PIX/ASA 7.x: 인터페이스 간 통신 활성화/비활성화

목차

소개

이 문서에서는 ASA/PIX 보안 어플라이언스의 인터페이스 간 다양한 형태의 통신에 대한 샘플 컨피그레이션을 제공합니다.

사전 요구 사항

요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- IP 주소 및 기본 게이트웨이 할당
- 장치 간 물리적 네트워크 연결
- 구현된 서비스에 대해 식별된 통신 포트 번호

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 소프트웨어 버전 7.x 이상을 실행하는 Adaptive Security Appliance
- Windows 2003 서버
- Windows XP 워크스테이션

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

관련 제품

이 컨피그레이션은 다음 하드웨어 및 소프트웨어 버전과 함께 사용할 수도 있습니다.

- 7.x 이상을 실행하는 PIX 500 Series 방화벽

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

배경 정보

이 문서에서는 서로 다른 인터페이스 간에 통신이 진행될 수 있도록 필요한 단계를 간략하게 설명합니다. 다음과 같은 통신 형식이 논의됩니다.

1. DMZ에 있는 리소스에 액세스해야 하는 외부에 있는 호스트로부터의 통신
2. DMZ에 있는 리소스에 액세스해야 하는 내부 네트워크의 호스트와의 통신
3. 외부의 리소스에 액세스해야 하는 내부 및 DMZ 네트워크의 호스트와의 통신

NAT

이 예에서는 컨피그레이션에 NAT(Network Address Translation) 및 PAT(Port Address Translation)를 사용합니다. 주소 변환은 패킷의 실제 주소(로컬)를 대상 네트워크에서 라우팅 가능한 매핑된 주소(전역)로 대체합니다. NAT는 두 단계로 구성됩니다. 실제 주소가 매핑된 주소로 변환된 다음 반환하는 트래픽에 대한 변환을 취소하는 프로세스 이 컨피그레이션 가이드에서는 두 가지 형태의 주소 변환을 사용합니다. 정적 및 동적.

동적 변환을 통해 각 호스트는 후속 변환마다 다른 주소 또는 포트를 사용할 수 있습니다. 로컬 호스트가 하나 이상의 공통 전역 주소를 공유하거나 "뒤에 숨기기"할 때 동적 변환을 사용할 수 있습니다. 이 모드에서는 한 로컬 주소가 변환을 위해 전역 주소를 영구적으로 예약할 수 없습니다. 대신 주소 변환은 다대일 또는 다대다 기준으로 수행되며 번역 항목은 필요한 경우에만 생성됩니다. 변환 엔트리를 사용할 수 없는 즉시 삭제되고 다른 로컬 호스트에서 사용할 수 있게 됩니다. 이러한 유형의 변환은 내부 호스트에 연결이 이루어질 때만 동적 주소 또는 포트 번호가 할당되는 아웃바운드 연결에 가장 유용합니다. 동적 주소 변환에는 두 가지 형식이 있습니다.

- 동적 NAT - 로컬 주소는 풀에서 사용 가능한 다음 전역 주소로 변환됩니다. 변환은 일대일로 이루어지므로 지정된 시간에 변환해야 하는 로컬 호스트 수가 많을 경우 전역 주소 풀을 소진할 수 있습니다.
- NAT 오버로드(PAT) - 로컬 주소가 단일 전역 주소로 변환됩니다. 각 연결은 전역 주소의 다음 사용 가능한 고주문 포트 번호가 연결의 소스로 할당될 때 고유합니다. 많은 로컬 호스트가 하

나의 공통 전역 주소를 공유하므로 번역은 다대일 방식으로 이루어집니다.
고정 변환은 실제 주소를 매핑된 주소로의 고정 변환을 생성합니다. 고정 NAT 컨피그레이션은 호스트에 의해 각 연결에 대해 동일한 주소를 매핑하며 영구 변환 규칙입니다. 고정 주소 변환은 내부 또는 로컬 호스트가 모든 연결에 대해 동일한 전역 주소를 가져야 하는 경우에 사용됩니다. 주소 변환은 일대일로 이루어집니다. 단일 호스트 또는 IP 서브넷에 포함된 모든 주소에 대해 고정 변환을 정의할 수 있습니다.

동적 NAT와 고정 NAT의 주소 범위 간의 주요 차이점은 고정 NAT는 원격 호스트가 변환된 호스트(이를 허용하는 액세스 목록이 있는 경우)에 대한 연결을 시작할 수 있도록 허용하지만 동적 NAT는 그렇지 않다는 것입니다. 또한 고정 NAT를 사용하는 매핑된 주소의 수가 같아야 합니다.

