PIX/ASA 7.x y posteriores: Ejemplo de Configuración de VPN IPsec de LAN a LAN con Redes Superpuestas

Contenido

Introducción

Este documento describe los pasos que hay que seguir para traducir (NAT) el tráfico VPN que viaja sobre un túnel IPsec de LAN a LAN (L2L) entre dos dispositivos de seguridad y también PAT el tráfico de Internet. Cada dispositivo de seguridad tiene una red privada protegida detrás de ella. En este ejemplo, se conectan dos dispositivos de seguridad adaptable (ASA) de Cisco con redes internas idénticas y superpuestas a través del túnel VPN. En un escenario normal, la comunicación a través de la VPN nunca ocurre porque los paquetes ping nunca salen de la subred local ya que el usuario hace ping a la dirección IP de la misma subred. Para que estas dos redes internas privadas se comuniquen entre sí, la política NAT se utiliza en ambos ASA para la traducción de la subred local de modo que la comunicación se realice según lo esperado.

Prerequisites

Requirements

Asegúrese de haber configurado el dispositivo de seguridad adaptable de Cisco con direcciones IP en las interfaces y de tener conectividad básica antes de continuar con este ejemplo de

configuración.

Componentes Utilizados

La información de este documento se basa en esta versión del software:

- Cisco Adaptive Security Appliance Software Version 7.x y posterior.

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.

Productos Relacionados

Esta configuración también se puede usar con Cisco PIX Security Appliance Version 7.x y posterior.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

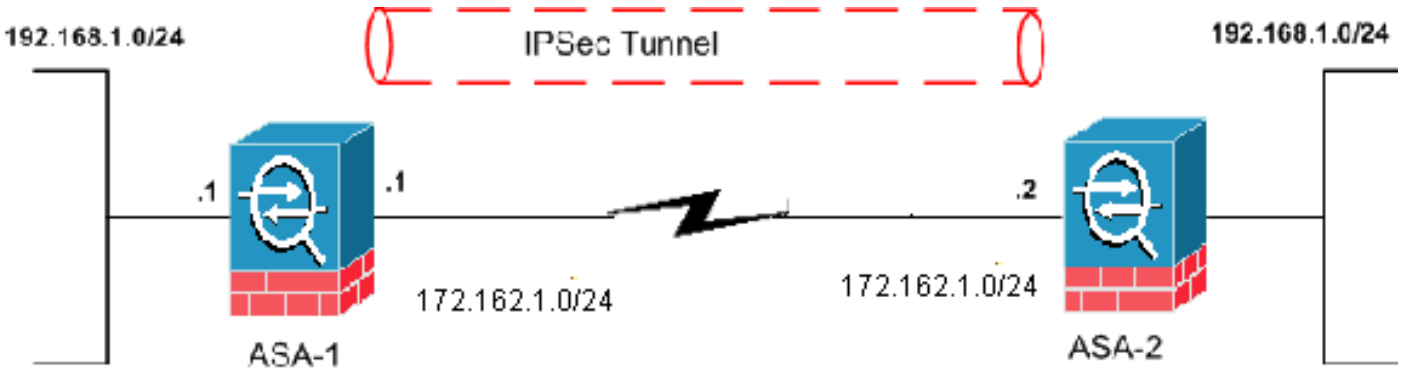
Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Use el Command Lookup Tool (únicamente clientes registrados) para obtener más información sobre los comandos que se utilizan en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configuraciones

En este documento, se utilizan estas configuraciones:

