ASA/PIX: esempio di configurazione del NTP con e senza tunnel IPsec

Sommario

Introduzione

In questo documento viene fornita una configurazione di esempio per sincronizzare l'orologio dell'appliance di sicurezza PIX/ASA con un time server usando il protocollo Network Time Protocol (NTP). ASA1 comunica direttamente con il time server della rete. ASA2 trasmette il traffico NTP tramite un tunnel IPSec ad ASA1, che a sua volta inoltra i pacchetti al time server della rete.

Per ulteriori informazioni sulla stessa configurazione sull'appliance Cisco ASA con versione 8.3 e successive, consultare il documento ASA 8.3 e successive: NTP con e senza configurazione del tunnel IPsec.

Nota: un router può essere usato anche come server NTP per sincronizzare l'orologio di PIX/ASA Security Appliance.

Prerequisiti

Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Prima di avviare questa configurazione NTP, è necessario stabilire la connettività IPsec end-to-end.
- È necessario abilitare la licenza di Security Appliance per la crittografia DES (Data Encryption Standard) (a un livello di crittografia minimo).

Componenti usati

Le informazioni fornite in questo documento si basano sulle versioni software e hardware riportate di seguito.

- Cisco Adaptive Security Appliance (ASA) con versione 7.x e successive
- ASDM versione 5.x.1 e successive

Nota: per consentire all'ASDM di configurare l'appliance ASA, consultare il documento sull'autorizzazione dell'accesso HTTPS per ASDM.

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.

Prodotti correlati

Questa configurazione può essere utilizzata anche con Cisco PIX serie 500 Security Appliance, con versione 7.x e successive.

Nota: il supporto NTP è stato aggiunto nella versione PIX 6.2. Per configurare il protocollo NTP sul firewall Cisco PIX, consultare la sezione PIX 6.2: esempio di configurazione del tunnel NTP con e senza tunnel IPsec.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Configurazione

Esempio di rete

Per la stesura di questo documento è stata utilizzata la configurazione di rete illustrata in questo diagramma.

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.

- Configurazione ASDM tunnel VPN

- Configurazione ASDM NTP
- Configurazione CLI di ASA1
- Configurazione ASA2 CLI

Configurazione ASDM tunnel VPN

Completare questi passaggi per creare il tunnel VPN:

1. Aprire il browser e digitare https://<Inside_IP_Address_of_ASA> per accedere ad ASDM sull'appliance ASA.

   Assicurarsi di autorizzare tutti gli avvisi che il browser visualizza relativi all'autenticità del certificato SSL. Il nome utente e la password predefiniti sono entrambi vuoti.

   L'appliance ASA visualizza questa finestra per consentire il download dell'applicazione ASDM. Questo esempio carica l'applicazione nel computer locale e non viene eseguito in un'applet Java.

2. Per scaricare il programma di installazione dell'applicazione ASDM, fare clic su Download ASDM Launcher (Scarica ASDM Launcher) e su Start ASDM (Avvia ASDM).

3. Una volta scaricato l'utilità di avvio ASDM, completare la procedura indicata dalle istruzioni per installare il software ed eseguire l'utilità di avvio Cisco ASDM.

4. Immettere l'indirizzo IP per l'interfaccia configurata con il comando http -, nonché un nome utente e una password, se specificati.

   In questo esempio vengono utilizzati il nome utente e la password vuoti predefiniti.

5. Eseguire la VPN Wizard una volta che l'applicazione ASDM si connette all'appliance ASA.

6. Scegliere il tipo di tunnel VPN IPSec da sito a sito.

7. Specificare l'indirizzo IP esterno del peer remoto. Immettere le informazioni di autenticazione da utilizzare, ovvero la chiave già condivisa in questo esempio.

8. Specificare gli attributi da utilizzare per IKE, noto anche come Fase 1. Questi attributi devono essere gli stessi su entrambi i lati del tunnel.

9. Specificare gli attributi da utilizzare per IPSec, noti anche come Fase 2. Questi attributi devono corrispondere su entrambi i lati.

10. Specificare gli host il cui traffico deve poter passare attraverso il tunnel VPN. In questo passo, vengono specificati gli host locali di ASA1.

11. Vengono specificati gli host e le reti sul lato remoto del tunnel.

12. In questo riepilogo vengono visualizzati gli attributi definiti dalla Creazione guidata VPN.

Verificare la configurazione e fare clic su Finish (Fine) quando le impostazioni sono corrette.

Configurazione ASDM NTP

Completare la procedura seguente per configurare l'NTP su Cisco Security Appliance:

1. Scegliere Configuration (Configurazione) nella home page ASDM come mostrato di seguito:
2. Scegliere Proprietà > Gestione dispositivi > NTP per aprire la pagina di configurazione NTP di ASDM, come mostrato di seguito:
3. Fare clic sul pulsante ADD (AGGIUNGI) per aggiungere un server NTP e fornire gli attributi richiesti, quali indirizzo IP, nome interfaccia (interna o esterna), numero chiave e valore chiave per l'autenticazione, nella nuova finestra che compare dopo aver fatto clic sul pulsante ADD (AGGIUNGI), come mostrato nella schermata. Quindi fare clic su OK.

   Nota: il nome dell'interfaccia deve essere scelto tra ASA1 e ASA2.

   Nota: la chiave di autenticazione ntp deve essere la stessa nell'ASA e nel server NTP.

   Di seguito è riportata la configurazione dell'attributo Authentication nella cli per ASA1 e ASA2:

   <#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. A questo punto, fare clic sulla casella di controllo Abilita autenticazione NTP e fare clic su Applica per completare il task di configurazione NTP.

Configurazione CLI di 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-IPsec

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
```

Questo video pubblicato nella Cisco Support Community spiega, con una demo, la procedura per configurare l'ASA come client NTP:

Come configurare un'appliance Cisco Adaptive Security (ASA) in modo che sincronizzi il proprio orologio con un server NTP (Network Time Protocol).

Configurazione ASA2 CLI

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#
```

Verifica

In questa sezione viene spiegato come verificare che la configurazione funzioni correttamente.

Alcuni comandi show sono supportati dallo strumento Output Interpreter (solo utenti registrati); lo strumento permette di visualizzare un'analisi dell'output del comando show.

- show ntp status: visualizza le informazioni sull'orologio 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 association [detail]: visualizza le associazioni del server di riferimento orario di rete configurate.

```
<#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
```

Risoluzione dei problemi

In questa sezione vengono fornite informazioni utili per risolvere i problemi di configurazione.

Comandi per la risoluzione dei problemi

Alcuni comandi show sono supportati dallo strumento Output Interpreter (solo utenti registrati); lo strumento permette di visualizzare un'analisi dell'output del comando show.

Nota: prima di usare i comandi di debug, consultare le informazioni importanti sui comandi di debug.

- debug ntp invalid: visualizza la validità del clock peer NTP.

  Questo è l'output del comando debug per la mancata corrispondenza della chiave:

<#root>

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

- debug ntp packet: visualizza le informazioni sul pacchetto NTP.

  In assenza di risposta dal server, solo il pacchetto `NTP xmit` viene visualizzato sull'appliance ASA senza pacchetto `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)
```

Informazioni correlate

- Software Cisco PIX Firewall
- Cisco Adaptive Security Device Manager
- Cisco ASA serie 5500 Adaptive Security Appliance
- Riferimenti per i comandi di Cisco Secure PIX Firewall
- RFC (Requests for Comments)
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).