보안 어플라이언스는 NAT 규칙이 트래픽과 일치할 때 주소를 변환합니다. 일치하는 NAT 규칙이 없으면 패킷에 대한 처리가 계속됩니다. NAT 제어를 활성화하는 경우는 예외입니다. NAT 제어에서는 상위 보안 인터페이스(내부)에서 하위 보안 수준(외부)으로 이동하는 패킷이 NAT 규칙과 일치하거나, 그렇지 않으면 패킷에 대한 처리가 중지되어야 합니다. 공통 컨피그레이션 정보를 보려면 PIX/ASA 7.x NAT 및 PAT 문서를 참조하십시오. NAT 작동 방식에 대한 자세한 내용은 How NAT works guide를 참조하십시오.

팁: NAT 컨피그레이션을 변경할 때마다 현재 NAT 변환을 지우는 것이 좋습니다. clear xlate 명령을 사용하여 변환 테이블을 지울 수 **있습니다**. **그러나 변환** 테이블**을** 지우면 변환을 사용하는 모든 현재 연결이 해제되므로 **이** 작업을 수행할 **때 주의하십시오**. 변환 테이블을 지우는 대신 현재 번역이 시간 초과될 때까지 기다리는 것이 좋습니다. 그러나 새 규칙으로 새 연결이 생성되어 예기치 않은 동작이 발생할 수 있으므로 이 방법은 권장되지 않습니다.

보안 수준

보안 수준 값은 서로 다른 인터페이스의 호스트/디바이스가 상호 작용하는 방식을 제어합니다. 기본적으로 보안 수준이 높은 인터페이스에 연결된 호스트/디바이스는 보안 수준이 낮은 인터페이스에 연결된 호스트/디바이스에 액세스할 수 있습니다. 하위 보안 인터페이스가 있는 인터페이스에 연결된 호스트/디바이스는 액세스 목록의 권한 없이 상위 보안 인터페이스가 있는 인터페이스에 액세스할 수 없습니다.

security **level** 명령은 버전 7.0에 새로 추가되며 인터페이스에 대한 보안 수준을 할당한 **nameif** 명령 부분을 대체합니다. "inside" 및 "outside" 인터페이스 2개는 기본 보안 레벨을 가지지만, **security-level** 명령을 사용하여 이러한 인터페이스를 재정의할 수 있습니다. 인터페이스 이름을 "inside"로 지정하면 기본 보안 수준이 100으로 지정됩니다. "outside"라는 이름의 인터페이스에는 기본 보안 레벨이 0입니다. 새로 추가된 다른 모든 인터페이스에는 기본 보안 레벨이 0입니다. 인터페이스에 새 보안 레벨을 할당하려면 인터페이스 명령 모드에서 **security-level** 명령을 사용합니다. 보안 레벨은 1~100입니다.

참고: 보안 레벨은 방화벽이 트래픽을 검사하고 처리하는 방법을 결정하는 데만 사용됩니다. 예를 들어, 상위 보안 인터페이스에서 하위 보안 인터페이스로 전달되는 트래픽은 하위 보안 인터페이스에서 상위 보안 인터페이스로 향하는 트래픽보다 덜 엄격한 기본 정책으로 전달됩니다. 보안 레벨에 대한 자세한 내용은 ASA/PIX 7.x 명령 참조 설명서를 참조하십시오.

또한 ASA/PIX 7.x는 동일한 보안 수준으로 여러 인터페이스를 구성하는 기능을 도입했습니다. 예를 들어, 파트너 또는 다른 DMZ에 연결된 여러 인터페이스에 모두 50의 보안 레벨을 지정할 수 있습니다. 기본적으로 이러한 동일한 보안 인터페이스는 서로 통신할 수 없습니다. 이 문제를 해결하기 위해 **same-security-traffic permit inter-interface** 명령이 도입되었습니다. 이 명령을 사용하면 동일한 보안 수준의 인터페이스 간에 통신을 수행할 수 있습니다. 인터페이스 간 동일한 보안에 대한 자세한 내용은 명령 참조 설명서인터페이스 매개변수 구성을 참조하고 이 예를 참조하십시오.

ACL

액세스 제어 목록은 일반적으로 Security Appliance가 연결된 목록에서 내부적으로 구성한 여러 ACE(액세스 제어 항목)로 구성됩니다. ACE는 호스트 또는 네트워크의 트래픽과 같은 트래픽 집합을 설명하고 해당 트래픽에 적용할 작업(일반적으로 허용 또는 거부)을 나열합니다. 패킷이 액세스 목록 제어를 받는 경우 Cisco Security Appliance는 패킷과 일치하는 ACE를 찾기 위해 이 연결된 ACE 목록을 검색합니다. **보안 어플라이언스와 일치하는 첫 번째 ACE는 패킷에 적용되는 ACE입니다.** 일치하는 항목이 발견되면 해당 ACE의 작업(허용 또는 거부)이 패킷에 적용됩니다.

