# PIX/ASA 7.x : Activer/Désactiver la communication entre les interfaces

## Contenu



# Introduction

Ce document fournit un exemple de configuration pour différents types de communications entre les interfaces sur le dispositif de sécurité ASA/PIX.

# Conditions préalables

## Conditions requises

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

- Adresses IP et affectation de passerelle par défaut
- Connectivité réseau physique entre les périphériques
- N° de port de communication identifié pour le service mis en application

## Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Appliances de sécurité adaptables exécutant la version 7.x et ultérieure
- Serveurs Windows 2003
- Stations de travail Windows XP

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 les versions de matériel et de logiciel suivantes :

- Pare-feux de la gamme 500 PIX qui exécutent la version 7.x et ultérieure

### Conventions

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

## Informations générales

Ce document trace les grandes lignes des étapes requises pour permettre la communication entre les différentes interfaces. Des types de communication de ce type sont discutés :

1. Communication des hôtes qui se trouvent sur l'extérieur requérant l'accès aux ressources situées dans le DMZ
2. Communication des hôtes sur le réseau interne qui ont besoin d'accéder aux ressources situées dans le DMZ
3. Communication des hôtes qui se trouvent sur l'intérieur et le réseau DMZ et qui requièrent l'accès aux ressources sur l'extérieur

### NAT

Dans notre exemple, nous utilisons la traduction d'adresses de réseau (NAT) et la traduction d'adresses de port (PAT) dans notre configuration. La traduction d'adresses substitue la vraie adresse (locale) dans un paquet par une adresse mappée (globale) qui est routable sur le réseau de destination. La NAT est composée de deux étapes : le processus dans lequel une vraie adresse est traduite en une adresse mappée, puis le processus pour annuler la traduction pour le trafic qui revient. Il y a deux formes de traduction d'adresses que nous utilisons dans ce guide de configuration : Statique et dynamique.

Les traductions dynamiques permettent à chaque hôte d'utiliser une adresse ou un port différent pour chaque traduction ultérieure. Des traductions dynamiques peuvent être utilisées quand les hôtes locaux partagent ou « sont masqués derrière » une ou plusieurs adresses globales communes. Dans ce mode, une adresse locale ne peut pas réserver de manière permanente une

adresse globale pour la traduction. Au lieu de cela, soit plusieurs adresses sont traduites en une, soit plusieurs adresses sont traduites en plusieurs. Les entrées de traduction sont créées au fur et à mesure des besoins. Dès qu'une entrée de traduction est libre, elle est supprimée et libérée pour d'autres hôtes locaux. Ce type de traduction est le plus utile pour les connexions sortantes, dans lesquelles une adresse dynamique ou un numéro de port est affecté(e) aux hôtes internes seulement lorsque ces connexions sont établies. Il y a deux formes de traduction d'adresses dynamiques :

- NAT dynamique - Des adresses locales sont traduites en adresse globale disponible dans un pool. La traduction se produit au coup par coup. Ainsi il est possible d'épuiser le pool d'adresses globales si un plus grand nombre d'hôtes locaux ont besoin de la traduction à un moment donné.
- Surcharge NAT (PAT) - Des adresses locales sont traduites en une adresse globale simple ; chaque connexion est unique lorsque le numéro de port de poids fort suivant disponible de l'adresse globale est attribué comme source de connexion. La traduction se produit sur une base « plusieurs adresses en une » car beaucoup d'hôtes locaux partagent une adresse globale commune.

La traduction statique crée une traduction fixe de l'adresse réelle en adresse mappée. Une configuration NAT statique mappe la même adresse pour chaque connexion d'un hôte et est une règle persistante de traduction. Des traductions d'adresse statique sont utilisées quand un hôte interne ou local doit avoir la même adresse globale pour chaque connexion. La traduction d'adresses se produit adresse par adresse. Des traductions statiques peuvent être définies pour un hôte unique ou pour toutes les adresses contenues dans un sous-réseau IP.

La principale différence entre NAT dynamique et une plage d'adresses pour la NAT statique est que la NAT statique permet à un hôte distant de se connecter à un hôte traduit (si une liste d'accès le lui permet), alors que la NAT dynamique ne le permet pas. Vous avez besoin également d'un nombre équivalent d'adresses mappées avec la NAT statique.

