PIX/ASA 7.x：启用/禁用接口之间的通信

目录

简介
先决条件
要求
使用的组件
相关产品
规则
背景信息
NAT
安全等级
ACL
配置
网络图
初始配置
DMZ 到内部
Internet 到 DMZ
内部/DMZ 到 Internet
同一安全等级上的通信
故障排除
相关信息

简介

本文档针对 ASA/PIX 安全设备上的接口之间各种形式的通信提供了一个配置示例。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- IP 地址和默认网关分配
- 设备之间的物理网络连接
- 为实施的服务标识的通信端口 #

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行软件版本 7.x 及更高版本的自适应安全设备
- Windows 2003 Server
- Windows XP 工作站

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

相关产品

此配置也可用于以下硬件和软件版本：

- 运行 7.x 及更高版本的 PIX 500 系列防火墙

规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

背景信息

本文档概述了允许在不同接口之间进行通信所需的步骤。讨论了如下所示的各种通信形式：

1. 位于外部的主机需要访问位于 DMZ 中的资源的通信
2. 内部网络上的主机需要访问位于 DMZ 中的资源的通信
3. 内部主机和 DMZ 网络上的主机需要访问外部资源的通信

NAT

在我们的示例中，我们在配置中使用网络地址转换 (NAT) 和端口地址转换 (PAT)。地址转换使用可在目标网络上路由的映射地址（全局）替代数据包中的实际地址（本地）。NAT 由两个步骤组成：将实际地址转换为映射地址的过程，以及随后对返回的数据流撤消转换的过程。在本配置指南中我们使用两种形式的地址转换：静态和动态。

动态转换允许每台主机对后续的每次转换都使用不同的地址或端口。本地主机共享一个或多个公用全局地址或“隐藏”在一个或多个公用全局地址后面时，可以使用动态转换。在此模式下，一个本地地址无法永久保留一个全局地址以用于转换。相反，地址转换在多对一或多对多的基础上进行，并且仅在需要转换条目时才创建它们。只要转换条目未在使用中，就会删除该条目并使其对其他本地主机可用。此类型的转换对于出站连接最有用。在出站连接中，仅在进行连接时才为内部主机分配动态地址或端口号。动态地址转换有两种形式：

- 动态 NAT - 将本地地址转换为池中下一个可用的全局地址。转换在一对一的基础上进行，因此如果在指定时间有大量的本地主机需要转换，则可能会用尽全局地址池中的地址。
- NAT 过载 (PAT) - 将本地地址转换为单一全局地址；将全局地址的下一个可用高位端口号指定为连接的源时，会将每个连接都设为唯一的。转换在多对一的基础上进行，因为多个本地主机共享一个公用全局地址。

静态转换创建实际地址到映射地址的固定转换。静态 NAT 配置为主机的每个连接映射同一个地址，是一个持久性转换规则。内部或本地主机需要对每个连接都具有同一全局地址时会使用静态地址转换。地址转换在一对一的基础上进行。可以为单个主机或一个 IP 子网中包含的所有地址定义静态转换。

动态 NAT 和一系列静态 NAT 地址之间的主要区别是：静态 NAT 允许远程主机发起到已转换主机

的连接（如果存在允许此操作的访问列表），而动态 NAT 却不允许这样。使用静态 NAT，还需要相同数量的映射地址。

当 NAT 规则与数据流匹配时，安全设备会转换地址。如果任何 NAT 规则都不匹配，则会继续进行数据包处理。但启用了 NAT 控制时例外。NAT 控制要求从安全等级较高的接口（内部）流向安全等级较低的接口（外部）的数据流与 NAT 规则匹配，否则将停止处理数据包。要查看常见配置信息，请参阅 PIX/ASA 7.x NAT 和 PAT 文档。要深入了解 NAT 的工作方式，请参阅 NAT 工作方式指南。

