PIX/ASA 7.x:啟用/禁用介面之間的通訊

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[相關產品](#)
[慣例](#)
[背景資訊](#)
[NAT](#)
[安全級別](#)
[ACL](#)
[設定](#)
[網路圖表](#)
[初始配置](#)
[DMZ到內部](#)
[網際網路到DMZ](#)
[內部/DMZ到網際網路](#)
[相同安全級別通訊](#)
[疑難排解](#)
[相關資訊](#)

簡介

本文檔為ASA/PIX安全裝置上的介面之間的各種通訊形式提供了一個示例配置。

必要條件

需求

嘗試此組態之前，請確保符合以下要求：

- IP地址和預設網關分配
- 裝置之間的物理網路連線
- 為實施的服務標識通訊埠#

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 運行軟體版本7.x及更高版本的自適應安全裝置
- Windows 2003伺服器
- Windows XP工作站

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

相關產品

此配置還可以用於以下硬體和軟體版本：

- 運行7.x及更高版本的PIX 500系列防火牆

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

背景資訊

本文檔概述了允許在不同介面之間傳輸通訊所需的步驟。下面將討論通訊形式：

1. 來自外部主機要求訪問DMZ中資源的通訊
2. 來自內部網路中需要訪問DMZ中資源的主機的通訊
3. 來自內部主機和DMZ網路中需要訪問外部資源的通訊

NAT

在我們的示例中，我們在配置中使用網路地址轉換(NAT)和埠地址轉換(PAT)。地址轉換將資料包中的實際地址（本地）替換為可在目標網路上路由的對映地址（全域性）。NAT由兩個步驟組成：將實際地址轉換為對映地址的過程，然後是恢復返回流量的轉換的過程。本配置指南中使用兩種地址轉換形式：靜態和動態。

動態轉換允許每台主機使用不同的地址或埠進行後續轉換。當本地主機共用或「隱藏」一個或多個通用全域性地址時，可以使用動態轉換。在此模式下，一個本地地址不能永久保留一個全域性地址進行轉換。相反，地址轉換以多對一或多對多的方式進行，轉換條目僅在需要時建立。一旦轉換條目不再使用，就會將其刪除並供其他本地主機使用。這種型別的轉換對於出站連線最有用，因為出站連線只能為內部主機分配動態地址或埠號。動態地址轉換有兩種形式：

- 動態NAT — 本地地址轉換為池中的下一個可用全域性地址。轉換以一對一的方式進行，因此，如果給定時間有較多的本地主機需要轉換，則可能會耗盡全域性地址池。
- NAT過載(PAT) — 本地地址轉換為單個全域性地址；當將全域性地址的下一個可用高位埠號指定為連線的源時，每個連線都是唯一的。轉換以多對一的方式進行，因為許多本地主機共用一個通用全域性地址。

靜態轉換建立實際地址到對映地址的固定轉換。靜態NAT配置按主機對映每個連線的相同地址，並且是持久轉換規則。當內部或本地主機需要為每個連線使用相同的全域性地址時，會使用靜態地址轉換。地址轉換以一對一的方式進行。可以為單個主機或IP子網中包含的所有地址定義靜態轉換。

動態NAT和靜態NAT地址範圍的主要區別在於，靜態NAT允許遠端主機發起到已轉換主機的連線（如果有允許該連線的訪問清單），而動態NAT則不允許。您還需要具有相同數量的具有靜態NAT的對映地址。

當NAT規則與流量匹配時，安全裝置轉換地址。如果沒有NAT規則匹配，則繼續處理資料包。例外是啟用NAT控制時。NAT控制要求從較高安全介面（內部）遍歷到較低安全級別（外部）的資料包與NAT規則匹配，否則資料包處理將停止。要檢視常見配置資訊，請參閱PIX/ASA 7.x NAT和PAT文檔。要深入瞭解NAT的工作方式，請參閱NAT的工作方式指南。

