DefensePro for Cisco Firepower 9300 사용 설명서
소프트웨어 버전 1.01.02
마지막 업데이트: 2016년 4월 4일 화요일

중요 공지 사항

다음 중요 공지 사항은 영어, 프랑스어 및 독일어로 표시됩니다.

중요 공지 사항

Notice importante

Wichtige Anmerkung

저작권 정보

다음 저작권 정보는 영어, 프랑스어 및 독일어로 표시됩니다.

Copyright Notices

The programs included in this product are subject to a restricted use license and can only be used in conjunction with this application.

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL, please contact openssl-core@openssl.org.

OpenSSL License

Copyright (c) 1998-2011 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.

This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgment:

   "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS”" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

This product contains the Rijndael cipher

The Rijndael implementation by Vincent Rijmen, Antoon Bosselaers and Paulo Barreto is in the public domain and distributed with the following license:

@version 3.0 (December 2000)

Optimized ANSI C code for the Rijndael cipher (now AES)

@author Vincent Rijmen <vincent.rijmen@esat.kuleuven.ac.be>

@author Antoon Bosselaers <antoon.bosselaers@esat.kuleuven.ac.be>

@author Paulo Barreto <paulo.barreto@terra.com.br>

The OnDemand Switch may use software components licensed under the GNU General Public License Agreement Version 2 (GPL v.2) including LinuxBios and Filo open source projects. The source code of the LinuxBios and Filo is available from Radware upon request. A copy of the license can be viewed at: http://www.gnu.org/licenses/old-licenses/gpl-2.0.html.

This code is hereby placed in the public domain.

This product contains code developed by the OpenBSD Project Copyright

©1983, 1990, 1992, 1993, 1995

The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

This product includes software developed by Markus Friedl. This

product includes software developed by Theo de Raadt. This product

includes software developed by Niels Provos This product includes

software developed by Dug Song This product includes software

developed by Aaron Campbell This product includes software

developed by Damien Miller This product includes software developed

by Kevin Steves This product includes software developed by Daniel

Kouril This product includes software developed by Wesley Griffin

This product includes software developed by Per Allansson This

product includes software developed by Nils Nordman

This product includes software developed by Simon Wilkinson

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

This product contains work derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm. RSA Data Security, Inc. makes no representations concerning either the merchantability of the MD5 Message - Digest Algorithm or the suitability of the MD5 Message - Digest Algorithm for any particular purpose. It is provided “as is” without express or implied warranty of any kind.

Notice traitant du copyright

Les programmes intégrés dans ce produit sont soumis à une licence d’utilisation limitée et ne peuvent être utilisés qu’en lien avec cette application.

L’implémentation de Rijindael par Vincent Rijmen, Antoon Bosselaers et Paulo Barreto est du domaine public et distribuée sous les termes de la licence suivante:

@version 3.0 (Décembre 2000)

Code ANSI C code pour Rijndael (actuellement AES)

@author Vincent Rijmen <vincent.rijmen@esat.kuleuven.ac.be>

@author Antoon Bosselaers <antoon.bosselaers@esat.kuleuven.ac.be>

@author Paulo Barreto <paulo.barreto@terra.com.br>.

Le commutateur OnDemand peut utiliser les composants logiciels sous licence, en vertu des termes de la licence GNU General Public License Agreement Version 2 (GPL v.2), y compris les projets à source ouverte LinuxBios et Filo. Le code source de LinuxBios et Filo est disponible sur demande auprès de Radware. Une copie de la licence est répertoriée sur: http://www.gnu.org/licenses/old-licenses/gpl-2.0.html.

Ce code est également placé dans le domaine public.

Ce produit renferme des codes développés dans le cadre du projet OpenSSL. Copyright

©1983, 1990, 1992, 1993, 1995

Les membres du conseil de l'Université de Californie. Tous droits réservés.

La distribution et l'usage sous une forme source et binaire, avec ou sans modifications, est autorisée pour autant que les conditions suivantes soient remplies:

1. La distribution d'un code source doit inclure la notice de copyright mentionnée ci-dessus, cette liste de conditions et l'avis de non-responsabilité suivant.
2. La distribution, sous une forme binaire, doit reproduire dans la documentation et/ou dans tout autre matériel fourni la notice de copyright mentionnée ci-dessus, cette liste de conditions et l'avis de non-responsabilité suivant.
3. Le nom de l'université, ainsi que le nom des contributeurs ne seront en aucun cas utilisés pour approuver ou promouvoir un produit dérivé de ce programme sans l'obtention préalable d'une autorisation écrite.

Ce produit inclut un logiciel développé par Markus Friedl. Ce

produit inclut un logiciel développé par Theo de Raadt. Ce produit

inclut un logiciel développé par Niels Provos.

Ce produit inclut un logiciel développé par Dug Song.

Ce produit inclut un logiciel développé par Aaron Campbell. Ce

produit inclut un logiciel développé par Damien Miller.

Ce produit inclut un logiciel développé par Kevin Steves. Ce produit

inclut un logiciel développé par Daniel Kouril. Ce produit inclut un

logiciel développé par Wesley Griffin. Ce produit inclut un logiciel

développé par Per Allansson. Ce produit inclut un logiciel développé

par Nils Nordman. Ce produit inclut un logiciel développé par Simon

Wilkinson.

La distribution et l'usage sous une forme source et binaire, avec ou sans modifications, est autorisée pour autant que les conditions suivantes soient remplies:

1. La distribution d'un code source doit inclure la notice de copyright mentionnée ci-dessus, cette liste de conditions et l'avis de non-responsabilité suivant.
2. La distribution, sous une forme binaire, doit reproduire dans la documentation et/ou dans tout autre matériel fourni la notice de copyright mentionnée ci-dessus, cette liste de conditions et l'avis de non-responsabilité suivant.

LE LOGICIEL MENTIONNÉ CI-DESSUS EST FOURNI TEL QUEL PAR LE DÉVELOPPEUR ET TOUTE GARANTIE, EXPLICITE OU IMPLICITE, Y COMPRIS, MAIS SANS S'Y LIMITER, TOUTE GARANTIE IMPLICITE DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER EST EXCLUE.

EN AUCUN CAS L'AUTEUR NE POURRA ÊTRE TENU RESPONSABLE DES DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, SPÉCIAUX, EXEMPLAIRES OU CONSÉCUTIFS (Y COMPRIS, MAIS SANS S'Y LIMITER, L'ACQUISITION DE BIENS OU DE SERVICES DE REMPLACEMENT, LA PERTE D'USAGE, DE DONNÉES OU DE PROFITS OU L'INTERRUPTION DES AFFAIRES), QUELLE QU'EN SOIT LA CAUSE ET LA THÉORIE DE RESPONSABILITÉ, QU'IL S'AGISSE D'UN CONTRAT, DE RESPONSABILITÉ STRICTE OU D'UN ACTE DOMMAGEABLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE), DÉCOULANT DE QUELLE QUE FAÇON QUE CE SOIT DE L'USAGE DE CE LOGICIEL, MÊME S'IL A ÉTÉ AVERTI DE LA POSSIBILITÉ D'UN TEL DOMMAGE.

Copyrightvermerke

Die in diesem Produkt enthalten Programme unterliegen einer eingeschränkten Nutzungslizenz und können nur in Verbindung mit dieser Anwendung benutzt werden.

Die Rijndael-Implementierung von Vincent Rijndael, Anton Bosselaers und Paulo Barreto ist öffentlich zugänglich und wird unter folgender Lizenz vertrieben:

@version 3.0 (December 2000)

Optimierter ANSI C Code für den Rijndael cipher (jetzt AES)

@author Vincent Rijmen <vincent.rijmen@esat.kuleuven.ac.be>

@author Antoon Bosselaers <antoon.bosselaers@esat.kuleuven.ac.be>

@author Paulo Barreto <paulo.barreto@terra.com.br>

Der OnDemand Switch verwendet möglicherweise Software, die im Rahmen der DNU Allgemeine Öffentliche Lizenzvereinbarung Version 2 (GPL v.2) lizensiert sind, einschließlich LinuxBios und Filo Open Source-Projekte. Der Quellcode von LinuxBios und Filo ist bei Radware auf Anfrage erhältlich. Eine Kopie dieser Lizenz kann eingesehen werden unter http://www.gnu.org/licenses/old-licenses/gpl-2.0.html.

Dieser Code wird hiermit allgemein zugänglich gemacht.

Dieses Produkt enthält einen vom OpenBSD-Projekt entwickelten Code Copyright ©1983,

1990, 1992, 1993, 1995

The Regents of the University of California. Alle Rechte vorbehalten.

Die Verbreitung und Verwendung in Quell- und binärem Format, mit oder ohne Veränderungen, sind unter folgenden Bedingungen erlaubt:

1. Die Verbreitung von Quellcodes muss den voranstehenden Copyrightvermerk, diese Liste von Bedingungen und den folgenden Haftungsausschluss beibehalten.
2. Die Verbreitung in binärem Format muss den voranstehenden Copyrightvermerk, diese Liste von Bedingungen und den folgenden Haftungsausschluss in der Dokumentation und/oder andere Materialien, die mit verteilt werden, reproduzieren.
3. Weder der Name der Universität noch die Namen der Beitragenden dürfen ohne ausdrückliche vorherige schriftliche Genehmigung verwendet werden, um von dieser Software abgeleitete Produkte zu empfehlen oder zu bewerben.

Dieses Produkt enthält von Markus Friedl entwickelte Software. Dieses

Produkt enthält von Theo de Raadt entwickelte Software. Dieses Produkt

enthält von Niels Provos entwickelte Software.

Dieses Produkt enthält von Dug Song entwickelte Software. Dieses

Produkt enthält von Aaron Campbell entwickelte Software. Dieses Produkt

enthält von Damien Miller entwickelte Software. Dieses Produkt enthält von

Kevin Steves entwickelte Software.

Dieses Produkt enthält von Daniel Kouril entwickelte Software. Dieses Produkt

enthält von Wesley Griffin entwickelte Software. Dieses Produkt enthält von

Per Allansson entwickelte Software. Dieses Produkt enthält von Nils Nordman

entwickelte Software. Dieses Produkt enthält von Simon Wilkinson entwickelte

Software.

Die Verbreitung und Verwendung in Quell- und binärem Format, mit oder ohne Veränderungen, sind unter folgenden Bedingungen erlaubt:

1. Die Verbreitung von Quellcodes muss den voranstehenden Copyrightvermerk, diese Liste von Bedingungen und den folgenden Haftungsausschluss beibehalten.
2. Die Verbreitung in binärem Format muss den voranstehenden Copyrightvermerk, diese Liste von Bedingungen und den folgenden Haftungsausschluss in der Dokumentation und/oder andere Materialien, die mit verteilt werden, reproduzieren.

SÄMTLICHE VORGENANNTE SOFTWARE WIRD VOM AUTOR IM IST-ZUSTAND (“AS IS”) BEREITGESTELLT. JEGLICHE AUSDRÜCKLICHEN ODER IMPLIZITEN GARANTIEN, EINSCHLIESSLICH, DOCH NICHT BESCHRÄNKT AUF DIE IMPLIZIERTEN GARANTIEN DER MARKTGÄNGIGKEIT UND DER ANWENDBARKEIT FÜR EINEN BESTIMMTEN ZWECK, SIND AUSGESCHLOSSEN.

UNTER KEINEN UMSTÄNDEN HAFTET DER AUTOR FÜR DIREKTE ODER INDIREKTE SCHÄDEN, FÜR BEI VERTRAGSERFÜLLUNG ENTSTANDENE SCHÄDEN, FÜR BESONDERE SCHÄDEN, FÜR SCHADENSERSATZ MIT STRAFCHARAKTER, ODER FÜR FOLGESCHÄDEN EINSCHLIESSLICH, DOCH NICHT BESCHRÄNKT AUF, ERWERB VON ERSATZGÜTERN ODER ERSATZLEISTUNGEN; VERLUST AN NUTZUNG, DATEN ODER GEWINN; ODER GESCHÄFTSUNTERBRECHUNGEN) GLEICH, WIE SIE ENTSTANDEN SIND, UND FÜR JEGLICHE ART VON HAFTUNG, SEI ES VERTRÄGE, GEFÄHRDUNGSHAFTUNG, ODER DELIKTISCHE HAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER ANDERE), DIE IN JEGLICHER FORM FOLGE DER BENUTZUNG DIESER SOFTWARE IST, SELBST WENN AUF DIE MÖGLICHKEIT EINES SOLCHEN SCHADENS HINGEWIESEN WURDE.

표준 보증

다음 표준 보증은 영어, 프랑스어 및 독일어로 표시됩니다.

Standard Warranty

Radware offers a limited warranty for all its products (“Products”). Radware hardware products are warranted against defects in material and workmanship for a period of one year from date of shipment. Radware software carries a standard warranty that provides bug fixes for up to 90 days after date of purchase. Should a Product unit fail anytime during the said period(s), Radware will, at its discretion, repair or replace the Product.

For hardware warranty service or repair, the product must be returned to a service facility designated by Radware. Customer shall pay the shipping charges to Radware and Radware shall pay the shipping charges in returning the product to the customer. Please see specific details outlined in the Standard Warranty section of the customer’s purchase order.

Radware shall be released from all obligations under its Standard Warranty in the event that the Product and/or the defective component has been subjected to misuse, neglect, accident or improper installation, or if repairs or modifications were made by persons other than Radware authorized service personnel, unless such repairs by others were made with the written consent of Radware.

EXCEPT AS SET FORTH ABOVE, ALL RADWARE PRODUCTS (HARDWARE AND SOFTWARE) ARE PROVIDED BY “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.

Garantie standard

Radware octroie une garantie limitée pour l’ensemble de ses produits (“Produits”). Le matériel informatique (hardware) Radware est garanti contre tout défaut matériel et de fabrication pendant une durée d’un an à compter de la date d’expédition. Les logiciels (software) Radware sont fournis avec une garantie standard consistant en la fourniture de correctifs des dysfonctionnements du logiciels (bugs) pendant une durée maximum de 90 jours à compter de la date d’achat. Dans l’hypothèse où un Produit présenterait un défaut pendant ladite (lesdites) période(s), Radware procédera, à sa discrétion, à la réparation ou à l’échange du Produit.

S’agissant de la garantie d’échange ou de réparation du matériel informatique, le Produit doit être retourné chez un réparateur désigné par Radware. Le Client aura à sa charge les frais d’envoi du Produit à Radware et Radware supportera les frais de retour du Produit au client. Veuillez consulter les conditions spécifiques décrites dans la partie “Garantie Standard” du bon de commande client.

Radware est libérée de toutes obligations liées à la Garantie Standard dans l'hypothèse où le Produit et/ou le composant défectueux a fait l'objet d'un mauvais usage, d'une négligence, d'un accident ou d'une installation non conforme, ou si les réparations ou les modifications qu'il a subi ont été effectuées par d'autres personnes que le personnel de maintenance autorisé par Radware, sauf si Radware a donné son consentement écrit à ce que de telles réparations soient effectuées par ces personnes.

SAUF DANS LES CAS PREVUS CI-DESSUS, L'ENSEMBLE DES PRODUITS RADWARE (MATERIELS ET LOGICIELS) SONT FOURNIS "TELS QUELS" ET TOUTES GARANTIES EXPRESSES OU IMPLICITES SONT EXCLUES, EN CE COMPRIS, MAIS SANS S'Y RESTREINDRE, LES GARANTIES IMPLICITES DE QUALITE MARCHANDE ET D'ADÉQUATION À UNE UTILISATION PARTICULIÈRE.

보증 및 책임 제한사항

다음 보증 및 책임 제한사항은 영어, 프랑스어 및 독일어로 표시됩니다.

Limitations on Warranty and Liability

IN NO EVENT SHALL RADWARE LTD. OR ANY OF ITS AFFILIATED ENTITIES BE LIABLE FOR ANY DAMAGES INCURRED BY THE USE OF THE PRODUCTS (INCLUDING BOTH HARDWARE AND SOFTWARE) DESCRIBED IN THIS USER GUIDE, OR BY ANY DEFECT OR INACCURACY IN THIS USER GUIDE ITSELF. THIS INCLUDES BUT IS NOT LIMITED TO ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION). THE ABOVE LIMITATIONS WILL APPLY EVEN IF RADWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF IMPLIED WARRANTIES OR LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

Limitations de la Garantie et Responsabilité

RADWARE LTD. OU SES ENTITIES AFFILIES NE POURRONT EN AUCUN CAS ETRE TENUES RESPONSABLES DES DOMMAGES SUBIS DU FAIT DE L'UTILISATION DES PRODUITS (EN CE COMPRIS LES MATERIELS ET LES LOGICIELS) DECRITS DANS CE MANUEL D'UTILISATION, OU DU FAIT DE DEFAUT OU D'IMPRECISIONS DANS CE MANUEL D'UTILISATION, EN CE COMPRIS, SANS TOUTEFOIS QUE CETTE ENUMERATION SOIT CONSIDEREE COMME LIMITATIVE, TOUS DOMMAGES DIRECTS, INDIRECTS, ACCIDENTELS, SPECIAUX, EXEMPLAIRES, OU ACCESSOIRES (INCLUANT, MAIS SANS S'Y RESTREINDRE, LA FOURNITURE DE PRODUITS OU DE SERVICES DE REMPLACEMENT; LA PERTE D'UTILISATION, DE DONNEES OU DE PROFITS; OU L'INTERRUPTION DES AFFAIRES). LES LIMITATIONS CI-DESSUS S'APPLIQUERONT QUAND BIEN MEME RADWARE A ETE INFORMEE DE LA POSSIBLE EXISTENCE DE CES DOMMAGES. CERTAINES JURIDICTIONS N'ADMETTANT PAS LES EXCLUSIONS OU LIMITATIONS DE GARANTIES IMPLICITES OU DE RESPONSABILITE EN CAS DE DOMMAGES ACCESSOIRES OU INDIRECTS, LESDITES LIMITATIONS OU EXCLUSIONS POURRAIENT NE PAS ETRE APPLICABLE DANS VOTRE CAS.

Haftungs- und Gewährleistungsausschluss

IN KEINEM FALL IST RADWARE LTD. ODER EIN IHR VERBUNDENES UNTERNEHMEN HAFTBAR FÜR SCHÄDEN, WELCHE BEIM GEBRAUCH DES PRODUKTES (HARDWARE UND SOFTWARE) WIE IM BENUTZERHANDBUCH BESCHRIEBEN, ODER AUFGRUND EINES FEHLERS ODER EINER UNGENAUIGKEIT IN DIESEM BENUTZERHANDBUCH SELBST ENTSTANDEN SIND. DAZU GEHÖREN UNTER ANDEREM (OHNE DARAUF BEGRENZT ZU SEIN) JEGLICHE DIREKTEN; IDIREKTEN; NEBEN; SPEZIELLEN, BELEGTEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH ABER NICHT BEGRENZT AUF BESCHAFFUNG ODER ERSATZ VON WAREN ODER DIENSTEN, NUTZUNGSAUSFALL, DATEN- ODER GEWINNVERLUST ODER BETRIEBSUNTERBRECHUNGEN). DIE OBEN GENANNTEN BEGRENZUNGEN GREIFEN AUCH, SOFERN RADWARE AUF DIE MÖGLICHKEIT EINES SOLCHEN SCHADENS HINGEWIESEN WORDEN SEIN SOLLTE. EINIGE RECHTSORDNUNGEN LASSEN EINEN AUSSCHLUSS ODER EINE BEGRENZUNG STILLSCHWEIGENDER GARANTIEN ODER HAFTUNGEN BEZÜGLICH NEBEN- ODER FOLGESCHÄDEN NICHT ZU, SO DASS DIE OBEN DARGESTELLTE BEGRENZUNG ODER DER AUSSCHLUSS SIE UNTER UMSTÄNDEN NICHT BETREFFEN WIRD.

보안 지침

다음 보안 지침은 영어, 프랑스어 및 독일어로 표시됩니다.

보안 지침

주의

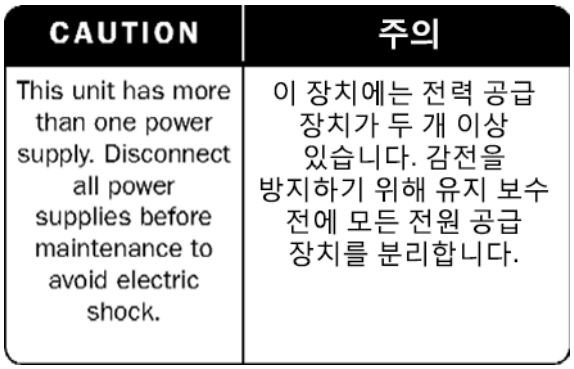
쉽게 액세스 가능한 분리형 디바이스는 빌딩 설치 배선에 통합되어야 합니다.

감전의 위험과 에너지, 기계 및 화재 위험으로 인해 패널을 열거나 구성 요소를 교체하는 모든 절차는 자격이 있는 서비스 담당자만 수행해야 합니다.

화재 및 감전의 위험을 줄이기 위해 덮개나 패널을 제거하기 전에 디바이스에서 전선을 분리하십시오.

다음 그림은 듀얼 전원 공급장치가 있는 Radware 플랫폼에 어태치된 주의 라벨을 보여줍니다.

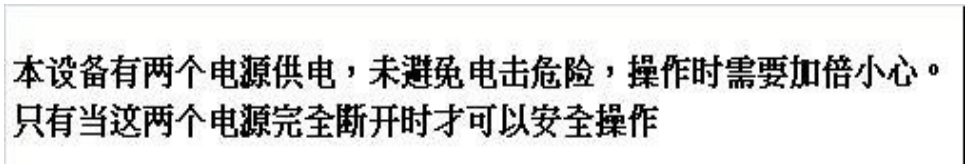
그림 1: 감전 위험 라벨



중국어로 된 듀얼 전원 공급장치 안전 경고

다음 그림은 듀얼 전원 공급장치가 있는 Radware 플랫폼의 경고입니다.

그림 2: 중국어로 된 듀얼 전원 공급장치 안전 경고



중국어로 된 듀얼 전원 공급장치 안전 경고 번역본:

이 장치에는 전력 공급 장치가 두 개 이상 있습니다. 감전을 방지하기 위해 유지 보수 전에 모든 전원 공급 장치를 분리합니다.

서비스 제공

자격을 갖춘 경우가 아니면 운영 지침에 포함된 내용 이외의 서비스를 수행하지 마십시오. 장치 내에 서비스 가능한 부품이 없습니다.

고전압

전압이 흐르는 개봉된 장비의 조정, 유지관리 및 수리는 최대한 피하고, 불가피한 경우에는 수반된 위험을 인지하고 있는 숙련된 사람만 수행해야 합니다.

전원 공급 장치에서 장비가 분리된 경우에도 장비 내부의 콘덴서가 계속 충전 중일 수 있습니다.

접지

이 디바이스를 전선에 연결하기 전에 이 디바이스의 보호 접지 터미널 나사를 빌딩 설치의 보호 접지에 연결해야 합니다.

레이저

이 장비는 IEC60825 - 1: 1993 + A1:1997 + A2:2001 표준을 준수하는 클래스 1 레이저 제품입니다.

퓨즈

교체 시 필수 정격 전류를 사용하고 지정된 유형의 퓨즈만 사용하십시오. 수리된 퓨즈와 합선된 퓨즈 홀더는 사용하지 않아야 합니다. 퓨즈에서 제공하는 보호가 손상된 경우 장비가 작동되지 않아야 하며 의도하지 않은 동작으로부터 보호되어야 합니다.

선간 전압

이 장비를 전선에 연결하기 전에 전원의 전압이 장비의 요구사항과 일치하는지 확인하십시오. 디바이스의 올바른 정격 용량에 대한 정보는 사양을 참조하십시오.

48V DC 전원 플랫폼의 입력 공차는 36-72V DC입니다.

사양 변경

사양은 예고 없이 변경될 수 있습니다.

참고: 이 장비는 테스트를 마쳤으며, Part 15B of the FCC Rules 및 EN55022 Class A, EN 55024; EN 61000-3-2; EN 61000-3-3; IEC 61000 4-2 to 4-6, IEC 61000 4-8 and IEC 61000-4-11For CE MARK Compliance에 따라 Class A 디지털 디바이스의 제한사항을 준수하는 것으로 확인되었습니다.
이러한 제한은 장비를 상업 환경에서 작동하는 경우 유해한 간섭을 적절하게 차단할 수 있도록 설계되었습니다. 이 장비는 무선 주파수 에너지를 생성, 사용 및 방사할 수 있으며 지침 매뉴얼에 따라 설치 및 사용하지 않는 경우 무선 통신에 유해한 간섭을 생성할 수 있습니다. 가정에서 이 장비를 작동하는 경우 유해한 간섭이 발생할 가능성이 높으며, 이러한 경우 사용자는 간섭을 직접 수정해야 합니다.

북미 사용자를 위한 특별 공지사항

북미에서 전원을 연결하는 경우 UL 승인 및 CSA 인증 3 전도체, [18AWG]이며, 끝이 몰드로 된 플러그 캡이고, 정격 125V, [10A]이며, 길이가 1.5m[6피트] 이상 4.5m 미만인 전원 공급장치 코드를 선택하십시오. 유럽에서 연결하는 경우에는 국제적으로 통일되어 “<HAR>”이 표시되는 3 - 전도체, 0,75mm2 최소 mm2 전선, 정격 300V의 PVC 절연 커버가 있는 전원 공급장치 코드를 선택하십시오. 코드는 정격 250V, 3A의 플러그 캡으로 덮여 있어야 합니다.

영역 액세스 제한

DC 전원 장비는 액세스가 제한된 액세스 영역에만 설치해야 합니다.

설치 코드

이 디바이스는 국정 전기 규격에 따라 설치해야 합니다. 북미의 경우, 장비는 US National Electrical Code, Articles 110 - 16, 110 -17 및 110 -18과 Canadian Electrical Code, Section 12에 따라 설치해야 합니다.

장비 상호 연결

RS232 장비와 이더넷 인터페이스를 연결하는 케이블은 UL 인증 유형 DP-1 또는 DP-2이어야 합니다. (참고- 비LPS 회로에 있는 경우)

과전류 보호

전류 보호 디바이스 정격 15A를 초과하는 쉽게 액세스할 수 있는 등록된 분기 회로는 각 전원 입력을 위한 빌딩 배선에 통합되어야 합니다.

교체 가능 배터리

장비에 교체 가능한 배터리가 장착되어 제공되는 경우, 올바르지 않은 유형의 배터리로 교체하면 폭발할 수 있습니다. 리튬 배터리를 사용하는 경우에 해당되며 다음이 적용됩니다.

- 배터리가 **작업자 액세스 영역**에 있는 경우, 배터리 가까이에 표시가 있거나 운영 지침과 서비스 지침 모두에 명시문이 있습니다.
- 배터리가 장비의 다른 위치에 있으면, 배터리 근처에 표시가 있거나 서비스 지침 모두에 명시문이 있습니다.

이 표시나 명시문에는 다음과 같은 텍스트 경고가 있습니다. 주의

배터리를 올바르지 않은 배터리 유형으로 교체하는 경우 폭발의 위험이 있습니다. 사용한 배터리는 지침에 따라 폐기하십시오.

주의 - 감전 및 화재의 위험을 줄이기 위해

1. 이 장비는 DC 공급회로의 접지 전도체와 접지 전도체 장비 사이에 연결이 가능하도록 설계되었습니다. 설치 지침을 참조하십시오.
2. 모든 서비스는 자격이 있는 서비스 담당자가 수행해야 합니다. 장치 내에 사용자가 서비스 가능한 부품이 없습니다.
3. 명확하게 손상된 장비의 플러그를 연결하거나 켜거나 작동하려고 하지 마십시오.
4. 장비의 섀시 통풍구가 막히지 않게 하십시오.
5. 퓨즈가 끊어진 경우에만 퓨즈가 들어 있는 전원 입력부 옆의 안전 라벨에 표시된 유형 및 등급과 동일한 퓨즈로만 교체하십시오.
6. 최대 주변 온도가 40°C/104°F를 넘는 위치에서 디바이스를 작동시키지 마십시오.
7. 주 전원 퓨즈를 제거 및/또는 확인하기 전에 벽 소켓에서 전원 공급장치 코드의 플러그를 빼십시오.
   CLASS 1 LASER PRODUCT AND REFERENCE TO THE MOST RECENT LASER STANDARDS IEC 60 825-1:1993 + A1:1997 + A2:2001 AND EN 60825-1:1994+A1:1996+ A2:2001

덴마크, 핀란드, 노르웨이, 스웨덴의 AC 장치(제품에 표시됨):

- 덴마크 - “Unit is class I - 덴마크 규격 차이점에 적합한 AC 코드 세트와 함께 사용되는 장치입니다. 코드에는 접지 전도체가 포함되어 있습니다. 장치의 플러그를 보호 접지에 연결된 벽 소켓 콘센트에 꽂습니다. 접지에 연결되지 않은 소켓 콘센트는 사용하면 안 됩니다.”
- 핀란드(표시 라벨 및 매뉴얼) - “Laite on liitettävä suojamaadoituskoskettimilla varustettuun pistorasiaan”
- 노르웨이(표시 라벨 및 매뉴얼) - “Apparatet må tilkoples jordet stikkontakt”
- 장치는 노르웨이의 IT 전원 시스템에만 연결해야 합니다.
- 스웨덴(표시 라벨 및 매뉴얼) - “Apparaten skall anslutas till jordat uttag.”

전원을 연결하려면 다음을 수행합니다.

1. 디바이스의 뒷면 패널에 있는 주 소켓에 전원 케이블을 연결합니다.
2. 전원 케이블을 접지된 AC 콘센트에 연결합니다. 주의

감전의 위험 및 에너지 위험이 있습니다. 하나의 전원 공급장치를 분리하면 하나의 전원 공급장치 모듈만 분리됩니다. 장치를 완전히 절연하려면 모든 전원 공급장치를 분리하십시오.

Instructions de sécurité

AVERTISSEMENT

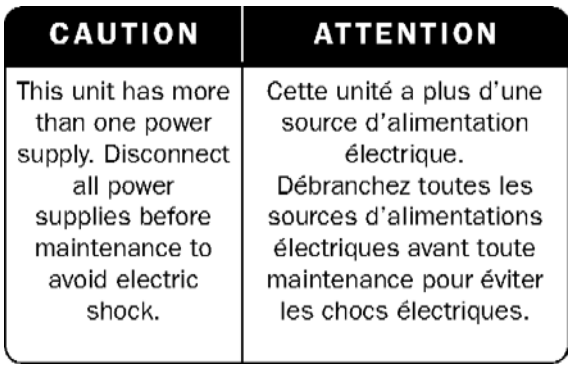
Un dispositif de déconnexion facilement accessible sera incorporé au câblage du bâtiment.

En raison des risques de chocs électriques et des dangers énergétiques, mécaniques et d’incendie, chaque procédure impliquant l’ouverture des panneaux ou le remplacement de composants sera exécutée par du personnel qualifié.

Pour réduire les risques d’incendie et de chocs électriques, déconnectez le dispositif du bloc d’alimentation avant de retirer le couvercle ou les panneaux.

La figure suivante montre l’étiquette d’avertissement apposée sur les plateformes Radware dotées de plus d’une source d’alimentation électrique.

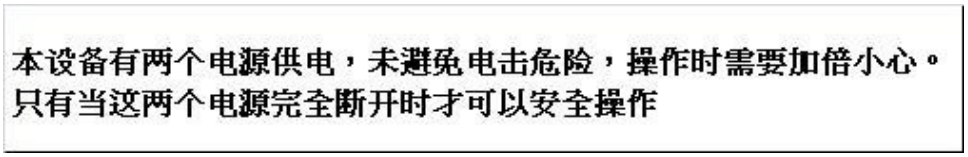
Figure 3: Étiquette d’avertissement de danger de chocs électriques



AVERTISSEMENT DE SÉCURITÉ POUR LES SYSTÈMES DOTÉS DE DEUX SOURCES D’ALIMENTATION ÉLECTRIQUE (EN CHINOIS)

La figure suivante représente l’étiquette d’avertissement pour les plateformes Radware dotées de deux sources d’alimentation électrique.

Figure 4: Avertissement de sécurité pour les systèmes dotes de deux sources d'alimentation électrique (en chinois)



Traduction de la Avertissement de sécurité pour les systèmes dotes de deux sources d'alimentation électrique (en chinois):

Cette unité est dotée de plus d'une source d'alimentation électrique. Déconnectez toutes les sources d'alimentation électrique avant d'entretenir l'appareil ceci pour éviter tout choc électrique.

ENTRETIEN

N'effectuez aucun entretien autre que ceux répertoriés dans le manuel d'instructions, à moins d'être qualifié en la matière. Aucune pièce à l'intérieur de l'unité ne peut être remplacée ou réparée.

HAUTE TENSION

Tout réglage, opération d'entretien et réparation de l'instrument ouvert sous tension doit être évité. Si cela s'avère indispensable, confiez cette opération à une personne qualifiée et consciente des dangers impliqués.

Les condensateurs au sein de l'unité risquent d'être chargés même si l'unité a été déconnectée de la source d'alimentation électrique.

MISE A LA TERRE

Avant de connecter ce dispositif à la ligne électrique, les vis de protection de la borne de terre de cette unité doivent être reliées au système de mise à la terre du bâtiment.

LASER

Cet équipement est un produit laser de classe 1, conforme à la norme IEC60825 - 1: 1993 + A1: 1997 + A2: 2001.

FUSIBLES

Assurez-vous que, seuls les fusibles à courant nominal requis et de type spécifié sont utilisés en remplacement. L'usage de fusibles réparés et le court-circuitage des porte-fusibles doivent être évités. Lorsqu'il est pratiquement certain que la protection offerte par les fusibles a été détériorée, l'instrument doit être désactivé et sécurisé contre toute opération involontaire.

TENSION DE LIGNE

Avant de connecter cet instrument à la ligne électrique, vérifiez que la tension de la source d'alimentation correspond aux exigences de l'instrument. Consultez les spécifications propres à l'alimentation nominale correcte du dispositif.

Les plateformes alimentées en 48 CC ont une tolérance d'entrée comprise entre 36 et 72 V CC. MODIFICATIONS DES SPÉCIFICATIONS

Les spécifications sont sujettes à changement sans notice préalable.

Remarque: Cet équipement a été testé et déclaré conforme aux limites définies pour un appareil numérique de classe A, conformément au paragraphe 15B de la réglementation FCC et EN55022 Classe A, EN 55024, EN 61000-3-2; EN 61000-3-3; IEC 61000 4-2 to 4-6, IEC 61000 4-8, et IEC 61000-4-11, pour la marque de conformité de la CE. Ces limites sont fixées pour fournir une protection raisonnable contre les interférences nuisibles, lorsque l'équipement est utilisé dans un environnement commercial. Cet équipement génère, utilise et peut émettre des fréquences radio et, s'il n'est pas installé et utilisé conformément au manuel d'instructions, peut entraîner des interférences nuisibles aux communications radio. Le fonctionnement de cet équipement dans une zone résidentielle est susceptible de provoquer des interférences nuisibles, auquel cas l'utilisateur devra corriger le problème à ses propres frais.

NOTICE SPÉCIALE POUR LES UTILISATEURS NORD-AMÉRICAINS

Pour un raccordement électrique en Amérique du Nord, sélectionnez un cordon d'alimentation homologué UL et certifié CSA 3 - conducteur, [18 AWG], muni d'une prise moulée à son extrémité, de 125 V, [10 A], d'une longueur minimale de 1,5 m [six pieds] et maximale de 4,5m...Pour la connexion européenne, choisissez un cordon d'alimentation mondialement homologué et marqué "<HAR>", 3 - conducteur, câble de 0,75 mm2 minimum, de 300 V, avec une gaine en PVC isolée. La prise à l'extrémité du cordon, sera dotée d'un sceau moulé indiquant: 250 V, 3 A.

ZONE A ACCÈS RESTREINT

L'équipement alimenté en CC ne pourra être installé que dans une zone à accès restreint. CODES

D'INSTALLATION

Ce dispositif doit être installé en conformité avec les codes électriques nationaux. En Amérique du Nord, l'équipement sera installé en conformité avec le code électrique national américain, articles 110-16, 110 -17, et 110 -18 et le code électrique canadien, Section 12.

INTERCONNEXION DES UNÎTES

Les câbles de connexion à l'unité RS232 et aux interfaces Ethernet seront certifiés UL, type DP-1 ou DP-2. (Remarque- s'ils ne résident pas dans un circuit LPS).

PROTECTION CONTRE LES SURCHARGES

Un circuit de dérivation, facilement accessible, sur le dispositif de protection du courant de 15 A doit être intégré au câblage du bâtiment pour chaque puissance consommée.

BATTERIES REMPLAÇABLES

Si l'équipement est fourni avec une batterie, et qu'elle est remplacée par un type de batterie incorrect, elle est susceptible d'exploser. C'est le cas pour certaines batteries au lithium, les éléments suivants sont donc applicables:

- Si la batterie est placée dans une zone d'accès opérateur, une marque est indiquée sur la batterie ou une remarque est insérée, aussi bien dans les instructions d'exploitation que d'entretien.
- Si la batterie est placée ailleurs dans l'équipement, une marque est indiquée sur la batterie ou une remarque est insérée dans les instructions d'entretien.

Cette marque ou remarque inclut l'avertissement textuel suivant:

AVERTISSEMENT

RISQUE D'EXPLOSION SI LA BATTERIE EST REMPLACÉE PAR UN MODÈLE INCORRECT. METTRE AU REBUT LES BATTERIES CONFORMÉMENT AUX INSTRUCTIONS.

Attention - Pour réduire les risques de chocs électriques et d'incendie

1. Cet équipement est conçu pour permettre la connexion entre le conducteur de mise à la terre du circuit électrique CC et l'équipement de mise à la terre. Voir les instructions d'installation.
2. Tout entretien sera entrepris par du personnel qualifié. Aucune pièce à l'intérieur de l'unité ne peut être remplacée ou réparée.
3. NE branchez pas, n'allumez pas ou n'essayez pas d'utiliser une unité manifestement endommagée.
4. Vérifiez que l'orifice de ventilation du châssis dans l'unité n'est PAS OBSTRUE.
5. Remplacez le fusible endommagé par un modèle similaire de même puissance, tel qu'indiqué sur l'étiquette de sécurité adjacente à l'arrivée électrique hébergeant le fusible.
6. Ne faites pas fonctionner l'appareil dans un endroit, où la température ambiante dépasse la valeur maximale autorisée. 40°C/104°F.
7. Débranchez le cordon électrique de la prise murale AVANT d'essayer de retirer et/ou de vérifier le fusible d'alimentation principal.

PRODUIT LASER DE CLASSE 1 ET RÉFÉRENCE AUX NORMES LASER LES PLUS RÉCENTES: IEC 60

825-1: 1993 + A1: 1997 + A2: 2001 ET EN 60825-1: 1994+A1: 1996+ A2: 2001

Unités à CA pour le Danemark, la Finlande, la Norvège, la Suède (indiqué sur le produit):

- Danemark - Unité de classe 1 - qui doit être utilisée avec un cordon CA compatible avec les déviations du Danemark. Le cordon inclut un conducteur de mise à la terre. L'unité sera branchée à une prise murale, mise à la terre. Les prises non-mises à la terre ne seront pas utilisées!
- Finlande (Étiquette et inscription dans le manuel) - Laite on liitettävä suojamaadoituskoskettimilla varustettuun pistorasiaan
- Norvège (Étiquette et inscription dans le manuel) - Apparatet må tilkoples jordet stikkontakt
- L'unité peut être connectée à un système électrique IT (en Norvège uniquement).
- Suède (Étiquette et inscription dans le manuel) - Apparaten skall anslutas till jordat uttag.

Pour brancher à l'alimentation électrique:

1. Branchez le câble d'alimentation à la prise principale, située sur le panneau arrière de l'unité.
2. Connectez le câble d'alimentation à la prise CA mise à la terre.

AVERTISSEMENT

Risque de choc électrique et danger énergétique. La déconnexion d'une source d'alimentation électrique ne débranche qu'un seul module électrique. Pour isoler complètement l'unité, débranchez toutes les sources d'alimentation électrique.

ATTENTION

Risque de choc et de danger électriques. Le débranchement d'une seule alimentation stabilisée ne débranche qu'un module "Alimentation Stabilisée". Pour Isoler complètement le module en cause, il faut débrancher toutes les alimentations stabilisées.

Attention: Pour Réduire Les Risques d'Électrocution et d'Incendie

1. Toutes les opérations d'entretien seront effectuées UNIQUEMENT par du personnel d'entretien qualifié. Aucun composant ne peut être entretenu ou remplacée par l'utilisateur.
2. NE PAS connecter, mettre sous tension ou essayer d'utiliser une unité visiblement défectueuse.
3. Assurez-vous que les ouvertures de ventilation du châssis NE SONT PAS OBSTRUÉES.
4. Remplacez un fusible qui a sauté SEULEMENT par un fusible du même type et de même capacité, comme indiqué sur l'étiquette de sécurité proche de l'entrée de l'alimentation qui contient le fusible.
5. NE PAS UTILISER l'équipement dans des locaux dont la température maximale dépasse 40 degrés Centigrades.
6. Assurez vous que le cordon d'alimentation a été déconnecté AVANT d'essayer de l'enlever et/ou vérifier le fusible de l'alimentation générale.

Sicherheitsanweisungen

VORSICHT

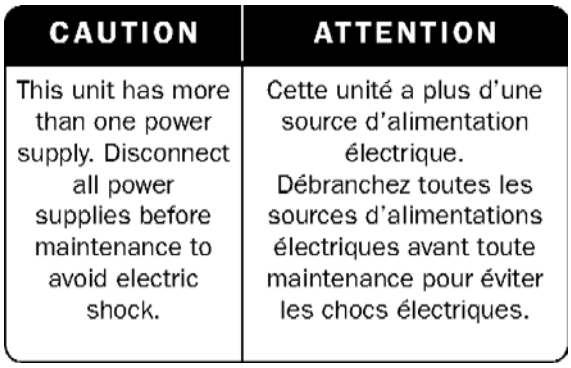
Die Elektroinstallation des Gebäudes muss ein unverzüglich zugängliches Stromunterbrechungsgerät integrieren.

Aufgrund des Stromschlagrisikos und der Energie-, mechanische und Feuergefahr dürfen Vorgänge, in deren Verlauf Abdeckungen entfernt oder Elemente ausgetauscht werden, ausschließlich von qualifiziertem Servicepersonal durchgeführt werden.

Zur Reduzierung der Feuer- und Stromschlaggefahr muss das Gerät vor der Entfernung der Abdeckung oder der Paneele von der Stromversorgung getrennt werden.

Folgende Abbildung zeigt das VORSICHT-Etikett, das auf die Radware-Plattformen mit Doppelspeisung angebracht ist.

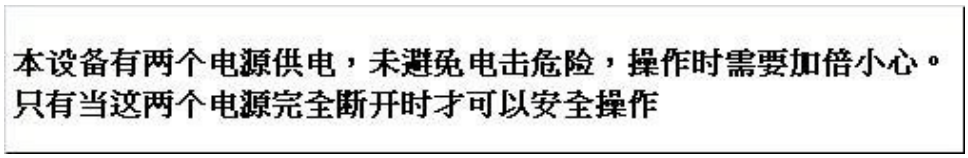
Figure 5: Warnetikett Stromschlaggefahr



SICHERHEITSHINWEIS IN CHINESISCHER SPRACHE FÜR SYSTEME MIT DOPPELSPEISUNG

Die folgende Abbildung ist die Warnung für Radware-Plattformen mit Doppelspeisung.

Figure 6: Sicherheitshinweis in chinesischer Sprache für Systeme mit Doppelspeisung



Übersetzung von Sicherheitshinweis in chinesischer Sprache für Systeme mit Doppelspeisung:

Die Einheit verfügt über mehr als eine Stromversorgungsquelle. Ziehen Sie zur Verhinderung von Stromschlag vor Wartungsarbeiten sämtliche Stromversorgungsleitungen ab.

WARTUNG

Führen Sie keinerlei Wartungsarbeiten aus, die nicht in der Betriebsanleitung angeführt sind, es sei denn, Sie sind dafür qualifiziert. Es gibt innerhalb des Gerätes keine wartungsfähigen Teile.

HOCHSPANNUNG

Jegliche Einstellungs-, Instandhaltungs- und Reparaturarbeiten am geöffneten Gerät unter Spannung müssen so weit wie möglich vermieden werden. Sind sie nicht vermeidbar, dürfen sie ausschließlich von qualifizierten Personen ausgeführt werden, die sich der Gefahr bewusst sind.

Innerhalb des Gerätes befindliche Kondensatoren können auch dann noch Ladung enthalten, wenn das Gerät von der Stromversorgung abgeschnitten wurde.

ERDUNG

Bevor das Gerät an die Stromversorgung angeschlossen wird, müssen die Schrauben der Erdungsleitung des Gerätes an die Erdung der Gebäudeverkabelung angeschlossen werden.

LASER

Dieses Gerät ist ein Laser-Produkt der Klasse 1 in Übereinstimmung mit IEC60825 - 1: 1993 + A1:1997 + A2:2001 Standard.

SICHERUNGEN

Vergewissern Sie sich, dass nur Sicherungen mit der erforderlichen Stromstärke und der angeführten Art verwendet werden. Die Verwendung reparierter Sicherungen sowie die Kurzschließung von Sicherungsfassungen muss vermieden werden. In Fällen, in denen wahrscheinlich ist, dass der von den Sicherungen gebotene Schutz beeinträchtigt ist, muss das Gerät abgeschaltet und gegen unbeabsichtigten Betrieb gesichert werden.

LEITUNGSSPANNUNG

Vor Anschluss dieses Gerätes an die Stromversorgung ist zu gewährleisten, dass die Spannung der Stromquelle den Anforderungen des Gerätes entspricht. Beachten Sie die technischen Angaben bezüglich der korrekten elektrischen Werte des Gerätes.

Plattformen mit 48 V DC verfügen über eine Eingangstoleranz von 36-72 V DC.

ÄNDERUNGEN DER TECHNISCHEN ANGABEN

Änderungen der technischen Spezifikationen bleiben vorbehalten.

Hinweis: Dieses Gerät wurde geprüft und entspricht den Beschränkungen von digitalen Geräten der Klasse 1 gemäß Teil 15B FCC-Vorschriften und EN55022 Klasse A, EN55024; EN 61000-3-2; EN; IEC 61000 4-2 to 4-6, IEC 61000 4-8 und IEC 61000-4- 11 für Konformität mit der CE-Bezeichnung.
Diese Beschränkungen dienen dem angemessenen Schutz vor schädlichen Interferenzen bei Betrieb des Gerätes in kommerziellem Umfeld. Dieses Gerät erzeugt, verwendet und strahlt elektromagnetische Hochfrequenzstrahlung aus. Wird es nicht entsprechend den Anweisungen im Handbuch montiert und benutzt, könnte es mit dem Funkverkehr interferieren und ihn beeinträchtigen. Der Betrieb dieses Gerätes in Wohnbereichen wird höchstwahrscheinlich zu schädlichen Interferenzen führen. In einem solchen Fall wäre der Benutzer verpflichtet, diese Interferenzen auf eigene Kosten zu korrigieren.

BESONDERER HINWEIS FÜR BENUTZER IN NORDAMERIKA

Wählen Sie für den Netzstromanschluss in Nordamerika ein Stromkabel, das in der UL aufgeführt und CSA-zertifiziert ist 3 Leiter, [18 AWG], endend in einem gegossenen Stecker, für 125 V, [10 A], mit einer Mindestlänge von 1,5 m [sechs Fuß], doch nicht länger als 4,5 m. Für europäische Anschlüsse verwenden Sie ein international harmonisiertes, mit “<HAR>” markiertes Stromkabel, mit 3 Leitern von mindestens 0,75 mm2, für 300 V, mit PVC-Umkleidung. Das Kabel muss in einem gegossenen Stecker für 250 V, 3 A enden.

BEREICH MIT EINGESCHRÄNKTEM ZUGANG

Das mit Gleichstrom betriebene Gerät darf nur in einem Bereich mit eingeschränktem Zugang montiert werden.

INSTALLATIONSCODES

Dieses Gerät muss gemäß der landesspezifischen elektrischen Codes montiert werden. In Nordamerika müssen Geräte entsprechend dem US National Electrical Code, Artikel 110 - 16, 110 - 17 und 110 - 18, sowie dem Canadian Electrical Code, Abschnitt 12, montiert werden.
VERKOPPLUNG VON GERÄTEN Kabel für die Verbindung des Gerätes mit RS232- und Ethernet- müssen UL-zertifiziert und vom Typ DP-1 oder DP-2 sein. (Anmerkung: bei Aufenthalt in einem nicht-LPS-Stromkreis)

ÜBERSTROMSCHUTZ

Ein gut zugänglicher aufgeführter Überstromschutz mit Abzweigstromkreis und 15 A Stärke muss für jede Stromeingabe in der Gebäudeverkabelung integriert sein.

AUSTAUSCHBARE BATTERIEN

Wird ein Gerät mit einer austauschbaren Batterie geliefert und für diese Batterie durch einen falschen Batterietyp ersetzt, könnte dies zu einer Explosion führen. Dies trifft zu für manche Arten von Lithiumsbatterien zu, und das folgende gilt es zu beachten:

- Wird die Batterie in einem Bereich für Bediener eingesetzt, findet sich in der Nähe der Batterie eine Markierung oder Erklärung sowohl im Betriebshandbuch als auch in der Wartungsanleitung.
- Ist die Batterie an einer anderen Stelle im Gerät eingesetzt, findet sich in der Nähe der Batterie eine Markierung oder einer Erklärung in der Wartungsanleitung.

Diese Markierung oder Erklärung enthält den folgenden Warntext: VORSICHT

EXPLOSIONSGEFAHR, FALLS BATTERIE DURCH EINEN FALSCHEN BATTERIETYP ERSETZT WIRD. GEBRAUCHTE BATTERIEN DEN ANWEISUNGEN ENTSPRECHEND ENTSORGEN.

- Denmark - “Unit is class I - mit Wechselstromkabel benutzen, dass für die Abweichungen in Dänemark eingestellt ist. Das Kabel ist mit einem Erdungsdraht versehen. Das Kabel wird in eine geerdete Wandsteckdose angeschlossen. Keine Steckdosen ohne Erdungsleitung verwenden!”
- Finland - (Markierungsetikett und im Handbuch) - Laite on liitettävä suojamaadoituskoskettimilla varustettuun pistorasiaan

- Norway - (Markierungsetikett und im Handbuch) - Apparatet må tilkoples jordet stikkontakt Ausschließlich für Anschluss an IT-Netzstromsysteme in Norwegen vorgesehen
- Sweden - (Markierungsetikett und im Handbuch) - Apparaten skall anslutas till jordat uttag.

Anschluss des Stromkabels:

1. Schließen Sie das Stromkabel an den Hauptanschluss auf der Rückseite des Gerätes an.
2. Schließen Sie das Stromkabel an den geerdeten Wechselstromanschluss an.

VORSICHT

Stromschlag- und Energiegefahr Die Trennung einer Stromquelle trennt nur ein Stromversorgungsmodul von der Stromversorgung. Um das Gerät komplett zu isolieren, muss es von der gesamten Stromversorgung getrennt werden.

Vorsicht - Zur Reduzierung der Stromschlag- und Feuergefahr

1. Dieses Gerät ist dazu ausgelegt, die Verbindung zwischen der geerdeten Leitung des Gleichstromkreises und dem Erdungsleiter des Gerätes zu ermöglichen. Siehe Montageanleitung.
2. Wartungsarbeiten jeglicher Art dürfen nur von qualifiziertem Servicepersonal ausgeführt werden. Es gibt innerhalb des Gerätes keine vom Benutzer zu wartenden Teile.
3. Versuchen Sie nicht, ein offensichtlich beschädigtes Gerät an den Stromkreis anzuschließen, einzuschalten oder zu betreiben.
4. Vergewissern Sie sich, dass sie Lüftungsöffnungen im Gehäuse des Gerätes NICHT BLOCKIERT SIND.
5. Ersetzen Sie eine durchgebrannte Sicherung ausschließlich mit dem selben Typ und von der selben Stärke, die auf dem Sicherheitsetikett angeführt sind, das sich neben dem Stromkabelanschluss, am Sicherungsgehäuse.
6. Betreiben Sie das Gerät nicht an einem Standort, an dem die Höchsttemperatur der Umgebung 40°C überschreitet.
7. Vergewissern Sie sich, das Stromkabel aus dem Wandstecker zu ziehen, BEVOR Sie die Hauptsicherung entfernen und/oder prüfen.

전자파 장애 설명

다음 설명은 영어, 프랑스어 및 독일어로 표시됩니다.

전자파 장애 설명

사양 변경

사양은 예고 없이 변경될 수 있습니다.

참고: 이 장비는 테스트를 마쳤으며, Part 15B of the FCC Rules 및 EN55022 Class A, EN 55024; EN 61000-3-2; EN 61000-3-3; IEC 61000 4-2 to 4-6, IEC 61000 4-8 and IEC 61000-4-11For CE MARK Compliance에 따라 Class A 디지털 디바이스의 제한사항을 준수하는 것으로 확인되었습니다.
이러한 제한은 장비를 상업 환경에서 작동하는 경우 유해한 간섭을 적절하게 차단할 수 있도록 설계되었습니다. 이 장비는 무선 주파수 에너지를 생성, 사용 및 방사할 수 있으며 지침 매뉴얼에 따라 설치 및 사용하지 않는 경우 무선 통신에 유해한 간섭을 생성할 수 있습니다. 가정에서 이 장비를 작동하는 경우 유해한 간섭이 발생할 가능성이 높으며, 이러한 경우 사용자는 간섭을 직접 수정해야 합니다.

VCCI 전자파 장애 설명

그림 7: Class A VCCI 인증 장비에 대한 문구

この装置は，クラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。　VCCI－A

Class A VCCI 인증 장비에 대한 문구 번역:

VCCI(Voluntary Control Council for Interference by Information Technology Equipment)의 표준을 기반으로 하는 Class A 제품입니다. 이 장비를 국내 환경에서 사용하는 경우 라디오 주파수 장애가 발생할 수 있으므로, 사용자가 정정 조치를 수행해야 할 수도 있습니다.

KCC KOREA

그림 8: KCC—방송 통신 위원회의 방송 통신 장비 인증

그림 9: 대한민국의 Class A KCC 인증 장비에 대한 문구

이 기기는 업무용(A급) 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의 지역에서 사용하는 것을 목적으로 합니다.

대한민국의 Class A KCC 인증 장비에 대한 문구 번역:

이 장비는 산업용 (Class A) 전자파 적합 장비이며 판매자나 사용자가 이 점에 유의해야 합니다. 이 장비는 가정 이외의 장소에서 사용해야 합니다.

BSMI

그림 10: Class A BSMI 인증 장비에 대한 문구

這是甲類的資訊產品，在居住的環境使用中時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

Class A BSMI 인증 장비에 대한 문구 번역:

이 제품은 주거 환경에서 사용하는 Class A 제품이며, 무선 주파수 장해가 발생할 수 있으므로 사용자가 적절한 조치를 취해야 합니다.

Déclarations sur les Interférences Électromagnétiques

MODIFICATIONS DES SPÉCIFICATIONS

Les spécifications sont sujettes à changement sans notice préalable.

Remarque: Cet équipement a été testé et déclaré conforme aux limites définies pour un appareil numérique de classe A, conformément au paragraphe 15B de la réglementation FCC et EN55022 Classe A, EN 55024, EN 61000-3-2; EN 61000-3-3; IEC 61000 4-2 to 4-6, IEC 61000 4-8, et IEC 61000-4-11, pour la marque de conformité de la CE. Ces limites sont fixées pour fournir une protection raisonnable contre les interférences nuisibles, lorsque l'équipement est utilisé dans un environnement commercial. Cet équipement génère, utilise et peut émettre des fréquences radio et, s'il n'est pas installé et utilisé conformément au manuel d'instructions, peut entraîner des interférences nuisibles aux communications radio. Le fonctionnement de cet équipement dans une zone résidentielle est susceptible de provoquer des interférences nuisibles, auquel cas l'utilisateur devra corriger le problème à ses propres frais.

DÉCLARATIONS SUR LES INTERFÉRENCES ÉLECTROMAGNÉTIQUES VCCI

Figure 11: Déclaration pour l'équipement de classe A certifié VCCI

この装置は，クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI－A

Traduction de la Déclaration pour l'équipement de classe A certifié VCCI:

Il s'agit d'un produit de classe A, basé sur la norme du Voluntary Control Council for Interference by Information Technology Equipment (VCCI). Si cet équipement est utilisé dans un environnement domestique, des perturbations radioélectriques sont susceptibles d'apparaître. Si tel est le cas, l'utilisateur sera tenu de prendre des mesures correctives.

KCC Corée

Figure 12: KCC—Certificat de la commission des communications de Corée pour les equipements de radiodiffusion et communication.

Figure 13: Déclaration pour l'équipement de classe A certifié KCC en langue coréenne

이 기기는 업무용(A급) 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의 지역에서 사용하는 것을 목적으로 합니다.

Translation de la Déclaration pour l'équipement de classe A certifié KCC en langue coréenne:

Cet équipement est un matériel (classe A) en adéquation aux ondes électromagnétiques et le vendeur ou l'utilisateur doit prendre cela en compte. Ce matériel est donc fait pour être utilisé ailleurs qu' á la maison.

BSMI

Figure 14: Déclaration pour l'équipement de classe A certifié BSMI

這是甲類的資訊產品，在居住的環境使用中時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

Translation de la Déclaration pour l'équipement de classe A certifié BSMI:

Il s'agit d'un produit de Classe A; utilisé dans un environnement résidentiel il peut provoquer des interférences, l'utilisateur devra alors prendre les mesures adéquates.

Erklärungen zu Elektromagnetischer Interferenz

ÄNDERUNGEN DER TECHNISCHEN ANGABEN

Änderungen der technischen Spezifikationen bleiben vorbehalten.

