PIX/ASA 7.x: Enable/Disable Communication Between Interfaces

Contents

Introduction

This document provides a sample configuration for various forms of communication between interfaces on the ASA/PIX security appliance.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- IP addresses and default gateway assignment
- Physical network connectivity between devices
- Communication port # identified for the service implemented

Components Used

The information in this document is based on these software and hardware versions:

- Adaptive Security Appliance that runs software Version 7.x and later
- Windows 2003 Servers
- Windows XP workstations

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.

Related Products

This configuration can also be used with these hardware and software versions:

- PIX 500 Series firewalls that run 7.x and later

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Background Information

This document outlines the required steps to allow communication to flow between different interfaces. Forms of communication such as these are discussed:

1. Communication from hosts that are located on the outside that require access to resource located in the DMZ
2. Communication from hosts on the inside network that require access to resources located in the DMZ
3. Communication from hosts on the inside and the DMZ network that require access to resources on the outside

NAT

In our example, we use Network Address Translation (NAT) and Port Address Translation (PAT) in our configuration. Address translation substitutes the real address (local) in a packet with a mapped address (global) that is routable on the destination network. NAT is comprised of two steps: the process in which a real address is translated into a mapped address and then the process to undo translation for the traffic that returns. There are two forms of address translation that we use in this configuration guide: Static and Dynamic.

Dynamic translations allows each host to use a different address or port for each subsequent translation. Dynamic translations can be used when local hosts share or "hide behind" one or more common global addresses. In this mode, one local address cannot permanently reserve a global address for translation. Instead, address translation occurs on a many-to-one or many-to-many basis, and translation entries are created only as they are needed. As soon as a translation entry is free from use, it is deleted and made available to other local hosts. This type of translation is most useful for outbound connections, in which inside hosts are assigned a dynamic address or port number only as connections are made. There are two forms of Dynamic address translation:

- Dynamic NAT - Local addresses are translated into the next available global address in a pool. Translation occurs on a one-to-one basis, so it is possible to exhaust the pool of global addresses if a greater number of local hosts require translation at a given time.
- NAT Overload (PAT) - Local addresses are translated into a single global address; each connection is made unique when the next available high-order port number of the global

address is assigned as the source of the connection. Translation occurs on a many-to-one basis because many local hosts share one common global address.

Static translation creates a fixed translation of the real address(es) to mapped address(es). A static NAT configuration maps the same address for each connection by a host and is a persistent translation rule. Static address translations are used when an internal or local host needs to have the same global address for every connection. Address translation occurs on a one-to-one basis. Static translations can be defined for a single host or for all addresses contained in an IP subnet.

The main difference between dynamic NAT and a range of addresses for static NAT is that static NAT allows a remote host to initiate a connection to a translated host (if there is an access list that allows it), while dynamic NAT does not. You also need an equal number of mapped addresses with static NAT.

The security appliance translates an address when a NAT rule matches the traffic. If no NAT rule matches, processing for the packet continues. The exception is when you enable NAT control. NAT control requires that packets that traverse from a higher security interface (inside) to a lower security level (outside) match a NAT rule, or else processing for the packet stops. In order to view common configuration information, refer to the PIX/ASA 7.x NAT and PAT document. For a deeper understanding of how NAT works, refer to the How NAT works guide.

Tip: Whenever you change the NAT configuration, it is recommended that you clear current NAT translations. You can clear the translation table with the **clear xlate** command. **However, take caution when you do this** since clearing the translation table disconnects all current connections that use translations. The alternative to clearing the translation table is to wait for current translations to time out, but this is not recommended because unexpected behavior can result as new connections are created with the new rules.

Security Levels

The Security-level value controls how hosts/devices on the different interfaces interact with each other. By default, hosts/devices connected to interfaces with higher-security levels can access hosts/devices connected to interface with lower-security levels. Hosts/devices connected to interfaces with lower-security interfaces cannot access hosts/devices connect to interfaces with higher-security interfaces without the permission of access lists.

The **security-level** command is new to Version 7.0 and replaces the portion of the **nameif** command that assigned the security level for an interface. Two interfaces, "the inside" and "outside" interfaces, have default security levels, but these can be overridden with the **security-level** command. If you name an interface "inside," it is given a default security level of 100; an interface named "outside" is given a a default security level of 0. All other newly added interfaces receive a default security level of 0. In order to assign a new security level to an interface, use the **security-level** command in the interface command mode. Security levels range from 1-100.

