Endian UTM 5.0 참조 설명서

버전 5의 Endian 장치를 가지고 있다면, 그것들의 전용 참조 설명서를 다음에서 찾을 수 있습니다.

- UTM series: Security 게이트웨이들, 즉 Mini 25, Mercury Series, Macro Series – 본 매뉴얼
- Hotspot series: Hotspot 장치들
- 4i series: 산업용 장치들, 즉, 4i Edge 112/313/515.

서론

Endian UTM Appliance는 오픈 소스 통합 위험 관리(UTM) 어플라이언스 소프트웨어입니다. 본 문서는 Endian UTM Appliance 웹 인터페이스의 여러 부분과 그것의 기능들의 구성에 대한 사용 설명서 및 안내서입니다.

Endian UTM Appliance의 최신 버전에 대한 본 설명서의 최신 업데이트 및 수정본은 http://docs.endian.com/3.2/utm/에서 온라인으로 제공됩니다. 간단한 오타 또는 심지어 내용 오류와 같은 문제를 발견했다면, Endian 웹 사이트의 양식을 사용하여 의견을 보내주십시오.

법적 고지

이 문서는 2.4 버전을 작성했던 Andreas Ender, Diego Gagliardo, Luca Giovenzana, Christian Graffer, Raphael Lechner, Chris Mair, Raphael Vallazza, Peter Warasin (알파벳 순으로 작성)와 같은 다른 Endian 팀원들의 도움을 받아 Stefano David이편집 및 작성하였습니다. 2.4 문서 중 일부는 Chris Clancey, Harry Goldschmitt, John Kastner, Eric Oberlander, Peter Walker가 작성한 IPCop 관리 가이드와 Marco Sondermann이 쓴 IPCop 고급 프록시 관리 가이드를 기반으로 합니다.

본 문서에 포함된 정보는 한 버전에서 다음 버전으로 변경될 수 있으며, 시간이 지나면서 내용을 개선하고 오류나 실수를 수정하거나 새로운 기능이나 변경된 기능을 설명하기 위해 예고없이 변경될 수 있습니다. 마지막 업데이트 날짜는 항상 모든 페이지 하단에 표시되어 있습니다.

본 문서에 포함된 모든 프로그램 및 세부 정보는 최선을 다해 작성되었으며 신중하게 테스트되었습니다. 그러나 오류를 완전히 배제할 수는 없습니다. 따라서 Endian은본 문서 내의 오류나 본 문서 또는 관련 자료의 유효성, 성능 또는 사용으로 인해 발생하는 결과적 손해에 대해 어떠한 보증을 표현하거나 암시하지 않습니다.

상표일 수도 있습니다.

감사 인사

Smoothwall과 IPCop 팀의 위대한 업적이 없었다면, Endian UTM Appliance나 본 문서가 존재하지 않았을 겁니다. 그러므로, 우리는 이렇게 어려운 작업에 헌신한 그들 모두에게 감사드립니다.

그리고 호스팅을 허락해 준 소스포지 (Sourceforge)에 감사드립니다. Sourceforge가 없었다면, 우리는 전 세계적으로 그렇게 크게 눈에 띄게 되는 기회를 확보할 수 있는 가능성을 갖지 못했을 것입니다. 여러분들 모두 진정으로 저희를 도와주셔서 감사합니다!

Endian 웹 사이트

Endian S.p.A., Italy 및 해당 제품에 대한 자세한 내용은 Endian 웹 사이트 (http://www.endian.com/)를 참조하십시오.

이 설명서의 많은 리소스 (자습서, 사용 방법들, 예제들)는 해당 웹 사이트에서 가져옵니다.

- http://help.endian.com/ 고객 및 사용자를 지원하기 위한 참조 사이트가 되어야하는 Endian 제품들에 대한 새로운 지원 센터입니다. 이 사이트의 사용 방법들에 대한 몇 개의 링크는 여러 하위 섹션의 끝에 있는 본 문서에서 제공됩니다.
- http://kb.endian.com/ Endian의 오래된 지식 기반은 현재 중단되었습니다. 구성 예제들을 포함하여, 그 내용은 help.endian.com 사이트의 참조 설명서에 포함되어 있습니다.
- http://jira.endian.com/ Endian의 버그 추적기는 기존 버그와 해결 방법이나 그 문제의 회피 방법을 찾아내고, 새로운 문제를 보고하는 장소입니다. 이 도구는 여전히 액세스 가능하며 이전 시스템에서 발견된 문제들에 대한 팁과 해결 방법을 찾을 수 있는 http://bugs.endian.com/사이트의 이전 버그 추적기를 대체합니다.

또한 Community Edition의 사용자들에게 도움을 주기 위해 인터넷 상에 여러 포럼이 생성되어 있습니다. Endian에서 유지 관리하지는 않지만, 그럼에도 불구하고, 등록된 기기들의 경우라도, Endian UTM Appliance 사용자들 모두에게 유용한 리소스입니다.

- http://endian.anxalug.org (이탈리아어)
- http://www.efw-forum.de (독일어)
- http://efwsupport.com (영어)
- http://www.securitywithpassion.com.au/ (영어)
- http://endian.eth0.com.br (포르투갈어)

- http://linux.eduardosilva.eti.br/endian ( 포르투갈어)
- http://www.endianturk.org/ ( 터키어)
- http://www.bilside.com/forum/endian-firewall.html ( 터키어)
- http://forum.endian-utm.ru ( 러시아어)

모든 포럼과 함께 업데이트된 목록은 Endian 웹 사이트에서 찾을 수 있습니다.

마지막으로 Endian UTM Appliance 프로젝트의 sourceforge 페이지에서 가입 안내에 대한 설명이 있는 메일링 리스트를 찾을 수 있습니다.

시작하기

이 섹션은 설명서의 나머지 부분에서 사용된 규칙을 소개하고 난 후에, 영역(zones)의 개념에 대한 소개 개념을 제공하고, Endian UTM 3.0 제품의 GUI 및 Endian UTM Appliance (기기)에 접근 가능한 방법들에 대해 설명합니다.

본 참조 설명서에 대하여

이 설명서는 Software Enterprise 3.0을 지침서로 삼아 3.0 릴리스 용으로 작성되었지만, 모든 유형의 Endian UTM 어플라이언스와 UTM 시리즈를 대상으로 만들어 졌습니다. 다양한 Endian UTM Appliances들 간에 기능과 성능이 다를 수 있으므로, 일부 표시된 데이터 또는 구성 옵션에 대한 설명이 일부 기기에 따라 약간 다를 수 있거나 아예 존재하지 않을 수 있습니다. 이 지침서는 Endian UTM Appliance에서 제공하는 다양한 기능들 이면에 숨겨진 일부 개념에 대한 간략한 소개 설명을 제공하는 사용자 설명서뿐만 아니라 온라인 및 상황별 도움말입니다.

이 안내서에 대한 피드백이나 발견된 모든 오류는 Endian의 웹 페이지 (http://www.endian.com/us/community/get-help/documentation/)를 이용하여 보고할 수 있습니다.

이 섹션의 나머지 부분에서는 이 안내서에 대한 약간의 기본 정보와 Endian UTM Appliance 내에서 여러분이 첫 단계를 수행하는 방법 그리고 몇 가지 중요한 개념을 소개하고 GUI의 가장 중요한 부분을 포함하고 있습니다.

이 문서에 사용된 규칙

이 문서의 가독성과 명확성을 높이기 위해 몇 가지 규칙이 사용됩니다.

툴팁(tooltip)은 마우스를 그것들 위로 움직일 때 다양한 용어들이 표시됩니다.

버튼(Button)은 현재 설정을 저장(Save)하거나 Endian UTM Appliance에서 파일을 업로드하기 위해 팝업 메뉴를 여는데 사용되는 클릭할 수 있는 GUI 부분을 표시합니다. 동일한 버튼이 다른 브라우저들에서는 다르게 렌더링 될 수 있습니다. 예를 들어, Firefox 기반 브라우저들의 Browse... 버튼은 Chrome 기반 브라우저들에서 파일 선택...(Choose File...)으로 표시됩니다.

F5 또는 Ctrl + F5는 각각 키보드 단축키 또는 함께 눌러야 할 키 조합을 표시합니다.

(하이퍼)링크는 클릭할 때 새 페이지를 열 수 있는 GUI의 클릭 가능한 항목입니다.

강조 표시 외에, *이탤릭체*는 웹 GUI에서 비대화형

이것은 예제 상자입니다.

이와 같은 상자들에는 주 문서에 설명된 일부 기능이나 서비스를 빠르게 설정하기 위한 환경설정 또는 짧은 실용안내 예제가 들어 있습니다.

객체 또는 레이블을 나타내는데 사용됩니다.

경고는 특별한 주의가 필요한 항목, 동작 또는 작업을 표시하는데 사용됩니다.

경고: 이 값을 변경하면 서비스가 다시 시작됩니다!

참고: 나중에 수정할 수 있음을 기억하십시오.

힌트: 옵션들의 환경설정에 대한 팁들

관련 주제 또는 예제

이것과 같은 상자들 ("주제")에서는 그렇게 간단하지 않은 설명이 필요한 일부 주제에 대한 설명을 찾을 수 있으며, 섹션의 해당 주제 또는 일부 설정의 환경구성과 관련이 있습니다. 또한 빠른 실용적인 사용 방법이나 예제가 나타날 수 있습니다. 그것들의 아래쪽에는 온라인 리소스에 대한 하나 이상의 하이퍼링크가 있을 수 있습니다.

새로 도입되거나 수정된 기능들에는 명시적으로 태그가 지정됩니다.

버전 5.0의 새로운 기능(NEW IN VERSION 5.0): *해당 기능이 처음 등장한 버전 및 간단한 설명이 표시됩니다.*

버전 5.0에서 변경됨(CHANGED IN VERSION 5.0): *이전 릴리스에 있었던 기능이지만 5.0에서 변경된 기능 또는 해당 버전에서 제거된 기능을 나타냅니다.*

*메뉴 바 ‣ 방화벽 ‣ 포트 포워딩/DNAT ‣ 시스템 규칙 표시*와 같은 시퀀스는 특정 페이지 나 구성 항목에 도달하기 위해 표시된 순서대로 항목들 각각을 클릭하는 것을 필요로 합니다. 본 예제에서는 방화벽의 DNAT에 대한 시스템 규칙의 구성을 보여주는 페이지에 접근하는 방법을 보여줍니다.

그렇지 않으면, *Menubar ‣ 방화벽 ‣ 포트 포워딩/DNAT ‣ [규칙 목록] ‣ 편집*과 같은 순서에서, *[...]*는 동작 (*편집*)을 수행하기 위해 선택된 어떤 것에 많은 수의 객체 (이 경우, 방화벽 규칙 목록이 있음)가 있음을 의미합니다.

이러한 순서는 다음과 같은 하이퍼링크 밑의 "참고 항목(see-also)" 박스에서 찾을 수 있습니다.

참고 항목:

네트워크 환경 구성

메뉴 바 ‣ 시스템 ‣ 네트워크 환경 구성

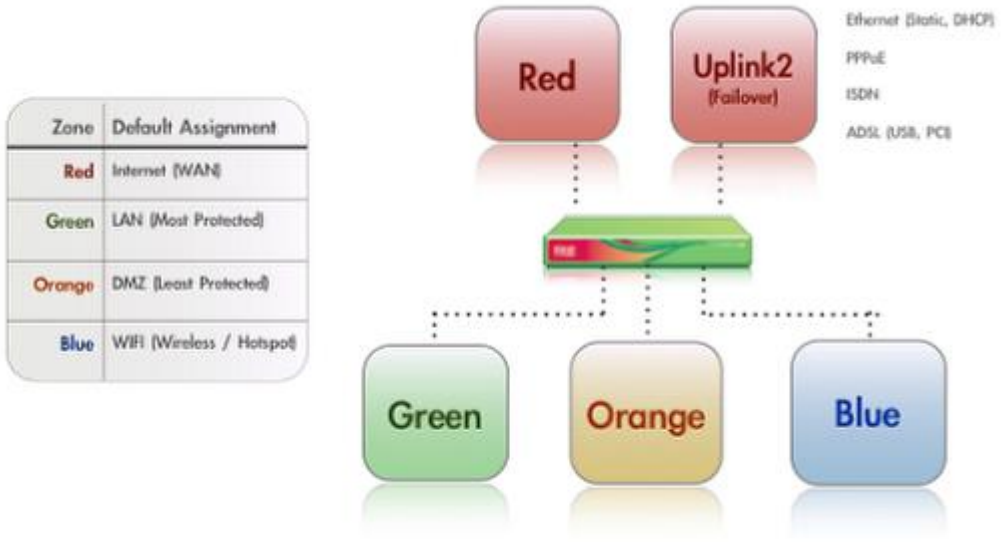
이 상자에서 하이퍼링크를 누르면 문서에 직접 액세스 할 수 있으며, 그 아래의 동작 순서는 해당 기능을 구성 할 페이지인 홈페이지로부터 접근하는 방법을 보여줍니다.

흔히 "참고 항목" 상자는 예를 들어, 온라인 사용방법 또는 문서의 다른 부분과 같은 리소스에 대한 링크를 제공하는데 사용됩니다.

본 설명서 전반에 걸쳐 특별한 사용법이나 의미를 가지고 있는 일부 용어들이 있으며, 용어집에서 찾을 수도 있습니다.

영역들 (zones)

Endian UTM Appliance를 기반으로 하는 가장 중요한 개념 중 하나인 Zone은 네트워크를 보호하기 위해 IPCOP의 아이디어에 뿌리를 두고 있으며, 그것들을 여러 세그먼트들로 - 그 영역들을 실제로 - 그룹화하여 트래픽을 이들 세그먼트들 사이에서 특정 방향으로만 교환할 수 있도록 합니다.



RED는 *신뢰할 수 없는 세그먼트 (Untrusted segment)* 라고 불리는 것입니다. 즉, WAN은 Endian UTM Appliance 외부 또는 폭넓게 말해서 인터넷 외부의 모든 네트워크를 포함하며 들어오는 연결의 소스입니다. 이것은 **관리할 수 없는** 유일한 영역이지만 그곳에 액세스 하거나 그곳으로부터 액세스 권한만 부여받거나 제한할 수 있습니다.

GREEN은 내부 네트워크, 즉 LAN입니다. 이 영역은 가장 보호된 영역이며 워크 스테이션 전용이므로 RED 영역에서 직접 액세스해서는 절대 안됩니다. 또한 기본적으로 관리 인터페이스에 액세스 할 수 있는 유일한 영역이기도 합니다.

ORANGE, DMZ 영역입니다. 이 영역은 서비스를 제공하기 위해 인터넷에 액세스해야 하는 서버 (예: SMTP/POP, SVN 및 HTTP 등)를 호스팅해야 합니다. ORANGE 구역을 RED 구역에서 직접 접근할 수 있는 유일한 구역으로 지정하는 것이 좋습니다. 실제로 공격자가 서버 중 하나에 침입한다면, 그 공격자는 DMZ에 갇히게 되고 GREEN 영역에 도달할 수 없기 때문에, GREEN 영역의 로컬 시스템에서 중요한 정보를 얻을 수 없게 만들 수 있습니다.

블루, 즉 무선 영역 (WiFi)입니다. 즉, 무선 클라이언트가 인터넷에 액세스 할 때 사용해야 하는 영역입니다. 무선 네트워크는 안전하지 않은 경우가 자주 있으므로, 이 아이디어는 기본적으로 모든 무선 연결된 클라이언트를RED 영역을 제외한 다른 영역에 액세스하지 않고 자신의 영역으로 트랩 (특별히 정해 놓은 조건이나 한계값에 도달하게 된 것과 같은 이벤트가 발생했음을 알려주는 것)하는 것이 좋습니다.

Endian UTM Appliance가 올바르게 작동하게 만들기 위해, ORANGE 및 BLUE 영역을 환경 구성할 필요가 없습니다. 실제로 RED 존은 어떤 경우에는 구성되지 않은 상태로 유지될 수 있기 때문에 GREEN 존을 정의하는 것으로 충분합니다.

Endian UTM Appliance에는 일부 영역들 간에 네트워크 트래픽이 흐르지 않도록 사전 정의된 방화벽 규칙을 가지고 있습니다. 4개의 주요 영역 외에도, 2개의 영역이 있지만 고급 설정에서만 사용됩니다: OpenVPN 클라이언트 영역 (간혹 PURPLE 영역이라고도 함)과 HA 영역이 그것들입니다. 이 두개의 특별한 영역은 Endian UTM Appliance에 연결해야 하는 OpenVPN 원격 사용자 및 HA 서비스 용 네트워크로 사용됩니다. 기본적으로, 이들은 192.168.15.0/24 및 192.168.177.0/24 네트워크를 각각사용하므로 이러한 네트워크들의 범위를 주 영역에서 사용하면 안됩니다. 특히 이러한 서비스 중 하나를 사용하려는 경우 특히 그렇습니다. 실제로 이러한 네트워크들은 중복되어 바람직하지 않은 영향을 미칠 수 있습니다. 그러나 이 두 영역의 IP 범위는 OpenVPN 또는 HA 서비스를 설정하는 동안 수정할 수 있습니다.

각 영역에 (네트워크) 인터페이스와 IP 주소를 일치시키려면, 인터페이스는 네트워크 트래픽이 영역을 통과하는 (이더넷 또는 무선) 포트이므로, RED는 RED 영역 및 인터넷에 연결할 수 있는 포트와 인터페이스합니다. 인터페이스의 IP 주소는 <Zone> IP입니다. 예를 들어, GREEN 영역을 위한 초기 (공장출하) 설정은 192.168.0.15/24 네트워크이므로, GREEN 인터페이스는 GREENIP로 참조되는 IP 주소 192.168.0.15를 가질 것입니다.

See also

High availability

for a description of High Availability

VPN

for a description of OpenVPN

참고 항목:

고 가용성

고 가용성에 대한 설명

VPN (가상 사설망)

OpenVPN에 대한 설명

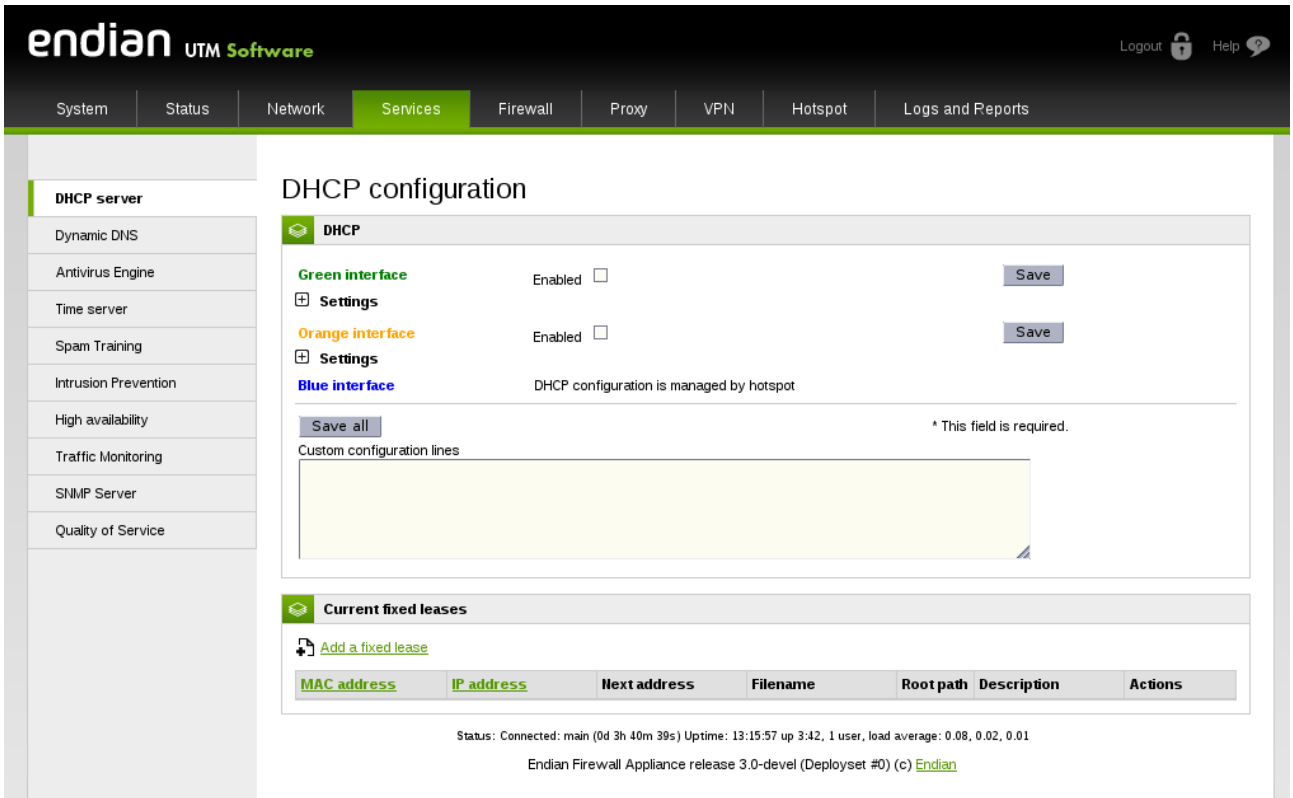
Endian UTM 어플라이언스 관리 인터페이스

버전 2.5에서 변경: *핫스팟 관리 인터페이스. 메뉴 바 › 핫스팟 › 관리 인터페이스 메뉴를 선택하면, 메인 메뉴 바가 사라지고 새로운 메뉴 바로 바뀝니다. 실제로 핫스팟 관리 인터페이스에는 많은 기능, 환경 구성 옵션들 및 메뉴가 있으므로 선택은 전용 메뉴 바(menubar)를 생성하는 것이었습니다.*

버전 3.0에서 변경됨: *인터페이스 스타일이 향상되었으며 글꼴을 더 읽기 쉽게 되었습니다.*

버전 3.0에서 변경됨: *긴 페이지를 스크롤 할 때, 메인 탐색 바(Navigation bar)와 하위 메뉴(Sub menu)가 현재 각각 창의 맨 위와 왼쪽에 고정된 채 남아 있습니다.*

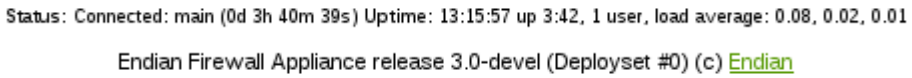
Endian UTM Appliance의 GUI(그래픽 사용자 인터페이스)는 사용하기 쉽도록 설계되었으며, 헤더, 기본 메뉴 바(main menubar), 하위 메뉴(sub-menu), 주 영역 및 바닥글(footer)의 5 가지 주요 부분으로 구성됩니다. 아래에 서비스 모듈의 샘플 스크린 샷을 볼 수 있습니다.



헤더(Header)

페이지의 헤더에는 왼쪽에 엔디안(Endian) 로고가 포함되어 있는 반면, 오른쪽에는 Endian UTM Appliance의 유형을 나타내는 이미지가 있으며, 그 위에 두 개의 링크가 나타납니다. 하나는 온라인 설명서 (도움말), 즉 컨텍스트 의존성 (즉, 각 페이지에서 대응되는 도움말이 표시됨)을 갖는 도움말을 보여주는 링크이고, 하나는 GUI에서 로그 아웃하기 위한 링크가 표시되어 있습니다. 이 부분은 정적이며 변경되지 않습니다.

바닥글(Footer)



바닥글은 페이지 맨 아래에 배치됩니다. 실행중인 Endian UTM Appliance에 대한 몇 가지 정보가 포함된 두 줄의 텍스트로 구성됩니다. 맨 위 줄에는 업링크가 어느 것(만약 정의된 업링크가 한개 보다 많은 경우에)과 연결되어 있는지 여부인 **상태(Status:)**와 uptime 명령의 출력, 즉 마지막 부팅 이후의 시간, 사용자 수 및 로드(부하량) 평균으로 보고되는 연결이 설정된 마지막 시간과 시스템의 가동 시간 이후로 경과된 시간인 **가동시간(Uptime:)**이 표시됩니다. 페이지를 변경하면, 정보가 업데이트됩니다. 맨 마지막 줄은 Endian 웹 사이트로의 링크와 배포판 및 저작권을 포함한 어플라이언스의 버전을 표시합니다.

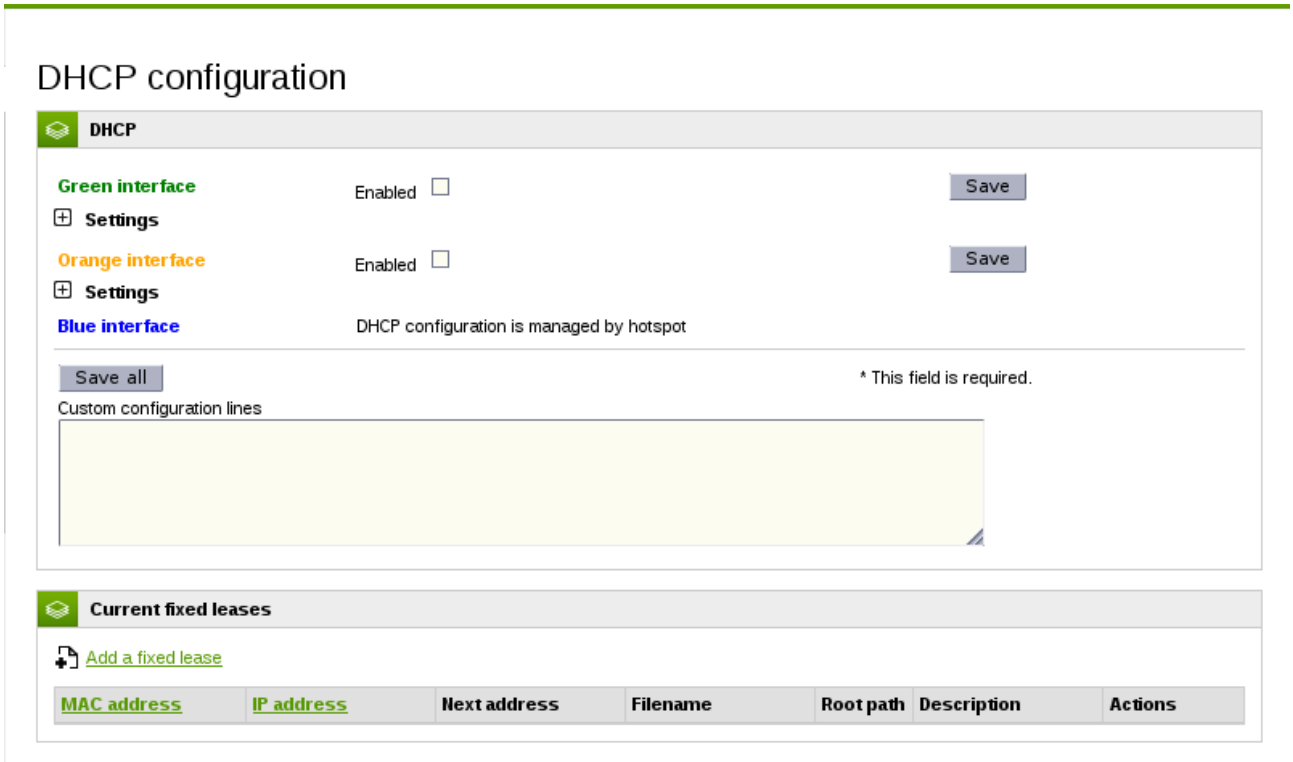
메인 탐색 바

헤더 바로 아래에 위치한 기본 탐색 바는 검정색 배경의 메뉴 막대와 Endian UTM Appliance의 사용 가능한 모든 섹션을 표시하는 녹색 밑줄입니다. 모듈 (예: *서비스*) 중 하나를 클릭하면, 그 배경이 녹색으로 바뀌어 현재 열려 있는 모듈을 강조합니다. 메뉴 항목을 클릭하면, 페이지 왼쪽의 하위 메뉴와 주 영역 상단의 제목이 상황에 따라 다르기 때문에 변경됩니다. 기본적으로, GUI는 *시스템* 메뉴에서 열립니다.

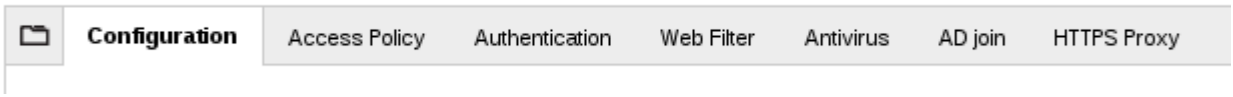
하위 메뉴

하위 메뉴는 GUI의 왼쪽에 나타나며, 메뉴 바에서 선택한 모듈에 따라 변경됩니다. 기본 영역의 컨텐츠를 변경하고 해당 Endian UTM Appliance 모듈에 포함된 모든 기능에 접근하기 위해 클릭할 수 있는 항목들의 수직 목록으로 나타납니다.

주요 영역



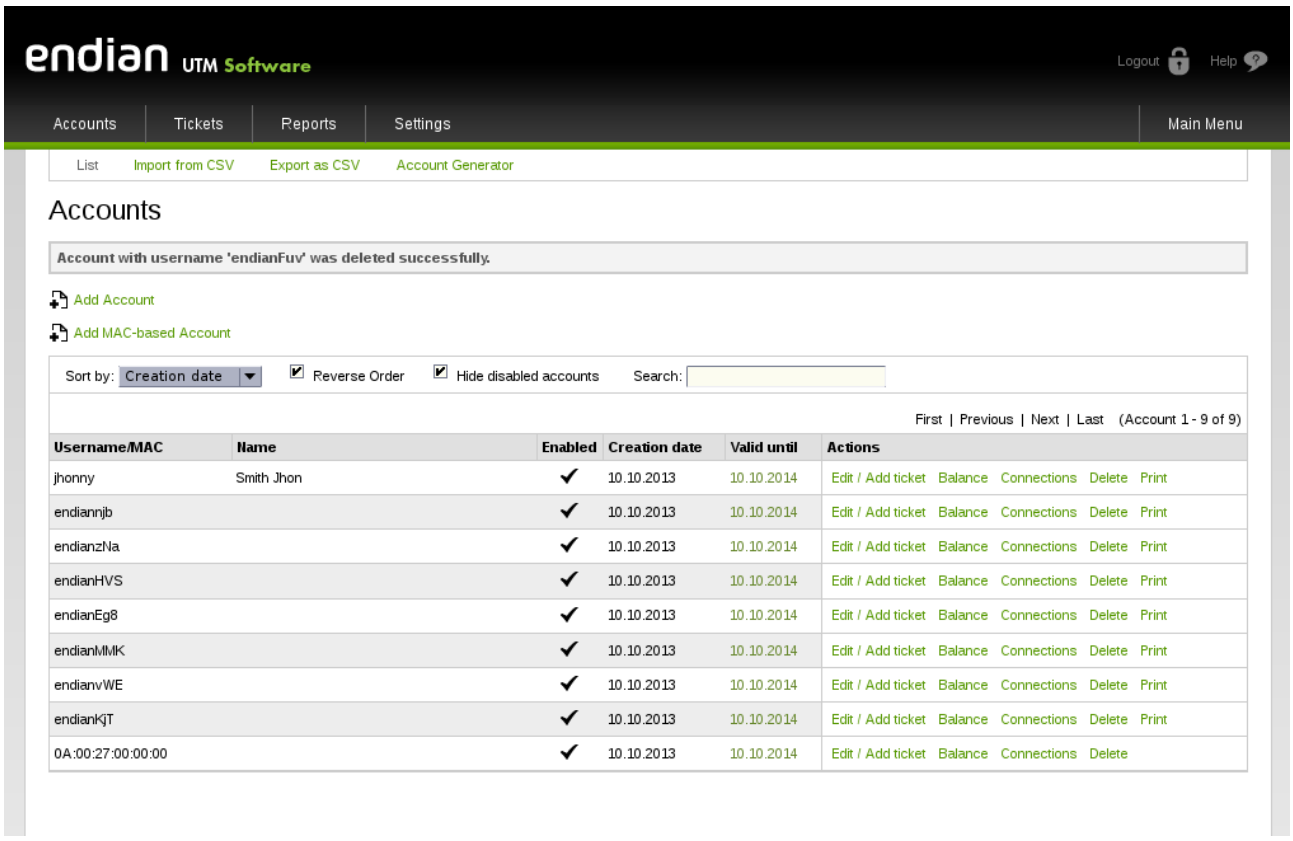
주 영역에는 메뉴/하위 메뉴 조합의 현재 선택에 포함된 모든 정보와 설정들이 포함됩니다. 일부 페이지 (예: 대시 보드 또는 *서비스* 및 *로그* 모듈의 일부)는 단지 유익한 정보로, Endian UTM Appliance의 현재 상태를 그래픽 또는 텍스트로 표시합니다. 후자의 경우, Linux 명령어들의 출력을 화면에 표시합니다. 그러나 대부분의 페이지에는 현재 구성된 설정에 대한 다양한 정보를 포함하는 테이블이 표시되어 기존 항목 및 설정을 수정 또는 삭제하고 새 항목을 추가할 수 있게 해줍니다. 특히 예를 들어, HTTP 프록시 또는 방화벽과 같은 정교한 서비스들은 단일 페이지로는 그것들 모두를 나타내는데 충분하지 않은 많은 구성 옵션을 포함하므로 사용 가능한 설정이 그룹화되고 탭으로 구성됩니다.



탭(tab) 내에서, 흔히 구성 옵션들은 전체 환경 구성의 공통 부분을 참조하는 설정들을 함께 모아서 하나 이상의 상자에 묶어서 보여줍니다.

핫스팟 관리 인터페이스

Endian UTM Appliance GUI의 레이아웃에 대한 유일한 예외는 핫스팟 관리 인터페이스입니다. 아래 스크린 샷에 그려져 있으며, 바닥글은 없고, 메인 메뉴 바 아래에 서브 메뉴가 있으며, 메뉴 바의 맨 오른쪽에는 다시 주 메뉴로 돌아갈 수 있는 메인 메뉴 링크가 있습니다.



핫스팟 관리 인터페이스 아래의 항목을 참조할 때, 초기 메뉴 바는 일반적으로 생략된다는 것에

주의하십시오.

아이콘들

Endian UTM Appliance가 제공하는 페이지들 곳곳에 많은 아이콘이 사용되어 신속하게 수행할 수 있는 작업을 나타내거나 표시된 설정에 약간의 의미를 전달합니다.

스위치(Switches) 

스위치는 서비스를 완전히 활성화 또는 비활성화하는 데 사용되며 주 영역의 맨 위에 있습니다. 회색 스위치는 기본 영역에 설정 또는 환경 구성 옵션이 표시되지 않고 서비스가 비활성화되어 사용 불능 상태임을 나타냅니다. 이를 클릭하면, 적절한 기능을 수행하는데 필요한 서비스와 데몬이 시작되고 초기화됩니다. 몇 초 후에 스위치의 색상이 녹색으로 바뀌며 사용 가능한 모든 환경 구성 옵션들이 나타납니다. 서비스를 사용하지 않으려면, 스위치를 다시 클릭하십시오. 그러면 모든 데몬이 중지되고 스위치가 회색으로 바뀌며 설정이 사라집니다.

정책(Policies)

이러한 아이콘들은 예를 들어, 방화벽 규칙 또는 프록시 사양과 같은 일부 형태의 접근 정책 또는 트래픽 제어가 필요한 서비스들에서 발견됩니다. 패킷이 규칙과 일치할 때마다, 해당 규칙에 지정된 정책이 적용되어 패킷의 통과 여부 및 패킷이 통과하는 방법을 결정합니다.

➔ 제한없이 액세스를 허용합니다.

패킷이 긍정적으로 IPS를 통과한 후에 만 액세스를 허용합니다. 이 정책은 방화벽 규칙에서만 사용할 수 있습니다.

패킷을 차단하고 그것을 버립니다.

패킷을 차단하지만 통지는 소스(패킷 발송지)로 전송됩니다.

부분적으로 규칙을 수락합니다. 이는 정책 목록 제목에서만 발견되며, 예를 들어, Menubar ‣ 프록시 ‣ HTTP ‣ Contentfilter와 같이 목록의 정책 중 일부는 수락되고 일부는 거부되는 것을 한눈에 알 수 있습니다.

다른 아이콘들

추가 아이콘들은 Endian UTM Appliance에서 찾을 수있습니다.

패널을 확장하여 내용을 표시합니다.

⊟ 패널을 닫아 내용을 숨 깁니다.

탐색 바(Navigation bar) 

항목의 긴 목록이 나타나는 대부분의 위치에서, 몇개의 셀로 구성된 항목 목록을 쉽게 탐색할 수 있는 탐색 바(Navigation bar)가 나타납니다. *첫 번째(First)* 및 왼쪽의 *이전(Previous)*, 오른쪽의 *다음(Next)* 및 *마지막(Last)*과 같은 다양한 양의 셀들은 페이지 번호를 포함합니다. 다양한 셀을 클릭하면, 숫자로 표시된 페이지, 첫 번째 또는 마지막 페이지 또는 이전 및 다음 페이지로 연결됩니다.

일반적인 조치(Actions) 및 작업(Tasks)

GUI 내에서 수행할 수 있는 두 가지 유형의 조치들이 있습니다. 환경 구성 설정 목록 (즉, 하나의 방화벽 규칙)에있는 단일 항목에 대한 조치와 목록, 상자 또는 페이지에 있는 모든 설정을 저장, 보관 및 적용할 수 있는 '전역' 조치입니다.

조치(Action) 및 아이콘

이 아이콘들은 페이지에 나타나는 다양한 테이블의 오른쪽에 있는 조치(Actions) 열에 배치되며, 일반적으로 정의된 항목 목록 (예: 방화벽 규칙 또는 OpenVPN 사용자)을 표시합니다. 조치 아이콘은 해당 목록의 요소에서 하나의 작업을 실행할 수 있게 해줍니다. 일부 조치는 일부 목록 유형에서만 사용할 수 있습니다.

☑ 및 ☐ 는 각각 활성화 및 비활성화 된 항목의 상태를 나타냅니다. 아이콘을 클릭하여 상태를 변경할 수 있습니다. 그런 다음, 콜아웃(callout)은 필요할 경우 데몬이 환경 구성을 다시 로드하고 변경 사항을 활성화할 수 있도록 서비스를 다시 시작하도록 사용자에게 알려줄 수 있습니다.

⬆ 및 ⬇ 순서가 중요한 목록 (예: 방화벽 규칙)에서만 사용할 수 있으며, 해당 항목을 ⬆ (위) 또는 ⬇ (아래)로 이동하여 순서를 수정할 수 있게 해줍니다.

✎ 편집을 사용하면 현재 항목을 수정할 수 있습니다. 이 아이콘을 클릭하면 해당 항목에 대한 적절한 편집기가 열립니다.

🗑 삭제는 선택한 항목이 목록 및 환경 구성에서 제거되도록 합니다. 항목이 완전히 삭제되기 전에 확인을 요청하는 메시지가 나타납니다.

🖴 항목 (일반적으로 아카이브)을 다운로드 할 수 있게 해줍니다.

✒ 테스트는 제한된 위치 (예: Menubar ‣ 서비스 ‣ 스팸 교육)에서 원격 서버로의 항목 연결을 테스트하는데 사용됩니다.

⚠(passlog) 및 (blocklog)는 IPS (Menubar ▸ Services ▸ Intrusion Prevention)에 나타나며, 통과가 허용되거나 규칙과 일치한 후에 차단되는 패킷을 기록하도록 허용합니다.

교환기 (Switchboard) 및 4i Connect Client에는 다음과 같은 아이콘이 나타납니다.

항목에 대한 로그를 열기 위해 *Menubar ▸ Switchboard*를 클릭합니다.

*(Menubar ▸ Switchboard)*를 사용하여 원격 장치 또는 게이트웨이 (4i 연결 클라이언트 전용)에 연결하거나 연결을 끊습니다.

*(Menubar ▸ Switchboard ▸ Gateway)*을 사용하면 게이트웨이의 환경 구성을 암호화된 파일로 다운로드 할 수 있습니다

'전역' 조치 ('Global' Actions)

하나 이상의 옵션들을 사용자 정의할 수 있는 모든 페이지의 맨 아래에 디스크에 새 구성을 보관 또는 저장하거나 지금까지 완료된 사용자 정의를 취소하는 옵션이 있습니다. 후자의 경우, 구성이 실제로 변경되지 않았으므로 더 이상의 조치가 필요하지 않습니다. 그러나 전자의 경우에는 방금 수정한 서비스를 재시작해야 하며, 실행중인 환경 구성에서 새로운 설정을 다시로드하고 사용하려면 몇개의 다른 관련 서비스들 또는 종속 서비스들도 다시 시작해야 할 수 있습니다. 편의상, 이 작업이 필요할 때, 설정을 저장한 후에 설명문(콜아웃)이 표시되고, 적용 버튼으로 클릭하면 서비스가 다시 시작됩니다.

다중 선택(Multiselect) 상자 (예: Menubar ▸ 핫스팟 설정)를 사용할 때마다, 모두 추가 및 모두 제거를 바로 가기로 클릭하여 사용 가능한 항목 또는 선택된 항목과 활성 항목의 목록에서 사용 가능한 항목을 모두 추가하거나 제거할 수 있습니다.

하나의 구성 옵션 내의 다중 항목들

여러 위치에서 예를 들어, 방화벽 규칙의 소스 또는 대상에서 처럼, 단일 구성 항목에 대해 여러 값을 입력할 수 있습니다. 이 경우, 텍스트 영역 또는 드롭 다운 메뉴 중 어느 하나가 표시됩니다. 전자의 경우, 예컨대 MAC 어드레스, (CIDR 표기법에서의) 네트워크 범위, 또는 OpenVPN 사용자와 같이 라인 당 하나의 값을 입력하는 것이 가능합니다. 후자의 경우에는, 키보드에서 Ctrl (Control) 키를 누른 상태에서 선택하려는 값을 클릭하여 선택할 수 있는 사전 정의된 많은 값들 사이에서 선택 사항이 제한됩니다.

IPv4 및 CIDR 표기법.

IPv4 주소는 길이가 4 비트, 8 비트 길이의 옥텟으로 나뉘어 32 비트인 네트워크 주소입니다. 10 진수로, 각 옥텟은 0에서 255 사이의 어떤 값도 가질 수 있습니다 (2^8 = 256).

네트워크 범위를 지정할 때, 해당 네트워크에서 사용할 수 있는 호스트 수를 정의하는 서브넷 마스크(subnet mask) 또는 줄여서 넷 마스크(netmask)와 함께 네트워크의 첫 번째 호스트의 IP 주소가 제공됩니다. 서브넷(subnet)은 네트워크 프리픽스의 길이, 즉 네트워크 내의 모든 호스트들에 의해 공유되는 주소 부분으로 정의됩니다.

네트워크/넷마스크 쌍을 표시하는데는 두 가지 가능성이 있습니다.

- 명시적으로, 즉, 둘 다 쿼드-점 표기법으로 주어진다. 예를 들어:

  이것은 192.168.0.0 주소에서 시작하는 네트워크로, 즉, 192.168.0.0부터 192.168.0.255 사이의 네트워크 범위에서 사용할 수 있는 256개의 호스트로 시작하는 네트워크입니다. netmask의 처음 3개의 옥텟(octet)은 255이고, 사용 가능한 호스트가 없다는 것을 나타내는 반면에 (또는 주소의 이 부분이 네트워크 접두사입니다), 네 번째는 0이며, 모든 호스트 (256 - 0 = 0)를 사용할 수 있음을 의미합니다.

- CIDR 표기법으로 사용 가능한 호스트 대신 사용 가능한 비트가 제공되는 네트워크 범위를 표시하는 좀 더 간결한 방법입니다. 위와 동일한 네트워크 범위는 다음과 같이 표현됩니다.

  이 표기법은 IP 주소의 공유 부분의 비트 길이를 표시합니다. 24는 첫 번째 3개의 옥텟(각각 8 비트로 구성됨)이 공유되는 반면, 네 번째 옥텟은 비어 있으며, 32 - 24 = 8 비트, 즉 256개의 호스트와 동일한 사용 가능한 호스트 수를 제공한다는 것을 의미합니다.

  동일한 추론 라인이 IPv6 주소에 적용될 수 있습니다. IPv6 주소의 유일한 차이점이라면 길이가 128 비트라는 것입니다.

Endian UTM Appliance에 접근하기

Endian UTM Appliance에 접근하는 방법은 몇 가지가 있습니다. 가장 직관적이고 직접적인 방법은 웹 기반 GUI에서 접근하는 것입니다. SSH 및 직렬 콘솔을 통한 콘솔 기반 액세스도 있지만 고급 사용자에게만 권장됩니다.

Endian UTM Appliance GUI

> **힌트**: Endian UTM Appliance의 기본 IP 주소는 192.168.0.15입니다.

Endian UTM Appliance GUI에 대한 접근은 매우 간단합니다. 브라우저를 시작하고 Endian UTM Appliance가 처음 사용되는지 여부에 관계없이 GREENIP 주소를 입력하십시오.

브라우저는 포트 10443에 보안 HTTPS 연결로 리디렉션될 것입니다. Endian UTM Appliance는 자체 서명된 HTTPS 인증서를 사용하기 때문에, 브라우저는 첫 번째 연결 중에 인증서를 수락하도록 요청했을 수 있습니다. 그러면 시스템에서 사용자 이름과 암호를 묻습니다. 사용자 이름으로 "admin"을 지정하고, 리셀러로부터 받은 비밀번호를 제공하거나 Endian UTM Appliance가 이미 사용자 정의된 경우에는 설치 중에 제공된 비밀번호를 삽입하십시오.

암호를 입력하면 Endian UTM Appliance GUI의 대시보드(Dashboard)가 표시되며, 이 인터페이스에서 사용할 수 있는 정보를 즉시 탐색하거나 장비를 더 찾아보고 구성할 수 있습니다. 본 설명서의 나머지 부분은 주 탐색 바(main navigation bar)의 레이아웃을 따릅니다. 주 메뉴 막대의 각 항목은 Endian UTM Appliance의 다른 섹션을 나타내며, 하위 메뉴 항목과 하위(sub-) 섹션 및 하위의 하위(sub-sub-) 섹션 제목 표식이 개별적으로 있는 탭으로 된 별도의 장(챕터)로 제공됩니다.

콘솔 기반 액세스

Endian UTM Appliance에 대한 콘솔 기반 액세스는 Linux 명령 줄에 익숙한 사용자에게만 권장됩니다.

CLI(명령행 인터페이스)에 연결할 수 있는 두 가지 방법이 있습니다: SSH 액세스 사용 또는 직렬 콘솔을 이용하는 방법입니다. SSH 액세스는 기본적으로 비활성화되어 있지만, Menubar ‣ System ‣ SSH 액세스 아래에서 활성화 할 수 있는 반면에, 직렬 콘솔 액세스는 다음과 같은 매개 변수를 사용하는 모든 기기에서 기본적으로 가 활성화되어 있습니다.

- 포트: ttyS0
- 비트, 패리티 비트, 정지 비트: 8, N, 1
- 속도: 최신 기기에서 115200 baud.

> 힌트: 아직 3.0 릴리스로 업그레이드하지 않은 구형 기기의 보드율(baud rate)은 38400입니다.

직렬 콘솔을 사용하는 연결에는 다음이 필요합니다.

- Unix/Linux 박스용 minicom이나 MS Windows 용 putty와 같은 적당한 터미널 프로그램.
- 직렬 인터페이스가 있는 워크스테이션
- 워크스테이션을 기기에 연결하는 널 모뎀 케이블

또는

- 터미널 프로그램.
- 네트워크 직렬-이더넷 어댑터
- 어플라이언스를 어댑터에 연결하는 직렬 이더넷 케이블.

> 참고: 네트워크가 올바르게 구성되지 않은 경우, 직렬 콘솔이 Endian UTM Appliance에 액세스하는 유일한 방법 일 수 있습니다.

시스템 메뉴

시스템 메뉴는 Endian UTM Appliance 및 그 기기의 상태에 대한 몇 가지 정보를 제공하며, 네트워크 설정 및 일부 액세스 방식 (예: SSH를 통하거나 또는 Endian 지원을 위해)을 정의할 수 있게 해줍니다.

왼쪽의 하위 메뉴에는 기본적인 관리 작업을 수행하고 Endian UTM Appliance의 실행중인 활동을 모니터링 할 수 있는 다음과 같은 항목이 포함되어 있습니다.

- 대시 보드 - 시스템 및 연결 상태 개요를 보여줍니다.
- 네트워크 구성 - 네트워크 및 네트워크 인터페이스 구성.
- 이벤트 알림 - 전자 메일 또는 SMS를 통해 알림을 설정합니다.
- 업데이트 - 시스템 업데이트의 관리.
- 지원 - 지원 요청 양식..
- 엔디안 네트워크(Endian Network) - 엔디안 네트워크 등록 정보.
- 배전반(Switchboard)에 연결 - 자동으로 Endian 장치를 배전반에 연결합니다.
- 암호 - 시스템 암호를 설정합니다.
- 웹 콘솔 - 브라우저의 콘솔 쉘.
- SSH 액세스 - Endian UTM Appliance에 대한 SSH 액세스를 활성화 및 구성합니다.
- GUI 설정 - 웹 인터페이스 언어 설정.
- 백업 - Endian UTM Appliance 설정을 백업 또는 복원하고, 공장 기본값으로 재설정합니다.
- 종료 - Endian UTM Appliance를 종료하거나 재부팅합니다.
- 사용권 계약 - 사용자 라이센스 계약서 사본.

버전 5.0.5의 새로운 기능*: 배전반(switchboard) 절차에 연결하십시오.*
이 섹션의 나머지 부분에서는 시스템 메뉴 항목을 구성하는 다양한 부분들에 대해 설명합니다.

대시 보드

대시 보드는 모든 로그인시에 표시되는 기본 방문 페이지입니다. 실행중인 시스템과 그 상태 및 운영 상태에 대한 전체 개요를 제공하는 두 개의 열(column)로 구성된 여러 상자들 ("플러그인")을 포함합니다. 각 상자의 상단에는 상자의 이름이 표시되고, 각 플러그인의  (openplugin) 아이콘을 클릭하면 제목 표시줄 만 표시될 것입니다. 화면에 표시되는 정보는 정기적으로 업데이트됩니다.
플러그인을 간단히 클릭한 다음 원하는 위치로 드래그 앤 드롭하여 이동할 수 있습니다. 하나의 구성 옵션을 사용할 수 있습니다.

설정 표시

이 링크를 클릭하면, 작은 테이블이 열리고 사용 가능한 플러그인, 그것들에 대한 설명 및 새로고침 간격이 표시됩니다. 각 플러그인은 활성화 또는 비활성화 할 수 있으며, 드롭 다운 메뉴에서 업데이트 간격을 선택하여 업데이트 간격을 사용자 정의할 수 있습니다.

사용 가능한 플러그인과 그 플러그인이 표시하는 정보가 다음에 설명됩니다.

시스템 정보 플러그인

설치된 시스템에 대한 몇 가지 정보를 보여줍니다. 일반적으로 제목에 Endian UTM Appliance의 호스트 이름과 도메인 이름을 표시합니다.

어플라이언스(Appliance): 어플라이언스 유형입니다.
버전(Version): 펌웨어의 버전입니다.
커널(Kernel): 현재 실행중인 커널.
가동 시간(Uptime): 마지막 재부팅 이후 시간.
업데이트 상태(Update Status): Endian UTM Appliance 상태에 따른 메시지:

- **최신 정보**. 사용할 수 있는 업데이트가 없습니다.
- **업데이트가 필요함.** 새 패키지를 설치할 수 있습니다: 메시지를 클릭하면 새 패키지 목록을 검토할 수 있는 업데이트 페이지로 연결됩니다.
- **등록하십시오.** 시스템이 Endian Network에 아직 등록되지 않았습니다: 메시지를 클릭하면 Endian UTM Appliance의 Endian Network 페이지가 열리고, 등록을 완료하기 위해 양식을 컴파일합니다.

유지 관리(Maintenance): 유지 관리 지원의 유효 기간 중 남은 날짜 또는 등록되지 않은 문자열.
지원 액세스(Support access): 지원 팀이 Endian UTM Appliance에 액세스할 수 있는지 여부. 전자의 경우에는 액세스 권한이 부여될 때까지 날짜가 표시됩니다.

하드웨어 정보 플러그인

여기서는 Endian UTM Appliance의 주요 하드웨어 정보와 리소스 가용성을 보여줍니다. 모든 정보는 절대 값 (해당 라인의 끝에 작은 막대와 숫자를 이용해서 그래픽으로 표시)과 사용률로 제공됩니다. 유일한 예외는 그래픽 및 숫자로 사용률만 표시하는 CPU 부하입니다.

CPU x: 하나 이상의 CPU가 있는 기기들의 CPU 부하를 표시하며, x는 CPU 숫자를 나타냅니다.
메모리(Memory): 사용된 RAM 메모리의 양.

스왑(Swap): 얼마나 많은 스왑 디스크 공간이 사용됩니까? 여기서 높은 비율은 일반적으로 올바르게 작동하지 않는 무언가가 있음을 의미합니다.
주 디스크(Main disk): 루트 파티션의 사용.
데이터 디스크(Data disk): /var 파티션의 사용.
구성 디스크(Configuration disk): 모든 Endian UTM Appliance 서비스 및 설정을 포함하고 있는 파티션이 차지하는 공간.
로그 디스크(Log disk): 로그를 포함하고 있는 파티션에 사용된 공간의 양.

디스크 공간 가용성을 나타내는 후자의 값은 데이터, 시스템 및 로그 파티션이 다른 장소에 위치해 있을 수 있기 때문에 어플라이언스(기기)에 따라 다를 수 있습니다.

> **경고**: 하드 디스크의 파티션 (예: 주 디스크, 데이터 디스크 및 특히 /var/log)에는 서비스 중단 및 데이터 손실을 유발할 수 있으므로 95% 이상을 채우지 않아야 합니다.

서비스 정보 플러그인

이 플러그인은 Endian UTM Appliance에 설치된 가장 중요한 서비스들 중의 일부에 의해 기록된 이벤트 및 그것들의 실제 상태에 대한 정보를 제공합니다. 서비스 이름을 클릭하면 서비스에 의해 수행된 작업들이 표시되거나 숨겨집니다.

실행중인 각 서비스에 대해 지난 1시간 및 마지막 날 동안에 수행된 작업들에 대한 요약이 표시되며, 각각의 라이브 로그(Live Logs)를 새 창에서 열 가능성이 있습니다.

따라서, 요약에서 일부 수치가 정상적인 활동 (예: IDS가 일부 공격을 감지함)에 비해 이상하거나 일반적이지 않은 것으로 보이면, 기록되어 있던 일부 유용한 메시지를 검색하도록 로그를 제어할 수 있습니다.

지원되는 서비스들은 다음과 같습니다:

침입 탐지(Intrusion Detection): 스노트(snort, 오픈소스 네트워크 침입방지시스템)에 의해 기록된 공격의 횟수.

SMTP 프록시(Proxy): Endian UTM Appliance를 통해 전송된 처리된 전자 메일에 대한 통계입니다.

HTTP 프록시(Proxy): HTTP 프록시를 사용하여 액세스 한 웹 페이지에 대한 통계입니다.

POP3 프록시(Proxy): 받은 전자 메일, 발견된 바이러스, 그리고 수신된 스팸 전자 메일.

> **힌트:** 비활성 서비스는 **OFF** 메시지로 표시됩니다.

서명 정보 플러그인

이 플러그인은 서비스에 대한 서명이 마지막으로 다운로드된 시간 스탬프 (날짜와 시간)를 보여줍니다. 서비스가 아직 활성화되지 않은 경우, 목록에 보이지 않습니다.

여기에 표시될 수 있는 서비스는 Clamav, IPS, Panda 및 Urlfilter입니다.

> **참고:** 하나의 업링크에 대해 "*업링크가 온라인 인 경우 시그너처 업데이트 사용 안함*" 옵션이 활성화되어 있으면 (*네트워크 ‣ 인터페이스 ‣ 업링크 편집기* 참조), 서명이 다운로드되지 않고 "**시그니처 다운로드가 업링크 구성에 의해 비활성화 됩니다**"라는 메시지가 표시됩니다.

업링크 정보 플러그인

이 플러그인은 업링크의 연결 상태를 자세히 설명하는 표를 보여줍니다. 정의된 각 업링크에 대해 이름, IP 주소, 상태, 가동 시간, 활성화 ☑ 또는 비활성화 ☐ 여부, 관리 여부 ☑ 또는 수동 여부 ☐ 가 표시됩니다. 순환 화살표 ↻ 를 클릭하면 해당 업링크를 즉시 다시 연결할 수 있습니다. 특히 관심사항은 각각의 개별 업링크의 상태 필드이며, 다음과 같을 수 있습니다.

중지됨: 연결되지 않았습니다.

비활성: 연결되지 않았습니다.

연결 중: 아직 연결되어 있지 않지만 연결이 진행 중입니다.

연결됨 또는 **UP**: 연결이 설정되고 완전히 작동합니다.

연결 끊는 중: 업링크가 연결을 종료하고 있습니다. Endian UTM Appliance는 게이트웨이에 핑 (ping)을 계속하고 언제 사용 가능한지 알려줍니다.

실패: 업링크에 연결하는 동안 오류가 발생했습니다.

실패, 재연결: 업링크에 연결하는 동안 오류가 발생했지만, Endian UTM Appliance가 다시 연결을 시도하는 중입니다.

죽은 링크(Dead link): 업링크가 연결되었지만 작동하지 않습니다.

이 마지막 경우는 업링크 구성 (*Menubar ‣ Network ‣ Interfaces*)에서 "*이러한 호스트들에 연결할 수 있는지 확인*" 옵션이 하나 이상의 원격 IP 주소 또는 호스트로 구성되어 있지만 연결할 수 없음을 의미합니다.

관리 및 수동 업링크.

각 업링크는 *관리* 모드 (기본값) 또는 *수동* 모드에서 작동할 수 있습니다. 관리 모드에서 Endian UTM Appliance는 필요한 경우 업링크를 자동으로 모니터링하고 다시 시작합니다. 관리 모드가 비활성화 된 경우에는 업 링크를 수동으로 활성화 또는 비활성화해야 합니다. 즉, 연결이 끊어지면 자동 재 연결 시도가 없지만 `다시 연결(Reconnect)` 을 클릭하는 것은 운용불가 업링크를 다시 시작하는 것을 필요로 합니다. 업링크의 관리 모드는 *Menubar ▸ Network ▸ Interfaces*에서 선택할 수 있습니다.

업링크는 접속 손실의 경우 빠른 재 연결을 허용하도록 항상 관리되어야 하지만 수동 모드는 실제로 연결을 설정하기 전에 연결 문제를 해결하거나 연결을 테스트하는데 유용한 것으로 입증되었습니다.

네트워크 구성(Network configuration)

이 8 단계 마법사를 사용하면 영역을 제공하는 네트워크 및 네트워크 인터페이스의 구성이 빠르고 쉽습니다. `<<<` 및 `>>>` 버튼을 사용하여 단계를 앞뒤로 자유롭게 탐색할 수 있으며 지금까지 수행된 작업을 언제든지 취소를 결정할 수 있습니다. 마지막 단계에서만 새 설정을 확인해야 합니다. 이 경우 모든 변경 사항이 적용됩니다. 새 설정을 적용하는 동안 웹 인터페이스가 잠시 동안 응답하지 않을 수 있다는 것에 유의하십시오.

스텔스 업링크 모드.

스텔스 업링크(Stealth Uplink) 모드는 기존 라우팅 또는 방화벽 규칙을 수정할 필요없이 Endian UTM Appliance를 기존 네트워크 인프라에 원활하게 통합할 수 있는 새로운 가능성을 나타냅니다.

스텔스 업링크 모드에서는 GREEN, ORANGE 또는 BLUE일 수 있는 동일한 영역(zone)을 담당하는 NIC가 최소 2개 이상 장착된 Endian UTM Appliance가 필요합니다. 이러한 인터페이스 중 하나는 영역(zone)에서 게이트웨이로 향하는 모든 트래픽을 라우팅하며 실제로는 Endian UTM Appliance의 '업 링크'를 나타냅니다.

'업링크'로 지정된 명시적 인터페이스의 존재로 인해 스텔스 업링크에 의해 제공되던 영역 외부로 흐르는 트래픽의 방향을 식별하고, 발신 방화벽을 사용하여 필터링 할 수 있게 합니다. 이것은 외부로 나가는 트래픽을 필터링 할 가능성이 없는 "*업링크 모드 없음*" (이전에는 *게이트웨이 모드*로 알려짐)과의 주요 차이점이기 때문에 응용 프로그램 제어를 적용할 수 없었습니다.

Stealth Uplink 작동 모드에서는 Endian UTM Appliance의 방화벽 설정에서 특정 설정이 필요합니다.

- 시스템 액세스 규칙이 정상적으로 처리되었습니다.
- 포트 전달 및 대상 NAT 규칙도 정상적으로 구성할 수 있습니다. 그러나 내부 네트워크와 동일한 영역에서 외부로 보내는 인터페이스이므로 규칙은 영역의 양쪽에서 적용됩니다.
- 원본 NAT는이 설정에서 나가는 연결에 적용되지 않습니다. 그렇지 않으면 동작이 더 이상 투명하지 않게 됩니다.
- 외부로 나가는 방화벽(outgoing firewall)은 스텔스 업링크에 의해 제공되는 영역에서 업링크로 지정된 NIC를 통해 전송되는 모든 트래픽에 사용되며, 응용프로그램 제어 기능을 활용할 수 있게 해줍니다.
- 영역간(interzone) 방화벽이 정의된 경우라면, 다른 영역들 간의 모든 나머지 트래픽에 적용됩니다. 스텔스 업링크 브리지는 세 개 이상의 인터페이스로 구성되며, 따라서 두 개 이상의 영역이 해당 영역에 서비스를 제공하며, 이들 영역과 다른 영역 간의 트래픽은 영역간 방화벽에 의해 필터링 될 수 있습니다.

이 업링크 모드가 사용 가능하기 때문에, 다양한 업링크 및 각 구성 요소에서 사용할 수 있는 구성 옵션들 간의 차이점을 명확히하기 위해 특히 마법사의 첫 번째 페이지에서 네트워크 구성 마법사의 GUI도 변경되었습니다.

마법사에서 나뉘어진 8단계는 다음과 같습니다:

1/8 - 네트워크 모드 및 업링크 유형 선택

네트워크 구성 마법사의 첫 번째 페이지에는 업링크의 작동 모드를 선택하는 *네트워크 모드*와 업 링크를 선택하는 *업링크 유형*이라는 두 개의 상자가 있습니다.

네트워크 모드

첫 번째 상자는 상호 배타적인 세 가지 선택 중에서 Endian UTM Appliance에서 사용하는 업링크의 작동 모드를 선택할 수 있습니다. 선택할 때 또는 마우스를 옵션들 중 하나 위에 가져가보면 간단한 설명이 나타납니다.

- 라우팅 됨(Routed). 이 선택 사항은 게이트웨이 모드를 제외하고 Endian UTM Appliance에서 사

용할 수 있는 전형적인 업링크에 해당합니다.

- 브릿지 됨(Bridged). 기존의 인프라에서 Endian UTM Appliance를 완벽하게 통합하도록 설정할 수 있는 새로운 스텔스 업링크(Stealth Uplink) 모드입니다.
- 업링크 없음(No uplink). 이 선택 사항은 이전에 게이트웨이 모드로 알려진 모드에 해당합니다.

> **참고**: "*업링크 없음*" 모드에서는 업 링크를 통해 Endian UTM Appliance의 트래픽을 필터링하는 외부로 나가는 방화벽에 정의된 규칙이 고려되지 않습니다.

다른 경우에서는 모드가 자동으로 RED 인터페이스를 결정하기 때문에 다음 상자는 Routed 옵션을 선택한 경우에만 나타납니다.

업링크 유형 (RED 영역)

이 상자는 *네트워크 모드*가 **라우팅 된** 경우에만 표시됩니다. 설치시 Endian UTM Appliance는 웹 구성 인터페이스에 대한 로컬 연결을 허용하지만 업링크가 구성되지 않은 기본값으로 GREEN(녹색 영역) IP인 **192.168.0.15**를 수신합니다. 이 페이지에서 구성할 수 있습니다. 사용할 수있는 유형은 다음과 같습니다.

동적 이더넷 (Ethernet DHCP)

RED 인터페이스는 로컬 서버, 라우터 또는 모뎀에서 (동적) DHCP를 통해 네트워크 구성을 수신합니다. 즉, RED 인터페이스는 단순한 라우터에 연결되지만 고정 주소를 가질 필요는 없습니다.

정적 이더넷 (Ethernet Static)

RED 인터페이스는 LAN에 있으며 고정 IP 주소와 넷마스크를 가지고 있습니다. 예를 들어, RED 인터페이스를 단순한 라우터에 연결할 때, Endian UTM Appliance가 항상 동일한 IP 주소에서 도달할 수 있는 편의성을 제공합니다.

모바일 광대역 (Mobile Broadband, 3G/4G)

RED 인터페이스는 연결을 설정하기 위해 모바일 3G 또는 4G 모뎀을 사용합니다. 모뎀은 장비와 함께 내장형 모뎀으로 제공되거나 USB 포트에 연결될 수 있습니다.

> **참고 자료:** 5.0 릴리스에서 지원되는 3G/4G/HDSPA 모뎀들의 목록은 당사 기술 자료를 참조하십시오.

PPPoE

RED 인터페이스는 ADSL 모뎀에 연결됩니다. 이 옵션은 모뎀이 브리징 모드를 사용하고 PPPoE를 사용하여 공급자에 연결해야 하는 경우에만 필요합니다. 이 옵션을 PPPoE 자체를 처리하는

ADSL 라우터에 연결하는 데 사용되는 정적 이더넷 (ETHERNET STATIC) 또는 동적 이더넷 (ETHERNET DHCP) 옵션과 혼동하지 마십시오.

아날로그 모뎀 (ANALOG Modem)

RED 인터페이스는 아날로그 (전화 접속) 또는 UMTS (휴대폰) 모뎀입니다.

> **참고:** *모바일 광대역*은 기존 *ANALOG/UMTS 모뎀 구현*을 대체하며 *더 많은 3G/4G 모뎀들과 호환됩니다. ANALOG 모뎀*은 여전히 호환성을 이유로해서 사용 가능합니다.

시스템에서 사용할 수 있는 네트워크 인터페이스의 수를 상기시키는 작은 상자가 사용 가능한 선택 항목의 오른쪽에 표시됩니다. RED 인터페이스는 4단계에서 완전히 구성할 수 있습니다.

2/8 - 네트워크 영역 선택

Endian UTM Appliance는 이 섹션에 설명된대로 네 개의 주 영역으로 연결된 네트워크를 분리합니다. 이 시점에서 가장 중요한 두 영역인 *GREEN (녹색)과 RED (빨간색)* 영역이 이미 설치 중에 접촉하게 됩니다. 이 단계에서는 Endian UTM Appliance에서 제공해야 하는 서비스에 따라 하나 또는 두 개의 추가 영역을 활성화할 수 있습니다. 즉, *ORANGE 영역*은 DMZ 네트워크 부분으로 사용되며 *BLUE 영역*은 무선 클라이언트용 세그먼트로 사용됩니다. 전체 구성은 다음 단계에서 가능합니다.

> **참고:** Endian UTM Appliance에서는 RED 인터페이스에 네트워크 카드가 필요한 경우에, 하나의 네트워크 인터페이스가 GREEN 영역용으로 예약되고 다른 하나는 RED 영역에 할당될 수 있습니다. 따라서 추가 네트워크 인터페이스가 없기 때문에 ORANGE 또는 BLUE 영역을 활성화 할 수 없는 지점까지 여기서 선택을 제한할지도 모릅니다.

3/8 - 네트워크 환경 설정

이 단계는 필요한 경우 GREEN (녹색) 영역 및 이전 단계에서 선택한 영역의 구성과 관련됩니다. 활성화된 각 영역에 대해 다음 옵션을 구성할 수 있습니다.

이 영역에서 DHCP 서버 사용 (Enable DHCP server on this zone)

이 옵션은 GREEN(녹색) 영역에서만 사용할 수 있으며, 네트워크 구성 절차를 완료한 후 DHCP 서비스를 자동으로 활성화할 수 있게 해줍니다.

IP 주소 (IP address)

네트워크에서 이미 사용 중이 아닌 인터페이스의 IP 주소 (예: 192.168.0.1)입니다.

> **힌트:** 인터페이스가 전체 서브넷의 트래픽을 수집하기 때문에 마지막 옥텟을 1로 지정하는 것이 좋은 관행입니다.

특히 실제 운영 환경에서 Endian UTM Appliance의 IP 주소를 변경하면, 예를 들어, 워크스테이션의 HTTP 프록시 구성과 같이, 어떤 다른 곳에서 추가 설정을 조정해야 할 수도 있습니다. 그렇지 않으면 웹 브라우저가 올바르게 작동하지 않습니다.

> **경고:** GREEN (녹색) 영역의 인터페이스를 구성할 때, 웹 인터페이스에서 잠겨 있지 않도록 주의하십시오! 이 상황은 예를 들어 GREEN IP 주소를 현재 GREEN 세그먼트로부터 도달할 수 없는 주소로 변경한 다음 설정을 저장할 때 발생할 수 있습니다. 이 경우 Endian UTM Appliance에 대한 유일한 액세스는 직렬 콘솔을 통해서 접근하는 것뿐입니다.

네트워크 마스크 (Network mask)

가능한 마스크가 포함된 드롭 다운 메뉴에서 네트워크 마스크를 정의하십시오 (예: */24 - 255.255.255.0*).

> **힌트:** 동일한 서브넷에 연결된 모든 장치들은 적절하게 통신하기 위해 동일한 넷마스크를 가져야 합니다.

추가 주소 추가 (Add additional addresses)

다른 서브넷에 대한 추가 IP 주소를 여기 인터페이스에 추가할 수 있습니다.

인터페이스 (Interfaces)

다음 규칙을 사용하여 네트워크 인터페이스를 영역에 매핑하십시오:

1. 각 인터페이스는 하나의 영역에만 매핑될 수 있으며, 각 영역에는 적어도 하나 이상의 인터페이스가 있어야 합니다.
2. 하나 이상의 인터페이스가 하나의 영역에 할당되면, 이러한 인터페이스들은 서로 브리지되어 마치 스위치의 일부인 것처럼 작동합니다.

사용 가능한 각 인터페이스에 대해 다음 정보가 표시됩니다:

- *색이 지정된 체크박스*, 인터페이스가 작동하는 영역을 보여줍니다. 색상이 없으면 인터페이스가 어떤 영역에도 지정되어 있지 않다는 의미입니다.
- *포트(Port)*는 포트 번호입니다.
- *링크*, 아이콘을 통해 현재 상태를 표시합니다: ✔ - 링크가 활성화되어 있고, ✘ - 링크가 없거나 케이블이 연결되어 있지 않습니다. ? - 드라이버의 정보가 없습니다.

- *설명*, **lspci**에 의해 반환된 인터페이스의 PCI 식별 문자열입니다. 문자열은 잘려있지만 마우스를 ?로 움직여서 보이게 할 수 있습니다.
- *MAC*, 인터페이스의 MAC 주소입니다.
- *장치*, 장치의 논리적 이름입니다.

> **참고:** 내부적으로 Endian UTM Appliance는 할당된 인터페이스의 수에 관계없이 모든 영역을 브리지로 처리합니다. 따라서 인터페이스들의 Linux 이름은 ethX가 아닌 brX입니다.

마지막으로 시스템의 호스트 이름과 도메인 이름을 화면 하단의 두 텍스트 상자에 설정할 수 있습니다.

사설 IP 주소

RFC 1918 (**RFC 6761**에 의해 최근에 업데이트 됨)에 설명된 표준을 따르고, IANA가 개인적으로 사용하도록 예약한 네트워크 세그먼트에 포함된 IP 주소만 영역 설정에 사용하는 것을 추천드립니다.

10.0.0.0 to 10.255.255.255 (10.0.0.0/8, 16,777,216 addresses)
172.16.0.0 to 172.31.255.255 (172.16.0.0/12, 1,048,576 addresses)
192.168.0.0 to 192.168.255.255 (192.168.0.0/16, 65,536 addresses)

이 선택은 IP 주소가 이 범위에 속하지 않기 때문에 다른 조직에서 자신들의 공용 IP로 예약할 가능성이 있으므로 DNS 확인 오류가 발생하는 것을 피할 수 있습니다. 또한 각 인터페이스에 대해 서로 다른 네트워크 세그먼트에서 다른 IP 범위를 사용해야 합니다. 예를 들면 다음과 같습니다:

IP = 192.168.0.1, 네트워크 마스크 = / 24 - 255.255.255.0, GREEN 영역
IP = 192.168.10.1, 네트워크 마스크 = / 24 - 255.255.255.0 ORANGE 영역
IP = 10.0.0.1, 네트워크 마스크 = / 24 - 255.255.255.0, BLUE 영역

네트워크 세그먼트의 첫 번째 및 마지막 IP 주소 (일반적으로 .0 및 .255)는 각각 네트워크 주소 및 브로드 캐스트 주소로 예약되며 어떠한 장치에도 할당되어서는 안됩니다.

4/8 - 인터넷 액세스 환경 설정

버전 3.0-20141505에서 변경됨: *브리지 및 업링크 없는 네트워크 모드의 도입으로 이 페이지가 약간 변경되었습니다.*

이 단계에서는 1단계에서 선택한 인터페이스를 구성하여 인터넷 또는 Endian UTM Appliance 외부의 다른 신뢰할 수 없는 네트워크에 연결할 수 있습니다.

1단계에서 선택한 네트워크 모드에 따라, 여기에 다른 옵션들이 있습니다. **업링크 모드가 없는 (No uplink mode)** 경우, 단 하나의 옵션만 제공됩니다.

기본 게이트웨이 (Default gateway)

영역 외부로 흐르는 네트워크 트래픽 라우팅을 담당할 게이트웨이의 IP 주소입니다. 게이트웨이의 IP 주소는 Endian UTM Appliance가 설치되어 있는 네트워크 내에 있어야 합니다.

브리지 모드 (Bridged mode)를 선택하면 추가 옵션을 사용할 수 있습니다:

브릿지 영역 (Bridged zone)

이 드롭 다운 메뉴는 활성화된 영역 중 트래픽이 브리징 될 어느 영역을 선택할 수 있게 해줍니다.

네트워크 모드가 **라우트** 되었을 경우, 사용할 수 있는 옵션이 더 많으며 선택한 업 링크 유형에 따라 다릅니다. 페이지 하단에는 일반적으로 사용할 수 있는 두 가지 옵션, 즉 아래에 설명된 *MTU* 및 *스푸핑 (Spoof) MAC 주소* 및 *동적* 또는 *수동*인지를 결정할 수 있는 거의 모든 인터페이스 유형에 사용할 수 있는 DNS resolver (확인 프로그램)의 선택 사항이 표시됩니다. 이 경우 다음 단계에서 DNS 서버의 유효한 IP 주소 하나를 수동으로 제공해야 합니다. 다른 구성 옵션은 다음과 같습니다:

동적 이더넷 (Ethernet DHCP)

단 하나의 가능한 옵션만 있으며, 즉 DNS 선택만 할 수 있습니다.

정적 이더넷 (Ethernet Static)

RED 인터페이스의 IP 주소 및 네트워크 마스크와 기본 게이트웨이의 IP 주소, 즉 Endian UTM Appliance를 인터넷 또는 다른 신뢰할 수 없는 네트워크에 연결하는 게이트웨이의 IP 주소입니다. 선택적으로 인터페이스의 이더넷 하드웨어 주소 (MAC 주소)를 지정할 수 있습니다.

모바일 광대역 (Mobile Broadband, 3G/4G)

이 연결 유형을 사용하면, 시스템이 자동으로 사용중인 모뎀을 감지합니다. 모든 모뎀이 감지되면 2개의 하위 화면이 있습니다.

1. 첫 번째로 구성하려는 모뎀을 선택하십시오.
2. 두 번째 하위 화면에서, 시스템은 공급자를 식별하고 구성 필드를 미리 채울 것입

니다. 이 단계가 실패하였다면, *제공자 선택*, *APN* 및 *액세스 포인트 이름 선택* 필드에 수동으로 정보를 입력하십시오.

필요한 경우 사용자 *이름*과 *암호*도 입력하십시오. 인증 방법은 *PAP* 또는 *CHAP*로 미리 구성되며 필요한 경우 변경할 수 있습니다 (확실하지 않은 경우이를 그대로 두십시오).

마지막으로 DNS 옵션에 대해 수동 또는 자동을 선택하여 사용자 지정 DNS 서버를 지정할지 또는 해당 공급자의 DNS 서버를 지정할 지를 선택할 수 있습니다.

> **참고:** 일부 SIM 카드는 작동하기 위해 PIN (개인 식별 번호)이 필요하지만, 이 기능은 지원되지 않습니다. 이러한 카드가 Endian UTM Appliance와 함께 작동하도록 하려면, 카드에서 PIN을 제거해야 합니다.

PPPoE

PPPoE를 구성하려면, 공급자가 할당한 사용자 이름과 암호 및 인증 방법을 사용하여 양식을 작성하십시오. 선택적으로 공급자의 서비스 및 집중 장치 이름을 구성할 수 있지만 일반적으로 필요하지는 않습니다.

> **힌트:** PAP 또는 CHAP 인증 중에서 어느 것을 선택할지 모르는 경우에는 기본 옵션을 유지하십시오.

아날로그 모뎀 (Analog Modem)

Endian UTM Appliance는 대부분의 현대 UMTS 모뎀을 지원하지만, 그것들을 Endian UTM Appliance와 함께 사용할 때는 약간의 주의가 필요합니다. 한 쪽에서는 일부 UMTS 모뎀도 USB 대용량 저장 장치이며, 일반적으로 두 개의 장치 (예: /dev/ttyUSB0, /dev/ttyUSB1)를 등록합니다. 이 경우에, 첫 번째 장치인 /dev/ttyUSB0은 모뎀이고, 두 번째 저장 장치입니다. 이러한 종류의 모뎀은 Endian UTM Appliance가 USB 대용량 저장 장치에서 부팅을 시도하기 때문에 방화벽을 다시 시작할 때 문제를 일으킬 수 있습니다. 다른 측면에서 일부 SIM 카드는 PIN (개인 식별 번호)이 필요하지만 이 기능은 지원되지 않습니다. 이러한 카드가 Endian UTM Appliance와 함께 작동하도록 하려면, 카드에서 PIN을 제거해야 합니다.

> **참고:** Endian UTM Appliance가 꺼지면 SIM 카드를 연결해야 합니다.

이 선택을 위한 2개의 하위 화면이 있습니다.

1. 첫 번째 화면에서는 모뎀이 연결된 직렬 포트와 아날로그 모뎀인지 또는 UMTS/HSDPA 모뎀인지 지정하십시오.

   > **힌트:** /dev/ttyS0 장치는 직렬 콘솔 용으로 예약되어 있으므로 모뎀용 포트

로 사용할 수 없습니다.

2. 두 번째 화면에서는 모뎀의 비트 전송률, 전화 접속 전화 번호 또는 액세스 지점명, 공급자 및 인증 방법에 의해 할당된 사용자 이름과 암호 (알 수없는 경우 기본 PAP 또는 CHAP를 유지하세요)를 구성합니다. UMTS 모뎀의 경우, 액세스 포인트 이름을 지정할 필요가 있을 수 있습니다.

일반적인 옵션은 다음과 같습니다:

MTU (최대 전송 단위)

네트워크를 통해 전송된 패킷의 MTU 크기입니다.

스푸핑 MAC 주소 (Spoof MAC address with)

RED 인터페이스에 대한 사용자 정의 MAC 주소를 지정하십시오. 이 설정은 HA 설정에서 슬레이브(종속) 장치의 적절한 장애시 시스템 대체 작동 조치에 필요합니다. HA 설정의 RED 주소에 대한 자세한 정보는 고 가용성(High availability)을 참조하십시오.

MTU 크기.

대다수의 ISP는 표준 값인 1500 바이트를 사용하지만 표준 MTU 크기가 너무 높은 경우도 있습니다. 이러한 상황이 발생하면, 예를 들어 다운로드가 잠시 항상 중단되거나 또는 연결 후에 전혀 작동하지 않는 연결과 같은 약간 이상한 네트워크 동작이 나타납니다.

ISP가 표준 MTU 크기를 사용하지 않으면, 오류가 발생하지 않을 때까지 낮출 수있는 특정 값의 특수 ICMP 패킷을 전송하여 올바른 MTU 크기를 쉽게 찾을 수 있습니다. 이 시점에서 MTU 크기는 정확하며, 이 값은 구성 옵션에 입력해야 합니다.

icmp 패킷을 보내려면 다음을 수행하십시오:

EFW에 로그인하고 실제로 도달할 수 있는 호스트 (예: ISP의 DNS, 이는 항상 도달할 수 있어야 함)를 선택하고, 다음 명령을 사용하여 해당 호스트에 대해 ping을 수행합니다.

ping -c1 -M do -s 1460 <host> (자세한 내용은 ***ping(8)*** 도움말 페이지를 참조하십시오).

MTU 크기 1460이 맞으면, 다음과 같은 ping 응답을 받습니다.

PING 10.10.10.10 (10.10.10.10) 1460(1488) bytes of data.
1468 bytes from 10.10.10.10: icmp_seq=1 ttl=49 time=75.2 ms

현재 MTU 크기가 여전히 1460 크기의 패킷에 비해 너무 크다면, 다음과 같은 오류 메시지가 나타납니다.

PING 10.10.10.10 (62.116.64.82) 1461 (1489) bytes의 데이터
ping: sendmsg : 메시지가 너무 깁니다.

올바른 크기가 발견되고 오류가 표시되지 않을 때까지, 다른 패킷 크기 (즉, -s 옵션 다음의 값)로 다시 시도하십시오. ping 명령의 출력에서 대괄호 안에 표시된 값은 MTU 크기입니다. 이 예에서, 출력은 1460(1488)이므로, 1488은 MTU 크기를 선택하는 값입니다.

MTU 값이 1500보다 낮으면 OpenVPN 설정에서도 문제가 발생할 수 있으며, 일부 설정을 조정할 필요가 있습니다.

5/8 - DNS resolver (DNS 확인프로그램) 구성하기

이 단계에서는 IP 주소가 자동으로 할당되지 않는 한 DNS 서버에 대해 최대 두 개의 IP 주소를 정의할 수 있습니다. 이 경우에는 구성 옵션을 설정할 수 없으므로 다음으로 이동하는 것이 안전합니다. 하나의 DNS 서버 만 사용해야 하는 경우라면, 동일한 IP 주소를 두 번 입력해야 합니다. DNS의 IP 주소는 Endian UTM Appliance에서 액세스 할 수 있어야 합니다. 그렇지 않으면, URL 및 도메인 확인이 작동하지 않을 것입니다.

참고 자료: RED 인터페이스 (예: 업링크)의 변경 사항 및 DNS 서버는 다른 네트워크 구성과 별도로 나중에 수정할 수 있습니다.

업 링크 편집기

메뉴 바 ‣ 네트워크 ‣ 인터페이스 ‣ [편집 업링크]

6/8 - 기본 관리 메일 구성하기

전자 메일을 보내기 위해 모든 서비스에서 사용하는 전역 관리자 전자 메일 주소의 구성이 여기서 수행됩니다. 문제가 발생하거나 비상 사태가 발생할 경우에 관리자 전자 메일 주소가 알림에 사용됩니다. 이 전자 메일 주소는 이벤트 알림에서도 사용됩니다.

세 가지 필드를 구성해야 합니다.

관리자 이메일 주소 (Admin email address)

시스템 전자 메일을 보내야 하는 유효한 전자 메일 주소입니다.

보낸 사람 전자 메일 주소 (Sender email address)

보낸 사람 주소로 나타나는 유효한 전자 메일 주소입니다. 수신자가 Endian UTM Appliance에서 보낸 메시지를 필터링하려면, 사용자 정의 보낸 사람 주소가 유용합니다.

스마트호스트의 주소 (Address of smarthost)

전자 메일을 보내면서 거치는 SMTP 서버입니다.

> **힌트:** 모든 입력란을 비워 둘 수 있지만, 적어도 하나 이상의 유효한 관리 이메일 주소를 입력하는 것을추천드립니다.

7/8 - 구성 적용

이 단계는 이제 네트워크 설정이 완료되고 모든 새로운 설정이 수집되었음을 알립니다. `확인 (OK)`, `구성 적용` 버튼을 클릭하면 설정이 저장되고, 필요한 모든 서비스와 데몬들 (daemon)이 다시 시작되어 구성이 적용됩니다.

8/8 – 종료 (End)

마지막 단계에서, 모든 구성 파일이 디스크에 기록되고 모든 장치가 재구성되며, 필요에 따라 네트워크 기반 서비스 및 데몬 (예: 방화벽 및 ntpd)들이 다시 시작됩니다. 전체 프로세스는 관리 인터페이스로의 연결 및 Endian UTM Appliance를 통한 연결이 불가능할 수 있는 동안인 최대 20초가 소요될 수 있습니다.

그러면 관리 인터페이스가 자동으로 다시 로드됩니다. GREENIP 주소가 변경되면, GUI가 새 IP 주소로 다시 로드됩니다. 이 경우 또는 호스트 명이 변경된 경우에, 새 호스트를 식별하기 위해 새로운 SSL 인증서가 생성됩니다.

> **참고:** 나중에 네트워크 구성 (예: 호스트 이름 또는 영역의 네트워크 범위)의 일부 설정 만 변경하려면, 단순히 네트워크 구성을 시작하고, 원하는 변경을 수행할 때까지 모든 단계를 건너뛰고, 적절한 값을 편집한 다음 마지막 단계까지 진행하고 마지막으로 저장하십시오.

이벤트 알림

Endian UTM Appliance에서 어떤 중요한 이벤트가 발생할 때마다 (예: 파티션이 가득 찼거나 누군가 SSH 또는 HTTPS를 통해 액세스하거나 사용 가능한 업데이트가 있을 때) 이벤트 알림 기능을 사용하면 전자 메일이나 SMS로 즉시 알릴 수 있습니다. 이벤트의 결과로 즉각적인 조치를 취하기 위해 파이썬 스크립트를 각 이벤트에 연계해서 사용할 수도 있습니다.

이 페이지에서는 *구성 (Configuration), 이벤트 (Events), SMS 및 스크립트 (Script)*의 네 가지 탭을 사용할 수 있습니다.

구성

이 탭에는 알림을 보내도록 전자 메일 및 SMS 설정을 구성하는 기본 옵션이 포함되어 있습니다.

이벤트 알림 기능을 시작하려면 회색 스위치  클릭하고 몇 초 기다리십시오.

사용할 수 있는 옵션들은 다음과 같습니다.

기본 이메일 설정 사용

설치 마법사에서 지정된대로 기본 전자 메일 주소를 사용하거나 메뉴 바 ‣ 시스템 ‣ 네트워크 구성의 6 단계에서 체크박스를 선택합니다. 그렇지 않으면, 다른 SMTP 서버를 구성하는 몇 가지 옵션들이 나타납니다.

SMTP 프록시 서비스 사용

가능한 경우 시스템의 SMTP 프록시를 사용하려면 체크박스를 체크표시를 하십시오.

이전 두 옵션들을 선택하지 않으면, 다음 몇 개의 옵션들이 나타납니다.

이메일 발신자 주소

전자 메일의 보낸 사람으로 표시되는 전자 메일 주소입니다.

이메일 수신자 주소

전자 메일이 배달될 전자 메일 주소입니다.

이메일 전송을 위해 스마트호스트 사용

체크박스를 선택하여 알림 전자 메일을 배달하는데 사용할 스마트호스트를 구성합니다.

> **참고:** SMTP 프록시가 암호화를 지원하는 동안, 외부 스마트호스트가 SMTP 프록시로 사용될 때, SSL/TLS 및 STARTTLS 프로토콜을 사용할 수 없습니다.

스마트호스트 주소

스마트호스트의 URL 또는 IP 주소입니다.

스마트호스트 포트

스마트호스트가 청취(대기)하는 포트입니다.

스마트 호스트가 인증을 요구합니다.

스마트호스트가 전자 메일을 보내기 위해 자격 증명을 요구하면, 체크박스를 선택합니다. 다음 두 옵션들이 나타납니다.

스마트 호스트 사용자 이름

스마트호스트로 인증하는데 사용할 사용자 이름입니다.

스마트 호스트 암호

이전 옵션에서 제공한 사용자 이름과 연관된 암호.

인증 방법

스마트호스트가 사용자를 인증하는데 사용할 방법을 선택하십시오.

다음 두 옵션은 SMS로 알림을 구성하는데 사용됩니다.

도착지 전화 번호 국가 프리픽스

전화 번호가 속한 국가 코드.

목적지 전화 번호

SMS를 보낼 실제 전화 번호.

이벤트

이 탭에는 알림 메시지를 생성할 수 있는 모든 이벤트의 목록이 표시되며, 각 이벤트가 발생할 때 수행할 작업을 구성할 수 있습니다. 목록 바로 위에 작은 탐색 모음(막대)과 검색 필드가 있습니다. 후자는

관련 항목 만 필터링하는데 사용할 수 있습니다.

이 목록은 6개의 열을 포함하고 있습니다.

이벤트 ID

다음과 같이 빌드된 이벤트의 8자리 ID ABBCCCCD 코드입니다.

- A는 레이어 번호, 즉 이벤트가 발생한 시스템 구성 요소를 나타냅니다.
  - 1 = 커널
  - 2 = 시스템
  - 3 = 서비스
  - 4 = 구성
  - 5 = GUI.
- BB는 모듈 번호입니다.
- CCCC는 이벤트에 할당된 일련 번호입니다.
- D는 이벤트의 심각도, 즉 이벤트의 불량의 정도입니다. 숫자가 낮을수록 심각도는 가장 심합니다.
  - 0 : 중대한 사건(critical event)
  - 1 : 오류(an error)
  - 4 : 경고 (a warning)
  - 6 : 나쁜 상태에서 회복
  - 8 : 정보 메시지.