Hinweis: Dieses Gerät wurde geprüft und entspricht den Beschränkungen von digitalen Geräten der Klasse 1 gemäß Teil 15B FCC-Vorschriften und EN55022 Klasse A, EN55024; EN 61000-3-2; EN; IEC 61000 4-2 to 4-6, IEC 61000 4-8 und IEC 61000-4- 11 für Konformität mit der CE-Bezeichnung.
Diese Beschränkungen dienen dem angemessenen Schutz vor schädlichen Interferenzen bei Betrieb des Gerätes in kommerziellem Umfeld. Dieses Gerät erzeugt, verwendet und strahlt elektromagnetische Hochfrequenzstrahlung aus. Wird es nicht entsprechend den Anweisungen im Handbuch montiert und benutzt, könnte es mit dem Funkverkehr interferieren und ihn beeinträchtigen. Der Betrieb dieses Gerätes in Wohnbereichen wird höchstwahrscheinlich zu schädlichen Interferenzen führen. In einem solchen Fall wäre der Benutzer verpflichtet, diese Interferenzen auf eigene Kosten zu korrigieren.

ERKLÄRUNG DER VCCI ZU ELEKTROMAGNETISCHER INTERFERENZ

Figure 15: Erklärung zu VCCI-zertifizierten Geräten der Klasse A

この装置は，クラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 ＶＣＣＩ－Ａ

Übersetzung von Erklärung zu VCCI-zertifizierten Geräten der Klasse A:

Dies ist ein Produkt der Klasse A gemäß den Normen des Voluntary Control Council for Interference by Information Technology Equipment (VCCI). Wird dieses Gerät in einem Wohnbereich benutzt, können elektromagnetische Störungen auftreten. In einem solchen Fall wäre der Benutzer verpflichtet, korrigierend einzugreifen.

KCC KOREA

Figure 16: KCC—Korea Communications Commission Zertifikat für Rundfunk-und Nachrichtentechnik

Figure 17: Erklärung zu KCC-zertifizierten Geräten der Klasse A

이 기기는 업무용(A급) 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의 지역에서 사용하는 것을 목적으로 합니다.

Übersetzung von Erklärung zu KCC-zertifizierten Geräten der Klasse A:

Verkäufer oder Nutzer sollten davon Kenntnis nehmen, daß dieses Gerät der Klasse A für industriell elektromagnetische Wellen geeignete Geräten angehört und dass diese Geräte nicht für den heimischen Gebrauch bestimmt sind.

BSMI

Figure 18: Erklärung zu BSMI-zertifizierten Geräten der Klasse A

這是甲類的資訊產品，在居住的環境使用中時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

Übersetzung von Erklärung zu BSMI-zertifizierten Geräten der Klasse A:

Dies ist ein Class A Produkt, bei Gebrauch in einer Wohnumgebung kann es zu Funkstörungen kommen, in diesem Fall ist der Benutzer verpflichtet, angemessene Maßnahmen zu ergreifen.

Altitude and Climate Warning

This warning only applies to The People's Republic of China.

1. 对于在非热带气候条件下运行的设备而言，Tma：为制造商规范允许的最大环境温度，或者为 25°C，采用两者中的较大者。
2. 关于在海拔不超过 2000m 或者在非热带气候地区使用的设备，附加警告要求如下：

关于在海拔不超过 2000m 的地区使用的设备，必须在随时可见的位置处粘贴包含如下内容或者类似用语的警告标记、或者附件 DD 中的符号。

“只可在海拔不超过2000m的位置使用。”

关于在非热带气候地区使用的设备，必须在随时可见的位置处粘贴包含如下内容的警告标记：

附件 DD：有关新安全警告标记的说明。

DD.1 海拔警告标记

标记含义：设备的评估仅基于 2000m 以下的海拔高度，因此设备只适用于该运行条件。如果在海拔超过 2000m 的位置使用设备，可能会存在某些安全隐患。

DD.2 气候警告标记

标记含义：设备的评估仅基于温带气候条件，因此设备只适用于该运行条件。如果在热带气候地区使用设备，可能会存在某些安全隐患。

문서 표기 규칙

다음은 이 설명서에서 사용하는 규칙과 기호에 대해 설명합니다.

항목	설명	설명	Beschreibung
예	예제 시나리오	Un scénario d’exemple	Ein Beispielszenarium
주의:	장비, 소프트웨어 또는 데이터가 손상될 수 있음	Endommagement possible de l’équipement, des données ou du logiciel	Mögliche Schäden an Gerät, Software oder Daten
참고:	추가 정보	Informations complémentaires	Zusätzliche Informationen
변경 후	설명 및 지침	Références et instructions	Eine Erklärung und Anweisungen
정보:	제안사항 또는 해결 방법	Une suggestion ou solution	Ein Vorschlag oder eine Umgehung
경고:	운영자가 신체적 손상을 입을 수 있음	Blessure possible de l’opérateur	Verletzungsgefahr des Bedieners

목차

중요 공지사항 3
저작권 정보 4
표준 보증 9
보증 및 책임 제한사항 10
보안 지침 11
전자파 장애 설명 20
고도 및 기후 경고 24
문서 표기 규칙 25

1장 – 소개 33
DefensePro—개요 33
DefensePro 시스템 구성 요소 33
DefensePro for Cisco Firepower 9300 34
일반적인 구축 35
네트워크 연결성 36
관리 인터페이스—APSolute Vision 및 기타 36
DefensePro 기능 37
보안 보호 37
터널링된 트래픽 검사 38
DefensePro의 실시간 보안 보고 38
이력 보안 보고—APSolute Vision Reporter 38
DefensePro 플랫폼 및 모델 39
관련 문서 39
DefensePro 릴리스 노트 39
APSolute Vision 문서 39
APSolute Vision Reporter 문서 39

2장 – 시작하기 41
APSolute Vision에 로그인 41
로컬 사용자에 대한 비밀번호 변경 42
APSolute Vision 사용자 인터페이스 개요 42
APSolute Vision 설정 보기 43
디바이스 속성 호버 팝업 44
설정 보기—환경 설정 관점 44
설정 보기—대시보드 관점 44
설정 보기—시스템 관점 45
디바이스 창 45
컨피그레이션 관점 47
모니터링 관점 48

보안 모니터링 관점 ... 48
APSolute Vision 사이트 및 DefensePro 디바이스 ... 49
DefensePro 디바이스를 APSolute Vision에 추가 및 APSolute Vision에서 제거 ... 50
디바이스 이벤트에 등록된 APSolute Vision 서버—DefensePro ... 54
APSolute Vision에서 DefensePro 디바이스 잠금 및 잠금 해제 ... 54
APSolute Vision에서 일반 GUI 요소 사용 ... 56
테이블 항목 관리를 위한 아이콘 및 명령 ... 56
테이블 행 필터링 ... 57

3장 – 디바이스 운영 및 유지 관리 ... 59
DefensePro 디바이스에서 정책 컨피그레이션 업데이트 ... 59
DefensePro 디바이스 재부팅 또는 종료 ... 60
APSolute Vision 클라이언트에 디바이스의 로그 파일 다운로드 ... 60
기술 지원 및 컨피그레이션 파일 다운로드 ... 61
DefensePro 디바이스 컨피그레이션 관리 ... 61
DefensePro 컨피그레이션 파일 콘텐츠 ... 61
디바이스 컨피그레이션 파일 다운로드 ... 61
디바이스 컨피그레이션 복원 ... 62
DefensePro의 베이스라인 재설정 ... 63
APSolute Vision 및 디바이스 작업 일정 예약 ... 64
일정 예약 개요 ... 64
스케줄러에서 작업 구성 ... 65
작업 매개변수 ... 66
공격 설명 파일 업데이트 ... 71

4장 – DefensePro 설정 관리 ... 73
DefensePro 전역 매개변수 구성 ... 73
기본 전역 매개변수 보기 및 구성 ... 73
인증서 관리 ... 74
DefensePro 디바이스의 라이센스 업그레이드 ... 79
DefensePro에서 날짜 및 시간 설정 구성 ... 80
DefensePro 네트워킹 설정 구성 ... 81
DefensePro 네트워킹 설정의 기본 매개변수 구성 ... 81
네트워킹 설정에서 IP 인터페이스 관리 구성 ... 82
DefensePro 네트워킹 설정을 위한 DNS 구성 ... 85
DefensePro 디바이스-보안 설정 구성 ... 86
DefensePro 디바이스-보안 설정에 맞게 액세스 프로토콜 구성 ... 86
DefensePro 디바이스-보안 설정에서 SNMP 구성 ... 88
DefensePro 디바이스-보안 설정에서 디바이스 사용자 구성 ... 96
DefensePro 디바이스-보안 설정에서 고급 매개변수 구성 ... 97
포트 Ping 구성 ... 98
디바이스 관리를 위한 인증 프로토콜 구성 ... 98

DefensePro 보안-설정 설정 구성 100
DoS 실드 보호 구성 100
글로벌 동작 기반 DoS 보호 구성 102
글로벌 SYN 플러드 보호 구성 107
글로벌 패킷 이상 보호 구성 107
글로벌 DNS 플러드 보호 구성 110
DefensePro 보고-설정 설정 구성 113
DefensePro 시스템 로그 설정 구성 113
DefensePro 디바이스에서 컨피그레이션 감사 사용 115
보안 보고 설정 구성 115
DefensePro 클러스터링 설정 구성 118

5장 – 클래스 관리 121
네트워크 클래스 구성 121
상황 그룹 클래스 구성 122
애플리케이션 클래스 구성 123
MAC 주소 클래스 구성 124
SGT 클래스 구성 124

6장 – DefensePro 네트워크 보호 정책 관리 127
네트워크 보호 정책 구성 127
네트워크 보호를 위한 시그니처 보호 구성 130
DefensePro for Cisco Firepower의 시그니처 보호 131
시그니처 보호가 포함된 컨피그레이션 고려사항 131
시그니처 보호 프로필 구성 132
시그니처 보호 시그니처 구성 134
시그니처 보호 특성 구성 139
특성 유형 속성 보기 및 수정 141
네트워크 보호를 위한 BDoS 프로필 구성 142
네트워크 보호를 위한 SYN 프로필 구성 145
SYN 플러드 보호 정의 146
SYN 보호 프로필 매개변수 관리 147
네트워크 보호를 위한 DNS 플러드 보호 프로필 구성 150

7장 – DefensePro 운영 상태 모니터링 및 제어 155
일반 DefensePro 디바이스 정보 모니터링 155
DefensePro 리소스 사용률 모니터링 156
DefensePro CPU 사용률 모니터링 156
DefensePro 인증 테이블 모니터링 및 지우기 157
구성된 정책에 따른 DME 사용률 모니터링 158
DefensePro 시스템 로그 정보 모니터링 158
Cisco SGT(Security Group Tag) 모니터링 159

8장 – DefensePro 클러스터링 모니터링 **161**

9장 – DefensePro 통계 모니터링 **163**
DefensePro SNMP 통계 모니터링 **163**
DefensePro IP 통계 모니터링 **164**

10장 – DefensePro 네트워킹 모니터링 및 제어 **167**
라우팅 테이블 정보 모니터링 **167**
DefensePro ARP 테이블 정보 모니터링 **168**

11장 – 실시간 보안 모니터링 사용 **171**
위험 레벨 **171**
대시보드 사용 **172**
보안 대시보드 차트 보기 사용 **174**
보안 대시보드 테이블 보기 사용—현재 공격 테이블 **175**
공격 세부 정보 **179**
샘플링된 데이터 탭 **187**
실시간 트래픽 보고서 보기 **188**
동시 연결 통계 보기 **191**
보호 모니터링 **192**
공격 상태 정보 표시 **192**
BDoS 트래픽 모니터링 **192**
DNS 트래픽 모니터링 **195**
새로운 보안 공격 경고 **197**

12장 – DefensePro 관리 **199**
CLI(Command Line Interface) **199**
CLI 세션 시간 초과 **200**
CLI 기능 **200**
CLI 트랩 **201**
모든 CLI 사용자에게 트랩 전송 **201**
웹 서비스 **201**
API 구조 **202**
APSolute API SDK(Software Development Kit) **202**

부록 A – 사용 공간 바이패스 필드 및 값 **203**
BDoS 사용 공간 바이패스 필드 및 값 **204**
DNS 사용 공간 바이패스 필드 및 값 **210**

부록 B – 미리 정의된 기본 필터 **213**

부록 C – DefensePro 공격 보호 ID **223**

부록 D – DefensePro에서 지원되는 프로토콜 **237**

부록 E – 문제 해결 **239**

기술 지원 파일 **239**

부록 F – 용어집 **241**

Radware Ltd. End User License Agreement **247**

1장 – 소개

이 설명서에서는 DefensePro for Cisco Firepower 9300 버전 1.01 및 사용 방법에 대해 설명합니다.

별도로 명시되지 않는 한, 이 설명서에 설명된 절차는 APSolute Vision™ 버전 3.30을 사용하여 수행합니다.

이 장에서는 Radware의 DefensePro를 소개하고 DefensePro의 기본 기능과 모듈을 일반적으로 설명합니다.

이 장에는 다음 섹션이 포함되어 있습니다.

- DefensePro—개요, 33페이지
- DefensePro 시스템 구성 요소, 33페이지
- DefensePro for Cisco Firepower 9300, 34페이지
- 일반적인 구축, 35페이지
- 네트워크 연결성, 36페이지
- 관리 인터페이스—APSolute Vision 및 기타, 36페이지
- DefensePro 기능, 37페이지
- 관련 문서, 39페이지

DefensePro—개요

Radware의 수상 경력이 있는 DefensePro™는 실시간 IPS(Intrusion Prevention System) 및 DOS 보호 디바이스로서, 네트워크 리소스 및 애플리케이션 리소스 오용, 악성코드 확산, 인증 결함 및 정보 도용과 같이 기존 IPS에서 탐지할 수 없는 기존 및 신규 네트워크 기반 위협으로부터 애플리케이션 인프라를 보호하여 비즈니스 연속성을 유지합니다.

DefensePro는 사전 대응적 시그니처 업데이트를 통한 기존의 취약성 기반 공격으로부터 완전하게 보호하는 기능을 제공하므로, 웜, Trojan, bots, SSL 기반 공격 및 VoIP 공격과 같이 이미 알려진 공격을 방지합니다.

현재 시장에 출시된 정적 시그니처에 의존하는 대체 제품과 달리, DefensePro는 고유한 동작 기반의 자동으로 생성되는 실시간 시그니처를 제공하여, 네트워크와 애플리케이션 플러드, HTTP 페이지 플러드, 악성코드 전파, 웹 애플리케이션 해킹, 인증 체계를 무산시키려는 의도의 무차별 대입 공격과 같은 취약성 기반 및 제로 미닛(zero-minute) 공격이 아닌 공격을 방지합니다. 이 모든 기능은 합법적인 사용자 트래픽을 차단하지 않고 사람이 개입할 필요 없이 수행됩니다.

DefensePro 시스템 구성 요소

Radware DefensePro는 실시간으로 네트워크 위협을 탐지하고 방지하는 인라인 침입 방지 및 DoS(Denial-of-Service) 보호 시스템입니다. DefensePro는 잠재적인 공격을 확인하기 위해 들어오고 나가는 트래픽을 검사하여, 네트워크에서 원하지 않는 악성 트래픽을 제거합니다.

DefensePro 시스템에는 다음 구성 요소가 포함되어 있습니다.

- **DefensePro 디바이스**—*디바이스*라는 용어는 가상 플랫폼 및 DefensePro 제품을 나타냅니다.
- **관리 인터페이스**—APSolute Vision 및 기타.
- **웹에서의 Radware 보안 업데이트 서비스**.

DefensePro for Cisco Firepower 9300

Radware *DefensePro for Cisco Firepower 9300*은 Cisco Firepower 9300 플랫폼에서 DDoS(Distributed Denial-of-Service) 탐지 및 차단 기능을 제공하는 가상 플랫폼입니다. Firepower 9300은 Cisco의 새로운 보안 서비스 제공 방법입니다. Firepower 9300은 DDoS 보호 프로그램, IPS 및 방화벽과 같은 여러 애플리케이션을 호스트할 수 있습니다. 애플리케이션을 통해 다른 보안 플랫폼 애플리케이션 및 최종 고객에게 서비스를 제공하도록 애플리케이션이나 서비스를 연쇄적으로 연결할 수 있습니다. Firepower 9300은 다른 고객 사용 사례를 지원하기 위해 다양한 구축 시나리오에 구축할 수 있습니다.

DefensePro for Cisco Firepower 9300 플랫폼은 최대 세 개의 컴퓨팅 블레이드에서 실행할 수 있습니다. 각 컴퓨팅 블레이드는 다음 구성 요소를 호스트합니다.

- **Firepower 9300 소프트웨어 인프라 인스턴스**—다양한 API를 통해 액세스 가능한 로깅, 소프트웨어 이미지 관리 등의 일반 서비스 집합이 있는 Linux 기반 운영 환경이 포함되어 있습니다.
- **인프라에 있는 하나 이상의 보안 애플리케이션**—이러한 애플리케이션은 Cisco 또는 서드파티에서 제공할 수 있습니다. Radware의 DefensePro for Cisco Firepower 9300은 서드파티 애플리케이션입니다. DefensePro for Cisco Firepower 9300은 KVM 기반 가상 머신에서 실행됩니다. 여러 서비스(예: DefensePro for Cisco Firepower 9300, IPS 및 방화벽)가 블레이드에 공존할 수 있습니다. 서비스를 연쇄적으로 연결할 수 있습니다. 예를 들어, DefensePro for Cisco Firepower 9300을 제일 앞에 두어 DoS(Denial-of-Service) 공격으로부터 고객과 다른 애플리케이션을 보호할 수 있습니다.

Cisco Unified Manager에서 Firepower 9300의 섀시를 관리하며, Radware APSolute Vision에서는 DefensePro for Cisco Firepower 9300 애플리케이션을 관리합니다.

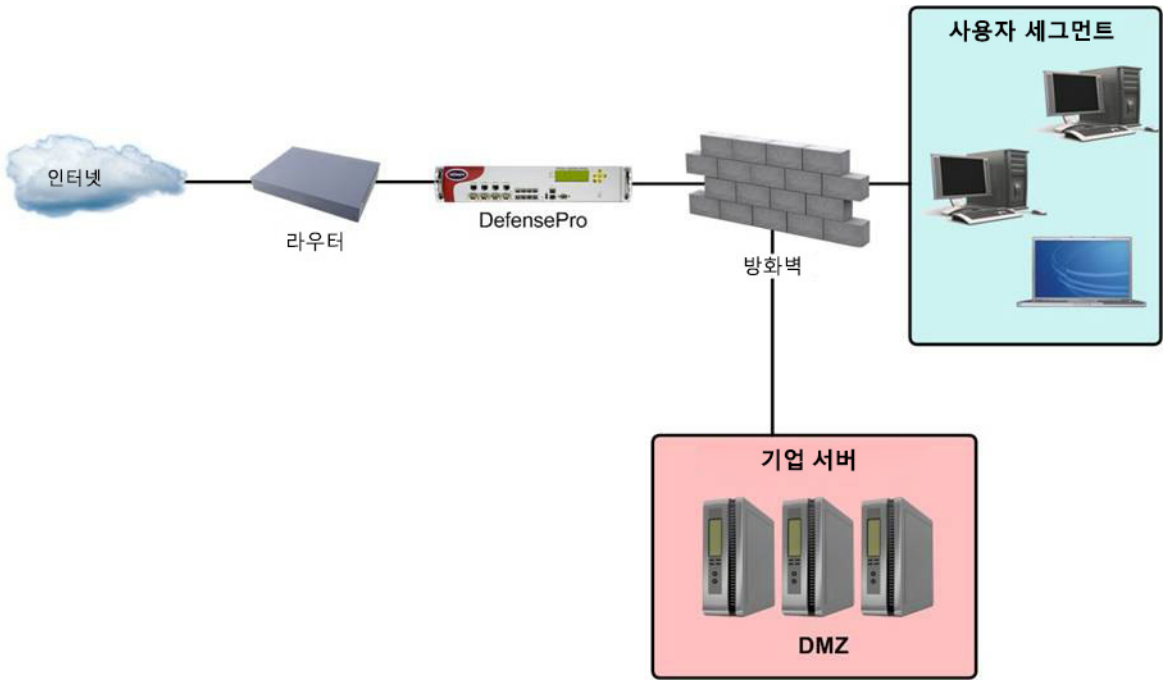
초기 시작 컨피그레이션은 DefensePro for Cisco Firepower 9300을 프로비저닝하는 XML 파일을 사용하여 수행합니다.

DefensePro for Cisco Firepower 설치, 유지관리 및 업그레이드에 대한 정보는 Cisco Technical Support에 문의하십시오.

일반적 구축

다음 그림은 엔터프라이즈에 인라인으로 설치하는 DefensePro IPS를 보여줍니다. 이 구축에서 DefensePro는 게이트웨이에 위치하며, 수신되는 네트워크 공격으로부터 호스트, 서버 및 네트워크 리소스를 보호합니다. DefensePro는 웹, 이메일, VoIP 및 기타 서비스를 목표로 하는 공격으로부터 DMZ 서버도 보호합니다. 이 Radware는 DMZ 서버 앞의 엔터프라이즈 게이트웨이에 구축되어 있습니다. 여기서 DefensePro는 엔터프라이즈 서버, 사용자, 라우터 및 방화벽의 경계를 보호합니다.

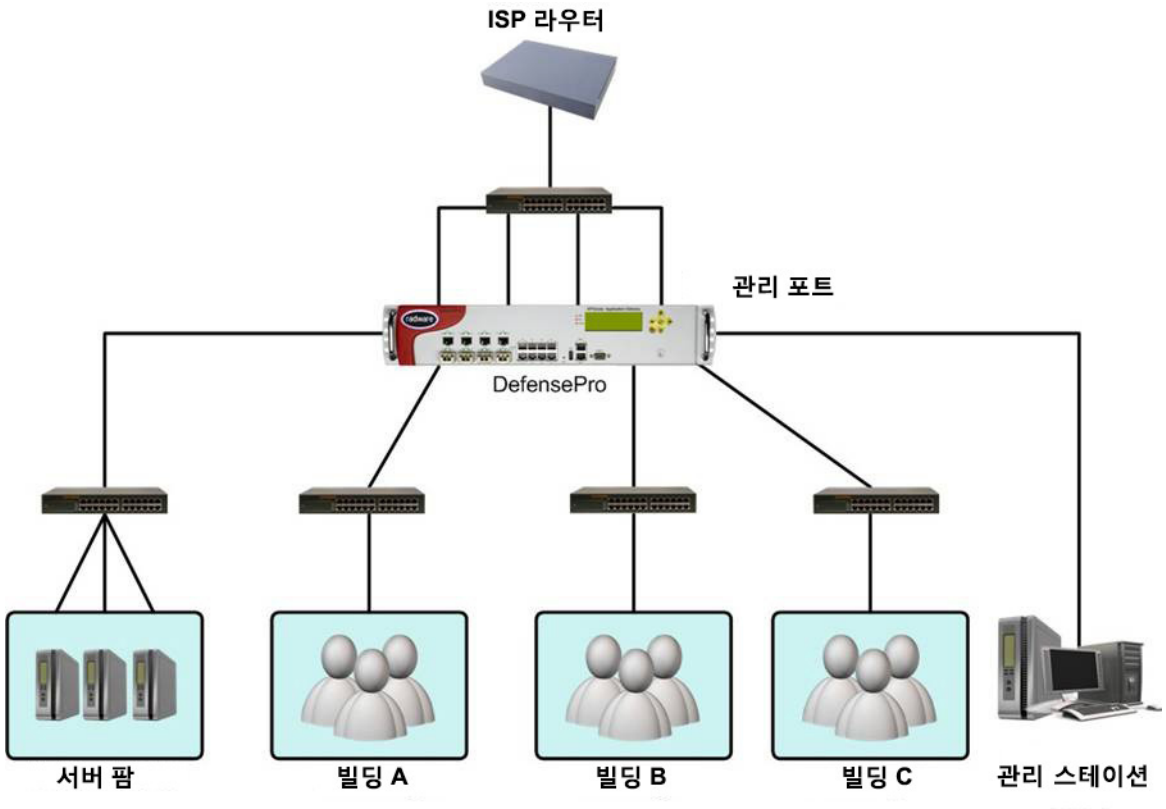
그림 19: 일반적인 DefensePro 구축



네트워크 연결성

다음 그림은 일반적인 DefensePro 네트워크 토폴로지를 보여줍니다.

그림 20: 일반적인 네트워크 연결성



관리 인터페이스—APSolute Vision 및 기타

APSolute Vision은 DefensePro의 기본 관리 인터페이스입니다.

DefensePro 디바이스의 추가적인 관리 인터페이스는 다음과 같습니다.

- WBM(Web-Based Management)
- CLI(Command Line Interface)

이러한 관리 시스템을 사용하여 대부분의 작업을 수행할 수 있습니다. 그러나 이 설명서의 대부분에서는 APSolute Vision을 사용하는 관리 작업을 설명합니다.

APSolute Vision은 단일 또는 다중 DefensePro 구축을 위해 중앙에서 보고서를 구성, 수정, 모니터링 및 생성할 수 있는 그래픽 애플리케이션입니다.

DefensePro 기능

이 절에서는 다음 주제를 포함하여 기본 DefensePro 기능을 간략하게 설명합니다.

- 보안 보호, 37페이지
- 터널링된 트래픽 검사, 38페이지
- DefensePro의 실시간 보안 보고, 38페이지
- 이력 보안 보고—APSolute Vision Reporter, 38페이지

보안 보호

참고: DefensePro 버전과 플랫폼이 DefensePro 디바이스가 지원하는 보안 정책의 유형에 영향을 미칠 수 있습니다.

조직의 보안 정책은 보안 네트워크를 구성하는 요소와 이 요소가 보안 위반에 대응하는 방식을 정의하는 규칙 및 규정 집합입니다. 글로벌 보안 설정, 네트워크 보호 정책 및 서버 보호 정책을 사용하여 조직의 보안 정책을 구현합니다. 여러 네트워크 세그먼트부터 단일 서버에 이르는 보안 요구사항을 만족하도록 보안 정책을 조정하여 조직을 포괄적으로 보호합니다.

각 정책은 여러 규칙으로 구성됩니다. 정책의 각 규칙을 통해 네트워크 세그먼트 또는 서버, 적용할 하나 이상의 보호 프로필 및 디바이스에서 공격을 탐지할 때 수행할 조치를 정의합니다.

각 보호 프로필은 특정 네트워크 위협으로부터 보호를 제공하는 보안 방어를 정의합니다. 예를 들어, 시그니처 보호 프로필은 침입 시도를 방지하고, 동작 기반 DoS 프로필은 DoS 생성을 목표로 하는 플러드 공격을 방지합니다.

참고

- 별도로 명시하지 않는 한, 이 설명서의 보안 정책 구성 절차에서는 ApSolute Vision을 사용합니다.
- 일부 보호는 관리 인터페이스에서 지원되지 않습니다.

DefensePro의 멀티 레이어 보안 방식은 광범위한 네트워크 및 서버 공격을 탐지하고 차단하는 기능을 조합합니다.

DefensePro for Cisco Firepower 9300에서는 *네트워크 측면 보호*를 제공합니다.

네트워크 측면 보호에는 다음을 포함합니다.

- **동작 기반 DoS**—SYN 플러드, TCP 플러드, UDP 플러드, ICMP 및 IGMP 플러드 등의 제로 데이 플러드 공격으로부터 보호합니다.
- **SYN 플러드 보호**—SYN 쿠키를 사용하여 모든 유형의 SYN 플러드 공격으로부터 보호합니다. 일반적으로 SYN 플러드 공격은 서버의 리소스를 사용할 의도로 특정 서버를 대상으로 삼습니다. 그러나 SYN 보호를 네트워크 보호로 구성하여 여러 네트워크 요소를 더 쉽게 보호할 수 있습니다.
- **시그니처 기반 보호**—DoS 효과를 초래하는 알려진 플러드 공격 및 플러드 공격 툴로부터 보호하는 *DoS 실드* 보호를 사용하여 보호합니다.
- **패킷 이상 보호**.

터널링된 트래픽 검사

캐리어, 통신 사업자 및 대규모 조직에서는 다양한 터널링 프로토콜을 사용하여 한 위치에서 다른 위치로 데이터를 전송합니다. 이 작업은 네트워크 요소가 터널에서 캡슐화된 데이터를 인식하지 못하도록 IP 네트워크를 사용하여 수행합니다.

터널링은 트래픽 라우팅이 소스 및 대상 IP 주소를 기반으로 함을 암시합니다. 터널링을 사용하면 IPS 디바이스 및 로드 밸런서가 알려진 오프셋의 IP 패킷에 있는 정보를 기반으로 결정을 내리고 원본 IP 패킷이 터널에 캡슐화되어 있으므로 관련 정보를 찾을 수 없습니다.

다른 터널링 프로토콜을 사용하는 캡슐화된 트래픽을 포함할 수 있는 여러 환경에 DefensePro를 설치할 수 있습니다. 일반적으로 유선 운영자는 터널링을 위해 MPLS 및 L2TP를 구축하고 모바일 운영자는 GRE 및 GTP를 구축합니다.

DefensePro 버전 1.01에서는 다양한 캡슐화 프로토콜을 사용할 수 있는 트래픽을 검사할 수 있습니다. 일부 경우, 외부 헤더(터널 데이터)는 DefensePro에서 검사해야 하는 데이터입니다. 다른 경우에는 DefensePro에서 내부 데이터(IP 헤더 및 페이로드)를 검사해야 합니다.

DefensePro 버전 1.01에서는 BDoS 보호 및 DoS 실드 보호를 위해 다음 유형의 터널링된 트래픽을 검사합니다.

- VLAN(802.1Q) 및 MPLS 트래픽

  참고: 보호 기준의 일부로 이러한 유형의 L2 터널을 검사하는 작업은 MSSP(Managed Security Service Providers)와 같은 환경에서 매우 중요합니다.
- 캡슐화된 GRE 트래픽
- 캡슐화된 L2TP 트래픽
- 캡슐화된 GTP 트래픽
- 캡슐화된 IP-in-IP 트래픽
- 캡슐화된 QinQ(802.1ad) 트래픽

DefensePro는 항상 IPsec 트래픽을 바이패스(통과)합니다.

DefensePro의 실시간 보안 보고

DefensePro 디바이스에서 APSolute Vision을 사용하면 실시간으로 공격을 보고 보안 서비스 알람을 제공받을 수 있습니다. DefensePro에서 공격을 탐지하면 보안 이벤트로 공격이 보고됩니다.

DefensePro의 보안 모니터링을 사용하면 실시간 및 과거 공격을 분석할 수 있습니다.

DefensePro에서 공격을 탐지하면 다양한 모니터링 툴을 사용하여 관찰하고 분석할 수 있는 대응 조치를 자동으로 생성합니다. DefensePro에서는 실시간 네트워크 트래픽 및 애플리케이션 동작 매개변수를 표시하는 모니터링 툴을 제공합니다. 보안 모니터링에서는 고급 통계 알고리즘을 사용하여 생성되는 일반 동작 베이스라인을 나타내는 통계 매개변수도 제공합니다.

이력 보안 보고–APSolute Vision Reporter

APSolute Vision Reporter는 다음을 제공하는 이력 보안 보고 엔진입니다.

- 맞춤형 대시보드, 보고서 및 알림
- SOC(Security Operating Centers)와 NOC(Network Operating Centers)를 위한 고급 사고 처리
- 표준 보안 보고서
- 심층 포렌식 기능
- 티켓 워크플로우 관리

DefensePro 플랫폼 및 모델

DefensePro for Cisco Firepower 9300은 KVM 가상 인프라에서 실행됩니다. 자세한 내용은 Cisco Technical Support에 문의하십시오.

관련 문서

DefensePro와 관련된 정보는 다음 문서를 참조하십시오.

- DefensePro 릴리스 노트
- APSolute Vision 문서
- APSolute Vision Reporter 문서

DefensePro 릴리스 노트

관련 DefensePro 버전에 대한 정보는 *DefensePro 릴리스 노트*를 참조하십시오.

APSolute Vision 문서

APSolute Vision 문서에는 다음이 포함됩니다.

- **APSolute Vision 설치 및 유지관리 설명서** —여기에서 다음에 대한 정보를 참조하십시오.
  - APSolute Vision 설치.
  - APSolute Vision 초기화.
- **APSolute Vision 사용 설명서**—여기에서 다음에 대한 정보를 참조하십시오.
  - APSolute Vision 기능.
  - APSolute Vision 인터페이스 탐색.
  - 사용자 관리—예를 들어, 사용자 추가 및 해당 권한 정의.
  - DefensePro 디바이스 추가 및 제거.
  - 사이트 구성—관리되는 디바이스 그룹의 물리적 또는 논리적 표시.
  - 관리되는 디바이스에 대한 관리 및 유지관리 작업(예: APSolute Vision, 디바이스 작업 일정 예약, 백업 등).
  - APSolute Vision CLI
  - APSolute Vision 모니터링—예: 버전, 서버, 데이터베이스, 디바이스 컨피그레이션 파일, APSolute Vision 운영 제어, APSolute Vision 데이터베이스 백업.
  - 감사 및 경고 관리.
- **APSolute Vision 온라인 도움말**—여기에서 관리되는 디바이스 모니터링에 대한 정보를 참조하십시오.

APSolute Vision Reporter 문서

APSolute Vision Reporter 및 사용 방법에 대한 정보는 APSolute Vision Reporter 온라인 도움말과 *APSolute Vision Reporter 사용 설명서*를 참조하십시오.

2장 – 시작하기

이 장에서는 보안 정책을 사용하여 DefensePro를 설정하고 구성하기 전에 수행할 사항에 대해 설명합니다.

DefensePro for Cisco Firepower 9300 설치, 유지관리 및 업그레이드에 대한 정보는 Cisco Technical Support에 문의하십시오.

APSolute Vision 서버의 물리적 사양 및 기본 설정과 관련된 정보와 절차는 관련 정보를 읽고 이 장에 설명된 기타 작업을 수행하기 전에 *APSolute Vision 설치 및 유지관리 설명서*의 지침을 따르십시오.

이 장에는 다음 섹션이 포함되어 있습니다.

- APSolute Vision에 로그인, 41페이지
- 로컬 사용자에 대한 비밀번호 변경, 42페이지
- APSolute Vision 사용자 인터페이스 개요, 42페이지
- APSolute Vision 사이트 및 DefensePro 디바이스, 49페이지
- DefensePro 디바이스를 APSolute Vision에 추가 및 APSolute Vision에서 제거, 50페이지
- APSolute Vision에서 DefensePro 디바이스 잠금 및 잠금 해제, 54페이지
- APSolute Vision에서 일반 GUI 요소 사용, 56페이지

APSolute Vision에 로그인

APSolute Vision에 대한 작업을 시작하려면 WBM(*Web Based Management*)이라는 APSolute Vision 웹 애플리케이션에 로그인합니다.

APSolute Vision WBM에 처음으로 로그인하려면 *APSolute Vision 활성화 라이센스*(**vision-activation** 접두사 포함)가 있어야 합니다. 라이센스는 CLI 명령 net ip get이 표시하는 APSolute Vision G1 또는 G2 포트의 MAC 주소를 기반으로 합니다. Radware Technical Support에서 라이센스를 요청할 수 있습니다. radware.com의 라이센스 생성기를 통해서도 라이센스를 사용할 수 있습니다.

최대 50명의 동시 사용자가 APSolute Vision 서버에 동시에 액세스할 수 있습니다.

APSolute Vision에서는 사용자 권한을 관리하기 위해 RBAC(Role-Based Access Control)를 지원합니다. 자격 증명 및 권한은 인증 서버나 로컬 APSolute Vision 사용자 데이터베이스를 통해 관리할 수 있습니다.

기존 사용자로 APSolute Vision에 로그인

1. 웹 브라우저에서 APSolute Vision 서버의 호스트 이름 또는 IP 주소를 입력합니다.
2. 로그인 대화 상자에서 다음을 지정합니다.
   - User Name(사용자 이름)—사용자 이름입니다.
   - Password(비밀번호)—사용자 비밀번호입니다. 서버의 컨피그레이션에 따라 비밀번호를 즉시 변경해야 할 수도 있습니다. 기본값: radware.
   -  (지구 아이콘)—APSolute Vision 그래픽 사용자 인터페이스(GUI)의 언어입니다.
3. **Login(로그인)**을 클릭합니다.

로컬 사용자에 대한 비밀번호 변경

사용자 자격 증명을 APSolute Vision *로컬 사용자* 테이블(RADIUS와 같은 인증 서버를 사용하지 않음)을 통해 관리하는 경우 로그인에서 또는 *APSolute Vision 설정* 보기 *환경 설정* 관점에서 사용자 비밀번호를 변경할 수 있습니다. 비밀번호 요구사항에 대한 정보는 APSolute Vision 비밀번호 요구사항, 99페이지를 참조하십시오.

비밀번호가 만료된 경우 *APSolute Vision Login(APSolute Vision 로그인)* 대화 상자에서 변경해야 합니다.

참고: APSolute Vision 사용자 관리에 대한 정보는 APSolute Vision 사용자 관리, 79페이지를 참조하십시오.

로컬 사용자에 대한 비밀번호를 변경하려면

1. *APSolute Vision Settings(APSolute Vision 설정)* 보기 *Preferences(환경 설정)* 관점에서 **User Preferences(사용자 환경 설정) > User Password Settings(사용자 비밀번호 설정)**를 선택합니다.
2. 매개변수를 구성하고 **Update Password(비밀번호 업데이트)**를 클릭합니다.

표 1: 사용자 비밀번호 설정 매개변수

매개변수	설명
현재 사용자 이름	(읽기 전용) 현재 사용자 이름입니다.
현재 비밀번호	현재 비밀번호입니다.
새 비밀번호	새 비밀번호입니다.
새 비밀번호 확인	새 비밀번호입니다.

APSolute Vision 사용자 인터페이스 개요

이 섹션에 포함되는 주제는 다음과 같습니다.

- APSolute Vision 설정 보기, 43페이지
- 디바이스 창, 45페이지
- 컨피그레이션 관점, 47페이지
- 모니터링 관점, 48페이지
- 보안 모니터링 관점, 48페이지

APSolute Vision 인터페이스는 기능적으로 구성된 일관된 계층 구조를 따르므로 옵션에 쉽게 액세스할 수 있습니다. 상위 기능 레벨에서 시작하여 특정 모듈, 기능 또는 개체로 드릴 다운합니다.

참고: APSolute Vision 인터페이스 요소에 대한 액세스 및 권한은 RBAC(Role-Based Access Control)에 따라 결정됩니다. 자세한 내용은 *APSolute Vision 사용 설명서*를 참조하십시오. 자세한 내용은 RBAC(Role-Based Access Control), 80페이지 및 APSolute Vision의 로컬 사용자 구성, 90페이지를 참조하십시오.

APSolute Vision 설정 보기

주 화면의  (Settings(설정)) 버튼을 클릭하여 *APSolute Vision Settings(APSolute Vision 설정)* 보기를 선택합니다.

APSolute Vision Settings(APSolute Vision 설정) 보기에는 다음 관점이 포함되어 있습니다.

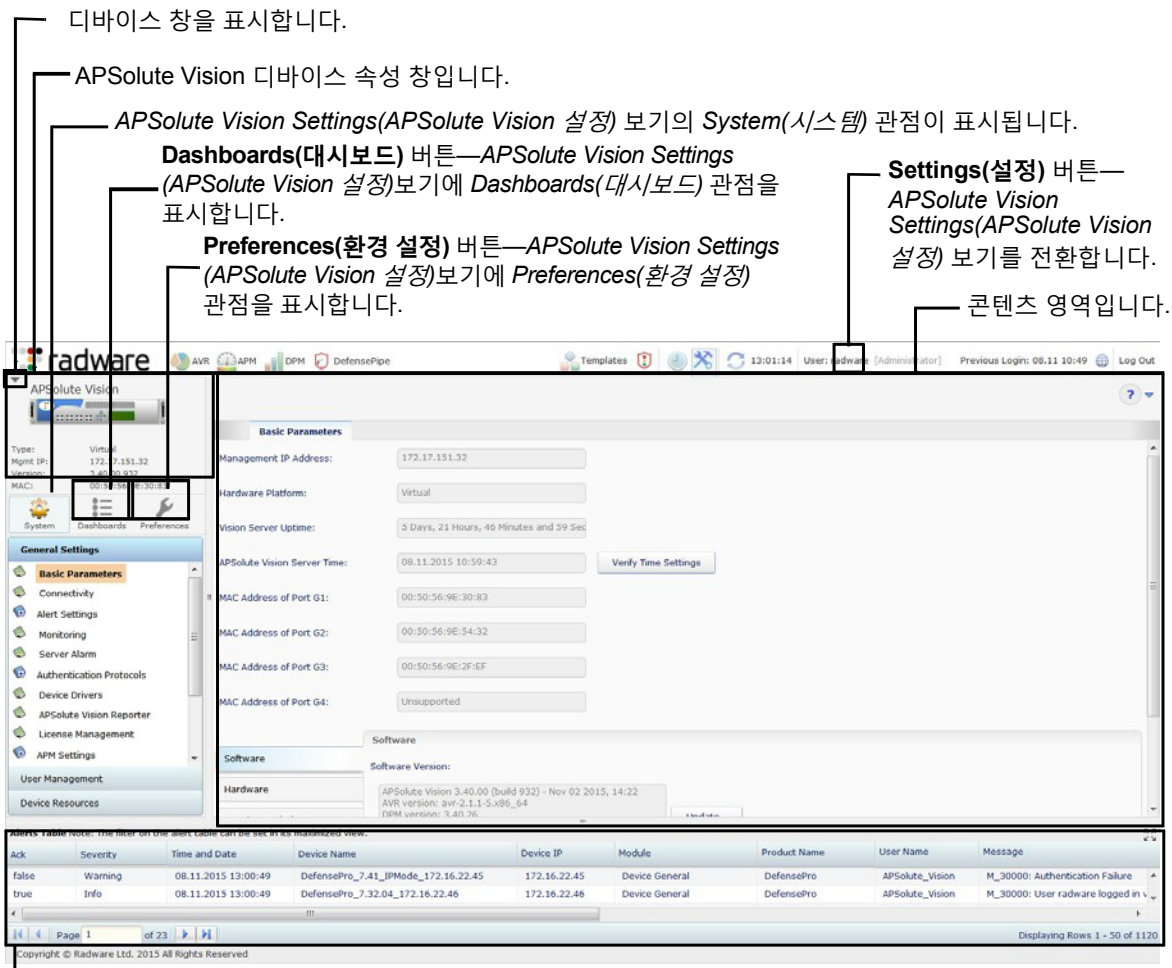
- **System(시스템)**—자세한 내용은 설정 보기—시스템 관점, 45페이지를 참조하십시오. 이 *APSolute Vision Settings(APSolute Vision 설정)* 보기 *System(시스템)* 관점에 대한 액세스는 관리자로 제한됩니다.
- **Dashboards(대시보드)**—자세한 내용은 설정 보기—대시보드 관점, 44페이지를 참조하십시오.
- **Preferences(환경 설정)**—자세한 내용은 설정 보기—환경 설정 관점, 44페이지를 참조하십시오.

필요한 관점을 표시하려면 관련 버튼(**System(시스템)**, **Dashboards(대시보드)** 또는 **Preferences(환경 설정)**)을 클릭합니다.

APSolute Vision Settings(APSolute Vision 설정) 보기의 왼쪽 위에 *APSolute Vision 디바이스 속성 창*이 표시됩니다. 자세한 내용은 APSolute Vision 디바이스 속성 창, 44페이지를 참조하십시오.

디바이스 창의 디바이스 노드 위에 마우스를 올려두면 팝업이 표시됩니다. 자세한 내용은 디바이스 속성 호버 팝업, 44페이지를 참조하십시오.

그림 21: 설정 보기(시스템 관점 표시)



APSolute Vision 디바이스 속성 창

*APSolute Vision 디바이스 속성 창*에서는 현재 선택한 디바이스를 위한 다음과 같은 매개변수를 표시합니다.

- *디바이스 유형(Alteon, AppWall, DefensePro 또는 LinkProof NG) 및 사용자 정의 디바이스 이름.*
- *디바이스 잠금 여부를 표시하는 아이콘.*
- *디바이스 전면 패널의 그림. 디바이스가 잠기면*  *버튼을 클릭하여 디바이스를 재설정하거나 종료할 수 있습니다.*
- **Status(상태)**—디바이스 일반 상태: **Up(가동)**, **Down(중단)** 또는 **Maintenance(유지관리).**
- **Locked By(잠근 사람)**—디바이스가 잠긴 경우 디바이스를 잠근 사용자.
- **Type(유형)**—플랫폼 및 폼 팩터.
- **Mngt IP(관리 IP)—**디바이스의 호스트 또는 IP 주소.
- **Version(버전)**—디바이스 버전.
- **MAC**—MAC 주소.
- **License(라이센스)**—디바이스의 라이센스.
- **Device Driver(디바이스 드라이버)**—디바이스 드라이버 이름.

디바이스 속성 호버 팝업

디바이스 창의 디바이스 노드 위에 마우스를 올려두면 팝업에 다음 매개변수가 표시됩니다.

- **Device Name(디바이스 이름)**—사용자 정의 디바이스 이름.
- **Status(상태)**—디바이스 일반 상태: **Up(가동)**, **Down(중단)** 또는 **Maintenance(유지관리).**
- **Locked By(잠근 사람)**—디바이스가 잠긴 경우 디바이스를 잠근 사용자.
- **Management IP Address(관리 IP 주소)**—디바이스의 호스트 또는 IP 주소.
- **Device Type(디바이스 유형)**—디바이스 유형(즉, **DefensePro**).
- **Version(버전)**—디바이스 버전.
- **MAC**—MAC 주소.
- **License(라이센스)**—디바이스의 라이센스.
- **Form Factor(폼 팩터)**—이 필드에는 폼 팩터가 표시됨: **Virtual(가상)**.
- **Platform(플랫폼)**—플랫폼 유형.
- **HA Status(HA 상태)**.
- **Device Driver(디바이스 드라이버)**—디바이스 드라이버 이름.

설정 보기—환경 설정 관점

Preferences(환경 설정) 관점을 사용하여 비밀번호를 변경합니다.

설정 보기—대시보드 관점

적절한 역할의 사용자가 *APSolute Vision Settings(APSolute Vision 설정)* 보기 *Dashboards(대시보드)* 관점을 사용하여 다음에 액세스할 수 있습니다.

- **애플리케이션 SLA 대시보드**—자세한 내용은 애플리케이션 SLA 대시보드 사용, 491페이지를 참조하십시오.
- **보안 제어 센터**—자세한 내용은 보안 제어 센터 사용, 495페이지를 참조하십시오.

설정 보기—시스템 관점

관리자가 *APSolute Vision Settings(APSolute Vision 설정)* 보기 *System(시스템)* 관점을 사용하여 다음을 수행할 수 있습니다.

- **APSolute Vision 서버의 일반 설정 모니터링 또는 관리**—APSolute Vision 서버의 일반 설정 모니터링 및 관리에는 다음 항목이 포함됩니다.
  - APSolute Vision 서버의 일반 속성, 세부 정보 및 통계
  - APSolute Vision 서버의 통계
  - 연결성
  - 경고 브라우저 및 보안 경고
  - 모니터링 매개변수
  - 서버 알람 임계값
  - 인증(Authentication) 프로토콜
  - 디바이스 드라이버
  - APSolute Vision Reporter for DefensePro
  - 라이센스
  - APM(Application Performance Monitoring)
  - DefensePipe URL
  - 고급 일반 매개변수
  - 표시 형식
  - 유지관리 파일
- **사용자 관리 및 모니터링**—사용자가 동시에 여러 디바이스를 차례대로 관리할 수 있습니다. APSolute Vision RBAC를 사용하면 관리자가 디바이스의 여러 액세스 제어 레벨을 사용자에게 허용할 수 있습니다. RBAC에서는 사용자 및 작업 범위(디바이스 또는 디바이스 그룹)에 따라 할당할 수 있는 사전 정의된 역할 집합을 제공합니다. RBAC 정의는 내부적으로(APSolute Vision 내부) 및 원격 인증(RADIUS 또는 TACACS+ 사용)을 통해 모두 지원됩니다.
- **디바이스 리소스 관리**—예를 들어, 디바이스 백업 파일.

참고: *APSolute Vision Settings(APSolute Vision 설정)* 보기 *System(시스템)* 관점에 노출된 대부분의 작업에 대한 자세한 내용은 APSolute Vision 시스템 관리 및 모니터링, 101페이지를 참조하십시오.

디바이스 창

적절한 역할의 사용자가 *디바이스 창*을 사용하여 APSolute Vision 서버에서 관리하는 Radware 디바이스를 추가하거나 삭제할 수 있습니다.

왼쪽 위 모서리 근처에 있는 작은 버튼을 클릭하여 디바이스 창을 표시합니다. 매니지드

디바이스를 고가용성 *클러스터* 및 *사이트*로 구성할 수 있습니다.

일반적으로 사이트는 위치, 서비스 또는 디바이스 유형과 같은 속성을 공유하는 디바이스 그룹입니다. 사이트를 중첩할 수 있습니다. 즉, 각 사이트에는 하위 사이트와 디바이스를 포함할 수 있습니다. RBAC(Role-Based Access Control)의 상황에서 사이트를 통해 관리자가 각 사용자의 범위를 정의할 수 있습니다.

디바이스 창에서 디바이스를 두 번 클릭하면 APSolute Vision에서 디바이스 속성 창과 디바이스에서 본 마지막 관점을 해당 콘텐츠 영역과 함께 표시합니다.

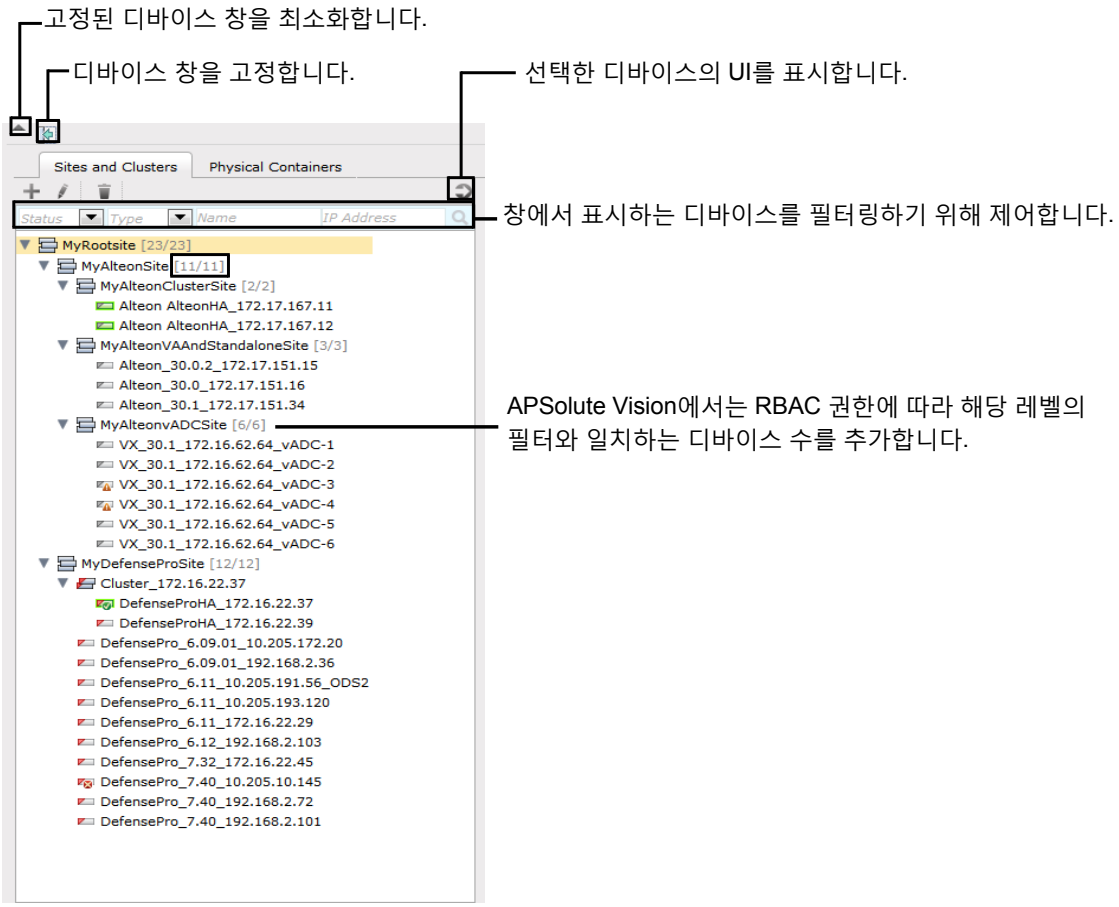
APSolute Vision에서 표시하는 사이트와 디바이스를 필터링할 수 있습니다. 필터는 트리의 모든 사이트와 디바이스에 적용됩니다. 필터에서는 트리의 콘텐츠는 변경하지 않으며, APSolute Vision에서 트리를 표시하는 방식만 변경합니다. 기본적으로 APSolute Vision에서는 볼 권한이 있는 모든 사이트와 디바이스를 표시합니다. APSolute Vision에서는 RBAC 권한에 따라 해당 레벨의 필터와 일치하는 디바이스 수를 트리의 각 노드에 추가합니다.

다음 기준에 따라 APSolute Vision에서 표시하는 사이트와 디바이스를 필터링할 수 있습니다.

- **Status(상태)—Up(가동)**, **Down(중단)**, **Maintenance(유지관리)** 또는 **Unknown(알 수 없음)**.
- **Type(유형)—Alteon**, **AppWall**, **DefensePro** 또는 **LinkProof NG**. *Physical Containers(물리적 컨테이너)* 탭에는 이 필드가 표시되지 않습니다.
- **Name(이름)**—디바이스의 이름, 사이트 또는 이름에 포함된 문자열(예: **aRy** 값은**Primary1** 및 **SecondaryABC**라는 요소와 일치).
- **IP Address(IP 주소)**—IP 주소, IP 범위 또는 IP 마스크.

필터 기준을 구성한 다음 필터를 적용하려면  버튼을 클릭하여 필터를 적용합니다.  버튼을 클릭하여 필터를 취소합니다.

그림 22: 디바이스 창(고정되지 않음)



컨피그레이션 관점

Configuration(컨피그레이션) 관점을 사용하여 Radware 디바이스를 구성합니다. 디바이스 창에서 구성할 디바이스를 선택합니다.

콘텐츠 영역에서 디바이스 컨피그레이션을 보고 수정할 수 있습니다.

다음 사항이 *Configuration(컨피그레이션)* 관점의 모든 컨피그레이션 작업에 적용됩니다.

- 디바이스를 구성하려면 잠가야 합니다. 자세한 내용은 APSolute Vision 문서를 참조하십시오.
- 필드 값을 변경할 때(및 **Submit(제출)** 조치를 보류 중인 컨피그레이션이 있는 경우) 탭 제목이 기울임꼴로 변경되며 별표(*)가 포함됩니다.
- 기본적으로 테이블에는 테이블 페이지당 최대 20행이 표시됩니다.
- 테이블 항목에서 다음 작업 중 하나 이상을 수행할 수 있습니다.
  - 테이블에 새 항목을 추가하고 해당 매개변수를 정의합니다.
  - 기존 테이블 항목의 매개변수를 하나 이상 편집합니다.
  - 테이블 항목 삭제
  - 디바이스 컨피그레이션 정보는 APSolute Vision 데이터베이스가 아니라 매니지드 디바이스에만 저장됩니다.

디바이스에 정보를 확정하려면 컨피그레이션 대화 상자나 컨피그레이션 페이지에서 설정을 수정할 때 **Submit(제출)**을 클릭해야 합니다.

일부 컨피그레이션을 변경하려면 즉시 디바이스를 재부팅해야 합니다. 컨피그레이션 변경을 제출하면 디바이스가 즉시 재부팅됩니다.

일부 컨피그레이션 변경이 적용되려면 디바이스를 재부팅해야 하지만, 즉시 재부팅하지 않고 변경사항을 저장할 수 있습니다. 재부팅하지 않고 변경사항을 제출하면 디바이스를 재부팅할 때까지 *Properties(속성)* 창에 “Reboot Required(재부팅 필요)” 알림이 표시됩니다.

필요한 경우 **Update Policies(정책 업데이트)**를 클릭하여 정책 컨피그레이션 변경사항을 구현합니다. 디바이스의 정책 컨피그레이션 변경사항은 DefensePro 디바이스에 저장되지만, 디바이스 컨피그레이션 업데이트를 수행할 때까지 디바이스가 변경사항을 적용하지 않습니다. 새 컨피그레이션에 정책 업데이트 작업이 적용되어야 하는 경우 주황색 배경의 버튼이 표시됩니다.

그림 23: Update Policies(정책 업데이트) 버튼

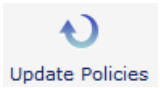


그림 24: Update Policies Required(정책 업데이트 필요) 버튼

Configuration(컨피그레이션) 관점의 디바이스 선택 예

다음 예에서는 Radware 디바이스의 컨피그레이션 매개변수를 보거나 변경하기 위해 선택할 사항을 표시합니다.

