

RV016, RV042, RV042G 및 RV082 VPN Router에서 서브넷 마스크를 사용하는 DeMilitarized Zone 포트 구성

목표

DMZ(De-Militarized Zone)는 조직의 내부 네트워크에서 인터넷과 같은 신뢰할 수 없는 네트워크에 사용할 수 있는 부분입니다. DMZ는 조직 내부 네트워크의 보안을 개선하는 데 도움이 됩니다. 인터넷에서 모든 내부 리소스를 사용할 수 있는 대신 웹 서버와 같은 특정 호스트만 사용할 수 있습니다.

ACL(Access Control List)이 인터페이스에 바인딩되면 해당 인터페이스에 도착하는 패킷에 ACE(Access Control Element) 규칙이 적용됩니다. ACL의 ACE와 일치하지 않는 패킷은 일치하지 않는 패킷을 삭제하는 작업을 수행하는 기본 규칙과 일치합니다. 이 문서에서는 DMZ 포트를 구성하고 DMZ에서 특정 목적지 IP 주소로 이동하는 트래픽을 허용하는 방법을 보여줍니다.

적용 가능한 디바이스

- RV016
- RV042
- RV042G
- RV082

소프트웨어 버전

- v4.2.2.08

서브넷을 포함한 DMZ 구성

1단계. Router Configuration Utility(라우터 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

IPv4

IPv6

LAN Setting

MAC Address : 64:9E:F3:88:C6:88

Device IP Address :

Subnet Mask :


Multiple Subnet : Enable

WAN Setting

Interface	Connection Type	Configuration
WAN1	Static IP	

DMZ Setting

Enable DMZ

Interface	IP Address	Configuration
DMZ	0.0.0.0	

2단계. IPv4 또는 IPv6 주소에서 DMZ를 구성하려면 LAN Setting(LAN 설정) 필드에 있는 해당 탭을 클릭합니다.

참고: IPv6를 구성하려면 IP Mode 영역에서 Dual-Stack IP를 활성화해야 합니다.

3단계. 아래로 스크롤하여 DMZ 설정 필드로 이동하고 DMZ 사용 라디오 버튼을 클릭하여 DMZ를 활성화합니다.

WAN Setting

Please choose how many WAN ports you prefer to use : 2 (Default value is 2)

Interface	Connection Type	Configuration
WAN1	Obtain an IP automatically	
WAN2	Obtain an IP automatically	

Interface	IP Address	Configuration
DMZ	0.0.0.0	

4단계. 서브넷을 구성하려면 DMZ 컨피그레이션 아이콘을 클릭합니다. IPv4 및 IPv6에 대해 다음 방법으로 구성할 수 있습니다.

IPv4 컨피그레이션

Network

Edit DMZ Connection

Interface : DMZ

Subnet Range (DMZ & WAN within same subnet)

Specify DMZ IP Address : 10.10.10.1

Subnet Mask : 255.255.255.0

Save Cancel

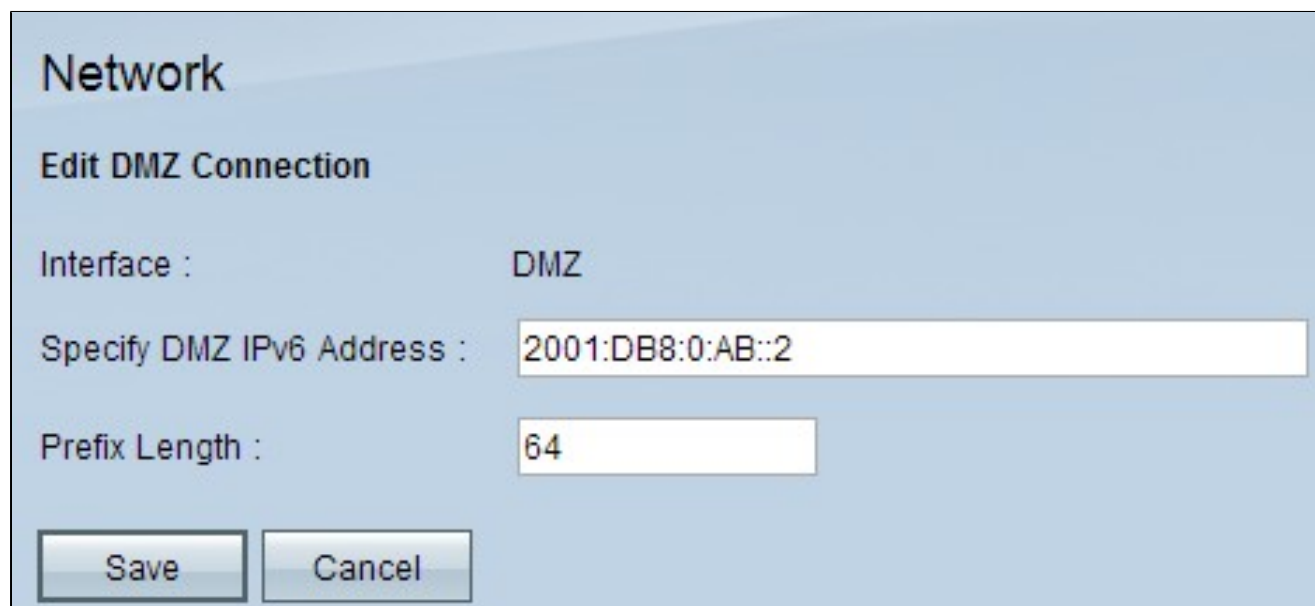
5단계. DMZ를 WAN이 아닌 다른 서브넷으로 구성하려면 Subnet(서브넷) 라디오 버튼을 클릭합니다. 서브넷 IP에 대해 다음을 구성해야 합니다

- DMZ IP 주소 지정 — DMZ IP 주소 지정 필드에 DMZ IP 주소를 입력합니다.
- 서브넷 마스크 — 서브넷 마스크 필드에 서브넷 마스크를 입력합니다.

경고: DMZ에 IP 주소가 있는 호스트는 내부 LAN 내부의 호스트만큼 안전하지 않습니다.

6단계. Range(범위)를 클릭하여 DMZ를 WAN과 동일한 서브넷에 있도록 구성합니다. IP 주소의 범위를 DMZ 포트의 IP 범위 필드에 입력합니다.

IPv6 컨피그레이션



Network

Edit DMZ Connection

Interface : DMZ

Specify DMZ IPv6 Address : 2001:DB8:0:AB::2

Prefix Length : 64

Save Cancel

참고: IPv6 컨피그레이션의 경우 다음 옵션을 사용할 수 있습니다.

7단계. Specify DMZ IPv6 Address — IPv6 주소를 입력합니다.

8단계. Prefix Length(접두사 길이) - 위에서 언급한 DMZ IP 주소 도메인의 접두사 길이를 입력합니다.

9단계. 컨피그레이션을 저장하려면 Save를 클릭합니다.

액세스 규칙 컨피그레이션

이 컨피그레이션은 여러 서브넷 마스크에 구성된 IP에 대한 액세스 목록을 정의하기 위해 수행됩니다.

1단계. Router Configuration Utility(라우터 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: 기본 액세스 규칙은 편집할 수 없습니다.

2단계. 새 액세스 규칙을 추가하려면 Add 버튼을 클릭합니다. Access Rules(액세스 규칙) 페이지가 변경되어 Services(서비스) 및 Scheduling(예약) 영역이 표시됩니다.

참고: 이 컨피그레이션은 Access Rules(액세스 규칙) 페이지에서 해당 탭을 선택하여 IPv4 및 IPv6 모두에 대해 수행할 수 있습니다. IPv4 및 IPv6에 특정한 컨피그레이션 단계는 다음 단계에서 언급됩니다.

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(작업) 드롭다운 목록에서 Allow(허용)를 선택합니다.

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

5단계. 액세스 규칙과 일치하는 로그만 선택하려면 Log 드롭다운 목록에서 Log packets that match this rule을 선택합니다.

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

7단계. Source IP 드롭다운 목록에서 Any를 선택합니다.

8단계. Destination IP 드롭다운 목록에서 사용 가능한 다음 옵션 중 하나를 선택합니다.

- Single — 단일 IP 주소에 이 규칙을 적용하려면 Single을 선택합니다.
- 범위 — 범위를 선택하여 IP 주소 범위에 이 규칙을 적용합니다. 범위의 첫 번째와 마지막 IP 주소를 입력합니다. 이 옵션은 IPv4에서만 사용할 수 있습니다.
- Subnet — 이 규칙을 서브네트워크에 적용하려면 Subnet을 선택합니다. 서브넷에 대한 IP 주소 할당 및 인터넷 프로토콜 패킷 라우팅에 사용되는 IP 주소 및 CIDR 표기법 번호를 입력합니다. 이 옵션은 IPv6에서만 사용할 수 있습니다.
- Any — IP 주소에 규칙을 적용하려면 Any를 선택합니다.

시간 절약: IPv6 액세스 규칙을 구성하는 경우 10단계로 건너뛩니다.

9단계. Time 드롭다운 목록에서 규칙이 활성화 상태일 때 정의할 방법을 선택합니다. 제품:

- Always — Time 드롭다운 목록에서 Always를 선택하면 액세스 규칙이 트래픽에 항상 적용됩니다.
- Interval — Time 드롭다운 목록에서 Interval을 선택하면 액세스 규칙이 활성화되는 특정 시간 간격을 선택할 수 있습니다. 시간 간격을 지정한 후 Effective on(유효 날짜) 확인란에서 액세스 규칙을 활성화할 날짜를 선택합니다.

10단계. Save(저장)를 클릭하여 설정을 저장합니다.

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		

Item 1-4 of 4 Rows per page : 5

Add Restore to Default Rules Page 1 of 1

11단계. 생성된 액세스 규칙을 수정하려면 Edit(수정) 아이콘을 클릭합니다.

12단계. 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.