RV320 및 RV325 VPN Router Series의 시스템 로그 구성

목표

시스템 로그는 네트워크 이벤트의 레코드입니다.로그는 네트워크가 작동하는 방식을 이해하는 데 사용되는 중요한 도구입니다.네트워크 관리 및 네트워크 문제 해결에 유용합니다.

이 문서에서는 기록할 로그 유형을 구성하는 방법, RV32x VPN Router Series의 로그를 보는 방법, SMS를 통해 수신자에게 로그를 전송하거나, 시스템 로그 서버로 또는 이메일을 통해 수신자에게 보내는 방법에 대해 설명합니다.

적용 가능한 디바이스

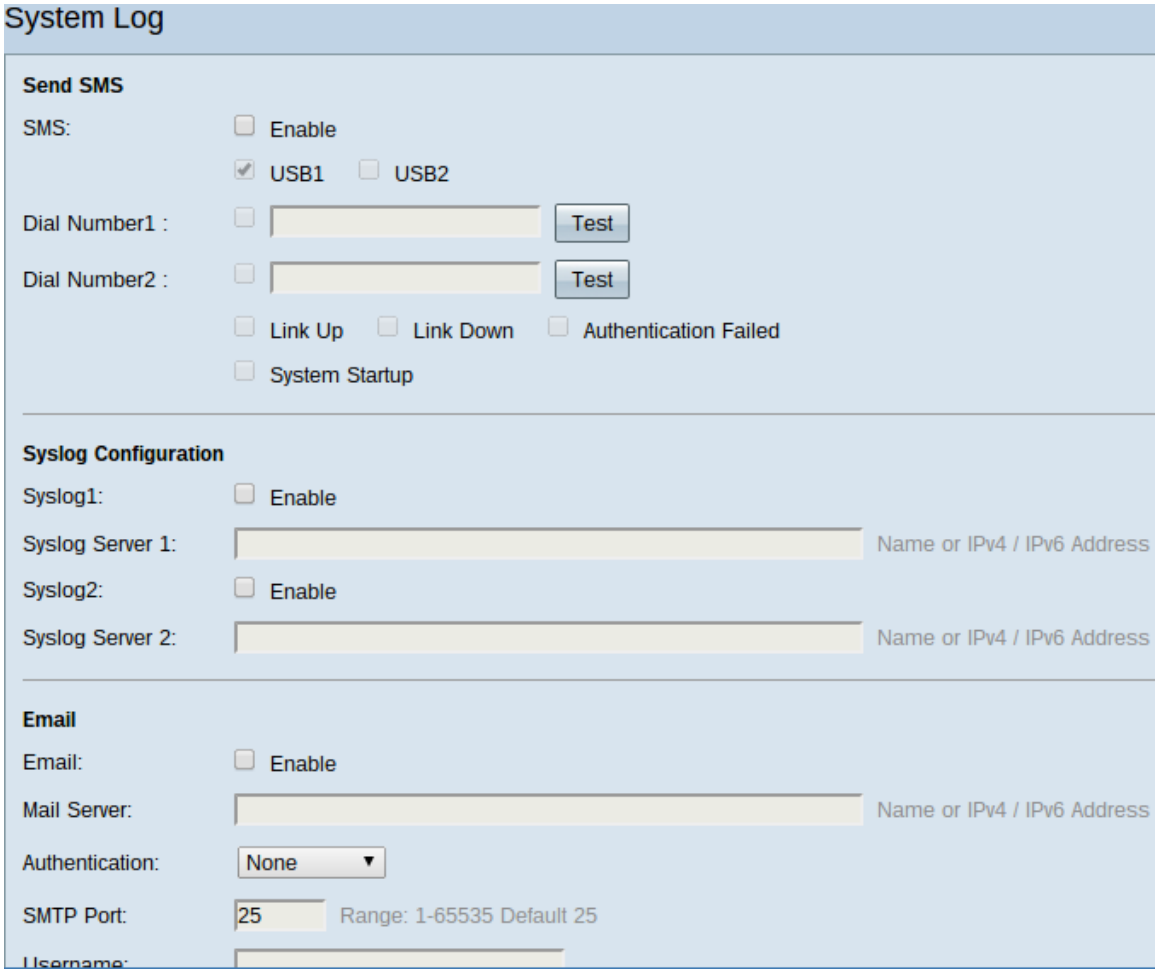
·RV320 Dual WAN VPN Router
· RV325 Gigabit Dual WAN VPN Router

소프트웨어 버전

·v1.1.0.09

시스템 로그 구성

1단계. Web Configuration Utility에 로그인하고 **Log > System Log**를 선택합니다.System *Log* 페이지가 열립니다.