인터페이스당 방향당 하나의 액세스 목록만 허용됩니다. 이는 인터페이스의 인바운드 트래픽에 적용되는 액세스 목록과 인터페이스의 트래픽 아웃바운드에 적용되는 액세스 목록을 하나만 가질 수 있음을 의미합니다. NAT ACL과 같이 인터페이스에 적용되지 않는 액세스 목록은 무제한입니다.

참고: 기본적으로 모든 액세스 목록에는 모든 트래픽을 거부하는 암시적 ACE가 마지막에 있으므로, 액세스 목록에 입력한 ACE와 일치하지 않는 모든 트래픽은 마지막에 암시적 거부와 일치하고 삭제됩니다. 트래픽이 흐르도록 하려면 인터페이스 액세스 목록에 하나 이상의 permit 문이 있어야 합니다. permit 문이 없으면 모든 트래픽이 거부됩니다.

참고: 액세스 목록은 **access-list** 및 **access-group** 명령**으로** 구현됩니다. 이러한 명령은 **도관** 및 **아웃바운드** 명령 대신 사용되며 이전 버전의 PIX 방화벽 소프트웨어에서 사용되었습니다. ACL에 대한 자세한 내용은 IP 액세스 목록 구성을 참조하십시오.

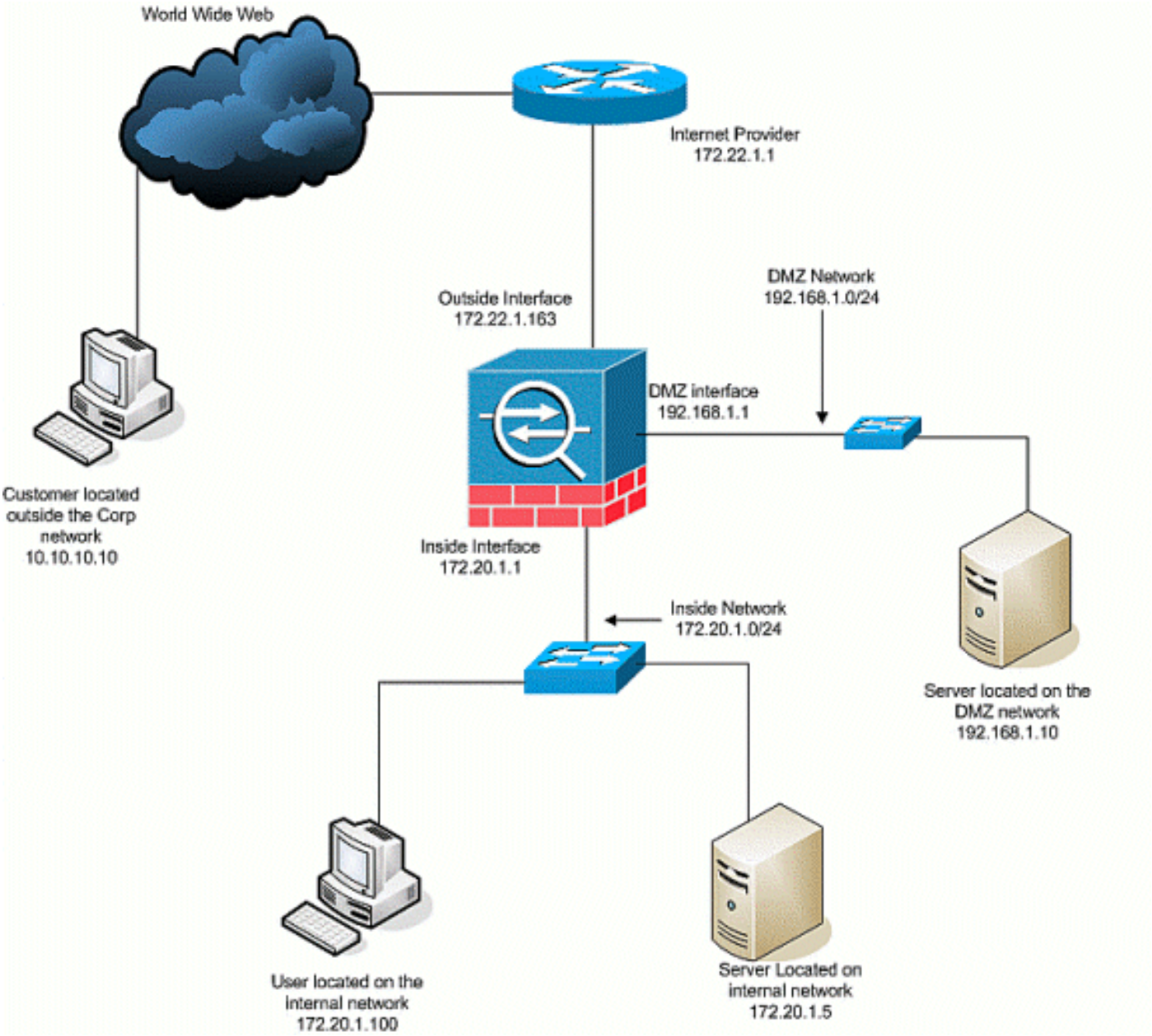
구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 섹션에 사용된 명령에 대한 자세한 내용을 확인하십시오.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



초기 컨피그레이션

이 문서에서는 다음 구성을 사용합니다.

- 이 기본 방화벽 컨피그레이션에서는 현재 NAT/STATIC 문이 없습니다.
- 적용된 ACL이 없으므로 의 암시적 ACE가 현재 사용되고 있습니다.

장치 이름 1

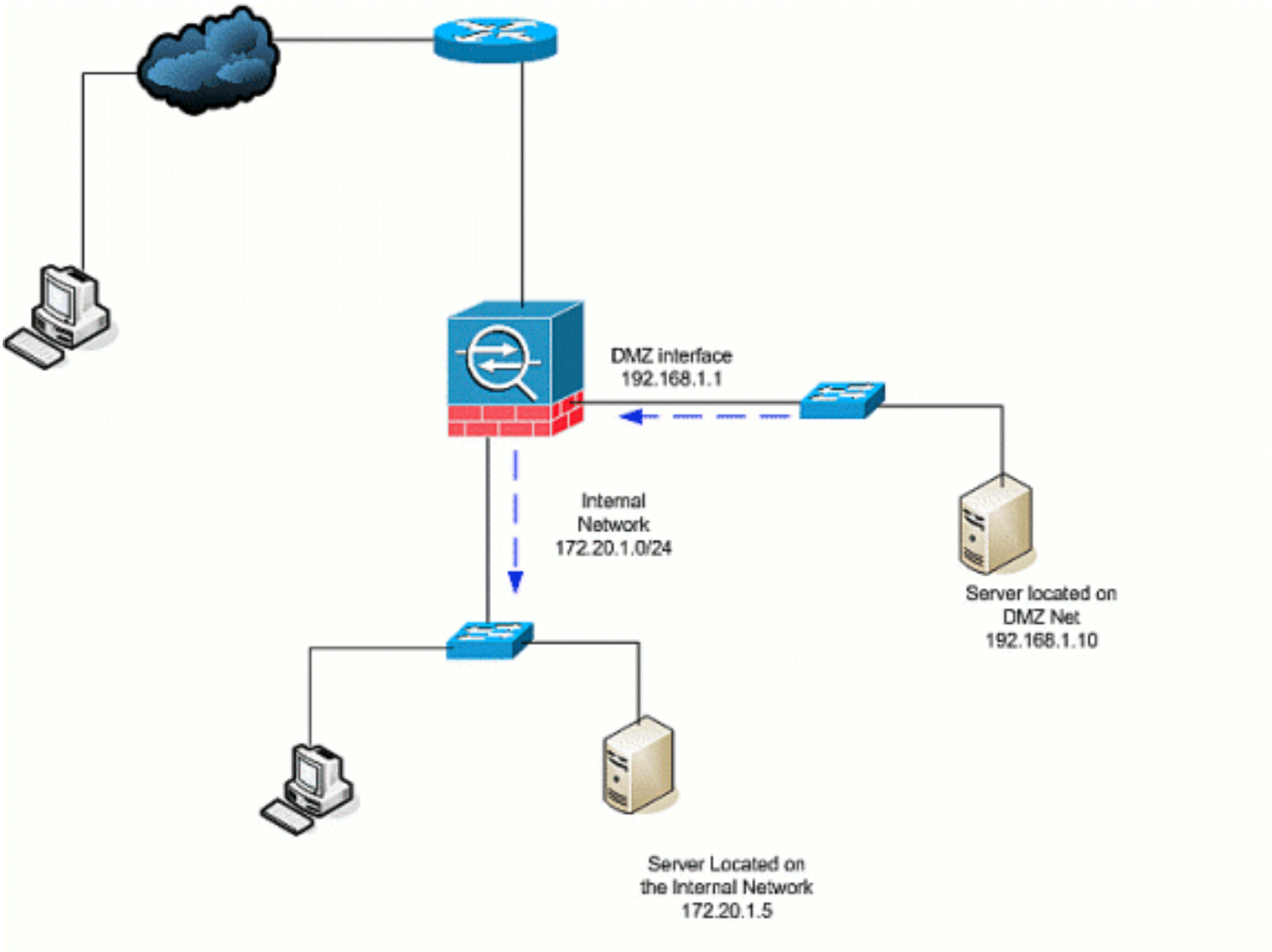
```
ASA-AIP-CLI(config)#show running-config

 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)#
```

DMZ에서 내부

DMZ에서 내부 네트워크 호스트로의 통신을 허용하려면 다음 명령을 사용합니다. 이 예에서는 DMZ의 웹 서버가 내부의 AD 및 DNS 서버에 액세스해야 합니다.



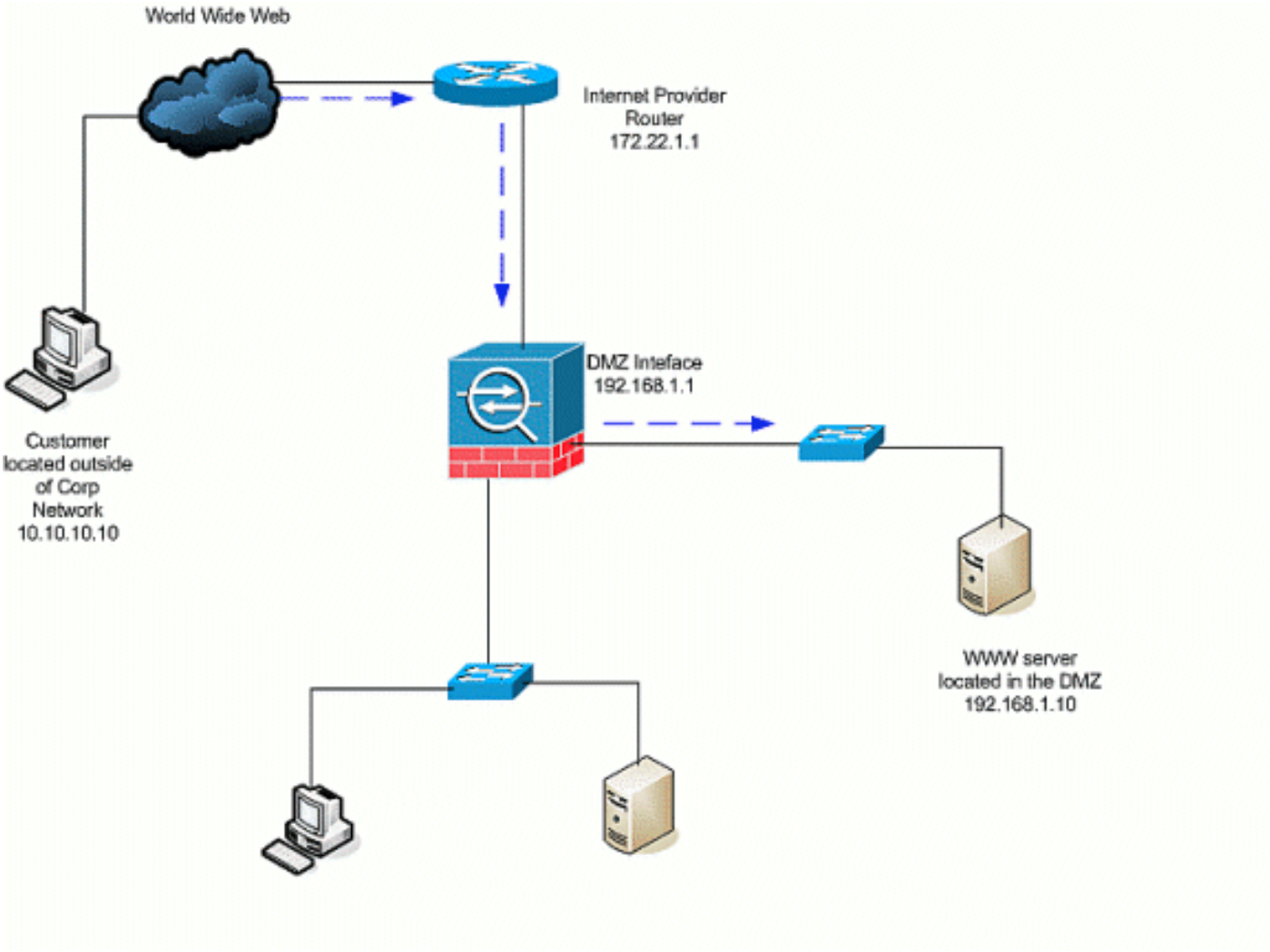
1. DMZ의 AD/DNS 서버에 대한 고정 NAT 항목을 생성합니다. 고정 NAT는 실제 주소의 고정 변환을 매핑된 주소로 생성합니다. 이 매핑된 주소는 서버의 실제 주소를 알 필요 없이 DMZ 호

스트가 내부 서버에 액세스하는 데 사용할 수 있는 주소입니다. 이 명령은 DMZ 주소 192.168.2.20을 실제 내부 주소 172.20.1.5에 매핑합니다.`ASA-AIP-CLI(config)# static (inside,DMZ) 192.168.2.20 172.20.1.5  255.255.255.255`

2. 보안 수준이 낮은 인터페이스에서 더 높은 보안 레벨에 액세스할 수 있도록 하려면 ACL이 필요합니다. 이 예에서는 DMZ(Security 50)에 있는 웹 서버에 다음 특정 서비스 포트를 사용하여 내부(Security 100)의 AD/DNS 서버에 대한 액세스를 제공합니다. DNS, Kerberos 및 LDAP입니다.`ASA-AIP-CLI(config)# access-list DMZtoInside  udp  192.168.1.10  192.168.2.20 eq ASA-AIP-CLI(config)# access-list DMZtoInside  tcp  192.168.1.10  192.168.2.20 eq 88ASA-AIP-CLI(config)# access-list DMZtoInside  udp  192.168.1.10  192.168.2.20 eq 389`**참고:** ACL은 실제 내부 주소가 아니라 이 예에서 생성된 AD/DNS 서버의 매핑된 주소에 대한 액세스를 허용합니다.
3. 이 단계에서는 다음 명령을 사용하여 인바운드 방향의 DMZ 인터페이스에 ACL을 적용합니다.`DMZ ASA-AIP-CLI(config)# access-group DMZtoInside`**참고:** 포트 88을 차단하거나 비활성화하려면 예를 들어 DMZ에서 내부 트래픽으로 다음 항목을 사용합니다.
```
ASA-AIP-CLI(config)# no access-list DMZtoInside extended permit
tcp host 192.168.1.10 host 192.168.2.20 eq 88
```
팁: NAT 컨피그레이션을 변경할 때마다 현재 NAT 변환을 지우는 것이 좋습니다. clear xlate 명령을 사용하여 변환 테이블을 지울 수 **있습니다**. 변환 테이블**을** 지우면 변환을 사용하는 모든 현재 연결이 끊어지기 때문에 **이** 작업을 수행할 **때 주의하십시오**. 변환 테이블을 지우는 대신 현재 번역이 시간 초과될 때까지 기다리는 것이 좋습니다. 그러나 예기치 않은 동작이 새 규칙으로 새 연결을 만들 수 있으므로 이 방법은 권장되지 않습니다.기타 일반적인 컨피그레이션에는 다음이 포함됩니다.DMZ의 메일 서버SSH 액세스 내부 및 외부PIX/ASA 디바이스를 통해 허용된 원격 데스크톱 세션DMZ에서 사용되는 기타 DNS 솔루션

인터넷-DMZ

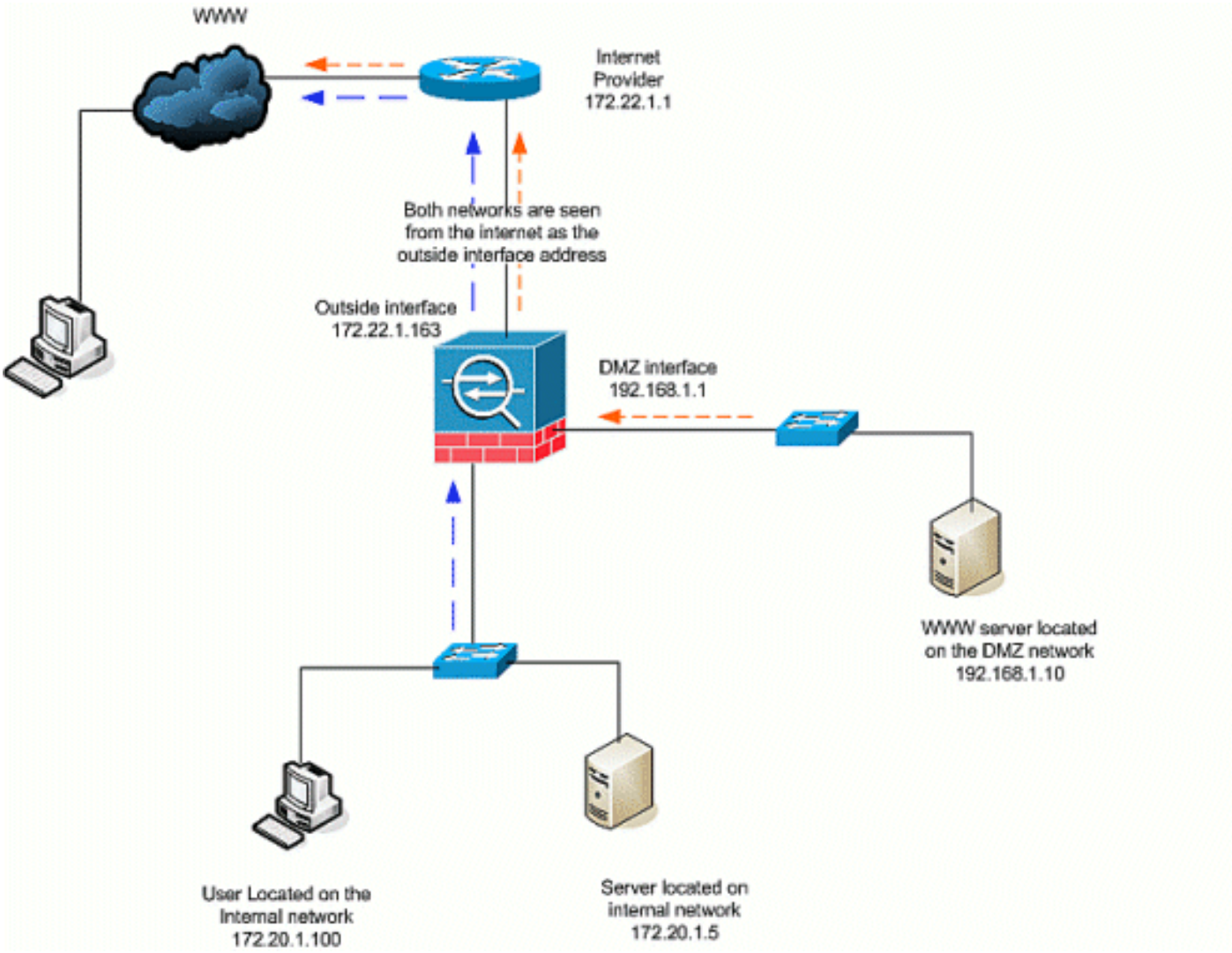
인터넷 또는 외부 인터페이스(Security 0)에서 DMZ(Security 50)에 있는 웹 서버로의 통신을 허용하려면 다음 명령을 사용합니다.