提示：无论何时更改NAT配置，建议清除当前NAT转换。可以使用 **clear xlate 命令清除转换表。但是，执行此操作时要小心，因为清除转换表时会断开所有使用转换的当前连接。**清除转换表的替代方法是等待当前转换超时，但并不建议使用此方法，因为使用新规则创建新连接时可能会导致意外行为。

安全等级

安全等级值用于控制不同接口上的主机/设备互相交互的方式。默认情况下，连接到安全等级较高的接口的主机/设备可以访问连接到安全等级较低的接口的主机/设备。如果没有访问列表的许可，连接到安全等级较低的接口的主机/设备不能访问连接到安全等级较高的接口的主机/设备。

security-level 命令是版本 7.0 的新功能，替换了用于为接口分配安全等级的 nameif 命令的一部分。两种接口（“inside”和“outside”接口）都具有默认安全等级，但可以使用 **security-level 命令覆盖这些安全等级。**如果将一个接口指定为“inside”，则它将被赋予的默认安全等级为 100；名为“outside”的接口的默认安全级别为0。所有其他新添加的接口的默认安全级别为0。要为接口分配新的安全级别，请在接口命令模式下使用**security-level**命令。安全等级范围为 1-100。

注意：安全级别仅用于确定防火墙如何检查和处理流量。例如，转发从安全性较高的接口流向安全性较低的接口的数据流时所用的默认策略，不像转发从安全性较低的接口流向安全性较高的接口的数据流时所用的默认策略那样严格。有关安全等级的详细信息，请参阅 ASA/PIX 7.x 命令参考指南。

ASA/PIX 7.x 还引入了配置多个具有相同安全等级的接口的功能。例如，连接到合作伙伴或其他DMZ的多个接口的安全级别都可指定为50。默认情况下，这些相同的安全接口无法相互通信。为了解决此问题，引入了 **same-security-traffic permit inter-interface 命令。**此命令允许安全等级相同的接口之间进行通信。有关接口之间的相同安全性的详细信息，请参阅《命令参考指南》中的配置接口参数，并参阅此示例。

ACL

访问控制列表通常由安全设备内部组织成一个链接列表的多个访问控制条目 (ACE) 组成。ACE 描述一组来自主机或网络等的数据流，并会列出对该数据流应用的操作（通常为允许或拒绝）。当数据包受到访问列表控制时，Cisco 安全设备会搜索 ACE 的该链接列表以找到与此数据包匹配的 ACE。**第一个与安全设备匹配的 ACE 将应用到数据包。**找到匹配的 ACE 后，会将该 ACE 中的操作（允许或拒绝）应用于数据包。

每个接口在每个方向上只允许一个访问列表。这意味着，在一个接口上，您只能有一个应用于入站数据流的访问列表和一个应用于出站数据流的访问列表。未应用于接口的访问列表（如 NAT ACL）不受此限制。

注意：默认情况下，所有访问列表的末尾都有一个隐式ACE，该ACE拒绝所有流量，因此，与您在访问列表中输入的任何ACE不匹配的所有流量都与末尾的隐式拒绝匹配并被丢弃。一个接口访问列表中必须至少具有一个 permit 语句才能使数据流流动。如果没有 permit 语句，则将拒绝所有数据

流。

注意：访问列表是使用access-list**和access-group**命**令实现**的。应使用这些命令，而不使用 PIX 防火墙软件的早期版本中使用的 **conduit 和 outbound 命令。**有关 ACL 的详细信息，请参阅配置 IP 访问列表。