설명

이벤트에 대한 간단한 설명.

이메일

체크박스에 체크 표시가 되어 있는 경우 이벤트가 발생하면 전자 메일이 전송됩니다.

SMS

체크 표시가 있는 체크박스는 이벤트가 발생할 때 SMS가 전송됨을 의미합니다.

스크립트

이벤트가 발생할 때 스크립트가 실행됩니다.

조치(Actions)

사용 가능한 유일한 조치는 (swedit) 아이콘을 클릭하여 해당 이벤트를 수정하는 것입니다.

이벤트를 수정할 때, 다음 구성 옵션들이 표시되면서 새 패널이 목록 위에 나타납니다.

이벤트 ID 및 설명

이는 이벤트의 식별자이며 시스템에서 자동으로 생성하므로 수정할 수 없습니다.

이 일정에 대한 이메일 보내기

이 체크박스를 체크 선택하면 이벤트 발생시 전자 메일이 전송됩니다.

이 이벤트에 SMS 보내기

이 체크박스를 체크하면, 이벤트 발생시 SMS가 전송됩니다.

이 이벤트에 대한 사용자 지정 스크립트 실행

이 옵션을 선택하면, SMS 또는 전자 메일을 보내지 않고 이벤트가 발생할 때 사용자 지정 스크립트가 실행됩니다. 스크립트는 이미 Endian UTM Appliance에 업로드 되어 있어야 합니다. 자세한 정보는 스크립트 탭을 참조하십시오. 체크 박스를 선택하면 오른쪽에 드롭 다운 메뉴가 나타납니다.

실행할 사용자 지정 스크립트

이 드롭 다운 메뉴에서 이벤트에 연결할 스크립트를 선택하십시오.

다음 표에서는 이벤트에 해당하는 모든 ID 목록을 보여줍니다. 기기 유형에 따라, Endian UTM Appliance에서 일부 이벤트가 발생하지 않을 수 있습니다 (예: RAID 컨트롤러가 없는 기기에서는 이벤트 10100011, 10100026 및 10100038가 발생하지 않을 것입니다).

이벤트 **ID**	설명
10100011	One device of the RAID array failed.
10100026	The rebuild of RAID array has completed.
10100038	Start recovery of RAID array.
20100016	One uplink has gone online.
20100024	One uplink has gone offline.
20100036	The system has started.
20100044	The system has shut down.
20100054	The system is rebooting.
20110030	All uplinks have gone offline.
20110046	All uplinks are online.
20110054	An uplink is dead.
20110066	An uplink turned back alive.

이벤트 ID	설명
20200018	An SSH user has successfully logged in from a remote location.
20200024	An SSH user failed to log in from a remote location.
20300014	A disk is getting full.
20400014	An user has failed to log in to the management interface.
20500018	The number of available SMS is low
20500028	There is no SMS left
20700018	OpenVPN client opened tunnel on an interface
20700218	OpenVPN client closed tunnel on an interface
20800014	An OpenVPN user failed a login failed
20800024	An IPsec/Xauth use failed to login
20800034	An L2TP user failed to login
20800048	An Open VPN user has logged in successfully
20800058	An IPsec/Xauth user has logged in successfully
20800068	An L2TP user has logged in successfully
20800078	An Openvpn user has logged out
20800088	An IPsec/Xauth user has logged out
30100018	The system upgrade has completed successfully.
30100021	The system upgrade has failed.
30100038	There are system updates available.
40100016	The remote access to support user has been revoked.
40100024	The remote access to support users has been granted.
40100034	The access for support user has been extended until ...

SMS

이벤트 알림 외에도 SMS는 핫스팟에서 계정이나 티켓을 활성화하는데 사용됩니다. 번들제품은 Endian S.p.A., Italy에서 구입할 수 있으며, 여기에서 Endian UTM Appliance에 추가됩니다.

이 상자는 두 부분으로 나누어져 있습니다. 상단에는 SMS 번들을 추가하는 것이 가능하고, 하단에는 SMS 조건에 대한 정보가 표시됩니다.

활성화 코드 입력 ...

새 SMS 번들을 추가하려면, Endian Network에서 먼저 구입해야 하며, 그 후에 활성화 코드가 생성됩니다. 이 활성화 코드는 이 텍스트상자에 제공되어야 합니다.

활성화

유효한 정품 인증 코드를 입력한 후, 이 버튼을 클릭하면 알림 전송에 사용될 SMS 조건이 추가될 것입니다.

사용 가능한 SMS

처분할 수 있는 SMS의 갯수.

예약된 SMS

이미 사용되었지만 아직 수령인에게 배달되지 않은 SMS 수입니다. 예를 들어, 이 이벤트는 수신자에게 도달할 수 없는 경우에 발생할 수 있습니다.

스크립트

전자 메일이나 SMS를 전송하는 것 외에도, 세 번째 옵션은 Endian UTM Appliance에서 이벤트가 발생한 직후에 Python 스크립트를 업로드하고 실행할 수 있습니다. 이 탭에서는 Python 스크립트를 다양한 이벤트에 업로드하고 연결할 수 있습니다. 보다 정확하게는 각 이벤트에 하나의 Python 스크립트를 할당할 수 있습니다.

맨 아래에는 이미 업로드 된 스크립트들의 목록이 표시되고, 처음에는 비어 있으며 각 스크립트에 대한 다음 정보를 보여줍니다.

- *이름:* 스크립트에 주어진 이름.
- *설명:* 스크립트에 대한 설명.
- *조치:* 스크립트에 사용할 수 있는 작업들:
  - 는 스크립트를 수정합니다. 이 아이콘을 클릭하면, 스크립트를 관리할 수 있는 패널이 나타납니다.
  - 로컬 워크 스테이션에서 스크립트를 다운로드합니다.
  - Endian UTM Appliance에서 스크립트를 제거합니다.

테이블 상단에 *새로운 스크립트 추가(Add new script)* 하이퍼링크에 있는 시계가 Endian UTM Appliance에 Python 스크립트를 업로드 할 수 있게 해줍니다. 업로드 된 스크립트는 몇 가지 지침을 따라야 합니다. 자세한 내용은 아래를 참조하십시오. 다음 옵션을 사용할 수 있습니다.

이름

스크립트에 주어진 이름.

설명

스크립트의 선택적 설명 (예: 스크립트의 목적에 대한 설명입니다).

Python 스크립트 파일 업로드

업로드 할 파일을 선택할 수 있는 대화 상자 창을 열기 위해 버튼을 클릭하십시오.

Python 스크립트의 요구 사항.

Endian UTM Appliance에서 실행될 Python 스크립트는 다음과 같이 요약할 수 있는 시스템과의 적절한 상호 작용을 보장하기 위해 몇 가지 설계 지침을 따라야 합니다.

1. 스크립트를 가져올 수 있어야 합니다. 즉, 스크립트는 시스템에 설치된 다른 파이썬 모듈을 사용할 수 있지만 시스템에 없는 파이썬 모듈에는 의존할 수 없습니다
2. 스크립트는 **ScriptEvent**라는 클래스를 구현해야 합니다.
3. **process**라는 메서드는 ScriptEvent 클래스에 구현되어야 합니다. 이 메소드는 그것과 연관된 이벤트가 발생할 때 호출됩니다.
4. 프로세스 메소드는 ****kwargs** 매개 변수를 승인해야 합니다. 즉, key : value 매개 변수의 사전을 허용해야 합니다.

위의 요구 사항을 충족하므로 Endian UTM Appliance에 업로드 할 수 있는 예제 스크립트는 다음과 같습니다.

```
import time
class ScriptEvent(object):
   def __init__(self):
      self.filename = "/tmp/fubar"

   def process(self, **kwargs):
      open(self.filename, "a").write("Hello world, it is now %s₩n" %
      time.time())
```

참고 자료: Endian 코드 문서는 곧 사용할 수 있는 스크립트를 작성하는데 유용합니다.

업데이트

소프트웨어 업데이트 관리는 여기에서 수행됩니다. 언제든지 사용 가능한 업데이트된 패키지를 수동으로 확인하거나 정기적인 검사를 예약할 수 있습니다.

이 페이지에는 두 개의 상자가 있습니다. 하나는 시스템의 현재 상태이고, 다른 하나는 업데이트에 대한 일상적인 점검을 예약하는 상자입니다.

상태

상태 상자는 시스템에 업데이트가 필요한지 여부를 알려줍니다. 전자의 경우, 사용 가능한 패키지 목록이 표시되는 반면, 후자의 경우에는 다음과 같은 메시지가 표시됩니다.

> 엔디안 방화벽이 **최신 상태**입니다!
> **마지막 업그레이드**가 2011 년 3 월 13 일 15:22:50에 수행되었습니다.
> 25.05.2017, 11:04:58에 **업데이트되었는지 마지막으로 확인했습니다**.

다음 옵션을 사용할 수 있습니다.

새 업데이트 확인

업데이트된 패키지에 대한 수동 확인이 시작되고, 발견된 업그레이드할 수 있는 패키지가 여기에 나열됩니다. 개별 패키지를 목록에서 선택하여 설치할 수 있습니다.

지금 업데이트 프로세스 시작

업데이트 프로세스가 시작됩니다. 시스템은 설치된 업데이트 된 패키지를 다운로드 한 다음 이전 패키지를 대체합니다.

> 참고: 업데이트를 확인하려면, 유효한 유지 관리가 필요합니다. 그렇지 않으면 사용 가능한 경우에도 업데이트가 표시되지 않습니다.

업데이트 목록 검색 일정

Schedule 상자는 업데이트 된 패키지 목록을 검색하는 cron 데몬에 의해 관리되는 주기적인 작업을 설정하도록 허용합니다. 사용 가능한 옵션은 *Hourly(시간별), Daily(일별), Weekly(주간별) 및 Monthly(월별)* 등이 있습니다. 각 옵션 옆에 있는 작은 물음표(?) 위로 마우스를 이동해보면, 작업이 실행될 정확한 시간이 보이는 툴팁이 표시됩니다.

지원

이 페이지에서는 Endian 지원에 대한 도움 요청을 관리할 수 있습니다.

> **참고:** 지원 요청을 제출하려면, 시스템이 Endian Network에 등록되어 있어야 합니다. 그렇지 않은 경우에는, "현재 이용할 수 있는 실행 중인 유지 관리가 없습니다."라는 메시지가 표시됩니다.
>
> 시스템이 등록되지 않았다면, Endian 웹 사이트 섹션에 열거된 여러 포럼 또는 메일 목록 중 하나에 지원 요청을 할 수 있습니다.

이 페이지는 용도가 다른 두 개의 상자로 나뉩니다. 첫 번째 페이지에는 지원 홈페이지를 열 수 있는 링크가 포함되어 있으며, 두 번째 페이지에서는 지원 팀이 SSH 및 HTTPS를 사용하여 Endian UTM Appliance에 액세스 할 수 있게 해줍니다.

지원 웹 사이트 방문

이 상자에는 지원 홈 페이지에 대한 하이퍼 링크만 있습니다.

지원 웹 사이트를 방문하십시오.

> 이 링크를 클릭하면, 브라우저의 새 탭이 열리고, 지원 팀에 도움 요청을 작성하는 방법에 대한 지침을 찾을 수 있습니다.

Endian 지원 팀을 위한 액세스

선택적으로 방화벽에 대한 액세스는 SSH를 통해 부여할 수 있으며, 보안 및 암호화된 연결은 지원부서의 직원이 Endian UTM Appliance에 로그인하고, 기기의 구성을 확인한 다음 문제가 있는 곳을 찾을 수 있도록 검사할 수 있게 해줍니다. 이 상자에는 액세스 상태 (**DENIED** 또는 **ALLOWED**)라는 유익한 메시지가 있습니다. 상태가 **DENIED**이면 버튼이 상자 하단에 나타납니다.

액세스 허용

> 이 버튼을 클릭하면 지원 팀에게 Endian UTM Appliance에 대한 4 일간 액세스 권한을 부여할 수 있습니다.

지원 팀 액세스가 허용되면, 상태 메시지 아래에 새 메시지가 나타납니다: *다음 시간까지 액세스가 허용됩니다:* Endian UTM Appliance에 대한 액세스가 취소되는 날짜와 시간까지 이어서 접근이 허용됩니다. 또한 상자 하단에는 두 개의 버튼이 있습니다.

접근 거부

> Endian UTM Appliance에 액세스할 수 있는 권한 허가를 즉시 취소합니다.

4일 이상 동안 액세스 연장

지원 팀이 Endian UTM Appliance를 검사하는데 더 많은 시간이 필요한 경우에는, 이 버튼을 클릭하면 액세스 권한이 4일 더 연장됩니다.

> **참고:** 활성화되도록 설정하면, 지원 팀의 공용 SSH 키가 시스템에 복사되고, 해당 키를 통해 액세스가 허용됩니다. 지원팀은 Endian UTM Appliance에 대한 사용자 이름/암호로 인증하지 않습니다. Endian UTM Appliance의 루트 암호는 어떤 방식 으로든 지원 팀에 공개되지 않습니다.

엔디안 네트워크

Endian UTM Appliance를 유지 관리 패키지와 함께 구입한 경우에는, 등록된 모든 Endian UTM Appliance 시스템을 쉽고, 중앙 집중적으로 모니터링, 관리 및 업그레이드할 수 있도록 Endian 솔루션 인 Endian Network에 등록하고 연결할 수 있습니다.

Endian UTM Appliance의 많은 기능 (예: 지원 팀 액세스, SMS 알림 등)을 사용하려면 기기를 엔디언 네트워크에 등록해야 합니다.

시스템이 아직 등록되지 않았거나 유지 보수가 만료된 경우에는, 이 페이지에는 기기를 등록하기 위해 작성해야 하는 양식만 표시됩니다.

Endian Network 등록이 중요한 이유는 무엇입니까?

활성화 코드 구매 후 30일 이내에 시스템을 등록해야 합니다. 그렇지 않으면, 지원을 제공할 수 없습니다.

구매 후 30일이 지났지만, Endian UTM Appliance가 계속 작동하고 이미 구성된 서비스를 제공하고 있는 경우에는, Endian Network, GUI, SSH 및 직렬 콘솔에서의 액세스는 금지됩니다. 즉, Endian UTM Appliance에 지원 팀이 연결할 수 없으므로 지원이 제공되지 않는다는 것을 의미합니다. 또한, 업데이트를 더 이상 설치할 수 없습니다.

Endian UTM Appliance에 대한 완전한 액세스 권한을 다시 얻으려면, 새로운 활성화 코드 또는 유지 관리 갱신 권한을 구매해야 합니다.

이 페이지는 구독(Subscription)과 원격 액세스(Remote Access)라는 두 개의 탭으로 구성되어 있습니다.

구독(Subscription)

방화벽이 아직 엔디안 네트워크에 등록되지 않은 경우, 등록 요청서를 제출하기 전에 기입해야 하는 등

록 양식이 표시됩니다. 등록이 완료되면 구독 탭에 세 개의 상자가 표시됩니다.

시스템 정보

Endian UTM Appliance에 대한 기본 데이터: 일련 번호, 정품 인증 코드, 어플라이언스(기기) 모델 및 선택한 유지 관리 패키지 등이 표시됩니다.

등록 상태

엔디안 네트워크에 기록된 시스템 정보의 요약: 시스템 명, Endian UTM Appliance가 등록된 조직, 시스템 ID 및 최종 업데이트 날짜, 즉, Endian UTM Appliance가 등록된 날짜 등의 정보가 표시됩니다.

활성화 키

엔디안 네트워크에 참가하여 업데이트를 받으려면, 유효 기간이 만료되지 않고 유효한 활성화 키(정품 인증 키)가 적어도 하나 이상 있어야 합니다. 각 채널에는 키가 있지만 일반적으로 만료일과 남은 유지 관리 일수가 표시된 하나 또는 두 개의 키가 있습니다.

만료된 키는 해당 채널 이름이 선으로 지워진채 표시되고 해당 *남은 날짜* 열에 *만료됨(expired)* 문자열로 표시됩니다. 이는 일반적으로 선택 채널에 대해 발생합니다.

원격 액세스

Remote Access (원격 액세스) 탭에서는 Endian Network를 통해 Endian UTM Appliance에 연결할 수 있는지 여부와 프로토콜을 선택할 수 있습니다. 액세스를 허용하려면, 페이지 상단의 회색 스위치  를 켜기 위해 클릭하십시오. 색상이 녹색으로 바뀌고, 확인란을 체크하여 두 가지 액세스 옵션을 선택할 수 있습니다.

HTTPS 액세스 사용 ...

Endian UTM Appliance는 웹 인터페이스를 통해 액세스 할 수 있습니다.

SSH 액세스 활성화 ...

보안 셸을 통해 Endian UTM Appliance에 로그인 할 수 있습니다. 이 옵션을 활성화하면, SSH 액세스가 자동으로 활성화됩니다.

> **참고 항목:** Endian Network에 Endian UTM Appliance를 등록하는 단계별 강좌는 여기에서 볼 수 있습니다.

스위치보드에 연결하기

버전 5.0.5의 새로운 기능.

이 페이지에서는 플러그 및 연결 절차를 사용하여 Endian UTM Appliance를 스위치보드 인스턴스에 연결하고 등록할 수 있습니다.

> 참고: 이 기능은 아직 모든 기기에서 사용할 수 없습니다.

Endian UTM Appliance를 스위치보드에 연결하는데 적격이 되도록 하려면, 몇 가지 요구 사항을 충족해야 합니다.

1. 네트워크 마법사 (네트워크 구성 참조)가 성공적으로 수행되고 영역이 구성되었습니다.
2. Endian UTM Appliance는 아직 Endian Network에 등록되지 않았습니다. 이 경우에, 엔디안 네트워크에서 삭제해야 합니다.
3. 작동중인 업링크가 있어야 하며, 인터넷에 연결할 수 있어야 합니다.

Endian UTM Appliance가 이 두 가지 조건을 충족하면, 절차를 시작할 수 있습니다.

> **참고:** 전원을 연결하고 연결 절차는 옵션 6을 선택하고 지침에 따라 웹 콘솔에서 수행할 수 있습니다.

이 페이지에 처음 액세스하면, 단 하나의 옵션만 포함되어 있습니다.

활성화 코드

유효한 정품 인증 코드를 입력한 다음에, Endian UTM Appliance를 스위치보드에 등록하기 위해 다음>> 를 누르십시오.

한번 연결이 끝나면, 페이지가 변경되고, Endian UTM 어플라이언스에 성공적으로 연결하기 위해 활성화 코드 및 **클레임 기간**, 즉, 플러그 및 연결 절차를 수행해야 하는 과정 내에 날짜와 시간이 표시됩니다.

여기에는 하나의 옵션만 있습니다.

클레임 기간 연장

이 버튼을 클릭하면, 클레임 기간이 24 시간 연장됩니다.

이 시점에서 스위치보드에 Endian UTM Appliance를 요청하고 원격 관리를 허용할 수 있습니다. 이 단계가 완료되면, Endian UTM Appliance도 엔디안 네트워크에 등록되며 (그리고 그것으로부터 접근할 수 있는), 이 페이지에 몇 가지 정보가 표시됩니다.

- 메시지. **스위치보드에 연결되었습니다.**
- 스위치보드 인스턴스. Endian UTM Appliance가 요청된 스위치보드에 부여된 이름.
- 게이트웨이 이름. 스위치보드에 등록된 Endian UTM Appliance의 이름입니다.

참고: 우리의 포털에는 플러그와 연결 및 요청 절차에 대해 자세히 설명하는 방법이 제공됩니다.

암호

이 페이지에서 두 명의 기본 사용자들 각각에 대해 새 암호를 두 번 각각 작성한 다음 해당 `암호 변경` 단추를 눌러 암호를 변경할 수 있습니다.

Admin

관리를 위해 웹 인터페이스에 연결할 수 있는 사용자입니다.

Root

관리를 위해 쉘에 로그인 할 수 있는 사용자입니다. 시리얼 콘솔을 통해 로그인하거나 SSH 클라이언트를 통해 원격으로 로그인 할 수 있습니다.

> **힌트:** 암호는 6자 이상이어야 합니다. 좋은 암호는 8자 이상이어야 하며 문자, 숫자 및 $ % @ !와 같은 특수 문자가 포함되어야 합니다.

웹 콘솔

웹 콘솔은 브라우저 창에서 터미널을 에뮬레이트하는 애플릿을 제공합니다. 이 애플릿은 관리 작업을 수행하는 CLI (명령행 인터페이스) 역할을 합니다.

웹 콘솔의 기능은 직렬 콘솔 또는 SSH를 통해 로그인 할 때와 동일합니다. 애플릿 왼쪽 하단에 콘솔의 상태 (*연결됨* 또는 *연결 끊김*)를 보여주는 메시지가 표시됩니다. 일반적인 콘솔과 마찬가지로 콘솔에서 exit를 입력한 다음 키보드에서 `Enter` 키를 눌러 언제든지 종료할 수 있습니다.

연결이 끊어지면, *웹 콘솔* 하위 메뉴 항목을 클릭하여 다시 연결하십시오. 애플릿의 오른쪽 아래에 두 개의 하이퍼 링크가 나타납니다.

가상 키보드 사용

이 링크를 클릭하면, 콘솔 아래에 키보드 애플릿이 나타나 다양한 *키들(keys)*을 마우스로 클릭하여 명령을 입력하고 실행할 수 있습니다.

> **참고**: 웹 콘솔이 분리되면이 애플릿은 콘솔과 통신하지 않습니다.

입력 사용 중지

이 링크는 키보드에서 웹 콘솔로 입력을 보낼 수 있는 기능을 토글합니다.

> **힌트:** 이 옵션은 가상 키보드에는 적용되지 않습니다.

SSH 접속

이 화면에서는 기본적으로 비활성화되어 있는 Endian UTM Appliance에 대한 원격 SSH 접속을 활성화할 수 있습니다. SSH를 사용하여 액세스하면 로그 파일을 제어해야 할 필요성, 문제 해결, 구성 파일을 수동으로 편집하는 등의 여러 시나리오에서 유용합니다. 그리고 일반적으로 서비스의 사용자 정의 또는 기존 버그에 대한 대안 구현과 같은 고급 작업을 위해 예약되어 있습니다.

이 페이지는 처음에는 비어 있으며, 회색 스위치  를 클릭하여 SSH 액세스를 활성화하면, 페이지에 *보안 쉘 옵션*과 *SSH 호스트 키의* 두 개의 상자가 표시됩니다.

SSH 서비스가 처음 활성화되면, 새로운 SSH 호스트 키가 생성되어야 하므로 Endian UTM Appliance에 액세스 할 수 있게 되기까지 잠시 시간이 걸립니다.

보안 쉘 옵션

SSH 서비스가 시작되면 다음 구성 옵션이 표시됩니다.

Allow password based authentication (암호 기반 인증 허용)

암호 인증을 사용하여 로그인을 허용합니다.

Allow TCP forwarding (TCP 포워딩 허용)

이 옵션을 선택하면 다른 프로토콜들을 SSH를 통해 터널링할 수 있습니다. 샘플 사용 사례는 SYS-1 예제를 참조하십시오.

Allow public key based authentication (공개 키 기반 인증 허용)

공개 키가 있는 로그인은 허용됩니다. 키 인증을 사용하여 로그인 할 수 있는 클라이언트의 공개 키는 /root/.ssh/authorized_keys 파일에 추가되어야 합니다.

저장

위의 네 가지 옵션의 설정을 저장하기 위해 상자의 맨 아래에 있는 이 버튼을 클릭하십시오.

> **참고:** SSH 액세스는 다음 옵션 중 하나 이상에 해당하면 자동으로 활성화됩니다:
>
> - Endian 지원팀 액세스는 *Menubar ‣ System ‣ Support*에서 허용됩니다.
> - *Menubar ‣ -Services -> High Availability*에서 고가용성을 활성화할 수 있습니다.
> - 엔디안 네트워크의 SSH 액세스는 *Menubar ‣ System ‣ Endian Network ‣ Remote Access*에서 활성화할 수 있습니다.

예제 SYS-1 - SSH를 통한 트래픽 터널링.

텔넷 (또는 SSH를 통해 터널링 할 수 있는 다른 서비스)과 같은 서비스는 GREEN 구역 내에 있는 컴퓨터, 예를 들어 IP 주소 10.0.0.20인 *myhost* 호스트의 포트 23에서 실행되고 있다고 가정합니다. Endian UTM 어플라이언스를 통해 SSH 터널을 설정하여 LAN 외부 (즉, RED 구역)에서 안전하게 서비스에 액세스 할 수 있습니다. RED 인터페이스로부터 GREEN 구역으로의 액세스는 일반적으로 권장되지 않지만, 일부 경우, 예를 들어 서비스 테스트 단계에서 유용할 수 있습니다.

1. SSH를 활성화하고 호스트에 액세스 할 수 있는지 확인하십시오. 즉, 외부에서 접근할 수 있도록 *Menubar ‣ Firewall ‣ System access*에서 myhost를 위한 방화벽을 구성하십시오.
2. 외부 시스템에서 **ssh -N -f -L 12345: 10.0.0.20: 23 root@appliance** 명령을 사용하여 Endian UTM Appliance에 연결합니다. 여기서 -N은 SSH에 명령을 실행하지 말고 트래픽을 전달만 하도록 만드는 것입니다. -f는 SSH를 백그라운드에서 실행되게 만들며, -L 12345: 10.0.0.20: 23은 Endian UTM Appliance에서 볼 수 있듯이 외부 시스템의 포트 12345를 *myhost*의 포트 23에 매핑합니다.
3. 외부 시스템의 포트 12345에서 *myhost*의 포트 23까지의 SSH 터널이 설정되었습니다. 이제 외부 시스템에서 *myhost*에 도달하기 위해 로컬 호스트의 포트 12345에 telnet으로 연결하면 됩니다.

SSH 호스트 키들

페이지 맨 아래의 표에는 첫 번째 시작시 ECDSA 256 비트, RSA2 2048 비트 및 DSA 1024 비트가 생성

된 세 가지 호스트 키가 나와 있습니다. 각 키의 위치, 지문 및 크기가 비트 단위로 표시됩니다.

GUI 설정

GUI에 대한 두 가지 구성 옵션이 여기에 있습니다.

언어 선택

웹 인터페이스 (섹션 이름, 레이블, 모든 문자열)에 사용될 언어이며 드롭 다운 메뉴에서 선택할 수 있습니다. 현재 지원되는 언어는 영어, 독일어, 이탈리아어, 중국어 간체, 일본어, 포르투갈어, 러시아어, 스페인어 및 터키어입니다.

창 제목에 호스트 이름을 표시합니다.

확인란을 선택하여 활성화하면, 이 옵션은 브라우저의 창 제목에 Endian UTM Appliance의 호스트 이름을 표시합니다.

> **힌트:** 호스트 이름은 네트워크 구성 (*시스템 ‣ 네트워크 구성*)의 3단계에서 설정됩니다.

커뮤니티 릴리스에서는 이 프로젝트 번역 도움말 링크를 클릭하면, Endian Firewall 커뮤니티 번역 페이지가 열립니다. 누락된 번역에 기여할 수 있습니다. 어떠한 도움이라도 감사합니다!

백업

이 섹션에서는 현재 Endian UTM Appliance 상태 및 구성의 새 백업을 만들거나 필요할 때 이러한 백업 중 하나를 복원할 수 있습니다. 백업은 Endian UTM Appliance 호스트, USB 스틱 또는 워크스테이션에 로컬로 저장할 수 있습니다. 백업 복사본을 안전한 위치에 보관하는 것이 좋습니다.

vfat 형식의 USB 스틱이 Endian UTM Appliance에 연결되면 자동으로 감지되어 마운트됩니다. 이 경우 몇 가지 추가 USB 관련 옵션이 페이지 전체에 표시됩니다.

여기에서 구성을 공장 기본값으로 재설정하고, 완전 자동화된 백업을 만들고, 다양한 다른 백업 관련 작업을 수행할 수도 있습니다.

이 섹션은 *백업* 및 *예약된 백업*의 두 가지 탭으로 구성됩니다. 전자는 수동 백업을 관리하는 반면 후자는 자동 백업을 설정하는데 사용됩니다.

백업

백업 탭에는 *백업 세트*, *암호화 백업 아카이브*, *백업 아카이브 가져오기* 및 *구성을 출고시 기본값으로 재설정* 및 *재부팅*과 같이 백업으로 수행할 수 있는 다른 작업에 각각 해당하는 네 개의 상자가 있습니

다.

백업 세트

첫 번째 상자에는 테이블이 수동 및 예약된 Endian UTM Appliance에 저장된 백업을 보여줍니다. USB 스틱이 Endian UTM Appliance에 연결되어 감지되면 해당 USB 스틱에 저장된 백업도 표시됩니다.

각 항목에 대해 다음과 같이 표시됩니다:

- 생성 날짜
- 백업에 포함된 컨텐츠. 각 문자는의 다른 요소에 해당합니다. 자세한 내용은 아래를 참조하십시오.
- 비고. "업그레이드 전 자동 백업" 문자열은 패키지 또는 시스템 업그레이드 전에 자동 백업이 수행되었음을 의미합니다.
- 사용 가능한 작업:
  - 암호화된 백업을 다운로드합니다 [*]
  - 백업을 삭제합니다
  - 현재 워크스테이션에서 백업을 다운로드
  - Endian UTM Appliance에서 백업을 복원.

[*] 백업 아카이브 암호화 옵션이 활성화된 경우에만 사용할 수 있습니다 - 아래 참조.

각 백업의 내용은 작성 중에 지정된 옵션에 해당하는 다음 문자 또는 기호 중 적어도 하나에 의해 표시됩니다.

Archive. 백업에는 아카이브 된 로그 파일이 들어 있습니다.
Cron. 백업은 예약된 백업 작업에 의해 자동으로 생성됩니다.
Datebase dumps. 백업에 데이터베이스 덤프가 있습니다.
Encrypted. 백업 파일이 암호화됩니다.
Hardware. 어플라이언스의 하드웨어에 대한 정보가 포함되어 있습니다.
Log files. 백업에는 오늘의 로그 파일이 포함됩니다.
Settings. 백업에는 구성 및 설정이 포함됩니다.
USB. 백업이 USB 스틱에 저장되었습니다
! (Error). 이메일로 백업 파일을 보내는 동안 문제가 발생했습니다.

테이블 위에는 새 백업 만들기 링크가 있습니다. 이 탭을 클릭하면 백업에 포함될 데이터를 선택할 수 있는 대화 상자가 열립니다. 괄호 안의 문자는 위에 열거된 문자들과 일치합니다.

현재 구성 Current configuration (**S**)

백업에는 지금까지 수행된 모든 변경 및 사용자 정의, 즉 /var/efw 디렉토리의 모든 내용을 포함하여 모든 구성 설정이 포함됩니다.

데이터베이스 덤프 포함 Include database dumps (**D**)

데이터베이스의 내용도 백업됩니다.

> **경고:** 데이터베이스 덤프에는 중요한 데이터가 포함될 수 있으므로 백업에 데이터베이스 덤프가 포함될 때마다 안전한 장소에 저장되어 있는지 확인하십시오.

로그 파일 포함 Include log files (**L**)

현재 로그 파일 (예: /var/log/messages)은 포함시키지만 이전 요일의 로그 파일은 포함하지 않습니다.

로그 아카이브 포함 Include log archives (**A**)

교체된 이전 로그 파일도 포함하고 /var/log/archive/ 디렉토리 아래에 저장됩니다. 이 옵션으로 생성된 백업은 시간이 지나면 매우 커질 수 있습니다.

하드웨어 데이터 포함 Include hardware data (**H**)

어플라이언스 하드웨어에 대한 데이터를 포함하십시오. 동일한 유형의 어플라이언스에서 백업을 복원할 때 필요하지만 백업을 다른 어플라이언스의 모델 (예: 머큐리에서부터 매크로까지)로 가져올 때 이 정보가 포함되지 않아야 합니다.

비고 Remark

테이블에 대한 설명 열에 나타나는 백업에 대한 설명입니다. 따라서 콘텐츠를 빨리 불러올 수 있을 만큼 의미가 있어야 합니다.

USB 스틱에 백업 생성 Create backup on USB Stick

USB 스틱에 백업을 저장합니다.

새 백업을 만들려면 하나 이상의 확인란을 선택해야 합니다. `백업 만들기` 버튼을 클릭하면, 백업에 필요한 파일이 수집되어 아카이브로 통합됩니다. 몇 분 후에 백업에 포함된 내용에 따라 새 백업이 목록에 나타납니다. 백업 프로세스의 끝 부분에는 상자 위에 나타나는 노란색 설명선이 표시되며 *백업이 성공적으로 완료되었다*는 메시지가 표시됩니다.

> **참고:** USB 스틱의 백업은 /mnt/usbstick/efw-backups 디렉토리에 저장됩니다. USB 스틱에 저장된 백업의 경우, /var/backups/ 디렉토리 아래에 symlink가 생성됩니다.

백업 파일의 형식과 이름.

백업 파일은 표준 Linux의 tar 및 gzip 도구를 사용하여 **tar.gz** 아카이브로 생성됩니다. 아카이브에 저장된 파일은 **tar zxf archivename.tar.gz** 또는 **tar vzxf archivename.tar.gz**를 사용하여 처리 및 압축 해제된 모든 파일을 볼 수 있으며, 화면에서 *v* 옵션의 자세한(*verbose)* 정보를 나타내는 일부 유익한 메시지를 볼 수 있습니다. 백업 파일의 이름은 고유하도록 만들어지며 내용에 대해 가능한 최대 정보를 전달하므로 예를 들어, **backup-20130208093337-myappliance.mydomain-settings-db-logs-logarchive.tar.gz**와 같이 긴 문자열이 될 수 있습니다. 이 백업 파일에서 *20130208093337*은 YYYYMMDDHHMMSS 형식으로 백업 생성의 타임 스탬프입니다. 이 예는 2013년 2월 8일 오전 9:33:37을 표시하는 것입니다. 이 옵션을 사용하면 가장 오래된 백업부터 가장 최근의 백업까지 사전 편집 순으로 백업을 정렬할 수 있습니다. *myappliance.mydomain*은 네트워크 구성 (*Menubar ‣ System ‣ Network configuration*)의 3단계에서 설정한 Endian UTM Appliance의 호스트 이름 및 도메인 이름이며, *settings-db-logs-logarchive*는 백업 내용을 나타냅니다. 이 경우에, 네 부분이 모두 이름으로 나타나기 때문에 전체 백업입니다. 예를 들어, 설정 및 로그만 포함하는 백업은 문자열 *설정-로그*로 식별됩니다.

백업 아카이브 암호화

페이지의 두 번째 상자는 GPG 공개 키를 제공하여 이후의 모든 백업을 암호화할 수 있습니다. 다음 옵션을 사용할 수 있습니다.

Encrypt backup archives (백업 아카이브 암호화)

아카이브를 암호화해야 한다면 체크 박스를 선택하십시오. 이 옵션은 수동 및 예약 백업 모두에 적용됩니다.

Import GPG public key (GPG 공개 키 가져 오기):

찾아보기... (또는 Chrome 브라우저에서 파일 선택...) 버튼을 클릭하여 로컬 파일 시스템에서 키 파일을 업로드하여 GPG 공개 키를 선택하십시오.

키가 업로드되고 백업 아카이브 암호화(*Encrypt backup archives*) 옵션이 선택되면 키에 대한 정보가 다음 예제와 같이 옵션 위에 표시됩니다.

다음 GPG 공개 키가 백업 아카이브를 암호화하는 데 사용됩니다.

```
pub     1024R/00000000 2010-10-10 [expires: 2020-10-09]
        Key fingerprint = 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
uid                    Jane Doe <j.doe@example.org>
sub     1024R/00000001 2010-10-10 [expires: 2020-10-10]
```

> **힌트:** 핫스팟의 사용자 데이터 및 청구 정보와 같이 의미있는 데이터가 포함되어있을 때마다 백업 아카이브를 암호화하는 것이 좋습니다.

백업 아카이브 가져 오기

페이지의 세 번째 상자는 로컬 워크 스테이션에서 Endian UTM Appliance로 백업을 가져올 수 있습니다.

찾아보기...

백업 파일은 이 버튼을 클릭하여 선택할 수 있습니다. 로컬 파일 시스템에서 백업 파일을 선택하는 팝업 창이 열립니다.

비고 Remark

이 필드는 가져온 백업에 대한 사용자 정의 설명을 작성하는데 사용될 수 있습니다.

마지막으로 가져오기 버튼을 클릭하여 백업을 업로드합니다. 백업은 페이지 상단의 백업 목록에 나타나며, 복원 아이콘  을 클릭하여 복원할 수 있습니다.

> **참고:** Endian UTM Appliance에서는 암호화된 백업을 가져올 수 없습니다: 모든 암호화된 백업은 업로드 되기 전에 복호화해야 합니다.

구성을 공장 기본값으로 재설정하고 재부팅하기

네 번째 상자는 지금까지 설정된 모든 구성 및 설정값을 지우고 기본 구성으로 시스템을 재부팅합니다. 이 결과는 사용 가능한 유일한 옵션을 클릭하여 달성할 수 있습니다.

공장 기본값

이 버튼을 클릭하면 **공장 기본** 프로세스가 시작됩니다. 현재 설정의 백업 사본이 생성되고 Endian UTM Appliance가 재부팅 된 후 즉시 기본 IP 주소인 **192.168.0.15**를 포함하여 공장 기본값으로 복원됩니다.

> **참고:** 잠재적으로 이것은 매우 위험한 옵션이므로, 팝업 창은 프로세스를 시작하기 전에 확인을 요청합니다. 확인(OK)을 클릭하면, 프로세스가 시작되고 중단될 수 없습니다.

예약된 백업

시스템의 자동 백업은 *예약된 자동 백업*과 *이메일로 백업 보내기*라는 두 개의 상자가 포함된 *예약된 백업* 탭에서 활성화 및 환경설정을 할 수 있습니다.

예약된 자동 백업

첫 번째 상자에서, 자동 백업이 활성화되고 구성됩니다. 백업에 포함될 Endian UTM Appliance의 구성요소들이 다른 탭에 있는 백업 세트 상자에서 보이는 것과 같이 선택될 수 있습니다. 유일한 차이점은 예약된 백업에 대한 설명을 지정할 가능성이 없다는 것입니다. 추가 옵션은 다음과 같습니다

활성화 (Enabled)

예약된 백업을 활성화합니다.

아카이브의 # 유지 (Keep # of archives)

얼마나 많은 백업을 Endian UTM Appliance에 유지하기 위해 드롭-다운에서 선택합니다. (2에서 10까지, 그러나 이 공간을 절약하기 위해 내보낼 수 있습니다).

자동 백업 예약 (Schedule for automatic backups)

시간별, 일별, 주별 또는 월별 백업들 간의 빈도입니다.

예약된 백업은 항상 Endian UTM Appliance에 저장됩니다.

이메일을 통해 백업 보내기

두 번째 상자에서는 백업을 전자 메일로 보내도록 시스템을 구성할 수 있습니다. 다음 옵션들을 사용할 수 있습니다.

활성화 (Enabled)

백업 아카이브를 전자 메일로 보낼 수 있습니다.

수신자의 이메일 주소 (email address of recipient)

백업과 함께 전자 메일을 보낼 전자 메일 주소입니다.

발신자의 이메일 주소 (email address of sender)

보낸 사람의 전자 메일 주소로 표시되는 전자 메일 주소로 특수 주소 (예: backups@myappliance.mydomain)에서 백업이 전송된 것으로 보이는 경우에 유용하며, 도메인 또는 호스트명을 DNS가 해석할 수 없는 경우 제공해야 하는 전자 메일 주소입니다.

사용할 스마트 호스트 주소 (Address of smarthost to be used)

보내는 전자 메일을 Endian UTM Appliance에서 직접 보내지 않고 다른 SMTP 서버에서 보내는 경우 필요한 전자 메일을 보내는데 사용되는 스마트 호스트의 주소입니다.

> **참고:** smarthost의 명시 적 주소는 SMTP 프록시 (Menubar -> Proxy -> SMTP)가 비활성화 된 경우 필요합니다.

즉시 백업 보내기

이 버튼을 클릭하면 설정이 저장되고 즉시 백업 아카이브를 첨부 파일로 첨부하여 전자 메일을 보내려고 합니다.
이 작업은 또한 제공된 데이터의 정확성을 테스트하는데도 사용됩니다 (필요한 경우 이메일 주소 및 스마트호스트).

참고사항: USB 스틱에 백업을 생성하는 방법을 참고하십시오.

종료

이 페이지에서는 각각 종료(Shutdown) 또는 재부팅(Reboot) 버튼을 클릭하여 Endian UTM Appliance를 종료하거나 재부팅할 수 있습니다.

> **경고:** 추가 확인 요청없이, 해당 버튼을 클릭하면 즉시 종료 또는 재부팅 프로세스가 시작됩니다.

다시 부팅 한 후에는, 새 인증없이 GUI를 계속 사용할 수 있습니다.

라이센스 계약

이 섹션에는 Endian과 Endian UTM Appliance 소유자 간의 사용권 계약이 표시됩니다.

> **참고:** 업그레이드 후, 라이센스 계약이 변경되면, 처음 로그인할 때 업그레이드된 시스템에 액세스하고 Endian UTM Appliance를 사용하기 전에 새로운 라이센스 계약에 동의해야 합니다.

상태메뉴(The Status Menu)

상태 메뉴는 Endian UTM Appliance에서 실행되는 다양한 데몬 및 서비스에 대한 텍스트 및 그래픽 보기의 정보를 표시하는 일련의 페이지를 제공합니다. 이 모듈에서는 Endian UTM Appliance의 현재 및 최근 상태만 보여주는 구성 옵션을 사용할 수 없습니다.

화면 왼쪽의 하위 메뉴에는 Endian UTM Appliance의 일부 기능에 대한 자세한 상태 정보를 제공하는 다음 항목이 나타납니다.

- 시스템 상태 - 서비스, 자원, 가동 시간, 커널
- 네트워크 상태 - 네트워크 인터페이스, 라우팅 테이블, ARP 캐시의 구성
- 시스템 그래프 - 리소스 사용량 그래프
- 트래픽 그래프 - 대역폭 사용량 그래프
- 프록시 그래프 - 최근 24 시간 (주, 월, 년)의 HTTP 프록시 액세스 통계 그래프
- 연결 - 열려있는 모든 TCP/IP 연결 목록
- OpenVPN 연결 - 모든 OpenVPN 연결 목록
- SMTP 메일 통계 - SMTP 서비스에 대한 그래프
- 메일 큐 - SMTP 서버의 메일 큐

시스템 상태

*메뉴 바 (Menubar) ‣ 상태(Status)*를 클릭하면 열리는 기본 페이지는 시스템 상태 (System status)페이지입니다. 이것은 실행중인 시스템에 대한 많은 일반 정보를 구조화된 상자 형태로 제공합니다. 페이지 상단에는 서비스, 메모리, 디스크 사용, 가동 시간 및 사용자, 로드된 모듈 및 커널 버전 등의 각각의 상자에 대한 하이퍼 링크가 있습니다. 보다 자세한 내용은 각 상자에 표시되는 정보로서 일반적으로 Linux 명령의 출력 형태입니다.

서비스

이 상자는 Endian UTM Appliance에 설치된 각 서비스의 상태를 **Stopped** 또는 **Running** 중 하나로 표시하고 각각의 빨간색 또는 녹색 사각형과 함께 표시합니다. 해당 데몬 또는 스크립트가 활성화 되지 않았기 때문에 서비스가 중지된 것으로 나타날 수 있습니다.

메모리

Linux **free** 명령의 출력은 여기에 표시된 데이터를 제공합니다. 모든 숫자는 메모리의 킬로바이트를 나타냅니다. 막대(bar)는 사용된 메모리의 시각화를 용이하게 합니다.

첫 번째 행은 총 사용된 RAM 메모리를 보여줍니다. Linux 커널은 사용 가능한 모든 RAM을 디스크 캐시로 사용하여 입출력(I/O) 작업 속도를 높이기 때문에 장시간 실행되는 시스템에서는 100%에 가깝게 나타나는 것이 정상입니다.

두 번째 행은 버퍼에서 사용되고 프로세스에 의해 캐시된 RAM의 양을 보여줍니다. 디스크 캐싱을 위해 일부 메모리를 사용할 수 있도록 하려면 이 값이 RAM의 80% 미만으로 유지하는 것이 이상적입니다.

마지막으로, 세 번째 행은 디스크에 있는 스왑 공간을 보여줍니다. 장시간 실행되는 시스템의 경우, 특히 모든 서비스가 항상 사용되는 것은 아니라면, 적당한 스왑 사용량을 (이 값은 20% 미만이어야 함) 보게 되는 것이 정상입니다.

사용된 **RAM**이 높고 Linux에서 새 프로세스를 시작할 때마다, 사용중인 메모리 부분이 버려지거나 스왑 공간으로 이동되어 해당 프로세스들에 필요한 RAM을 확보합니다. Linux 시스템이 거의 모든 RAM을 차지하는 것은 정상이지만, 오랜 기간 동안 전체 메모리 (RAM 및 스왑)를 많이 사용하면 Endian UTM Appliance에 문제가 있음을 나타낼 수 있습니다. 실제로 실행중인 프로세스가 너무 많은 메모리를 필요로 하고 모든 프로세스에 할당될 수 없으면, 시스템의 속도가 결국 느려지므로 RAM의 일부를 스왑 공간으로 이동하거나 그 반대로 이동하는데 많은 시간이 필요할 수 있습니다.

디스크 사용량

Linux **df** 명령의 출력은 디스크 장치, 즉, 물리적 디스크 및 파티션, 해당 마운트 지점 및 각 디스크 파티션의 공간을 표시합니다. 표시된 주 파티션은 다음과 같습니다.

- 메인 디스크
- 데이터 디스크
- 모든 Endian UTM Appliance 설정이 저장되는 구성 디스크
- 로그 디스크
- /dev/shm/ 및 /var/volatile와 같은 메모리 마운트 파일 시스템.

> **참고:** 데이터 디스크와 로그 디스크는 시간이 지남에 따라 커질 수 있으므로 그것들을 위한 충분한 공간을 확보해야 합니다 (특히 로그 디스크의 경우). 또한 95% 이상 가득 찬 디스크는 시스템의 올바른 작동을 방해할 수 있음을 기억하십시오. 예를 들어, 로그 파일을 더 이상 저장할 수 없거나 구성의 변경 사항을 실제로 디스크에 저장할 수 없습니다.

추가사항: 이 가이드의 채워진 파티션의 여유 공간을 위한 몇 가지 제안 사항이 있습니다.

가동시간과 사용자

이 상자는 현재 시간 (아래 예에서 15:21:38), 가동 시간 (6:18), 현재 시스템에 로그인 된 콘솔 사용자들의 수 (1명의 사용자) 및 지난 1, 5, 15 분 동안의 시스템 로드 평균 (0.03, 0.02, 0.00)를 보고하는 Linux **w** 명령의 출력을 표시합니다.

또한 콘솔 사용자가 시스템에 로그인 한 경우, 사용자 이름 (root), 사용자가 연결된 곳의 IP 주소 또는 호스트 이름 (192.168.1.97), 사용자가 실행시킨 명령어 (-bash)를 포함한 일부 정보는 아래쪽에 표시됩니다.

```
15:21:38  up  6:18,  0 users,  load average: 0.03,  0.02,  0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU  WHAT
root     pts/0    192.168.1.97     Tue18    7:57   0.54s  0.54s -bash
```

이 상자의 내용에 대한 자세한 내용은 ***w(1)*** 매뉴얼 페이지를 참조하십시오.

로드된 모듈

Linux **lsmod** 명령의 출력입니다. 현재 메모리에 로드된 커널 모듈을 보여줍니다. 이 정보는 고급 사용자에게만 유용합니다.

커널 버전

현재 Lunix **uname -r** 명령의 출력이며, 현재 커널 버전을 보여줍니다.

네트워크 상태

이 페이지에는 네트워크 인터페이스의 실행 상태에 대한 여러 정보가 들어 있습니다. 페이지에는 4개의 상자가 있으며, 시스템 상태와 마찬가지로 페이지 상단에 인터페이스, 현재 동적 임대, NIC 상태, 라우팅 테이블 항목 및 ARP 테이블 항목에 대한 빠른 접근을 위한 하이퍼링크가 제공됩니다.

보다 자세한 내용은 각 상자에 표시되는 정보로서 일반적으로 Linux 명령의 출력입니다.

인터페이스

첫 번째 상자는 각 네트워크 인터페이스에 연결된 MAC 주소, IP 주소 및 추가 통신 매개 변수를 제공하는 **ip addr show** 명령의 출력을 보고합니다. 활성 인터페이스는 서비스 중인 영역의 색상으로 강조 표시됩니다. 표시된 NIC는 이더넷 인터페이스 또는 브리지 중 하나이며, VLAN 및 연결된 네트워크 인터페

이스는 표시되지 않습니다.

현재 동적 임대

이 상자는 Endian UTM 어플라이언스의 DHCP 서버에 의해 할당된 모든 임대를 나열합니다. 각 항목에 대해 IP 주소와 MAC 주소, 정의된 경우 호스트 이름 및 임대 만료 날짜와 시간이 표시됩니다. 만료된 임대는 제외됩니다.

NIC 상태

각 NIC의 실행 구성 및 기능은 다음과 같습니다. 각 인터페이스는 서비스 중인 구역의 색상으로 강조 표시되고 작동 중임을 나타내기 위해 [Link OK (연결 확인)]로 표시됩니다. 사용되지 않는 인터페이스에는 [NO Link (연결 없음)]이라는 레이블이 붙어 있습니다. 출력을 제공하는 명령은 **ip link show**입니다.

라우팅 테이블 항목

route -n 명령에서 제공하는 커널 라우팅 테이블입니다. 일반적으로 Endian UTM 어플라이언스가 제공하는 구역 내에서 트래픽을 올바르게 라우팅하는 활성 인터페이스 당 하나의 라인과 트래픽이 인터넷에 도달할 수 있는 기본 경로가 (0.0.0.0 대상 필드에 의해 인식 가능) 있어야 합니다.

기본 게이트웨이의 경우 인터페이스 당 하나 이상의 항목이 있을 수 있습니다. 또는 한 로컬 네트워크의 일부 특수 호스트가 Endian UTM Appliance에서 직접 서비스하지 않는 다른 로컬 네트워크에 대한 게이트웨이 역할을 하는 경우에 사용할 수 있습니다.

ARP 테이블 항목

마지막 상자는 **arp -n** 명령의 출력을 보여주며, ARP 표, 즉 로컬 네트워크에서 각각의 알려진 IP 주소 (업링크의 원격 게이트웨이에 해당하는 IP주소 포함)와 연관된 MAC 주소를 포함하는 테이블을 표시합니다.

시스템 그래프

이 페이지에 표시된 그래프는 지난 24시간 동안 CPU, 메모리 및 스와핑의 세 가지 상자로 나누어져 자원 사용을 나타냅니다.

각 그래프는 범례에 설명된 색상을 사용하여 다양한 구성 요소를 강조 표시하고, 최대, 평균 및 현재 값의 요약을 보여줍니다.

그래프나 상자 중 하나를 클릭하면, 요일, 월 및 연도에 대한 개별적인 사용 그래프를 포함한 4개의 상

자가 있는 새 페이지가 열립니다. 이 페이지에서 페이지 하단의 뒤로 링크를 클릭하면 이전 페이지로 돌아갈 수 있습니다.

> **참고:** 요약에 때때로 표시되는 *nan* ("숫자가 아님(Not A Number)"의 준말인) 문자열은 선택한 자원의 사용을 계산하기에 충분한 데이터가 수집되지 않았음을 의미합니다. Endian UTM 어플라이언스를 불과 몇 주 동안 사용하였다면, 예를 들어 연간 사용량(Usage per Year) 그래프에 나타날 수 있습니다.

자세하게 살펴보자면, 메인 페이지에 있는 3개의 상자는 다음 정보를 표시합니다.

CPU 그래프

이 상자는 Endian UTM Appliance의 CPU 사용량을 프로세스 상태 별 CPU 시간 합계로 그룹화하여 보여줍니다. 각 상태를 나타내는 데 사용되는 색상은 다음과 같습니다.

- 백색 - 유휴, 즉 CPU가 어떤 프로세스에 의해서도 사용되지 않는 시간.
- 초록색 - 좋은 프로세스, 즉 기본 우선 순위가 변경된 사용자 프로세스
- 파란색 - 기본 우선 순위를 갖고 있는 사용자 프로세스
- 오렌지색 - I/O 작업이 완료될 때까지 CPU가 소비하는 시간입니다.
- 빨간색 – 시스템 (커널) 프로세스
- 분홍색 - softirq, 즉 소프트웨어 인터럽트에 소비된 시간
- 갈색 - 인터럽트, 즉 하드웨어 인터럽트에 소비된 시간입니다.
- 검정색 - 가상 머신으로 실행하는 경우에만 의미가 있는 것은 하이퍼바이저가 VM을 실행하는 데 사용된 시간입니다.

메모리 그래프

이 그래프는 RAM 메모리 사용을 보여줍니다. 다음 색상은 메모리를 나타내는 데 사용됩니다.

- 녹색 - 할당되지 않은 메모리로 새 프로세스에 할당될 수 있습니다.
- 파란색 - 캐시 메모리, 프로세스에서 사용하는 최근 데이터의 사본.
- 오렌지색 - 버퍼 메모리, 외부 장치에서 수신하거나 외부 장치로부터 수신할 데이터를 저장하는 임시 메모리 부분입니다.
- 빨간색 - 사용 메모리.

스왑 그래프

이 상자에는 하드 디스크에 있는 스왑 영역의 사용량이 표시됩니다. 사용된 색상은 다음과 같습니다.

- 녹색 - 할당되지 않은 교환.
- 블루 - 캐쉬 스왑.
- 빨간색 - 사용된 스왑 공간.

> 추가사항: 여기에 Linux 메모리 관리를 명확하게 설명하는 좋은 페이지가 있습니다 (이탈리아어로도 제공됩니다).

트래픽 그래프

이 페이지에는 구역 및 업링크로 나뉘어진 지난 24시간 동안의 트래픽 그래프를 표시하는 상자들이 있습니다. 따라서 사용 및 설정되는 구역에 따라 이 페이지는 대개 2 ~ 6개의 상자를 포함하며 각 상자에는 하나의 그래프가 포함됩니다. 시스템 그래프와 마찬가지로, 그래프에는 표시된 데이터의 범례가 수반됩니다.

- 녹색 - 나가는 트래픽.
- 파란색 - 들어오는 트래픽

그래프 아래에는 송수신된 데이터의 평균, 최대 및 현재 트래픽 양의 요약이 실시간으로 표시되고 업데이트됩니다.

그래프 중 하나를 클릭하면 마지막 날, 주, 월 및 연도의 해당 구역 또는 업링크를 통해 이동한 데이터의 요약과 함께 새 페이지가 열립니다.

> **힌트:** 모든 영역의 그래프가 표시된 페이지로 돌아가려면 페이지 하단의 BACK 하이퍼링크를 클릭하십시오.

프록시 그래프

지난 24시간 동안 HTTP 프록시의 액세스 통계가 여기에 표시됩니다. HTTP 프록시 서비스가 활성화되어 있지 않고 활성화된 적이 없는 경우, 이 페이지에는 그래프가 없습니다. 이 경우, 그래프 대신 상자에 *정보 없음*이라는 문자열이 표시됩니다.

그러나 작년에도 짧은 기간 동안 서비스가 실행 중이면 그래프를 클릭하여 생성된 데이터에 계속 액세스 할 수 있습니다. 다른 그래프와 마찬가지로 마지막 날, 주, 월 및 연도의 통계가 표시됩니다. 이 페이지에서 하단의 BACK 하이퍼 링크를 클릭하면 기본 페이지로 돌아갈 수 있습니다.

> **참고:** 프록시 그래프를 표시하려면, *로깅 사용 (Enable logging)* 확인란을 선택하여 *프록시 (Proxy) ‣ HTTP ‣ 구성(Configuration) ‣ 로그 설정(Log settings)*에서 HTTP 프록시 로깅을 활성화해야 합니다. 또한 더 자세한 로그와 그래프를 생성하기 위해 *쿼리된 용어(queried terms)*와 *사용자 에이전트(useragents)*를 기록할 수 있습니다.

HTTP 프록시가 활성화되면 네 개의 상자에 다음 데이터가 표시됩니다.

- *하루 총 트래픽*: Endian UTM Appliance의 프록시 서비스를 통해 이동한 데이터의 양입니다. 녹색은 나가는 트래픽을 나타내고 파란색은 들어오는 트래픽을 나타냅니다.
- *1 일 총 액세스 수*. Endian UTM Appliance에서 수신한 파란색으로 표시된 HTTP 요청 수.
- 캐시 히트 하루. 요청된 캐시 데이터의 수.
- 캐시 히트 비율은 하루에 5분 이상. 5분 동안 요청된 캐시 데이터 수입니다.

연결(Connections)

이 페이지는 Endian UTM Appliance으로 들어오고 나가는 현재 연결 목록을 포함하는 표를 보여줍니다. 여기에 표시된 데이터는 커널 컨트랙트 테이블에 의해 고안되었습니다. 다음 색상이 테이블에서 사용되며 테이블의 셀 배경으로 사용되어 연결 원본과 대상을 나타냅니다.

- 녹색, 빨간색, 오렌지색 및 파란색은 Endian UTM Appliance가 관리하는 구역입니다.
- 검은색은 SSH 또는 웹 액세스와 같은 데몬 및 서비스를 포함하여 방화벽과 관련된 연결에 사용됩니다.
- 자주색은 VPN 또는 IPsec을 사용하여 연결을 표시합니다.

표에 표시된 데이터는 다음과 같습니다.

Source IP

연결이 시작된 IP 주소입니다.

Source port

연결이 시작된 포트입니다.

Destination IP

연결 대상 IP입니다.

Destination port

연결 대상 포트입니다.

Protocol

연결에 사용되는 프로토콜로, 일반적으로 tcp 또는 udp입니다.

Status

TCP 연결에만 의미가 있는 연결의 현재 상태입니다. 이들은 RFC 793에 정의되어 있으며, 중요한 상태는 *ESTABLISHED* (연결이 활성화되어 있음), *TIME_WAIT* (연결이 닫힘), *CLOSE* (연결되지 않음)입니다.

Expires

특정 상태에서 연결이 얼마나 오래 유지되는지를 나타냅니다.

> **참고:** 페이지는 5초마다 자동으로 새로 고침됩니다.

각 IP 주소와 테이블의 각 IP 포트를 클릭하면 유용한 정보를 얻을 수 있습니다 .

IP 주소를 클릭하면 IP 주소 및 IP 주소에 대한 다양한 정보를 표시하는 whois 쿼리가 실행됩니다.

포트 번호를 클릭하면 인터넷 스톰센터 웹 페이지가 열리고, 여기는 포트 (예: 사용 목적) 및 해당 포트를 악용할 수 있는 서비스 또는 멀웨어 (예: 트로이 목마, 바이러스)에 대한 정보와 전 세계 여러 서버에서 해당 포트에서 받은 공격 수를 보여줍니다.

VPN 연결

Endian UTM Appliance에 OpenVPN 또는 IPsec 서버가 실행 중일 때, 이 페이지에는 연결된 사용자들과 함께 그것들이 연결에 사용되는 서비스 (OpenVPN, L2TP, IPsec Xauth), 그것들이 연결되어 있는 시간 스탬프를 보여주며, 가능한 조치들이 수행될 수 있습니다. 현재 사용 가능한 유일한 조치는 사용자의 연결을 끊는 것입니다.

SMTP 메일 통계

이 페이지에는 네 개의 상자가 보이며, 현재 요일, 주, 월 및 연도의 Endian UTM Appliance에서 로컬 SMTP 서버가 보낸 전자 메일에 대한 그래프를 보여줍니다.

> **참고:** SMTP 그래프는 너무 많은 리소스가 필요하기 때문에 Mini Appliance에서 재현되지 않습니다.

프록시 그래프의 경우와 마찬가지로 SMTP 프록시를 사용하도록 설정하지 않은 경우, 그래프 대신 정보 없음 (No information available) 문자열이 표시됩니다.

각 상자에는 y-축에 분당 전자 메일 수가 나타나고 x-축에 그래프의 유형에 따라 측정 단위가 변경되는 두 그래프가 들어 있습니다: (*일 그래프(Day graphs)에서 2시간, 주 그래프(week graphs)*에서 하루, *월 그래프(Month graphs)* 일주일, *연도 그래프(Year graphs)*에서 한달)

상단의 그래프는 Endian UTM Appliance가 보내거나 (파란색) 받기 (녹색)를 한 분당 메시지 수의 요약을 보여줍니다.

하단의 그래프는 거절된 (빨간색) 전자 메일 또는 되돌아온 (검은색) 전자 메일을 표시하기 때문에 다른 그래프의 보다 세분화된 버전으로 볼 수 있습니다. 그것들이 바이러스 (노란색)를 포함하고 있고, 스팸 (회색)으로 인식되기 때문에 가로채기가 되었던 것입니다.

각 그래프 아래에는 처리된 전자 메일 ("msgs")의 총 수, 평균 및 최대 수에 대한 각각의 전자 메일 범주 (전송, 수신, 거부, 반송, 바이러스 및 스팸)에 관한 텍스트 정보가 있으며, 추가로 페이지에 대한 최신 업데이트의 타임 스탬프 (날짜 및 시간)가 포함됩니다.

> **참고:** 요약에 때때로 표시되는 "숫자가 아님"문자열 인 "nan"은 선택한 자원의 사용을 계산하기에 충분한 데이터가 수집되지 않았 음을 의미합니다.

메일 큐

SMTP 프록시를 사용하면, 이 페이지에 현재 전자 메일 큐가 표시됩니다. 대기열에 전자 메일이 없으면, 메일 대기열이 비어 있습니다(Mail queue is empty) 라는 메시지가 표시되지만 일부 전자 메일이 있는 경우, `플러시 메일 큐` 버튼을 클릭함으로써 큐를 플러싱 (즉, 큐 내의 이메일을 즉시 송신)하는 것이 가능합니다.

SMTP 프록시를 사용하지 않으면, *SMTP 프록시가 현재 비활성화되어 있습니다. 따라서 어떠한 정보도 제공되지 않습니다* 라는 메시지가 표시됩니다.

네트워크 메뉴

네트워크 메뉴는 특정 호스트 및 경로를 추가하거나 업링크를 구성하고 VLAN을 추가하여 네트워킹 구성을 조정하는데 사용할 수 있습니다. 이 메뉴를 인터페이스, 구역을 구성하고 업링크를 정의할 수 있는 *메뉴바 (Menubar) ‣ 시스템 (System) ‣ 네트워크 구성 (Network Configuration)*에서 사용할 수 있는 **네트워크 구성** 마법사와 혼동하면 안됩니다. 특히 **인터페이스** 메뉴 항목의 많은 설정과 구성 옵션들이 거기에 있는 것들과 동일합니다.

화면 왼쪽의 하위 메뉴에는 다음 항목이 포함되어 있으며 각 항목에는 여러 가지 구성 옵션이 그룹화되어 있습니다.

- 호스트 편집 - 로컬 도메인 이름 해석을 위한 호스트를 정의하십시오.
- 라우팅 - 고정 경로 및 정책 라우팅을 설정합니다.
- 인터페이스 - 업링크를 편집하거나 VLAN을 생성합니다.
- 무선 - 무선 네트워크 연결을 설정합니다.

호스트 수정

이 페이지에는 **시스템 서비스를 위한 호스트**, 그 호스트들이 올바르게 작동되어야 하기 때문에 HTTP 프록시와 같은 일부 서비스가 사용 가능해졌을 때, Endian UTM Appliance에 의해 자동으로 추가되는 호스트들을 보여주는 테이블 위에 사용자 정의된 호스트에 대한 테이블이 있는 두 개의 테이블들이 있습니다 .

두개의 테이블들은 동일한 구조와 내용을 공유합니다. 각 항목은 그것들이 지정되어 있다면 IP 주소, 관련 호스트 이름 및 도메인 이름을 포함합니다. 유일한 차이점은 **시스템 서비스를 위한 호스트**를 편집할 수 없으므로 첫 번째 테이블의 각 항목에 대해 세 가지 사용 가능한 작업을 사용할 수 있다는 것입니다.

- ☑ ☐선택되면 그것을 활성화하거나 비활성화합니다.
- 수정합니다.
- 삭제합니다.

> **경고:** 작은 (삭제) 아이콘을 클릭하여 호스트 항목을 삭제해도 확인이 필요없고 되돌릴 수 없습니다. 실수로 삭제한 경우 수동으로 항목을 다시 추가해야 합니다.

테이블 바로 위에 새 호스트 추가 링크를 클릭하여 파일의 새 항목을 추가할 수 있습니다.

힌트: 새로운 항목은 /etc/hosts 파일에 추가되므로 수동으로 해당 파일을 편집하지 마십시오 귀하의 변

경 사항은 다음 변경 사항에 의해 덮어쓰여 질 것입니다.

다음 옵션을 입력하기 위해 간단한 양식이 표를 대체합니다.

IP 주소(IP address)

원격 호스트의 IP 주소.

호스트 이름(Hostname)

IP 주소와 연관된 호스트 이름.

도메인 이름(Domain name)

선택적인 도메인 이름. 지정하지 않으면 Endian UTM Appliance의 기본 도메인 이름이 사용됩니다.

> **힌트:** 도메인 이름은 아래의 *시스템 서비스를 위한 호스트* 테이블에 표시되며 **hostname -d** 명령을 사용하여 CLI에서 검색할 수 있습니다.

설명(Remark)

선택적 호스트 설명.

활성화(Enabled)

호스트를 사용하려면 확인란을 선택하십시오. 활성화하지 않으면, 사용할 수 없습니다.

> **참고:** 표준 Linux 시스템과 달리 /etc/hosts 파일 (아래 참조)에서 각 IP 주소는 하나의 호스트 이름에 해당하며 그 반대도 마찬가지입니다. 동일한 IP 주소에 더 많은 호스트 이름을 연결하려면 동일한 IP 주소이지만 다른 이름을 삽입하여 절차를 반복하십시오.

선택 사항은 추가 버튼을 클릭하면 확인할 수 있습니다. 그러면 녹색 설명 선에서 적용 버튼을 클릭하면 데몬이 새 호스트로 다시로드됩니다.

첫 번째 테이블 아래의 드롭 다운 메뉴를 사용하면 테이블에 정의된 여러 호스트에서 동일한 작업을 실행할 수 있습니다.

액션 선택

테이블의 첫 번째 열에 있는 작은 확인란을 클릭하여 하나 이상의 호스트를 선택한 후, 이 버튼을 클릭하면 선택한 모든 호스트에서 수행할 작업을 선택할 수 있습니다.

페이지 하단에는 시스템 서비스에 의해 자동으로 생성된 호스트도 표시됩니다. 이 호스트는 서비스가

올바르게 작동하도록 정의되어야 하며 수동으로 수정할 수 없습니다.

dnsmasq, /etc/hosts 파일 및 그 내용에 대한 간략한 소개와 자동으로 추가된 항목의 일부 예가 여기에 설명되어 있습니다.

호스트 관리, dnsmasq 및 /etc/hosts

dnsmasq 응용프로그램은 소규모 네트워크에서 로컬 호스트의 DNS 서버로 사용되며, 전 세계 DNS 서버의 DNS 전달자 및 캐싱 서버로 사용됩니다. Endian UTM Appliance는 dnsmasq를 사용하여 GREEN, ORANGE 및 BLUE 구역에서 오는 DNS 요청을 올바르게 해석하고 응답할 수 있습니다. 경우에 따라 원격 웹 사이트의 테스트 목적으로 dnsmasq의 일부 항목을 무시하거나 로컬 클라이언트가 연결할 수 있도록 dnsmasq의 캐시에 일부 로컬 서버를 추가하는 것이 바람직합니다.

이 페이지에 나열된 사용자 및 시스템 호스트는 모두 데몬이 다시 시작될 때마다 /etc/hosts 파일에 저장됩니다. CLI를 통해 해당 파일에 직접 추가된 호스트는 Endian UTM Appliance를 재부팅하거나 dnsmasq를 다시 시작한 후에도 유지되지 않습니다.

/etc/hosts 파일에는 정적 검색 테이블이라는 형식이 있습니다.

```
IP1 호스트이름1 [호스트이름2]
IP2 호스트이름3 [호스트이름4] [호스트이름5]
```

여기서 IP1 및 IP2는 고유한 (숫자) IP 주소이며 hostname1, hostname2, hostname3, hostname4 및 hostname5는 해당 IP에 지정된 사용자 정의 이름입니다. 대괄호 안의 이름은 선택 사항입니다. 즉, 각 IP 주소는 알려진 호스트의 하나 이상의 이름과 연관될 수 있습니다. 사용자 지정 호스트 항목을 파일에 추가할 수 있으며 Endian UTM Appliance를 통해 연결하는 모든 클라이언트에 대해 확인됩니다. 일반적인 Endian UTM Appliance에서 / etc / hosts 파일에는 최소한 다음 항목이 포함되어 있습니다.

```
127.0.0.1       localhost.localhost localhost
172.20.0.21     myappliance.localdomain myappliance
172.20.0.21     spam.spam spam
172.20.0.21     ham.ham         ham
172.20.0.21     wpad.localdomain wpad
```

127.0.0.1은 루프백 장치의 localhost IP 주소입니다. 이 호스트는 모든 Linux 시스템의 올바른 작동을 위한 필수 항목입니다. 172.20.0.21은 GREEN 인터페이스의 IP 주소입니다. 해당 IP를 위해 나열된 항목들의 의미와 용도는 다음과 같습니다.

myappliance.localdomain

네트워크 구성 중에 설정된 Endian UTM Appliance의 호스트 이름과 도메인 이름입니다.

spam.spam spam 및 ham.ham ham

이 두 항목을 결합하여 spamassassin 전자 메일 필터를 학습시키는데 사용됩니다.

wpad.localdomain wpad

프록시가 투명하지 않을 때, 사용자의 상호 작용없이 프록시 설정을 자동으로 감지하고 적용하는 브라우저입니다.

라우팅

*메뉴바 (Menubar) ‣ 상태 (Status) ‣ 네트워크 상태 (Network Status)*에서 볼 수 있는 기본 라우팅 테이블 외에도 정적 및 정책 라우팅 규칙을 사용하여 Endian UTM Appliance의 라우팅을 향상시킬 수 있습니다. 이 페이지에는 추가된 모든 사용자 정의 규칙을 포함하는 고유 테이블이 표시됩니다. 그러나 정적 및 정책 라우팅 규칙에는 다양한 옵션과 설정이 있으므로, *정적 라우팅*과 *정책 라우팅*의 두 가지 탭으로 구성됩니다.

정적 라우팅과 정책 라우팅의 주요 차이점은 전자가 (정적) 게이트웨이를 통해 소스 네트워크 또는 대상 네트워크로 모든 트래픽을 라우팅하는 반면 후자는 트래픽의 소스 및 대상과 게이트웨이 유형을 정의하는데 더 많은 선택권을 제공합니다. 또한 추가 옵션은 트래픽과 서비스 유형(TOS)을 생성하는 서비스를 선택할 수 있게 해줍니다. 이러한 이유로, 정책 라우팅 규칙을 정의할 때는 규칙의 순서가 중요합니다.

라우팅 테이블에서 변경이 수행될 때마다 변경 사항을 저장하고 서비스를 다시 시작해야 합니다.

정적 라우팅

규칙이 정의되지 않다면, 이 페이지는 비어 있습니다. 그렇지 않으면, **현재 라우팅 항목**이라는 테이블이 표시되며, 여기에는 소스 및 대상 네트워크 또는 구역, 게이트웨이, 설명 및 사용 가능한 작업 목록에 대한 정보들이 포함됩니다.

- ☑ ☐ On 또는 Off를 사용하여 활성화 또는 비활성화할 수 있습니다.
- 편집 아이콘으로 수정할 수 있습니다.

- 삭제 아이콘으로 삭제할 수 있습니다.

정적 경로는 특정 소스 및 대상 네트워크를 지정된 게이트웨이 또는 업링크와 연관시킬 수 있습니다. 표 위의 `새 경로 추가` 링크를 클릭하면 나타나는 양식에 다음 필드를 정의하여 새 경로를 만들 수 있습니다.

소스 네트워크 (Source Network)

소스 네트워크 (CIDR 표기법).

대상 네트워크 (Destination Network)

대상 네트워크 (CIDR 표기법).

> **힌트:** 단일 소스 또는 대상 호스트를 지정하려면, **/32** 접미사 (예: **192.168.100.1/32**)를 사용하십시오.

경유 경로 (Route Via)

네가지 옵션들은 Static Gateway, Uplink, OpenVPN User 또는 L2TP User라는 트래픽을 전송해야 하는지를 정의하는데 사용할 수 있습니다. 정적 게이트웨이를 선택한 경우, 오른쪽 텍스트 상자에 게이트웨이의 IP 주소를 입력해야 합니다. 그렇지 않으면 드롭 다운에서 업링크, OpenVPN 사용자 또는 L2TP 사용자 중에서 사용 가능한 선택 항목을 제공합니다.

활성화

체크 표시가 된 체크 박스는 규칙이 활성화되어 있음을 의미합니다. 그렇지 않으면 규칙만 생성되고 나중에 활성화할 수 있습니다.

설명

이 규칙의 목적을 설명하는 발언이나 의견.

기본 고정 경로를 설정하는 가이드도 참조하십시오.

정책 라우팅

정책 경로 규칙은 특정 네트워크 주소, 구역 또는 서비스 (포트 및 프로토콜로 표시됨)를 특정 업링크와 연관시킬 수 있습니다.

표에는 정적 라우팅과 정책 라우팅 모두에 대해 이미 정의된 모든 규칙이 나와 있습니다. 실제로 정적 라우팅 규칙은 고정 소스에서 고정 대상 네트워크로 정적 호스트를 통해 라우팅된 전체 트래픽에 대한 정책 라우팅 규칙으로 볼 수 있습니다.

이 표에는 정적 라우팅의 해당 테이블보다 많은 속성이 표시됩니다. 즉, 원본 및 대상 네트워크, TOS (서비스 유형), 게이트웨이, 서비스, 설명 및 사용 가능한 작업 등입니다.

- ⬆⬇: 규칙을 위로 또는 아래로 이동
- ☑☐: 규칙을 활성화 또는 비활성화
- ✎: 편집 아이콘을 이용해 규칙을 수정
- 🗑: 규칙을 삭제합니다.

앞에서 언급했듯이, 테이블에서 더 높은 순위로 나타나는 규칙은 더 높은 우선 순위를 갖습니다. 즉, 먼저 평가됩니다.

정책 라우팅 규칙 만들기 링크를 클릭하면, 양식이 열리며, 이는 방화벽 규칙 편집기와 매우 유사합니다. 이 편집기는 규칙 정의를 보다 잘 제어할 수 있으며, 규칙 설정은 규칙 생성에 도움이 되는 여러 드롭 다운 메뉴로 안내합니다.

다음 옵션을 사용할 수 있습니다.

소스

첫 번째 드롭 다운 메뉴에서 트래픽 소스를 선택할 수 있습니다. 한 줄에 하나씩 더 많은 항목이 허용되지만 모든 항목은 동일한 유형 (구역 또는 인터페이스, OpenVPN 또는 L2TP 사용자, IP 또는 네트워크 또는 MAC 주소)에 속해야 합니다. 선택에 따라, 다른 값이 제공되어야 합니다. 모든 소스에 규칙을 적용하려면, <ANY>를 선택하십시오.

대상

두 번째 드롭 다운 메뉴에서는 IP, 네트워크, OpenVPN 또는 L2TP 사용자들을 목록의 형태로 트래픽 대상을 선택할 수 있습니다. 다시, <ANY>를 선택하면, 규칙이 모든 대상과 일치하게 됩니다.

서비스/포트

다음 두 개의 드롭 다운 메뉴는 TCP, UDP 또는 TCP + UDP 프로토콜을 선택한 경우 규칙에 대한 서비스, 프로토콜 및 대상 포트를 지정할 수 있게 해줍니다. HTTP/TCP/80, <ALL>/TCP+UDP/0:65535 또는 모든 서비스, 프로토콜 및 포트의 바로가기(shortcut)인 <ANY>와 같이 미리 정의된 *서비스/프로토콜/포트* 조합이 있습니다. 사용자 정의 프로토콜 및 차단할 포트를 지정할 수 있는 *사용자 정의된(User defined)* 허가가 있으며, 옵션은 표준 포트와 다른 포트들에서 서비스를 실행할 때 유용합니다.

프로토콜

TCP, UDP, TCP + UDP, ESP, GRE 및 ICMP와 같은 트래픽 유형은 규칙에 의해 관심받게 되는 프로토콜들입니다 TCP와 UDP가 가장 많이 사용되고, GRE (일반 라우팅 캡슐화, Generic Routing Encapsulation)는 **ping** 및 **traceroute** 명령에 의해 터널, ESP (보안 페이로드 캡슐화, Encapsulating Security Payloads) by IPsec 및 ICMP (망간 제어 메시지 프로토콜, Internet Control Message Protocol)에서 사용됩니다.

경유 경로 (Route Via)

이 규칙에 따라 트래픽을 라우팅하는 방법입니다. 네 가지 옵션을 사용할 수 있습니다.

1. 정적 게이트웨이: 이 경우 IP 주소가 제공됩니다.
2. 업링크: 업링크는 이 규칙을 위해서 사용해야 합니다. 업링크가 이용 불가능하게 될 때, 라우팅이 선택된 업링크에 대응하는 백업 링크로까지 계속 이어질 수 있는 옵션이 있습니다. 이 옵션은 드롭 다운 메뉴 옆에 있는 확인란이 선택된 경우에 활성화됩니다.
3. OpenVPN 사용자: 드롭 다운 메뉴에서 사용할 수 있는 OpenVPN 사용자입니다.
4. L2TP 사용자: 드롭 다운 메뉴에서 사용할 수 있는 L2TP 사용자들 중에서 선택합니다.

서비스 유형

여기서 서비스 유형 (TOS)을 선택할 수 있습니다. 해당 규칙에 의해 관심이 있는 트래픽의 가장 중요한 특성 (*기본값, 저지연(lowdelay), 신뢰성 또는 처리량*)이 무엇인가에 따라 네 가지 값을 선택할 수 있습니다.

설명

이 규칙의 목적을 설명하는 설명문이나 의견입니다.

위치

규칙을 삽입할 위치 (규칙 목록의 상대 위치)입니다.

활성화

규칙을 사용하려면 이 확인란을 선택하십시오 (기본값). 이 옵션을 선택하지 않으면, 규칙이 생성되지만 활성화되지는 않습니다. 나중에 규칙을 활성화할 수 있습니다.

허용된 모든 패킷 기록

이 규칙의 영향을 받는 모든 패킷을 기록하려면 이 확인란을 선택해야 합니다.

> **경고:** 이 옵션을 활성화하면 로그 파일의 크기가 크게 증가할 수 있습니다.

Create Rule (규칙 작성)을 클릭하면 규칙이 저장되고, 라우팅 규칙이 새 항목으로 다시 로드되며, 녹색 설명선에 있는 Apply (적용) 버튼을 클릭합니다.

> **추가 참고사항:** 여기에 사용할 수 있는 기본 정책 경로를 설정하는 자습서가 있습니다.

인터페이스

업링크 관리자는 업링크 및 인터페이스와 관련된 여러 작업을 수행할 수 있으며, 특히 네트워크 인터페이스에서 사용자 정의 VLAN을 정의할 수 있습니다.

업링크 편집기

기본적으로 업링크 편집기는 마지막 열의 *Actions* 아이콘을 클릭하여 생성된 사용 가능한 업링크 및 각 링크에서 실행할 수 있는 작업을 표시합니다.

- ☑☐: 항목의 상태를 토글합니다 (활성화 또는 비활성화).
- : 항목의 속성을 수정합니다. • : 항목을 삭제합니다

> **참고:** 기본 업링크를 삭제할 수 없습니다. 따라서 삭제 아이콘이 없습니다.

추가 업링크는 업링크 목록 위의 업링크 생성 하이퍼링크를 클릭하여 정의할 수 있습니다. 열리는 페이지에서, 선택한 업링크 유형에 따라 사용 가능한 설정이 달라집니다.

여기의 업링크 구성 옵션의 대부분은 네트워크 구성 마법사와 동일하며 선택한 업링크 유형에 따라 다르므로 사용 가능한 모든 옵션이 여기에 설명되어 있지는 않습니다. 각 옵션에 대한 자세한 설명은 해당 섹션을 참조하십시오.

이 섹션에서는 하나의 추가 업링크 유형인 **PPTP**를 정의할 수 있습니다. 이 업링크의 경우 다음 값을 사용할 수 있습니다.

PPTP 방법

이것은 PPTP가 정적 모드에서 작동하는지 아니면 DHCP모드에서 작동해야 하는지를 결정합니다.

IP 주소, 넷마스크

정적 방법을 선택한 경우, 이 두 텍스트 필드에 필요한 값을 씁니다.

추가 주소 추가

이 확인란을 선택하면, 추가적인 IP 주소/넷마스크 또는 IP 주소/CIDR 조합을 아래에 있는 텍스트 영역에 추가할 수 있습니다.

다음 세 가지 옵션은 필수는 아니지만 공급자의 설정에 따라, 일부 구성이 작동하는데 필요할 수 있습니다.

전화 번호

PPTP 연결을 설정하는데 사용되는 전화번호입니다.

사용자 이름

PPTP 인증의 사용자 이름입니다.

암호

PPTP 인증의 사용자 이름입니다.

인증 방법

ISP에 따라, 이 값은 PAP 또는 CHAP이 될 수 있습니다. 확실하지 않은 경우, 기본값인 **PAP 또는 CHAP**를 유지하십시오.

기본 게이트웨이

PPTP 연결에 사용되는 게이트웨이의 IP 주소입니다.

선택한 모든 업링크 유형에 사용할 수 있는 나머지 옵션들은 다음과 같습니다.

설명(Description)

업링크에 대한 설명.

네트워크 모드

업링크가 작동할 모드. *라우팅 (Routed), 브리지 (Bridged) 및 업링크 없음 (No uplink)* 중에서 선택합니다.

업링크 유형

드롭 다운 메뉴에서 사용 가능한 업링크 유형을 선택하십시오.

> **참고:** 이동 광대역 또는 아날로그 모뎀을 선택할 때, Endian UTM Appliance가 켜지면 SIM 카드를 연결해야 합니다.

업링크가 사용 설정됨

업링크를 활성화하려면, 이 확인란을 선택하십시오.

부팅시 업링크 활성화

이 체크 박스는 부팅시에 업링크를 활성화해야 하는지 여부를 지정합니다. 이 옵션은 관리되지만 부팅 절차 중에 시작할 필요가 없는 백업 업링크에 유용합니다.

업링크는 시스템에 의해 자동 관리됩니다.

업링크를 관리하려면, 이 체크 박스를 선택하십시오. 관리 모드와 수동 모드에 대한 설명은 *Menubar ‣ System ‣ Dashboard*의 업링크 정보 플러그인 (Uplink Information Plugin)을 참조하십시오.

업링크가 온라인 상태인 경우, 서명 업데이트 사용 안함

이 업링크를 사용할 때마다 최신 서명을 다운로드하지 않으려면, 이 확인란을 선택합니다. 이것은 높은 데이터 전송률로 모바일 또는 위성 연결에 유용할 수 있습니다.

> **참고:** 서명 다운로드를 비활성화하면 최신 위협이 인식되지 않을 수 있기 때문에 보안 문제가 발생할 수 있습니다.

이 업링크가 실패할 경우

만약 활성화된 경우, 드롭 다운 메뉴에서 대체 연결을 선택할 수 있습니다. 드롭 다운 메뉴는 이 업링크가 실패할 때 활성화됩니다.

이 호스트에 연결할 수 있는지 확인

업링크가 실패할 때, **핑 (ping)** 될 IP 또는 호스트 이름 목록을 입력하여 재 연결 여부를 확인하려면 이 옵션을 선택하십시오.

> **힌트:** 이러한 호스트 중 하나는 공급자의 DNS 서버 또는 게이트웨이가 될 수 있습니다.

고급 설정 패널에서, 다음 세 가지 옵션을 사용자 정의할 수 있습니다.

사용자 정의 MAC 주소 사용

업링크와 관련된 네트워크 인터페이스의 MAC 주소를 사용자 정의해야 하는 경우 확인란을 선택하십시오.

재 연결 시간 초과

실패한 경우, 업링크가 다시 연결을 시도하는 시간 간격 (초)입니다. 이 값은 공급자의 설정에 따라 다릅니다. 확실하지 않으면, 이 필드를 비워 두십시오.

MTU

MTU 크기에 대한 사용자 정의 값입니다. 기본값을 수정하는 이유에 대한 설명은 여기를 참고하십시오.

> **추가 사항:**
>
> **네트워크 구성**, 1 단계, 4 단계 및 5 단계.
>
> *Menubar ‣ System ‣ Network Configuration*
>
> 장애 조치 업링크의 설정을 설명하는 자습서입니다.

VLAN

Endian UTM 어플라이언스에서 VLAN 지원을 제공한다는 아이디어는 구역에 VLAN ID를 임의로 연관시키고 구역들 간에 추가 수준의 분리 (따라서 다른 보안 수준)를 제공하는 것입니다. 기존 VLAN이 이미 생성된 경우 표에 표시됩니다. 사용할 수 있는 유일한 동작은 다음과 같습니다.

- 🗑 - VLAN을 제거합니다. 삭제를 확인하는 팝업 창이 열립니다.

VLAN 목록 위에 있는 Add new VLAN (새 VLAN 추가) 하이퍼링크를 클릭하여 새 VLAN을 정의할 수 있습니다. 열리는 양식에서 몇 가지 클릭만으로 다음 옵션들을 구성하여 인터페이스와 VLAN 사이의 연결을 만들 수 있습니다.

인터페이스

VLAN이 연결된 실제 인터페이스입니다. 드롭 다운 메뉴에서 사용 가능한 인터페이스만 선택할 수 있습니다. 메뉴에는 인터페이스 링크의 상태도 표시됩니다.

VLAN ID

VLAN ID는 0에서 4095 사이의 정수여야 합니다.

구역(Zone)

VLAN이 연결된 영역입니다. 네트워크 구성 마법사에 정의된 영역만 선택할 수 있습니다. 해당 인터페이스가 고가용성 관리 포트로 사용되는 경우, "NONE" 옵션을 선택할 수 있습니다.

> **경고:** 이미 다른 영역 (예: GREEN을 제공하는 eth1)을 제공되는 인터페이스에서 한 구역 (예: BLUE의 VLAN)을 제공하는 VLAN을 정의할 수 없습니다. 이렇게 하려고 시도하면, 양식이 닫히고 빨간색 콜 아웃이 나타나 VLAN을 만들 수 없음을 알려줍니다.

가상 LAN이 생성될 때마다, 새로운 인터페이스가 생성되고 ethX.y로 명명됩니다. 여기서 X는 인터페이스 번호이고 y는 VLAN ID입니다. 그런 다음, 이 인터페이스는 선택된 영역에 할당되며 *Menubar ‣ Status ‣ Network Configuration* 또는 대시 보드와 같은 네트워크 정보를 보고하는 다양한 섹션에 일반 인터페이스로 표시됩니다. 여기에서 그래프에 그려지도록 선택할 수 있습니다.

무선 전화

무선 모듈은 Endian UTM 어플라이언스를 액세스 포인트로 구성하기 위한 몇 가지 옵션을 제공합니다. 만약 활성화되지 않았다면, 무선 지원을 활성화할 스위치만 페이지에 표시됩니다. 활성화가 이루어지면, 새 SSID 추가 링크에 의해 두 부분으로 나뉜 상자가 나타납니다. 위쪽에는 전반적인 구성 옵션이 있는 패널이 표시되고, 아래쪽에는 사용 가능한 SSID 목록이 탐색 및 검색 표시 바로 아래에 표시되고, 한 번에 더 많은 SSID에 대한 작업을 수행하는 단추 집합 위에 표시됩니다. 다음 옵션을 사용하여 무선 모듈을 구성할 수 있습니다.

국가

드롭 다운 메뉴에서 선택한 Endian UTM Appliance가 작동하는 국가입니다. 채널의 가용성을 맞추기 위해 사용됩니다.

채널

무선이 무선 신호를 브로드 캐스팅해야 하는 채널입니다. 무선 채널은 통신에 관한 국가 규정에 따라 다릅니다.

무선 모드

802.11 표준 (b, g 또는 n)의 측면에서 무선에 사용되는 모드입니다.

3.0.5 릴리스 이후 무선 모듈의 뉴스

릴리스 3.0.5-YYYYMM에서는 GUI의 동작이 약간 변경되었습니다. 첫 번째 설정에서만 발생해야 하는 선택인 국가가 변경되면, *무선 모드*와 *채널*을 선택하기 전에 설정을 저장해야 합니다. 해당 국가에서 법률 및 규정이 변경되거나 Endian 어플라이언스가 다른 국가로 옮겨지면 현재 구성된 채널이 더 이상 유효하지 않을 수 있습니다. 이 경우 Endian 어플라이언스는 비호환성을 감지하여 사용 가능한 가장 안전한 채널인 **6**으로 되돌아갑니다.

또한 하드웨어 어댑터가 교체되거나 변경된 경우, 새 어댑터가 하드웨어 어댑터를 이전 어댑터에서 구성한 동일한 채널을 지원하지 않으면 다시 Endian 어플라이언스가 **6** 채널로 돌아갑니다.

초기에 비어 있는 SSID의 목록은 다음 정보를 제공합니다. 아래에 설명된 SSID 이름, 구역, 암호화 및 설명 등입니다.

새 SSID를 추가하려면, 새 SSID 추가를 클릭하여 다음 정보를 제공하는 편집기를 엽니다.

SSID

로컬 클라이언트가 볼 수 있는 SSID의 이름입니다.

