

# RV042, RV042G 및 RV082 VPN Router의 DMZ(DeMilitarized Zone)에 있는 여러 공용 IP 구성

## 목표

DMZ(Demilitarized Zone)는 신뢰할 수 없는 네트워크에서 사용할 수 있도록 구성된 조직의 내부 네트워크입니다. 보안에 따라 DMZ는 신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 사이에 있습니다. DMZ를 유지 보수하면 조직의 내부 네트워크에 대한 보안을 향상하는 데 도움이 됩니다. ACL(Access Control List)이 인터페이스에 바인딩되면 해당 ACE(Access Control Element) 규칙이 해당 인터페이스에 도착하는 패킷에 적용됩니다. 액세스 제어 목록의 ACE와 일치하지 않는 패킷은 일치하지 않는 패킷을 삭제하는 작업을 수행하는 기본 규칙과 일치합니다.

이 문서의 목적은 여러 공용 IP 주소를 허용하도록 DMZ 포트를 구성하고 라우터 디바이스의 IP에 대한 ACL(Access Control List)을 정의하는 방법을 보여 주는 것입니다.

## 적용 가능한 디바이스

- RV042
- RV042G
- RV082

## 소프트웨어 버전

- v4.2.2.08

## DMZ 구성

1단계. Web Configuration Utility(웹 컨피그레이션 유틸리티) 페이지에 로그인하고 Setup(설정) > Network(네트워크)를 선택합니다. Network(네트워크) 페이지가 열립니다.

## Network

Host Name :  (Required by some ISPs)

Domain Name :  (Required by some ISPs)

---

### IP Mode

Mode	WAN	LAN
<input type="radio"/> IPv4 Only	IPv4	IPv4
<input checked="" type="radio"/> Dual-Stack IP	IPv4 and IPv6	IPv4 and IPv6

---

### LAN Setting

MAC Address : 50:57:A8:79:F3:7A

Device IP Address :

Subnet Mask :

Multiple Subnet :  Enable

---

### WAN Setting

Interface	Connection Type	Configuration
WAN1	Obtain an IP automatically	

---

### DMZ Setting

Enable DMZ

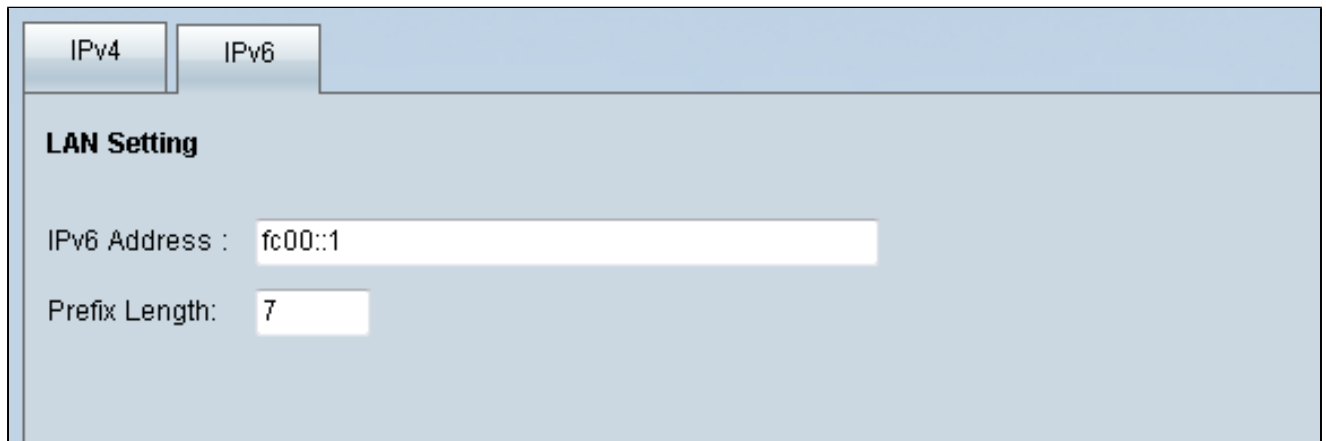
Interface	IP Address	Configuration
DMZ	0.0.0.0	

2단계. IP Mode(IP 모드) 필드에서 Dual-Stack IP(듀얼 스택 IP) 라디오 버튼을 클릭하여 IPv6 주소의 컨피그레이션을 활성화합니다.

### IP Mode

Mode	WAN	LAN
<input type="radio"/> IPv4 Only	IPv4	IPv4
<input checked="" type="radio"/> Dual-Stack IP	IPv4 and IPv6	IPv4 and IPv6

3단계. IPv6 주소에 DMZ를 구성할 수 있도록 LAN Setting(LAN 설정) 필드에 있는 IPv6 탭을 클릭합니다.