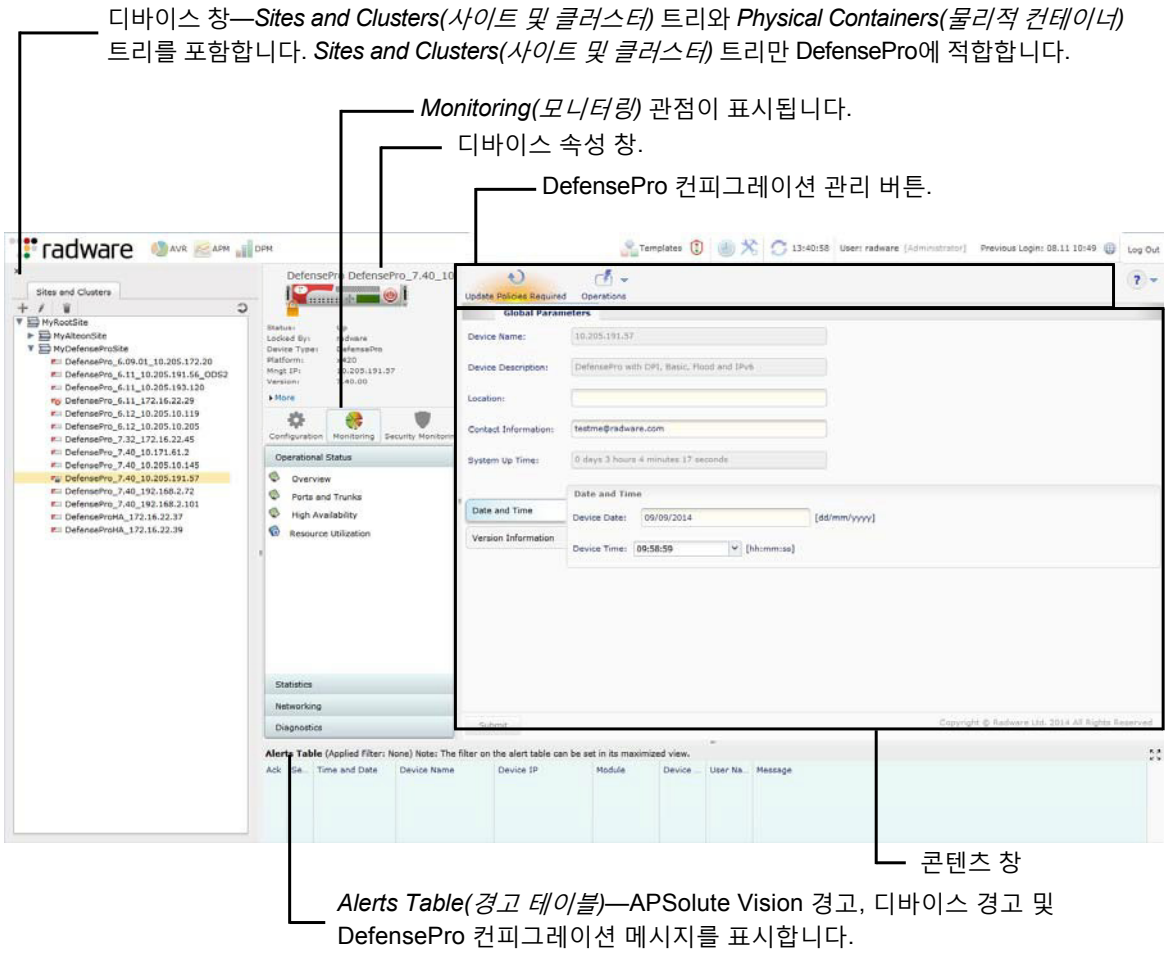
1. 사이트와 하위 사이트를 드릴 다운하여 디바이스 창에서 필수 디바이스를 선택합니다.
2. 디바이스 속성 창에서 아이콘을 클릭하여 디바이스를 잠급니다. 아이콘이 (잠긴 자물쇠 그림)으로 변경됩니다.

3.  을 클릭하여 *Configuration(컨피그레이션)* 관점을 엽니다.
4. 콘텐츠 창에서 컨피그레이션 개체로 이동합니다.

모니터링 관점

Monitoring(모니터링) 관점에서 물리적 디바이스와 인터페이스 및 논리적 개체를 모니터링할 수 있습니다.

그림 25: 모니터링 관점— DefensePro



보안 모니터링 관점

DefensePro 및 DefenseFlow의 경우 APSolute Vision에서 *Security Monitoring(보안 모니터링)* 관점을 표시합니다.

Security Monitoring(보안 모니터링) 관점은 단일 디바이스뿐 아니라 다중 디바이스에도 사용할 수 있습니다. 다중 디바이스에 대한 보안 모니터링에서는 두 개의 보고 카테고리, 즉 *대시보드 보기 및 트래픽 모니터링*을 지원합니다. 단일 디바이스에 대한 보안 모니터링에서는 두 개의 추가 보고 카테고리인 *보호 모니터링* 및 *HTTP 보고서*를 지원합니다.

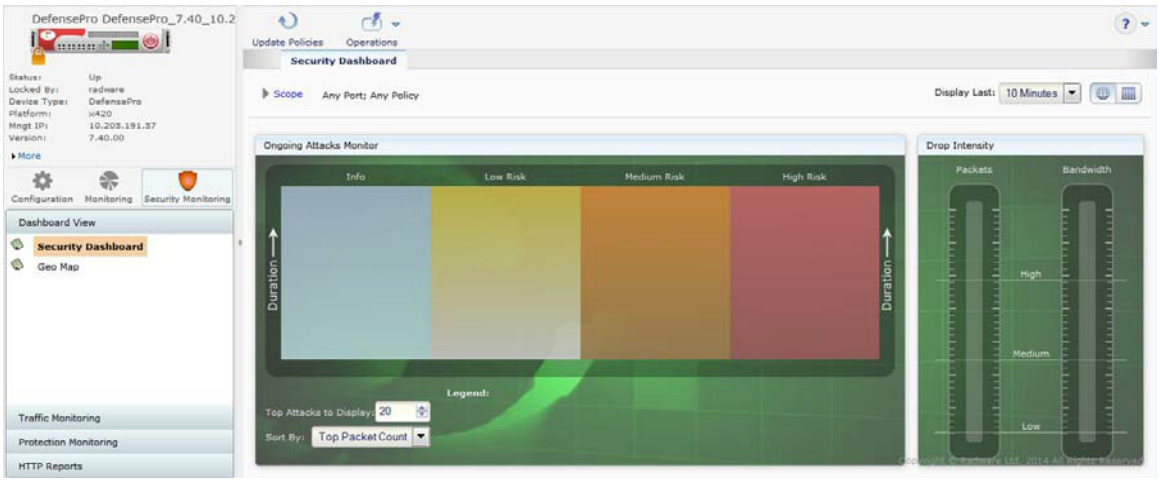
APSolute Vision에서 표시하는 사이트와 디바이스를 필터링할 수 있습니다. 필터에서는 트리의 콘텐츠는 변경하지 않으며, APSolute Vision에서 트리를 표시하는 방식만 변경합니다.

Security Monitoring(보안 모니터링) 관점에서, DefensePro 디바이스를 통해 탐지한 현재 공격과 관련된 가시성을 제공하는 실시간 보안 모니터링 툴 컬렉션에 액세스할 수 있습니다. *Properties(속성)* 창에 현재 선택한 디바이스에 대한 정보가 표시됩니다.

Security Monitoring(보안 모니터링) 관점에는 다음 탭이 포함됩니다.

- **Dashboard View(대시보드 보기)**—다음으로 구성됩니다.
  - **Security Dashboard(보안 대시보드)**—네트워크에서 현재 활성인 모든 공격을 요약하여 그래픽으로 표시하며, 색상 분류된 공격 카테고리 식별, 그래픽 위협 레벨 표시 및 공격 세부 정보에 대한 즉각적인 드릴 다운 기능이 포함되어 있습니다.
  - **Current Attacks(현재 공격)**—테이블 형식으로 현재 공격을 표시하며, 공격 카테고리 그래픽 표시, 위협 레벨 표시, 공격 세부 정보 드릴 다운 및 즉각적인 미세 조정을 위한 보호 정책에 손쉽게 액세스하는 기능이 포함되어 있습니다.
- **Traffic Monitoring(트래픽 모니터링)**—네트워크 정보를 표시하는 실시간 그래프 및 테이블이며, 지정된 트래픽 방향 및 프로토콜에 따라 필터링된 공격 트래픽 및 합법적 트래픽이 포함되어 있습니다.
- **Protection Monitoring(보호 모니터링)**—정책에 대한 통계, 지정된 트래픽 방향 및 프로토콜에 따른 보호와 함께 학습된 트래픽 베이스라인을 포함하는 실시간 그래프 및 테이블입니다.
- **HTTP Reports(HTTP 보고서)**—정책에 대한 통계, 지정된 트래픽 방향 및 프로토콜에 따른 보호와 함께 학습된 트래픽 베이스라인을 포함하는 실시간 그래프 및 테이블입니다.

그림 26: 보안 모니터링 관점—보안 대시보드 표시



참고: *Security Monitoring(보안 모니터링)* 관점에 대한 자세한 내용은 실시간 보안 모니터링 사용, 171페이지를 참조하십시오.

APSolute Vision 사이트 및 DefensePro 디바이스

APSolute Vision의 사이트는 매니지드 DefensePro 디바이스와 같은 매니지드 디바이스 그룹의 물리적 또는 논리적 표시입니다. 사이트는 영역 위치, 관리 기능, 디바이스 유형 등을 기반으로 할 수 있습니다. 각 사이트에는 중첩 사이트와 디바이스를 포함할 수 있습니다.

APSolute Vision을 통해 DefensePro 디바이스 및 보안 정책을 구성하려면 먼저 DefensePro 디바이스가 APSolute Vision 서버에 있고 여기에 연결되어 있어야 합니다. *사이트* 및 DefensePro 디바이스는 *System(시스템)* 탭에 표시됩니다.

적절한 권한이 있는 사용자만 사이트와 DefensePro 디바이스를 APSolute Vision 서버에 추가할 수 있습니다.

APSolute Vision 사이트에 대한 자세한 내용은 *APSolute Vision 사용 설명서*를 참조하십시오.

DefensePro 디바이스를 APSolute Vision에 추가 및 APSolute Vision에서 제거

APSolute Vision에서 Radware 디바이스를 관리하려면 먼저 디바이스 창의 적절한 사이트 트리에 디바이스를 추가해야 합니다.

디바이스를 추가할 때 디바이스의 이름을 정의할 수 있습니다. 디바이스와 APSolute Vision 서버 간의 통신을 위한 인증 매개변수(자격 증명)를 비롯한 디바이스 연결 정보도 제공합니다.

디바이스 연결 정보를 제출하고 나면 APSolute Vision 서버에서 디바이스에 연결할 수 있는지 검증합니다. 그런 다음 APSolute Vision에서 디바이스 정보와 라이센싱 정보를 검색하여 저장합니다.

연결이 설정되고 나면 일부 연결 정보를 수정하고 디바이스를 구성할 수 있습니다.

디바이스를 추가하거나 디바이스 속성을 수정할 때 APSolute Vision 서버가 디바이스 이벤트의 대상으로 자신을 구성하는지 여부와 APSolute Vision 서버가 디바이스에서 자신의 고유 주소를 제외한 디바이스 이벤트의 모든 수신자를 제거하는지 여부를 지정할 수 있습니다.

디바이스를 추가한 후 기본 디바이스와 백업 디바이스 또는 1차 디바이스와 2차 디바이스(*디바이스 유형*에 따라 다름)의 클러스터를 생성할 수 있습니다.

- 디바이스는 사이트와 같은 이름을 사용할 수 없습니다.
- 여러 사이트의 디바이스가 같은 이름을 사용할 수 없습니다.
- 디바이스의 이름을 변경하려면 먼저 사이트 트리에서 디바이스를 삭제한 다음 필요한 대상 사이트에 추가해야 합니다.
- 사이트 간에 디바이스를 이동하려면 먼저 사이트 트리에서 디바이스를 삭제한 다음 필요한 대상 사이트에 추가해야 합니다.
- 디바이스를 동일한 관리 IP 주소를 할당할 새 디바이스로 바꾸려면 사이트에서 디바이스를 삭제한 다음 교체할 디바이스를 다시 생성해야 합니다.
- 디바이스를 삭제하면 해당 디바이스의 이력 보고서를 더 이상 볼 수 없습니다.
- 디바이스를 삭제하면 디바이스 알람 및 보안 모니터링 정보도 제거됩니다.
- HTTP 및 HTTPS는 컨피그레이션 파일, 인증서 및 키 파일(HTTPS만 해당), 공격 시그니처 파일, 디바이스 소프트웨어 파일 등의 다양한 파일을 매니지드 디바이스에서 다운로드하거나 매니지드 디바이스에 업로드하는 데 사용됩니다.

새 DefensePro 디바이스를 추가하려면

1. 디바이스 창 *Sites and Clusters(사이트 및 클러스터)* 트리에서 디바이스를 추가할 사이트 이름으로 이동하여 선택합니다.
2. 탭 툴바에서  (Add(추가)) 버튼을 클릭합니다.
3. **Type(유형)** 드롭다운 목록에서 필요에 따라 **DefensePro**를 선택합니다.
4. 매개변수를 구성하고 **Submit(제출)**을 클릭합니다.

   APSolute Vision이 디바이스에 연결되면 콘텐츠 창에 기본 디바이스 정보가 표시되고 디바이스 속성 정보가 디바이스 속성 창에 표시됩니다.

표 2: 디바이스 속성: 일반 매개변수

매개변수	설명
유형	디바이스 또는 사이트의 유형입니다. 이 경우, DefensePro를 선택합니다.
이름	디바이스의 이름입니다. 기본값을 변경할 수 있습니다. **참고:** APSolute Vision 컨피그레이션에 디바이스를 추가하면 해당 이름을 변경할 수 없습니다.

표 3: 디바이스 속성: SNMP 매개변수

매개변수	설명
관리 IP	매니지드 디바이스에 정의된 관리 IP 주소입니다. **참고:** APSolute Vision 컨피그레이션에 디바이스를 추가하면 해당 IP 주소를 변경할 수 없습니다.
SNMP 버전	연결에 사용한 SNMP 버전입니다.
SNMP 읽기 커뮤니티 (이 매개변수는 **SNMP 버전**이 **SNMPv1** 또는 **SNMPv2**인 경우에만 표시됩니다.)	SNMP 읽기 커뮤니티 이름입니다.
SNMP 쓰기 커뮤니티 (이 매개변수는 **SNMP 버전**이 **SNMPv1** 또는 **SNMPv2**인 경우에만 표시됩니다.)	SNMP 쓰기 커뮤니티 이름입니다.
사용자 이름 (이 매개변수는 **SNMP 버전**이 **SNMPv1** 또는 **SNMPv3**인 경우에만 표시됩니다.)	SNMP 연결에 사용하는 사용자 이름입니다. 최대 문자 수: 18
인증 사용 (이 매개변수는 **SNMP 버전**이 **SNMPv1** 또는 **SNMPv3**인 경우에만 표시됩니다.)	디바이스에서 성공적인 연결을 위해 사용자를 인증할 것인지 지정합니다. 기본값: Disabled(사용 안 함)
인증 프로토콜 (이 매개변수는 **Use Authentication(인증 사용)** 확인란이 선택된 경우에만 표시됩니다.)	인증에 사용된 프로토콜입니다. 값: MD5, SHA 기본값: MD5
인증 비밀번호 (이 매개변수는 **Use Authentication(인증 사용)** 확인란이 선택된 경우에만 표시됩니다.)	인증에 사용되는 비밀번호입니다.

표 3: 디바이스 속성: SNMP 매개변수(계속)

매개변수	설명
개인정보 사용 (이 매개변수는 **Use Authentication(인증 사용)** 확인란이 선택된 경우에만 표시됩니다.)	디바이스에서 보안을 강화하기 위해 SNMPv3 트래픽을 암호화할 것인지 지정합니다. 기본값: Disabled(사용 안 함)
개인정보 비밀번호 (이 매개변수는 **Use Privacy(개인정보 사용)** 확인란이 선택된 경우에만 표시됩니다.)	개인정보 기능에 사용되는 비밀번호입니다.

표 4: 디바이스 속성: HTTP/S 액세스 매개변수

매개변수	설명
HTTP 액세스 검증	APSolute Vision에서 매니지드 디바이스에 대한 HTTP 액세스를 검증할 것인지 지정합니다. 기본값: Enabled(사용) **참고:** 이 옵션은 Alteon에 사용되지 않습니다.
HTTPS 액세스 검증	APSolute Vision에서 매니지드 디바이스에 대한 HTTPS 액세스를 검증할 것인지 지정합니다. 기본값: Enabled(사용)
사용자 이름	HTTP 및 HTTPS 통신에 사용하는 사용자 이름입니다. 기본값: admin(관리자) 최대 문자 수: 18
비밀번호	HTTP 및 HTTPS 통신에 사용되는 비밀번호입니다. 기본값: admin(관리자)
HTTP 포트	디바이스와 HTTP 통신에 사용하는 포트입니다. 기본값: 80
HTTPS 포트	디바이스와 HTTPS 통신에 사용하는 포트입니다. 기본값: 443

표 5: 디바이스 속성: 이벤트 알림 매개변수

매개변수	설명
이 APSolute Vision 서버를 디바이스 이벤트에 등록	APSolute Vision 서버가 디바이스 이벤트의 대상으로 자신을 구성할 것인지 지정합니다. 값: ● Enabled(사용)—APSolute Vision 서버에서 디바이스 이벤트(예: 트랩, 경고, IRP 메시지 및 패킷 보고 데이터) 대상으로 자신을 구성합니다. ● Disabled(사용 안 함)—*새 디바이스의 경우* APSolute Vision 서버가 이벤트 대상으로 자신을 등록하지 않고 디바이스를 추가합니다. *기존 디바이스의 경우* APSolute Vision 서버가 디바이스 이벤트의 대상으로 자신을 제거합니다. 기본값: Enabled(사용) **참고:** 사용자가 대화 상자에서 **Submit(제출)**을 클릭할 때마다 APSolute Vision에서 이 조치가 실행됩니다.
APSolute Vision 서버 IP 등록 (이 매개변수는 **Register This APSolute Vision Server for Device Events(이 APSolute Vision 서버를 디바이스 이벤트에 등록)** 확인란을 선택한 경우에만 사용할 수 있습니다.)	매니지드 디바이스에서 이벤트를 보낼 APSolute Vision 서버의 IP 주소 및 포트입니다.
디바이스 이벤트의 기타 모든 대상 제거 (이 매개변수는 **Register This APSolute Vision Server for Device Events(이 APSolute Vision 서버를 디바이스 이벤트에 등록)** 확인란을 선택한 경우에만 사용할 수 있습니다.)	APSolute Vision 서버에서 고유 주소를 제외하고 디바이스 이벤트(예: 트랩 및 IRP 메시지)의 모든 수신자를 디바이스에서 제거할 것인지 지정합니다. 기본값: Disabled(사용 안 함) **참고:** 사용자가 대화 상자에서 **Submit(제출)**을 클릭할 때마다 APSolute Vision에서 이 조치가 실행됩니다. 예를 들어, 확인란을 선택하고 **Submit(제출)**을 클릭한 후 나중에 트랩 대상 주소 테이블에 트랩 대상을 추가하는 경우 사용자가 다음번에 대화 상자에서 **Submit(제출)**을 클릭하면 APSolute Vision에서 추가 주소를 제거합니다. 자세한 내용은 디바이스 이벤트에 등록된 APSolute Vision 서버—DefensePro, 54페이지를 참조하십시오.

디바이스 연결 정보를 편집하려면

1. 디바이스 창 *Sites and Clusters(사이트 및 클러스터)* 트리에서 디바이스 이름을 선택합니다.
2.  (Edit(편집)) 버튼을 클릭합니다.
3. 새 DefensePro 디바이스를 추가하려면, 50페이지 절차에 설명된 매개변수를 수정하고 **Submit(제출)**을 클릭합니다.

디바이스를 삭제하려면

1. 디바이스 창 *Sites and Clusters(사이트 및 클러스터)* 트리에서 디바이스 이름을 선택하고 (Delete(삭제)) 버튼을 클릭합니다.
2. 확인 상자에서 **Yes(예)**를 클릭합니다. 매니지드 디바이스 목록에서 디바이스가 삭제됩니다.

디바이스 이벤트에 등록된 APSolute Vision 서버—DefensePro

디바이스 속성 대화 상자의 *Event Notification(이벤트 알림)* 탭에서(표 5 - 디바이스 속성: 이벤트 알림 매개변수, 53페이지) APSolute Vision 서버가 디바이스 이벤트의 대상으로 자신을 구성할지 여부(**Register This APSolute Vision Server for Device Events(이 APSolute Vision 서버를 디바이스 이벤트에 등록)** 확인란)와 APSolute Vision 서버가 자신의 고유 주소를 제외하고 디바이스 이벤트의 모든 수신자를 디바이스에서 제거할지 여부(**Remove All Other Targets of Device Events(디바이스 이벤트의 다른 모든 대상 제거)** 확인란)를 지정할 수 있습니다. APSolute Vision에서는 사용자가 대화 상자에서 **Submit(제출)**을 클릭할 때마다 이러한 조치를 실행합니다.

일반적으로 여러 APSolute Vision 서버에서 동일한 DefensePro 디바이스를 관리할 수 있습니다.

여러 APSolute Vision 서버에서 동일한 DefensePro 디바이스를 관리하는 경우 디바이스에서 다음을 전송합니다.

- 관리하는 모든 APSolute Vision 서버에 트랩 전송. 대상 주소 테이블 및 대상 매개변수 테이블에는 모든 APSolute Vision 서버의 항목이 포함되어 있습니다.
- *디바이스에 등록된 마지막 APSolute Vision 서버에만* 패킷 보고 데이터 전송.

주의: Register This APSolute Vision Server for Device Events(이 APSolute Vision 서버를 디바이스 이벤트에 등록) 확인란의 선택을 취소하면 경고 브라우저, 보안 보고 및 APSolute Vision Reporter에서 디바이스에 대한 정보를 수집하여 표시할 수 없습니다.

APSolute Vision에서 DefensePro 디바이스 잠금 및 잠금 해제

특정 디바이스에서 디바이스 컨피그레이션을 수행할 권한이 있는 경우 디바이스를 구성하려면 먼저 디바이스를 잠가야 합니다. 디바이스를 잠그면 다른 사용자가 동시에 컨피그레이션을 변경할 수 없습니다. 디바이스의 잠금을 해제하거나, 연결을 끊거나, *디바이스 잠금 시간 초과*가 경과하거나 *관리자*가 잠금을 해제할 때까지 디바이스가 잠긴 상태로 유지됩니다.

디바이스 잠금은 WBM(Web Based Management) 또는 CLI를 사용하여 다른 APSolute Vision 서버에서 구성한 동일한 디바이스에는 적용되지 않습니다.

참고: 하나의 APSolute Vision 서버에서만 하나의 Radware 디바이스를 관리해야 합니다. 디바이스가 잠긴 동안에는:

- 디바이스 장치의 디바이스 아이콘에 DefensePro에 작은 잠금 기호— 을 포함합니다.
- 컨피그레이션 창은 디바이스에 대한 컨피그레이션 권한이 있는 다른 사용자에게 읽기 전용 모드로 표시됩니다.

- 해당되는 경우 **Submit(제출)** 버튼을 사용할 수 있습니다.
- 해당되는 경우  (Add(추가)) 버튼이 표시됩니다.

단일 디바이스를 잠그려면

1. 디바이스 창에서 디바이스를 선택합니다.
2. 디바이스 속성 창에서  (디바이스 그림의 왼쪽 아래 모서리에 있는 잠금 해제된 자물쇠 그림)을 클릭합니다. 그림이  (잠긴 자물쇠 그림)으로 변경됩니다.

단일 디바이스 잠금을 해제하려면

1. 디바이스 창에서 디바이스를 선택합니다.
2. 디바이스 속성 창에서  (디바이스 그림의 왼쪽 아래 모서리에 있는 잠긴 자물쇠 그림)을 클릭합니다. 그림이  (잠금 해제된 자물쇠 그림)으로 변경됩니다.

여러 디바이스를 잠그려면

1. 디바이스 창에서 잠글 디바이스를 선택합니다.
2.  (View(보기)) 버튼을 클릭합니다.
3. 디바이스 속성 창에서  (잠금 해제된 자물쇠 그림)을 클릭합니다.

여러 디바이스 잠금을 해제하려면

1. 디바이스 창에서 잠금을 해제할 디바이스를 선택합니다.
2.  (View(보기)) 버튼을 클릭합니다.
3. 디바이스 속성 창에서  (잠금 해제된 자물쇠 그림)을 클릭합니다.

APSolute Vision에서 일반 GUI 요소 사용

이 절에는 다음 항목이 포함되어 있습니다.

- 테이블 항목 관리를 위한 아이콘 및 명령, 56페이지
- 테이블 행 필터링, 57페이지

테이블 항목 관리를 위한 아이콘 및 명령

다음 표에서는 APSolute Vision WBM(Web Based Management)을 사용하여 테이블 항목(행)을 관리할 때 사용할 수 있는 아이콘/버튼 및 해당 명령에 대해 설명합니다. 사용 가능한 명령은 기능에 따라 다릅니다. 아이콘은 항상 왼쪽 표 위에 있습니다. 마우스 커서(포인터)를 아이콘 위에 두면 아이콘 표시가 단색(회색) 컬러로 변경됩니다.

참고

- 디바이스가 잠긴 경우에만 매니지드 디바이스를 구성하고 제어할 수 있습니다(디바이스 잠금 및 잠금 해제, 162페이지 참조).
- APSolute Vision 문서에서는 컬러가 지정된 상태로 아이콘과 버튼을 표시합니다.

표 6: 테이블 항목 관리를 위한 아이콘 및 명령

아이콘/버튼	명령	설명
	추가	“Add New...(새로 추가...)” 탭을 열어 새 항목을 구성합니다.
	편집	“Edit...(편집...)” 탭을 열어 선택한 기존 항목을 수정합니다.
	중복	인덱스를 제외하고 선택한 항목의 값으로 채워지는 “Add New...(새로 추가...)” 탭을 엽니다.
	삭제	선택을 삭제합니다.
	수출	선택한 항목을 내보냅니다.
	보기	“View...(보기...)” 탭을 열어 선택한 항목의 값을 봅니다.

테이블 행 필터링

APSolute Vision 및 매니지드 디바이스에 있는 수많은 테이블의 경우 테이블 열의 값에 따라 테이블 행을 필터링할 수 있습니다.

필터에서는 사용자가 지정한 필터 기준에 대해 Boolean AND 연산자를 사용합니다. 즉, 필터링된 테이블에 *임의*의 검색 매개변수가 아니라 *모든* 검색 매개변수와 일치하는 행이 표시됩니다. 예를 들어, 테이블에 *Policy(정책)* 및 *Port(포트)* 열이 포함되어 있으며 정책 값 **ser**에 대해 필터링하고 포트 값이 **80**이면, 필터링된 테이블에는 정책 매개변수의 값에 **ser**이 포함되고 포트 매개변수의 값에 **80**이 포함된 행이 표시됩니다.

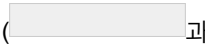
테이블 행을 필터링하려면

1. 다음을 수행합니다.
   - 테이블 열에 드롭다운 목록이 표시되면(

과 같은 화살표 포함), 화살표를 클릭하고 필터링할 기준 값을 선택합니다.
   - 테이블 열에 흰색의 텍스트 상자가 표시되면(

과 비슷함), 필터링할 기준 값을 입력합니다.

   참고
   - 텍스트 상자의 경우 필터에서 *contains* 알고리즘을 사용합니다. 즉, 입력한 문자열이 값에 *포함*되기만 하면 필터에서는 일치하는 것으로 간주합니다. 예를 들어, 텍스트 상자에 **ser**을 입력하면 필터에서 값이 **ser**, **service1** 및 **service2**인 행을 반환합니다.
   - 열의 맨 위에 있는 상자가 회색이면( 과 비슷함) 해당 매개변수에 따라 필터링할 수 없습니다.
2.  (Filter(필터)) 버튼을 클릭하거나 **Enter**를 누릅니다.

3장 – 디바이스 운영 및 유지 관리

이 장에서는 다음 운영과 유지관리 작업에 대해 설명합니다.

- DefensePro 디바이스에서 정책 컨피그레이션 업데이트, 59페이지
- DefensePro 디바이스 재부팅 또는 종료, 60페이지
- APSolute Vision 클라이언트에 디바이스의 로그 파일 다운로드, 60페이지
- 기술 지원 및 컨피그레이션 파일 다운로드, 61페이지
- DefensePro 디바이스 컨피그레이션 관리, 61페이지
- DefensePro의 베이스라인 재설정, 63페이지
- APSolute Vision 및 디바이스 작업 일정 예약, 64페이지
- 공격 설명 파일 업데이트, 71페이지

참고

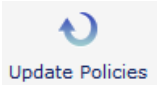
- APSolute Vision을 사용하여 DefensePro for Cisco Firepower 9300을 업그레이드할 수 없습니다. DefensePro for Cisco Firepower 9300의 디바이스 업그레이드에 대한 내용은 관련 릴리스 노트를 참조하십시오.
- DefensePro for Cisco Firepower 9300에서는 APSolute Vision *템플릿* 기능을 지원하지 않습니다.
- APSolute Vision을 사용하여 시그니처 파일을 업데이트하는 작업은 DefensePro for Cisco Firepower 9300과 관련이 없습니다.

DefensePro 디바이스에서 정책 컨피그레이션 업데이트

단일 운영으로 DefensePro 디바이스에 다음 컨피그레이션 변경사항을 적용할 수 있습니다.

- 네트워크 보호 정책
- 클래스

DefensePro 디바이스에서 정책 컨피그레이션을 업데이트하려면

> 디바이스 창에서 디바이스를 선택한 다음 

버튼을 클릭합니다.

DefensePro 디바이스 재부팅 또는 종료

APSolute Vision에서 디바이스 재부팅(재설정) 또는 디바이스 종료를 활성화할 수 있습니다.

디바이스에서 일부 컨피그레이션 변경사항이 적용되려면 디바이스를 재부팅해야 합니다. APSolute Vision에서 디바이스 재부팅을 활성화할 수 있습니다.

디바이스를 재부팅하려면

1. 디바이스를 잠급니다.
2. *Properties(속성)* 창에서 디바이스 그림의 일부인  (On-Off(켜기-끄기)) 버튼을 클릭합니다.
3. **Reset(재설정)**을 선택합니다.

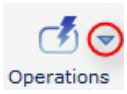
디바이스를 종료하려면

1. 디바이스를 잠급니다.
2. *Properties(속성)* 창에서 디바이스 그림의 일부인  (On-Off(켜기-끄기)) 버튼을 클릭합니다.
3. **Shut Down(종료)**를 선택합니다.

APSolute Vision 클라이언트에 디바이스의 로그 파일 다운로드

DefensePro 로그 파일을 APSolute Vision 클라이언트 시스템에 다운로드할 수 있습니다. 로그 파일은 디바이스에서 자동으로 생성되며 컨피그레이션 오류 보고서를 포함합니다. 로그 파일은 디버깅에 사용할 수 있습니다.

디바이스 로그 파일을 다운로드하려면

1. 디바이스 창에서 디바이스를 선택합니다.
2. 

(Operations(운영)) 아이콘의 화살표를 클릭합니다.
3. **Export Log File(로그 파일 내보내기)**를 클릭합니다.
4. 다운로드 매개변수를 구성하고 **Submit(제출)**을 클릭합니다.

표 7: 디바이스 로그 파일 다운로드 매개변수

매개변수	설명
Download Via(다운로드 방법)	(읽기 전용) 로그 파일을 다운로드하는 데 사용되는 프로토콜입니다. 값: HTTPS
Save As(다른 이름으로 저장)	다운로드한 로그 파일을 클라이언트 시스템에 텍스트 파일로 저장합니다. 저장된 로그 파일의 위치를 입력하거나 찾아보고 파일 이름을 선택하거나 입력합니다.

기술 지원 및 컨피그레이션 파일 다운로드

디버깅용으로 DefensePro 디바이스에서는 Radware Technical Support에 필요한 기술 정보를 포함하는 TAR 파일을 생성할 수 있습니다. 파일에는 다양한 CLI 명령의 출력이 포함됩니다(예: 클라이언트 테이블의 인쇄물).

DefensePro 기술 지원 파일을 다운로드하여 Radware Technical Support에 보낼 수 있습니다.

DefensePro 디바이스 컨피그레이션 관리

이 섹션에서는 APSolute Vision에서 구성한 DefensePro 디바이스의 컨피그레이션 관리 방법을 설명합니다.

DefensePro 컨피그레이션 파일 콘텐츠

컨피그레이션 파일 콘텐츠는 다음 두 개의 섹션으로 나뉩니다.

- **디바이스를 재부팅해야 하는 명령**—애플리케이션 보안 상태, 디바이스 운영 모드, 조정 매개변수 등이 포함됩니다. 이 섹션에서 명령을 복사하여 붙여넣기는 디바이스를 재부팅한 후에만 적용됩니다. 이 섹션에는 다음과 같은 표제가 있습니다. 다음 명령은 디바이스를 재부팅한 후에만 적용됩니다!
- **디바이스를 재부팅하지 않아도 되는 명령**—이 섹션에서 명령을 복사하여 붙여넣기는 붙여넣은 후에 바로 적용됩니다. 이 섹션의 명령은 SNMP로 바인드되지 않습니다. 이 섹션에는 다음과 같은 표제가 있습니다. 다음 명령은 실행 시 즉시 적용됩니다!

명령은 구현 순서대로 각 섹션에 인쇄됩니다.

파일의 끝에서 디바이스가 컨피그레이션 파일의 시그니처를 인쇄합니다. 이 시그니처는 파일의 진본 여부를 검증하고 손상되지 않았는지 확인하는 데 사용됩니다. 컨피그레이션 파일을 디바이스에 업로드할 때마다 시그니처를 검증합니다. 검증 확인에 실패하면 디바이스에서 컨피그레이션을 승인하지만, 컨피그레이션 파일이 조작되었으며 이 파일이 작동한다는 보장이 없음을 사용자에게 알립니다. 시그니처는 다음 파일 시그니처와 같이 표시됩니다. 063390ed2ce0e9dfc98c78266a90a7e4.

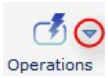
디바이스 컨피그레이션 파일 다운로드

백업을 위해 매니지드 디바이스에서 APSolute Vision으로 컨피그레이션 파일을 다운로드할 수 있습니다. APSolute Vision 서버에 다운로드하도록 선택하면 사본이 항상 APSolute Vision 데이터베이스에 저장됩니다.

기본적으로 디바이스당 최대 다섯(5) 개의 컨피그레이션 파일을 APSolute Vision 서버에 저장할 수 있습니다. APSolute Vision Setup(APSolute Vision 설정) 페이지에서 이 매개변수를 최대 10개까지 변경할 수 있습니다. 한계에 도달하면 가장 오래된 파일을 삭제하도록 메시지가 표시됩니다.

참고: APSolute Vision 스케줄러에서 컨피그레이션 파일 백업을 예약할 수 있습니다. 자세한 내용은 스케줄러에서 작업 구성, 65페이지를 참조하십시오.

디바이스 컨피그레이션 파일을 다운로드하려면

1. 디바이스 창에서 디바이스를 선택합니다.
2. 

(Operations(운영)) 아이콘의 화살표를 클릭합니다.
3. **Export Configuration File(컨피그레이션 파일 내보내기)**을 선택합니다.
4. 다운로드 매개변수를 구성한 다음 **Save(저장)**를 클릭합니다.

표 8: 디바이스 컨피그레이션 파일 다운로드 매개변수

매개변수	설명
Download to(다운로드 위치)	디바이스 컨피그레이션 파일을 백업할 위치입니다. 값: 클라이언트, 서버
Download Via(다운로드 방법)	(읽기 전용) 컨피그레이션 파일을 다운로드하는 데 사용되는 프로토콜입니다. 값: HTTPS
Save As(다른 이름으로 저장)	다운로드한 컨피그레이션 파일을 클라이언트 시스템에 텍스트 파일로 저장합니다. 서버에서 기본 이름은 디바이스 이름과 백업 날짜 및 시간의 조합입니다. 기본 이름을 변경할 수 있습니다.
Include Private Keys(개인 키 포함)	사용하도록 설정된 경우 인증서 개인 키 정보가 다운로드한 파일에 포함됩니다. 개인 키를 복원하려면 개인 키 정보를 포함해야 합니다. 그렇지 않으면 디바이스가 기본 키로 되돌아 갑니다.

디바이스 컨피그레이션 복원

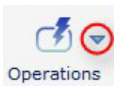
DefensePro 또는 DefenseFlow 컨피그레이션을 APSolute Vision 서버나 클라이언트 시스템의 백업 컨피그레이션 파일에서 DefensePro 또는 DefenseFlow 디바이스로 복원할 수 있습니다. 컨피그레이션 파일을 디바이스로 업로드하면 기존 디바이스 컨피그레이션을 덮어씁니다.

복원 작업이 완료되면 디바이스를 재부팅해야 합니다.

주의: 편집한 컨피그레이션 파일을 가져오는 기능은 지원되지 않습니다.

주의: 다른 버전에서 컨피그레이션 파일을 가져오는 기능은 지원되지 않습니다.

디바이스의 컨피그레이션을 복원하려면

1. 디바이스 창에서 디바이스를 선택합니다.
2. 

(Operations(운영)) 아이콘의 화살표를 클릭합니다.
3. **Import Configuration File(컨피그레이션 파일을 가져오기)**을 클릭합니다.
4. 업로드 매개변수를 구성하고 **Submit(제출)**을 클릭합니다.
5. 업로드가 완료되면 디바이스를 재부팅합니다.

표 9: 디바이스 컨피그레이션 파일 업로드 매개변수

매개변수	설명
Upload from(업로드 소스 위치)	전송할 백업 디바이스 컨피그레이션 파일의 위치입니다. 값: 클라이언트, 서버
Upload Via(업로드 방법)	(읽기 전용) 컨피그레이션 파일을 업로드하는 데 사용되는 프로토콜입니다. 값: HTTPS
File Name(파일 이름)	클라이언트 시스템에서 업로드할 때 업로드할 컨피그레이션 파일의 이름을 입력하거나 찾아봅니다. 서버에서 업로드할 때 업로드할 컨피그레이션을 선택합니다.
Passphrase(암호 문구) (이 매개변수는 Alteon 디바이스에서만 사용할 수 있습니다.)	HTTPS용 암호 문구입니다.

DefensePro의 베이스라인 재설정

베이스라인 학습 통계를 재설정하면 베이스라인 트래픽 통계를 지우고 기본 정상 베이스라인을 재설정합니다. 보호된 네트워크의 특성이 완전히 변경되고 네트워크 변경사항에 맞게 대역폭 할당량을 변경해야 하는 경우에만 베이스라인 통계를 재설정합니다.

BDoS 또는 DNS 보호 프로필을 포함하는 모든 네트워크 보호 정책 및 BDoS 또는 DNS 보호 프로필을 포함하는 선택한 네트워크 보호 정책에 대한 베이스라인을 재설정할 수 있습니다.

BDoS 베이스라인 통계를 재설정하려면

1. *Configuration(컨피그레이션)* 관점에서 **Setup(설정) > Security Settings(보안 설정) > BDoS Protection(BDoS 보호) > Reset BDoS Baseline(BDoS 베이스라인 재설정)**을 선택합니다.
2. BDoS 프로필을 포함하는 모든 네트워크 보호 정책 및 BDoS 프로필을 포함하는 특정 네트워크 보호 정책에 대한 베이스라인을 재설정할지 선택합니다.
3. **Submit(제출)**를 클릭합니다.

DNS 베이스라인 통계를 재설정하려면

1. *Configuration(컨피그레이션)* 관점에서 **Setup(설정) > Security Settings(보안 설정) > BDoS Protection(BDoS 보호) > Reset DNS Baseline(DNS 베이스라인 재설정)**을 선택합니다.
2. DNS 프로필을 포함하는 모든 네트워크 보호 정책 또는 DNS 프로필을 포함하는 특정 네트워크 보호 정책에 대한 베이스라인을 재설정할지 선택합니다.
3. **Submit(제출)**를 클릭합니다.

APSolute Vision 및 디바이스 작업 일정 예약

다음 항목에서는 APSolute Vision Scheduler에서 작업 일정을 예약하는 방법에 대해 설명합니다.

- 일정 예약 개요, 64페이지
- 스케줄러에서 작업 구성, 65페이지
- 작업 매개변수, 66페이지

참고: APSolute Vision 서버에서 작업 일정을 예약하는 방법에 대한 정보는 *APSolute Vision 사용 설명서* 또는 APSolute Vision 온라인 도움말을 참조하십시오.

일정 예약 개요

APSolute Vision 서버 및 매니지드 디바이스의 다양한 작업 일정을 예약할 수 있습니다. 예약된 작업은 *작업(task)*이라고 합니다.

APSolute Vision Scheduler에서는 작업이 마지막으로 수행된 시기와 다음에 수행될 시기를 추적합니다. 여러 디바이스의 작업을 구성하면 작업이 각 디바이스에서 순차적으로 실행됩니다. 작업이 한 디바이스에서 완료되고 나면 다음 디바이스에서 시작됩니다. 작업이 디바이스에서 완료되지 못하면 Scheduler가 다음으로 나열된 디바이스에서 작업을 활성화합니다.

작업을 생성하고 실행할 시간을 지정하는 경우 해당 시간은 로컬 OS에 따라 달라집니다. 그런 다음 APSolute Vision에서 시간을 저장하고 APSolute Vision 서버의 시간대로 변환한 다음 적절하게 실행합니다. 즉, 작업을 구성하고 나면 APSolute Vision 시간 설정에 따라 실행되며 로컬 OS 시간 설정의 변경사항을 무시합니다.

주의: APSolute Vision 클라이언트 시간대가 APSolute Vision 서버나 매니지드 디바이스의 시간대와 다르면 시간 차감을 고려하십시오.

작업을 정의할 때 작업을 사용하거나 사용하지 않도록 설정할 것인지 선택할 수 있습니다. 구성된 모든 작업은 APSolute Vision 데이터베이스에 저장됩니다.

다음 유형의 DefensePro 관련 예약 작업을 정의할 수 있습니다.

- 디바이스 컨피그레이션 백업
- APSolute Vision Reporter 데이터 백업
- 디바이스 재부팅

참고

- APSolute Vision에서 노출하는 일부 작업은 특정 DefensePro 버전에서는 작동하지/적합하지 않습니다.
- *Monitoring(모니터링)* 관점에서 수동으로 작업을 수행할 수 있습니다. 자세한 내용은 다음 링크를 참고하십시오.
- DefensePro 디바이스 재부팅 또는 종료, 60페이지
- 디바이스 컨피그레이션 파일 다운로드, 61페이지

스케줄러에서 작업 구성

Tasks(작업) 테이블은 예약된 작업인 작업(task)을 보고 구성하는 시작 위치입니다.

Tasks(작업) 테이블에는 구성된 각 작업에 대한 다음 정보가 표시됩니다.

표 10: 작업 테이블 매개변수

매개변수	설명
Task Type	수행할 작업 유형입니다.
Name	구성된 작업의 이름입니다.
Enabled	선택한 경우 정의된 일정에 따라 작업이 실행됩니다. 사용하지 않도록 설정한 작업은 활성화되지 않지만, 데이터베이스에 작업이 저장됩니다.
Description	작업의 사용자 정의 설명입니다.
Current Status	작업의 현재 상태입니다. 값: 대기 중, 진행 중
Last Execution Status	마지막 작업 실행의 성공 여부입니다. 작업을 사용하지 않도록 설정하거나 작업이 아직 시작되지 않은 경우 상태는 **실행되지 않음**입니다.
Last Execution Time	마지막 작업 실행 날짜 및 시간입니다. 작업을 사용하지 않도록 설정하거나 작업이 아직 시작되지 않은 경우 이 필드는 비어 있습니다.
Next Execution Time	다음 작업의 실행 날짜 및 시간입니다. 작업을 사용하지 않도록 설정한 경우 이 필드는 비어 있습니다.
Run	작업이 실행되는 빈도입니다(예: 매일 또는 매주). 일정 시작 날짜를 정의한 경우 표시됩니다.

예약된 작업을 구성하려면

1. 기본 툴바에서 정보가 (스케줄러) 아이콘을 클릭합니다. *Tasks(작업)* 테이블에 예약된 각 작업의 표시됩니다.
2. 다음 중 하나를 수행합니다.
   - 테이블에 항목을 추가하려면 (Add(추가)) 버튼을 클릭합니다. 그런 다음 작업 유형을 선택하고 **Submit(제출)**을 클릭합니다. 선택한 작업 유형의 대화 상자가 표시됩니다.
   - 테이블의 항목을 편집하려면 항목을 선택하고 (Edit(편집)) 버튼을 클릭합니다.
3. 작업 매개변수를 구성하고 **Submit(제출)**을 클릭합니다. 모든 작업 컨피그레이션에는 기본 매개변수와 예약 매개변수가 포함됩니다. 기타 매개변수는 선택하는 작업 유형에 따라 달라집니다.

기존 작업을 실행하려면

1. 기본 툴바에서 (Scheduler(스케줄러)) 아이콘을 클릭합니다. *Tasks(작업)* 테이블에 예약된 각 작업의 정보가 표시됩니다.
2. 필요한 작업을 선택하고 (Run Task(작업 실행)) 버튼을 클릭합니다.

작업 매개변수

다음 절에서는 DefensePro 관련 Scheduler 작업의 매개변수를 설명합니다.

- APSolute Vision Reporter 백업—매개변수, 66페이지
- 디바이스 컨피그레이션 백업—매개변수, 68페이지
- 디바이스 재부팅 작업, 70페이지

APSolute Vision Reporter 백업— 매개변수

APSolute Vision Reporter 백업 작업에서는 APSolute Vision Reporter 데이터의 백업을 생성하여 지정된 대상에 내보냅니다. 백업에는 APSolute Vision Reporter 데이터가 모두 포함됩니다.

참고

- APSolute Vision에서는 최대 3회의 APSolute Vision Reporter 데이터 반복을 *스토리지 위치*에 저장합니다. 세 번째 reporter 백업 후에 시스템에서는 가장 오래된 백업을 삭제합니다.
- *스토리지 위치*는 기본적으로 APSolute Vision 서버에 하드 코딩된 위치입니다.
- *스토리지 위치*의 백업 파일 이름은 지정된 파일 이름의 처음 5자에 10자의 타임스탬프를 추가하여 생성합니다. 작업을 통해 백업 파일을 내보내면 작업 컨피그레이션에 지정된 대로 파일 이름이 지정됩니다.
- 스토리지 위치의 백업 파일에는 하드 코딩된 설명 Scheduler- generated(스케줄러-생성됨)를 포함합니다.

표 11: APSolute Vision Reporter 백업: 일반 매개변수

매개변수	설명
Name	작업의 이름입니다. 기본값: 선택한 작업 유형 이름입니다. 이 이름을 사용하는 기존 작업이 있으면 이름에 **n**이 추가됩니다. 여기서 **n**은 다음으로 사용 가능한 순서 번호입니다.
Description	작업의 사용자 정의 설명입니다.
Enabled	선택한 경우 정의된 일정에 따라 작업이 실행됩니다. 사용하지 않도록 설정된 작업은 활성화되지 않지만, 데이터베이스에 작업 컨피그레이션이 저장됩니다.

표 12: APSolute Vision Reporter 백업: Scheduler 매개변수

매개변수	설명
Run	작업이 실행되는 빈도입니다. 빈도를 선택한 다음 관련 시간과 일/날짜 매개변수를 구성합니다. 값: ● Once(한 번)—작업이 지정된 날짜와 시간에 한 번만 실행됩니다. ● Minutes(분)—작업 시작 사이에 지정된 시간(분) 간격으로 작업이 실행됩니다. TBD: 최소 ● Daily(매일)—작업이 매일 지정된 시간에 실행됩니다. ● Weekly(매주)—작업이 매주 지정된 날, 지정된 시간에 실행됩니다. **참고:** 작업은 APSolute Vision 클라이언트에 구성된 대로 시간에 따라 실행됩니다.
Time[1]	작업이 실행되는 시간입니다.
Date[2]	작업이 실행되는 날짜입니다.
Minutes[3]	작업이 실행되는 간격(분)입니다.
Run Always[4]	작업이 항상 실행되는지 아니면 정의된 기간 동안에만 실행되는지 지정합니다. 값: ● Enabled(사용)—시작 또는 종료 시간이 없이 작업이 즉시 활성화되며 무한대로 실행됩니다. *Schedule(일정)* 탭의 빈도에 구성된 첫 번째 시간에 실행됩니다. ● Disabled(사용 안 함)—작업이 (*Schedule(일정)* 탭에 지정된 시간과 빈도로) 지정된 시작 날짜의 시작 시간부터 종료 날짜의 종료 시간까지 실행됩니다. 기본값: Enabled(사용)
Start Date[5]	작업이 활성화되는 날짜와 시간입니다.
Start Time	
End Date	작업이 더 이상 실행되지 않는 날짜와 시간입니다.
End Time	

1 – 이 매개변수는 지정된 **Run(실행)** 값이 **Once(한 번), Daily(매일)** 또는 **Weekly(매주)**인 경우에만 사용할 수 있습니다.
2 – 이 매개변수는 지정된 **Run(실행)** 값이 **Once(한 번)**인 경우에만 사용할 수 있습니다.
3 – 이 매개변수는 지정된 **Run(실행)** 값이 **Minutes(분)**인 경우에만 사용할 수 있습니다.
4 – 이 매개변수는 지정된 **Run(실행)** 값이 **Minutes(분)**, **Daily(매일)** 또는 **Weekly(매주)**인 경우에만 사용할 수 있습니다.
5 – 이 매개변수는 지정된 **Run Always(항상 실행)** 확인란의 선택을 취소한 경우에만 사용할 수 있습니다.

표 13: APSolute Vision Reporter 백업: 대상 매개변수

매개변수	설명
Protocol	APSolute Vision에서 이 작업에 사용하는 프로토콜입니다. 값: ● FTP ● SCP ● SFTP ● SSH 기본값: FTP
IP Address	서버의 IP 주소입니다.
Directory	공백이 포함되지 않는 내보내기 디렉토리의 경로입니다. 영숫자 문자와 밑줄(_)만 허용됩니다.
Backup File Name	공백이 포함되지 않는 최대 15자의 백업 이름입니다. 영숫자 문자와 밑줄(_)만 허용됩니다.
User	사용자 이름입니다.
Password	사용자 비밀번호입니다.
Confirm Password	사용자 비밀번호입니다.

디바이스 컨피그레이션 백업— 매개변수

디바이스 컨피그레이션 백업 작업은 지정된 디바이스의 컨피그레이션 백업을 저장합니다.

참고: 기본적으로 디바이스당 최대 다섯(5) 개의 컨피그레이션 파일을 APSolute Vision 서버에 저장할 수 있습니다. APSolute Vision *Setup(설정)* 탭에서 이 매개변수를 변경할 수 있습니다.

표 14: 디바이스 컨피그레이션 백업: 일반 매개변수

매개변수	설명
Name	작업의 이름입니다. 기본값: 선택한 작업 유형 이름입니다. 이 이름을 사용하는 기존 작업이 있으면 이름에 **n**이 추가됩니다. 여기서 **n**은 다음으로 사용 가능한 순서 번호입니다.
Description	작업의 사용자 정의 설명입니다.
Enabled	선택한 경우 정의된 일정에 따라 작업이 실행됩니다. 사용하지 않도록 설정된 작업은 활성화되지 않지만, 데이터베이스에 작업 컨피그레이션이 저장됩니다.

표 15: 디바이스 컨피그레이션 백업: 일정 매개변수

매개변수	설명
Run	작업이 실행되는 빈도입니다. 빈도를 선택한 다음 관련 시간과 일/날짜 매개변수를 구성합니다. 값: ● Once(한 번)—작업이 지정된 날짜와 시간에 한 번만 실행됩니다. ● Minutes(분)—작업 시작 사이에 지정된 시간(분) 간격으로 작업이 실행됩니다. ● Daily(매일)—작업이 매일 지정된 시간에 실행됩니다. ● Weekly(매주)—작업이 매주 지정된 날, 지정된 시간에 실행됩니다. **참고:** 작업은 APSolute Vision 클라이언트에 구성된 대로 시간에 따라 실행됩니다.
Time[1]	작업이 실행되는 시간입니다.
Date[2]	작업이 실행되는 날짜입니다.
Minutes[3]	작업이 실행되는 간격(분)입니다.
Run Always[4]	작업이 항상 실행되는지 아니면 정의된 기간 동안에만 실행되는지 지정합니다. 값: ● Enabled(사용)—시작 또는 종료 시간이 없이 작업이 즉시 활성화되며 무한대로 실행됩니다. *Schedule(일정)* 탭의 빈도에 구성된 첫 번째 시간에 실행됩니다. ● Disabled(사용 안 함)—작업이 (*Schedule(일정)* 탭에 지정된 시간과 빈도로) 지정된 시작 날짜의 시작 시간부터 종료 날짜의 종료 시간까지 실행됩니다. 기본값: Enabled(사용)
Start Date[5]	작업이 활성화되는 날짜와 시간입니다.
Start Time	
End Date	작업이 더 이상 실행되지 않는 날짜와 시간입니다.
End Time	

1 – 이 매개변수는 지정된 **Run(실행)** 값이 **Once(한 번)**, **Daily(매일)** 또는 **Weekly(매주)**인 경우에만 사용할 수 있습니다.
2 – 이 매개변수는 지정된 **Run(실행)** 값이 **Once(한 번)**인 경우에만 사용할 수 있습니다.
3 – 이 매개변수는 지정된 **Run(실행)** 값이 **Minutes(분)**인 경우에만 사용할 수 있습니다.
4 – 이 매개변수는 지정된 **Run(실행)** 값이 **Minutes(분)**, **Daily(매일)** 또는 **Weekly(매주)**인 경우에만 사용할 수 있습니다.
5 – 이 매개변수는 지정된 **Run Always(항상 실행)** 확인란의 선택을 취소한 경우에만 사용할 수 있습니다.

표 16: 디바이스 컨피그레이션 백업: 매개변수 매개변수

매개변수	설명
Include Private Keys	개인 키를 지원하는 디바이스의 컨피그레이션 파일에 인증서 개인 키 정보를 포함할지를 지정합니다. 기본값: Disabled(사용 안 함)

표 17: 디바이스 컨피그레이션 백업: 디바이스 목록 매개변수

매개변수	설명
Available(사용 가능한) 목록 및 *Selected(선택한)* 목록입니다. *Available(사용 가능한)* 목록에 사용 가능한 디바이스가 표시됩니다. *Selected(선택한)* 목록에는 이 작업을 통해 해당 컨피그레이션을 백업하는 디바이스가 표시됩니다.	

디바이스 재부팅 작업

디바이스 재부팅 작업을 통해 지정된 디바이스를 재부팅합니다.

표 18: 디바이스 재부팅: 일반 매개변수

매개변수	설명
Name	작업의 이름입니다. 기본값: 선택한 작업 유형 이름입니다. 이 이름을 사용하는 기존 작업이 있으면 이름에 **n**이 추가됩니다. 여기서 **n**은 다음으로 사용 가능한 순서 번호입니다.
Description	작업의 사용자 정의 설명입니다.
Enabled	선택한 경우 정의된 일정에 따라 작업이 실행됩니다. 사용하지 않도록 설정된 작업은 활성화되지 않지만, 데이터베이스에 작업 컨피그레이션이 저장됩니다.

표 19: 디바이스 재부팅: 일정 매개변수

매개변수	설명
Run	작업이 실행되는 빈도입니다. 빈도를 선택한 다음 관련 시간과 일/날짜 매개변수를 구성합니다. 값: ● Once(한 번)—작업이 지정된 날짜와 시간에 한 번만 실행됩니다. ● Minutes(분)—작업 시작 사이에 지정된 시간(분) 간격으로 작업이 실행됩니다. ● Daily(매일)—작업이 매일 지정된 시간에 실행됩니다. ● Weekly(매주)—작업이 매주 지정된 날, 지정된 시간에 실행됩니다. **참고:** 작업은 APSolute Vision 클라이언트에 구성된 대로 시간에 따라 실행됩니다.
Time[1]	작업이 실행되는 시간입니다.
Date[2]	작업이 실행되는 날짜입니다.
Minutes[3]	작업이 실행되는 간격(분)입니다.
Run Always[4]	작업이 항상 실행되는지 아니면 정의된 기간 동안에만 실행되는지 지정합니다. 값: ● Enabled(사용)—시작 또는 종료 시간이 없이 작업이 즉시 활성화되며 무한대로 실행됩니다. *Schedule(일정)* 탭의 빈도에 구성된 첫 번째 시간에 실행됩니다. ● Disabled(사용 안 함)—작업이 (*Schedule(일정)* 탭에 지정된 시간과 빈도로) 지정된 시작 날짜의 시작 시간부터 종료 날짜의 종료 시간까지 실행됩니다. 기본값: Enabled(사용)

표 19: 디바이스 재부팅: 일정 매개변수(계속)

매개변수	설명
Start Date[5]	작업이 활성화되는 날짜와 시간입니다.
Start Time	
End Date	작업이 더 이상 실행되지 않는 날짜와 시간입니다.
End Time	

1 – 이 매개변수는 지정된 **Run(실행)** 값이 **Once(한 번), Daily(매일)** 또는 **Weekly(매주)**인 경우에만 사용할 수 있습니다.
2 – 이 매개변수는 지정된 **Run(실행)** 값이 **Once(한 번)**인 경우에만 사용할 수 있습니다.
3 – 이 매개변수는 지정된 **Run(실행)** 값이 **Minutes(분)**인 경우에만 사용할 수 있습니다.
4 – 이 매개변수는 지정된 **Run(실행)** 값이 **Minutes(분)**, **Daily(매일)** 또는 **Weekly(매주)**인 경우에만 사용할 수 있습니다.
5 – 이 매개변수는 지정된 **Run Always(항상 실행)** 확인란의 선택을 취소한 경우에만 사용할 수 있습니다.

표 20: 디바이스 재부팅: 디바이스 목록 매개변수

매개변수	설명
Available(사용 가능한) 목록 및 *Selected(선택한)* 목록입니다. *Available(사용 가능한)* 목록에 사용 가능한 디바이스가 표시됩니다. 선택한 목록에는 이 작업이 재부팅하는 디바이스가 표시됩니다.	

공격 설명 파일 업데이트

APSolute Vision 서버에서 공격 설명 파일의 최신 업데이트 시간을 보고 파일을 업데이트할 수 있습니다.

