# ASA/PIX: NTP com e sem um exemplo de configuração do túnel de IPsec

## Índice



## Introdução

Este documento fornece uma configuração de exemplo sincronizando o pulso de disparo da ferramenta de segurança PIX/ASA com um server de tempo de rede usando o Network Time Protocol (NTP). ASA1 comunica-se diretamente com o tráfego das passagens NTP do tempo de rede server.ASA2 através de um túnel de IPsec a ASA1, que por sua vez para a frente os pacotes ao server de tempo de rede.

Refira ASA 8.3 e mais atrasado: NTP com e sem um exemplo de configuração do túnel de IPsec para obter mais informações sobre da configuração idêntica em Cisco ASA com versões 8.3 e mais recente.

**Nota:** Um roteador pode igualmente ser usado como um servidor de NTP sincronizando o pulso de disparo da ferramenta de segurança PIX/ASA.

## Pré-requisitos

### Requisitos

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- A Conectividade do IPSec de ponta a ponta deve ser estabelecida antes de começar esta configuração de NTP.
- A licença da ferramenta de segurança deve ser permitida para a criptografia do Data Encryption Standard (DES) (a nível mínimo da criptografia).

## Componentes Utilizados

As informações neste documento são baseadas nas versões de software e hardware abaixo.

- Segurança adaptável Appliance(ASA) de Cisco com versão 7.x e mais recente
- Versão 5.x.and ASDM mais atrasada

**Nota:** Consulte Habilitação de Acesso HTTPS para o ASDM para permitir que o ASA seja configurado pelo ASDM.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

## Produtos Relacionados

Esta configuração pode igualmente ser usada com a ferramenta de segurança da série do Cisco PIX 500, que executa a versão 7.x e mais recente.

**Nota:** O apoio NTP foi adicionado na versão de PIX 6.2. Refira PIX 6.2: NTP com e sem um exemplo de configuração do túnel de IPsec a fim configurar o NTP no Cisco PIX Firewall.

## Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

# Configuração

## Diagrama de Rede

Este documento utiliza a configuração de rede mostrada neste diagrama.

**Nota:** Os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. São os endereços do RFC 1918, que foram usados em um ambiente de laboratório.

- Configuração ASDM do túnel VPN
- Configuração ASDM NTP
- Configuração de CLI ASA1
- Configuração de CLI ASA2

## Configuração ASDM do túnel VPN

Termine estas etapas para criar o túnel VPN:

1. Abra seu navegador e datilografe o **<Inside_IP_Address_of_ASA> de https://** para alcançar o ASDM no ASA.Seja certo autorizar todos os avisos que seu navegador o der relativo à autenticidade de certificado de SSL. O nome de usuário padrão e a senha são ambos placa.O ASA apresenta este indicador para permitir a transferência do aplicativo ASDM. Este exemplo carrega o aplicativo no computador local e não o é executado em um Java applet.
2. Clique a **launcher ASDM da transferência e comece o ASDM** a fim transferir o instalador para o aplicativo ASDM.
3. Uma vez as transferências da launcher ASDM, terminam as etapas dirigidas pelas alertas a fim instalar o software e executar o lançador ASDM Cisco.
4. Incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT para a relação que você configurou com o **HTTP -** comande e um nome de usuário e senha se você especificou um.Este exemplo usa o nome de usuário e senha da placa do padrão.
5. Execute o wizard VPN uma vez que o aplicativo ASDM conecta ao ASA.
6. Escolha o tipo de túnel do **IPSec local a local** VPN.
7. Especifique o endereço IP externo do peer remoto. Incorpore a informação da autenticação para usar-se, que é a chave pré-compartilhada neste exemplo.
8. Especifique os atributos para usar-se para o IKE, igualmente sabido como a fase 1. Estes atributos devem ser os mesmos em ambos os lados do túnel.
9. Especifique os atributos para usar-se para o IPsec, igualmente sabido como a fase 2. Estes atributos devem combinar em ambos os lados.
10. Especifique os anfitriões cujo o tráfego deve ser permitido passar através do túnel VPN. Nesta etapa, os anfitriões locais a ASA1 são especificados.
11. Os anfitriões e as redes no lado remoto do túnel são especificados.
12. Os atributos definidos pelo wizard VPN são indicados neste sumário. Verifique novamente a configuração e clique o **revestimento** quando você é satisfeito os ajustes está correto.