The screenshot shows the 'LAN Setting' configuration page with the 'IPv6' tab selected. The 'IPv6 Address' field contains 'fc00::1' and the 'Prefix Length' field contains '7'.

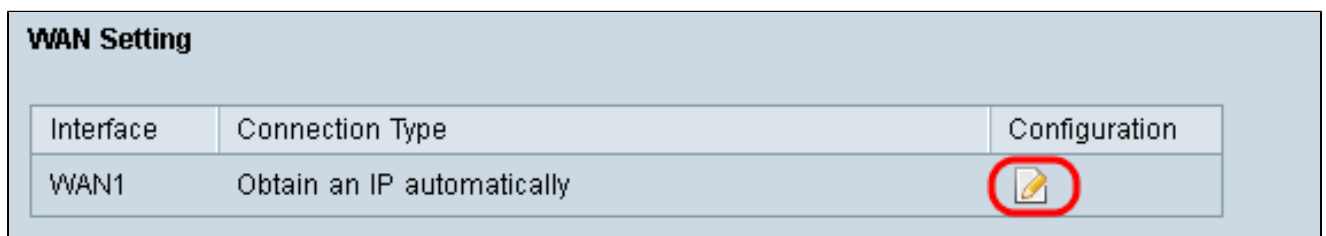
4단계 DMZ 설정 영역으로 스크롤하여 DMZ 확인란을 클릭하여 DMZ를 활성화합니다




The screenshot shows the 'DMZ Setting' configuration page. The 'Enable DMZ' checkbox is checked and circled in red. Below it is a table with columns for Interface, IP Address, and Configuration.

Interface	IP Address	Configuration
DMZ	::/64	

5단계. WAN Setting(WAN 설정) 필드에서 Edit(편집) 버튼을 클릭하여 WAN1 설정의 IP Static(IP 고정)을 편집합니다.



The screenshot shows the 'WAN Setting' configuration page. A table lists WAN settings with columns for Interface, Connection Type, and Configuration. The 'Configuration' column for 'WAN1' has an edit icon circled in red.

Interface	Connection Type	Configuration
WAN1	Obtain an IP automatically	

Network(네트워크) 페이지가 열립니다.

# Network

## Edit WAN Connection

Interface :	WAN1
WAN Connection Type :	Static IP
Specify WAN IP Address :	192.168.3.1
Subnet Mask :	255.255.255.0
Default Gateway Address :	192.168.3.2
DNS Server (Required) 1 :	0.0.0.0
2 :	0.0.0.0
MTU :	<input checked="" type="radio"/> Auto <input type="radio"/> Manual <input type="text" value="1500"/> bytes
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

6단계. WAN Connection Type 드롭다운 목록에서 Static IP를 선택합니다.

7단계. Specify WAN IP Address(WAN IP 주소 지정) 필드의 System Summary(시스템 요약) 페이지에 표시되는 WAN IP 주소를 입력합니다.

8단계. Subnet Mask 필드에 서브넷 마스크 주소를 입력합니다.

9단계. Default Gateway Address 필드에 기본 게이트웨이 주소를 입력합니다.

10단계. DNS Server (Required) 1(DNS 서버(필수) 1) 필드에서 System Summary(시스템 요약) 페이지에 표시되는 DNS 서버 주소를 입력합니다.

참고: DNS 서버 주소 2는 선택 사항입니다.

11단계. Maximum Transmission Unit (MTU)(최대 전송 단위(MTU))를 Auto(자동) 또는 Manual(수동)로 선택합니다. manual(수동)을 선택하는 경우 Manual MTU(수동 MTU)에 대한

바이트를 입력합니다.

12단계. 설정을 저장하려면 Save(저장) 탭을 클릭합니다.

## ACL 정의

1단계. Web Configuration Utility(웹 컨피그레이션 유틸리티) 페이지에 로그인하고 Firewall(방화벽) > Access Rules(액세스 규칙)를 선택합니다. Access Rules 페이지가 열립니다.

Priority	Enable	Action	Service	Source Interface	Source	Destination	Time	Day	Delete
	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always		
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN	Any	Any	Always		
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	DMZ	Any	Any	Always		

참고: Access Rules(액세스 규칙) 페이지를 입력하면 기본 액세스 규칙을 편집할 수 없습니다

2단계. 새 액세스 규칙을 추가하려면 Add 버튼을 클릭합니다.

Priority	Enable	Action	Service	Source Interface	Source	Destination	Time	Day	Delete
	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always		
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN	Any	Any	Always		
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	DMZ	Any	Any	Always		

이제 Access Rules(액세스 규칙) 페이지에 Service(서비스) 및 Scheduling(예약) 영역에 대한 옵션이 표시됩니다.

## Access Rules

**Services**

Action :

Service :

Log :

Source Interface :

Source IP :

Destination IP :

---

**Scheduling**

Time :

From :  (hh:mm) To :  (hh:mm)

Effective on :  Everyday  Sun  Mon  Tue  Wed  Thu  Fri  Sat

3단계. 서비스를 허용하려면 Action 드롭다운 목록에서 Allow를 선택합니다.