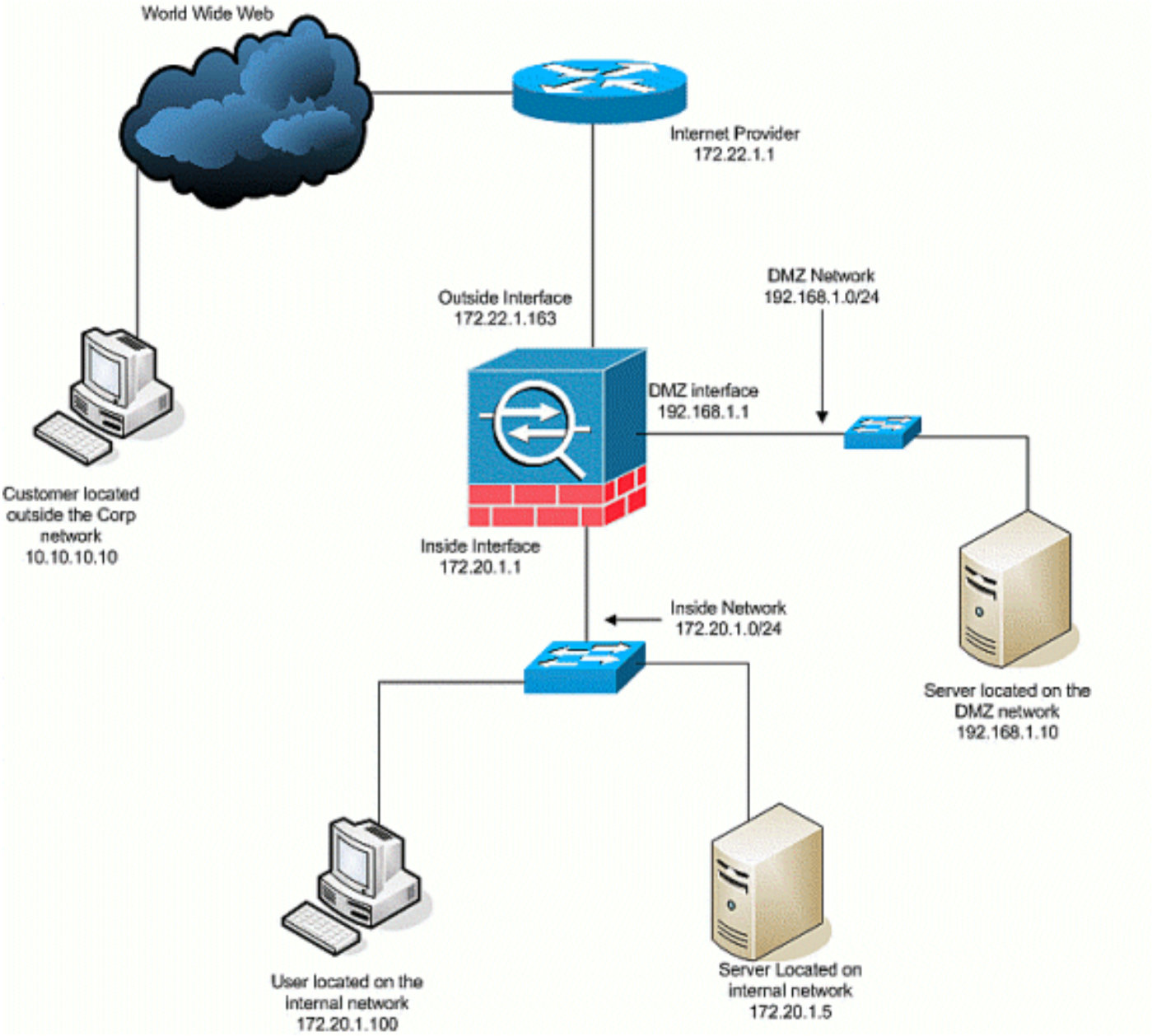
配置

本部分提供有关如何配置本文档所述功能的信息。

注意：使用命令查找工具(仅限注册客户)可获取有关本节中使用的命令的详细信息。

网络图

本文档使用以下网络设置：



初始配置

本文档使用以下配置：

- 在此基本防火墙配置中，目前没有 NAT/STATIC 语句。
- 由于未应用 ACL，因此目前使用隐式 ACE deny any any

设备名称 1

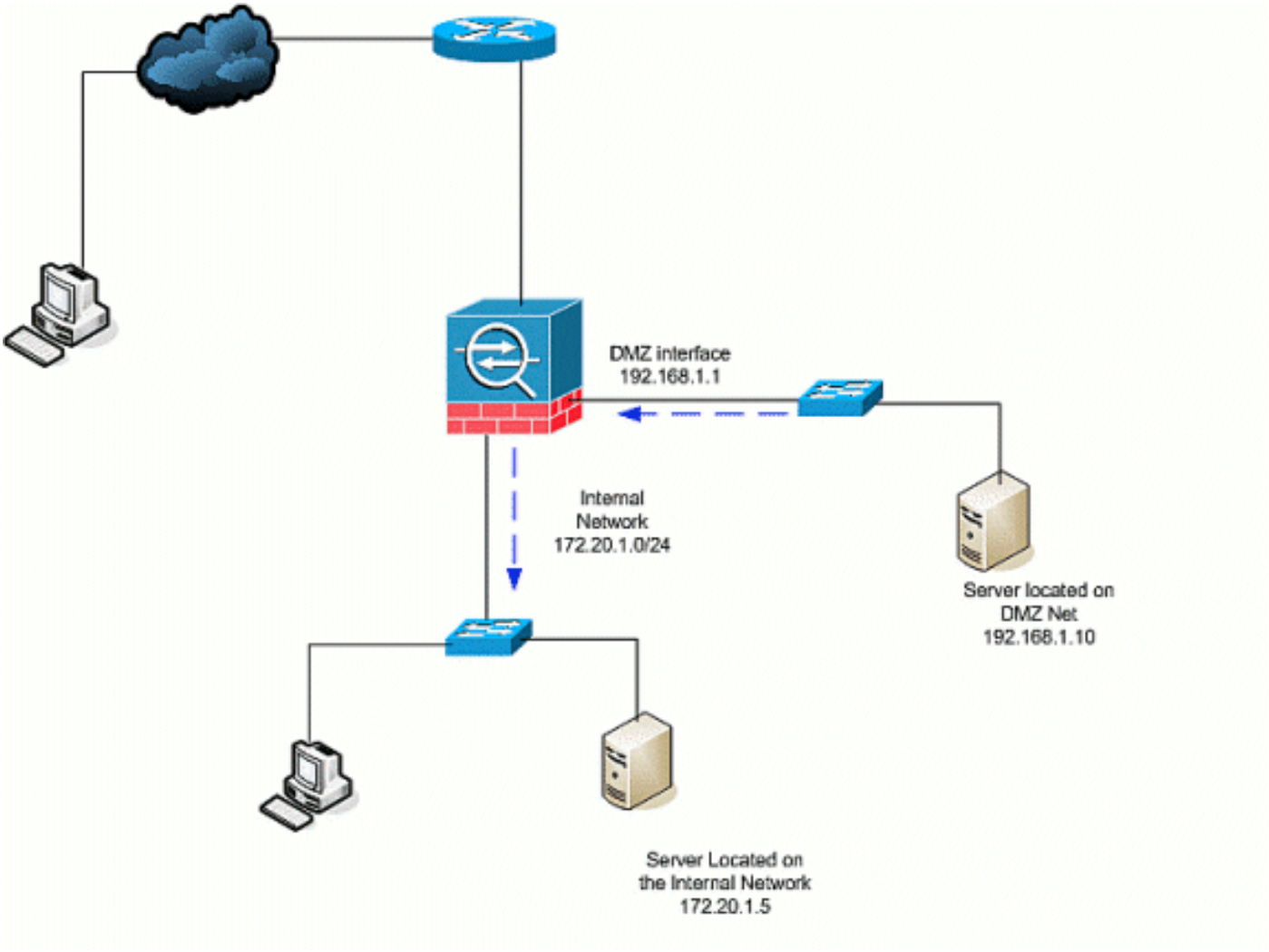
```
ASA-AIP-CLI(config)#show running-config

 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 到内部

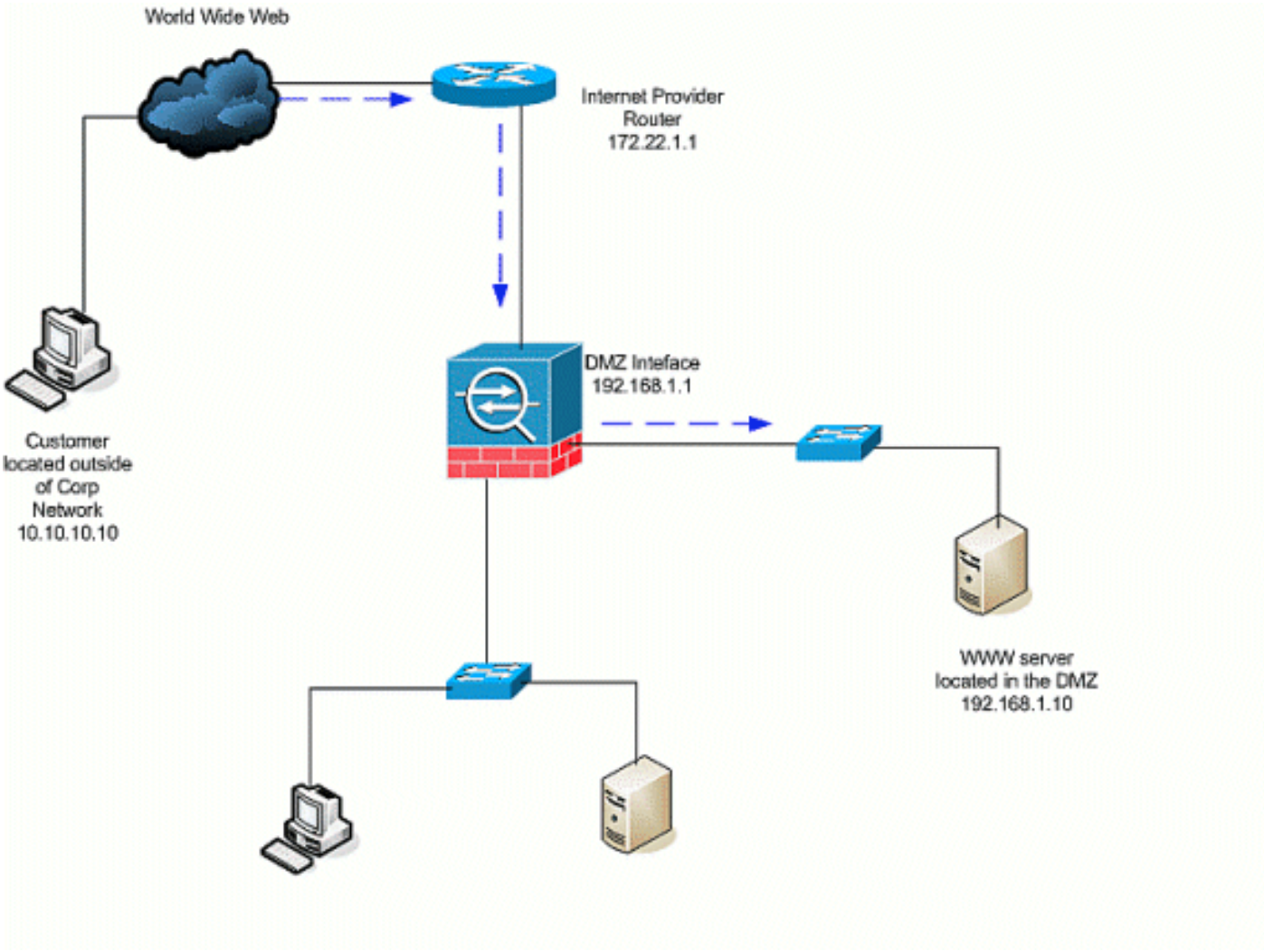
要允许从 DMZ 到内部网络主机的通信，请使用这些命令。在本示例中，DMZ 上的 Web 服务器需要访问内部的 AD 和 DNS 服务器。



1. 在 DMZ 上为 AD/DNS 服务器创建静态 NAT 条目。静态 NAT 会创建从实际地址到映射地址的固定转换。此映射地址是 DMZ 主机在无需知道内部服务器实际地址的情况下可用来访问该服务器的地址。