1. DMZ의 웹 서버에 대한 정적 변환을 외부에서 생성합니다. 고정 NAT는 실제 주소의 고정 변환을 매핑된 주소로 생성합니다. 이 매핑된 주소는 서버의 실제 주소를 알 필요 없이 인터넷의 호스트가 DMZ의 웹 서버에 액세스하는 데 사용할 수 있는 주소입니다. 이 명령은 외부 주소 172.22.1.25을 실제 DMZ 주소 192.168.1.10에 매핑합니다.`ASA-AIP-CLI(config)# static(DMZ,Outside) 172.22.1.25  255.255.255.255`
2. 외부 사용자가 매핑된 주소를 통해 웹 서버에 액세스할 수 있도록 하는 ACL을 만듭니다. 웹 서버에서도 FTP를 호스팅합니다.`ASA-AIP-CLI(config)# access-list OutsideDMZ extended permit tcp any host 172.22.1.25 eq wwwASA-AIP-CLI(config)# access-list OutsideDMZ extended permit tcp any host 172.22.1.25 eq ftp`
3. 이 컨피그레이션의 마지막 단계는 인바운드 방향의 트래픽에 대해 외부 인터페이스에 ACL을 적용하는 것입니다. `ASA-AIP-CLI(config)# access-group OutsideDMZ`**참고:** 인터페이스당 방향당 하나의 액세스 목록만 적용할 수 있습니다. 이미 인바운드 ACL이 외부 인터페이스에 적용된 경우 이 예제 ACL을 적용할 수 없습니다. 대신 이 예의 ACE를 인터페이스에 적용되는 현재 ACL에 추가합니다.**참고:** 예를 들어 인터넷에서 DMZ로 가는 FTP 트래픽을 차단하거나 비활성화하려면 다음을 사용합니다.
   `ASA-AIP-CLI(config)# no access-list OutsidetoDMZ extended permit tcp any host 172.22.1.25 eq ftp`
   팁: NAT 컨피그레이션을 변경할 때마다 현재 NAT 변환을 지우는 것이 좋습니다. clear xlate 명령을 사용하여 변환 테이블을 지울 수 **있습니다**. 변환 테이블**을** 지우면 변환을 사용하는 모든 현재 연결이 끊어지기 때문에 **이** 작업을 수행할 **때 주의하십시오**. 변환 테이블을 지우는 대신 현재 번역이 시간 초과될 때까지 기다리는 것이 좋습니다. 그러나 새 규칙으로 새 연결이 생성되어 예기치 않은 동작이 발생할 수 있으므로 이 방법은 권장되지 않습니다.

인터넷 내부/DMZ

이 시나리오에서 보안 어플라이언스의 내부 인터페이스(Security 100)에 있는 호스트는 외부 인터페이스의 인터넷 액세스(Security 0)와 함께 제공됩니다. 이는 동적 NAT의 형식인 PAT 또는 NAT 오버로드를 통해 실현됩니다. 다른 시나리오와 달리 이 경우 보안 수준이 낮은 인터페이스의 보안 수준이 높은 인터페이스 액세스 호스트에 있는 호스트가 있기 때문에 ACL이 필요하지 않습니다.



