ASA/PIX : exemple de configuration de NTP avec et sans tunnel IPsec

Table des matières

Introduction

Ce document fournit un exemple de configuration pour la synchronisation de l'horloge de l'appareil de sécurité PIX/ASA avec un serveur temporel de réseau à l'aide du protocole NTP (Network Time Protocol). ASA1 communique directement avec le serveur temporel du réseau. ASA2 achemine le trafic NTP par un tunnel IPSec à ASA1, qui à son tour transmet les paquets au serveur temporel du réseau.

Référez-vous à ASA 8.3 et versions ultérieures : NTP avec et sans exemple de configuration de tunnel IPsec pour plus d'informations sur la configuration identique sur Cisco ASA avec les versions 8.3 et ultérieures.

Remarque : un routeur peut également être utilisé comme serveur NTP pour synchroniser l'horloge du dispositif de sécurité PIX/ASA.

Conditions préalables

Exigences

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- La connectivité IPsec de bout en bout doit être établie avant de démarrer cette configuration NTP.
- La licence du dispositif de sécurité doit être activée pour le chiffrement Data Encryption Standard (DES) (à un niveau de chiffrement minimal).

Composants utilisés

Les informations dans ce document sont basées sur les versions de logiciel et de matériel ci-dessous.

- Appareil de sécurité adaptatif Cisco (ASA) avec version 7.x et ultérieure
- ASDM version 5.x et ultérieures

Remarque : référez-vous à Autoriser l'accès HTTPS pour ASDM afin de permettre à l'ASA d'être configuré par l'ASDM.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Produits connexes

Cette configuration peut également être utilisée avec le dispositif de sécurité de la gamme Cisco PIX 500, qui exécute la versions 7.x et les versions ultérieures.

Remarque : la prise en charge de NTP a été ajoutée dans PIX version 6.2. Référez-vous à PIX 6.2 : Exemple de configuration de NTP avec et sans tunnel IPsec afin de configurer NTP sur le pare-feu Cisco PIX.

Conventions

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

Configuration

Diagramme du réseau

Ce document utilise la configuration réseau indiquée dans le diagramme suivant.

Remarque : les schémas d'adressage 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.

- Configuration ASDM du tunnel VPN

- Configuration NTP ASDM
- Configuration CLI ASA1
- Configuration CLI ASA2

Configuration ASDM du tunnel VPN

Complétez ces étapes pour créer le tunnel VPN :

1. Ouvrez votre navigateur et tapez https://<Inside_IP_Address_of_ASA> pour accéder à l'ASDM sur l'ASA.

   Assurez-vous d'autoriser tous les avertissements que votre navigateur vous donne en ce qui concerne l'authenticité de certificat SSL. Le nom d'utilisateur par défaut et le mot de passe sont tous deux vides.

   L'ASA présente cette fenêtre pour permettre le téléchargement de l'application ASDM. Cet exemple charge l'application sur l'ordinateur local et ne fonctionne pas dans une applet Java.

2. Cliquez sur Download ASDM Launcher and Start ASDM pour télécharger le programme d'installation de l'application ASDM.

3. Une fois le lanceur d'ASDM téléchargé, exécutez les étapes stipulées par les invites afin d'installer le logiciel et d'exécuter le lanceur de Cisco ASDM.

4. Entrez l'adresse IP pour l'interface que vous avez configurée avec la commande http - et un nom d'utilisateur et mot de passe, le cas échéant.

   Cet exemple n'utilise pas de nom d'utilisateur ni de mot de passe (configuration par défaut).

5. Exécutez l'assistant VPN une fois que l'application ASDM se connecte à l'ASA.

6. Sélectionnez le type de tunnel VPN IPsec site à site.

7. Spécifiez l'adresse IP externe du partenaire distant. Entrez les informations d'authentification à utiliser, qui sont la clé pré-partagée dans cet exemple.

8. Spécifiez les attributs à utiliser pour l'IKE, également connus sous le nom de « Phase 1 ». Ces attributs doivent être identiques des deux côtés du tunnel.

9. Spécifiez les attributs à utiliser pour IPsec, également connus sous le nom de « Phase 2 ». Ces attributs doivent correspondre des deux côtés.