以下命令将 DMZ 地址 192.168.2.20 映射到实际内部地址 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. 需要使用 ACL 来允许安全等级较低的接口访问安全等级较高的接口。在本示例中，我们使用以下特定服务端口授予位于 DMZ（安全等级为 50）上的 Web 服务器访问位于内部（安全等级为 100）的 AD/DNS 服务器的权限：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允许访问本示例中创建的AD/DNS服务器的映射地址，而不是实际内部地址。
3. 在此步骤中，使用以下命令将 ACL 应用到入站方向的 DMZ 接口：`ASA-AIP-CLI(config)# access-group DMZtoInside in interface DMZ`**注意：**如果要阻止或禁用端口88，则从DMZ到内部的流量，例如，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：无论何时更改NAT配置，建议清除当前NAT转换。可以使用 **clear xlate 命令清除转换表。执行此操作时要小心，因为清除转换表时会断开所有使用转换的当前连接。**清除转换表的替代方法是等待当前转换超时，但并不建议使用此方法，因为使用新规则创建新连接时可能会导致意外行为。其他常见配置包括以下各项：DMZ 中的邮件服务器内部和外部 SSH 访问通过 PIX/ASA 设备允许的远程桌面会话DMZ 中使用的其他 DNS 解决方案

Internet 到 DMZ

为了允许从 Internet 或外部接口（安全等级为 0）上的用户到位于 DMZ（安全等级为 50）中的 Web 服务器的通信，请使用这些命令：



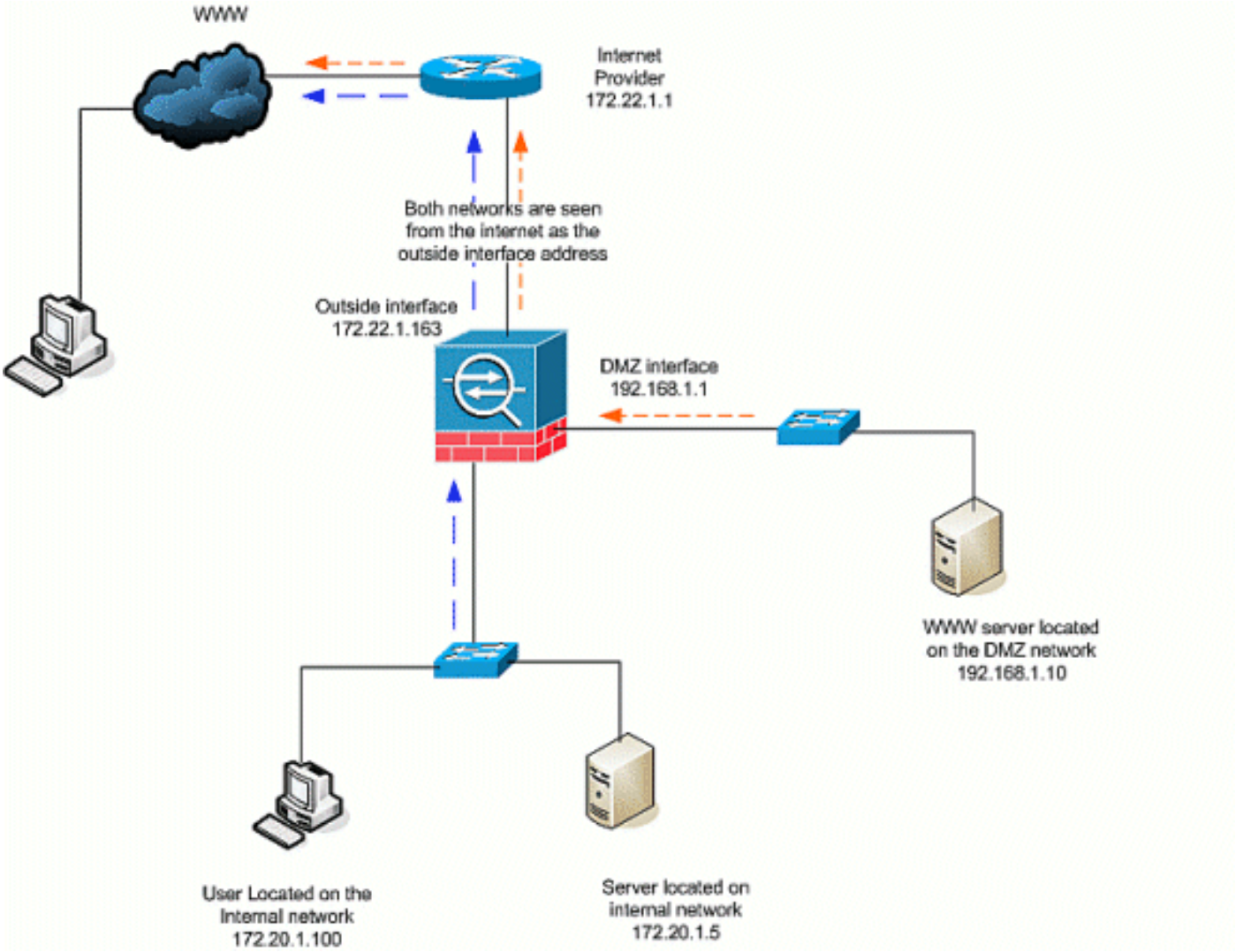
1. 创建从 DMZ 中的 Web 服务器到外部的静态转换。静态 NAT 会创建从实际地址到映射地址的固定转换。此映射地址是 Internet 上的主机在无需知道 DMZ 中 Web 服务器的实际地址的情况下可用来访问该服务器的地址。以下命令将外部地址 172.22.1.25 映射到实际 DMZ 地址 192.168.1.10。`ASA-AIP-CLI(config)# static (DMZ,Outside) 172.22.1.25 192.168.1.10 netmask 255.255.255.255`