시스템 로그 페이지에 대한 자세한 내용은 다음 절을 참조하십시오.

·SMS별 시스템 로그 — SMS를 통해 시스템 로그를 전화로 보내는 방법

·시스템 로그 서버의 시스템 로그 — 시스템 로그를 시스템 로그 서버로 전송하는 방법.

·이메일 시스템 로그 — 시스템 로그를 이메일 주소로 보내는 방법

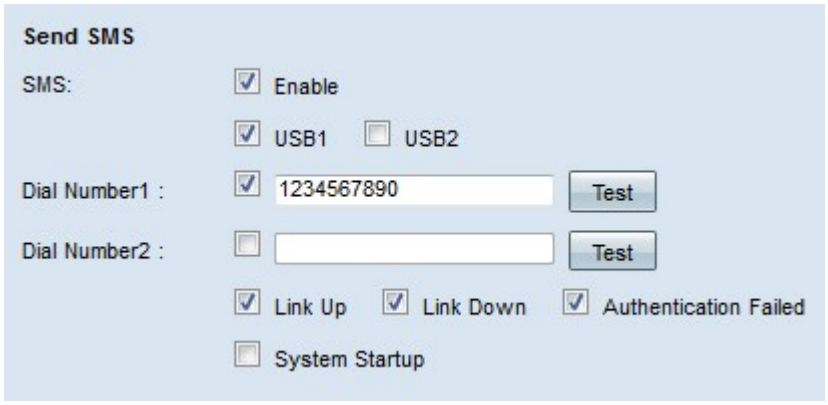
·로그 설정 — 로그에 저장된 메시지 유형을 구성하는 방법

·시스템 로그 보기 — 디바이스의 시스템 로그를 보는 방법

·View Outgoing Log Table(발신 로그 테이블 보기) - 발신 패킷과 관련된 시스템 로그를 보는 방법.

·View Incoming Log Table(수신 로그 테이블 보기) - 수신 패킷과 관련된 시스템 로그를 보는 방법.

SMS별 시스템 로그



1단계. SMS(Short Message Service) 메시지를 통해 클라이언트에 시스템 로그를 전송하려면 SMS 필드에서 Enable(활성화)을 선택합니다.

2단계. 3G USB 모뎀이 연결된 USB 포트의 확인란을 선택합니다.

3단계. Dial Number1(다이얼 번호1) 필드의 확인란을 선택하고 메시지를 보낼 전화 번호를 입력합니다.

참고:전화 번호 1에 대한 연결을 테스트하려면 **테스트**를 클릭하십시오. 구성된 번호가 테스트 메시지를 받지 못하면 전화 번호가 전화 번호1 필드에 올바르게 입력되었는지 확인하십시오.

4단계. (선택 사항) Dial Number2(다이얼 번호2) 필드의 확인란을 선택하고 메시지를 보낼 전화 번호를 입력합니다.

참고:전화 번호 2에 대한 연결을 테스트하려면 **테스트**를 클릭하십시오. 구성된 번호가 테스트 메시지를 받지 못하면 전화 번호가 전화 번호2 필드에 올바르게 입력되었는지 확인하십시오.

5단계. 로그를 전송할 이벤트를 트리거할 이벤트의 확인란을 선택합니다.

·Link Up — RV320에 대한 연결이 설정되었습니다.

·Link Down — RV320에 대한 연결이 중단되었습니다.

·인증 실패 — 인증에 실패했습니다.

·시스템 시작 — 라우터가 부팅됩니다.

6단계. **저장**을 클릭합니다.SMS를 통한 시스템 로그가 구성됩니다.

시스템 로그 서버의 시스템 로그

1단계. Syslog1 필드에서 Enable(활성화)을 선택하여 시스템 로그를 시스템 로그 서버로 전송합니다.