4단계. DMZ에 대해 모든 서비스를 활성화하려면 Service 드롭다운 목록에서 All Traffic [TCP&UDP/1~65535]을 선택합니다.

5단계. Log(로그) 드롭다운 목록에서 Log packets match this rule(이 규칙과 일치하는 로그 패킷)을 선택하여 액세스 규칙과 일치하는 로그만 선택합니다.

6단계. Source Interface 드롭다운 목록에서 DMZ를 선택합니다. 액세스 규칙의 소스입니다.

7단계. Source IP 드롭다운 목록에서 Any를 선택합니다.

8단계. Destination IP 드롭다운 목록에서 Single을 선택합니다.

9단계. 액세스 규칙을 허용할 대상의 IP 주소를 Destination IP 필드에 입력합니다.

10단계. Scheduling(예약) 영역에서 Time(시간) 드롭다운 목록에서 Always(항상)를 선택하여 액세스 규칙을 항상 활성화합니다.

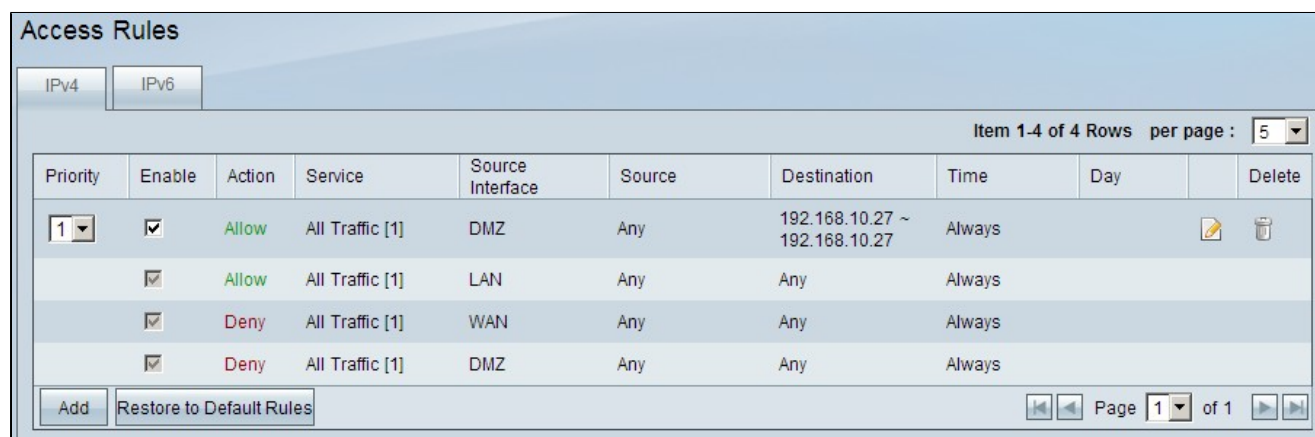
참고: Time 드롭다운 목록에서 Always(항상)를 선택하면 Effective on(유효 날짜) 필드에서 액세스 규칙이 Everyday(매일)로 기본 설정됩니다.

참고: Time 드롭다운 목록에서 Interval(간격)을 선택하여 특정 시간 간격(액세스 규칙이 활성화)을 선택할 수 있습니다. 그런 다음 Effective on(유효 날짜) 확인란에서 액세스 규칙을 활성화할 날짜를 선택할 수 있습니다.



11단계. Save(저장)를 클릭하여 설정을 저장합니다.

참고: 팝업 창이 나타나면 '확인'을 눌러 다른 액세스 규칙을 추가하거나 '취소'를 눌러 액세스 규칙 페이지로 돌아갑니다.

이전 단계에서 생성한 액세스 규칙이 표시됩니다



The screenshot shows the 'Access Rules' configuration window. It has tabs for 'IPv4' and 'IPv6'. The table below lists the rules. The first rule is selected, and its priority is shown as '1' in a dropdown menu. The table has columns for Priority, Enable, Action, Service, Source Interface, Source, Destination, Time, Day, and Delete. At the bottom, there are buttons for 'Add' and 'Restore to Default Rules', and a page indicator showing 'Page 1 of 1'.

Priority	Enable	Action	Service	Source Interface	Source	Destination	Time	Day	Delete
1	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	DMZ	Any	192.168.10.27 ~ 192.168.10.27	Always		 
	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always		
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN	Any	Any	Always		
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	DMZ	Any	Any	Always		

12단계. 생성된 액세스 규칙을 수정하려면 Edit(수정) 아이콘을 클릭합니다.

13단계. 생성된 액세스 규칙을 삭제하려면 Delete(삭제) 아이콘을 클릭합니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.