2. 创建 ACL 以允许外部用户通过映射地址访问 Web 服务器。请注意，Web 服务器还托管 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. 此配置中的最后一步是将 ACL 应用到外部接口以用于入站方向的数据流。`ASA-AIP-CLI(config)# access-group OutsidetoDMZ in interface Outside`**注意：**请记住，每个接口、每个方向只能应用一个访问列表。如果已将一个入站 ACL 应用到外部接口，则您不能再将此示例 ACL 应用到该接口。而是应将此示例中的 ACE 添加到当前已应用于该接口的 ACL 中。**注意：**例如，如果要阻止或禁用从互联网到DMZ的FTP流量，请使用以下命令：

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

   提示：无论何时更改NAT配置，建议清除当前NAT转换。可以使用 **clear xlate 命令清除转换表。执行此操作时要小心，因为清除转换表时会断开所有使用转换的当前连接。**清除转换表的替代方法是等待当前转换超时，但并不建议使用此方法，因为使用新规则创建新连接时可能会导致意外行为。

内部/DMZ 到 Internet

在此方案中，将向位于安全设备内部接口（安全等级为 100）上的主机提供对外部接口（安全等级为 0）上的 Internet 的访问。 这是通过 PAT（或 NAT 过载）、动态 NAT 形式实现的。与其他方案不同，本例中不需要 ACL，因为是安全性较高的接口上的主机访问安全性较低的接口上的主机。