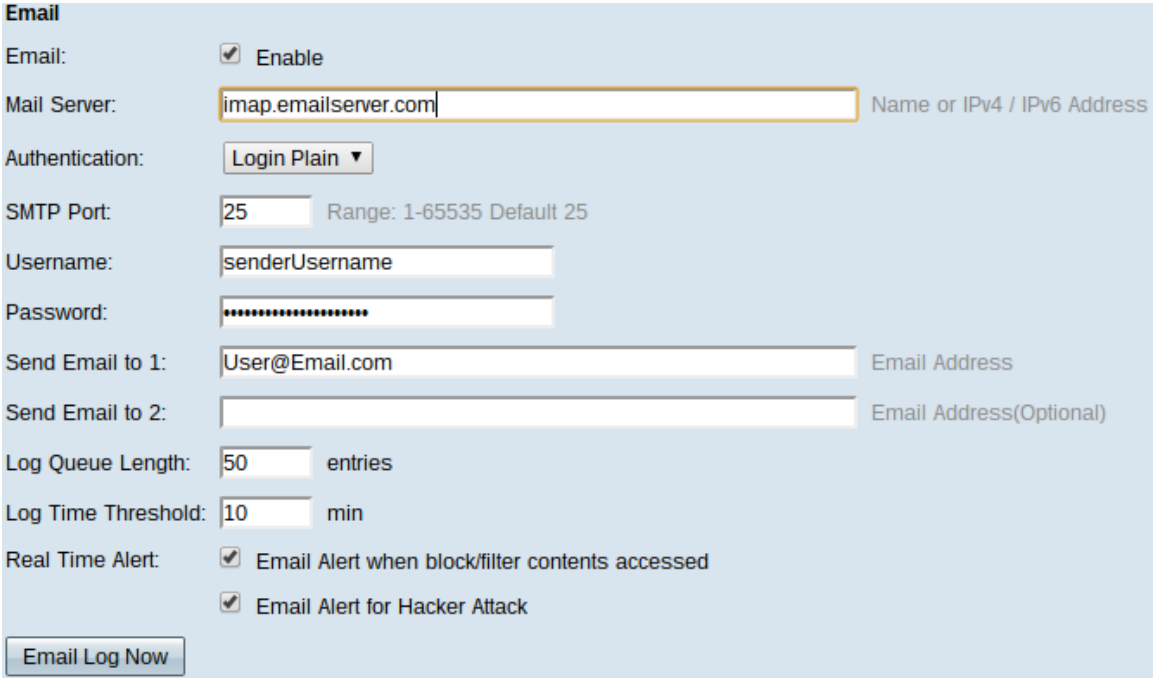
2단계. Syslog Server 1 필드에 시스템 로그 서버의 호스트 이름 또는 IP 주소를 입력합니다.

3단계. (선택 사항) 로그를 다른 시스템 로그 서버로 보내려면 Syslog2 필드에서 Enable을 선택합니다.

4단계. Syslog2 필드에 확인란이 선택되어 있으면 Syslog Server 2 필드에 시스템 로그 서버의 호스트 이름 또는 IP 주소를 입력합니다.

9단계. **저장**을 클릭합니다.시스템 로그 서버를 통한 시스템 로그가 구성됩니다.

이메일 시스템 로그



1단계. Email(이메일) 필드에서 Enable(활성화)을 선택하여 이메일을 통해 수신자에게 시스템 로그를 전송합니다.

2단계. 메일 서버 필드에 메일 서버의 도메인 이름 또는 IP 주소를 입력합니다.

3단계. 메일 서버가 Authentication(인증) 필드에서 사용하는 인증 유형을 선택합니다.

