ASA 8.3 et plus tard : Exemple de configuration de l'accès au serveur de messagerie (SMTP) sur un réseau externe

Contenu

Introduction

Cette configuration d'échantillon fournit des informations sur la façon dont installer l'appliance de sécurité adaptable (ASA) pour l'accès à un serveur de messagerie situé sur le réseau extérieur.

Référez-vous à ASA 8.3 et plus tard : Serveur Access de messagerie (SMTP) sur l'exemple de configuration DMZ pour plus d'informations sur la façon installer les dispositifs de sécurité ASA pour l'accès à un serveur mail/SMTP situé sur le réseau DMZ.

Référez-vous à ASA 8.3 et plus tard : De messagerie (SMTP) de serveur d'Access exemple de configuration réseau d'intérieur en fonction afin d'installer les dispositifs de sécurité ASA pour l'accès à un serveur mail/SMTP situé sur le réseau intérieur.

Consultez PIX/ASA 7.x et versions ultérieures : Accès de serveur de messagerie (SMTP) sur l'exemple extérieur de configuration réseau pour la configuration identique sur l'appliance de sécurité adaptable Cisco (ASA) avec des versions 8.2 et antérieures.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

- L'appliance de sécurité adaptable Cisco (ASA) cette exécute la version 8.3 et ultérieures
- Routeur de Cisco 1841 avec la version de logiciel 12.4(20)T de Cisco IOS®

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

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

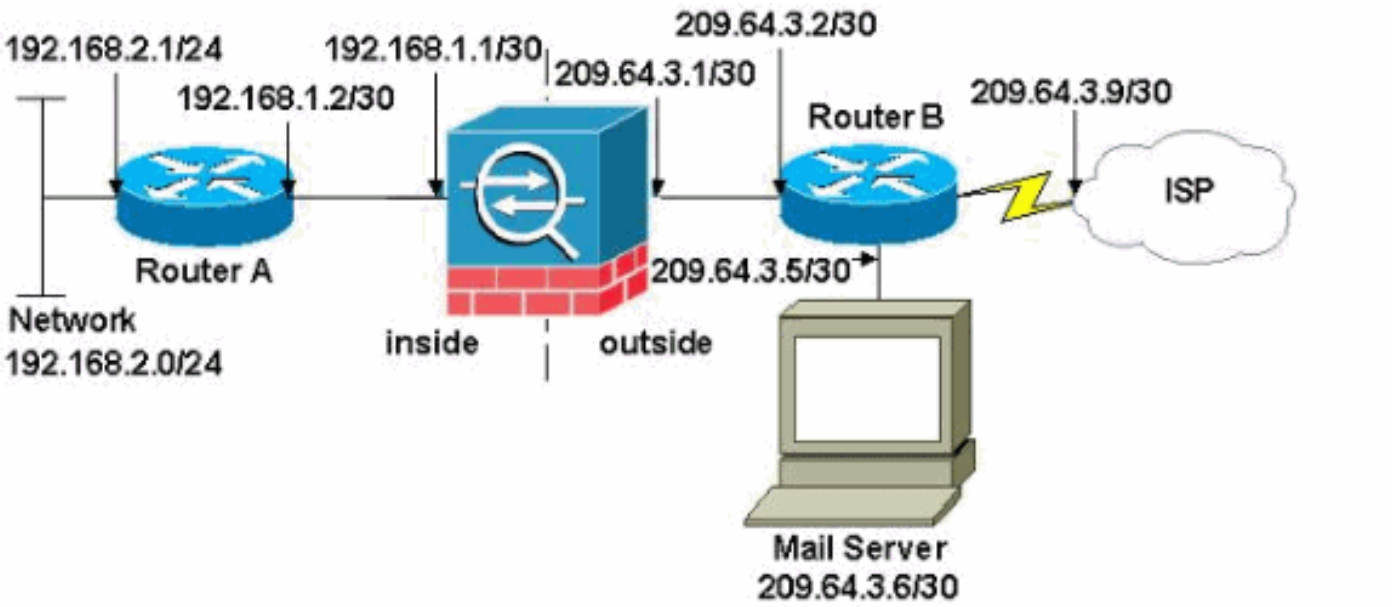
Configurez

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

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Remarque: Les schémas d'adressage d'IP utilisés dans cette configuration ne sont pas légalement routables sur Internet. Ce sont des adresses RFC 1918 qui ont été utilisées dans un environnement de laboratoire.

La configuration réseau utilisée dans cet exemple a l'ASA avec le réseau intérieur (192.168.1.0/30) et le réseau extérieur (209.64.3.0/30). Le serveur de messagerie avec l'adresse IP 209.64.3.6 se trouve dans le réseau extérieur. Configurez la déclaration NAT de sorte qu'en trafiquent du réseau 192.168.2.x qui passe de l'interface interne (Ethernet0) à l'interface extérieure (l'Ethernet 1) se traduit à une adresse de l'ordre de 209.64.3.129 par 209.64.3.253. La dernière adresse disponible (209.64.3.254) est réservée pour la translation d'adresses d'adresse du port (PAT).

Configurations

Ce document utilise les configurations suivantes :

- ASA
- routeur A
- routeur 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
```

routeur 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
```

routeur 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
```

Configuration de TLS ESMTP

Remarque: Si vous utilisez le cryptage de Transport Layer Security (TLS) pour la transmission de courrier électronique puis la caractéristique d'inspection ESMTP (activée par défaut) dans l'ASA relâche les paquets. Afin de permettre les courriers électroniques avec le TLS activé, désactivez la configuration d'inspection ESMTP comme cette sortie affiche. Référez-vous au pour en savoir plus de l'ID de bogue Cisco CSCtn08326 (clients enregistrés seulement).

```
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
```

Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannez

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** .

La commande du **logging buffered 7** dirige des messages vers la console ASA. Si la Connectivité au serveur de messagerie est un problème, examinez les messages de débogage de console pour localiser les adresses IP de l'envoi et des stations de réception afin de déterminer le

problème.

Informations connexes

- Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500
- Demandes de commentaires (RFC)
- Support et documentation techniques - Cisco Systems