1. 변환해야 하는 트래픽의 소스를 지정합니다. 여기서 NAT 규칙 번호 1이 정의되고 내부 및 DMZ 호스트의 모든 트래픽이 허용됩니다.`ASA-AIP-CLI(config)# nat() 1 172.20.1.0 255.255.255.0ASA-AIP-CLI(config)# nat() 1 192.168.1.0 255.255.255.0`
2. NATed 트래픽이 외부 인터페이스에 액세스할 때 사용해야 하는 주소, 주소 풀 또는 인터페이스를 지정합니다. 이 경우 PAT는 외부 인터페이스 주소로 수행됩니다. 이는 DHCP 컨피그레이션과 같이 외부 인터페이스 주소를 미리 알지 못할 때 특히 유용합니다. 여기서 global 명령은 동일한 NAT ID가 1인 동일한 ID의 NAT 규칙에 연결됩니다.`ASA-AIP-CLI(config)# () 1`

팁: NAT 컨피그레이션을 변경할 때마다 현재 NAT 변환을 지우는 것이 좋습니다. clear xlate 명령을 사용하여 변환 테이블을 지울 수 **있습니다**. 변환 테이블**을** 지우면 변환을 사용하는 모든 현재 연결이 끊어지기 때문에 **이** 작업을 수행할 **때 주의하십시오**. 변환 테이블을 지우는 대신 현재 번역이 시간 초과될 때까지 기다리는 것이 좋습니다. 그러나 새 규칙으로 새 연결이 생성되어 예기치 않은 동작이 발생할 수 있으므로 이 방법은 권장되지 않습니다.

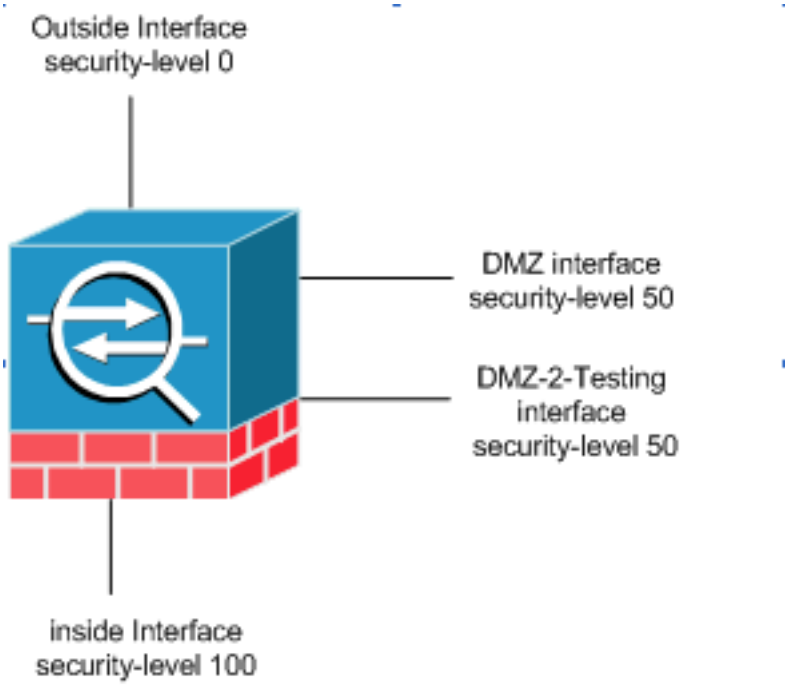
참고: 상위 보안 영역(내부)에서 하위 보안 영역(인터넷/DMZ)까지의 트래픽을 차단하려면 ACL을 생성하여 PIX/ASA의 내부 인터페이스에 인바운드로 적용합니다.

참고: 예: 내부 네트워크의 호스트 172.20.1.100에서 인터넷으로 향하는 포트 80 트래픽을 차단하려면 다음을 사용합니다.

```
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
```

동일한 보안 수준 통신

초기 컨피그레이션에서는 인터페이스 "DMZ" 및 "DMZ-2-testing"이 보안 수준(50)으로 구성되었음을 보여줍니다. 기본적으로 이 두 인터페이스는 통신할 수 없습니다. 여기서는 이러한 인터페이스가 다음 명령과 통신할 수 있습니다.




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

참고: "same-security traffic permit inter-interface"가 동일한 보안 수준 인터페이스("DMZ" 및 "DMZ-2-testing")에 대해 구성되었지만 이러한 인터페이스에 배치된 리소스에 액세스하려면 변환 규칙(고정/동적)이 여전히 필요합니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

- PIX 및 ASA를 통한 연결 문제 해결
- NAT 컨피그레이션NAT 및 트러블슈팅 확인

관련 정보

- Cisco ASA 명령 참조
- Cisco PIX 명령 참조
- Cisco ASA 오류 및 시스템 메시지
- Cisco PIX 오류 및 시스템 메시지
- 기술 지원 및 문서 – Cisco Systems