


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
!
!--- The  inspect esmtp  command (included in the map)
```

```
allows !--- SMTP/ESMTP to inspect the application.

service-policy global_policy global
Cryptochecksum:2653ce2c9446fb244b410c2161a63eda
: end
[OK]
```

### Configurazione TLS ESMTP

**Nota:** se si usa la crittografia Transport Layer Security (TLS) per la comunicazione della posta elettronica, la funzione di ispezione ESMTP (abilitata per impostazione predefinita) nell'appliance ASA scarta i pacchetti. Per consentire i messaggi di posta elettronica con TLS abilitato, disabilitare la funzione di ispezione ESMTP come mostrato nell'output. per ulteriori informazioni, fare riferimento all'ID bug Cisco CSCtn08326 (solo utenti registrati).

```
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
```

## Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

## Risoluzione dei problemi

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

### Comandi per la risoluzione dei problemi

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

- debug icmp trace: visualizza se le richieste ICMP (Internet Control Message Protocol) provenienti dagli host raggiungono l'appliance ASA. Per eseguire il debug, è necessario aggiungere il comando **access-list** per autorizzare l'ICMP nella configurazione.**Nota:** per utilizzare questo comando di debug, verificare di consentire l'uso di ICMP nell'`access-list outside_int`, come mostrato di seguito:
  ```
  access-list outside_int extended permit tcp any host  192.168.200.227 eq smtp
  access-list outside_int extended permit icmp any any
  ```
- logging buffered 7: utilizzato in modalità di configurazione globale per consentire all'appliance adaptive security di inviare messaggi syslog al log buffer. Il contenuto del buffer di registro ASA è visibile con il comando show logging.

Per ulteriori informazioni su come configurare la registrazione, consultare il documento sulla configurazione del syslog con ASDM.

## Informazioni correlate

- Cisco ASA serie 5500 Adaptive Security Appliance
- RFC (Requests for Comments)
- Documentazione e supporto tecnico – Cisco Systems