提示：每次更改NAT配置時，建議您清除當前的NAT轉換。您可以使用**clear xlate**命令清除轉換表。**但是，請謹慎執行此操作，因為**清除轉換表會斷開所有使用轉換的當前連線。清除轉換表的替代方法是等待當前轉換超時，但不建議這樣做，因為使用新規則建立新連線時可能會導致意外行為。

安全級別

安全級別值控制不同介面上的主機/裝置如何相互互動。預設情況下，連線到安全級別較高的介面的主機/裝置可以訪問連線到安全級別較低介面的主機/裝置。連線到具有較低安全介面的介面的主機/裝置無法訪問主機/裝置連線到具有較高安全介面的介面，而無需訪問清單的許可權。

security-level命令是7.0版的新命令，它取代了**nameif**命令中為介面分配安全級別的部分。兩個介面「inside」和「outside」具有預設安全級別，但是可以用**security-level命令覆蓋**它們。如果將介面命名為「inside」，則預設安全級別為100;名為「outside」的介面的預設安全級別為0。所有其他新新增的介面都收到預設安全級別為0。為了向介面分配新的安全級別，請在介面命令模式下使用**security-level**命令。安全級別範圍為1-100。

注意：安全級別僅用於確定防火牆如何檢查和處理流量。例如，與從較低安全介面流向較高安全介面的流量相比，從較高安全介面流向較低安全介面的流量使用不太嚴格的預設策略進行轉發。有關安全級別的詳細資訊，請參閱ASA/PIX 7.x命令參考指南。

ASA/PIX 7.x還引入了以相同安全級別配置多個介面的功能。例如，連線到合作夥伴或其他DMZ的多個介面的安全級別可以全部為50。預設情況下，這些相同的安全介面不能彼此通訊。為了解決此問題，引入了**same-security-traffic permit inter-interface**命令。此命令允許相同安全級別的介面之間的通訊。有關介面之間相同安全性的詳細資訊，請參閱《命令參考指南》配置介面引數，並參見以下示例。

ACL

訪問控制清單通常由多個訪問控制條目(ACE)組成，這些條目由安全裝置在連結清單中內部組織。ACE描述一組流量（例如來自主機或網路的流量），並列出要應用到該流量的操作（通常是允許或拒絕）。當資料包受到訪問清單控制時，思科安全裝置會搜尋此連結的ACE清單，以查詢與資料包匹配的ACE。**與安全裝置匹配的第一個ACE是應用於資料包的ACE。**找到相符專案後，該ACE中的動作（允許或拒絕）會套用到封包。

每個介面每個方向只允許一個訪問清單。這表示您只能有一個應用於介面上入站流量的訪問清單和一個應用於介面上出站流量的訪問清單。未應用於介面（如NAT ACL）的訪問清單不受限制。

注意：預設情況下，所有訪問清單在結尾都有一個拒絕所有流量的隱式ACE，因此，所有與您在訪問清單中輸入的任何ACE不匹配的流量都會與結尾的隱式deny匹配並被丟棄。介面訪問清單中必須至少有一個permit語句，流量才能流動。如果沒有permit語句，則會拒絕所有流量。

注意：訪問清單是使用**access-list**和**access-group命令**實現的。這些命令用來代替**conduit**和**outbound**命令，後者在早期版本的PIX防火牆軟體中使用。有關ACL的詳細資訊，請參閱設定IP存取清單。