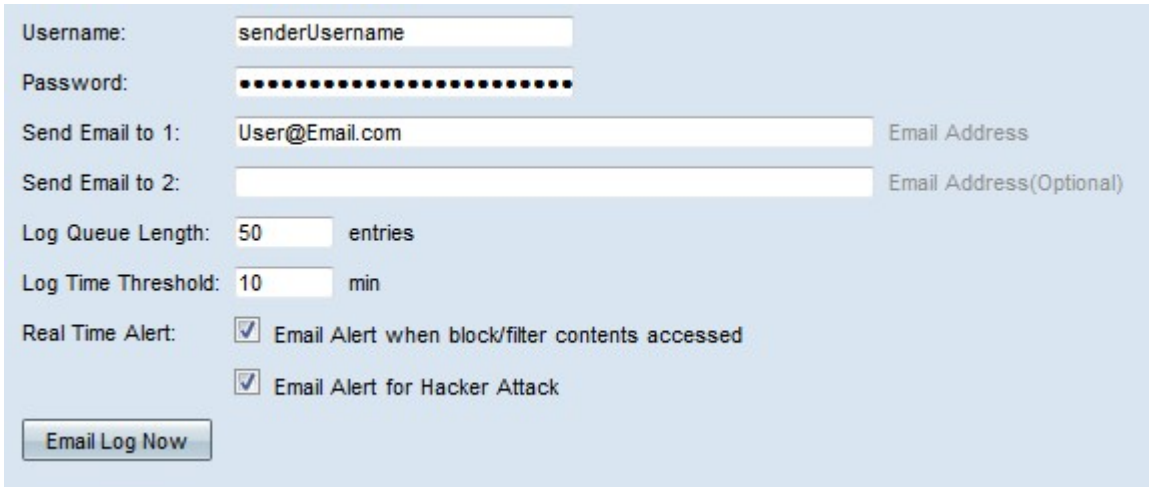
·없음 — 메일 서버에서 인증을 사용하지 않습니다.

·로그인 일반 — 메일 서버는 일반 텍스트 형식의 인증을 사용합니다.

·TLS — 메일 서버는 TLS(Transport Layer Security)를 사용하여 클라이언트와 서버가 인증 정보를 안전하게 교환할 수 있도록 합니다.

·SSL — 메일 서버는 SSL(Secure Sockets Layer)을 사용하여 클라이언트와 서버가 인증 정보를 안전하게 교환할 수 있도록 합니다.

4단계. 메일 서버가 SMTP 포트 필드에 사용하는 SMTP(Simple Mail Transfer Protocol) 포트를 입력합니다.SMTP는 IP 네트워크를 통해 이메일을 전송할 수 있는 프로토콜입니다.



5단계. Username(사용자 이름) 필드에 이메일 발신자의 사용자 이름을 입력합니다.

6단계. Password(비밀번호) 필드에 이메일 발신자의 비밀번호를 입력합니다.

7단계. 이메일 수신자의 이메일 주소를 Send Email to 1 필드에 입력합니다.

8단계. (선택 사항) Send Email to 2 필드에 로그 이메일을 보낼 추가 이메일 주소를 입력합니다.

9단계. 로그를 전자 메일 수신자에게 보내기 전에 만들어야 하는 로그 항목의 수를 Log Queue Length 필드에 입력합니다.

10단계. 디바이스가 Log Time Threshold(로그 시간 임계값) 필드에 이메일을 보내는 간격을 입력합니다.

11단계. Real Time Alert(실시간 알림) 필드의 첫 번째 확인란을 선택하여 차단 또는 필터링된 사용자가 라우터에 액세스하려고 시도할 때 이메일을 즉시 전송합니다.

12단계. 해커가 DOS(Denial of Service) 공격을 통해 라우터에 액세스하려고 할 때 즉시 이메일을 보내려면 Real Time Alert 필드의 두 번째 확인란을 선택합니다.

참고: Email **Log Now(지금** 이메일 로그)를 클릭하여 즉시 로그를 전송합니다.

13단계. 저장을 **클릭합니다**.이메일을 통한 시스템 로그가 구성됩니다.

로그 설정

1단계. 로그 항목을 트리거할 이벤트의 확인란을 선택합니다.

·경보 로그 — 이러한 로그는 공격 또는 공격 시도가 발생했을 때 생성됩니다.

- Syn Flooding — SYN 요청은 라우터가 처리할 수 있는 것보다 빠르게 수신됩니다.

- IP 스푸핑 — RV320은 위조된 소스 IP 주소가 있는 IP 패킷을 수신했습니다.

- 무단 로그인 시도 — 네트워크에 로그온하려는 거부된 시도가 실패했습니다.

- Ping of Death — 대상 장치를 손상시키기 위해 비정상적인 크기의 ping이 인터페이스에 전송되었습니다.

- WinNuke — WinNuke로 알려진 원격 DDOS(Distributed Denial of Service Attack)가 대상 장치를 파괴하려고 인터페이스에 전송되었습니다.

·일반 로그 — 일반 네트워크 작업이 발생할 때 이러한 로그가 생성됩니다.

- Deny Policies(정책 거부) - 라우터의 구성된 정책에 따라 사용자에게 액세스가 거부되었습니다.

- Authorized Login(인증된 로그인) - 사용자가 네트워크에 액세스할 수 있는 권한이 부여되었습니다.