L'appliance de sécurité traduit une adresse quand une règle NAT correspond au trafic. Si aucune règle NAT ne s'applique, le traitement du paquet se poursuit. L'exception se produit lorsque vous activez le contrôle NAT. Le contrôle NAT requiert que les paquets qui passent d'une interface à sécurité élevée (à l'intérieur) à une sécurité moins élevée (à l'extérieur) correspondent à une règle NAT. Dans le cas contraire, le traitement du paquet est arrêté. Afin d'afficher les informations de configuration communes, consultez le document PIX/ASA 7.x NAT et PAT. Pour une meilleure compréhension de la NAT, reportez-vous au guide Fonctionnement de NAT.

**Conseil :** Toutes les fois que vous modifiez la configuration NAT, il est recommandé d'effacer les traductions NAT actuelles. Vous pouvez effacer la table de traduction avec la commande **clear xlate**. **Cependant, faites attention quand vous faites ceci** car la suppression de la table de traduction déconnecte toutes les connexions actuelles qui utilisent des traductions. L'alternative à la suppression de la table de traduction est d'attendre que les traductions actuelles expirent, mais ceci n'est pas recommandé parce qu'un comportement inhabituel peut en résulter lorsque de nouvelles connexions sont créées avec les nouvelles règles.

## Niveaux de sécurité

Les valeurs de niveau de sécurité vérifient comment les hôtes/périphériques des différentes interfaces interagissent les uns avec les autres. Par défaut, les hôtes/périphériques connectés aux interfaces de niveau de sécurité élevé peuvent accéder à des hôtes/périphériques connectés à une interface de niveau de sécurité bas. Les hôtes/périphériques connectés aux interfaces de

niveau de sécurité bas ne peuvent pas accéder aux hôtes/périphériques connectés à des interfaces de niveau de sécurité élevé sans l'autorisation des listes d'accès.

La commande **security-level** est nouvelle dans la version 7.0 et remplace la partie de la commande **nameif** qui attribuait le niveau de sécurité d'une interface. Deux interfaces, l'interface « intérieure » et l'interface « extérieure » possèdent des niveaux de sécurité par défaut, mais ceux-ci peuvent être ignorés via la commande **security-level**. Si vous nommez une interface « intérieure », elle aura un niveau de sécurité par défaut de 100 ; une interface « extérieure » aura un niveau de sécurité par défaut de 0. Toutes les autres interfaces nouvellement ajoutées ont un niveau de sécurité par défaut de 0. Afin d'attribuer un nouveau niveau de sécurité à une interface, utilisez la commande **security-level** dans le mode commande de l'interface. Les niveaux de sécurité s'étendent de 1-100.

**Remarque:** Les niveaux de sécurité sont utilisés seulement pour déterminer comment le pare-feu inspecte et gère le trafic. Par exemple, le trafic passant d'une interface de niveau de sécurité élevé vers une interface de niveau de sécurité bas est transféré avec des stratégies par défaut moins rigoureuses que le trafic qui provient d'une interface de niveau de sécurité inférieur et va vers une interface de niveau de sécurité élevé. Pour plus d'informations sur les niveaux de sécurité, consultez le guide Référence des commandes PIX/ASA 7.x.

ASA/PIX 7.x propose également la nouvelle fonctionnalité de configuration de plusieurs interfaces avec le même niveau de sécurité. Par exemple, plusieurs interfaces connectées aux partenaires ou à d'autres DMZ peuvent toutes se voir attribuer le niveau de sécurité de 50. Par défaut, ces interfaces de mêmes niveaux de sécurité ne peuvent pas communiquer entre elles. Afin de contourner le problème, la commande **same-security-traffic permit inter-interface** a été ajoutée. Cette commande autorise la communication entre les interfaces du même niveau de sécurité. Pour plus d'informations sur la communication entre les interfaces de même niveau de sécurité, consultez le Guide de référence des commandes Configuration des paramètres d'interface et consultez cet exemple.

## ACL

Les listes de contrôle d'accès se composent typiquement de plusieurs entrées de contrôle d'accès (ACE) organisées intérieurement par l'appliance de sécurité dans une liste liée. Les ACE décrivent un ensemble du trafic comme celui provenant d'un hôte ou d'un réseau et indiquent une action à appliquer à ce trafic, généralement une autorisation ou un refus. Quand un paquet est soumis au contrôle de la liste d'accès, l'appliance de sécurité Cisco recherche cette liste liée des ACE afin de rechercher une entrée qui correspond au paquet. **La première ACE qui correspond à l'appliance de sécurité est celle qui est appliquée au paquet.** Une fois une correspondance trouvée, l'action de cette ACE (autorisation ou refus) est appliqué au paquet.