10. Spécifiez les hôtes dont le trafic devrait être autorisé à passer par le tunnel VPN. Au cours de cette étape, les hôtes locaux d'ASA1 sont spécifiés.

11. Les hôtes et les réseaux du côté distant du tunnel sont spécifiés.

12. Les attributs définis par l'assistant VPN sont affichés dans ce récapitulatif. Vérifiez une deuxième fois la configuration et cliquez sur Finish quand vous êtes sûr que les paramètres sont corrects.

Configuration NTP ASDM

Complétez ces étapes pour configurer NTP sur le dispositif de sécurité Cisco :

1. Choisissez Configuration dans la page d'accueil ASDM comme indiqué ici :
2. Maintenant, choisissez Properties > Device Management > NTP afin d'ouvrir la page de configuration NTP d'ASDM comme indiqué ici :
3. Cliquez sur le bouton ADD afin d'ajouter un serveur NTP et fournir les attributs requis tels que l'adresse IP, le nom de l'interface (interne ou externe), le numéro de clé et la valeur de clé pour l'authentification dans la nouvelle fenêtre qui apparaît après que vous avez cliqué sur le bouton ADD comme indiqué dans la capture d'écran. Cliquez ensuite sur OK.

   Remarque : le nom de l'interface doit être choisi comme interne pour ASA1 et externe pour ASA2.

   Remarque : la clé d'authentification ntp doit être la même dans ASA et le serveur NTP.

   La configuration de l'attribut Authentication dans l'interface de ligne de commande pour ASA1 et ASA2 est indiquée ci-dessous :

   ```
   <#root>

   ASA1#

   ntp authentication-key 1 md5 cisco

   ntp trusted-key 1
   ntp server 172.22.1.161 key 1 source inside
   ```

   ```
   <#root>

   ASA2#

   ntp authentication-key 1 md5 cisco

   ntp trusted-key 1
   ntp server 172.22.1.161 key 1 source outside
   ```

4. Cliquez à présent sur la case à cocher Enable NTP Authentication et cliquez sur Apply, qui termine la tâche de configuration NTP.

Configuration CLI ASA1

```
<#root>

ASA#

show run

: Saved
ASA Version 7.1(1)
!
hostname ASA1
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names

!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 10.10.10.1 255.255.255.0

!--- Configure the outside interface. !

interface Ethernet1
 nameif inside
 security-level 100
 ip address 172.22.1.163 255.255.255.0

!--- Configure the inside interface. !



 !-- Output suppressed !

passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name default.domain.invalid



access-list inside_nat0_outbound extended permit ip 172.22.1.0 255.255.255.0 172
.16.1.0 255.255.255.0

 !--- This access list

(inside_nat0_outbound)

 is used !--- with the

nat zero

 command. This prevents traffic which !--- matches the access list from undergoing network address tra

(outside_cryptomap_20)

. !--- Two separate access lists should always be used in this configuration.

access-list outside_cryptomap_20 extended permit ip 172.22.1.0 255.255.255.0 172
.16.1.0 255.255.255.0

!--- This access list
```

```
(outside_cryptomap_20)

 is used !--- with the crypto map

outside_map

 !--- to determine which traffic should be encrypted and sent !--- across the tunnel. !--- This ACL is

(inside_nat0_outbound)

. !--- Two separate access lists should always be used in this configuration.

pager lines 24
mtu inside 1500
mtu outside 1500
no failover

asdm image flash:/asdm-511.bin

!--- Enter this command to specify the location of the ASDM image.

asdm history enable
arp timeout 14400


nat (inside) 0 access-list inside_nat0_outbound

!--- NAT 0 prevents NAT for networks specified in !--- the ACL

inside_nat0_outbound

.

route outside 0.0.0.0 0.0.0.0 10.10.10.2 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


http server enable

!--- Enter this command in order to enable the HTTPS server !--- for ASDM.


http 172.22.1.1 255.255.255.255 inside

!--- Identify the IP addresses from which the security appliance !--- accepts HTTPS connections.


no snmp-server location
no snmp-server contact


!--- PHASE 2 CONFIGURATION ---! !--- The encryption types for Phase 2 are defined here.

crypto ipsec transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac

!--- Define the transform set for Phase 2.
```

```
crypto map outside_map 20 match address outside_cryptomap_20

!--- Define which traffic should be sent to the IPsec peer.


crypto map outside_map 20 set peer 10.20.20.1

!--- Sets the IPsec peer


crypto map outside_map 20 set transform-set ESP-AES-256-SHA

!--- Sets the IPsec transform set "ESP-AES-256-SHA" !--- to be used with the crypto map entry "outside_


crypto map outside_map interface outside

!--- Specifies the interface to be used with !--- the settings defined in this configuration.


!--- PHASE 1 CONFIGURATION ---! !--- This configuration uses isakmp policy 10. !--- Policy 65535 is in


isakmp enable outside
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption aes-256
isakmp policy 10 hash sha
isakmp policy 10 group 5
isakmp policy 10 lifetime 86400

isakmp policy 65535 authentication pre-share
isakmp policy 65535 encryption 3des
isakmp policy 65535 hash sha
isakmp policy 65535 group 2
isakmp policy 65535 lifetime 86400



tunnel-group 10.20.20.1 type ipsec-l2l

!--- In order to create and manage the database of connection-specific !--- records for ipsec-l2l-IPse

tunnel-group

 in global configuration mode. !--- For L2L connections the name of the tunnel group

MUST

 be the IP !--- address of the IPsec peer.



tunnel-group 10.20.20.1 ipsec-attributes
 pre-shared-key *

!--- Enter the pre-shared-key in order to configure the !--- authentication method.


telnet timeout 5
ssh timeout 5
console timeout 0
!
```

```
class-map inspection_default
 match default-inspection-traffic
!
!
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
!
service-policy global_policy global


!--- Define the NTP server autentication-key,Trusted-key !--- and the NTP server address for configuri


ntp authentication-key 1 md5 *
ntp trusted-key 1



!--- The NTP server source is to be mentioned as inside for ASA1


ntp server 172.22.1.161 key 1 source inside

Cryptochecksum:ce7210254f4a0bd263a9072a4ccb7cf7
: end
```