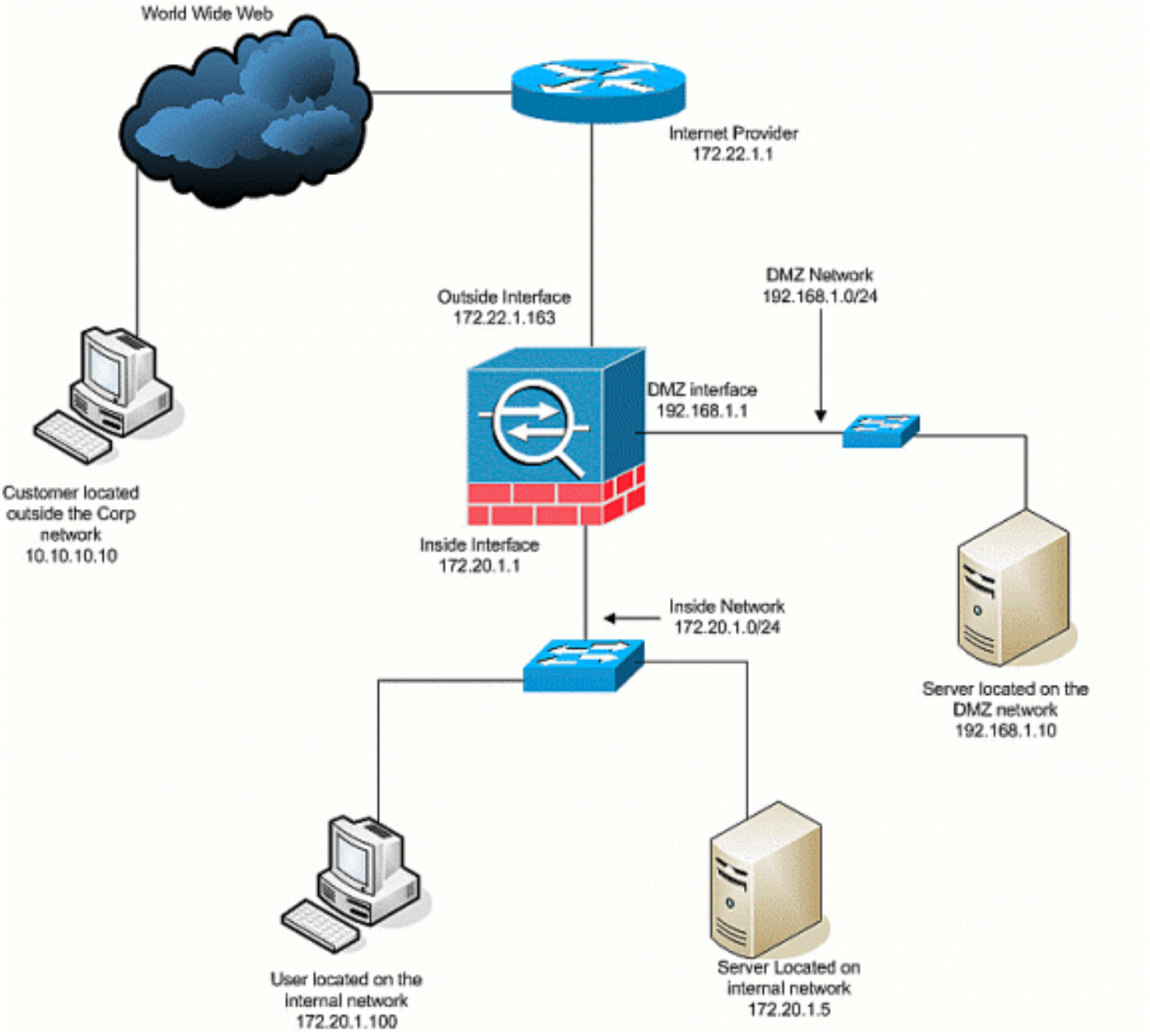
設定

本節提供用於設定本文件中所述功能的資訊。

註：使用 Command Lookup Tool(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

網路圖表

本檔案會使用以下網路設定：



初始配置

本檔案會使用以下設定：

- 使用此基本防火牆配置，當前沒有NAT/STATIC語句。