Note: Security-levels are used only to determine how the firewall inspects and handles traffic. For example, traffic that passes from a higher-security interface toward a lower one is forwarded with less stringent default policies than traffic that comes from a lower security interface toward a higher-security one. For more information on security-levels, refer to the ASA/PIX 7.x command reference guide.

ASA/PIX 7.x also introduced the ability to configure multiple interfaces with the same level of security. For example, multiple interfaces connected to partners or other DMZs can all be given a security level of 50. By default, these same security interfaces cannot communicate with one

another. In order to work around this, the **same-security-traffic permit inter-interface** command was introduced. This command allows for communication between interfaces of the same security level. For more information on same-security between interfaces, refer to the Command Reference guideConfiguring Interface Parameters, and see this example.

ACL

Access Control lists typically consist of multiple access control entries (ACE) organized internally by the Security Appliance in a linked list. ACEs describe a set of traffic such as that from a host or network and list an action to apply to that traffic, generally permit or deny. When a packet is subjected to access list control, the Cisco Security Appliance searches this linked list of ACEs in order to find one that matches the packet. **The first ACE that matches the security appliance is the one that is applied to the packet.** Once the match is found, the action in that ACE (permit or deny) is applied to the packet.

Only one access list is permitted per interface, per direction. This means that you can only have one access list that applies to traffic inbound on an interface and one access list that applies to traffic outbound on an interface. Access lists that are not applied to interfaces, such as NAT ACLs, are unlimited.

Note: By default, all access-lists have an implicit ACE at the end that denies all traffic, so all traffic that does not match any ACE that you enter in the access list matches the implicit deny at the end and is dropped. You must have at least one permit statement in an interface access list for traffic to flow. Without a permit statement, all traffic is denied.

Note: Access list are implemented with the **access-list** and **access-group** commands. These commands are used instead of the **conduit** and **outbound** commands, which were used in earlier versions of PIX firewall software. For more information on ACLs, refer to Configuring IP Access List.

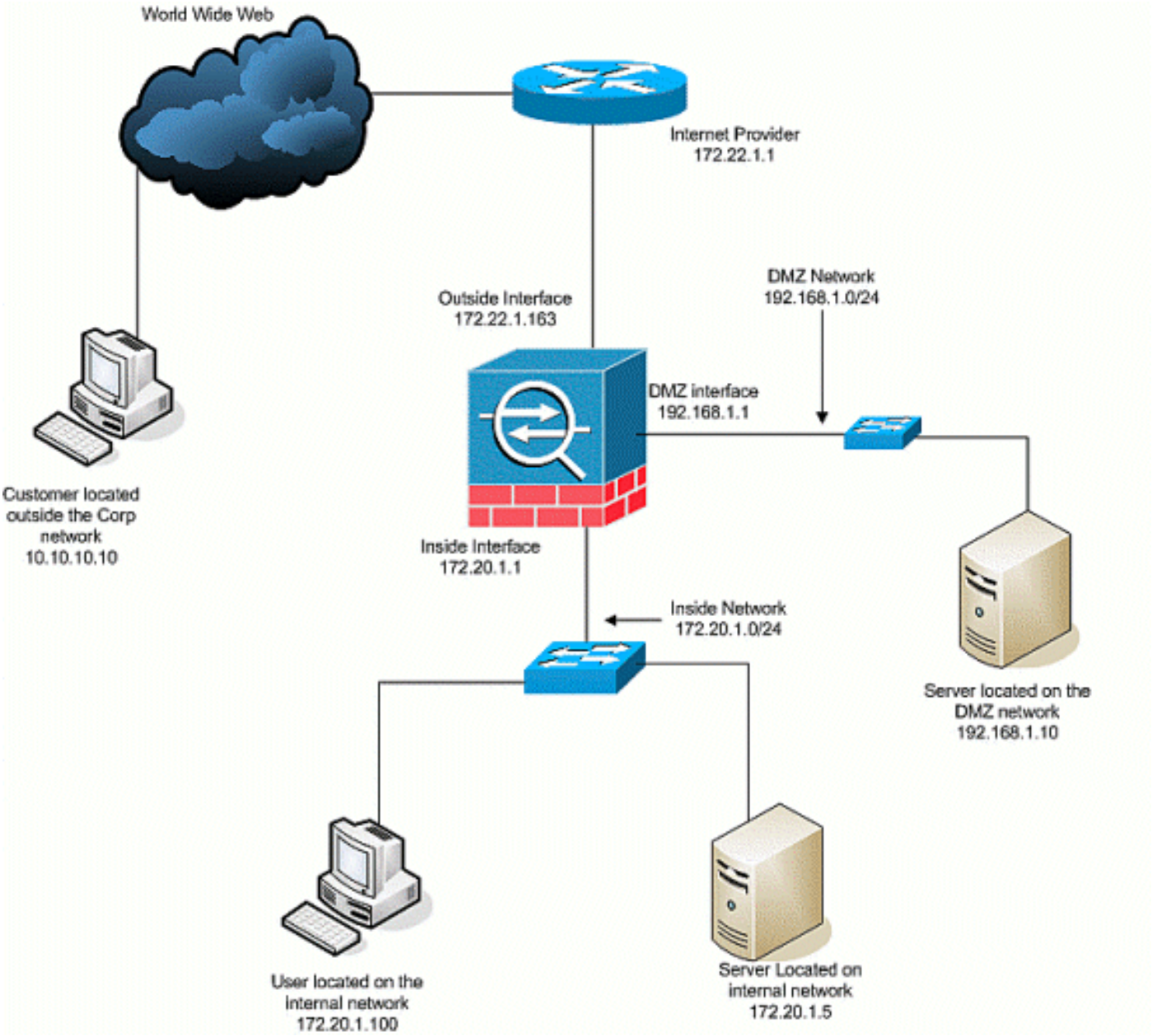
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

