PIX/ASA 7.x et versions ultérieures : Exemple de configuration VPN IPSec LAN à LAN avec chevauchement des réseaux

Contenu

Introduction

Ce document décrit les étapes utilisées pour traduire (NAT) le trafic VPN passant à travers un tunnel LAN à LAN (L2L) IPsec entre deux appliances de sécurité et effectuer également une traduction d'adresses de port (PAT) du trafic Internet. Chaque dispositifs de sécurité ont un réseau privé et protégé derrière eux. Dans les appliances de sécurité adaptable Cisco de cet exemple deux (ASA) avec les réseaux internes identiques et superposants sont connectés au-dessus du tunnel VPN. Dans un scénario normal, la transmission à travers le VPN ne se produit jamais parce que les paquets de ping ne partent jamais du sous-réseau local puisque l'utilisateur cingle l'adresse IP du même sous-réseau. Pour que ces deux réseaux internes privés communiquent les uns avec les autres, la stratégie NAT est utilisée sur les deux ASA pour la traduction du sous-réseau local de sorte que la transmission se produise comme prévu.

Conditions préalables

Conditions requises

Veillez-vous pour avoir configuré l'appliance de sécurité adaptable Cisco avec des adresses IP sur

les interfaces, et ayez la Connectivité de base avant que vous poursuiviez cet exemple de configuration.

Composants utilisés

Les informations dans ce document sont basées sur cette version de logiciel :

- Version de logiciel 7.x d'appliance de sécurité adaptable Cisco et plus tard.

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.

Produits connexes

Cette configuration peut également être utilisée avec la version 7.x et ultérieures d'appareils de Sécurité de Cisco PIX.

Conventions

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

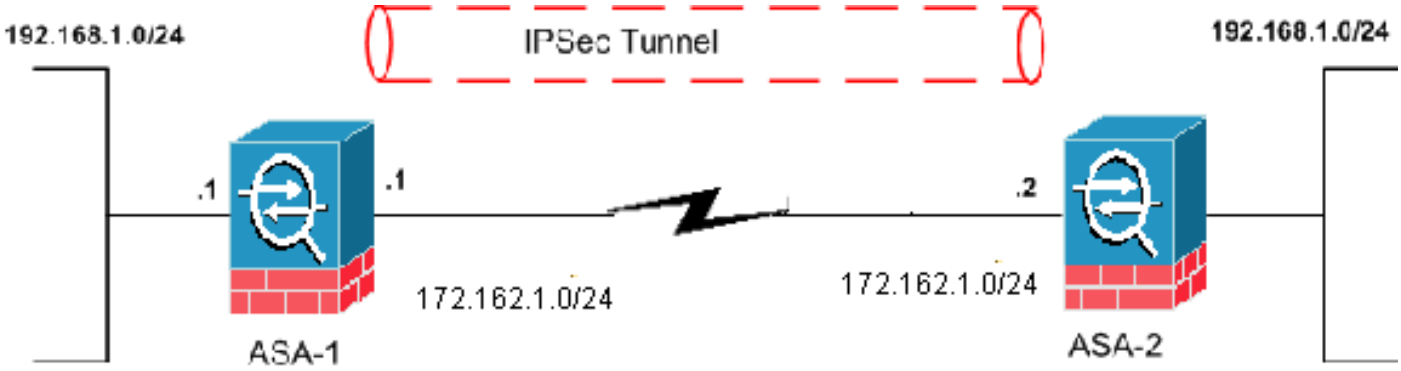
Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Utilisez l'Outil de recherche de commande (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 :



Configurations

Ce document utilise les configurations suivantes :

- Configuration ASA-1
- Configuration 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
```

Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Employez l'OIT afin de visualiser une analyse de sortie de commande show :

- **show crypto isakmp sa** - Affiche toutes les associations de sécurité en cours d'IKE (SAS) à un pair.
- **show crypto ipsec sa** - Affiche les configurations utilisées par le courant SAS.

commandes show d'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
```

commandes show d'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
```

Dépannez

Suppression des associations de sécurité

Quand vous dépannez, soyez sûr d'effacer SAS existante après que vous apportiez une modification. En mode privilégiée du PIX, utilisez les commandes suivantes :

- **clear crypto ipsec sa** - Supprime l'IPsec actif SAS.
- **clear crypto isakmp SA** - Supprime l'IKE actif SAS.

Dépannage des commandes

L'Output Interpreter Tool (clients enregistrés seulement) prend en charge certaines **commandes show**. Employez l'OIT afin d'afficher une analyse de la sortie de la commande show.

Remarque: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

- **debug crypto ipsec** - Affiche les négociations IPSecs du Phase 2.
- **debug crypto isakmp** - Affiche les négociations ISAKMP du Phase 1.

Informations connexes

- Solutions de dépannage les plus fréquentes concernant un VPN IPsec LAN à LAN et d'accès à distance
- PIX 7.0 et Port Redirection(Forwarding) d'appliance de sécurité adaptable avec nat, global, statique, le conduit, et les commandes access-list
- PIX/ASA 7.x et FWSM : Instructions NAT et PAT
- Dispositifs de sécurité de la gamme Cisco ASA 5500
- Dispositifs de sécurité de la gamme Cisco PIX 500
- Négociation IPSec/Protocoles IKE
- Support et documentation techniques - Cisco Systems