공격 설명 파일에는 DefensePro에서 처리할 수 있는 서로 다른 모든 공격의 설명이 포함되어 있습니다. 공격 이름을 입력하여 특정 설명을 볼 수 있습니다. 처음으로 APSolute Vision을 구성할 때 APSolute Vision 서버에 최신 공격 설명 파일을 다운로드해야 합니다. 파일은 DefensePro 디바이스에서 들어오는 공격에 대한 공격 설명을 보여주는 실시간 및 이력 보고서에 사용됩니다.

APSolute Vision과 DefensePro 디바이스의 파일 버전은 같아야 합니다. Radware에서는 APSolute Vision과 개별 디바이스에서 정기적 간격으로 파일의 정기적 업데이트를 동기화하도록 권장합니다.

참고: 또한 Radware에서는 DefensePro 디바이스에서 시그니처 파일을 업데이트할 때마다 공격 설명 파일을 업데이트하도록 권장합니다.

공격 설명 파일을 업데이트할 때, APSolute Vision이 Radware.com에서 직접 또는 지원되는 프록시 파일 서버에서 파일을 다운로드합니다.

공격 설명 파일의 최신 업데이트 날짜 및 시간을 보려면

1. *APSolute Vision Settings(APSolute Vision 설정)* 보기 *System(시스템)* 관점에서 **General Settings(일반 설정) > Basic Parameters(기본 매개변수)**를 선택합니다.
2. *Attack Descriptions File(공격 설명 파일)* 탭을 선택합니다.

표 21: 공격 설명 파일 매개변수

매개변수	설명
Attack Descriptions Last Update	APSolute Vision 서버에 있는 공격 설명 파일의 최신 업데이트 시간입니다.

공격 설명 파일을 업데이트하려면

1. *APSolute Vision Settings(APSolute Vision 설정)* 보기 *System(시스템)* 관점에서 **General Settings(일반 설정) > Basic Parameters(기본 매개변수)**를 선택합니다.
2. 다음 중 하나를 수행합니다.
   - Radware에서 공격 설명 파일을 업데이트하려면 **Radware.com** 라디오 버튼을 선택합니다.
   - APSolute Vision 클라이언트 호스트에서 파일을 업데이트하려면 다음을 수행합니다.
     a. **Client(클라이언트)** 라디오 버튼을 선택합니다.
     b. **File Name(파일 이름)** 텍스트 상자에서 공격 설명 파일의 파일 경로를 입력하거나 **Browse(찾아보기)**를 클릭하여 파일로 이동한 후 선택합니다.
3. **Update(업데이트)**를 클릭합니다. *Alerts(경고)* 창에 성공 또는 실패 알림이 표시되며, 프록시 서버를 사용하여 작업이 수행되었는지 여부가 표시됩니다.

4장 – DefensePro 설정 관리

선택한 DefensePro 디바이스에 대해 다음 설정 매개변수를 구성할 수 있습니다.

- DefensePro 전역 매개변수 구성, 73페이지
- DefensePro 네트워킹 설정 구성, 81페이지
- DefensePro 디바이스-보안 설정 구성, 86페이지
- DefensePro 보안-설정 설정 구성, 100페이지
- DefensePro 보고-설정 설정 구성, 113페이지
- DefensePro 클러스터링 설정 구성, 118페이지

DefensePro 전역 매개변수 구성

이 섹션에 포함되는 주제는 다음과 같습니다.

- 기본 전역 매개변수 보기 및 구성, 73페이지
- 인증서 관리, 74페이지
- DefensePro 디바이스의 라이센스 업그레이드, 79페이지
- DefensePro에서 날짜 및 시간 설정 구성, 80페이지

기본 전역 매개변수 보기 및 구성

다음을 보고 구성할 수 있습니다.

- 기본 디바이스 설정 매개변수
- 디바이스의 시간 및 날짜 설정
- 디바이스 하드웨어 및 소프트웨어 버전

기본 전역 매개변수를 보고 구성하려면

1. *Configuration(컨피그레이션)* 관점에서 **Setup(설정) > Global Parameters(전역 매개변수)**를 선택합니다.
2. 필요한 경우 매개변수를 구성한 다음 **Submit(제출)**을 클릭합니다.

표 22: 전역 매개변수: 일반 매개변수

매개변수	설명
Device Name	(읽기 전용) 디바이스에 구성된 디바이스 이름입니다.
Device Description	(읽기 전용) 디바이스에 구성된 디바이스 설명입니다.
Base MAC Address	(읽기 전용) 디바이스에 있는 첫 번째 포트의 MAC 주소입니다.
Location	필요한 경우 디바이스 위치입니다.
Contact Information	필요한 경우 연락처 정보입니다.
System Up Time	(읽기 전용) 마지막으로 디바이스를 재부팅한 이후로 디바이스가 가동된 기간입니다.

표 23: 전역 매개변수: 날짜 및 시간 매개변수

매개변수	설명
Device Date	디바이스의 날짜 설정입니다. 필드를 클릭하여 날짜를 수정합니다.
Device Time	디바이스의 시간 설정입니다. 필드를 클릭하여 시간을 수정합니다.

표 24: 전역 매개변수: 버전 정보 매개변수

매개변수	설명
Software Version	(읽기 전용) 디바이스에 있는 제품 소프트웨어의 버전입니다.
Hardware Version	(읽기 전용) 디바이스 하드웨어의 버전입니다.

인증서 관리

이 절에서는 DefensePro의 인증서와 APSolute Vision을 사용하여 인증서를 관리하는 방법에 대해 설명합니다.

이 섹션에 포함되는 주제는 다음과 같습니다.

- 인증서, 74페이지
- 키, 75페이지
- 자체 서명된 인증서, 75페이지
- 선택한 디바이스의 인증서 정보 수정, 75페이지
- 인증서 구성, 75페이지
- 기본 인증서 특성 구성, 77페이지
- 인증서 가져오기, 77페이지
- 인증서 내보내기, 78페이지
- 인증서 콘텐츠 표시, 79페이지

인증서

인증서는 디지털로 서명된 지표로서, 서버 또는 사용자를 식별합니다. 일반적으로 전자 키 또는 값의 형식으로 제공됩니다. 디지털 인증서는 개별 비즈니스 또는 조직 공개 키의 인증서를 나타내지만, 보유자가 인증된 권한과 역할을 표시하기 위해 사용할 수도 있습니다. ID를 확인하는 서드파티의 정보도 포함할 수 있습니다. 통신 또는 트랜잭션의 사용자가 요청자인지 확인하기 위해 인증이 필요합니다.

기본 인증서는 다음을 포함합니다.

- 인증서 보유자 ID
- 인증서의 일련 번호
- 인증서 만료 날짜
- 인증서 보유자의 공개 키 사본
- 올바른 기관에서 디지털 인증서를 발행했는지 확인하기 위한 CA(Certificate Authority)의 ID 및 해당 디지털 시그니처

키

키는 인터넷을 통해 전송할 데이터를 암호화하기 위해 전송자가 적용하는 가변 숫자 집합입니다. 일반적으로 공개 및 개인 키 쌍이 사용됩니다. 개인 키는 기밀로 유지되며 소유자가 데이터를 암호화하고 암호를 해독하는 데만 사용됩니다. 공개 키는 광범위하게 배포되며 기밀이 아닙니다. 데이터를 암호화하고 시그니처를 검증하는 데 사용됩니다. 한 개의 키는 전송자가 데이터를 암호화하거나 해석하는 데 사용합니다. 또한 수신자는 이 키를 사용하여 전송자가 보낸 데이터를 인증합니다.

키를 사용하면 인증되지 않은 개인이 데이터 암호를 해독할 수 없습니다. 적절한 키가 있는 경우에만 정보를 쉽게 암호 해독하거나 이해할 수 있습니다. 도난당하거나 복사된 데이터는 암호를 해독하는 데 적합한 키가 없으면 이해할 수가 없게 되므로 위조가 방지됩니다. DefensePro에서는 512, 1024 또는 2048바이트의 키 크기 길이를 지원합니다.

자체 서명된 인증서

자체 서명된 인증서에는 서드파티 검증이 포함되지 않습니다. 보안 WBM(즉, HTTPS 세션)을 사용할 때 DefensePro 디바이스에서는 인증서를 사용하여 식별합니다. 기본적으로 디바이스에는 자체 서명된 Radware SSL 인증서가 있습니다. 고유 자체 서명된 SSL 인증서를 지정할 수도 있습니다.

선택한 디바이스의 인증서 정보 수정

선택한 디바이스의 인증서 정보를 보고 수정할 수 있습니다.

선택한 디바이스의 인증서 정보를 보고 수정하려면

> *Configuration(컨피그레이션)* 관점에서 **Setup(설정) > Global Parameters(전역 매개변수) > Certificates(인증서)**를 선택합니다.
>
> *Certificates(인증서)* 테이블에는 디바이스에 저장된 각 인증서의 정보가 표시됩니다. 여기에서 인증서를 추가, 편집 및 삭제할 수 있습니다. 인증서를 가져오고 내보내며, 인증서 텍스트를 표시할 수도 있습니다.

인증서 구성

WBM(Web Based Management)에 대한 보안 액세스를 위해 자체 서명된 인증서를 생성하거나 수정할 수 있습니다.

새 인증서에 대한 인증서 서명 요청 및 키를 생성할 수도 있습니다.

인증서 또는 키를 생성하거나 수정하려면

1. *Configuration(컨피그레이션)* 관점에서 **Setup(설정) > Global Parameters(전역 매개변수) > Certificates(인증서)**를 선택합니다.
2. 다음 중 하나를 수행합니다.
   - 인증서를 추가하려면 (Add(추가))을 클릭합니다.
   - 인증서를 편집하려면 인증서 이름을 두 번 클릭합니다.
3. 인증서 매개변수를 구성하고 **Submit(제출)**을 클릭합니다.

표 25: 인증서 매개변수

매개변수	설명
Name	키 또는 인증서 이름입니다. **주의:** 인증서 이름을 49자보다 길게 정의하지 마십시오. 그렇게 하면 인증서 테이블이 손상될 수 있습니다.

표 25: 인증서 매개변수(계속)

매개변수	설명
Type	인증 유형입니다. 값: ● 인증서 ● 클라이언트 CA의 인증서[1] ● 인증서 서명 요청 ● Key(키)—*Key(키)*를 선택하면 키 크기와 암호 문구 필드만 사용할 수 있습니다. 기본값: Key(키)
Key Size	키 크기(바이트)입니다. 키 크기가 더 크면 향상된 레벨의 보안이 제공됩니다. Radware에서는 키 크기가 1024 이상인 인증서를 권장합니다. 이 크기의 인증서를 사용하면 디지털 시그니처를 위조하거나 암호화된 메시지를 디코딩하기가 극도로 어려워집니다. 값: 512 Bytes(512바이트), 1024 Bytes(1024바이트), 2048 Bytes(2048바이트) 기본값: 1024 Bytes(1024바이트)
Common Name	조직의 도메인 이름(예: www.radware.com) 또는 IP 주소입니다.
Organization	조직의 이름입니다.
Email Address	인증서에 포함할 이메일 주소입니다.
Key Passphrase	키 암호 문구는 스토리지의 키를 암호화하고 키를 내보내는 데 필요합니다. 개인 키는 PKI 데이터의 가장 민감한 부분이므로 암호 문구로 보호해야 합니다. 암호 문구는 4자 이상이어야 하며 Radware에서는 문자, 숫자 및 기호를 기반으로 하는 암호 문구보다 강력한 암호 문구를 사용하도록 권장합니다.
Verify Key Passphrase	키 암호 문구를 정의한 후 확인을 위해 다시 입력합니다.
Locality	구/군/시의 이름입니다.
State/Province	주/도입니다.
Organization Unit	조직의 부서 또는 유닛입니다.
Country Name	조직 국가입니다.
Certificate Expiration	인증서가 유효한 상태로 유지되는 기간(일)입니다. 값: 1–4,294,967,295(4GB) 기본값: 365

1 – 허용되지 않을 때 이 옵션을 선택하면(사용 중인 인증서 유형에 따라) 디바이스에서 오류 메시지로 경고를 표시합니다.

기본 인증서 특성 구성

인증서 기본값을 사용하여 서명 요청 또는 자체 서명된 인증서를 생성할 때 사용되는 조직의 기본 매개변수를 정의합니다.

기본 특성을 구성하려면 APSolute Vision 서버와 관련 디바이스 사이의 연결에서 SNMPv3을 사용해야 합니다.

기본 인증서 특성을 구성하려면

1. *Configuration(컨피그레이션)* 관점에서 **Setup(설정) > Global Parameters(전역 매개변수) > Certificates(인증서) > Default Attribute(기본 특성)**를 선택합니다.
2. 매개변수를 구성한 다음 **Submit(제출)**을 클릭합니다.

표 26: 기본 인증서 매개변수

매개변수	설명
Common Name	조직의 도메인 이름입니다. 예: www.radware.com.
Locality	구/군/시의 이름입니다.
State/Province	주/도입니다.
Organization	조직의 이름입니다.
Organization Unit	조직의 부서 또는 유닛입니다.
Country Name	조직 국가입니다.
Email Address	인증서 내에 포함할 이메일 주소입니다.

인증서 가져오기

다른 머신에서 키와 인증서를 가져오고 기존 서명 요청에 인증서를 가져와서 프로세스를 완료할 수 있습니다.

키와 인증서는 PEM 형식으로 가져옵니다. 키와 인증서의 PEM 파일이 별개인 경우 동일한 항목 이름으로 해당 파일을 연속적으로 가져와야 합니다.

인증서 또는 키를 가져오려면

1. *Configuration(컨피그레이션)* 관점에서 **Setup(설정) > Global Parameters(전역 매개변수) > Certificates(인증서)**를 선택합니다.
2. 테이블 아래에 있는 **Import(가져오기)** 버튼을 클릭합니다.
3. 매개변수를 구성한 다음 **Submit(제출)**을 클릭합니다.

표 27: 인증서 매개변수 가져오기

매개변수	설명
Entry Name(항목 이름)	가져오기로 생성할 새로운 항목 이름이거나 키 또는 CSR을 덮어쓰거나 완료할 기존 항목 이름입니다.

표 27: 인증서 매개변수 가져오기(계속)

매개변수	설명
Entry Type(항목 유형)	값: • Key(키)—다른 시스템에서 내보내거나 백업에서 키를 가져옵니다. 컨피그레이션을 완료하려면 이 키에 인증서를 가져와야 합니다. • Certificate(인증서)—다른 머신에서 내보내거나 백업에서 인증서를 가져옵니다. 인증서는 일치하는 키나 서명 요청에 가져와야 합니다. • Certificate of Client CA(클라이언트 CA의 인증서)—클라이언트 CA 인증서를 가져옵니다. 기본값: Key(키) **참고:** WBM(Web Based Management)의 DefensePro에서는 세 가지 추가 옵션(중간 CA 인증서, 인증서 및 키, SSH 공개 키)을 지원합니다.
Passphrase(암호 문구) (이 매개변수는 **Entry Type(입력 유형)**이 **Key(키)**인 경우에만 사용할 수 있습니다.)	게인 키는 PKI 데이터의 가장 민감한 부분이므로 암호 문구로 보호해야 합니다. 암호 문구는 4자 이상이어야 하며 Radware에서는 문자, 숫자 및 기호를 기반으로 하는 비밀번호보다 강력한 비밀번호를 사용하도록 권장합니다.
Verify Passphrase(암호 문구 확인) (이 매개변수는 **Entry Type(입력 유형)**이 **Key(키)**인 경우에만 사용할 수 있습니다.)	게인 키는 PKI 데이터의 가장 민감한 부분이므로 암호 문구로 보호해야 합니다. 암호 문구는 4자 이상이어야 하며 Radware에서는 문자, 숫자 및 기호를 기반으로 하는 비밀번호보다 강력한 비밀번호를 사용하도록 권장합니다.
File Name(파일 이름)	가져올 인증서 파일입니다.

인증서 내보내기

키, 인증서 및 서명 요청 내보내기는 백업 용도, 기존 컨피그레이션을 다른 시스템으로 이동 또는 서명 요청 프로세스를 완료하는 데 사용됩니다. 키를 복사하여 붙여넣거나 파일을 다운로드하여 디바이스에서 인증서를 내보낼 수 있습니다. 키와 인증서는 PEM 형식으로 내보냅니다.

참고: Radware 키는 시스템 시작 시 Radware 비밀번호 없이 생성되므로, Radware 비밀번호 없이 내보낼 수 있습니다.

인증서 또는 키를 내보내려면

1. *Configuration(컨피그레이션)* 관점에서 **Setup(설정) > Global Parameters(전역 매개변수) > Certificates(인증서)**를 선택합니다.
2. 테이블 아래에 있는 **Export(내보내기)** 버튼을 클릭합니다.
3. 매개변수를 구성한 다음 **Submit(제출)**을 클릭합니다.

표 28: 인증서 매개변수 내보내기

매개변수	설명
Entry Name	내보낼 항목의 이름을 선택합니다. 기본적으로 인증서 테이블에서 선택한 인증서의 이름이 표시됩니다.
Entry Type	선택한 항목 이름에 따라 인증서, 인증서 체인, 클라이언트 CA 인증서, 키 또는 인증서 서명 요청을 내보낼 수 있습니다.
Passphrase	키를 내보낼 때 필요합니다. 키를 생성하거나 가져올 때 입력한 암호 문구를 사용합니다. 키를 내보내도록 인증되었음을 검증하기 위해 키 암호 문구를 입력해야 합니다.

인증서 콘텐츠 표시

Certificates(인증서) 테이블에 나열된 키, 인증서 또는 서명 요청 콘텐츠를 표시할 수 있습니다. 콘텐츠는 복사하여 붙여넣기(예: 인증서 서명 기관에 서명 요청을 보내기) 위해 암호화된 텍스트로 표시됩니다.

인증서 콘텐츠를 표시하려면

1. *Configuration(컨피그레이션)* 관점에서 **Setup(설정) > Global Parameters(전역 매개변수) > Certificates(인증서)**를 선택합니다.
2. 테이블 아래 **Show(표시)**를 클릭합니다.
3. 표시할 항목 이름을 선택합니다. 기본적으로 인증서 테이블에서 선택한 인증서의 이름이 표시됩니다.
4. 필요한 경우 항목 유형과 키의 비밀번호를 선택합니다.
5. **Show(표시)**를 클릭하여 *Certificate(인증서)* 필드에 콘텐츠를 표시합니다.

DefensePro 디바이스의 라이센스 업그레이드

라이센싱 절차를 사용하여 디바이스 기능을 업그레이드할 수 있습니다.

DefensePro for Cisco Firepower 9300에는 DefensePro 애플리케이션의 라이센스가 필요하지 않지만, 유용한 처리량을 지원하기 위한 *처리량 라이센스*가 필요합니다.

처리량 라이센스를 주문할 때 다음을 포함해야 합니다.

- 디바이스의 MAC 주소 *또는* 디바이스에 구성된 관리 IP 주소(*Configuration(컨피그레이션)* 관점에서 **Setup(설정) > Networking(네트워킹) > IP Management(IP 관리)** 선택).
- 새 라이센스를 사용할 때마다 변경되는 처리량 라이센스 ID.

새로운 처리량 라이센스 키는 이메일로 전송됩니다. *License Upgrade(라이센스 업그레이드)* 창에 새로운 처리량 라이센스를 입력한 후에는 이전 라이센스를 다시 사용할 수 없습니다.

새 처리량 라이센스 키를 받은 후 처리량 라이센스를 업그레이드하려면

1. *Configuration(컨피그레이션)* 관점에서 **Setup(설정) > Global Parameters(전역 매개변수) > License Upgrade(라이센스 업그레이드)**를 선택합니다.
2. 새 라이센스 키에 대한 라이센스 업그레이드 매개변수 구성을 입력한 다음 **Submit(제출)**을 클릭합니다.

표 29: DefensePro 라이센스 업그레이드 매개변수

매개변수	설명
Throughput License Key	디바이스 처리량 라이센스의 키입니다.
Throughput License Method	(읽기 전용) 라이센스를 생성하는 데 사용되는 방법입니다. 값: • IP—라이센스를 생성하기 위해 디바이스의 IP 주소를 사용한 라이센스 생성기입니다. • MAC—라이센스를 생성하기 위해 디바이스의 MAC 주소를 사용한 라이센스 생성기입니다.
IP Address (이 매개변수는 **Throughput License Method(처리량 라이센스 방법)**이 **IP**인 경우에만 사용됩니다.)	(읽기 전용) 디바이스의 IP 주소입니다.
MAC (이 매개변수는 **Throughput License Method(처리량 라이센스 방법)**가 **MAC**인 경우에만 표시됩니다.)	(읽기 전용) 디바이스의 MAC 주소입니다.
Throughput License ID	(읽기 전용) 처리량 라이센스를 생성하는 데 사용한 ID입니다.

DefensePro에서 날짜 및 시간 설정 구성

이 절에서는 기본 DefensePro 날짜 및 시간 설정 구성에 대해 설명하고 DefensePro 일광 절약 구성, 80페이지에 대해서도 설명합니다.

DefensePro for Cisco Firepower 9300에서는 NTP(Network Time Protocol) 동기화를 지원하지 않습니다.

DefensePro for Cisco Firepower 9300은 호스트의 시간 및 날짜와 동기화됩니다.

DefensePro for Cisco Firepower 9300의 시간 또는 날짜를 변경할 수 없습니다. 그러나 일광 절약 시간 매개변수를 설정*할 수 있습니다*. 또한 CLI에서 services ntp time-zone 명령을 사용하여 시간대를 설정할 수 있습니다.

DefensePro 일광 절약 구성

DefensePro에서는 일광 절약 시간을 지원합니다. 일광 절약 시간 시작 및 종료 날짜와 시간을 구성할 수 있습니다. 일광 절약 시간 중에 디바이스에서 자동으로 시스템 시계에 한 시간을 추가합니다. 디바이스에서는 또한 표준 시간을 사용하는지 아니면 일광 절약 시간을 사용하는지 표시합니다.

참고: 시스템 시계를 수동으로 구성한 경우, 일광 절약 시간이 시작하거나 종료할 때에만 시스템 시간이 변경됩니다. 일광 절약 기간 동안 일광 절약 시간을 사용하도록 설정하면 디바이스에서 시스템 시간을 변경하지 않습니다.

DefensePro 일광 절약 구성

1. *Configuration(컨피그레이션)* 관점에서 **Setup(설정) > Global Parameters(전역 매개변수) > Time Settings(시간 설정) > Daylight Saving(일광 절약)**을 선택합니다.
2. 매개변수를 구성한 다음 **Submit(제출)**을 클릭합니다.

표 30: 일광 절약 매개변수

매개변수	설명
Enabled	일광 절약 시간을 사용하거나 사용하지 않도록 설정합니다. 기본값: Disabled(사용 안 함)
Begins at	일광 절약 시간의 시작 날짜 및 시간입니다.
Ends at	일광 절약 시간의 종료 날짜 및 시간입니다.
Current Mode	디바이스에서 표준 시간을 사용할지 아니면 일광 절약 시간을 사용할지 지정합니다.

DefensePro 네트워킹 설정 구성

이 섹션에 포함되는 주제는 다음과 같습니다.

- DefensePro 네트워킹 설정의 기본 매개변수 구성, 81페이지
- 네트워킹 설정에서 IP 인터페이스 관리 구성, 82페이지
- DefensePro 네트워킹 설정을 위한 DNS 구성, 85페이지

DefensePro 네트워킹 설정의 기본 매개변수 구성

Basic(기본) 창을 사용하여 IP 프래그멘테이션 매개변수를 구성합니다.

IPv4 및 IPv6 지원

DefensePro에서는 IPv6 및 IPv4 프로토콜을 지원하고 IPv6/IPv4 패킷을 위한 모든 기능을 갖춘 IPS 및 DoS 방지 솔루션을 제공합니다. 관리는 IPv4에서만 작동합니다.

DefensePro에서는 다음을 포함하여 IPv6 패킷 및 ICMPv6 패킷의 처리를 지원합니다.

- IPv6 주소로 네트워크 설정
- 보안 정책 적용
- 공격 차단
- 보안 보고

IP 단편화

IP 패킷의 길이가 너무 길어 전송할 수 없으면 패킷의 작성자 또는 패킷을 전송하는 라우터 중 하나가 패킷을 여러 개의 짧은 패킷으로 프래그멘테이션해야 합니다.

IP 프래그멘테이션을 사용하면 DefensePro에서 IP 프래그먼트의 레이어 4 정보를 분류할 수 있습니다. 디바이스에서 동일한 데이터그램에 속한 모든 프래그먼트를 식별한 다음 적절하게 분류하여 전달합니다. 디바이스에서는 원본 IP 패킷을 재조립하지는 않지만, 데이터그램이 정리되지 않은 채로 디바이스에 도착해도 프래그먼트 데이터그램을 대상에 전달합니다.

트래픽 제외

*트래픽 제외*는 DefensePro가 디바이스에 구성된 네트워크 정책과 일치하지 않는 모든 트래픽을 통과하는 시기입니다.

DefensePro for Cisco Firepower 9300에서 트래픽 제외 동작은 항상 사용하도록 설정됩니다. 즉, 디바이스는 디바이스에 구성된 네트워크 정책과 일치하지 않는 모든 트래픽을 항상 통과합니다.

기본 네트워킹 매개변수 구성

이 절에서는 기본 네트워킹 매개변수 구성 방법에 대해 설명합니다.

기본 네트워킹 매개변수를 구성하려면

1. *Configuration(컨피그레이션)* 관점에서 **Setup(설정) > Networking(네트워킹) > Basic(기본)**을 선택합니다.
2. 매개변수를 구성한 다음 **Submit(제출)**을 클릭합니다.

표 31: 기본: IP 프래그멘테이션 매개변수

매개변수	설명
Enable IP Fragmentation	IP 프래그멘테이션 사용 여부를 지정합니다.
Queuing Limit	디바이스가 순서에 맞지 않는 프래그먼트 IP 데이터그램에 할당하는 IP 패킷의 백분율입니다. 값: 0–100 기본값: 25
Aging Time	디바이스가 큐에서 프래그먼트 데이터그램을 유지하는 기간(초)입니다. 값: 1-255 기본값: 1

네트워킹 설정에서 IP 인터페이스 관리 구성

DefensePro에서는 레이어 2 인터페이스(포트, 트렁크 및 VLAN)에 정의된 모든 IP 인터페이스 간 라우팅을 수행합니다. 또한 DefensePro에서는 레이어 4와 레이어 7과 같은 다른 네트워크 레이어를 기반으로 라우팅을 수행합니다.

IP 인터페이스를 구성하려면

1. *Configuration(컨피그레이션)* 관점에서 **Setup(설정) > Networking(네트워킹) > IP Management(IP 관리)**를 선택합니다.
2. 다음 중 하나를 수행합니다.
   - IP 인터페이스를 추가하려면 (Add(추가)) 버튼을 클릭합니다.
   - IP 인터페이스를 편집하려면 행을 두 번 클릭합니다.
3. 매개변수를 구성한 다음 **Submit(제출)**을 클릭합니다.

표 32: IP 인터페이스 매개변수

매개변수	설명
IP Address	인터페이스의 IP 주소입니다.
Mask	연관된 서브넷 마스크입니다.
Port	인터페이스 식별자(예: G-1)입니다.

표 32: IP 인터페이스 매개변수(계속)

매개변수	설명
Broadcast Address	브로드캐스트 주소의 호스트 ID를 1 또는 0으로 채울지 지정합니다. 값: ● Fill 1(1로 채우기)—브로드캐스트 주소의 호스트 ID를 1로 채웁니다. ● Fill 0(0으로 채우기)—브로드캐스트 주소의 호스트 ID를 0으로 채웁니다. 기본값: Fill 1(1로 채우기)
VLAN Tag	이 IP 인터페이스와 연결할 VLAN 태그입니다. 여러 VLAN이 동일한 스위치 포트와 연결되는 경우 스위치에서 해당 특정 포트에서 수신되는 트래픽을 직접 연결할 VLAN을 식별해야 합니다. VLAN 태깅에서는 스위치를 통해 올바른 의사결정을 내릴 수 있는 레이어 2 헤더의 지표를 제공합니다.

DefensePro에서 IP 라우팅 구성

이 절에서는 DefensePro의 IP 라우팅에 대해 설명합니다.

DefensePro 디바이스에서는 IP 라우팅 테이블을 사용하여 관리 IP 패킷을 대상에 전달합니다. 이 테이블에서는 대상에 대한 정보와 대상에 도달할 수 있는 방법을 저장합니다. 기본적으로 디바이스에 직접 연결된 모든 네트워크는 IP 라우팅 테이블에 등록됩니다. 기타 항목은 정적으로 구성하거나 라우팅 프로토콜을 통해 동적으로 생성할 수 있습니다.

DefensePro에서 관리할 IP 라우팅을 구성하려면

1. *Configuration(컨피그레이션)* 관점에서 **Setup(설정) > Networking(네트워킹) > IP Routing(IP 라우팅)**을 선택합니다.
2. 다음 중 하나를 수행합니다.
   - 정적 경로를 추가하려면 (Add(추가)) 버튼을 클릭합니다.
   - 정적 경로를 편집하려면 행을 두 번 클릭합니다.
3. 정적 경로 매개변수를 구성한 다음 **Submit(제출)**을 클릭합니다.
4. 전역 고급 매개변수를 구성합니다.
5. **Submit(제출)**를 클릭합니다.

참고

- 정적 경로를 편집할 때 **Metric(메트릭)** 필드만 수정할 수 있습니다.
- **Type(유형)** 필드는 *Static Routes(정적 경로)* 테이블에만 표시됩니다. 구성할 수 없습니다.

표 33: IP 라우팅: 기본(정적 경로) 매개변수

매개변수	설명
Destination Network	경로가 정의되는 대상 네트워크입니다.
Netmask	대상 서브넷의 네트워크 마스크입니다.
Next Hop	대상 서브넷으로 전달되는 다음 홉의 IP 주소입니다. (다음 홉은 항상 디바이스에 대해 로컬인 서브넷에만 있습니다.)

표 33: IP 라우팅: 기본(정적 경로) 매개변수(계속)

매개변수	설명
Via Interface	(읽기 전용) 값 **3**(읽기 전용)입니다. 이 값은 관리 인터페이스의 값입니다.
Type	(읽기 전용) 이 필드는 정적 경로 테이블에만 표시됩니다. 값: ● Local(로컬)—서브넷을 디바이스에서 직접 연결할 수 있습니다. ● Remote(원격)—서브넷을 디바이스에서 직접 연결할 수 없습니다.
Metric	이 경로에 정의되었거나 계산된 메트릭 값입니다.

표 34: IP 라우팅 고급 매개변수

매개변수	설명
Enable Proxy ARP	사용되는 경우 네트워크 호스트에서 수신 인터페이스에 구성되지 않은 네트워크 주소의 ARP 쿼리에 응답합니다. 다른 호스트 대신 프록싱 ARP 요청이 해당 호스트로 향하는 모든 LAN 트래픽을 효과적으로 프록싱 호스트로 연결합니다. 그런 다음 캡처된 트래픽은 다른 인터페이스를 통해 대상 호스트에 라우팅됩니다. 기본값: Enabled(사용)
Enable Sending Trap on ICMP Error	ICMP(Internet Control Message Protocol)는 Internet Protocol Suite의 핵심 프로토콜 중 하나이며, 네트워크된 컴퓨터 운영 체제에서 오류 메시지(예: 요청된 서비스를 사용할 수 없거나 호스트 또는 라우터에 연결할 수 없음)를 전송하는 데 사용합니다. 기본값: Enabled(사용) **참고:** 이 옵션을 사용하도록 설정하면 ICMP 오류 메시지가 있을 때 트랩이 전송됩니다.

ARP 테이블 구성

프록시 ARP가 사용하도록 설정된 경우 네트워크 호스트는 수신 인터페이스에 구성되지 않은 네트워크 주소에 대한 ARP 쿼리에 응답합니다. 다른 호스트 대신 프록싱 ARP 요청이 해당 호스트로 향하는 모든 LAN 트래픽을 효과적으로 프록싱 호스트로 연결합니다. 그런 다음 캡처된 트래픽은 다른 인터페이스를 통해 대상 호스트에 라우팅됩니다.

로컬 라우터에서 정적 ARP 항목을 구성하고 관리할 수 있습니다.

ARP 테이블을 구성하려면

1. *Configuration(컨피그레이션)* 관점에서 **Setup(설정) > Networking(네트워킹) > IP Management(IP 관리) > ARP Table(ARP 테이블)**을 선택합니다.
2. 다음 중 하나를 수행합니다.
   - 새 항목을 추가하려면  (Add(추가)) 버튼을 클릭합니다.
   - 항목을 편집하려면 행을 두 번 클릭합니다.
3. ARP 매개변수를 구성하고 **Submit(제출)**을 클릭합니다.
4. 필요한 경우 고급 매개변수를 수정한 다음 **Submit(제출)**을 클릭합니다.

표 35: ARP: 항목 매개변수

매개변수	설명
Port	스테이션이 있는 인터페이스 번호입니다.
IP Address	스테이션의 IP 주소입니다.
MAC Address	스테이션의 MAC 주소입니다.
Type	항목 유형입니다. 값: ● Other(기타)—정적 또는 동적이 아님. ● Invalid(유효하지 않음)—ARP 항목을 무효화하고 효과적으로 삭제합니다. ● Dynamic(동적)—ARP 프로토콜에서 항목을 학습합니다. 사전 결정된 시간에 항목이 활성화되지 않은 경우 노드가 테이블에서 삭제됩니다. ● Static(정적)—항목이 네트워크 관리 스테이션에서 구성되었으며 영구적입니다.

표 36: ARP: 고급 매개변수

매개변수	설명
Inactive ARP Timeout	디바이스에서 비활성 ARP 캐시 항목을 삭제하기 전에 이러한 항목이 ARP 테이블에 남아 있을 수 있는 시간(초)입니다. 지정된 기간 내에 ARP 캐시 항목을 새로 고치지 않으면 해당 주소에 문제가 있는 것으로 가정합니다. 값: 10-86,400

DefensePro 네트워킹 설정을 위한 DNS 구성

DNS(Domain Name Service) 클라이언트로 작동하도록 DefensePro를 구성할 수 있습니다. DNS 클라이언트를 사용하지 않도록 설정하면 IP 주소를 분석할 수 없습니다. DNS 클라이언트를 사용하도록 설정하면 DefensePro가 호스트 이름 분석을 위해 쿼리를 전송할 서버를 구성해야 합니다.

DNS 매개변수를 설정하고 동적 DNS에 대한 기본 및 대체 DNS 서버를 정의할 수 있습니다. 또한 정적 DNS 매개변수를 설정할 수 있습니다.

DNS 설정을 구성하려면

1. *Configuration(컨피그레이션)* 관점에서 **Setup(설정) > Networking(네트워킹) > DNS**를 선택합니다.
2. 기본 DNS 클라이언트 매개변수를 구성하고 **Submit(제출)**을 클릭합니다.
3. 정적 DNS 항목을 추가 또는 수정하려면 다음 중 하나를 수행합니다.
   - 항목을 추가하려면 (Add(추가)) 버튼을 클릭합니다.
   - 항목을 수정하려면 테이블에서 항목을 두 번 클릭합니다.
4. 매개변수를 구성하고 **Submit(제출)**을 클릭합니다.

표 37: DNS 클라이언트 매개변수

매개변수	설명
DNS 클라이언트	DefensePro 디바이스가 IP 주소를 분석하기 위해 DNS 클라이언트로 작동하는지 지정합니다. 값: Enable(사용), Disable(사용 안 함) 기본값: Disable(사용 안 함)
기본 DNS 서버	DefensePro에서 쿼리를 전송하는 기본 DNS 서버의 IP 주소입니다.
대체 DNS 서버	DefensePro에서 쿼리를 전송하는 대체 DNS의 IP 주소입니다.
정적 DNS 테이블 정적 DNS 호스트입니다. (Add(추가)) 버튼을 클릭하여 새 정적 DNS를 추가합니다. 각 정적 DNS의 컨피그레이션은 다음 매개변수로 구성됩니다. ● Host Name(호스트 이름)—지정된 IP 주소의 도메인 이름 ● IP Address(IP 주소)—지정된 도메인 이름의 IP 주소	

DefensePro 디바이스-보안 설정 구성

이 섹션에 포함되는 주제는 다음과 같습니다.

- DefensePro 디바이스-보안 설정에 맞게 액세스 프로토콜 구성, 86페이지
- DefensePro 디바이스-보안 설정에서 SNMP 구성, 88페이지
- DefensePro 디바이스-보안 설정에서 디바이스 사용자 구성, 96페이지
- DefensePro 디바이스-보안 설정에서 고급 매개변수 구성, 97페이지
- 디바이스 관리를 위한 인증 프로토콜 구성, 98페이지

DefensePro 디바이스-보안 설정에 맞게 액세스 프로토콜 구성

APSolute Vision을 사용하여 DefensePro 디바이스를 관리하는 것 외에도 WBM(Web Based Management) 및 CLI(Command Line Interface)도 사용할 수 있습니다.

DefensePro 디바이스를 다음에 연결할 수 있습니다.

- HTTP 및 HTTPS를 통한 디바이스의 WBM
- 텔넷 및 SSH를 통한 CLI
- 웹 서비스

WBM 및 CLI에 대한 액세스 프로토콜을 구성하려면

1. *Configuration(컨피그레이션)* 관점에서 **Setup(설정) > Device Security(디바이스 보안) > Access Protocols(액세스 프로토콜)**을 선택합니다.
2. 매개변수를 구성한 다음 **Submit(제출)**을 클릭합니다.

표 38: 액세스 프로토콜 웹 액세스 매개변수

매개변수	설명
Enable Web Access	웹 서버에 대한 액세스를 사용하도록 설정할지를 지정합니다. 기본값: Disabled(사용 안 함)
L4 Port	WBM이 할당된 포트입니다. 기본값: 80
Web Help URL	웹 도움말 파일의 위치(경로)입니다.

표 39: 액세스 프로토콜 보안 웹 액세스 매개변수

매개변수	설명
Enable Secured Web Access	웹 서버에 보안 액세스를 사용하도록 설정할지를 지정합니다. 기본값: Disabled(사용 안 함)
L4 Port	HTTPS에서 요청을 수신하는 포트입니다. 기본값: 443
Certificate	암호화를 위해 보안 웹 서버에서 사용되는 인증서 파일입니다.

표 40: 액세스 프로토콜 텔넷 매개변수

매개변수	설명
Enable Telnet	디바이스에 텔넷 액세스를 사용하도록 설정할지를 지정합니다. 기본값: Disabled(사용 안 함)
L4 Port	텔넷에서 사용하는 TCP 포트입니다. 기본값: 23
Session Timeout	비활성 기간 동안 디바이스에서 연결을 유지관리하는 기간(분)입니다. 미리 정의된 기간이 종료되어도 세션이 여전히 비활성이면 세션이 종료됩니다. 값: 1-120 기본값: 5 **참고:** 디바이스 성능에 영향을 미치지 않도록 10초마다 시간 제한을 확인합니다. 따라서 실제 시간 제한은 구성된 시간보다 최대 10초까지 길 수 있습니다.
Authentication Timeout	인증 프로세스를 완료하는 데 필요한 시간 제한(초)입니다. 값: 10-60 기본값: 30

표 41: 액세스 프로토콜 SSH 매개변수

매개변수	설명
Enable SSH	디바이스에 SSH 액세스를 사용하도록 설정할지를 지정합니다. 기본값: Disabled(사용 안 함)
L4 Port	SSH 서버 연결을 위한 소스 포트입니다. 기본값: 22

표 41: 액세스 프로토콜 SSH 매개변수(계속)

매개변수	설명
Session Timeout	비활성 기간 동안 디바이스에서 연결을 유지관리하는 기간(분)입니다. 미리 정의된 기간이 종료되어도 세션이 여전히 비활성이면 세션이 종료됩니다. 값: 1-120 기본값: 5 **참고:** 디바이스 성능에 영향을 미치지 않도록 10초마다 시간 제한을 확인합니다. 따라서 실제 시간 초과는 구성된 시간보다 최대 10초가 길 수 있습니다.
Authentication Timeout	인증 프로세스를 완료하는 데 필요한 시간 제한(초)입니다. 값: 10-60 기본값: 10

표 42: 액세스 프로토콜 웹 서비스 매개변수

매개변수	설명
Enable Web Services	웹 서비스에 대한 액세스를 사용하도록 설정할지를 지정합니다. 기본값: Enabled(사용)

DefensePro 디바이스-보안 설정에서 SNMP 구성

SNMP(Simple Network Management Protocol)는 APSolute Vision과 네트워크 디바이스 사이에 관리 정보를 쉽게 교환할 수 있는 애플리케이션 레이어 프로토콜입니다.

Radware 디바이스는 모든 SNMP 버전(SNMPv1, SNMPv2c 및 SNMPv3)에서 작동할 수 있습니다. 기본

Radware 사용자는 SNMPv1에서 구성됩니다.

주의: APSolute Vision에서는 SNMPv2c 트랩을 지원하지 않습니다. APSolute Vision에 도착하는 SNMPv2c 트랩은 폐기합니다.

참고: SNMPv3을 사용하여 Radware 디바이스를 APSolute Vision에 추가할 때 사용자 이름과 인증 세부 정보가 디바이스에 구성된 사용자 중 하나와 일치해야 합니다.

다음 주제에서는 선택한 디바이스에 SNMP를 구성하는 절차에 대해 설명합니다.

- DefensePro SNMP 사용자 구성, 89페이지
- SNMP 커뮤니티 설정 구성, 90페이지
- SNMP 그룹 테이블 구성, 91페이지
- SNMP 액세스 설정 구성, 60페이지
- SNMP 알림 설정 구성, 92페이지
- SNMP 보기 설정 구성, 93페이지
- SNMP 대상 매개변수 테이블 구성, 93페이지
- SNMP 대상 주소 구성, 94페이지
- SNMP 지원 버전 구성, 95페이지

DefensePro SNMP 사용자 구성

SNMPv3 사용자 기반 관리에서 각 사용자는 사용자 이름과 인증 방법을 기반으로 여러 가지 권한을 갖을 수 있습니다. 디바이스에 연결할 수 있는 사용자를 정의하고 각 SNMP 사용자의 액세스 매개변수를 저장합니다.

참고: SNMP 컨피그레이션에서 사용자 이름은 보안 이름이라고도 합니다.

인증 및 개인정보를 사용하여 SNMPv3과 연결된 디바이스에 대해 SNMP 사용자를 구성하려면

1. *Configuration(컨피그레이션)* 관점에서 **Setup(설정) > Device Security(디바이스 보안) > SNMP > SNMP User Table(SNMP 사용자 테이블)**을 선택합니다.
2. 다음 중 하나를 수행합니다.
   - 사용자를 추가하려면 (Add(추가))을 클릭합니다.
   - 항목을 편집하려면 행을 두 번 클릭합니다.
3. SNMP 사용자 매개변수를 구성하고 **Submit(제출)**을 클릭합니다.

표 43: SNMP 사용자 매개변수

매개변수	설명
사용자 이름	사용자 이름이며 보안 이름이라고도 합니다. 이름은 최대 18자일 수 있습니다.
인증 프로토콜	인증 프로세스 중에 사용된 프로토콜입니다. 값: ● None ● MD5 ● SSH 기본값: None(없음)
인증 비밀번호	인증 프로토콜이 지정된 경우 인증 비밀번호를 입력합니다.
프라이버시 프로토콜	암호화에 사용된 알고리즘입니다. 값: ● None(없음) — 데이터가 암호화되지 않습니다. ● DES—디바이스에서 데이터 암호화 표준을 사용합니다. 기본값: None(없음)
개인정보 비밀번호	개인정보 프로토콜이 지정된 경우 사용자 개인정보 비밀번호를 입력합니다.

SNMP 커뮤니티 설정 구성

SNMP 커뮤니티 테이블은 커뮤니티 문자열을 사용자와 연결하기 위해 SNMP 버전 1과 2에서만 사용합니다. SNMPv1 또는 SNMPv2로 사용자를 디바이스에 연결하면 디바이스에서 SNMP 패킷에 보낸 커뮤니티 문자열을 확인합니다. 특정 커뮤니티 문자열을 기반으로 디바이스에서는 커뮤니티 문자열을 특정 액세스 권한이 있는 그룹에 속한 미리 정의된 사용자에게 매핑합니다.
따라서 SNMPv1 또는 SNMPv2를 사용하여 작업할 때 사용자, 그룹 및 액세스를 정의해야 합니다.

*커뮤니티 테이블*을 사용하여 사용자 이름과 커뮤니티 문자열을 연결(그 반대도 마찬가지)하고 SNMP 요청을 승인하고 트랩을 전송할 수 있는 주소 범위를 제한합니다.

참고: 현재 사용 중인 사용자 이름과 연결된 커뮤니티 문자열을 변경할 수 없습니다.

SNMP 커뮤니티 설정을 구성하려면

1. *Configuration(컨피그레이션)* 관점에서 **Setup(설정) > Device Security(디바이스 보안) > SNMP > Community(커뮤니티)**를 선택합니다.
2. 다음 중 하나를 수행합니다.
   - SNMP 커뮤니티 항목을 추가하려면 (Add(추가))을 클릭합니다.
   - 항목을 편집하려면 행을 두 번 클릭합니다.
3. SNMP 사용자 매개변수를 구성하고 **Submit(제출)**을 클릭합니다.

표 44: SNMP 커뮤니티 매개변수

매개변수	설명
Index	이 항목을 설명하는 이름입니다. 이 이름을 생성한 후에는 수정할 수 없습니다. 기본값: public(공개)
Community Name	커뮤니티 문자열입니다. 기본값: public(공개)
Security Name	보안 이름을 통해 알림을 생성할 때 사용되는 SNMP 커뮤니티를 식별합니다. 기본값: public(공개)
Transport Tag	SNMP에서 SNMP 요청을 승인하고 트랩을 전송할 수 있는 대상 주소 집합을 지정합니다. 이 태그로 식별한 대상 주소는 SNMP 대상 주소 테이블에 정의됩니다. SNMP 대상 주소 테이블의 하나 이상의 항목에는 지정된 전송 태그를 포함해야 합니다. 태그가 지정되지 않은 경우 SNMP 요청을 수신하거나 트랩을 전송할 때 주소를 확인하지 않습니다.

SNMP 그룹 테이블 구성

SNMPv3 권한은 사용자 그룹에 대해 정의됩니다. 연결 방법에 따라 동일한 사용자에게 다른 권한을 부여해야 하는 경우 사용자를 두 개 이상의 그룹에 연결할 수 있습니다. 다른 사용자와 보안 모델에 대해 그룹 이름이 동일한 여러 항목을 생성할 수 있습니다.

액세스 권한은 *SNMP 액세스* 테이블에서 사용자 그룹에 대해 정의됩니다.

SNMP 그룹 설정을 구성하려면

1. *Configuration(컨피그레이션)* 관점에서 **Setup(설정) > Device Security(디바이스 보안) > SNMP > Group Table(그룹 테이블)**을 선택합니다.
2. 다음 중 하나를 수행합니다.
   - 그룹 항목을 추가하려면 (Add(추가))을 클릭합니다.
   - 항목을 편집하려면 행을 두 번 클릭합니다.
3. 매개변수를 구성한 다음 **Submit(제출)**을 클릭합니다.

표 45: SNMP 그룹 매개변수

매개변수	설명
Group Name	SNMP 그룹의 이름입니다.
Security Model	필수 **보안 모델**을 나타내는 SNMP 버전입니다. 보안 모델은 그룹에서 사용할 수 있는 미리 정의된 권한 집합입니다. 이러한 집합은 SNMP 버전에 따라 정의됩니다. 이 매개변수의 SNMP 버전을 선택하여 사용할 권한 집합을 결정합니다. 값: ● SNMPv1 ● SNMPv2c ● 사용자 기반(SNMPv3) 기본값: SNMPv1
Security Name	사용자 기반 보안 모델을 사용하는 경우, 보안 이름을 통해 알림을 생성할 때 사용되는 사용자를 식별합니다. 기타 보안 모델의 경우 보안 이름을 통해 알림을 생성할 때 사용되는 SNMP 커뮤니티를 식별합니다.

SNMP 액세스 설정 구성

SNMP 액세스 테이블은 그룹과 보안 모델을 SNMP 보기와 바인드합니다. 이 보기에서 MIB 개체의 하위 집합을 정의합니다. 각 그룹과 보안 모델에 대해 액세스 가능한 MIB 개체를 정의할 수 있습니다. **읽기 보기 이름**, **쓰기 보기 이름** 및 **알림 보기 이름** 매개변수를 기반으로 읽기, 쓰기 또는 알림 조치를 수행하기 위해 MIB 개체에 액세스할 수 있습니다.

SNMP 액세스 설정 구성

1. *Configuration(컨피그레이션)* 관점에서 **Setup(설정) > Device Security(디바이스 보안) > SNMP > Access(액세스)**를 선택합니다.
2. 다음 중 하나를 수행합니다.
   - 액세스 항목을 추가하려면 (Add(추가))을 클릭합니다.
   - 항목을 편집하려면 행을 두 번 클릭합니다.
3. SNMP 액세스 매개변수를 구성하고 **Submit(제출)**을 클릭합니다.

표 46: SNMP 액세스 매개변수

매개변수	설명
Group Name	그룹의 이름
Security Model	보안 모델은 그룹에서 사용할 수 있는 미리 정의된 권한 집합입니다. 이러한 집합은 SNMP 버전에 따라 정의됩니다. 필수 보안 모델을 나타내는 SNMP 버전을 선택하여 사용할 권한 집합을 판별합니다. 값: ● SNMPv1 ● SNMPv2c ● 사용자 기반—즉, SNMPv3 기본값: SNMPv1
Security Level	액세스하는 데 필요한 보안 레벨입니다. 값: ● No Authentication(인증하지 않음)—인증 또는 개인정보가 필요하지 않습니다. ● Authentication & No Privacy(인증 필요 및 개인정보 없음)—인증이 필요하지만 개인정보는 필요하지 않습니다. ● Authentication & Privacy(인증 및 개인정보)—인증과 개인정보가 모두 필요합니다. 기본값: No Authentication(인증하지 않음)
Read View Name	이 그룹에서 읽을 수 있는 MIB 트리의 개체를 지정하는 보기의 이름입니다.
Write View Name	이 그룹에서 쓸 수 있는 MIB 트리의 개체를 지정하는 보기의 이름입니다.
Notify View Name	이 그룹에서 알림(트랩)으로 액세스할 수 있는 MIB의 개체를 지정하는 보기 이름입니다.

SNMP 알림 설정 구성

알림을 받을 관리 대상과 선택된 각 관리 대상에 보낼 알림의 유형을 선택할 수 있습니다. 태그 매개변수를 통해 대상 주소 집합을 식별합니다. Notify(알림) 테이블에 지정된 태그를 포함하는 *Target Address(대상 주소)* 테이블의 항목에서 알림을 수신합니다.

SNMP 알림 설정을 구성하려면

1. *Configuration(컨피그레이션)* 관점에서 **Setup(설정) > Device Security(디바이스 보안) > SNMP > Notify(알림)**를 선택합니다.
2. 다음 중 하나를 수행합니다.
   - SNMP 알림 항목을 추가하려면 (Add(추가))을 클릭합니다.
   - 항목을 편집하려면 행을 두 번 클릭합니다.
3. SNMP 알림 매개변수를 구성하고 **Submit(제출)**을 클릭합니다.

표 47: SNMP 알림 매개변수

매개변수	설명
Name	이 항목을 설명하는 이름입니다(예: 알림 유형).
Tag	이 알림을 보낸 대상 주소를 정의하는 문자열입니다. 태그 목록에 이 태그가 있는 모든 대상 주소에 이 알림을 전송합니다.

SNMP 보기 설정 구성

액세스 테이블에 사용할 MIB 트리의 하위 집합을 정의할 수 있습니다. 다른 항목의 이름이 같을 수 있습니다. 이름이 같은 모든 항목의 연합은 MIB 트리의 하위 집합을 정의하며 해당 이름을 통해 액세스 테이블에서 참조할 수 있습니다.

SNMP 보기 설정을 구성하려면

1. *Configuration(컨피그레이션)* 관점에서 **Setup(설정) > Device Security(디바이스 보안) > SNMP > View(보기)**를 선택합니다.
2. 다음 중 하나를 수행합니다.
   - SNMP 보기 항목을 추가하려면 (Add(추가))을 클릭합니다.
   - 항목을 편집하려면 행을 두 번 클릭합니다.
3. SNMP 보기 매개변수를 구성하고 **Submit(제출)**을 클릭합니다.

표 48: SNMP 보기 매개변수

매개변수	설명
View Name	이 항목의 이름입니다.
Sub-Tree	MIB 하위 트리의 개체 ID입니다.
Type	항목에 정의된 개체가 MIB 보기에 포함되는지 아니면 제외되는지 지정합니다. 값: Included(포함됨), Excluded(제외됨) 기본값: Included(포함됨)

SNMP 대상 매개변수 테이블 구성

대상 매개변수 테이블에서 특정 관리 대상에 알림을 전송할 때 사용되는 메시지 처리 및 보안 매개변수를 정의합니다. 대상 매개변수 테이블의 항목은 대상 주소 테이블에서 참조됩니다.

SNMP 대상 매개변수를 구성하려면

1. *Configuration(컨피그레이션)* 관점에서 **Setup(설정) > Device Security(디바이스 보안) > SNMP > Target Parameters Table(대상 매개변수 테이블)**을 선택합니다.
2. 다음 중 하나를 수행합니다.
   - 대상 매개변수 항목을 추가하려면 (Add(추가))을 클릭합니다.
   - 항목을 편집하려면 행을 두 번 클릭합니다.
3. 대상 매개변수 설정을 구성하고 **Submit(제출)**을 클릭합니다.

표 49: SNMP 대상 매개변수

매개변수	설명
Name	대상 매개변수 항목의 이름입니다. 최대 문자 수: 32
Message Processing Model	SNMP 알림을 생성할 때 사용할 SNMP 버전입니다. 값: SNMPv1, SNMPv2c, SNMPv3 기본값: SNMPv1 **주의:** APSolute Vision에서는 SNMPv2c 트랩을 지원하지 않습니다. APSolute Vision에 도착하는 SNMPv2c 트랩은 폐기합니다.
Security Model	필수 보안 모델을 나타내는 SNMP 버전입니다. 보안 모델은 그룹에서 사용할 수 있는 미리 정의된 권한 집합입니다. 이러한 집합은 SNMP 버전에 따라 정의됩니다. 이 매개변수의 SNMP 버전을 선택하여 사용할 권한 집합을 결정합니다. 값: ● SNMPv1 ● SNMPv2c ● 사용자 기반—즉, SNMPv3 기본값: SNMPv1 **주의:** APSolute Vision에서는 SNMPv2c 트랩을 지원하지 않습니다. APSolute Vision에 도착하는 SNMPv2c 트랩은 폐기합니다.
Security Name	사용자 기반 보안 모델을 사용하는 경우, 보안 이름을 통해 알림을 생성할 때 사용되는 사용자를 식별합니다. 기타 보안 모델의 경우 보안 이름을 통해 알림을 생성할 때 사용되는 SNMP 커뮤니티를 식별합니다.
Security Level	트랩을 전송하기 전에 인증하고 암호화할지 지정합니다. 값: ● No Authentication(인증하지 않음)—인증 또는 개인정보가 필요하지 않습니다. ● 인증 필수 및 개인정보 없음—인증이 필요하지만 개인정보는 필요하지 않습니다. ● 인증 및 개인정보—인증과 개인정보가 모두 필요합니다. 기본값: No Authentication(인증하지 않음)

SNMP 대상 주소 구성

SNMPv3에서 대상 주소 테이블에는 트랩을 생성할 때 사용할 전송 주소가 포함됩니다. 항목의 태그 목록에 SNMP 알림 테이블의 태그가 포함된 경우 알림을 수신하도록 이 대상을 선택합니다. SNMP 버전 1 및 2의 경우 이 테이블을 사용하여 SNMP 요청을 승인하고 SNMP 트랩을 전송할 주소 범위를 제한합니다. 커뮤니티 테이블에 있는 항목의 전송 태그가 비어 있지 않으면 대상 주소 테이블에 있는 하나 이상의 항목에 포함되어야 합니다.

SNMP 대상 주소를 구성하려면

1. *Configuration(컨피그레이션)* 관점에서 **Setup(설정) > Device Security(디바이스 보안) > SNMP > Target Address(대상 주소)**를 선택합니다.
2. 다음 중 하나를 수행합니다.
   - 대상 주소를 추가하려면 (Add(추가))을 클릭합니다.
   - 항목을 편집하려면 행을 두 번 클릭합니다.
3. 대상 주소 매개변수를 구성하고 **Submit(제출)**을 클릭합니다.

표 50: SNMP 대상 주소 매개변수

매개변수	설명
Name	대상 주소 항목의 이름입니다.
IP Address and L4 Port [Ip-port number]	SNMP 트랩의 대상으로 사용할 TCP 포트와 관리 스테이션(APSolute Vision 서버)의 IP 주소입니다. 값의 형식은 <IP address >-<TCP port>입니다. 여기서 <TCP port>는 162여야 합니다. 예를 들어, **IP Address and L4 Port(IP 주소 및 L4 포트)**의 값은 1.2.3.4-162입니다. 여기서 1.2.3.4는 APSolute Vision 서버의 IP 주소이며 162는 SNMP 트랩의 포트 번호입니다. **참고:** APSolute Vision에서는 162 포트에서만 트랩을 수신합니다.
Mask	관리 스테이션의 서브넷 마스크입니다.
Tag List	대상 주소의 집합을 지정합니다. 태그는 공백으로 구분합니다. 목록에 포함된 태그는 알림 테이블의 태그이거나 커뮤니티 테이블의 전송 태그일 수 있습니다. 각 태그는 두 개 이상의 태그 목록에 표시될 수 있습니다. 네트워크 디바이스에서 중요한 이벤트가 발생하면 태그 목록을 통해 알림을 전송할 대상을 식별합니다. 기본값: v3Traps
Target Parameters Name	SNMP 트랩을 전송할 때 사용할 대상 매개변수 집합입니다. 대상 매개변수는 대상 매개변수 테이블에 정의되어 있습니다.

SNMP 지원 버전 구성

SNMP 지원 버전을 구성하려면

1. *Configuration(컨피그레이션)* 관점에서 **Setup(설정) > Device Security(디바이스 보안) > SNMP > SNMP Versions(SNMP 버전)**를 선택합니다.
2. 매개변수를 구성한 다음 **Submit(제출)**을 클릭합니다.

표 51: SNMP 지원 버전 매개변수

매개변수	설명
Supported SNMP Versions	현재 지원되는 SNMP 버전입니다.
Supported SNMP Versions after Reset	디바이스를 재설정한 후 SNMP 에이전트에서 지원하는 SNMP 버전입니다. 지원할 SNMP 버전을 선택합니다. 지원되지 않는 버전의 선택을 취소합니다.

DefensePro 디바이스-보안 설정에서 디바이스 사용자 구성

각 디바이스에 대해 지원되는 액세스 방법(웹, 텔넷, SSH, SWBM)을 통해 해당 디바이스에 액세스하도록 승인된 사용자 목록을 구성할 수 있습니다. 컨피그레이션 추적을 사용하도록 설정하는 경우 사용자가 디바이스 변경사항에 대한 이메일 알림을 수신할 수 있습니다.

선택한 디바이스에 대한 디바이스 사용자를 구성하려면

1. *Configuration(컨피그레이션)* 관점에서 **Setup(설정) > Device Security(디바이스 보안) > User Table(사용자 테이블)**을 선택합니다.
2. 다음 중 하나를 수행합니다.
   - 사용자를 추가하려면 (Add(추가)) 버튼을 클릭합니다.
   - 항목을 편집하려면 행을 두 번 클릭합니다.
3. 매개변수를 구성한 다음 **Submit(제출)**을 클릭합니다.

표 52: 디바이스 사용자 매개변수

매개변수	설명
User Name	사용자의 이름입니다.
Password	사용자의 비밀번호입니다. 그런 다음 확인을 반복합니다.
Email Address	알림이 전송될 사용자의 이메일 주소입니다.
Minimal Severity for Sending Traps	이 사용자에게 전송되는 트랩의 최소 심각도 레벨입니다. 값: ● None(없음)—사용자가 트랩을 수신하지 않습니다. ● Info(정보)—심각도가 정보 이상인 트랩을 수신합니다. ● Warning(경고)—사용자가 경고, 오류 및 치명적 트랩을 수신합니다. ● Error(오류)—사용자가 오류 및 치명적 트랩을 수신합니다. ● Fatal(치명적)—사용자가 치명적 트랩만 수신합니다. 기본값: None(없음)
Enable Configuration Tracing	선택하면, 지정된 사용자가 디바이스에서 변경한 컨피그레이션에 대한 알림을 수신합니다. 구성 가능한 변수 값이 변경될 때마다 동일한 MIB 항목의 모든 변수에 대한 정보가 지정된 사용자에게 보고됩니다. 버퍼가 가득 차거나 60초의 시간 제한이 만료되면 디바이스에서 보고서를 수집하여 단일 알림 메시지로 전송합니다. 알림 메시지는 다음 세부 정보를 포함합니다. ● 변경된 MIB 변수의 이름. ● 변수의 새 값. ● 컨피그레이션 변경 시간. ● 사용된 컨피그레이션 툴(APSolute Vision, 텔넷, SSH, WBM). ● 적용 가능한 경우 사용자 이름.
Access Level	WBM 및 CLI에 대한 사용자 액세스 레벨. 기본값: Read-Write(읽기-쓰기)

디바이스 사용자에 대한 고급 매개변수를 구성하려면

1. *Configuration(컨피그레이션)* 관점에서 **Setup(설정) > Device Security(디바이스 보안) > User Table(사용자 테이블)**을 선택합니다.
2. *Advanced Parameters(고급 매개변수)* 탭에서 매개변수를 구성한 다음 **Submit(제출)**을 클릭합니다.

표 53: 디바이스 사용자에 대한 고급 매개변수

매개변수	설명
Authentication Mode	디바이스에 대한 사용자 액세스를 인증하기 위한 방법입니다. 값: • Local User Table(로컬 사용자 테이블)—디바이스에서 사용자 테이블을 사용하여 액세스를 인증합니다. • RADIUS and Local User Table(RADIUS 및 로컬 사용자 테이블)—디바이스에서 RADIUS 서버를 사용하여 액세스를 인증합니다. RADIUS 서버에 대한 요청 시간 초과되는 경우 디바이스에서 사용자 테이블을 사용하여 액세스를 인증합니다. 기본: Local User Table(로컬 사용자 테이블)

DefensePro 디바이스-보안 설정에서 고급 매개변수 구성

디바이스에 대한 액세스를 지정된 물리적 인터페이스로 제한할 수 있습니다. 디바이스 자체에 직접 연결된 일부 또는 모든 관리 트래픽을 폐기하도록 비보안 네트워크 세그먼트에 연결된 인터페이스를 구성할 수 있습니다. 관리자가 디바이스에 대한 특정 유형의 관리 트래픽(예: SSH)은 허용하지만 SNMP와 같은 다른 트래픽 유형은 거부할 수 있습니다. 침입자가 사용되지 않도록 설정된 포트를 통해 디바이스에 액세스하려고 하면 디바이스에서 액세스를 거부하고 시스템 로그와 CLI 트랩을 알림으로 생성합니다.

선택한 디바이스의 액세스 권한을 구성하려면

1. *Configuration(컨피그레이션)* 관점에서 **Setup(설정) > Device Security(디바이스 보안) > Advanced(고급)**를 선택합니다.
2. 포트에 대한 권한을 편집하려면 관련 행을 두 번 클릭합니다.
3. 확인란을 선택하거나 선택을 취소하여 액세스를 허용하거나 거부한 다음 **Submit(제출)**을 클릭합니다.

표 54: 포트 권한 매개변수

매개변수	설명
Port	(읽기 전용) 물리적 포트의 이름입니다.
SNMP Access	선택한 경우 SNMP를 사용하여 포트에 대한 액세스를 허용합니다.
Telnet Access	선택한 경우 텔넷을 사용하여 포트에 대한 액세스를 허용합니다.
SSH Access	선택한 경우 SSH를 사용하여 포트에 대한 액세스를 허용합니다.
Web Access	선택한 경우 WBM을 사용하여 포트에 대한 액세스를 허용합니다.
SSL Access	선택한 경우 SSL을 사용하여 포트에 대한 액세스를 허용합니다.

포트 Ping 구성

Ping할 수 있는 물리적 인터페이스를 정의할 수 있습니다. Ping이 허용되지 않는 인터페이스에 Ping을 전송하면 패킷이 폐기됩니다. 기본적으로 디바이스의 모든 인터페이스에서 Ping을 허용합니다.

Ping할 포트를 정의하려면

1. *Configuration(컨피그레이션)* 관점에서 **Setup(설정) > Device Security(디바이스 보안) > Advanced(고급) > Ping Ports(포트 Ping)**를 선택합니다.
2. 포트 Ping 설정을 편집하려면 관련 행을 두 번 클릭합니다.
3. 확인란을 선택하거나 선택을 취소하여 Ping을 허용하거나 허용하지 않은 다음 **Submit(제출)**을 클릭합니다.

디바이스 관리를 위한 인증 프로토콜 구성

이 절은 다음으로 구성됩니다.

- 디바이스 관리를 위한 RADIUS 인증 구성, 98페이지

디바이스 관리를 위한 RADIUS 인증 구성

DefensePro에서는 관리 용도로 디바이스에 액세스하는 사용자를 인증하여 추가 보안을 제공합니다. RADIUS 인증으로 사용자가 CLI, 텔넷, SSH 또는 웹 기반 관리를 사용하여 디바이스 관리에 액세스하도록 허용할지를 결정하는 데 RADIUS 서버를 사용할 수 있습니다. RADIUS 서버를 사용할 수 없을 경우 디바이스 로컬 사용자 테이블을 사용할지 선택할 수도 있습니다.

DefensePro는 디바이스 관리를 위한 RADIUS 인증을 사용하여 액세스 승인 응답에서 서비스 유형 특성(AVP 6)(모든 RADIUS 서버에 기본으로 제공되는)을 검색합니다. 읽기 쓰기(관리자) 사용자 권한은 모든 RADIUS 서버(서비스 유형 값 6)에 기본 제공됩니다. 읽기 전용 사용자 권한은 서비스 유형 값 7에 제공되며 RADIUS 사전에 정의되어 있어야 합니다.

참고

- 기본 **Authentication Mode(인증 모드)**는 RADIUS가 *없는* **Local User Table(로컬 사용자 테이블)**입니다. 컨피그레이션을 수정하려면 *Configuration(컨피그레이션)* 관점의 *Device Security(디바이스 보안)* 탭 이동 창에서 **Users Table(사용자 테이블)**을 선택합니다. 그런 다음 *Advanced Parameters(고급 매개변수)* 탭의 *Authentication Mode(인증 모드)* 드롭다운 목록에서 필요한 옵션을 선택하고 **Submit(제출)**을 클릭합니다.
- DefensePro 디바이스는 RADIUS 서버에 대한 액세스 권한이 있어야 하며 디바이스 액세스를 허용해야 합니다.

디바이스 관리를 위한 RADIUS 인증을 구성하려면

1. *Configuration(컨피그레이션)* 관점에서 **Setup(설정) > Device Security(디바이스 보안) > Authentication Protocols(인증 프로토콜) > RADIUS Authentication(RADIUS 인증)**을 선택합니다.
2. 매니지드 Radware 디바이스에 대한 RADIUS 인증 매개변수를 구성한 다음 **Submit(제출)**을 클릭합니다.

표 55: RADIUS 인증: 일반 매개변수

매개변수	설명
Timeout	재시도하기 전에 또는 재시도 값이 초과된 경우에는 디바이스에서 서버가 오프라인임을 확인하기 전에 디바이스에서 RADIUS 서버의 응답을 기다리는 기간입니다. 기본값: 1

표 55: RADIUS 인증: 일반 매개변수(계속)

매개변수	설명
Retries	RADIUS 서버가 첫 번째 연결 시도에 응답하지 않은 후 RADIUS 서버에 연결을 재시도하는 횟수입니다. 지정된 재시도 횟수 후에 모든 연결 시도에 실패하면(시간 초과) 백업 RADIUS 서버가 사용됩니다. 기본값: 2
Client Lifetime	클라이언트 인증 기간(초)입니다. 클라이언트가 라이프타임 중에 다시 로그인하면 DefensePro에서 RADIUS 서버로 클라이언트를 다시 인증하지 않습니다. 클라이언트가 라이프타임이 만료된 후에 다시 로그인하면 DefensePro에서 클라이언트를 다시 인증합니다. 기본값: 30

표 56: RADIUS 인증: 기본 매개변수

매개변수	설명
L4 Port	기본 RADIUS 서버의 액세스 포트 번호입니다. 값: 1645, 1812 기본값: 1645
Secret	기본 RADIUS 서버의 인증 비밀번호입니다. 최대 문자 수: 64 **참고:** DefensePro에서 암호를 저장하면 암호화됩니다. 따라서 컨피그레이션 파일의 암호 길이는 사용자가 구성한 문자 수보다 깁니다.
Verify Secret	비밀번호를 정의할 때 확인을 위해 다시 입력합니다.
Server IP Address Type	값: IPv4, IPv6
Server IP Address	기본 RADIUS 서버의 IP 주소입니다.

표 57: RADIUS 인증: 백업 매개변수

매개변수	설명
L4 Port	백업 RADIUS 서버의 액세스 포트 번호입니다. 값: 1645, 1812 기본값: 1645
Secret	백업 RADIUS 서버의 인증 비밀번호입니다. 최대 문자 수: 64 **참고:** DefensePro에서 암호를 저장하면 암호화됩니다. 따라서 컨피그레이션 파일의 암호 길이는 사용자가 구성한 문자 수보다 깁니다.
Verify Secret	비밀번호를 정의할 때 확인을 위해 다시 입력합니다.
Server IP Address Type	값: IPv4, IPv6
Server IP Address	백업 RADIUS 서버의 IP 주소입니다.

DefensePro 보안-설정 설정 구성

서버 보호 정책 또는 네트워크 보호 정책 및 해당 보호 프로필을 구성하기 전에 사용할 보호 기능을 사용하도록 설정하고 보호 기능에 대한 전역 매개변수를 구성해야 합니다.

참고: 디바이스에서 보호 기능을 사용하도록 설정한 후 디바이스를 재부팅해야 합니다. 그러나 동일한 탐색 브랜치에서 기능을 사용하도록 설정한 경우 한 번만 재부팅하면 됩니다.

이 섹션에 포함되는 주제는 다음과 같습니다.

- DoS 실드 보호 구성, 100페이지
- 글로벌 동작 기반 DoS 보호 구성, 102페이지
- 글로벌 SYN 플러드 보호 구성, 107페이지
- 글로벌 패킷 이상 보호 구성, 107페이지
- 글로벌 DNS 플러드 보호 구성, 110페이지

DoS 실드 보호 구성

DoS 실드 메커니즘은 서비스 거부 효과를 초래하여 의도한 사용자에게 컴퓨터 리소스를 제공하지 못하게 할 수 있는 알려진 플러드 공격과 플러드 공격 툴로부터 보호해 줍니다.

참고

- 기본적으로 DoS 실드 보호는 사용하도록 설정됩니다.
- 이 기능은 관리 인터페이스에서도 지원됩니다.

DoS 실드 프로필은 다음을 방지합니다.

- 알려진 TCP, UDP 및 ICMP 플러드
- 인터넷에서 사용 가능한 알려진 공격 툴
- 자동화된 공격인 Bots를 통해 생성되는 알려진 플러드

DoS 실드 보호에서는 *Radware Signatures* 데이터베이스의 시그니처를 사용합니다. 이 데이터베이스는 계속 업데이트되며 알려진 모든 위협으로부터 보호됩니다.

Radware Signature 프로필에는 이미 DoS 실드 보호를 포함하는 Radware 미리 정의된 프로필과 시그니처 데이터베이스의 일부로 모든 DoS 실드 시그니처가 포함되어 있습니다. DoS 실드 보호를 포함하는 프로필을 생성하려면 *Threat Type(위협 유형)* 특성을 **Floods(플러드)**로 설정하여 프로필을 구성합니다.

Radware에서는 알려진 모든 DoS 공격으로부터 보호를 제공하는 미리 정의된 프로필인 *All-DoS-Shield* 프로필도 제공합니다. *All-DoS-Shield* 프로필은 DoS 전용 솔루션이 필요할 때 적용됩니다. DoS 실드 Radware 정의 프로필을 적용하는 경우 동일한 보안 정책에 다른 시그니처 프로필을 적용할 수 없습니다.

서비스 거부를 방지하기 위해 DoS 실드에서는 디바이스를 통한 트래픽 흐름을 샘플링하고 미리 정의된 조치를 통해 DoS 공격으로 인식되는 트래픽의 대역폭을 제한합니다.

대부분의 네트워크에서는 무시해도 좋은 양의 대역폭을 사용하는 산발적 공격은 용인할 수 있습니다. 이러한 공격에는 대응 조치가 필요하지 않습니다. 공격이 대량의 네트워크 대역폭을 사용하기 시작하면 네트워크에 위협이 됩니다. DoS 실드에서는 성능을 최적화하기 위해 고급 샘플링 알고리즘을 사용하여 이러한 이벤트를 탐지하고 자동으로 대응하여 문제를 해결합니다.

DoS 실드에서는 다음과 같은 두 가지 보호 상태를 고려합니다.

- **Dormant state(휴면 상태)**—적극적으로 개입하기 전에 샘플링 메커니즘을 사용하여 인식함을 표시합니다. 휴면 상태의 보호는 네트워크에 입력되는 패킷 수가 미리 정의된 한계를 초과하는 경우에만 활성화됩니다.
- **Active state(활성 상태)**—샘플링 없이 공격 시그니처와 일치하는 각 패킷에서 조치가 구현됨을 나타냅니다.

DoS 실드에서는 휴면 상태 및 활성 상태와 일치하는 패킷 수를 셉니다. 이 트래픽의 샘플을 휴면 상태에서 보호 목록과 비교합니다. 지정된 수의 패킷에 도달하면 보호 상태가 활성으로 변경됩니다.

DoS 실드 모듈에서는 병렬로 작동하는 두 개의 프로세스를 사용합니다. 한 프로세스에서 통계적으로 트래픽을 모니터링하여 휴면 보호가 활성화되었는지 확인합니다. 그런 다음, DoS 실드에서 보호가 활성임을 탐지하면 모듈이 디바이스를 통과하는 각 패킷을 *현재 활성 보호* 목록과 비교합니다. 이 모듈은 활성 시그니처와 일치하지 않는 일부 패킷을 휴면 보호 목록과 비교합니다. 모듈에서는 검사하지 않고 나머지 패킷을 네트워크에 전달합니다.

DoS 실드 보호를 구성하려면

1. *Configuration(컨피그레이션)* 관점에서 **Setup(설정) > Security Settings(보안 설정) > DoS Shield(DoS 실드)**를 선택합니다.
2. 매개변수를 구성한 다음 **Submit(제출)**을 클릭합니다.

표 58: DoS 실드 매개변수

매개변수	설명
Enable DoS Shield	DoS 실드 기능을 사용하도록 설정할지를 지정합니다. **참고:** 보호를 사용하도록 설정하지 않은 경우 보호 프로필을 구성하기 전에 사용하도록 설정합니다.
Sampling Time	DoS 실드가 각 휴면 공격에 대해 미리 정의된 임계값을 공격과 일치하는 현재 패킷 카운터 값과 비교하는 빈도(초)입니다. 기본값: 5 **참고:** 샘플링 시간이 매우 짧으면 임계값과 카운터를 자주 비교하므로 정기적인 트래픽 급증을 공격으로 간주할 수 있습니다. 샘플링 시간이 너무 길면 DoS 실드 메커니즘에서 실시간 공격을 신속하게 탐지할 수 없습니다.
Packet Sampling Ratio	패킷 샘플링 비율입니다. 예를 들어, 지정된 값이 5001이면 DoS 실드 메커니즘에서 5001개의 패킷마다 하나를 확인합니다. 기본값: 5001

네트워크 보호 정책에 DoS 실드 보호를 포함하려면

> *Configuration(컨피그레이션)* 관점에서 **Network Protection(네트워크 보호) > Network Protection Policies(네트워크 보호 정책) >**  **(Add(추가)) > Action(조치) > Signature Protection Profile(시그니처 보호 프로필) > All-DoS-Shield**를 선택합니다. 자세한 내용은 DefensePro 네트워크 보호 정책 관리, 127페이지를 참조하십시오.

글로벌 동작 기반 DoS 보호 구성

네트워크 보호 정책에서 사용할 수 있는 동작 기반 DoS(Behavioral Denial-of-Service) 보호를 통해 제로 데이 네트워크 플러드 공격으로부터 네트워크를 방어합니다. 이러한 공격은 사용 가능한 네트워크 대역폭을 부적절한 트래픽으로 채워, 합법적인 사용자의 네트워크 리소스 사용을 거부합니다. 공격은 공개 네트워크에서 시작되며 인터넷 연결 조직을 위협합니다.

동작 기반 DoS 프로필에서 이상 트래픽의 공간을 식별하여 트래픽 이상 징후를 탐지하고 알 수 없는 제로 데이 플러드 공격을 방지합니다.

네트워크 플러드 보호 유형은 다음과 같습니다.

- TCP 플러드—SYN Flood, TCP Fin + ACK 플러드, TCP 재설정 플러드, TCP SYN + ACK 플러드 및 TCP 프래그멘테이션 플러드 포함
- ICMP 플러드
- IGMP 플러드

BDoS 보호의 주된 이점은 통계 트래픽 이상을 탐지하고 휴리스틱 프로토콜 정보 분석을 기반으로 정확한 DoS 공격 공간을 생성하는 기능입니다. 따라서 오탐의 위험을 최소화하며 정확한 공격 필터링을 보장합니다. 새로운 시그니처 생성의 기본 평균 시간은 10~18초입니다. 플러드 공격은 몇 분 및 경우에 따라 몇 시간 동안 지속될 수 있으므로 이 시간은 상대적으로 짧습니다.

BDoS 보호 사용

BDoS 보호 프로필을 구성하기 전에 BDoS 보호를 사용하도록 설정합니다. BDoS 보호에 대한 기본 전역 디바이스 설정도 변경할 수 있습니다. BDoS 보호 전역 설정은 디바이스에 BDoS 프로필이 있는 모든 네트워크 보호 정책에 적용됩니다.

BDoS 보호를 사용하도록 설정하고 전역 설정을 구성하려면

1. *Configuration(컨피그레이션)* 관점에서 **Setup(설정) > Security Settings(보안 설정) > BDoS Protection(BDoS 보호)**을 선택합니다.
2. 매개변수를 구성한 다음 **Submit(제출)**을 클릭합니다.

표 59: BDoS 보호(전역): 기본 매개변수

매개변수	설명
Enable BDoS Protection	BDoS 보호 사용 여부를 지정합니다. **참고:** 이 매개변수의 설정을 변경하려면 재부팅해야 합니다.
Learning Response Period	베이스라인이 주로 측정되는 초기 기간입니다. 기본 및 권장되는 학습 응답 기간은 1주일이 좋습니다. 트래픽 비율이 정당하게 크게 변동하는 경우(예: TCP 또는 UDP 트래픽 베이스라인이 매일 50% 이상 변경) 학습 응답을 한 달로 설정합니다. 테스트 용도일 경우에만 하루 동안의 기간을 사용합니다. 값: Day(일), Week(주), Month(월) 기본값: Week(주)

표 59: BDoS 보호(전역): 기본 매개변수(계속)

매개변수	설명
Enable Traffic Statistics Sampling	BDoS 공간 생성 단계 중에 BDoS 모듈에서 트래픽 통계 샘플링을 사용할지 지정합니다. BDoS 모듈에서 실시간 시그니처를 생성하려고 하며 트래픽 비율이 높으면 디바이스에서 트래픽의 일부만 평가합니다. BDoS 모듈에서 트래픽 비율에 따라 샘플링 요인을 자동으로 조정합니다. BDoS 모듈에서는 낮은 트래픽 비율(100K PPS 미만)의 모든 트래픽과 높은 비율(100K PPS 이상)의 트래픽은 일부만 검사합니다. 기본값: Enabled(사용) **참고:** 최상의 성능을 위해 Radware에서는 매개변수를 *Enabled(사용)*로 설정하도록 권장합니다.
Footprint Strictness	동작 기반 DoS 모듈에서 새로운 공격을 탐지하면 모듈에서 공격 트래픽을 차단하는 공격 공간을 생성합니다. 동작 기반 DoS 모듈에서 공간 엄격도 조건을 충족하는 공간을 생성할 수 없는 경우 모듈에서 공격 알림을 발행하지만 공격을 차단하지는 않습니다. 엄격도가 높을수록 공간의 정확도가 높아집니다. 그러나 엄격도를 높이면 디바이스에서 공간을 생성하지 못할 가능성이 커집니다. 값: ● High(높음)—공간에 두 개 이상의 Boolean AND 연산자가 필요하며 기타 Boolean OR 값은 필요하지 않습니다. 이 레벨에서는 오탐의 가능성이 줄어들지만 미탐의 가능성은 늘어납니다. ● Medium(중간)—공간에 한 개 이상의 Boolean AND 연산자와 두 개 이하의 Boolean OR 값이 필요합니다. ● Low(낮음)—동작 기반 DoS 모듈에서 제안하는 모든 공간을 허용합니다. 이 레벨에서는 공격 차단을 극대화할 수 있지만 오탐의 가능성이 늘어납니다. 기본값: Low(낮음) **참고:** ● DefensePro에서는 항상 체크섬 필드와 순서 번호 필드를 *높은* 공간 엄격도 필드로 간주합니다. 따라서 하나의 체크섬과 순서 번호만 있는 공간은 항상 공간 엄격도가 *높음*으로 간주됩니다. ● 표 61 - 공간 엄격도 예, 105페이지에서는 공간 엄격도 요구사항의 예를 보여줍니다.

표 60: BDoS 보호(전역): 고급 매개변수

매개변수	설명
이러한 설정은 주기적 공격 동작에 영향을 미칩니다. 이 설정을 사용하여 이러한 공격 유형을 효과적으로 탐지하여 차단합니다.	
Duration of Non-attack Traffic in Blocking State	*공격 정도*가 차단 상태에서 하드 코딩된 임계값 미만으로 떨어져 유지되는 기간(초)입니다. 시간이 경과하면 DefensePro에서 공격이 종료된 것으로 선언합니다. 값: 45-300 기본값: 45
Duration of Non-attack Traffic in Anomaly or Non-Strictness State	*공격 정도*가 비정상 상태 또는 엄격하지 않은 상태의 하드 코딩된 임계값 미만으로 떨어져 유지되는 기간(초)입니다. 시간이 경과하면 DefensePro에서 공격이 종료된 것으로 선언합니다. 값: 45-300 기본값: 45
Reset BDoS Baseline	클릭하여 BDoS 베이스라인을 재설정합니다. 그런 다음 BDoS 프로필을 포함하는 모든 네트워크 보호 정책 및 BDoS 프로필을 포함하는 특정 네트워크 보호 정책의 베이스라인을 재설정할지 선택한 다음 **Submit(제출)**을 클릭합니다. 베이스라인 학습 통계를 재설정하면 베이스라인 트래픽 통계를 지우고 기본 정상 베이스라인을 재설정합니다. 보호된 네트워크의 특성이 완전히 변경되고 네트워크 변경사항에 맞게 대역폭 할당량을 변경해야 하는 경우에만 베이스라인 통계를 재설정합니다.

표 60: BDoS 보호(전역): 고급 매개변수(계속)

매개변수	설명
Learning Suppression Threshold	*지정된 대역폭*의 백분율로, 이 값 미만이 되면 DefensePro에서 BDoS 베이스라인 학습을 억제합니다. 학습 억제 임계값 기능을 사용하면 경우에 따라 DefensePro에서 매우 적은 양의 트래픽을 처리하는 시나리오에서 유용한 BDoS 베이스라인 값을 유지할 수 있습니다. 때때로 DefensePro에서 매우 적은 양의 트래픽을 처리하는 일반적인 시나리오는 다음 두 가지입니다. ● 경로 이탈 구축—경로 이탈 구축에서는 공격 탐지 시 DefensePro가 트리거됩니다. 이때 공격 차단을 위해 트래픽이 DefensePro를 통과하도록 방향을 바꿉니다. 공격 중에 트래픽이 방향을 바꾸어 DefensePro를 통과하도록 경로가 지정됩니다. 공격이 없는 동안에는 트래픽이 DefensePro를 통과하지 않습니다(유지관리 메시지 제외). DefensePro로 트래픽 방향이 바뀌지 않으면 BDoS 학습이 매우 낮은 값을 방지하도록 억제되어, 베이스라인에 영향을 미치므로 궁극적으로 오탐 가능성이 증가합니다. ● 하루 내내 트래픽 비율이 현저히 변경되는 환경입니다. *지정된 대역폭*은 *Network Protection(네트워크 보호)* 탭, **BDoS Profiles(BDoS 프로필) > Outbound Traffic(아웃바운드 트래픽)|Inbound Traffic(인바운드 트래픽)**에 있는 *Outbound Traffic(아웃바운드 트래픽)*과 *Inbound Traffic(인바운드 트래픽)*을 나타냅니다. 학습 억제 임계값은 모든 BDoS 프로필에 적용되지만, DefensePro에서는 네트워크 보호 정책 및 지정된 *방향*(*Network Protection(네트워크 보호)* 탭, **Network Protection Policy(네트워크 보호 정책) > Direction(방향)**)당 임계값을 계산합니다. *단방향* 정책의 경우 학습 억제 임계값에서 인바운드 대역폭을 고려합니다. DefensePro는 *양방향* 정책을 두 개의 정책으로 처리하므로, 학습 억제 임계값에서 각 정책(인바운드/아웃바운드)의 대역폭을 계산합니다. 값: ● 0—BDoS 프로필에서 학습 억제 임계값을 사용하지 *않도록* 지정합니다. ● 1–50 기본값: 0

표 61: 공간 엄격도 예

공간 예	낮은 엄격도	중간 엄격도	높은 엄격도
TTL	예	아니요	아니요
TTL AND 패킷 크기	예	예	아니요
TTL AND 패킷 크기 AND 대상 포트	예	예	예

BDoS 사용 공간 바이패스 구성

실시간 시그니처의 일부로 사용하지 않을 사용 공간 바이패스 유형 및 값을 정의할 수 있습니다. 정의하는 유형과 값은 보호 엔진에서 트래픽이 실시간 시그니처 후보임을 암시하는 경우에도 차단 규칙(실시간 시그니처) 내의 OR 또는 AND 연산에서 사용되지 않습니다.

사용 공간 바이패스를 구성하려면

1. *Configuration(컨피그레이션)* 관점에서 **Setup(설정) > Security Settings(보안 설정) > BDoS Protection(BDoS 보호) > BDoS Footprint Bypass(BDoS 사용 공간 바이패스)**를 선택합니다.
2. **Footprint Bypass Controller(사용 공간 바이패스 컨트롤러)** 드롭다운 목록에서 사용 공간 바이패스를 구성할 공격 보호를 선택하고  (Search(검색)) 버튼을 클릭합니다. 표에 선택한 공격 보호의 바이패스 유형과 값이 표시됩니다.
3. 바이패스 유형 설정을 편집하려면 해당 행을 두 번 클릭합니다.
4. 선택한 바이패스 유형의 사용 공간 바이패스 매개변수를 구성한 다음 **Submit(제출)**을 클릭합니다.

표 62: BDoS 사용 공간 바이패스 매개변수

매개변수	설명
Footprint Bypass Controller	(읽기 전용) 사용 공간 바이패스를 구성하고 있는 선택된 공격 보호입니다.
Bypass Field	(읽기 전용) 구성할 선택한 바이패스 유형입니다.
Bypass Status	바이패스 옵션입니다. 값: ● Bypass(바이패스)—동작 기반 DoS 모듈이 사용 공간을 생성할 때 선택한 바이패스 필드의 가능한 모든 값을 건너뜁니다. ● Accept(수락)—동작 기반 DoS 모듈에서 사용 공간을 생성할 때 선택한 **바이패스 필드**의 지정된 값(값이 있는 경우)만 건너뜁니다.
Bypass Values	*Bypass Status(바이패스 상태)* 매개변수의 값이 **Accept(수락)**이면 사용 공간을 생성할 때 동작 기반 DoS 메커니즘에서 선택한 해당 *Bypass Field(바이패스 필드)*의 지정된 *Bypass Values(바이패스 값)*을 사용하지 않습니다. 올바른 *Bypass Values(바이패스 값)*은 선택한 *Bypass Field(바이패스 필드)*에 따라 달라집니다. *Bypass Values(바이패스 값)* 필드의 여러 값은 쉼표로 구분해야 합니다.

DoS 트래픽의 초기 차단 구성

이 기능은 DefensePro for Cisco Firepower 9300에서 작동하지 않습니다.

DoS 트래픽의 초기 차단을 위한 패킷 헤더 필드 선택

이 기능은 DefensePro for Cisco Firepower 9300에서 작동하지 않습니다.

글로벌 SYN 플러드 보호 구성

일반적으로 SYN 플러드 공격은 서버의 리소스를 사용할 의도로 특정 *서버*를 대상으로 삼습니다. 그러나 SYN 보호를 네트워크 보호로 구성하여 여러 네트워크 요소를 더 쉽게 보호할 수 있습니다.

네트워크 보호 정책의 SYN 프로필을 구성하기 전에 SYN 보호가 사용되며 SYN 플러드 보호 전역 매개변수가 구성되었는지 확인합니다.

글로벌 SYN 플러드 보호를 구성하려면

1. *Configuration(컨피그레이션)* 관점에서 **Setup(설정) > Security Settings(보안 설정) > SYN Flood Protection Settings(SYN 플러드 보호 설정)**를 선택합니다.
2. 매개변수를 구성한 다음 **Submit(제출)**을 클릭합니다.

표 63: SYN 플러드 보호: 일반 매개변수

매개변수	설명
Enable SYN Flood Protection	디바이스에서 SYN 플러드 보호를 사용하도록 설정할지를 지정합니다. 기본값: Enabled(사용) **참고:** 이 매개변수의 설정을 변경하려면 재부팅해야 합니다.

표 64: SYN 보호 매개변수: 고급 매개변수

매개변수	설명
Tracking Time	단일 보호 대상의 공격 상태가 종료가 되도록 해당 대상으로 직접 연결되는 SYN 패킷 수가 종료 임계값보다 낮아야 하는 기간(초)입니다. 값: 1-10 기본값: 5

글로벌 패킷 이상 보호 구성

이 기능은 관리 인터페이스에서 지원되지 *않습니다*.

패킷 이상 보호에서 패킷 이상을 탐지하고 이로부터 보호합니다.

패킷 이상 보호 구성

다음 절차에 따라 패킷 이상 보호를 적절하게 구성합니다.

패킷 이상 보호를 구성하려면

1. *Configuration(컨피그레이션)* 관점에서 **Setup(설정) > Security Settings(보안 설정) > Packet Anomaly(패킷 이상)**를 선택합니다.
2. 관련 행을 두 번 클릭합니다.
3. 매개변수를 구성한 다음 **Submit(제출)**을 클릭합니다.

   이러한 매개변수 및 기본 컨피그레이션에 대한 자세한 내용은 표 65 - 패킷 이상 보호 매개변수, 108페이지를 참조하십시오.

표 65: 패킷 이상 보호 매개변수

매개변수	설명
ID	(읽기 전용) 패킷 이상 보호의 ID 번호입니다. ID는 APSolute Vision 보안 로그에 보낸 트랩에 표시되는 Radware ID입니다.
Protection Name	(읽기 전용) 패킷 이상 보호의 이름입니다.
Action	패킷 이상이 탐지되면 디바이스에서 수행하는 조치입니다. 조치는 지정된 패킷 이상 보호용으로만 수행됩니다. 값: ● Drop(삭제)—디바이스에서 비정상 패킷을 폐기하고 트랩을 발행합니다. ● Report(보고)—디바이스에서 비정상 패킷에 대한 트랩을 발행합니다. **Report Action(보고 조치)**이 **Process(처리)**인 경우 패킷이 나머지 디바이스 모듈로 이동합니다. **Report Action(보고 조치)**이 **Bypass(바이패스)**인 경우 패킷이 나머지 디바이스 모듈을 건너뜁니다. ● No Report(보고하지 않음)—디바이스에서 비정상 패킷의 트랩을 발행하지 않습니다. **Report Action(보고 조치)**이 **Process(처리)**인 경우 패킷이 나머지 디바이스 모듈로 이동합니다. **Report Action(보고 조치)**이 **Bypass(바이패스)**인 경우 패킷이 나머지 디바이스 모듈을 건너뜁니다. **참고:** **Drop All(모두 삭제)**을 클릭하여 모든 패킷 이상 보호 조치를 **Drop(삭제)**으로 설정합니다. **Report All(모두 보고)**을 클릭하여 모든 패킷 이상 보호 조치를 **Report(보고)**로 설정합니다. **No Report All(모두 보고하지 않음)**을 클릭하여 모든 패킷 이상 보호 조치를 **No Report(보고하지 않음)**로 설정합니다.
Risk	특정 이상에 대한 트랩과 관련된 위험입니다. 값: Info(정보), Low(낮음), Medium(중간), High(높음) 기본값: Info(정보)
Report Action	지정된 **Action(조치)**가 **Report(보고)**이거나 **No Report(보고하지 않음)**일 때 DefensePro 디바이스에서 이상 징후 패킷에 대해 수행하는 조치입니다. 보고 조치는 지정된 패킷 이상 보호용으로만 수행됩니다. 값: ● Bypass(바이패스)—비정상 패킷이 디바이스를 건너뜁니다. ● Process(처리)—DefensePro 모듈이 비정상 패킷을 처리합니다. 비정상 패킷이 공격의 일부이면 DefensePro에서 공격을 차단할 수 있습니다. **참고:** 다음 패킷 이상 보호에는 **Process(처리)**를 선택할 수 없습니다. ● 104—올바르지 않은 IP 헤더 또는 총 길이 ● 107—일치하지 않는 IPv6 헤더 ● 131—유효하지 않은 L4 헤더 길이

표 66: 패킷 이상 보호의 기본 컨피그레이션

이상	설명
Invalid IPv4 Header or Total Length(유효하지 않은 IPv4 헤더 또는 총 길이)	IP 패킷 헤더 길이가 실제 헤더 길이와 일치하지 않거나 IP 패킷 총 길이가 실제 패킷 길이와 일치하지 않습니다. ID: 104 기본 조치: 삭제 기본 위험: 낮음 보고 조치: 바이패스[1]
TTL Less Than or Equal to 1(TTL이 1 이하)	TTL 필드 값이 1 이하입니다. ID: 105 기본 조치: 보고 기본 위험: 낮음 기본 보고 조치: 처리
Inconsistent IPv6 Headers(일치하지 않는 IPv6 헤더)	일치하지 않는 IPv6 헤더입니다. ID: 107 기본 조치: 삭제 기본 위험: 낮음 보고 조치: 바이패스
IPv6 Hop Limit Reached(IPv6 홉 제한 도달)	홉 제한이 1보다 크지 않습니다. ID: 108 기본 조치: 보고 기본 위험: 낮음 기본 보고 조치: 처리
Unsupported L4 Protocol(지원되지 않는 L4 프로토콜)	UDP, TCP, ICMP 또는 IGMP 이외의 트래픽입니다. ID: 110 기본 조치: 보고하지 않음 기본 위험: 낮음 기본 보고 조치: 처리
Invalid TCP Flags(올바르지 않은 TCP 플래그)	TCP 플래그 조합이 표준을 따르지 않습니다. ID: 113 기본 조치: 삭제 기본 위험: 낮음 기본 보고 조치: 바이패스
Invalid L4 Header Length(유효하지 않은 L4 헤더 길이)	레이어 4, TCP/UDP/SCTP 헤더의 길이가 유효하지 않습니다. ID: 131 기본 조치: 삭제 기본 위험: 낮음 보고 조치: 바이패스

1 - 이 패킷 이상 보호에는 *Process(처리)*를 선택할 수 없습니다.

글로벌 DNS 플러드 보호 구성

네트워크 보호 정책에서 사용할 수 있는 DNS 플러드 보호를 통해 제로 데이 DNS 플러드 공격으로부터 네트워크를 방어합니다. 이러한 공격은 사용 가능한 DNS 대역폭을 부적절한 트래픽으로 채워, 합법적인 사용자의 DNS 조회를 거부합니다. 공격은 공개 네트워크에서 시작되며 인터넷 연결 조직을 위협합니다.

DNS 플러드 프로필에서 이상 징후 트래픽의 공간을 식별하여 트래픽 이상 징후를 탐지하고 알 수 없는 제로 데이 DNS 플러드 공격을 방지합니다.

DNS 플러드 보호 유형에는 다음 DNS 쿼리 유형이 포함될 수 있습니다.

- A
- MX
- PTR
- AAAA
- Text
- SOA
- NAPTR
- SRV
- 기타

DNS 플러드 보호에서는 DNS 트래픽에서 통계 이상을 탐지하고 휴리스틱 프로토콜 정보 분석을 기반으로 정확한 공격 공간을 생성할 수 있습니다. 따라서 오탐의 위험을 최소화하며 정확한 공격 필터링을 보장합니다. 새로운 시그니처 생성의 기본 평균 시간은 10~18초입니다. 플러드 공격은 몇 분 및 경우에 따라 몇 시간 동안 지속될 수 있으므로 이 시간은 상대적으로 짧습니다.

DNS 플러드 보호 프로필을 구성하기 전에 DNS 플러드 보호가 사용하도록 설정되어 있는지 확인합니다. DNS 플러드 보호에 대한 기본 전역 디바이스 설정도 변경할 수도 있습니다. DNS 플러드 보호 전역 설정은 디바이스에 DNS 플러드 프로필이 있는 모든 네트워크 보호 정책에 적용됩니다.

DNS 플러드 보호를 사용하도록 설정하고 및 전역 설정을 구성하려면

1. *Configuration(컨피그레이션)* 관점에서 **Setup(설정) > Security Settings(보안 설정) > DNS Flood Protection(DNS 플러드 보호)를** 선택합니다.
2. 매개변수를 구성한 다음 **Submit(제출)**을 클릭합니다.

표 67: DNS 플러드 보호: 일반 매개변수

매개변수	설명
Enable DNS Flood Protection	DNS 플러드 보호 사용 여부를 지정합니다. **참고:** 이 매개변수의 설정을 변경하려면 재부팅해야 합니다.
Learning Response Period	베이스라인이 주로 측정되는 초기 기간입니다. 기본 및 권장되는 학습 응답 기간은 1주일이 좋습니다. 트래픽 비율이 정당하게 크게 변동하는 경우(예: TCP 또는 UDP 트래픽 베이스라인이 매일 50% 이상 변경) 학습 응답을 한 달로 설정합니다. 테스트 용도일 경우에만 하루 동안의 기간을 사용합니다. 값: Day(일), Week(주), Month(월) 기본값: Week(주)

표 67: DNS 플러드 보호: 일반 매개변수(계속)

매개변수	설명
Footprint Strictness	DNS 플러드 보호 모듈에서 새로운 공격을 탐지하면 모듈에서 공격 트래픽을 차단하는 공격 공간을 생성합니다. 모듈에서 공간 엄격도 조건을 충족하는 공간을 생성할 수 없는 경우 모듈에서 공격 알림을 발행하지만 공격을 차단하지는 않습니다. 엄격도가 높을수록 공간의 정확도가 높아집니다. 그러나 엄격도를 높이면 모듈에서 공간을 생성하지 못할 가능성이 커집니다. 값: ● High(높음)—공간에 두 개 이상의 Boolean AND 연산자가 필요하며 기타 Boolean OR 값은 필요하지 않습니다. 이 레벨에서는 오탐의 가능성이 줄어들지만 미탐의 가능성은 늘어납니다. ● Medium(중간)—공간에 한 개 이상의 Boolean AND 연산자와 두 개 이하의 Boolean OR 값이 필요합니다. ● Low(낮음)—DNS 플러드 보호 모듈에서 제안하는 모든 공간을 허용합니다. 이 레벨에서는 공격 차단을 극대화할 수 있지만 오탐의 가능성이 늘어납니다. 기본값: Low(낮음) **참고**: DNS 플러드 보호 모듈에서는 항상 체크섬 필드와 순서 번호 필드를 *높은* 공간 엄격도 필드로 간주합니다. 따라서 하나의 체크섬과 순서 번호만 있는 공간은 항상 공간 엄격도가 *높음*으로 간주됩니다. 표 70 - DNS 공간 엄격도 예, 112페이지 에서는 공간 엄격도 요구사항의 예를 보여줍니다.

표 68: DNS 플러드 보호: 차단 조치 매개변수

매개변수	설명
보호를 사용하도록 설정하고 디바이스에서 DNS 플러드 공격이 시작되었음을 탐지하면 디바이스에서 탭에 표시되는 순서인 에스컬레이션 순으로 차단 조치를 구현합니다. 첫 번째로 사용된 차단 조치가 공격을 만족스럽게 차단하지 않으면 (일정한 *에스컬레이션 기간* 후) 디바이스에서 다음으로 더 심각한 사용 차단 조치를 계속해서 구현하는 방식입니다. 가장 심각한 차단 조치로 디바이스에서는 항상 *종합적인 비율 제한*을 구현합니다. 이 제한은 모든 DNS 쿼리 비율을 보호 서버로 제한합니다.	
Enable Signature Rate Limit	디바이스에서 실시간 시그니처와 일치하는 DNS 쿼리 비율을 제한할지를 지정합니다. 기본값: Enabled(사용)
Enable Collective Rate Limit	(읽기 전용) 디바이스가 모든 DNS 쿼리 비율을 보호되는 서버로 제한합니다. 값: Enabled(사용)
Reset DNS Baseline	클릭하여 DNS 베이스라인을 재설정합니다. 그런 다음 DNS 프로필을 포함하는 모든 네트워크 정책 규칙 또는 DNS 프로필을 포함하는 특정 네트워크 보호 정책에 대한 베이스라인을 재설정할지를 선택한 다음 **Submit(제출)**을 클릭합니다. 베이스라인 학습 통계를 재설정하면 베이스라인 트래픽 통계를 지우고 기본 정상 베이스라인을 재설정합니다. 보호된 네트워크의 특성이 완전히 변경되고 네트워크 변경사항에 맞게 대역폭 할당량을 변경해야 하는 경우에만 베이스라인 통계를 재설정합니다.

표 69: DNS 플러드 보호: 고급 매개변수

매개변수	설명
이러한 설정은 주기적 공격 동작에 영향을 미칩니다. 이 설정을 사용하여 이러한 공격 유형을 효과적으로 탐지하여 차단합니다.	
Duration of Non-attack Traffic in Blocking State	*공격 정도*가 차단 상태에서 하드 코딩된 임계값 미만으로 떨어져 유지되는 기간(초)입니다. 시간이 경과하면 DefensePro에서 공격이 종료된 것으로 선언합니다. 값: 45-300 기본값: 45
Duration of Non-attack Traffic in Anomaly or Non- Strictness State	*공격 정도*가 비정상 상태 또는 엄격하지 않은 상태의 하드 코딩된 임계값 미만으로 떨어져 유지되는 기간(초)입니다. 시간이 경과하면 DefensePro에서 공격이 종료된 것으로 선언합니다. 값: 45-300 기본값: 45
Reset DNS Baseline	클릭하여 DNS 베이스라인을 재설정합니다. 그런 다음 DNS 프로필을 포함하는 모든 네트워크 보호 정책 또는 DNS 프로필을 포함하는 특정 네트워크 보호 정책에 대한 베이스라인을 재설정할지를 선택한 다음 **Submit(제출)**을 클릭합니다. 베이스라인 학습 통계를 재설정하면 베이스라인 트래픽 통계를 지우고 기본 정상 베이스라인을 재설정합니다. 보호된 네트워크의 특성이 완전히 변경되고 네트워크 변경사항에 맞게 대역폭 할당량을 변경해야 하는 경우에만 베이스라인 통계를 재설정합니다.

표 70: DNS 공간 엄격도 예

공간 예	낮은 엄격도	중간 엄격도	높은 엄격도
DNS Query(DNS 쿼리)	예	아니요	아니요
DNS Query AND DNS ID(DNS 쿼리 AND DNS ID)	예	예	아니요
DNS Query AND DNS ID AND Packet Size(DNS 쿼리 AND DNS ID AND 패킷 크기)	예	예	예

DNS 사용 공간 바이패스 구성

실시간 시그니처의 일부로 사용하지 않을 사용 공간 바이패스 유형 및 값을 정의할 수 있습니다. 정의하는 유형과 값은 보호 엔진에서 트래픽이 실시간 시그니처 후보임을 암시하는 경우에도 차단 규칙(실시간 시그니처) 내의 OR 또는 AND 연산에서 사용되지 않습니다.

DNS 사용 공간 바이패스를 구성하려면

1. *Configuration(컨피그레이션)* 관점에서 **Setup(설정) > Security Settings(보안 설정) > DNS Flood Protection(DNS 플러드 보호) > DNS Footprint Bypass(DNS 사용 공간 바이패스)**를 선택합니다.
2. *Footprint Bypass Controller(사용 공간 바이패스 컨트롤러)* 목록에서 사용 공간 바이패스를 구성할 DNS 쿼리 유형을 선택하고  (Search(검색)) 버튼을 클릭합니다. 테이블에 선택한 DNS 쿼리 유형의 바이패스 필드가 표시됩니다.
3. 바이패스 유형 설정을 편집하려면 해당 행을 두 번 클릭합니다.
4. 선택한 바이패스 필드에 대한 사용 공간 바이패스 매개변수를 구성한 다음 **Submit(제출)**을 클릭합니다.

표 71: DNS 사용 공간 바이패스 매개변수

매개변수	설명
Footprint Bypass Controller	(읽기 전용) 사용 공간 바이패스를 구성하고 있는 선택된 DNS 쿼리 유형입니다.
Bypass Field	(읽기 전용) 구성할 선택한 바이패스 필드입니다.
Bypass Status	바이패스 옵션입니다. 값: ● Bypass(바이패스)—DNS 플러드 보호 모듈이 사용 공간을 생성할 때 선택한 바이패스 필드의 가능한 모든 값을 건너뜁니다. ● Accept(수락)—DNS 플러드 보호 모듈에서 사용 공간을 생성할 때 선택한 바이패스 필드의 지정된 값(값이 있는 경우)만 건너뜁니다.
Bypass Values	바이패스 상태 매개변수의 값이 **Accept(수락)**인 경우 사용합니다. DNS 플러드 보호는 선택한 바이패스 유형의 값만 건너뛰고, 기타 모든 값을 사용할 수 있습니다. 이러한 값은 선택한 바이패스 필드에 따라 달라집니다. 필드의 값은 쉼표로 구분해야 합니다.

DNS 트래픽의 초기 차단 구성

이 기능은 DefensePro for Cisco Firepower 9300에서 작동하지 않습니다.

DNS 트래픽의 초기 차단을 위한 패킷 헤더 필드 선택

이 기능은 DefensePro for Cisco Firepower 9300에서 작동하지 않습니다.

DefensePro 보고-설정 설정 구성

이 섹션에 포함되는 주제는 다음과 같습니다.

- DefensePro 시스템 로그 설정 구성, 113페이지
- DefensePro 디바이스에서 컨피그레이션 감사 사용, 115페이지
- 보안 보고 설정 구성, 115페이지

DefensePro 시스템 로그 설정 구성

DefensePro에서 최대 5개의 시스템 로그 서버에 이벤트 트랩을 보낼 수 있습니다. DefensePro 디바이스마다 적절한 정보를 구성할 수 있습니다.

참고: 개별 디바이스를 각각 구성하는 대신 Radware에서는 모든 디바이스의 시스템 로그 메시지를 전달하도록 APSolute Vision 서버를 구성하는 것을 권장합니다.

시스템 로그 설정을 구성하려면

1. *Configuration(컨피그레이션)* 관점에서 **Setup(설정) > Reporting Settings(보고 설정) > Syslog(시스템 로그)**를 선택합니다.
2. 다음 중 하나를 수행합니다.
   - 시스템 로그 기능을 사용하도록 설정하려면 **Enable Syslog(시스템 로그 사용)** 확인란을 선택합니다.
   - 시스템 로그 기능을 사용하지 않도록 설정하려면 **Enable Syslog(시스템 로그 사용)** 확인란의 선택을 취소합니다.

   기본값: Enabled(사용)
3. 다음 중 하나를 수행합니다.
   - 항목을 추가하려면 (Add(추가)) 버튼을 클릭합니다.
   - 항목을 수정하려면 테이블에서 항목을 두 번 클릭합니다.
4. 매개변수를 구성한 다음 **Submit(제출)**을 클릭합니다.

표 72: DefensePro for Cisco Firepower 9300의 시스템 로그 매개변수

매개변수	설명
Enable Syslog Server	시스템 로그 서버의 사용 여부를 지정합니다. 기본값: Enabled(사용) **참고:** 디바이스에서 UDP를 사용하여 시스템 로그 메시지를 보냅니다. 즉, 디바이스에서 메시지 전송을 검증하지 않고 시스템 로그 메시지를 전송합니다. *Status(상태)*는 DefensePro 시스템 로그 모니터에서 **N/R**입니다(*Monitoring(모니터링)* 관점 > *Resource Utilization(리소스 사용률)* 탭 > **Syslog Monitor(시스템 로그 모니터)**).
Syslog Server	시스템 로그 서비스(syslogd)를 실행 중인 디바이스의 IP 주소 또는 호스트 이름입니다.
Source Port	시스템 로그 소스 포트입니다. 기본값: 514 **참고:** 포트 0은 임의의 포트를 지정합니다.
Destination Port	시스템 로그 대상 포트입니다. 기본값: 514

표 72: DefensePro for Cisco Firepower 9300의 시스템 로그 매개변수(계속)

매개변수	설명
Facility	전송자의 디바이스 유형입니다. 이 유형은 시스템 로그 메시지를 통해 전송됩니다. 이 매개변수를 사용하여 여러 다른 디바이스 사이에서 구분하고 메시지를 분할하는 규칙을 정의할 수 있습니다. 값: ● Authorization Messages(인증 메시지) ● Clock Daemon(클록 데몬) ● Clock Daemon2(클록 데몬2) ● FTP Daemon(FTP 데몬) ● Kernel Messages(커널 메시지) ● Line Printer Subsystem(라인 프린터 하위 시스템) ● Local 0(로컬 0) ● Local 1(로컬 1) ● Local 2(로컬 2) ● Local 3(로컬 3) ● Local 4(로컬 4) ● Local 5(로컬 5) ● Local 6(로컬 6) ● Local 7(로컬 7) ● Log Alert(로그 경고) ● Log Audit(로그 감사) ● Mail System(메일 시스템) ● Network News Subsystem (네트워크 뉴스 하위 시스템) ● NTP Daemon(NTP 데몬) ● Syslogd Messages(Syslogd 메시지) ● System Daemons(시스템 데몬) ● User Level Messages(사용자 레벨메시지) ● UUCP 기본값: Local Use 6(로컬 사용 6)

DefensePro 디바이스에서 컨피그레이션 감사 사용

디바이스에 대한 컨피그레이션 감사가 APSolute Vision 서버와 디바이스에서 사용하도록 설정되어 있는 경우 APSolute Vision을 사용하는 디바이스에서 컨피그레이션을 변경하면 감사 데이터베이스에 두 가지 레코드(APSolute Vision 서버의 레코드와 디바이스 감사 메시지의 레코드)가 생성됩니다.

참고: 매니지드 디바이스에 과부하가 걸리지 않고 성능이 저하되지 않도록 이 기능은 기본적으로 사용되지 않도록 설정됩니다.

매니지드 디바이스에 대한 컨피그레이션 감사를 사용하도록 설정하려면

1. *Configuration(컨피그레이션)* 관점에서 **Setup(설정) > Advanced Parameters(고급 매개변수) > Configuration Audit(컨피그레이션 감사)**를 선택합니다.
2. **Enable Configuration Auditing(컨피그레이션 감사 사용)** 확인란을 선택하고 **Submit(제출)**을 클릭합니다.

보안 보고 설정 구성

이력 및 실시간 보안 모니터링 기능을 지원하고 각 공격 이벤트에 대한 자세한 공격 정보를 제공하기 위해 DefensePro에서는 디바이스와 APSolute Vision 사이의 데이터 보고 프로토콜을 설정합니다. SRP(Statistical Real-time Protocol)라는 이 프로토콜은 UDP 패킷을 사용하여 공격 정보를 전송합니다.

DefensePro에서 사용하는 보고 채널을 사용하도록 설정하여 공격에 대한 정보를 수신하고 다양한 위험 레벨을 기반으로 탐지된 공격을 보고할 수 있습니다.

또한 DefensePro에서는 특정 공격의 일부로 DefensePro 디바이스에서 식별한 샘플링 캡처 패킷을 APSolute Vision 서버에 제공할 수 있습니다. DefensePro에서는 이러한 패킷을 UDP 패킷으로 캡슐화하여 지정된 IP 주소로 전송합니다.

참고

- DefensePro에서는 DefensePro가 조사한 의심스러운 소스에서 샘플링된 캡처 패킷을 제공하지 않습니다. (DefensePro에서는 HTTP 플러드 보호, SYN 플러드 보호, DNS 플러드 보호 및 SSL 보호의 소스를 조사하는 옵션을 지원합니다.)
- DefensePro에서는 샘플링된 GRE 캡슐화 캡처 패킷을 제공하지 않습니다.

추가적인 오프라인 분석을 위해 공격 이벤트와 함께 캡처된 공격 패킷을 전송하도록 DefensePro 디바이스도 구성할 수 있습니다. 패킷 보고 및 SRP에서는 동일한 기본 포트, 2088을 사용합니다.

DefensePro for Cisco Firepower 9300에서 보안 보고 설정을 구성하려면

1. *Configuration(컨피그레이션)* 관점에서 **Setup(설정) > Reporting Settings(보고 설정) > Advanced Reporting Settings(고급 보고 설정)**를 선택합니다.
2. 매개변수를 구성한 다음 **Submit(제출)**을 클릭합니다.

표 73: 고급 보고 설정: 보안 보고 매개변수

매개변수	설명
Report Interval(보고서 간격)	보고 채널을 통해 보고서를 전송하는 빈도(초)입니다. 값: 1-65,535 기본값: 5
Maximal Number of Alerts per Report (보고서당 최대 경고 수)	(보고 간격 내에 전송되는) 각 보고서에 표시될 수 있는 최대 공격 이벤트 수입니다. 값: 1-2000 기본값: 1000
Report per Attack Aggregation Threshold (공격 집계 임계값당 보고)	이벤트를 보고서에 집계하기 전에 보고 간격 동안 발생하는 특정 공격의 이벤트 수입니다. 생성된 이벤트 수가 집계 임계값을 초과하면 이벤트의 IP 주소 값이 *임의의 IP 주소*를 지정하는 0.0.0.0으로 표시됩니다. 값: 1-50 기본값: 5
L4 Port for Reporting(보고용 L4 포트)	패킷 보고 및 SRP에 사용되는 포트입니다. 값: 1-65,535 기본값: 2088
Enable Sending Traps(트랩 전송 사용)	선택한 경우 디바이스에서 트랩 보고 채널을 사용합니다. 기본값: Enabled(사용)
Minimal Risk Level for Sending Traps (트랩 전송을 위한 최소 위험 레벨)	보고 채널에 대한 최소 위험 레벨입니다. 지정된 위험 값 이상의 공격이 보고됩니다. 기본값: Low(낮음)
Enable Sending Syslog(시스템 로그 전송 사용)	선택한 경우 디바이스에서 시스템 로그 보고 채널을 사용합니다. 기본값: Enabled(사용)
Minimal Risk Level for Sending Syslog (시스템 로그 전송을 위한 최소 위험 레벨)	보고 채널에 대한 최소 위험 레벨입니다. 지정된 위험 값 이상의 공격이 보고됩니다. 기본값: Low(낮음)

표 73: 고급 보고 설정: 보안 보고 매개변수(계속)

매개변수	설명
Enable Sending Terminal Echo(터미널 에코 전송 사용)	선택한 경우 디바이스에서 터미널 에코 보고 채널을 사용합니다. 기본값: Disabled(사용 안 함)
Minimal Risk Level for Sending Terminal Echo(터미널 에코 전송을 위한 최소 위험 레벨)	보고 채널에 대한 최소 위험 레벨입니다. 지정된 위험 값 이상의 공격이 보고됩니다. 기본값: Low(낮음)
Enable Security Logging(보안 로깅 사용)	선택한 경우 디바이스에서 보안 로깅 보고 채널을 사용합니다.