Network Diagram

This document uses the this network setup:



Initial Configuration

This document uses these configurations:

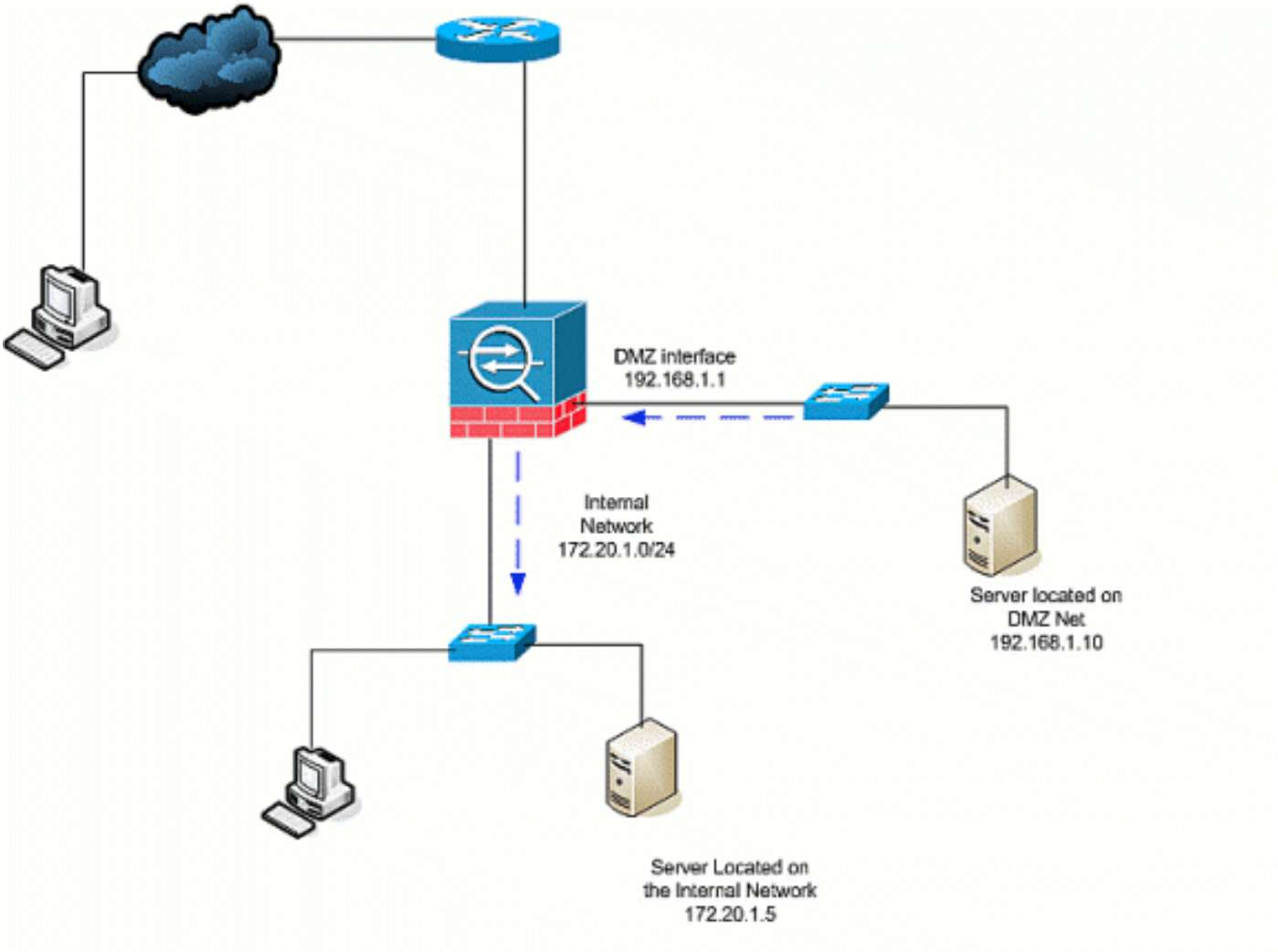
- With this basic firewall configuration, there are currently no NAT/STATIC statements.
- There are no ACLs applied, so the implicit ACE of `deny any any` is currently used.