1. 指定必须转换的流量的源。下面定义了 NAT 规则号 **1，并且允许来自内部和 DMZ 主机的所有数据流。**`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. 指定已经过 NAT 处理的数据流在访问外部接口时必须使用的地址、地址池或接口。在本例中，使用了外部接口地址执行 PAT。这在事先不知道外部接口地址时尤其有用，例如在 DHCP 配置中。下面使用相同的 NAT ID **1** 发出了全局命令，该命令将外部接口与相同 ID 的 NAT 规则绑定在一起。`ASA-AIP-CLI(config)# global (Outside) 1 interface`

提示：无论何时更改NAT配置，建议清除当前NAT转换。可以使用 **clear xlate 命令清除转换表。执行此操作时要小心，因为清除转换表时会断开所有使用转换的当前连接。**清除转换表的替代方法是等待当前转换超时，但并不建议使用此方法，因为使用新规则创建新连接时可能会导致意外行为。

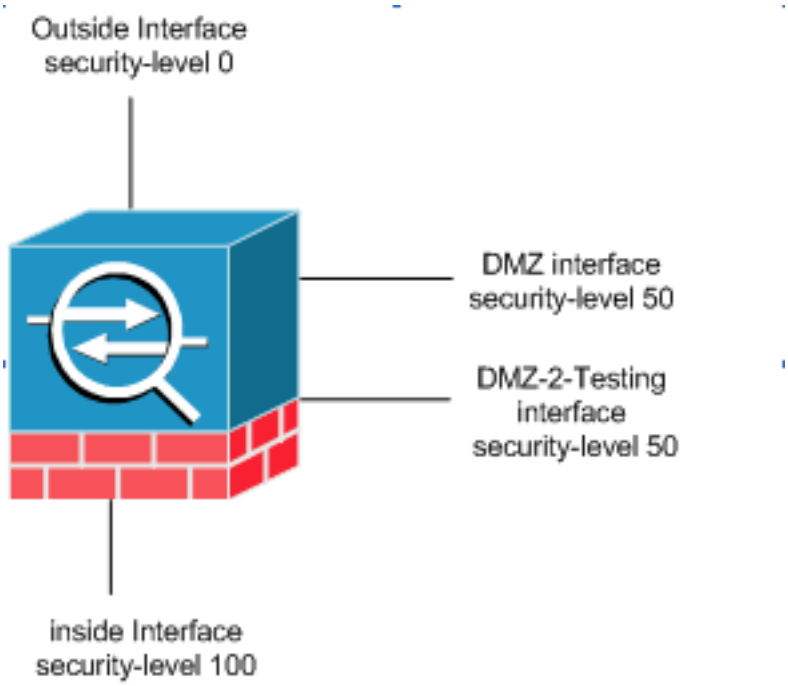
注意：如果要阻止从较高安全区域（内部）到较低安全区域（互联网/DMZ）的流量，请创建ACL并将其作为入站应用到PIX/ASA的内部接口。

注意： 示例：要阻塞端口 80 上从内部网络上的主机 172.20.1.100 流向 Internet 的数据流，请使用以下命令：

```
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
```

同一安全等级上的通信

初始配置显示接口“DMZ”和“DMZ-2-testing”已配置了安全等级 (50)；默认情况下，这两个接口无法通信。下面我们使用以下命令允许这些接口进行通信：




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

注意：即使为相同安全级别接口（“DMZ”和“DMZ-2-testing”）配置了“相同安全流量允许接口间”，它仍需要转换规则（静态/动态）来访问这些接口中放置的资源。

故障排除

本部分提供的信息可用于对配置进行故障排除。

- 排除通过 PIX 和 ASA 的连接故障
- NAT 配置验证 NAT 和故障排除

相关信息

- Cisco ASA 命令参考
- Cisco PIX 命令参考
- Cisco ASA 错误和系统消息
- Cisco PIX 错误和系统消息
- 技术支持和文档 - Cisco Systems