표 74: 고급 보고: 패킷 보고 및 패킷 추적 매개변수

매개변수	설명
참고: 이 탭의 매개변수는 패킷 보고에만 적용됩니다. 이 버전에서는 패킷 추적 기능을 지원하지 않습니다.	
Enable Packet Reporting(패킷 보고 사용)	DefensePro 디바이스에서 공격 이벤트와 함께 샘플링된 공격 패킷을 전송할지 지정합니다. 기본값: Enabled(사용)
Maximum Packets per Report(보고서당 최대 패킷 수)	디바이스에서 보고 간격 내에 전송할 수 있는 최대 패킷 수입니다. 값: 1-65,535 기본값: 100
Destination IP Address(대상 IP 주소)	패킷 보고서의 대상 IP 주소입니다. 기본값: 0.0.0.0 **참고:** 두 개 이상의 APSolute Vision 서버에서 디바이스를 관리하는 경우에도 패킷 보고에 대해 단 하나의 대상 IP 주소만 구성할 수 있습니다.

표 75: 고급 보고 설정: netForensics 매개변수

매개변수	설명
Enable netForensics Reporting(netForensics 보고 사용)	선택한 경우 netForensics 보고 에이전트를 사용하여 보고할 수 있습니다. 기본값: Disabled(사용 안 함)
Agent IP Address(에이전트 IP 주소)	netForensics 에이전트의 IP 주소입니다.
L4 Port(L4 포트)	netForensics 보고에 사용되는 포트입니다. 값: 1-65,535 기본값: 555

표 76: 고급 보고 설정: 데이터 보고 대상 매개변수

매개변수	설명
Destination IP Address(대상 IP 주소)	데이터 보고용 대상 주소입니다. 테이블에는 최대 10개의 주소를 포함할 수 있습니다. 기본적으로 테이블에 공간이 있으면 디바이스 창의 트리에 DefensePro 디바이스를 추가할 때 주소가 자동으로 추가됩니다. 주소를 추가하려면 (Add(추가)) 버튼을 클릭합니다. 대상 IP 주소를 입력하고 **Submit(제출)**을 클릭합니다.

DefensePro 클러스터링 설정 구성

Clustering(클러스터링) 탭을 사용하여 DefensePro for Cisco Firepower 9300의 여러 인스턴스 클러스터링을 구성합니다.

클러스터링을 사용하면 여러 DefensePro 인스턴스를 통해 클러스터 멤버 간에 SYN 플러드 보호를 지원할 수 있습니다.

동일한 Firepower 9300 플랫폼에서 DefensePro의 여러 인스턴스를 개별적으로 실행할 때, 동일한 보호와 네트워크로 각 인스턴스를 구성하면 보호되는 네트워크의 보호 기능이 향상될 수 있습니다. Firepower 9300의 내부 스위치에서 DefensePro 인스턴스 사이의 트래픽 로드를 공유할 수 있습니다. 각 DefensePro 인스턴스는 개별적으로 구성되며 독립형 인스턴스로 작동합니다. 따라서 동일한 보호 네트워크에 정의된 일부 또는 모든 인스턴스에서 보호를 활성화하면 인스턴스 간 로드 공유 트래픽이 활성화되므로 (Firepower 9300 스위치 로드 공유 메커니즘 기반) 디바이스 용량을 늘릴 수 있습니다.

웹 쿠키 인증에서 조사-응답 프로세스가 수행됩니다. 이 프로세스에서는 인스턴스별 HTTP 세션 지속성이 필요합니다. Firepower 9300 로드 공유 스위치에서 L4 매개변수를 기반으로 트래픽을 분배하므로 HTTP 세션 지속성 문제가 발생할 수 있습니다. 다중 인스턴스 클러스터링을 사용하면 동일한 Firepower 9300의 DefensePro 인스턴스 간에 웹 쿠키 지속성이 유지관리되는지 검증할 수 있습니다. 이 작업은 *클러스터 마스터*로 정의된 하나의 클러스터 인스턴스를 사용하여 인스턴스 간에 쿠키를 주기적으로 동기화하는 내부 메커니즘을 통해 수행합니다.

참고: DefensePro for Cisco Firepower 9300의 설치 정보는 관련 Cisco 문서를 참조하십시오.

클러스터링을 구성하려면

1. *Configuration(컨피그레이션)* 관점에서 **Setup(설정) > Advanced Parameters(고급 매개변수) > Clustering(클러스터링)**을 선택합니다.
2. 매개변수를 구성한 다음 **Submit(제출)**을 클릭합니다.

표 77: 클러스터링 매개변수

매개변수	설명
Device-Management- Channel IP Address(디바이스-관리-채널 IP 주소)	(읽기 전용) DefensePro 디바이스 관리 채널의 IP 주소입니다.[1]
Device-Management-Channel Default Gateway(디바이스-관리-채널 기본 게이트웨이)	(읽기 전용) 디바이스 관리 채널의 기본 게이트웨이입니다.[1]

표 77: 클러스터링 매개변수(계속)

매개변수	설명
Device-Management- Channel Netmask(디바이스-관리-채널 넷마스크)	(읽기 전용) 디바이스 관리 채널의 네트워크 마스크입니다.[1]
Cluster-Master IP Address(클러스터-마스터 IP 주소)	클러스터 마스터의 IP 주소입니다. 즉, 클러스터 멤버가 연결하는 IP 주소입니다. 이 DefensePro 인스턴스가 클러스터 *마스터*가 되도록 **Device-Management-Channel IP Address(디바이스-관리-채널 IP 주소)** 필드에 값을 지정합니다. 이 DefensePro 인스턴스가 클러스터 *멤버*가 되도록 마스터 DefensePro 인스턴스의 **Device-Management-Channel IP Address(디바이스-관리-채널 IP 주소)**를 지정합니다. **주의: Submit(제출)**을 클릭한 후에 **Cluster State(클러스터 상태)**가 **Disabled(사용 안 함)**인 경우에만 값을 변경할 수 있습니다.
Cluster State(클러스터 상태)	클러스터 또는 클러스터 멤버십의 상태입니다. 값: ● Enabled(사용)—다음 중 하나입니다. — 이 DefensePro 인스턴스가 마스터인 경우—클러스터를 사용합니다. — 이 DefensePro 인스턴스가 클러스터 멤버인 경우—클러스터와 결합합니다. ● Disabled(사용 안 함)—다음 중 하나입니다. — 이 DefensePro 인스턴스가 마스터인 경우—클러스터를 사용하지 않도록 설정하고 클러스터와의 관계를 단절합니다. — 이 DefensePro 인스턴스가 클러스터 멤버인 경우—클러스터를 제외합니다. 기본값: Disabled(사용 안 함)

1 – Firepower 부트스트랩 XML 파일에서 이 값을 정의합니다. DefensePro for Cisco Firepower 인스턴스는 초기화할 때마다 부트스트랩 XML 파일을 읽습니다.

5장 – 클래스 관리

*클래스*는 DefensePro에서 동일한 유형의 엔티티로 구성되는 요소 그룹을 정의합니다.

이 장에는 다음 섹션이 포함되어 있습니다.

- 네트워크 클래스 구성, 121페이지
- 상황 그룹 클래스 구성, 122페이지
- 애플리케이션 클래스 구성, 123페이지
- MAC 주소 클래스 구성, 124페이지
- SGT 클래스 구성, 124페이지

다음을 기반으로 클래스를 구성할 수 있습니다.

- **네트워크**—네트워크 보호 정책에서 트래픽을 분류합니다.
- **상황 그룹**—네트워크 보호 정책에서 트래픽을 분류합니다.
- **애플리케이션 포트**—레이어 4 대상 포트를 기반으로 애플리케이션을 정의하거나 수정합니다.
- **MAC 주소**—소스 또는 대상이 투명한 네트워크 디바이스인 트래픽을 분류합니다.
- **SGT**—DefensePro for Cisco Firepower 9300에 대한 SGT(Security Group Tags)를 구성합니다.

클래스를 생성하거나 수정하고 나면 컨피그레이션이 APSolute Vision 데이터베이스에 저장됩니다. 디바이스에 다운로드할 컨피그레이션을 활성화해야 합니다. 디바이스의 현재 클래스 컨피그레이션도 볼 수 있습니다. 생성한 후에는 클래스의 이름이나 애플리케이션 클래스의 컨피그레이션을 수정할 수 없습니다.

네트워크 클래스 구성

DefensePro for Cisco Firepower 9300에서 네트워크 보호 정책의 네트워크 클래스를 사용하여 소스 또는 대상 트래픽과 일치시킬 수 있습니다. 네트워크 클래스는 이름으로 식별되며 네트워크 주소 및 IPv4 마스크 또는 IPv6 접두부로 정의합니다.

네트워크 클래스를 구성하려면

1. *Configuration(컨피그레이션)* 관점에서 **Class(클래스) > Network(네트워크)**를 선택합니다.
2. 네트워크 클래스를 추가하거나 수정하려면 다음 중 하나를 수행합니다.
   - 클래스를 추가하려면  (Add(추가)) 버튼을 클릭합니다.
   - 클래스를 편집하려면 테이블의 항목을 두 번 클릭합니다.
3. 네트워크 클래스 매개변수를 구성한 다음 **Submit(제출)**을 클릭합니다.
4. 디바이스에서 컨피그레이션 변경을 활성화하려면 **Update Policies(정책 업데이트)**()를 클릭합니다.

표 78: 네트워크 클래스 매개변수

매개변수	설명
Network Name	네트워크 클래스의 이름입니다. 네트워크 이름은 대/소문자를 구분합니다. 네트워크 이름은 IP 주소일 수 없습니다. 최대 문자 수: 64
Entry Type	네트워크를 서브넷 및 마스크로 정의할지 아니면 IP 범위로 정의할지 지정합니다. 값: IP Mask(IP 마스크), IP Range(IP 범위) 값: IP Mask(IP 마스크), IP Range(IP 범위)
Network Type	값: IPv4, IPv6
Network Address	네트워크 주소.
Prefix	다음 방법 중 하나로 입력할 수 있는 서브넷의 마스크입니다. ● 점으로 구분된 10진수 표기법으로 된 서브넷 마스크—예를 들면, 255.0.0.0 또는 255.255.0.0입니다. ● 마스크 비트 수인 IP 접두부는—예를 들면, 8 또는 16입니다.

상황 그룹 클래스 구성

상황 그룹 클래스를 사용하여 네트워크 세그먼트를 정의할 수 있습니다. 보안 정책의 트래픽을 분류하는 데 사용합니다.

각 DefensePro 디바이스에서는 최대 64개의 상황 그룹 클래스를 지원합니다. 각 상황 그룹 클래스에는 최대 32개의 개별 태그와 32개의 범위를 포함할 수 있습니다. 즉, 실제로 각 DefensePro 디바이스에서는 최대 64개[2]의 정의를 지원합니다.

상황 그룹 클래스를 구성하려면

1. *Configuration(컨피그레이션)* 관점에서 **Class(클래스) > Context Group(상황 그룹)**을 선택합니다.
2. 다음 중 하나를 수행합니다.
   - 항목을 추가하려면 (Add(추가)) 버튼을 클릭합니다.
   - 항목을 편집하려면 테이블의 항목을 두 번 클릭합니다.
3. 매개변수를 구성한 다음 **Submit(제출)**을 클릭합니다.
4. 디바이스에서 컨피그레이션 변경을 활성화하려면 **Update Policies(정책 업데이트)**( )를 클릭합니다.

표 79: 상황 그룹 클래스 매개변수

매개변수	설명
Context Group Name(상황 그룹 이름)	그룹의 이름 최대 문자 수: 19

표 79: 상황 그룹 클래스 매개변수(계속)

매개변수	설명
Group Mode(그룹 모드)	값: • Discrete(개별)—디바이스의 인터페이스 매개변수에 정의된 개별 상황 그룹입니다. • Range(범위)—디바이스의 인터페이스 매개변수에 정의된 순차적 상황 그룹 번호의 그룹입니다. 기본값: Discrete(개별)
Tag(태그) (이 매개변수는 **Discrete(개별)** 모드에서만 사용할 수 있습니다.)	상황 그룹 번호입니다. 값: 0-4095
Range From(시작 범위) (이 매개변수는 **Range(범위)** 모드에서만 사용할 수 있습니다.)	범위의 첫 번째 상황 그룹입니다. 값: 0-4095 **참고:** 상황 그룹을 생성한 후에는 값을 수정할 수 없습니다.
Range To(종료 범위) (이 매개변수는 **Range(범위)** 모드에서만 사용할 수 있습니다.)	범위의 마지막 상황 그룹입니다. 값: 0-4095

애플리케이션 클래스 구성

애플리케이션 클래스는 UDP 및 TCP 트래픽의 레이어-4 포트 그룹입니다. 각 클래스는 고유 이름으로 식별되며 단일 클래스에 멀티 레이어-4 포트를 정의할 수 있습니다. 표준 애플리케이션의 미리 정의된 애플리케이션 클래스를 수정할 수 없지만, 클래스의 항목은 추가할 수 있습니다. *Application Port Group(애플리케이션 포트 그룹)* 테이블에 사용자 정의 클래스를 추가하고 수정할 수 있습니다.

애플리케이션 클래스를 구성하려면

1. *Configuration(컨피그레이션)* 관점에서 **Class(클래스) > Application(애플리케이션)**을 선택합니다.
2. 애플리케이션 클래스를 추가하거나 수정하려면 다음 중 하나를 수행합니다.
   - 클래스를 추가하려면  (Add(추가)) 버튼을 클릭합니다.
   - 클래스를 편집하려면 테이블의 항목을 두 번 클릭합니다.
3. 애플리케이션 클래스 매개변수를 구성한 다음 **Submit(제출)**을 클릭합니다.
4. 디바이스에서 컨피그레이션 변경을 활성화하려면 **Update Policies(정책 업데이트)**()를 클릭합니다.

표 80: 애플리케이션 클래스 매개변수

매개변수	설명
Ports Group Name(포트 그룹 이름)	애플리케이션 포트 그룹의 이름입니다. 여러 범위를 동일한 포트 그룹과 연결하려면 그룹에 포함할 모든 범위에 동일한 이름을 사용합니다. Application Port Group(애플리케이션 포트 그룹) 테이블에서 각 범위는 이름이 같은 개별 행으로 표시됩니다.

표 80: 애플리케이션 클래스 매개변수(계속)

매개변수	설명
Type of Entry(항목 유형)	(읽기 전용) 값: System Defined(시스템 정의됨), User Defined(사용자 정의됨)
From L4 Port(시작 L4 포트)	범위의 첫 번째 포트입니다.
To L4 Port(종료 L4 포트)	범위의 마지막 포트입니다. 단일 포트가 있는 그룹을 정의하려면 **From L4 Port(시작 L4 포트)**와 **To L4 Port(종료 L4 포트)** 매개변수에 동일한 값을 설정합니다.

MAC 주소 클래스 구성

MAC 그룹은 소스 또는 대상이 투명한 네트워크 디바이스인 트래픽을 식별합니다.

MAC 주소 클래스를 구성하려면

1. *Configuration(컨피그레이션)* 관점에서 **Class(클래스) > Address(주소)**를 선택합니다.
2. MAC 주소 클래스를 추가하거나 수정하려면 다음 중 하나를 수행합니다.
   - 클래스를 추가하려면 (Add(추가)) 버튼을 클릭합니다.
   - 클래스를 편집하려면 테이블의 항목을 두 번 클릭합니다.
3. MAC 그룹의 이름 및 해당 그룹과 연결된 MAC 주소를 입력한 다음 **Submit(제출)**을 클릭합니다.
4. 디바이스에서 컨피그레이션 변경을 활성화하려면 **Update Policies(정책 업데이트)**( )를 클릭합니다.

SGT 클래스 구성

각 DefensePro에는 사용하도록 설정된 SGT(Security Group Tags)가 0개 또는 한 개 있을 수 있습니다.

SYN 플러드 보호 모듈에서 조사할 패킷을 수신하고 패킷에 SGT가 포함되어 있는 경우 DefensePro에서 패킷의 SGT를 DefensePro 컨피그레이션에서 사용하도록 설정된 SGT로 바꿉니다. DefensePro에 사용하도록 설정된 SGT가 *없거나* 조사할 패킷에 SGT가 포함되지 *않으면* DefensePro에서 패킷을 바꾸지 않고 조사합니다.

참고

- 각 DefensePro에서는 최대 16개의 SGT를 지원합니다.
- 지정된 시간에 하나의 SGT 값만 사용할 수 있습니다.
- SGT 상태(사용/사용 안 함)를 변경하려면 정책 업데이트 조치를 적용해야 합니다.

SGT를 구성하려면

1. *Configuration(컨피그레이션)* 관점에서 **Class(클래스) > SGT**를 선택합니다.
2. 다음 중 하나를 수행합니다.
   - 항목을 추가하려면 (Add(추가)) 버튼을 클릭합니다.
   - 항목을 편집하려면 테이블의 항목을 두 번 클릭합니다.
3. 매개변수를 구성한 다음 **Submit(제출)**을 클릭합니다.
4. 디바이스에서 컨피그레이션 변경을 활성화하려면 **Update Policies(정책 업데이트)**()를 클릭합니다.

표 81: SGT 클래스 매개변수

매개변수	설명
Name	SGT의 이름입니다. 최대 문자 수: 20
Value	숫자로 된 SGT 값입니다. 값: 0-65535 기본값: 0
Status	값: Enabled(사용), Disabled(사용 안 함) 기본값: Disabled(사용 안 함) **참고:** DefensePro 컨피그레이션에 사용하도록 설정된 SGT 값이 있지만 다른 SGT 값을 사용하는 경우 DefensePro에서 이전에 사용하도록 설정한 값을 사용하지 않도록 설정하고 적절한 메시지를 발행합니다.

6장 – DefensePro 네트워크 보호 정책 관리

네트워크 보호 정책은 *보호 프로필*을 사용하여 구성된 네트워크를 보호합니다. 각 네트워크 보호 정책에서는 미리 정의된 네트워크 세그먼트에 적용된 하나 이상의 보호 *프로필*을 사용합니다. 또한 각 정책에는 공격이 탐지될 때 수행할 조치가 포함되어 있습니다.

네트워크 보호 정책 및 프로필을 구성하기 전에 **Setup(설정) > Security Settings(보안 설정)**에서 필요한 모든 보호를 사용하도록 설정하고 해당 전역 보호 매개변수를 구성했는지 확인합니다.

참고: *네트워크 보호 정책* 및 *네트워크 정책*은 APSolute Vision과 문서에서 서로 번갈아가며 사용할 수 있습니다.

표 82 - DefensePro 보호, 127페이지에서는 DefensePro for Cisco Firepower 9300 버전 1.01에서 지원하는 보호에 대해 설명합니다.

표 82: DefensePro 보호

보호	설명
DoS Shield(DoS 실드)	DoS 효과를 초래할 수 있는 알려진 플러드 공격 및 플러드 공격 툴로부터 보호합니다.
동작 기반 DoS (Behavioral DoS)	제로 데이 DoS/DDoS 플러드 공격으로부터 보호합니다.
SYN 보호	SYN 쿠키를 사용하여 SYN 플러드 공격으로부터 보호합니다.
DNS 보호	제로 데이 DNS 플러드 공격으로부터 보호합니다.

네트워크 보호 정책 구성

각 네트워크 보호 정책은 다음 두 부분으로 구성됩니다.

- 보호 네트워크 세그먼트를 정의하는 분류.
- 일치하는 네트워크 세그먼트에서 공격이 탐지되면 적용되는 조치. 조치는 네트워크 세그먼트에 적용된 보호 프로필과 악성 트래픽 차단 여부를 정의합니다. 악성 트래픽에 대해 항상 보고됩니다.

참고: *네트워크 보호 정책*과 *네트워크 정책* 두 용어는 APSolute Vision과 문서에서 번갈아 사용될 수 있습니다.

구성할 수 있는 최대 네트워크 보호 정책 수는 DefensePro 버전에 따라 달라집니다. DefensePro for Cisco Firepower 9300에서 최대 50개의 정책을 구성할 수 있습니다.

정책을 구성하기 전에 다음을 구성했는지 확인합니다.

- 보호 네트워크 세그먼트를 정의하는 데 필요한 클래스.
- 네트워크 보호 프로필. 자세한 내용은 다음을 참조하십시오.
  - 네트워크 보호를 위한 시그니처 보호 구성, 130페이지
  - 네트워크 보호를 위한 BDoS 프로필 구성, 142페이지
  - 네트워크 보호를 위한 SYN 프로필 구성, 145페이지
  - 네트워크 보호를 위한 DNS 플러드 보호 프로필 구성, 150페이지

주의: 정책을 구성할 때 APSolute Vision에서 컨피그레이션 변경사항을 저장하지만, 컨피그레이션 변경사항을 디바이스에 다운로드하지 않습니다. 디바이스에 변경사항을 적용하려면 컨피그레이션 변경사항을 활성화해야 합니다. *최신 변경사항 활성화*는 *정책 업데이트*라고도 합니다.

네트워크 보호 정책을 구성하려면

1. *Configuration(컨피그레이션)* 관점에서 **Network Protection(네트워크 보호) > Network Protection Policies(네트워크 보호 정책)**를 선택합니다.
2. 다음 중 하나를 수행합니다.
   - 항목을 추가하려면 (Add(추가)) 버튼을 클릭합니다.
   - 테이블의 항목을 편집하려면 항목을 두 번 클릭합니다.
3. 네트워크 보호 정책 매개변수를 구성한 다음 **Submit(제출)**을 클릭합니다.
4. 디바이스에서 컨피그레이션 변경을 활성화하려면 **Update Policies(정책 업데이트)**( )를 클릭합니다.

표 83: 네트워크 보호 정책: 일반 매개변수

매개변수	설명
Enabled	정책 사용 여부를 지정합니다.
Policy Name	네트워크 보호 정책의 이름입니다. 최대 문자 수: 19 **주의:** 이름에는 쉼표(,)가 포함되지 않아야 합니다.

표 84: 네트워크 보호 정책: 분류 매개변수

매개변수	설명
SRC Network Input	**SRC Network(SRC 네트워크)** 매개변수의 입력 방법입니다. 값: ● From List(목록에서)—**SRC Network(SRC 네트워크)** 매개변수는 구성된 모든 네트워크 클래스를 포함하는 드롭다운 목록입니다(*Configuration (컨피그레이션)* 관점, **Classes(클래스) > Networks(네트워크)**). ● User-Defined Value(사용자 정의 값)—**SRC Network(SRC 네트워크)** 매개변수는 사용자 정의 IP 주소를 포함할 수 있는 텍스트 필드입니다. 기본값: From List(목록에서)
SRC Network	정책에서 사용하는 패킷의 소스입니다. **SRC Network Input(SRC 네트워크 입력)**이 **From List(목록에서)**이면 목록에서 필수 값을 선택합니다. **SRC Network Input(SRC 네트워크 입력)**이 **User-Defined Value(사용자 정의 값)**이면 IP 주소를 입력합니다. *임의의* 네트워크를 지정하려면 필드에 **임의** 값을 포함하거나 비어 있을 수 있습니다.

표 84: 네트워크 보호 정책: 분류 매개변수(계속)

매개변수	설명
DST Network Input	**DST 네트워크(DST Network)** 매개변수의 입력 방법입니다. 값: ● From List(목록에서)—**DST Network(DST 네트워크)** 매개변수는 구성된 네트워크 클래스를 모두 포함하는 드롭다운 목록입니다(*Configuration (컨피그레이션)* 관점, **Classes(클래스) > Networks(네트워크)**). ● User-Defined Value(사용자 정의 값)—**DST Network(DST 네트워크)** 매개변수는 사용자 정의 IP 주소를 포함할 수 있는 텍스트 필드입니다. 기본값: From List(목록에서)
DST Network	정책에서 사용하는 패킷의 대상입니다. **DST Network Input(DST 네트워크 입력)**이 **From List(목록에서)**이면 목록에서 필수 값을 선택합니다. **DST Network Input(DST 네트워크 입력)**이 **User-Defined Value(사용자 정의 값)**이면 IP 주소를 입력합니다. *임의의* 네트워크를 지정하려면 필드에 **임의** 값을 포함하거나 비어 있을 수 있습니다.
Direction	정책이 관련된 트래픽의 방향입니다. 값: ● One Way(단방향)—정책의 네트워크 정의와 일치하는 세션에 보호가 적용되며 소스에서 시작하여 대상으로 적용됩니다. ● Two Way(양방향)—방향과 관계없이 정책의 네트워크 정의와 일치하는 세션에 보호가 적용됩니다. 기본값: One Way(단방향)
Context	정책에서 사용하는 상황 그룹 클래스입니다. 값: ● *Classes(클래스) 탭에 표시된 상황 그룹 클래스입니다.* ● *None(없음).*

표 85: 네트워크 보호 정책: 조치 매개변수

매개변수	설명
Protection Profiles	(컨피그레이션이 아니라 테이블에 표시됨) 이 정책에 정의된 네트워크 세그먼트에 적용되는 프로필입니다.
BDoS Profile	이 정책에 정의된 네트워크 세그먼트에 적용되는 BDoS 프로필입니다. **참고:** 인접한 버튼을 클릭하면 프로필을 추가하고 수정할 수 있는 대화 상자를 열 수 있습니다.
DNS Profile	이 정책에 정의된 네트워크 세그먼트에 적용되는 DNS 보호 프로필입니다. **참고:** 인접한 버튼을 클릭하면 프로필을 추가하고 수정할 수 있는 대화 상자를 열 수 있습니다.
Signature Protection Profile	이 정책에 정의된 네트워크 세그먼트에 적용되는 시그니처 보호 프로필입니다. **참고:** 인접한 버튼을 클릭하면 프로필을 추가하고 수정할 수 있는 대화 상자를 열 수 있습니다.
SYN Flood Profile	이 정책에 정의된 네트워크 세그먼트에 적용되는 SYN 플러드 프로필입니다. **참고:** 인접한 버튼을 클릭하면 프로필을 추가하고 수정할 수 있는 대화 상자를 열 수 있습니다.

표 85: 네트워크 보호 정책: 조치 매개변수(계속)

매개변수	설명
Action	이 정책이 적용되는 모든 공격의 기본 조치입니다. 값: ● Block and Report(차단 및 보고)—악성 트래픽이 종료되고 보안 이벤트가 생성되어 기록됩니다. ● Report Only(보고만 수행)—악성 트래픽이 대상에 전달되고 보안 이벤트가 생성되어 기록됩니다. 기본값: Block and Report(차단 및 보고) **참고:** 시그니처별 조치가 정책의 기본 조치보다 우선합니다.

표 86: 네트워크 보호 정책 패킷 보고 설정 매개변수

매개변수	설명
Packet Reporting	디바이스에서 오프라인 분석을 위해 샘플링된 공격 패킷을 APSolute Vision에 전송할지를 지정합니다. 기본값: Disabled(사용 안 함) **주의:** 여기에서 이 기능이 사용하도록 설정되는 경우 기능이 적용되려면 전역 설정을 사용하도록 설정해야 합니다(*Configuration(컨피그레이션)* 관점, **Setup(설정) > Reporting Settings(보고 설정) > Advanced Reporting Settings(고급 보고 설정) > Packet Reporting and Packet Trace(패킷 보고 및 패킷 추적) > Enable Packet Reporting(패킷 보고 사용)**).
Packet Reporting Configuration on Policy Takes Precedence	이 정책의 패킷 보고 기능 컨피그레이션이 관련된 프로필의 패킷 보고 기능의 컨피그레이션보다 우선합니다.

하나 이상의 네트워크 보호 정책을 삭제하려면

1. *Configuration(컨피그레이션)* 관점에서 **Network Protection(네트워크 보호) > Network Protection Policies(네트워크 보호 정책)**를 선택합니다.
2. 하나 이상의 행을 선택합니다.
3.  (Delete Network Protection Policy(네트워크 보호 정책 삭제)) 버튼을 클릭합니다.

네트워크 보호를 위한 시그니처 보호 구성

시그니처 보호에서는 각 패킷을 시그니처 데이터베이스에 저장된 시그니처 집합과 비교하여 네트워크 중심 공격, OS(Operation System) 중심 공격 및 애플리케이션 중심 공격을 탐지하고 방지합니다.

이 섹션에 포함되는 주제는 다음과 같습니다.

- DefensePro for Cisco Firepower의 시그니처 보호, 131페이지
- 시그니처 보호가 포함된 컨피그레이션 고려사항, 131페이지
- 시그니처 보호 프로필 구성, 132페이지
- 시그니처 보호 시그니처 구성, 134페이지
- 시그니처 보호 특성 구성, 139페이지

DefensePro for Cisco Firepower의 시그니처 보호

DefensePro for Cisco Firepower에서 All-DoS-Shield 프로필 사용 및/또는 사용자 정의 시그니처 추가를 통해 시그니처 보호를 구성할 수 있습니다.

All-DoS-Shield 프로필의 시그니처는 OMPC(Offset Mask Pattern Condition) 매개변수로 제한됩니다. OMPC 매개변수는 패턴 조회에 대한 규칙을 정의하는 공격 매개변수 집합입니다. 자세한 내용은 표 95 - 시그니처 매개변수 필터링: OMPC 매개변수, 138페이지를 참조하십시오.

Radware에서는 필드 설치를 위해 미리 정의된 시그니처 프로필 집합이 있는 All-DoS-Shield 프로필을 제공합니다.

All-DoS-Shield 프로필은 Radware에서 관련 새 OMPC 시그니처를 생성할 때 업데이트됩니다.

All-DoS-Shield 프로필은 편집할 수 없지만 환경 요구사항에 따라 새 프로필을 생성할 수 있습니다. 예를 들어, 소규모의 커스텀 시그니처 집합만 사용해야 하는 경우 해당 시그니처가 있는 새 프로필과 새 위협 유형 특성(표 96 - 특성 유형, 140페이지)을 생성할 수 있습니다.

참고

- Radware VRT(Vulnerability Research Team)에서는 취약성, DDoS 툴 및 DDoS 악성코드를 연구조사, 처리 및 차단하는 작업을 담당합니다.
- 새 시그니처를 생성하는 데 지원이 필요한 경우 서비스 계약에 따라 관련 Radware 부서에 문의할 수 있습니다.

시그니처 보호가 포함된 컨피그레이션 고려사항

상황 그룹, 애플리케이션 포트 및 물리적 포트를 사용하도록 정책을 구성할 수 있습니다.

정책 및 보호에 대한 방향 설정이 암시하는 내용은 표 87 - 정책 방향의 의미, 131페이지를 참조하십시오.

시그니처 보호 프로필을 포함하는 정책은 방향을 *One Way(단방향)* 또는 *Two Way(양방향)*로 설정하여 구성할 수 있습니다.

보호는 *Inbound(인바운드)*, *Outbound(아웃바운드)* 또는 *In-Outbound(인-아웃바운드)*의 방향 값으로 구성할 수 있습니다.

대부분의 공격(예: 웜 감염)은 인바운드 패턴을 통해 탐지되지만 일부 공격에서는 감염된 호스트에서 시작하는 아웃바운드 패턴을 검사해야 합니다. 예를 들어, 트로이에서는 감염된 호스트에서 시작하는 아웃바운드 패턴을 검사해야 합니다.

소스 = *임의* 및 대상 = *임의*로 구성된 정책은 *인-아웃바운드* 공격만 검사합니다.

표 87: 정책 방향의 의미

정책 방향	정책 조치	패킷 방향	시그니처 방향		
			인바운드	아웃바운드	인바운드 또는 아웃바운드
시작에서 종료로	단방향	외부에서 내부로	Inspect	무시	Inspect
		내부에서 외부로	무시	Inspect	무시
시작에서 종료로	양방향	외부에서 내부로	Inspect	무시	Inspect
		내부에서 외부로	무시	Inspect	Inspect
높은 연결성	해당 없음	해당 없음	무시	무시	Inspect

시그니처 보호 프로필 구성

시그니처 보호 프로필에는 보호하려는 네트워크 세그먼트의 *규칙*이 하나 이상 포함되어 있습니다. 각 규칙은 시그니처 데이터베이스에 쿼리를 정의합니다. DefensePro에서는 규칙 집합과 일치하는 시그니처 데이터베이스의 보호를 활성화합니다. 사용자 정의 프로필은 업데이트된 시그니처 데이터베이스를 다운로드할 때마다 업데이트됩니다.

시그니처 보호 프로필을 구성하려면 전역 DoS 실드 매개변수를 구성해야 합니다. 자세한 내용은 DoS 실드 보호 구성, 100페이지를 참조하십시오.

DefensePro 디바이스에서 최대 300개의 시그니처 보호 프로필을 구성할 수 있습니다. 프로필의 각 규칙에는 다양한 *특성 유형*의 항목이 하나 이상 포함될 수 있습니다. 규칙은 다음 로직을 기반으로 시그니처 데이터베이스에 쿼리를 정의합니다.

- 동일한 *유형*의 값은 논리 OR과 결합됩니다.
- 다른 *유형*의 값은 논리 AND와 결합됩니다.

규칙은 프로필에서 논리 OR과 결합됩니다.

모든 필터 사이의 시그니처에 있는 관계는 논리 AND입니다.

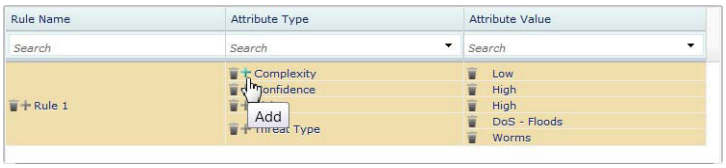
참고: 프로필의 규칙은 *암시적*입니다. 즉, 값을 정의할 때 선택한 특정 특성과 일치하는 모든 시그니처와 해당 유형의 특성이 *없는* 모든 시그니처를 *결합*합니다. 이 논리를 사용하면 보호 네트워크와 관련될 수 있는 시그니처가 (SOC를 통해) 네트워크의 애플리케이션과 명시적으로 연결되지 않아도 포함*될 수* 있습니다.

시그니처 보호 프로필을 구성하려면

1. *Configuration(컨피그레이션)* 관점에서 **Network Protection(네트워크 보호) > Signature Protection(시그니처 보호) > Profiles(프로필)**를 선택합니다.
2. 다음 중 하나를 수행합니다.
   - 프로필을 추가하려면 (Add(추가)) 버튼을 클릭하고 프로필 이름을 입력합니다.
   - 프로필을 편집하려면 테이블의 항목을 두 번 클릭합니다.
   - 프로필에 구성된 보호와 연결된 시그니처 목록을 표시하려면 테이블의 항목을 두 번 클릭하고 **Show Matching Signatures(일치하는 시그니처 표시)**를 클릭합니다.
3. 프로필의 규칙을 다음과 같이 구성합니다.
   - 새 규칙을 구성하려면 다음을 수행합니다.
     a. 규칙 테이블 위에 있는 (Add(추가)) 버튼을 클릭합니다.
     b. **Rule Name(규칙 이름)** 텍스트 필드에 새 규칙의 이름을 입력합니다.
     c. **Attribute Type(특성 유형)** 드롭다운 목록에서 필요한 값을 선택합니다.
     d. **Attribute Value(특성 값)** 드롭다운 목록에서 필요한 값을 선택합니다.
     e. **Submit(제출)**를 클릭합니다.

- 규칙의 특성 유형 및/또는 특성 값을 편집하려면 다음을 수행합니다.
  a. 테이블의 *Rule Name(규칙 이름)* 열에서 마우스 커서를 관련 규칙의 이름 위로 이동하고 작은 Add(추가) 버튼을 클릭합니다. 선택한 규칙의 이름으로 채워진 *Add Signature Profile Rule (시그니처 프로필 규칙 추가)* 탭이 열립니다.

  b. **Attribute Type(특성 유형)** 드롭다운 목록에서 필요한 값을 선택합니다.
  c. **Attribute Value(특성 값)** 드롭다운 목록에서 필요한 값을 선택하거나 입력합니다.
  d. **Submit(제출)**를 클릭합니다.
- 규칙의 특성 값을 편집하려면 다음을 수행합니다.
  a. 표의 *Attribute Type(특성 유형)* 열에서 마우스 커서를 관련 규칙의 관련 특성 유형 위로 이동하고 작은 Add(추가) 버튼을 클릭합니다. 선택한 특성 유형의 이름과 규칙의 이름으로 채워진 *Add Signature Profile Rule(시그니처 프로필 규칙 추가)* 탭이 열립니다.



  b. **Attribute Value(특성 값)** 드롭다운 목록에서 필요한 값을 선택하거나 입력합니다.
  c. **Submit(제출)**를 클릭합니다.

참고: 또는 기존 프로필의 특성 및/또는 특성 유형을 편집하려면 다음을 수행할 수 있습니다(APSolute Vision 버전 3.20 이전에서 지원됨).

  a. 규칙 테이블 위에 있는 (Add(추가)) 버튼을 클릭합니다.
  b. **Rule Name(규칙 이름)** 텍스트 필드에서 수정하려는 규칙의 이름을 입력합니다.
  c. **Attribute Type(특성 유형)** 드롭다운 목록에서 필요한 값을 선택합니다.
  d. **Attribute Value(특성 값)** 드롭다운 목록에서 필요한 값을 선택합니다.
  e. **Submit(제출)**를 클릭합니다.

4. 필요한 대로 3단계를 반복하여 프로필의 추가 규칙, 규칙의 추가 특성 또는 기존 특성의 추가 값을 구성합니다.
5. 시그니처 프로필 컨피그레이션을 저장하려면 **Submit(제출)**을 클릭합니다.

표 88: 시그니처 프로필 매개변수

매개변수	설명
Profile Name	시그니처 프로필의 이름입니다. 새 프로필의 프로필 이름을 입력합니다.

표 88: 시그니처 프로필 매개변수(계속)

매개변수	설명
Number of Matching Signatures	(읽기 전용) 프로필과 일치하는 시그니처 수입니다. 일치하는 시그니처 수는 특성 유형의 일치 방법에 따라 다릅니다(특성 유형 속성 보기 및 수정, 141페이지 참조). 최소 일치 방법은 오름차순-내림차순 레벨의 특성 값이 있는 복잡성, 신뢰도 및 위험과 같은 특성 유형에만 적합합니다. 최소는 *특성 값*에 하위 레벨 특성 값의 결과가 포함됨을 나타냅니다. 예를 들어, *Risk(위험)* 특성 유형에서 *Match Method(일치 방법)*가 *Minimum(최소)*인 경우 *Attribute Value High(특성 값 높음)*는 *Info(정보)*, *Low(낮음)* 또는 *Medium(중간)*이 아니라 *High(높음)*와만 일치시킵니다. *Minimum(최소)*은 *Complexity(복잡성)*, *Confidence(신뢰도)* 및 *Risk(위험)*입니다.
Show Matching Signatures	이 버튼은 프로필을 편집할 때만 표시됩니다. 프로필에 구성된 보호와 연결된 시그니처 목록을 표시하려면 클릭합니다.

표 89: 시그니처 프로필 규칙 테이블 매개변수

매개변수	설명
표에 선택한 프로필에 구성된 규칙의 세부 정보가 표시됩니다. 각 규칙에는 두 개 이상의 특성 유형이 포함될 수 있으며, 각 특성 유형에는 하나 이상의 특성 값이 포함될 수 있습니다.	
Rule Name	시그니처 프로필 규칙의 이름입니다.
Attribute Type	미리 정의된 특성 유형 목록으로서, 새 공격을 정의할 때 고려해야 하는 다양한 요소를 기반으로 합니다.
Attribute Value	정의된 특성 유형의 값입니다.

시그니처 보호 시그니처 구성

시그니처는 보호 프로필의 구성 요소입니다. 각 시그니처에는 악의적인 패킷과 처리 방법을 결정하는 보호 *필터*와 *특성*이 하나 이상 포함되어 있습니다.

트래픽에서 악성 패킷의 시그니처가 인식되고 나면 시그니처 설정 매개변수를 통해 악성 패킷을 추적하고 처리하는 방법을 정의합니다. 각 공격은 시그니처와 일치할 때 패킷을 처리하는 방법을 정의하는 *추적* 기능에 연결됩니다. 이 기능의 주된 용도는 패킷이 유해한지 판별하고 적절한 조치를 적용하는 것입니다.

시그니처 테이블에서는 Radware 정의 시그니처 및 사용자 정의 시그니처를 볼 수 있는 필터가 제공됩니다. 기준에 맞는 모든 시그니처가 시그니처 테이블에 표시될 수 있도록 필터링 기준을 정의할 수 있습니다. 사용자 정의 시그니처도 추가할 수 있습니다.

시그니처 유형은 사용자 정의 시그니처와 Radware 정의 시그니처의 두 가지가 있습니다. Radware 정의 시그니처는 정적 시그니처라고 합니다. 사용자 정의 시그니처만 편집하고 제거할 수 있습니다. Radware 정의 시그니처의 경우 일반 매개변수만 편집할 수 있습니다.

참고: 사용자 정의 시그니처만 편집하고 제거할 수 있습니다. Radware 정의 시그니처의 경우 일반 매개변수만 편집할 수 있습니다.

주의: DefensePro에서는 특성이 완전히 일치하지 않아도 기존 프로필에 사용자 정의 시그니처를 자동으로 추가할 수 있습니다. 사용자 정의 시그니처를 구성하는 경우 *기본* 특성 외에 다른 특성을 지정해야 합니다. 더 많이 지정할수록 좋습니다. 사용자 정의 시그니처의 기본 특성은 위험 및 신뢰도뿐입니다. 추가 특성을 지정하지 않으면 사용자 정의 시그니처의 기타 모든 특성은 NULL입니다. 사용자 정의 시그니처의 기타 모든 특성이 NULL이면 DefensePro에서 기존 *정적* 프로필(예: DoS-ALL, DoS-SSL, 사기 및 All-DoS-Shield)과 시그니처를 일치시키며 누락된 특성(NULL인 특성)을 기본값을 갖는 기존 특성으로 처리합니다. 그러면 DefensePro가 정적 프로필에 사용자 정의 시그니처를 추가하게 되지만, 이 동작은 적절하지 않습니다. 따라서 Radware에서는 최대한 많은 추가 특성을 지정하도록 권장하여 DefensePro에서 사용자 정의 시그니처를 잘못 사용하는 것을 방지합니다.

시그니처 보호 시그니처를 보려면

> *Configuration(컨피그레이션)* 관점에서 **Network Protection(네트워크 보호) > Signature Protection(시그니처 보호) > Signature(시그니처)**를 선택합니다.

참고: 시그니처를 모두 보려면 테이블 열의 맨 위에 있는 텍스트 상자를 선택 취소한 다음 (Filter(필터)) 버튼을 클릭합니다.

시그니처 보호 시그니처를 보고 시그니처 매개변수로 테이블을 필터링하려면

1. *Configuration(컨피그레이션)* 관점에서 **Network Protection(네트워크 보호) > Signature Protection(시그니처 보호) > Signature(시그니처)**를 선택합니다.
2. **Filter by ID(ID로 필터링)** 옵션 버튼을 선택합니다.
3. 열 표제 아래 상자에 검색 기준을 입력합니다.
4. (Filter(필터)) 버튼을 클릭합니다.

시그니처 보호 시그니처를 보고 특성 매개변수로 테이블을 필터링하려면

1. *Configuration(컨피그레이션)* 관점에서 **Network Protection(네트워크 보호) > Signature Protection(시그니처 보호) > Signature(시그니처)**를 선택합니다.
2. **Filter by Attribute(특성으로 필터링)** 옵션 버튼을 선택합니다.
3. 열 표제 아래 상자에 검색 기준을 입력합니다.

참고: 예를 들어,**특성 유형**의 경우, 새 공격을 정의할 때 고려해야 하는 다양한 요소를 기반으로 하는 미리 정의된 특성 유형 목록에서 선택합니다.

4. (Filter(필터)) 버튼을 클릭합니다.

시그니처 보호 시그니처를 구성하려면

1. *Configuration(컨피그레이션)* 관점에서 **Network Protection(네트워크 보호) > Signature Protection(시그니처 보호) > Signature(시그니처)**를 선택합니다.
2. 시그니처를 추가하거나 편집하려면 다음 중 하나를 수행합니다.
   - 시그니처를 추가하려면 (Add(추가)) 버튼을 클릭합니다.
   - 시그니처를 편집하려면 필수 시그니처를 표시한 다음 시그니처를 두 번 클릭합니다.
3. 매개변수를 구성한 다음 **Submit(제출)**을 클릭합니다.

표 90: 시그니처 매개변수

매개변수	설명
Signature Name	시그니처의 이름입니다. 최대 문자 수: 29
Signature ID	(읽기 전용) 시스템에서 시그니처에 할당한 ID입니다.
Enabled	보호 프로필에서 시그니처를 사용할 수 있는지 지정합니다.
Tracking Time	활성 임계값을 측정하는 시간(밀리초)입니다. 임계값을 초과하는 패킷 수가 구성된 추적 시간 내에 디바이스를 통과하는 경우 디바이스에서 이를 공격으로 간주합니다. 기본값: 1000
Tracking Type	(읽기 전용) DefensePro에서 공격 중에 삭제하거나 차단할 트래픽을 결정하는 방법을 지정합니다. 값: Sampling(샘플링)—이 옵션은 DoS 실드 메커니즘에 맞게 설계되었습니다.
Action Mode	공격이 탐지되면 DefensePro에서 수행하는 조치입니다. 값: ● Drop(삭제)—DefensePro에서 패킷을 폐기합니다. ● Report Only(보고만 수행)—DefensePro에서 정의된 대상에 패킷을 전달합니다. ● Reset Source(소스 재설정)—DefensePro에서 TCP 재설정 패킷을 패킷 소스 IP 주소에 전송합니다. ● Reset Destination(대상 재설정)—DefensePro에서 TCP 재설정 패킷을 대상 주소에 전송합니다. ● Reset Bidirectional(양방향 재설정)—DefensePro에서 TCP 재설정 패킷을 패킷 소스 IP와 패킷 대상 IP 주소 둘 다에 전송합니다. 기본값: Drop(삭제) **참고:**
Direction	보호 검사 경로입니다. 보호를 통해 입력 트래픽만, 출력 트래픽만 또는 둘 다를 검사할 수 있습니다. 값: Inbound(인바운드), Outbound(아웃바운드), Inbound & Outbound (인바운드 및 아웃바운드) 기본값: Inbound & Outbound(인바운드 및 아웃바운드)

표 90: 시그니처 매개변수(계속)

매개변수	설명
Activation Threshold	각 추적 시간에 허용되는 최대 공격 패킷 수입니다. 공격 패킷이 추적 시간 내에 전송되면 합법적인 트래픽으로 인식됩니다. **Tracking Type(추적 유형)**의 값이 **Drop All(모두 삭제)**이면 DefensePro에서 이 매개변수를 무시합니다. 기본값: 50
Drop Threshold	공격이 탐지된 후 DefensePro에서 과도한 트래픽 삭제를 시작하는 최소 PPS입니다. **Tracking Type(추적 유형)**의 값이 **Drop All(모두 삭제)**이면 프로필에서 이 매개변수를 무시합니다. 기본값: 50
Termination Threshold	공격 PPS 비율이 이 임계값 미만이 되면 프로필에서 공격을 활성 모드에서 비활성 모드로 변경합니다. **Tracking Type(추적 유형)**의 값이 **Drop All(모두 삭제)**이면 DefensePro에서 이 매개변수를 무시합니다. 기본값: 50
Packet Reporting	오프라인 분석을 위해 샘플링된 공격 패킷을 APSolute Vision에 전송할 수 있습니다. 기본값: Disabled(사용 안 함)

표 91: 시그니처: 공격 설명

매개변수	설명
(읽기 전용) 정적 시그니처의 설명입니다. 사용자 정의 시그니처의 설명을 구성할 수 없습니다.	

표 92: 시그니처: 필터 테이블

매개변수	설명
필터는 보호의 구성 요소이며, 각각 미리 정의된 트래픽을 스캔하여 분류하는 특정 공격 시그니처가 하나 포함되어 있습니다. 필터에서는 스캔한 패킷이 시그니처 데이터베이스의 공격 시그니처와 일치하는지 확인합니다. 각 커스텀 보호에 맞는 커스텀 필터를 정의합니다. 보호 정의를 맞춤 설정할 때 다른 보호의 필터를 사용할 수 없습니다. 필터를 추가하려면 **Add New Filter(새 필터 추가)**를 선택합니다. 필터를 편집하려면 필터를 선택하고 **Edit Filter(필터 편집)**를 선택합니다.	

표 93: 시그니처: 특성 테이블

매개변수	설명
시그니처에 대해 선택하는 특성에 따라 규칙 생성 프로세스에서 사용하는 공격 특성이 결정됩니다. 특성 값을 추가하려면 표에서 (Add(추가)) 버튼을 클릭합니다.	

표 94: 시그니처의 필터 매개변수: 일반 매개변수

매개변수	설명
각 필터에는 지정된 이름과 지정된 프로토콜 속성 매개변수가 있습니다.	
Filter Name	시그니처 필터의 이름입니다.
Protocol	사용된 프로토콜입니다. 값: ● ICMP ● ICMPv6 ● IP ● Non IP(비IP) ● TCP ● UDP 기본값: IP **주의: Non IP(비IP)** 옵션을 선택하지 마십시오. 예상치 못한 결과가 초래됩니다.
Source Application Port	UDP 및 TCP 트래픽 전용입니다. 미리 정의된 애플리케이션 포트 그룹 목록에서 선택합니다.
Destination Application Port	UDP 및 TCP 트래픽 전용입니다. 미리 정의된 애플리케이션 포트 그룹 목록에서 선택합니다.

표 95: 시그니처의 필터 매개변수: OMPC 매개변수

매개변수	설명
OMPC(Offset Mask Pattern Condition) 매개변수는 패턴 검색의 규칙을 정의하는 공격 매개변수 집합입니다. OMPC 규칙에서는 고정 옵셋 마스킹을 사용하는 최대 4바이트의 고정 크기 패턴을 검색합니다. 공격 시그니처가 고정 옵셋의 데이터/페이로드에 있는 패턴 또는 TCP/IP 헤더 필드인 경우 공격을 인식하는 데 유용합니다.	
OMPC Condition	OMPC 조건입니다. 값: ● 같음 ● 보다 큼 ● 해당 없음 ● 보다 작음 ● Not Equal(같지 않음) 기본값: Not Applicable(해당 없음)
OMPC Length	OMPC(Offset Mask Pattern Condition) 데이터의 길이입니다. 값: ● 해당 없음 ● 1 Byte(1바이트) ● 2 Bytes(2바이트) ● 3 Bytes(3바이트) ● 4 Bytes(4바이트) 기본값: 1 Byte(1바이트)

표 95: 시그니처의 필터 매개변수: OMPC 매개변수(계속)

매개변수	설명
OMPC Offset	IP/TCP 헤더에서 데이터 검사를 통해 특정 비트 검색을 시작하는 패킷의 위치입니다. 값: 0-1513 기본값: 0
OMPC Offset Relative to	선택한 옵셋이 관련된 OMPC 옵셋을 지정합니다. 값: ● None(없음) ● IP Header(IP 헤더) ● IP Data(IP 데이터) ● L4 Data(L4 데이터) ● L4 Header(L4 헤더) ● Ethernet(이더넷) 기본값: None(없음)
OMPC Pattern	OMPC 규칙을 통해 패킷에서 찾으려고 하는 고정 크기 패턴입니다. 값: 16진수 조합(0–9, a–f). 값은 **OMPC Length(OMPC 길이)** 매개변수로 정의됩니다. **OMPC Pattern(OMPC 패턴)** 정의에는 8개의 기호가 포함됩니다. **OMPC Length (OMPC 길이)**가 4바이트 미만이면 끝을 0으로 채웁니다. 예를 들어, **OMPC Length(OMPC 길이)**가 2바이트이면 **OMPC Pattern(OMPC 패턴)**은 abcd0000일 수 있습니다. 기본값: 00000000
OMPC Mask	OMPC 데이터의 마스크입니다. 값: 16진수 조합(0–9, a–f). 값은 OMPC Length(OMPC 길이) 매개변수로 정의됩니다. **OMPC Mask(OMPC 마스크)** 정의에는 8개의 기호가 포함됩니다. **OMPC Length(OMPC 길이)** 값이 4바이트 미만이면 끝을 0으로 채웁니다. 예를 들어, **OMPC Length(OMPC 길이)**가 2바이트이면 OMPC 마스크는 abcd0000일 수 있습니다. 기본값: 00000000

시그니처 보호 특성 구성

특성은 *규칙 기반* 프로필 컨피그레이션의 프로세스에 있는 보호 정책 집합의 구성 요소입니다. 특성은 새 공격을 정의할 때 고려하는 다양한 요소(예: 환경, 애플리케이션, 위협 레벨, 위험 레벨 등)를 기반으로 하는 유형에 따라 구성합니다.

각 시그니처에는 여러 다른 유형의 특성이 할당됩니다. Radware VRT(Vulnerability Research Team)에서는 시그니처를 생성할 때 시그니처를 설명하는 방법으로 특성을 할당합니다.

기존 특성을 사용하거나 새 특성을 추가하거나 목록에서 특성을 제거할 수 있습니다.

참고: 특성 유형의 속성을 볼 수 있으며, 복잡성, 신뢰도 및 위험과 같은 특성 유형의 경우 *Match Method(일치 방법)* (*Minimum(최소)* 또는 *Exact(정확)*)도 지정할 수 있습니다. 자세한 내용은 특성 유형 속성 보기 및 수정, 141페이지를 참조하십시오.

특성은 시그니처 데이터베이스에서 파생되며 모든 업데이트와 함께 동적으로 추가됩니다.

시그니처 보호 특성을 구성하려면

1. *Configuration(컨피그레이션)* 관점에서 **Network Protection(네트워크 보호) > Signature Protection(시그니처 보호) > Attribute(특성)**를 선택합니다.
2. 특성을 보려면 다음을 수행하십시오.
   - 모든 특성을 보려면 모두를 선택하고 (Search(검색)) 버튼을 클릭합니다.
   - 단일 특성 유형의 특성을 보려면 특성 유형을 선택하고 (Search(검색)) 버튼을 클릭합니다.
3. 새 특성을 추가하려면 다음을 수행합니다.
   a. (Add(추가)) 버튼을 클릭합니다.
   b. 특성 유형을 선택하고 특성 이름을 입력합니다.
   c. **Submit(제출)**를 클릭합니다.

표 96: 특성 유형

특성 유형	설명
애플리케이션	이와 같은 익스플로잇에 취약한 애플리케이션입니다. 예: 웹 서버, 메일 서버, 브라우저 매개변수는 선택사항입니다. 즉, 특성에 값이 포함되거나 포함되지 않을 수 있습니다. 값이 여러 개일 수 있습니다.
복잡성	공격 검색 메커니즘의 일부로 수행되는 분석 레벨입니다. 매개변수의 값은 단 하나여야 합니다. 값: ● Low(낮음)—이 시그니처는 디바이스 성능에 영향을 거의 미치지 않습니다. ● High(높음)—이 시그니처는 디바이스 성능에 상당한 영향을 미칩니다.
확신	공격을 신뢰할 수 있는 신뢰도 레벨입니다. 신뢰도 레벨은 공격과 연결된 오탐 레벨과 반대입니다. 예를 들어, 공격 신뢰도 레벨이 높음으로 설정된 경우 오탐 레벨은 낮습니다. 매개변수는 필수입니다. 매개변수의 값은 단 하나여야 합니다. 값: Low(낮음), High(높음), Medium(중간)
그룹	맞춤 설정된 공격 그룹을 생성할 수 있습니다.
플랫폼	이와 같은 익스플로잇에 취약한 운영 체제입니다. 예: Windows, Linux, Unix 매개변수는 선택사항입니다. 즉, 특성에 값이 포함되거나 포함되지 않을 수 있습니다. 값이 여러 개일 수 있습니다.

표 96: 특성 유형(계속)

특성 유형	설명
위험	공격과 연관된 위험입니다. 예를 들어, 네트워크에 영향을 미치는 공격은 매우 심각하므로 위험이 높은 공격으로 정의됩니다. 매개변수는 필수입니다. 매개변수의 값은 단 하나여야 합니다. 값: Info(정보), Low(낮음), Medium(중간), High(높음)
서비스	이와 같은 익스플로잇에 취약한 프로토콜입니다. 예: FTP, HTTP, DNS 매개변수는 선택사항입니다. 즉, 매개변수에 값이 포함되거나 포함되지 않을 수 있습니다. 매개변수의 값은 단 하나여야 합니다.
대상	위협의 대상(클라이언트 측 또는 서버 측)입니다.
Threat Type(위협 유형)	시그니처를 가장 잘 설명하는 위협입니다. 예: 플러드, 웜 값이 여러 개일 수 있습니다.

특성 유형 속성 보기 및 수정

디바이스에서 지원하는 특성 유형의 다음 속성을 볼 수 있습니다.

- **Multiple Values in Attack(공격의 여러 값)**—특성 유형이 한 시그니처에 여러 값을 포함할 수 있는지 지정합니다.
- **Multiple Values in Rule(규칙의 여러 값)**—특성 유형이 한 시그니처 프로필 규칙에 여러 값을 포함할 수 있는지 지정합니다.
- **Multiple Values in Static(정적의 여러 값)**—특성 유형이 시그니처 파일의 시그니처에 여러 값을 포함할 수 있는지 지정합니다.
- **Match Method(일치 방법)**—오름차순-내림차순 레벨의 특성 값이 있는 **Complexity(복잡성)**, **Confidence(신뢰도)** 및 **Risk(위험)**와 같은 *특성 유형*에만 적합합니다.