Device Name 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 to Inside

In order to allow communication from the DMZ to internal network hosts, use these commands. In this example, a web server on the DMZ needs to access an AD and DNS server on the inside.



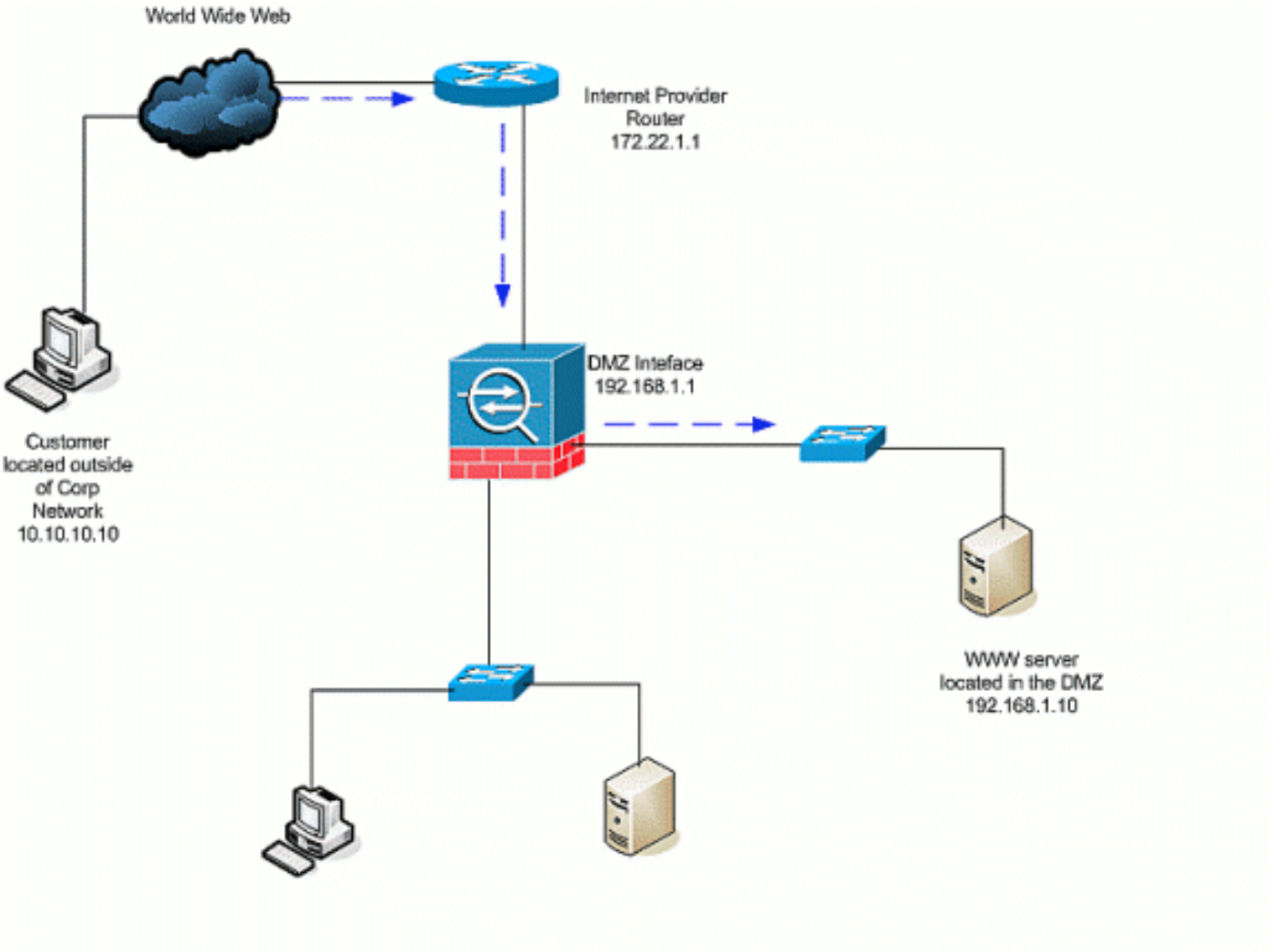
1. Create a static NAT entry for the AD/DNS server on the DMZ. Static NAT creates a fixed