Cette vidéo publiée sur la communauté d'assistance Cisco explique avec une démonstration, la procédure pour configurer ASA comme client NTP :

Comment configurer un dispositif de sécurité adaptatif Cisco (ASA) pour synchroniser son horloge avec un serveur NTP (Network Time Protocol).

Configuration CLI ASA2

ASA2

<#root>

```
ASA Version 7.1(1)
!
hostname ASA2
domain-name default.domain.invalid
```

```
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 10.20.20.1 255.255.255.0
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 172.16.1.1 255.255.255.0
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name default.domain.invalid

access-list inside_nat0_outbound extended permit ip 172.16.1.0 255.255.255.0 172
.22.1.0 255.255.255.0

!--- Note that this ACL is a mirror of the

inside_nat0_outbound

 !--- ACL on ASA1.

access-list outside_cryptomap_20 extended permit ip 172.16.1.0 255.255.255.0 172
.22.1.0 255.255.255.0

!--- Note that this ACL is a mirror of the

outside_cryptomap_20

 !--- ACL on ASA1.

pager lines 24
mtu inside 1500
mtu outside 1500
no failover
asdm image flash:/asdm-511.bin
no asdm history enable
arp timeout 14400
nat (inside) 0 access-list inside_nat0_outbound
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
http server enable
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
crypto ipsec transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto map outside_map 20 match address outside_cryptomap_20
crypto map outside_map 20 set peer 10.10.10.1
crypto map outside_map 20 set transform-set ESP-AES-256-SHA
crypto map outside_map interface outside
isakmp enable outside
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption aes-256
isakmp policy 10 hash sha
isakmp policy 10 group 5
```

```
isakmp policy 10 lifetime 86400
tunnel-group 10.10.10.1 type ipsec-l2l
tunnel-group 10.10.10.1 ipsec-attributes
 pre-shared-key *
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
!
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
!
service-policy global_policy global


!--- Define the NTP server autentication-key,Trusted-key !--- and the NTP server address for configuri


ntp authentication-key 1 md5 *
ntp trusted-key 1



!--- The NTP server source is to be mentioned as outside for ASA2.


ntp server 172.22.1.161 key 1 source outside

Cryptochecksum:d5e2ee898f5e8bd28e6f027aeed7f41b
: end
ASA#
```

Vérifier

Cette section fournit des informations qui vous permettront de vérifier que votre configuration fonctionne correctement.