- Configuración de ASA-1

- Configuración de ASA-2

ASA-1

```
ASA-1#show running-config
: Saved
:
ASA Version 8.0(3)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 172.162.1.1 255.255.255.0
!--- Configure the outside interface. ! interface
Ethernet1 nameif inside security-level 100 ip address
192.168.1.1 255.255.255.0 !--- Configure the inside
interface. passwd 2KFQnbNIdI.2KYOU encrypted ftp mode
passive access-list new extended permit ip 192.168.2.0
255.255.255.0 192.168.3.0 255.255.255.0 !--- This access
list (new) is used with the crypto map (outside_map) !--
- in order to determine which traffic should be
encrypted !--- and sent across the tunnel.
access-list policy-nat extended permit ip 192.168.1.0
255.255.255.0 192.168.3.0 255.255.255.0

!--- The policy-nat ACL is used with the static !---
command in order to match the VPN traffic for
translation.

pager lines 24
mtu outside 1500
mtu inside 1500
no failover
asdm image flash:/asdm-615.bin
no asdm history enable
arp timeout 14400


static (inside,outside) 192.168.2.0  access-list policy-
nat
!--- It is a Policy NAT statement. !--- The static
command with the access list (policy-nat), !--- which
matches the VPN traffic and translates the source
(192.168.1.0) to !--- 192.168.2.0 for outbound VPN
traffic.


global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
!--- The previous statements PAT the Internet traffic !-
-- except for the VPN traffic that uses the IP address
172.17.1.1. route outside 0.0.0.0 0.0.0.0 172.162.1.2 1
!--- Output is suppressed. !--- PHASE 2 CONFIGURATION --
-! !--- The encryption types for Phase 2 are defined
here. crypto ipsec transform-set CISCO esp-des esp-md5-
hmac !--- Define the transform set for Phase 2. crypto
map outside_map 20 match address new !--- Define which
traffic should be sent to the IPsec peer with the !---
```

```
access list (new). crypto map outside_map 20 set peer
172.162.1.2 !--- Sets the IPsec peer (remote end point)
crypto map outside_map 20 set transform-set CISCO !---
Sets the IPsec transform set "CISCO" !--- 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 65535. !--- Policy
65535 is included in the configuration by default. !---
These configuration commands define the !--- Phase 1
policy parameters that are used. crypto isakmp identity
address crypto isakmp enable outside crypto isakmp
policy 65535 authentication pre-share encryption des
hash md5 group 2 lifetime 86400 tunnel-group 172.162.1.2
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 tunnel-group !--
- command in global configuration mode. !--- For L2L
connections, the name of the tunnel group must be !---
the IP address of the IPsec peer (remote peer end).

tunnel-group 172.162.1.2 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
Cryptochecksum:33e1e37cd1280d908210dac0cc26e706 : end
```

ASA-2

```
ASA-2#show running-config
: Saved
:
ASA Version 8.0(3)
!
hostname ASA-2
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 172.162.1.2 255.255.255.0
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
!--- Output is suppressed. access-list new extended
permit ip 192.168.3.0 255.255.255.0 192.168.2.0
255.255.255.0 !--- This access list (new) is used with
the crypto map (outside_map) !--- in order to determine
which traffic needs to be encrypted !--- and sent across
the tunnel.
access-list policy-nat extended permit ip 192.168.1.0
```

```
255.255.255.0 192.168.2.0 255.255.255.0

!--- The policy-nat ACL is used with the static !---
command in order to match the VPN traffic for
translation.

pager lines 24
mtu outside 1500
mtu inside 1500
no failover
asdm image flash:/asdm-615.bin
no asdm history enable
arp timeout 14400



static (inside,outside) 192.168.3.0  access-list policy-
nat
!--- This is a Policy NAT statement. !--- The static
command with the access list (policy-nat), !--- which
matches the VPN traffic and translates the source
(192.168.1.0) to !--- 192.168.3.0 for outbound VPN
traffic.

global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
!--- The previous statements PAT the Internet traffic !-
-- except the VPN traffic that uses the outside
interface IP address. route outside 0.0.0.0 0.0.0.0
172.162.1.2 1 !--- PHASE 2 CONFIGURATION ---! !--- The
encryption types for Phase 2 are defined here. crypto
ipsec transform-set CISCO esp-des esp-md5-hmac !---
Define the transform set for Phase 2. crypto map
outside_map 20 match address new !--- Define which
traffic needs to be sent to the IPsec peer. crypto map
outside_map 20 set peer 172.162.1.1 !--- Sets the IPsec
peer. crypto map outside_map 20 set transform-set CISCO
!--- Sets the IPsec transform set "CISCO" !--- 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 65535 !--- which
is included in the configuration by default. !--- The
configuration commands here define the !--- Phase 1
policy parameters that are used. crypto isakmp identity
address crypto isakmp enable outside crypto isakmp
policy 65535 authentication pre-share encryption des
hash md5 group 2 lifetime 86400 !--- Output is
suppressed. !--- In order to create and manage the
database of connection-specific !--- records for IPsec-
L2L—IPsec (LAN-to-LAN) tunnels, use the !--- tunnel-
group  command in global configuration mode. !--- For
L2L connections, the name of the tunnel group must be !-
-- the IP address of the IPsec peer.



tunnel-group 172.162.1.1 type ipsec-l2l
tunnel-group 172.162.1.1 ipsec-attributes
 pre-shared-key *
!--- Enter the pre-shared key in order to configure the
authentication method. prompt hostname context
Cryptochecksum:6b505b4a05c1aee96a71e67c23e71865 : end
```

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilize el OIT para ver una análisis de la salida del comando show:

- **show crypto isakmp sa: muestra todas las asociaciones actuales de seguridad IKE (SA) de un par.**
- **show crypto ipsec sa** - Muestra la configuración utilizada por las SA actuales.