translation of a real address to a mapped address. This mapped address is an address that DMZ hosts can use to access the server on the inside without the need to know the real address of the server. This command maps the DMZ address 192.168.2.20 to the real inside address 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. ACLs are required to allow an interface with a lower security-level to have access to a higher security level. In this example, we give the web server that sits on the DMZ (Security 50) access to the AD/DNS server on the inside (Security 100) with these specific service ports: DNS, Kerberos, and 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`**Note:** The ACLs permit access to the mapped address of the AD/DNS server that was created in this example and not the real internal address.
3. In this step, you apply the ACL to the DMZ interface in the inbound direction with this command:`ASA-AIP-CLI(config)# access-group DMZtoInside in interface DMZ`**Note:** If you want to block or disable port 88, traffic from DMZ to inside, for instance, use this:`ASA-AIP-CLI(config)# no access-list DMZtoInside extended permit tcp host 192.168.1.10 host 192.168.2.20 eq 88`**Tip:** Whenever you change the NAT configuration, it is recommended that you clear current NAT translations. You can clear the translation table with the **clear xlate** command. **Exercise caution when you do this** since clearing the translation table disconnects all current connections that use translations. The alternative to clearing the translation table is to wait for the current translations to time out, but this is not recommended because unexpected behavior can result as new connections are created with the new rules.Other common configurations include these:Mail Servers in the DMZSSH Access inside and outsideAllowed Remote Desktop sessions through PIX/ASA devicesOther DNS solutions when used in the DMZ

Internet to DMZ

In order to allow communication from users on the Internet, or outside interface (Security 0), to a web server that is located in the DMZ (Security 50), use these commands:

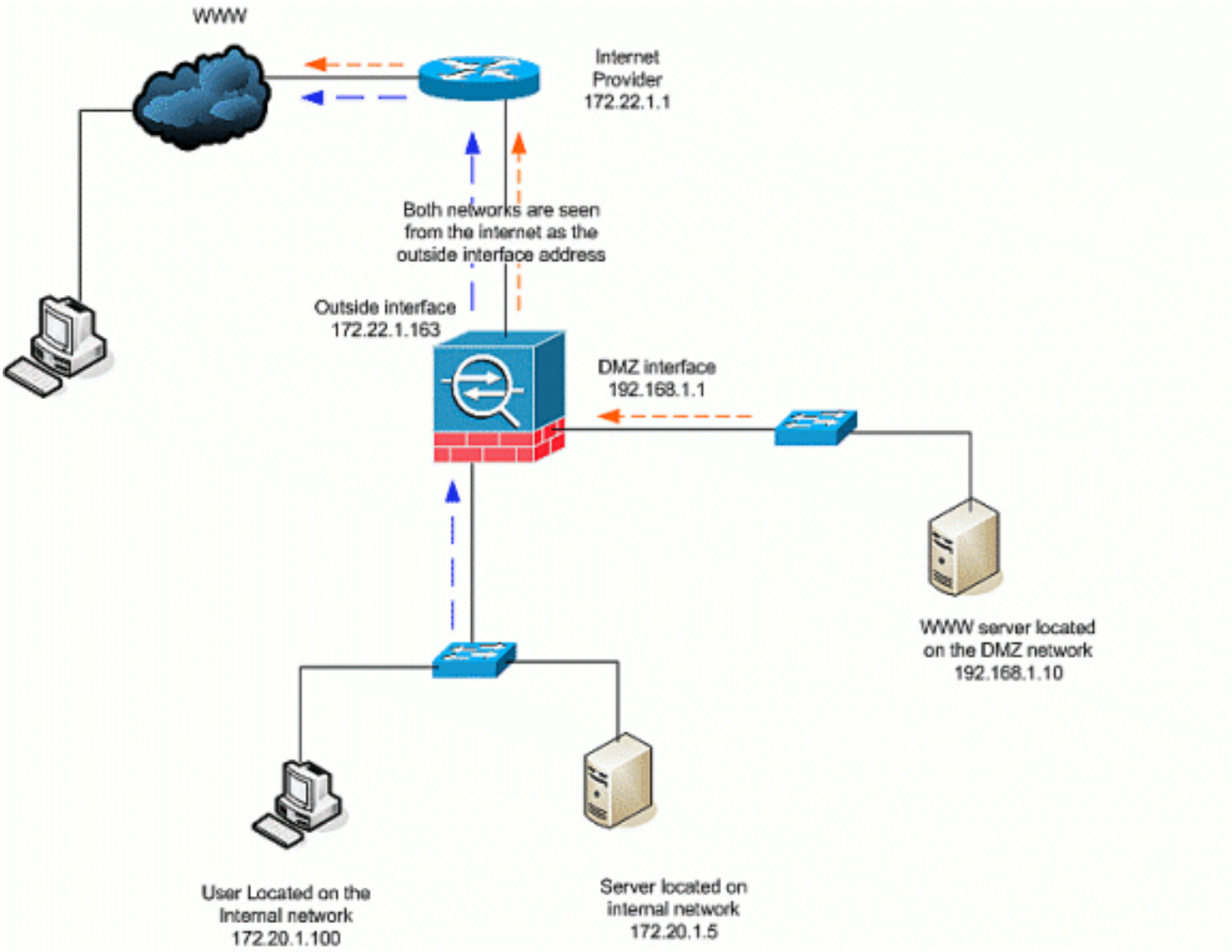


1. Create a static translation for the web server in the DMZ to the outside. Static NAT creates a fixed translation of a real address to a mapped address. This mapped address is an address that hosts on the Internet can use to access the web server on the DMZ without the need to know the real address of the server. This command maps the outside address 172.22.1.25 to the real DMZ address 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. Create an ACL that allows users from the outside to access the web server through the mapped address. Note that the web server also hosts the 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. The last step in this configuration is to apply the ACL to the outside interface for traffic in the inbound direction.`ASA-AIP-CLI(config)# access-group OutsidetoDMZ in interface Outside`**Note:** Remember, you can only apply one access list per interface, per direction. If you already have an inbound ACL applied to the outside interface, you cannot apply this example ACL to it. Instead add the ACEs in this example into the current ACL that is applied to the interface.**Note:** If you want to block or disable the FTP traffic from internet to DMZ, for instance, use this:`ASA-AIP-CLI(config)# no access-list OutsidetoDMZ extended permit tcp any host 172.22.1.25 eq ftp`**Tip:** Whenever you change the NAT configuration, it is recommended that you clear current NAT translations. You can clear the translation table with the **clear xlate** command. **Exercise caution when you do this** since clearing the translation table disconnects all current connections that use translations. The alternative to clearing the translation table is to wait for current translations to time out, but this is not recommended because unexpected behavior can result as new connections are created with

the new rules.