Certaines commandes show sont prises en charge par l'Output Interpreter Tool (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

- show ntp status : affiche les informations d'horloge NTP.

```
<#root>

ASA1#

show ntp status

Clock is synchronized

, stratum 2, reference is 172.22.1.161
nominal freq is 99.9984 Hz, actual freq is 99.9983 Hz, precision is 2**6
reference time is ccf22b77.f7a6e7b6 (13:28:23.967 UTC Tue Dec 16 2008)
clock offset is 34.8049 msec, root delay is 4.78 msec
root dispersion is 60.23 msec, peer dispersion is 25.41 msec
```

- show ntp associations [detail] : affiche les associations de serveur de temps réseau configurées.

```
<#root>

ASA1#

show ntp associations detail

172.22.1.161 configured, authenticated

, our_master, sane, valid, stratum 1
ref ID .LOCL., time ccf2287d.3668b946 (13:15:41.212 UTC Tue Dec 16 2008)
our mode client, peer mode server, our poll intvl 64, peer poll intvl 64
root delay 0.00 msec, root disp 0.03, reach 7, sync dist 23.087
delay 4.52 msec, offset 9.7649 msec, dispersion 20.80
precision 2**19, version 3
org time ccf22896.f1a4fca3 (13:16:06.943 UTC Tue Dec 16 2008)
rcv time ccf22896.efb94b28 (13:16:06.936 UTC Tue Dec 16 2008)
xmt time ccf22896.ee5691dc (13:16:06.931 UTC Tue Dec 16 2008)
filtdelay =     4.52    4.68    4.61    0.00    0.00    0.00    0.00    0.00
filtoffset =    9.76    7.09    3.85    0.00    0.00    0.00    0.00    0.00
filterror =    15.63   16.60   17.58 14904.3 14904.3 14904.3 14904.3 14904.3
```

Dépannage

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

Dépannage des commandes

Certaines commandes show sont prises en charge par l'Output Interpreter Tool (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

Remarque : avant d'émettre des commandes debug, reportez-vous à Informations importantes sur les commandes de débogage.

- debug ntp valid : affiche la validité de l'horloge de l'homologue NTP.

  Voici la sortie de débogage de la non-correspondance de clé :

  <#root>

  ```
  NTP: packet from 172.22.1.161 failed validity tests 10
         Authentication failed
  ```

- debug ntp packet : affiche les informations de paquet NTP.

  Quand il n'y a pas de réponse du serveur, seul le paquet `NTP xmit` est vu sur l'ASA avec aucun paquet `NTP rcv`.

```
ASA1# NTP: xmit packet to 172.22.1.161:
 leap 0, mode 3, version 3, stratum 2, ppoll 64
 rtdel 012b (4.562), rtdsp 0cb6 (49.652), refid ac1601a1 (172.22.1.161)
 ref ccf22916.f1211384 (13:18:14.941 UTC Tue Dec 16 2008)
 org ccf22916.f426232d (13:18:14.953 UTC Tue Dec 16 2008)
 rec ccf22916.f1211384 (13:18:14.941 UTC Tue Dec 16 2008)
 xmt ccf22956.f08ee8b4 (13:19:18.939 UTC Tue Dec 16 2008)
NTP: rcv packet from 172.22.1.161 to 172.22.1.163 on inside:
 leap 0, mode 4, version 3, stratum 1, ppoll 64
 rtdel 0000 (0.000), rtdsp 0002 (0.031), refid 4c4f434c (76.79.67.76)
 ref ccf2293d.366a4808 (13:18:53.212 UTC Tue Dec 16 2008)
 org ccf22956.f08ee8b4 (13:19:18.939 UTC Tue Dec 16 2008)
 rec ccf22956.f52e480e (13:19:18.957 UTC Tue Dec 16 2008)
 xmt ccf22956.f5688c29 (13:19:18.958 UTC Tue Dec 16 2008)
 inp ccf22956.f982bcd9 (13:19:18.974 UTC Tue Dec 16 2008)
```

Informations connexes

- Logiciels pare-feu Cisco PIX
- Cisco Adaptive Security Device Manager
- Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500
- Références des commandes du pare-feu Cisco Secure PIX
- Demandes de commentaires (RFC)
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.