- 시스템 오류 메시지 — 시스템 오류가 발생했습니다.

- Allow Policies(정책 허용) - 라우터의 구성된 정책에 따라 사용자에게 액세스가 부여되었습니다.

- 커널 — 모든 커널 메시지를 로그에 포함합니다.커널은 부팅 시 메모리로 로드하는 운영 체제의 첫 번째 부분입니다.커널 메시지는 커널과 연결된 로그입니다.

- 컨피그레이션 변경 — 라우터 컨피그레이션이 수정되었습니다.

- IPSEC 및 PPTP VPN — IPSEC 및 PPTP VPN 협상, 연결 또는 연결이 끊어졌습니다.

- SSL VPN — SSL VPN 협상, 연결 또는 연결이 끊어졌습니다.

- 네트워크 — WAN 또는 DMZ 인터페이스에서 물리적 연결이 생성되었거나 끊어졌습니다.

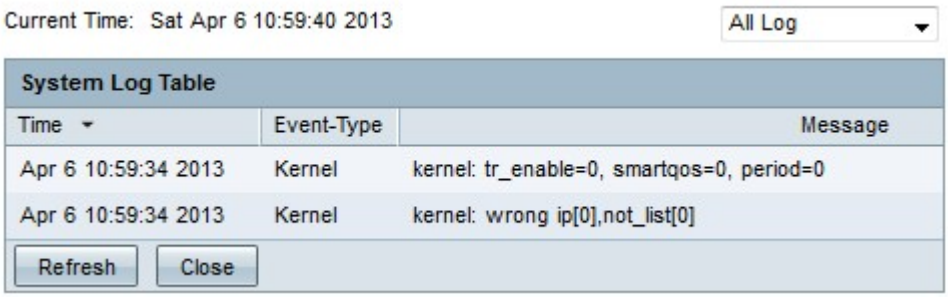
2단계. **저장**을 클릭합니다.로그 설정이 구성됩니다.

참고:현재 로그**를** 지우려면 Clear Log를 클릭합니다.

시스템 로그 보기

1단계. **View System Log(시스템 로그 보기)**를 클릭하여 시스템 로그 테이블을 확인합니다

.System *Log Table* 창이 나타납니다.



2단계. (선택 사항) 드롭다운 목록에서 볼 로그 유형을 선택합니다.

·모든 로그 — 모든 로그 메시지를 포함합니다.

·시스템 로그 — 시스템 오류 메시지만 포함합니다.

·방화벽/DoS 로그 — 경고 로그만 포함합니다.

·VPN 로그 — IPSec 및 PPTP VPN 및 SSL VPN 로그만 포함합니다.

·네트워크 로그 — 네트워크 로그만 포함합니다.

·커널 로그 — 커널 메시지만 포함합니다.

·사용자 로그 — 거부 정책, 허용 정책, 인증된 로그인 및 구성 변경 로그만 포함

·SSL 로그 — SSL VPN 로그만 포함합니다.

시스템 로그 테이블에는 다음 정보가 표시됩니다.

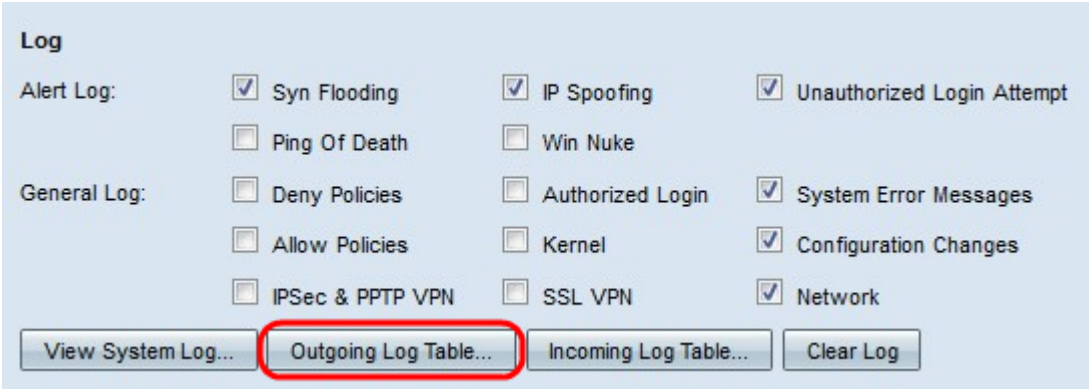
·시간 — 로그가 생성된 시간입니다.