Comandos show de ASA-1

```
ASA-1#show crypto isakmp sa



Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 172.162.1.2
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE

ASA-1#show crypto ipsec sa
interface: outside
    Crypto map tag: outside_map, seq num: 20, local addr: 172.162.1.1

      access-list new permit ip 192.168.2.0 255.255.255.0 192.168.3.0

255.255.2
5.0
      local ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
      current_peer: 172.162.1.2

      #pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
      #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 9, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.162.1.1, remote crypto endpt.: 172.162.1.2

      path mtu 1500, ipsec overhead 58, media mtu 1500
      current outbound spi: 0BA6CD7E

    inbound esp sas:
      spi: 0xFB4BD01A (4216049690)
         transform: esp-des esp-md5-hmac none
         in use settings ={L2L, Tunnel, }
         slot: 0, conn_id: 8192, crypto-map: outside_map
         sa timing: remaining key lifetime (kB/sec): (3824999/27738)
         IV size: 8 bytes
         replay detection support: Y
```

```
    outbound esp sas:
      spi: 0x0BA6CD7E (195480958)
         transform: esp-des esp-md5-hmac none
         in use settings ={L2L, Tunnel, }
         slot: 0, conn_id: 8192, crypto-map: outside_map
         sa timing: remaining key lifetime (kB/sec): (3824999/27738)
         IV size: 8 bytes
         replay detection support: Y

ASA-1#show nat


NAT policies on Interface inside:
  match ip inside 192.168.1.0 255.255.255.0 outside 192.168.3.0 255.255.255.0
    static translation to 192.168.2.0
    translate_hits = 12, untranslate_hits = 5
  match ip inside any outside any
    dynamic translation to pool 1 (172.162.1.1 [Interface PAT])
    translate_hits = 0, untranslate_hits = 0
  match ip inside any inside any
    dynamic translation to pool 1 (No matching global)
    translate_hits = 0, untranslate_hits = 0
  match ip inside any dmz any
    dynamic translation to pool 1 (No matching global)
    translate_hits = 0, untranslate_hits = 0

ASA-1#show xlate

1 in use, 1 most used
Global 192.168.2.0 Local 192.168.1.0
```

Comandos show de ASA-2

```
ASA-2#show crypto ipsec sa

interface: outside
    Crypto map tag: outside_map, seq num: 20, local addr: 172.162.1.2

      access-list new permit ip 192.168.3.0 255.255.255.0 192.168.2.0

255.255.25
5.0
      local ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
      current_peer: 172.162.1.1

      #pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
      #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 9, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.162.1.2, remote crypto endpt.: 172.162.1.1

      path mtu 1500, ipsec overhead 58, media mtu 1500
      current outbound spi: FB4BD01A

    inbound esp sas:
      spi: 0x0BA6CD7E (195480958)
         transform: esp-des esp-md5-hmac none
```

```
        in use settings ={L2L, Tunnel, }
        slot: 0, conn_id: 8192, crypto-map: outside_map
        sa timing: remaining key lifetime (kB/sec): (4274999/26902)
        IV size: 8 bytes
        replay detection support: Y
    outbound esp sas:
      spi: 0xFB4BD01A (4216049690)
        transform: esp-des esp-md5-hmac none
        in use settings ={L2L, Tunnel, }
        slot: 0, conn_id: 8192, crypto-map: outside_map
        sa timing: remaining key lifetime (kB/sec): (4274999/26902)
        IV size: 8 bytes
        replay detection support: Y
```

```
ASA-2#show crypto isakmp sa

Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 172.162.1.1
    Type    : L2L             Role    : responder
    Rekey   : no              State   : MM_ACTIVE
```

Troubleshoot

Despeje las asociaciones de seguridad

Cuando resuelva problemas, asegúrese de borrar las SA existentes después de realizar un cambio. En el modo privilegiado del PIX, use estos comandos:

- **clear crypto ipsec sa** - Elimina las SAs IPsec activas.
- **clear crypto isakmp sa** - Elimina las SA IKE activas.

Comandos para resolución de problemas

La herramienta de interpretación de información de salida (disponible para clientes registrados únicamente) admite ciertos comandos show. Utilize el OIT para ver una análisis de la salida del comando show.

Nota: Consulte Información Importante sobre Comandos Debug antes de utilizar los comandos **debug**.

- **debug crypto ipsec - Muestra los IPSec Negotiations de la Fase 2.**
- **debug crypto isakmp - Muestra las negociaciones ISAKMP para la fase 1.**

Información Relacionada

- Soluciones y Troubleshooting para los Problemas más Comunes con VPN IPSec de Acceso Remoto y L2L
- PIX 7.0 y Adaptive Security Appliance Port Redirection (Reenvío) con Comandos nat, global, static, conduit y access-list

- PIX/ASA 7.x y FWSM: Declaraciones NAT y PAT
- Cisco ASA 5500 Series Security Appliances
- Dispositivos de seguridad Cisco PIX de la serie 500
- Negociación IPSec/Protocolos IKE
- Soporte Técnico y Documentación - Cisco Systems