Une seule liste d'accès est autorisée par interface, par direction. Ceci signifie que vous pouvez seulement avoir une liste d'accès qui s'applique au trafic d'arrivée sur une interface et une liste d'accès qui s'applique pour trafic sortant sur une interface. Les listes d'accès qui ne sont pas appliquées aux interfaces, telles que ACL NAT, sont illimitées.

**Remarque:** Par défaut, toutes les listes d'accès ont une ACE implicite à la fin qui refuse tout le trafic. Ainsi, tout trafic qui ne correspond à aucune ACE entrée dans la liste d'accès correspond au refus implicite à la fin et est perdu. Vous devez avoir au moins une autorisation indiquée dans une liste d'accès d'interface pour que le trafic circule. Sans autorisation, tout le trafic est refusé.

**Remarque:** La liste d'accès est mise en application avec les commandes **access-list** et **access-**

**group**. Ces commandes sont utilisées au lieu des commandes **conduit** et **outbound** qui étaient utilisées dans les versions antérieures du logiciel pare-feu PIX. Pour plus d'informations sur les ACL, consultez la rubrique Configuration des listes d'accès IP.

# Configurez

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

**Remarque:** Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

## Diagramme du réseau

Ce document utilise cette configuration du réseau :

## Configuration initiale

Ce document utilise les configurations suivantes :

- Avec cette configuration de pare-feu de base, il n'y a actuellement aucune instruction NAT/STATIC.
- Aucune ACL n'est appliquée, ainsi l'ACE implicite deny any any est actuellement utilisée.

**Nom du périphérique 1**

```
ASA-AIP-CLI(config)#show running-config ASA Version
7.2(2) ! hostname ASA-AIP-CLI domain-name corp.com
enable password WwXYvtKrnjXqGbu1 encrypted names !
interface Ethernet0/0 nameif Outside security-level 0 ip
address 172.22.1.163 255.255.255.0 ! interface
Ethernet0/1 nameif inside security-level 100 ip address
172.20.1.1 255.255.255.0 ! interface Ethernet0/2 nameif
DMZ security-level 50 ip address 192.168.1.1
255.255.255.0 ! interface Ethernet0/3 nameif DMZ-2-
testing security-level 50 ip address 192.168.10.1
255.255.255.0 ! interface Management0/0 shutdown no
nameif no security-level no ip address ! passwd
2KFQnbNIdI.2KYOU encrypted ftp mode passive dns server-
group DefaultDNS domain-name corp.com pager lines 24 mtu
inside 1500 mtu Outside 1500 mtu DMZ 1500 no failover
icmp unreachable rate-limit 1 burst-size 1 no asdm
history enable arp timeout 14400 nat-control route
Outside 0.0.0.0 0.0.0.0 172.22.1.1 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 mgcp-pat 0:05:00 timeout sip
0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-
disconnect 0:02:00 timeout uauth 0:05:00 absolute no
snmp-server location no snmp-server contact snmp-server
enable traps snmp authentication linkup linkdown
coldstart telnet timeout 5 ssh timeout 5 console timeout
0 ! class-map inspection_default match default-
inspection-traffic ! ! policy-map type inspect dns
preset_dns_map parameters message-length maximum 512
policy-map global_policy class inspection_default
```

```
inspect dns preset_dns_map 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 prompt hostname context
Cryptochecksum:4b2f54134e685d11b274ee159e5ed009 : end
ASA-AIP-CLI(config)#
```

## Communication DMZ/intérieur

Afin d'autoriser la communication entre le DMZ et les hôtes de réseau interne, utilisez ces commandes. Dans cet exemple, un serveur Web sur le DMZ doit accéder à un serveur DNS et AD à l'intérieur.

1. Créez une entrée NAT statique pour le serveur AD/DNS sur le DMZ. La NAT statique crée une traduction fixe d'une vraie adresse pour une adresse mappée. Cette adresse mappée est une adresse que les hôtes DMZ peuvent employer pour accéder au serveur à l'intérieur sans devoir connaître la vraie adresse du serveur. Cette commande mappe l'adresse du DMZ 192.168.2.20 sur la vraie adresse intérieure 172.20.1.5.`ASA-AIP-CLI(config)# static (inside,DMZ) 192.168.2.20 172.20.1.5 netmask 255.255.255.255`
2. Des ACL sont requises pour autoriser une interface d'un niveau de sécurité bas à accéder à un niveau de sécurité plus élevé. Dans cet exemple, nous donnons au serveur Web placé sur le DMZ un accès (sécurité 50) au serveur AD/DNS (sécurité 100) sur l'intérieur avec ces ports de service spécifiques : DNS, Kerberos et LDAP.`ASA-AIP-CLI(config)# access-list DMZtoInside extended permit udp host 192.168.1.10 host 192.168.2.20 eq domainASA-AIP-CLI(config)# access-list DMZtoInside extended permit tcp host 192.168.1.10 host 192.168.2.20 eq 88ASA-AIP-CLI(config)# access-list DMZtoInside extended permit udp host 192.168.1.10 host 192.168.2.20 eq 389`**Remarque:** Les ACL autorisent l'accès à l'adresse mappée du serveur AD/DNS qui a été créé dans cet exemple, mais pas à la vraie adresse interne.
3. Dans cette étape, avec cette commande, vous appliquez l'ACL à l'interface DMZ dans la direction entrante :`ASA-AIP-CLI(config)# access-group DMZtoInside in interface DMZ`**Remarque:** Si vous voulez bloquer ou désactiver le port 88, le trafic de DMZ vers l'intérieur, par exemple, utilisez cette commande :`ASA-AIP-CLI(config)# no access-list DMZtoInside extended permit tcp host 192.168.1.10 host 192.168.2.20 eq 88`**Conseil :** Toutes les fois que vous modifiez la configuration NAT, il est recommandé d'effacer les traductions NAT actuelles. Vous pouvez effacer la table de traduction avec la commande **clear xlate**. **Cependant, faites attention quand vous faites ceci** car la suppression de la table de traduction déconnecte toutes les connexions actuelles qui utilisent des traductions. L'alternative à la suppression de la table de traduction est d'attendre que les traductions actuelles expirent, mais ceci n'est pas recommandé parce qu'un comportement inhabituel peut en résulter lorsque de nouvelles connexions sont créées avec les nouvelles règles.D'autres configurations courantes incluent les suivantes :Serveurs de messagerie dans le DMZAccès SSH à l'intérieur et à l'extérieurSessions autorisées de bureau distant par des périphériques PIX/ASAAutres solutions DNS pour une utilisation dans le DMZ

## Communication Internet/DMZ

Afin de permettre la communication entre les utilisateurs d'Internet, ou l'interface externe (sécurité 0), et un serveur Web qui se trouve dans le DMZ (sécurité 50), utilisez ces commandes :

1. Créez une traduction statique pour le serveur Web dans le DMZ vers l'extérieur. La NAT statique crée une traduction fixe d'une vraie adresse pour une adresse mappée. Cette adresse mappée est une adresse que les hôtes sur Internet peuvent employer pour accéder au serveur Web sans connaître la vraie adresse du serveur. Cette commande mappe l'adresse extérieure 172.22.1.25 sur la vraie adresse du DMZ 192.168.1.10.`ASA-AIP-CLI(config)# static (DMZ,Outside) 172.22.1.25 192.168.1.10 netmask 255.255.255.255`
2. Créez une ACL qui autorise les utilisateurs de l'extérieur à accéder au serveur Web via l'adresse mappée. Notez que le serveur Web héberge également le FTP.`ASA-AIP-CLI(config)# access-list OutsidetoDMZ extended permit tcp any host 172.22.1.25 eq wwwASA-AIP-CLI(config)# access-list OutsidetoDMZ extended permit tcp any host 172.22.1.25 eq ftp`
3. La dernière étape de cette configuration est d'appliquer l'ACL à l'interface extérieure pour le trafic dans la direction entrante.`ASA-AIP-CLI(config)# access-group OutsidetoDMZ in interface Outside`**Remarque:** Souvenez-vous, vous pouvez seulement appliquer une liste d'accès par interface, par direction. Si vous avez déjà une ACL entrante appliquée à l'interface extérieure, vous ne pouvez pas appliquer cette ACL. Au lieu de cela, ajoutez les ACE de cet exemple dans l'ACL actuelle qui est appliquée à l'interface.**Remarque:** Si vous voulez bloquer ou désactiver le trafic FTP de l'Internet vers le DMZ, par exemple, utilisez ceci :`ASA-AIP-CLI(config)# no access-list OutsidetoDMZ extended permit tcp any host 172.22.1.25 eq ftp`**Conseil :** Toutes les fois que vous modifiez la configuration NAT, il est recommandé d'effacer les traductions NAT actuelles. Vous pouvez effacer la table de traduction avec la commande **clear xlate**. **Cependant, faites attention quand vous faites ceci** car la suppression de la table de traduction déconnecte toutes les connexions actuelles qui utilisent des traductions. L'alternative à la suppression de la table de traduction est d'attendre que les traductions actuelles expirent, mais ceci n'est pas recommandé parce qu'un comportement inhabituel peut en résulter lorsque de nouvelles connexions sont créées avec les nouvelles règles.