브로드캐스트 SSID

SSID는 기본적으로 브로드캐스팅 됩니다 (즉, 체크 박스가 선택되어 있음). 클라이언트가 활성 상태 일 때, SSID가 표시됩니다. SSID가 브로드캐스트되지 않는 경우 클라이언트의 보기에서 숨겨지고 액세스하려면 클라이언트가 SSID의 이름을 제공해야 합니다.

구역(Zone)

클라이언트가 속할 영역으로, 사용 가능한 영역들 중에서 드롭 다운 메뉴로부터 선택합니다.

암호화

무선 연결에 사용할 암호화 유형입니다. 옵션으로 암호화 없음(No encryption), WPA, 개인 WPA2 또는 기업 WPA2가 있습니다.

활성화

이 체크 박스를 선택하면, SSID가 활성화됩니다.

설명

이 연결에 대한 사용자 정의 주석입니다.

서비스 메뉴

Endian UTM Appliance에는 위협을 방지하고 네트워크 및 실행 중인 데몬을 모니터링 하기 위한 유용한 서비스가 많이 포함되어 있습니다. 이 서비스의 활성화 및 설정은 이 섹션에서 설명합니다. 특히, 그것들 가운데, 우리는 안티 바이러스 엔진, 침입 탐지 시스템, 고가용성 및 트래픽 모니터링과 같은 다양한 프록시 서비스를 강조합니다. 사용 가능한 서비스는 화면의 왼쪽에 있는 하위 메뉴 목록에 항목으로 나타납니다.

- DHCP 서버 - 자동 IP 할당을 위한 DHCP 서버.
- 동적 DNS - DynDNS와 같은 동적 DNS 공급자 용 클라이언트 (가정용 / 소규모 사무실 용).
- 바이러스 백신 엔진 - 전자 메일, 웹, 팝 및 FTP 프록시에서 사용하는 바이러스 백신 엔진을 구성합니다.
- Time server (시간 서버) - NTP 시간 서버를 활성화 및 구성하고, 시간대를 설정하거나 수동으로 시간을 업데이트합니다.
- Mail Quarantine (메일 격리) - 격리된 전자 메일을 관리합니다.
- 스팸 교육 - 메일 프록시에서 사용하는 스팸 필터에 대한 교육을 구성합니다.
- 침입 방지 - IPS인 snort를 구성합니다.
- 고 가용성 - 고 가용성 설정에서 Endian UTM Appliance를 구성합니다.
- 트래픽 모니터링 - ntop을 사용하여 트래픽 모니터링을 활성화 또는 비활성화합니다.
- SNMP 서버 - SNMP (Simple Network Management Protocol) 지원을 활성화 또는 비활성화합니다.
- Quality of Service - IP 트래픽 우선 순위 지정.

DHCP 서버

DHCP 서버는 Endian UTM Appliance가 제어하는 영역에서 클라이언트 (워크 스테이션 및 서버)가 IP 주소 ("임대")를 수신하는데 사용됩니다.

고객에게 동적 유형과 고정 유형의 두 가지 유형의 임대를 지정할 수 있습니다. DHCP 서버 페이지는 DHCP 서버를 구성할 *서버 구성*, 고정 임대를 보여주는 *현재 고정 임대*, 그리고 *현재 동적 임대*의 세 가지 탭으로 구분됩니다.

서버 구성

Endian UTM Appliance의 DHCP 서버는 각 활성 존에서 독립적으로 활성화할 수 있습니다. 이 페이지는 정의된 영역에 따라 처음에 하나, 둘 또는 세 개의 확인란을 표시하며, *AAAAAA*가 **GREEN(녹색), ORANGE(오렌지)** 또는 **BLUE(파란색)**이 될 수 있는 **AAAAAA 인터페이스**에서 **DHCP 서버 사용으로 레**

이블이 지정됩니다.

> **참고:** 파란색 구역과 핫스팟이 모두 활성화되어 있으면, 파란색 구역의 IP 할당이 핫스팟으로 관리되기 때문에 DHCP 구성 메시지가 핫스팟으로 표시되고 확인란이 비활성화 됩니다.

페이지 하단에는 고급 사용자가 dhcpd.conf 파일 (예: 서브넷에 대한 사용자 지정 경로)에 추가할 사용자 지정 구성 라인을 작성하는데 사용할 수 있는 **사용자 정의 구성 행 (Custom configuration lines)**이라는 텍스트 필드가 있습니다. 이 예제에서는 여기에 표시됩니다.

각 영역의 DHCP 매개 변수를 사용자 정의하려면, 확인란을 선택하십시오. 설정(Settings)이라는 패널이 나타나면, 클릭하여 확장하고 사용 가능한 옵션을 표시하십시오.

시작 주소, 끝 주소

클라이언트에 제공할 IP 주소의 범위. 이 주소는 해당 영역에 할당된 서브넷 내에 있어야 합니다. 일부 호스트가 고정 임대를 해야하는 경우 (아래 참조) 충돌을 피하기 위해 IP 주소가 이 범위 또는 OpenVPN 주소 풀 범위 (*Menbar ‣ VPN ‣ OpenVPN server* 참조)에 포함되어 있지 않은지 확인하십시오.

이 두 필드를 공백으로 두면, 동적 임대를 위해 영역의 전체 IP 범위가 사용됩니다.

고정 리스만 허용

고정리스 만 사용하려면, 이 체크 박스를 선택하십시오. 동적리스가 지정되지 않습니다.

기본 임대 시간, 최대 임대 시간

각 임대의 할당이 만료되고 클라이언트가 DHCP 서버에서 새 임대를 요청하기 전의 기본값과 최대 시간 (분)입니다.

도메인 이름 접미사

클라이언트에 전달되고 로컬 도메인 검색에 사용되는 기본 도메인 이름 접미사입니다.

기본 게이트웨이

영역의 클라이언트가 사용할 기본 게이트웨이입니다. 비워두면 기본 게이트웨이는 Endian UTM Appliance 자체입니다.

1차 DNS, 2차 DNS

클라이언트가 사용하는 DNS. Endian UTM 어플라이언스에는 캐싱 DNS 서버가 포함되어 있으므로 두 번째 서버 또는 기본 값까지도 변경할 수 있지만 기본값은 각 영역의 방화벽 자체 IP 주소입니

다.

기본 NTP 서버, 보조 NTP 서버

클럭 동기화를 유지하기 위해 클라이언트가 사용하는 NTP 서버이며, Endian UTM Appliance의 기본 NTP 서버로 사용하려면 이 부분을 비워두십시오.

기본 WINS 서버, 보조 WINS 서버

클라이언트가 사용하는 WINS 서버입니다. 이 옵션은 WINS를 사용하는 Microsoft Windows 네트워크에만 필요합니다.

일단 완료되면, 페이지 하단의 Save (저장) 버튼을 클릭한 다음 녹색 설명선에 있는 Apply (적용) 버튼을 클릭하면 새 구성으로 DHCPD 서버가 다시 시작됩니다.

고정리스

특정 장치가 DHCP를 사용하는 동안 동일한 IP 주소 (예: VoIP 상자, SVN 저장소, 파일 서버 또는 프린터 또는 스캐너와 같은 장치를 제공하는 서버)를 항상 사용하는 것이 때때로 필요하거나 바람직합니다. DHCP 서버에서 임대를 요청할 때 장치가 항상 동일한 IP 주소를 수신하므로 고정 임대는 고정 IP 주소라고도 합니다.

이 탭에는 로컬 네트워크에 정의된 모든 고정리스의 목록이 포함되어 있습니다. MAC 주소 및 할당된 IP 주소, 설명 및 사용 가능한 작업은 다음과 같습니다.

- ☑☐ - 임대 상태, 사용 또는 사용 안함을 토글할 수 있습니다
-  - 임대의 속성을 수정합니다.
-  - 임대를 제거합니다.

고정 임대 추가 링크를 클릭하면 새로운 고정리스를 장치에 할당하고 목록에 표시될 모든 정보를 삽입할 수 있습니다. 장치는 MAC 주소로 식별됩니다.

예제 SRV-1 - PXE 시동 및 dhcpd.conf 구성.

DHCP 서버의 사용자 정의는 다른 네트워크 구성에서 유용합니다.

하나의 일반적인 사용 사례는 부팅시 HTTP 서버에서 구성 파일을 검색해야 하는 VoIP 전화기입니다. 이 경우 파일은 Endian UTM Appliance에도 있을 수 있으므로 tftp 서버의 구성을 추가 라인으로 전달할 수 있습니다 다음과 같이하십시오.

```
option tftp-server-name "http://192.168.0.15";
option bootfile-name "download/voip/{mac}.html";
```

192.168.0.15를 올바른 IP 주소로 바꾸고 **download/voip/{mac}.html** 문자열을 올바른 경로로 바꾸는 것을 잊지 마십시오. 사용 가능한 옵션에 대한 추가 정보는 ***dhcpd(5)*** 매뉴얼 페이지를 참조하십시오.

> 경고: 이들 행에 대한 구문 검사는 수행되지 않습니다. 행들은 구성 파일에 글자 그대로 추가됩니다. 여기서 실수를 하면 DHCP 서버가 시작될 수 없습니다!

> 참고: DHCP 서버에서 고정 임대를 할당하는 것은 장치에서 수동으로 IP 주소를 설정하는 것과 매우 다릅니다. 실제로 후자의 경우 장치는 여전히 DHCP 서버에 접속하여 주소를 수신하고 네트워크 상에 존재를 알립니다. 그러나 장치에 필요한 IP 주소가 이미 할당되어 있으면 장치에 동적 임대가 부여됩니다.

고정리스에 대해 다음 매개 변수를 설정할 수 있습니다.

MAC 주소

클라이언트의 MAC 주소.

IP 주소

클라이언트에 항상 할당되는 IP 주소입니다.

설명

임대를 수신하는 장치에 대한 선택적 설명입니다.

고급 옵션을 클릭하면, 필요한 경우 고정리스의 구성을 개선하는 패널이 나타납니다.

다음 주소

TFTP 서버의 주소. 이 옵션과 다음 두 옵션은 몇 가지 경우에만 유용합니다 (아래 예제 참조).

파일 이름

부팅 이미지 파일 이름입니다. 씬 클라이언트 또는 네트워크 부팅에만 필요한 옵션입니다.

루트 경로

부팅 이미지 파일의 경로입니다.

활성화

이 확인란을 선택하지 않으면, 고정 임대가 저장되지만 dhcpd.conf 파일에 기록되지 않습니다.

표 아래에 작업 선택이라는 드롭 다운 메뉴에서 모든 고정 임대 또는 선택한 모든 임대를 동시에 활성화 또는 비활성화 할 수 있습니다.

고정 임대용 사용 사례.

고정 임대의 유용성을 보여주는 사용 사례는 PXE를 사용하는 네트워크상의 씬 클라이언트 또는 디스크가 없는 워크 스테이션의 경우입니다. 즉, 네트워크로 연결된 tftp 서버에서 제공한 이미지에서 운영 체제를 부팅합니다. tftp 서버가 DHCP가 있는 동일한 서버에서 호스트되는 경우 씬 클라이언트는 임대와 이미지를 동일한 서버에서 수신합니다. 그러나 tftp 서버는 네트워크의 다른 서버에서 호스팅되기 때문에 DHCP 서버에서 클라이언트를이 서버로 리디렉션해야 합니다. 이 작업은 씬 클라이언트 용 DHCP 서버에 고정된 임대를 쉽게 추가할 수 있습니다 부팅할 이미지의 파일 이름과 다음 주소를 추가합니다.

고정리스 생성 과정에서 제공되는 정보 외에도, 작업 열의 아이콘을 클릭하여 각각의 리스를 활성화 또는 비활성화 (확인란 선택), 편집 또는 삭제할 수 있습니다. 임대를 편집하면, 새 임대 작성과 동일한 양식이 열리고, 임대를 삭제하면 즉시 구성에서 제거됩니다.

> **참고:** DHCP 서버에 의해 할당된 모든 임대는 기본적으로 /var/lib/dhcp/dhcpd.leases 파일에 저장됩니다. DHCP 데몬이 해당 파일을 정리 처리하지만 이미 만료되었고, 꽤 오래된 임대 파일을 저장하는 경우가 있습니다. 이것은 문제가 되지 않으며 정상적인 DHCP 서버 작동을 방해하지 않습니다. 이 파일의 일반적인 항목은 다음과 같습니다.
>
> ```
> lease 192.168.58.157 {
> starts 2 2013/06/11 13:00:21;
> ends 5 2013/06/14 01:00:21;
> binding state active;
> next binding state free;
> hardware ethernet 00:14:22:b1:09:9b;
> }
> ```

동적 임대

DHCP 서버가 활성화되고 적어도 하나의 클라이언트가 (동적) IP 주소를 받으면, 이 탭에는 할당된 동적 IP 주소, MAC 주소, 호스트 이름, 만료 날짜 및 시간, 상태가 만료되거나 활성화 될 수 있습니다.

동적 DNS

DNS 서버는 호스트 이름이 주어진 호스트의 (숫자) IP 주소를 분석할 수 있는 서비스를 제공하며 *고정* IP 주소 및 호스트 이름을 가진 호스트에 완벽하게 작동합니다.

DynDNS 또는 no-IP와 같은 DDNS 공급자는 주거 ADSL 연결을 사용할 때 일반적으로 사용되는 IP 주소가 동적인 경우 비슷한 서비스를 제공합니다. 모든 도메인 이름을 등록할 수 있으며 모든 IP 주소 변경 사항을 DDNS 공급자에게 전달합니다. 호환이 가능하고 루트 DNS 서버와 통합하려면 IP 주소가 변경될 때마다 업데이트를 DDNS 공급자로부터 적극적으로 전파해야 합니다.

엔디안 UTM 어플라이언스에는 14개의 다른 공급자를 위한 동적 DNS 클라이언트가 포함되어 있으며, 활성화된 경우 동적 DNS 공급자에 자동으로 연결되어 변경될 때마다 새 IP 주소와 통신합니다.

> **참고:** 동적 DNS 계정이 설정되지 않은 경우, 새로운 DNS 등록을 위한 자세한 지침, 공급자의 웹 사이트에서 자세한 온라인 도움말 및 방법을 볼 수 있습니다.

이 페이지에는 동적 DNS 계정 목록이 표시됩니다. 사실, 둘 이상의 DDNS 공급자를 사용할 수 있습니다. 각 계정에 대해 목록에는 사용된 서비스, 등록된 호스트 이름 및 도메인 이름, 익명 프록시 및 와일드 카드 기능이 활성화된 경우, 활성화된 경우 가능한 작업에 대한 정보가 표시됩니다.

- ☑ ☐ 임대 상태를 토글합니다 (사용 또는 사용 불가능).
- 임대의 속성을 수정합니다.
- 임대를 삭제합니다.

다음 매개 변수를 제공하여 `호스트 추가` 링크를 클릭하여 새 계정을 만들 수 있습니다.

서비스

드롭 다운 메뉴에 사용 가능한 DDNS 공급자가 표시됩니다.

프록시 뒤에서(Behind a proxy)

이 옵션은 noip.com 제공 업체에만 적용됩니다. Endian UTM 어플라이언스가 프록시를 통해 인터넷에 연결되어 있으면 이 확인란을 선택해야 합니다.

와일드 카드 활성화

일부 동적 DNS 공급자는 도메인 지점의 모든 하위 도메인이 동일한 IP 주소를 허용합니다. 이것은 www.example.myddns.org와 second.example.myddns.org와 같은 두 호스트가 모두 동일한 IP 주소에 있는 상황입니다. 이 상자를 선택하면, 이 기능이 활성화되어 모든 가능한 하위 도메인이 동일한 IP 주소로 리디렉션됩니다. 가능한 경우 DDNS 공급자 서버의 계정에서도 이 기능을 구성해야 합니

다.

호스트 이름 및 도메인

"example"및 "myddns.org"와 같이 DDNS 공급자에 등록된 호스트 이름 및 도메인

사용자 이름과 비밀번호

동적 DNS 공급자가 서비스에 액세스하기 위해 제공한 자격 증명입니다.

라우터 (NAT) 뒤에서

Endian UTM 어플라이언스가 인터넷에 직접 연결되어 있지 않은 경우, 즉 인터넷에 액세스하기 전에 다른 라우터나 게이트웨이가 있는 경우, 이 옵션을 활성화하십시오. 이 경우 http://checkip.dyndns.org의 서비스를 사용하여 라우터의 IP 주소를 찾을 수 있습니다.

활성화

계정을 활성화하려면, 이 확인란을 선택하십시오 (기본값).

> **참고:** 동적 DNS 공급자는 도메인 이름만 확인하고 관련 서비스는 확인하지 않습니다. 일부 서비스를 인터넷에서 Endian UTM Appliance 또는 Endian UTM Appliance 뒤에 있는 일부 호스트에 액세스해야 하는 경우, 일부 포트 전달 규칙을 설정해야 합니다 (*Menubar ‣ Firewall ‣ Port forwarding / NAT* 참조).

구성을 변경하거나 정의된 모든 계정에 대한 동적 DNS를 즉시 업데이트하려면, `업데이트 강제 적용` 버튼을 클릭하십시오. 예를 들어, 업링크가 연결 해제되고, **REDIP**가 변경된 경우 유용합니다. 이 경우 모든 DDNS 계정을 업데이트해야 합니다. 그렇지 않으면, DDNS를 통해 제공되는 서비스에 도달할 수 없습니다.

바이러스 백신 엔진

Endian UTM Appliance에는 ClamAV 및 Panda Antivirus의 두 가지 안티 바이러스 엔진이 제공됩니다. 이 파일은 Endian UTM Appliance를 통과하는 파일 (웹 페이지, 아카이브, 스프레드 시트, 텍스트 문서 등)을 스캔하기 위해 파일 및 문서 내의 바이러스 및 맬웨어 연구 및 프록시 서비스와 함께 사용할 수 있습니다.

설치된 안티 바이러스에 따라, 이 페이지는 하나, 둘 또는 세 개의 탭으로 구성됩니다. Panda antivirus가 설치되어 있지 않으면, ClamAv 바이러스 백신 탭만 나타나고 그렇지 않은 경우, 전역 설정 및 팬더 바이러스 차단 탭이 나타납니다.

아카이브 폭탄 및 DoS.

아카이브 폭탄 (archive bomb)은 바이러스 백신 소프트웨어를 호스팅하는 컴퓨터의 리소스 대부분을 차지하는 지점까지 DoS 공격이라고 불리는 많은 트릭을 사용하여 바이러스 백신 소프트웨어를 오버로드하는 아카이브입니다. 이러한 트릭들에는 다음과 같은 것들이 포함됩니다. 압축이 잘되는 반복되는 내용의 큰 파일로 구성된 작은 아카이브 (예: 0만 포함된 1GB 크기의 파일은 zip을 사용하여 1MB로 압축됩니다). 여러 개의 중첩된 아카이브 (즉, zip 파일 내부의 zip 파일). 많은 수의 빈 파일을 포함하는 아카이브 등이 있습니다. 많은 특성 (특히 RAM과 CPU)이 필요하고 사용자의 가용성에서 벗어났기 때문에 그러한 특성을 가진 아카이브 파일의 압축을 풀면 서버나 워크 스테이션의 정상적인 활동에 심각한 문제가 발생합니다.

전역 설정

전역 설정 탭에는 몇 가지 드롭 다운 메뉴가 포함되어 있어 어떤 서비스에 어떤 바이러스 백신을 사용할지 선택할 수 있습니다. 동시에 두 바이러스 백신을 동시에 사용할 수 있지만 동일한 서비스에는 사용할 수 없습니다.

기본 안티 바이러스 엔진

모든 서비스에 기본적으로 사용될 안티 바이러스를 선택하십시오. 이 드롭 다운 메뉴에서 선택한 옵션에 따라 다른 옵션의 값이 설정됩니다.

HTTP 용 바이러스 백신 엔진 | SMTP | POP | FTP 프록시

네 개의 각 드롭 다운 메뉴에서 각 프록시 서비스에 대한 바이러스 백신을 개별적으로 선택하십시오.

팬더 안티 바이러스

이 탭에는 Panda Antivirus를 구성하는 모든 옵션이 있습니다. 단일 옵션은 두 개의 패널, 즉 파일 내용 분석 및 패키지 및/또는 압축 파일에 표시되며 나머지 모든 파일 검색 옵션을 그룹화합니다.

업데이트 주기

드롭 다운 메뉴에서 안티 바이러스 시그니처의 업데이트주기를 **매시간, 매일, 매주** 또는 **매월** 중에서 선택하십시오.

구성할 스캔 옵션은 다음 두 섹션으로 그룹화됩니다.

파일 내용 분석

다음 세 가지 옵션은 Panda Antivirus가 감염된 것으로 인식된 파일을 처리하는 방법을 정의합니다.

감염된 파일 정리

안티 맬웨어 검사 중에 파일 자동 치료를 사용하려면 확인란을 선택하십시오. 이 옵션을 비활성화하면 파일을 치료하지 않고 감염된 파일을 삭제합니다.

지능형 분석 사용

맬웨어의 휴리스틱 분석을 사용하여 아직 서명에 포함되지 않은 새로운 유형의 맬웨어를 검색하십시오.

경험적 수준

사용 가능한 세 가지 값, **낮음, 중간** 및 강함: *높음* 중에서 휴리스틱 분석의 원하는 감도 수준을 선택하십시오.

패키지 및 / 또는 압축 파일

이러한 옵션은 압축 파일을 처리할 때, 안티 바이러스의 동작과 관련이 있습니다. 자세한 정보는 여기를 살펴보십시오.

최대 재귀 수준

압축 파일 내의 최대 재귀 수준.

제어 압축 해제 크기

확인란을 선택하면 압축 해제된 파일의 크기를 제어할 수 있습니다.

최대 감압 크기

압축되지 않은 항목에 허용되는 압축 해제된 파일의 최대 크기 (KB)입니다.

최대 중첩 수준

압축 파일에 허용되는 가장 높은 중첩 수준.

ClamAv 안티 바이러스

이 탭은 두 개의 상자로 구성됩니다. 첫 번째는 ClamAV를 구성하고 특히 아카이브 폭탄을 관리하고, 두 번째는 서명의 현재 동기화 상태를 표시합니다.

ClamAV 안티 바이러스 구성

DoS 공격을 피하기 위해 ClamAV는 여기에서 수정할 수 있는 특정 속성이 있는 아카이브를 **검색하지 않도록** 구성됩니다.

최대 아카이브 크기

이 크기보다 큰 아카이브는 메가 바이트 단위로 검색되지 않습니다.

최대 중첩된 아카이브

재귀 적으로이 값을 초과하는 중첩된 아카이브가 포함된 아카이브는 검색되지 않습니다.

아카이브에 있는 최대 파일들

여기에 설정된 수보다 많은 파일이 포함된 아카이브는 검색되지 않습니다.

최대 압축률

압축되지 않은 크기가 압축된 아카이브 크기를 **X**번 이상 초과하는 아카이브 (여기서 X는 여기에 지정된 압축 비율 임)는 검색되지 않습니다. 기본값은 1000입니다.

> **참고:** 일반 파일의 압축률은 사용되는 알고리즘에 따라 다르지만 약 10 ~ 15입니다. 즉, 압축되지 않은 파일 크기는 아카이브 크기의 10 ~ 15 배입니다.

불량 자료실 처리

위의 설정 중 하나 이상에 설정된 제한을 통과했기 때문에 스캔되지 않은 아카이브는 어떻게 됩니까? 선택 사항은 **검사하지 않지만 통과하고 바이러스로 차단**합니다. 첫 번째 경우에는 파일을 검사하지 않고 컨트롤을 전달하므로 전자 메일을 받는 사람은 신중하게 검사해야 하며 두 번째 경우에는 바이러스로 간주되어 차단됩니다.

> 참고: 파일이 위의 *최대 보관 파일 크기 필드*에 지정된 크기보다 클 경우, 여기 정책은 *바이러스로 차단*되어 있습니다. 그러나 크기 제한에 도달할 때까지 다운로드 되기 때문에 다운로드가 성공적으로 완료되지 않았다는 인상을 줄 수 있습니다. 이 문제를 방지하려면, 이 옵션 또는 위의 크기를 변경하십시오.

암호화된 아카이브 차단

암호화된 (즉, 암호로 보호된) 아카이브를 스캔하는 것은 기술적으로 불가능하지만 보안 위험을 나타낼 수 있습니다. 차단하려면, 이 확인란을 선택하십시오.

ClamAV 서명 업데이트 일정

이 옵션은 페이지의 오른쪽에 나타나며, 시간 경과에 따라 변경되는 ClamAV 시그니처의 다운로드 빈도를 선택할 수있게 하며, 최신 바이러스 및 악성 프로그램까지도 인식할 수 있도록 최신 상태로 유지해야 합니다. **시간별** (기본값), **매일, 매주** 및 **매월**의 네 가지 옵션을 사용할 수 있습니다.

> **힌트:** 물음표 위로 마우스를 움직이면, 각각의 경우에 업데이트가 수행되는 정확한 시간이 표시됩니다. 기본 설정은 전체 시간에서 1분입니다.

ClamAV 바이러스 서명

이 상자에는 서명 바이러스에 대한 몇 가지 정보가 표시됩니다. 상자 맨 위에는 다음과 같은 메시지가 표시됩니다.

> 마지막 서명은 **9월 16일 13:21:28**에 **db.local.clamav.net**에서
> 업데이트되었으며 총 **1040149** 개의 서명이 로드되었습니다.

이 메시지는 굵은 글꼴로 최신 다운로드 날짜와 시간, 서명이 다운로드 된 서버 및 다운로드 된 서명 수를 보고합니다.

> **참고:** ClamAV를 바이러스 백신으로 사용하는 프록시 서비스가 없으면, 서명을 다운로드하지 않습니다. 이 경우, 이 상자에는 활성화된 서비스 중 현재 ClamAV Antivirus를 사용하고 있지 않음이라는 메시지가 표시됩니다. 따라서 업데이트가 비활성화됩니다.

메시지 아래에 목록에는 다운로드 한 서명의 유형, 마지막 동기화 시간, 버전 및 마지막 업데이트 시간이 표시됩니다. 마지막 동기화 확인에 서명 업데이트가 포함되어 있지 않으면, 업데이트 및 동기화 시간이 다를 수 있습니다.

지금 서명 업데이트 버튼을 클릭하면, 특정 바이러스에 대한 정보를 찾기 위해 ClamAV의 온라인 데이터베이스 탭의 새 브라우저에 열려 있는 온라인 바이러스 데이터베이스 검색을 클릭하는 동안 시간이 걸릴 수도 있는 즉시 업데이트가 (예약된 업데이트에 관계없이 이전처럼 계속됩니다) 수행됩니다.

> **힌트:** 서명 데이터베이스는 공급자로부터 하루에 여러 번 업데이트 될 수 있으므로 다운로드 빈도를 높게 설정하는 것이 좋습니다.

시간 서버 (Time server)

Endian UTM Appliance는 NTP를 사용하여 시스템 시간을 인터넷의 시간 서버와 동기화합니다. 사용 가능한 설정은 *네트워크 시간 서버를 사용*하여 자동으로 시간을 동기화하고 *수동으로 조정*하여 수동으로

시간을 수정하는 두 개의 상자로 그룹화됩니다

네트워크 시간 서버 사용 (User a network time server)

인터넷상의 수 많은 시간 서버 호스트가 시스템에 의해 사전 구성되어 사용되지만, *기본 NTP 서버 대체* 선택란을 체크한 후 사용자 정의 시간 서버를 지정할 수 있습니다. 이것은 Endian UTM 어플라이언스가 인터넷에 연결할 수 없는 설치 프로그램을 실행할 때 필요합니다. 행당 하나씩 여러 개의 시간 서버 주소가 작은 양식으로 보여주는 형태로 제공될 수 있습니다.

또한 이 상자에는 현재 시간대 설정이 표시되며, 드롭 다운 메뉴에서 다른 설정을 선택하여 변경할 수도 있습니다. 즉시 동기화 단추를 클릭하면, 즉시 동기화 할 수 있습니다.

수동으로 조정

두 번째 상자는 수동으로 시스템 시간을 변경할 수 있는 가능성을 제공합니다. 권장 사항은 아니지만 시스템 시계가 꺼져 있고 Endian UTM 어플라이언스의 시계를 정확한 시간으로 즉시 업데이트해야 하는 경우에 유용합니다.

시간 서버를 사용하는 자동 동기화는 즉시 수행되지 않지만 클록 속도를 정확한 시간으로 복원되거나 맞추기 위해 조금 느려지거나 빨라집니다.

따라서 시간에 중대한 오류가 있는 시스템은 정확한 시간과 정렬되는데 오랜 시간이 필요할 수 있지만 차이가 너무 큰 경우 자동 동기화가 실패하고 직접적인 수동 동기화를 강제하는 것이 유일한 해결책입니다.

메일 격리

메일 격리는 Endian UTM Appliance 하드 디스크의 특별한 위치로, SMTP 프록시가 스팸, 멀웨어, 바이러스 또는 의심스러운 첨부 파일을 포함하고 있는 것으로 인식하는 모든 전자 메일이 배달되는 대신 저장됩니다. 여기에서 이러한 전자 메일을 안전하게 분석하고 해당 전자 메일을 관리하기 위한 조치를 취할 수 있습니다. 메일 격리를 활성화하려면, *Menubar ‣ proxy ‣ SMTP ‣ Configuration*으로 이동하고, 스팸 설정, 바이러스 설정 및 파일 설정 상자에서 드롭 다운 메뉴로부터 *기본 격리 위치로 이동 (Move to default quarantine location)* 옵션을 선택합니다.

메일 격리 저장소에있는 전자 메일은 격리 보존 기간에 도달할 때까지 Endian UTM Appliance의 특수 폴더에 남아 있습니다 (SMTP 프록시 모듈의 격리 설정 참조). 그러나 격리된 전자 메일이 디스크에 많이 저장되어 있으면, 격리 폴더가 채워질 수 있으므로 격리된 전자 메일을 수동으로 삭제해야 합니다.

메일 격리 전용 공간은 어플라이언스의 유형, 격리된 전자 메일의 크기 (특히 첨부 파일이 많거나 다른 활성 서비스 등)와 같은 여러 요소에 따라 달라집니다.

메일 격리는 *격리(Quarantine)* 및 *요약 보고서(Summary Reports)* 라는 두 개의 탭으로 구성됩니다. 전자는 격리 저장소에 저장된 전자 메일 목록을 포함하고 탐색 및 관리할 수 있으며, 후자는 격리 저장소의 콘텐츠에 대한 정기 보고서를 생성하고 해당 발송을 관리할 수 있습니다.

격리

메일 격리 페이지에는 스팸 격리 저장소로 이동한 모든 메일 목록이 있는 테이블이 있으며 여기 위에는 전자 메일을 탐색할 탐색 모음이 있습니다.

이 표에는 격리 보관된 메일에 대한 다음 정보가 포함되어 있습니다.

선택

한 번에 하나 이상의 메시지를 선택하고 모든 메시지를 처리할 수 있는 확인란입니다.

격리 날짜

전자메일이 검역소로 옮겨진 날짜와 시간.

이유

전자 메일이 배달되지 않은 이유는 **멀웨어** 중 하나일 수 있습니다. 전자 메일에 바이러스 또는 기타 유형의 위협이 포함되어 있습니다. **스팸** - 전자 메일이 스팸으로 표시되고, **금지됨** - 전자 메일이 전송할 수 없는 첨부 파일 및 **잘못된 헤더**를 가지고 있습니다 - 헤더에 포함된 정보가 유효하지 않습니다.

발신인(From)

이메일 발신자.

수신인(To)

전자 메일이 처음 전송된 받는 사람입니다.

제목

이메일 제목입니다.

크기

전자 우편의 크기.

첨부

전자 메일에 첨부된 파일의 수입니다.

각 전자 메일에서 네 가지 작업을 실행할 수 있습니다.

- 메시지 보기
- 메시지를 다운로드 합니다.
- 메시지를 발송하고 원래 수신자에게 배달합니다.
- 이메일을 삭제합니다 - 자세한 내용은 아래를 참조하십시오.

표 아래에 액션 선택이라고 된 드롭 다운 메뉴에서 모든 이메일 또는 선택한 이메일만 보내거나 삭제할 수 있습니다.

보기 메시지 아이콘을 클릭하면, 전자 메일 목록이 3개의 박스가 있는 페이지로 바뀌어 선택한 전자 메일에 대한 다양한 세부 정보가 표시됩니다.

격리된 전자 메일

이 상자는 전자 메일 목록에 보고된 전자 메일 데이터를 좀 더 자세하게 보여줍니다. 전자 메일이 보낸 사람 및 받는 사람, 전자 메일의 참조 수신자, 제목, 날짜, 수신 시간 및 전자 메일의 크기와 함께 격리 저장소로 옮겨진 이유를 보여줍니다.

헤더

원본 전자 메일의 전체 헤더이며, 예를 들어 경로 뒤에 전자 메일이 오는 것과 같은 유용한 정보를 제공합니다.

콘텐츠

하나 이상의 첨부 파일이 있는 전자 메일의 경우, 여기에 세부 정보와 함께 첨부 파일이 표시됩니다. 또한 모든 HTML 첨부 파일은 전체 소스 코드와 함께 표시됩니다.

하단에는 사용할 수 있는 옵션이 있습니다.

발송 후 격리 보관소에서 삭제

전자 메일은 원래 수신자에게 발송된 후 격리 저장소에서 제거됩니다.

요약 보고서

격리된 전자 메일에 대한 정기 보고서를 자동으로 보내 전자 메일을 원래 받는 사람에게 알릴 수 있습니다. 이 페이지에서는 이 서비스의 빈도와 설정을 활성화하고 관리할 수 있습니다.

> **참고:** 이 기능을 사용하려면 SMTP 프록시를 올바르게 설정하고 실행해야 합니다. 그렇지 않으면, 보고서를 보내지 않습니다.

격리된 전자 메일을 받는 사람에게 알릴 수 있는 대안.

격리 저장소에서 끝난 하나 이상의 전자 메일을 받았다는 것을 사용자에게 알리는 두 가지 방법이 있습니다.

1. 전체 수신 도메인 선택. 이 경우 적절한 목록에 있지 않으면, 해당 도메인의 모든 사용자에게 알림이 전송됩니다. 수신 도메인은 SMTP 프록시 모듈 (*Menubar ‣ Proxy ‣ SMTP ‣ Incoming domains*)에서 구성할 수 있습니다. "*아래 주소로 요약 보고서 이메일을 보내지 마십시오*"라는 옵션을 보십시오.
2. 알림을 받을 사용자를 명시적으로 나열합니다. "*아래의 주소로 요약 보고서 이메일 보내기*" 옵션을보십시오.

이 두 가지 접근법은 배타적이지 않습니다. 두 가지를 모두 사용할 수 있습니다.

또한, 전자 메일이 요약 보고서의 일부가 되지 않는 보낸 사람 주소 목록을 제공할 수도 있습니다.

마지막으로 와일드카드와 정규 표현식을 사용하여 긴 주소 목록을 작성하지 않아도 됩니다.

> **경고:** 와일드 카드를 오용하지 않도록 주의하십시오! 특히 행에 단일 별표 (*)를 쓰면 Endian UTM Appliance에서 관리하는 **모든 도메인**의 **모든 사용자**에게 전자 메일 알림을 보냅니다.

요약 보고서 서비스는 기본적으로 활성화되어 있지 않습니다. 시작하려면 요약 보고서 이메일 활성화라고 표시된 회색 스위치를 클릭하십시오. 녹색으로 바뀌고, 많은 구성 옵션이 나타납니다.

기본 발신자 이메일 주소 사용

확인란을 선택하면, 기본 주소가 보고서의 보낸 사람으로 나타납니다.

> **참고:** 기본 전자 메일 주소는 네트워크 구성 중에 지정된 주소입니다. 네트워크 구성의 6단계를 참조하십시오.

이메일 발신자 주소

이전 옵션에 체크 표시가 없으면, 사용자 지정 보낸 사람 주소를 지정할 수 있습니다.

요약 보고서 이메일 일정

보고서는 **매일, 매주** 또는 **매월** 보낼 수 있습니다.

> **참고:** *Menubar ‣ Proxy ‣ SMTP ‣ Configuration ‣ Qurantine settings*에 있는 격리 보관 기간 옵션 값이 30 일보다 적으면, **월간** 옵션을 사용할 수 없습니다.

포함할 이메일

이 드롭 다운 메뉴에서는 두 가지 옵션을 사용할 수 있습니다. **최근 보고서 이후에 수신된 이메일**을 선택하여 가장 최근에 격리된 이메일 (즉, 마지막 보고서를 보낸 후 도착한 이메일) 또는 **모든 격리된 전자 메일**을 포함하여 모든 격리 컨텐트를 대량으로 발송합니다.

메일 템플릿 언어 선택

사용 가능한 **영어, 독일어, 이탈리아어** 및 **일본어** 값으로 선택된 요약 보고서를 작성하는데 사용되는 언어입니다.

전자 메일에 포함할 연락처 데이터

이 양식은 보고서에 사용자 지정 메시지를 포함하는데 사용될 수 있습니다.

> **힌트:** 예를 들어, 사용자가 정보를 요청하거나 격리된 전자 메일을 릴리스하기 위해 연락할 수 있는 전자 메일 주소를 포함시킵니다.

요약 보고서 이메일 내용

이 **다중 선택 상자는** 격리된 각 전자 메일에 대한 요약 보고서에 포함할 데이터를 선택할 수 있게 해줍니다. 기본적으로 발신인, 격리 이유, 제목 및 날짜가 포함되어 있지만 수신자 주소, 첨부 파일 정보 및 크기도 포함될 수 있습니다.

수신 도메인

이 다중 선택 상자를 사용하면 위험한 전자 메일을 모니터링 할 도메인을 선택하고, 이를 격리 저장소로 보낼 수 있습니다. 이러한 도메인 중 하나에 있는 사용자가 스팸 격리 저장소에서 끝나는 메일을 받으면, 이메일로 알림을 받게 됩니다.

> **힌트:** 이 상자에 새 도메인을 추가하려면, Menubar ‣ Proxy ‣ SMTP ‣ Incoming domains에 도메인을 추가하십시오.

이 주소로 최종 요약 보고서 이메일 보내기

한 줄에 하나씩 요약 보고서를 항상 받는 수신자 목록입니다.

> 경고: 와일드카드를 오용하지 않도록 주의하십시오! 특히 한 줄에 하나의 별표 (*)를 쓰면, Endian UTM Appliance에서 관리하는 모든 도메인의 모든 사용자에게 전자 메일 알림을 보냅니다!

이 주소로 요약 보고서 이메일을 보내지 마십시오.

한 줄에 하나씩 써 있으며, 요약 보고서를 절대 받지 않는 수신 도메인의 전자 메일 주소 목록입니다.

이 발신자 주소의 이메일은 포함하지 마십시오.

전자 메일이 요약 보고서에 한 줄에 하나씩 포함되지 않는 보낸 사람 목록입니다.

추가 참고:

SMTP 프록시

Menubar ▸ Proxy ▸ SMTP proxy의 SMTP Configuration

스팸 학습

Endian UTM Appliance에는 스팸 전자 메일을 찾고 싸울 엔진으로 SpamAssassin이 포함되어 있습니다. 대다수의 경우 성공적이긴 했지만, SpamAssassin은 스팸 전자 메일을 가로 채기 위한 능력을 향상시키도록 학습받아야 합니다. 스팸 방지 엔진에 대한 학습 구성은 이 페이지에서 수행할 수 있습니다. 실제로 SpamAssassin은 어떤 전자 메일이 스팸이고 어떤 전자 메일이 아닌지 (소위, *햄(ham)* 메일)를 자동으로 알 수 있습니다. 학습할 수 있게 하려면, IMAP 호스트에 연결하여 미리 정의된 폴더에서 스팸 및 햄 메시지를 확인해야 합니다.

SpamAssassin의 페이지는 학습에 사용되는 IMAP 호스트 목록을 포함하는 두 개의 상자, *현재 스팸 학습 소스* 및 다양한 수준에서 관리할 수 있는 기능이 있는 상자와 업데이트의 일정을 수정할 수 있는 *SpamAssassin 규칙 업데이트 일정*을 갖고 있는 상자로 구성되어 있습니다.

현재 스팸 학습 소스

첫 번째 상자는 두 개의 링크와 두 개의 버튼을 사용하여 학습 소스를 구성하고 관리할 수 있습니다. 각 링크는 다양한 구성 값을 지정하는 새 패널을 표시합니다.

상자의 오른쪽 상단에 있는 두 개의 단추는 정의된 모든 연결에서 수행할 작업을 즉시 시작할 수 있게 해줍니다.

모든 연결 테스트

한 번에 모든 연결을 확인하려면, 많은 학습 소스가 정의되었거나 IMAP 서버에 대한 연결 속도가 느린 경우, 이 작업을 수행하는데 약간의 시간이 걸릴 수 있습니다.

지금 교육 시작

즉시 교육을 시작합니다. 버튼이 Training is running ... (학습 실행 중 ...)이라는 레이블로 바뀝니다.

> **참고:** 교육은 많은 요소에 따라 매우 오랜 시간이 걸릴 수 있습니다. 소스의 수, 연결 속도, 가장 중요한 것은 다운로드 할 전자 메일 수입니다.

기본적으로 비어있는 기본 구성은 학습에 사용되지 않지만 나중에 바로 추가할 수 있는 실제 학습 소스에 의해 나중에 상속되는 값만 제공합니다. 기본 설정 편집 링크를 클릭하면, 다음 설정을 구성할 수 있습니다.

기본 IMAP 호스트

교육 폴더가 포함된 IMAP 호스트

기본 사용자 이름

IMAP 호스트의 로그인 이름.

기본 암호

사용자의 암호.

기본 햄(ham) 폴더

햄(ham) 메시지 만 포함된 폴더의 이름입니다. 예를 들어, '깨끗한' 메시지 또는 받은 편지함만 저장하는 전용 폴더일 수 있습니다.

기본 스팸 폴더

스팸 메시지만 포함하는 폴더의 이름입니다.

자동 스팸 필터 교육 예약

두 번 연속 검사 사이의 시간 간격으로, **비활성화**하거나 **시간별, 일별, 주별** 또는 **월별** 간격으로 지정할 수 있습니다. 마우스 커서를 물음표 위로 옮길 때, 예정된 정확한 시간이 표시됩니다. 비활성화된 경우 스팸 방지 엔진을 수동으로 교육해야 합니다.

추가 스팸 학습 소스는 IMAP 스팸 학습 소스 추가 링크를 클릭하면, 나타나는 패널에 추가할 수 있습니다. 추가 학습 호스트에 대한 옵션은 기본 구성 옵션과 동일하지만 스케줄링은 항상 기본 구성에서 상속되며 3가지 새로운 옵션이 있습니다.

활성화

트레이닝 소스는 SpamAssassin을 교육받을 때마다 사용됩니다. 활성화되지 않은 경우, 소스는 자동 학습 중에 사용되지 않고, 수동 소스에서만 사용됩니다.

설명

이 소스에 대한 설명.

처리된 메일 삭제

전자 메일을 처리한 후에 삭제할지 여부를 선택합니다.

다른 옵션은 기본 구성처럼 정의할 수 있습니다. 이 옵션들이 다를 경우, 그것들이 기본값을 대체합니다. 소스 구성을 저장하려면, 원하는 모든 값을 설정한 후에 Add Training Source 버튼을 클릭해야 합니다. 교육 소스에서 여러 가지 조치를 수행할 수 있습니다.

- ☑☐ - IMAP 호스트의 상태를 사용 또는 사용 안함으로 토글합니다.
- - IMAP 호스트의 속성을 수정합니다.
-  - IMAP 호스트를 제거합니다.
-  - IMAP 호스트에 대한 연결을 테스트합니다.

> **참고:** 스팸 메일은 발신 메일뿐만 아니라 수신 메일에서도 SMTP 프록시가 활성화된 경우, 다른 방법으로 학습할 수 있습니다. 스팸 메일을 **spam@spam.spam**이라는 특수 주소로 보내고, 스팸이 아닌 메일을 **ham@ham.ham**으로 보내면 됩니다 .햄. 호스트 이름 **spam.spam** 및 **ham.ham**은 네트워크 설정 직후에 네트워크 구성에 추가되며 localhost의 별명입니다. 이 두 주소가 없으면, Endian UTM 어플라이언스의 *Menubar ‣ Network ‣ Edit hosts ‣ Add a host (호스트 추가)*에 추가할 수 있습니다.

SpamAssassin 규칙 업데이트 일정

이 상자에서는 **시간별, 일별, 주별** 및 **월별**의 네 가지 옵션 중에서 SpamAssassin 서명 자동 다운로드를 예약할 수 있습니다.

침입 방지

Endian UTM Appliance는 원치 않는 또는 불신하는 출처로부터의 연결을 차단하고 제거하기 위해 iptables에 직접 내장된 잘 알려진 침입 탐지 (IDS) 및 예방 (IPS) 시스템 스노트(snort)를 포함합니다.

이 페이지에는 침입 방지 시스템 및 규칙이라는 두 개의 탭이 있습니다.

버전 5.0에서 변경됨: *편집기 탭이 규칙 탭에 통합되었습니다.*

침입 방지 시스템

snort가 활성화되어 있지 않으면 IPS 활성화(Enable IPS) 레이블 옆의 회색 스위치  가 페이지에 나타나고 이를 클릭하여 서비스를 시작할 수 있습니다. 짧은 시간 간격 후에, 페이지는 상자들로 그룹화된 서비스를 구성할 수 있는 일부 옵션들을 포함할 것입니다.

침입 방지 시스템 설정

이 상자는 스노트 (snort) 규칙의 자동 다운로드 및 설치를 정의합니다.

SNORT 규칙 자동 가져 오기

이 상자를 선택하면 Endian UTM 어플라이언스가 Endian Network에서 자동으로 Snort 규칙을 다운로드합니다.

> **참고:** Endian UTM Appliance가 등록되지 않았거나 유지 관리가 만료된 경우, 규칙은 더 이상 다운로드되지 않습니다. 유익한 메시지는 페이지 하단에도 표시됩니다.

SNORT 규칙 업데이트 일정

규칙 다운로드 빈도: 드롭 다운 메뉴에서 *시간별, 일별, 주별* 또는 *월별* 옵션 중 하나를 선택할 수 있습니다. 이 옵션은 이전 옵션이 활성화된 경우에만 나타납니다.

새로운 위협 SNORT 규칙

이 상자에는 Endian 저장소에서 신종 위협 (Emerging Threats) 규칙을 다운로드하는 버튼과 마지막으로 규칙을 수동으로 다운로드한 정보 메시지가 있습니다.

```
Rules last updated:        2017-08-01 10:48:31
```

지금 규칙 업데이트

이 버튼을 클릭하면, IPS 서비스에 대한 서명이 emitingthreats.net 웹 사이트에서 즉시 다운로드 됩니다.

맞춤 SNORT 규칙

이 상자는 사용자 지정 SNORT 규칙이 포함된 파일을 Endian UTM Appliance에 업로드하는데 사용할 수 있습니다.

검색

이 버튼을 클릭하면, 열리는 파일 선택 창에서 파일 하나를 선택하십시오.

맞춤 규칙 업로드

이 버튼을 클릭하여 파일을 업로드하고 snort와 함께 사용하십시오.

규칙

규칙 탭에는 Endian UTM Appliance에 저장된 규칙 집합 목록과 포함된 규칙 수 및 수행할 수 있는 작업이 표시됩니다.

- ☑☐ - 규칙 세트의 상태를 사용 또는 사용 안함으로 토글합니다.
- ⚠ - 패킷에 적용되는 정책으로 통과하거나 삭제할 수 있습니다.
- ✎ - 규칙 세트의 속성을 수정합니다
- 🗑 - 규칙 세트를 제거합니다.

목록의 맨 아래에 있는 액션 선택 Choose an action 버튼을 사용하여 하나 이상의 규칙 세트에 대해 한 꺼번에 작업을 수행할 수 있습니다. 그것들을 선택하고 (파일 이름 왼쪽에 있는 체크 박스를 선택), 목록의 아래에 있는 버튼의 하나를 누르십시오.

Snort의 정책.

기본적으로 모든 규칙 세트에 대한 정책은 아이콘 passlog로 표시된 alert로 설정됩니다. 즉, 트래픽 흐름이 해당 규칙 또는 규칙 집합과 일치할 때마다 트래픽이 통과되고 침입 시도가 기록됩니다.

이 동작은 경고 아이콘을 클릭함으로써 정책을 *블록*으로 전환하며, 아이콘 로 표시하고 침입 시도가 차단되지만 로그 파일에 메시지가 기록되지 않도록 변경할 수 있습니다.

규칙 또는 전체 규칙 세트의 정책이 변경된 후에는 적용 버튼을 클릭하여 변경 사항을 적용해야 합니다.

휴지통 아이콘 🗑를 클릭하면, 규칙 집합을 삭제할 수 있고, 연필 아이콘 ✎을 클릭하면, 규칙 집합의 각 규칙을 독립적으로 편집할 수 있는 규칙 편집기가 열립니다.

편집 버튼을 선택하고 클릭하면 선택한 규칙 집합에 포함된 규칙 목록이 표시됩니다. 검색 레이블 옆의 텍스트 상자에 일부 용어를 입력하여 목록을 좁힐 수 있습니다. 이전 페이지로 돌아가려면 뒤로 버튼을 클릭합니다.

> **경고:** IPS를 켜는 것은 snort가 실행 중임을 의미하지만 아직 트래픽을 필터링하지 않습니다. snort에서 패킷을 필터링하려면 다양한 방화벽 구성 페이지에 정의 된 규칙에 대해 IPS 필터로 허용 정책을 선택해야합니다.

추가 참고:

방화벽 메뉴

Menubar ▸ Firewall

IPS를 설정하기위한 시각적인 단계별 자습서입니다.

고가용성 (High availability)

Endian UTM Appliance는 2개 이상의 Endian UTM Appliances를 사용하여 쉽게 설정할 수 있는 HA(고가용성) 모드를 지원합니다. 이 중 하나는 활성 (즉, **마스터**) 방화벽의 역할을 맡고, 나머지는 대기 (즉, **슬레이브**) 방화벽의 역할을 맡습니다.

고가용성의 배경은 동일한 시스템을 연결하여 마스터에 장애가 발생하면 슬레이브 중 하나가 즉시 인계받아 새로운 마스터가 되어 투명하게 대체 작동을 제공하는 것입니다. 이렇게 하면 중요한 네트워크 작업과 보안에 대해 탁월한 하드웨어 가용성과 중복성을 제공합니다. 시스템 대체 작동이 발생하는 일반적인 시나리오 중 하나는 기본 시스템에서 하드웨어 오류가 발생하는 경우입니다.

하지만 하나의 슬레이브 만 있으면 마스터의 직무를 즉시 수행하고, 2차 Endian UTM 어플라이언스로 원활한 장애 극복을 할 수 있습니다. 이 방식은 엔디안에서 지원하는 방식이므로 HA 서비스를 시작하려면 마스터 및 슬레이브 UTM 어플라이언스 하나를 다음 지침에 따라 구성해야 합니다.

> **참고:** Endian HA 시스템은 Endian 하드웨어 및 소프트웨어 어플라이언스에서 모두 지원됩니다. 하드웨어 또는 소프트웨어 선택에 관계없이 고가용성 모듈에는 2개의 완전히 동일한 하드웨어 플랫폼 (예: 2개의 미니, 2개의 매크로, 2대의 x86 시스템 등)이 필요합니다.

고가용성을 배치할 때 집중해야 할 중요한 점은 Endian UTM Appliance에 대한 모든 연결에 대한 복제 방법을 제공해야 한다는 것입니다. 완전한 복제 기능이 존재하도록 기본 장치 (예: WAN, LAN 등)의 모든 연결을 대기 장치에 복제해야 합니다.

이 페이지에는 처음에는 단 하나의 옵션 만 있습니다.

고 가용성 활성화

Endian UTM Appliance에서 HA를 사용하도록 설정합니다 (기본적으로 사용하지 않도록 설정됨).

> 경고: HA는 현재 핫스팟의 데이터베이스 자동 동기화를 지원하지 않습니다.

예(Yes)를 선택하면, 두 번째 드롭 다운 메뉴와 몇 가지 옵션이 나타납니다.

고 가용성 측면

Endian UTM Appliance가 마스터 또는 슬레이브로 작동하는 경우, 드롭 다운 메뉴에서 선택하십시오. 이 선택 사항에 따라 다른 구성 옵션을 사용할 수 있습니다. 그러나 슬레이브 장치를 구성하려면 마스터 장치가 이미 설정되어 있어야 합니다.

마스터 측에 대해 다음 옵션을 사용할 수 있습니다.

관리 네트워크

동일한 HA 설정의 일부인 모든 Endian UTM Appliance가 연결되어야하고 192.168.177.0/24로 기본 설정되는 특수 서브넷. 이 서브넷이 이미 다른 용도로 사용되지 않는 한 변경하지 않아도 됩니다.

마스터 IP 주소

관리 네트워크의 첫 번째 IP 주소입니다. 선택한 네트워크에서 자동으로 1로 설정되고 기본값은 192.168.177.1입니다.

다음 네 가지 옵션을 설정하여 장애 조치 이벤트가 발생할 때, 전자 메일로 알림을 받을 수 있습니다. 그것들은 *Menubar ‣ System ‣ Event notification*의 다음 행으로 단어를 넘기지 않습니다! (do not word wrap the following line!)의 다른 **이벤트 알림**을 위해 구성된 것과 같은 방법으로 구성됩니다.

알림: 수신자 이메일 주소

알림 전자 메일을 보내야하는 전자 메일 주소입니다.

알림: 보낸 사람 전자 메일 주소

알림을 보낸 사람으로 표시될 사용자 지정 전자 메일 주소입니다.

알림: 이메일 제목

알림 전자 우편의 제목.

알림: 사용할 SMTP 서버

알림 전자 메일을 보내는데 사용되는 SMTP 서버입니다.

STP 사용

스패닝 트리 프로토콜 STP를 사용할지 여부를 드롭 다운 메뉴에서 선택합니다. 이 옵션과 다음 옵션은 Endian UTM Appliance가 게이트웨이 모드에 있을때 중요합니다.

STP 브리지 우선 순위

브릿지의 우선 순위. 마스터 쪽에서는 1이어야 합니다.

HA가 활성화된 후 IP 주소가 있는 슬레이브 목록, 관리 GUI에 액세스 할 수 있는 링크 및 슬레이브를 삭제할 수 있는 두 번째 상자가 나타납니다.

HA(고가용성) 관리 네트워크

Endian UTM Appliance는 특수 네트워크를 사용하여 마스터를 슬레이브 장치에 연결합니다 (기본값은 192.168.177.0/24). 이 네트워크가 다른 영역에서 이미 사용된 경우, HA 관리 네트워크에 다른 범위의 IP 주소 (예: 172.19.253.0/24 또는 10.123.234.0/28)를 할당하면 됩니다.

관리 네트워크의 요구 사항은 다음과 같습니다.

다른 영역과는 다른 고유한 서브넷이어야 합니다.

마스터와 모든 슬레이브를 수용할 만큼 충분히 커야 하므로 마스터와 슬레이브 장치만 있으면 192.168.177.0/29만큼 작은 네트워크여야 합니다.

관리 네트워크는 GREEN 네트워크의 인터페이스로 생성되며, 장치 또는 네트워크 상태를 볼 때 이와 같이 표시됩니다.

> **경고:** 현재 LAN 설정에서 관리 네트워크에 도달할 수 있는지 확인하십시오. 그렇지 않으면, 마스터 장치에 로그인 할 수 없습니다!

마스터 유닛이 구성된 후에는 슬레이브가 될 두 번째 Endian UTM Appliance를 설정할 수 있습니다.

슬레이브 측에서는 다음과 같은 옵션을 사용할 수 있습니다.

마스터 IP 주소

마스터 장치의 IP 주소. 관리 네트워크가 변경되지 않은 경우, 기본값은 192.168.177.1/24입니다. 이 값은 마스터 장치의 *마스터 IP 주소* 옵션 값으로 나타나는 값과 **반드시** 일치해야 합니다.

마스터 루트 암호

마스터의 콘솔 **루트** 사용자 (그래픽 관리 인터페이스가 **아닌**!)의 암호.

이 데이터는 마스터가 필요한 모든 정보를 검색하고 동기화를 유지하기 위해 슬레이브에서 사용됩니다.

STP 사용

스패닝 트리 프로토콜 STP를 사용할지 여부를 드롭 다운 메뉴에서 선택합니다. 슬레이브 측에서는 이 옵션은 마스터 측에서와 동일한 값을 가져야 합니다.

STP 브리지 우선 순위

브릿지의 우선 순위. 슬레이브 쪽에서는 마스터 쪽보다 높아야 합니다. 슬레이브에서 이 값이 **1**로 설정된 경우, 여기에 **2**로 설정하십시오.

저장 직후, 관리 네트워크가 생성된 후 마스터와 슬레이브가 동기화를 시작하기 때문에 장치에 대한 연결이 일시적으로 손실됩니다.

동기화 프로세스가 완료되면, 대기 모드 상태가 되어 관리 네트워크를 통해서만 마스터에 연결되기 때문에 슬레이브 자체는 이전 IP 주소 (공장 출하시 또는 이전의 GREENIP 주소)를 통해 더 이상 도달할 수 없습니다 . 업데이트, 업그레이드, 또는 장치 백업 (이것들은 슬레이브 장치에서 수동으로 수행해야 함) 등을 제외하고는 기본 장치 (서비스 활성화, 설정 변경, VPN 사용자 삭제 등)의 모든 변경 사항이 종속 장치에 자동으로 동기화됩니다.

또한, 슬레이브 엔디안 장치는 마스터의 슬레이브 목록에 자동으로 나타나고, 슬레이브 목록에서 각 항목 옆에 있는 `관리 GUI로 이동` 링크를 따라 마스터에서 액세스 할 수 있는 정보 전용 웹 인터페이스로 전환합니다.

RED MAC 주소

HA 페일 오버 동안 RED 인터페이스 MAC 주소는 슬레이브 장치로 복제되지 않습니다. 이것은 ISP가 *고정 IP* 설정을 사용해야 하는 경우 문제를 나타낼 수 있습니다. 이 경우 ISP에서 할당한 IP 주소는 DHCP 서버에서 클라이언트로 할당된 고정 IP와 마찬가지로 클라이언트 네트워크 인터페이스의 MAC 주소에서 결정됩니다. 슬레이브 장치로 다시 연결할 수 없습니다. 이러한 상황을 피하려면, HA(고가용성)가 제대로 작동하려면 RED 인터페이스에서 스푸핑 된 MAC 주소 기능을 사용해야 합니다. 이렇게 하면, HA가 활성화될 때, MAC 주소가 대기 장치로 전달되어 수동 개입이 필요하지 않습니다. 이것은 활성화되기 전에, 슬레이브에서 *Menbar ‣ Network ‣ Interface ‣ Edit main uplink (메인 업링크 편집) ‣ Advanced settings (고급 설정)*과 마스터에서 RED 인터페이스의 MAC 주소 지정 아래의 사용자 정의 MAC 주소 사용 옵션을 선택하여 수행할 수 있습니다. 또는 MAC 주소를 네트워크 설치 마법사의 4단계에서 입력하여, *스푸핑 MAC 주소*에 마스터의 MAC 주소를 옵션으로 쓸 수 있습니다.

추가 참고: Endian UTM Appliance에서 HA를 구성하는 단계별 안내서.

트래픽 모니터링

> **참고:** 사용 가능한 리소스가 제한되어 있어, Mini Appliance에서 트래픽 모니터링 서비스를 사용할 수 없습니다.

트래픽 모니터링은 ntopng에 의해 수행되며, 이 페이지의 주 스위치를 클릭하여 활성화 또는 비활성화 할 수 있습니다. 트래픽 모니터링이 활성화되면, 관리 인터페이스에 대한 링크가 페이지의 아래쪽에 표시됩니다. 관리 인터페이스에서 트래픽은 호스트, 프로토콜, 로컬 네트워크 인터페이스 및 기타 여러 유형의 정보로 시각화하고 분석할 수 있습니다. 이러한 모든 작업은 **로그 및 보고서 메뉴**의 트래픽 모니터링 모듈에서 직접 수행할 수 있습니다.

미니 어플라이언스가 아닌 한, 이 페이지에서는 단 하나의 옵션만 사용할 수 있습니다. 이 경우 옵션이 전혀 없습니다.

호스트의 기록 보관

기본적으로 각 호스트의 기록에 대한 정보는 디스크에 저장되지 않습니다. 호스트 별 로깅을 사용하려면 확인란을 선택하십시오.

> 경고: 이 옵션을 사용하면, 각 호스트에 대한 여러 파일이 디스크에 기록되고 해당 호스트가 Endian UTM Appliance에 연결할 때마다 업데이트 됩니다. 트래픽 모니터링이 활성화되고, 네트워크 트래픽이 많으면, 디스크 공간이 빠르게 채워지고 디스크 액세스가 시스템 성능의 병목 현상이 될 수 있습니다.

SNMP 서버

SNMP는 네트워크에 연결된 장치를 모니터링하는데 사용되며, 예를 들어, 내부 인프라의 상태를 제어하는데 사용될 수 있습니다.

SNMP 서버를 활성화하려면, *Enable SNMP server* label 옆에 있는 회색 스위치를 클릭하기만 하면 됩니다. 설정을 마치면, *설정* 상자에 몇 가지 옵션이 나타납니다.

커뮤니티 문자열

SNMP 클라이언트로 데이터를 읽는데 필요한 키입니다.

위치

식별 문자열은 무엇이든 설정할 수 있지만, Endian UTM Appliance의 위치를 설명하는 것이 좋습니다.

전체 알림 전자 메일 주소 덮어쓰기

SNMP 서버는 전자 메일 주소를 시스템 연락처로 구성해야 하며, 설치 과정에서 제공되는 글로벌 전자 메일 주소가 기본적으로 사용됩니다. 사용자 지정 전자 메일 주소를 사용하려면, 확인란을 선택하여 다음(next) 옵션을 활성화하십시오.

시스템 담당자 전자 메일 주소

연락할 관리자의 전자 메일 주소를 작성하십시오.

서비스 품질

QoS 모듈의 목적은 서비스에 따라 Endian UTM Appliance를 통해 흐르는 IP 트래픽의 우선 순위를 정하는 것입니다. 즉, QoS는 주어진 서비스에 대해 주어진 양의 수신 가능 대역폭과 송신 가능 대역폭을 예약하는 편리한 방법입니다. 일반적으로 대량 트래픽보다 우선 순위가 필요한 애플리케이션은 SSH 또는 VoIP와 같은 대화형 서비스입니다.

QoS 구성 옵션은 *장치, 클래스, 규칙* 및 *태깅*의 네 가지 탭으로 배열됩니다.

장치들

장치 탭은 QoS의 시작 페이지이기도 하며 처음에는 비어 있습니다. 일단 채워지면, 모든 Quality of Service 장치 목록을 보여주는 테이블이 나타나고, 각 장치에 대해 일부 매개 변수와 사용 가능한 작업이 표시됩니다.

목록 위에 있는 Quality of Service Device 추가 링크를 클릭하고, 몇 가지 옵션을 구성하여 새 QoS 장치를 추가할 수 있습니다.

대상 장치

이 장치에서 사용할 네트워크 인터페이스입니다. 선택 사항은 존재하는 네트워크 인터페이스, 시스템에서 활성화된 구역, 업링크 및 정의된 경우 OpenVPN 터널이며, 드롭 다운 메뉴에서 선택할 수 있습니다.

다운 스트림 대역폭 (kbit/s)

인터페이스의 다운 스트림 속도.

업스트림 대역폭 (kbit / s)

인터페이스의 업스트림 속도.

활성화

QoS (기본값)를 사용할지 여부를 설정합니다.

장치에서 사용할 수 있는 작업은 다음과 같습니다.

- ☑☐ - 장치를 활성화 또는 비활성화합니다.
- ✎ - 장치의 속성을 수정합니다.
- 🗑 - 장치를 제거합니다.

장치를 편집할 때, 현재 장치의 매개 변수를 수정하는 새 장치를 추가할 때와 동일한 양식이 열립니다.

추가된 모든 장치에 대해 클래스 탭 아래에 4개의 항목이 표시됩니다. 각각 높음(high), 보통(medium) 및 낮음(low)의 3개의 우선 순위와 대량 트래픽 용 (아래 참조)의 4개 항목입니다.

클래스

이 탭에는 작성된 모든 Quality of Service 클래스 목록 (있는 경우)이 표시됩니다. 각 항목에 대해 여러 데이터가 표시됩니다. 새 항목은 클래스 목록 위에 있는 서비스 클래스 추가 링크를 클릭하여 추가할 수 있습니다. 구성할 매개 변수는 목록에 표시된 것과 동일합니다.

이름

Quality of Service 클래스의 이름.

QOS 장치

드롭 다운 메뉴를 사용하여, 클래스를 작성되기 위한 Quality of Service 디바이스를 선택할 수 있습니다.

> **힌트:** QoS 클래스를 정의하기 전에, 하나 이상의 QoS 장치가 만들어져 있어야 합니다.

예약

장치의 전체 사용 가능한 대역폭에서 이 클래스에 대해 예약된 대역폭의 양 (백분율 또는 초당 킬로 비트).

한도

이 클래스에서 사용할 수 있는 최대 대역폭 양 (백분율 또는 초당 킬로 비트).

우선 순위

드롭 다운 메뉴에서 선택한 클래스 우선 순위 0 (낮음) ~ 10 (높음)

> **참고:** 예약된 비율의 합은 장치 당 100보다 클 수 없습니다. 또한 예약된 대역폭은 한계 대역폭보다 클 수 없습니다.

사용할 수 있는 작업은 다음과 같습니다.

-  - 장치의 속성을 수정합니다.
-  - 목록에서 클래스를 이동합니다.
-  - 장치를 제거합니다.

등급은 목록 위아래로 이동할 수 있습니다. 목록의 맨 위에 있는 항목은 대역폭이 모든 트래픽에 충분하지 않고, Endian UTM Appliance가 우선 순위를 정해야 하는 트래픽을 선택할 필요가 있을 때, 가장 먼저 처리됩니다.

규칙

세 번째 탭에는 이미 정의된 QoS (Quality of Service) 규칙 목록이 표시되며, 각 클래스에 속해야 하는 트래픽 유형을 지정할 수 있습니다. 새 서비스 품질 규칙을 추가하려면, 서비스 품질 규칙 추가 링크를 클릭하십시오. 열리는 양식에서는 방화벽 규칙을 정의하는데 사용되는 것과 매우 유사하므로 여러 값을 구성해야 합니다. 선택을 쉽게 하고 구성을 안내하기 위해 여기에 많은 드롭 다운 메뉴가 사용됩니다.

> **힌트:** 2.5.X 버전의 IPsec 사용자와 관련된 규칙과 유사한 규칙을 정의하려면, 두 가지 옵션에 대해 다음 값을 지정해야 합니다.
>
> - 원본: IPsec 사용자가 브리지된 영역입니다.
> - 대상 네트워크/IP: IPsec 사용자 뒤에 있는 원격 서브넷입니다.

소스

드롭 다운 메뉴에서 트래픽 소스 (Zone 또는 인터페이스, 네트워크, IP 또는 MAC 주소)를 선택하십시오. 이 선택 사항에 따라 다른 값을 지정할 수 있습니다. 표시될 사용가능한 구역 또는 인터페이스, 또는 하나 이상의 IP 주소, 네트워크 또는 MAC 주소가 표시될 것입니다.

대상 장치/트래픽 클래스

드롭 다운 메뉴에서 대상 장치 또는 트래픽 클래스를 선택하십시오.

대상 네트워크 / IP

텍스트 영역에 대상 네트워크 또는 IP 주소를 작성하십시오. 이 주소는 이전 옵션에서 선택한 장치 또는 트래픽 클래스에서 도달할 수 있어야 합니다.

서비스/포트, 프로토콜

이 두 개의 드롭 다운 메뉴는 규칙 (TCP, UDP 또는 TCP + UDP 프로토콜 중 하나를 선택할 때)에 대한 서비스, 프로토콜 및 대상 포트를 정의하는데 사용됩니다. 서비스/프로토콜/포트는 HTTP/TCP/80, <ALL>/TCP+UDP/0:65535 또는 <ANY>와 같이 미리 정의된 일부 조합으로 모든 서

비스, 프로토콜 및 포트의 바로가기입니다. 마지막으로 대상 포트에서 하나 이상의 사용자 지정 포트 번호를 제공할 수 있습니다 (이는 일부 서비스가 표준 포트에서 실행되지 않을 때 유용함).

유형

트래픽을 표시하는데 사용할 태그를 (TOS 플래그, DSCP 클래스 또는 DSCP 값) 드롭 다운 메뉴에서 선택하십시오. 선택에 따라 <ANY>를 선택하지 않으면, 이 옵션 중 하나가 나타납니다.

다음 TOS 플래그로 트래픽 일치

이전 드롭 다운 메뉴에서 TOS 또는 DSCP 클래스를 선택하면, 다른 드롭 다운 메뉴에서 일치시킬 트래픽에 적합한 값을 선택할 수 있습니다.

DSCP 값

이 필드는 위의 TOS/DSCP 유형에서 DSCP 값을 선택한 경우에만 나타납니다. 일치할 때, 규칙을 실행하는데 사용되는 DSCP에 대한 사용자 지정 값을 입력할 수 있습니다.

활성화

규칙을 사용하려면 확인란을 선택하십시오.

주석

규칙을 식별하는 주석.

> **참고:** Quality of Service 클래스에 둘 이상의 서비스가 있는 경우, 이 모든 서비스가 함께 예약된 대역폭을 공유하게 됩니다.

규칙에서 사용할 수 있는 작업은 다음과 같습니다.

- ☑☐ - 규칙을 활성화 또는 비활성화합니다.
- ✎ - 규칙의 속성을 수정합니다.
- 🗑 - 규칙을 제거합니다.

태깅

네 번째 탭은 트래픽을 분류하고 우선 순위를 지정하는 데 사용되므로 다른 탭과 다릅니다. 즉, 트래픽을 표시하거나 태그를 지정하여 외부 장치가 트래픽을 적절하게 처리하도록 할 수 있습니다. 이것은 대역폭이 제한된 시나리오에서 특히 유용하며, 모뎀과 같은 업 링크 장치는 패킷 내의 TOS 또는 DSCP 플래그에 기초하여 트래픽의 우선 순위를 정할 수있다. `서비스 품질 규칙 추가` (Add Quality of Service Rule) 링크를 클릭하면 규칙 탭에있는 편집기와 비슷한 편집기가 열립니다. 사용할 수있는 옵션은 다음과 같습니다.

소스

드롭 다운 메뉴에서 트래픽 소스 (Zone 또는 인터페이스, 네트워크 또는 IP 또는 MAC 주소)를 선택하십시오. 이 선택 사항에 따라 다른 값을 지정할 수 있습니다. 표시되는 영역 또는 사용 가능한 인터페이스의 영역 또는 인터페이스 또는 하나 이상의 IP 주소, 네트워크 또는 MAC 주소. 기본값은 <ANY>입니다. 즉, 규칙이 모든 트래픽에 적용됩니다.

대상

드롭 다운 메뉴에서 트래픽 대상 (Zone 또는 인터페이스, 네트워크 또는 IP)을 선택하십시오. 이 선택 사항에 따라 다른 값을 지정할 수 있습니다. 영역 또는 표시된 인터페이스의 인터페이스 또는 하나 이상의 IP 주소 또는 네트워크.

서비스/포트, 프로토콜

이 두 개의 드롭 다운 메뉴는 규칙 (TCP, UDP 또는 TCP + UDP 프로토콜 중 하나를 선택할 때)에 대한 서비스, 프로토콜 및 대상 포트를 선택하는데 사용됩니다. 서비스/프로토콜/포트는 HTTP/TCP/80, <ALL>/TCP+UDP/0:65535 또는 <ANY>와 같이 미리 정의된 일부 조합으로 모든 서비스, 프로토콜 및 포트의 바로가기입니다.

대상 포트

이 텍스트 필드에서 하나 이상의 사용자 정의 포트 번호를 제공할 수 있습니다. 일부 서비스가 표준 포트에서 실행되지 않을 때 유용함).

유형

트래픽을 표시하는데 사용할 태그 (TOS 플래그, DSCP 클래스 또는 DSCP 값) 드롭 다운 메뉴에서 선택하십시오. 선택에 따라, 이 옵션 중 하나가 나타납니다.

다음 TOS 플래그로 트래픽 태그를 지정

이 드롭 다운은 위에서 TOS를 선택한 경우에만 나타납니다. 일치하는 모든 패킷에 설정할 TOS 플래그를 정의할 수 있습니다.

다음 DSCP 클래스로 트래픽 태그 지정

위의 DSCP 클래스를 선택하면이 드롭 다운이 나타납니다. 일치하는 모든 패킷에 설정할 DSCP 클래스를 정의할 수 있습니다.

다음 DSCP 값으로 트래픽 태그를 지정.

이 필드는 위의 유형 필드에서 DSCP 값을 선택한 경우에만 나타납니다. DSCP에 대한 사용자 지

정 값을 입력할 수 있으며, 일치하는 모든 패킷에 설정됩니다.

활성화

규칙을 사용하려면 확인란을 선택하십시오.

주석

규칙을 식별하는 주석.

규칙에서 사용할 수 있는 작업은 다음과 같습니다.

- ☑☐ - 규칙을 활성화 또는 비활성화합니다.
-  - 규칙의 속성을 수정합니다.
-  - 규칙을 제거합니다.

방화벽

이 섹션에서는 네트워크 트래픽이 Endian UTM Appliance를 통해 흐르는지 여부 및 방법을 지정하는 규칙을 설정할 수 있습니다. Endian UTM 어플라이언스의 방화벽은 각기 다른 모듈로 나누어져 있으며 각각 특정 유형의 트래픽을 모니터링하고 허용하거나 차단합니다. 사용할 수 있는 모듈은 다음과 같습니다.

- 포트 포워딩/NAT - 포트 포워딩 및 abbr:NAT (네트워크 주소 변환).
- 발신 트래픽 - 발신 트래픽, 즉 RED 인터페이스로 향하는 트래픽
- 영역 간 트래픽 - 영역 간 트래픽.
- VPN 트래픽 - VPN 사용자가 생성한 트래픽입니다.
- 시스템 액세스 - Endian UTM Appliance 호스트 자체에 대한 액세스 권한을 부여합니다.
- 방화벽 다이어그램 - 각 유형의 방화벽에 의해 가로챌 트래픽을 보여주는 그림입니다.

해당하는 모든 기존 규칙이 나열된 각 하위 메뉴 내에서 모든 유형의 서비스 또는 모든 포트/프로토콜에 대해 사용자 정의된 규칙을 추가할 수 있습니다. 방화벽이 구성되는 다양한 부분은 다양한 유형의 트래픽을 나타냅니다 (예: OpenVPN이 VPN 사용자와의 트래픽을 관리하고 영역 간 트래픽은 영역에서 영역으로 트래픽을 제어함). 겹치거나 심지어 겹치지 않도록 설계되었습니다. 규칙 대조. 즉, 두 개의 다른 방화벽 모듈에 두 개의 규칙을 작성하여 결합 효과로 인해 원치 않는 블록 또는 패킷 액세스가 발생하는 것입니다.

Endian UTM Appliance에 의해 제어되는 네트워크를 분리하는 선택은 방화벽 구성을 매우 복잡하게 만드는 방화벽 관리를 용이하게 합니다. 사실, 각 모듈은 독립적인 방화벽으로 간주될 수 있으며, 그 결합된 효과는 Endian UTM Appliance를 통해 가능한 모든 패킷 흐름을 포괄합니다.

또한 위에 나열된 모듈 중 하나 이상이 비활성화되거나 제거될 수 없는 규칙이 있을 수 있습니다. 이것들은 Endian UTM Appliance에서 실행중인 서비스의 Endian Network 인프라와의 정확한 상호 운용성을 가능하게 하는 시스템 서비스 (또는 시스템 규칙)의 규칙입니다.

여기에 정의된 규칙은 2.4 커널 이후의 표준 Linux 방화벽 도구인 iptables 명령으로 변형되어 테이블, 체인 및 규칙으로 구성됩니다. 방화벽 규칙을 구성하는 여러 가지 요소에 대해 더 자세히 설명하거나 복잡한 방화벽을 미세 조정하고 관리하는 방법을 배우려면 모든 Linux 상자의 ***iptables(8)*** 매뉴얼 페이지를 읽는 것이 좋습니다. 또는 인터넷에서 사용할 수 있는 수많은 온라인 리소스 또는 자습서 중 일부를 선택하십시오.

공통 구성 항목

규칙을 추가할 때 방화벽 부품의 대부분의 구성 옵션은 동일한 소프트웨어인 **iptables**로 구성되므로 동

일한 유형 (예: 소스 또는 대상 인터페이스)입니다. 따라서, 이 섹션을 짧고 읽기 쉽게 유지하기 위해 모든 공통 구성 항목을 그룹화해서 설명합니다. 다음 섹션에는 방화벽의 해당 부분에 고유한 옵션에 대한 설명만 포함됩니다.

힌트: 선택할 값 목록이있는 경우 Ctrl 키 (독일어 STRG)를 누른 상태에서 각 값을 클릭하고, 그렇지 않고, 텍스트 상자가 있으면 한 줄에 하나의 값을 씁니다.

소스 또는 수신 IP

일반적으로 드롭 다운 메뉴의 형태로, 이 설정이 일치되어야 하는 소스 또는 수신 연결의 유형입니다. 유형에 따라 텍스트 상자에 다른 값을 쓰거나 선택할 수 있습니다.

- 구역/ VPN/업링크. 소스 구역, VPN 클라이언트 또는 업링크
- 네트워크/IP/범위. 네트워크 주소, IP 주소 또는 IP 범위.
- OpenVPN 사용자 및 L2TP 사용자. 각각의 OpenVPN 또는 2TP 사용자.

대상 또는 대상

규칙이 일치해야 하는 세 가지 유형의 대상 중에서 선택할 수 있는 다른 드롭 다운 메뉴는 소스(Source)에서와 동일합니다.

- 영역/VPN/업링크. 원본 영역, VPN 클라이언트 또는 업 링크
- 네트워크/IP/범위. 네트워크 주소, IP 주소 또는 IP 범위.
- OpenVPN 사용자 및 L2TP 사용자. 각각의 OpenVPN 또는 2TP 사용자.

서비스, 포트 및 프로토콜

서비스는 대개 포트와 프로토콜의 조합으로 정의됩니다. 예를 들어, SSH 서비스는 기본적으로 포트 22에서 실행되며 TCP 프로토콜을 사용합니다. 이 옵션은 규칙에 대한 포트 및 프로토콜을 정의하고, 텍스트 영역에서 프로토콜과 포트 범위를 설정하게 될 사전 정의된 *서비스*를 선택하거나 하나의 *프로토콜*과 선택적으로 포트 또는 포트 범위를 선택하는 2개의 드롭다운 메뉴로 구성되어 있습니다. 사용 가능한 프로토콜은 다음과 같습니다. 가장 많이 사용되는 TCP 및 UDP, 터널에서 사용되는 GRE, IPsec에서 사용되는 ESP 및 **ping** 및 **traceroute** 명령에 사용되는 ICMP가 있습니다.

> **참고:** 드롭 다운 메뉴에서 선택할 수 있는 수십 개의 사전 정의된 서비스가 있으며, 가장 일반적인 서비스가 인터넷에 액세스 할 수 있도록 충분해야 합니다. 사용자 정의 포트 및 프로토콜 조합은 서비스가 표준 포트에서 실행되고 있지 않은 경우에만 사용해야 합니다 (예: SSH 서버가 포트 2345를 수신 대기하거나 웹 서버가 포트 7981에서 수신 대기) 또는 서비스가 특정 포트를 사용하는 경우 (예: 인터넷상의 멀티 플레이어 게임)에만 사용해야 합니다.

정책, 필터 정책

현재 규칙과 일치하는 패킷을 수행하는 작업입니다. 드롭 다운 메뉴는 다음 네 가지 옵션 중에서 선택할 수 있습니다.

- IPS로 허용하십시오. 패킷은 통과시키되 **침입 방지 시스템**으로 확인하십시오.
- 허용. 체크하지 않고 패킷을 전달하십시오.
- 하락. 보낸 사람에게 알리지 않고 패킷을 버립니다.
- 거절. 패킷을 폐기하고 응답으로 오류 패킷을 보냅니다.

활성화

생성된 모든 규칙은 기본적으로 사용하도록 설정되어 있지만 체크 박스를 해제하여 저장하고 활성화할 수는 없습니다. 규칙을 사용하지 않으면 연결 문제를 해결하는데 유용할 수 있습니다.

로그, 허용된 모든 패킷 기록

기본적으로 트래픽이 필터링되면 로그 항목이 기록되지 않습니다. 규칙에 대한 로깅을 사용하려면 상자를 선택하십시오.

> **경고:** 분석할 많은 트래픽과 패킷이 있는 경우, 로그 파일의 크기가 급격히 커질 수 있으므로, 이 경우에는 로그 디렉토리를 정기적으로 확인하여 공간이 부족하지 않도록 하십시오!

설명

규칙의 목적을 기억하기 위한 규칙에 대한 설명 또는 주석.

위치

iptables 규칙은 목록에 나타나는 순서대로 처리되고 일부는 "종결"규칙, 즉 패킷을 삭제하거나 거부하고 후속 규칙의 처리를 중지할 수 있습니다. 이 드롭 다운 메뉴를 사용하면, 이 규칙을 저장할 위치를 선택할 수 있습니다.

액션(작업)

모든 규칙에서 몇 가지 작업을 수행할 수 있습니다.

- ⬆ ⬇ - 목록에서 규칙을 위 또는 아래로 이동합니다.
- ☑ ☐ - 규칙을 활성화 또는 비활성화합니다.
- ✎ - 규칙을 수정합니다.
- 🗑 - 규칙을 제거합니다.

> **힌트:** 순서가 중요하다는 것을 기억하십시오! 방화벽 규칙은 위에서 아래로 나타나는 페이지 순서대로 처리됩니다.

마지막으로, 모든 변경 사항이 방화벽 규칙에 저장되면, 구성을 다시 로드하기 위해 방화벽을 다시 시작해야 합니다. 클릭할 수 있는 적용 버튼이 있는 설명선이 나타나 이 필요성을 상기시켜줄 것입니다.

포트 포워딩 / NAT

포트 포워딩 / NAT 모듈은 *포트 포워딩 / 목적지 NAT, 소스 NAT* 및 *수신 라우트 된 트래픽*의 세 가지 탭으로 구성됩니다. 이 모듈의 목적은 RED 구역 (Uplink)으로부터 Endian UTM Appliance 및 다른 구역 (ORANGE, GREEN, BLUE)들로 흐르는 모든 트래픽을 관리하는 것입니다.

포트 포워딩 / 목적지 NAT

*대상 NAT*는 일반적으로 신뢰할 수 없는 네트워크에서 네트워크 액세스를 제한하거나 신뢰할 수 없는 네트워크에서 오는 트래픽을 지정된 포트 또는 주소-포트 조합으로 리디렉션하는데 사용됩니다. 어떤 인터페이스에서 어떤 포트를 어떤 호스트 및 포트로 전달해야 하는지 정의할 수 있습니다.

구성된 규칙 목록에는 여러 정보가 표시됩니다. 트래픽과 규칙이 일치하는 순서를 나타내는 ID (#), 수신 IP 주소, 트래픽이 전송되는 서비스 (예: 포트 및 프로토콜), 트래픽에 적용된 *정책, 변환* 대상 주소 (즉, 트래픽을 리디렉션 할 호스트 및 포트), 사용자 지정 *비고* 및 사용 가능한 *작업* 등입니다.

규칙을 편집할 때, 새 규칙을 추가할 때와 같은 양식이 새 포트 전달 / 대상 NAT 추가 규칙을 클릭하여 열립니다. 양식의 오른쪽 상단에 있는 링크를 사용하면 단순 모드 또는 고급 모드를 선택할 수 있습니다. 후자의 모드는 액세스 규칙, 정책 및 번역 유형을 고급 설정으로 구성할 수도 있습니다.

일반 옵션 외에도 다음과 같은 다른 설정을 구성할 수 있습니다.

번역 대상

양식의 이 부분은 현재 편집 모드 (단순 또는 고급)에 따라 변경됩니다. 모드가 고급으로 설정된 경우, 하위 규칙에서 Access를 추가하는 것 외에도 다양한 유형의 번역 중에서 선택할 수 있는 추가 유형 드롭 다운 메뉴가 있습니다.

> **경고:** 항상 **번역 대상** 옵션 아래의 텍스트 입력란에 유효한 값 (IP 주소, 네트워크, OpenVPN 사용자 등)을 추가하는 것을 잊지 마십시오. 그렇지 않으면, 규칙이 **적용되지 않습니다**.

1. 첫 번째는 IP이며 단순 모드에서 사용할 수 있는 유일한 IP에 해당합니다. 여기에는 목적지 IP 주소 (포트 및 NAT 외), 전달할 포트 또는 포트 범위, NAT를 적용할 것인지 또는 들어오는 패킷에 적용할 것인지를 기록해야 합니다.

2. *OpenVPN 사용자*: 하나의 OpenVPN 사용자를 트래픽의 대상 대상으로 선택합니다.

3. *로드 밸런싱*: 단일 IP의 병목 현상이나 과부하를 피하기 위해 트래픽을 분할할 IP 주소의 범위를 지정하십시오.

4. *네트워크를 매핑하십시오*. 들어오는 트래픽을 번역할 하위 네트워크를 삽입하십시오.

> **참고:** *지도 네트워크* 변환은 정적으로 주소의 전체 네트워크를 다른 주소 네트워크에 매핑합니다. 자회사가 모두 동일한 내부 네트워크를 사용하는 회사에 유용할 수 있습니다. 실제로, 이 경우에 모든 네트워크는 네트워크 매핑을 통해 서로 연결할 수 있습니다.
>
> 예를 들면 다음과 같습니다.
>
> 원본 네트워크 1: 192.168.0.0/24
> 매핑된 네트워크 1: 192.168.1.0/24
> 원본 네트워크 2: 192.168.0.0/24
> 매핑된 네트워크 2: 192.168.2.0/24

5. L2TP 사용자 : 하나의 L2TP 사용자를 트래픽의 대상 대상으로 선택합니다.

네트워크 맵핑 옵션을 선택할 때를 제외하고는 트래픽을 전송할 포트 또는 포트 범위를 정의하고 트래픽에 NAT를 적용할지 여부는 항상 정의할 수 있습니다. Do not NAT를 선택한 경우 Access From (고급 모드)에서 필터 정책을 정의할 수 없습니다.

> **경고:** IP, OpenVPN 사용자, L2TP 사용자 또는로드 밸런싱을 선택할 때는 포트 범위가 1에서 1로 매핑되지 않고 라운드 로빈 밸런싱이 수행됩니다. 예를 들어 들어오는 포트 137:139를 대상 포트 137:139에 매핑하면 이러한 포트가 임의로 사용됩니다. 포트 138으로 들어오는 트래픽은 예기치 않게 137, 138 또는 139로 리디렉션 될 수 있습니다. 변환 *포트/범위* 필드 그러한 경우를 피하려면 비워 두십시오.

- '하위 규칙'에서 액세스하십시오. 거의 모든 규칙은 Endian UTM Appliance에 연결되는 영역에 따라 클라이언트에 대한 액세스를 제한하는 등 몇 가지 규칙을 규칙에서 추가하여 거의 자세히 규정할 수 있습니다. 고급 모드를 선택하면 규칙에서 액세스 할 수 있습니다 (아래 참조). 결과적으로 정의된 액세스 정책의 수에 따라 둘 이상의 행에 규칙이 나뉘어 나타날 수 있습니다. 하위 규칙의 각 액세스는 주 규칙을 변경하지 않고 개별적으로 삭제할 수 있습니다. 각 하위 규칙은 다른 필터 정책을 가질 수도 있습니다.

포트-전달 문제 해결.

포트 포워딩이 작동하지 않는데에는 주로 두 가지 이유가 있습니다.

1. Endian UTM 어플라이언스는 NAT 장치 뒤에 있습니다.

   이 경우 Endian UTM 어플라이언스와 인터넷 사이에 라우터와 같은 장치 또는 다른 방화벽과 같은 장치가 있는 경우에는 직접 들어오는 연결을 허용하지 않습니다. 해결책은 가능한 경우, Endian UTM Appliance의 RED IP로 해당 장치에서도 포트 포워딩을 구성하는 것입니다.

2. 대상 서버가 잘못된 기본 게이트웨이를 가지고 있습니다.

   포트 전달 규칙의 대상으로 설정된 서버가 잘못되었거나 기본 게이트웨이가 구성되지 않았습니다. 연결은 대상 IP 주소로 보내지지만 잘못된 기본 게이트웨이로 인해 패킷은 Endian UTM Appliance를 통해 전달되지 않습니다. 해결 방법은 서버의 게이트웨이를 수정하는 것입니다.

소스 NAT

이 탭에서 나가는 연결에 SNAT를 적용하는 규칙을 정의할 수 있습니다. 소스와 대상 IP 주소, 서비스, NAT 상태, 규칙의 사용자 정의 설명, 및 사용 가능한 조치가 각각 표시되는 이미 정의된 목록이 표시됩니다.

원본 NAT는 Endian UTM Appliance 뒤에 있는 서버가 자체 외부 IP를 가지고 있으므로 나가는 패킷이 방화벽의 RED IP 주소를 사용하지 않아야 하고, 서버 중 하나인 경우 유용할 수 있습니다. 새 규칙을 추가하려면, 새 소스 NAT 규칙 추가를 클릭하고 포트 전달 규칙을 추가하는 경우처럼 진행합니다. **공통 옵션** 외에도, 하나의 다른 설정 만 구성할 수 있습니다.

NAT

NAT, No NAT 또는 **Map Network**를 적용하려면 선택하십시오. NAT를 사용하도록 선택하면 드롭 다운 메뉴에 표시된 IP 주소 중 사용할 IP 주소를 선택할 수 있습니다. *자동(Auto)* 항목은 송신(outgoing) 인터페이스에 해당하는 IP 주소를 자동으로 선택할 것입니다.

Orange 구역에 있는 SNAT 및 SMTP 서버.

어떤 경우에는, *소스 NAT*를 수행하지 않도록 명시적으로 선언하는 것이 좋습니다. 예를 들어, 외부 IP로 구성되었지만 나가는 연결에 REDIP가 소스로 있어야 하는 DMZ의 SMTP 서버가 있습니다. 소스 NAT가 있는 DMZ에서 IP 123.123.123.123 (123.123.123.123이 업링크의 추가 IP 주소라고 가정)에서 실행중인 SMTP 서버를 구성하는 방법은 다음과 같습니다.

1. 모든 서브넷으로 ORANGE 영역을 구성하십시오 (예: 192.168.100.0).
2. SMTP 서버가 ORANGE 영역의 IP (예: 129.168.100.13)의 포트 25에서 청취하도록 설정합니다.
3. Menubar ‣ Network ‣ Interface 섹션에서 Endian UTM Appliance에 IP 123.123.123.123이 포함된 정적 이더넷 업링크를 추가하십시오.
4. 원본 NAT 규칙을 추가하고 원본 주소로 SMTP 서버의 ORANGE IP를 지정하십시오. NAT를 사용하고 NAT 소스 IP 주소를 123.123.123.123으로 설정하였는지 확인하십시오.

추가 참고사항: DNAT (기본 설정), DNAT (고급 설정) 및 SNAT (기본 설정) 규칙을 정의하려면 자습서를 참조하십시오.

들어오는 라우팅 트래픽

이 탭에서는 Endian UTM Appliance를 통해 라우팅된 트래픽을 리디렉션 할 수 있습니다. 이것은 하나 이상의 외부 IP 주소를 가질 때 매우 유용하며, NAT를 사용할 필요없이도 DMZ에서 그것들의 일부를 사용해야 합니다. 목록의 모든 규칙에 대해 표시된 필드들은 트래픽 소스 및 대상, 서비스, 적용할 정책, 설명(remark) 및 사용 가능한 작업(action)입니다.

공통 옵션 외에는 다른 설정을 구성할 수 없습니다.

수신중인 라우팅된 트래픽의 일반적인 시나리오.

수신중인 라우팅된 방화벽이 어떤 종류의 네트워크 트래픽을 가로 채는지를 보여주는 고전적인 예는 공용 IP 주소를 가진 서버가 있는 로컬 DMZ (Orange) 네트워크입니다.
Endian UTM Appliance가 다음과 같이 구성되어 있다고 가정합니다.

- 업링크 (RED)

Endian UTM Appliance는 ISP에 연결하여 하나의 공용 IP 주소 (1.1.1.2)와 게이트웨이 (1.1.1.1)를 수신하여 인터넷에 연결합니다.

- DMZ (오렌지)

  2.2.2.1/28 - Endian (DMZ 네트워크의 기본 게이트웨이)
  2.2.2.2-14 - 서버용 공용 IP

  2.2.2.0/28 - 네트워크 주소
  2.2.2.15 – 브로드캐스트

로컬 DMZ 네트워크는 2.2.2.1/28 네트워크에 있는 14개의 공용 IP 주소로 구성되며, 2.2.2.1 게이트웨이 (Endian UTM Appliance의 ORANGE IP)를 사용하여 인터넷에 연결됩니다.

- 1.1.1.2를 통해 2.2.2.0/28 경로

ISP는 공개 2.2.2.0/28 서브넷으로 향하는 모든 트래픽을 Endian UTM Appliance로 보냅니다.

이 구성을 사용하면, 주 업링크에서 Endian UTM 어플라이언스의 업링크에 대한 연결인 대상 1.1.1.2를 가진 (들어오는) 패킷이 수신될 것이고, OpenVPN, IPsec 등과 같이 제공되는 서비스에 연결됩니다.

그러나 Endian UTM 어플라이언스는 2.2.2.2-2.2.2.14 범위의 대상과 함께 패킷을 수신할 것입니다. ISP에서 설정한 경로가 있기 때문입니다. 이 트래픽은 업링크 및 **ROUTED**에서 유래하기 때문에 ISP는 해당 목적지가 있는 패키지에 대한 라우팅 규칙을 가지고 있기 때문에 모두 **들어오지 (INCOMING)** 않습니다.

기본적으로, 이 트래픽은 삭제되므로 *들어오는 라우팅된 방화벽 (incoming routed firewall)*에서 규칙을 허용해야 합니다. 또한 대상 IP 주소가 이미 공개되어 있으므로, 이러한 종류의 트래픽을 DNAT 규칙으로 구성할 수 없습니다.

발신(나가는) 트래픽

Endian UTM 어플라이언스는 발신 트래픽에 대해 미리 구성된 규칙 세트, 즉 특정 서비스, 포트 및 애플리케이션을 다양한 구역에서 RED 인터페이스로, 따라서 인터넷으로 트래픽 흐름을 허용하기 위해 사전 구성된 규칙 세트와 함께 제공됩니다. 이러한 규칙은 가장 일반적인 서비스가 항상 인터넷에 액세스하고 올바르게 작동할 수 있도록 하기 위해 필요합니다. 이 페이지에는 현재 규칙을 보여주고 새 규칙을 추가할 수 있는 상자와 나가는(Outgoing) 방화벽 옵션을 설정할 수 있는 상자가 있습니다.

참고: Endian UTM 어플라이언스가 *업링크 모드에 있지 않으면*, 나가는 방화벽에 정의된 규칙이 무시됩니다. *스텔스 업링크* 모드에서 작동하는 경우 Endian UTM 어플라이언스 뒤의 영역에서 외부로 가는 트래픽의 일부만이 나가는 것으로 간주됩니다. 스텔스 업링크에 대한 설명을 참조하십시오.

Endian UTM 어플라이언스 및 애플리케이션 방화벽 (애플리케이션 제어).

응용프로그램 방화벽은 상태 보존형 방화벽에 대한 최근 개발 및 개선 사항으로, 웜, 바이러스, 멀웨어 및 모든 유형의 위협으로부터 더 높은 보안을 제공하는 목적으로 패킷의 내용을 검사하기 위해침입 차단 시스템의 방화벽들로 연결 원점 및 경로를 추적하는 기능을 결합합니다. 사용자 경험 관점의 최종 결과는 방화벽이 포트와 IP 주소 간의 트래픽뿐만 아니라 단일 응용 프로그램에 의해 생성된 트래픽도 차단할 수 있다는 것입니다. 그러나 이것은 방화벽에서의 더 많은 노력을 필요로 합니다. IP 주소들 사이의 트래픽은 첫 번째 패킷을 검사하여 전체 흐름을 차단하거나 전체 흐름을 허용해야 하며, 응용프로그램에서 생성된 트래픽을 올바르게 인식해야 하는 경우도 있고, 전체 흐름에서 일부 몇 개의 패킷 수를 분석해야 하는 경우가 간혹 있지만 일반적으로 전체 흐름의 3배보다 많지 않습니다.
버전 5.0부터 모든 Endian UTM Appliance에는 Deep Packet Inspection을 구현하는 오픈 소스 라이브러리인 nDPI가 장착되어 있어 응용프로그램 방화벽을 위한 규칙을 배포할 수 있습니다. nDPI는 커널 모듈로 배포되며, 패킷 분석을 위해 iptables과 상호 작용합니다.
따라서, 나가는 방화벽에서 정의할 수 있는 두 가지 다른 유형의 규칙이 있습니다.

- IP 주소와 포트 사이의 트래픽을 필터링하는 *상태 기반 방화벽* 규칙
- *응용프로그램 규칙*, 즉 응용프로그램에서 생성된 트래픽을 필터링하는 규칙

응용 프로그램 규칙이 정의되지 않은 경우, 방화벽의 동작은 이전 버전과 완전히 동일합니다. 그러나 응용프로그램 규칙이 정의될 때마다 그 앞에 있는 상태 기반 규칙은 정상적으로 작동하지만 nDPI를 거친 후에는 모든 규칙이 작동합니다.
nDPI를 사용하면, 다음 예에서 설명한 것처럼 약간의 미묘함이 나타날 수 있으므로, 원하지 않는 부작용이 발생할 수 있습니다.
회사에서 youtube 및 gmail을 제외한 모든 HTTP 트래픽을 허용하려고 한다고 가정합시다. Endian UTM Appliance에 정의된 첫 번째 기본 규칙은 제한없이 모든 HTTP 트래픽을 허용하는 것입니다. 따라서 이 규칙은 첫 번째 단계로 비활성화되어야 합니다. 그런 다음 두 가지 규칙을 정의해야 합니다.

1. Gmail 및 YouTube 프로토콜을 차단하는 응용프로그램 규칙
2. 모든 http 트래픽을 허용하는 상태 저장 규칙.

규칙 2가 프로토콜 HTTP를 사용하는 응용프로그램 규칙인 경우, nDPI가 HTTP로 인식하는 트래픽만 허용되지만, nDPI가 HTTP가 아닌 독립적인 프로토콜로 그것들을 인식하기 때문에, HTTP를 사용하는 다른 프로토콜 (예: Yahoo 및 FaceBook)은 통과합니다.

현재 규칙

자세히 말하자면, 이들은 구역에서 REDIP에 액세스하고 상단 상자에 표시된 기본적으로 허용되는 서비스 및 프로토콜입니다.

GREEN: HTTP, HTTPS, FTP, SMTP, POP, IMAP, POP3s, IMAPs, DNS, ICMP
ORANGE: DNS, ICMP
BLUE: HTTP, HTTPS, DNS, ICMP

엔디안 네트워크의 서비스에 대한 액세스를 허용하는 *시스템 규칙*을 제외하고는 다른 모든 것이 기본적으로 금지됩니다. 시스템 규칙은 해당 구역이 활성화되지 않은 경우에도 정의됩니다.

> **참고:** Endian Network에 대한 액세스는 Community Edition 장비에 허용되지 않습니다.

각 규칙에 대해 가능한 액션들은 그것을 편집하거나 삭제하기 위해 활성화 또는 비활성화됩니다. 추가 규칙은 페이지 상단에 있는 새 방화벽 규칙 추가 링크를 클릭하여 추가할 수 있습니다. 규칙의 순서는 중요합니다는 것을 명심하십시오. 첫 번째 일치 규칙은 얼마나 많은 일치하는 규칙이 따르는지 상관없이, 패킷의 허용 또는 거부 여부를 결정합니다. 규칙의 순서는 각 규칙 옆의 위쪽 및 아래쪽 화살표 아이콘을 사용하여 변경할 수 있습니다.

다음 설정은 기본 **공통 옵션**과 다릅니다.

출처

하나 이상의 구역/인터페이스, 네트워크/IP 또는 MAC 주소가 될 수 있습니다.

목적지

RED 영역, 하나 이상의 업링크 또는 RED 인터페이스 외부에서 액세스 할 수 있는 하나 이상의 네트워크/호스트 주소가 될 수 있습니다.

신청

이 검색 위젯은 규칙의 일부가 되어야 하는 응용프로그램을 선택할 수 있게 합니다. 응용프로그램은 범주 (예: 데이터베이스, 파일 공유 등)로 배분됩니다.

> **힌트:** 해당 문자로 시작하는 이름의 모든 응용 프로그램을 표시하려면, 최소한 하나의 문자를 입력하십시오.

발신(Outgoing) 방화벽 설정

발신 방화벽 사용 스위치를 클릭하여 발신 방화벽 전체를 비활성화하거나 활성화할 수 있습니다. 사용하지 않도록 설정하면, 나가는 모든 트래픽이 허용되고 패킷이 필터링되지 않습니다. 그러나 이 설정은 권장하지 않으며, 발신 방화벽을 계속 사용하도록 설정하는 것이 좋습니다.

허용된 발신 연결 로그

이 확인란을 선택하면 RED 인터페이스에 허용된 모든 연결이 기록됩니다.

프록시 및 발신 방화벽.

프록시가 특정 서비스 (예 : HTTP, POP, SMTP, DNS)에 대해 활성화될 때마다 발신 방화벽의 방화벽 규칙은 프록시 특성으로 인해 영향을 받지 않습니다.

프록시가 활성화되면 클라이언트에서 인터넷으로 연결이 시작될 때마다 (투명 모드에서) Endian UTM Appliance의 프록시가 가로 채거나 직접 방화벽으로 이동하지만 방화벽을 통과하지 않습니다. 그런 다음 프록시는 실제 대상에 대한 새 연결을 시작하고 데이터를 가져와서 클라이언트로 보냅니다. 이러한 인터넷 연결은 항상 클라이언트 내부 IP 주소를 숨기는 Endian UTM Appliance에서 시작됩니다. 따라서 이러한 연결은 실제로 로컬 연결이기 때문에 나가는 방화벽을 통과하지 못합니다.

영역 간 트래픽

이 모듈은 RED 구역 (RED 구역을 통한 트래픽은 **발신 트래픽**과 **포트 포워딩** / **NAT**에서 필터링 될 수 있음)을 제외하고, 로컬 네트워크 구역들 간에 트래픽이 흐르는 방식을 결정하는 규칙을 설정하도록 허용합니다. 구역 간 방화벽을 활성화하려면, 회색 스위치  를 클릭하십시오. 이 페이지에는 현재 규칙을 보여주고 새 규칙을 추가할 수 있는 상자와 영역 간 방화벽 옵션을 설정할 수 있는 상자가 있습니다.

> **참고:** Endian UTM 어플라이언스가 *업링크 모드로 구성되어 있지 않으면 (No upling)*, 모든 네트워크 트래픽이 interzone 방화벽을 사용하여 필터링됩니다. 또한 하나 이상의 영역이 정의된 *스텔스 업링크 모드*에서 게이트웨이를 통해 라우팅되지 않은 모든 트래픽은 영역 간 방화벽으로 필터링됩니다. 자세한 정보는 ref: *스텔스 링크 설명 <stealth>*를 참조하십시오.

현재 규칙

Endian UTM 어플라이언스에는 녹색(GREEN) 구역에서 다른 구역 (ORANGE 및 BLUE) 및 각 구역 내에서 트래픽 허용이 기본적으로 금지되어 있습니다.

발신 트래픽 방화벽과 마찬가지로, 테이블의 오른쪽에 있는 해당 아이콘을 클릭하여 규칙을 비활성화/활성화, 편집 또는 삭제할 수 있습니다. 페이지 상단의 새로운 구역 간 방화벽 규칙 추가 링크를 클릭하여 새 규칙을 추가할 수 있습니다. **공통 옵션**만 구성할 수 있습니다.

구역 간 방화벽 설정

구역 간 방화벽 활성화 스위치를 사용하여 구역 간 방화벽을 사용하거나 사용하지 않도록 설정할 수 있습니다. 사용 중지되면, 모든 트래픽이 모든 BLUE, GREEN 및 ORANGE 구역에서 허용됩니다. 구역 간 방화벽을 비활성화하면 안됩니다.

허용된 구역 간 연결 로그 기록

이 확인란을 선택하면 구역 간에 허용되는 모든 연결이 기록됩니다.

VPN 트래픽

VPN 트래픽 방화벽은 OpenVPN을 통해 연결된 사용자 및 호스트에 적용되는 방화벽 규칙을 추가할 수 있게 해줍니다.

VPN 트래픽 방화벽은 일반적으로 활성화되어 있지 않습니다. 즉, 한쪽에서 GREEN 구역의 VPN 클라이언트와 호스트간에 트래픽이 자유롭게 흐를 수 있고, 다른 쪽에서는 VPN 호스트가 Endian UTM 어플라이언스 뒤에 있는 모든 구역들에 접근할 수 있습니다.

> **참고:** VPN 클라이언트는 발신 트래픽 방화벽이나 구역 간 트래픽 방화벽의 **영향을 받지 않습니다.**

이 페이지에는 현재 규칙을 보여주고 새 규칙을 추가할 수 있는 상자와 VPN 방화벽 옵션을 설정할 수 있는 2개의 상자가 있습니다.

현재 규칙

기본적으로 규칙이 정의되어 있지 않으므로, 규칙을 추가하려면 페이지 상단의 새 VPN 방화벽 규칙 추가 링크를 클릭하십시오. **공통 옵션**만 규칙을 정의하는데 사용할 수 있습니다.

VPN 방화벽 설정

VPN 방화벽은 **VPN 방화벽 활성화** 스위치를 사용하여 비활성화하거나 활성화할 수 있습니다.

허용된 VPN 연결 로그

이 확인란을 선택하면, VPN 사용자의 모든 허용된 연결이 로그됩니다.

시스템 액세스

이 섹션에서는 Endian UTM Appliance 자체 및 이 노드에서 실행되는 서비스에 대한 액세스를 허용 또는 거부하는 규칙을 관리합니다.

Endian UTM Appliance에서 실행되는 서비스가 로컬 또는 원격 구역에 있는 클라이언트에서 액세스해야 하는 적절한 작업을 보장하기 위해 변경될 수 없는 미리 구성된 규칙 목록이 있습니다.

페이지 하단의 `시스템 서비스 규칙 표시` 버튼을 클릭하면, 사전 정의된 규칙 목록이 표시됩니다.

시스템 액세스 규칙의 예로는 호스트 이름 (포트 53이 열려 있어야 함)을 확인하는 DNS 서비스 또는 (포트 10443을 사용하는) 관리 웹 인터페이스에 대한 액세스와 같이 항상 활성인 서비스들이 포함되어 있습니다. 또한, 서비스 (예: OpenVPN, 핫스팟, 다른 것들 중에 SNMP 서버)가 활성화될 때마다, 하나 이상의 규칙이 자동으로 생성되어 서비스 자체의 적절한 효율성을 허용합니다.

새 시스템 액세스 규칙 추가 링크를 클릭하면, 더 많은 시스템 액세스 규칙을 추가할 수 있습니다. 방화벽의 이 모듈과 관련된 설정은 다음과 같습니다.

로그 패킷

> 이 확인란을 선택하면, Endian UTM Appliance에 액세스하거나 액세스하려고 하는 모든 패킷이 기록됩니다. 이 옵션은 누가 액세스했는지 또는 시스템에 액세스하려고 했는지를 아는데 유용합니다.

출발지 주소

> 들어오는 연결의 MAC 주소입니다.

소스 인터페이스

> 시스템에 액세스 할 수 있는 인터페이스
>
> **참고:** *대상* 주소는 액세스가 부여되거나 시도된 인터페이스의 IP 주소이므로 없습니다.

방화벽 다이어그램

이 페이지는 이 페이지에서 설명하는 각 모듈에 대해 트래픽이 영역간에 어떻게 전달되는지, 다양한 흐름을 담당하는 방화벽 모듈을 보여주는 다이어그램을 보여줍니다. 녹색 화살표가 있는 선은 각 영역에서 허용되는 트래픽과 방향을 보여줍니다. VPN의 경우 RED 인터페이스에서 또는 RED 인터페이스로 가는 화살표는 빨간색 'X'로 표시되어 트래픽이 서로 간에 가능하지 않음을 의미합니다.

이미지를 클릭하면, 슬라이드 쇼처럼 모든 이미지를 탐색할 수 있는 갤러리로 이미지가 열립니다.

프록시 메뉴

- HTTP
  - Configuration
  - Access policy
  - Authentication
  - Web Filter
  - AD join
  - HTTPS Proxy
- POP3
  - Global settings
  - Spam filter
- FTP
- SMTP
  - Configuration
  - Black- & Whitelists
  - Incoming domains
  - Domain routing
  - Mail Routing
  - Advanced
  - Anti-Spam
- DNS
  - DNS proxy
  - DNS Routing
  - Anti-spyware

온라인 보안을 향상시키기 위해, Endian UTM Appliance는 자신의 능력을 프록시의 기능과 결합한 여러 가지 서비스를 제공합니다. 페이지 왼쪽의 하위 메뉴는 다음과 같이 요약된 구성 페이지 및 옵션에 대한 액세스 권한을 부여합니다.

- HTTP - 웹 프록시 : 액세스 정책, 인증, 컨텐츠 필터, SSL 지원 (HTTPS) 및 바이러스 백신.
- POP3 - 전자 메일 검색을위한 프록시 : 스팸 필터 및 바이러스 백신.
- FTP - FTP를 통해 다운로드 한 파일 : 안티 바이러스.
- DNS - 캐싱 DNS : 스파이웨어 차단

각 프록시 서비스는 다른 프록시 서비스와 독립적으로 구성 및 활성화/비활성화 될 수 있으며, 적절한 기능을 수행하는데 필요한 다른 서비스도 시작합니다. 예를 들어, SMTP 프록시가 구성되고 시작되면 SMTP 서비스가 아직 실행되지 않은 경우 시작됩니다. 따라서 SMTP 프록시를 사용하기 전에 SMTP 서비스를 구성해야 합니다.

프록시 서버는 클라이언트 (웹 페이지 또는 일부 리소스를 요청하는)와 외부 네트워크 사이에 위치하여 모든 클라이언트 요청을 포착하고, 요청된 리소스를 검색하여 클라이언트에 전송하는 시스템입니다. 프록시 서버의 주된 이점은 요청된 모든 페이지를 캐시 (즉, 로컬에 저장)하여 향후 동일한 페이지에 대한 요청을 더 빨리 수행할 수 있다는 점입니다.

과거의 HTTP 프록시 및 새로운 HTTP 프록시 아키텍처

Endian UTM Appliance 5.0 릴리스에서는 HTTP 프록시에 대한 더 가볍고 강력한 아키텍처가 구현 및 배포되었습니다.

이전 HTTP 프록시 아키텍처는 *프록시 체인 (proxy chaining)*에 기반을 두었습니다. 즉, 클라이언트가 이전에 캐시되지 않은 원격 리소스를 요청할 때마다 5단계 프로세스가 수행되었습니다.

1. HTTP 프록시 -squid-는 서버에 GET 요청을 보내고 HTML 페이지를 응답으로 받습니다.
2. 전체 HTML 페이지가 콘텐츠 필터링 데몬 (dansguardian)으로 전송되어 분석되었습니다.
3. 그런 다음 Dansguardian은이 페이지를 안티 바이러스 데몬 -havp-로 보내고 바이러스 및 기타 멀웨어를 분석했습니다.
4. 마지막으로, 바이러스 또는 악성 콘텐츠가 발견되지 않으면, 전체 HTML 페이지가 squid로 다시 전송되고, 그렇지 않으면 HTML 오류 메시지 (*"오류 페이지"*)가 원본 페이지를 대체하게됩니다.
5. squid는 앞으로의 요청을 위해, HTML 페이지 (또는 오류 페이지)를 저장하고, 원래 HTML 페이지를 요청한 클라이언트에게 전달했습니다.

이 아키텍처의 주요 단점 및 병목 현상은 리소스 집약성입니다. 전체 HTML 페이지는 사실 전체 체인을 순차적으로 순차적으로 이동하여 프로세스를 가속화할 가능성이 전혀 없습니다. HTML 페이지가 squid로부터 수신되어 dansguardian으로 전송되어 콘텐츠를 분석했습니다. 이 시점에서 콘텐츠 필터가 악의적인 콘텐츠를 발견했음을 의미하는 경우에도 페이지를 요청한 클라이언트에 제공할 수 없으므로, HTML 페이지가 havp로 체인을 계속 이어 squid로 돌아갑니다. 이 시점에서 squid는 원래 클라이언트에게 오류 페이지를 보냈습니다.

따라서이 문제를 다르게 해결하고 더 많은 신뢰성을 보장하고 자원을 훨씬 적게 사용하는 완전히 새로운 접근 방식을 채택하기로 결정했습니다. HTTP 프록시는 이제 ICAP 서버에 의해 백업되며, 이는 처음에는 좀 더 복잡한 아키텍처를 나타낼 수 있지만 상당한 성능 향상을 나타냅니다.

요컨대 ICAP는 **RFC 3507**에 정의된 프로토콜로, 웹 페이지의 컨텐트를 조작하고 다시 클라이언트에 제공할 수 있게 해줍니다. 이 기능은 여러 가지 방법으로 악용될 수 있지만, Endian UTM Appliance에서는 **c-icap**과 함께 배포되어 컨텐츠 필터링 분석 및 원격 리소스 (HTML 페이지뿐만 아니라 오디오, 비디오 및 텍스트 문서, 이미지)들의 안티 바이러스 스캔을 제공합니다..

C-icap 덕분에, 두 가지 영역에서 성과를 올렸습니다.

1. squid에서 C-icap까지 :

   c-icap은 HTTP 프록시로부터 두 개의 병렬 요청을 받습니다.

2. cicap과 데몬들 사이.

추가 참고사항: ICAP에 대한 자세한 내용은 **icap 포럼** 웹 페이지에서 확인할 수 있습니다.

HTTP

이 페이지에서 다음 항목들을 찾을 수 있습니다.

Endian UTM 어플라이언스에 사용되는 HTTP 프록시는 squid (캐싱 프록시)로, 웹 요청을 캐시하여 나중에 같은 페이지의 요청을 처리하는 기능을 갖추고 있지만 이 섹션의 나머지 기능에 설명된 다른 서비스와의 완벽한 통합을 가능하게 하는 더 많은 기능이 있습니다. HTTP 프록시 설정 페이지는 **구성, 액세스 정책, 인증, 웹 필터, AD 조인** 및 **HTTPS 프록시**와 같은 다양한 옵션을 구성하는 6 개의 탭으로 구성되어 있습니다.

구성(Configuration)

Enable HTTP Proxy 스위치  를 클릭하면, HTTP 프록시가 활성화됩니다. 필요한 모든 서비스를 시작하는데 필요한 몇 초가 지나면, *구성* 탭에 여러 개의 컨트롤이 여섯 개의 패널로 그룹화되어 나타납니다. 각 패널에는 제목이 있으며, 그 뒤에 **?** 툴팁이 표시되며 라벨 왼쪽에 있는 펼치기(⊞) 또는 접기(⊟) 아이콘을 클릭하여 펼치거나 접을 수 있습니다.

투명 및 투명하지 않은 프록시.

투명한 프록시는 게이트웨이와 결합된 프록시 시스템입니다. 투명한 프록시는 리소스 검색 및 캐싱 외에도 클라이언트가 요청하는 웹 페이지 또는 리소스에 대한 많은 유용한 작업을 수행할 수 있습니다.

이것은 내용을 필터링하고 바이러스가 있는지 스캔하여 살펴보거나 게이트웨이에서 실행중인 여러 서비스를 결합하여 정보를 차단할 수 있습니다.

또한 이러한 모든 활동은 사용자가 어떤 방식으로든 자신이 사용하는 클라이언트를 구성할 필요 없이 수행됩니다.

반대로 투명하지 않은 프록시는 사용되는 클라이언트의 공동 작업 (예: 웹 브라우저에서 프록시 설정 구성)에 의존하므로 사용자가 브라우저 설정에서 프록시 위치를 수동으로 지정해야 하며, 또는 인터넷에 접속할 수 없게 될 것입니다.

> **참고:** New Mini Arm에서 *캐시 관리* 패널 (추가 참조)이 표시되지 않으므로 여기에 설명된 옵션 중 일부는 사용할 수 없습니다.

첫 번째 설정은 드롭 다운 메뉴에서 활성화된 각 구역 (예: GREEN, ORANGE, BLUE)의 사용자가 프록시에 액세스 할 수 있는 방법을 선택하는 것입니다 (사용할 수 없는 구역에는 드롭 다운 메뉴 없음).

투명하지 않음

프록시 서버는 로그인 할 필요없이, 모든 사용자가 사용할 수 있지만 클라이언트는 브라우저를 수동으로 구성하거나 브라우저에 프록시를 검색하도록 요청해야 합니다 (즉, PAC (프록시 자동 구성) 또는 WPAD (웹 프록시 자동 검색) 프로토콜을 사용하여 브라우저의 프록시 설정을 설정해야 함) .

투명

모든 사용자가 프록시 서버를 사용할 수 있으며, 브라우저 구성은 필요하지 않습니다. 모든 HTTP 트래픽이 가로 채어져 프록시 서버로 전달됩니다. 프록시 서버는 요청된 웹 페이지를 검색하고, 이를 클라이언트에 제공합니다.

투명 (원본 IP 주소 유지)

이 구성은 이전 옵션과 매우 유사합니다. 단, 프록시를 나가는 모든 패킷은 클라이언트의 원래 정보 중 일부 (IP 주소, 트래픽이 시작된 영역 및 인터페이스)를 유지한다는 점만 다릅니다.

> **참고:** Internet Explorer 및 Firefox를 포함한 일부 브라우저는 WPAD를 사용하여 프록시 서버를 자동으로 검색할 수 있습니다. 대부분의 브라우저는 특수 URL을 통해 PAC를 지원합니다.

Endian UTM Appliance를 프록시 서버로 사용하는 경우, URL은 http://<GREENIP>/proxy.pac와 같습니다.

> **영역 당 HTTP 프록시를 비활성화하는 방법**
>
> 특정 구역에 대한 프록시를 완전히 비활성화하려면, 구역의 프록시를 투명하게 설정하고, *Bypass 투명한 프록시* 패널을 확장할 때 나타나는 필드인 *SUBNET/IP/MAC의 투명 프록시를 우회하는* 필드에 구역의 서브넷 (*Menubar ‣ Services ‣ DHCP server*에서 찾을 수 있는 값)을 추가해야 합니다.

프록시 설정

프록시 설정 패널에는 프록시 서비스에 대한 몇 가지 전역 구성 옵션이 있습니다.

프록시가 사용하는 포트

프록시 서버가 연결을 청취하는 TCP 포트. 기본값은 8080입니다.

오류 언어

오류 메시지가 표시되는 언어입니다. 기본적으로 *Menubar ‣ System ‣ GUI settings*에서 선택한 오류 메시지가 표시됩니다.

프록시에서 사용하는 호스트 이름 보이기

프록시 서버에 의해 가정된 호스트 이름이며, 오류 메시지의 맨 아래에 보고됩니다.

알림에 사용되는 이메일 (캐시 관리자)

오류 메시지에 프록시 서버가 표시한 전자 메일 주소입니다.

> **참고:** 캐시 관리를 사용할 수 없기 때문에, 캐시 관리 전자 메일 주소는 Mini 어플라이언스에 없습니다.

최대 다운로드 크기 (KB 단위로 들어옴)

HTTP 파일 다운로드 제한. 0은 무제한을 의미합니다.

최대 업로드 크기 (KB 단위로 나감)

HTTP 파일 업로드 제한 (예: 파일 업로드가 있는 HTML 양식에서 사용되는 제한). 0은 무제한을 의미합니다.

원본 IP 주소 유지

이 옵션은 비 투명 모드로 구성된 모든 영역에 영향을 줍니다. 체크 표시가 있으면, 프록시에서 오는 모든 패킷은 요청자 (클라이언트)의 정보를 유지합니다. IP 주소와 트래픽이 시작된 구역/인터페이스입니다.

허용된 포트 및 SSL 포트

클라이언트가 탐색할 때 사용할 수 있는 포트에 대한 구성 옵션 :

허용된 포트 (클라이언트에서)

HTTP를 사용할 때 프록시 서버가 연결을 수락할 TCP 대상 포트입니다. 한 줄당 한 개의 포트 또는 한 개의 포트 범위가 허용되며 주석이 허용되고, #로 시작합니다.

허용된 SSL 포트 (클라이언트에서)

HTTPS를 사용할 때 프록시 서버가 연결을 수락할 TCP 대상 포트입니다. 한 줄당 하나의 포트 또는 포트 범위가 허용되며, 주석은 허용되며 #으로 시작하며, 줄 끝에서 끝납니다.

로그 설정

로깅 기능을 사용하고 기록할 항목을 선택하는 구성 옵션.

HTTP 프록시 로깅

프록시를 통해 액세스되는 모든 URL을 기록합니다. 이 스위치는 마스터 스위치이므로 다음 네 가지 옵션이 활성화되어 있으며, 로깅이 활성화되어 있는 경우에만 구성할 수 있습니다 (기본값은 아닙니다). 더 많은 정보가 기록될수록, Endian UTM Appliance의 하드 디스크 공간이 더 필요함을 상기하십시오).

질의 용어 로깅

URL에 매개 변수를 기록하십시오 (예: ?id = 123).

사용자 에이전트 로깅

각 브라우저에서 보낸 사용자 에이전트를 기록하십시오.

Contentfilter 로깅

웹 페이지의 내용이 필터링되면 기록하십시오.

방화벽 로깅 (투명한 프록시만 해당)

방화벽이 나가는 웹 액세스, 즉 RED 인터페이스를 통해 인터넷으로 향하는 액세스를 로그하게하십시오. 이 옵션은 투명한 프록시에서만 작동합니다.

투명 프록시 우회

이 패널에서는 투명한 프록시 (위 참조)에 대한 몇 가지 예외가 정의될 수 있습니다. 즉, 소스 (즉, 클라이언트) 및 대상 (즉, 원격 서버)은 해당 영역에서 활성화되어 있어도 프록시가 무시해야 합니다.

SUBNET/IP/MAC에서 투명 프록시 우회

투명한 프록시의 대상이 되어서는 안되는 소스. 항목들은 단일 IP 주소, 서브넷 또는 MAC 주소일 수 있습니다.

투명 프록시를 SUBNET / IP로 우회

투명 프록시의 대상이 아닌 대상입니다. 항목은 단일 IP 주소 또는 서브넷일 수 있습니다.

> **힌트:** CIDR 표기법을 사용하여 서브넷을 입력하십시오.

캐시 관리

캐시에 의해 디스크에 있는 공간과 저장된 오브젝트의 크기에 대한 구성 옵션.

하드 디스크의 캐시 크기 (MB)

프록시가 하드 디스크의 웹 사이트 캐싱을 위해 할당해야하는 양 (MB)입니다.

캐시 지우기

디스크의 캐시를 즉시 지우려면, 캐시 지우기 버튼을 클릭하십시오.

메모리 내의 캐시 크기 (MB)

프록시가 시스템 메모리에 웹 사이트를 캐싱하기 위해 할당해야 하는 메가 바이트 단위의 양입니다.

이 대상을 캐시하지 않는다.

이러한 사이트에서 다운로드 한 리소스는 절대로 캐시에 저장되지 않습니다. 항목은 도메인 이름 또는 IP 주소일 수 있습니다 (서브넷이 허용되지 않음).

최대 개체 크기 (KB)

캐시되어야 하는 단일 오브젝트의 상위 크기 제한 (MB).

최소 개체 크기 (KB)

캐시해야 하는 단일 개체의 크기 제한 (메가 바이트)입니다.

> **참고:** 크기가 위의 정의된 범위에 속하지 않는 객체는 디스크의 캐시에 저장되지 않지만, 클라이언트가 요청할 때마다 다운로드됩니다.

오프라인 모드 캐시

이 옵션을 사용하면, 프록시가 원격 웹 서버에서 캐시된 객체를 업데이트하지 않으므로, 클라이언트는 업링크가 다운된 후에도 캐시된 정적 웹 사이트를 탐색할 수 있습니다.

> **경고:** 이 옵션은 요청한 페이지가 이전에 캐시된 경우, 업링크가 다운되어 있는 동안 인터넷을 서핑하는 데 유용합니다. 그러나 HTTP 프록시가 항상 캐시된 페이지를 제공하므로 작업 업링크가 있는 경우에도, 이 옵션을 사용하면 페이지를 새로 고칠 때 문제가 발생할 수 있습니다. 이 경우 프록시 서버의 캐시를 지우는 것이 웹 페이지의 새로 고친 사본을 가질 수 있는 유일한 방법입니다.

상향 프록시

LAN에 다른 프록시 서버가있는 경우 실제로 원래의 자원을 요청하기 전에 연결할 수 있습니다. 이 패널에는 Endian UTM Appliance와 업스트림 프록시 간의 연결을 위한 구성 옵션이 있습니다.

상향 프록시

업스트림 프록시를 활성화하고, 더 많은 옵션을 표시하려면 이 확인란을 선택하십시오. 사용 설정되면 캐시에 아직없는 원격 웹 페이지를 검색하기 전에, Endian UTM Appliance의 프록시가 업스트림 프록시에 접속하여 해당 페이지를 요청합니다.

상류 서버

업스트림 서버의 호스트 이름 또는 IP 주소.

업스트림 포트

프록시가 업스트림 서버에서 수신 대기중인 포트입니다.

상류 사용자 이름 / 암호

업스트림 프록시에 대한 인증이 필요한 경우 여기에 자격 증명을 지정하십시오

클라이언트 사용자 이름 전달

확인란을 선택하면, 사용자 이름이 업스트림 프록시로 전달됩니다.

클라이언트 IP 전달

체크 박스를 선택하면 클라이언트 IP 주소가 업스트림 프록시로 전달됩니다.

액세스 정책

액세스 정책은 인증에 관계없이 프록시를 통해 연결하는 모든 클라이언트에 적용됩니다. 액세스 정책 규칙은 사용자에 대한 다양한 매개 변수 (예: 트래픽의 소스 또는 대상), 사용된 클라이언트 또는 다운로드된 콘텐츠 (예: 사용자 에이전트, 사용자 에이전트, 사용자 에이전트)에 따라 액세스를 허용하거나 금지하는 시간 기반 스키마입니다. (예: 사용자 에이전트, MIME 검색 유형, 바이러스 검색 및 컨텐츠 필터링).

이미 정의된 규칙 목록이 페이지에 표시됩니다. 모든 규칙은 웹 액세스가 차단 또는 허용되는지 여부를 지정할 수 있으며, 후자의 경우 필터 유형을 활성화하고 선택할 수 있습니다. 이 테이블은 그 안에 나열된 모든 규칙에 대해 다음 정보를 전달합니다. 프로그래시브 식별 번호 (#), 이름 (` `), 관심 있는 소스 및 대상, 인증 유형, 필요한 경우 활성화 기간, 사용자 에이전트 일치 및 사용 가능한 작업 등입니다.

-  - 정책을 수정하십시오.
-  - 정책을 제거합니다.
-  - 정책을 목록의 위쪽 또는 아래쪽으로 이동합니다.
- - 정책을 활성화 또는 비활성화합니다.

새 액세스 정책 규칙을 추가하기 위해, Add Access Policy (액세스 추가 정책)를 클릭하기만 하면 모든 매개 변수를 구성할 수 있는 폼이 열립니다.

소스 유형

이 규칙이 적용되는 트래픽 소스. **<ANY>**, 구역, 네트워크 목록, IP 주소 또는 MAC 주소일 수 있습니다.

대상 유형

이 규칙이 적용될 트래픽의 대상입니다. **<ANY>**, 구역 또는 네트워크, IP 주소 또는 도메인 목록일 수 있습니다.

인증

클라이언트에 적용할 인증 유형입니다. **그룹 기반** 또는 **사용자 기반** 인증이 필요없는 경우, **비활성화** 할 수 있습니다. 정책을 적용할 하나 이상의 사용자 또는 그룹을 목록에 있는 기존 사용자 중에서 선택할 수 있습니다.

> **힌트:** 인증은 로컬에만 적용되므로 사용하기 전에, 인증 탭에 하나 이상의 사용자 또는 그룹을 만들어야 합니다.

시간 제한

규칙이 특정 요일 및/또는 기간에 영향을 미치는지 여부를 결정하십시오. 기본적으로 규칙은 항상 활성화되어 있지만, 유효 기간은 간격 또는 일주일 중 일부 요일로 제한될 수 있습니다.

체크 박스를 선택하면 다음 옵션을 사용할 수 있습니다.

활동 일

요일을 하나 이상 선택하십시오.

> **힌트:** 둘 이상의 요일을 선택하려면, CTRL 키를 누른 채로 하루의 이름에 마우스 단추를 클릭하십시오.

시작 시간, 중지 시간, 시작 분, 중지 분

액세스 정책이 활성화되는 요일의 간격을 미세 조정하려면, 드롭 다운 메뉴에서 시작 및 종료 시간을 선택하십시오.

사용자 에이전트

사용자 에이전트가 식별한 허용된 클라이언트 및 브라우저, 즉 그것들의 식별 문자열입니다.

Mimetypes

들어오는 파일의 MIME 형식 목록을 한 줄에 하나씩 차단해야 합니다. MIME 유형은 차단 (블랙리스트) 될 수 있지만 허용되지는 않습니다 (즉, 화이트리스트에 있음). 따라서 이 옵션은 액세스 거부 정책에서만 사용할 수 있습니다. 이 옵션을 사용하면 회사 정책 (예: 멀티미디어 파일)에 해당하지 않는 파일을 모두 차단할 수 있습니다.

> **참고:** 사용 가능한 MIME 유형 목록은 모든 Linux 상자의 /etc/mime.types 파일, 공식 IANA 웹 페이지 및 RFC 2045 및 RFC 2046에서 찾을 수 있습니다.

액세스 정책

규칙에 따라 드롭 다운 메뉴에서 웹 액세스를 허용할지 또는 거부할지 선택하십시오. 액세스 거부로 설정하면 위의 Mimetypes 옵션이 활성화됩니다.

정책 상태

규칙의 사용 가능 여부. 사용 중지된 규칙은 적용되지 않으며, 기본값은 규칙을 사용하도록 설정

하는 것입니다.

프로필 필터링

액세스 정책이 **액세스 허용(Allow access)**으로 설정된 경우 사용할 수 있는 이 드롭 다운 메뉴는 규칙에서 수행해야 하는 검사 유형을 선택할 수 있게 합니다. 사용할 수 있는 옵션은 체크하지 않은 경우, **없음(none)**과 **바이러스만 검색(Virus detection only)**하는 경우만 탐지합니다. 또한 콘텐츠 필터 프로필이 만들어지면 (아래 **웹 필터** 섹션 참조) 규칙에 적용할 수 있습니다.

위치

새 규칙을 삽입해야 하는 위치입니다. 낮은 위치는 우선 순위가 높습니다.

사용 가능한 작업(액션)을 통해 규칙 목록에서 각 규칙을 편집, 활성화/비활성화 또는 삭제할 수 있습니다.

인증(Authentication)

Endian UTM Appliance의 프록시는 로컬 인증 (NCSA), LDAP (v2, v3, Novell eDirectory, AD), Windows Active Directory의 네 가지 인증 유형을 페이지 상단의 드롭 다운 메뉴에 표시합니다. (NTLM) 및 RADIUS. NCSA 유형은 액세스 자격 증명을 Endian UTM Appliance에 저장하지만, 다른 방법은 외부 서버에 의존합니다. 이러한 경우 해당 서버에 액세스하는데 필요한 모든 정보를 제공해야 합니다.

인증 유형을 선택할 드롭 다운 메뉴 아래에 두 개의 패널이 있습니다. 위의 인증 설정에는 일반적인 구성 항목이 포함되어 있으며, 인증 유형을 선택할 때 아래의 인증 유형이 변경되어 각 방법에 고유한 설정이 제공됩니다.

인증 설정

이 패널에서 구성할 수 있는 공통 항목은 다음과 같습니다.

인증 영역

인증 대화 상자에 표시된 텍스트로, Active Directory 도메인에 가입할 때, kerberos 또는 winbind의 영역으로 사용됩니다. Windows Active Directory를 인증에 사용하는 경우, PDC의 FQDN을 사용해야 합니다.

> **힌트:** 서버 이름이 localauth이고 도메인 이름이 example.org인 경우, FQDN은 localauth.example.org입니다.

인증 차일드의 수

동시에 실행할 수 있는 최대 인증 프로세스 수입니다.

인증 캐시 TTL (분)

삭제되기 전에 인증 데이터를 캐시해야 하는 시간 (분).

사용자 당 다른 IP 수

사용자가 프록시에 동시에 연결할 수 있는 최대 IP 주소 수입니다.

사용자 / IP 캐시 TTL (분)

IP 주소가 로그인 한 사용자와 관련된 시간 (분).

공통 구성 양식이 채워지면, 선택한 인증 유형에 따라, 선택된 인증 유형에 대한 특정 설정을 구성하는 것이 가능합니다. **로컬 인증 (NCSA)**, **Windows Active Directory (NTLM)**, **LDAP (v2, v3, Novell eDirectory, AD)**, **RADIUS**.

NCSA 특정 설정

NCSA 사용자 관리

사용자 관리 버튼을 클릭하면 기존 사용자의 간단한 목록 (작성된 경우)으로, 구성된 사용자의 관리 GUI가 열립니다. 각 사용자에 대해 수행할 작업은 다음과 같습니다.

-  - 사용자의 사용자 이름 또는 암호를 수정합니다.
-  - 사용자를 삭제합니다.

표 위에서 NCSA 사용자 추가 링크를 클릭하여 사용자를 추가하십시오. 양식에 사용자 이름과 비밀번호를 입력하기 만하면됩니다.

적용 단추를 클릭하여 사용자에 대한 변경 사항을 저장하십시오.

NCSA 그룹 관리

그룹 관리 버튼을 클릭하면, 그룹의 관리 GUI가 열리고, 기존 그룹 및 해당 구성원이 작성된 경우, 해당 구성원의 간단한 목록으로 구성됩니다. 각 그룹에서 수행할 작업은 다음과 같습니다.

-  - 이름이나 구성원을 변경하여 그룹을 수정합니다.
-  - 그룹을 제거합니다.

표 위에 NCSA 그룹 추가 링크를 클릭하여 그룹을 추가하십시오. 그룹은 그룹 이름을 입력하고 해당 그룹에 속해야 하는 하나 이상의 사용자를 선택하여 작성됩니다. 사용자는 둘 이상의 그룹에 속할 수 있습니다.

> **경고:** 동일한 사용자가 합법적으로 하나 이상의 그룹에 속할 수는 있지만 사용자가 속한 그룹이 대조 액세스 정책을 정의하지 않도록 주의해야 합니다. 예를 들어, 두 그룹의 사용자 구성원을 생각해보십시오. 하나는 정책이 웹 사이트 www.example.org에 액세스하도록 허용하고, 두 번째 그룹의 정책은 해당 웹 페이지에 대한 액세스를 차단합니다. 이 경우 해당 사용자가 사이트에 대한 액세스 권한을 부여받았는지 여부를 예측하는 것은 쉽지 않습니다. 이러한 문제의 관리는 액세스 정책의 설계자에게 맡깁니다.

최소 암호 길이

로컬 사용자 암호의 최소 길이는 기본적으로 6자입니다.

NTLM 특정 설정

AD 서버의 도메인 이름

연결할 액티브 디렉토리 도메인. 서버의 FQDN(전체 주소 도메인 이름, Fully Qualified Domain Name)을 사용해야 합니다.

AD 도메인 가입

도메인 가입 버튼을 클릭하여 도메인에 가입하십시오. 이 액션은 인증 설정을 저장하고 적용한 후에만 수행해야 합니다. 그러면 **AD 가입** 탭이 열립니다.

레거시 시스템의 도메인 이름

Active Directory가 Windows 2000 또는 이전 시스템에 있는 경우 여기에 도메인 이름을 작성하십시오.

버전 5.0의 새로운 기능.

AD 서버의 PDC 호스트 이름, ADC 서버의 PDC IP 주소

PDC의 호스트 이름과 IP 주소. DNS 항목을 작성하려면 호스트 이름과 IP 주소가 모두 필요합니다.

AD 서버의 BDC 호스트 이름 및 AD 서버의 BDC IP 주소

BDC(백업 도메인 컨트롤러)의 호스트 이름 및 IP 주소 (있는 경우). DNS 항목을 작성하려면, 호스트 이름과 IP 주소가 모두 필요합니다.

NTLM 사용 요구 사항.

Active Directory (NTLM)로 Windows의 고유 인증을 사용하려면, 몇 가지 조건이 충족되어야 합니다.

추가 참고사항: NTLM 인증을 사용하는 영역 설정은 이 자습서에 설명되어 있습니다.

Windows Vista 및 Windows 7에서의 NTLM 인증.

Endian UTM Appliance의 HTTP 프록시는 *협상된(negotiated)* NTLMv2를 사용하는 반면, Windows Vista 및 Windows 7은 기본적으로 *직접적(straight)* NTLMv2 만 허용합니다. 따라서 이러한 운영 체제 중 하나를 사용하는 클라이언트는 올바른 자격 증명을 제공할 때도 HTTP 프록시에 인증하지 못할 수 있습니다. 올바르게 인증하려면 클라이언트 구성을 다음과 같이 변경해야 합니다.

1. 시작 ‣ gpedit.msc (관리자 권한으로 실행)
2. 이동 : 컴퓨터 구성 ‣ Windows 설정 ‣ 보안 설정 ‣ 로컬 정책 ‣ 보안 옵션
3. 구성 옵션 찾기 네트워크 보안 : LAN MANAGER 인증 수준
4. "LM * NTLM 보내기 - 협상 된 경우 NTLMv2 세션 보안 사용"값을 선택하십시오.

이러한 변경 사항을 적용한 후, 클라이언트 브라우저는 HTTP 프록시의 AD 로그인 이름을 사용하여 올바르게 인증해야 합니다.

LDAP 관련 설정

LDAP 서버

LDAP 서버의 IP 주소 또는 FQDN입니다.

LDAP 서버의 포트

서버가 수신하는 포트입니다. 기본값은 389입니다.

바인드 DN 설정

기본 식별 이름, 검색 시작점입니다.

LDAP 유형

이 드롭 다운 메뉴에서는 **Active Directory, LDAP 버전 3, LDAP 버전 2** 또는 **Novell eDirectory** 중에서 인증 서버 유형을 선택할 수 있습니다.

바인드 DN 사용자 이름

사용자 특성을 읽을 수 있는 권한이 있어야 하는 사용자의 완전히 구별된 이름

바인드 DN 암호

바인드 DN 사용자의 비밀번호

user objectClass

바인드 DN 사용자가 속해야하는 objectClass입니다.

group objectClass

바인드 DN 그룹이 속해야하는 objectClass입니다.

RADIUS 관련 설정

RADIUS 서버

RADIUS 서버의 IP 주소 또는 URL입니다.

RADIUS 서버 포트

RADIUS 서버가 수신하는 포트입니다. 기본값은 **1645**입니다.

식별자

추가 식별자.

공유된 비밀

사용할 암호.

웹 필터

Endian UTM Appliance의 컨텐츠 필터 기능은 각 필터 프로파일에 대해 사용자 정의할 수 있는 두 가지 필터링 기술을 사용하는 Cyren URL 필터링 솔루션을 기반으로 합니다.

첫 번째 방법은 콘텐츠에 따라, 웹 페이지 분류의 고급 방법으로 구성되며, 두 번째 방법은 화이트리스트 및 블랙리스트 URL과 도메인의 조합을 사용합니다. 클라이언트가 요청한 모든 URL은 이 목록에서 조회되며, 허용된 사이트 목록(화이트리스트)에 있는 경우 게재됩니다.

> **참고:** 시스템이 아직 Endian Network에 등록되지 않은 경우, URL 필터 목록을 다운로드 할 수 없습니다. 이 경우 유익한 메시지가 나타납니다. 이를 클릭하면 등록 양식이 열립니다.

콘텐츠 필터를 사용하려면 프로필이 필요합니다. 모든 웹 페이지에 대한 액세스를 허용하며 절대로 삭제해서는 안되는 기본 프로필이 있습니다. 새로운 **액세스 정책**을 정의할 때, 필요한 추가 프로필을 쉽게 만들 수 있습니다.

이 페이지에는 설명(remark)과 함께 사용 가능한 작업(actions)별로 기존 프로필 목록이 있습니다.

-  - 프로필을 편집합니다.
-  - 프로필을 삭제합니다.

표 위에는 새 프로필 추가 링크가 있습니다. 이것을 클릭하면, 링크가 기존 프로필 목록이 페이지 아래쪽으로 이동하면서 새 프로필을 구성하는데 사용되는 프로필 편집기로 바뀝니다. 다음 설정을 정의할 수 있습니다.

프로필 이름

프로파일에 주어진 이름.

바이러스 백신 검색 활성화

콘텐츠 필터에서 바이러스 백신을 사용하도록 설정합니다.

세이프 서치 시행

이 다중 선택 입력란에서는 현재 지원되는 검색 엔진에 대해 SafeSearch 적용 기능을 활성화할 수 있습니다.

- Bing
- DuckDuckGo
- Google
- Yahoo
- Yandex

세이프 서치 시행

표준 웹 필터링 기능을 사용하면, 어린이 또는 학생을 위해 부적절한 웹 사이트를 필터링 할 수 있습니다. 그러나 검색 엔진의 미리보기 이미지와 같은 결과에는 영향을 미치지 않습니다.

다음 설정은 패널 형태로 제공되며, 제목 왼쪽에 확장 또는 축소 아이콘을 클릭하여 확장하거나 축소할 수 있습니다.

URL 필터

콘텐츠 필터 적용을 위해 활성화할 카테고리를 선택하십시오. 범주 이름의 맨 오른쪽에는, 포함된 항목이 콘텐츠 필터링에 사용되었거나 (➡) 또는 사용되지 않았는지 (🚫), 아니면 부분적으로 허용된 경우 (➡)인지를 아이콘들로 표시됩니다. 화살표를 클릭하면, 모든 항목의 상태를 신속하게 전환할 수 있습니다.

각 카테고리에는 개별적으로 선택할 수 있는 추가 하위 카테고리가 있습니다.

맞춤 블랙리스트(차단 목록) 및 화이트리스트(허용 목록)

이 텍스트 필드에서 개인화 된 웹 페이지 목록을 추가할 수 있습니다.

다음 사이트 허용

> 웹 페이지가 허용 목록(화이트리스트)에 있습니다. 즉, 항상 클라이언트에게 제공되는 웹 페이지입니다.

다음 사이트 차단

> 웹 페이지가 차단 목록(블랙리스트)에 있습니다. 즉, 클라이언트에 결코 제공되지 않습니다.

콘텐츠 필터링은 허위 긍정적 판단(false positive)과 허위 부정적 판단(false negative)을 유발할 수 있으므로 항상 금지 또는 허용되어야 하는 목록 도메인을 여기에 입력할 수 있습니다. 이 정책은 콘텐츠 필터의 분석 결과에 관계없이 적용됩니다.

광고 조인

이 섹션에서는 Active Directory Server에 가입하는데 필요한 자격 증명을 제공할 수 있습니다. 이 작업은 인증 탭에서 *Windows Active Directory* (NTLM) 옵션을 선택한 경우에만 가능합니다.

ADS admin의 사용자 이름

Active Directory Server의 사용자 이름입니다.

ADS admin의 비밀번호

Active Directory Server의 암호입니다. 기본적으로 표시되지 않지만, 텍스트 필드의 오른쪽에 있는 확인란을 선택하여 표시할 수 있습니다.

HTTPS 프록시

버전 5.0.5의 새로운 기능: URL 필터링 옵션.

이 페이지에서 HTTPS 프록시 서버를 구성하고, 콘텐츠 암호화를 SSL 암호화 트래픽 (즉, 443 포트를 통한 트래픽)에 가로 채서 적용하는 방식을 구성할 수 있습니다.

이 페이지는 처음에 3 개의 패널로 나뉘며, 첫 번째 패널은 HTTPS 프록시의 작동 모드를 선택하고, 다른 하나는 **해독 및 검색** 모드에서 필요한 인증서와 관련이 있습니다.

HTTPS 프록시 작동 모드

드롭 다운 메뉴에서 프록시가 HTTPS 암호화된 트래픽을 분석하는 방법을 선택하십시오. 다음 옵션을 사용할 수 있습니다.

- **비활성화(Disabled).** HTTPS 프록시는 트래픽을 분석하지 않습니다.
- **URL 필터링만(URL filtering only)**. 아래에 설명된 이 방식에서는 HTTP 프록시가 페이지에 콘텐츠 필터링만 적용하고 암호를 해독하지는 않습니다.
- **해독 및 검색.** HTTPS 프록시는 페이지를 해독하고 완전히 검사합니다.

양식(modality)이 선택되면, 저장을 클릭한 다음, 녹색 설명 선에 있는 적용 단추를 클릭하십시오.

URL 필터링 모드

URL 필터링 모드는 **해독 및 검색** 모드와 비교하여 덜 침략적으로 HTTPS 페이지에 콘텐츠 필터링을 적용할 수 있게 해줍니다. 또한 배포가 쉬우나 효과가 떨어질 수 있습니다. 자세한 내용은 해

해독 및 검색 모드로 설정하면, squid는 모든 클라이언트의 요청을 가로 채고 HTTP 요청의 경우처럼 원격 서버로 전달합니다. 유일한 차이점은 HTTPS 요청의 경우, 클라이언트가 HTTPS를 통해 Endian UTM Appliance에 연결하기 위한 중간 인증서가 필요하다는 것입니다. 그런 다음 Endian UTM Appliance는 요청을 전달하고, 원격 리소스를 검색하여 제어한 다음, 그것을 요청한 클라이언트에게 보냅니다.

이 모드에서는 다음과 같은 추가 옵션을 사용할 수 있습니다.

모든 인증서 수락

이 옵션은 Endian UTM Appliance가 유효하지 않거나 오래 되었더라도 원격 서버의 모든 인증서를 자동으로 수락할 수 있게 해줍니다.

업스트림 프록시에 직접 HTTPS 연결 전달

이 옵션이 사용되면, HTTPS 트래픽이 업스트림 프록시에 의해 직접 관리되고, 그렇지 않으면 Endian UTM Appliance에서 관리됩니다.

> **참고:** 이 옵션은 업스트림 프록시가 업스트림 프록시에 정의된 경우에만 작동합니다 (Menubar ‣ proxy ‣ HTTP ‣ Configuration ‣ Upstream proxy 참조).

대상에 HTTPS 프록시 사용 안함

텍스트 필드에 HTTPS 프록시가 점검하지 않아야 하는 원격 웹 사이트의 IP 주소 또는 도메인 이름을 한 줄에 하나씩 입력하십시오.

하단의 두 패널은 **해독 및 검색** 모드에서만 사용되며, Endian UTM Appliance에서 사용할 인증서를 관리할 수 있습니다.

> **경고:** 새 인증서를 업로드하거나 만들면 이전에 업로드되거나 생성된 인증서가 무효화됩니다. 또한 모든 클라이언트에 새 인증서를 배포해야 합니다.

HTTPS 프록시 화이트리스트의 항목.

항목이 IP 주소인 경우, 해당 IP로 향하는 HTTPS 트래픽은 HTTPS 프록시로부터 전달되지 않습니다. 항목이 도메인 이름일 (예: **www.example.org**) 때는, 해당 사이트만 바이 패스됩니다. 그러나 도메인 이름의 시작 부분에 점(.)을 사용하면, 그 사이트의 모든 하위 도메인에 대한 트래픽도 허용됩니다. 몇 가지 예는 다음과 같습니다.

*93.184.216.119*는 IP https://93.184.216.119/ 만 허용합니다.
*www.example.org*는 https://www.example.org/ 사이트만 허용
*.example.org*는 .example.org로 끝나는 모든 사이트를 허용합니다. 예를 들어,
https://www.example.org/index.html
https://mail.example.org/mail.html
https://www.news.example.org/news.html
사이트들이 모두 허용됩니다.

프록시 인증서 업로드

기존 인증서를 사용하려면 찾아보기... 를 클릭하고 로컬 하드 디스크에서 인증서를 선택한 다음, 업로드를 클릭하여, 인증서를 Endian UTM Appliance에 복사합니다.

새 인증서 만들기

처음부터 새 인증서를 만들려면, 이 단추를 클릭하십시오. 확인을 요구하는 확인 대화 상자가 나타납니다. 계속하려면 확인을 클릭하고, 대화 상자를 닫고 돌아가려면, 취소를 클릭하십시오.

인증서를 업로드하거나 만든 후에는 프록시 인증서 업로드 라벨 옆에 하이퍼링크 형식의 새로운 옵션이 나타납니다.

다운로드

이 하이퍼링크를 클릭하면, 클라이언트가 필요로 하는 인증서를 다운로드 할 수 있습니다.

추가 참고사항: 지식 기반에서는 이러한 자습서들을 사용할 수 있습니다.

HTTPS 프록시 설정 방법 (해독 및 스캔 모드 만),

HTTPS 프록시에 대한 URL 필터링 및

HSTS 지원 사이트에 액세스하는 방법

POP3

이 페이지에서 다음 항목을 찾을 수 있습니다:

이 페이지에는 spamassassin 메일 필터의 구성 옵션과 스팸으로 인식된 전자 메일을 관리하는 방법이 포함되어 있습니다.

전역 설정

이 페이지에서 적절한 확인란을 선택하면 POP3 프록시의 몇 가지 글로벌 구성 설정을 사용할 수 있습니다.

Green 구역에서 활성화, Blue 구역에서 활성화, Orange 구역에서 활성화

GREEN, BLUE 및 ORANGE 구역에서 각각 POP3 전자 메일 스캐너를 사용하도록 설정합니다. 해당 영역이 활성화된 경우에만 나타납니다.

바이러스 스캐너

바이러스 스캐너를 활성화하십시오.

스팸 필터

전자 메일에서 스팸 필터링을 사용합니다.

SSL/TLS 암호화 연결 차단

확인란을 선택하면 SSL/TLS를 통한 연결에서 바이러스가 있는지 검사합니다.

방화벽이 발신 연결을 기록.

모든 나가는 연결이 방화벽에 의해 기록되도록 하십시오.

스팸 필터

이 페이지에서는 스팸 전자 메일을 발견했을 때 POP3 프록시가 어떻게 진행되어야 하는지 구성할 수 있습니다.

> **참고:** 전자 메일이 스팸으로 표시되더라도, 원래 받는 사람에게 배달됩니다. 실제로 이메일을 전달하지 않으면 수신자에게 전자 메일을 전달해야 한다는 RFC 2821을 위반하게됩니다.

스팸 주제 태그

스팸으로 인식된 전자 메일의 제목에 추가될 접두사입니다.

메일 본문에 스팸 보고서 추가

확인란을 선택하여, 각 스팸 전자 메일에서 원래 전자 메일의 본문을 spamassassin 데몬의 보고서로 대체하고, 전자 메일이 스팸으로 표시된 이유를 확인하십시오.

필수 조회수

스팸으로 간주되는 메시지에 필요한 조회 횟수.

일본어 이메일 지원 활성화

이 체크 박스를 선택하면, 일본어 스팸을 검색하기 위해 전자 메일에서 일본어 문자 집합에 대한 지원을 활성화합니다.

메시지 다이제스트 스팸 탐지 사용 (pyzor)

pyzor를 사용하여 스팸 전자 메일을 처리하는 확인란을 선택합니다. (간단히 말해, 스팸 전자 메일은 유사한 스팸 전자 메일을 식별하는데 사용할 수 있는 고유 다이제스트 메시지로 변환됩니다.)

> **경고:** 이 옵션을 활성화하면, POP3 프록시가 상당히 느려질 수 있습니다!

화이트 리스트

와일드카드를 사용하여 한 줄에 하나씩 지정되는 전자 메일 주소 또는 전체 도메인의 목록입니다. 이러한 주소와 도메인에서 보낸 전자 메일은 **절대로** 스팸을 확인하지 않습니다.

블랙 리스트

와일드카드를 사용하여 한 줄에 하나씩 지정되는 전자 메일 주소 또는 전체 도메인의 목록입니다. 이러한 주소와 도메인에서 보낸 전자 메일은 **항상** 스팸으로 표시됩니다.

> **참고:** 전체 도메인에 대해 와일드 카드를 사용하려면 다음 구문을 사용하십시오. ***@example.com**

저장 버튼을 클릭하여 설정을 저장할 수 있습니다.

암호화된 전자 메일.

Endian UTM Appliance는 암호화된 채널이기 때문에, POP3 SSL 연결을 통해 보낸 전자 메일을 검사할 수 없습니다.

따라서 클라이언트가 SSL을 통해 POP3를 사용할 수 있게 하려면, 적절하게 구성하고 클라이언트에서 Endian UTM Appliance로의 암호화를 비활성화해야 합니다. 암호화를 사용 중지해야 합니다 (예: SSL을 사용하지 않음). 일반 텍스트의 POP3 트래픽 포트가 기본 110에서 995로 변경되었습니다.

이 구성을 설정하면, 클라이언트에서 Endian UTM Appliance 로의 연결은 일반 텍스트로 유지되지만, 포트 995를 사용하여 Endian UTM Appliance 설정에서 암호화된 POP3 over SSL 연결을 POP3 서버로 설정합니다.

FTP

FTP 프록시는 활성화된 영역에서 투명한 프록시로만 사용할 수 있으며, FTP를 통해 다운로드한 파일을 검사하여 바이러스를 검색할 수 있습니다. Endian UTM Appliance는 frox를 FTP 프록시로 사용합니다.

> **참고:** 표준 FTP 포트 (21)에 대한 연결만 프록시로 리디렉션됩니다. 즉, 클라이언트가 FTP 프록시에도 HTTP 프록시를 사용하도록 구성된 경우, FTP 프록시의 설정이 무시됩니다.

이 페이지에서는 몇 가지 옵션을 구성할 수 있습니다.

Green 구역에서 활성화, Blue 구역에서 활성화, Orange 구역에서 활성화

각 영역에서 FTP 프록시를 활성화합니다. 활성화된 영역에서만 사용할 수 있습니다.

방화벽이 발신 연결을 기록.

방화벽에 나가는 연결을 기록하십시오.

소스로부터 투명 프록시 우회

아래 텍스트 영역에 작성된 클라이언트가 FTP 프록시를 거치지 않고 원격 사이트에 직접 액세스할 수 있게 해줍니다.

투명한 프록시를 목적지로 우회

클라이언트가 FTP 프록시를 통하지 않고, 아래 텍스트 영역에 작성된 원격 사이트에 직접 액세스할 수있게 해줍니다.

FTP 프록시 및 FTP 클라이언트의 활성 및 수동 모드

Endian UTM Appliance는 인터넷에 직접 연결되어 있는 경우에만 **frox**로 투명한 FTP 프록시를 지원합니다.

FTP 투명 프록시가 활성화되어 있고, Endian UTM Appliance와 인터넷 사이에 NAT 장치가 있는 경우, 문제가 발생할 수도 있습니다. 이 설정에서 원격 FTP 사이트에 대한 모든 FTP 연결은 시간이 초과될 때까지 차단되고, 로그에 다음과 같은 메시지가 표시됩니다

이 예에서 *192.168.1.2*는 원격 FTP 사이트에 액세스하려는 클라이언트의 IP 주소입니다.

이 문제를 극복하려면, FTP 클라이언트가 **수동 모드 (PASV)**를 전송 모드로 사용하도록 구성해야 하며, *Menubar ▸ Firewall ▸ System access* 아래에 있는 규칙을 만들어야 NAT-ed 클라이언트에 대한 **50000 ~ 50999** 포트의 트래픽을 허용하게 됩니다. 보안상의 이유로, 이 포트는 필요한 경우에만 활성화해야 합니다. 이 설정의 동기를 이해하기 위해, 여기서는 활성 모드와 수동 모드가 작동하는 방식과 FTP 프록시와 상호 작용하는 방식에 대해 자세히 설명합니다.

활성 모드에서는 서버 (이 경우 FTP 프록시)가 클라이언트에 대한 데이터 연결을 시작해야 합니다. 그러나 클라이언트와 프록시 사이의 NAT 장치가 서버의 연결을 클라이언트에 도달하지 못하게 합니다. 이러한 이유로 클라이언트는 패시브 모드를 사용해야합니다.

수동 모드에서는 ftp 클라이언트가 제어 연결을 통해 협상된 동적 포트를 사용하여 서버 (다시, FTP 프록시)에 대한 연결을 시작해야 합니다. ftp 프록시는 해당 포트를 청취하지만, 시스템 액세스 방화벽은 해당 포트로의 트래픽을 허용해야 합니다.

다중 동시 데이터 연결이 ftp 프록시에 액세스하려고 하므로, 전체 포트 범위에 대한 연결을 허용해야 합니다. 따라서 수동 데이터 연결용으로 예약된 모든 포트 (예: **50000-50999**)는 시스템 액세스 방화벽에서 허용해야 합니다 .

SMTP

이 페이지에서는 다음 내용을 찾으실 수 있습니다.

SMTP 프록시는 클라이언트에서 메일 서버로 전자 메일 트래픽이 전송될 때, 전자 메일 트래픽을 릴레이 및 필터링 할 수 있습니다.

> **참고**: SMTP 프록시가 암호화를 지원하는 동안, 외부 스마트 호스트가 SMTP 프록시로 사용될 때, SSL/TLS 및 STARTTLS 프로토콜을 사용할 수 없습니다.

SMTP 프록시의 목적은 SMTP 트래픽을 제어 및 최적화하고 SMTP 프로토콜을 사용할 때, 로컬 네트워크를 위협으로부터 보호하는 것입니다. SMTP는 로컬 전자 메일 클라이언트에서 원격 메일 서버로 전자 메일이 전송될 때마다, 즉, 보내는 전자 메일에 사용될 때마다 사용됩니다. 또한 메일 서버가 LAN (즉, GREEN 영역내) 또는 DMZ (ORANGE 영역)에서 실행 중이고, 전자 메일을 t hat 메일 서버를 통해 로컬 네트워크 (수신 요청) 외부에서 전송될 수 있는 경우, 즉, 클라이언트가 RED 인터페이스에서 전자 메일을 보낼 수 있는 경우에도 사용됩니다.

원격 메일 서버에서 로컬 전자 메일 클라이언트로 메일을 다운로드하려면, POP3 또는 IMAP 프로토콜이 사용됩니다. 또한 해당 트래픽을 보호하려면, *Menubar ‣ Proxy ‣ POP3*에서 POP3 프록시를 활성화하십시오.

> **경고:** IMAP 트래픽 검색은 현재 지원되지 않습니다.

전자 메일 프록시 기능을 사용하면, 수신 및 발신 전자 메일 트래픽 모두에서 바이러스, 스팸 및 기타 위협을 검색할 수 있습니다. 전자 메일은 필요한 경우 차단되며, 이 경우에 받는 사용자와 관리자에게 통보됩니다. 전자 메일 프록시는 들어오는 전자 메일을 검색할 수 있으므로 RED 인터페이스에서 들어오는 연결을 처리하고 전자 메일을 하나 이상의 내부 메일 서버로 전달할 수 있습니다. 따라서 적절한 포트 전달 규칙을 정의할 필요없이, 방화벽 뒤에서 자체 메일 서버를 실행할 수 있습니다.

SMTP 프록시 구성 옵션은 SMTP 프록시의 다른 부분에 대해 각각 탭으로 그룹화되어 있습니다.

구성 (Configuration)

이것은 SMTP 프록시의 기본 구성 페이지입니다. 토글 스위치  를 클릭하여 SMTP 프록시를 활성화할 수 있습니다. 활성화된 경우, 각 활성 구역에 대해 SMTP 프록시가 활성, 비활성 또는 투명해야 하는지 여부를 선택할 수 있습니다.

활성화(Active)

SMTP 프록시는 영역에서 사용하도록 설정되고, 포트 25에서 요청을 수락합니다.

투명 모드(Transparent mode)

투명 모드를 사용하면 대상 포트 25에 대한 모든 요청이 가로 채어져 클라이언트의 구성을 변경할 필요없이 SMTP 프록시로 전달됩니다. RED 구역에서는 이 옵션을 사용할 수 없습니다.

비활성(Inactive)

해당 영역에 대해 SMTP 프록시를 사용할 수 없습니다.

5개의 패널로 그룹화된 추가 옵션을 사용할 수 있습니다. 펼치기 ⊞ 아이콘을 클릭하거나 접기 ⊟ 아이콘을 클릭하여 각 패널을 펼칠 수 있습니다.

스팸 설정 (Spam settings)

이 패널에는 다음 옵션을 구성하여, Endian UTM Appliance에서 스팸을 인식하고 필터링하도록 사용하는 소프트웨어 응용 프로그램을 구성할 수 있습니다.

스팸 메일 필터링

메일 스팸 필터를 사용하고 아래에 표시되는 추가 옵션을 구성할 수 있습니다.

스팸 처리 선택

스팸으로 인식된 전자 메일에는 다음 세 가지 작업을 수행할 수 있습니다.

- **기본 격리 보관 위치로 이동:** 스팸 전자 메일이 기본 위치로 이동합니다.
- **격리 전자 메일 주소로 보내기:** 스팸 전자 메일은이 옵션을 선택하면 표시되는 스팸 격리 전자 메일 주소 텍스트 상자에 지정할 수있는 사용자 지정 전자 메일 주소로 전달됩니다.
- **스팸으로 표시:** 전자 메일은 배달 전에 스팸으로 표시됩니다.
- **이메일 삭제:** 스팸 전자 메일은 즉시 삭제됩니다.

스팸 제목

스팸으로 표시된 모든 전자 메일의 제목에 적용되는 접두사입니다.

스팸 알림에 사용되는 이메일 (스팸 관리자)

처리된 각 스팸 전자 메일에 대한 알림을받을 전자 메일 주소입니다.

스팸 태그 레벨

SpamAssassin의 스팸 점수가 이 숫자보다 크면, **X-Spam-Status** 및 **X-Spam-Level** 헤더가 전자 메일에 추가됩니다.

스팸 표시 수준

SpamAssassin의 스팸 점수가 이 숫자보다 크면, **스팸 제목**과 **X-Spam-Flag** 헤더가 전자 메일에 추가됩니다.

스팸 격리 수준

이 스팸 점수를 초과하는 전자 메일은 격리 위치로 이동됩니다.

아래 수준에서만 알림 보내기

스팸 점수가 이 숫자보다 낮으면 알림 전자 메일을 보냅니다.

스팸 필터링

스팸 greylisting을 활성화하고 다음 옵션을 표시하십시오.

그레이리스트 (greylisting) 지연 (초)

그레이리스트 지연은 **30 ~ 3600** 초 사이의 값일 수 있습니다.

스팸 신고

확인란을 선택하여, 스팸으로 인식되는 전자 메일 본문에 보고서를 추가합니다.

일본화(Japanization)

전자 메일에서 일본어 문자 세트에 대한 지원을 활성화하고 일본어 스팸 전자 메일을 필터링하려면, 이 확인란을 선택하십시오.

> **참고:** 대부분의 간단하고 잘 알려진 스팸 메시지와 알려진 스팸 호스트가 보낸 메일은 차단되지만 스패머는 스팸 필터를 우회하기 위해 항상 메시지를 수정합니다. 따라서 개인화되고 강력한 (베이지안) 필터에 도달하려면 스팸 필터를 항상 교육해야합니다.

바이러스 설정 (Virus settings)

이 패널에는 처리된 전자 메일에서 발견된 바이러스를 관리하는 방법을 구성하는 옵션이 나타납니다.

메일 바이러스 스캐너

바이러스에 대한 전자 메일 필터링을 사용하고 추가 옵션을 표시합니다.

바이러스 처리 선택

스팸으로 인식된 전자 메일에서 수행할 수 있는 세 가지 또는 네 가지 사용 가능한 작업 (Endian UTM Appliance 유형에 따라 다름)이 있습니다. 위의 *스팸 설정*과 동일합니다.

- **기본 격리 보관 위치로 이동:** 바이러스가 포함된 모든 전자 메일이 기본 위치로 이동됩니다.
- **격리된 전자 메일 주소로 보내기:** 바이러스가 포함된 전자 메일은 이 옵션을 선택하면, 표시되는 바이러스 차단 전자 메일 주소 텍스트 상자에 지정할 수 있는 사용자 지정 전자 메일 주소로 전달됩니다.
- **수신자에게 전달 (불량 내용에 관계없이):** 바이러스가 포함된 이메일은 정상적으로 배달됩니다.
- **이메일 삭제:** 바이러스가 포함된 이메일이 즉시 삭제됩니다.

바이러스 알림에 사용되는 이메일 (바이러스 관리자)

바이러스가 포함하고 있어서 처리된 전자 메일에 대한 알림을 받을 전자 메일 주소입니다.

알림 발신자 주소

알림의 보낸 사람으로 표시될 전자 메일 주소입니다.

수신자에게 바이러스가 포함된 이메일 알림

확인란을 선택하여 전자 메일의 원래 수신자에게 전자 메일이 차단되었다는 알림을 보냅니다.

구성된 수신 도메인의 주소에만 알림을 보냅니다.

수신 도메인 (Incoming domains)에 구성된 도메인의 수신자에게만 통지를 보내려면, 체크 박스를 선택하십시오 (*Proxy ‣ SMTP ‣ Incoming domains* 참조).

파일 설정 (File settings)

이 패널에는 전자 메일에 첨부된 파일을 확장명에 따라 차단하는 설정이 있습니다. 파일 확장명이 첨부 파일에서 발견될 때마다 선택한 작업이 수행됩니다.

확장명으로 파일 차단

파일에 확장자 기반 필터링을 활성화하고 추가 바이러스 필터 옵션을 표시하십시오.

차단된 파일 처리 선택

차단된 전자 메일에는 다음 세 가지 작업을 수행할 수 있습니다 (이전 **스팸 설정** 및 **바이러스 설정** 패널과 동일 함).

- **기본 격리 보관 위치로 이동:** 차단된 파일이 포함된 전자 메일은 기본 위치로 이동됩니다.
- **격리된 전자 메일 주소로 보내기:** 차단된 파일이 포함된 전자 메일은 이 옵션을 선택하면, 표시되는 차단된 파일 알림용 텍스트 상자에 지정할 수 있는 사용자 지정 전자 메일 주소로 전달됩니다.
- **수신자에게 전달 (차단된 파일과 관계없음):** 차단된 파일이 포함된 전자 메일은 정상적으로 배달됩니다.

차단된 파일 알림에 사용되는 이메일 (파일 관리자)

차단된 첨부 파일이 포함하고 있는 전자메일을 각각 처리한 것에 대한 알림을 받을 전자 메일 주소입니다.

차단된 파일 유형이 포함된 아카이브 차단

체크 박스를 선택하면 확장자가 차단된 파일이 포함된 모든 보관 파일을 차단할 수 있습니다.

> **힌트: 프로그램 (.exe)**이 차단할 하나의 파일 유형으로 선택되면, .zip, .tar.gz 또는 **.exe**로 끝나는 파일을 포함하는 다른 아카이브가 차단됩니다.

확장자가 두 개인 파일 차단

exe.jpg 또는 **bat.jpg**와 같은 두 개의 확장자를 가진 파일의 차단을 활성화하십시오. 체크하면 다음 옵션이 나타납니다.

확장자가 두 개인 파일 차단

이 텍스트 영역에서는 파일의 두 번째 확장자로 나타날 때 차단되어야 하는 모든 확장을 한 줄에 하나씩 쓸 수 있습니다. 텍스트 영역에 적어도 하나를 제공해야 합니다. 그렇지 않으면 효과가 없습니다. 와일드카드는 허용되지 않습니다.

> **힌트:** 엔트리 **.jpg**는 확장자가 **exe.jpg** 또는 **bat.jpg**인 파일을 차단하지만, 확장자가 **jpg.exe, jpg.bat**인 파일은 허용합니다.

> **참고:** 이중 확장명을 가진 파일은 일반적으로 파일 브라우저에서 불쾌한 이미지나 문서로 나타날 수 있는 악의적인 파일이지만 클릭할 때, 컴퓨터를 손상시키거나 개인 데이터를 훔치는 목적을 가진 응용프로그램이 실행됩니다. 이중 확장명을 가진 파일은 일반 파일과 동일하지만, 이름 (예: image.jpg) 뒤에 **.exe, .com, .vbs, .pif, .scr, .bat, .cmd** 또는 **.dll** (예: image.jpg.exe)과 같은 다른 확장자가 뒤따릅니다.

차단할 파일 형식을 선택하십시오 (확장자 기준).

차단할 파일 확장자.

> **힌트:** CTRL 키를 누른 상태에서 마우스 왼쪽 버튼을 클릭하면, 여러 확장자를 선택할 수 있습니다.

각 로컬 서버가 담당해야하는 전자 메일 도메인을 구성해야합니다. 도메인 - SMTP 서버 조합 목록은 *Menubar ‣ Proxy ‣ SMTP ‣ Incoming domains*의 수신 도메인에서 정의할 수 있습니다.

격리 설정 (Quarantine settings)

이 패널에는 하나의 옵션만 있습니다.

격리 보존 기간 (일)

이메일이 자동으로 삭제되기 전에 Endian UTM Appliance의 특별 검역 위치에 저장되는 일 수.

힌트: 검역소에 저장된 전자 메일은 Menubar ‣ Services ‣ Mail Quarantine에 있는 메일 격리 (Mail Quarantine)에서 관리할 수 있습니다.

투명 프록시 우회 (Bypass transparent proxy)

마지막 패널에서 투명한 프록시를 사용하지 않도록 설정해야 하는 도메인의 사용자 지정 목록을 정의할 수 있습니다.

SUBNET/IP/MAC에서 투명 프록시 우회

이러한 소스에서 보낸 전자 메일은 투명한 프록시의 영향을 받지 않습니다.

투명 프록시를 SUBNET/IP로 우회

이러한 대상으로 보낸 전자 메일은 투명한 프록시의 영향을 받지 않습니다.

블랙리스트 및 화이트리스트 (Black- & Whitelists)

이 페이지에는 네 개의 패널이 있습니다. 세 개는 사용자 정의 블랙리스트 및 화이트리스트의 정의를 허용하고, 네 번째는 기존 RBL(실시간 블랙리스트)을 선택하고 사용합니다.

수락된 메일 (블랙리스트 및 화이트리스트)

첫 번째 패널에서는 화이트리스트 또는 블랙리스트에 등록할 도메인, 하위 도메인 또는 단일 전자 메일 주소를 원하는 수만큼 입력할 수 있습니다. 두 목록 모두 다음과 같이 원하는 수의 보낸 사람, 받는 사람 및 클라이언트를 적절한 텍스트 영역에 입력할 수 있습니다.

수신자/발신자 블랙리스트 및 화이트리스트의 예:

전체 (하위) 도메인은 다음과 같이 화이트리스트 또는 블랙리스트에 올 수 있습니다.

- 하위 도메인을 포함한 도메인: example.com
- 하위 도메인: .example.com 만
- 단일 주소: info@example.com, admin@example.com

클라이언트 블랙리스트 및 화이트리스트의 예:

- 도메인 또는 IP: example.com, 10.10.121.101, 192.168.100.0/24

화이트리스팅 발신자

이 주소 또는 도메인에서 보낸 모든 전자 메일이 허용됩니다. 이것은 전자 메일의 보낸 사람 (From): 필드입니다.

블랙리스트 발신자

이러한 주소들이나 도메인들에서 보낸 모든 전자 메일은 거부됩니다. 이것은 전자 메일의 보낸 사람 (From): 필드입니다.

화이트리스트(허용 목록) 수신자

이러한 주소들이나 도메인들에서 보낸 모든 전자 메일이 수락됩니다. 이것은 전자 메일 To: 필드입니다.

블랙리스트 수신자

이러한 주소들이나 도메인들에서 전송된 모든 전자 메일은 거부됩니다. 이것은 전자 메일 To: 필드입니다.

화이트리스트 클라이언트

이러한 IP 주소 또는 호스트에서 보낸 모든 전자 메일이 허용됩니다.

블랙리스트 클라이언트

이러한 IP 주소 또는 호스트에서 보낸 모든 전자 메일은 거부됩니다.

실시간 블랙리스트 (Realtime Blacklist (RBL))

스팸 전자 메일을 차단하는데 자주 사용되는 방법인 RBL은 두 번째 패널에서 사용을 구성할 수 있습니다. 이 목록은 스팸 메일을 보내고 차단하는데 사용되는 새로운 SMTP 서버를 가능한 빨리 식별할 목적으로 여러 조직에서 만들고 관리하고 업데이트합니다. 도메인 또는 발신자 IP 주소가 블랙리스트 중 하나에 나타나면, 거기에서 보낸 전자 메일은 더 이상의 통지없이 거부됩니다. RBL을 사용하면 메일이 합법적인 전자 메일처럼 받아들여지거나 처리되지 않고 발신자의 IP 주소나 도메인이 차단 목록에 포함되는 즉시 삭제되기 때문에 대역폭이 절약됩니다. Endian UTM Appliance는 IP 기반 및 도메인 기반으로 구분되는 다양한 RBL을 사용합니다. 각 카테고리에 속한 차단 목록은 작은 확장 아이콘을 클릭하여 표시되며 목록 상단의 빨간색 또는 녹색 화살표를 클릭하거나 개별적으로 클릭 또는 사용 중지할 수 있습니다. 목록을 컴파일하는 다양한 조직의 홈페이지는 목록의 이름을 클릭하여 접근할 수 있습니다.

> **경고:** 때때로 IP 주소 또는 도메인이 RBL 운영자에 의해 잘못 나열될 수 있습니다. 만약 이러한 일이 발생하고, 해당 도메인의 합법적인 전자 메일조차도 복구할 수 없으면 거부되므로 통신에 부정적인 영향을 미칠 수 있습니다. RBL에 직접 영향을 줄 가능성은 없으므로 RBL을 사용하기 전에 RBL을 관리하는 조직에서 적용한 정책을 고려해야 합니다. Endian은 RBL을 사용하여 손실될 수 있는 전자 메일에 대해서는 책임을 지지 않습니다.

설치된 블랙리스트에는 다음과 같은 것들이 있습니다.

bl.spamcop.net

사용자들의 제출물을 기반으로 한 블랙리스트.

zen.spamhaus.org

이 목록에는 Spamhaus 블록 목록과 Spamhaus의 공격 차단 목록 및 해당 정책 차단 목록이 포함됩니다.

cbl.abuseat.org

CBL은 매우 큰 스팸 함에서 원본 데이터를 가져옵니다. 그것은 단지 스팸, 웜, 자신의 다이렉트 메일 전송을 수행하는 바이러스 또는 일부 유형을 전송하기 위해 악용된 다양한 종류의 프록시 (예: HTTP, 양말, AnalogX, wingate 등)에 특정한 특성을 나타내는 IP만을 나열합니다 어떤 종류의

개방형 프록시 테스트를 수행하지 않고도 일부 유형의 트로이 목마 또는 "스텔스" 스팸웨어를 차단할 수 있습니다.

[이름] .dnsbl.sorbs.net 및 rhsbl.dnsbl.sorbs.net

이 기관에서 몇가지의 블랙리스트가 제공되며 ([이름]을 **safe, relays, spam** 및 **zombie**로 대체하십시오.), **dsnbl.sorbs.net** 블랙리스트를 사용함으로써, 개별적으로 또는 모두 함께 활성화할 수 있습니다.

uceprotect.net

알려진 스팸 소스의 도메인을 최대 7일 동안 보유하고 있는 목록입니다. 이 기간이 지나면, 도메인은 삭제되지만 이후의 위반은 더 제한적인 정책이 적용되게 만듭니다.

RBL은 두 개의 상자로 그룹화됩니다. 왼쪽에는 IP 기반 RBL이 있고, 오른쪽에는 도메인 기반 RBL이 있습니다. 하나의 상자에서 모든 RBLS를 활성화하려면, 상자의 제목 표시 줄 옆에 있는 ⃠ 아이콘을 클릭하십시오 (아이콘이 ➔가 될것입니다). 반면, 일부 RBL만 활성화하려면, 각 RBL 이름 옆에 있는 ⃠ 아이콘을 클릭하십시오. 이 경우, 제목 표시줄의 ⃠ 또는 ➔ 아이콘이 ⇄ 아이콘으로 바뀔 것입니다.

스팸 그레이리스트 (Spam greylisting)

스팸 그레이리스트

스팸 그레이리스트는 처음 전자 메일을 거부하고 동일한 전자 메일의 두 번째 발송을 기다리면서 전자 메일이 합법적인지 여부를 확인하기 위해 MTA에서 사용하는 방법입니다. 전자 메일을 더 이상 수신하지 않으면, 보낸 사람이 스팸 소스로 간주됩니다. greylisting의 배경은 모든 대량 스팸 봇이 거부된 전자 메일을 다시 보내려고 하지 않으므로 유효한 전자 메일만 다시 보낼 것이라는 것입니다.

세 번째 패널에서 Greylisting 화이트리스트는 두 개의 텍스트 영역에 있는 모든 수신자, IP 주소 또는 네트워크에 대한 항목을 추가하여 만들 수 있습니다. 화이트리스트의 항목에는 그레이리스트가 적용되지 않습니다.

화이트리스트 수신자

이 텍스트 영역에 작성된 모든 전자 메일 주소 또는 전체 도메인 (예: **test@example.com** 또는 **example.com**)은 "안전한" 것으로 간주됩니다. 즉, 수신된 전자 메일은 스팸으로 검사되지 않습니다.

화이트리스트 클라이언트

이 텍스트 영역의 모든 메일 서버의 주소는 "안전한" 것으로 간주됩니다. 즉, 이 서버의 주소에서 오는 모든 전자 메일은 스팸으로 검사되지 않습니다.

스팸 (블랙리스트 및 화이트리스트)

네 번째 및 마지막 패널에는 스팸 필터에 대한 명시 적 블랙 및 화이트리스트가 정의되어 있습니다.

화이트 리스팅 발신자

전자 메일 주소 또는 전체 도메인은이 텍스트 영역에서 허용 목록에 포함될 수 있습니다 (예: 스팸으로 감지되지 않음). test@example.com 또는 example.com 도메인

블랙리스트 발신자

전자 메일 주소 또는 전체 도메인은 이 텍스트 영역에 블랙리스트에 올릴 수 있습니다 (예: 전자 메일 주소는 항상 스팸으로 탐지됩니다). test@example.com 또는 example.com 도메인

수신 도메인 (Incoming domains)

*수신 도메인*은 RED 인터페이스 외부의 클라이언트가 로컬 SMTP 서버에서 전자 메일을 보내도록 허용되어 있고, 전자 메일이 보통 ORANGE 영역에 설정된 Endian UTM 어플라이언스 뒤의 메일 서버로 전달되어야 할 때 구성해야 합니다. 서로 다른 도메인에 대해 Endian UTM Appliance 뒤에 여러 메일 서버를 지정할 수 있습니다.

이 페이지는 메일 서버가 정의되어 있는 경우, 각 메일 서버와 함께 도메인 목록을 제공합니다. 새 도메인을 추가하려면, 도메인 추가 버튼을 클릭하십시오. 도메인 메일 서버 조합을 작성할 수 있는 간단한 양식이 열립니다.

도메인

메일 서버가 담당하는 도메인.

메일 서버 IP

메일 서버의 IP 주소.

새 항목이 목록 맨 아래에 표시됩니다. 각 도메인에서 사용할 수 있는 작업은 다음과 같습니다.

-  - 도메인 속성을 수정합니다.
-  - 도메인을 제거합니다.

> **경고:** 삭제 () 아이콘을 클릭한 후 확인을 요청하지 않습니다. 도메인이 즉시 제거됩니다.

도메인 라우팅

이 페이지는 해당 도메인으로 또는 도메인으로부터 발송된 전자 메일을 전달할 책임이 있는 스마트호스트와 함께 도메인 목록을 표시합니다. 목록에 표시된 정보는 새 도메인을 추가할 때 제공되는 정보와 동일합니다. 사용 가능한 작업들(액션들)은 다음과 같습니다.

-  - 도메인 라우팅을 수정하십시오.
-  - 도메인 라우팅을 제거합니다.

새 도메인을 추가하려면, 새 도메인 경로 추가 버튼을 클릭하십시오. 도메인 메일 서버 조합을 생성할 수 있는 간단한 양식이 열립니다.

방향

규칙을 보낸 사람과 관련된 도메인에 적용할지 받는 사람에 적용할지를 결정합니다.

도메인

이 메일 서버가 담당하는 도메인.

발신 주소

드롭 다운 메뉴에서 전자 메일을 보낼 업링크의 인터페이스 또는 IP 주소를 선택하십시오.

> **참고:** 공란으로 남겨두면 스마트 호스트가 사용할 업링크 또는 IP 주소를 선택합니다.

스마트 호스트

이 확인란을 선택하면, 시스템의 스마트호스트를 사용하여 o 대신에 사용자 정의 스마트호스트를 구성할 수 있습니다. 인증을 위한 옵션을 포함하여 나타나는 옵션은 아래의 스마트호스트 구성에 있는 것과 동일합니다.

도메인 라우팅의 규칙 우선 순위

도메인 라우팅에 대해 두 개의 규칙을 설정했다고 가정해봅시다. 하나는 mydomain.com 도메인을 보낸 사람, 업링크 *main* 경로로, 다른 하나는 도메인 example.org를 받는 사람으로, 업링크 *Secondary* 경로로 설정했다고 합시다. bar.example.org의 사용자에게 foo.mydomain.com 서버에서 보낸 전자 메일은 어떻게 됐을까요? 대답은 Endian UTM Appliance의 MTA인 postfix가 전자 메일의 보내는 규칙을 처리하는 방법에서 찾을 수 있습니다. 먼저 *소스(Source)*와 관련된 모든 규칙을 읽은 다음, *받는 사람*과 관련된 규칙을 읽습니다. 따라서 foo.mydomain.com에서 bar.example.org로 보낸 전자 메일은 *보조(Secondary)* 업링크를 통해 라우팅됩니다.

메일 라우팅

이 옵션은 지정된 전자 메일 주소로 전자 메일의 숨은 참조(BCC)를 보낼 수 있게 해주며, 특정 받는 사람에게 또는 특정 보낸 사람 주소에서 보낸 모든 전자 메일에 적용됩니다. 목록에는 방향, 주소 및 숨은 참조 주소 (있는 경우에)와 사용 가능한 작업이 표시됩니다.

-  - 메일 라우팅을 수정합니다.
-  - 메일 라우팅을 제거합니다.

새 메일 경로를 추가하려면, 메일 경로 추가 버튼을 클릭하십시오. 열린 양식에서 다음 옵션을 구성할 수 있습니다.

방향

> 전자 메일의 보낸 사람 또는 받는 사람에 대해 메일 경로를 정의할지 여부를 드롭 다운 메뉴에서 선택합니다.

메일 주소

> 선택한 방향에 따라, 이것은 경로가 적용되어야 하는 수신자 또는 발신자의 전자 메일 주소가 됩니다.

숨은 참조 주소

> 여기에 있는 것은 전자 메일의 복사본을 받는 전자 메일 주소입니다.

> **경고:** 발신자와 수신자 모두 제3자에게 사본이 전송되었다는 통지를 받지 않습니다. 대부분의 국가에서 다른 사람들의 비공개 메시지를 읽는 것은 매우 불법입니다. 따라서 이 기능을 오용하거나 남용하지 마십시오.

고급

이 SMTP 프록시 구성 페이지에는 4개의 패널로 그룹화된 고급 설정 옵션들이 있습니다. 이 옵션은 패널 제목 왼쪽의 확장(⊞) 또는 축소(⊟) 아이콘을 클릭하여 표시하거나 숨길 수 있습니다.

스마트 호스트 구성

첫 번째 패널에서 스마트호스트를 활성화하고 구성할 수 있습니다. SMTP 서버에 동적 IP 주소가 있는 경우라면, 예를 들어, ISDN 또는 ADSL 전화 접속 인터넷 연결을 사용하는 경우처럼, 다른 IP 주소가 일부 RBL에 블랙리스트에 있었을 수 있으므로 다른 메일 서버로 전자 메일을 보내는데 문제가 있을 수 있습니다. (위에 있는 블랙리스트와 화이트리스트 참조) 따라서 원격 메일 서버가 전자 메일을 거부할 수

있습니다. 따라서 전자 메일을 보내기 위해 스마트호스트를 사용해야 합니다.

전송용 스마트 호스트

전자 메일 전송 및 추가 옵션 표시를 위해 스마트 호스트를 활성화하려면, 이 확인란을 선택하십시오.

스마타 호스트 주소

스마트 호스트의 IP 주소 또는 호스트 이름.

스마트호스트 포트

스마트 호스트가 듣는 포트는 기본값이 25입니다.

스마트 호스트 인증

스마트 하우스에 인증이 필요한 경우, 이 체크 박스를 선택합니다. 다음 세 가지 추가 옵션이 표시됩니다.

스마트 호스트 사용자 이름

스마트 호스트에서 인증에 사용되는 사용자 이름입니다.

스마트 호스트 암호

스마트 호스트에서 인증에 사용되는 암호입니다.

인증 방법 선택

스마트 호스트가 요구하는 인증 방법은 **PLAIN, LOGIN, CRAM-MD5** 및 **DIGEST-MD5**입니다. 다중 선택 드롭 다운 메뉴에서 확인란을 선택하여 여러 가지 방법을 선택할 수 있습니다.

SMTP 인증을위한 IMAP 서버

이 패널에는 전자 메일을 보낼 때, 인증에 사용해야 하는 IMAP 서버 구성 옵션이 있습니다. 이 설정은 RED 영역에서 열리는 SMTP 수신 연결에 특히 중요합니다. 다음 설정을 구성할 수 있습니다.

SMTP 인증

IMAP 인증을 사용하고 추가 옵션을 표시하려면이 확인란을 선택하십시오.

인증 데몬 수 선택

Endian UTM Appliance를 통해 가능한 동시 로그인 수입니다.

IMAP 인증 서버

IMAP 서버의 IP 주소입니다.

IMAP 인증 포트

IMAP 서버가 수신하는 포트는 일반 IMAP의 경우, 143, SSL을 통한 IMAP의 경우 993을 기본값으로 사용합니다.

메일 서버 설정

이 패널에서 SMTP 서버의 추가 매개 변수를 정의할 수 있습니다.

SMTP HELO 필요

이 확인란을 선택하면, 연결하는 클라이언트가 SMTP 세션이 시작될 때, HELO (또는 EHLO) 명령을 보내야 합니다.

잘못된 호스트 이름 거부

클라이언트 HELO 또는 EHLO 매개 변수가 잘못된 호스트 이름을 제공하면, 연결 클라이언트를 거부합니다.

SMTP HELO 이름

SMTP EHLO 또는 HELO 명령과 함께 전송할 호스트 이름입니다. 사용되는 기본값은 REDIP이지만 FQDN 형식의 사용자 정의 호스트 이름을 제공할 수 있습니다.

> **힌트:** 도메인의 MX 호스트 이름을 사용하십시오.

주소에 항상 숨은 참조

여기에 SMTP 프록시를 통과하는 각 메시지의 숨은 참조를 받는 전자 메일 주소입니다.

메일 템플릿 언어

영어, 독일어, 이탈리아어 및 **일본어** 중에서 오류 메시지를 보낼 언어입니다.

수취인 주소 확인

메시지를 보내기 전에 유효한 수신자 주소를 확인하십시오.

하드 오류 제한

원격 SMTP 클라이언트가 메일을 배달하지 않고 생성할 수 있는 최대 오류 수입니다. 이 제한을

초과하면 SMTP 프록시 서버의 연결이 끊어집니다 (기본값 20).

최대 이메일 콘텐츠 크기

단일 전자 메일 메시지에 허용되는 최대 크기입니다. 드롭 다운 메뉴에서 미리 정의된 몇 가지 값을 선택할 수 있습니다. **사용자 지정** 값을 선택하면 다음 옵션이 나타납니다.

맞춤 최대 이메일 콘텐츠 (KB)

SMTP 서버에서 허용할 전자 메일의 최대 크기 (메가 바이트)입니다.

영역에서 DSN 사용

사용 가능한 영역에서 바운스 메시지 (즉, DSN 메시지)를 배달할 수 없는 전자 메일이나 올바르게 보낼 수 없는 전자 메일로 보낼지 선택합니다. 즉, 여기에서 선택한 영역에서만 전자 메일의 배달 알림 메시지를 받을 수 있습니다.

HELO / EHLO 및 호스트 이름

거의 모든 메일 서버는 SMTP를 통해 연결하는 클라이언트가 HELO/EHLO와 함께 *유효한 호스트 이름*으로 자신을 알리거나 연결을 끊을 것을 요구합니다. 그러나 Endian UTM Appliance는 외부 전자 메일 서버에 알리기 위해 자체 호스트 이름을 사용합니다. 외부 전자 메일 서버는 글로벌 DNS에서 공개적으로 유효하지 않은 경우가 있습니다.

이 경우에, 원격 메일 서버가 이해할 수 있는 *Menubar ‣ Proxy ‣ SMTP ‣ Advanced ‣ Mail server settings ‣ SMTP Helo Name*에서 FQDN (전체 주소 도메인 이름) 형식의 다른 사용자 정의 호스트 이름을 구성할 수 있습니다.

스팸 방지

마지막으로 이 마지막 패널에서 네 개의 확인란 중 하나 이상을 선택하여, 스팸 필터에 대한 추가 매개 변수를 정의할 수 있습니다.

잘못된 받는 사람 거부 (FQDN 아님)

RFC 821에서 요구하는 것처럼 RCPT TO 주소가 FQDN 형식이 아닌 경우 요청을 거부합니다.

잘못된 발신자 거부 (FQDN 아님)

HELO 또는 EHLO 명령과 함께 제공된 호스트 이름이 RFC 821에서 요구하는 FQDN이 아닌 경우 연결 클라이언트를 거부합니다.

알 수 없는 받는 사람 도메인 거부

받는 사람 전자 메일 주소의 도메인에 DNS A 또는 MX 레코드가 없는 경우, 연결을 거부합니다.

알 수 없는 도메인에서 발신자 거부

보낸 사람 전자 메일 주소의 도메인에 DNS A 또는 MX 레코드가 없는 경우, 연결을 거부합니다.

STMP 프록시 문제 해결.

로그 파일에 **"Mail for xxx loops back to myself (xxx의 메일이 자기 자신에게 되돌아 갑니다)"** 라는메시지가 나타나면 어플라이언스의 사용자 정의 SMTP HELO 이름이 잘못 설정되었음을 나타냅니다. 이것은 들어오는 전자 메일이 전달되어야 하는 내부 메일 서버의 호스트 이름과 동일합니다

이 경우 내부 메일 서버에서 수신한 SMTP 연결에는 내부 메일 서버의 호스트 이름과 동일한 호스트 이름 (SMTP 프록시 설정의 HELO 행에 있는 호스트 이름)이 포함되므로, 내부 메일 서버는 오류 메시지를 생성하는 동일한 전자 메일을 보내고 받는 것으로 간주합니다.

가능한 솔루션은 다음과 같습니다.

- 내부 메일 서버의 호스트 이름을 변경합니다.
- DNS 영역 내에 Endian UTM Appliance를 가리키는 새로운 공개적이고 유효한 A 레코드를 만들고, 이 호스트 이름을 SMTP 프록시 내의 HELO 행으로 사용합니다.

추가 참조사항: 기본 전자 메일 프록시를 설정하는 단계별 지침서는 여기에서 찾을 수 있습니다.

안티 스팸

이 페이지에는 스팸 방지 엔진의 구성 설정이 포함되어 있습니다. 다음 옵션을 구성할 수 있습니다.

spamassassin 단락 사용

Cyren (이전 회사명 Commtouch)이 메시지를 스팸으로 표시할 때마다 이 상자를 선택하여 spamassassin을 건너뛸 수 있습니다.

IP/네트워크 무시

여기서 Cyren에 의해 점검되어서는 안되는 IP와 네트워크를 정의할 수 있습니다.

스팸 태그 레벨 패널에서 다음 옵션을 구성할 수 있습니다. 각 옵션의 유효한 값은 **-10과 -1** 사이의 유효한 값을 갖는 *NONSPAM* 옵션을 제외하고, **1과 10** 사이입니다.

확인됨(Confirmed)

이 값을 초과하는 태그 레벨을 가진 모든 전자 메일은 스팸으로 인식됩니다.

대량(Bulk)

이 값을 초과하는 태그 레벨을 가진 모든 전자 메일은 대량 메일로 식별됩니다.

의심스러운(Suspected)

이 값을 초과하는 태그 레벨의 모든 전자 메일에는 스팸이 포함될 것으로 예상됩니다.

알 수 없는(Unknown)

이 값 아래의 태그 레벨을 가진 전자 메일은 알 수 없음으로 분류됩니다.

NONSPAM

이 값 아래의 태그 레벨을 가진 전자 메일은 스팸이 아닌 메일로 인식됩니다.

DNS

이 페이지에서는 다음과 같은 내용을 찾을 수 있습니다.

DNS 프록시는 IP 주소나 호스트 이름을 확인할 필요가 있을 때마다, 원격 DNS 서버에 연결할 필요없이 DNS 쿼리를 가로채서 응답하는 프록시 서버입니다. 동일한 쿼리가 반복되는 경우, 로컬에서 결과를 캐싱하면 성능이 현저하게 향상될 수 있습니다. DNS 프록시에 사용할 수 있는 설정은 세 개의 탭으로 그룹화됩니다.

DNS 프록시

이 페이지에서는 DNS 프록시에 대한 몇 가지 옵션을 구성할 수 있습니다.

Green에 투명, Blue에 투명, Orange에 투명

> GREEN, BLUE 및 ORANGE 영역에서 DNS 프록시를 투명하게 활성화합니다. 해당 영역이 활성화된 경우에만 나타납니다.

특정 소스 및 대상은 두 텍스트 영역에서 값을 채워서 프록시를 우회하도록 설정할 수 있습니다.

SUBNET/IP/MAC로부터 우회

> 해당 텍스트 영역에 작성된 소스가 DNS 프록시의 영향을 받지 않도록 하십시오. 소스는 IP 주소, 네트워크 또는 MAC 주소로 지정할 수 있습니다.

SUBNET/IP로 우회

> 해당 텍스트 영역 아래에 작성된 대상이 DNS 프록시의 영향을 받지 않도록 허용하십시오. 대상은 IP 주소 또는 네트워크로 지정할 수 있습니다.

DNS 라우팅

이 페이지에서는 주어진 도메인에 대한 사용자 정의 이름 서버를 정의할 수 있습니다. 즉, 해당 도메인에 대한 모든 DNS 쿼리는 해당 이름 서버로 리디렉션되어 올바른 해결 방법을 검색합니다.

새 도메인 이름 서버 조합은 도메인의 새 사용자 정의 이름 서버 추가 링크를 클릭하여 추가할 수 있습니다. 항목을 추가할 때, 다음 옵션을 사용할 수 있습니다.

도메인

커스텀 네임 서버를 사용할 도메인.

DNS 서버

사용할 네임 서버의 IP 주소.

설명

추가 코멘트.

목록의 각 도메인에서 다음 작업을 수행할 수 있습니다.

-  - 규칙을 편집합니다.
-  - 규칙을 삭제하십시오.

안티 스파이웨어

이 페이지는 스파이웨어를 전파하는데 사용되거나 피싱 사이트로 사용되는 것으로 알려진 도메인 이름을 확인하라는 요청을 받았을 때, Endian UTM Appliance의 반응에 대한 구성 옵션을 제공합니다. 이 서비스는 phishtank에서 유지 관리하는 악성 도메인 목록을 기반으로 하며, Endian UTM Appliance의 클라이언트가 이 도메인 중 하나에 액세스하려고 하면, 존재하지 않는 도메인으로 리디렉션 될 것입니다. 서비스를 활성화하려면, 회색 스위치 ()를 클릭하십시오. 다음 옵션이 나타납니다.

화이트리스트 도메인

아래 텍스트 영역에 입력된 도메인 이름은 목록의 내용에 관계없이, 스파이웨어 대상으로 처리되지 않으므로 올바른 IP 주소로 확인됩니다.

> **참고:** 사이트가 phishtank에 의해 잘못 차단된 경우, 여기에 도메인 이름을 입력하여 액세스를 허용하십시오.

블랙리스트 도메인

아래 텍스트 영역에 입력된 도메인 이름은 목록의 내용에 관계없이 항상 스파이웨어 대상으로 처리됩니다.

스파이웨어 도메인 목록 업데이트 일정

스파이웨어 도메인 목록의 업데이트 빈도를 말하며, 가능한 선택 항목은 **매일, 매주** 및 **매월**입니다.

> **참고:** 업데이트된 서명을 다운로드하려면, 시스템이 Endian Network에 등록되어 있어야 합니다.

The VPN Menu

- OpenVPN server
  - Server configuration
  - VPN client download
- OpenVPN client (Gw2Gw)
  - Add tunnel configuration
  - Advanced tunnel configuration
  - Import profile from OpenVPN Access Server
- IPsec
  - IPsec
  - L2TP
- Portal
  - Configuration
  - Paths
- Authentication
  - Users
  - Groups
  - Settings
- Certificates
  - Certificates
  - Certificate Authority
  - Revoked Certificates
  - Certificate Revocation List

VPN을 사용하면, 두 개의 분리된 로컬 네트워크가 인터넷과 같은 잠재적으로 안전하지 않은 네트워크를 통해 서로 직접 연결할 수 있습니다. VPN 연결을 통한 모든 네트워크 트래픽은 암호화된 터널 내에서 안전하게 전송되며, 사람들의 호기심 어린 눈을 피해 숨겨지게 됩니다. 이러한 구성을 *Gateway-to-Gateway VPN* 또는 간단히 *Gw2Gw VPN*이라고도 합니다. 마찬가지로 인터넷상의 단일 원격 컴퓨터는 VPN 터널을 사용하여 로컬의 신뢰할 수 있는 LAN에 연결할 수 있습니다. 간혹 *Road Warrior*라고도 불리는 원격 컴퓨터는 VPN 터널이 활성화되어 있는 동안 신뢰할 수 있는 LAN에 직접 연결되어 있는 것으로 나타납니다.

Endian UTM Appliance는 대부분의 운영 체제 및 네트워크 장비에서 지원되는 *IPsec* 프로토콜 또는 *OpenVPN* 서비스를 기반으로 VPN을 만들 수 있도록 지원합니다.

Microsoft Windows, Linux 및 MacOS X 용 사용자 친화적인 OpenVPN 클라이언트는 Endian Network에서 다운로드 할 수 있습니다.

Endian UTM Appliance는 OpenVPN으로 연결된 기기의 네트워크를 생성하기 위해 OpenVPN 서버 또는 클라이언트로 설정될 수 있으며, 동시에 두 가지 역할을 모두 수행할 수도 있습니다. 하위 메뉴에서 사용할 수 있는 메뉴 항목은 다음과 같습니다.

- OpenVPN 서버 - OpenVPN 서버를 설정하여 클라이언트 (게이트웨이 대 게이트웨이 설정에서 *roadwarriors* 및 다른 Endian UTM Appliances 모두)가 로컬 영역 중 하나에 연결할 수 있도록 합니다.
- OpenVPN 클라이언트 (Gw2Gw) - 둘 이상의 Endian UTM 어플라이언스간에 게이트웨이 대 게이트웨이 설정의 클라이언트 측 설정

- IPsec - IPsec 기반 VPN 터널 및 L2TP 연결 설정
- 인증 - VPN 연결 사용자를 관리합니다.
- 인증서는 VPN 연결과 함께 사용되는 인증서를 관리합니다.

OpenVPN 서버

이 페이지에서는 다음과 같은 내용을 살펴봅니다.

OpenVPN 서버로 구성되면, Endian UTM Appliance는 업링크로부터의 원격 연결을 허용할 수 있으며, 로컬 워크 스테이션 또는 서버인 것처럼, VPN 클라이언트를 설정하여 로컬 리소스와 상호 작용할 수 있게 해줍니다.

Endian UTM Appliance의 OpenVPN 서버에는 여러 서버 인스턴스가 동시에 존재할 수 있습니다. 각 인스턴스는 다른 포트에서 수신 대기하고, 해당 포트에 대한 수신 연결 만 수락합니다.

또한 Endian UTM Appliance가 설치된 하드웨어에 여러 개의 CPU 코어가 있는 경우에는 모든 인스턴스에 하나 이상의 코어가 할당될 수 있으므로, 해당 인스턴스의 처리량과 데이터 처리가 증가합니다. 그럼에도 불구하고, 단일 코어 CPU가 장착된 장치에서 OpenVPN의 다중 인스턴스를 실행하는 것이 가능하지만, CPU가 모든 인스턴스의 부하를 전달하기 때문에 성능이 저하될 수 있습니다.

OpenVPN 서버 설정 페이지는 *서버 구성*과 *VPN 클라이언트 다운로드*의 두 가지 탭으로 구성됩니다.

서버 구성

이 페이지에는 *OpenVPN 서버 활성화*  라 불리는 스위치와 그것을 클릭함으로써 OpenVPN 서버와 관련된 모든 서비스 (예: 활성화된 경우, VPN 방화벽과 같은)를 시작할 스위치가 표시됩니다.

아래에는 *OpenVPN 설정(settings)*이라는 두 개의 상자가 있습니다. 이 상자는 Endian UTM Appliance에 정의된 OpenVPN 서버 인스턴스의 목록을 포함하는 모든 인스턴스와 *OpenVPN 인스턴스*가 공유하는 일부 전역 설정을 설정할 수 있습니다

바로 아래에 새 OpenVPN 서버 인스턴스 추가 링크를 사용하여 새로운 서버 인스턴스를 정의할 수 있습니다.

> **참고:** OpenVPN 서버를 처음 시작하면. 루트 및 호스트 인증서가 자동으로 생성됩니다.

OpenVPN 설정

상단의 상자는 인증 방법과 관련된 현재 OpenVPN 설정을 보여줍니다.

인증 유형(Authentication type)

클라이언트를 Endian UTM Appliance에서 실행되는 OpenVPN 서버에 연결하는데 사용할 수 있는 인증 방법에는 세 가지가 있습니다.

- *PSK (사용자 이름 및 암호).* 올바른 사용자 이름과 암호를 제공한 후 연결이 설정됩니다.
- *X.509 인증서.* 연결에 유효한 인증서 만 필요합니다.
- *X.509 인증서 및 PSK (두 가지 요소).* 유효한 인증서와 사용자 이름/암호 조합이 모두 필요합니다.

> **경고:** 인증서만(certificate-only) 이용한 인증을 사용하면, 유효한 인증서가 있는 클라이언트에게 유효한 계정이 없는 경우일지라도 OpenVPN 서버에 대한 액세스가 허용됩니다.

엔디안 UTM 어플라이언스의 기본 방법은 **PSK (사용자 이름/암호)**입니다. 클라이언트는 사용자 이름과 암호를 사용하여 인증합니다. 이 방법을 사용하려면, 추가로 변경할 필요가 없으며, 다른 두 가지 방법은 아래에 설명되어 있습니다.

인증서 구성(Certificate configuration)

이 드롭 다운 메뉴는 새 인증서 생성 방법을 선택하는 데 사용됩니다. 사용 가능한 옵션은 다음과 같습니다.

- *새 인증서를 생성하십시오.* 처음부터 새 인증서를 만듭니다. 이 옵션은 이미 호스트 인증서가 생성되지 않은 경우에만 사용할 수 있습니다. 새 인증서를 만드는데 필요한 모든 옵션을 지정하는 양식이 열립니다. 이것은 새 인증서 생성 편집기에서 찾을 수 있는 두 가지 사소한 변경 사항과 동일합니다. 그 두개의 변경사항들은 즉, *공통 이름*은 *시스템 호스트 이름*이 되고 *조직 단위 이름*은 *부서 이름*이 되는 것입니다.
- *선택한 인증서를 사용하십시오.* 드롭 다운 메뉴의 오른쪽에 표시된 사용 가능한 인증서 중 하나를 선택하십시오. 세부 정보보기 하이퍼링크를 클릭하여, 이 인증서의 전체 세부 사항을 볼 수 있습니다.

  > **힌트:** 선택된 인증서의 이름은 하이퍼링크 바로 위에 나타납니다.

- *기존 인증서를 사용하십시오.* 왼쪽에 있는 두 번째 드롭 다운 메뉴는 Endian UTM Appliance에 이미 생성되어 저장된 인증서를 선택할 수 있게 합니다.
- *인증서를 업로드하십시오.* 드롭 다운 메뉴 아래에 나타나는 찾아보기... 단추를 클릭하면, 워

크스테이션에서 기존 인증서를 선택하고 업로드 할 수 있습니다. 필요한 경우, 인증서의 비밀번호는 오른쪽 텍스트 필드에 제공될 수 있습니다.

- *인증서 서명 요청을 업로드하십시오.* 드롭 다운 메뉴 아래에 나타나는 찾아보기... 단추를 클릭하면, 워크스테이션에서 기존 인증서 서명 요청을 선택하고 업로드 할 수 있습니다. 날짜들의 인증서의 유효 기간은 오른쪽 텍스트 필드에 제공될 수 있습니다.

인증서 구성 드롭 다운 메뉴의 오른쪽에는 현재 사용되는 인증서의 이름이 정보 (ℹ) 아이콘과 세부 정보 보기 링크 위에 표시됩니다. 후자는 클릭할 때, 인증서에 대한 모든 정보를 보여줍니다.

인증서 구성 드롭 다운 메뉴 아래에는 다운로드 (⬇) 아이콘이 있습니다. 여기에는 클라이언트 연결에 필요한 인증서를 다운로드 할 수 있는 인증 기관 이름 및 인증서 다운로드 링크가 있습니다.

*고급 옵션 패널*에서 몇 가지 옵션을 사용하여 OpenVPN 서버를 사용자 정의할 수 있습니다.

지연 트리거(Delay triggers)

확인란을 선택하면 클라이언트가 OpenVPN 서버에 연결하거나 OpenVPN 서버와의 연결을 끊을 때마다 실행되는 트리거를 지연시킬 수 있습니다. 트리거는 대부분 라우팅 및 방화벽 규칙을 다시로드하기 때문에, 이 옵션은 많은 클라이언트가 동시에 연결하거나 연결을 끊을 때 유용합니다.

로그의 자세한 정보 표시(Log verbosity)

이 옵션은 로그 파일에 기록된 메시지의 양을 늘리거나 줄일 수 있게 해줍니다. 기본값은 **1**이며, 가장 관련있는 메시지 만 로그 파일에 기록되며, 최대 5개까지 증가할 수 있습니다.

> **힌트:** 디버깅을 위한 적당한 값은 **4**입니다.

연결된 각 클라이언트에 대한 DNS 항목 만들기(Create a DNS entry for each connected client)

이 옵션을 선택하면, 클라이언트가 연결할 때마다 로컬 DNS 서버에 항목이 수신되어 다른 클라이언트가 쉽게 연결할 수 있게 해줍니다. 다음 옵션이 나타납니다.

클라이언트 DNS 항목 접두사(*Clients DNS entry prefix)*

로컬 DNS를 사용할 때, 고유하게 식별할 수 있도록 클라이언트의 사용자 이름에 접두사로 붙일 사용자 정의 접두사입니다.

> **힌트:** 여기에 작성된 접두사가 **vpn**이면, 항목은 **vpn-johndoe**와 같이 **vpn**-username이 됩니다.

OpenVPN 서버 인스턴스

이미 정의된 OpenVPN 인스턴스 목록이 이 패널에 표시됩니다. 이 패널 위에는 새 OpenVPN 서버 인스턴스 추가 하이퍼링크가 있습니다. 이 링크를 클릭하면, toq가 새 VPN 인스턴스에 필요한 모든 구성 값을 제공하는 편집기가 열립니다.

> **참고:** 코어보다 OpenVPN 인스턴스의 수가 큰 경우에는, 노란색 지시선이 성능이 저하될 수 있음을 알립니다.

편집기에는 다음과 같은 구성 옵션이 표시됩니다.

이름(Name)

OpenVPN 서버 인스턴스에 주어진 이름입니다.

설명(Remark)

이 인스턴스에 대한 설명입니다.

~에만 바인딩(Bind only to)

인스턴스가 청취해야 하는 IP 주소입니다.

포트(Port)

인스턴스가 들어오는 연결을 대기하는 포트입니다.

기기 종류(Device type)

드롭 다운 메뉴에서 TUN과 TAP 사이에서 선택한 인스턴스에서 사용하는 장치입니다. TUN 장치는 라우팅 될 트래픽이 필요하므로, 아래의 *Bridged* 옵션은 TUN 장치에서 사용할 수 없습니다.

프로토콜(Protocol)

사용된 프로토콜이며, 드롭 다운 메뉴에서 TCP와 UDP 사이에서 선택됩니다.

브릿지된(Bridged)

브릿지 모드에서 OpenVPN 서버를 (즉, 기존 구역 중 하나) 실행하려면, 이 옵션을 선택합니다.

> **참고:** OpenVPN 서버가 브리징되지 않은 경우 (즉, 라우팅 된 경우), 클라이언트는 전용 서브넷에서 IP 주소를 수신합니다. 이 경우, 클라이언트가 모든 영역이나 일부 서버/리소스 (예: 소스 코드 저장소)에 액세스할 수 있도록 VPN 방화벽에서 적절한 방화벽 규칙을 만들어야 합니다. OpenVPN 서버가 브리지 된 경우, 정의된 영역의 방화벽 설정을 상속받습니다.

VPN 서브넷

이 옵션은 브리지 모드가 비활성화 된 경우에만 사용할 수 있습니다. OpenVPN 서버는 자체 전용 서브넷에서 실행될 수 있으며, 텍스트 상자에 지정할 수 있으며 다른 영역의 서브넷과 달라야합니다.

브릿지

OpenVPN 서버가 연결된 영역입니다. 드롭 다운 메뉴에는 사용 가능한 영역만 표시됩니다.

동적 IP 풀 시작 주소

OpenVPN 클라이언트에 사용해야 하는 선택한 영역의 네트워크에서 가능한 첫 번째 IP 주소입니다.

동적 IP 풀 최종 주소

OpenVPN 클라이언트에 사용해야 하는 선택한 영역의 네트워크에서 가능한 마지막 IP 주소입니다.

라우팅 및 브리지 OpenVPN 서버, 정적 및 동적 IP 주소.

OpenVPN을 통해 연결하는 클라이언트를 위해 예약된 IP 주소의 풀을 구성할 때, 향후 오작동을 예방하고 보다 간편하고 쉽게 설계 및 설정하는데 도움이 되는 몇 가지 지침을 명심해야 할 필요가 있습니다.

서버 구성을 시작하기 전에, VPN 멀티 코어 아키텍처의 구현과 관련하여 기억해야 할 황금률이 있습니다. 멀티 코어 VPN 서버 인스턴스에 사용되는 브리지 모드 또는 라우팅 모드에 관계없이, 고정 IP 주소의 예약은 무시됩니다. 즉, 이 VPN 서버에 연결하는 클라이언트는 그것의 구성에 고정 IP 할당이 있을지라도 동적 IP 주소를 받게 될 것입니다.

첫 번째 선택은 OpenVPN 서버가 라우트되거나 브리지 모드로 작동해야 하는지 여부를 정의하는 것입니다. 전자의 경우, 클라이언트에 IP 주소를 제공할 적절한 *VPN 서브넷*을 정의해야 합니다. 필요한 경우, VPN 방화벽을 사용하여, 이 서브넷으로 향하는 트래픽을 필터링해야 합니다. 후자의 경우, OpenVPN 서버는 연결시 클라이언트가 해당 구역에 물리적으로 연결되어 있는 것처럼 클라이언트를 고려하도록 구성됩니다. 즉, 서버는 클라이언트를 구역 중 하나에 브리징합니다. 이 경우에, 이 상자 바로 앞에 나타나는 두 가지 옵션을 사용하여 해당 구역 내에서 IP 주소 풀을 정의해야 합니다. 이 풀은 구역의 서브넷에 완전히 포함되어야 하며, 그것보다 작아야 합니다. 이 풀이 해당 구역에 정의된 다른 풀 (예: DHCP 서버)과 충돌하는지 확인하는 것도 중요합니다.

브릿지된 OpenVPN 서버에서는 일부 (또는 전체) 사용자에게 고정 IP 주소를 할당할 수 있습니다. 이 가능성을 계획할 때, 이러한 고정 IP 주소는 주소 충돌과 잘못된 라우팅을 방지하기 위해 해당 구역에 정의된 IP 풀 중 하나에 속하지 않는 것이 좋습니다. 이 특정 클라이언트에 대한 트래픽은 VPN (또는 IPsec) 사용자를 방화벽 규칙의 트래픽 소스 또는 대상으로 사용하여 필터링 할 수 있습니다.

인증서 구성

이 옵션을 사용하면 전역 옵션에 정의된 기본 인증서와 다른 인스턴스를 위한 인증서를 선택할 수 있습니다. 이 옵션의 선택은 OpenVPN 구성의 전역 섹션에서와 동일합니다.

고급 옵션 상자에서 추가 옵션을 구성할 수 있습니다.

코어 수

드롭 다운 메뉴는 인스턴스에 의해 사용될 수 있는 Endian UTM Appliance의 CPU 수를 선택할 수 있게해주므로, 드롭 다운 메뉴의 옵션이 달라질 수 있습니다.

하나의 계정에서 여러 개의 연결 허용 :

일반적으로 하나의 클라이언트는 한 번에 하나의 위치에서 연결이 허용됩니다. 이 옵션을 선택하면 다른 위치에서 조차도 여러 개의 클라이언트 로그인이 허용됩니다. 그러나 동일한 클라이언트가 두 번 이상 연결되면, VPN 방화벽 규칙이 더 이상 적용되지 않습니다.

터널로부터 들어오는 DHCP 응답 차단

로컬 DHCP 서버와 충돌하는 VPN 터널의 반대편에 있는 LAN에서 DHCP 응답을 수신할 때에는 이 확인란을 선택하십시오.

클라이언트 대 클라이언트 연결

드롭 다운 메뉴에서 OpenVPN 서버의 클라이언트들 사이의 통신 방식을 선택하십시오. 이 옵션은 단일 프로세스 서버, 즉 OpenVPN 서버 인스턴스가 하나만 실행되고 있는 서버에서만 사용할 수 있습니다.

- **허용되지 않음:** 클라이언트는 상대방과 통신할 수 없습니다.
- **직접 연결 허용:** 클라이언트는 서로 직접 통신할 수 있지만, 필터링은 불가능합니다.
- **VPN 방화벽의 필터 연결:** 클라이언트는 서로 통신할 수 있지만, 해당 트래픽은 VPN 방화벽으로 리디렉션되며, 적합한 해당 규칙을 사용하여 필터링 할 수 있습니다.

> **참고:** 멀티 코어 CPU가 있는 어플라이언스의 경우, 선택이 불가능하며, *VPN 방화벽*의 *필터 연결*이 자동으로 활성화됩니다.

재협상 데이터 채널 키 간격

이 옵션은 데이터 채널 키가 재협상 된 후에 시간 간격을 수정할 수 있게 해줍니다. 값은 초 단위로 측정되며, 기본값은 **3600 초**입니다.

이 네임서버들을 푸시

이 체크 박스를 선택하면, 아래의 텍스트 필드에 지정된 네임 서버가 연결시 클라이언트에 전송됩니다.

네임 서버들

이 텍스트 필드에 지정된 네임서버들은 이전 확인란이 선택되었을 때, 연결된 클라이언트로 전송됩니다.

이 네트워크들을 푸시

이 확인란을 선택하면, 아래의 텍스트 필드에 정의된 네트워크에 대한 경로가 연결된 클라이언트로 전송됩니다.

네트워크

이 텍스트 필드에 지정된 네트워크는 이전 확인란이 선택되었을 때, 연결된 클라이언트로 전송됩니다.

이 도메인을 푸시

이 확인란을 선택하면, 오른쪽 텍스트 필드에 정의된 검색 도메인이 연결된 클라이언트의 검색 도메인에 추가됩니다.

> **참고:** *이 네임서버를 푸시* 및 *도메인 푸시* 옵션은 Microsoft Windows 운영 체제를 실행하는 클라이언트에서만 작동합니다.

도메인

VPN 네트워크 (즉 검색 도메인)에서 서버 및 네트워크 리소스를 식별하는데 사용할 도메인입니다.

인증 유형

OpenVPN의 해당 인스턴스에 대한 인증 유형입니다. 기본적으로 글로벌 구성을 상속합니다. 그러나 이 옵션은 여기에서 사용 가능한 옵션 중 하나를 수동으로 지정하여 무시할 수 있습니다. 그

것들은 *PSK (사용자 이름/암호), X.509 인증서* 및 *X.509 인증서* 및 *PSK (두 가지 요소)*입니다. 그것들은 전역 옵션과 동일합니다.

암호(Cipher)

이 드롭 다운 메뉴는 OpenVPN 서버에서 사용되는 암호를 선택할 수 있게 해줍니다. 기본값은 **Auto** (자동)입니다. 이는 암호가 자동으로 협상됨을 의미합니다.

메시지 요약 알고리즘

이 드롭 다운 메뉴는 OpenVPN 서버에서 사용되는 메시지 요약 알고리즘을 선택할 수 있게 해줍니다. 기본값은 **Auto** (자동)입니다. 이는 암호가 자동으로 협상됨을 의미합니다.

채널 암호화 사용 안함

이 옵션을 선택하면, 해당 인스턴스를 통과하는 전체 VPN 트래픽이 암호화되지 **않습니다**. 즉, 일반 텍스트로 그대로 전송됩니다. 또한, 이전 두 옵션이 사라집니다.

> **경고:** OpenVPN 서버에서 암호화를 사용하지 않도록 설정하는 것이 좋습니다. 전체 트래픽이 암호화되지 않고, 통신이 가로채는 경우에 읽을 수 있기 때문입니다.

처음 서비스가 시작되면,이 OpenVPN 서버에 대한 자체 서명된 새 CA 인증서가 생성됩니다. 이 인증서는 오랜 시간이 걸릴 수 있습니다. 인증서가 생성되면, CA 인증서 다운로드 링크를 클릭하여, 인증서를 다운로드 할 수 있습니다. 이 인증서는 이 OpenVPN 서버에 연결하려는 모든 클라이언트에서 사용해야 하며, 그렇지 않으면 액세스 할 수 없습니다.

서버가 설정되면, *인증* 탭에서 Endian UTM Appliance에 연결할 수 있는 클라이언트 계정을 생성하고 구성할 수 있습니다.

활성화

이 확인란을 선택하면, OpenVPN 서버가 시작되었는지 확인할 수 있습니다.

VPN 연결 문제 해결.

구성을 보면, VPN 연결에 대한 몇 가지 문제점을 쉽게 발견할 수 있지만, 연결 문제의 한 가지 미묘한 원인은 MTU 크기의 잘못된 값입니다. Endian UTM Appliance는 ISP가 사용하는 일반적인 MTU 값이 1500이나 되는 문제를 방지하기 위해 VPN의 MTU 크기에 1450 바이트 제한을 설정합니다. 그러나 일부 ISP는 일반적으로 사용되는 값보다 낮은 MTU 값을 사용할 수 있습니다. Endian MTU 값이 너무 커서 연결 문제가 발생합니다. (가장 눈에 띄는 것은 대용량 파일을 다운로드 할 수 없을 가능성이 높습니다.) 이 값은 CLI에서 Endian UTM Appliance에 액세스하고 다음 지침에 따라 수정될 수 있습니다.

1. ISP에서 사용하는 MTU 크기를 적어 두십시오 (아래 링크 참조).
2. 쉘 또는 *Menubar ‣ System ‣ Web Console*에서 CLI에 로그인하십시오.
3. 선택된 편집기 **nano /etc/openvpn/openvpn.conf.tmpl**로 OpenVPN 템플릿을 편집하십시오.
4. **mssfix 1450** 문자열을 검색하십시오.
5. 1450을 더 낮은 값 (예: 1200)으로 바꾸십시오.
6. 다음을 호출하여 OpenVPN을 다시 시작하십시오. **jobcontrol restart openvpnjob.**

추가 참고사항: MTU 크기에 대한 더 자세한 정보는 http://docs.endian.com/5.0/utm/system.html#mtusize를 참고하십시오.

VPN 클라이언트 다운로드

Endian Network에서 Microsoft Windows 및 MacOS X 용 Endian VPN 클라이언트를 다운로드하기 위해 링크를 클릭하십시오. Endian Network에 유효한 계정이 필요합니다.

OpenVPN client (Gw2Gw)

이 페이지에서는 다음과 같은 내용을 살펴봅니다.

- 터널 구성 추가
- 고급 터널 구성
- OpenVPN 액세스 서버에서 프로파일 가져오기

이 페이지에는 OpenVPN 클라이언트 (즉, 원격 OpenVPN 서버에 대한 모든 터널링 연결)로서의 Endian UTM Appliance 연결 목록이 표시됩니다. 모든 연결에 대해, 목록은 상태, 이름, 추가 옵션, 설명 및 사용 가능한 작업을 보고합니다.

- ☑☐ - 서버가 활성 또는 중지되었습니다.
-  - 서버 구성을 수정합니다.
-  - 구성과 서버를 제거합니다.

연결이 비활성화되면 상태가 *닫히고 (Closed),* 연결이 활성화되면 *설정되며 (established),* 연결이 설정되는 동안 *연결됩니다 (connecting...).* 연결을 활성화하거나 비활성화하는 것 이외에도, 사용 가능한 작업은 연결을 편집하거나 삭제하는 것입니다. 전자의 경우, 양식이 열리며, 이는 현재 설정을 보고 수정하는 연결을 추가할 때 열리는 양식과 동일합니다 (아래 참조). 반면에, 후자의 경우에는 Endian UTM 어플라이언스에서 해당 프로필 만 삭제하는 것이 허용됩니다.

새로운 OpenVPN 클라이언트 연결을 만드는 것은 직접적이고 간단하며, 두 가지 방법으로 수행할 수 있습니다. `터널 구성 추가` 버튼을 클릭하고, 연결할 OpenVPN 서버에 대한 필요한 정보를 입력하거나 (하나 이상 있을 수 있음) `OpenVPN Access Server에서 프로파일 가져오기`를 클릭하여 OpenVPN 액세스 서버의 클라이언트 설정을 가져옵니다.

터널 구성 추가

각 터널 구성에 대해 구성할 수 있는 두 가지 유형의 설정이 있습니다. 기본 터널 설정에는 터널 설정을 위한 필수 옵션이 포함되지만, 고급 터널 설정은 선택 사항이며, 일반적으로 OpenVPN 서버가 비표준 설정인 경우에만 변경해야 합니다 . 고급 설정에 액세스하려면, 고급 터널 구성 레이블 옆에있는 `>>` 버튼을 클릭하십시오. 기본 설정은 다음과 같습니다.

연결 이름

연결을 식별하는 레이블.

~에 연결 (Connect to)

원격 OpenVPN 서버의 FQDN, 포트 및 프로토콜은 myvpn.example.com:port:protocol 형식입니다. 포트 및 프로토콜은 선택 사항이며, 지정되지 않은 경우 각각 기본값인 *1194* 및 *udp*로 유지됩니다. 프로토콜은 소문자로 지정해야 합니다.

인증서 업로드

터널 연결에 필요한 서버 인증서. 로컬 파일 시스템을 검색하는 것이 허용되면, 파일을 검색하고 경로 및 파일 이름을 입력할 수 있습니다. 서버가 PSK 인증 (암호/사용자 이름)을 사용하도록 구성된 경우에는 서버의 호스트 인증서 (즉, 서버의 *Menubar ‣ VPN ‣ OpenVPN server* 섹션의 `Download CA 인증서` 링크에서 다운로드 한 인증서)를 Endian UTM Appliance에 업로드해야 합니다. 그렇지 않으면, 인증서 기반 인증을 사용하기 위해, 서버의 PKCS #12 파일 (즉, 서버의 *Menubar ‣ VPN ‣ OpenVPN server ‣ Advanced* 섹션에서 `PKCS #12 파일로 CA 내보내기` 링크에서 다운로드한 파일)를 업로드해야 합니다.

PKCS #12 챌린지 암호

인증서 작성 전이나 작성 중에 CA에 제공된 경우에는 여기에 *Challenge 암호*를 입력하십시오. PKCS #12 인증서를 업로드 할 때만 필요합니다.

사용자 이름, 암호

서버가 PSK 인증 (암호/사용자 이름) 또는 인증서와 암호 인증을 사용하도록 구성된 경우에는 여기에 OpenVPN 서버에 있는 계정의 사용자 이름과 암호를 제공하십시오.

설명

연결에 대한 주석.

고급 터널 구성

이 상자에서 이전 상자의 `>>` 단추를 클릭하면, 추가 옵션을 수정할 수 있지만, 서버 쪽이 표준 값으로 구성되지 않은 경우에만, 이 상자의 값을 수정해야 합니다.

대체 VPN 서버

기본 서버에 사용되는 동일한 형식 (예: myvpn.example.com:port:protocol)의 하나 이상의 OpenVPN 서버 (하나의 행에 하나씩)를 대체합니다. 포트 및 프로토콜 값은 생략될 때 각각 1194 및 udp가 기본값입니다. 주 서버에 대한 연결이 실패하면, 이러한 대체 서버 중 하나가 인계받습니다.

> **힌트:** 프로토콜은 소문자로 작성해야합니다.

기기 종류

TAP 또는 TUN인 서버에서 사용하는 장치.

연결 타입

이 드롭 다운 메뉴는 장치 유형으로 TUN을 선택한 경우, 사용할 수 없습니다. 이 경우 연결 유형이 항상 라우팅되기 때문입니다. 사용 가능한 옵션은 라우트 (즉, 클라이언트가 원격 LAN에 대한 게이트웨이 역할을 함) 또는 브리지 (즉, 클라이언트 방화벽이 원격 LAN의 일부로 나타남)됩니다. 기본값이 라우트됩니다.

~에 브릿지(Bridge to)

이 필드는 장치 유형으로 TAP을 선택하고, 연결 유형을 연결한 경우에만 사용할 수 있습니다. 이 드롭 다운 메뉴에서 이 클라이언트 연결을 브리지 할 영역을 선택하십시오.

NAT

이 옵션은 *연결 유형*이 *라우팅* 된 경우에만 사용할 수 있습니다. 방화벽의 VPN IP 주소 뒤에 이 Endian UTM Appliance를 통해 연결된 클라이언트를 숨기려면 이 확인란을 선택합니다. 이 구성은 클라이언트에 들어오는 연결 요청을 방지합니다. 즉, 들어오는 연결은 로컬 네트워크의 클라이언트를 보지 못합니다.

터널에서 오는 DHCP 응답 차단

이 체크 박스를 선택하면, 로컬 DHCP 서버와 충돌하는 VPN 터널의 반대편에 있는 LAN에서 DHCP 응답을 받지 않게 됩니다.

LZO 압축 사용

터널을 통과하는 트래픽을 압축하면 기본적으로 활성화됩니다.

프로토콜

서버가 사용하는 프로토콜: UDP (기본값) 또는 TCP. HTTP 프록시를 사용해야 하는 경우에만 TCP로 설정:이 경우, 그것을 구성하기 위해 폼이 나타납니다.

Endian UTM Appliance가 업스트림 HTTP 프록시를 통해서만 인터넷에 액세스 할 수 있으면, 게이트웨이 대 게이트웨이 설정에서 OpenVPN 클라이언트로 계속 사용할 수 있지만 OpenVPN의 *TCP* 프로토콜을

양쪽에서 선택해야 합니다. 또한 텍스트 필드에 HTTP 업스트림 프록시의 계정 정보를 제공해야 합니다.

HTTP 프록시

HTTP 프록시 호스트 (예: proxy.example.com:port). 포트를 입력하지 않은 경우, 기본값은 8080입니다.

프록시 사용자 이름, 프록시 비밀번호

프록시 계정 정보: 사용자 이름과 암호.

위임 프록시 사용자 에이전트

위조된 사용자 에이전트 문자열은 Endian UTM Appliance를 일반 웹 브라우저 (예: 브라우저로 프록시에 연결)로 가장하는데 사용될 수 있습니다. 프록시가 일부 유형의 브라우저에 대해서만 연결을 허용하는 경우에는 이 작업이 유용할 수 있습니다.

연결이 구성되면, 연결에 사용할 TLS 키 파일을 업로드 할 수 있는 *TLS 인증*이라고 불리우는 페이지 하단에 새로운 상자가 나타납니다. 다음 옵션을 사용할 수 있습니다.

TLS 키 파일

업로드 할 핵심 파일이며, 로컬 워크스테이션에서 검색할 수 있습니다.

MD5

업로드 된 파일의 MD5 체크섬입니다. 파일이 Endian UTM Appliance에 저장되는 즉시 나타납니다.

방향

이 값은 서버에서는 0으로 설정되고 클라이언트에서는 1로 설정됩니다.

OpenVPN 액세스 서버에서 프로파일 가져 오기

두 번째로 계정을 추가할 수 있는 방법은 OpenVPN 액세스 서버에서 프로필을 직접 가져오는 것입니다. 이 경우 다음 정보를 제공해야 합니다.

연결 이름

연결에 대한 사용자 정의 이름.

액세스 서버 URL

OpenVPN 액세스 서버의 URL입니다.

참고: Endian UTM Appliance는 OpenVPN Access Server의 XML-RPC 구성만 지원하므로 여기에 입력되는 URL 형식은 https://<SERVERNAME>/RPC2입니다.

사용자 이름, 암호

액세스 서버의 사용자 이름과 암호.

SSL 인증서 확인

이 확인란을 선택하고, 서버를 SSL 암호화 연결에서 실행하면, SSL 인증서의 유효성이 검사됩니다. 인증서가 유효하지 않으면 연결이 즉시 닫힙니다. 이 기능은 자체 서명된 인증서를 사용할 때, 비활성화 될 수 있습니다.

설명

연결 목적을 상기시키는 설명.

IPsec

이 페이지에서는 다음과 같은 내용을 살펴봅니다.

- IPsec
  - IPsec 설정
  - 디버그 옵션
  - 연결
- L2TP

IPsec 페이지에는 IPSec 터널을 설정 및 구성하고, L2TP 지원을 활성화할 수 있는 두 개의 탭, IPsec 및 L2TP가 있습니다.

IPsec

Endian UTM 어플라이언스에서 IPsec을 활성화하려면, *Enable IPsec* 레이블 옆의 스위치가 녹색  이어야 합니다. 회색  인 경우, 그것을 클릭하여 서비스를 시작하십시오.

IPsec 탭에는 두 개의 상자가 있습니다. 첫 번째는 *IPsec 설정*이며 모든 터널에 대한 다양한 일반 옵션을 디버깅 목적으로 구성할 수 있습니다. 두 번째 것은 정의된 모든 연결을 표시하고 이를 관리할 수 있는 *연결*입니다.

IPsec, L2TP 및 XAuth를 간략하게 설명

IPsec은 범용 표준화된 VPN 솔루션으로 암호화 및 인증 작업이 IP 프로토콜의 확장으로 OSI 레이어 3에서 수행됩니다. 따라서 IPsec은 커널의 IP 스택에 구현되어야 합니다. IPsec은 표준화된 프로토콜이며, IPsec 솔루션을 구현하는 대부분의 공급 업체와 호환되지만, 실제 구현은 공급 업체마다 매우 다를 수 있으며, 때때로 상호 운용성 문제가 발생합니다.
또한 IPsec의 구성과 관리는 복잡성과 디자인으로 인해 어려워질 수 있습니다. 일부 특정 상황에서는 처리가 불가능할 수도 있습니다. 예를 들어, NAT에 대처할 필요가 있는 경우입니다.
IPsec과 비교할 때, OpenVPN은 설치, 구성 및 관리가 더 쉽습니다. 그러나 모바일 장치는 IPsec에 의존하므로, Endian UTM Appliance는 L2TP 또는 XAuth와 함께 사용하면, 서로 다른 인증 방법과 2단계 인증을 지원하는 IPsec용 관리 인터페이스를 쉽게 구현합니다.
실제로, IPsec은 클라이언트 (즉, 터널)를 인증하는데 사용되지만, 사용자는 인증하지 않으므로 한 번에 하나의 클라이언트만 하나의 터널을 사용할 수 있습니다.
L2TP와 XAuth는 IPsec에 사용자 인증을 추가하므로 많은 클라이언트가 동일한 암호화된 터널을 사용하여 서버에 연결할 수 있으며, 각 클라이언트는 L2TP 또는 XAuth에 의해 인증됩니다.
추가 옵션은 XAuth를 사용할 때 사용할 수 있으며 사용자를 인증하는 XAuth 하이브리드 모드라고 합니다.

IPsec 설정

이 상자에는 몇 가지 글로벌 IPsec 옵션, 즉 IPsec 터널에 사용되는 인증서, Dead Peer Detection (죽은 피어 감지) 및 많은 디버깅 옵션을 설정할 수 있습니다.

Roadwariors 가상 IP 풀

모든 roadwarrior 연결이 IP 주소를받는 IP 간격입니다.

핑 지연 (초)

두 개의 연속적인 ping 사이의 초 단위 시간. 연결이 여전히 활성 상태인지 여부를 감지하는데 사용됩니다.

시간 초과 간격 (초) - IKEv1 전용

IKEv1 프로토콜의 교환 간격 최대 시간 (초).

> **힌트:** IKEv2는 다른 끝 점이 응답하지 않을 때, 및 취할 조치를 감지할 수 있기 때문에, 시간 초과 간격을 필요로 하지 않습니다.

인증서 구성

인증서 구성 및 관리는 모든 다양한 관리 방법을 설명하는 OpenVPN 서버 (*Menbar ‣ VPN ‣ OpernVPN server*의 경우)와 동일하게 수행됩니다.

인증서 구성 드롭 다운 메뉴 아래에는 다운로드 아이콘(⬇)이 있습니다. 여기에는 인증 기관 이름 및 인증서 다운로드 링크가 있어서, 클라이언트 연결에 필요한 인증서를 다운로드 할 수 있습니다.

디버그 옵션

디버그 옵션은 오히려 고급 설정이며 일반적으로 필요하지 않습니다. 로그 파일에 기록되는 이벤트 및 메시지의 수가 증가하기 때문입니다.

이러한 모든 옵션의 활성화는 연결 설정 중 문제가 발생하거나, 터널의 정상 작동에 대한보다 정확하고 기술적인 메시지를 생성할 때 유용합니다. 이렇게하면 로그 파일에 매우 상세한 옵션이 포함됩니다.

연결

이 테이블에는 다음 정보와 함께 이미 구성된 IPsec 연결이 모두 표시됩니다.

- 이름. 연결에 지정된 이름입니다.
- 유형. 어떤 종류의 터널이 사용됩니까?
- 공통 이름. 연결을 인증하는 데 사용되는 인증서의 이름입니다.
- 설명. 연결에 대한 설명입니다.

- 상태. 연결이 Closed, Connecting 또는 Established 중 하나인지 여부
- 작업. 각 터널에서 수행할 수 있는 작업은 다음과 같습니다.

    - ☑☐ - 연결이 활성화되어 있는지 여부.
    - 🖉 - 연결 설정 수정합니다.
    - 🗘 - 연결을 재시작합니다.
    - 🛈 - 연결에 대한 자세한 정보를 표시합니다.
    - 🗑 - 연결을 제거하십시오.

> **힌트:** Endian UTM 어플라이언스에서 연결을 재설정하면, 클라이언트가 다시 연결하여 연결을 설정해야 합니다.

새 연결 추가를 클릭하면, 새 IPsec 연결을 설정하는데 필요한 모든 옵션이 포함된 패널이 나타납니다.

이름

연결 이름입니다.

설명

연결에 대한 설명입니다.

연결 타입

IPsec 터널에는 네 가지 연결 모드가 선택될 수 있습니다.

- *Host-to-Net*. 클라이언트가 Endian의 IPsec 서버에 연결 중입니다. UTM 어플라이언스는 단일 원격 워크 스테이션, 서버 또는 리소스입니다.
- *Net-to-Net.* 클라이언트는 전체 서브넷입니다. 즉, 원격 서브넷간에 IPsec 연결이 설정됩니다.
- *L2TP Host-to-Net*. 클라이언트는 L2TP를 사용하는 단일 장치입니다.
- *XAuth Host-to-Net*. 클라이언트는 단일 장치이며 인증은 XAuth에 의해 수행됩니다.

각각의 옵션은 기본적으로 동일하며 Net-to-Net 연결에 사용할 수 있는 옵션이 하나만 있습니다.

인증 유형

드롭 다운 메뉴에서 선택한 옵션에 따라 클라이언트의 인증 방법이 결정됩니다. 사용할 수 있는 값은 다음과 같습니다.

- *암호 (PSK).* 클라이언트는 오른쪽에 있는 *사전-공유 키 사용* (*Use a pre-shared key)* 텍스트 필드에 지정된 암호를 제공해야 합니다.
- *피어는 원격 ID 필드의 IPV4_ADDR, FQDN, USER_FQDN 또는 DER_ASN1_DN 문자열로 식별됩니다.* 클라이언트는 IP 주소, 도메인 이름 또는 IPsec 터널의 다른 고유한 정보로 인증됩니다.

- *기존 인증서를 사용하십시오.* 오른쪽의 드롭 다운 메뉴에서 선택한 인증서를 사용해야 합니다.
- *새 인증서를 생성하십시오.* 새 인증서를 만들 수 있는 추가 옵션이 표시됩니다.
- *인증서를 업로드하십시오.* 로컬 워크스테이션에서 사용할 인증서를 선택하십시오.
- *인증서 요청을 업로드하십시오.* 새 인증을 확보하기 위해 로컬 워크스테이션에서 인증 요청을 선택하십시오.
- *XAUTH 하이브리드. XAuth Host-to-Net* 연결에서만 사용 가능: 사용자가 인증해야 하며, 암호화 터널은 인증하지 않아야 합니다.

로컬 ID

로컬 네트워크 내에서 클라이언트를 식별하는 문자열.

인터페이스

호스트가 연결하는 인터페이스입니다.

로컬 서브넷

클라이언트에서 액세스할 수 있는 로컬 서브넷입니다.

> **참고:** 이 값을 설정하지 않으면, iOS를 실행하는 모바일 장치가 XAuth를 통해 Endian UTM Appliance에 제대로 연결할 수 없으므로, *연결 유형*이 XAuth로 설정되면, 특수 서브넷 *0.0.0.0/0*이 *자동으로 추가됩니다.*

> **힌트:** IKEv1을 사용할 때만 IKEv1이 하나의 서브넷만 지원하므로, 둘 이상의 서브넷을 한 줄에 하나씩 추가할 수 있습니다.

원격 ID

연결의 원격 호스트를 식별하는 ID입니다.

원격 서브넷

Net-to-Net 연결에서만 사용할 수 있으며, 원격 서브넷을 지정합니다.

> **참고:** IKEv2를 사용할 때 둘 이상의 서브넷을 추가할 수 있습니다.

Roadwarrior 가상 IP

텍스트 필드에 지정된 IP 주소가 원격 클라이언트에 할당됩니다.

> **힌트:** 이 IP 주소는 아래의 IPsec 설정에 정의된 풀 내에 있어야 합니다.

> **참고:** 이 옵션은 클라이언트에 대한 IP 주소 할당을 담당하는 L2TP 또는 Net-to-Net 연결이기 때문에, L2TP 호스트 간 연결에는 사용할 수 없습니다.

데드 피어 감지 작업

피어가 단절된 경우 수행할 작업입니다. 드롭 다운 메뉴에서 사용할 수 있는 선택 사항으로는 *지우기, 보류* 또는 피어 *재시작*이 있습니다.

고급 레이블을 클릭하면, 다양한 유형의 암호화 알고리즘을 선택하고, 구성할 수 있는 추가 옵션을 사용할 수 있습니다. 모든 옵션에 대해, 다양한 유형의 알고리즘을 선택할 수 있습니다.

> **경고:** 여기서 선택한 알고리즘의 값은 다른 피어에 정의된 값과 정확히 일치해야 합니다. 그렇지 않으면, 연결이 올바르게 설정되지 않을 수 있습니다.

IKE 암호화

IKE에서 지원해야 하는 암호화 방법.

선택한 암호화 알고리즘 만 허용

확인란을 선택하여 IKE에 대한 소위 엄격 모드를 활성화합니다. 이 모드에서는 선택한 알고리즘만 연결시 허용됩니다.

버전 5.0의 새로운 기능.

IKE 무결성

패킷의 무결성을 검증하기 위해, 지원되어야 하는 알고리즘.

IKE 그룹 유형

IKE 그룹 유형입니다.

IKE 수명

몇 시간 동안 IKE 패킷이 유효합니까?

ESP 암호화

ESP에서 지원해야 하는 암호화 방법.

선택한 암호화 알고리즘 만 허용

확인란을 선택하여 ESP에 대한 소위 엄격 모드를 활성화합니다. 이 모드에서는 선택한 알고리즘만 연결시 허용됩니다.

버전 5.0의 새로운 기능.

ESP 무결성

패킷의 무결성을 검증하기 위해, 지원되어야 하는 알고리즘.

ESP 그룹 유형

ESP 그룹 유형입니다.

ESP 수명

ESP 키는 몇 시간 동안 유효해야합니까?

페이로드 압축 협상

페이로드 압축을 허용하려면, 확인란을 선택하십시오.

페이로드 압축 협상

이 옵션은 트래픽 압축을 협상합니다.

버전 5.0의 새로운 기능.

모드 구성

이 옵션은 **푸시(내보내거나)** 또는 **풀(당겨올)** 클라이언트에 가상 IP를 할당하는 방법을 결정합니다. 이 옵션은 IKEv1에만 해당됩니다.

버전 5.0의 새로운 기능

연결 시작

이 옵션에는 연결시 터널의 동작을 결정하는 세 가지 옵션이 있습니다.

- 즉시 연결을 설정합니다. 터널 구성이 IPsec 구성으로 로드된 직후에 연결이 시작됩니다. 이것은 **auto=start** 구성 값에 해당합니다.
- 트래픽이 감지되면 연결을 시작합니다. 연결이로드 되지만 실제 연결은 터널에서 일부 트래픽이 감지되자 마자 설정됩니다. 이는 **auto=route** 구성 값에 해당합니다.
- 연결을 시작하지 않고 로드합니다. 연결은 로드되지만 시작되지 않습니다. 이는 **auto=add** 구성 값에 해당합니다.

> **힌트:** 연결이 설정된 경우에도, IPsec 트래픽이 감지되지 않으면, **auto=route** 옵션, 즉, 두 번째 옵션을 사용하십시오.

버전 5.0의 새로운 기능.

추가 참고사항: IKE는 RFC 5996에 정의되어 있으며 이전 RFC 2409 (IKEv1) 및 RFC 4306 (IKEv2)보다 우선합니다.

ESP는 RFC 4303 (ESP) 및 RFC 4305 (ESP의 암호화 알고리즘)에 설명되어 있습니다.

추가 참고사항: 웹 사이트 help.endian.com에서 다음 자습서를 사용할 수 있습니다.

1. IPsec VPN - Roadwarrior 연결을 만드는 방법 (Shrewsoft)
2. SSL VPN - Net-to-Net 연결을 만드는 방법
3. SSL VPN – (HTTP를 통한) Net-to-Net 연결 생성 방법
4. IPsec VPN - Net-to-Net 연결을 만드는 방법 (엔디안-to-엔디안 연결)
5. SSL VPN - Roadwarrior 연결을 만드는 방법
6. IPsec VPN - Net-to-Net 연결을 생성하는 방법 (Endian-to-Cisco ASA)

L2TP

Endian UTM Appliance에서 L2TP를 활성화하려면, Enable *L2TP* 레이블 옆에 있는 스위치가 녹색이어야 합니다. 회색이면, 그것을 클릭하여 서비스를 시작하십시오.

계층 2 터널링 프로토콜인 L2TP는 RFC 2661에 설명되어 있습니다. 다음 구성 옵션을 사용할 수 있습니다.

구역

L2TP 연결이 연결되는 영역입니다. 드롭 다운 메뉴에서 활성화된 영역만 선택할 수 있습니다.

L2TP IP 풀 시작 주소, L2TP IP 풀 끝 주소

Endian UTM Appliance에 연결할 때, L2TP 사용자가 IP 주소를 수신하는 IP 범위입니다.

디버그 사용

이 확인란을 선택하면, L2TP가 자세한 로그를 생성합니다.

추가 참고사항: 웹 사이트 help.endian.com에는 Endian UTM Appliance를 IPsec 서버로 설정하고, 클라이언트로 스마트 폰을 설정하는데 도움이 되는 몇 가지 자습서가 있습니다.

1. IPsec 및 L2TP 터널을 사용하는 VPN 설정
2. Android를 사용하여 L2TP (IPSec)를 통해 Endian UTM에 연결
3. iOS를 사용하여 L2TP (IPSec)를 통해 Endian UTM에 연결
4. Windows 7을 사용하는 L2TP (IPSec)를 통해 Endian UTM에 연결

포털(Portal)

VPN 포털은 클라이언트와 서버간에 원활하게 작동하여, 클라이언트가 서버에 직접 연결하지 않고도 원격 HTTP 및 HTTPS 리소스를 검색할 수 있습니다. 그렇게 하기 위해, 클라이언트로부터의 요청을 처리

한 다음, 서버에서 자원을 가져오고 마지막으로 다시 클라이언트에 전달합니다. 즉, VPN 포털은 일종의 프록시 역할을 합니다. 즉, *역방향 프록시* (즉, 일반 (정방향) 프록시와 달리) 서버는 Endian UTM Appliance가 서비스 하는 하나의 구역 내에 상주하는 프록시입니다 - 일반적으로 DMZ이며, 클라이언트는 원격지에서 연결합니다. 따라서 연결은 REDT 신뢰할 수 없는 네트워크 세그먼트에서 시작되며, VPN 포털이 없으면, 허용되지 않습니다.

원칙적으로 포트 포워딩과 같은 방법이지만, Endian UTM 어플라이언스의 VPN 포털의 장점은 다양한 기능을 갖추고 있기 때문에, 클라이언트를 인증하고 연결에 필요한 소스 IP를 제한할 수 있는 기능을 제공합니다. 통신을 보다 안전하게 합니다. 또한 원격 연결에서 서버의 다른 리소스로 여러 경로를 정의할 수 있으므로, 가능한 구성에 유연성이 추가됩니다.

이 설명에서 고안될 수 있는 즉각적인 사용 사례는 OpenVPN 서버를 설정하고, 활성화할 필요없이 회사의 직원 또는 동료가 회사의 인트라넷에 있는 리소스에 원격으로 액세스 할 수 있게 하는 것입니다. 동일한 Endian UTM Appliance에서 VPN 서버와 VPN 포털이 공존할 수 있습니다.

이 사용 사례를 구현하려면, 새 경로와 대상을 정의한 다음, Endian UTM Appliance에서 로컬로 수행하거나 인트라넷의 LDAP/AD 설치에 연결하여, 사용자에 대한 인증이 필요합니다.

구성

이 탭에서는 사용된 도메인 이름 및 업 링크와 관련된 주요 포털의 옵션을 구성할 수 있습니다.

포털 사용

포털을 활성화하려면, 몇 초 후에 녹색으로 바뀌는 회색 스위치를 클릭하십시오.

이름

포털에 지정된 이름입니다.

도메인

포털이 책임지고, 트래픽을 허용하는 도메인입니다.

포털 소유자의 이름

도메인을 소유한 회사의 이름. 도움말 페이지에서 사용되며 다음 옵션을 참조하십시오.

도움말 페이지

이 옵션을 선택하면, 도메인의 루트 경로가 구성되지 않은 경우, 정보를 제공하는 페이지가 도메인에 연결하는 사용자에게 표시됩니다. 포털의 소유자 이름은 해당 페이지의 컨텐트에 대한 참조 연락처로 포함됩니다.

업링크 / IP 주소

도메인과 연결된 자원에 액세스하는 업 링크.

HTTPS 지원

이 확인란을 선택하면, VPN 포털에서 HTTPS 도메인에 연결할 수 있습니다.

인증서 구성

HTTS 사이트에 연결하는데 사용할 인증서입니다.

고급 패널에서 몇 가지 옵션을 구성할 수 있습니다.

HTTP 포트

일반 HTTP 트래픽에 대해 포털에서 사용하는 포트입니다.

HTTPS 포트

암호화된 HTTPS 트래픽에 대해 포털에서 사용하는 포트입니다.

추가 도메인

텍스트 필드에 주 도메인과 관련된 추가 도메인 이름을 한 줄에 하나씩 작성하십시오.

경로

기본 포털 구성이 수행되면, 영역 내에서 액세스 할 수 있는 다양한 리소스를 설정할 수 있습니다. 여기에서 이미 로컬 리소스에 정의된 모든 경로를 포함하는 테이블이 테이블의 맨 아래에 나타납니다. 각 경로에서 다음 작업을 수행할 수 있습니다.

- ☑☐ - 경로를 비활성화하거나 활성화합니다.
- ✎ - 경로를 수정합니다.
- 🗑 - 경로를 삭제합니다.

새 경로는 표 위에 있는 *새 경로 추가* 링크를 클릭하여 정의할 수 있습니다.

경로(Path)

클라이언트가 요청한 자원에 대한 경로.

> **참고:** 경로와 관련된 모든 하위 경로가 포함됩니다.

목적지

포털에 의해 트래픽이 리디렉션되는 로컬 리소스입니다. 이 리소스는 Endian UTM Appliance에서 도달할 수 있는 영역에 위치해야 합니다.

확장된 내용 재작성

이 확인란을 선택하면, 로컬 리소스의 헤더에 있는 내용도 다시 작성됩니다.

> **힌트:** 경로에 문제 (예: 잘못 표시된 페이지, 로드되지 않은 페이지, 브라우저 크래시)가 있는 경우에는 이 옵션을 사용하지 마십시오.

허용된 소스 IP 주소

경로에 액세스 할 수 있는 소스 IP 주소.

설명

사용자 정의 설명.

인증 필요

경로에 인증을 요구하려면, 확인란을 선택하십시오.

포털 인증 설정 무시

경로에 액세스하는데 사용자 정의 인증 서버를 사용해야 하는 경우에, 확인란을 선택하고 아래의 다중 선택란에서 하나를 선택하십시오.

활성화

경로를 활성화하려면, 확인란을 선택하십시오.

중첩 인증에 대한 우수 사례.

인증은 VPN 포털과 포털을 통해 도달한 경로 모두에 존재할 수 있지만, 두 측면 중 하나에서만 인증을 수행하는 것이 좋습니다. 실제로 중첩된 인증에는 미묘한 문제가 있습니다.

경로가 **mary/otherpass를** 필요한 반면에, 포털은 **john/somepass** 쌍의 username-password로 필요하는 시나리오를 고려해보십시오. 첫 번째 연결에서, 인증이 필요한 팝업에서 **john/somepass** 쌍이 제공되어야 포털 뒤의 경로에 액세스 할 수 있습니다. 이제, **mary/pass** 쌍이 경로에 대한 액세스를 제공합니다. 그러나 경로의 다른 페이지가 필요할 때, 포털은 경로의 포털과 포털에 필요한 포털과 일치하지 않는 것들을 저장한 마지막 자격 증명을 수신하고, 인증을 위한 또 다른 팝업이 표시됩니다.

인증(Authentication)

이 페이지에서는 다음과 같은 내용을 살펴봅니다.

- 사용자
  - 새 로컬 사용자 추가
    - OpenVPN 옵션

이 페이지에는 세 가지 탭이 있습니다. 사용자 및 그룹은 OpenVPN 또는 IPsec 및 설정과 같은 VPN 서비스에 액세스 할 수 있는 모든 클라이언트를 관리하여, Endian UTM Appliance의 로컬 또는 원격의 다양한 인증 방법을 정의할 수 있습니다.

> **참고:** 스위치 보드가 Endian UTM Appliance에 설치된 경우에, 사용자 및 그룹 관리가 스위치 보드 모듈에서 수행되므로, 이 페이지에는 설정 탭만 표시됩니다.

사용자

이 페이지에서는 Endian UTM Appliance의 VPN 서버에 계정이 있는 모든 사용자가 테이블에 표시되고 각 사용자에 대해 다음 정보가 표시됩니다.

- 이름. 사용자의 이름.
- 설명. 주석입니다.
- 인증 서버. 로컬 인증 (Endian UTM Appliance 자체) 또는 LDAP (설정 탭에서 구성 가능한 외부 LDAP 서버) 중 하나인 사용자 인증에 사용되는 서버.
- 작업. 계정에서 수행할 수 있는 작업입니다. LDAP 사용자의 경우, *사용/사용 안함* 및 *편집*, 로컬 사용자의 경우에는, *삭제*될 가능성도 있습니다. LDAP 사용자를 편집하면, 사용자 이름이나 암호 같은 LDAP 서버가 완전히 관리하는 로컬 옵션 만 수정할 수 있습니다.

표 위에 `새 로컬 사용자 추가`를 클릭하여 새 로컬 계정을 추가하십시오. 표시되는 양식에서 각 사용자에 대해 다음 옵션을 지정할 수 있습니다.

새 로컬 사용자 추가

사용자 이름

사용자의 로그인 이름

설명

추가 코멘트.

외부 인증 서버를 사용하여 인증

이 확인란은 하나 이상의 외부 인증 서버가 구성된 경우에만 표시됩니다. 일단 선택되면, 다음의 암호 입력 필드가 사라지고, 사용자는 외부 인증 서버를 사용하여 인증됩니다.

암호, 암호 확인

사용자의 암호를 두 번 입력해야 합니다. 비밀번호는 실제로 표시되지 않습니다. 비밀번호를 보려면, 오른쪽에 있는 두 개의 체크 박스를 선택하십시오.

일회성 암호 비밀(One Time Password secret)

이 필드에는 특정 사용자의 TOTP 암호가 들어 있습니다. 이러한 비밀 정보를 생성하는데, 제약이 있으므로 수동으로 삽입할 수는 없지만, `새 비밀 생성` 버튼을 클릭하여 생성해야 합니다. 비밀 번호의 QR 코드 표현은 `QR 코드 표시` 버튼을 클릭하여 표시할 수 있습니다.

일회성 암호

다양한 일회용 암호 알고리즘이 있습니다. Endian UTM Appliance 시스템에서 Time-based One-Time Password 알고리즘은 RFC 6238에 설명 된대로 구현되었습니다. 이는 공개 표준이므로 거의 모든 장치 (Android, iOS 및 Windows 스마트 폰, PC 등)에 응용 프로그램이 존재합니다. 장치를 사용하려면 일회용 암호로 초기화해야 합니다. 수동으로 암호를 입력하거나 QR 코드를 찍어 암호를 입력하십시오.

인증서 구성

사용자에게 인증서를 할당하려면, 모드를 선택하십시오. 사용 가능한 모드는 드롭 다운 메뉴에서 선택할 수 있습니다: *새 인증서 생성, 인증서 업로드* 및 *인증서 서명 요청 업로드* 등이 있습니다. 선택시 드롭 다운 메뉴 아래에, 각 모드에 사용할 수 있는 옵션이 표시되며, 인증서 페이지에 설명되어 있습니다.

조직 단위 이름

사용자가 속한 조직 단위, 즉 인증서로 식별된 회사, 기업 또는 기관 부서입니다.

조직 이름

사용자가 속한 조직입니다.

도시(City)

조직이 위치한 도시 (인증서의 **L**)입니다.

국가 또는 지방

조직이 위치한 주 또는도 (인증서의 **ST**)입니다.

국가

조직이 위치한 국가 (인증서의 **C)**이며 선택 메뉴에 있는 국가에서 선택합니다. 하나 이상의 문자를 입력하여, 일치하는 국가를 검색하여 표시합니다.

이메일 주소

사용자의 전자 메일 주소입니다.

그룹 회원

패널의이 부분에서는 하나 이상의 그룹에 회원 자격을 할당할 수 있습니다. 검색 위젯에서 일치하는 그룹을 찾기 위해, 기존 그룹을 필터링할 수 있습니다. 그룹 이름의 오른쪽에 있는 `+` 를 클릭하면 그룹 회원이 추가됩니다. 아래 텍스트 필드에 사용자가 속한 그룹이 표시됩니다. `모두 추가`에 대한 바로 가기와 한 번에 `모든 그룹 구성원 자격 제거`가 있습니다.

OpenVPN 옵션 재정의

OpenVPN 프로토콜을 사용하려면, 이 확인란을 선택하십시오. 이 옵션은 계정에 대한 사용자 정의 옵션을 지정하는 상자를 표시합니다. 아래를 참조하십시오.

L2TP 옵션 무시

사용할 L2TP 터널을 선택할 상자를 표시하려면, 이 확인란을 선택하십시오.

> **힌트:** OpenVPN 옵션도 무시할 경우, L2TP 옵션 상자가 OpenVPN 옵션 상자 아래에 나타납니다.

서비스 사용중지

이 다중 선택 상자에서 이 사용자가 사용할 수 있는 VPN 서비스를 선택하십시오. 기본적으로 **OpenVPN, IPsec XAuth** 및 **L2TP** 만 존재하지만 사용자 지정 VPN 인증 서버가 정의되어 있으면, 더 많은 기능이 나타납니다.

활성화

사용자를 활성화하기 위해 이 확인란을 선택하십시오. 즉, 사용자가 Endian UTM Appliance의 OpenVPN 서버에 연결할 수 있도록 허용합니다.

OpenVPN 옵션

VPN 서버를 통해 모든 클라이언트 트래픽을 유도

이 옵션을 선택하면, 대상에 관계없이 연결 클라이언트의 모든 트래픽이 Endian UTM Appliance의 업링크를 통해 라우팅됩니다. 기본값은 대상이 클라이언트의 업링크를 통해 내부 구역 (예: 인터넷 호스트) 외부에 있는 모든 트래픽을 라우팅하는 것입니다.

이 클라이언트에만 글로벌 옵션 푸시

고급 사용자 전용. 일반적으로 클라이언트가 연결되면, VPN을 통해 액세스 할 수 있는 네트워크에 대한 터널 경로가 클라이언트의 라우팅 테이블에 추가되어 Endian UTM Appliance에서 도달할 수 있는 다양한 로컬 네트워크에 연결할 수 있습니다. 이 동작을 원하지 않을 경우, 이 옵션을 사용해야 하지만 클라이언트의 라우팅 테이블 (특히 내부 구역의 라우팅 테이블)은 수동으로 수정해야 합니다.

GREEN [BLUE, ORANGE] 구역으로 경로를 푸시,

이 옵션이 활성화되면, 클라이언트는 GREEN, BLUE 또는 ORANGE 영역에 액세스 할 수 있습니다. 이 옵션은 해당 영역을 사용할 수 없는 경우에는 아무 효과가 없습니다.

클라이언트 뒤에 있는 네트워크

사용자가 GW2GW 설정에서 원격 게이트웨이를 연결하는데 사용될 때, 이 상자에는 OpenVPN 서버를 통해 다른 클라이언트에서 연결할 수 있어야 하는 클라이언트 뒤에 있는 네트워크 목록이 포함됩니다. roadwarrior (single) 사용자에게는 사용되지 않습니다.

> **경고:** 이 옵션은 사용자가 GW2GW 클라이언트에 연결하는데 사용되는 경우에는 **필수**입니다. 여기에 네트워크가 지정되어 있지 않으면, 다른 네트워크로 연결되는 경로가 없으므로 연결할 수 없습니다.

정적 IP 주소

동적 IP 주소는 클라이언트에 할당되지만, 여기에 제공된 고정 IP 주소는 연결될 때마다 클라이언트에 할당됩니다.

> **참고:** 클라이언트가 Endian UTM Appliance에서 실행중인 멀티 코어 VPN 서버에 연결하는 경우에, 이 할당은 고려되지 않습니다.

이 네임 서버 푸시

여기에 클라이언트별로 맞춤 네임 서버를 할당하십시오. 이 설정 (및 다음 설정)은 정의할 수 있지만 사용 여부에 관계없이 설정할 수 있습니다.

이 도메인 푸시

클라이언트별로 맞춤 검색 도메인을 할당하십시오.

> **참고:** 게이트웨이 대 게이트웨이 VPN을 통해, 둘 이상의 브랜치를 연결하려는 경우에, 다른 지점의 LAN에 대해 서로 다른 서브넷을 선택하는 것이 좋습니다. 예를 들어, 한 브랜치는 192.168.1.0/24 서브넷이있는 GREEN 영역을 가지며, 다른 브랜치는 192.168.2.0/24를 사용합니다. 이 솔루션을 사용하면, 오류 및 충돌에 대한 여러 가지 원인을 피할 수 있습니다. 실제로, 사용자 정의 경로를 푸시할 필요없이, 올바른 경로를 자동으로 할당하고, 충돌할 수 있는 경로에 대해 경고 메시지를 표시하지 않으며, 올바른 로컬 이름 확인 및 WAN 네트워크 설정을 쉽게 하는 등의 기능을 포함한 몇 가지 이점이 무료로 제공됩니다.

L2TP 옵션

IPsec 터널

이 드롭 다운 메뉴에서는 이미 정의된 터널 중에서 사용자가 사용할 터널을 선택할 수 있습니다.

> **참고:** IPsec 터널이 아직 구성되지 않은 경우에, IPsec 터널 목록 대신 *터널 선택...* 메시지가 나타납니다.

그룹

이 페이지에는 Endian UTM Appliance 또는 외부 LDAP 서버에 정의된 모든 그룹을 보여주는 표가 표시됩니다. 각 그룹에 대해 다음 정보가 표시됩니다.

- 그룹 이름. 그룹의 이름.
- 설명. 주석.
- 인증 서버. *로컬* 인증 (Endian UTM Appliance 자체) 또는 *LDAP* (외부 LDAP 서버, vpnauthsettings 탭에서 구성) 중 하나인 사용자 인증에 사용되는 서버.
- 작업. 계정에서 수행할 수 있는 작업입니다. LDAP 서버의 경우, 유일한 작업은 로컬 특성을 *편집*하는 것인 반면에, 로컬 그룹의 경우, 그룹을 *삭제*할 가능성도 있습니다.

새 로컬 그룹을 추가하려면, 테이블 위에 `새 로컬 그룹 추가`를 클릭하십시오. 표시되는 양식에서 각 그룹에 대해 다음 옵션을 지정할 수 있습니다.

그룹 이름

그룹에 주어진 이름.

설명

주석이나 설명입니다.

사용자

패널의 이 부분에서는, 사용자를 그룹에 할당할 수 있습니다. 검색 위젯에서 기존 로컬 사용자를 필터링하여 일치하는 사용자를 찾을 수 있습니다. 사용자는 사용자 이름 오른쪽에 있는 `+` 를 클릭하여, 그룹에 추가됩니다. 그룹의 사용자는 아래의 텍스트 필드에 표시됩니다. `전체 추가` 및 그룹으로/그룹으로부터 `모든 사용자 제거`에 대한 바로 가기도 있습니다.

OpenVPN 옵션 재정의

OpenVPN 프로토콜을 사용하려면, 이 확인란을 선택하십시오. 이 옵션은 계정에 대한 사용자 지정 옵션을 지정하는 상자를 표시하며, 로컬 사용자에 대해 지정된 옵션과 동일합니다.

L2TP 옵션 무시

이 확인란을 선택하면, 드롭 다운 메뉴에서 사용할 L2TP 터널을 선택할 상자가 표시됩니다.

> **참고:** 아직 L2TP 터널이 구성되어 있지 않으면, 이 옵션을 선택할 수 없습니다. 이 경우에, 유익한 메시지가 하이퍼링크로 나타납니다. 그것을 클릭하면, IPsec 연결 편집기가 열립니다. 일단 새로운 L2TP 터널이 생성되면, 이를 사용자에게 연결할 수 있습니다.

> **힌트:** OpenVPN 옵션도 무시할 경우, L2TP 옵션 상자가 OpenVPN 옵션 상자 아래에 나타납니다.

활성화

확인란을 선택하여, 사용자를 활성화합니다. 즉, 사용자가 Endian UTM Appliance의 OpenVPN 서버에 연결할 수 있도록 허용합니다.

> **경고:** 동일한 사용자가 합법적으로 하나 이상의 그룹에 속할 수는 있지만 사용자가 속한 그룹이 대비 무시 (contrasting *override*) 옵션을 정의하지 않도록 주의해야 합니다. 예를 들어, GREEN 영역에만 액세스를 허용하고, BLUE에만 액세스를 허용하는 두 그룹의 사용자 구성원을 고려하십시오. 이 경우에, BLUE 또는 GREEN 구역에 대한 사용자 권한 부여 여부를 예측하는 것은 쉽지 않습니다. 이러한 문제의 관리는 OpenVPN 서버의 관리자에게 맡깁니다.

설정

이 페이지는 Endian UTM Appliance가 의존하고, 관리할 수 있는 인증 서버의 현재 구성을 포함합니다. LDAP/Active 디렉토리, 로컬, 일회용 패스워드, 반경 및 분할 데이터와 같은 여러 인증 서버를 사용할

수 있습니다.

스위치보드가 설치되면, 스위치보드 몽고 DB라는 추가 옵션이 표시됩니다.

이 페이지에는 *인증 서버*에 대한 정보를 표시하는 테이블과 *인증 서버 맵핑*을 표시하는 테이블이 있습니다. 전자의 경우, 이 정보가 표시됩니다.

- 이름. 서버에 주어진 이름
- 유형. 서버가 로컬 또는 외부 LDAP인지 여부
- 서비스. 해당 서버에서 사용할 수있는 인증.
- 작업. 각 인증 서버마다 다음 작업이 가능합니다.
    - ☑☐ - 서버를 활성화 또는 비활성화합니다.
    - - 서버 편집합니다.
    - - 서버를 삭제합니다.
    -  - LDAP 서버의 사용자 및 그룹을 동기화합니다 (LDAP / Active Directory 서버에만 해당).

하단의 표에는 IPsec XAuth, OpenVPN 또는 L2TP와 같이 사용 가능한 각 서비스에서 사용되는 인증 서버가 나와 있습니다.

매핑을 위한 유일한 작업은 그것들을 편집하는 것입니다. actedit 아이콘을 클릭하면, 선택기에서 해당 서비스에 사용할 인증 백엔드를 선택할 수 있는 양식이 나타납니다.

> **힌트:** 여러 서버를 서비스에 매핑하고, 더 많은 서비스에 동일한 인증 서버를 사용할 수 있습니다.

표 위에 있는 새 인증 서버 추가 링크를 클릭하면, 모든 데이터를 제공하여 새 인증 서버를 설정하는 양식이 열립니다.

이름

인증 서버에 주어진 이름.

활성화

확인란을 선택하여, 서버를 활성화하십시오.

유형

드롭 다운 메뉴에서 서버 유형을 선택하십시오. 다음 옵션을 사용할 수 있습니다.

- *LDAP / Active Directory*

  LDAP 서버를 사용하여, 사용자를 인증하려면 이 옵션을 선택하십시오. 이 유형에는 다음 옵션

이 지원됩니다.

LDAP 서버 URI

LDAP 서버의 URI.입니다.

LDAP 서버 유형

이 드롭 다운 메뉴에서는 일반**, Active Directory, Novell eDirectory** 또는 **OpenLDAP** 중에서 인증 서버 유형을 선택할 수 있습니다. 이 선택 사항에 따라, 추가 필드가 표시되거나 숨겨집니다.

LDAP 바인드 DN 사용자 이름

LDAP 서버에서 사용자 데이터를 검색하는데 사용되는 LDAP 계정의 완전히 구별되는 이름입니다.

LDAP 바인드 DN 암호

바인드 DN 사용자의 비밀번호

다음 옵션은 서버 설정에 따라 다르며, 서버의 사용자 및 그룹을 선택하는데 사용됩니다. *LDAP 사용자 기본 DN, LDAP 그룹 기본 DN*의 두가지가 있습니다.

일반 LDAP 서버 유형을 사용하는 경우, *LDAP 사용자 검색 필터, LDAP 사용자 고유 ID 속성, LDAP 그룹 고유 ID 속성, LDAP 그룹 구성원 속성, LDAP 그룹 검색 필터*와 같은 추가 매개 변수를 구성해야 합니다.

지정된 그룹으로 제한. 이 옵션을 사용하면, LDAP 서버에서 Endian UTM Appliance의 OpenVPN 서버에 연결할 수 있는 그룹을 선택할 수 있습니다.

- 로컬

로컬에서 사용자를 만들고 관리하려면, 이 옵션을 선택하십시오. 다음 옵션을 사용할 수 있습니다.

특정 그룹으로 제한

이 옵션을 사용하면, LDAP 서버에서 Endian UTM Appliance의 OpenVPN 서버에 연결할 수 있는 그룹을 선택할 수 있습니다.

- *RADIUS*

RADIUS 서버를 구성하려면, 이 옵션을 선택하십시오. RADIUS 서버는 일회용 암호 및 분할 데이터 인증 서버에서 암호 공급자로만 사용할 수 있습니다. RADIUS 서버를 사용하려면, 다음 옵션을

정의해야 합니다.

RADIUS 서버

RADIUS 서버의 주소입니다.

RADIUS 공유 비밀

RADIUS 서버와 Endian UTM Appliance 간의 공유 비밀.

RADIUS 인증 포트

RADIUS 인증에 사용되는 TCP 포트입니다.

RADIUS 계정 포트

계정에 사용되는 TCP 포트.

RADIUS 식별자

Endian UTM 어플라이언스의 RADIUS 식별자 또는 NAS ID

- 데이터 분할 (사용자 정보 및 비밀번호)

  이 서버 유형은 두 개의 다른 공급자에 대한 프록시로 작동하지만, 이중 인증을 추가하지 않습니다. 이 서버를 선택하면, 두 개의 드롭 다운 메뉴를 통해, 사용자와 암호에 대해 다른 공급자를 선택할 수 있습니다.

  사용자 정보 제공자

  사용자 정보를 검색할 인증 서버를 선택하십시오.

  암호 공급자

  사용자를 인증하는데 사용되는 인증 서버를 선택하십시오.

- *일회성 암호*

  이 옵션을 선택하면, 이중 인증이 가능합니다. 이전 옵션인 데이터 분할과 마찬가지로, 이 서버 유형은 시간 기반 일회용 암호를 사용한 두 가지 요소 인증을 추가하여 두 가지 공급자에 대한 프록시 역할을 합니다. 이 유형을 선택하는 것은 사용자 정보와 암호 공급자 모두의 소스를 선택할 수 있습니다. 옵션은 데이터 분할 옵션과 동일합니다.

  사용자 정보 제공자

사용자 정보를 검색할 인증 서버를 선택하십시오.

암호 공급자

사용자를 인증하는데 사용되는 인증 서버를 선택하십시오.

- *스위치보드 MongoDB*

  이 옵션을 선택하면, 스위치 보드, MongoDB에 의해 사용되는 인터넷 데이터베이스를 인증에 사용할 것입니다. 이 인증 서버를 위한 옵션은 없습니다.

인증서(Certificates)

이 페이지에서는 다음과 같은 정보를 찾으실 수 있습니다.

- 인증서
  - 새로운 인증서 생성하기

인증서 페이지에서는 Endian UTM Appliance에서 실행되는 다양한 OpenVPN 서버 인스턴스에 필요한 인증서를 관리할 수 있으며, *인증서, 인증 기관, 해지된 인증서* 및 *인증서 해지 목록*의 네 가지 탭으로 구성되어 있습니다.

인증서

여기에서 Endian UTM Appliance에 저장된 모든 인증서를 관리할 수 있습니다. 처음에는 비어 있는 테이블은 모든 인증서를 각 열(column)당 하나씩 다음 세부 정보와 함께 표시합니다.

- *이름(Name).* 인증서에 지정된 이름입니다.
- *제목(Subject).* 인증서를 식별하는 정보 모음. 그 자체이며, 아래 옵션을 참조하십시오.
- *CA(Certificate Authority).* 인증 기관
- *만료일(Expiration Date).* 인증서 유효 기간의 최종 날짜.
- *작업(Actions).* 인증서로 수행할 수 있는 작업은 다음과 같습니다.
    - - 모든 상세 정보를 표시합니다.
    - - PEM 형식으로 다운로드합니다.
    - - PKCS12 형식으로 다운로드합니다.
    - - 관련된 비공개 키를 삭제합니다.
    - - 삭제합니다.
    - - 인증서를 해지합니다.

테이블의 하단의 왼쪽에는, 인증서가 많은 경우, 테이블을 구성하는 다양한 페이지들 사이를 탐색할 수 있는 탐색 위젯이 있고, 반면에 오른쪽에는 재로드 위젯이 있으며, 인증서 목록을 새로 고치는데 사용됩니다.

목록 위에 있는 링크를 클릭하여, 새 인증서 추가할 수 있습니다. 클릭하면, 페이지가 새 인증서 생성에 필요한 모든 데이터를 제공할 수 있는 양식으로 대체될 것입니다. Endian UTM Appliance에 새 인증서를 저장하는데 사용할 수 있는 세 가지 대안 방법으로 이 드롭 다운 메뉴에서 선택할 수 있습니다. 이 세 가지 방법은 *새 인증서 생성, 인증서 업로드* 및 *인증서 서명 요청 업로드* 등입니다.

새 인증서 생성

첫 번째 대안은 다음 정보를 제공하여, Endian UTM Appliance에서 직접 새 인증서를 만들 수 있습니다. 괄호 안의 대문자는 제공된 값으로 채워지고, 인증서 *제목*을 구성하는 인증서 필드를 나타냅니다.

> **참고:** 인증서를 만들려면, 루트 인증 기관이 필요하므로 인증서를 만들기 전에 루트 CA를 만드십시오.

일반 이름

인증서 소유자의 일반 이름 (CN), 즉 소유자를 식별할 이름입니다.

이메일 주소

인증서 소유자의 전자 메일 주소입니다.

주체 대체 이름

단일 인증서가 여러 도메인이나 리소스에 연결될 수 있도록 하는 제목의 대체 이름입니다. 사용 가능한 옵션은 다음과 같습니다.

- *DNS.* 사이트의 DNS 항목
- *IP.* 사이트의 IP 주소
- *이메일.* 이메일 주소.

각 옵션의 실제 값은 오른쪽 텍스트 상자에 작성해야 합니다.

버전 5.0에서 변경됨: *이 옵션은 제목 대체 명이라고 불립니다.*

조직 단위 이름

소유자가 속한 조직 단위 (OU) (즉, 인증서로 식별된 회사, 기업 또는 기관 부서).

조직 이름

소유자가 속한 조직 (O).

도시

조직이 위치한 도시 (L).

주 또는 도

조직이 위치한 주 또는 지방 (ST).

국가

조직이 위치한 국가 (C)로서 선택 메뉴의 국가에서 선택합니다. 하나 이상의 문자를 입력해야만, 일치하는 국가를 검색하여 표시합니다.

인증서 유형

드롭 다운 메뉴에서 클라이언트와 서버 사이에서 선택된 인증서 유형입니다.

유효 기간 (일)

인증서가 만료되기 전의 일 수입니다.

PKCS12 파일 암호

필요한 경우 인증서의 비밀번호입니다.

PKCS12 파일 암호 (확인)

확인을 위해, 인증서의 암호를 한 번 더 입력하십시오.

인증서 요약 알고리즘

인증서를 생성하는데 사용할 알고리즘을 드롭 다운 메뉴에서 선택하십시오.

버전 5.0의 새로운 기능.

인증서 키 크기

드롭 다운 메뉴에서 인증서 생성에 사용된 키 크기 (비트 단위)를 선택하십시오.

버전 5.0의 새로운 기능.

인증서 업로드

다음 대안은 로컬 워크스테이션의 기존 인증서를 Endian UTM Appliance에 업로드하는 것입니다.

인증서 (PKCS12 / PEM)

찾아보기 버튼이나 텍스트 필드를 클릭하면, 업로드 할 인증서의 경로를 제공하는 파일 선택기가 열립니다.

PKCS12 파일 암호

필요한 경우, 인증서의 비밀번호입니다.

인증서 서명 요청 업로드

세 번째 대안은 로컬 워크스테이션에서 엔디안 UTM 어플라이언스로 CSR을 업로드하는 것입니다. 즉, 서버에서 인식할 수 있는 새로운 인증서를 생성하는데, 필요한 모든 정보가 포함된 암호화된 텍스트 파일입니다.

인증서 서명 요청 (CSR)

찾아보기 버튼이나 텍스트 필드를 클릭하면, 업로드 할 CSR 경로를 제공하는 파일 선택기가 열립니다.

유효 기간 (일)

인증서 유효 기간이 얼마나 남았는지를 표시합니다.

인증 기관

이 페이지에서는 OpenVPN 암호화 연결의 올바른 작동에 필요한 CA를 관리할 수 있습니다. CA를 추가하는 방법에는 두 가지가 있습니다. 이미 존재하는 인증서 테이블 위에 있는 새 루트/호스트 인증서 생성 링크를 클릭하여, 새 인증서를 생성하거나 테이블 아래의 버튼을 사용하여 업로드합니다.

한 번 채워진 표에는 인증서 탭과 동일한 정보가 표시되며, 사용할 수 있는 작업의 유일한 차이점은 다음과 같습니다.

-  - 모든 CA 세부 정보를 표시합니다.
-  - PEM 형식으로 다운로드 하십시오.
-  - 인증서를 삭제합니다.

새로운 인증 기관을 생성하는 대신 기존 인증서를 업로드할 수 있습니다.

인증서 (PEM)

찾아보기 버튼이나 텍스트 필드를 클릭하면 업로드 할 인증서의 경로를 제공하는 파일 선택기가 열립니다. 일단 선택하고, 업로드 CA 인증서를 클릭하면, 업로드 프로세스가 완료됩니다.

새로운 루트 / 호스트 인증서 생성

이 절차는 한 번만 적용할 수 있으며, 두 개의 인증서를 생성합니다. 루트 인증 기관 및 호스트 인증서. *인증서* 탭에 표시됩니다. 링크를 클릭하면, 양식이 새 루트 및 호스트 인증서에 사용될 다음 데이터를 제공하는 목록을 대체합니다.

> **참고:** 새 루트 인증서를 생성하는 유일한 방법은 명령 줄에서 기존 인증서를 삭제하는 것입니다.

시스템의 정규화 된 도메인 이름 또는 IP 주소

인증서의 일반 이름으로 사용될 시스템의 이름입니다.

이메일 주소

시스템 소유자 또는 책임자의 전자 메일 주소입니다.

조직 단위 이름

시스템이 속한 조직 단위 (OU).

조직 이름

시스템이 속한 조직 (O).

도시

조직이 위치한 도시 (L).

주 또는 도

조직이 위치한 주 또는 지방 (ST).

국가

조직이 위치한 국가(C)로서, 선택 메뉴의 국가에서 선택합니다. 하나 이상의 문자를 입력해야만, 일치하는 국가를 검색하여 표시합니다.

제목 대체 이름 (subjectAltName = email:,URI:*,DNS:*,RID:*)*

제목, 즉 인증서의 대체 이름입니다.

유효 기간 (일)

인증서가 만료되기 전의 일 수입니다.

인증서 요약 알고리즘

인증서를 생성하는데, 사용할 알고리즘을 드롭 다운 메뉴에서 선택하십시오.

버전 5.0의 새로운 기능.

인증서 키 크기

드롭 다운 메뉴에서 인증서 생성에 사용된 키 크기 (비트 단위)를 선택하십시오.

버전 5.0의 새로운 기능.

해지된 인증서

해지된 인증서는 표에 나열되어 있으며, 일련 번호와 인증서 제목이 표시됩니다.

인증서 해지 목록 다운로드

이 링크를 클릭하면, 로컬 워크스테이션에서 인증서 해지 목록을 다운로드 할 수 있습니다.

인증서 해지 목록

이 페이지에서 업로드 된 모든 인증서 철회 목록을 관리할 수 있습니다.

표에는 모든 인증서 해지 목록과 표의 각 항목에 대해 인증서 이름, 발급자 및 발급 날짜가 표시됩니다. 사용 가능한 작업은 다음과 같습니다.

- - 증명서의 상세를 표시합니다.
- - 로컬 워크 스테이션에서 인증서를 다운로드하십시오.

핫스팟 메뉴

Endian UTM Appliance와 함께 제공되는 핫스팟은 유선 LAN 연결은 물론 안전하고 안정적인 무선 연결을 제공하는 매우 유연하고 사용자 정의 가능한 솔루션입니다. 핫스팟에 구현된 주요 기능은 다음과 같습니다.

- 핫스팟에 대한 세 가지 역할 : 독립 실행 형 핫스팟, 마스터 - 위성 구성 또는 외부 인증 서버에 의존하여 작동할 수 있습니다.
- 핫스팟 관리자 (전체 관리 액세스), 계정 편집기 (일부 사용자 관리) 및 일반 사용자 (인터넷 탐색 만)의 세 가지 유형의 사용자
- 다양한 유형의 티켓: 시간 기반 vs. 데이터 기반, 선불 및 후불 액세스, 순환.
- 사용자를 위한 세 가지 액세스 포털: 일반 모드, 자바 스크립트 없음, 모바일

- 로그인 배경 이미지 및 사용자 인터페이스 언어의 사용자 정의.
- 사용자가 신용 카드로 액세스 권한을 구입할 수 있게 하는 SmartConnect ™ 옵션
- 사용자의 재 연결 시 식별을 피하기 위한 스마트 로그인.
- 소셜 네트워크 통합.
- SMS 를 통한 사용자 생성 및 활성화.
- 티켓 없이도 특정 웹 사이트에 액세스 할 수 있는 옵션.

버전 5.0의 새로운 기능: *외부 LDAP / AD 인증 서버, 소셜 네트워크 통합.*

버전 5.0의 새로운 기능: *Instagram 및 Twitter 소셜 로그인.*

Endian UTM 어플라이언스에서 파란색 영역은 무선 장치 전용이므로 파란색 영역이 비활성화 된 경우, 핫스팟이 작동하지 않습니다. BLUE 영역에서 RED 영역으로의 연결은 발신 방화벽에서 적절한 규칙을 사용하여 필터링 할 수 있습니다.

왼쪽 메뉴 항목은 핫스팟 설정, 관리 인터페이스 및 핫스팟 사용자에 대한 다양한 구성 및 관리 옵션에 대한 액세스를 제공합니다.

- 핫스팟 설정은 핫스팟 및 인증 서버의 양식을 선택하는 시작 핫스팟 페이지입니다.
- 관리 인터페이스는 모든 관리 작업을 수행할 수 있는 핫스팟의 주요 부분입니다.
- 핫스팟 사용자는 핫스팟의 수퍼 유저 관리를 허용합니다.

또한 핫스팟에 대한 클라이언트 액세스는 핫스팟에 액세스 한 다음, 인터넷에 연결하는 과정을 통해 클라이언트를 유도하는 지침입니다.

추가 참고사항: 엔디안 포털에는 핫스팟의 노하우 전용 카테고리가 있습니다.

또한 포털의 전용 HYPERLINK "https://help.endian.com/hc/en-us/sections/204102028" 섹션에서 4 가지 비디오 자습서를 사용할 수 있습니다.

핫스팟 설정

핫스팟 페이지에 들어갈 때 *핫스팟 스위치 ()를 켜고* 끄기를 클릭하여 핫스팟을 시작하고, 이 페이지의 나머지 부분에서 설명하는 첫 번째 구성 옵션을 표시합니다. 필요한 경우, 핫스팟 및 외부 인증 서버의 역할을 수행합니다.

사용 가능한 추가 옵션 설정은 선택한 역할에 따라 다르므로 다음 세 섹션에서 설명합니다.

1. 마스터 / 독립 실행 형 핫스팟 또는 독립 실행형 핫스팟

핫스팟이 모든 구성 데이터, 즉 사용자 데이터베이스, 포털 구성, 설정, 로그 등의 모든 구성 데이터가 마스터로 사용되면 로컬로 저장되고 관리 작업이 이 핫스팟에서 수행됩니다.

이 역할은 가장 작은 하드웨어인 Endian UTM 어플라이언스의 *독립형 핫스팟* 일 수 있지만, Software, Virtual 및 큰 하드웨어인 Endian UTM 어플라이언스의 경우, 역할은 *마스터*가 될 수도 있습니다. 마스터란 OpenVPN 계정을 통해 마스터에 연결하는 위성 핫스팟에 의해 다시 사용되는 모든 관리 설정 및 데이터를 저장한다는 의미입니다.

마스터 역할의 경우 하나의 설정을 사용할 수 있으며, 인공위성에 할당할 수 있는 사용 가능한 VPN 계정도 표시됩니다.

핫스팟 비밀번호

> 이것은 마스터 핫스팟에 연결하기 위해, 위성 시스템에서만 필요로 하는 마스터 핫스팟의 암호입니다. 이 필드를 비워두면 새로운 임의 암호가 생성됩니다.

핫스팟 위성

> 마스터에 연결하기 위해 원격 위성 시스템에서 사용할 수 있는 사용 가능한 OpenVPN 터널의 목록입니다. 설정에 위성이 필요하지 않거나, OpenVPN 계정이 생성되지 않은 경우이 목록은 비어 있습니다. 그렇지 않으면, 이 목록에서 하나 이상의 시스템을 선택할 수 있습니다.

외부 인증 사용

핫스팟의 역할이 *마스터/독립 실행형 핫스팟*일 때, 계정, 로깅, 사용자 데이터베이스 및 기타 모든 설정을 로컬에서 유지하면서 사용자 인증 목적으로만 외부 리소스 (RADIUS 또는 LDAP 서버)에 의존할 수 있습니다 . 즉, 새 계정을 만들 필요없이 외부 서버에서 사용자 데이터를 검색합니다.

핫스팟이 원격 서버에 연결되어 계정 데이터를 검색할 수 있게 하려면, 사용할 수 있는 옵션이 하나 있습니다.

외부 인증 사용

> 이 확인란을 선택하면, 지원되는 두 인증 방법의 구성을 허용하는 새로운 옵션이 나타납니다.

서버 유형

> 이 드롭 다운 메뉴는 지원되는 두 개의 서버 (LDAP 또는 RADIUS) 중 하나를 선택하고 그에 따

라 표시되는 구성 옵션을 변경합니다.

> **참고:** 여기에 나타나는 추가 구성 옵션은 *Menubar ‣ Proxy ‣ HTTP ‣ Authentication*과 *Menubar ‣ OpenVPN ‣ Authentication ‣ Settings ‣ Add new authentication server* (새 인증 서버 추가)에 나타나는 구성 옵션과 매우 유사합니다.

LDAP 서버의 경우 다음 구성 옵션을 사용할 수 있습니다 (자세한 내용은 오른쪽의 예를 참조하십시오).

LDAP 서버 유형

드롭 다운 메뉴에서는 지원되는 LDAP 서버 유형 중 하나인 **Generic (일반), 액티브 디렉토리 (Active Directory)** 또는 **노벨 디렉토리 (Novell eDirectory)** 중 하나를 선택할 수 있습니다.

LDAP 서버

LDAP 형식의 LDAP 서버의 IP 주소 또는 호스트 이름입니다.

> **힌트:** 필요한 경우 포트 사양을 URL 뒤에 쓸 수 있습니다 (예: ldap://192.168.0.20:389/). 표준 포트 389는 안전하게 생략할 수 있습니다.

바인드 DN 설정

이 설정은 LDAP 서버의 고유 이름, 즉 LDAP 트리 구조의 최상위 노드를 정의합니다.

바인드 DN 사용자 이름

DN을 쿼리하는데 사용할 사용자 이름입니다. 핫스팟 사용자의 자격 증명을 검색하고 인증해야 합니다.

바인드 DN 암호

앞의 옵션에서 지정한 사용자의 암호입니다. 오른쪽에 있는 체크 상자를 클릭하면, 문자가 표시되거나 숨겨집니다.

사용자 검색 필터

예제 HS1 - LDAP를 사용한 외부 인증.

LDAP 서버의 설정은 표준 Active Directory 형식을 사용하여, 다음과 같이 채울 수 있습니다.

- DC가 도메인 컨트롤러입니다.
- OU는 조직 단위이며 DC 내의 개체 그룹입니다.
- CN은 OU에있는 사용자의 공통 이름입니다.

따라서 **ldap.example.org**에 있는 LDAP 서버의 **ACME** 도메인에 있는 **스태프** 조직의 사용자에게 핫스폿을 사용하도록 권한을 부여하려면, 다음 설정이 필요합니다.

1. *LDAP 서버:* ldap://ldap.example.com
2. *바인딩 DN 설정* ou = Staff, dc = ACME
3. *바인드 DN 사용자 이름* cn = admin, dc = ACME
4. *바인드 DN 암호* - 사용자 admin의 원격 암호 -
5. *사용자 검색 필터* (& (uid=%(u)s))

원격 LDAP 서버를 조회하는데 사용되는 문자열.

LDAP 백업 서버

기본 서버에 도달할 수 없을 때, LDAP 형식의 LDAP 대체 서버의 IP 주소 또는 호스트 이름을 사용합니다.

기본 비율

이 방법을 통해 인증하는 사용자와 관련된 비율입니다.

RADIUS 서버의 경우, 다음 구성 옵션을 사용할 수 있습니다.

RADIUS 서버

RADIUS 서버의 IP 주소 또는 URL입니다.

RADIUS 서버의 포트

RADIUS 서버가 수신하는 포트입니다.

식별자

추가 식별자.

공유된 비밀

사용할 암호.

RADIUS 백업 서버

기본 서버에 도달할 수 없을 때, 사용되는 대체 RADIUS 서버의 IP 주소 또는 URL입니다.

기본 비율

이 방법을 통해 인증하는 각 사용자와 관련된 비율입니다.

2. 위성 핫스팟 (Satellite hotspot)

위성 핫스팟은 구성을 저장하지 않지만, 마스터에 의존하여 사용자 데이터, 티켓 가용성 및 모든 설정을 확인합니다. 이 옵션을 선택하면, 마스터 핫스팟의 IP 주소와 암호를 VPN 터널 이름과 함께 지정해야합니다. 구체적으로 다음과 같은 옵션을 사용할 수 있습니다.

마스터 핫스팟 IP 주소

이 필드에 마스터 핫 스폿의 IP 주소를 지정합니다. 이 IP 주소는 일반적으로 마스터 핫스팟의 OpenVPN 서버 설정 (Menubar ‣ VPN ‣ OpenVPN server ‣ Server configuration 아래에 있음)에 정의된 특수 OpenVPN 서브넷 (구역 참조)에서 사용할 수 있는 첫 번째 IP 주소입니다.

마스터 핫스팟 암호

마스터 핫스팟 암호. 일반적으로 마스터에서 자동 생성됩니다. 암호 마스크를 표시하려면, 표시 확인란을 클릭하십시오.

핫스팟 VPN 터널

이 드롭 다운 메뉴에서 마스터 핫스팟에 연결하는데, 사용되는 OpenVPN 터널을 선택합니다.

> **추가 참고사항:** 마스터/위성 핫스팟 설정은 *이 문서 <https://help.endian.com/hc/en-us/articles/115012672027>*에 설명되어 있습니다.

3. 외부 RADIUS 서버

이 구성에서 핫스팟은 그것의 활동을 FreeRadius와 같은 외부 RADIUS 서버에 의존합니다. 이 서버는 계정, 설정, 티켓팅 및 연결에 대한 모든 데이터를 저장하는 RADIUS 서버에 연결하고, 인증을 요청합니다. IP 주소, 암호 및 포트, 대체 서버의 IP 주소와 같은 올바른 기능을 위해서는 RADIUS 서버에 대한 몇 가지 정보가 필요합니다. 또한 외부 포털을 사용할 수 있습니다.

RADIUS 서버 IP 주소

외부 RADIUS 서버의 IP 주소.

RADIUS 서버 암호

RADIUS 서버의 암호입니다. 표시 확인란을 클릭하여 암호를 표시하십시오.

폴백 RADIUS 서버 IP 주소

대체 외부 RADIUS 서버의 IP 주소입니다.

RADIUS 서버 AUTH 포트

RADIUS 서버 AUTH (인증) 포트 번호.

RADIUS 서버 ACCT 포트

RADIUS 서버 ACCT (Accounting) 포트 번호입니다.

RADIUS 서버 COA 포트

RADIUS 서버 COA (권한 변경) 포트 번호.

> **힌트:** RADIUS 포트의 기본값은 **1812** (AUTH), **1813** (ACCT) 및 **3799** (COA)입니다.

외부 포털 사용

이 옵션을 선택하면, 사용자가 핫스팟을 통해 연결할 때, 볼 수 있는 로그인 인터페이스로 외부 포털을 구성할 수 있습니다. 외부 포털은 호환 가능하고 칠리(chilli)와 통신해야 합니다. 외부 포털을 활성화하려면, 다음 옵션을 구성해야 합니다.

외부 포털 URL

포털의 위치입니다.

NAS ID

포털을 식별하는 RADIUS 서버의 네트워크 액세스 서버 ID입니다.

UAM 비밀

외부 RADIUS 서버에서 UAM 공유 비밀. 이 옵션에 대한 값을 정의할 수는 없지만, 보안을 향상시키기 때문에 이 옵션을 정의하는 것이 좋습니다.

허용된 사이트 / 액세스

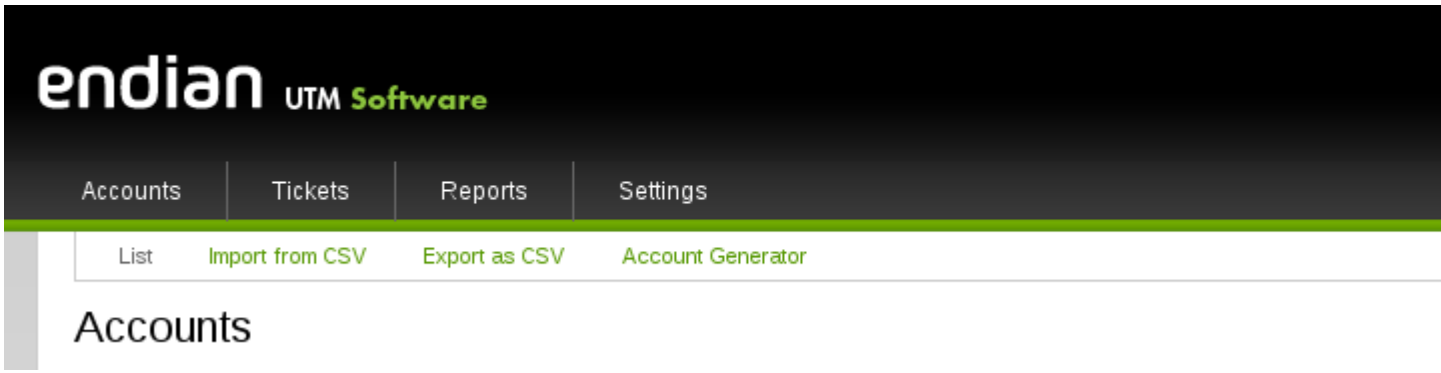
핫스팟에 등록하지 않아도 액세스 할 수 있는 웹 사이트 목록.

AnyIP 사용

활성 DHCP 클라이언트가 없는 클라이언트가 핫스팟에 연결할 수 있습니다.

> **참고:** RADIUS 서버의 설정은 이 작업에서 지원을 제공하지 않는 Endian의 범위와 임무를 벗어나는 것이므로 여기에서 설명하지 않습니다.

관리 인터페이스



핫스팟 관리 메뉴 바

이 섹션에서는 핫스팟의 핵심 구성 요소에 대해 설명하고, 계정, 티켓 및 티켓 요금을 관리하며, 보고서를 작성하고, 핫스팟을 구성하는 방법을 설명하는 페이지를 포함합니다. 이 그래픽 인터페이스는 다른 모듈과 디자인을 공유하지만, 완전히 새로운 메뉴 구조를 포함하고 있습니다. 복잡성과 수많은 구성 옵션을 사용하면, 다른 레이아웃을 사용해야 합니다. 선택은 핫스팟을 Endian UTM 어플라이언스의 독립 모듈로 간주하여, Endian UTM 어플라이언스의 다른 모든 주요 섹션과 공통인 표준 메뉴 바를 위의 그림에서 처럼, 2개의 부분으로 구성된 새로운 섹션으로 대체하는 것이었습니다. 위쪽 부분은 관리 인터페이스의 여러 부분에서 변경되지 않고, '적절한' 메뉴를 포함하며, 아래쪽 부분은 관리 인터페이스의 섹션이 선택된 것에 따라 변경되는 하위 메뉴입니다.

4개의 주요 섹션 각각은 하나의 핫스팟 구성 요소를 관리합니다.

계정 - 사용자 계정을 생성, 관리, 가져 오기 및 내보내기합니다.

티켓 - 요금을 정의하고 티켓을 생성합니다.

보고서 - 다양한 잔액, 연결 및 트랜잭션 로그를 참조하십시오.

설정 - 웹 인터페이스의 모양을 변경하고, SmartConnect™, 소셜 계정을 설정하며, API를 활성화하여, 모든 기능을 구성합니다.

맨 오른쪽에는 메인 메뉴가 기본 대시 보드 및 메뉴 모음으로 돌아갈 수 있습니다.

계정(Accounts)

핫스팟 관리 인터페이스의 이 섹션에는 핫스팟의 클라이언트를 생성, 삭제 및 관리할 수 있는 목록, CSV에서 가져 오기, CSV로 내보내기 및 계정 생성기의 네 가지 하위 메뉴 항목이 있습니다.

목록(List)

이 페이지는 기본적으로 *Username/MAC Address, Name* (사용자의 성명, *Enabled* (계정 상태), *Creation Date* 및 *Valid until* 까지의 일부 정보와 함께 사용 가능한 사용자 계정의 목록을 표시합니다.

몇 가지 옵션들은 보기(View)를 사용자 정의할 수 있게 해줍니다.

정렬 기준(Sort by)

사용자는 상태를 제외하고, 위에서 언급한 필드 중 하나를 기준으로 정렬할 수 있습니다.

역순으로(Reverse order)

목록을 오름차순 또는 내림차순으로 정렬합니다.

사용 중지된 계정 숨기기

비활성화 된 사용자, 즉 존재하지만 핫스팟에 액세스 할 수 없는 사용자를 목록에서 숨깁니다.

검색

거대한 결과 집합에 페이지 매김을 사용할 수 있으므로 계정을 검색할 수도 있습니다.

> **참고:** 이 섹션에서 언급한 사용자는 인터넷에 액세스하고 찾아볼 수 있는 클라이언트 인 핫스팟의 사용자를 대상으로 합니다. 그러나 두 가지 유형의 사용자, 즉 관리자 및 계정 편집기가 있으며, 그 기능과 임무는 핫스팟 사용자 섹션에 설명되어 있습니다.

각 계정에서 몇 가지 조치를 사용할 수 있으며, 테이블의 오른쪽에 있는 각 계정에 표시됩니다.

티켓 수정 / 추가. 계정을 편집하고 티켓을 할당할 수 있습니다.

밸런스. 계정의 밸런스를 표시합니다.

연결. *계정의 모든 연결을 보여줍니다.*

삭제. 계정의 모든 연결을 삭제합니다.

인쇄. 계정의 자격 증명 (사용자 이름 및 암호)을 포함한 환영 메시지를 인쇄합니다. MAC 기반 계정에서는 이 작업을 수행할 수 없습니다.

> **참고:** 환영 메시지는 핫스팟 템플릿 (*Hotspot ‣ Adminstration Interface ‣ Settings ‣ Language*)에서 사용자 정의할 수 있습니다.

계정 관리 (예: 사용자 및 티켓 관리)가 이 섹션의 나머지 부분을 구성하는 동안, 밸런스와 연결을 보여주는 작업과 그것들의 관리 옵션이 보고서 섹션에 아래에 설명되어 있습니다.

새 계정은 사용자 이름과 암호를 지정하거나 MAC 주소를 제공하여 만들 수 있습니다. 두 작업 모두 계정 테이블 위의 해당 링크를 클릭하여 수행할 수 있습니다.

각 계정과 관련된 데이터는 **로그인 정보, 계정 정보** 및 **티켓**의 세 가지 유형으로 구분됩니다. 계정 정보와 티켓은 완전히 동일하지만 로그인 정보는 두 가지 유형의 계정에서 약간 다릅니다.

계정 추가를 클릭하면, 사용자 이름과 암호가 필요한 새 계정을 만들 수 있습니다. 일부 설정은 기본값에서 수정할 수 있습니다. 설정 섹션의 만료 일자 ('유효 기간'), 계정 활성 여부, 언어 및 대역폭 제한 (kb/s)을 참조하십시오. Hotspot (핫스팟) ‣ Admin interface ‣ Settings ‣ Language (*Hotspot ‣ Admin interface ‣ Settings ‣ language*.)에서 활성화된 언어 중에서 언어를 선택할 수 있습니다.

MAC 기반 계정 추가를 클릭하여 MAC 기반 계정을 만듭니다. 따라서 MAC 기반 계정은 장치에 연결되며, 사용자 이름과 암호는 필요하지 않습니다. 나머지 설정은 이전과 동일하지만, MAC 기반 주소에도 고정 IP 주소를 지정할 수 있습니다.

각 계정에 다음 데이터를 연결할 수 있습니다.

로그인 정보

이 상자에는 새로 생성된 계정과 관련된 정보와 핫스팟 액세스 및 사용에 필요한 정보가 들어 있습니다.

사용자 이름

계정과 연결된 사용자 이름입니다. 비워두면 임의의 사용자 이름이 생성됩니다.

암호

필드를 비워두면 시스템에서 자동으로 생성할 수 있는 새 계정의 암호입니다.

> **참고:** 암호는 핫스팟에 액세스하기 위한 자격 증명을 사용하여, 사용자에게 넘겨줄 메시지를 인쇄할 때만 나타납니다.

MAC 주소

계정을 식별하는 사용되는 MAC 주소입니다. MAC 기반 계정에만 사용할 수 있습니다.

~까지 유효 (유효기간)

계정이 만료되는 날짜. 1년 또는 365의 기본값은 설정에서 변경할 수 있습니다. 현재 계정의 값을 변경하려면 DD.MM.YYYY 형식으로 새 날짜를 제공하거나 ... 단추를 클릭하고, 달력 팝업에서

새 날짜를 선택하십시오.

활성화?

체크 박스가 선택되면, 계정이 활성화되어 핫스팟에 액세스 할 수 있습니다.

언어

드롭 다운 메뉴에서 사용자가 모든 핫스팟의 메시지를 볼 때 사용할 언어를 선택하십시오.

대역폭 제한

체크 박스를 선택하면, 계정의 대역폭이 제한됩니다. 두 개의 새로운 필드를 사용하여 계정에 대한 업로드 및 다운로드 제한을 KB/s 로 설정할 수 있습니다. 이를 비워두면, 전역 설정이 사용됩니다 (설정된 경우).

SmartLogin 사용

확인란을 선택하면, 사용자가 핫스팟의 SmartLogin 기능을 이용할 수 있습니다. MAC 기반 계정에는 이 옵션을 사용할 수 없습니다.

SmartLogin 쿠키 수명

이 옵션은 SmartLogin 이 활성화된 경우에만 나타납니다. smartlogin 에서 사용하는 쿠키가 클라이언트에 상주할 날의 시간입니다.

정적 IP 주소

이 옵션은 여기에 지정된 고정 IP 주소에 연결할 수 있는 MAC 기반 계정에서만 사용할 수 있습니다.

> **경고:** 사용자 이름과 같은 일부 계정의 기존 로그인 정보를 변경하면, 새 계정이 만들어지게 됩니다.

계정 정보

이 상자에는 계정 소유자와 관련된 모든 개인 정보가 들어 있습니다.

직함

그 사람의 직함 (예: Mrs., Dr.).

이름

사용자의 이름.

성

사용자의 성입니다.

거리

사용자가 거주하는 거리.

ZIP (우편번호)

사용자의 고향의 우편 번호입니다.

도시

사용자가 유입한 도시 또는 마을.

국가

사용자가 유입되는 국가는 드롭 다운 메뉴에서 선택해야 합니다.

이메일 주소

계정과 관련된 전자 메일 주소입니다. 전자 메일 주소는 제한없이 계정 편집기에서 변경할 수 있습니다.

> **참고:** 이미 등록된 이메일 주소는 새로운 SmartConnect™ 계정에 사용할 수 없습니다.

전화 번호

계정과 연결된 전화 번호입니다. 국가 코드는 왼쪽에 있는 드롭 다운 메뉴에서 선택할 수 있으며, 숫자는 오른쪽 텍스트 상자에 작성해야 합니다.

생일

사용자의 생일.

태어난 도시

사용자가 태어난 도시 또는 마을.

문서 유형

사용자를 식별하는데 사용된 문서 유형입니다. 드롭 다운 메뉴에서 **출생 증명서, 신분증, 여권** 및 **운전 면허증**의 네 가지 유형의 문서를 사용할 수 있습니다.

문서 ID

사용자를 식별하는데 사용된 문서의 ID입니다.

> **참고:** 일부 국가에서는 문서를 수집하여 공개 핫스팟에 액세스해야 할 수도 있습니다.

~에 의해 발행된 문서

문서 발행자 (예: 뉴욕시).

성별

사용자의 성별입니다. **알 수 없음, 남성, 여성** 및 **기타** 네 가지 값을 사용할 수 있습니다.

버전 5.0의 새로운 기능.

회사

사용자가 속한 회사.

버전 5.0의 새로운 기능.

직위

사용자의 직위.

버전 5.0의 새로운 기능.

설명

계정에 대한 추가 설명.

티켓

이 상자를 사용하면 현재 계정과 관련된 티켓을보고 관리할 수 있으며 다음 옵션들이 표시됩니다.

새 티켓 추가

드롭 다운 메뉴에는 사용 가능한 티켓 요금이 표시되며 트래픽 기반 시간대인 경우 표시됩니다.

> **참고:** 시간 기반 트래픽 기반 티켓과 트래픽 기반 티켓을 혼합할 수 없으므로, 사용자가 이미 하나 이상의 시간 기반 티켓을 가지고 있는 경우에 트래픽 기반 티켓을 추가할 수 없으며, 그 반대의 경우도 마찬가지입니다.

효력

사용 가능한 티켓 요금을 한 번 선택하면, 이 옵션이 표시되어 티켓 유효 기간을 사용자 정의할 수 있습니다. 사용 가능한 값은 티켓 가격 생성 중에 정의된 것과 동일하며, 티켓의 기본값 (텍스트 상자 및 아래의 드롭 다운 메뉴로 표시)보다 우선합니다.

추가

티켓이 선택되면, 이 버튼을 클릭하여, 현재 계정에 연결할 수 있습니다.

> **참고:** 기존 계정을 편집할 때, 인쇄 버튼을 클릭하여, 자격 증명이 포함된 시작 메시지를 인쇄할 수도 있습니다. 이것은 계정 목록에서 수행할 수 있는 동일한 작업입니다.

상자 하단에는 작은 표에 계정과 관련된 모든 티켓과 각 계정에 대한 몇 가지 정보가 표시됩니다. 티켓이 여전히 유효한 경우 삭제할 수 있지만 만료된 경우 티켓은 계정의 계정에 이미 저장되어 있으므로 그대로 유지됩니다 (잔액 및 계정에 대한 자세한 내용은 Reports를 참조하십시오).

선택한 티켓이 순환 티켓인 경우에는, 다음 옵션들이 있는 *유효성* 있는 드롭 다운 메뉴 대신 작은 양식이 표시됩니다.

시작일

티켓의 첫 번째 주기가 시작되는 날. 티켓 기간이 *매월*인 경우, 유효 기간의 첫 번째 달만 선택할 수 있습니다. 월별 주기가 있는 티켓의 경우에는, 실제로 기간의 시작이 월의 첫 번째 날인 반면, 마지막은 월의 마지막 날입니다.

종료일

티켓의 첫 번째 주기가 끝나는 날. 티켓 기간이 *매월*인 경우에, 유효 기간의 마지막 달만 선택할 수 있습니다.

이러한 otpion 아래에서, 변수 메시지는 티켓의 총 사이클 수, 주기 당 가격을 표시하고 티켓의 총 가격을 계산합니다. 일반 티켓의 경우와 마찬가지로 테이블은 계정과 관련된 순환 티켓의 목록을 유지 관리합니다. 명확하게 하기 위해이 테이블은 다른 테이블과 분리되어 있습니다.

CSV에서 가져 오기

CSV 파일에서 계정 이름을 가져올 때, 파일 이름은 중요하지 않습니다 (내보낸 파일에는 고유한 이름이 있습니다. 다음 절 참조). 고정된 형식의 필드가 필요합니다. 다음 옵션을 사용할 수 있습니다.

파일 선택

찾아보기 버튼을 클릭하여, 업로드 할 CSV 파일을 선택하십시오. 파일은 일반 텍스트여야 하므로

ZIP 보관 파일, GPG 암호화 파일 등이 허용되지 않습니다.

구분 기호

문자는 구분 기호로 사용되며, 일반적으로 쉼표 또는 세미콜론입니다. 제공되지 않으면, Endian UTM Appliance는 올바른 문자인지 추측합니다.

> **힌트:** Endian UTM 어플라이언스는 내 보낸 파일의 필드를 구분하기 위해 쉼표를 사용합니다.

CSV 파일의 첫 번째 행에는 열 제목이 있음

확인란을 체크하면, Endian UTM Appliance가 CSV 파일의 첫 번째 행에 열 헤더가 포함되어 있음을 알리고, 그것을 가져올 때 무시합니다.

> **참고:** Endian UTM Appliance가 CSV 파일로 인식하지 못하는 파일은 "*주어진 파일이 CSV 형식으로 보이지 않는다*"는 메시지와 함께 거부됩니다.

계정 가져 오기

CSV 파일을 가져오려면, 이 버튼을 클릭하십시오.

계정을 가져오면, 페이지는 파일에서 발견된 계정 수에 따라 일부 열을 포함하는 새로운 파일로 대체됩니다. 첫 번째 열은 사용 가능한 모든 필드를 포함하고, 두 번째 필드는 CSV 파일에서 인식된 모든 필드를 포함합니다.

> **힌트:** 첫 번째 열의 모든 레이블이 빨간색 배경이고, 두 번째 열의 레이블이 녹색 배경인 경우, 데이터를 제대로 가져왔습니다.

나머지 열은 파일의 내용과 파일의 데이터 해석 방법을 보여줍니다. 인식되지 않은 모든 필드는 노란색으로 표시됩니다. 가장 왼쪽 열의 빨간색 레이블을 두 번째 열의 노란색 필드로 드래그하여 사용 가능한 필드와 연결할 수 있습니다.

> **참고:** 이러한 열의 데이터는 수정할 수 없으므로 잘못된 것이 있으면, 이전 페이지로 돌아가서 가져 오기 프로세스를 중지하고, 가져 오기를 다시 시도하기 전에 CSV 파일을 수정하십시오.

표 아래에 다음 옵션이 표시됩니다.

가져온 계정을 확인하시겠습니까?

확인란을 선택하면, 새 계정을 실제로 가져오고, 저장하기 전에 계정 요약이 두 부분으로 나뉘어 표시됩니다. 페이지 상단에 새 계정이 표시되는 반면에, 하단에는 업데이트 될 계정이 표시됩니다.

계정들 저장하기

이 버튼을 클릭하면, Endian UTM Appliance에서 계정의 저장이 시작되고, 가져 오기 프로세스가 끝납니다.

> **힌트:** 위의 확인란이 선택된 경우, 요약을 표시한 후에, 이 버튼을 다시 클릭하여, 가져 오기 프로세스를 완료하십시오.

> **경고:** 사용자의 로그인 정보 중 하나를 수정하면, 새 계정이 만들어집니다. 일부 로그인 정보에서 기존 로그인 정보와 약간 다른 계정만 가져오는 경우에도 마찬가지입니다. 나중에 잠재적인 문제를 피하기 위해, 그들을 가져오기 전에 검사해야 합니다.

CSV에서 내보내기

기존 계정 목록을 CSV 형식으로 내보내고 저장할 수 있습니다. 목록을 내보낼 때, 내보낸 파일에 표시되는 필드는 고정되어 있으므로 파일을 열 것인지 (보기) 또는 저장할 디렉토리만 결정할 수 있습니다. 편의를 위해, 파일 이름은 accounts_YYYYMMDD_HHMM으로 저장됩니다. 여기서 YYYYMMDD는 년, 월, 일을 나타내고, HHMM은 목록을 내보낼 때의 시간과 분을 나타냅니다. 이 선택 사항은 내 보낸 파일이 저장된 디렉토리에서 사전 순으로 나열되도록 합니다. 그러나 파일 이름은 자유롭게 수정할 수 있습니다. 내 보낸 파일을 백업으로 사용하고 나중에 가져올 수 있습니다.

> **경고:** 내보낸 목록에는 일반 텍스트로 된 사용자의 암호도 들어 있으므로 안전한 장소에 보관하십시오.

계정 생성기

계정 생성기의 사용은 디폴트 티켓이 이미 할당되어, 다수의 새로운 계정을 생성할 필요가 있고, 따라서 예를 들어, 사용자 그룹에 넘겨줄 수 있는 경우에 특히 유용할 수 있습니다. 예를 들어, 많은 사람들이 핫스팟에 액세스하고 작은 시간 간격으로 자격 증명을 수신해야 하는 컨퍼런스 또는 컨벤션과 같은 이벤트가 시작되는 시점의 등록 단계를 고려하십시오.

이 페이지는 네 개의 상자로 나뉩니다. 첫 번째 세 개는 계정 생성기를 구성하고, 네 번째 페이지는 생성된 대량 계정 목록으로, 적어도 일부 대량이 이미 생성된 후 페이지 하단에 표시됩니다.

계정 생성기는 아래에 설명된 사용자 이름, 암호 및 설정의 세 부분으로 그룹화된 몇 가지 공통 옵션만 제공하여, 특정 수의 계정을 한 번에 만들 수 있습니다.

사용자이름(Username)

두 가지 유형의 사용자 이름 생성기가 있습니다: **순차(Sequential)** 및 **무작위(Random)**, 둘다 두 가지 공통 옵션을 공유합니다

접두사

대량의 모든 계정에서 공유하는 사용자 이름의 시작 부분입니다. 빈 접두사도 사용할 수 있습니다.

길이

사용자 이름의 전체 길이입니다.

예제 HS2 - 여러 계정 생성.

이 예제에서는 동일한 공통 설정을 사용하는 4개의 계정 출력에서 순차 생성기와 임의 생성기 간의 차이점을 보여줍니다.

- 사용자 이름 접두사: **사용자** (4자).
- 사용자 이름 길이: **8**자 (따라서 4자 이상 입력해야 함)
- 암호 길이: **8**자.
- 캐릭터 세트: **모두**.

순차 사용자 이름 생성기를 사용하여, *시퀀스 시작* 옵션이 **10**으로 설정됩니다. 결과 출력 (사용자 이름/비밀번호)은 다음과 같습니다.

사용자 이름에 필요한 8 자 길이에 도달하기 위해 두 개의 **0**을 사용합니다.

Extra를 제외한 모든 *문자 세트*를 가지고, *임의의* 사용자 이름 생성기를 사용하면, 결과 출력 (사용자 이름 / 비밀번호)은 다음과 유사합니다.

> **참고:** 길이는 접두사보다 길어야 하며, 그렇지 않으면 오류 메시지가 표시됩니다.

사용자 이름은 두 생성자에 대해 다르게 완료됩니다. 순차적 생성기의 경우, 증가하는 숫자가 사용되며 옵션으로 정의됩니다.

시퀀스 시작

시퀀스가 시작되는 숫자 또는 숫자입니다.

> **힌트:** 필요한 길이에 도달하기 위해 접두사 길이와 시퀀스 외에도 더 많은 문자가 필요한 경우 _strong : 0이 추가됩니다. (예제 HS2 참조).

무작위 생성기의 경우, 선택한 문자 세트에서 대문자와 소문자, 숫자 및 추가 문자 (아래 참조) 중에서 선택된 문자가 사용됩니다.

암호

여기에 계정과 관련된 암호가 생성됩니다. 다음 옵션을 사용할 수 있습니다.

길이

암호를 만들기 위해 얼마나 많은 문자 길이가 필요한지 지정합니다.

문자 집합

무작위 암호를 생성하는데 사용할 문자 범주를 선택할 수 있습니다. 그것들은 다음과 같습니다.

- 대문자 (A-Z)
- 소문자 (a-z)
- 숫자 (0-9)
- 추가 문자 (._- +)

> **참고:** 암호의 강도는 길이 및 사용되는 문자 qq세트의 수에 따라 다릅니다. 일반적으로 8자의 긴 암호와 모든 문자 집합을 선택하면, 48 비트 암호가 생성되므로 대부분의 경우 충분합니다.

설정

생성된 계정에 대한 추가 옵션:

생성할 계정 수

얼마나 많은 새 계정을 만들 수 있는지 지정합니다.

계정 사용

즉시 사용 가능한 계정을 만들려면, 확인란을 선택하십시오.

지정된 티켓

드롭 다운 메뉴에서 티켓을 계정에 할당해야 합니다.

계정 만료 (일)

계정이 유효한 기간을 선택하십시오. 기본값은 1년 또는 365일입니다.

언어

계정에 메시지 및 인터페이스를 표시하는데 사용할 기본 언어를 선택하십시오.

지정된 설정으로 사용자를 생성하려면, `계정 생성` 버튼을 클릭하십시오. 처음 5개의 사용자 이름 - 비밀번호 조합의 샘플이 나타납니다. 전체 대량 사용자 생성은 `확인`을 클릭한 후에만 생성됩니다. 그렇지 않으면, `취소`를 클릭하여 전체 작업을 삭제합니다.

대량의 계정을 처음 생성하면, 페이지가 확인 메시지와 함께 다시 로드되고, 계정 생성기 아래에 생성된 계정에 대한 정보가 포함된 새 테이블이 표시됩니다. 특히 다음 열이 표에 나와 있습니다.

날짜

계정이 생성된 날짜입니다.

생성된 사용자

생성된 사용자 수입니다.

작업들

각 일괄 처리에는 세 가지 작업(Actions)이 있습니다.

- *Load settings,* 계정들을 만드는데 사용한 설정을 로드하고, 새 계정을 재사용하여 새 계정을 대량으로 생성합니다.
- *Delete users,* 그 생성에서 만들어진 모든 사용자를 제거합니다. 이 작업을 수행하면, 아직 연결되지 않았거나 남은 크레딧이 없는 사용자만 삭제되며, 핫스팟에 이미 연결되어 있거나 크레딧이 남아있는 사용자는 삭제되지 않습니다.
- CSV 형식으로 사용자이름 / 암호 조합을 내보내려면 *CSV로 내보내십시오.* 이것은 선불 카드에 데이터를 인쇄하는데 유용합니다.

티켓

이 섹션에서는 티켓 (및 티켓이 기반으로 하는 요금)을 관리하기 위한 목적으로 사용됩니다.

주기적인지 아닌지, 시간 기반인지 또는 트래픽 기반인지 여부를 나타냅니다. 옵션은 *티켓* 하위 메뉴인 *요금, 빠른 티켓* 및 *티켓 생성기*의 세 가지 범주로 그룹화됩니다.

요금

Endian UTM Appliance는 요금 추가 링크를 클릭하여 특정 페이지에서 여러 요금을 정의할 수 있는 가능성을 제공합니다. 여기에서 지불금 (후불과 선불), 측정 (교통량과 시간 기준), 가격 및 순환 옵션의 다양한 조합을 선택하여 다양한 유형의 티켓을 생성할 수 있습니다.

특히 요금의 가격에 대해 후불 결제를 사용하면, 1시간 (시간 기준) 또는 10MB (트래픽 기반) 당 가격을 정의할 수 있습니다. 대신 선불 결제 방식을 사용하면, 보다 정확한 가격과 단위까지 정의할 수 있습니다. 이 경우에, 실제로 시간 (분, 시간 또는 일) 또는 트래픽 (Mb 또는 Gb 단위)과 티켓 가격 또는 단가가 제공될 수 있습니다.

> **참고:** 티켓 가격을 입력할 때, 단위 당 가격이 자동으로 계산되며 반대의 경우도 마찬가지입니다. 이는 여러 선불 유형의 티켓을 제공할 때 유용하며, 예를 들어, 4개의 선불, 15분 소요 티켓의 비용은 1개의 선불, 1시간 소요 티켓보다 비쌉니다.

순환 티켓

순환 티켓은 핫스팟 사용자에게 제공할 수 있는 새로운 유형의 티켓입니다. 이것을 도입하게 된 아이디어는 사용자에게 일정 기간 (*주기*) 내에 동일한 양의 트래픽을 할당하는 것입니다. 이 양은 임의의 횟수 (*주기 기간*) 반복될 수 있습니다. 모든 사용자에게 한 번에 하나의 순환 티켓을 할당할 수 있습니다.

더 자세한 내용은 순환 티켓이 세 부분으로 구성됩니다.

1. 다른 요금과 마찬가지로, 시간의 합계 당 또는 트래픽의 MB 당 비용인 *요금(rate)*
2. 트래픽이 소비되어야 하는 동안, 1일, 1주, 1개월 또는 1년의 기간인 *주기 지속 기간(cycle duration)*
3. 티켓이 얼마나 많이 연속적으로 사용될 수 있는지 보여주는 *주기의 수(a number of cycle)*. 이 숫자는 핫스팟 관리자가 결정하며, 기본적으로 1입니다.

모든 유형의 항공권을 언제든지 구입하여 즉시 사용할 수 있지만, 한 가지 예외가 있습니다. *순환 기간*이 **매월**인 순환 티켓은 항상 *해당 월의 첫 번째 날*에 주기를 시작하고, *그 달의 마지막 날*에 만료됩니다. 예를 들어, 6월 20일에 구입한 월간 순환 티켓을 고려하십시오.

즉시 사용할 수 있지만, 첫 번째 주기는 6월 30일에 완료됩니다. 따라서 7월 1일에 이 티켓의 유효 기간을 시작하는 것이 좋습니다. 따라서 첫 번째 주기는 7월 31일에 만료됩니다.

순환 티켓은 선불로만 구매할 수 있습니다. 즉, 미리 구매해야 합니다. 한 주기 내의 잔여 트래픽은 다음 주기에 추가되지 **않습니다**. 즉, 주기가 끝나기 전에 사용해야 하거나 그렇지 않으면 손실됩니다. 빠른 티켓, 스마트 연결 티켓, 티켓 생성기 및 계정 생성기에는 순환 요금을 사용할 수 없습니다. 기존 사용자 또는 새로운 사용자의 생성 기간 중에 명시적으로 할당해야 합니다.

티켓은 SmartConnect ™ 트랜잭션 (아래 참조)에서 사용할 수 있습니다.

요금 추가(Add Rates) 링크를 클릭할 때, 정의할 수 있는 옵션에 해당하는 여러 열로 구성된 테이블에서 *티켓* 페이지를 열 때 사용할 수 있는 티켓 유형이 표시됩니다. 튜플(tuples)은 표 위에 있는 드롭 다운 메뉴를 사용하여 *요율 이름*, *지불* 또는 *측정 모드*로 정렬할 수 있습니다. *역순*으로 확인란을 선택하면, 주문 기준을 반대로 할 수 있습니다. 특정 요율 이름을 검색하거나 그 중에서 필터링하려면, 적어도 하나 이상의 문자가 있는 테이블 상단에 있는 입력 양식을 채우고, Enter 키를 누릅니다.

새 **보통** 요금을 정의할 때, 다음 옵션을 사용할 수 있습니다. 순환 티켓에는 몇 가지 옵션을 사용할 수 있습니다. 자세한 내용은 아래를 참조하십시오.

평가 이름

티켓 요금에 주어진 이름입니다.

티켓 코드

티켓 요금에 대한 ASA 코드. ASA 호텔 관리 시스템에만 사용되지만, 이 필드는 필수 항목입니다.

> **힌트:** ASA 시스템을 사용하지 않는 경우, 요금 이름에 사용된 동일한 문자열로 이 필드를 채웁니다.

요율 유형

보통 또는 **순환** 요금 중에서 선택하십시오. 순환 티켓의 정의는 여기를 참조하십시오.

스마트커넥트(SmartConnect)?

이 열은 본 요금이 SmartConnect™ 트랜잭션에 사용 가능한지 여부를 보여줍니다. 이 경우 목록에 ✔ 아이콘이 나타나고, 그렇지 않으면 ✖가 표시됩니다.

> **힌트:** 테이블에서 아이콘을 클릭하면 비율의 통계가 토글됩니다.

대역폭 제한?

요금에 고정된 대역폭 한도를 설정하려면 확인란을 선택하십시오. 활성화된 경우에는, 다음 두 옵션이 나타납니다. 순환 티켓에는 이 옵션을 사용할 수 없습니다.

다운로드

해당 요금에서 이용할 수 있는 가장 높은 다운로드 대역폭.

업로드

해당 요금에서 이용할 수 있는 가장 높은 업로드 대역폭.

빠른 티켓?

새로운 빠른 티켓을 만들 때, 이 요금을 사용하려면 확인란을 선택하십시오. 이 경우 티켓 목록에 ✔아이콘이 나타나고, 그렇지 않으면 ✖가 표시됩니다.

> **힌트:** 테이블에서 아이콘을 클릭하면, 요금의 상태가 토글됩니다.

지불

이 열은 요금에 **선불** 또는 **후불** 결제가 필요한지 여부를 보여줍니다.

측정 모드

이 열은 요율이 **시간 기반**인지 **트래픽 기반**인지 나타냅니다. 선택 항목에 따라, 다음 옵션 (**금액** 및 **가격**)이 변경됩니다.

총량

이 요금으로 단일 티켓을 만들 때, 사용할 수 있는 시간 또는 트래픽 양을 텍스트 필드에 입력하고, 드롭 다운 메뉴에서 시간 (분, 시간 또는 일 수) 또는 트래픽 (메가 바이트 또는 기가 바이트 수)을 선택하십시오. 단위는 **측정 모드**에 따라 사용 가능합니다.

효력

이 옵션은 이 유형에서 생성된 단일 티켓의 만료일을 정의하며 요율 편집기에서만 나타납니다. 드롭 다운 메뉴에서 선택할 수 있는 4가지 값은 다음과 같습니다.

- 항상, 무제한 유효성
- 티켓 생성에서 티켓 생성 유효 기간을 분, 시간, 일, 주 또는 개월 단위로 지정할 수 있습니다.

- 이전 티켓과 같이 티켓을 먼저 사용하지만 티켓이 핫스팟에 처음 액세스할 때 유효성이 시작됩니다.
- 하루가 끝날 때까지 티켓은 당일 이내에 사용되어야 합니다.
  이 값은 *계정(Accounts) ‣ 리스트(List) ‣ 티켓 편집/추가 (Edit/Add ticket) ‣ 티켓 추가 (Add ticket)*에서 사용자와 연결될 때, 사용자 별로 무시될 수 있지만, 생성될 새 티켓의 기본값이 됩니다.

가격

이것은 시간당 또는 10MB 당 가격과 이 요금에 대해 지정된 티켓 가격을 표시합니다. 요율 편집기에서 통합 가격 (10Mb 또는 1 시간)을 티켓 가격으로 신속하게 변환하는 두 개의 텍스트 상자가 나타납니다. 이는 정의된 변동 요금의 단위당 평균 가격을 제어하는데 유용합니다.

*요율 유형*을 **Cyclic**으로 선택하면, 요율 편집기가 약간 변경되어, *가격* 대신 다음 구성 옵션이 표시됩니다.

주기

요율의 한주기의 기간으로 **일일, 주간, 월간** 또는 **연간** 중 하나일 수 있습니다.

주기 당 가격

각 주기의 비용.

> **힌트:** 핫스팟 설정에서 통화를 변경할 수 있습니다 (*핫스팟(Hotspot) ‣ 관리 인터페이스 (Administration interface) ‣ 설정(Settings) ‣ 기본(Main)).*

기본 사이클 수

티켓 유효 기간의 기본 주기 수입니다. 지정되지 않으면, 값 1이 적용됩니다.

총 가격 예

주기 당 가격이 입력되면, 이 표는 관련주기 (예: 7일 또는 14일, 3 또는 6개월 등)에 대한 주기적 티켓의 총 가격을 계산합니다.

> **경고:** 티켓 요금을 저장 한 후에는 SmartConnect™ 트랜잭션의 요율 이름, 요율 코드 또는 사용 가능 여부만 수정할 수 있습니다. 다른 것을 변경하면, 회계 데이터에 불일치가 생길 수 있습니다. 요율에 대한 가격을 수정하려면, 기존 요율의 이름을 바꾸고 원래 요율로 새 요율을 만드십시오. 예를 들어, **시간당(hourly)** 요금이 수정되어야 하는 비용이 있다고 가정해 보십시오. 먼저 **오래된 시간당(OLD-hourly)** 요금과 같은 이름으로 이름을 변경한 다음, **시간당** 원래 이름으로 새 요금을 만듭니다.

빠른 티켓

이 페이지는 사용자 이름과 암호가 자동으로 생성되는 새로운 단일 사용자 계정을 만드는데 사용됩니다. 그렇게 하려면 선택적으로 사용자의 성과 이름을 입력한 다음 표시된 비율 중에서 원하는 비율을 클릭하십시오.

요율 버튼을 클릭하면, 사용자 이름, 비밀번호 및 요율이 화면에 표시됩니다. 이 시점에서 사용자의 언어 선택이 가능합니다. 이러한 회계 데이터는 정보 인쇄 버튼을 클릭하여 인쇄할 수 있습니다. 새 계정은 *핫스팟 ‣ 설정*에서 정의된 모든 기본 설정을 상속받으며 계정 페이지에 표시됩니다.

티켓 생성기

티켓 생성기를 이용하면, 미리 정의된 티켓 비율을 포함하여 공통 설정을 공유하는 특정 수의 티켓을 만들 수 있습니다. 이 옵션은 SmartConnect™에서 직접 핫스팟에 액세스하거나 데모 또는 평가 코드로 사용할 수 있는 고객을 위해 많은 선불 항공권 코드를 생성해야 하는 경우에 유용합니다. 그러나 여기에서 생성된 티켓을 사용하려면 고객을 등록하거나 새 계정을 만들어야 합니다.

티켓 생성기 페이지는 두 개의 상자로 나뉩니다. 위쪽에는 입력 양식을 채워 새 티켓을 빠르게 작성하고, 하단에는 이미 생성된 티켓 대량을 나열하는 테이블이 들어 있습니다. 적어도 대량의 티켓이 생성된 후에는, 생성된 티켓 표시를 클릭하여, 사용 가능한 모든 티켓을 표시할 수 있는 링크 (아래 참조)가 양쪽면에 나타납니다.

새 티켓을 생성하기 위해 생성기에서 사용할 수 있는 두 가지 옵션 그룹이 있습니다.

티켓 코드

> 대량의 티켓을 만들 때, 사용할 접두어 텍스트 (문자열), 티켓 이름의 길이 및 임의의 티켓을 생성하는 데 사용해야 하는 문자 집합을 정의하십시오.

설정

> 요금에 이미 있는 티켓 중에서, 생성해야 하는 티켓 수와 티켓에 할당해야 할 할당된 요금입니다.

지정된 설정으로 대량의 티켓을 생성하려면, 티켓 생성 버튼을 클릭하십시오. 처음 5개의 티켓 코드 조합 샘플이 나타납니다. 전체 대량은 확인(Confirm)을 클릭한 후에만 생성됩니다. 그렇지 않으면, 취소(Cancel)을 클릭하면 표시된 5개의 샘플도 삭제됩니다.

표 생성기 옵션 아래에, 이전에 생성된 모든 대량 티켓들이 다음과 같은 표 전체 열에 나열됩니다.

날짜

> 티켓이 생성된 날짜와 시간.

생성된 티켓

생성된 티켓 수입니다.

작업(Actions)

각 대량 작업에는 세 가지 작업(액션)이 있습니다.

- 설정로드. 해당 대량 생성 작업에서 사용된 설정을 사용하여 새 것을 생성하십시오.
- 티켓을 삭제하십시오. 해당 생성에서 만들어진 모든 티켓을 제거하십시오. 사용된 티켓만 삭제하십시오.
- CSV로 내보내기. 티켓 목록을 CSV 형식으로 내보냅니다.

생성된 티켓 표시 링크를 클릭하면, 생성된 모든 티켓이 있는 페이지가 표시되며, 티켓의 코드 또는 생성 날짜별로 정렬할 수 있습니다. 사용하지 않거나 만료된 티켓을 숨길 수 있습니다. 특정 코드는 *Code*: 레이블 옆에 있는 입력 양식을 사용하여 검색할 수도 있습니다.

표에는 사용자가 티켓을 사용했거나 할당한 티켓 코드 (any), 티켓 요금, 티켓 생성 날짜 및 사용되지 않은 단일 티켓 코드를 삭제하거나 사용중인 티켓 코드를 만료시키기 위한 옵션 링크가 표시됩니다. 테이블에 많은 수의 티켓이 포함되어 있으면, 목록을 분할하는데 페이지 매김을 사용할 수 있습니다.

보고서(Report)

보고서 섹션에는 핫스팟과 관련된 활동, 사용자, 티켓, 트래픽, 연결 및 회계 데이터에 대한 정보 및 통계가 있는 몇 개의 페이지가 있습니다. 이 섹션에서는 사용자의 통계와 연결 및 핫스팟 사용에 대한 자세한 보기를 제공하기 위한 목적으로 몇 가지 액션을 취할 수 있습니다.

> **참고:** 위성 핫스팟에서, 핫스팟 관리 인터페이스에서 이용할 수 있는 유일한 메뉴 항목은 *보고서(Reports)*입니다.

연결(Connections)

보고서 페이지를 열 때의 기본 보기는 어떠한 경우에도, 위성에 있는 연결을 포함하여 핫스팟에 대한 현재 활성 연결을 모두 보고하는 테이블을 표시하는 것입니다. 각 연결마다 다음 정보가 표시됩니다.

위성

이 Endian UTM Appliance가 마스터/위성 구성에서 마스터이고 (핫스팟 섹션의 역할에 대한 것보다 많음), 사용자가 위성에 연결되어 있다면, 원격 핫스팟 위성 시스템의 이름 (예: OpenVPN 계정 이름)입니다.

사용자 이름

연결된 계정의 사용자 이름입니다.

설명

연결된 계정에 대한 설명입니다.

인증됨

연결이 인증되었는지 여부를 표시합니다.

지속 기간

연결이 설정된 이후의 총 시간입니다.

유휴(IDLE) 시간

계정과 핫스팟 간에 트래픽이 감지되지 않은 이후에 경과한 시간의 양입니다.

IP 주소

핫스팟에 연결된 클라이언트의 IP 주소입니다.

MAC 주소

클라이언트의 연결된 인터페이스의 MAC 주소입니다.

작업(액션)

이 열(column)에서 *로그아웃*을 클릭하면 모든 활성 연결을 닫을 수 있습니다.

계정 잔액(Balance)

이 페이지에는 페이지 하단에 전체 요약이 따라오는 연결에 대한 정보가 표시되는 계정 목록을 포함합니다. `필터 기간`과 `열린 계정 항목`이라 불리는 두 가지 대체 보기들은 사용자의 잔액을 표시하는데 이용할 수 있으며, 전자가 기본 보기입니다. 그것들은 페이지의 맨 오른쪽에 있는 링크를 클릭하여, 상호 액세스 할 수 있습니다. 두 가지 보기에 표시된 실제 데이터는 다르지만, 다음과 같은 동일한 유형의 정보를 보고합니다.

사용자 이름

계정의 사용자 이름 또는 MAC 주소입니다. 사용자 이름을 클릭하면, 해당 사용자의 계정 균형 페이지가 열립니다. (아래 참조).

사용량

이 계정에서 사용된 금액입니다.

유료

이미 사용자가 지불한 돈.

지속 기간

이 사용자가 핫스팟에 연결된 시간입니다.

트래픽

이 계정에 의해 생성된 트래픽입니다.

표의 맨 위에서, 시작일과 종료일을 각각 *From*과 *Until* 필드에 쓸 수 있습니다: 오른쪽의 `Filter` 버튼을 클릭하면, 이 두 날짜 사이의 간격으로 제한된 통계를 보여주는 페이지가 다시 로드됩니다. 달력을 표시하여, 날짜 검색을 쉽게 하려면, 텍스트 필드의 오른쪽에 있는 `...`버튼을 클릭하십시오. 긴 목록을 분할할 때, 페이지 매김을 사용할 수 있습니다.

> **힌트:** 날짜 형식은 DD.MM.YYYY입니다. 예를 들어, 03.06.2017 (2017년 6월 3일) 같이 표시됩니다.

계정 항목의 대체 보기에는 위에서 언급한 것과 동일한 데이터가 표시되지만, 하나의 추가 열이 표시됩니다.

지불할 금액

해당 계정에서 아직 지불하지 않은 금액의 양.

두 가지 보기 중 하나에서, 사용자 이름 또는 MAC 주소를 클릭하면, 해당 계정에 대한 계정 잔액 페이지가 열리며 사용자의 티켓 및 결제에 대한 자세한 통계가 네 부분으로 그룹화됩니다. 이 페이지는 *Accounts (계정) ‣ [User list (사용자 목록)] ‣ [Actions (작업)] ‣ Balance (잔액)*에서도 접근할 수 있습니다.

사용자 정보

모든 사용자의 로그인 정보, 즉, 이름, 사용자 이름, 출생 도시 및 생일, 문서 ID 및 문서를 발행하는 당사자 등의 정보입니다.

계정 잔액

모든 시간 기반 관련 통계 다음에 트래픽 기반 통계가 따라오는 계정 잔액에 대한 자세한 정보입니다. 두 경우, 모두 사용자에게 할당된 전체 선불 및 후불 티켓과 사용된 총 시간 및 사용 가능한 총 시간 또는 트래픽이 표시됩니다.

후불 지불

이 열에는 두 개의 상자에 사용자가 이미 지불한 금액과 설정 페이지에 구성된 통화로 표시된 금액을 지불해야 한다는 내용이 표시됩니다. 하단의 상자는 모든 것이 이미 지불된 경우에, 녹색 배경을 가지며 그렇지 않은 경우에는 빨간색입니다. 두 상자 아래의 입력 필드에 금액을 입력하고, *신용 추가*를 클릭하여, 신용을 사용자에게 추가할 수 있습니다 (차변 해결 또는 단순히 트래픽 추가 구매 허용).

회계 항목

이 테이블은 페이지 하단에 있으며, 사용자와 관련된 티켓 목록을 포함합니다. 각 티켓마다 많은 정보가 표시됩니다.

티켓 이름

티켓 요금의 이름.

금액

이 계정과 관련된 대변 (녹색 배경) 또는 차변 (빨간색 배경)이 표시됩니다.

> **참고:** 사용자가 구입한 순환 티켓은 이 열에 여러 번 표시됩니다. *Cyclyc [이름]*이라는 티켓

이름으로 생성된 후에는 각 주기의 시작 부분에 *[이름]*이라는 금액의 티켓이 0.00 EUR (또는 핫스팟에서 사용된 통화로)가 회계에 추가됩니다.

날짜 시간

티켓 생성의 타임 스탬프입니다.

지속 기간

얼마나 많은 시간이 티켓에 사용되었는지를 지정합니다.

트래픽

티켓에서 소비한 트래픽입니다.

처리됨

티켓 사용 여부를 표시합니다.

다시 시도

이 옵션은 ASA 인터페이스에서 사용되며, 시스템이 이 항목을 계산하려고 시도한 횟수를 표시합니다.

메시지

사용자 지정 메시지.

순환 티켓인 각 항목에 대해, 메시지에는 다음 정보가 포함됩니다.

- *기간 ID*는 티켓을 고유하게 식별하는 점진적 숫자입니다.
- *사이클*: 및 주기 횟수는 티켓을 참조하고, 티켓 기간 및 주기 구입의 횟수를 나타냅니다.
- *시작일*과 *종료일*은 티켓의 유효 기간의 첫 번째와 마지막 날을 표시합니다.

사용자 정보 위의 *시작 날짜* 및 *종료 날짜* 필드를 채운 다음 (또는 팝업 캘린더에서 날짜를 선택하는 `...` 버튼을 클릭) `필터` 버튼을 클릭하면, 해당 기간의 통계만 표시될 것입니다.

현재 표시된 통계는 `>>>인쇄` 버튼을 클릭하여 인쇄할 수 있습니다.

연결 로그

이 페이지는 현재 및 과거 연결에 대한 여러 정보를 보여주는 표를 포함합니다. 항목은 두 열에 의해 (역순으로) 정렬될 수 있으며, 필터링 된 경우에도, 두 날짜 내에 설정된 연결만 표시할 수 있습니다. 표시된 정보는 다음과 같습니다.

사용자 이름

연결하는 사용자 이름입니다.

IP 주소

연결된 클라이언트의 IP 주소입니다.

MAC 주소

연결된 클라이언트 인터페이스의 MAC 주소입니다.

연결 시작

연결 시작 시간입니다.

연결 중지

연결 종료 시간.

다운로드

이 연결 중에 다운로드된 데이터의 양입니다.

업로드

이 연결 중에 업로드된 데이터의 양입니다.

지속 기간

연결 기간입니다.

CSV로 연결 로그 내보내기

하위 메뉴에서 `CSV로 연결 로그 내보내기` 링크를 클릭하면, 세부 정보와 관련된 정보가 포함된 연결 로그를 다운로드하거나 CSV 형식으로 저장할 수 있습니다. 로그 파일의 기본 파일 이름은 *hotspot-YYYYMMDD-FULL.csv*입니다. 여기서 YYYYMMDD는 파일이 만들어진 날짜이고, FULL은 파일에 모든 연결에 대한 세부 정보가 들어 있음을 나타냅니다.

> **경고:** 내보낸 목록에는 **일반 텍스트**로 된 사용자의 암호도 들어 있으므로, 안전한 장소에 보관해야 합니다.

SmartConnect 트랜잭션

이 페이지는 모든 SmartConnect™ 연결 및 거래의 목록을 보고합니다. 이 목록은 거래 ID 또는 주문 시간순으로 (역순으로) 정렬될 수 있습니다. 특정 거래는 *Search*.레이블 근처의 입력 양식에 일부 문자를 제공하여 검색할 수 있습니다. 표에 제공된 정보는 다음과 같습니다.

거래 ID

트랜잭션 식별 문자열. 주로 책임이나 고객의 티켓 등록 문제의 경우에 유용합니다. 모든 트랜잭션은 여기에서 조회할 수 있습니다.

주문 시간

거래 날짜와 시간.

지불

결제 완료되었는지 여부를 (무료 티켓은 항상 완료로 표시됨) 보여주며, 결재 상태를 나타냅니다.

사용자

생성된 계정의 사용자 이름으로, SMS 기반 SmartConnect™ 트랜잭션의 경우 전화 번호입니다.

전화 번호

계정 생성을 하는 동안에 제공된 전화 번호입니다.

SMS

계정 자격 증명이 있는 SMS는 엔디안 네트워크를 통해 핫스팟에서 전송됩니다. 어떤 이유로 든 메시지가 전송되지 않았거나 클라이언트가 메시지를 받지 못한 경우에, 이 필드는 실패를 표시하고 그렇지 않으면 성공을 표시합니다.

SMS 시간

SMS가 처리된 날짜와 시간.

이름

계정 생성시 제공된 이름입니다.

정보

계정 생성시 제공되는 주소, 우편 번호 및 국가 정보.

많은 항목이 있는 테이블에 페이지 매김을 사용할 수 있습니다.

추가 참고사항:

SmartConnect

Hotspot(핫스팟) ‣ Settings(설정) ‣ SmartConnect

설정

이 섹션에서는 핫스팟을 구성할 수 있는 모든 옵션을 메인화면, SmartConnect™, 소셜 네트워크, API 및 언어의 다섯 가지 기본 그룹으로 정렬합니다.

메인화면

이 페이지는 4 가지 부분으로 나뉘어 진 모든 시스템 설정을 포함합니다. 첫 번째 **Portal(포탈)**에서는 포털 모양의 기본값을 정의할 수 있습니다. 둘째, **전역 설정**을 사용하면 핫스팟의 다양한 부분에서 사용되는 옵션을 지정할 수 있습니다. 세 번째 **계정**에서는 계정에 대한 공통 옵션이 정의됩니다. 넷째, Quick Ticket에 사용된 **생성 암호에 대한 Character set(문자세트)**이 선택됩니다.

> **경고:** 포털 및 전역 설정의 일부 설정을 변경하면, 모든 연결 사용자가 강제로 로그 오프됩니다. 이러한 설정에는 GUI에 빨간색 별표가 표시됩니다.

포털

첫 번째 상자에는 사용자 정의할 수 있는 다음 옵션을 포함합니다.

방문(랜딩) 페이지

이 옵션은 핫스팟의 종속 포털을 사용하는 세 가지 방법 중 하나를 선택할 수 있게 해줍니다. 선택 항목에 따라 다른 옵션이 나타납니다.

로그인 포털. 이것을 선택하면, Endian UTM Appliance의 포털이 표시됩니다. 포털의 배경으로 사용할 웹 사이트와 로그인 양식을 다음 옵션을 통해 표시하려는 경우를 정의할 수 있습니다.

SurfNow 버튼이 있는 웹 사이트. 이 옵션을 선택하면, 네트워크에 로그인할 때, 입력한 웹 사이트가 사용자에게 직접 표시됩니다. 여러분이 해야 할 유일한 일은 사용자가 그것을 보고 핫스팟에 로그인 할 수 있도록 홈페이지에 SurfNow 버튼을 놓는 것입니다.

전체 자바 스크립트 통합 웹 사이트 - 이 옵션은 전문가만 사용할 수 있습니다. 그러나, 그것은 여러분이 자신의 웹 사이트와 핫스팟을 밀도있게 통합할 수 있게 할 것입니다. 웹 사이트에서 직접 사용자가 핫스팟에 로그인하고 로그인한 후 원하는 URL을 열 수 있습니다. 유일한 옵션은 다음과 같습니다.

웹 사이트에 *SurfNow 버튼* 또는 *JavaScript API*를 통합하는 방법

*SurfNow 버튼*과 *JavaScript API*는 핫스팟을 웹 사이트에 직접 통합하는 훌륭한 방법입니다. 어떻게 하는지 방법은 여기에 있습니다.

- *SurfNow 버튼*의 경우, 이 스니펫과 같은 것을 웹 사이트 코드에 추가하기만 하면 됩니다.

```
<button onclick="window.open('http://hotspot.endian.com/', '_self')">
Surf Now</button>
```

- JavaScript API를 통합하려면, 더 깊은 지식이 필요합니다. API를 통해 웹 사이트에서 직접 호출할 수있는 다음 기능에 액세스 할 수 있습니다.
  - window.parent.hotspotAPI.showLoginPage ( ) 핫스팟의 통합 로그인 대화 상자를 엽니다.
  - window.parent.hotspotAPI.connectWithCredentials(username, password) 통합 로그인 대화 상자를 열지 않고 직접 로그인을 수행합니다. 찾아보기 시작 대화 상자가 나타납니다.
  - window.parent.hotspotAPI.changeStartBrowsingUrl(url) 검색 시작 버튼을 클릭하면, 지정된 URL로 열리는 URL을 변경합니다.

로그인 포털 배경 URL

핫스팟 로그인 포털의 백그라운드로 사용되는 URL입니다. 로그인 포털이 방문 페이지로 선택된 경우에만 사용할 수 있습니다.

여러분의 웹 사이트 URL

사용자 로그인시 표시될 맞춤 URL입니다. SurfNow가 포함된 웹 사이트 버튼이 방문 페이지로 선택된 경우에만 사용할 수 있습니다.

로그인 양식 표시

핫스팟 로그인 양식이 표시되면, 드롭 다운 메뉴에서 선택하십시오.

- *즉시(immediately).* 로그인 양식은 백그라운드 홈페이지에 즉시 표시됩니다.
- *수동으로(manually).* 배경 홈페이지가 나타나고 등록 없이도 열람할 수 있습니다. 사용자는 화면 상단의 탐색 줄에서 언제든지 등록 페이지에 액세스 할 수 있습니다. 다른 사이트에 액세스하려면 등록 또는 로그인이 필요하지만 허용된 사이트 (아래 참조)에 나열된 사이트는 항상 액세스할 수 있습니다.
- x 초가 지나면 백그라운드 홈페이지에 사용자가 지정한 초 후에 로그인 폼이 표시되고, 탐색 막대에 등록 시간이 임박한 것으로 사용자에게 통보됩니다.

로그인 성공 후 웹 사이트

로그인 성공 후 사용자에게 표시될 웹 페이지의 URL입니다.

모바일 장치용 미니 포털 사용

체크 박스를 선택하면, 자바스크립트가 없는 포털 유형과 모바일 장치용으로 포털 유형이 추가로 활성화됩니다. 사용자는 핫스팟의 포털에 액세스할 때, 이 세 가지 중에서 선택할 수 있습니다.

허용된 사이트

인증없이도 액세스 할 수 있는 사이트 또는 IP 주소 목록. 한 줄에 하나의 사이트가 도메인 이름 (예: www.endian.com) 또는 프로토콜 형식의 문자열로 허용됩니다: IP[/mask]:포트 (예: **tcp:192.168.20.0/24:443**).

> **참고:** 웹 사이트가이 목록 외부의 사이트에서 위젯, 자바 스크립트, CSS 또는 기타 구성 요소를 통합하는 경우, 올바르게 표시되지 않을 수 있습니다.

전역 설정

핫스팟 이름

핫스팟을 식별하기 위해 제공된 이름입니다.

페이지 당 항목

페이지 매김 값, 즉 표시되는 페이지 당 목록 또는 표의 최대 항목 수입니다.

통화

핫스팟에서 모든 지불 계산에 사용된 통화입니다.

> **참고:** 일부 통화는 PayPal에서 지원하지 않으므로, SmartConnect 티켓에는 사용할 수 없습니다.

인기있는 국가

인기 국가는 등록시 사용자에게 제공되는 국가 목록에서 가장 먼저 등록되어, 등록에 필요한 시간을 줄여줍니다.

AnyIP 사용

이 옵션은 DHCP를 사용하지 않는 클라이언트를 지원하고, Hotspot의 IP 서브넷 (즉, BLUE 구역)에 속하지 않는 고정 IP가 있는 경우에도 Hotspot에 액세스할 수 있게 해주는 AnyIP 기능을 활성화합니다.

대역폭 제한

사용자 당 기본 업로드 및 다운로드 제한은 킬로바이트/초입니다. 이 필드가 비어 있으면, 아무 제한도 적용되지 않습니다.

> **참고:** 1킬로바이트는 8킬로비트에 해당하므로, 필드에 적절한 값을 입력해야 합니다.

DHCP 동적 범위

확인란을 선택함으로써, 이 옵션을 사용하면 핫스팟에 연결된 장치에 동적 IP 주소가 할당됩니다.

동적 IP 범위

이 옵션은 이전 옵션이 활성화되어 있을 때 나타납니다. Blue 구역 내에서 IP 주소의 사용자 정의 범위를 지정하여, 핫스팟의 클라이언트에 동적으로 할당할 수 있습니다.

계정

핫스팟 사용자의 익명 로그인.

사용자 인증없이, 익명의 로그인을 허용할 수 있지만, 모든 사용자에게 서비스 약관에 동의하도록 요구할 수 있습니다. 이렇게 하려면, 먼저 **후불 유형**의 티켓을 만든 다음, **로그인 할 때 사용자 인증 필요** 옵션을 비활성화하고, **사용자가 '서비스 약관'에 동의하도록 요구하는 것을 활성화**해야 합니다. 후불 티켓이 지정된 유효 기간과 함께 생성된 경우에는, 해당 기간이 지나면 사용자는 다시 서비스 약관에 동의해야 합니다.

사용자 인증 필요

핫스팟에 액세스하는 클라이언트가 유효한 등록된 계정을 필요로 하는 경우에는 체크 박스를 선택하십시오.

사용자가 로그인시 '서비스 약관'에 동의하도록 요구하십시오.

이 옵션을 선택하면, 사용자는 로그인하기 전에 서비스 약관에 동의해야 합니다.

기본 언어

새 사용자에게 기본적으로 사용되는 언어입니다.

버전 5.0의 새로운 기능.

비밀번호 복구

자신의 자격 증명을 분실했거나 잊어 버린 사용자가 재설정 할 수 있게 해줍니다. 세 가지 옵션을 선택할 수 있습니다.

- *사용 안 함:* 암호 복구가 허용되지 않습니다.
- *SmartConnect 설정 사용:* 자격 증명은 SmartConnect™에서 사용된 동일한 방법을 통해 전송됩니다.
- *맞춤 설정 사용:* 맞춤 설정을 정의할 수 있습니다 (아래 상자 참조).

유휴 사용자의 시간 초과

사용자가 강제로 로그 아웃 (기본적으로 15 분)되는 비활성 시간으로 티켓 유효 기간이 많이 낭비되지 않습니다.

기본 계정 유효 기간 (일)

계정이 유효한 일 수 (기본값은 365 일). 이 기간이 지나면, 사용자는 자동으로 비활성화됩니다.

사용된 계정 삭제 허용

이 옵션은 티켓의 일부를 이미 사용한 계정을 삭제할 수 있습니다. 선택하면 다음 옵션이 나타납니다.

SmartConnect로 티켓을 구입한 사용자는 삭제하지 않기

이 옵션은 이전 옵션을 선택했을 때 나타납니다. 기본적으로 이 기능은 이미 활성화되어 있어, SmartConnect를 이용한 신용카드로 티켓을 구매한 사용자는 시스템에서 삭제되지 않습니다.

매일 사용 중지된 계정 삭제

사용 중지된 계정을 자동으로 매일 삭제하도록 설정합니다.

만료된 계정을 매일 삭제하기

사용 중지된 계정을 자동으로 매일 삭제하도록 설정합니다.

동시에 여러 로그인 허용

체크 박스를 선택하면, 사용자가 다른 장치에서 동시에 연결할 수 있습니다.

생성된 암호에 대한 문자 집합

기본 설정의이 부분은 자동 생성된 암호의 기본값을 정의할 수 있게 합니다.

> **힌트:** 기본적으로 암호는 6자이며, 자릿수로만 구성됩니다.

다음 값을 사용자 정의할 수 있습니다.

길이

암호의 길이로 몇 자를 지정할 지 정하게 해줍니다.

대문자

암호에 대문자가 포함되어야 하는 경우에는, 체크 박스를 선택하십시오.

소문자

암호에 소문자가 포함되어야 하는 경우에는, 확인란을 선택하십시오.

숫자

비밀번호에 숫자가 포함되어야 하는 경우에는, 체크 박스를 선택하십시오.

특수 문자

암호에 대문자가 포함되어야 하는 경우에는, 체크 박스를 선택하십시오.

암호 복구 사용자 정의 설정.

사용자 지정 설정으로 암호 복구를 허용하도록 선택하면, 성공적인 복구 프로세스에 필요한 몇 가지 구성 옵션이 나타납니다. 첫 번째는 복구가 완료되는 방식입니다.

비밀번호 복구가 완료되었습니다.

이 옵션에는 SMS, 이메일을 통해, 또는 둘 다 선택할 수 있는 세 가지 옵션이 있습니다. 선택 항목에 따라 SMS 또는 전자 메일을 보내는 방법을 구성하는 다양한 옵션이 나타납니다. 전자 메일 및 SMS 암호 복구가 모두 활성화된 경우 모든 옵션이 나타납니다.

SMS 복구 모드의 경우에는, 추가 옵션은 하나뿐입니다.

암호 복구에 허용된 국가 코드

선택한 국가에 속한 휴대 전화에만 SMS를 보낼 수 있습니다. 새 국가 코드를 추가하려면, 해당 국가 이름 옆에 있는 다중 선택 입력란에 국가 이름이 표시되고, 아래 상자에 국가 이름이 나타나면, 선택하고 마지막으로 국가 이름 오른쪽에 있는 + 를 클릭하십시오. 허용된 국가는 오른쪽 상자에 표시되고, 오른쪽에 있는 - 를 클릭하면, 허용되지 않을 수 있습니다.

전자 메일 복구 모드의 경우 두 가지 옵션을 사용할 수 있습니다.

메일 서버

복구 이메일을 보내는 데 사용된 SMTP 서버입니다. 드롭 다운 메뉴에서 세 가지 옵션 중 하나를 선택할 수 있습니다.

1. 시스템 SMTP 서버. 이 옵션을 선택하려면 *Menubar ‣ Proxy ‣ SMTP*가 활성화되어 있어야합니다.
2. 사용자 지정 SMTP 서버. 이 경우, 메일 서버의 이름을 텍스트 상자에 지정할 수 있습니다.

보낸 사람 전자 메일 주소

복구 전자 메일의 사용자 지정 보낸 사람으로 사용할 사용자 지정 전자 메일 주소입니다.

두 가지 복구 모드에서 추가 옵션을 사용할 수도 있습니다.

암호 복구를 다음으로 제한하십시오.

또 다른 시간내에 암호를 복구하기 전에 통과해야 하는 시간 간격입니다. 드롭 다운 메뉴에서 10분에 한 번, 30분에 한 번, 매시간 한 번, 매일 한 번씩 네 가지 옵션 중 하나만 선택할 수 있습니다.

SmartConnect

이 페이지에서 핫스팟의 SmartConnect™ (셀프 서비스) 및 SmartLogin 기능을 구성할 수 있습니다. SmartConnect™ 시스템은 고객 지불없이, 유료 셀프 서비스 티켓 생성 또는 무료 티켓 사용을 완벽하게 지원하며, SmartLogin은 핫스팟을 닫고 브라우저를 열어, 재인증 할 필요가 없도록 사용자에게 제공합니다. 아직 활성화되지 않은 경우, 이 페이지가 처음 열리면, 사용할 수 있는 옵션은 하나뿐입니다.

SmartConnect

SmartConnect 사용

SmartConnect™ 기능은 이 체크 박스가 선택된 경우에만 활성화됩니다.

SmartConnect™가 활성화되면, 추가 옵션이 나타나서 이 기능을 보다 잘 제어할 수 있습니다 :

셀프 서비스 사용자 등록

이 드롭 다운 메뉴를 통해 사용자에게 성공적인 계정 등록을 알리는 양식을 선택할 수 있습니다. 상호 배타적인 3가지 옵션 (즉, 한 번에 하나만 선택할 수 있음)은 SMS 및 전자 메일을 통해, 그리고 알림을 전혀받지 않고 (비활성화) 선택할 수 있습니다. 선택 사항에 따라 추가 옵션을 사용할 수 있습니다.

- **비활성화 됨:** 추가 옵션을 사용할 수 없습니다. SmartConnect™ 사용자는 티켓을 탐색하고, 구매할 수 있지만 SmartConnect ™를 통해 새로운 사용자를 만들 수는 없습니다.
- **SMS.** 이 옵션을 활성화하려면 시스템 ‣ 이벤트 알림 ‣ SMS 알림에서 확인할 수있는 확인을 사용자에게 보내는 데 사용되는 SMS 번들을 사용할 수 있어야합니다. 추가 SMS 번들은 Endian Network에서 구입할 수 있습니다. 하나의 추가 옵션을 사용할 수 있습니다.

  전화 번호 확인 필요 없음

  확인을 보낼 핸드폰 번호를 두 번 쓸 수 있는 요청을 비활성화 하십시오. 스마트 폰에서 요청을 컴파일할 때 유용합니다.

- **이메일.** 액세스 자격 증명이 있는 전자 메일은 등록 프로세스 중에 제공된 전자 메일 주소로 보내집니다. 사용자가 프로세스를 성공적으로 완료하고 계정을 활성화하기 위해 클릭해야 하는 확인 링크도 포함되어 있습니다. 이 옵션을 사용하려면 스마트호스트 또는 SMTP 서버가 필요합니다.

  전자 메일 주소 확인 필요 없음

  확인을 보낼 전자 메일 주소를 두 번 쓰는 요청을 해제하십시오. 스마트 폰에서 요청을 컴파일할 때 유용합니다.

전자 메일 주소 확인을 위한 티켓 요금

이 드롭 다운 메뉴를 사용하면, 사용자가 잠시 접속하여 확인 이메일을 읽고 받을 수 있도록 해주는 사용 가능한 요금 중 하나를 선택할 수 있게 해줍니다.

> **힌트:** 여기에서 선택할 수 있는 요금은 **시간 기반** 및 **선불 방식**으로 정의되고 **티켓 생성으로 인해** 유효해야하며 SmartConnect™에 대해 활성화되어서는 안됩니다.

메일 서버

이 드롭 다운 메뉴를 사용하면, 액세스 자격 증명으로 전자 메일을 보낼 스마트 호스트를 선택할 수 있습니다. 사용 가능한 옵션은 다음과 같습니다. 사용자 정의된 메일 서버의 URL을 제공할 수 있는 **사용자 정의 메일 서버**, **시스템 스마트호스트** 및 **시스템 SMTP 프록시** 등입니다. 후자의 옵션은 스마트호스트 및 SMTP 프록시가 구성되어, 어플라이언스에서 실행중인 경우에만 사용할 수 있습니다.

보낸 사람 전자 메일 주소

확인 전자 메일의 보낸 사람으로 표시될 사용자 지정 전자 메일 주소입니다.

허용된 국가 코드

선택한 국가에 속한 휴대폰 만 SmartConnect™ 액세스를 위해 등록할 수 있습니다. 새 국가를 추가하려면, 해당 국가 이름 옆에 있는 다중 선택 입력란에 나라 이름이 아래 상자에 나타날 때까지 국가 이름 또는 코드를 작성한 다음에 선택하고, 마지막으로 국가 이름 오른쪽에 있는 `+` 를 클릭하십시오. 허용된 국가는 오른쪽 상자에 표시되고 오른쪽에 있는 `-` 를 클릭하면 허용되지 않을 수 있습니다.

사용자 등록 필드

이 다중 선택 상자에서는 등록 프로세스 중에 제공할 필수 계정의 속성을 정의할 수 있습니다. 사용자에게 표시되는 속성은 **필수** 또는 **선택적** 표시와 함께, 오른쪽 열에 표시됩니다. 선택 또는 필수 속성의 총 수는 왼쪽 상단에 표시됩니다.

> **참고:** 사용자 등록 유형에 따라 일부 필드는 필수 항목이며, 비활성화 할 수 없습니다. 전자 메일로 등록할 때 사용자 이름, 암호 및 전자 메일 주소가 필요하며, sms로 등록할 때, 전화 번호만 필요하며 사용자 이름으로 사용됩니다.

계정 당 무료 티켓 제한

모든 계정에서 사용할 수 있는 무료 티켓의 양입니다. 기본 옵션은 "제한 없음"입니다. 즉, 매 순간 새로운 티켓을 구매할 수 있지만, 사용자는 주어진 시간 (분)마다 하나의 새로운 무료 티켓을

구매할 수 있는 "시간 제한" 옵션이 있습니다.

유료 티켓 사용

이 옵션을 사용하면, 사용자가 Paypal 또는 신용 카드를 사용하여 핫스팟 티켓을 지불할 수 있습니다. 사용하도록 설정하면, 이 기능을 사용하여 지불금이 수금되는 PayPal 계정을 구성할 수 있습니다.

> **경고:** 사용자가 핫스팟에 연결되어있는 동안이 옵션을 활성화하면 모두 강제로 연결이 끊어집니다.

다음 옵션은 이전 옵션을 선택한 경우에만 표시됩니다.

Paypal 샌드 박스 사용

이 상자는 테스트/데모 용도로만 PayPal 샌드 박스를 사용하거나 사용하지 않도록 설정합니다. 실물 돈을 가지고 사용중인 라이브 트랜잭션을 실제로 실행하지 않고, 샌드 박스 사용을 통해 Paypal API 통합이 작동하는지 확인할 수 있습니다.

> **참고:** Endian 핫스팟의 SmartConnect™ 기능을 올바르게 설정하고, 고객 지불을 받으려면 PayPal 계정을 등록하고 만들어야 합니다.

Paypal API 사용자 이름

PayPal API 사용자 이름.

Paypal API 비밀번호

PayPal API 비밀번호.

Paypal API 서명

PayPal API 서명.

추가 참고사항: PayPal 샌드 박스 및 SmartConnect™ 설정에 대한 단계별 안내는 help.endian.com 웹 페이지에서 제공됩니다.

SmartLogin

일반적으로 브라우저를 닫은 후에는 핫스팟 사용자가 다시 인터넷에 액세스할 수 있도록 인증해야 합니다. SmartLogin 기능은 핫스팟 사용자에게 브라우저를 다시 열고 핫스팟에 다시 연결할 때, 새로운 인증

을 피할 수 있는 편리한 방법을 제공합니다.

SmartLogin 기능은 모든 핫스팟 사용자를 위해 전역적으로 또는 각 사용자에 대해 개별적으로 활성화할 수 있습니다. 후자의 경우, SmartLogin은 전역적으로 활성화되지 않았더라도 해당 사용자에 대해 작동하며, 계정 편집기의 로그인 정보 섹션에서 활성화할 수 있습니다.

다음 옵션을 사용할 수 있습니다.

SmartLogin 사용

모든 사용자에 대해 SmartLogin을 사용하려면 확인란을 선택하십시오.

SmartLogin 쿠키 수명

사용자의 시간 (일)은 SmartLogin 기능을 사용할 수 있습니다.

사용자가 로그 아웃시 SmartLogin 쿠키 제거를 무시하도록 허용

이 옵션을 사용하면 로그인 포털에 사용자가 SmartLogin 기능을 사용할지 여부를 선택할 수 있는 새로운 옵션 (자동 로그인 사용 안함)이 나타납니다.

이메일 확인 요금.

사용자가 확인 이메일을 읽을 수 있게 하려면, 새로 만든 계정의 자격증명을 읽기 위해 인터넷과 메일 계정에 무료로 액세스할 수 있어야 합니다. 따라서 정확한 특성을 갖춘 적절한 요금이 SmartConnect™ 사용자 등록 프로세스와 연결되어야 합니다. 요금을 아직 이용할 수 없는 경우, Ticket ▸ Rates 밑에 생성될 수 있는 티켓에 필요한 필수 옵션을 설명하는 메시지가 표시됩니다. 티켓 요금은 선불, 무료, 시간 기반이어야 하며, SmartConnect™에는 사용할 수 없습니다. 또한 'From ticket creation' 유효 값으로 정의해야 합니다. 사용자에게 자격 증명을 검색할 수 있는 가능성을 주기 위해, 이 값을 몇 분으로 제한하는 것이 좋습니다.

티켓 가격 생성에 대한 도움말은 온라인 도움말을 참조하십시오.

> **경고:** 이 경고 아래에 소셜 네트워크 설명서가 표시되지 않으면 브라우저에서 광고 차단기를 사용하고 있는 것일 수 있습니다. 문서의 이 부분을 읽으려면, 이 페이지의 광고 차단기를 비활성화하십시오.

소셜 네트워크

핫스팟은 가장 중요한 소셜 네트워크를 지원하고 사용하는 방식으로 구성될 수 있습니다. 두 가지 기능

이 구현되었습니다. 첫 번째는 소셜 로그인이라고 하며, 사용자가 소셜 네트워크 계정 (예: Google 또는 Facebook)을 사용하여 핫스팟에 로그인할 수 있습니다. 두 번째 기능은 사용자가 다양한 소셜 네트워크에서 귀하의 비즈니스에 대한 정보를 공유하도록 요구함으로써 마케팅 목적으로 핫스팟을 사용할 수 있게 합니다. 이 기능을 소셜 활성화기(Social Enabler)라고 합니다.

소셜 로그인

소셜 로그인을 사용하면 Facebook 또는 Google 계정이 있는 사용자가 새 사용자 계정을 만들지 않고도 Endian 핫스팟에 액세스할 수 있습니다. 이 경우 사용자의 인증은 Facebook 또는 Google에 대해 원격으로 수행되는 반면, 로컬로 새 사용자가 생성되며 사용자 이름은 각각의 이메일 주소입니다. 첫 번째 로그인시 티켓이 사용자에게 할당됩니다. 사용자는 암호가 필요 없지만 다른 사용자처럼 취급됩니다. 즉, 사용자의 잔액, 정보 및 연결을 확인하고 계정과 연결된 티켓 또는 데이터를 수정할 수 있습니다.

소셜 로그인에 대해 다음 옵션을 사용할 수 있습니다.

기본 티켓 요금

> 소셜 로그인을 사용하여 핫스팟에 액세스하는 사용자에게 연결할 티켓을 드롭 다운 메뉴에서 선택하십시오. 이것은 소셜 로그인 기능을 사용할 때, 티켓을 선택할 수 있는 가능성이 없기 때문에 필요합니다.

Facebook 로그인 사용

> 사용자가 Facebook 자격 증명을 사용하여 핫스팟에 액세스할 수 있도록 하려면 체크 박스를 선택합니다.

Google 로그인 사용

> 사용자가 Google 자격 증명을 사용하여, 핫스팟에 액세스할 수 있도록 하려면 체크 박스를 선택합니다.

활성화된 각 소셜 로그에 대해 인증 페이지에 핫 스폿에 액세스하기 위해, 클릭할 수 있는 버튼이 나타납니다.

소셜 활성화기(Social Enabler)

Social Enabler는 지원되는 다양한 소셜 네트워크 중 하나에서 사용자가 서비스에 대한 정보를 게시하면 게스트 액세스를 가능하게 합니다.

소셜 활성화기는 다음 옵션을 통해 구성할 수 있습니다.

연결을 활성화하기 전에 소셜 버튼이 있는 잠금 화면 표시

이 확인란을 선택하면, Social Enabler가 활성화됩니다. 사용자는 인터넷에 연결할 수 있도록 사용 가능한 소셜 활동 중 하나를 수행해야 합니다.

사용자가 잠금 화면을 닫음으로써이 단계를 건너 뛰도록 허용

이 기능은 기본적으로 사용하도록 설정되어있어 사용자가 잠금 화면을 닫고 인터넷 연결을 직접 사용할 수 있습니다.

> **참고:** 이 옵션을 비활성화하면 다양한 소셜 네트워크의 정책을 침해할 수 있으며, Endian은 이러한 네트워크가 귀하의 계정을 차단하기로 결정할 경우 책임을 질 수 없습니다.

자동으로 화면 잠금 해제

이 옵션을 사용하면 일정 시간이 지난 후, 잠금 화면을 자동으로 사라지게 할지 여부를 구성할 수 있습니다. 옵션은 30초에서 5분 사이입니다. 기본적으로 화면 잠금은 자동으로 해제되지 않습니다.

소셜 버튼 테마

여기에서 소셜 버튼에 사용할 수 있는 테마 중 하나를 선택할 수 있습니다.

소셜 카운터 표시

이 옵션을 선택하면 소셜 활동을 수행하는 버튼뿐만 아니라 이미 수행된 횟수가 표시됩니다.

핫스팟 잠금 해제를 위한 소셜 활동 선택

이 다중 선택 필드에서 어떤 사회 활동이 잠금 화면을 잠금 해제할 수 있어야 하는지 정의할 수 있습니다. 활동을 왼쪽에서 오른쪽 열로 끌어서 사용할 수 있습니다. 사용 가능한 옵션은 다음과 같습니다.

- 페이스 북처럼
- 페이스 북에 공유
- Google +1
- Google 공유
- LinkedIn Share
- 트위터 팔로우
- 트위터 트위터
- YouTube 구독

> **참고:** LinkedIn 공유를 사용하는 경우, Twitter Follow 및 Twitter Tweet 사용자는 공유하지 않고, 창을 닫더라도 인터넷 연결을 사용할 수 있습니다.

소셜 네트워크 구성

이 섹션에서는 모든 단일 소셜 네트워크에 필요한 구성 매개 변수를 삽입할 수 있습니다. 소셜 네트워크별로 그룹화되어 있습니다.

페이스북

Facebook 앱 ID

응용 프로그램 ID는 Facebook Share 옵션을 활성화할 때 필요하며, 여기에 입력할 수 있습니다.

Facebook에서 좋아요(like) URL

각 버튼을 클릭하면, 사용자가 좋아요(like)를 누른 것에 대한 URL입니다.

Facebook에서 공유하기를 위한 URL

사용자가 각 버튼을 클릭하면, 공유하기를 위한 URL입니다.

Google+

Google+에서 +1하는 URL

사용자가 각 버튼을 클릭하면 Google+에 +1을 추가할 URL입니다.

Google+에서 공유할 URL

각 버튼을 클릭하면 사용자가 Google+에서 공유할 URL입니다.

트위터

트위터에 트윗 하기 위한 URL

이것은 사용자가 트위터 트윗 버튼을 클릭하면, 트윗될 URL입니다.

트윗 텍스트

이것은 사용자가 트위터 트윗 버튼을 클릭하면, 트윗될 추가 텍스트 메시지입니다.

~을 통한 트윗

이 필드를 사용하면, Twitter 사용자 이름을 트윗의 원본 소스로 지정할 수 있습니다. 여기에 이름을 추가하면, 메시지에 "via @username"으로 표시됩니다. 여기에는 사용자 이름만 필요하므로, @ 기호를 앞에 추가하지 마십시오 (@username이 아닌

username).

Follow 할 트위터 프로필의 URL

여기에 해당 버튼을 클릭한 후, 사용자가 Follow 하는 트위터 프로필의 전체 URL을 붙여 넣으십시오.

링크드인

LinkedIn에서 공유할 URL

이 URL은 사용자가 해당 버튼을 클릭하면, LinkedIn에서 공유하게 됩니다.

YouTube

구독할 YouTube 채널 ID

해당 버튼을 클릭한 후, 사용자가 구독하길 원하는 YouTube 채널의 ID를 지정하십시오. 채널 ID는 채널의 URL에서 찾을 수 있습니다. 위치 표시 줄(location bar)의 초기 'https://www.youtube.com/channel/'을 직접 따라가는 문자열이며, 'UC3UU4klSmn2dg8qApAO8Otw'와 유사합니다.

Google 클라이언트 ID

YouTube 채널을 구독하려면, Google 클라이언트 ID가 필요합니다. 이 ID는 여기에 입력해야 합니다.

추가 참고 사항: 지식 기반에서는 다음 자습서를 사용할 수 있습니다.

- Google 클라이언트 ID를 만드는 방법
- 페이스 북 ID를 만드는 방법

API

이 섹션에서는 이미 실행중인 시스템에 Endian UTM Appliance의 핫스팟을 통합할 수 있도록 Endian Hotspot의 API 설정을 제어합니다. 선택한 모드에 따라 다른 매개 변수를 설정할 수 있습니다.

모드

Endian UTM Appliance는 Endian의 일반 API/JSON, ASA jHotel 및 PC Phoenix 인터페이스의 세 가지 API 모드를 제공합니다. ASA jHotel 및 pcs phoenix 인터페이스는 ASA jHotel 또는 PC phoenix

호텔 관리 소프트웨어를 사용하는 호텔에서만 필요하며, 일반 API는 다른 소프트웨어 시스템과 상호 작용할 수 있습니다. 세 가지 사용 가능한 모드는 상호 배타적입니다. 즉, 한 번에 하나씩 활성화할 수 있습니다. 3개의 인터페이스 중 하나가 활성화되어 있고 다른 인터페이스가 활성화되어 있는 경우에는, 후자 인터페이스만 활성화되며 전자는 자동으로 비활성화됩니다.

다른 구성 옵션은 선택한 모드에 따라 다릅니다. 다음은 ASA jHotel 모드를 지정하는 옵션입니다.

ASA jHotel Interface enabled

이 확인란을 선택하면, ASA jHotel 인터페이스가 활성화됩니다.

ASA jHotel URL

ASA jHotel 관리 인터페이스의 URL입니다. 그 정확성은 입력 상자의 오른쪽에 있는 테스트 버튼을 클릭하여 테스트할 수 있습니다.

> **힌트:** 제공된 샘플 URL에서 ASA 설치의 IP_ADDRESS 및 COMPANY 이름을 바꿉니다.

게스트 등록 허용 (게스트 로그인 / SmartConnect)

이 확인란을 선택하여, 게스트가 자동 등록하도록 허용합니다.

게스트 등록 기본 요금

이 드롭 다운 메뉴에서 새 계정에 적용할 기본 요율을 선택하십시오. 이용 가능한 요율은 *Ticket(티켓) ‣ Rates(요율)*에서 이미 정의되어 있어야 합니다.

체크인하지 않은 손님을 위해 비 무료 우편 유료 티켓을 허용하십시오.

체크인하지 않은 호텔 투숙객이 유료 티켓을 구매할 수 있도록 체크 박스를 선택합니다.

ASA jHotel 관리 소프트웨어를 사용한 핫스팟 액세스.

핫 스폿이 올바르게 구성된 경우, ASA 관리 소프트웨어에 이미 계정이 있는 사용자는 계정을 만들지 않고도 핫스팟에 빠르게 액세스 할 수 있습니다. 핫스팟에 필요한 단계는 다음과 같습니다.

1. *ASA jHotel Interface enabled* 체크 박스를 선택하고 핫스팟이 ASA jHotel 인터페이스의 URL에 액세스 할 수 있는지 확인하십시오.
2. *티켓(Ticket) ‣ 요금(Rates)*에서 ASA가 사용하는 *티켓 코드*와 함께 새로운 *후불 지불* 요금을 생성하고 고유한 이름을 부여하십시오 (예: "my-ASA").
3. *설정(Settings) ‣ API*로 돌아가서 *ASA jHotel* 모드를 선택하고 이전 단계에서 만든 요금 이름 ("my-ASA")을 *게스트 등록 기본 요금*으로 선택하십시오.

일반 API / JSON 또는 PC Phoenix 인터페이스의 경우 세 가지 옵션을 사용할 수 있습니다.

API 사용

확인란을 선택하여, API를 사용하도록 설정합니다.

계정 URL

핫스팟은 사용자가 제공한 데이터를 확인하기 위해, 이 URL에 계정 정보를 보냅니다. 핫스팟이 계정을 가져서는 안되면 이 필드를 비워 둡니다.

계정 URL에 HTTP 인증이 필요합니다.

이전 옵션에서 제공된 URL에 HTTP 인증이 필요한 경우, 이 확인란을 선택합니다. 두 개의 새로운 텍스트 필드가 각각 사용자 이름과 암호를 제공합니다.

마지막으로 API는 Generic API/JSON 인터페이스가 선택된 경우, **https://GREENIP:10443/admin/api/** 의 특별 페이지에서 테스트할 수 있습니다.

언어

언어 섹션에서는 모든 언어 별 옵션을 설정하고, 다양한 언어로 표시된 모든 문자열과 포털 템플리트를 사용자 정의할 수 있습니다. 이 페이지는 두 개의 상자로 구성됩니다: 지원되는 언어, 언어 편집, 두 번째 상자에서 수행된 편집 선택에 따라 세 번째 언어가 표시됩니다.

지원 언어

첫 번째 상자에서 핫스팟에서 지원되는 언어를 선택하고, 사용자가 사용할 수 있도록 할 수 있습니다. 다중 선택 상자에서 언어를 선택하고, 저장 버튼을 클릭하여 저장해야 합니다. 등록 프로세스 중 및 포털에 연결할 때, 여기에서 선택한 언어만 사용할 수 있습니다.

언어 수정

두 번째 상자에서는 이전 상자에서 활성화된 모든 언어에 대해 네 개의 포털 템플리트 또는 사용자 인터페이스 문자열 중 하나를 수정할 수 있습니다. 템플릿과 문자열을 개인화하기 위해 사용할 수 있는 몇 가지 변수가 있습니다. 메시지가 사용자에게 전송될 때 (예: 사용자가 계정 비밀번호를 잃어버렸습니다. 각 변수는 핫스팟에 저장된 데이터에서 가져온 실제 값으로 대체됩니다.)

언어

번역을 수정하거나 추가할 언어입니다. 드롭 다운 메뉴에서 사용 가능한 옵션은 활성화된 언어에 따라 다릅니다.

편집

수정할 객체입니다. 포털 템플리트 또는 포털 문자열이 될 수 있습니다. 포털 문자열을 수정하는 선택인 경우에, 편집기는 핫스팟의 GUI 및 포털에서 사용되는 영어 단어 및 문장 목록으로 대체됩니다. 각 단어 상자에는 선택한 언어로 번역을 작성하는 입력 상자가 있습니다. 포탈 템플리트를 선택하면, *시작 페이지, 계정 인쇄, 서비스 약관, 도움말, 전자 메일 본문 및 분실한 암호 전자 메일 본문* 등과 같이 열리는 상자에서 템플릿 중 하나를 편집할 수 있습니다.

포털을 사용자 정의하는 방법에 대한 자세한 내용을 보려면 아래의 핫스팟 사용자 정의로 건너 뛰십시오.

각 템플릿의 내용은 완전한 기능을 갖춘 WYSIWYG 편집기를 사용하여, 변경하고 개인화할 수 있습니다.

핫스팟 사용자 정의 설정

사용자가 처음 핫스팟에 연결할 때, 사용자에게 제공되는 포털은 포털에서 사용되는 언어, 다양한 페이지에 포함된 텍스트, CSS, 핫스팟을 운영하는 회사의 로고 및 포털의 이름과 같은 여러 가지 방법으로 사용자 정의할 수 있습니다. 마지막 설정은 CLI(명령행)에서만 구성할 수 있지만 나머지는 모두 핫스팟의 관리 인터페이스에서 언어 섹션 (*핫스팟(Hotspot) ‣ 관리 인터페이스 (Administration interface) ‣ 설정 (Settings) ‣ 언어 (Languages)*)에서 수행할 수 있습니다.

사용 가능한 언어.

기본적으로 활성화되는 영어 (en) (영어, 기본값으로 사용됨), de (독일어), it (이탈리아어), ja (일본어), es (스페인어), pt (포르투갈어)입니다. 포털에 연결하는 사용자는 각 언어를 사용자 정의하도록 선택할 수 있습니다. 추가 언어는 핫스팟에서 다중 선택 상자에서 원하는 언어를 선택하여 제공할 수 있습니다

템플릿.

다음은 수정할 수 있는 템플릿입니다.

환영 페이지

로그인하기 전에 사용자에게 표시되는 페이지입니다.

계정 인쇄

사용자 이름과 비밀번호와 함께 등록 후 환영 메시지가 인쇄되어 사용자에게 전달됩니다. 사용할 수있는 변수는 $title, $firstname, $lastname, $username, $password입니다.

서비스 약관

그들은 로그인할 수 있기 전에, 서비스 약관에 동의하도록 요청하는 체크 박스 옆의 링크를 클릭할 때 사용자에게 표시됩니다.

도움

이 페이지의 내용은 사용자에게 도움말 메시지로 표시됩니다.

이메일 본문

등록시 사용자의 자격 증명과 함께 전송되는 전자 메일에 포함될 텍스트로 전자 메일로 등록할 때 사용됩니다. 사용할 수 있는 변수는 *$hotspot_name, $activation_link, $rate_name, $username, $password, $amount, $price, $currency, $txn_id*입니다.

비밀번호 이메일 본문 분실

사용자 자격 증명으로 전송된 전자 메일에 포함될 텍스트 (사용자가 전자 메일을 분실했을 때, 사용되며 *전자 메일로 암호 복구* 옵션이 선택됨). 사용할 수 있는 변수는 *$username, $password*입니다.

각 템플릿은 핫 스폿에서 사용할 수있는 모든 언어에 대해 편집할 수 있으며, 미리 정의된 변수를 사용할 수 있습니다 (이 표 참조).

텍스트 및 이미지.

이미지 또는 텍스트일지도 모르는 포털의 컨텐츠는 편집기에서 수정할 수 있으며, 이 이미지에서 사용자 정의 이미지, CSS 및 기타 파일을 업로드할 수도 있습니다. 편집기를 사용하려면, 언어 편집 섹션으로 이동하여 편집: 레이블 옆에 있는 드롭 다운 메뉴에서 포탈 템플리트를 선택한 다음, 사용 가능한 템플리트 아래의 드롭 다운 메뉴에서 템플리트로 선택하십시오.

- *시작 페이지:* 연결하기 전에 모든 사용자가 볼 수있는 페이지입니다.
- *계정 인쇄:* 인쇄할 사용자의 자격 증명으로 사용자에게 넘겨줄 문서입니다.
- *서비스 약관:* 사용자가 핫스팟 사용 중에 따라야하는 규칙.
- *도움말:* 사용자를위한 도움말 및 문제 해결이 포함된 페이지입니다.
- *이메일 본문:* 성공적인 계정 생성을 위한 확인 메시지로 사용자에게 전송된 전자 메일의 텍스트입니다.
- *분실한 이메일 이메일 본문:* 핫스팟에 액세스 하기 위한 자격 증명을 알리는 메시지로 사용자에게 전송된 전자 메일의 텍스트입니다.

페이지 하단의 편집기에서 텍스트와 이미지가 있는 문서를 만들 수 있습니다. 이미지와 커스텀 파일을 추가하는 것은 매우 간단합니다 : 커즌을 이미지를 삽입할 위치에 놓은 다음, 버튼을 클릭하여, *Image Properties*라는 팝업 윈도우를 엽니다. 여기, 이미지 정보 탭에는 이미지 삽입을 위한 두 가지 방법이 있습니다.

1. URL 텍스트 필드에서 웹의 이미지에 대한 하이퍼 링크를 제공하십시오.
2. 서버 **찾아보기(Browse Server)** 버튼을 클릭하여, 파일 브라우저를 열고 서버의 기존 이미지를 선택하거나 페이지 하단의 **파일 선택** 버튼을 클릭하여, 로컬 워크 스테이션에서 이미지를 선택한 다음 **업로드** 버튼을 클릭하십시오.

> **힌트:** 업로드된 파일은 Endian UTM Appliance에 /home/httpd/html/userfiles/ 디렉토리에 저장됩니다. 맞춤 파일은 해당 위치의 SSH를 통해 직접 업로드할 수도 있습니다.

CSS.

사용자 정의 CSS 파일을 사용할 수도 있습니다 : Endian UTM Appliance에 업로드하여 /home/httpd /html/userfiles 디렉토리에 배치하십시오. 이미지 파일과 마찬가지로 버튼이나 SSH를 사용하여 업로드할 수 있습니다. 파일의 이름은 다음과 같습니다.

- **hotspotcustom.css**, 관리 인터페이스에 사용되는 CSS
- **portalcustom.css,** Hotspot 포털에 사용되는 CSS
- **miniportalcustom.css**: 핫스팟 미니 포털에 사용되는 CSS로, 휴대 기기에 맞게 자바 스크립트가 비활성화된 CSS입니다.

> **힌트:** 이러한 파일의 원본은 /home/httpd/html/include 디렉토리에서 찾을 수 있으며 hotspot.css, portal.css 및 miniportal.css로 각각 지정됩니다. 그것들은 커스텀 것들의 기반으로 사용될 수 있습니다.

로고.

포털의 사용자에게 표시되는 로고는 사용자 정의 CSS portalcustom.css 또는 miniportalcustom.css 파일을 사용하여 바꿀 수 있습니다. /home/httpd/html/userfiles 디렉토리 (100x40 픽셀 크기)에 로고를 업로드하고, 다음과 같이 CSS 파일을 열어서 수정합니다.

```
div.logo img { display: none; }
div.logo { background-image: url('images/your-logo.png'); }
```

핫스팟 명

도메인 이름을 포털로 변경하는 작업은 CLI (명령행)에서 수동으로 수행해야합니다. Endian UTM Appliance에 대한 CLI 액세스는 Menubar ‣ System ‣ SSH 액세스 (Endian UTM Appliance 액세스 섹션 참조)에서 활성화할 수 있습니다.

> **경고:** CLI 파일에서 모든 구성 파일을 수동으로 편집하고 수정하면서, 파일을 잘못 편집하면 서비스가 중지될 수 있으므로 Endian UTM Appliance 내부에 대해 어느 정도 알고 있어야 합니다. 주의해서 편집하기 전에 파일의 백업 복사본을 저장하는 것이 좋습니다.

구성 파일을 직접 편집 및 수정하여 Endian UTM Appliance 내부 정보를 알아야 합니다. 주의해서 편집하기 전에 파일의 백업 복사본을 저장하는 것이 좋습니다.

```
HOTSPOT_HOSTNAME=hotspot
HOTSPOT_DOMAINNAME=example.com
```

오른쪽 (hotspot 및 example.com)의 값을 사용자 정의 값으로 바꿉니다.

또한 캡 티브 포털에 대한 연결이 암호화되어 있으므로 올바른 SSL 구성이 필요합니다. 이는 다음을 생성합니다.

- 유효한 인증서 (즉, **자체 서명된** 인증서 없음)
- 암호화되지 않은 개인 키 파일
- 인증서의 SSL 키 체인을 포함하는 파일.

이 파일들은 모든 디렉토리에 생성될 수 있지만 권장되는 권장 사항은 /var/efw/hotspot/ 아래에 이러한 파일을 복사하여, 모든 구성 백업에 포함되도록 하는 것입니다. 모든 인증서가 만들어지면, Hotspot 엔진이 자신의 존재를 인식하고 기본 인증서 설정을 덮어쓰고 /var/efw/hotspot/settings 파일을 다시 편집하고 다음 변수를 추가해야 합니다.

```
HOTSPOT_CERT=/<CUSTOM_PATH>/hotspot.example.com-cert.pem
HOTSPOT_KEY=/<CUSTOM_PATH>/hotspot.example.com-key.pem
HOTSPOT_CHAIN=/<CUSTOM_PATH>/hotspot.example.com-cabundle.pem
```

*<CUSTOM_PATH>*를 세 인증서의 전체 경로로 바꾸십시오.

마지막으로 SSL 키 체인 파일이 필요하지 않은 경우, 빈 값을 위의 구성의 마지막 변수에 지정할 수 있습니다.

HOTSPOT_CHAIN=

변수의 의미.

이것은 핫스팟의 포털 템플리트 및 포털 문자열을 사용자 정의할 때, 사용할 수 있는 변수에 대한 완전한 참조입니다. 템플릿은 각 사용자에게 맞춤 설정된 메시지를 작성하는데 유용합니다. 이러한 변수 중 하나가 템플릿에 표시될 때마다 해당 계정에 정의된 해당 값으로 대체됩니다. 변수는 3개의 테이블로 그룹화됩니다. 표 1은 모든 포털 템플리트에서 사용할 수 있는 변수를 포함하고, 표 2는 인쇄 계정 템플릿에서만 사용할 수 있는 변수를 포함하고 표 3은 포털 문자열에서 사용되는 변수를 포함합니다.

표 1: 모든 포탈 템플리트의 변수.

변수	에 의해 대체됨
$title	계정 소유자의 제목
$firstname	계정 소유자의 이름
$lastname	계정 소유자의 성
$username	계정의 사용자 이름
$password	계정 암호
$rate_name	핫스팟 티켓 요금의 이름입니다.
$amount	사용 가능한 트래픽 또는 시간의 양
$price	티켓 가격
$currency	티켓이 지불된 통화.
$txn_id	트랜잭션의 ID.

다음 표의 변수는 인쇄된 계정 정보에서 계정 편집기의 해당 필드에 제공된 값으로 대체됩니다.

표 2: 계정 인쇄 포털 템플리트의 변수.

변수	에 의해 대체됨
$language	사용자의 언어
$birth_city	사용자 출생 도시 또는 마을
$birth_date	사용자의 출생 일자
$document_type	사용자를 식별하는 문서
$document_party	

$document_id	문서의 ID입니다.
$street	사용자가 사는 거리
$country	사용자가 거주하는 국가
$city	사용자가 거주하는 도시
$zip	사용자 도시의 ZIP 코드
$description	계정의 설명
$static_ip	
$external_id	
$phonenumber	사용자가 제공한 전화번호
$areacode	
$email	사용자의 전자메일

포털 문자열에 대한 변수.

변수	에 의해 대체됨 [문자열 #]
%(recovery_freq)s	새 암호를 얼마나 자주 복구할 수 있습니까 [4]
%(phonenumber)s	사용자의 전화 번호 [9 42]
%(transaction_id)s	트랜잭션 ID [9 11 28 31 37 42 44 105 121]
%(email)s	사용자의 이메일 주소 [11 44 121]
%(grant_ticket_duration)s	무료 인터넷 접속 시간 [44, 121]
%(seconds)s	사용자가 대기해야하는 시간 (초) [55 113]
%(home)s	핫스팟의 홈페이지로 연결되는 링크입니다. [107]

포털 문자열 중 일부 (123에 14) 만 변수를 포함합니다. 이러한 14개의 문자열의 경우 원래 문자열에 포함된 모든 변수 (예: 문자열 #4, 모든 % (*recovery_freq)s마다 하나의 요청으로 제한됨*)가 번역된 문자열에도 포함되어야 합니다.

일부 변수를 포함하는 문자열 (및)은 다음과 같습니다.

4 % (recovery_freq)s

9, 42 % (전화 번호)와 % (transaction_id)

11 % (이메일) 및 % (거래_ID)

28, 31, 37, 105, % (거래id)

44, 121 % (*grant_ticket_duration*) s, % (*email*)s 및 % (*transaction_id*)s

55, 113 % (초)

107 % (홈페이지)

핫스팟 사용자

이 섹션에서는 다양한 관리 작업을 수행할 수 있고,두 그룹으로 나누어진 핫스팟 (슈퍼) 사용자 목록을 제공합니다. *핫스팟 관리자*는 핫스팟 인터페이스를 완벽하게 관리할 수 있지만 Endian UTM Appliance 기본 메뉴에는 액세스 할 수 없습니다. *핫스팟 계정 편집기*는 기존 사용자 이름을 제공하여 핫스팟 사용자 계정 만 편집하고 활성화 또는 비활성화 할 수 있습니다. 따라서 관리자에게는 계정 편집기의 기능 또한 갖고 있지만 그 반대는 아닙니다.

이 페이지에는 사용자의 이름, 사용자가 속한 그룹 및 계정에서 사용 가능한 작업을 보여주는 사용자 목록이 있습니다. 삭제할 수없는 보호된 관리자 계정인 "*핫스팟*"이 있습니다. 사용 가능한 동작은 사용자 계정을 편집하고 삭제하는 것입니다. 목록을 삭제하면 목록에서 사용자가 삭제되고, 편집은 사용자 편집기가 열립니다 (아래 참조). 핫스팟 사용자를 편집할 때, 비밀번호만 변경할 수 있지만 이름이나 그룹을 수정할 수는 없습니다.

관리자는 *https://GREENIP:10443/admin/* 페이지에 액세스 할 수 있으며, 이 안내서의 전체 핫스팟 섹션에 설명되어 있습니다. 반대로 계정 편집기에는 간단한 웹 인터페이스인 *https://GREENIP:10443/admin/infoedit/*에 있는 제한된 정보 편집기 페이지에 대한 액세스 권한이 부여됩니다. 여기서 계정 편집기는 관련 계정 정보를 수정할 수 있는 기존 사용자 이름을 삽입할 수 있습니다.

사용자를 추가하려면, 목록 위의 `사용자 추가` 링크를 클릭하기만 하면 됩니다. 새 사용자 작성에 필요한 모든 데이터를 입력할 수 있는 사용자 편집기 상자가 열립니다.

사용자 이름

새 계정의 사용자 이름입니다.

그룹

새 사용자가 속한 그룹입니다. 드롭 다운 메뉴에서 핫스팟 계정 편집기와 핫스팟 관리자라는 두 가지 사용 가능한 그룹 중 하나를 선택할 수 있습니다.

비밀번호, 비밀번호 (확인)

확인을 위해 두 번 삽입해야 하는 사용자의 비밀번호

핫스팟에 대한 클라이언트 액세스

이 절에서는 무선을 통해 핫 스폿에 연결할 때, 클라이언트가 보는 핫스팟 사용자 인터페이스에 대해 설명합니다. 포털 모양 및 설정은 핫스팟 관리자에 의해 munubar ‣ hotspot ‣ Administration interface ‣ Settings 아래에서 사용자 정의할 수 있습니다

> **참고:** 핫스팟 소셜 로그인 기능을 도입하면, 모바일 장치 사용자가 전자 메일 클라이언트나 다른 응용 프로그램을 사용하여 인터넷에 연결할 수 있게 되기 전에 핫 스폿에 연결하여 인증해야 합니다.

인터넷 서핑을 하기 전에 사용자는 핫스팟에 액세스하여 로그인해야 합니다. 이 목적을 위해서, 브라우저를 실행하고 웹 페이지를 여는데 충분하기 때문에, 소프트웨어를 설치할 필요가 없습니다. 브라우저는 사용자가 로그인, 새로운 핫스팟 계정을 등록 또는 직접 로그인하고 인터넷 서핑할 수 있는 핫스팟의 포털로 리디렉션 될 것입니다. 핫스팟은 다양한 유형의 포털에 서비스를 제공할 수 있으므로 클라이언트는 사용되는 장치, 모바일 장치용 포털, JavaScript 없는 브라우저용 포털 또는 다른 모든 유형의 장치용 포털을 보게 됩니다.

로그인 페이지는 두 부분으로 구성되어 있습니다. 왼쪽에는 드롭 다운 메뉴에서 인터페이스 언어를 선택하고 유익한 메시지를 읽을 수 있습니다. 오른쪽 섹션은 사용자가 로그인을 진행하거나 새 계정을 등록하거나 새 티켓을 구입할 수 있는 로그인 양식입니다.

로그인 양식에는 게스트(손님) 액세스 용과 등록된 사용자 액세스 용의 두 가지 버전이 있습니다. 전자는 ASA가 핫스팟에서 실행될 때만 작동하며 다음 옵션을 포함합니다.

게스트가 아닙니다.

이 버튼을 클릭하면 등록된 사용자의 로그인 양식이 표시되며 그 옵션은 아래에 나와 있습니다.

성

게스트의 성입니다.

이름

게스트의 이름.

생년월일

게스트의 생년월일은 DD.MM.YYYY 형식입니다. (예: 1980년 2월 5일이 05.02.1980처럼 표기됩니다).

로그인

필요한 정보를 입력한 후, 이 버튼을 클릭하면, 핫스팟에 액세스할 수 있습니다.

등록된 사용자의 로그인 양식은 다음 옵션을 표시합니다.

Google+로 로그인

기존 Google 계정의 자격증 명을 사용하여 핫스팟에 액세스하려면, 이 버튼을 클릭하십시오. 팝업 창이 나타나 사용자 이름과 암호를 입력하고 인증을 수행합니다.

페이스 북으로 로그인

기존 Facebook 계정의 자격 증명을 사용하여 핫스팟에 액세스하려면, 이 단추를 클릭하십시오. 팝업 창이 나타나 사용자 이름과 암호를 입력하고 인증을 수행합니다.

> **참고:** Google 및 Facebook 계정의 자격 증명 사용은 핫 스폿 소셜 로그인에서 *메뉴 바 ‣ 핫 스폿 ‣ 관리 인터페이스 ‣ 설정*에서 구성할 수 있습니다.

사용자 이름

사용자의 사용자 이름입니다.

암호

사용자의 암호.

새 계정 등록

등록되지 않은 사용자는 인터넷 서핑을 위한 새로운 계정을 만들 수 있습니다. 이는 SmartConnect™가 핫스팟에서 실행 중일 때만 허용됩니다. 새 계정 설정 절차는 아래에서 확인할 수 있습니다.

티켓 추가

사용자는 핫스팟에 액세스하기 위한 필수 요구 사항인 티켓을 구입할 수 있습니다. SmartConnect™가 활성화된 경우에도 이 옵션을 사용할 수 있습니다.

로그인

로그인 자격 증명을 제공한 후, 이 버튼을 클릭하면 핫스팟에 액세스 할 수 있습니다.

핫스팟이 서비스 약관에 동의하도록 구성되어 있는 경우, 두 경우 모두 로그인 버튼을 클릭하면, 창 아래쪽에 하나의 버튼이 있는 창이 열립니다.

이용 약관에 동의합니다

이 링크를 클릭하면, 서비스 약관이 표시된 창이 열립니다.

새 계정 등록

새로운 계정 등록 버튼을 클릭하면, 새로운 핫스팟 계정을 설정하고 활성화하는 4단계 마법사가 열립니다. 첫 번째 단계에서 사용자 계정이 만들어지며, 성공적인 생성을 위해 다음 필수 데이터가 필요합니다.

이름, 성

사용자의 이름과 성.

거리, 우편 번호, 도시, 국가

사용자가 거주하는 주소, 우편 번호, 도시 및 국가.

사용자 이름과 암호를 받기 위한 전화번호(Phonenumber)

드롭 다운 메뉴에서 사용할 수 있는 사용자 전화 번호의 국가 코드와 사용자의 실제 전화 번호를 차례로 선택합니다.

전화 번호 확인

전화 번호를 확인으로 다시 입력하십시오.

또한 계정을 만들려면, 서비스 약관에 동의합니다라는 링크 옆에 있는 확인란을 선택해야 합니다. 링크를 클릭하면, 서비스 약관이 있는 창이 열리고, 수락 전에 읽을 수 있습니다.

모든 데이터가 제공되고, 양식의 오른쪽 하단에 있는 Register 버튼을 클릭하면, 두 번째 단계로 연결됩니다. 등록 후 사용자 이름과 암호가 포함된 SMS가 전송되어 핫스팟에 대한 로그인을 인증합니다.

2단계에서 계정에 연결된 드롭 다운 메뉴에서 티켓을 선택하고 핫스팟을 사용하여 인터넷에 액세스하도록 허용합니다. 핫스팟 설정에 따라 무료 티켓 또는 선불 또는 후불 티켓 중 하나만 선택할 수 있습니다. 사용 가능한 티켓마다 이름, 기간 및 비용이 표시됩니다. 이 옵션을 사용하려면, 핫스팟에서 SmartConnect™를 활성화해야 하며, PayPal을 통한 지불을 설정해야 합니다.

티켓을 선택한 후, 계속 버튼을 클릭하여 3단계로 진행하십시오.

> **참고:** 선불 및 후불 티켓 구매에는 제한이 없지만 동시에 시간 기반 및 트래픽 기반 티켓을 가질 수는 없습니다. 즉, 하나 이상의 유효한 시간 기반 티켓을 소지한 클라이언트는 계정과 연관된 모든 유효한 시간 기반 티켓이 소비되거나 만료될 때까지 트래픽 기반 티켓을 구매할 수 없습니다. 트래픽 기반 티켓에도 동일하게 적용됩니다. 시간 기반 티켓을 구입하기 전에 모든 티켓을 사용

하거나 만료시켜야 합니다.

3단계에서 지불이 필요한 티켓을 선택하면 PayPal 웹 사이트로 리디렉션되어 거래에 필요한 데이터를 제공하고 신용 카드 또는 PayPal 계정을 사용하여 티켓 구매를 완료합니다. 그렇지 않은 경우, 무료 티켓을 선택하면, 이 단계는 건너 뛰고 프로세스는 4단계로 계속 진행됩니다.

4단계에서 성공적인 등록을 알리는 메시지가 나타나거나 등록 프로세스의 일부가 성공적이지 않은 경우에는 오류 메시지가 표시됩니다. 어쨌든 트랜잭션 ID 문자열도 보고됩니다. **트랜잭션 ID**는 추후 참조를 위해 적어 두거나 등록 프로세스 중에 문제가 발생하거나 연결 중에 문제가 발생할 경우에 사용됩니다. 전자의 경우 핫스팟 관리자에게 신속하게 연락하여 등록을 완료하고 로그인 자격 증명을 얻으십시오.

로그인

사용자 이름과 비밀번호를 제공한 후 로그인하면, 페이지의 정보제공 패널에 연결 상태에 대한 다양한 세부 정보가 표시됩니다. 이 페이지는 열려 있어야 합니다. 만약 닫히게 되면, 세션이 즉시 종료되고 핫스팟에 액세스하기 위한 새 로그인이 이루어져야 합니다. 다음 정보가 페이지에 표시됩니다.

남은 시간

총 소요 시간. 트래픽 기반 티켓을 사용할 때 *무제한* 문자열이 나타납니다.

세션 시간

현재 세션의 기간입니다.

남은 트래픽

현재 티켓에 사용할 수 있는 트래픽의 Gb에 대한 Mb 양입니다. *무제한* 문자열은 시간 기반 티켓을 사용할 때 나타납니다.

세션 트래픽

탐색하는 동안 교환된 데이터의 양. 총계가 제공되며, 다운로드 및 업로드된 데이터의 양도 대괄호 안에 표시됩니다.

유휴 시간 초과

기기의 유휴 시간, 즉 기기와 핫스팟 사이의 마지막 활동 이후 경과한 시간을 보여주는 카운트다운입니다. 카운트 다운이 0에 도달하면, 장치가 자동으로 연결 해제됩니다.

세션 시작 시간

세션 시작 시간의 타임 스탬프입니다.

자동 로그인 사용 중지

확인란을 선택하면, 사용자가 Smartlogin 설정에 관계없이 다시 연결될 때 인증해야 합니다. 그렇지 않고, 확인란이 선택되지 않으면, 핫스팟에 다시 연결할 때, 사용자가 인증할 필요가 없습니다.

> 참고: 이 옵션은 핫스팟 관리자가 SmartLogin 기능을 활성화한 경우에만 나타납니다.

패널 하단에는 두 개의 단추가 나타납니다.

탐색 시작

왼쪽에 있는 이 단추를 클릭하면, 브라우저에 핫스팟의 홈 페이지로 연결되는 새 탭이 열립니다.

로그 아웃

이 버튼을 클릭하면, 즉시 핫스팟에서 로그 아웃됩니다.

티켓 추가

핫스팟과 인터넷에 액세스하기 전에 유효한 티켓을 소유하고 있어야 합니다. 티켓을 구매하는 절차는 등록 프로세스의 2단계 및 3단계에서 설명한 것과 동일합니다.

스위치보드 메뉴 (선택적)

이 섹션에서는 다음과 같은 내용들을 살펴볼 수 있습니다.

- 대시보드
  - 연결
  - 맵
- 사용자
  - 사용자
    - 사용자
    - 그룹
    - 권한
    - 추가 사용자 정보
    - 프로비저닝
  - 그룹
    - 그룹
    - 멤버
- 장치
  - 장치
    - 게이트웨이
    - 그룹
    - 종점
    - 권한
    - 프로비저닝
    - 포트 포워딩
    - 위치
  - 그룹
    - 그룹
    - 멤버
    - 권한
- 응용프로그램
  - 응용프로그램
    - 응용프로그램
    - 고급 매개변수
  - 프로파일
- 조직
- 통계
  - 조직
  - 사용자
  - 장치

- 설정
  - 설정
  - 포털
  - 프로비저닝
- 로그
- 관리 센터
  - 장치
    - 상세
    - VPN
    - 패키지
    - 업데이트
    - 프로세스
    - Jobs
    - 하드웨어
  - 프로파일
    - 프로파일
    - 장치
      - 골드 게이트웨이
      - 대량 작업
      - 장치
- 클라이언트 다운로드
- 스위칭보드 API

이 섹션에서는 장치, 사용자 및 해당 권한에 대한 관리 옵션을 포함하여 Endian Switchboard와 이 기능이 제공하는 기능에 대해 설명합니다.

버전 5.0.5의 새로운 기능: *엔디안 관리 센터.*

Endian Switchboard는 **게이트웨이**를 통해 중앙 집중식 서버에 **엔드포인트**라는 다양한 원격 장치를 완벽하게 연결함으로써 복잡한 인프라를 제어 및 관리할 수 있는 VPN 기반 솔루션입니다. 원격 게이트웨이 및 엔드 포인트는 스위치 보드에서 직접 중앙에서 관리하거나 스위치 보드와 동일한 기능을 제공하는 데스크탑 애플리케이션인 Endian ConnectApp를 사용하여 중앙에서 관리할 수 있습니다. 장치는 **사용자**가 액세스하고 관리할 수 있으며, 스위치보드에서 작성 및 관리되고, 게이트웨이 및 엔드포인트에 대해 다른 **액세스 레벨**을 가질 수 있습니다. 엔드포인트는 **응용 프로그램 프로파일**을 사용하여 원격 워크스테이션에서 액세스할 수 있습니다.

게이트웨이를 Endian Network에 등록하고 Switch와 Green Zone 및 VPN 터널을 Switchboard에 구성하여 관리할 수 있는 **플러그 앤 커넥트 / 자동 등록** 절차를 활용하면 게이트웨이를 스위치보드에 몇 분만에 추가할 수 있습니다. **플러그 앤 커넥트** 절차가 성공적으로 완료되면, 스위치보드 사용자가 게이트웨

이를 즉시 사용할 수 있습니다.

> **추가 참고사항:** Plug & Connect 절차에 대한 자세한 설명은 *<http://help.endian.com/hc/en-us/>*에서 찾을 수 있습니다.

더 자세히 설명하자면, 여기에 아키텍처와 관련된 다양한 액터에 대한 설명이 있습니다.

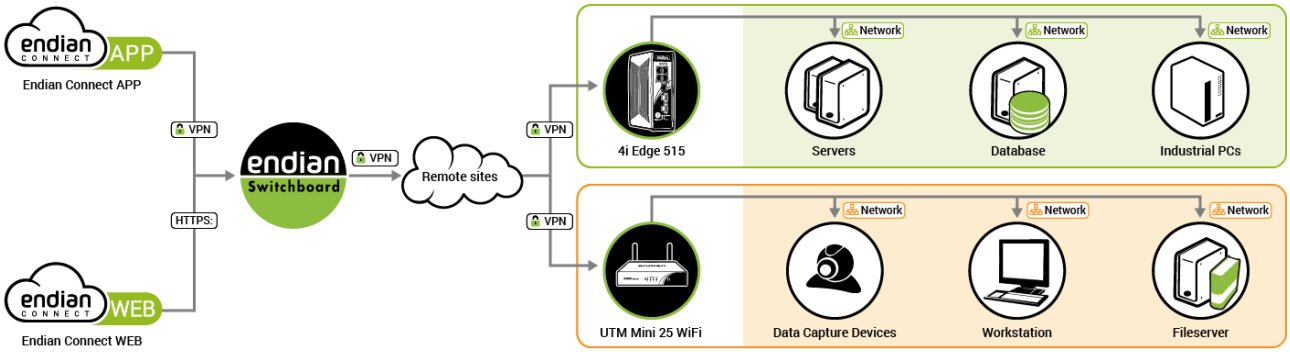


그림 1 : 가능한 관련 액터의 대부분이 표시된 스위치 보드 설치의 예.

스위치보드

스위치보드는 전체 인프라의 핵심입니다. 게이트웨이 및 사용자, 로그 파일, 액세스 정책에 대한 모든 구성 데이터를 저장하고 연결을 추적합니다. 두 가지 방법으로 액세스 할 수 있습니다.

1. GREENIP가 설치된 기기의 IP 주소인 GREENIP에서 **https://GREENIP:10443/manage/access** URL을 가리키는 브라우저를 사용하여 접근합니다.
2. 스위치보드가 설치된 기기에 원격으로 액세스하는 워크스테이션에 ConnectApp를 설치하여 접근합니다.

엔드포인트

엔드포인트는 원칙적으로 인터넷을 통해 연결할 수 있는 모든 종류의 장비가 될 수 있으므로, 원격 워크스테이션, 서버 등 모든 종류의 산업 기계가 될 수 있습니다. 각 엔드포인트는 자체 IP 주소를 가지며, 게이트웨이가 아닌 다른 방법으로 로컬 네트워크 및/또는 인터넷에 연결할 수 있습니다. 유일한 요구 사항은 엔드포인트가 게이트웨이에 의해 도달할 수 있어야 한다는 것입니다.

각 엔드포인트는 하나의 게이트웨이에만 연결될 수 있으며, 게이트웨이의 GREEN 네트워크 내에 있는 고유한 IP 주소 (아키텍처에서 가상 IP라고 함)를 수신합니다. 엔드포인트의 가상 IP는 네트워크의 크기가 조정되어야 할 때, 변경될 수 있습니다 (예: 네트워크에 새 엔드포인트가 추가되는 경우).

게이트웨이

게이트웨이는 교환기가 관리할 수 있는 문이며, 엔드포인트에 대한 연결을 허용합니다. 게이트웨이 프로비저닝을 사용하여 쉽게 구성하고 활성화할 수 있습니다. 게이트웨이는 VPN 터널을 통해, 스위치보드에 직접 연결되며, 스위치보드와 엔드포인트 간의 라우팅 연결을 처리합니다.

게이트웨이는 그룹으로 구성할 수 있으며, 일반적으로 "일반" 모달리티입니다. GREEN 인터페이스를 사용하여 제어하는 엔드포인트와 RED 인터페이스를 사용하여 인터넷에 연결합니다. 일부 특정 설정에서 게이트웨이는 업링크와 네트워크 모두에 고유한 영역으로 설정될 수 있습니다. GREEN 서브넷은 엔드포인트 수가 증가할 때 크기에 맞게 조정할 수 있습니다.

장치

장치를 이용하여, 엔드포인트 또는 게이트웨이로 사용할 수 있습니다.

사용자

사용자는 어떤 식으로든 스위치보드, 게이트웨이 또는 엔드포인트에 액세스하여 상호 작용할 수 있는 모든 사람을 말합니다. 사용자는 그룹의 구성원이거나 관리자인 두 가지 역할을 수행할 수 있는 사용자 그룹으로 배열될 수 있습니다. 후자의 경우, 그는 그룹 구성원을 관리할 수 있습니다.

응용프로그램 프로필

응용프로그램은 원격 워크스테이션에서 원격으로 엔드포인트에 액세스하는 한 방법이며, 워크스테이션의 경로와 프로그램 실행 파일 및 선택적 명령 인수에 의해 정의됩니다. 엔드포인트에 연결할 수 있는 몇 가지 가능성이 있기 때문에, 동일한 유형의 엔드포인트에 액세스 할 수 있는 모든 가능성을 포함하는 응용프로그램을 응용프로그램 프로파일에 함께 그룹화 할 수 있습니다. 각 엔드포인트에는 연결된 하나의 응용프로그램 프로파일이 있으며, 이 프로파일은 도달할 수 있는 모든 가능성을 정의합니다.

액세스 정책

교환기의 기본 액세스 정책은 사용자가 하나 이상의 게이트웨이 및 이 게이트웨이가 관리하는 모든 엔드포인트에 대한 액세스 권한을 가질 수 있다는 것입니다.

사용자, 장치, 응용프로그램, 조직을 관리하고 API를 사용할 수 있는 기능을 포함하여 사용자에게 더 많은 고급 사용 권한을 부여할 수 있습니다.

독점적인 접근

Endian Switchboard는 종점, 게이트웨이 또는 조직 수준에서 부여할 수 있는 Exclusive 액세스라는

추가 액세스 정책을 구현합니다. 이 정책을 사용하면, 한 번에 한 명의 사용자만 해당 구성 요소에 연결할 수 있습니다. 다른 사용자가 이 구성 요소에 액세스하려고 시도하면, 다른 사용자가 연결하려고 시도할 때, 스위치보드가 연결을 차단합니다. 이 정책의 근거는 사용자가 인프라의 중요한 부분 (예: 여러 가지 감각적인 엔드포인트를 제어하는 게이트웨이)에서 작업할 때, 다른 사람이 간섭할 수 없다는 것입니다.

이 정책은 전역적으로 설정됩니다. 동일한 스위치보드 설치에서는 독점 액세스를 허용하는 일부 조직 (게이트웨이, 엔드 포인트)과 그렇지 않은 조직 (게이트웨이, 엔드 포인트)이 있을 수 없습니다. 또한 정책은 계층 구조의 아래쪽으로 전파됩니다. 조직이 독점 액세스로 설정된 경우, 모든 게이트웨이에도 독점 액세스 세트와 엔드포인트가 있습니다.

마지막으로 이 정책을 사용 중지하면, 모든 인프라에 대한 동시 액세스가 모든 사람에게 부여됩니다.

조직

규모가 크고, 복잡한 시나리오가 전개된 경우에, 스위치보드에 있는 사용자 및 장치 관리는 사용 가능한 모든 리소스를 조직이라고 하는 작고 독립적인 단위로 나누어 단순화할 수 있습니다. 조직은 계층 구조로 구성될 수 있으며, 각 조직은 사용자, 장치 및 응용프로그램 프로파일로 구성됩니다. 루트 조직은 루트 노드 특성이라고 하는 고유한 설정을 유지합니다 (자세한 내용은 조직 참조). 일반적으로 하위 조직은 액세스 정책과 응용프로그램 프로필을 상속받지만 재정의 할 수는 있습니다.

계기반

이 페이지는 스위치 보드에 의해 관리되는 엔드포인트와 게이트웨이에 대한 많은 정보를 표시하며, 연결 및 맵이라는 두 개의 탭으로 나뉩니다. 전자는 장치에 대한 연결 정보를 포함하고, 후자는 장치의 위치가 구성된 경우, 장치를 세계지도에 표시합니다.

연결

이 페이지에는 스위치 보드에 구성된 모든 장치와 각 장치에 대한 다음 정보가 표시된 표가 있습니다.

- 두 가지 유형의 객체 (게이트웨이  및 끝점 )를 포함할 수 있는 장치 이름이며, 후자는 해당 역할과 연결된 게이트웨이를 강조 표시하기 위해 들여 쓰기 되어 있습니다. 장치의 아이콘이 오프라인이면 회색으로 표시되고, 누군가가 연결되어 있으면 녹색으로 표시됩니다.

  > **참고:** 게이트웨이 왼쪽의 작은 삼각형은 해당 게이트웨이가 관리하는 하나 이상의 엔드 포인트가 있음을 나타냅니다.

- 장치가 속한 그룹입니다.
- 장치에 대한 설명.
- 문자열 및 다음 아이콘 중 하나로 표시되는 장치의 상태는 다음과 같습니다:
    - Online: 장치가 온라인 상태이고 연결을 허용합니다.
    - Offline: 장치가 스위치보드에 연결되어 있지 않습니다.
    - Connected: 로컬 워크스테이션에서 장치에 연결되어 있습니다.
    - In use: 장치에 누군가가 연결되어 있지만 동시에 연결을 설정할 수 있습니다.
    - Busy: 장치에 독점 액세스가 활성화되었기 때문에, 누군가가 장치에 연결되어 있고, 연결을 끊을 때까지 연결할 수 없습니다.

이 테이블 위에는 스위치를 클릭하여, 모든 엔드포인트를 한 번에 숨기거나 표시할 수 있으며, 오른쪽에는 스위치보드에 정의된 모든 장치를 검색하는데 유용한 필터가 나타납니다. 일치하는 장치는 한 문자가 쓰여 지자마자 나타나며, 일치하지 않는 모든 장치를 숨깁니다. 검색은 테이블의 모든 필드에서 이루어지므로 필터링이 보다 효율적입니다.

장치, 게이트웨이 또는 엔드포인트를 클릭하면, 장치에 대한 다양한 유형의 정보를 보여주는 오버레이가 나타납니다.

상단에는 장치 및 장치의 이름과 상태 (온라인 또는 오프라인)가 표시됩니다.

중간 섹션에는 응용 프로그램 및 로그라는 두 개의 탭이 있습니다. 첫 번째 응용프로그램에는 장치에 연결하는데 사용할 수 있는 응용 프로그램 목록이 있습니다. 범례는 장치 상태에 대해 알려줍니다.

- 활성화(Active). 현재 워크스테이션에서 스위치보드에 대한 지속적인 연결이 있습니다.
- 바쁜(Busy). 다른 사용자가 다른 위치에서 기기에 연결 중입니다.
- 비활성(Inactive). 장치에 연결되어 있지 않습니다.

로그 탭에는 선택한 장치에서 발생한 모든 동작과 이벤트가 포함됩니다. 여기에 표시된 로그는 장치 이름을 포함하는 필터를 적용할 때, 스위치보드의 로그 섹션에서 볼 수 있는 로그와 동일합니다. 테이블에 포함된 데이터 및 기록된 작업에 대한 자세한 내용은 위에서 언급한 로그 섹션에서 확인할 수 있습니다.

맨 아래쪽에 표시되는 정보는 장치에 따라 달라집니다. 게이트웨이의 경우, 이름과 조직이 표시되고 엔드포인트의 경우, 실제 IP 주소와 가상 IP 주소 및 도달할 수 있는 게이트웨이가 표시됩니다.

> **참고:** 끝점에 원격으로 연결하려면, 응용프로그램은 대부분의 경우에 스위치 보드에서 할당한 가상 IP 주소를 사용하지만 경우에 따라 실제 IP 주소가 필요합니다.

맵

Switchboard Map은 OpenStreetMap 및 전단지를 기반으로 구성된 모든 게이트웨이 및 엔드포인트를 세

계 지도에 표시하는 유용한 기능입니다. 어플라이언스를 지도에 표시하려면, 올바른 주소로 적절히 구성해야합니다.

장치 옆에 있는 아이콘을 클릭한 다음, *위치* 탭에서 *Menubar ‣ Switchboard ‣ Devices* 아래에서 각 장치에 대해 개별적으로 위치를 설정할 수 있습니다. 자세한 내용은 여기를 참조하십시오.

지도 탭을 처음 열었을 때, 이미 정의된 위치가 있는 장치가 없으면, 오버레이 상자에 지금 또는 나중에 정의할지 묻습니다. 나중에 설정을 클릭하면 지도가 나타나고, 위치 설정을 클릭하면 위치가 없는 기기 목록이 열립니다.

여기에서 각 장치에 대해 주어진 텍스트 필드에 도시와 주소를 작성한 다음, 오른쪽에 있는 아이콘을 클릭하여 위치를 확인하십시오. 빠른 검색은 OpenStreetMap에서 검색된 정확한 이름을 표시하며, 장치는 즉시 지도에 배치되어 표시됩니다. 검색 아이콘을 대체하는 체크 표시를 클릭하면, 방금 배치된 게이트웨이가 지도에 표시됩니다. 주소가 없으면, 검색 아이콘이 로 바뀝니다.

오버레이를 종료하려면 오른쪽 상단의 **X**를 클릭하기만 하면 위치가 설정된 모든 장치가 지도에 표시됩니다.

지도를 열 때, 세계지도는 위치 정보가 알려진 모든 장치를 보여줍니다. 각 장치는 이름과 아이콘으로 식별되며, 일부 정보를 표시하기 위해 클릭할 수 있습니다. 지도 주변에서 많은 위젯이 지도에서 다른 작업을 수행할 수 있습니다.

오른쪽 상단의 검색 창을 사용하면, 특정 장치를 빠르게 찾을 수 있습니다. 몇 개의 글자가 쓰여진 후 결과가 하나만 있으면, 즉시지도에 표시되고, 그렇지 않으면, 가능한 일치 항목 목록이 표시되어 원하는 것을 선택할 수 있습니다.

왼쪽에는 지도에 몇 가지 작업을 수행할 수 있는 몇 가지 아이콘이 있습니다.

- 지도를 확대하십시오.
- 지도를 축소합니다.
- 지도를 전체 화면으로 엽니다.
- 새 탭에서 지도를 엽니다.
- 장치의 위치 목록을 열어 검사하거나 수정합니다.

지도가 검색 모드인지 일반 모드인지에 따라 오른쪽 하단에 버튼이 표시됩니다.

검색 종료 (ESC)

현재 검색에서 빠져 나와 전체지도로 돌아갑니다.

필터 재설정 (ESC)

현재 필터를 재설정하십시오.

> **힌트:** 버튼 단축키로 ESC 키를 누릅니다.

사용자

이 페이지는 사용자 및 그룹이라는 두 개의 탭으로 구성됩니다. 전자의 경우 사용자 관리가 수행될 수 있지만, 후자의 경우 사용자는 그룹으로 정렬될 수 있습니다.

사용자들

이 페이지에서 스위치보드에 연결할 권한이 있는 모든 사용자는 다음 데이터가 표시된 테이블에 나열됩니다.

- 사용자 이름으로도 작동하는 사용자의 전자 메일입니다.
- 사용자에 대한 설명 (예: 실제 이름).
- 사용자가 속한 그룹입니다.
- 각 사용자에 대해 수행할 수 있는 작업은 다음과 같습니다.
  - ☑ ☐ - 사용자를 활성화 또는 비활성화합니다.
  -  - 사용자를 수정합니다.
  - - 사용자를 삭제합니다.
  -  - 사용자의 활동 로그를 참조하십시오.

페이지 상단의 `사용자 추가` 링크를 클릭하면, 새 사용자를 추가할 수 있으며, 사용자가 스위치보드에 연결하는데 필요한 인증서는 `CA 인증서 다운로드` 링크를 클릭하여, 다운로드 할 수 있습니다.

사용자 편집기에서 정의할 수 있는 구성 옵션은 *사용자, 그룹, 사용 권한, 추가 사용자 정보* 및 *프로비저닝* 탭으로 그룹화됩니다.

사용자

이 탭에서는 사용자에 대한 기본 정보에 액세스할 수 있습니다.

이메일 주소

새 사용자의 사용자 이름입니다. 고유해야 합니다.

조직

사용자가 속한 조직입니다. 이 옵션은 하나 이상의 조직이 생성된 경우에만 사용할 수 있습니다.

설명

사용자의 실제 이름 또는 설명.

암호, 암호 확인

사용자의 암호를 두 번 쓰십시오. 암호는 8자 이상이어야 하며, 영숫자가 아닌 문자가 포함되어야 합니다.

그룹

이 탭에는 사용자가 속한 그룹을 선택할 수 있는 다중 선택 상자가 있습니다. 하나 이상의 사용자 그룹이 정의되어 있어야 합니다.

사용자 그룹의 역할

모든 그룹에서 사용자가 취할 수 있는 역할은 구성원 또는 관리자의 역할을 갖습니다. 선택한 그룹당 하나의 역할을 선택할 수 있습니다.

권한

이 탭에서는 사용자가 교환기의 다른 노드와 사용자에 대한 사용 권한을 선택할 수 있습니다. 다중 선택 입력란의 오른쪽 열에 있는 항목은 사용자에게 부여된 권한이지만 왼쪽 열에 있는 항목은 사용자가 사용할 수 없습니다. 해당 항목의 오른쪽에 있는 + 를 클릭하여 권한을 부여하십시오. 그리고 - 를 클릭하여 권한을 제거할 수 있습니다.

전역 권한

사용자에게 여러 권한을 부여할 수 있습니다.

- *수퍼 유저 (모든 권한):* 사용자는 스위치보드를 완벽하게 관리할 수 있습니다.
- *하위 조직에 대한 액세스:* 사용자는 조직에 액세스할 수 있습니다.
- *사용자 관리.* 사용자는 다른 사용자를 관리할 수 있습니다.
- *장치 관리.* 사용자는 장치를 관리할 수 있습니다.
- *응용프로그램 관리:* 사용자가 작업(actions)을 관리할 수 있습니다.
- *조직 관리:* 사용자는 조직을 관리할 수 있습니다.
- *API 사용:* 사용자는 스위치보드의 API를 액세스하고 사용할 수 있습니다.
- Green | Blue | Orange 구역으로의 경로 푸시: 이 옵션 중 하나 이상을 선택하면, 스위치보드에 의해 관리되는 서브넷에 대한 적절한 경로가 사용자에게 푸시됩니다.

이러한 값의 조합을 사용자와 연결할 수 있습니다.

> **힌트:** 한번에 모든 권한을 할당하거나 제거할 수 있는 `모두 추가` 및 `모두 제거`라는 이 두개의 단축키를 사용하는 것이 가능합니다.

추가 사용자 정보

이 탭에는 인증에 사용할 인증서를 포함하여, 사용자에 대한 보다 자세한 정보가 제공될 수 있습니다.

주소, 주소 2

필요한 경우, 사용자의 주소를 두 줄로 나눠서 입력합니다.

도시

사용자가 거주하고 있는 도시입니다.

우편 번호

사용자가 거주하는 도시의 우편 번호.

주 또는 지방

사용자가 위치한 주 또는 지방.

국가

사용자가 위치한 국가 (드롭 다운 메뉴에서 선택)

직업

사용자의 직업 또는 역할.

인증서 구성

드롭 다운 메뉴에서 사용자의 인증서를 구성할 수 있습니다. 사용 가능한 옵션은 다음과 같습니다.

- **변경하지 마십시오.** 현재 인증서를 그대로 두십시오. 사용자가 아직 인증서를 갖고 있지 않다면, 인증서를 만들어야 합니다.
- **새 인증서를 생성하십시오.** 인증서를 만듭니다.
- **인증서를 업로드하십시오.** 사용자 인증서를 업로드하십시오.
- **인증서 요청을 업로드하십시오.** 사용자 인증서 요청을 업로드하십시오.

사용자에게 할당된 인증서가 없으면, *'인증서 구성'을 통한 인증서 작성하시오* 라는 메시지가 표시됩니다.

선택을 변경하지 마십시오 라는 메시지를 제외하고, 옵션을 선택할 때, 추가 옵션이 나타납니다.

*새 인증서 생성*을 선택함으로써, 다음과 같은 새 옵션이 제공됩니다.

조직 단위 이름

사용자가 속한 조직 단위의 이름.

조직 이름

사용자 조직의 이름입니다.

제목 대체 이름

인증서 제목에 대한 대체 이름입니다.

인증서 요약 알고리즘

선택된 인증서를 암호화하는데 사용되는 알고리즘으로 사용 가능한 옵션은 다음과 같습니다: **SHA1, SHA2 224, SHA2 256, SHA2 384** 또는 **SHA2 512.**

PKCS12 파일 암호, PKCS12 파일 암호 확인

인증서가 저장된 파일을 보호하기 위한 암호입니다.

유효 기간 (일)

인증서가 얼마 기간 동안 유효한지를 일(day)로 표시합니다.

인증서 *업로드*를 선택하면 다음과 같은 옵션들이 표시됩니다:

인증서 (PKCS12 / PEM)

찾아보기 버튼이나 텍스트 필드를 클릭하면, 파일 선택기가 업로드 할 인증서의 경로를 제공하면서 열립니다.

PKCS12 파일 암호

필요한 경우, 인증서의 비밀번호입니다.

마지막으로, 다음 두 옵션이 *인증서 요청 업로드*의 선택 항목과 함께 나타납니다.

인증서 서명 요청 (CSR)

찾아보기 버튼이나 텍스트 필드를 클릭하면, 업로드 할 CSR 경로를 제공하는 파일 선택기가 열립니다.

유효 기간 (일)

인증서가 얼마 기간동안 유효한지를 나타냅니다.

프로비저닝

이 탭에는 사용자의 엔디안 네트워크 자격 증명 관리를 위한 두 가지 옵션이 표시됩니다.

엔디안 네트워크 계정

엔디안 네트워크에 액세스하는데 사용되는 사용자 이름

엔디안 네트워크 암호 또는 등록 키

엔디안 네트워크 계정의 암호 또는 Endian UTM 어플라이언스의 등록 키입니다.

그룹들

사용자 그룹은 특정 역할 및 권한을 가진 하나 이상의 게이트웨이 또는 게이트웨이 그룹에 액세스 할 수 있는 사용자 집합입니다.

이 페이지에는 처음에 `새 사용자 그룹 추가` 링크와 모든 그룹 목록과 그 그룹에 대한 일부 정보가 있는 빈 테이블만 표시됩니다.

- 그룹에 할당된 이름입니다.
- 그룹에 대한 설명.
- 그것들 각각에서 가능한 행동 :
  -  - 사용자 그룹을 수정합니다.
  -  - 사용자 그룹을 제거합니다.
  -  - 사용자 그룹의 로그 파일을 보여줍니다.

`새 사용자 그룹 추가` 링크를 클릭하면 (하나 이상의 그룹이 이미 존재할 때, `그룹 추가`가 되는), 편집기가 테이블 바로 위에 열립니다. 편집기를 구성하는 세 개의 탭에서, 다음 데이터를 제공하여 새 사용자 그룹을 정의할 수 있습니다.

그룹

새 사용자 그룹을 정의하는 탭입니다.

그룹 이름

그룹에 주어진 이름. 그것은 필수적이며 고유해야 합니다.

조직

그룹이 속한 조직입니다. 이 옵션은 하나 이상의 조직이 생성된 경우에만 사용할 수 있습니다.

설명

그룹에 대한 설명.

회원들

이 탭에서는 다중 선택 상자를 사용하여, 그룹에 사용자를 추가할 수 있습니다.

이 사용자 그룹에서의 사용자 역할

그룹에 속한 사용자 및 그들의 역할 선택: 다중 선택 상자에서 다음을 클릭하여 *추가*합니다. 그룹의 *구성원*이거나 *관리자*로서의 역할을 선택한 다음, 각 사용자 옆에 있는 `+` 를 클릭하여 역할을 선택합니다.

장치들

이 페이지에는 스위치보드에서 도달할 수 있는 모든 장치를 관리하는 *장치(Devices)* 탭과 장치 그룹을 구성하는 *그룹(Groups)*이라는 두 개의 탭이 있습니다.

장치들

이 페이지에는 이미 구성된 모든 게이트웨이 목록이 포함된 테이블이 표시됩니다. 여기에는 다음 정보가 들어 있습니다.

- 게이트웨이의 이름.
- 게이트웨이에 대한 설명.
- 게이트웨이의 일련 번호입니다.
- 게이트웨이가 속한 그룹입니다.
- 사용 가능한 작업 :
    - ☑☐ - 게이트웨이를 활성화 또는 비활성화합니다.
    -  - 게이트웨이를 수정합니다.
    -  - 게이트웨이를 복사합니다.
    -  - 게이트웨이를 제거합니다.
    -  - 게이트웨이의 활동 로그를 참조하십시오.
    -  - 게이트웨이 구성을 다운로드합니다.

> **참고:** 게이트웨이의 구성은 모든 구성 옵션과 게이트웨이에서 사용하는 인증서가 포함된 텍스트 파일입니다.

표 위에는 세 개의 링크가 표시됩니다.

첫 번째는 `Plug & Connect (자동 등록)`로, 스위치보드에 대한 원격 게이트웨이의 등록을 시작할 수 있습

니다. 이 3단계 절차를 수행하려면, 인터넷에 연결된 원격 장치와 해당 장치에 대한 유효한 정품 인증 코드가 필요합니다. 링크를 클릭하면, 하나의 옵션만 사용할 수 있는 새 패널이 나타납니다.

활성화 코드

연결할 원격 장치의 활성화 코드를 제공하십시오.

Next (다음) 버튼을 클릭하면, Appliance의 이미지와 몇 가지 옵션이 표시된 새로운 화면이 나타납니다.

설명

어플라이언스에 대한 설명. 기본값으로 자체 생성 값을 사용할 수 있습니다.

관리자 비밀번호

HTTPS로 어플라이언스에 액세스 할 관리자의 암호를 입력하십시오.

루트 암호

SSH 또는 콘솔에 의해 어플라이언스에 액세스 할 루트 사용자의 암호를 입력하십시오.

admin 및 root 사용자에게 동일한 비밀번호 사용

두 사용자 모두에게 동일한 암호를 사용하려면, 이 확인란을 선택하십시오.

이 단계가 끝나면 절차의 마지막 단계에서 원격 기기의 WAN 포트를 인터넷에 연결해야 합니다.

> **힌트:** 원격 장치는 절차를 성공적으로 완료하려면, 포트 443 TCP를 사용하여 통신할 수 있어야 합니다.

몇 분 후에 새 게이트웨이가 스위치보드에 이미 등록된 게이트웨이를 따라 목록에 표시됩니다. 몇 가지 이유로 인해 절차가 성공적이지 않은 경우 문제 해결 문서에 대한 링크와 함께 오류 메시지가 표시됩니다.

추가 참고사항: 자세한 요구 사항, 보다 자세한 설명 및 문제 해결 옵션을 포함하는 plug & connect (플러그 및 연결) 절차에 대한 자세한 설명은 이 문서 *<http://help.endian.com/hc/en-us/>*에서 찾을 수 있습니다.

게이트웨이 추가 링크를 클릭하면, 게이트웨이 편집기가 테이블 바로 위에 열리고 새로운 장치를 만들 수 있습니다. 편집기는 게이트웨이의 모든 다른 옵션을 구성할 수 있는 몇 개의 탭 페이지로 구성됩니

다.

Download CA certificate 링크를 클릭하면, 교환기의 CA 인증서가 다운로드됩니다. 이 인증서는 장치 자체에서 VPN 연결을 구성할 때 사용해야 합니다.

게이트웨이

이 탭에는 게이트웨이의 기본 설치 옵션이 있습니다.

이름

새 게이트웨이에 할당된 이름으로 고유해야 합니다. 기본 이름이 생성되지만, 원하는대로 변경할 수 있습니다.

조직

게이트웨이가 속한 조직입니다. 이 옵션은 하나 이상의 조직이 생성된 경우에만 사용할 수 있습니다.

설명

장치에 대한 설명.

일련 번호

게이트웨이의 일련 번호입니다. 이 옵션은 *자동 등록*이 활성화되지 않은 경우에만 표시됩니다.

암호, 암호 확인

게이트웨이에 액세스하기 위한 암호. 텍스트 상자의 오른쪽에 있는 확인란을 선택하면, 일반 텍스트로 암호가 표시됩니다. 이 옵션은 자동 등록이 비활성화된 경우에만 표시됩니다.

활성화

장치를 사용하려면, 확인란을 선택하십시오.

그룹들

이 탭에서는 게이트웨이가 속할 그룹을 선택할 수 있습니다.

엔드포인트

이 탭에는 게이트웨이에서 도달할 수 있고, 이를 관리하는데 사용할 수 있는 모든 엔드 포인트에 대한 정보가 들어 있습니다.

최대 엔드포인트 수

제공될 첫 번째 정보는 게이트웨이가 관리할 엔드포인트의 대략적인 추정치입니다.

> **참고:** 이 정보는 각 끝점에 할당된 모든 IP를 수용할 수 있는 가상 네트워크를 만드는데 사용되므로 특히 중요합니다. 의심스러운 경우, 실제 엔드포인트 수보다 큰 크기를 선택하거나 네트워크가 추가 엔드포인트를 수용하기에 충분하지 않을 것입니다.

지역 네트워크

CIDR 표기법으로 엔드포인트가 사용하는 네트워크.

실제 IP를 가상 IP로 변환하지 마십시오.

이 확인란을 선택하면, 가상 IP 주소를 통해가 아니라 실제 IP 주소를 통해 엔드포인트에 액세스할 수 있습니다.

가상 네트워크

엔드포인트에 할당할 가상 IP 주소입니다.

> **참고:** 스위치보드 설정 섹션에서 *자동 가상 서브넷 할당 사용 옵션이 활성화된* 경우, 이 옵션은 나타나지 않습니다. 사실, 각 엔드포인트의 IP 주소는 위에서 언급한 옵션을 사용하여 자동으로 할당됩니다.

엔드포인트

다음 정보와 함께 게이트웨이가 제어하는 모든 엔드 포인트를 보여주는 표.

- 엔드 포인트의 이름.
- 엔드 포인트의 IP 주소.
- 엔드 포인트에 대한 설명.
- 엔드 포인트에 액세스하는 데 사용되는 어플리케이션 프로파일.
- *사용 가능* 상태, 즉 엔드 포인트의 활성 여부.
- *Source Nat* 상태. 만약 활성 상태 ("예")인 경우, 엔드포인트는 모든 트래픽을 게이트웨이에서 시작된 것으로 간주합니다. 이 설정은 예를 들어 엔드포인트가 방화벽 뒤에 있고 외부와 통신할 수 없는 경우에 유용할 수 있습니다.
- 사용자 정의 필드.

각 테이블 행의 각 필드는 두 번 클릭하여 편집할 수 있습니다. 전달되는 정보의 유형에 따라 각 필드에 드롭 다운 메뉴 (즉, *사용 가능(Enabled)* 열 또는 *응용프로그램 프로파일*에 사용 가능한 프로파일에 대한 "예-아니오" 선택) 또는 텍스트 필드 (다른 모든 프로파일)가 표시될 수 있습니다.

엔드포인트 관리는 테이블 하단의 단추를 사용하여 수행할 수 있습니다.

행 추가

이 옵션을 사용하면, 새 엔드포인트를 게이트웨이에 추가할 수 있습니다. 새로운 행의 필드를 두 번 클릭하여 구성을 수행할 수 있습니다.

행 삭제

이 버튼을 클릭하면, 강조 표시된 엔드포인트가 게이트웨이에서 제거됩니다. 이 버튼은 하나의 행이 선택된 경우에만 활성화됩니다.

> **경고:** 행 삭제는 즉시 수행되며 되돌릴 수 없습니다.

CSV 표시

이 버튼은 모든 엔드포인트의 구성을 내보내는데, 유용한 CSV 형식의 테이블에 있는 동일한 정보를 포함하는 텍스트 필드로 표를 전환합니다.

유효성 검사

강조 표시된 행에 삽입된 정보가 유효한지 확인하십시오.

권한

이 게이트웨이에 액세스해야 하는 사용자 또는 사용자 그룹은이 탭의 다중 선택 상자에서 추가할 수 있습니다. 각 사용자는 *일반 사용자* 또는 게이트웨이 *관리자* 역할을 맡을 수 있습니다.

그룹을 선택하면 해당 그룹의 모든 구성원을 *일반 사용자* 또는 *관리자*로 선택할 수 있습니다.

프로비저닝

이 섹션에서는 원격 게이트웨이의 구성을 정의할 수 있습니다. 사용 가능한 구성 옵션은 다음과 같습니다.

모델

드롭 다운 메뉴에서 사용 가능한 장치 모델을 선택하십시오.

활성화 코드

게이트웨이 설정에 사용되는 활성화 코드.

모델을 선택한 직후에 모델의 모든 구성 옵션이 표시되고 구성할 수 있습니다.

> **참고:** 선택한 모델의 유형에 따라, 사용 가능한 옵션 중 일부가 적절한 값으로 채워집니다.

루트 암호

SSH (콘솔) 액세스에 사용되는 루트 사용자의 암호를 선택하십시오.

관리자 비밀번호

HTTPS (브라우저) 액세스에 사용되는 관리자의 비밀번호를 선택하십시오.

호스트 이름

게이트웨이의 호스트 이름

도메인 이름

게이트웨이의 도메인 이름입니다.

회사

게이트웨이가 속한 회사

이메일

게이트웨이에 대한 참조 전자 메일 (일반적으로 해당 게이트웨이에 대한 책임자의 전자 메일)입니다.

시간대

게이트웨이가 위치해 있는 표준 시간대입니다.

국가

게이트웨이가 위치한 국가.

레드 타입

RED 인터페이스의 유형, 즉 게이트웨이가 인터넷에 어떻게 연결하는 방법. **DHCP, Static(정적), 업링크 없음(No uplink)** 및 **3G**의 네 가지 유형을 사용할 수 있습니다. 자세한 내용은 네트워크 구성을 참조하십시오.

레드 장치

게이트웨이를 인터넷에 연결하는 인터페이스입니다. 이 드롭 다운 메뉴에서 사용할 수 있는 옵션은 위에서 선택한 *모델*에 따라 결정됩니다. *레드 유형*을 **업링크 없음(No uplink)**으로 설정하면,

이 옵션이 표시되지 않습니다.

선택한 옵션의 빨간색 장치에 따라 다음 옵션이 표시됩니다. **DHCP**를 선택하면 아무 것도 나타나지 않습니다.

레드 IP / CIDR

RED 인터페이스의 IP 주소. 이 옵션은 RED 유형이 **정적(Static)**인 경우에만 나타납니다.

레드 게이트웨이 IP

RED 인터페이스용 게이트웨이의 IP 주소입니다. 이 옵션과 다음 옵션은 인터넷에 액세스하는데 필요하며 RED 유형이 **정적** 또는 **업링크 없음**인 경우에만 나타납니다.

DNS 서버

게이트웨이에서 사용하는 DNS 서버의 IP 주소입니다 (한 줄에 하나씩). RED 유형이 **Static (정적)** 이거나 **No uplink (업링크 없음)**인 경우에만 나타납니다.

액세스 포인트 이름

액세스 포인트의 이름은 **3G/4G** 및 **UMTS** 적색 유형에서만 나타납니다.

모뎀 유형

이 옵션은 **3G/4G** 레드 유형에만 나타나며, 드롭 다운 메뉴에서 사용할 모뎀 유형을 **3G/4G** 또는 **CDMA**로 선택할 수 있습니다

Green 장치

Green 구역의 인터페이스, 즉, 엔드포인트가 있는 영역의 인터페이스입니다.

Green IP/CIDR

Green 영역에 할당된 IP 주소 풀입니다.

Blue 장치

Blue 구역의 인터페이스.

Blue IP/CIDR

Blue 구역에 할당된 IP 주소 풀입니다.

오렌지 장치

ORANGE 영역의 인터페이스.

Orange IP/CIDR

ORANGE 영역에 할당된 IP 주소 풀입니다.

사용자 정의 OpenVPN 서버 IP/FQDN, 포트 및 프로토콜

엔드포인트에서 OpenVPN 서버에 연결하는데 사용하는 사용자 지정 주소입니다.

> **힌트:** 이 옵션과 다음 옵션의 주소에 사용되는 형식은 **hostname.domain:port:protocol** 또는 **IP.address:port:protocol**이며 포트 또는 프로토콜은 선택 사항이므로, 유효한 값은 **vpn.example.com:1197:udp**와 **123.45.67.89:1192**입니다. 프로토콜이 지정되면 포트도 지정해야 합니다.

사용자 지정 OpenVPN 폴백 IP 주소 / FQDN, 포트 및 프로토콜

엔드포인트가 폴백(대체) OpenVPN 서버에 연결하는데 사용하는 사용자 정의 주소입니다.

HTTP 프록시를 통한 OpenVPN

게이트웨이가 인터넷 연결을 위해 프록시를 사용할 때, 체크 박스를 선택하십시오. 다음 네 가지 옵션이 해당 프록시를 구성하는데 표시됩니다.

업스트림 서버

업스트림 프록시 서버의 IP 주소입니다.

업스트림 포트

프록시 서비스가 서버에서 실행되는 포트입니다.

업스트림 사용자 이름

필요한 경우, 프록시 서버에 연결할 사용자 이름입니다.

업스트림 비밀 번호

필요한 경우, 프록시 서버에 연결할 암호입니다.

업스트림 NTLM 프록시 인증

업스트림 HTTP 프록시에 NTLM 인증이 필요한 경우 확인란을 클릭하십시오.

프록시 사용자 에이전트 구축

업스트림 HTTP 프록시가 주어진 사용자 에이전트와 접촉해야 하는 경우, 여기에 작성하십시오.

포트 포워딩

이 탭의 옵션을 사용하여 게이트웨이에서 엔드 포인트에서 지정된 호스트로 오는 트래픽을 리디렉션 할 수 있는 적합한 포트 전달 규칙을 정의할 수 있습니다.

표에는 각 엔드 포인트에 대한 다음 정보가 들어 있습니다.

- 엔드포인트. 규칙이 정의된 엔드포인트입니다. 엔드포인트가 이미 설정되어 있지 않으면, 선택 사항을 사용할 수 없습니다.
- 들어오는 IP. 규칙을 적용할 게이트웨이의 공개 IP 주소입니다.
- 들어오는 포트/범위. 규칙을 적용할 포트 또는 포트 범위입니다.
- 프로토콜. 규칙에 사용되는 프로토콜: 사용 가능한 선택 사항은 *tcp, udp, tcp + udp* 또는 *icmp* 입니다.
- 원격 IP. 트래픽이 전달되는 원격 IP 주소입니다.
- 원격 포트/범위. 트래픽이 전달되는 원격 IP의 포트입니다.
- 설명. 게이트웨이에 대한 사용자 지정 주석.

각 테이블 행의 각 필드는 두 번 클릭하여 편집할 수 있습니다. 전달되는 정보의 유형에 따라 각 필드는 드롭 다운 메뉴 (예: 엔드포인트 열의 엔드포인트 목록 또는 사용 가능 프로토콜 열에 대한 프로토콜) 또는 텍스트 필드 (다른 모든 필드)를 보여줄 수 있습니다.

엔드포인트와 관련된 규칙 관리는 테이블 하단의 단추를 사용하여 수행할 수 있습니다.

행 추가

이 옵션을 사용하면, 새 규칙을 추가할 수 있습니다. 새로운 행의 필드를 두 번 클릭하여, 구성을 수행할 수 있습니다.

행 삭제

이 버튼을 클릭하면, 강조 표시된 규칙이 세트에서 삭제됩니다. 행을 선택하지 않으면, 이 단추가 비활성화됩니다.

> **경고:** 행 삭제는 즉시 수행되며 되돌릴 수 없습니다.

CSV 표시

이 버튼은 CSV 형식의 테이블에 있는 동일한 정보를 포함하는 텍스트 필드로 표를 토글합니다.

이렇게하면 전체 규칙 세트를 내보내는데 유용합니다.

유효성 검사

삽입된 정보가 유효한지 확인하십시오.

위치

이 탭에서는 위치 편집기 맵 또는 아래의 두 개의 작은 텍스트 필드 중 하나를 사용하여 장치에 위치를 지정할 수 있습니다.

지도에서 + 및 - 버튼을 사용하여, 원하는대로 지도의 크기를 조정하거나 텍스트 입력란을 직접 사용하십시오.

검색...

이 텍스트 필드에는 주소와 선택적으로 도시와 국가를 기입하십시오. 일치하는 항목이 발견되면, 지도에 아이콘이 표시됩니다. 더 많은 결과가 있는 경우, 가장 적합한 것을 선택하십시오.

> **참고:** 주소를 선택하면 아래의 두 텍스트 필드가 자동으로 입력됩니다.

주소를 제공하는 대신 장치 위치 좌표를 제공하는 것도 가능합니다.

위도

장치가 설치된 위도를 10 진수 형식으로 입력하십시오.

경도

장치가 설치된 경도를 10 진수 형식으로 입력하십시오.

장치를 현재 위치에서 가까운 위치로 이동할 경우, 아이콘을 새 위치로 끌 수 있습니다. 새 주소와 좌표가 자동으로 업데이트됩니다.

그룹들

이 페이지에는 기존의 모든 그룹 목록과 그 그룹에 대한 정보가 있는 테이블 위의 그룹 추가 링크 (처음에는 비어 있음)만 있습니다.

- 그룹에 할당된 이름입니다.
- 그룹에 대한 설명.
- 사용 가능한 작업 :

-  - 게이트웨이 그룹을 수정합니다.
-  - 게이트웨이 그룹을 제거합니다.
-  - 게이트웨이 그룹의 활동 로그를 참조하십시오.

그룹 추가 링크를 클릭하면 편집기가 테이블 바로 위에 열립니다. 설정 옵션은 *Group (그룹), Members (구성원) 및 Permissions (권한)*의 세 가지 탭으로 그룹화됩니다.

그룹

이 탭에는 그룹에 대한 기본 정보가 들어 있습니다.

그룹 이름

그룹에 할당된 이름입니다.

조직

그룹이 속한 조직입니다. 이 옵션은 하나 이상의 조직이 생성된 경우에만 사용할 수 있습니다.

설명

그룹에 대한 설명.

회원

이 탭에는 그룹 구성원에 대한 정보가 들어 있습니다.

이 게이트웨이 그룹의 장치

이 그룹에 속하는 게이트웨이를 선택하십시오.

권한

이 장치 그룹에 대한 사용자 권한

이 그룹에 액세스할 수 있는 모든 사용자와 그들이 맡고 있는 역할 (일반 사용자 또는 관리자)을 선택하십시오.

응용프로그램

이 페이지에는 엔드포인트에 연결할 수 있는 모든 수단을 정의하는 *응용프로그램*과 여러 응용 프로그램을 그룹화하여 장치에 할당하는 *프로파일*이라는 두 개의 탭이 있습니다.

응용프로그램

응용프로그램은 Endian S.p.A., Italy ConnectApp가 설치된 원격 PC 또는 워크스테이션에서 엔드포인트 또는 엔드포인트에서 실행중인 서비스로 액세스할 수 있는 수단으로 볼 수 있습니다 (워크스테이션에 설치된 타사 소프트웨어 사용 가능).

이 페이지에는 기본적으로 `응용프로그램 추가` 링크와 기본적으로 사용할 수 있는 응용프로그램 및 기타 정보가 포함된 표가 표시됩니다.

- 응용 프로그램을 식별하기 위해 제공된 이름입니다.
- 응용 프로그램의 유형 (자세한 내용은 다음을 참조하십시오).
- 응용 프로그램에 대한 설명
- 각 응용 프로그램에 대해 사용할 수 있는 작업 :
    - ☑☐ - 응용 프로그램을 활성화 또는 비활성화합니다.
    - 🖉 - 응용 프로그램을 수정합니다.
    - 🗑 - 응용 프로그램을 제거합니다.

테이블 위의 오른쪽에는 스위치보드에 정의된 모든 응용 프로그램을 검색하는데 유용한 필터가 나타납니다.

`응용 프로그램 추가` 링크를 클릭하면, 테이블 바로 위에 응용 프로그램 편집기가 열리고 추가 응용 프로그램을 정의할 수 있습니다.

이 편집기에는 *응용 프로그램* 및 *고급 매개 변수*의 두 가지 탭이 있습니다. 후자는 사용 가능한 일부 *응용 프로그램 유형*에만 나타납니다.

응용프로그램

이름

응용프로그램을 식별하는 이름입니다.

조직

어플라이언스의 사용이 예약된 조직의 이름. 이 옵션을 표시하려면, 적어도 조직 섹션에 조직이 정의되어 있어야 합니다.

설명

응용프로그램에 대한 설명.

응용 프로그램 유형

드롭 다운 메뉴에서 선택할 수 있는 응용프로그램의 유형입니다.

> **참고:** 응용프로그램 유형의 선택은 다음 옵션 중 일부의 가용성에도 영향을 줍니다. 또한 고급 매개 변수 탭에 나타나는 옵션은 선택한 응용프로그램 유형에 따라 다릅니다.

프로토콜

응용 프로그램에서 사용해야 하는 프로토콜이며, 드롭 다운 메뉴에서 선택합니다. *TCP, UDP* 또는 *TCP & UDP* 일 수 있습니다.

포트

응용프로그램에서 사용하는 포트입니다.

열려는 URL

연결에 사용할 URL입니다. 이 옵션은 위의 응용프로그램 유형이 HTTP 또는 HTTPS인 경우에만 사용할 수 있습니다.

활성화

응용프로그램을 사용하려면, 확인란을 선택하십시오.

다음 옵션은 위의 응용 프로그램 유형이 사용자 지정이고, 프로그램에 전달할 응용 프로그램과 인수를 시작할 워크스테이션의 경로를 정의할 수 있는 경우에만 나타납니다. 동일한 응용 프로그램이 Microsoft Windows 및 Mac OS X에서 실행될 수 있으므로 경로와 인수를 두 번 지정할 수 있습니다. 자리 표시자를 사용하여 운영 체제에서 바꿀 수도 있습니다. 자세한 내용은 아래를 참조하십시오.

명령 경로

사용할 프로그램의 전체 경로.

명령 인수

프로그램에 전달할 추가 인수.

다음 옵션은 ConnectAPP가 원격 장치에 연결하기 위해, 응용프로그램을 시작하는 방법에 관한 것입니다. 이 옵션은 Windows 및 Mac OS X에서 사용할 수 있습니다.

통합 애플리케이션 사용

이 옵션을 선택하면 ConnectAPP가 원격 연결을 위해 통합 응용 프로그램을 사용합니다.

외부 응용 프로그램 열기

이 확인란을 선택하면, 원격 장치에 연결하기 위해 시작할 외부 응용 프로그램을 지정할 수 있습니다. *Command path(경로)*와 *Command augument(인수)*는 위에 설명된 것과 정확히 같고, 다음에 설명하는 자리 표시자를 사용할 수 있는 두 가지 옵션이 나타납니다.

사용 가능한 자리 표시자

자리 표시 자의 목적은 각 장치의 다양한 구성 값 (예: 공개 IP 주소)과 관계없이 모든 장치에서 동일한 응용 프로그램을 사용할 수있게하는 것입니다.

자리 표시자를 **HTTP, HTTPS** 및 **사용자 정의** 응용프로그램 유형에서 사용할 수 있습니다.

HTTP 및 HTTPS 유형의 경우 사용 가능한 자리 표시 자입니다.

- **%DEVICE_IP%** 장치에 할당된 IP 주소입니다.
- **%PHYSICAL_IP%**는 장치의 물리적 IP입니다.
- **%SERVER_EXTERNAL_HOST%** 서버의 공용 호스트 이름의 FQDN입니다.
- 내부, 개인 IP 주소에 대한 **%SERVER_INTERNAL_IP%**.

사용자 지정 응용 프로그램 유형에서 사용 가능한 자리 표시자는 다음과 같습니다.

- **%PROGRAM_PATH%**: 응용프로그램의 기본 설치 디렉토리 (일반적으로 C:₩Program Files) 입니다.
- **%SYSTEM_DRIVE%**: Windows 루트 디렉토리 (C : ₩)가있는 드라이브.
- **%SYSTEM_ROOT%**: Windows 루트 디렉토리 (C : ₩ Windows).
- **%HOME_PATH%**: 사용자의 홈 디렉토리 (C : ₩ Documents and Settings ₩`username`).

응용 프로그램의 예로 Windows와 ConnectApp가 설치된 각 워크 스테이션에 사용자 홈 디렉토리에 PuTTy 프로그램이 설치되어 있다고 가정합니다. 사용자가 퍼티를 사용하여 SSH를 통해 연결할 수있게하려면 다음 구성 값으로 응용 프로그램을 정의하십시오.

- *이름:* **PuTTy -SSH**
- *설명*: **PuTTy를 통한 SSH**
- *응용프로그램 유형:* **사용자 지정**
- *프로토콜:* **TCP**
- *항구:* **22**
- *명령 경로:* **%HOME_PATH%₩putty.exe**
- *명령 인수:* **username@%DEVICE_IP%**

사용자 이름은 끝점의 유효한 사용자 계정이어야 합니다.

고급 매개 변수

다른 탭에서 선택한 응용 프로그램 유형에 따라, 다음 일반 옵션을 **사용자 지정(custom)**을 제외한 모든 유형에서 사용할 수 있습니다.

사용자 이름

원격 로그인에 사용되는 사용자 이름입니다.

암호, 암호 확인

로그인에 사용되는 암호로 확인을 위해 두 번 반복됩니다.

또한 다음 유형의 고급 옵션을 정의할 수도 있습니다.

- SSH

  개인 키

  텍스트 필드를 사용하여 연결에 사용된 개인 키를 붙여 넣습니다.

  암호, 암호 확인

  여기에 개인 키에 해당하는 암호를 적어주십시오.

  터미널 색 구성표

  드롭 다운 메뉴에서 SSH 터미널에 사용된 색상을 선택하십시오.

  글꼴

  터미널에서 사용된 글꼴.

  글자 크기

  글꼴의 크기.

- RDP

  이 유형의 연결로 구성할 수 있는 옵션이 많이 있지만, 대부분의 경우에는 필요하지 않습니다. 이러한 옵션을 사용하여, 인증, 세션, 오디오 지원, 성능 향상 및 RemoteApp를 사용자 지정할 수 있습니다.

- VNC

연결 재시도 횟수

시도가 실패한 후 연결을 시도해야 하는 횟수입니다.

색상 심도

연결에 사용되는 색상 수를 선택하십시오.

빨간색 파란색 전환

빨강 및 파랑 색상을 반전시킵니다.

커서

드롭 다운 메뉴에서 로컬 또는 원격 커서 사용 여부를 선택하십시오.

읽기 전용 연결

체크 박스를 선택하면 클라이언트가 원격 장치에서 변경을 허용하지 않습니다.

클립 보드 인코딩

- 텔넷

사용자 이름 정규식

원격 장치에 사용자 이름을 보낼 정확한 시점을 인식하는 정규 표현식.

암호 정규식

원격 장치에 암호를 보낼 순간을 인식하는 정규 표현식.

터미널 색 구성표

드롭 다운 메뉴에서 SSH 터미널에 사용된 색상을 선택하십시오.

글꼴

터미널에서 사용된 글꼴.

글꼴 크기

글꼴의 크기.

- 사용자 정의

사용자 정의 응용 프로그램의 경우, 행 추가를 클릭하여, 새 매개 변수를 추가한 후 다음 정보를 입력하십시오.

매개 변수 이름

매개 변수의 이름입니다.

값

해당 매개 변수의 값입니다.

원하는 옵션과 값을 추가할 수 있으며, 명령 행에서 응용프로그램으로 전달됩니다.

프로필

응용프로그램을 프로파일로 그룹화하고 단일 끝점에 연결하여 액세스 할 수 있는 기능을 조정할 수 있습니다. 즉, 주어진 엔드포인트에서 애플리케이션을 구성하여 주어진 프로토콜 (예: RDP, SSH 또는 HTTP) 또는 서비스 (예: VNC)를 통해서만 액세스 할 수 있도록 할 수 있습니다. 응용프로그램의 선택은 엔드포인트의 실행중인 운영 체제 및 서비스의 영향을 받을 수 있습니다.

이 페이지에는 현재 사용 가능한 모든 프로필 목록들과 각 프로필들에 대한 정보가 포함되어 있는 테이블 위에 프로필 추가 링크가 있습니다.

- 프로파일에 주어진 이름.
- 프로필 설명
- 프로파일의 일부인 응용 프로그램.
- 각자에게 가능한 행동 :
    -  - 응용 프로그램 프로파일을 수정합니다.
    -  - 응용 프로그램 프로파일을 제거합니다.

> **참고:** 하나 이상의 프로필이 삭제된 경우, 단일 응용프로그램은 삭제되지 않습니다. 기존 응용 프로그램을 제거하려면 응용 프로그램으로 이동하십시오.

표 위의 오른쪽에는 스위치보드에 정의된 모든 프로파일 중에서 검색하는데 유용한 필터가 나타납니다.

프로필 추가 링크를 클릭하면, 편집기가 표 바로 위에 열립니다. 여기에 다음 정보를 제공하여 추가 프로필을 만들 수 있습니다.

이름

프로파일을 식별하는 이름.

조직

프로파일을 사용할 조직을 선택하십시오.

설명

프로파일에 대한 메모.

응용프로그램

사용 가능한 응용프로그램은 다중 선택 상자에 나열됩니다. 프로파일에 응용프로그램을 추가하려면, 응용프로그램의 이름 옆에 있는 `+` 를 클릭하십시오. 응용프로그램을 검색하려면, 상자 상단의 텍스트 상자를 사용하십시오. `모두 추가` 링크는 프로파일 내의 모든 응용프로그램을 이동하기 위한 바로 가기로 사용할 수 있습니다. 응용프로그램은 오른쪽 열의 응용프로그램 이름 옆에 있는 `-` 를 클릭하여, 프로파일에서 제거할 수 있습니다.

조직

스위치보드의 중요한 특징은 스위치보드 *조직(Organization)*으로, 복잡한 기업을 계층 구조로 구성될 수 있는 실제 *조직(Organization)*이라 불리는 소규모 독립적인 단위로 좀 더 세분화하여 지원할 수 있도록 도입되었습니다.

스위치보드 조직은 하나 이상의 사용자와 하나 이상의 장치 (게이트웨이 또는 엔드 포인트)로 구성됩니다. 한 조직 내의 사용자와 장치는 다른 조직의 사용자와 장치를 보거나 액세스하거나 관리할 수 없습니다. 사용자, 사용자 그룹 또는 장치는 정확히 하나의 조직에만 속할 수 있습니다.

조직 내에서 기본 정책은 사용자가 계층의 하위 조직에 있는 다른 모든 사용자 및 모든 장치를 볼 수 있다는 것입니다.

조직 내의 계층 구조는 루트 노드와 최소한 하나의 하위 또는 하위 노드가 있는 정렬되지 않은 트리로 구성되며, 각 노드는 조직 내 하나의 (하위) 조직입니다.

기술적 측면에서, 하위 조직은 루트 노드와 조금 다릅니다. 실제로 하위 조직은 전체 조직 또는 스위치보드 설치에 내재되어 있기 때문에, 자식 노드가 상속하고 수정할 수 없는 일부 속성이 있습니다. 이러한 루트 노드 특성은 다음과 같습니다.

- OpenVPN : 전용 서버 또는 인스턴스 (대체적으로 폴백 포함) 및 공용 IP 주소 (FQDN).
- 수동 또는 자동 가상 서브넷 할당이있는 전용 IP 주소 풀입니다.
- 가상 IP 풀 전체를 연결된 클라이언트에 푸시 할 수있는 가능성.
- 고유 한 교환기 바인드 IP 주소, 대체로 대체 가능.

이 페이지에는 처음에는 사용 가능한 조직의 빈 테이블과 각 조직에 대한 몇 가지 정보가 포함되어 있습니다.

- 조직의 이름.
- 루트 조직의 경로
- 각 조직에서 사용할 수있는 작업 :
    -  - 응용프로그램 프로파일을 수정합니다.
    -  - 응용프로그램 프로파일을 제거합니다.

표 위의 링크인 조직 추가를 사용하면 새 조직을 정의할 수 있습니다.

편집자는 새로운 조직을 구성하기 위해 여러 가지 옵션을 사용할 수 있습니다.

고유 조직 식별자

조직 식별에 사용되는 식별자로, 스위치보드 인스턴스 내에서 고유해야 합니다.

상위 조직

이것이 루트 조직이 아닌 경우, 드롭 다운 메뉴에서 그것의 상위를 선택하십시오.

독점적인 접근

드롭 다운 메뉴에서 전체 조직에 대한 단독 액세스를 사용할지 여부를 선택하십시오.

스위치보드 바인드 IP 주소

이 조직에 액세스하는데 사용해야 하는 스위치보드의 IP 주소.

전체 주소 도메인 이름

조직에 액세스하는데 사용되는 FQDN (전체 주소 도메인 이름)입니다.

최대 노드 수

이 조직을 구성하는 최대 노드 수입니다.

조직 이름

조직의 이름.

VAT 번호

조직의 VAT 번호.

주소, 주소 2

조직의 주소.

도시

조직이 위치한 도시입니다.

우편 번호

도시의 우편 번호.

주 또는 지방

조직이 위치한 주 또는 지방.

국가

조직이 위치한 국가입니다.

이메일

조직의 전자 메일입니다.

웹 사이트

조직의 웹 사이트.

전화 번호

조직의 전화 번호.

팩스 번호

조직의 팩스 번호.

OpenVPN 인스턴스

이 조직에 사용할 OpenVPN 서버 인스턴스를 드롭 다운 메뉴에서 선택하십시오.

OpenVPN 서버 공용 IP/FQDN 및 포트

조직에서 액세스 할 OpenVPN 인스턴스의 공용 IP 주소 또는 FQDN입니다.

폴백 OpenVPN 인스턴스 사용

확인란을 선택하면 기본 인스턴스가 실행되지 않는 경우, 조직에 액세스하는데 사용할 폴백(대체) OpenVPN 인스턴스를 사용할 수 있습니다.

이 옵션을 사용하면, 다음 두 옵션이 나타납니다.

폴백 OpenVPN 인스턴스

드롭 다운 메뉴에서 OpenVPN 서버 인스턴스를이 조직의 폴백으로 사용해야 하는지 선택하십시오.

폴백 OpenVPN 서버 공용 IP/FQDN 및 포트

폴백 OpenVPN 인스턴스에 사용되는 공용 IP 주소 또는 FQDN입니다.

자동 가상 서브넷 할당 사용

서브넷의 가상 IP 주소가 자동으로 할당되도록 하려면, 이 확인란을 선택합니다.

글로벌 가상 IP 풀

이 옵션은 조직 내의 게이트웨이 주소에 대한 IP 주소 서브넷을 정의합니다.

클라이언트 연결시 전체 가상 IP 풀 푸시

이 옵션을 사용하면, 클라이언트가 연결할 때마다 전체 가상 IP 서브넷이 서버에 푸시됩니다.

원격 API 사용

체크 박스를 선택하면, 원격 API를 사용할 수 있습니다.

API 키

API 액세스 및 사용을 위한 키로 사용되는 문자열입니다.

게이트웨이 프로비저닝 사용

이 확인란을 선택하면, 게이트웨이 프로비저닝이 활성화됩니다. 자세한 내용은 아래를 참조하십시오.

엔디안 네트워크 계정

게이트웨이의 자동 등록에 사용되는 Endian Network에 액세스하기 위한 사용자 이름.

엔디안 네트워크 암호 또는 등록 키

엔드 포인트의 등록 키. 오른쪽에 있는 확인란을 선택하여 암호를 표시하십시오. 그렇지 않은 경우, 숨겨집니다.

알림 메시지의 필수 확인 사용

알림 메시지를 수신하려면, 이 체크 박스를 선택하십시오.

기본 응용 프로그램 및 프로파일 추가

확인란을 선택하여, 기본 응용 프로그램을 이 조직에 추가하십시오.

통계

이 페이지는 스위치보드에 있는 조직, 사용자 및 장치에 대한 통계를 제공하며, 3개의 탭으로 나뉩니다. 각 탭에는 테이블의 요소 내에서 검색할 수 있는 필터 막대가 있는 표가 있습니다.

- 필터: 여기에 연구 문자열을 삽입하십시오.
- 조직: 검색할 조직을 드롭 다운 메뉴에서 선택하십시오.
- From, To: 검색할 시간 간격을 선택하십시오. 주어진 요일을 선택하려면, 시작 날짜와 종료 시간 필드에서 요일을 선택하십시오.

단체

이 페이지는 많은 정보와 함께 현재 정의된 조직의 목록을 갖고 있는 표를 보여줍니다.

> **참고:** 괄호 안의 숫자는 하위 조직의 값입니다.

- 조직. 루트 조직의 ID 및 경로와 함께 조직의 이름입니다.
- 사용자. 조직에 속한 사용자 수입니다.
- 장치. 게이트웨이, 엔드 포인트 및 엔디 언 어플라이언스의 세 가지 범주로 그룹화 된 장치 수입니다.
- 노드. 노드와 관련된 두 값: **계산된 노드** – 조직에 있는 노드 수 및 **노드 제한** - 허용되는 최대 노드 수입니다.
- 트래픽. 조직에서 **보내거나 받는** 트래픽 양.

사용자

이 페이지에는 스위치보드를 통해 연결된 사용자 목록이 포함된 표가 표시됩니다.

- 사용자. 계정 이름과 그것이 속한 조직.
- 연결. **To Switchboard**는 사용자가 만든 스위치보드에 대한 연결 수이며, 반면 **To device**는 장치에 대한 연결 수입니다.
- 연결 시간. **To Switchboard**는 사용자가 교환기에서 보낸 시간의 양이며, **To device**는 장치에서 보낸 시간을 나타냅니다.
- 트래픽. 사용자가 보낸 트래픽 양, 사용자가 보내고 받은 트래픽으로 나누어진 양.

장치들

이 페이지는 스위치보드에 연결된 장치 목록과 그에 대한 많은 정보가 들어있는 표를 보여줍니다.

- 장치. 장치 및 장치가 속한 조직의 이름입니다.
- 연결. **To Switchboard**는 사용자가 만든 스위치보드에 대한 연결 수입니다. 반면에 **To device**는 장치에 연결된 수를 표시합니다.
- 연결 시간. **To Switchboard**는 사용자가 스위치보드에서 소비한 시간의 양을 나타내는 반면, To devices는 장치에서 소비한 시간입니다.
- 트래픽. 사용자가 만들어낸 트래픽 양, 사용자가 보내고, 받은 것으로 나누어진 트래픽 양입니다.

설정

이 페이지에서는 스위치보드의 모든 글로벌 구성 옵션을 설정할 수 있습니다. 스위치보드를 실제로 구성하기 전에 **방화벽**과 **VPN**의 두 가지 다른 모듈에서 두 가지 작업을 수행해야 합니다.

첫 번째 작업은 OpenVPN 서버의 한 옵션에서 필요하기 때문에 VPN 방화벽의 활성화로 구성됩니다. 작업을 완료하려면, *Menubar ‣ firewall ‣ VPN Traffic* (VPN traffic)으로 이동하고 아직 활성화되지 않은 경우,  를 클릭하십시오.

일단 VPN 방화벽이 활성화되면, 두 번째 작업은 VPN 모듈에 몇 가지 옵션을 설정해야 합니다.

실제로 스위치보드는 클라이언트와 장치 사이에 안전한 연결을 제공하기 위해 Endian UTM Appliance에서 실행되는 OpenVPN 인스턴스를 사용합니다. 대부분의 OpenVPN 인스턴스 매개 변수는 자유롭게 선택할 수 있지만 그 중 두 개는 다음과 같이 구성되어야 합니다.

- OpenVPN 장치의 트래픽은 라우팅되어야 합니다.
- 클라이언트 간의 트래픽을 필터링해야 합니다.

관심있는 구성 옵션은 다음과 같습니다.

- 네트워크 옵션에서 브리지 확인란을 선택하지 않아야 합니다. 따라서 **TAP**을 선택한 경우 확인란을 선택하지 마십시오.

  > **참고:** TUN 장치를 선택하면, 트래픽을 라우팅할 수 있고 확인란에 액세스할 수 없습니다.

- *고급 옵션*에서 *클라이언트 - 클라이언트 연결* 옵션을 **VPN 방화벽에서 연결 필터**로 설정해야 합니다.

  앞에서 설명한 옵션에 대한 자세한 내용은 *Menubar ‣ VPN ‣ OpenVPN server ‣ Server configuration*을 참조하십시오 (OpenVPN 서버 섹션 참조).

이 페이지에는 스위치보드의 모든 구성 옵션 (설정, 포털 및 프로비저닝)을 그룹화하는 3개의 탭이 있습니다.

설정

독점적인 접근

이 옵션은 게이트웨이 또는 전체 게이트웨이 내에서 단일 엔드포인트를 잠글 수 있는 기능을 제어하므로 한 번에 한 사용자만 독점적으로 액세스 할 수 있습니다. 세 가지 옵션을 사용할 수 있으며, 사용 불가능합니다. - 독점적인 액세스가 게이트웨이 레벨에서 허용되지 않습니다. - 게이트웨이 전체를 잠글 수 있고, 엔드포인트 레벨에서 단일 엔드포인트를 잠글 수 있습니다.

스위치보드 바인드 IP 주소

스위치보드가 연결을 청취하는 IP 주소입니다. 스위치보드에 더 많은 IP 주소가 할당되면 필수입니다.

VPN 연결 확인 사용 (ping)

체크 박스가 선택되면, ICMP 핑 패킷이 VPN 터널을 통해 주기적으로 전송되어 연결이 아직 활성 상태인지 확인합니다.

활성화되면 다음 두 옵션이 나타납니다.

VPN 연결 확인 시간 초과 (초)

연속된 두 확인 사이의 간격.

VPN 연결 확인 시도

VPN 연결이 작동하지 않는 것으로 확인되기 전에 실패한 검사가 다시 발행되는 횟수입니다.

오늘의 메시지

스위치보드에 연결하는 모든 사용자에게 표시되는 메시지.

OpenVPN 인스턴스

이 옵션은 Endian UTM Appliance에서 OpenVPN 서버의 여러 인스턴스가 실행 중일 때만 나타납니다. 드롭 다운 메뉴에서 스위치 보드에 사용할 인스턴스를 선택하십시오.

OpenVPN 서버 공용 IP/FQDN 및 포트

스위치보드에 할당할 공용 IP 주소 또는 FQDN입니다.

폴백 OpenVPN 인스턴스 사용

OpenVPN 서버의 기본 인스턴스에 도달할 수 없는 경우를 대비하여, OpenVPN 서버의 폴백 인스턴스를 허용하는 확인란을 선택합니다. 다음 두 옵션이 나타납니다.

폴백 OpenVPN 인스턴스

이전 옵션에서 지정한 옵션이 실행되지 않고 드롭 다운 메뉴에서 선택된 폴백 OpenVPN 인스턴스입니다.

폴백 OpenVPN 서버 공용 IP/FQDN 및 포트

스위치보드의 폴백 서버에 할당할 공용 IP 주소 또는 FQDN입니다.

자동 가상 서브넷 할당 사용

서브넷의 가상 IP 주소가 자동으로 할당되도록 하려면, 이 확인란을 선택합니다. 활성화되면 다음 옵션이 나타납니다.

글로벌 가상 IP 풀

이 옵션은 게이트웨이 주소에 대한 IP 주소 서브넷을 정의합니다.

클라이언트 연결시 전체 가상 IP 풀 푸시

이 옵션을 사용하면, 클라이언트가 연결할 때마다 전체 가상 IP 서브넷이 서버에 푸시됩니다.

원격 API 사용

체크 박스를 선택하면, 원격 API를 사용할 수 있습니다.

API 키

API 액세스 및 사용을 위한 키로 사용되는 문자열입니다.

포털

이 페이지에서는 포털을 구성할 수 있으며, 초기에는 두 가지 옵션만 있습니다.

포털 사용

확인란을 선택하면, 추가 구성 옵션을 보여주는 새 패널이 나타납니다.

포털의 전체 주소 도메인 이름

스위치보드의 포털을 액세스하는데 사용될 FQDN을 작성하십시오.

포털 HTTPS 인증서

드롭 다운 메뉴에서 어떤 인증서를 사용하여 포털에 액세스해야 하는지 선택하십시오.

환영 메시지

포털에 연결하는 사용자에게 표시되는 메시지입니다.

알림 메시지의 필수 확인 사용

알림 메시지를 수신하려면, 이 체크 박스를 선택하십시오.

프로비저닝

이 탭에서는 게이트웨이 프로비저닝에 대한 옵션을 지정할 수 있습니다. 처음에는 옵션 및 모델 목록만 포함합니다.

게이트웨이 프로비저닝 사용

확인란을 선택하면 프로비저닝을 사용하도록 설정됩니다. 다음 옵션이 나타납니다.

엔디안 네트워크 계정

엔디안 네트워크에 액세스하는데 사용되는 사용자 이름

엔디안 네트워크 암호 또는 등록 키

엔디안 네트워크 계정의 암호 또는 엔디안 UTM 어플라이언스의 등록 키입니다.

프로비저닝 암호화 인증서 (PEM)

프로비저닝을 위해, 선택한 .pem 인증서 파일의 내용을 복사하여 여기에 붙여 넣습니다.

프로비저닝 암호화 개인 키 (PEM)

선택한 인증서에 해당하는 개인 키가 들어있는 .pem 파일의 내용을 여기에 복사하여 붙여 넣습니다.

페이지 하단에서 프로비저닝에 사용할 수 있는 새로운 엔디안 어플라이언스 모델을 추가할 수 있습니다.

테이블은 해당 필드로 구성됩니다.

이름

게이트웨이에 주어진 이름입니다.

인터페이스 장치

어플라이언스에서 사용 가능한 네트워크 인터페이스의 이름. 표 아래의 패널을 사용하여 올바른 네트워크 인터페이스를 복사하고 붙여 넣을 수 있습니다.

OpenVPN> = 2.3

어플라이언스가 OpenVPN 버전 2.3 이상을 지원하는지 여부를 드롭 다운 메뉴에서 선택하십시오.

모뎀 포트

모뎀 포트로 사용할 포트를 드롭 다운 메뉴에서 선택하십시오.

게이트웨이 관리는 테이블 하단의 버튼을 사용하여 수행할 수 있습니다.

행 추가

이 옵션을 사용하면, 새 게이트웨이를 목록에 추가할 수 있습니다. 새로운 행의 필드를 두 번 클릭하여 구성을 수행할 수 있습니다.

행 삭제

이 버튼을 클릭하면, 강조 표시된 게이트웨이가 목록에서 제거됩니다. 이 버튼은 하나의 행이 선택된 경우에만 활성화됩니다.

> **경고:** 행 삭제는 즉시 수행되며 되돌릴 수 없습니다.

유효성 검사

강조 표시된 행에 삽입된 정보가 유효한지 확인하십시오.

기본 모델

이 위젯을 클릭하면 위의 표에서 사용할 Endian 어플라이언스 목록과 기본값을 볼 수 있습니다.

로그

스위치보드의 로그는 교환기에 의해 관리되고, 시스템 이벤트를 기록하는 다른 모든 로그와 달리 스위

치보드 메뉴에서만 도달할 수 있는 모든 다양한 객체 (예: 게이트웨이, 사용자 그룹 등)에서 발생하는 모든 이벤트를 포함합니다 *Menubar ‣ Logs*서 액세스 할 수 있습니다.

이 페이지에는 스위치보드에서 발생한 모든 이벤트 목록이 있는 표가 있습니다. 표 위에서 `CSV 형식으로 내보내기` 버튼을 사용하면 로그 파일을 CSV 형식으로 다운로드 할 수 있습니다.

테이블의 각 행은 하나의 이벤트를 나타내며 이에 대한 다음 정보를 포함합니다. 이벤트는 원격 장치에 대한 연결 또는 사용자 관리 또는 응용프로그램 추가 또는 제거 같은 일부 관리 작업과 관련이 있습니다.

- 날짜: 이벤트의 타임 스탬프, 즉 이벤트가 발생한 날짜와 시간입니다.
- 액션: 이벤트와 관련된 키워드입니다. 각 키워드는 정확한 이벤트를 지정하며 거의 자명합니다. 알파벳순으로 다음과 같습니다.

  GATEWAYEDIT, GROUPCREATE, SYSTEMBOOT, TUNNELACTIVE, TUNNELINACTIVE, USERCELATE, USERDELETE, USEREDIT, USERLOGOFF, USERLOGON과 같은 개인 정보 취급 방침을 준수합니다.

  > **참고:** TUNNELACTIVE 및 TUNNELINACTIVE는 클라이언트 워크 스테이션에서 끝점까지 OpenVPN 터널을 만드는 것을 의미합니다.

- 사용자: 작업을 수행한 사용자입니다.
- 대상 사용자: 작업의 대상이었던 사용자.
- 게이트웨이: 장치에 연결한 경우, 게이트웨이가 사용됩니다.
- 끝점 : 연결이 설정되거나 종료된 엔드포인트니다.
- 응용 프로그램 : 수정된 응용 프로그램입니다.
- 프로파일: 수정된 응용 프로그램 프로필입니다.

관리 센터

버전 5.0.5의 새로운 기능.

엔디안 관리 센터는 스위치 보드에 연결된 모든 엔디안 게이트웨이의 관리를 단순화하는 주된 목적으로 구현된 모듈입니다. 추가 기능은 모든 게이트웨이의 구성을 동기화된 상태로 유지하고, 다른 프로파일을 정의하여 게이트웨이를 구성하고, 각 프로파일의 게이트웨이에 대한 구성 변경 내역을 저장 및 표시하는 기능입니다. 자세한 내용은 아래를 참조하십시오.

관리 센터 설명

Endian Management Center 모듈을 사용하면 스위치 보드에 등록된 모든 게이트웨이를 원격으로 관리하고 구성 저장소를 유지 관리하고 모든 구성을 *Gold Gateway*라는 참조 게이트웨이와 동기화 할 수 있습니다. 사용자의 관점에서 보았을 때, 이 모듈은 사용하기 쉽지만, 모듈이 어떻게 작동하고 원격 게이트웨이와 상호 작용하는지 이해하기 위해 몇 가지 강조점이 있습니다. 이 메시지에는 Endian Management Center의 가장 중요한 기능이 제시되어 있습니다.

Endian Management Center와 원격 게이트웨이 간의 통신에는 **Jabber** (XMPP) 프로토콜이 사용됩니다. 이것은 OpenVPN을 사용하는 스위치보드와 Endian 관리 센터가 관리하는 원격 장치와 상호 작용하는 방식과 가장 중요한 차이입니다. 이것은 동일한 장치가 스위치보드에서 온라인으로 표시될 수 있지만 Endian 관리 센터에서는 *오프라인*으로 표시될 수 있음을 의미합니다.

이러한 이유 때문에 다음 포트가 Endian UTM Appliance에서 열리 며 *(방화벽(Firewall) ‣ 시스템 액세스 (System Access)‣ 시스템 서비스 규칙 표시(Show rules of system services))* 관리 센터와 게이트웨이 간의 원활한 연결을 허용합니다.

- Portal **TCP 443**.
- Jabber **TCP 5222**.
- OpenVPN **TCP+UDP 1194**.

> **참고:** 포트 1194는 OpenVPN 서버 구성에 따라 달라질 수 있습니다.

관리 센터에서 프로파일을 작성하여 원격 액세스 모듈과 선택적 액세스를 허용할 수 있습니다. 많은 게이트웨이가 각 프로파일과 연관될 수 있으며, 프로파일 내의 하나의 게이트웨이는 **Gold Gateway**로 선택됩니다. 이는 다른 게이트웨이가 준수할 모델로 작동하는 게이트웨이입니다.

이 특별한 역할은 다음 기능인 **게이트웨이의 동기화**를 소개합니다. 골드 게이트웨이가 선택 되자마자, 구성이 Endian Management Center에 저장되고, 프로파일과 연관된 다른 게이트웨이로 푸시됩니다. 프로파일에서, 프로파일 내의 다른 모든 게이트웨이에서 구성이 동기화되는 여러 모듈 중에서 선택할 수 있습니다.

그러나 동기화는 무엇이며 그걸 하는 방법은 무엇입니까? Gold Gateway의 /var/efw/ 구성 (configuration) 디렉토리는 엔디안 관리 센터의 저장소에 복사되고, 업데이트 내역이 완료되며 프로필의 모든 게이트웨이로 푸시될 수 있습니다. 게이트웨이가 구성을 수신하면 /var/emc/ 폴더에 저장됩니다. 두 폴더의 구성간에 불일치가 있는 경우, 로컬 /var/efw/가 우선합니다. 마찬가지로 Gold Gateway와 하나 이상의 다른 게이트웨이에서 서비스의 상태가 다를 때마다 게이트웨이의 상태가 우선합니다.

예를 들어, 나가는 방화벽이 Gold Gateway에서 활성화되었지만 (예: 문제 해결과 같은) 일부 이유로 비활성화되어 있고 게이트웨이에서 게이트웨이가 동기화되어있는 경우, 나가는 방화벽은 **비활성화**된 상태로 유지됩니다.

구성이 게이트웨이에서 푸시 될 때마다 게이트웨이도 업데이트됩니다. 패키지 목록이 검색되고 필요하면 업그레이드됩니다. 이 두 작업이 성공적으로 완료된 후에야 구성이 게이트웨이로 전송됩니다.

> **경고:** 원격 게이트웨이에서 필요한 재부팅을 알리는 메커니즘이 현재 없기 때문에, 일부 패키지를 설치한 후, 업그레이드가 필요할 때, 주의해야 합니다.

장치들

이 페이지에는 다음 데이터와 함께 Endian Management Center에서 관리할 수 있는 게이트웨이 목록이 있는 테이블이 있습니다.

- 고유해야 하는 *이름*.
- **오프라인**의 **온라인** *상태*입니다.
- *프로파일* - 구성의 어떤 부분이 장치에 푸시되는지 정의합니다.
- 사용 가능한 **조치**(actions)는 다음과 같습니다.
    - 게이트웨이를 편집하려면, 자세한 내용은 아래를 참조하십시오.
    - 구성을 가져오기 위해서는, 이 아이콘을 클릭함으로써 게이트웨이의 /var/efw/ 디렉토리 내용이 검색되어 스위치보드에 복사됩니다.
    - 시간 경과에 따른 게이트웨이의 현재 구성 및 변경 내용을 보기 위해서는, 모든 이전 구성은 git 저장소에 저장되므로, 버전 간 변경 사항을 강조 표시할 수 있습니다.
    - 게이트웨이의 현재 구성을 다운로드합니다.

> **참고:** 구성은 교환기에 저장되지만, 이 기능은 백업을 구성하지 않으며 백업 정책을 대체하기 위한 것이 아닙니다.

편집 아이콘을 클릭하면, 시스템의 현재 상태에 대한 정보가 검색되어 여러 페이지의 구성 옵션을 제공하는 탭으로 구성된 새 페이지에 표시됩니다.

세부사항

이 탭에는 다음과 같은 정보가 표시됩니다.

이름

게이트웨이에 주어진 이름입니다. 고유해야 하며 변경할 수 없습니다.

설명

게이트웨이에 대한 선택적 설명.

윤곽

드롭 다운 메뉴에서 선택한 장치와 관련된 프로파일입니다. 하나의 프로파일만 하나의 장치에 연결할 수 있습니다.

VPN

이 탭은 VPN 연결에 대한 정보를 보고합니다.

- 이름: VPN 연결의 이름입니다.
- 상태: 게이트웨이가 VPN에 연결되어 있는지 여부.
- 조치: 현재 사용할 수 있는 유일한 조치는 체크 상자를 선택하여, VPN 터널을 사용 가능 또는 사용 불가능하게 하는 것입니다.

> **참고:** 여기서 상태의 수동 변경은 스위치보드의 대시 보드에 적절히 반영됩니다.

패키지

이 탭은 게이트웨이에 설치된 모든 패키지의 목록과 버전을 표시합니다.

업데이트

이 페이지의 모양은 업데이트 (*System ‣ Update*)와 매우 유사합니다. 메시지가 표시되고 게이트웨이가 업데이트되면, 마지막으로 취소된 날짜와 마지막으로 업데이트 확인이 표시됩니다. 그렇지 않으면, 패키지 목록이 표시됩니다 두 가지 옵션을 사용할 수 있습니다.

새 업데이트 확인

업데이트 된 패키지에 대한 수동 확인이 시작되고, 발견된 업그레이드할 수 있는 패키지가 여기에 나열됩니다.

지금 업데이트 프로세스 시작

업데이트 프로세스가 시작됩니다. 시스템은 새 패키지를 다운로드하여 설치하고, 이전 패키지를 대체합니다.

프로세스

이 탭에는 게이트웨이에서 실행중인 프로세스 목록이 맨 위 명령의 출력과 유사하게 많은 정보와 함께 표시됩니다. 각 프로세스에 대해 다음 정보가 표시됩니다.

- **PID.** 고유한 **프로세스 ID**
- **이름**. 실행중인 프로세스의 이름입니다.
- **CPU.** 프로세스가 시작된 이래 프로세스에서 사용된 CPU 시간.
- **우선 순위.** 프로세스의 우선 순위. 일반적으로 20보다 낮은 양수입니다. 문자열 **RT**는 프로세스가 실시간 우선 순위로 실행됨을 의미합니다.
- **가상 메모리.** 사용된 가상 메모리의 양 (KB)입니다.
- **사용자.** 프로세스를 시작한 사용자입니다.

작업들

이 탭은 작업 목록과 게이트웨이 상태를 표시합니다. 작업은 작업 프로세스가 관리하는 Endian 장치의 프로세스입니다. 표시된 정보는 다음과 같습니다.

- **이름.** 작업 이름.
- **지위.** 작업의 상태를 표시하는 문자열. 자세한 내용은 아래를 참조하십시오.

하드웨어

이 탭에는 게이트웨이에 대한 많은 정보가 다섯 개의 패널로 그룹화되어 있습니다. 엔디안 네트워크에서 볼 수 있는 것과 동일합니다.

일반 정보. 하드웨어, 커널 버전,로드 평균, 가동 시간 및 기타 몇 가지 데이터를 한눈에 알 수 있습니다.

회로망. 게이트웨이의 라우팅 테이블입니다.

디스크. 게이트웨이에서 정의된 파티션과 파티션에서 사용할 수있는 공간,

기억. RAM 사용,

하드웨어. 네트워크 인터페이스, USB 플러그, VGA 어댑터 등과 같은 게이트웨이의 다양한 하드웨어.

> **힌트:** 이러한 정보들은 어플라이언스의 하드웨어 탭 아래에 있는 엔디안 네트워크에 존재하는 정보를 반영합니다.

Jobsengine의 상태 메시지.

Jobsengine 상태 메시지는 세 부분으로 구성되며, 몇 가지 일반적인 예는 **start.ok/waiting, stop.err/waiting** 또는 **start.ok/restart pending**입니다.

첫 번째 부분 (점 앞에)은 **시작** 또는 **중지**이며, 작업 실행 여부를 보여줍니다.

가운데 부분 (점과 슬래시 사이)은 **ok** 또는 **err**이며 작업의 마지막 호출이 성공했는지 여부를 보여줍니다.

세 번째와 마지막 부분 (슬래시 다음)은 주로 **대기**하지만, 작업에서 필요한 일부 추가 프로세스가 시작되거나 작업이 재시작 중이면, 이 부분은 **보류를 재시작**할 수 있습니다.

프로필

이 페이지에서는 **프로파일** 관리를 할 수 있습니다. 여기에는 Endian Management Center를 통해 원격으로 구성할 수 있는 게이트웨이 모듈 목록이 있습니다. 모듈은 GUI의 일부입니다 (아래 참조).

이 페이지에는 다음 정보와 함께 이미 정의된 프로파일이 표시됩니다.

- 고유한 **이름**.
- 프로필에 대한 **설명**입니다.
- 사용 가능한 **액션들**:
    - 프로파일을 편집합니다.
    - 프로파일을 제거합니다.

새 프로파일을 만들려면, 표 위에 있는 프로파일 추가 링크를 클릭하십시오. 열린 페이지에는 각각 구성 옵션이 포함된 두 개의 탭, *프로파일* 및 *장치*가 들어 있습니다.

프로파일

이 탭에서 다음 옵션을 사용할 수 있습니다.

프로필 이름

프로필에 부여된 고유한 이름입니다.

> **힌트:** 영숫자 (0-9, a-z, A-Z), 밑줄 (_), 대시 (-), 점 (.) 또는 ats (@)로 구성되어야 합니다. 공백 및 기타 특수 문자는 허용되지 않습니다.

설명

프로파일에 대한 설명입니다.

모듈

어떤 모듈이 프로파일의 일부이고, 게이트웨이로 푸시되어야 하는지 선택하십시오.

> **힌트:** 정확히 하나의 프로파일을 게이트웨이에 할당할 수 있습니다.

장치들

이 페이지는 적어도 하나의 게이트웨이가 프로파일과 연결되어 있는 즉시 나타나며, 가장 중요한 게이트웨이입니다. 사실 구성 페이지가 아니지만, 모든 게이트웨이에서 일괄 작업을 수행하고, 게이트웨이에 연결된 프로파일을 관리하고 전송할 수도 있습니다. 이 페이지는 *골드 게이트웨이*, *대량 작업* 및 *장치*의 세 패널로 구분됩니다.

골드 게이트웨이

이 패널에서 골드 게이트웨이를 구성하고 관리할 수 있습니다. 다음 옵션 및 작업을 사용할 수 있습니다.

골드 게이트웨이

엔디안 관리 센터에서 관리하는 장치 중 골드 게이트웨이로 사용할 장치를 선택하십시오. 변경 단추를 클릭하면, 선택 사항을 수정할 수 있습니다.

제품

골드 게이트웨이의 제품.

버전

골드 게이트웨이에 설치된 소프트웨어 버전

> **참고:** 골드 게이트웨이를 선택하고, Endian Network에 표시된 항목과 일치하면 제품과 버전이 자동으로 가져옵니다.

구성 가져 오기

현재 /var/efw/ 디렉토리의 사본을 작성하고 로컬 저장소에 복사하십시오.

구성 저장소 표시

모든 버전의 구성으로 저장소를 보여주는 새 페이지를 엽니다.

대량 작업들

게이트웨이들의 상태가 골드 게이트웨이와 동기화하기 위해 모든 게이트웨이에서 대량으로 일괄 작업이 실행되고, 그것들은 다음과 같습니다. 대량 작업을 클릭하면, 팝업이 나타나 확인을 요청합니다.

`패키지 업데이트`

패키지 목록을 업데이트하십시오.

`패키지 업그레이드`

새 패키지를 설치하십시오.

> **참고:** 패키지를 설치 한 후에는 자동 재부트가 필요하지 않더라도 실행되지 않습니다.

`푸시 구성`

골드 게이트웨이의 현재 구성을 다른 게이트웨이로 복사하십시오.

> **참고:** 구성이 게이트웨이에 푸시되기 전에, 이러한 구성 요소도 업데이트됩니다. 이것은 앞의 두 조치 (패키지 갱신 및 업그레이드)가 게이트웨이로 푸시되었음을 의미합니다.

대량 작업이 시작되면, 이 세 개의 버튼이 비활성화 된 상태로 유지됩니다. 작업이 종료될 때만 (그 작업이 성공적이거나 또는 아닌 경우, 다음 섹션 참조), 다른 작업이 실행될 수 있습니다.

장치들

이 페이지는 Endian 관리 센터에서 관리하는 각 게이트웨이 및 상태에 대한 정보를 표시합니다.

이름

게이트웨이의 고유 이름 및 상태 (**온라인** 또는 **오프라인**).

제품

게이트웨이의 모델입니다.

업데이트

사용 가능한 업데이트 수

프로비저닝

골드 게이트웨이와 비교한 게이트웨이의 상태입니다. 특별 `GOLD GATEWAY` 레이블이 붙어 있습니다. 프로비저닝은 **OK** 또는 **NOT SYNC** 일 수 있습니다.

동작 상태

대량 작업이 시작되면, 이 열에 진행 상태가 표시됩니다. **DONE** 레이블은 조치가 완료되었음을, **TIMEOUT** 레이블은 조치가 성공적이지 않았 음을 의미합니다. 다른 레이블은 게이트웨이에서 실행된 현재 조치를 표시합니다.

클라이언트 다운로드

여기에서 로컬 워크스테이션에 설치하여 스위치 보드 관리에 사용하고 원격 장치에 직접 연결을 시작하고 스위치보드에 정의된 응용 프로그램 프로파일을 사용하여 4i Connect 클라이언트를 다운로드 할 수 있습니다. 필요한 응용 프로그램이 워크스테이션에 설치되었는지 확인하십시오.

스위치 보드 API

Switchboard API에 대한 문서는 여기에서 볼 수 있습니다.

로그 및 보고서 메뉴

이 섹션에서는 다음과 같은 내용들을 살펴보실 수 있습니다.

- 대시보드
  - 공통 요소
  - 요약
  - 시스템
  - 웹
    - 보고서 접근
    - 보고서 필터링
  - 메일
  - 침입 시도
  - 바이러스
  - 연결
- 트래픽 모니터링
  - 대시보드
  - 플로우
  - 호스트
  - 인터페이스
- 라이브
  - 설정
  - 라이브 로그
- 공통 작업
- 요약
- 시스템
- 서비스
- 방화벽
- 프록시
  - HTTP
  - 컨텐츠 필터
  - HTTP 보고서
  - SMTP
- 설정
  - 로그 보기 옵션
  - 로그 요약
  - 원력 로그인
  - 방화벽 로그인
- 신뢰할 수 있는 타임스탬핑

Endian UTM Appliance 의 로그 및 보고서 섹션에는 로그 파일을 보고 분석할 수 있는 여러 가지 방법이 있습니다.

화면 왼쪽의 하위 메뉴에는 다음 항목이 포함되어 있습니다.

- 대시 보드 - 보고 모듈, 로그 파일 및 이벤트의 그래픽 묘사.
- 트래픽 모니터링 - ntopng 그래픽 인터페이스는 차트를 사용하여, 네트워크 트래픽에 대한 실시간 개요를 제공합니다.
- 실시간 로그 - 생성되는 최신 로그 항목을 실시간으로 볼 수 있습니다.
- 요약 - 모든 로그의 일별 요약을 가져옵니다.
- 시스템 - 소스 및 날짜별로 필터링 된 시스템 로그 (/var/log/messages).
- 서비스 - 침입 탐지 시스템 (IDS), OpenVPN 및 바이러스 백신의 로그입니다.
- 방화벽 - iptables 규칙을 기록합니다.
- 프록시 - HTTP, SMTP 및 내용 필터 프록시에서 기록합니다.
- 설정 - 모든 로그 옵션을 사용자 정의합니다.
- 신뢰할 수있는 타임 스탬프 - 로그 파일을 안전하게 스탬프 처리하여 변경되지 않았는지 확인합니다.

간단하게 말하자면, GUI 에서 로그에 액세스하는 세 가지 방식이 있습니다. **그래픽 방식, 라이브 방식** 및 **서비스 별 방식**. 첫번째는 보고 모듈로 표시되고, **라이브** 모드에서는 로그 파일이 작성되자마자 시각화되고, **by-service 모드**에서는 한 번에 하나의 데몬 또는 서비스가 작성한 로그만 표시됩니다.

대시보드

보고 GUI 모듈은 시스템에서 다양한 유형의 이벤트 발생을 그래픽으로 표시하는 목적을 가지고 있습니다.

간단히 말해서, 보고서 모듈은 다른 위젯과 그래프를 사용하여, Endian UTM Appliance 에서 발생한 이벤트를 보여줍니다. 시스템에서 발생하는 모든 이벤트와 syslog 데몬에서 기록한 이벤트 관련 정보는 구문 분석되어, sqlite3 데이터베이스를 채우는데 사용됩니다. 여기에서 데이터는 옵션 및 GUI 에 적용된 필터에 따라 수집되어 사용자에게 표시됩니다.

이 페이지는 **요약, 시스템, 웹, 메일, 침입 시도, 바이러스** 및 **연결**의 6 개 탭으로 구분됩니다. 모든 이벤트의 개요를 보여주는 첫 번째 탭을 제외하고 각각의 이벤트는 Endian UTM Appliance 에서 실행되는 하나의 서비스 전용입니다.

공통 요소들

이 모듈의 모든 탭은 동일한 디자인을 공유합니다. 탭 아래의 왼쪽에는 *날짜 선택기*가 있고 오른쪽에는 인쇄 단추가 있습니다. 그런 다음, 바로 아래에 수평 슬라이더가 있는 선형 차트가 있고, 그 위에 유익한 정보 상자 (*요약 그리드*)와 파이 차트가 있습니다. 아래쪽에는 표시된 탭 및 데이터에 따라 하나 이상의

표들이 있습니다. 항상 존재하는 표는 표시된 이벤트와 관련된 syslog 메시지를 보여주는 표입니다.

더 자세히 설명하자면, 여기에서는 보고서 모듈에 있는 모든 위젯에 대한 설명입니다.

날짜 선택기

GUI의 왼쪽 상단에는 차트를 고려한 이벤트가 발생한 간격을 보여주는 하이퍼 링크가 있습니다. 작은 패널을 클릭하면 다른 간격 선택 항목에 액세스 할 수 있습니다. 두 가지 유형의 선택이 있습니다. 첫 번째는 *지난 ... 일,* 즉 마지막 날, 주 월, 분기 또는 연도의 이벤트와 관련됩니다. 두 번째 것은 지난 12 개월 중 하나에 발생한 모든 이벤트를 선택합니다. 새로운 기간을 선택하면, 다른 위젯도 업데이트됩니다. 취소를 클릭하여 표시된 간격을 변경하지 않을 수도 있습니다.

인쇄

이 버튼을 클릭하면 현재 페이지의 인쇄 미리보기가 표시됩니다.

선형 차트 및 시간 슬라이더

선형 차트는 선택된 시간 범위 동안, Endian UTM Appliance에서 발생한 이벤트를 2차원 그래프로 보여줍니다. 여기서 x 축은 시간 간격을 나타내고 y 축은 발생 횟수를 나타냅니다. 색깔이 있는 선은 같은 유형의 이벤트를 연결합니다.

> **힌트:** 다양한 유형의 이벤트는 서로 다른 색상으로 표시됩니다.

시간 슬라이더는 차트 아래에 있으며, 선택한 시간 범위 내에서 히스토그램으로 묘사된 이벤트의 보다 세분화된 보기를 허용합니다. 실제로 슬라이더의 왼쪽 및 오른쪽 경계에 있는 두 개의 회색 핸들을 클릭하고, 드래그하여 선형 차트에 표시된 시간 범위를 줄일 수 있습니다. 축소되면 슬라이더 가운데를 클릭하고, 왼쪽이나 오른쪽으로 드래그하여 이동할 수도 있습니다.

요약 그리드

요약 그리드에는 두 가지 목적이 있습니다. 선택한 기간에 Endian UTM 어플라이언스에서 발생한 다양한 이벤트 유형의 발생 횟수를 보여주는 목적과, 라인 차트에서 보여주는 이벤트 유형을 필터링하기 위한 또 다른 목적이 있습니다. 그 내용은 *메일, 침입 시도* 및 *바이러스* 탭이 존재하는 탭과 존재하지 않는 탭에 따라 달라지며, 이 탭은 이벤트에 대한 여러 가지 세부 정보를 그룹화하는 표로 대체됩니다.

파이 차트

파이(Pie) 차트 다이어그램은 선택한 시간 범위에서 발생한 이벤트 수를 그래픽으로 보여줍니다. *요약 탭*에서 각 슬라이스를 클릭하여, 이벤트 유형에 해당하는 탭을 열고, 좀 더 자세한 설명을 보여줄 수 있습니다.

Syslog 테이블

로그 파일에서 추출되고 차트에 표시된 이벤트와 관련된 syslog 메시지를 보여주는 표입니다. 테이블에 많은 메시지가 있는 경우에, 이 페이지는 여러 페이지로 나뉘며, 왼쪽 하단의 버튼과 번호를 사용하여 탐색할 수 있습니다. 오른쪽 하단에는 테이블 내용을 새로 고칠 수 있는 아이콘이 있습니다.

요약(Summary)

*Summary (요약) 탭*은 Endian UTM Appliance에 기록된 모든 범주의 이벤트에 대한 개요를 제공합니다. 요약 그리드를 사용하면, 다음과 같은 유형의 이벤트를 필터링 할 수 있습니다.

- 시스템. 시스템 관리 작업과 관련된 로그인 및 기타 이벤트 수 (예: 업링크 상태 변경, 로깅 시작 및 중지 등).
- 웹. 컨텐츠 필터에 의해 차단된 페이지 수입니다.
- 메일. 받은 스팸 전자 메일 수입니다.
- 침입 시도. IPS에서 기록한 이벤트입니다.
- 바이러스. 발견된 바이러스의 수.

각 카테고리는 별도로 표시할 수 있으며, 페이지의 다른 탭에 더 많은 정보와 세부 정보가 표시됩니다.

시스템

*시스템 탭*은 시스템 효율 및 시스템 관리와 관련된 모든 이벤트를 표시합니다. 다음은 모두 표시되는 이벤트입니다.

- 로그인. 로그인이 성공적이었는지 아니었는지 여부와 로그인 성공 횟수입니다.
- 상태. Endian UTM Appliance의 상태의 변경.
- 디스크. 디스크 I/O와 관련된 이벤트입니다.
- 지원. 지원 팀에서 제공하지 않은 액세스 및 작업 수입니다.
- 업그레이드. 시스템 또는 패키지 업그레이드와 관련된 이벤트.
- 업링크. 업링크가 온라인 또는 오프라인 상태가 된 시간입니다.

각 이벤트 카테고리의 왼쪽에 있는 작은 아이콘을 클릭하면, 해당 카테고리의 일부인 이벤트에 대한 세부 정보가 표시되고, 원형 차트가 업데이트됩니다.

웹

웹 탭은 URL 필터 엔진에 의해 액세스되거나 차단된 페이지 수를 표시합니다. 요약 그리드는 *보고서 액세스*와 *보고서 필터링*이라는 두 개의 탭으로 구성됩니다.

보고서 액세스

이 탭은 액세스 된 도메인을 HTTP 프록시가 기록한 *소스 IP 주소*, 액세스한 *도메인* 및 웹 페이지를 요

청한 *사용자* 각각을 표시하는 세 개의 테이블로 그룹화하여, 모든 항목의 총 개수와 함께 표시합니다.

> **참고:** 액세스 보고서 탭은 모든 어플라이언스에 없습니다.

보고서 필터링

이 탭은 액세스가 차단된 도메인을 표시합니다. 첫 번째 표에는 웹 필터 (*Menubar ‣ Proxy ‣ HTTP ‣ Web Filter* 참조)에있는 범주가 표시됩니다.

- 일반 용도.
- 부모의 통제.
- 생산력.
- 보안.
- 분류되지 않은 사이트.

*Blocked 카테고리*의 왼쪽에 있는 체크 박스가 선택되지 않으면, 해당 카테고리의 항목은 다이어그램과 파이 차트를 그리는데 사용되지 않습니다. 체크 박스 왼쪽에 있는 아이콘을 클릭하면, 카테고리가 확장되어 더 자세한 다이어그램을 그리기 위해, 선택 또는 선택 해제할 수 있는 모든 하위 카테고리가 표시됩니다.

아래쪽에있는 다른 테이블은 차단된 개체의 개수를 보여줍니다: *원본 IP 주소* 및 *도메인*.

메일

메일 탭에는 스팸으로 차단된 모든 전자 메일이 표시됩니다.

이 탭에는 요약 그리드가 없지만, 다음에 대한 세 개의 표가 표시됩니다.

- From. 스팸 전자 메일의 보낸 사람.
- To. 스팸 전자 메일의 수신자.
- 소스 IP 주소. 스팸 전자 메일을 보낸 IP 주소입니다.

침입 시도

Intrusion attempts (침입 시도) 탭에는 IPS가 탐지한 모든 잠정적 침입이 표시됩니다 (*Menubar ‣ Services ‣ Intrusion Prevention* 참조).

하단의 표에는 다음 정보가 표시됩니다.

- 침입 시도: 각 시도가 속하는 범주입니다.
- 소스 IP 주소. 공격이 발생한 곳의 IP 주소입니다.
- 대상 IP 주소. 접속이 시작된 IP 주소.

바이러스

바이러스 탭은 안티 바이러스 엔진에 의해 차단된 모든 바이러스를 표시합니다 (*Menubar ‣ Service ‣ Antivirus Engine* 참조).

하단의 표에는 다음 정보가 표시됩니다.

- 바이러스 이름. 발견된 바이러스의 이름.
- 소스 IP 주소. 바이러스가 원래 있던 IP 주소.
- 대상 IP 주소. 바이러스가 전파된 IP 주소입니다.

연결

Connections (연결) 탭에는 Endian UTM Appliance 사용자가 시작한 평균 연결 수가 표시됩니다.

- 로컬 연결. SSH 또는 콘솔을 통해 액세스합니다.
- IPsec 사용자. IPsec을 통해 연결된 클라이언트.
- 핫스팟 사용자. 핫스팟에 액세스하는 사용자.
- OpenVPN 사용자. 클라이언트는 OpenVPN을 사용하여 연결되었습니다.

트래픽 모니터링

ntopng 소프트웨어는 ntop 네트워크 트래픽 분석기의 후속 제품으로, 보다 직관적인 인터페이스와 Endian UTM Appliance를 통해 흐르는 트래픽을 그래픽으로 표현한 것입니다.

ntopng의 관리 인터페이스는 이제 더 많은 유용성을 제공하며, 모든 브라우저에서 쉽게 액세스 할 수 있으므로, 이전 버전보다 Endian UTM Appliance 인터페이스와 더 밀접하게 통합되었습니다.

몇 마디로, ntopng의 능력은 다음과 같이 요약될 수 있습니다 :

- Endian UTM Appliance의 모든 네트워크 인터페이스를 실시간으로 모니터링합니다.
- 웹 액세스 가능 관리 인터페이스.
- ntop에 비해 필요한 리소스가 적습니다.
- nDPI (응용 프로그램 방화벽)의 통합.
- 다른 매개 변수 (프로토콜, 소스 / 대상)에 따라 트래픽 분석.
- JSON 형식으로 보고서 내보내기
- 디스크의 트래픽 통계 저장.

ntopng GUI는 *Dashboard, Flows, Hosts* 및 *Interfaces*의 네 가지 탭으로 구성됩니다. 또한 주어진 호스트에 대한 정보를 빠르게 표시할 수 있는 검색 상자가 있습니다.

각 탭의 바닥글(footer)에는 몇 가지 정보가 표시됩니다. 저작권 공지 및 ntop 홈페이지 링크와 함께 지난 20초 동안 네트워크 트래픽을 보여주는 차트가 실시간으로 업데이트되고, 사용된 현재 대역폭에 대한 일부 수치 데이터, 호스트 및 플로우 갯수 및 Endian UTM Appliance의 가동 시간에 대해 설명합니다.

대시보드

대시 보드에는 Endian UTM Appliance와 관련된 모든 연결, 즉 Endian UTM Appliance와 연관되어 설정된 모든 *Flow*가 표시됩니다.

이 페이지는 여러 다이어그램으로 나누어져 있으며, 첫 번째 페이지는 실시간으로 업데이트되는 Endian UTM Appliance에서 이동하는 모든 플로우를 보여주는 소위 Sankey 다이어그램입니다. 수평 흐름은 두 호스트 사이의 트래픽을 나타내지만, 각 흐름의 수직 폭은 흐름에 의해 사용되는 대역폭, 즉 데이터 흐름의 양에 비례합니다. 연결과 그에 따라 전송되는 데이터의 방향은 왼쪽에서 오른쪽으로 표시됩니다. 다이어그램의 왼쪽에 있는 호스트는 오른쪽에 있는 호스트로 데이터를 보내고, IP 주소 또는 호스트 이름으로 식별됩니다. 하나의 호스트를 클릭하면, 해당 호스트에 대한 여러 정보가 표시된 Hosts (호스트) 탭의 *Overview* (개요) 페이지로 연결됩니다.

Sankey 다이어그램 아래의 4개의 유익한 전용 파이(pie) 차트는 트래픽을 가장 많이 생성하는 항목을 백분율로 나눠서 다음과 같이 나눕니다. 즉, 호스트 별 합계 (왼쪽 상단), 애플리케이션 프로토콜 (오른쪽 상단), ASN (왼쪽 하단) 및 라이브 플로우 발신자 (오른쪽 하단)에 표시됩니다.

흐름

활성 흐름 탭에는 활성 흐름에 대한 많은 정보가 포함된 큰 테이블이 있습니다.

- *정보.* 아이콘을 클릭하면, 해당 플로우에 대한 좀 더 자세한 정보가 표시된 새로운 페이지가 열립니다.
- *응용프로그램.* 흐름을 일으키는 응용 프로그램입니다. nDPI는 응용프로그램을 인식하는데 사용되므로 올바른 응용프로그램이 표시되는 것을 보기 위해 몇 개의 패킷이 나타날 때까지 기다려야 할 수 있습니다.이 경우, 응용프로그램 이름 대신 (너무 일찍) 메시지가 나타납니다.
- *L4 Proto.* 일반적으로 TCP 또는 UDP인 흐름(flow)에 사용되는 네트워크 프로토콜입니다.
- *클라이언트.* 클라이언트 측에서 흐름이 사용하는 호스트 이름과 포트. 호스트 이름이나 포트를 클릭하면, 해당 호스트나 포트에 흐르는 네트워크 트래픽에 대한 새로운 정보가 추가로 표시됩니다.
- *서버.* 서버 측에서 흐름이 사용하는 호스트 이름 및 포트. 위의 클라이언트와 마찬가지로 호스트 이름이나 포트를 클릭하면, 자세한 정보가 표시됩니다.

> **힌트:** 호스트 이름 또는 포트를 클릭하면 테이블에 대한 자세한 정보가 표시되고 호스트 탭에 하위 탭이 열립니다.

- *지속 기간.* 연결 길이.
- *고장.* 클라이언트와 서버가 생성한 트래픽의 비율.
- *처리량.* 클라이언트 (왼쪽, 검은 색)와 서버 (오른쪽, 녹색)간에 현재 교환되는 데이터의 양.
- *총 바이트.* 연결이 처음 설정된 이후에 교환된 총 데이터입니다.

표의 맨 아래에는 왼쪽에 표시되는 총 행 수가 표시되고, 오른쪽에는 표가 분할되어 있는 여러 페이지를 탐색할 수 있습니다. 행의 수가 그 페이지 번호보다 높습니다.

정보 아이콘을 클릭하면 특정 흐름에 대한 자세한 정보가 제공됩니다. 이미 위에 설명된 것 외에도 이러한 추가 데이터가 표시됩니다.

- *First Seen.* 연결이 설정되었을 때의 타임 스탬프와 그 이후 경과한 시간.
- *Last Seen.* 연결이 마지막으로 활성화된 타임 스탬프 및 그 순간 이후에 경과된 시간.
- *클라이언트 대 서버 트래픽.* 클라이언트에서 서버로 보낸 패킷 및 바이트 수입니다.
- *서버 대 클라이언트 트래픽.* 서버에서 클라이언트로 보낸 패킷 및 바이트 수입니다.
- *TCP Flags*. 현재 흐름의 TCP 상태.

테이블 바로 위 왼쪽에 있는 Flows 하이퍼링크를 클릭하여, 플로우 목록으로 되돌아 갈 수 있습니다.

호스트

호스트 탭을 사용하면, 관련된 참여자 (호스트, 포트, 응용 프로그램, 플로우 및 기간, 교환 된 데이터 등)에 대한 몇 가지 세부 정보를 볼 수 있습니다.

두 가지 설명을 사용할 수 있습니다: *호스트 목록* 및 *상위 호스트 (로컬)*

호스트 목록 표시는 Endian UTM Appliance의 일부 흐름과 관련된 모든 호스트에 대한 정보 및 다음 데이터를 표시합니다.

- *IP 주소*. 호스트의 IP 주소 또는 MAC 주소. 후자는 해당 호스트에 대한 DHCP 임대가 만료된 경우 표시됩니다.
- *위치.* 호스트가 로컬 또는 원격 네트워크에 있는지 여부.
- *상징적인 이름(Symbolic Name).* 사용 가능한 경우라면, 호스트의 호스트 이름입니다.
- *Seen Since(이후에 보여짐).* 첫 번째 설정된 연결의 타임 스탬프입니다.
- ASN.
- *장애.* 송수신 트래픽 간의 절충.
- *트래픽*. 호스트에 의해 교환되는 데이터의 양.

IP 주소를 클릭하면, 위에 열거된 것 외에도, 여러 가지 정보가 표시된 호스트 개요가 열립니다.

- *Last Seen (마지막으로 본).* 연결이 마지막으로 활성화된 타임 스탬프 및 그 순간 이후에 경과된 시간.
- *Sent vs. Received Traffic Breakdown (송신 대 수신된 트래픽 장애).* 호스트에 의해 생성되거나 수신된 트래픽.
- *Traffic Sent (전송된 트래픽).* 클라이언트에서 서버로 보낸 패킷 및 바이트 수입니다.
- *Traffic Received(수신된 트래픽).* 서버에서 클라이언트로 보낸 패킷 및 바이트 수입니다.
- JSON. 호스트에 대한 정보를 JSON 형식으로 다운로드합니다.
- *Activity map (활동지도).* 주어진 타임 스탬프에서 호스트가 얼마나 많은 흐름을 보였는지를 알려

줍니다. 각 사각형은 1 분을 나타내고 색상이 어두울수록 그 순간에 더 많은 흐름이 발생한 것입니다.

여기에서 해당 호스트에 대한 추가 정보 탭을 열 수도 있습니다. 각 탭에는 표시되는 데이터의 텍스트 요약 위에 하나 이상의 원형 차트 (연락처 및 내역 탭 제외)가 있습니다.

- *트래픽.* 호스트가 사용하는 네트워크 프로토콜. (TCP, UDP 및 ICMP가 가장 일반적 임).
- *패킷.* 각 플로우의 패킷 길이. (참고: 그냥 내 추측임)
- *프로토콜.* 호스트에서 사용하는 응용프로그램 프로토콜입니다.
- *흐름.* 호스트의 모든 네트워크 흐름과 함께 테이블.
- *Talkers.* 연결의 Sankey 다이어그램은 대시 보드에 표시된 다이어그램과 매우 유사하지만 가장 활발한 흐름만 표시합니다.
- *Contacts(콘택트).* 이 탭은 다른 탭과 약간 다릅니다. 상호 작용 맵 상단에 클라이언트 또는 수신자로 호스트가 있는 연결 목록을 맵 아래에 표시합니다.
- *Historical.* 그래프 위에 선택할 수 있는 주어진 시간 범위 (최대 1년)의 트래픽 흐름 양식 및 호스트에 대한 내역을 보여주는 대화식 그래프입니다.

상위 호스트 (로컬) 표현은 호스트에 활성 연결이 있는 호스트의 실시간 그래픽을 표시합니다. 지난 30 분을 표시합니다.

인터페이스

인터페이스 탭에서는 트래픽을 표시해야 하는 활성 네트워크 인터페이스를 선택할 수 있습니다.

> **참고:** 현재 다른 인터페이스에서 흐름 및/또는 호스트를 선택할 수 없습니다

라이브

실시간 로그 섹션에 입력하면, 실시간으로 볼 수 있는 모든 로그 파일 목록이 포함된 상자가 표시됩니다. 보려는 로그 수는 해당 확인란을 선택하여 선택할 수 있으며, `선택된 로그 표시` 버튼을 클릭하면, 새 창에 표시됩니다.

모든 항목을 선택 (Select all) 아래에 있는 확인란을 선택하고, `선택된 로그 표시` 버튼을 클릭하여, 모든 로그 파일을 한 번에 볼 수도 있습니다.

단일 로그 파일은 목록의 오른쪽에 있는, 이 로그만 표시 링크를 클릭하면 볼 수 있습니다.

열린 창에는 상단에 *설정*(Settings)과 하단에 *라이브 로그(live logs)*라는 두 개의 상자가 있습니다.

> **경고:** 생성되는 로그 항목의 수가 많기 때문에, (특히 트래픽이 많은 경우 초당 여러 로그 항목을 생성할 수 있는 방화벽 또는 프록시 로그로 인해) 많은 로그가 표시되면, 로그 항목 목록을 거의 읽을 수 없게 됩니다. 이 경우 표시할 로그는 *설정(Settings)* 상자에서 구성할 수 있습니다.

설정

이 상자를 사용하면 표시할 로그 파일, 색상 및 강조 표시하거나 특정 키워드를 찾는 옵션을 포함하여 로그 뷰어의 설정을 수정할 수 있습니다.

상자의 오른쪽에는 현재 표시되는 로그 목록과 강조 표시된 색상이 표시되며, 왼쪽에는 출력을 제한하는데 도움이 되는 몇 가지 추가 제어 요소가 표시됩니다.

필터

> 이 필드에 표현식이 들어있는 로그 항목 만 표시됩니다.

추가 필터

> 위의 필터와 같지만 첫 번째 필터의 출력에 적용됩니다. 즉, 두식이 모두 포함된 로그 항목만 로그에 표시됩니다.

출력 일시 중지

> 이 버튼을 클릭하면, 새 로그 항목이 라이브 로그에 나타나지 않습니다. 그러나 버튼을 한 번 더 클릭하면, 모든 새 항목이 한꺼번에 표시되어 이전 항목을 빠르게 스크롤합니다.

강조(하이라이트)

> 이 표현식을 포함하는 모든 로그 항목이 선택된 색상으로 강조 표시됩니다. 필터링 옵션의 차이점은 모든 컨텐츠가 계속 표시되고 표현식을 포함하는 로그 항목이 색상이 있는 배경으로 강조 표시된다는 것입니다.

하이라이트 색상

> 색상이 지정된 정사각형을 클릭하면, 강조 표시에 사용할 색상을 선택할 수 있습니다.

자동 스크롤

> 이 옵션은 *Menubar ‣ logs ‣ Settings 섹션의 역순으로 시간순의 정렬 옵션*을 해제한 경우에만 사용할 수 있습니다. 이렇게 하면 페이지의 맨 아래에 모든 새 항목이 표시됩니다. 이 옵션을 사용하면, 목록이 위쪽으로 스크롤 되어 페이지 하단에 최신 항목이 표시됩니다. 그렇지 않으면, 이전 항목만 표시되고 오른쪽에 있는 스크롤 막대가 새로운 것을 보기 위해 사용되어야 합니다.

디스플레이에서 일부 로그를 추가하거나 제거하려면, 오른쪽 상단의 로그 파일 목록 바로 아래에 있는 더 많이 보기 링크를 클릭하십시오. 컨트롤들은 각각의 확인란을 선택 또는 해제하여 원하는 로그 파일을 선택할 수 있는 테이블로 대체됩니다. 로그 파일의 색상을 변경하려면, 해당 로그 유형의 *색상 표*를

클릭한 다음 새로운 색상을 선택하십시오. 컨트롤을 다시 표시하려면, 테이블 아래 또는 표시된 로그 파일 목록 아래에 있는 *닫기* 링크 중 하나를 클릭하십시오.

실시간 로그

보기 위해 선택된 로그가 이 상자에 표시됩니다. 이 상자는 세 개의 열로 나뉘어진 테이블로 구성됩니다.

왼쪽 열

: 이 열은 로그 이름, 즉 로그 항목을 생성하는 데몬 또는 서비스를 포함합니다.

중간 열

: 기록된 이벤트의 타임 스탬프 (날짜 및 시간).

오른쪽 열

: 서비스 또는 데몬에 의해 생성되고 로그 파일에 기록된 실제 메시지.

> **참고:** 일부 로그 메시지, 특히 방화벽 항목은 두 줄 이상에 걸쳐 있습니다. 전체 메시지를 표시하려면, 해당 메시지를 클릭하거나 메시지 오른쪽에 있는 확장 버튼을 클릭하십시오.

마지막으로 상자 머리글에 있는 `높이 증가` 또는 `높이 감소` 버튼을 클릭하여, 창 크기를 늘리거나 줄일 수 있습니다.

공통 작업

시스템, 서비스 및 **방화벽**의 하위 메뉴 항목은 유사한 특성으로 그룹화 된 여러 서비스 및 데몬의 로그 파일을 표시합니다. 이러한 세 가지 항목의 로그 내에서 여러 가지 컨트롤을 사용할 수 있으며, 하나의 추가 옵션이 있는 *시스템* 메뉴 항목이 있습니다. 이 하위 메뉴 항목은 페이지의 공통 구조를 가지며 두 개의 상자로 구성되어 있습니다. 상단에 다음 옵션이 포함된 *설정*(Settings)과 로그 파일의 실제 *메시지*가 포함된 하단에 *로그*가 있습니다.

필터

: 입력된 표현식을 포함하는 행만 표시됩니다.

날짜로 이동

: 이 날짜의 로그 항목을 직접 보여줍니다.

페이지로 이동

결과 집합에 이 페이지의 로그 항목을 직접 보여줍니다. 페이지 당 표시되는 항목 수는 *Menubar ‣ logs ‣ Settings* 페이지에서 수정할 수 있습니다.

업데이트

위의 설정 중 하나를 변경하면, 이 버튼을 클릭하면 페이지 내용이 새로 고쳐집니다.

내보내기

이 버튼을 클릭하면, 로그 항목이 텍스트 파일로 내보내집니다.

로그 서명

이 링크를 클릭하면, 현재 로그에 서명됩니다. 이 버튼은 신뢰할 수 있는 타임 스탬핑이 활성화된 경우에만 사용할 수 있습니다.

이전항목, 새항목

이 두 버튼은 로그 상자에 나타나며 항목 수가 너무 많아지고 두 개 이상의 부분으로 나뉘어 나타날 때마다 표시됩니다. 검색 결과의 오래된 항목이나 새 항목을 클릭하여 검색할 수 있습니다.

> **참고:** 페이지 맨 위에 있는 메시지는 주어진 날짜에 사용 가능한 로그가 없는지를 알려줍니다. 이는 데몬이나 서비스가 실행 중이 아니거나 메시지를 생성하지 않은 경우 발생할 수 있습니다.

이 섹션의 나머지 부분에서는 모든 서비스와 그 고유한 설정이 제공됩니다.

요약

이 페이지는 엔디안 UTM 어플라이언스에서 생성된 로그에 대한 요약을 일 단위로 구분하고, 로그 모니터링 소프트웨어인 **logwatch**에서 생성합니다. 로그 섹션의 다른 부분과는 달리, 여기에는 표시된 세부사항의 레벨을 제어하는 자체 설정이 있습니다. 다음 컨트롤 요소는 페이지 상단의 첫 번째 상자에서 사용할 수 있습니다.

월

이 드롭 다운 메뉴에서 로그 메시지가 생성된 월을 선택하십시오.

일

두 번째 드롭 다운 메뉴에서는 로그 메시지가 생성된 요일을 선택할 수 있습니다.

<<, >>

기록을 탐색하여, 이전 또는 다음 날짜로 이동합니다. 페이지 내용이 자동으로 새로 고쳐집니다.

최신 정보

월/일 조합이 변경되면, 즉시 페이지 내용을 새로 고칩니다.

내보내기

이 버튼을 클릭하면, 텍스트 버전의 요약이 표시되고 로컬 파일 시스템에 저장할 수 있습니다.

설정 상자 아래에 로그 항목을 가지고 있는 실행중인 서비스에 따라, 다양한 수의 상자가 나타납니다. *디스크 공간* 상자는 최소한 볼 수 있어야 하며, 선택한 날짜에 사용 가능한 디스크 공간을 표시해야 합니다. 다른 상자에는 방화벽, DHCP 서버 및 SSHD가 포함될 수 있습니다.

전날 생성된 로그 파일에서 야간에 생성되므로 요일은 현재 날짜에 사용할 수 없다는 것을 주의하십시오.

시스템

이 섹션에서는 다양한 시스템 로그 파일에 대한 로그 뷰어가 나타납니다. Settings (설정) 상자에서는 일반적인 작업 외에도 하나 이상의 옵션을 사용할 수 있습니다.

섹션

드롭 다운 메뉴에서 *모든* 로그를 표시할지 아니면 특정 서비스 또는 데몬과 관련된 로그만 표시할지 선택하십시오. 그 중에는 커널 메시지, SSH 액세스, NTP 및 DHCP가 있습니다

섹션 선택에 따라 업데이트 버튼을 클릭하여, 페이지 하단의 로그 상자에 표시된 로그를 새로 고침하십시오. 이전 및 이후 버튼을 사용하여 페이지를 탐색할 수 있습니다.

서비스

이 섹션에서는 엔디안 UTM 어플라이언스에서 제공하는 세 가지 중요 서비스인 IDS, OpenVPN 및 ClamAV, Panda 또는 둘 다인 안티 바이러스에 대한 로그 항목이 나타납니다. 공통 작업만 사용할 수 있습니다.

방화벽

방화벽 로그 뷰어에는 방화벽의 활동을 기록하는 메시지가 있습니다. 공통 작업만 사용할 수 있습니다.

표의 각 행은 여러 정보와 함께 방화벽에서 기록한 연결입니다.

시간(Time)

메시지가 생성된 타임 스탬프.

체인(Chain)

패킷에 적용된 정책을 포함하여 패킷이 통과한 체인입니다.

Iface

패킷이 통과한 인터페이스입니다.

프로토(Proto)

패킷의 프로토콜.

소스, Src 포트

패킷이 도착한 IP 주소 및 포트입니다.

MAC 주소

원본 인터페이스의 MAC 주소입니다.

대상, Dst 포트

패킷이 도착한 IP 주소 및 포트입니다.

프록시

프록시 로그 뷰어는 프록시를 사용하는 네 개의 데몬에 대한 로그를 표시합니다. 각각의 탭에는 squid (*HTTP*), icap (*콘텐츠 필터*), sarg (*HTTP 보고서*) 및 smtpd (*SMTP, 전자 메일 프록시*) 탭이 있습니다.

HTTP

공통 작업 외에 HTTP 프록시의 로그 뷰어에서 다음 값을 지정할 수 있습니다.

소스 IP

드롭 다운 메뉴에서 선택한 선택한 소스 IP 주소가 포함된 로그 항목 만 표시합니다.

> **참고:** 드롭 다운 메뉴에서 사용할 수있는 IP 주소는 로그 파일에 기록된 IP 주소에 따라 다릅니다.

필터 무시

그것을 포함하는 모든 로그 항목을 걸러내는 정규식.

필터 무시 사용

무시 필터를 사용하려면, 이 확인란을 선택합니다.

기본값으로 복원

이 버튼을 클릭하면, 기본 검색 매개 변수가 복원됩니다.

표시된 로그 항목은 **squid** 소프트웨어에 의해 생성된 로그 항목입니다.

콘텐츠 필터

이 탭에는 이전 HTTP 탭과 동일한 설정이 들어 있으며, 콘텐츠 필터 엔진의 로그 항목이 표시됩니다.

HTTP 보고서

HTTP 보고서 탭에는 하나의 옵션 만 있습니다.

활성화

확인란을 선택하여, 프록시 분석 보고서 생성기를 활성화하고 저장 버튼을 클릭합니다.

보고서 생성기가 활성화되면, *일일 보고서, 주간 보고서* 및 *월간 보고서* 링크를 클릭하여 정기 보고서를 생성하고 액세스 할 수 있습니다.

SMTP

postfix 데몬의 탭에서 공통 작업 만 사용할 수 있습니다. 표시된 로그 항목은 postfix 디먼에 의해 생성된 로그 파일의 항목입니다.

설정

이 페이지에는 엔디안 UTM 어플라이언스의 로깅 기능에 대한 글로벌 구성 옵션이 포함되어 있으며, **로그 보기 옵션, 로그 요약, 원격 로깅** 및 **방화벽 로깅**의 네 가지 상자로 구성되어 있습니다.

로그보기 옵션

표시할 줄 수

페이지 매김 값, 즉 로그 페이지 당 표시되는 행 수입니다.

역순으로 정렬

이 확인란을 선택하면, 최신 로그 항목이 먼저 표시됩니다.

로그 요약

__ 일간 요약 보관

삭제하기 전에 로그 요약을 디스크에 저장하는 기간

상세 수준

로그 요약의 세부 수준: 수준이 높을수록, 더 많은 로그 항목이 저장되고 표시됩니다. 드롭 다운 메뉴는 낮음, 중간 및 높음의 3 가지 세부 수준을 허용합니다.

원격 로깅

활성화

이 상자를 선택하면, 원격 로깅을 사용할 수 있습니다. 다음 옵션을 사용하면 syslog 서버의 호스트 이름을 입력할 수 있습니다.

Syslog 서버

로그가 전송될 원격 서버의 호스트 이름입니다. 서버는 최신 IETF syslog 프로토콜 표준을 지원해야합니다.

프로토콜

원격 syslog 서버와의 통신이 **UDP** 또는 **TCP**를 사용해야하는 경우 드롭 다운 메뉴에서 선택하십시오.

방화벽 로깅

TCP 플래그의 BAD constellation이 있는 로그 패킷

이 옵션을 사용하면, 방화벽은 잘못된 constellation TCP 플래그가 있는 패킷을 기록합니다 (예: 모

든 플래그가 설정됨).

SYN 플래그 없이 새로운 연결을 기록하십시오

이 옵션을 사용하면, SYN 플래그가 없는 모든 새로운 TCP 연결이 기록됩니다.

허용된 발신 연결 로그

허용된 모든 나가는 연결을 기록하려면, 이 확인란을 선택해야 합니다.

거부된 패킷에 대한 로그

이 옵션을 사용하면, 거부된 모든 패킷이 방화벽에 의해 기록됩니다.

증가하는 로깅 파일 및 디스크 공간 관리

Endian UTM Appliance에 로그 파일을 저장하는 표준 정책은 다음과 같습니다. 매일 밤, 로그 파일은 순환하며, *daemonname.nnn.gz*로 저장되고, 새로운 메시지는 새 로그 파일에 기록됩니다. nnn은 1부터 시작하는 점진적 숫자입니다. 특히 New Mini ARM에서 일부 어플라이언스의 경우, 디스크 공간이 빠르게 채워질 수 있습니다 (특히 많은 데몬이 활발하게 로깅중인 경우).

이 정책은 2.5 릴리스 이후 변경되었습니다. 2.4 버전까지, Endian UTM Appliance의 로그 저장 정책은 각 서비스에 대해 365일 동안 로그 파일을 보관하고, 나중에 삭제하는 것이 었습니다. 2.5 버전 출시 이후의 새로운 정책은 로그를 저장하는 파티션의 공간이 부족할 때, 오래된 로그 파일을 삭제하고, 새로운 로그 파일을 저장할 공간을 마련하는 것입니다. 좀 더 정확히 말하자면, 처음 정책이 변경된 패키지는 efw-syslog-2.6.5-1.endian9.noarch.rpm (2.4-ARM), efw-syslog-2.9.8-1.endian9.noarch.rpm (2.5) 입니다.

새로운 정책은 여러 가지 필요에 맞게 수정하거나 되돌릴 수 있습니다.

추가 참고사항: 로깅에 대한 정책에 대한 자세한 내용은 이 문서에서 확인할 수 있습니다.

추가 참고사항: Endian UTM 어플라이언스의 여유 공간에 대한 몇 가지 지침은 여기에서 찾을 수 있습니다.

신뢰할 수있는 타임 스탬핑

신뢰할 수 있는 타임 스탬프는 로그 파일 (일반적으로 모든 문서)이 원본 및 원본 준수를 추적하고 인증하는 프로세스입니다. 즉, 신뢰할 수 있는 타임 스탬프를 사용하면, 원본 작성자가 아닌 모든 사람이 로그 파일을 수정하지 않았음을 인증하고 확인할 수 있습니다. 로그 파일의 경우, 신뢰할 수 있는 타임 스탬프는 예를 들어, 독립 감사의 경우에도 시스템에 대한 액세스 또는 VPN 사용자의 연결을 확인하는데 유용합니다.

신뢰할 수 있는 타임 스탬프는 기본적으로 사용하도록 설정되어 있지 않지만, 활성화하려면 회색 스위치를 클릭해야 합니다. 녹색으로 바뀌면, 일부 구성 옵션이 표시됩니다.

타임 스탬프 서버 URL

타임 스탬프 서버 (TSA라고도 함)의 URL은 로그 파일에 서명하는 것이 이 서버이기 때문에 필수 항목입니다.

> **참고:** 신뢰할 수있는 타임 스탬프를 사용하려면 유효한 TSA의 유효한 URL이 필요합니다. 여러 회사가 이러한 종류의 서비스를 제공할 수 있습니다.

HTTP 인증

타임 스탬프 서버가 인증을 요구하면, HTTP 인증 레이블 아래의 상자를 선택하십시오.

사용자 이름

타임 스탬프 서버에서 인증하는데 사용되는 사용자 이름입니다.

암호.

타임 스탬프 서버에서 인증하는데 사용되는 암호입니다.

타임 스탬핑 서버의 공개 키

서버와의 통신을 보다 쉽고 안전하게하기 위해 서버의 공용 키를 가져올 수 있습니다. 찾아보기... 버튼을 클릭하여 로컬 컴퓨터에서 인증서 파일을 검색한 다음 업로드 버튼을 클릭하여, Endian UTM Appliance에 업로드 할 수 있습니다. 인증서가 저장되면, *타임 스탬프 서버* 레이블의 *공개 키* 옆에 있는 다른 Endian UTM Appliance(기기)에 설치해야 하는 경우처럼, 인증서를 검색할 수 있도록 클릭할 수 있는 다운로드 링크가 나타납니다.

Save (저장) 버튼을 클릭하면, 설정이 저장되고 다음 요일에는 *Settings (설정)* 상자의 오른쪽에 있는 *Logs (로그)* 섹션에 새로운 버튼이 나타납니다.

로그 서명 확인

이것을 클릭하면, 노란색 설명 선에 메시지가 표시되어 로그의 상태를 알려줍니다.

추가 참고사항: 공식 OpenSSL 타임 스탬프 문서와 타임 스탬프 프로토콜의 원래 정의인 RFC 3161을 참조하십시오.