- 沒有應用任何ACL，因此目前使用`deny any any`的隱式ACE。

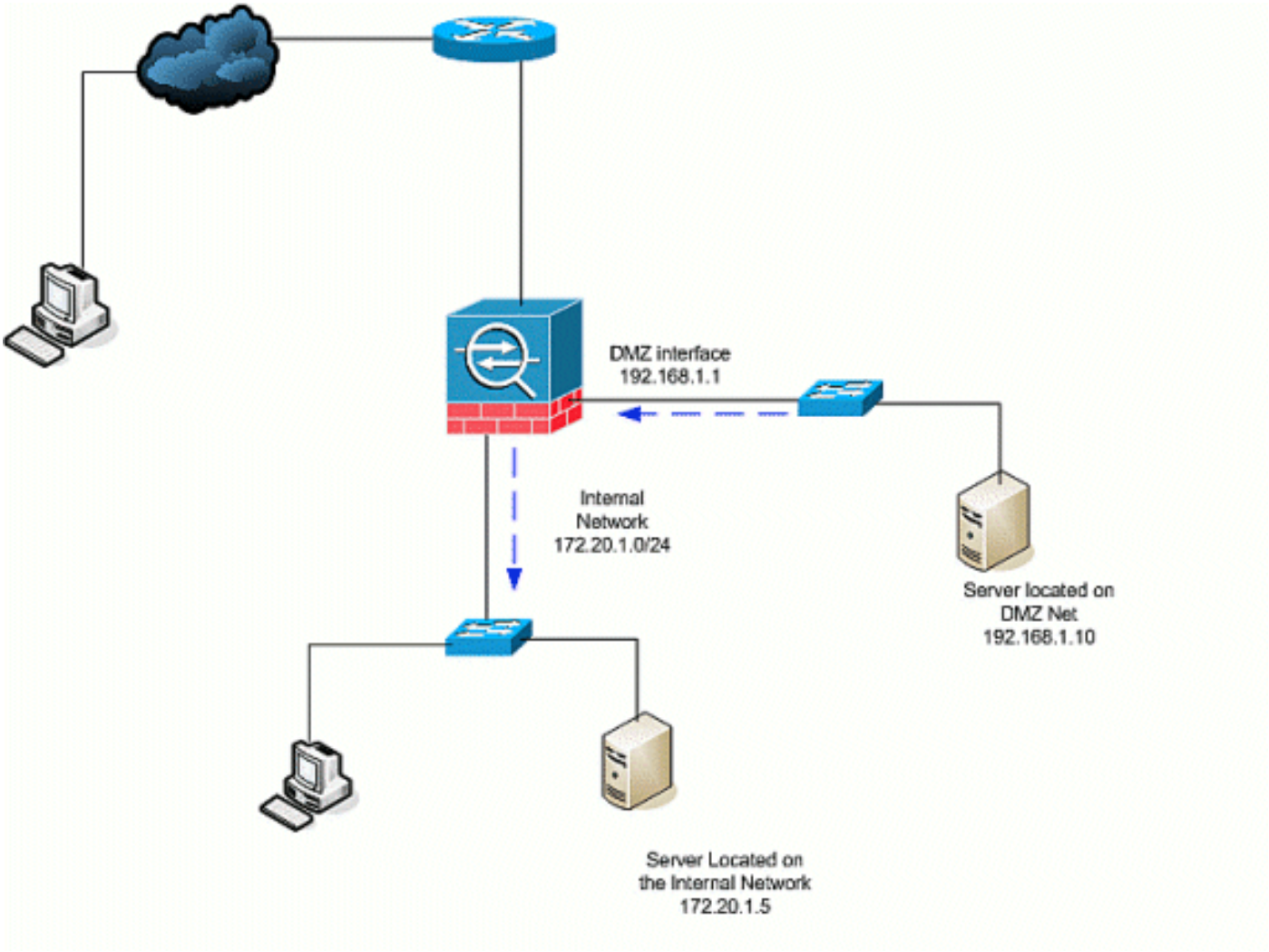
裝置名稱1
`ASA-AIP-CLI(config)#`**`show running-config`**

```
 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)#
```

DMZ到內部

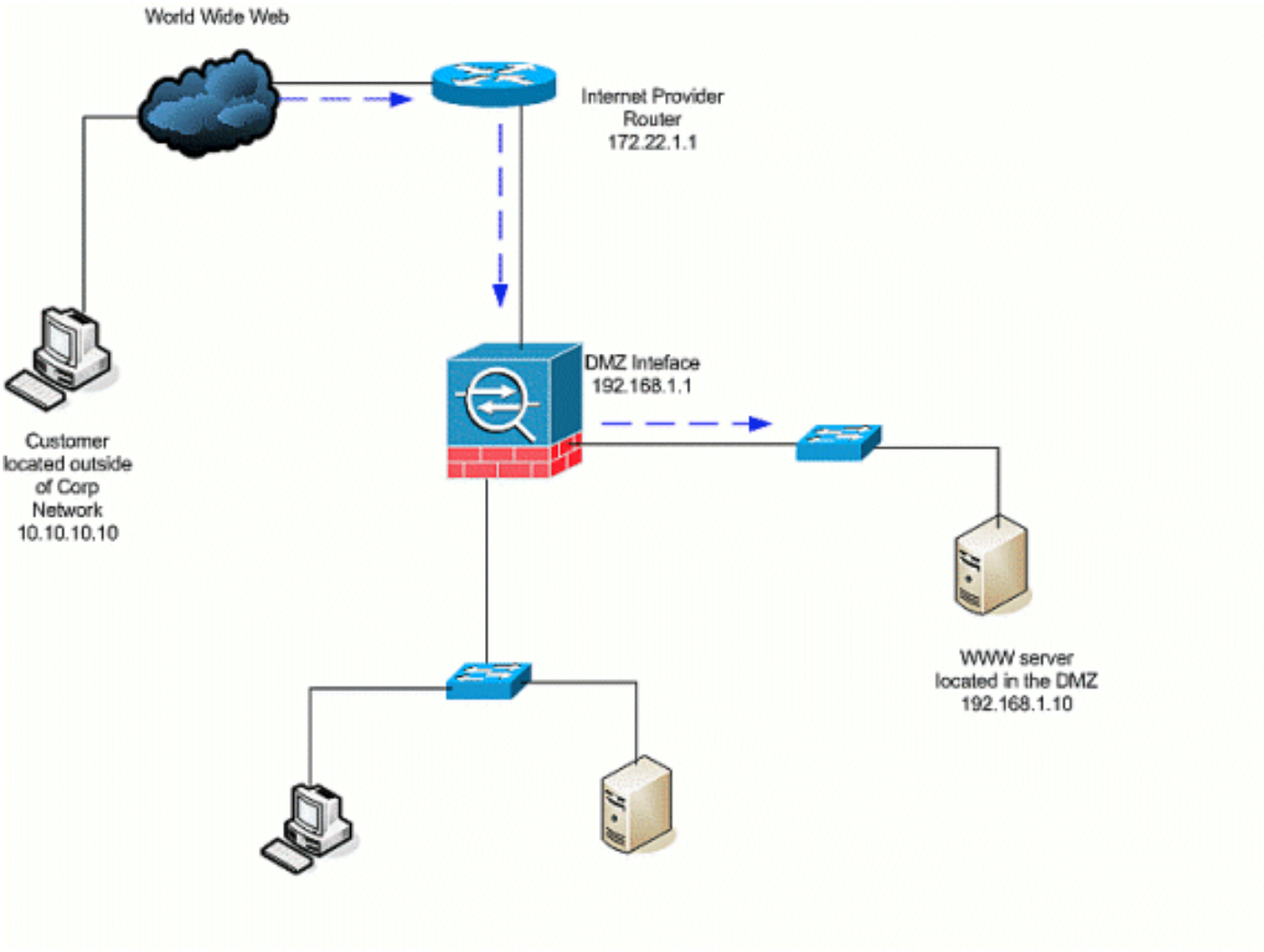
為了允許從DMZ到內部網路主機的通訊，請使用以下命令。在本示例中，DMZ上的Web伺服器需要訪問內部的AD和DNS伺服器。



1. 為DMZ上的AD/DNS伺服器建立靜態NAT條目。靜態NAT將實際地址轉換為對映地址。此對映地址是DMZ主機用來訪問內部伺服器的地址，無需知道伺服器的實際地址。此命令將DMZ地址192.168.2.20對映到實際內部地址172.20.1.5。`ASA-AIP-CLI(config)# static(insideDMZ)192.168.2.20 172.20.1.5 netmask 255.255.255.255`
2. ACL是允許安全級別較低的介面訪問更高安全級別所必需的。在本例中，我們為位於DMZ（安全50）上的Web伺服器提供訪問內部（安全100）的AD/DNS伺服器的許可權，這些特定服務埠為：DNS、Kerberos和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`**注意：**ACL允許訪問本示例中建立的AD/DNS伺服器的對映地址，而不是實際內部地址。
3. 在此步驟中，使用以下命令將ACL套用到傳入方向的DMZ介面：`ASA-AIP-CLI(config)# access-group DMZtoInside in interface DMZ`**註：如**果要阻止或禁用埠88，從DMZ到內部的流量，請使用以下命令：
   ```
   ASA-AIP-CLI(config)# no access-list DMZtoInside extended permit
   tcp host 192.168.1.10 host 192.168.2.20 eq 88
   ```
   提示：每次更改NAT配置時，建議您清除當前的NAT轉換。您可以使用**clear xlate**命令清除轉換表。**執行此操作時請小心，**因為清除轉換表會斷開所有使用轉換的當前連線。清除轉換表的替代方法是等待當前轉換超時，但不建議這樣做，因為使用新規則建立新連線時可能會導致意外行為。其他常見配置包括：DMZ中的郵件伺服器內部和外部的SSH訪問通過PIX/ASA設備允許的遠端案頭會話在DMZ中使用時的其他DNS解決方案

網際網路到DMZ

若要允許網際網路上的使用者或外部介面（安全0）與位於DMZ（安全50）中的Web伺服器進行通訊，請使用以下命令：



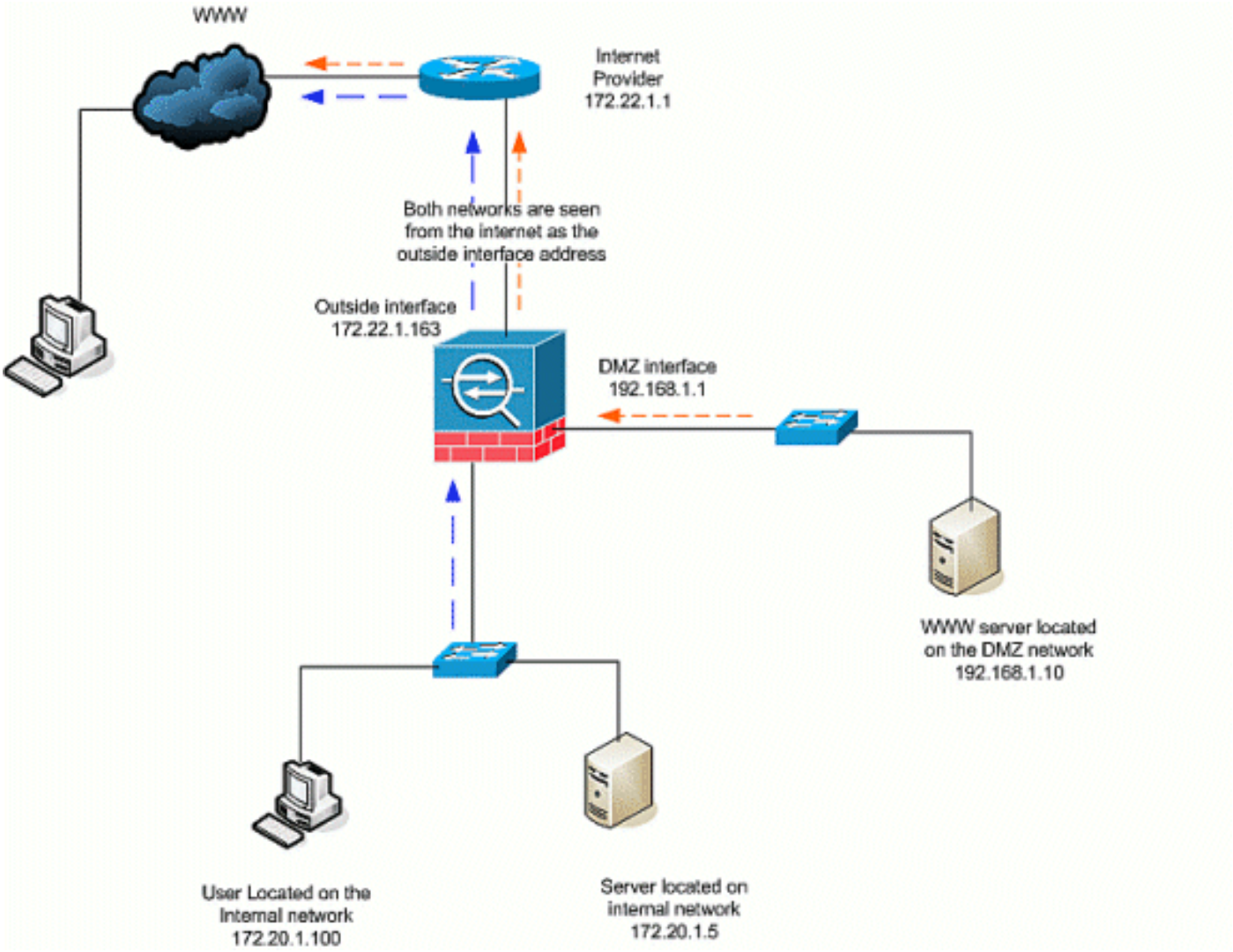
1. 為DMZ中的Web伺服器建立到外部的靜態轉換。靜態NAT將實際地址轉換為對映地址。此對映地址是Internet上的主機可用於訪問DMZ上的Web伺服器而不需要知道伺服器的實際地址的地址。此命令將外部地址172.22.1.25對映到實際DMZ地址192.168.1.10。`ASA-AIP-CLI(config)# static(DMZOutside)172.22.1.25 192.168.1.10 netmask 255.255.255.255`
2. 建立一個ACL，允許外部使用者通過對映地址訪問Web伺服器。請注意，Web伺服器也承載FTP。`ASA-AIP-CLI(config)# access-list OutsideDMZtcp any host 172.22.1.25 eq wwwASA-AIP-CLI(config)# access-list OutsideDMZtcp any host 172.22.1.25 eq ftp`
3. 此組態的最後一步是將ACL套用到外部介面，以便處理傳入方向的流量。`ASA-AIP-CLI(config)# access-group OutsideDMZ`**注意：**請記住，每個介面每個方向只能應用一個訪問清單。如果已將入站ACL應用於外部介面，則無法將此示例ACL應用於該介面。而是將本示例中的ACE新增到應用於介面的當前ACL中。**注意：**例如，如果要阻止或禁用從網際網路到DMZ的FTP流量，請使用以下命令：

   ```
   ASA-AIP-CLI(config)# no access-list OutsidetoDMZ extended permit
   tcp any host 172.22.1.25 eq ftp
   ```

   提示：每次更改NAT配置時，建議您清除當前的NAT轉換。您可以使用**clear xlate**命令清除轉換表。**執行此操作時請小心，**因為清除轉換表會斷開所有使用轉換的當前連線。清除轉換表的替代方法是等待當前轉換超時，但不建議這樣做，因為使用新規則建立新連線時可能會導致意外行為。

內部/DMZ到網際網路

在此場景中，位於安全裝置的內部介面（安全100）上的主機可訪問外部介面（安全0）上的網際網路。 這通過動態NAT的PAT（或NAT過載）形式實現。與其他情況不同，在此情況下不需要ACL，因為高安全性介面上的主機會訪問低安全性介面上的主機。



1. 指定必須轉換的流量的來源。此處定義了NAT規則編號**1**，並且允許來自內部和DMZ主機的所有流量。`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. 指定NATed流量訪問外部介面時必須使用的地址、地址池或介面。在這種情況下，使用外部介面地址執行PAT。這在事先不知道外部介面地址的情況下（例如DHCP配置中）尤其有用。這裡，使用相同的NAT ID **1**發出全域性命令，該命令將其繫結到同一ID的NAT規則。`ASA-AIP-CLI(config)# global(Outside)1 interface`

提示：每次更改NAT配置時，建議您清除當前的NAT轉換。您可以使用**clear xlate**命令清除轉換表。**執行此操作時請小心，**因為清除轉換表會斷開所有使用轉換的當前連線。清除轉換表的替代方法是等待當前轉換超時，但不建議這樣做，因為使用新規則建立新連線時可能會導致意外行為。

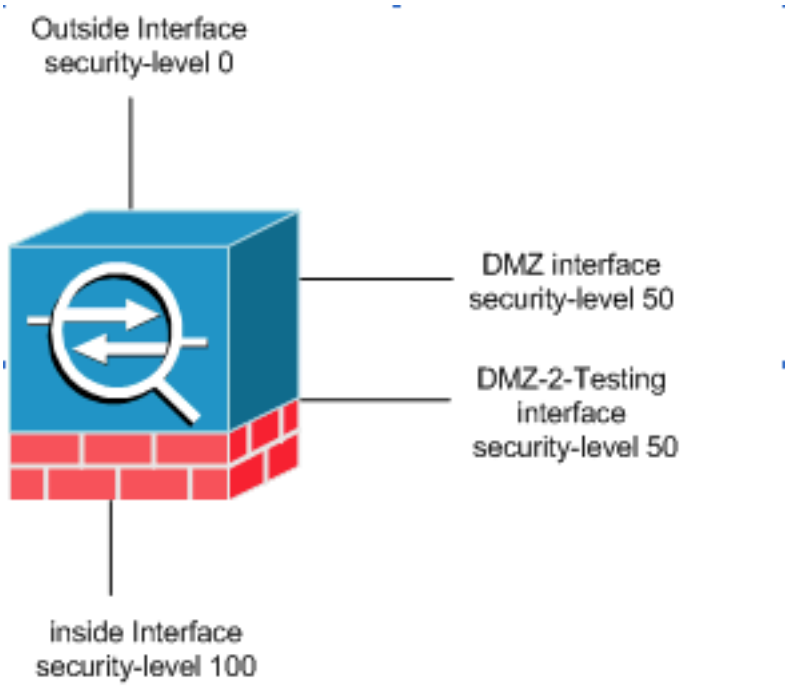
注意：如果您要阻止從較高安全區域（內部）到較低安全區域(internet/DMZ)的流量，請建立一個ACL並將其作為入站應用於PIX/ASA的內部介面。

附註： 範例：要阻止從內部網路上的主機172.20.1.100到Internet的埠80流量，請使用以下命令：

```
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
```

相同安全級別通訊

初始配置顯示，介面「DMZ」和「DMZ-2-testing」配置了安全級別(50);預設情況下，這兩個介面無法通訊。在此允許這些介面使用以下命令進行通訊：




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

注意：即使為相同的安全級別介面（「DMZ」和「DMZ-2-testing」）配置了「相同安全流量允許介面間」，它仍需要轉換規則（靜態/動態）來訪問位於這些介面中的資源。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

- 排除通過PIX和ASA的連線故障
- NAT配置檢驗NAT和故障排除

相關資訊

- Cisco ASA命令參考
- Cisco PIX命令參考
- Cisco ASA錯誤和系統消息
- Cisco PIX錯誤和系統消息
- 技術支援與文件 - Cisco Systems