## Communication intérieur/DMZ/Internet

Dans ce scénario, des hôtes situés sur l'interface interne (sécurité 100) de l'appliance de sécurité sont équipés d'un accès à Internet sur l'interface externe (sécurité 0). Pour ce faire, utilisez la surcharge PAT ou NAT, forme de NAT dynamique. À la différence des autres scénarios, une ACL n'est pas requise dans ce cas car les hôtes sur une interface de sécurité élevée accèdent aux hôtes sur une interface de basse sécurité.

1. Spécifiez les sources du trafic qui doit être traduit. Ici la règle NAT numéro **1** est définie, et tout le trafic de l'intérieur et des hôtes DMZ est autorisé.`ASA-AIP-CLI(config)# nat (inside) 1 172.20.1.0 255.255.255.0ASA-AIP-CLI(config)# nat (inside) 1 192.168.1.0 255.255.255.0`
2. Spécifiez l'adresse, le pool d'adresses ou l'interface que le trafic avec traduction d'adresses réseau doit utiliser quand il accède à l'interface externe. Dans ce cas, la PAT est effectuée avec l'adresse de l'interface externe. C'est particulièrement utile quand l'adresse de l'interface externe n'est pas connue à l'avance, comme dans une configuration DHCP. Ici, la commande globale est émise avec le même ID NAT de **1**, qui le lie aux règles NAT du même identifiant.`ASA-AIP-CLI(config)# global (Outside) 1 interface`

**Conseil :** Toutes les fois que vous modifiez la configuration NAT, il est recommandé d'effacer les traductions NAT actuelles. Vous pouvez effacer la table de traduction avec la commande **clear xlate**. **Cependant, faites attention quand vous faites ceci** car la suppression de la table de traduction déconnecte toutes les connexions actuelles qui utilisent des traductions. L'alternative à la suppression de la table de traduction est d'attendre que les traductions actuelles expirent, mais ceci n'est pas recommandé parce qu'un comportement inhabituel peut en résulter lorsque de

nouvelles connexions sont créées avec les nouvelles règles.

**Remarque:** Si vous voulez bloquer le trafic de la zone de sécurité élevée (à l'intérieur) vers la zone de sécurité basse (internet/DMZ), créez une ACL et appliquez-la comme entrante à l'intérieur de la interface interne du PIX/ASA comme arrivée.

**Remarque: Exemple :** Afin de bloquer le trafic du port 80 de l'hôte 172.20.1.100 sur le réseau interne à l'Internet, utilisez ceci :

```
ASA-AIP-CLI(config)#access-list InsidetoOutside extended deny tcp host 172.20.1.100 any eq www
ASA-AIP-CLI(config)#access-list InsidetoOutside extended permit tcp any any
ASA-AIP-CLI(config)#access-group InsidetoOutside in interface inside
```

### Communication au même niveau de sécurité

La configuration initiale montre que les interfaces « DMZ » et « DMZ-2-testing » sont configurées avec le niveau de sécurité (50) ; par défaut, ces deux interfaces ne peuvent pas communiquer. Ici, nous permettons à ces interfaces de communiquer grâce à cette commande :

```
ASA-AIP-CLI(config)# same-security-traffic permit inter-interface
```

**Remarque:** Même si la commande « same-security traffic permit inter-interface » a été configurée pour les interfaces de même niveau de sécurité (« DMZ » et « DMZ-2-testing »), une règle de traduction (statique/dynamique) est toujours nécessaire pour accéder aux ressources placées dans ces interfaces.

## Dépannez

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

- Dépannage des connexions via PIX et ASA
- Configurations NAT Vérification NAT et dépannage

## Informations connexes

- Référence des commandes Cisco ASA
- Référence des commandes Cisco PIX
- Messages d'erreur et messages système Cisco ASA
- Messages d'erreur et messages système Cisco PIX
- Support et documentation techniques - Cisco Systems