  값:

  - Minimum(최소)—*특성 값*에 하위 레벨 특성 값의 결과가 포함됨을 나타냅니다. 예를 들어, *Risk(위험)* 특성 유형에서 *Match Method(일치 방법)*가 **Minimum(최소)**인 경우 *Attribute Value High(특성 값 높음)*는 **Info(정보)**, **Low(낮음)** 또는 **Medium(중간)**이 아니라 **High(높음)**와만 일치시킵니다. **Minimum(최소)**은 **Complexity(복잡성)**, **Confidence(신뢰도)** 및 **Risk(위험)**입니다.
  - Exact(정확)—**Attribute Value(특성 값)**에서 고유 결과만 사용하도록 지정합니다. 예를 들어, **Attribute Type(특성 유형)**이 **Risk(위험)**이고 **Match Method(일치 방법) Exact (정확)**을 사용하는 경우 **Attribute Value(특성 값) High(높음)**에서는 위험이 높은 결과만 사용합니다.

Complexity(복잡성), **Confidence(신뢰도)** 및 **Risk(위험)** 특성 유형의 **Match Method(일치 방법)**를 변경할 수 있습니다.

디바이스에서 지원하는 특성 유형을 보려면

> *Configuration(컨피그레이션)* 관점에서 **Network Protection(네트워크 보호) > Signature Protection(시그니처 보호) > Attribute(특성) > Attribute Type Properties(특성 유형 속성)**를 선택합니다.

복잡성, 신뢰도 및 위험 특성 유형의 일치 방법을 변경하려면

1. *Configuration(컨피그레이션)* 관점에서 **Network Protection(네트워크 보호) > Signature Protection(시그니처 보호) > Attribute(특성) > Attribute Type Properties(특성 유형 속성)**를 선택합니다.
2. 특성 유형을 두 번 클릭합니다.
3. **Match Method(일치 방법)** 드롭다운 목록에서 **Minimum(최소)** 또는 **Exact(정확)**를 선택합니다.
4. **Submit(제출)**을 클릭합니다.

네트워크 보호를 위한 BDoS 프로필 구성

동작 기반 DoS 프로필을 구성할 때 대역폭과 할당량 설정을 구성해야 합니다. 초기 베이스라인과 공격 탐지 민감도는 대역폭과 할당량 값을 기반으로 하므로, 해당 값을 올바르고 정확하게 설정하는 것이 중요합니다.

BDoS 프로필을 구성하려면 BDoS 보호를 사용해야 합니다(*Configuration(컨피그레이션)* 관점, **Setup(설정) > Security Settings(보안 설정) > BDoS Protection(BDoS 보호)**).

DefensePro for Cisco Firepower 9300에서는 최소 50개의 프로필을 지원합니다. 동작 기반 DoS 프로필이 포함된 정책에 권장되는 설정은 다음과 같습니다.

- 소스 = 임의, 정책 네트워크 및 대상 = 보호 네트워크인 네트워크를 사용하여 동작 기반 DoS 프로필을 포함하는 규칙을 구성합니다. 각각 특정 서버 세그먼트를 보호하는 여러 동작 기반 DoS 규칙을 생성하는 것이 좋습니다(예: DNS 서버 세그먼트, 웹 서버 세그먼트, 메일 서버 세그먼트 등). 그러면 정상 트래픽 베이스라인의 학습을 최적화할 수 있습니다.
- 디바이스에서 인바운드 및 아웃바운드 방향에 상관없이 전역적으로 통계를 수집하므로 소스 및 대상을 *임의*로 설정하여 네트워크를 정의하는 것이 좋습니다. 그러면 공격을 탐지할 때 민감도가 저하됩니다.
- 규칙의 방향을 *단방향*으로 설정하면 규칙에서 입력되는 공격만 방지합니다. 규칙의 방향을 *양방향*으로 설정하면 규칙에서 수신 및 발신되는 공격을 모두 방지합니다. 두 경우 모두 탐지를 최적화하기 위해 수신 및 발신되는 패턴의 트래픽 통계를 수집합니다.

지정된 공간 유형 또는 값을 건너뛰도록 사용 공간 바이패스를 구성할 수 있습니다. 자세한 내용은 BDoS 사용 공간 바이패스 구성, 106페이지를 참조하십시오.

BDoS 프로필을 구성하려면

1. *Configuration(컨피그레이션)* 관점에서 **Network Protection(네트워크 보호) > BDoS Profiles(BDoS 프로필)**를 선택합니다.
2. 다음 중 하나를 수행합니다.
   - 프로필을 추가하려면 (Add(추가)) 버튼을 클릭합니다.
   - 프로필을 편집하려면 테이블의 항목을 두 번 클릭합니다.
3. 매개변수를 구성한 다음 **Submit(제출)**을 클릭합니다.

표 97: BDoS 프로필 매개변수

매개변수	설명
Profile Name(프로필 이름)	BDoS 프로필의 이름입니다.
Enable Transparent Optimization(투명 최적화 사용)	투명 최적화 사용 여부를 지정합니다. 일부 네트워크 환경은 패킷을 삭제하는 데 더욱 민감하므로(예: VoIP) IPS 디바이스에서 합법적인 트래픽을 삭제할 가능성을 최소화해야 합니다. 이 투명 최적화는 BDoS 폐쇄 피드백 반복 중에 최종 공간이 생성될 때까지 발생할 수 있습니다. **참고:** 투명 최적화를 사용하면 몇 초 간에 걸쳐 최종 공간이 생성될 때까지 프로필에서 공격을 차단하지 않습니다.

표 98: BDoS 프로필 플러드 보호 설정 매개변수

매개변수	설명
SYN 플러드	적용할 네트워크 플러드 보호 유형을 선택합니다.
TCP ACK + FIN 플러드	
TCP RST 플러드	
TCP SYN + ACK 플러드	
TCP 프래그멘테이션 플러드	
UDP 플러드	
ICMP 플러드	
IGMP 플러드	

표 99: BDoS 프로필 대역폭 매개변수

매개변수	설명
Inbound Traffic(인바운드 트래픽)	링크에서 예상되는 최대 인바운드 트래픽 대역폭(Kbit/s)입니다. DefensePro에서는 대역폭과 할당량 설정에서 초기 베이스라인을 파생합니다. 값: 1-2,147,483,647 **주의:** 동작 기반 DoS 보호를 시작하도록 이 설정을 구성해야 합니다.
Outbound Traffic(아웃 바운드 트래픽)	링크에서 예상되는 최대 아웃바운드 트래픽 대역폭(Kbit/s)입니다. DefensePro에서는 대역폭과 할당량 설정에서 초기 베이스라인을 파생합니다. 값: 1-2,147,483,647 **주의:** 동작 기반 DoS 보호를 시작하도록 이 설정을 구성해야 합니다.

표 100: BDoS 프로필 할당량 설정 매개변수

매개변수	설명
Radware에서는 기본값을 자동으로 사용할 수 있도록 처음에 이 필드를 공백으로 두도록 권장합니다. 프로필을 생성한 후 기본값을 보려면 테이블의 항목을 두 번 클릭합니다. 그런 다음 네트워크 성능에 따라 할당량 값을 조정할 수 있습니다. **주의:** 대역폭 설정(*인바운드 트래픽* 또는 *아웃바운드 트래픽*)을 변경하면 할당량 설정이 대역폭에 적절한 기본값으로 자동 변경됩니다. **참고:** 각 값은 프로토콜당 최대 볼륨을 나타내므로 총 할당량 값은 100%를 초과할 수 있습니다.	
TCP	총 트래픽 중에서 예상되는 최대 TCP 트래픽의 백분율입니다.
UDP	총 트래픽 중에서 예상되는 최대 UDP 트래픽의 백분율입니다.
ICMP	총 트래픽 중에서 예상되는 최대 ICMP 트래픽의 백분율입니다.
IGMP	총 트래픽 중에서 예상되는 최대 IGMP 트래픽의 백분율입니다.

표 101: BDoS 프로필 고급 매개변수

매개변수	설명
UDP Packet Rate Sensitivity (UDP 패킷 비율 민감도)	패킷 비율 탐지 민감도—즉, BDoS에서 UDP PPS 비율 값(베이스라인 값 및 현재 값)을 고려하는 범위입니다. 이 매개변수는 BDoS UDP 보호에만 적절합니다. 값: ● Disable(비활성화) ● Low(낮음) ● Medium(중간) ● High(높음) 기본값: Low(낮음) **참고:** 특정 레거시 버전에서 이 매개변수의 라벨은 **정규화 레벨**로 지정됩니다.

표 102: BDoS 프로필 패킷 보고 및 추적 설정 매개변수

매개변수	설명
Packet Report(패킷 보고)	프로필에서 오프라인 분석을 위해 샘플링된 공격 패킷을 APSolute Vision에 보내는지 지정합니다. **참고:** 이 기능이 사용되는 경우 기능이 적용되려면 전역 설정을 사용하도록 설정해야 합니다(*Configuration(컨피그레이션)* 관점, **Setup(설정) > Reporting Settings(보고 설정) > Advanced Reporting Settings(고급 보고 설정) > Packet Reporting and Packet Trace(패킷 보고 및 패킷 추적) > Enable Packet Reporting(패킷 보고 사용)**).
Packet Trace(패킷 추적)	*이 버전에서는 패킷 추적 기능을 지원하지 않습니다.*

네트워크 보호를 위한 SYN 프로필 구성

SYN 프로필은 SYN 플러드 공격으로부터 방어합니다.

SYN 플러드 공격 중에, 공격자가 TCP 핸드쉐이크를 완료하지 않고 새 TCP 연결을 요청하거나 TCP 핸드쉐이크는 완료하지만 데이터는 요청하지 않는 TCP SYN 패킷의 볼륨을 보냅니다. 그러면 서버 연결 큐가 가득 채워져, 합법적인 TCP 사용자에 대한 서비스를 거부하게 됩니다.

SYN 프로필을 구성하기 전에 다음을 확인합니다.

- SYN 플러드 보호가 사용하도록 설정되고 전역 매개변수가 구성되어 있습니다(*Configuration(컨피그레이션)* 관점, **Setup(설정) > Security Settings(보안 설정) > SYN Flood Protection(SYN 플러드 보호)**).
- 전역 설정을 변경할 수 있습니다. SYN 플러드 전역 설정은 디바이스의 모든 프로필에 적용됩니다. 자세한 내용은 전역 SYN 플러드 보호 구성, 107페이지를 참조하십시오.

SYN 보호 프로필을 구성하려면

1. *Configuration(컨피그레이션)* 관점에서 **Network Protection(네트워크 보호) > SYN Protection Profiles(SYN 보호 프로필)**를 선택합니다.
2. 프로필을 추가 또는 수정하려면 다음 중 하나를 수행합니다.
   - 프로필을 추가하려면 (Add(추가)) 버튼을 클릭합니다. 프로필 이름을 입력하고 **Submit(제출)**을 클릭합니다.
   - 프로필을 편집하려면 테이블의 항목을 두 번 클릭합니다.
3. 프로필에 SYN 플러드 보호를 추가하려면 다음을 수행합니다.
   a. (Add(추가)) 버튼을 클릭합니다.
   b. *Profile Name(프로필 이름)* 드롭다운 목록에서 보호를 선택합니다.
   c. **Submit(제출)**을 클릭합니다.
4. 프로필의 추가 SYN 플러드 보호를 정의하려면 **Go To Protection Table(보호 테이블로 이동)**을 클릭합니다.

참고: SYN 프로필에는 네트워크 보호 정책에 적용할 모든 SYN 플러드 보호가 포함되어야 합니다.

표 103: SYN 보호 프로필 매개변수

매개변수	설명
Profile Name(프로필 이름)	(읽기 전용) 프로필의 이름입니다.
SYN Protection Table(SYN 보호 테이블)	선택한 프로필에 적용된 보호가 포함되어 있습니다. 보호를 추가하려면 테이블에서 (Add(추가)) 버튼을 클릭하고 보호 이름을 선택한 다음, **Submit(제출)**을 클릭합니다. **참고:** 각 네트워크 보호 정책에서 SYN 프로필을 하나만 사용할 수 있습니다. 따라서 규칙에 적용할 모든 보호가 해당 정책에 지정된 프로필에 포함되어 있는지 확인하십시오.
Go To Protection Table(보호 테이블로 이동)	SYN 보호를 추가하고 수정할 수 있는 *SYN Protection(SYN 보호)* 대화 상자를 엽니다.

SYN 플러드 보호 정의

SYN 플러드 보호를 정의한 후 SYN 플러드에 추가할 수 있습니다.

SYN 보호를 구성하려면

1. *Configuration(컨피그레이션)* 관점에서 **Network Protection(네트워크 보호) > SYN Protection Profile(SYN 보호 프로필) > SYN Protection(SYN 보호)**을 선택합니다.
2. 보호를 추가 또는 수정하려면 다음 중 하나를 수행합니다.
   - 보호를 추가하려면 (Add(추가)) 버튼을 클릭합니다.
   - 보호를 편집하려면 테이블의 항목을 두 번 클릭합니다.
3. 매개변수를 구성한 다음 **Submit(제출)**을 클릭합니다.

표 104: SYN 플러드 보호 매개변수

매개변수	설명
Protection Name(보호 이름)	컨피그레이션 및 보고를 위해 공격을 쉽게 식별하기 위한 이름입니다. **참고:** 미리 정의된 SYN 보호는 가장 일반적인 애플리케이션, FTP, HTTP, HTTPS, IMAP, POP3, RPS, RTSP, SMTP 및 텔넷에 사용할 수 있습니다. 임계값은 Radware에서 미리 정의합니다. 이러한 공격의 임계값을 변경할 수 있습니다.
Protection ID(보호 ID)	(읽기 전용) 보호에 할당된 ID 번호입니다.
Application Port Group(애플리케이션 포트 그룹)	보호할 애플리케이션을 나타내는 TCP 포트 그룹입니다. 목록에서 미리 정의된 포트 그룹을 선택하거나 임의의 포트를 선택하도록 필드를 빈 상태로 둡니다.
Activation Threshold(활성화 임계값)	특정 대상에서 초당 받은 SYN 패킷 수로, 이 수를 초과하면 DefensePro에서 차단 조치를 시작합니다. 값: 1-150,000 기본값: 2500
Termination Threshold(종료 임계값)	지정된 *Tracking Time(추적 시간)*[1] 동안 특정 대상에서 초당 받은 SYN 패킷 수로, 이 수 미만이 되면 DefensePro에서 차단 조치를 중지합니다. 값: 0-150,000 기본값: 1500
Risk(위험)	보고 용도로 이 공격에 할당된 위험 레벨입니다. 값: Info(정보), Low(낮음), Medium(중간), High(높음) 기본값: Low(낮음)
Source Type(소스 유형)	(읽기 전용) SYN 보호가 미리 정의(정적)되어 있는지 아니면 사용자 정의(사용자) 보호인지 지정합니다.

1 – **Setup(설정) > Security Settings(보안 설정) > SYN Flood Protection(SYN 플러드 보호) > Tracking Time(추적 시간)**에서 이 값을 구성할 수 있습니다.

Radware-권장 검증 유형 값

표 105: 검증 유형 값 매개변수

프로토콜	Destination Port(대상 포트)	검증 유형
FTP_CNTL	21	ack
HTTP	80	request
HTTPS	443	request
IMAP	143	ack
POP3	110	ack
RPC	135	ack
RTSP	554	request
SMTP	25	ack
TELNET	23	ack

SYN 보호 프로필 매개변수 관리

SYN 보호 프로필을 정의한 후에 인증 매개변수를 구성할 수 있습니다.

기본적으로 DefensePro for Cisco Firepower 9300 버전 1.01에서는 안전한 재설정 인증 방법을 사용합니다. 즉, DefensePro에서 SYN 패킷을 수신하면 DefensePro에서 잘못된 순서 번호 필드를 쿠키로 사용하는 ACK 패킷으로 응답합니다. 클라이언트에서 RST와 쿠키로 응답하면 DefensePro에서 RST 패킷을 폐기하고 소스 IP 주소를 TCP 인증 테이블에 추가합니다. 동일한 소스의 다음 SYN 패킷(일반적으로 이전 SYN 패킷을 재전송)이 DefensePro를 통과하며, 서버에 대해 세션이 승인됩니다. DefensePro에서 지정된 시간 동안 소스 IP 주소를 저장합니다.

DefensePro for Cisco Firepower 9300 버전 1.01을 사용하면 다음 절차에 설명되어 있는 SYN 보호 프로필 매개변수도 수정할 수 있습니다.

SYN 보호 프로필 매개변수를 구성하려면

1. *Configuration(컨피그레이션)* 관점에서 **Network Protection(네트워크 보호) > SYN Protection Profile(SYN 보호 프로필) > Profiles Parameters(프로필 매개변수)**를 선택합니다.
2. 관련 프로필을 두 번 클릭합니다.
3. 매개변수를 구성한 다음 **Submit(제출)**을 클릭합니다.

표 106: SYN 플러드 보호 프로필 매개변수

매개변수	설명
Profile Name(프로필 이름)	(읽기 전용) 프로필의 이름입니다.
Use TCP Reset for Supported Protocols (지원되는 프로토콜에 대해 TCP 재설정 사용)	DefensePro에서 HTTP, HTTPS, SMTP 및 *커스텀 프로토콜* 트래픽에 대해 안전 재설정 방법이 아니라 TCP 재설정 방법을 사용하는지 지정합니다. Radware에서는 HTTP, HTTPS 및 SMTP 트래픽을 포함하는 대칭 및 인그레스 전용 환경에서 이 옵션을 사용하도록 권장합니다. 기본값: Disabled(사용 안 함)

표 106: SYN 플러드 보호 프로필 매개변수(계속)

매개변수	설명
HTTP 인증	
Use HTTP Authentication (HTTP 인증 사용)	DefensePro에서 SYN 쿠키를 사용하여 HTTP 트래픽의 전송 레이어를 인증한 다음 지정된 *HTTP 인증 방법*을 사용하여 HTTP 애플리케이션 레이어를 인증하는지 지정합니다. 값: ● Enabled(사용)—DefensePro에서 SYN 쿠키를 사용하여 HTTP 트래픽의 전송 레이어를 인증한 다음 지정된 *HTTP 인증 방법*을 사용하여 HTTP 애플리케이션 레이어를 인증합니다. ● Disabled(사용 안 함)—DefensePro에서 지정된 TCP *인증 방법*을 사용하여 HTTP 트래픽을 처리합니다. 기본값: Disabled(사용 안 함)
HTTP Authentication Method(HTTP 인증 방법)	프로필에서 애플리케이션 레이어의 HTTP 트래픽을 인증하는 데 사용하는 방법입니다. 값: ● 302-Redirect(302-리디렉션)—DefensePro에서 302- 리디렉션 응답 코드를 사용하여 HTTP 트래픽을 인증합니다. ● JavaScript—DefensePro에서 JavaScript 개체를 사용하여 HTTP 트래픽을 인증합니다. 이 개체는 DefensePro에서 생성합니다. 기본값: 302-Redirect(302-리디렉션) **참고:** ● 일부 공격 툴에서는 302-리디렉션 응답을 처리할 수 있습니다. *302-리디렉션* HTTP 인증 방법은 해당 툴을 사용하는 공격에는 효율적이지 않습니다. *JavaScript* HTTP 인증 방법에는 JavaScript를 지원하는 클라이언트 측 엔진이 필요하므로 JavaScript 옵션이 더 강력한 것으로 간주됩니다. 그러나 *JavaScript* 옵션에는 특정 시나리오에 해당하는 몇 가지 제한사항이 있습니다. ● *JavaScript* HTTP 인증 방법 사용 시 제한사항: — 브라우저에서 JavaScript 호출을 지원하지 않으면 브라우저에서 조사에 응답하지 않습니다. — JavaScript*만* 사용하는 다른 (기본) 페이지를 통해 하위 페이지로 보호 서버에 액세스하는 경우 사용자 세션이 실패합니다(즉, 브라우저에서 조사에 응답하지 않음). 예를 들어, 보호 서버에서 JavaScript 태그를 사용하여 요청되는 콘텐츠를 제공하면 DefensePro JavaScript가 원본 JavaScript 블록에 포함됩니다. 따라서 JavaScript 규칙을 위반하므로 결과적으로 조사에 실패합니다. 다음 예에서는 요청을 통해 보안 서버에 액세스합니다. 반환된 조사 페이지에는 다시 적절하지 않은 <script> 태그가 포함되므로 브라우저에서 리디렉션하지 않고 삭제합니다. <script> setTimeout(function(){ var js=document.createElement(“script”); js.src=”http://mysite.site.com.domain/service/appMy.jsp?dlid=12345”; document.getElementsByTagName(“head”)[0].appe n dChild(js); },1000); </script>

TCP 재설정

Radware에서는 HTTP, HTTPS 및 SMTP 트래픽을 포함하는 대칭 및 인그레스 전용 환경에서 TCP-재설정 옵션을 사용하도록 권장합니다.

주의: DefensePro에서 관련 RFC(HTTP, HTTPS 및 SMTP용)에 따라 TCP-재설정 메커니즘을 구현하면, 원래 연결을 재설정할 때(이 경우 TCP-재설정 메커니즘 사용) 새 연결이 자동으로 시작되어야 합니다. 이 RFC 요소를 완벽하게 준수하는 브라우저에서는 연결이 자동으로 다시 시작되므로, 사용자가 *인증 기간* 동안 예상되는 추가 레이턴시 없이 약 3초 간의 지연을 경험하게 됩니다. (인증 기간은 **TCP Authentication Table Aging(TCP 인증 테이블 에이징)** 매개변수를 통해 판별하며, 기본적으로 20분입니다.) 이 RFC 요소를 완벽하게 준수하지 않는 브라우저에서는 합법적인 사용자에게 연결이 재설정되므로 수동으로 연결을 재시도해야 함을 나타내는 알림이 전송됩니다. 재시도하고 나면 인증 기간 동안 예상되는 추가 레이턴시 없이 검색할 수 있습니다.

Use TCP Reset for Supported Protocols(지원되는 프로토콜에 TCP 재설정 사용) 확인란이 선택되면 DefensePro에서 인증 방법(DefensePro for Cisco Firepower 9300 1.01의 경우 Safe-Reset(안전-재설정)) 대신 HTTP, HTTPS, SMTP 및 *커스텀 프로토콜* 트래픽용 TCP 재설정 인증 방법을 사용합니다.

*커스텀 프로토콜*은 처리할 TCP 재설정 방법을 위해 정의하는 트래픽을 나타냅니다. 이 작업을 수행할 수 있도록 DefensePro에서는 두 개의 시스템 정의 애플리케이션 포트 그룹인 **TCPReset-ACK와 TCPReset-Data**를 노출합니다. 이러한 애플리케이션 포트 그룹은 레이어 4 포트 0(영)으로 정의된 더미 그룹입니다. (커스텀 프로토콜 트래픽을 정의하는 절차는 TCP 재설정 방법에 사용할 커스텀 프로토콜 트래픽을 정의하려면, 150페이지 절차를 참조하십시오.)

DefensePro에서 TCP 재설정 방법을 구현하면 DefensePro에서 다음 순서에 따라 패킷을 관련 애플리케이션 포트 그룹과 일치시킵니다.

1. HTTP
2. HTTPS
3. SMTP
4. TCPReset-Data
5. TCPReset-ACK

DefensePro에서는 관련 애플리케이션 포트 그룹 중 하나와 일치하는 첫 번째 패킷에 따라 세션의 패킷을 처리합니다.

TCP 재설정 옵션을 사용하는 경우 DefensePro에서 다음을 수행합니다.

1. SYN 패킷을 수신하면 DefensePro에서 추가 인증 매개변수(쿠키) 없이 원본 대상 IP 주소와 MAC를 사용하여 순서 번호 필드에 있는 쿠키와 SYN-ACK 패킷으로 응답합니다.
2. 응답이 쿠키를 사용하는 ACK이면 다음이 해당됩니다.
   - **TCPReset-Data** 애플리케이션 포트 그룹이 있는 HTTP나 HTTPS 트래픽 또는 *커스텀 프로토콜* 트래픽에서 DefensePro는 클라이언트의 첫 번째 데이터 패킷을 기다립니다. (DefensePro에서 첫 번째 데이터 패킷 전에 데이터가 없는 ACK를 수신하면 DefensePro에서 패킷을 삭제합니다.) DefensePro 디바이스에서 데이터를 수신하면 RST 패킷으로 응답하고 TCP 인증 테이블에 소스 IP 주소를 저장합니다.
   - **TCPReset-ACK** 애플리케이션 포트 그룹이 있는 SMTP 또는 *커스텀 프로토콜* 트래픽의 경우, DefensePro에서 RST 패킷으로 응답하고 TCP 인증 테이블에 소스 IP 주소를 저장합니다.

참고: HTTP, HTTPS 및 SMTP 소스에서 SYN을 다시 전송하여 RST 패킷에 자동으로 응답합니다. 즉, 소스에서 보호 서버와의 연결을 자동으로 다시 엽니다. 합법적인 클라이언트에서 재시도하여 보호 서버에 대한 새 연결을 열어야 합니다.

3. DefensePro에서 TCP 인증 테이블의 각 항목과 비교하여 각 SYN 패킷을 확인합니다. 일치하는 사항이 있으면 DefensePro에서 패킷을 다른 DefensePro 검사 모듈에 전달한 후, 나중에 SYN 패킷을 원래대로 대상에 전달하므로, 보호 서버에서 소스와의 연결을 엽니다.
4. DefensePro에서 소스를 인증하고 나면 DefensePro에서 *인증 기간* 중에 소스를 다시 조사하지 않습니다. (인증 기간은 **TCP Authentication Table Aging(TCP 인증 테이블 에이징)** 매개변수를 통해 판별하며, 기본적으로 20분입니다.)

참고

- DefensePro를 통해 동일한 소스에서 여러 SYN을 받으면 DefensePro에서 연결 중 하나가 인증될 때까지 SYN 패킷당 TCP 재설정 인증 프로세스를 구현합니다.
- DefensePro에서는 **HTTP** 애플리케이션 포트 그룹 및 **HTTPS** 애플리케이션 포트 그룹에 포함된 포트를 통한 트래픽에 대해 항상 TCPReset-Data 동작(위의 2단계)을 사용합니다.
- DefensePro에서는 **SMTP** 애플리케이션 포트 그룹에 포함된 포트를 통한 트래픽에 대해 항상 TCPReset-ACK 동작(위의 2단계)을 사용합니다.
- **Use HTTP Authentication(HTTP 인증 사용)** 및 **Use TCP Reset For Supported Protocols(지원되는 프로토콜에 TCP 재설정 사용)** 확인란을 모두 선택하는 경우 DefensePro에서 TCP 재설정 방법이 아니라 HTTP 인증 방법을 사용합니다.

TCP 재설정 방법에 사용할 커스텀 프로토콜 트래픽을 정의하려면

1. 다음과 같이 새 애플리케이션 포트 그룹을 생성합니다.
   a. *Configuration(컨피그레이션)* 관점에서 **Class(클래스) > Application(애플리케이션)**을 선택합니다.
   b. (Add(추가)) 버튼을 클릭합니다.
   c. *Ports Group Name(포트 그룹 이름)* 텍스트 상자에 필요한 TCP 재설정 동작에 따라 **TCPReset-ACK** 또는 **TCPReset-Data**를 입력합니다(위의 2단계 사용).
   d. **From L4 Port(시작 L4 포트)** 텍스트 상자에 범위에 있는 첫 번째 포트를 입력합니다.
   e. **To L4 Port(종료 L4 포트)** 텍스트 상자에 범위에 있는 마지막 포트를 입력합니다. 단일 포트가 있는 그룹을 정의하려면 **From L4 Port(시작 L4 포트)**와 **To L4 Port(종료 L4 포트)** 텍스트 상자에 동일한 값을 설정합니다.
   f. 디바이스에서 컨피그레이션 변경을 활성화하려면 **Update Policies(정책 업데이트)**()를 클릭합니다.
2. SYN 보호 프로필을 구성합니다(SYN 보호 프로필을 구성하려면, 145페이지를 참조하십시오).
3. 이전 단계의 SYN 보호 프로필에 맞게 SYN 보호를 구성(SYN 보호를 구성하려면, 146페이지 참조)하고 *Application Port Group(애플리케이션 포트 그룹)* 드롭다운 목록에서 필요에 따라 **TCPReset-ACK** 또는 **TCPReset-Data**를 선택합니다.

네트워크 보호를 위한 DNS 플러드 보호 프로필 구성

DNS 플러드 보호 프로필을 구성하려면 DNS 플러드 보호를 사용해야 합니다(*Configuration(컨피그레이션)* 관점, **Setup(설정) > Security Settings(보안 설정) > DNS Flood Protection(DNS 플러드 보호)**).

DNS 플러드 보호 프로필을 구성할 때 쿼리와 할당량 설정을 구성해야 합니다. 초기 베이스라인과 공격 탐지 민감도는 쿼리와 할당량 값을 기반으로 하므로, 해당 값을 올바르고 정확하게 설정하는 것이 중요합니다.

DNS 보호 프로필의 최대수를 조정할 수 있습니다(*Configuration(컨피그레이션)* 관점, **Setup(설정) > Advanced Parameters(고급 매개변수) > Tuning Parameters(조정 매개변수) > Security(보안) > Max. Number of DNS Policies(최대 DNS 정책 수)**). 기본값과 절대 최대값은 DefensePro 버전에 따라 다릅니다.

DNS 보호 프로필은 단방향 정책에서만 사용할 수 있습니다.

소스 = 임의, 공용 네트워크 및 대상 = 보호 네트워크인 네트워크를 사용하여 DNS 보호 프로필을 포함하는 규칙을 구성하는 것이 좋습니다.

지정된 공간 유형 또는 값을 건너뛰도록 사용 공간 바이패스를 구성할 수 있습니다.

DNS 보호 프로필을 구성하려면

1. *Configuration(컨피그레이션)* 관점에서 **Network Protection(네트워크 보호) > DNS Protection Profiles(DNS 보호 프로필)**를 선택합니다.
2. 다음 중 하나를 수행합니다.
   - 프로필을 추가하려면 (Add(추가)) 버튼을 클릭합니다.
   - 프로필을 편집하려면 테이블의 항목을 두 번 클릭합니다.
3. 매개변수를 구성한 다음 **Submit(제출)**을 클릭합니다.

표 107: DNS 보호 프로필: 일반 매개변수

매개변수	설명
Name(이름)	프로필의 이름.

표 108: DNS 보호 프로필: 쿼리 보호 및 할당량 매개변수

매개변수	설명
Radware에서는 기본값을 자동으로 사용할 수 있도록 처음에 이 필드를 공백으로 두도록 권장합니다. 프로필을 생성한 후 기본값을 보려면 테이블의 항목을 두 번 클릭합니다. 그런 다음 네트워크 성능에 따라 할당량 값을 조정할 수 있습니다. **참고:** 각 값은 프로토콜당 최대 볼륨을 나타내므로 총 할당량 값은 100%를 초과할 수 있습니다.	
A Query(A 쿼리)	보호할 DNS 쿼리 유형마다 할당량, 즉 전체 DNS 트래픽 중에서 예상되는 최대 DNS 트래픽 백분율을 지정하고 행에서 확인란을 선택합니다.
MX Query(MX 쿼리)	
PTR Query(PTR 쿼리)	
AAAA Query(AAAA 쿼리)	
Text Query(텍스트 쿼리)	
SOA Query(SOA 쿼리)	
NAPTR Query(NAPTR 쿼리)	
SRV Query(SRV 쿼리)	
Other Queries(기타 쿼리)	
Get Default Quotas(기본 할당량 확보)	**예상 DNS 쿼리 비율**을 지정한 다음 기본값을 하드 코딩하여 모든 할당량을 구성합니다.
Expected DNS Query Rate(예상 DNS 쿼리 비율)	DNS 쿼리의 예상 비율(초당 쿼리 수)입니다.

표 109: DNS 보호 프로필: 수동 트리거 매개변수

매개변수	설명
Use Manual Triggers(수동 트리거 사용)	프로필에서 학습된 베이스라인 대신 사용자 정의 DNS QPS 임계값을 사용하는지 지정합니다. 기본값: Disabled(사용 안 함)
Activation Threshold(활성화 임계값)	지정된 *활성화 기간* 후에 보호 대상 네트워크별 초당 총 쿼리 수이며, 이 값을 초과하면 DefensePro에서 공격이 진행 중인 것으로 간주합니다. DefensePro에서 공격을 감지하면 모든 소스 검사를 시작합니다. 지정된 *최대 QPS*(아래 참조) 이상이 되면 DefensePro가 보호 네트워크로 향하는 총 QPS 비율을 제한합니다. 값: 0-4,000,000 기본값: 0
Activation Period(활성화 기간)	단일 연결의 DNS 트래픽이 **활성화 임계값**을 초과하여, DefensePro에서 공격이 있는 것으로 간주하게 만드는 연속된 초 수입니다. 값: 1-30 기본값: 3
Termination Threshold(종료 임계값)	단일 연결에서 지정된 **종료 기간** 후의 초당 최대 쿼리 수입니다. 이 기간 후에는 DefensePro에서 공격이 있는 것으로 간주합니다. 값: 0-4,000,000 기본값: 0 **참고: 종료 임계값**은 **활성화 임계값** 이하여야 합니다.
Termination Period(종료 기간)	단일 연결의 DNS 트래픽이 **종료 임계값** 미만인 상태를 유지하여 DefensePro에서 공격이 종료된 것으로 간주하게 만드는 시간(초)입니다. 값: 1-30 기본값: 3
Max QPS(최대 QPS)	초당 허용되는 최대 DNS 쿼리 비율입니다. 값: 0-4,000,000 기본값: 0
Escalation Period(에스컬레이션 기간)	DefensePro에서 지정된 다음 차단 조치로 에스컬레이션하기 전에 기다리는 시간(초)입니다. 값: 0-30 기본값: 3

표 110: DNS 보호 프로필: 고급 보고 설정 매개변수

매개변수	설명
Packet Report(패킷 보고)	DefensePro에서 오프라인 분석을 위해 샘플링된 공격 패킷을 APSolute Vision에 보내는지 지정합니다. 기본값: Disabled(사용 안 함) **참고:** 이 기능이 사용되는 경우 기능이 적용되려면 전역 설정을 사용하도록 설정해야 합니다(*Configuration(컨피그레이션)* 관점, **Setup(설정) > Reporting Settings(보고 설정) > Advanced Reporting Settings(고급 보고 설정) > Packet Reporting and Packet Trace(패킷 보고 및 패킷 추적) > Enable Packet Reporting(패킷 보고 사용)**).
Packet Trace(패킷 추적)	*이 버전에서는 패킷 추적 기능을 지원하지 않습니다.*

표 111: DNS 보호 프로필: 조치 및 에스컬레이션 매개변수

매개변수	설명
참고: *Manual Triggers(수동 트리거)*옵션이 사용되지 *않은* 경우에만 디바이스에서 이 탭에 매개변수를 구현합니다.	
Profile Action(프로필 조치)	프로필이 공격 중에 DNS 트래픽에서 수행하는 조치입니다. 값: Block & Report(차단 및 보고), Report Only(보고만 수행) 기본값: Block & Report(차단 및 보고)
Max allowed QPS(허용된 최대 QPS)	*Manual Triggers(수동 트리거)* 옵션이 사용되지 *않은* 경우 초당 허용되는 최대 DNS 쿼리 비율입니다. 값: 0-4,000,000 기본값: 0 **참고:** *Manual Triggers(수동 트리거)* 옵션이 사용하도록 설정된 경우 **Max QPS(최대 QPS)**값(*Manual Triggers(수동 트리거)* 탭에 지정됨)이 우선순위를 갖습니다.
Signature Rate-limit Target (시그니처 비율 제한 대상)	프로필에서 베이스라인 이상을 차단하지 않는 실시간 시그니처와 일치하는 DNS 트래픽의 백분율입니다. 값: 0-100 기본값: 0

7장 – DefensePro 운영 상태 모니터링 및 제어

APSolute Vision의 온라인 DefensePro 모니터링은 네트워크 및 연결된 디바이스를 모니터링하고 분석하여 네트워크 성능에 영향을 미칠 수 있는 조건이 변경하는지 확인하는 NOC(Network Operating Center)의 일부로 제공됩니다.

이 섹션에 포함되는 주제는 다음과 같습니다.

- 일반 DefensePro 디바이스 정보 모니터링, 155페이지
- DefensePro 리소스 활용 모니터링, 156페이지
- Cisco SGT(Security Group Tag) 모니터링, 159페이지

일반 DefensePro 디바이스 정보 모니터링

Overview(개요) 탭에는 디바이스의 소프트웨어 버전 및 디바이스의 하드웨어 버전에 대한 정보를 포함하는 일반 디바이스 정보가 표시됩니다.

선택한 디바이스에 대한 일반 디바이스 정보를 표시하려면

> *Monitoring(모니터링)* 관점에서 **Operational Status(운영 상태) > Overview(개요)**를 선택합니다.

표 112: 개요: 기본 매개변수

매개변수	설명
Hardware Platform	이 디바이스의 하드웨어 플랫폼 유형입니다.
Uptime	일, 시간, 분 및 초로 지정되는 시스템 가동 시간입니다.
Base MAC Address	디바이스에 있는 첫 번째 포트의 MAC 주소입니다.

표 113: 개요: 시그니처 업데이트 매개변수

매개변수	설명
Radware Signature File Version	디바이스에 설치된 Radware 시그니처 파일의 버전입니다.

표 114: 개요: 소프트웨어 매개변수

매개변수	설명
Software Version	디바이스에 설치된 제품 소프트웨어의 버전입니다.
APSolute OS Version	디바이스에 설치된 APSolute OS 버전(예: 10.31-03.01:2.06.08)입니다.
Build	현재 소프트웨어 버전의 빌드 번호입니다.

표 114: 개요: 소프트웨어 매개변수(계속)

매개변수	설명
Version Status	이 소프트웨어 버전의 상태입니다. 값: ● Open(미정)—아직 릴리스되지 않음 ● Final(최종)—릴리스된 버전

표 115: 개요: 하드웨어 매개변수

매개변수	설명
RAM Size	RAM의 크기(메가바이트)입니다.
Flash Size	플래시(영구) 메모리 크기(메가바이트)입니다.

DefensePro 리소스 사용률 모니터링

이 섹션에 포함되는 주제는 다음과 같습니다.

- DefensePro CPU 사용률 모니터링, 156페이지
- DefensePro 인증 테이블 모니터링 및 지우기, 157페이지
- 구성된 정책에 따라 DME 사용률 모니터링, 158페이지
- DefensePro 시스템 로그 정보 모니터링, 158페이지

DefensePro CPU 사용률 모니터링

디바이스의 평균 리소스 사용률 및 Acclerator의 사용률 통계를 볼 수 있습니다.

선택한 DefensePro 디바이스에 대한 디바이스 사용률을 모니터링하려면

> *Monitoring(모니터링)* 관점에서 **Operational Status(운영 상태) > Resource Utilization(리소스 사용률) > CPU Utilization(CPU 사용률)**을 선택합니다.

표 116: CPU 사용률: 일반 매개변수

매개변수	설명
Resource Utilization	현재 활용되는 디바이스 CPU의 백분율입니다.
RS Resource Utilization	현재 활용되는 디바이스의 라우팅 서비스(RS) 리소스의 백분율입니다.
RE Resource Utilization	현재 활용되는 디바이스의 라우팅 엔진(RE) 리소스의 백분율입니다.
Last 5 sec. Average Utilization	지난 5초 동안의 평균 리소스 사용률입니다.
Last 60 sec. Average Utilization	지난 60초 동안의 평균 리소스 사용률입니다.

표 117: CPU 사용률: 엔진 사용률 매개변수

매개변수	설명
Engine ID	플로우 엔진의 이름입니다.
Forwarding Task	트래픽 처리에 사용된 CPU 주기의 백분율입니다.
Other Tasks	에이징 등의 기타 작업에 사용된 평균 CPU 리소스입니다.
Idle Task	사용 가능한 CPU 리소스의 평균입니다.

DefensePro 인증 테이블 모니터링 및 지우기

디바이스 인증 테이블의 통계를 볼 수 있습니다. 각 테이블의 콘텐츠도 지울 수 있습니다.

HTTP Authentication Table(HTTP 인증 테이블) 탭의 콘텐츠는 DefensePro for Cisco Firepower 9300과 관련이 없습니다.

선택한 DefensePro 디바이스의 인증 테이블을 모니터링하려면

> *Monitoring(모니터링)* 관점에서 **Operational Status(운영 상태) > Resource Utilization(리소스 사용률) > Authentication Tables(인증 테이블)**를 선택합니다.

표 118: TCP 인증 테이블 모니터링 매개변수

매개변수	설명
Table Size	테이블에서 보유할 수 있는 소스 주소 수입니다.
Table Utilization	현재 활용되는 테이블의 백분율입니다.
Aging Time	테이블의 에이징 타임(초)입니다.

표 119: DefensePro HTTP 인증 테이블 모니터링 매개변수

매개변수	설명
Table Size	보호 HTTP 서버의 소스-대상 쌍 수입니다. 예를 들어, 두 개의 HTTP 서버로 향하는 두 공격이 있으며 소스 주소가 동일한 경우, 해당 두 서버의 소스로 두 개의 항목이 테이블에 있습니다.
Table Utilization	현재 활용되는 테이블의 백분율입니다.
Aging Time	테이블의 에이징 타임(초)입니다. 값: 60-3600 기본값: 1200

표 120: DNS 인증 테이블 모니터링 매개변수

매개변수	설명
Table Size	테이블에서 보유할 수 있는 소스 주소 수입니다.
Table Utilization	현재 활용되는 테이블의 백분율입니다.
Aging Time	테이블의 에이징 타임(분)입니다.

선택한 DefensePro 디바이스의 인증 테이블을 지우려면

1. *Monitoring(모니터링)* 관점에서 **Operational Status(운영 상태) > Resource Utilization(리소스 사용률) > Authentication Tables(인증 테이블)**를 선택합니다.
2. 관련 탭(즉, **TCP Authentication Table(TCP 인증 테이블), HTTP Authentication Table(HTTP 인증 테이블)** 또는 **DNS Authentication(DNS 인증 테이블)**)에서 **Clean Table(테이블 지우기)**를 클릭합니다.

   참고: TCP 인증 테이블과 HTTP 인증 테이블의 경우 **표 지우기** 조치는 최대 10초가 걸릴 수 있습니다.

구성된 정책에 따라 DME 사용률 모니터링

이 탭의 콘텐츠는 DefensePro for Cisco Firepower 9300과 관련이 없습니다.

참고: 디바이스에 DME가 없으면 0(영) 값이 표시됩니다.

DefensePro 시스템 로그 정보 모니터링

시스템 로그 메커니즘과 관련된 정보를 볼 수 있습니다.

DefensePro 시스템 로그 정보를 모니터링하려면

> *Monitoring(모니터링)* 관점에서 **Operational Status(운영 상태) > Resource Utilization(리소스 사용률) > Syslog Monitor(시스템 로그 모니터)**을 선택합니다.

표 121: DefensePro 시스템 로그 모니터링 매개변수

매개변수	설명
Syslog Server	시스템 로그 서버의 이름입니다.
Status	시스템 로그 서버의 상태입니다. 값: ● Reachable(연결 가능)—서버에 연결할 수 있습니다. ● Unreachable(연결 불가능)—서버에 연결할 수 없습니다. ● N/R—시스템 로그 서버를 향하는 트래픽이 지정된 UDP를 초과하므로 *적절하지 않음*을 지정합니다(*Configuration(컨피그레이션)* 관점, **Setup(설정) > Syslog Server(시스템 로그 서버) > Protocol(프로토콜) > UDP**).
Messages in Backlog	시스템 로그 서버의 backlog에 있는 메시지 수입니다.

Cisco SGT(Security Group Tag) 모니터링

사용된 SGT가 있는 경우 해당 SGT의 이름과 값을 모니터링할 수 있습니다.

참고: DefensePro for Cisco Firepower 9300에서 SGT에 대한 자세한 내용은 SGT 클래스 구성, 124페이지를 참조하십시오.

SGT를 모니터링하려면

> *Monitoring(모니터링)* 관점에서 **Operational Status(운영 상태) > SGT**를 선택합니다.

표 122: SGT 모니터링 매개변수

매개변수	설명
이름	SGT의 이름입니다.
값	SGT의 값입니다.

8장 – DefensePro 클러스터링 모니터링

Clustering Status(클러스터링 상태) 탭을 사용하여 DefensePro for Cisco Firepower 9300의 클러스터 노드를 모니터링합니다.

클러스터링을 모니터링하려면

> *Monitoring(모니터링)* 관점에서 **Clustering(클러스터링) > Cluster Status(클러스터 상태)**를 선택합니다.

표 123: 클러스터링 모니터링 매개변수

매개변수	설명
IP 주소	클러스터 노드의 IP 주소입니다.
상태	클러스터 노드의 상태입니다.

9장 – DefensePro 통계 모니터링

DefensePro 통계 모니터링은 다음 항목으로 구성됩니다.

- DefensePro SNMP 통계 모니터링, 163페이지
- DefensePro IP 통계 모니터링, 164페이지

DefensePro SNMP 통계 모니터링

디바이스 SNMP 레이어의 통계를 볼 수 있습니다.

DefensePro SNMP 통계를 모니터링하려면

> *Monitoring(모니터링)* 관점에서 **Statistics(통계) > SNMP Statistics(SNMP 통계)**를 선택합니다.

표 124: DefensePro SNMP 통계

매개변수	설명
SNMP 수신 패킷 수	전송 서비스에서 SNMP 엔티티에 전달된 총 메시지 수입니다.
SNMP 전송 패킷 수	SNMP 프로토콜 엔티티에서 전송 서비스로 전달된 총 SNMP 메시지 수입니다.
SNMP의 성공적인 'GET' 요청 수	올바른 SNMP GET-Request 및 GET-Next PDU를 수신한 결과 SNMP 프로토콜 엔티티에서 성공적으로 검색한 총 MIB 개체 수입니다.
SNMP의 성공적인 'SET' 요청 수	올바른 SNMP SET-Request PDU를 수신한 결과 SNMP 프로토콜 엔티티에서 성공적으로 수정한 총 MIB 개체 수입니다.
SNMP의 'GET' 요청 수	SNMP 프로토콜 엔티티에서 승인하여 처리한 총 SNMP GET-Request PDU 수입니다.
SNMP 'GET-Next' 요청 수	SNMP 프로토콜 엔티티에서 승인하여 처리한 총 SNMP GET-Next Request PDU의 수입니다.
SNMP의 'SET' 요청 수	SNMP 프로토콜 엔티티에서 승인하여 처리한 총 SNMP SET-Request PDU의 수입니다.
수신된 SNMP 오류 "Too Big" 수	오류 상태 필드의 값이 'tooBig'인 SNMP 프로토콜 엔티티에서 생성한 SNMP PDU의 총 수입니다.
수신된 SNMP 오류 "No Such Name" 수	오류 상태의 값이 'noSuchName'인 SNMP 프로토콜 엔티티에서 생성한 SNMP PDU의 총 수입니다.
수신된 SNMP 오류 "Bad Value" 수	오류 상태 필드의 값이 'badValue'인 SNMP 프로토콜 엔티티에서 생성한 SNMP PDU의 총 수입니다.
수신된 SNMP 오류 "Generic Error" 수	오류 상태 필드의 값이 'genErr'인 SNMP 프로토콜 엔티티에서 생성한 SNMP PDU의 총 수입니다.
전송된 SNMP 'GET' 응답 수	SNMP 프로토콜 엔티티에서 생성한 SNMP GET-Responset PDU의 총 수입니다.
전송된 SNMP 트랩 수	SNMP 프로토콜 엔티티에서 생성한 SNMP Trap PDU의 총 수입니다.

DefensePro IP 통계 모니터링

버리거나 무시된 패킷 수를 포함하여 디바이스의 IP 레이어 통계를 모니터링할 수 있습니다. 그러면 지정된 인터페이스의 네트워크 혼잡 상태를 신속하게 요약할 수 있습니다.

선택한 DefensePro 디바이스의 IP 통계 정보를 표시하려면

> *Monitoring(모니터링)* 관점에서 **Statistics(통계) > IP Statistics(IP 통계)**를 선택합니다.

표 125: DefensePro IP 통계 매개변수

매개변수	설명
Number of IP Packets Received (수신된 IP 패킷 수)	오류로 받은 수를 포함하여 인터페이스에서 수신한 입력 데이터그램의 총 수입니다.
Number of IP Header Errors(IP 헤더 오류 수)	잘못된 체크섬, 버전 번호 불일치, 기타 형식 오류, TTL(Time-To-Live) 초과, IP 옵션을 처리하는 중에 발견한 오류 등의 IP 헤더 오류로 인해 폐기된 입력 데이터그램의 수입니다.
Number of Discarded IP Packets(폐기된 IP 패킷 수)	폐기된 관리용 입력 데이터그램의 총 수입니다. 이 수에는 다시 어셈블링하기 위해 대기하는 동안 폐기된 데이터그램은 포함되지 않습니다.
Number of Valid IP Packets Received(수신된 유효 IP 패킷 수)	IP 사용자 프로토콜(ICMP 포함)에 성공적으로 전달된 입력 데이터그램의 총 수입니다.
Number of Transmitted Packets (Inc. Discards)(전송된 패킷 수 (폐기 포함))	전송 요청에서 ICMP를 포함하는 로컬 IP 사용자 프로토콜에서 IP에 제공한 IP 데이터그램의 총 수입니다. 이 수에는 전달된 IP 패킷 수로 계수된 데이터그램은 포함되지 않습니다.
Number of Discarded Packets on TX(TX의 폐기된 패킷 수)	대상에 전송하지 못하게 하는 문제가 발생하지 않았지만 버퍼 공간 부족 등의 이유로 폐기된 출력 IP 데이터그램의 수입니다. 이 수에는 패킷이 (임의의) 폐기 기준을 만족하는 경우 전달된 IP 패킷 수로 계수되는 모든 데이터그램이 포함됩니다.

표 126: DefensePro 라우터 통계 매개변수

매개변수	설명
Number of IP Packets Forwarded(전달된 IP 패킷 수)	이 항목이 최종 IP 대상용이 아닌 입력 데이터그램의 수입니다. 결과적으로 최종 대상에 전달할 경로를 찾으려고 시도합니다. IP 게이트웨이로 작동하지 않는 엔티티에서 이 수에는 이 항목을 통해 소스로 라우팅된 패킷과 소스 라우팅 옵션 처리에 성공한 패킷만 포함됩니다.
Number of IP Packets Discarded Due to 'Unknown Protocol'('알 수 없는 프로토콜'로 인해 폐기된 IP 패킷 수)	성공적으로 수신되었지만, 알 수 없거나 지원되지 않는 프로토콜로 인해 폐기된 로컬 주소의 데이터그램 수입니다.
Number of IP Packets Discarded Due to 'No Route'('경로 없음'으로 인해 폐기된 IP 패킷 수)	대상에 전송하기 위한 경로를 찾을 수 없으므로 폐기된 IP 데이터그램의 수입니다. **참고:** 이 수에는 경로 없음 조건을 만족하는 전달된 IP 패킷 수로 계수되는 모든 패킷이 포함됩니다. 여기에는 기본 게이트웨이가 모두 작동 중지되어 호스트에서 라우팅할 수 없는 모든 데이터그램이 포함됩니다.
Number of IP Fragments Received(수신된 IP 프래그먼트 수)	이 엔티티에서 다시 어셈블해야 하는 수신된 IP 프래그먼트 수입니다.
Number of IP Fragments Successfully Reassembled (성공적으로 다시 어셈블된 IP 프래그먼트 수)	성공적으로 다시 어셈블된 IP 프래그먼트 수입니다.
Number of IP Fragments Failed Reassembly(다시 어셈블에 실패한 IP 프래그먼트 수)	IP 다시 어셈블 알고리즘에서 탐지한 실패(예: 시간 초과, 오류 등)의 수입니다. 참고: 일부 알고리즘(특히 RFC 815의 알고리즘)에서 프래그먼트를 수신할 때 프래그먼트를 결합하므로 해당 수를 파악하지 못한 결과 폐기된 IP 프래그먼트 수가 아닙니다.
Number of IP Datagrams Successfully Reassembled (성공적으로 다시 어셈블된 IP 데이터그램 수)	이 엔티티에서 성공적으로 다시 어셈블된 IP 데이터그램의 수입니다.
Number of IP Datagrams Discarded Due to Fragmentation Failure (프래그멘테이션 실패로 인해 폐기된 IP 데이터그램 수)	이 엔티티에서 프래그멘테이션해야 하지만 프래그멘테이션하지 않음 플래그가 설정되어 있는 등의 이유로 인해 프래그멘테이션을 수행할 수 없어 폐기된 IP 데이터그램 수입니다.
Number of IP Datagrams Fragments Generated(생성된 IP 데이터그램 프래그먼트 수)	이 엔티티에서 프래그멘테이션을 수행한 결과 생성된 IP 데이터그램 프래그먼트의 수입니다.
Valid Routing Entries Discarded (폐기된 유효 라우팅 항목 수)	폐기된 유효 라우팅 항목 수입니다.

10장 – DefensePro 네트워킹 모니터링 및 제어

DefensePro 네트워킹 모니터링 및 제어는 다음 항목으로 구성됩니다.

- 라우팅 테이블 정보 모니터링, 167페이지
- DefensePro ARP 테이블 정보 모니터링, 168페이지

참고: *일시중단 테이블* 노드의 콘텐츠는 DefensePro for Cisco Firepower 9300에서 작동하지 않습니다.

라우팅 테이블 정보 모니터링

라우팅 테이블에서는 대상에 대한 정보와 대상에 도달할 수 있는 방법을 저장합니다.

기본적으로 DefensePro 디바이스에 직접 연결된 모든 네트워크는 이 테이블에 등록됩니다. 기타 항목은 정적으로 구성하거나 라우팅 프로토콜을 통해 동적으로 생성할 수 있습니다.

참고: 라우팅 테이블에서는 주기적으로 자동 새로 고치기를 수행하지 않습니다. Routing Table(라우팅 테이블) 창을 표시하도록 선택하고 수동으로 표시를 새로 고치면 정보가 로드됩니다.

선택한 디바이스의 라우팅 테이블 정보를 표시하려면

> *Monitoring(모니터링)* 관점에서 **Networking(네트워킹) > Routing(라우팅)**을 선택합니다.

표 127: 라우팅 테이블 모니터링 매개변수

매개변수	설명
Destination Network	경로가 정의되는 대상 네트워크입니다.
Netmask	대상 서브넷의 네트워크 마스크입니다.
Next Hop	대상 서브넷으로 전달되는 다음 홉의 IP 주소입니다. (다음 홉은 항상 디바이스에 대해 로컬인 서브넷에만 있습니다.)
Via Interface	DefensePro for Cisco Firepower 9300에서 값은 **3**(읽기 전용)입니다. 이 값은 관리 인터페이스의 값입니다.
Type	이 필드는 정적 경로 테이블에만 표시됩니다. 라우팅 유형입니다. 값: ● Local(로컬)—서브넷을 디바이스에서 직접 연결할 수 있습니다. ● Remote(원격)—서브넷을 디바이스에서 직접 연결할 수 없습니다.
Metric	이 경로에 정의되었거나 계산된 메트릭 값입니다.

DefensePro ARP 테이블 정보 모니터링

정적 항목과 동적 항목을 모두 포함하는 디바이스의 ARP 테이블입니다. 항목 유형을 동적에서 정적으로 변경할 수 있습니다.

참고: ARP 테이블에서는 주기적으로 자동 새로 고치기를 수행하지 않습니다. ARP Table(ARP 테이블) 창을 표시하도록 선택하고 수동으로 표시를 새로 고치면 정보가 로드됩니다.

선택한 DefensePro 디바이스의 ARP 테이블 정보를 표시하려면

> *Monitoring(모니터링)* 관점에서 **Networking(네트워킹) > ARP**를 선택합니다.

표 128: DefensePro ARP 테이블 모니터링 매개변수

매개변수	제목
포트	스테이션이 있는 인터페이스 번호입니다.
IP 주소	스테이션의 IP 주소입니다.
MAC 주소	스테이션의 MAC 주소입니다.
유형	항목 유형입니다. 값: ● Other(기타)—정적 또는 동적이 아님. ● Dynamic(동적)—ARP 프로토콜에서 항목을 학습합니다. 사전 결정된 시간에 항목이 활성화되지 않은 경우 노드가 테이블에서 삭제됩니다. ● Static(정적)—항목이 네트워크 관리 스테이션에서 구성되었으며 영구적입니다.

항목 유형을 동적에서 정적으로 변경하려면

1. *Monitoring(모니터링)* 관점에서 **Networking(네트워킹) > ARP**를 선택합니다.
2. 항목을 선택하고 **Change Entry to Static(항목을 정적으로 변경)**을 선택합니다.

이 기능은 DefensePro 6.x 버전 및 7.40 이전의 7.x 버전에서만 지원됩니다.

MPLS RD 정보를 모니터링하고 MPLS RD를 구성할 수 있습니다. 각 MPLS RD에는 디바이스가 설치된 링크의 두 태그(상위 태그 및 하위 태그)가 할당됩니다. 다른 링크에서는 동일한 MPLS RD에 다른 태그가 할당될 수 있습니다.

선택한 DefensePro 디바이스의 MPLS RD 정보를 표시하려면

1. *Monitoring(모니터링)* 관점에서 **Networking(네트워킹) > MPLS RD**를 선택합니다. *MPLS RD* 테이블에는 현재 MPLS RD 정보가 표시됩니다.
2. MPLS RD를 추가하려면 (Add(추가)) 버튼을 클릭합니다.
3. 매개변수를 구성한 다음 **Submit(제출)**을 클릭합니다.