## Configuração ASDM NTP

Termine estas etapas para configurar o NTP no dispositivo do Cisco Security:

1. Escolha a **configuração no** Home Page ASDM como mostrado aqui:
2. Escolha agora **propriedades > Gerenciamento de dispositivos > NTP** a fim abrir como mostrado a página da **configuração de NTP do** ASDM aqui:
3. Clique o **botão Add** a fim adicionar um servidor de NTP e fornecer os atributos requerido tais como o nome do endereço IP de Um ou Mais Servidores Cisco ICM NT, da relação (dentro ou fora), o número e o valor chave chaves para Authetication na nova janela que vem acima depois que você clicou sobre o **botão Add** segundo as indicações do screen shot. Clique então sobre **ESTÁ BEM**.**Nota:** O nome da relação deve ser escolhido como para dentro para ASA1 e parte externa para ASA2.**Nota: A chave da autenticação de NTP** deve ser a mesma no ASA e no servidor de NTP.A configuração do atributo de Authetication no CLI para ASA1 e ASA2 são mostrados abaixo:`ASA1#ntp authentication-key 1 md5 cisco ntp trusted-key 1 ntp server 172.22.1.161 key 1 source inside ASA2#ntp authentication-key 1 md5 cisco ntp trusted-key 1 ntp server 172.22.1.161 key 1 source outside`
4. Clique agora a caixa de seleção **permitem a autenticação de NTP** e o clique **aplica-se**, que termina a tarefa da configuração de NTP.

## Configuração de CLI ASA1

**ASA1**

```
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 translation (NAT). !--- The traffic specified by
this ACL is traffic that is to be encrypted and !---
sent across the VPN tunnel. This ACL is intentionally !-
-- the same as (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 intentionally the same as (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_map". 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 included in the config
by default. !--- The configuration commands here define
the Phase !--- 1 policy parameters that are used. 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
(LAN-to-LAN) tunnels, use the command !--- 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 configuring NTP. 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
```

Este vídeo afixado à comunidade do apoio de Cisco explica com um programa demonstrativo, o procedimento para configurar o ASA como o cliente de NTP:

Como configurar uma ferramenta de segurança adaptável de Cisco (ASA) para sincronizar seu pulso de disparo com um server do Network Time Protocol (NTP).

## Configuração de CLI ASA2

**ASA2**

```
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 configuring NTP. 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#
```

# Verificar

Esta seção fornece informações que você pode usar para confirmar se sua configuração funciona adequadamente.

A Output Interpreter Tool (somente clientes registrados) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

- mostre a exibições de status NTP a informação de relógio NTP.`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`

- mostre o [detail] das associações NTP — Indica as associações do Time Server da rede configurada.
```
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
```

# Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

## Comandos para Troubleshooting

A Output Interpreter Tool (somente clientes registrados) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

**Nota:** Antes de emitir comandos de depuração, consulte as informações importantes sobre eles.

- **debugar a validez NTP** — Exibe validade de relógio correspondente de NTP.Este é **resultado do debug da** incompatibilidade de chave:
  **`NTP: packet from 172.22.1.161 failed validity tests 10 Authentication failed`**
- **debugar o pacote NTP** — Informação do pacote de NTP dos indicadores.Quando não houver nenhuma resposta do server, simplesmente o `pacote NTP xmit` está visto no ASA sem o pacote `receptor NTP.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)
```

# Informações Relacionadas

- Cisco PIX Firewall Software
- Cisco Adaptive Security Device Manager
- Cisco ASA 5500 Series Adaptive Security Appliances
- Referências do comando Cisco Secure PIX Firewall
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems