ASA 8.3 et plus tard : Exemple de configuration de l'accès au serveur de messagerie (SMTP) sur la zone DMZ

Contenu

Introduction

Cette configuration d'échantillon explique comment installer les dispositifs de sécurité ASA pour l'accès à un serveur de Protocole SMTP (Simple Mail Transfer Protocol) situé sur le réseau de la zone démilitarisée (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 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 intérieur.

Référez-vous à ASA 8.3 et plus tard : Serveur Access de messagerie (SMTP) sur l'exemple extérieur de configuration réseau 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 extérieur.

Référez-vous à PIX/ASA 7.x et en haut : Accès de serveur de messagerie (SMTP) sur l'exemple de configuration DMZ 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 (10.1.1.0/24) et le réseau extérieur (192.168.200.0/27). Le serveur de messagerie avec l'adresse IP 172.16.31.10 se trouve dans le réseau de la zone démilitarisée (DMZ). Pour que le mail server soit accédé à par l'intérieur, les utilisateurs configurent l'identité NAT. Configurez une liste d'accès, qui est **dmz_int** dans cet exemple, afin de permettre les connexions sortantes de SMTP du mail server aux hôtes dans le réseau intérieur et les lier à l'interface DMZ.

De même pour que les utilisateurs externes accèdent au mail server configurez un NAT statique et également une liste d'accès, qui est **outside_int** dans cet exemple, afin de permettre à des utilisateurs externes pour accéder au mail server et lier cette liste d'accès à l'interface extérieure.

Configuration ASA

Ce document utilise la configuration suivante :

Configuration 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]
```

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

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Dépannage des commandes

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** .

- mettez au point le suivi d'ICMP — Affiche si les demandes de Protocole ICMP (Internet Control Message Protocol) des hôtes atteignent l'ASA. Vous devez ajouter la **commande access-list** afin de permettre à l'ICMP dans votre configuration afin d'exécuter ceci mettez au point.**Remarque:** Afin d'utiliser ceci mettez- au point, veillez-vous pour permettre l'ICMP dans l'`outside_int de liste d'accès` comme cette sortie affiche :`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 — Utilisé en mode de configuration globale pour permettre à l'appliance de sécurité adaptable d'envoyer des messages de Syslog à la mémoire tampon de log. Le contenu de la mémoire tampon de log ASA peut être vu avec la commande de show logging.

Référez-vous configurent le Syslog utilisant l'ASDM pour plus d'informations sur la façon installer se connecter.

Informations connexes

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