·이벤트 유형 — 로그 유형입니다.

·메시지 — 로그에 해당하는 정보.여기에는 정책 유형, 소스 IP 주소 및 소스 MAC 주소가 포함됩니다.

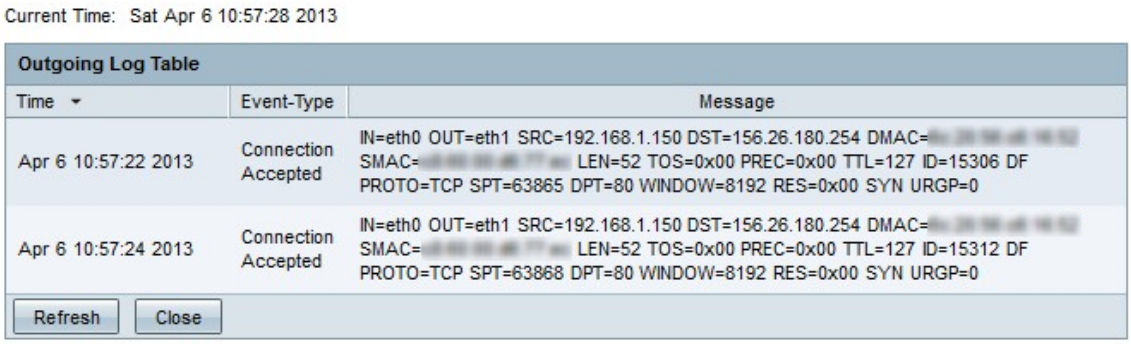
참고: Refresh(**새로** 고침)를 클릭하여 로그 테이블을 새로 고칩니다.

발송 로그 테이블 보기



1단계. 발신 패킷과 관련된 로그 테이블을 보려면 Outgoing Log Table을 클릭합니다

.Outgoing *Log Table* 창이 나타납니다.



발송 로그 테이블에는 다음 정보가 표시됩니다.

·시간 — 로그가 생성된 시간입니다.

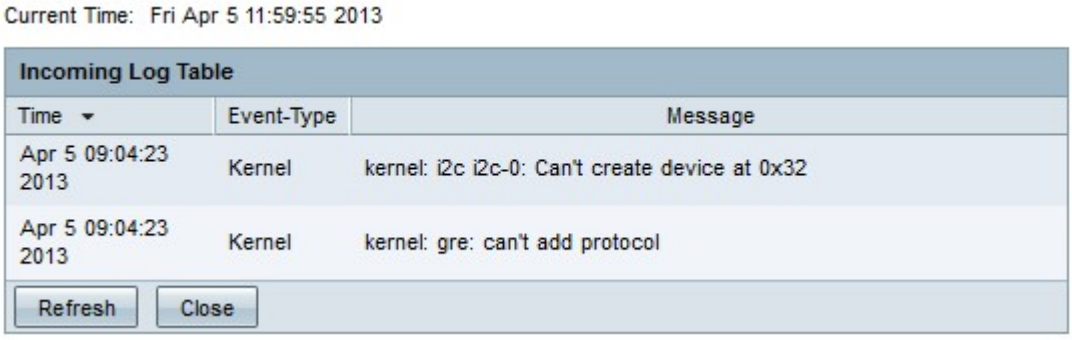
·이벤트 유형 — 로그 유형입니다.

·메시지 — 로그에 해당하는 정보.여기에는 정책 유형, 소스 IP 주소 및 소스 MAC 주소가 포함됩니다.

참고: Refresh(**새로** 고침)를 클릭하여 로그 테이블을 새로 고칩니다.

수신 로그 테이블 보기

1단계. 수신 패킷과 관련된 로그 테이블을 보려면 Incoming Log Table을 클릭합니다.Incoming *Log Table* 창이 나타납니다.



수신 로그 테이블에는 다음 정보가 표시됩니다.

·시간 — 로그가 생성된 시간입니다.

·이벤트 유형 — 로그 유형입니다.

·메시지 — 로그에 해당하는 정보.여기에는 정책 유형, 소스 IP 주소 및 소스 MAC 주소가 포함됩니다.

참고: Refresh(**새로** 고침)를 클릭하여 로그 테이블을 새로 고칩니다.