Inside/DMZ to Internet

In this scenario, hosts located on the inside interface (Security 100) of the security appliance are provided with access to the Internet on the outside interface (Security 0). This is achieved with the PAT, or NAT overload, form of dynamic NAT. Unlike the other scenarios, an ACL is not required in this case because hosts on a high-security interface access hosts on a low-security interface.



1. Specify the source(s) of the traffic that must be translated. Here NAT rule number **1** is defined, and all traffic from inside and DMZ hosts is allowed.`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. Specify what address, address pool, or interface the NATed traffic must use when it accesses the outside interface. In this case, PAT is performed with the outside interface address. This is especially useful when the outside interface address is not known beforehand, such as in a DHCP configuration. Here, the global command is issued with the same NAT ID of **1**, which ties it to the NAT rules of the same ID.`ASA-AIP-CLI(config)# global (Outside) 1 interface`

Tip: Whenever you change the NAT configuration, it is recommended that you clear current NAT translations. You can clear the translation table with the **clear xlate** command. **Exercise caution when you do this** since clearing the translation table disconnects all current connections that use translations. The alternative to clearing the translation table is to wait for current translations to

time out, but this is not recommended because unexpected behavior can result as new connections are created with the new rules.

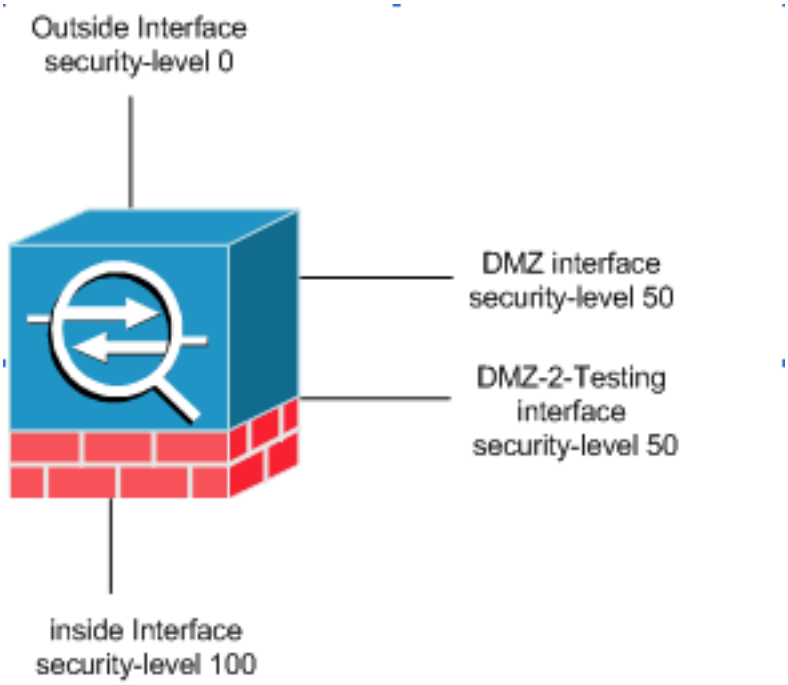
Note: If you want to block the traffic from the higher security zone (inside) to the lower security zone (internet/DMZ), create an ACL and apply it to the inside interface of the PIX/ASA as inbound.

Note: Example: In order to block the port 80 traffic from the host 172.20.1.100 on the inside network to the Internet, use this:

```
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
```

Same Security Level Communication

The initial configuration shows that interfaces "DMZ" and "DMZ-2-testing" are configured with security level (50); by default, these two interfaces cannot talk. Here we allow these interfaces to talk with this command:




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

Note: Even though the "same-security traffic permit inter-interface" has been configured for the same security level interfaces ("DMZ" and "DMZ-2-testing"), it still needs a translation rule (static/dynamic) to access the resources placed in those interfaces.

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

- Troubleshooting connections through the PIX and ASA
- NAT ConfigurationsVerify NAT and Troubleshooting

Related Information

- Cisco ASA Command Reference
- Cisco PIX Command Reference
- Cisco ASA Error and Systems Messages
- Cisco PIX Error and Systems Messages
- Technical Support & Documentation - Cisco Systems