표 129: MPLS RD 매개변수

매개변수	설명
MPLS RD	MPLS RD 이름입니다.
유형	MPLS RD 형식에 대해 설명합니다. 값: ● 2바이트 : 4바이트—AS(16비트): 숫자(32비트) ● 4바이트 : 2바이트—AS(32비트): 숫자(16비트) ● IP 주소 : 2바이트—IP: 숫자(16비트)
상위 태그	디바이스가 설치된 링크의 상위 태그입니다.
하위 태그	디바이스가 설치된 링크의 하위 태그입니다.

11장 – 실시간 보안 모니터링 사용

공격이 탐지되면 DefensePro 디바이스에서 특정 공격과 관련된 정보가 포함된 *보안 이벤트*를 생성하여 보고합니다. *Security Monitoring(보안 모니터링)* 관점에는 실시간 트래픽 및 통계 매개변수와 함께 특정 공격에 관한 정보가 표시됩니다. *Security Monitoring(보안 모니터링)* 관점을 사용하여 디바이스에서 탐지한 공격과 디바이스에서 구현한 대책을 관찰하고 분석합니다.

참고

- 사용자 권한(*RBAC 사용자 정의*)에 따라 *Security Monitoring(보안 모니터링)* 관점에서 표시하는 DefensePro 디바이스와 정책이 결정됩니다. 사용 가능한 DefensePro 디바이스와 정책에서 차단한 공격만 보고 모니터링할 수 있습니다.
- APSolute Vision에서는 새 보안 공격의 경고도 관리하고 발행합니다.
- DefensePro에서는 트래픽 베이스라인을 계산하고 이 베이스라인을 사용하여 트래픽 레벨의 비정상 항목도 식별합니다.
- 실시간 네트워크 트래픽과 통계 매개변수를 계산할 때 DefensePro에서는 처리량 라이센스를 초과한 트래픽은 포함하지 않습니다.

다음 기본 항목에서는 APSolute Vision의 보안 모니터링에 대해 설명합니다.

- 위험 레벨, 171페이지
- 대시보드 사용, 172페이지
- 실시간 트래픽 보고서 보기, 188페이지
- 보호 모니터링, 192페이지

위험 레벨

다음 표에서는 DefensePro에서 보안 이벤트를 분류하기 위해 지원하는 위험 레벨을 설명합니다.

참고: 일부 보호의 경우 사용자가 이벤트의 위험 레벨을 지정할 수 있습니다. 이러한 보호의 경우 다음 표에 있는 설명이 권장되는 내용이며, 위험 레벨에 대한 책임은 사용자에게 있습니다.

표 130: 위험 레벨

위험 레벨	설명
Info	이 위험은 정상적인 서비스 운영에 위협이 되지 않습니다.
Low	이 위험은 정상적인 서비스 운영에 위협이 되지 않지만, 악의적인 행동을 위한 예비 조치의 일부일 수 있습니다.
Medium	이 위험은 정상적인 서비스 운영에 위협이 될 수 있지만, 완전한 서비스 중단, 원격 코드 실행 및 무단 액세스를 초래할 가능성이 없습니다.
High	이 위험은 정상적인 서비스 가용성에 위협이 될 가능성이 매우 높으며, 완전한 서비스 중단, 원격 코드 실행 또는 무단 액세스를 초래할 수 있습니다.

대시보드 사용

이 섹션에서는 다음 주제에 대해 알아봅니다.

- 보안 대시보드 차트 보기 사용, 174페이지
- 보안 대시보드 테이블 보기—현재 공격 테이블 사용, 175페이지
- 공격 세부 정보, 179페이지
- 샘플링된 데이터 탭, 187페이지

보안 대시보드를 사용하여 네트워크의 활동과 보안 이벤트를 분석하고 보안 트렌드를 식별하며 위험을 분석합니다.

개별 디바이스, 사이트의 모든 디바이스 또는 네트워크의 모든 디바이스에 대한 보안 대시보드 정보를 볼 수 있습니다. 대시보드 모니터링 표시를 자동으로 새로 고쳐 시스템의 계속되는 실시간 분석을 제공합니다.

*보안 대시보드*는 *차트 보기*와 *테이블 보기*로 구성됩니다(그림 27 - 보안 대시보드(차트 보기, 175페이지 및 그림 28 - 보안 대시보드(테이블 보기—현재 공격 테이블), 176페이지 참조). 기본적으로 15초마다 표시를 새로 고칩니다. 관리자가 새로 고치기 비율을 구성할 수 있습니다(*APSolute Vision Settings(APSolute Vision 설정)* 보기 *System(시스템)* 관점, **General Settings(일반 설정) > Monitoring(모니터링) > Polling Interval for Reports(보고서 폴링 간격)**).

보안 모니터 차트 보기에 표시된 요약 정보는 보안 모니터 테이블 보기(*Current Attacks(현재 공격)* 테이블)에도 표시됩니다.

보안 대시보드를 표시하려면

> *Security Monitoring(보안 모니터링)* 관점에서 **Dashboard View(대시보드 보기) > Security Dashboard(보안 대시보드)**를 선택합니다.

보안 대시보드 차트 보기와 테이블 보기를 전환하려면

> 관련 버튼,  (Show Chart(차트 표시)) 또는  (Show Table(테이블 표시))을 클릭한 다음 표시 매개변수를 구성합니다.

표 131: 보안 대시보드 표시 매개변수

매개변수	설명
범위	대시보드에서 표시하는 물리적 포트와 네트워크 보호 정책입니다. 기본적으로 범위는 **모든 포트, 모든 정책**입니다. 즉, 기본적으로 대시보드에는 모든 정보가 표시됩니다. DefensePro에서 보안 대시보드에 표시되는 정보의 범위를 제어하려면 보안 대시보드에 표시되는 정보 범위를 제어하려면, 173페이지 절차를 참조하십시오.

표 131: 보안 대시보드 표시 매개변수(계속)

매개변수	설명
마지막 표시	공격이 종료된 후 모니터에서 공격을 표시하는 기간입니다. 즉, 모니터에서 현재 진행 중이거나 선택한 기간 내에 종료된 모든 공격을 표시합니다. 값: ● 10분 ● 20분 ● 30분 ● 1시간 ● 2시간 ● 6시간 ● 12시간 ● 24시간 기본값: 10분
표시할 상위 공격 (이 매개변수는 차트 보기에서만 사용할 수 있습니다.)	지속적 공격 모니터가 표시하는 공격 수입니다. 값: 1-50 기본값: 20 **참고:** 이 매개변수는 지속적 공격 모니터에만 관련됩니다.
정렬 기준 (이 매개변수는 차트 보기에서만 사용할 수 있습니다.)	값: ● 상위 패킷 수—지속적 공격 모니터에 패킷 수가 가장 높은 공격이 표시됩니다. ● 상위 패킷 수—지속적 공격 모니터에 대역폭이 가장 높은 공격이 표시됩니다. ● 최신—지속적 공격 모니터에 최신 공격이 표시됩니다. ● 공격 상태—지속적 공격 모니터에 공격 상태에 따라 가장 많이 나타나는 공격이 표시됩니다. ● 공격 위험—지속적 공격 모니터에 공격 위험에 따른 공격이 표시됩니다. 기본값: 상위 패킷 수 **참고:** 이 매개변수는 지속적 공격 모니터에만 관련됩니다.

보안 대시보드에서 표시하는 정보 범위를 제어하려면

1. ▶ Scope을 클릭합니다. 두 개의 테이블이 열립니다. 한 테이블에는 *Device Name(디바이스 이름)*과 *포트(Port)* 열이 있고, 다른 테이블에는 *Device Name(디바이스 이름)*과 *Policy(정책)* 열이 있습니다.

   참고: DefensePro for Cisco Firepower 9300에서는 범위의 물리적 포트 제한을 지원하지 않습니다.

2. 다음 중 하나를 수행합니다.
   - 보안 대시보드에서 표시하는 네트워크 보호 정책을 제한하려면 해당 확인란을 선택합니다.
   - 현재 관련된 모든 네트워크 보호 정책의 정보를 표시하려면 왼쪽 위 테이블 셀을 클릭한 다음 **Select All(모두 선택)**을 선택합니다.
   - 특정 포트 또는 특정 네트워크 보호 정책과 관련되지 않은 정보도 포함하여 데이터베이스의 모든 정보를 표시하려면 왼쪽 위 표 셀을 클릭한 다음 **Select None(선택하지 않음)**을 선택합니다.

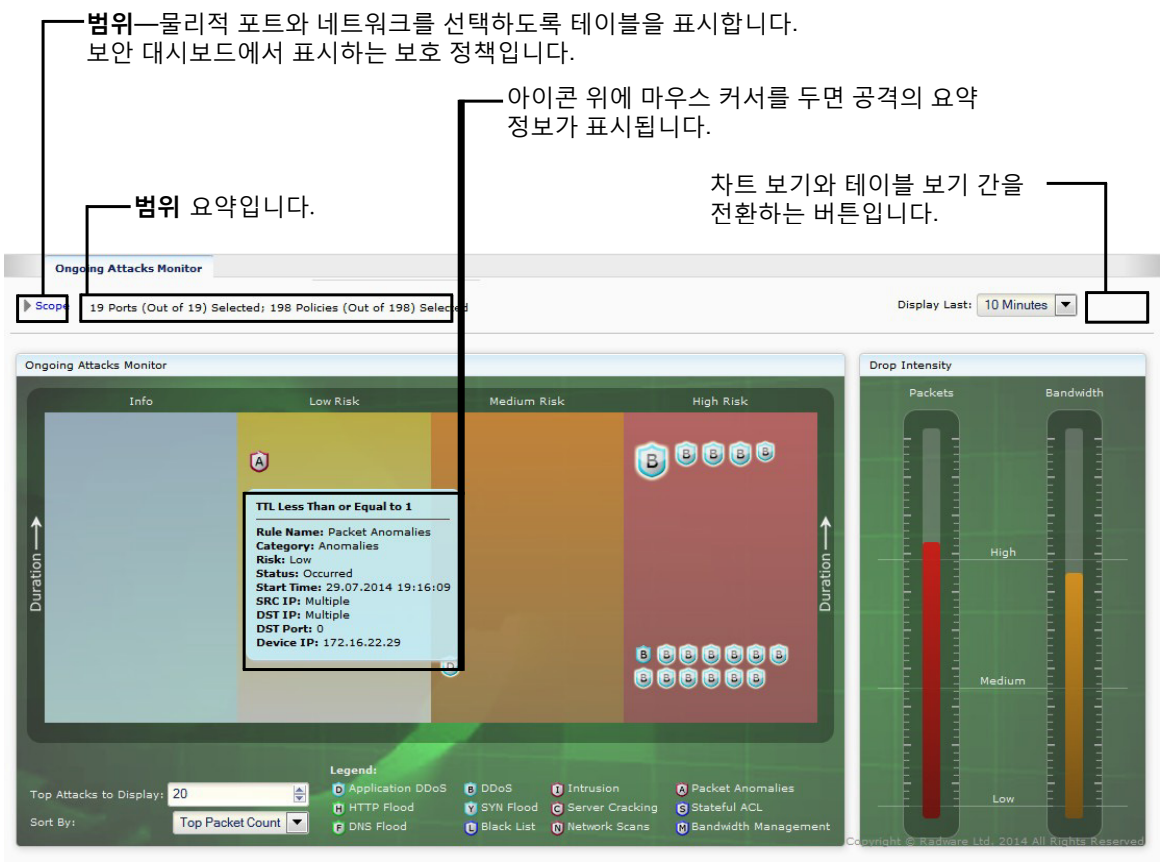
보안 대시보드 차트 보기 사용

보안 대시보드 차트 보기에는 *지속적 공격 모니터* 및 *삭제 강도* 게이지가 포함됩니다.

*지속적 공격 모니터*는 현재 공격과 최신 공격을 그래픽으로 나타냅니다. 모니터의 각 아이콘은 개별 공격을 나타냅니다. 아이콘 유형(범례 참조)은 공격이 위반하는 보호 유형을 나타냅니다. 플래시 아이콘은 진행 중인 공격을 나타냅니다. 차트에 있는 각 아이콘의 가로 위치는 공격 위험을 나타냅니다(위험 레벨, 171페이지 참조). 차트에 있는 아이콘의 세로 위치는 공격 기간을 나타내며, 차트에서 위치가 높을수록 공격 기간이 깁니다. 최근에 시작된 공격은 모니터의 하단에 있습니다. 아이콘 크기는 특정 공격 유형의 삭제된 데이터 양을 동일한 유형의 다른 공격에 비례하여 나타냅니다. 아이콘 위에 마우스 커서를 두면 공격의 요약 정보가 표시됩니다. 아이콘을 두 번 클릭하여 공격의 자세한 정보를 표시합니다. 자세한 내용은 공격 세부 정보, 179페이지를 참조하십시오.

삭제 강도 게이지는 두 개의 게이지, 즉 패킷과 대역폭을 제공합니다. 패킷 게이지는 총 패킷과 비교하여 삭제된 패킷의 비율을 표시합니다. 대역폭 게이지는 총 대역폭과 비교하여 삭제된 대역폭의 비율을 표시합니다(라이센스에 따라 다름). 게이지에서는 계산된 범위를 낮음(최대 30% 삭제), 중간(최대 70% 삭제) 및 높음(70% 이상 삭제)으로 표시합니다.

그림 27: 보안 대시보드(차트 보기)



보안 대시보드 테이블 보기—현재 공격 테이블 사용

테이블 보기, *Current Attack(현재 공격)* 테이블에는 현재 공격과 최신 공격에 대한 정보가 표시됩니다. 다음도 수행할 수 있습니다.

- **검색 또는 필터 기능 사용**—열에서 검색 기능을 지원하는 경우 오름차순에서 내림차순으로나 그 역으로 행 순서를 변경할 수 있습니다. 이 작업을 수행하려면 마우스 커서를 열 위에 두어 화살표를 표시하고 순서를 변경합니다.
- **특정 공격에 대한 추가 정보 보기**—이 작업을 수행하려면 관련 행을 선택하고 (View Attack Details(공격 세부 정보 보기))를 클릭합니다. 자세한 내용은 공격 세부 정보, 179페이지를 참조하십시오.
- **공격을 처리한 정책으로 이동**— 이 작업을 수행하려면 (Go to Policy(정책으로 이동))을 클릭합니다.
- **테이블의 정보를 CSV 파일로 내보내기**—이 작업을 수행하려면 (CSV)를 클릭합니다. 그런 다음 파일을 보거나 위치와 파일 이름을 지정할 수 있습니다.

  참고: 패킷 이상 내보내기는 지원되지 않습니다.
- **테이블 표시 새로 고침 일시정지**—이 작업을 수행하려면 (Pause(일시정지))을 클릭합니다. 테이블 표시를 일시정지하지 *않으면* 약 15초마다 새로 고칩니다.

그림 28: 보안 대시보드(테이블 보기—현재 공격 테이블)

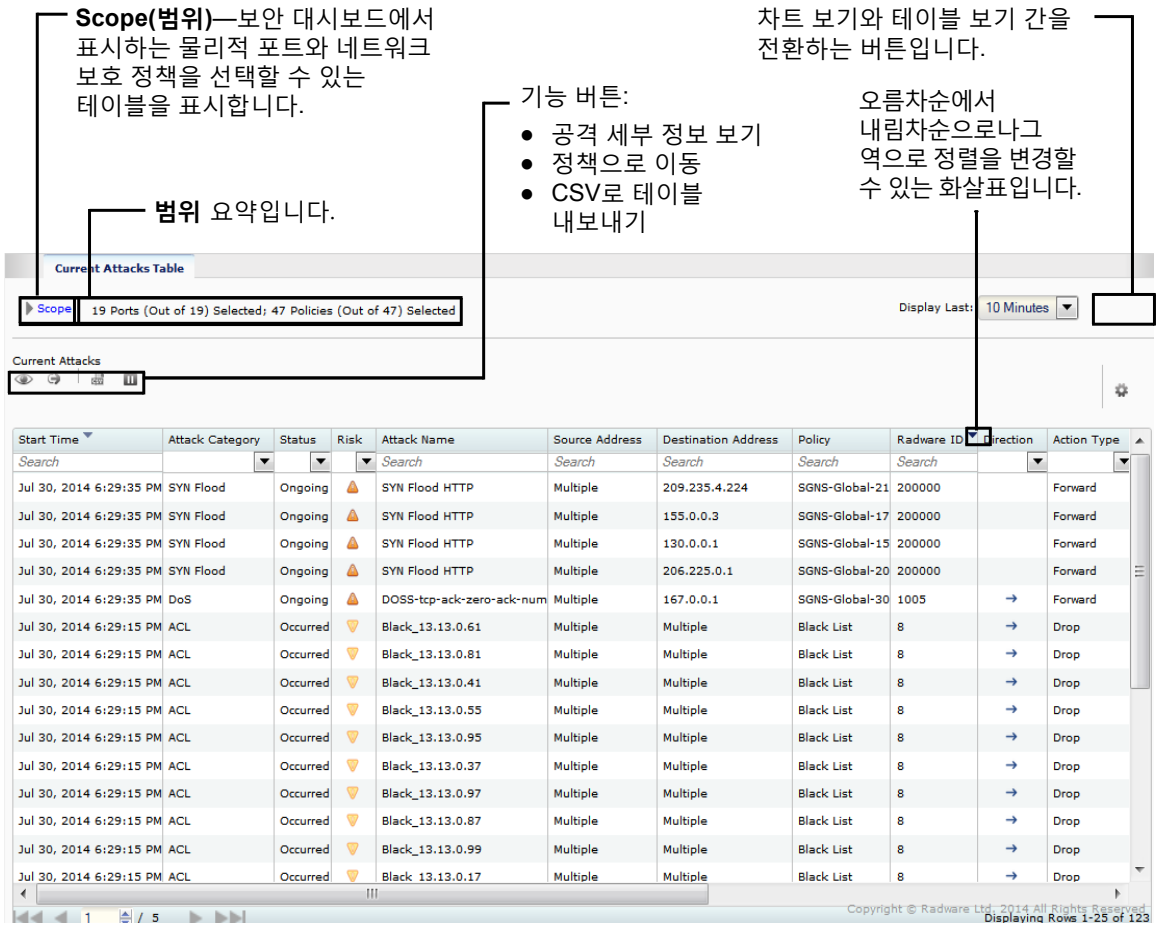


표 132: 현재 공격 테이블 매개변수

매개변수	설명
Start Time	공격이 시작된 날짜와 시간입니다.
Attack Category	이 공격이 속한 위협 유형입니다. 값: ● ACL ● 이상 징후 ● 스캔 방지 ● 대역폭 관리 ● 동작 기반 DoS(Behavioral DoS) ● DNS 플러드 ● DoS ● HTTP 플러드 ● 침입 ● 서버 크래킹 ● 상태 저장 ACL ● SYN 플러드

표 132: 현재 공격 테이블 매개변수(계속)

매개변수	설명
Status	마지막으로 보고된 공격 상태입니다. 값: ● 시작됨—두 개 이상의 보안 이벤트를 포함하는 공격이 탐지되었습니다(일부 공격에는 DoS, 스캔 등과 같은 여러 보안 이벤트가 포함됨). ● 발생함(시그니처 기반 공격)—시그니처와 일치하는 각 패킷이 공격으로 보고되어 삭제되었습니다. ● 진행 중—공격이 현재 이루어지고 있으며, 시작됨과 종료됨 사이의 시간입니다(DoS, 스캔 등과 같은 여러 보안 이벤트를 포함하는 공격의 경우). ● 종료됨—공격의 특징과 일치하는 패킷이 더 이상 없으며 디바이스에서 공격이 종료되었음을 보고합니다.
Risk	미리 정의된 공격 심각도 레벨(위험 레벨, 171페이지 참조). 값: • —High(높음) • —Medium(중간) • —Low(낮음) • —정보
Attack Name	탐지된 공격의 이름입니다.
Source Address	공격의 소스 IP 주소입니다. 공격의 IP 소스가 여러 개인 경우 이 필드에 **다중**이 표시됩니다. 여러 IP 주소가 *Attack Details(공격 세부 정보)* 창에 표시됩니다. **다중**은 DefensePro에서 특정 값을 보고할 수 없는 경우도 나타낼 수 있습니다. **검색 문자열**은 적절한 IPv4 또는 Ipv6 주소가 될 수 있으며 와일드카드(*)를 포함할 수 있습니다.
Destination Address	공격의 대상 IP 주소입니다. 공격의 IP 소스가 여러 개인 경우 이 필드에 **다중**이 표시됩니다. 여러 IP 주소가 *Attack Details(공격 세부 정보)* 창에 표시됩니다. **다중**은 DefensePro에서 특정 값을 보고할 수 없는 경우도 나타낼 수 있습니다.
Policy	이 공격을 통해 위반되는 구성된 네트워크 보호 정책 또는 서버 보호 정책의 이름입니다. 특정 공격의 정책을 보거나 편집하려면 공격 항목을 선택하고 (Go to Policy(정책으로 이동)) 버튼을 클릭합니다.
Radware ID	디바이스에서 발행한 고유 공격 ID입니다.
Direction	공격의 방향(인바운드 또는 아웃바운드)입니다. 값: 인, 아웃

표 132: 현재 공격 테이블 매개변수(계속)

매개변수	설명
Action Type	공격에 대해 보고된 조치입니다. 조치는 보호 프로필에 지정되어 있으며, 이 보호 프로필은 사용자의 시스템에 해당하거나 사용 가능할 수도 있고 그렇지 않을 수도 있습니다. 값: ● 바이패스 ● 당면 과제 ● 대상 재설정—DefensePro에서 TCP 재설정 패킷을 대상 주소에 전송합니다. ● 삭제—DefensePro에서 패킷을 버립니다. ● 삭제 및 격리 ● 전달—DefensePro에서 대상에 패킷을 전달합니다. ● 대리인 ● 격리 ● 소스 대상 재설정—DefensePro에서 TCP 재설정 패킷을 패킷 소스 IP와 패킷 대상 IP 주소 둘 다에 전송합니다. ● 소스 재설정—DefensePro에서 TCP 재설정 패킷을 패킷 소스 IP 주소에 전송합니다. ● Http 200 정상—DefensePro에서 미리 정의된 페이지를 사용하여 200 정상 응답을 보내고 서버 측 연결을 연 상태로 둡니다. ● Http 200 정상 대상 재설정—DefensePro에서 미리 정의된 페이지를 사용하여 200 정상 응답을 보내고 서버 측에 TCP 재설정 패킷을 전송하여 연결을 종료합니다. ● Http 403 금지—DefensePro에서 미리 정의된 페이지를 사용하여 403 금지 응답을 보내고 서버 측 연결을 연 상태로 둡니다. ● Http 403 금지 대상 재설정—DefensePro에서 미리 정의된 페이지를 사용하여 403 금지 응답을 보내고 서버 측에 TCP 재설정 패킷을 전송하여 연결을 종료합니다.
Total Packet Count	공격 시작부터 식별된 공격 패킷의 수입니다.
Volume	대부분의 보호에서 이 값은 공격이 시작된 때부터의 공격 볼륨(킬로비트)입니다. SYN 보호(SYN 쿠키)에서 이 값은 삭제된 SYN 패킷 수에 60바이트(SYN 패킷 크기)를 곱한 값입니다.
Device IP	공격된 디바이스의 IP 주소입니다.
Application Protocol	공격을 보내는 데 사용한 전송 프로토콜: 기본값: ● TCP ● UDP ● ICMP ● IP
MPLS RD	공격을 처리한 정책의 MPLS RD(Multi-protocol Label Switching Route Distinguisher) 입니다. 이 필드의 값이 **N/A** 또는 **0**(영)이면 MPLS RD를 사용할 수 없음을 표시합니다.

표 132: 현재 공격 테이블 매개변수(계속)

매개변수	설명
VLAN Tag/Context	공격을 처리한 정책의 VLAN 태그 값 또는 상황 그룹입니다. 이 필드의 값이 **N/A** 또는 **0**(영)이면 VLAN 태그 또는 상황 그룹을 사용할 수 없음을 표시합니다. **참고:** VLAN 태그나 상황 그룹은 이 필드에 비슷한 정보를 식별합니다. DefensePro 6.x 및 7.x 버전에서 VLAN 태그를 지원합니다. DefensePro for Cisco Firepower 9300에서 상황 그룹을 지원합니다.
Source Port[1]	공격의 레이어 4 소스 포트입니다.
Destination Port	공격의 레이어 4 대상 포트입니다. 대상 L4 포트가 여러 개인 경우 이 필드에 **다중**이 표시됩니다. DefensePro에서 특정 값을 보고할 수 없으면 필드에 **0**(영)이 표시됩니다.
Physical Port	공격 패킷이 도착한 디바이스의 포트입니다. DefensePro에서 특정 값을 보고할 수 없으면 필드에 **0**(영)이 표시됩니다.
Source MSISDN	*MSISDN 분석 기능은 APSolute Vision 버전 3.0 이상에서 지원되지 않습니다.*
Destination MSISDN	*MSISDN 분석 기능은 APSolute Vision 버전 3.0 이상에서 지원되지 않습니다.*

1 – 이 열은 *Current Attacks(현재 공격)* 탭에는 기본적으로 표시되지 않습니다. 열을 표시하려면 (Table Settings(테이블 설정)) 버튼을 클릭한 다음 관련 확인란을 선택합니다. 버튼을 다시 클릭하여 *Table Settings(테이블 설정)* 목록을 닫습니다.

공격 세부 정보

보안 대시보드 차트 보기 또는 테이블 보기에서 공격을 두 번 클릭하면 *Attack Details(공격 세부 정보)* 탭이 표시됩니다.

APSolute Vision에서는 다음 공격의 공격 세부 정보가 표시됩니다.

- BDoS 공격 세부 정보, 180페이지
- DNS 플러드 공격 세부 정보, 182페이지
- DoS 공격 세부 정보, 184페이지
- 패킷 이상 공격 세부 정보, 185페이지
- SYN 플러드 공격 세부 정보, 185페이지

참고: 이 창에 표시된 *공격 특징* 정보는 *Current Attack Summary(현재 공격 요약)* 테이블의 숨겨진 열에서도 사용할 수 있습니다.

공격 설명에는 공격 설명 파일의 정보가 표시됩니다. 공격 설명은 APSolute Vision 서버에 공격 설명 파일이 업로드된 경우에만 표시됩니다.

공격의 세부 정보 외에도 각 *Attack Details(공격 세부 정보)* 탭에서 다음을 수행할 수 있습니다.

- **공격에서 샘플링된 데이터 보기**—이 작업을 수행하려면  (View Sampled Data(샘플링된 데이터 보기))를 클릭합니다. 자세한 내용은 샘플링된 데이터 탭, 187페이지를 참조하십시오.
- **공격을 처리한 정책으로 이동**— 이 작업을 수행하려면  (Go to Policy(정책으로 이동))을 클릭합니다.
- **Attack Details(공격 세부 정보) 탭의 정보를 CSV 파일로 내보내기** —이 작업을 수행하려면  (CSV)를 클릭합니다. 그런 다음 파일을 보거나 위치와 파일 이름을 지정할 수 있습니다.
- **Attack Details(공격 세부 정보) 탭의 정보를 CAP 파일에 내보내기**—이 작업을 수행하려면  (Export Attack Capture Files(공격 캡처 파일 내보내기))를 클릭하고 파일 선택 대화 상자에 파일 이름을 입력합니다.

  참고

  - CAP 파일을 패킷 분석기에 보낼 수 있습니다.
  - 최대 255바이트의 패킷 정보가 CAP 파일에 저장됩니다. 즉, DefensePro에서 전체 패킷을 내보내지만, APSolute Vision에서 255바이트로 자릅니다.
  - *Current Attack(현재 공격)* 테이블에 표시되는 경우에만 파일을 사용할 수 있습니다.
  - 위반된 프로필의 보호 컨피그레이션에서 패킷 보고를 사용하는 경우에만 파일이 생성됩니다.
  - DefensePro에서는 필터와 일치하는 순서의 마지막 패킷만 내보냅니다. 또한 트래픽이 두 개 이상의 패킷으로 구성된 시그니처와 일치하는 경우 보고된 패킷에는 필터의 전체 식이 포함되지 않습니다.

BDoS 공격 세부 정보

표 133: BDoS 공격 세부 정보: 특징 매개변수

매개변수	설명
참고: 일부 필드에 여러 값이 표시될 수 있습니다(해당되고 사용 가능한 경우). 표시되는 값은 현재 공격 상태에 따라 달라집니다. 필드가 동적 시그니처의 일부이면(즉, 하나 이상의 특정 값이 모든 공격 트래픽에 표시) **Characteristics(특징)** 필드에 하나 이상의 관련 값이 표시됩니다.	
Protocol	공격에서 사용하거나 사용한 프로토콜입니다.
Source L4 Port	공격에서 사용하거나 사용한 소스 L4 포트입니다.
Physical Port	공격에서 사용하거나 사용한 물리적 포트입니다.
Packet Count	공격의 패킷 수입니다.
Volume (Kbits)	공격에서 사용하거나 사용한 볼륨(Kbits)입니다.
VLAN/Context	공격을 처리한 정책의 VLAN 태그 값 또는 상황 그룹입니다. **참고:** VLAN 태그나 상황 그룹은 이 필드에 비슷한 정보를 식별합니다. DefensePro 6.x 및 7.x 버전에서 VLAN 태그를 지원합니다. DefensePro for Cisco Firepower 9300에서 상황 그룹을 지원합니다.
MPLS RD	공격에서 사용하거나 사용한 MPLS RD입니다.
Device IP	공격에서 사용하거나 사용한 디바이스 IP 주소입니다.
TTL	공격에서 사용하거나 사용한 TTL입니다.
L4 Checksum	공격에서 사용하거나 사용한 L4 체크섬입니다.

표 133: BDoS 공격 세부 정보: 특징 매개변수(계속)

매개변수	설명
TCP Sequence Number	공격에서 사용하거나 사용한 TCP 시퀀스 번호입니다.
IP ID Number	공격에서 사용하거나 사용한 IP ID 번호입니다.
Fragmentation Offset	공격에서 사용하거나 사용한 프래그멘테이션 옵셋입니다.
Fragmentation Flag	공격에서 사용하거나 사용한 프래그멘테이션 플래그입니다. **0**은 프래그멘테이션이 허용됨을 나타냅니다. **1**은 프래그멘테이션이 허용되지 않음을 나타냅니다.
Flow Label	(IPv6 전용) 공격에서 사용하거나 사용한 플로우 라벨입니다.
ToS	공격에서 사용하거나 사용한 ToS입니다.
Packet Size	공격에서 사용하거나 사용한 패킷 크기입니다.
ICMP Message Type (프로토콜이 ICMP인 경우에만 표시됩니다.)	공격에서 사용하거나 사용한 ICMP 메시지 유형입니다.
Source IP	공격에서 사용하거나 사용한 소스 IP 주소입니다.
Destination IP	공격에서 사용하거나 사용한 대상 IP 주소입니다.
Source Ports	공격에서 사용하거나 사용한 소스 포트입니다.
Destination Ports	공격에서 사용하거나 사용한 대상 포트입니다.
DNS ID	공격에서 사용하거나 사용한 DNS ID입니다.
DNS Query	공격에서 사용하거나 사용한 DNS 쿼리입니다.
DNS Query Count	공격에서 사용하거나 사용한 DNS 쿼리 수입니다.

표 134: BDoS 공격 세부 정보: 정보 매개변수

매개변수	설명
Packet Size Anomaly Region	공격 패킷의 통계 영역입니다. 정책의 패킷 크기 베이스라인 공식은 다음과 같습니다. {(AnomalyBandwidth/AnomalyPPS)/(NormalBandwidth/NormalPPS)} 값: ● 대형 패킷—공격 패킷이 정책의 일반 패킷 크기 베이스라인보다 약 15% 큽니다. ● 일반 패킷—공격 패킷이 정책의 일반 패킷 크기 베이스라인의 약 15% 안에 포함됩니다. ● 소형 패킷—공격 패킷이 정책의 일반 패킷 크기 베이스라인보다 약 15% 작습니다.

표 134: BDoS 공격 세부 정보: 정보 매개변수(계속)

매개변수	설명
State	보호 프로세스의 상태입니다. 값: ● 공간 분석—동작 기반 DoS 보호에서 공격을 탐지했으며, 현재 공격 공간을 판별 중입니다. ● 차단—동작 기반 DoS 보호에서 생성된 공격 공간을 기반으로 공격을 차단 중입니다. 폐쇄 피드백 루프 작업을 통해 동작 기반 DoS 보호에서 공간 규칙을 최적화하여, 최소한의 작업으로 효율적인 차단 규칙을 달성합니다. ● 비공격—트래픽이 공격이 아니므로 차단되는 사항이 없습니다. 공간이 탐지되거나 차단 엄격도 레벨이 만족되지 않았습니다.

표 135: BDoS 공격 세부 정보: 공간 매개변수

매개변수	설명
동작 기반 DoS 보호에서 생성한 공간 차단 규칙으로, 최소한의 작업을 통해 플러드 공격에 대한 효율적인 차단 규칙을 제공합니다.	

표 136: BDoS 공격 세부 정보: 공격 통계 테이블

매개변수	설명
이 테이블에는 공격 트래픽(이상 징후)과 정상 트래픽 정보가 표시됩니다. 빨간색은 공격이 트리거되기 전에 15초간 의심스러운 것으로 식별된 실시간 값을 나타냅니다. 검은색은 학습된 정상 트래픽 베이스라인을 나타냅니다. 테이블 열은 TCP(모든 플래그 포함), UDP 또는 ICMP와 같은 프로토콜에 따라 표시됩니다.	

표 137: BDoS 공격 세부 정보: 공격 통계 그래프

매개변수	설명
그래프에서는 공격이 트리거된 동안 관련 트래픽 유형의 스냅샷을 15초 동안 표시합니다. 예를 들어, UDP 플러드 중에는 UDP 트래픽만 표시됩니다. 파란색 선은 정상 조정된 트래픽 베이스라인을 나타냅니다.	

표 138: BDoS 공격 세부 정보: 공격 설명

매개변수	설명
APSolute Vision 서버에 업로드된 경우 공격 설명 파일에 있는 공격 설명입니다.	

DNS 플러드 공격 세부 정보

표 139: DNS 플러드 공격 세부 정보: 특징 매개변수

매개변수	설명
참고: 일부 필드에 여러 값이 표시될 수 있습니다(해당되고 사용 가능한 경우). 표시되는 값은 현재 공격 상태에 따라 달라집니다. 필드가 동적 시그니처의 일부이면(즉, 하나 이상의 특정 값이 모든 공격 트래픽에 표시) **Characteristics(특징)** 필드에 하나 이상의 관련 값이 표시됩니다.	

표 139: DNS 플러드 공격 세부 정보: 특징 매개변수(계속)

매개변수	설명
Protocol	공격에서 사용하거나 사용한 프로토콜입니다.
Source L4 Port	공격에서 사용하거나 사용한 소스 L4 포트입니다.
Physical Port	공격에서 사용하거나 사용한 물리적 포트입니다.
Packet Count	공격의 패킷 수입니다.
Volume (Kbits)	공격에서 사용하거나 사용한 볼륨(Kbits)입니다.
VLAN/Context	공격을 처리한 정책의 VLAN 태그 값 또는 상황 그룹입니다. **참고:** VLAN 태그나 상황 그룹은 이 필드에 비슷한 정보를 식별합니다. DefensePro 6.x 및 7.x 버전에서 VLAN 태그를 지원합니다. DefensePro for Cisco Firepower 9300에서 상황 그룹을 지원합니다.
MPLS RD	공격에서 사용하거나 사용한 MPLS RD입니다.
Device IP	공격에서 사용하거나 사용한 디바이스 IP 주소입니다.
TTL	공격에서 사용하거나 사용한 TTL입니다.
L4 Checksum	공격에서 사용하거나 사용한 L4 체크섬입니다.
IP ID Number	공격에서 사용하거나 사용한 IP ID 번호입니다.
Packet Size	공격에서 사용하거나 사용한 패킷 크기입니다.
Destination IP	공격에서 사용하거나 사용한 대상 IP 주소입니다.
Destination Ports	공격에서 사용하거나 사용한 대상 포트입니다.
DNS ID	공격에서 사용하거나 사용한 DNS ID입니다.
DNS Query	공격에서 사용하거나 사용한 DNS 쿼리입니다.
DNS Query Count	공격에서 사용하거나 사용한 DNS 쿼리 수입니다.
DNS An Query Count	공격에서 사용하거나 사용한 DNS An 쿼리 수입니다.

표 140: DNS 플러드 공격 세부 정보: 정보 매개변수

매개변수	설명
State	보호 프로세스의 상태입니다.
Mitigation Action	차단 조치입니다. 값: ● 시그니처 조사 ● 시그니처 비율 제한 ● 종합적 조사 ● 종합적인 비율 제한

표 141: DNS 플러드 공격: 공간

매개변수	설명
동작 기반 DoS 보호에서 생성한 공간 차단 규칙입니다. 공간 차단 규칙에서는 최소한의 작업을 통해 플러드 공격에 대한 효율적인 차단 규칙을 제공합니다.	

표 142: DNS 플러드 공격 세부 정보: 공격 통계 테이블

매개변수	설명
이 테이블에는 공격 트래픽(이상 징후)과 정상 트래픽 정보가 표시됩니다. 빨간색은 공격이 트리거되기 전에 15초간 의심스러운 것으로 식별된 실시간 값을 나타냅니다. 검은색은 학습된 정상 트래픽 베이스라인을 나타냅니다. 테이블 열은 DNS 쿼리 유형(A, MX, PTR, AAAA, 텍스트, SOA, NAPTR, SRV, 기타)에 따라 표시됩니다.	

표 143: DNS 플러드 공격 세부 정보: 공격 통계 그래프

매개변수	설명
그래프에서는 공격이 트리거된 동안 관련 트래픽 유형의 스냅샷을 15초 동안 표시합니다. 예를 들어, UDP 플러드 중에는 UDP 트래픽만 표시됩니다. 파란색 선은 정상 조정된 트래픽 베이스라인을 나타냅니다.	

표 144: DNS 플러드 공격 세부 정보: 공격 설명

매개변수	설명
APSolute Vision 서버에 업로드된 경우 공격 설명 파일에 있는 공격 설명입니다.	

DoS 공격 세부 정보

표 145: DoS 공격 세부 정보: 특징 매개변수

매개변수	설명
프로토콜	공격에서 사용하거나 사용한 프로토콜입니다.
물리적 포트	공격에서 사용하거나 사용한 물리적 포트입니다.
패킷 수	공격의 패킷 수입니다.
소스 MSISDN	*MSISDN 분석 기능은 APSolute Vision 버전 3.0 이상에서 지원되지 않습니다.*
대상 MSISDN	*MSISDN 분석 기능은 APSolute Vision 버전 3.0 이상에서 지원되지 않습니다.*
VLAN / 상황	공격을 처리한 정책의 VLAN 태그 값 또는 상황 그룹입니다. **참고:** VLAN 태그나 상황 그룹은 이 필드에 비슷한 정보를 식별합니다. DefensePro 6.x 및 7.x 버전에서 VLAN 태그를 지원합니다. DefensePro for Cisco Firepower 9300에서 상황 그룹을 지원합니다.
MPLS RD	공격에서 사용하거나 사용한 MPLS RD입니다.
디바이스 IP	공격에서 사용하거나 사용한 디바이스 IP 주소입니다.

표 146: DoS 공격 세부 정보: 정보 매개변수

매개변수	설명
작업	수행한 보호 조치입니다.
공격자 IP	공격자의 IP 주소입니다.
보호된 호스트	보호된 호스트입니다.
보호 포트	보호 포트입니다.

표 146: DoS 공격 세부 정보: 정보 매개변수(계속)

매개변수	설명
공격 기간	공격 기간입니다.
현재 패킷 비율	현재 패킷 비율입니다.
평균 패킷 비율	평균 패킷 비율입니다.

표 147: DoS 공격 세부 정보: 공격 설명

매개변수	설명
APSolute Vision 서버에 업로드된 경우 공격 설명 파일에 있는 공격 설명입니다.	

패킷 이상 공격 세부 정보

표 148: 패킷 이상 공격 세부 정보: 특징 매개변수

매개변수	설명
프로토콜	공격에서 사용하거나 사용한 프로토콜입니다.
물리적 포트[1]	공격에서 사용하거나 사용한 물리적 포트입니다.
패킷 수	공격의 패킷 수입니다.
VLAN / 상황	공격을 처리한 정책의 VLAN 태그 값 또는 상황 그룹입니다. **참고:** VLAN 태그나 상황 그룹은 이 필드에 비슷한 정보를 식별합니다. DefensePro 6.x 및 7.x 버전에서 VLAN 태그를 지원합니다. DefensePro for Cisco Firepower 9300에서 상황 그룹을 지원합니다.
MPLS RD	공격에서 사용하거나 사용한 MPLS RD입니다.
디바이스 IP	공격에서 사용하거나 사용한 디바이스 IP 주소입니다.
공격 설명 APSolute Vision 서버에 업로드된 경우 공격 설명 파일에 있는 공격 설명입니다.	

1 – 이 매개변수는 분석되지 않으며, **다중** 값이 항상 표시됩니다.

표 149: 패킷 이상 공격 세부 정보: 공격 설명

매개변수	설명
APSolute Vision 서버에 업로드된 경우 공격 설명 파일에 있는 공격 설명입니다.	

SYN 플러드 공격 세부 정보

표 150: SYN 플러드 공격 세부 정보: 특징 매개변수

매개변수	설명
프로토콜	공격에서 사용하거나 사용한 프로토콜입니다.
물리적 포트	공격에서 사용하거나 사용한 물리적 포트입니다.
패킷 수	공격의 패킷 수입니다.

표 150: SYN 플러드 공격 세부 정보: 특징 매개변수(계속)

매개변수	설명
소스 MSISDN	*MSISDN 분석 기능은 APSolute Vision 버전 3.0 이상에서 지원되지 않습니다.*
대상 MSISDN	*MSISDN 분석 기능은 APSolute Vision 버전 3.0 이상에서 지원되지 않습니다.*
볼륨(Kbits)	공격에서 사용하거나 사용한 볼륨(Kbits)입니다.
VLAN / 상황	공격을 처리한 정책의 VLAN 태그 값 또는 상황 그룹입니다. **참고:** VLAN 태그나 상황 그룹은 이 필드에 비슷한 정보를 식별합니다. DefensePro 6.x 및 7.x 버전에서 VLAN 태그를 지원합니다. DefensePro for Cisco Firepower 9300에서 상황 그룹을 지원합니다.
MPLS RD	공격에서 사용하거나 사용한 MPLS RD입니다.

표 151: SYN 플러드 공격 세부 정보: 정보 매개변수

매개변수	설명
보호 조치가 차단 모드인 경우 정보가 표시됩니다. **주의:** SYN 보호가 보고만 수행 모드로 구성된 경우 평균 공격 비율, 공격 임계값 및 공격 볼륨 필드에 **0**(영)이 표시됩니다.	
평균 공격 비율	초당 도용된 SYN 비율 및 데이터 연결의 평균 비율로, 10초마다 계산됩니다.
공격 임계값	구성된 공격 트리거 임계값으로 초당 연결의 1/2입니다.
공격 볼륨	공격 라이프사이클 중에 도용된 TCP 연결의 패킷 수입니다(집계됨). 이 패킷은 SYN 쿠키 메커니즘을 통해 설정되거나 SYN 보호 신뢰 목록을 통해 전달된 세션에서 입력됩니다.
공격 기간	보호 포트에서의 공격 기간(hh:mm:ss 형식)입니다.
TCP 조사	공격을 식별한 *인증 방법*입니다.
HTTP 조사	공격을 식별한 *HTTP 인증 방법*: *302- 리디렉션 또는 JavaScript*.

표 152: SYN 플러드 공격 세부 정보: 인증 목록 사용률 매개변수

매개변수	설명
TCP 인증 목록	TCP 인증 테이블의 현재 사용률(%)입니다.
HTTP 인증 목록	테이블 인증 테이블의 현재 사용률(%)입니다.

표 153: SYN 플러드 공격 세부 정보: 공격 설명

매개변수	설명
APSolute Vision 서버에 업로드된 경우 공격 설명 파일에 있는 공격 설명입니다.	

샘플링된 데이터 탭

샘플링된 데이터를 지원하는 모든 공격 유형의 *Sampled Data(샘플링된 데이터)* 대화 상자를 표시할 수 있습니다.

Sampled Data(샘플링된 데이터) 탭에는 샘플링된 공격 패킷에 대한 데이터가 포함된 테이블이 있습니다. 테이블의 각 행에는 샘플링된 한 공격 패킷의 데이터가 표시됩니다. 제목 표시줄에는 데이터의 카테고리가 포함됩니다(예: *동작 기반 DoS*).

Sampled Data(샘플링된 데이터) 탭의 테이블은 다음 열로 구성됩니다.

- **시간**
- **소스 주소**
- **소스 MSISDN**—*MSISDN 분석 기능은 APSolute Vision 버전 3.0 이상에서 지원되지 않습니다.*
- **소스 L4 포트**
- **대상 주소**
- **대상 MSISDN**—*MSISDN 분석 기능은 APSolute Vision 버전 3.0 이상에서 지원되지 않습니다.*
- **대상 L4 포트**
- **프로토콜**
- **VLAN / 상황**
- **MPLS RD**
- **물리적 포트**

샘플링된 데이터 탭을 표시하려면

1. *Security Monitoring(보안 모니터링)* 관점에서 데이터를 표시할 DefensePro 디바이스 또는 사이트를 선택합니다.
2. **Dashboard View(대시보드 보기) > Security Dashboard(보안 대시보드)**를 선택합니다.
3. 다음 중 하나를 수행하여 *Attack Details(공격 세부 정보)* 탭을 엽니다.
   - 보안 대시보드 차트 보기()에서 아이콘을 두 번 클릭합니다.
   - 보안 대시보드 테이블 보기()에서 관련 행을 두 번 클릭합니다.
4.  (View Sampled Data(샘플링된 데이터 보기)) 버튼을 클릭합니다.

Sampled Data(샘플링된 데이터) 대화 상자에 있는 테이블의 행을 CSV 파일에 내보낼 수 있습니다.

샘플링된 데이터를 CSV 파일에 저장하려면

1. *Security Monitoring(보안 모니터링)* 관점에서 데이터를 표시할 DefensePro 디바이스 또는 사이트를 선택합니다.
2. **Dashboard View(대시보드 보기) > Security Dashboard(보안 대시보드)**를 선택합니다.

3. 다음 중 하나를 수행하여 *Attack Details(공격 세부 정보)* 탭을 엽니다.
   - 보안 대시보드 차트 보기()에서 아이콘을 두 번 클릭합니다.
   - 보안 대시보드 테이블 보기()에서 관련 행을 두 번 클릭합니다.
4.  (View Sampled Data(샘플링된 데이터 보기)) 버튼을 클릭합니다.
5. 파일에서 데이터 행이 시작되게 할 행을 선택합니다.
6.  (CSV) 버튼을 클릭합니다.
7. 파일을 보거나 위치와 파일 이름을 지정합니다.

실시간 트래픽 보고서 보기

기본적으로 모든 트래픽이 이러한 그래프와 테이블에 표시됩니다. 각 그래프에서 프로토콜이나 트래픽 방향별로 표시를 필터링할 수 있지만 동시 연결에 대해서는 수행할 수 없습니다.

Traffic Monitoring(트래픽 모니터링) 탭에서 다음 트래픽 정보를 모니터링할 수 있습니다.

- 트래픽 사용률 통계 보기, 188페이지
- 연결 비율 통계 보기, 191페이지
- 동시 연결 통계 보기, 191페이지

트래픽 사용률 통계 보기

APSolute Vision에서는 다음에 대한 트래픽 사용률 통계를 표시할 수 있습니다.

- **통계 그래프**—선택한 포트 쌍의 정보를 그래프로 표시합니다. 그래프에는 일정 기간 동안 모든 프로토콜의 총계 또는 선택한 프로토콜의 정보가 포함되어 있습니다.

  다음에 대한 그래프에는 각각 곡선이 있습니다.
  - 인바운드 IP 트래픽
  - 아웃바운드 IP 트래픽
  - 폐기된 인바운드 트래픽
  - 폐기된 아웃바운드 트래픽
  - 제외된 인바운드 트래픽
  - 제외된 아웃바운드 트래픽

  특정 트래픽 유형의 곡선을 숨기거나 표시하려면 범례에서 색상이 지정된 해당 정사각형을 클릭합니다.
- **트래픽 인증 통계(조사/응답)**—조사-응답 메커니즘을 지원하는 보호 모듈에서 관련 옵션이 사용되면 조사-응답 메커니즘의 통계를 표시합니다.
- **마지막 샘플 통계**—각 프로토콜의 마지막 측정값을 표시하고 단일 디바이스의 모든 프로토콜에 대한 총계를 제공합니다. (이 정보는 단일 디바이스를 볼 때만 사용할 수 있습니다.)

  CSV 파일을 보거나 저장하려면  (CSV)를 클릭합니다.

팁: 초당 바이트 또는 패킷으로 현재 트래픽 비율을 얻으려면(15초 동안의 평균 비율로 계산) DefensePro 디바이스에서 다음 CLI 명령을 사용할 수 있습니다.

dp rtm-stats get [포트 번호]

트래픽 사용률 통계를 표시하려면

1. *Security Monitoring(보안 모니터링)* 관점에서 데이터를 표시할 DefensePro 디바이스 또는 사이트를 선택합니다.
2. **Traffic Monitoring(트래픽 모니터링) > Traffic Utilization Report(트래픽 사용률 보고)**를 선택합니다.
3. 그래프 및 테이블의 표시 설정을 필요한 대로 변경합니다.
4. *통계 그래프* 및 *마지막 샘플링 통계*의 경우 표시된 트래픽 데이터의 필터 옵션을 필요한 대로 설정합니다. 표시된 정보를 자동으로 새로 고칩니다.

표 154: 트래픽 사용률 보고: 그래프 및 테이블의 표시 매개변수

매개변수	설명
범위 (테이블을 표시하는 링크입니다.)	트래픽 사용률 보고에서 표시하는 네트워크 보호 정책입니다. 기본적으로 범위는 **모든 범위** 또는 **모든 정책**입니다(**범위** 드롭다운 목록에 지정된 값에 따라 다름). 즉, 기본적으로 트래픽 사용률 보고에는 모든 정보가 표시됩니다. 트래픽 사용률 보고에서 표시하는 정보의 범위를 제어하려면 트래픽 사용률 보고에서 표시하는 정보 범위를 제어하려면, 190페이지 절차를 참조하십시오. **참고:** DefensePro for Cisco Firepower 9300에서는 범위의 물리적 포트 제한을 지원하지 않습니다.
마지막 표시	공격이 종료된 후 그래프에서 공격을 표시하는 기간입니다. 즉, 그래프에서 현재 진행 중이거나 선택한 기간 내에 종료된 모든 공격을 표시합니다. 값: ● 10분 ● 20분 ● 30분 ● 1시간 기본값: 10분
범위 (드롭다운 목록입니다.)	그래프 보기의 범위입니다. 값: ● 디바이스/물리적 포트—그래프에서 지정된 디바이스의 물리적 포트에 따라 트래픽을 표시합니다. ● 디바이스/정책—그래프에서 지정된 디바이스의 네트워크 보호 정책에 따라 트래픽을 표시합니다. 기본값: 디바이스/물리적 포트 **참고:** DefensePro for Cisco Firepower 9300에서는 범위의 물리적 포트 제한을 지원하지 않습니다.
단위	트래픽 비율의 단위입니다. 값: ● Kbps—초당 킬로비트입니다. ● 패킷/초—초당 패킷 수입니다.

트래픽 사용률 보고에서 표시하는 정보 범위를 제어하려면

1. Scope를 클릭합니다. 테이블이 열립니다. **Scope(범위)** 드롭다운 목록에 지정된 값(**Devices/Physical Ports(디바이스/물리적 포트)** 또는 **디바이스/정책(Devices/Policies)**)에 따라 테이블에는 *Device Name(디바이스 이름)* 및 *포트(Port)* 열 또는 *Device Name(디바이스 이름)* 및 *Policy(정책)* 열이 있습니다.

   참고: DefensePro for Cisco Firepower 9300에서는 범위의 물리적 포트 제한을 지원하지 않습니다.

2. 다음 중 하나를 수행합니다.
   - 트래픽 사용률 보고에서 표시하는 물리적 포트 또는 네트워크 보호 정책을 제한하려면 해당 확인란을 선택합니다.
   - 현재 관련된 모든 물리적 포트 또는 네트워크 보호 정책의 정보를 표시하려면 왼쪽 위 테이블 셀을 클릭한 다음 **Select All(모두 선택)**을 선택합니다.
   - 특정 포트 또는 특정 네트워크 보호 정책과 관련되지 않은 정보도 포함하여 데이터베이스의 모든 정보를 표시하려면 왼쪽 위 표 셀을 클릭한 다음 **Select None(선택하지 않음)**을 선택합니다.

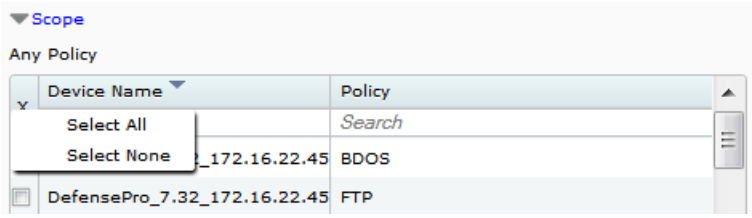


표 155: 트래픽 사용률 보고: 트래픽 사용률 그래프의 필터 매개변수

매개변수	설명
방향	그래프에서 표시하는 트래픽입니다. 값: ● Inbound(인바운드)—인바운드 트래픽을 표시합니다. ● Outbound(아웃바운드)—아웃바운드 트래픽을 표시합니다. ● Both(둘 다)—인바운드 및 아웃바운드 트래픽을 표시합니다. 인바운드 및 아웃바운드 데이터는 총계가 아니라 개별 라인으로 표시됩니다. **참고:** 포트 쌍 사이의 트래픽 방향은 포트 쌍 컨피그레이션의
프로토콜	표시할 트래픽 프로토콜입니다. 값: ● TCP—TCP 트래픽의 통계를 표시합니다. ● UDP—UDP 트래픽의 통계를 표시합니다. ● ICMP—ICMP 트래픽의 통계를 표시합니다. ● IGMP—IGMP 트래픽의 통계를 표시합니다. ● SCTP—SCTP 트래픽의 통계를 표시합니다. ● 기타—TCP, UDP, ICMP, IGMP 또는 SCTP가 아닌 트래픽의 통계를 표시합니다. ● 모두—전체 트래픽 통계를 표시합니다.

표 156: 트래픽 사용률 보고: 트래픽 인증 통계(조사/응답) 매개변수

매개변수	설명
프로토콜	행에 표시되는 통계의 프로토콜입니다. 값: HTTP, TCP, DNS **참고:** HTTP 행은 DefensePro for Cisco Firepower 9300에는 해당하지 않습니다.
현재 공격	디바이스의 현재 공격 수입니다.
인증 테이블 사용률 %	가득 찬 인증 테이블의 백분율입니다.
조사 비율	디바이스에서 조사를 전송 중인 비율(PPS)입니다.

표 157: 트래픽 사용률 보고: 마지막 샘플링 통계 매개변수

매개변수	설명
프로토콜	트래픽 프로토콜입니다. 값: ● TCP ● UDP ● ICMP ● IGMP ● SCTP ● 기타—TCP, UDP, ICMP, IGMP 또는 SCTP가 아닌 트래픽의 통계입니다. ● 모두—전체 트래픽 통계입니다.
인바운드	행에서 식별된 프로토콜의 인바운드 트래픽 양입니다.
아웃바운드	행에서 식별된 프로토콜의 아웃바운드 트래픽 양입니다.
Discarded Inbound (폐기된 인바운드)	행에서 식별된 프로토콜에 대해 폐기된 인바운드 트래픽의 양입니다.
Discarded Outbound (폐기된 아웃바운드)	행에서 식별된 프로토콜에 대해 폐기된 아웃바운드 트래픽 양입니다.
Discard %(폐기 %)	행에서 식별된 프로토콜에 대해 폐기된 트래픽의 백분율입니다.
Excluded Inbound (제외된 인바운드)	행에서 식별된 프로토콜에 대해 제외된 인바운드 트래픽의 양입니다.
Excluded Outbound (제외된 아웃바운드)	행에서 식별된 프로토콜에 대해 제외된 아웃바운드 트래픽의 양입니다.

연결 비율 통계 보기

이 기능은 DefensePro for Cisco Firepower 9300에서 작동하지 않습니다.

동시 연결 통계 보기

이 기능은 DefensePro for Cisco Firepower 9300에서 작동하지 않습니다.

보호 모니터링

보호 모니터링에서는 네트워크 전체(BDoS가 구성된 경우) 또는 DNS 트래픽(DNS가 구성된 경우)에 대한 네트워크 정책당 실시간 트래픽 모니터링을 제공합니다. 보호 모니터링에서 제공하는 통계 트래픽 정보를 사용하면 보호 네트워크를 통해 이동하는 트래픽, 구성된 보호 작동 방식 및 무엇보다도 중요하게 이상 징후 트래픽을 탐지하는 방법에 대한 이해를 높일 수 있습니다.

선택한 디바이스의 보호 정보를 표시하는 데 대한 정보는 다음을 참조하십시오.

- 공격 상태 정보 표시, 192페이지
- BDoS 트래픽 모니터링, 192페이지
- DNS 트래픽 모니터링, 195페이지

공격 상태 정보 표시

구성되어 사용되는 각 보호 정책의 공격에 대한 요약 상태 정보를 표시할 수 있습니다. 네트워크 보호 정책을 위반하는 공격이 있으면 테이블에서 관련 공격 트래픽의 해당 행에 공격 상태를 나타내는 아이콘이 표시됩니다.

공격 상태 정보를 표시하려면

1. *Security Monitoring(보안 모니터링)* 관점에서 모니터링할 DefensePro 디바이스를 선택합니다.
2. **Protection Monitoring(보호 모니터링) > Attack Status Report(공격 상태 보고)**를 선택합니다.

   이 테이블은 다음과 같은 열로 구성됩니다.
   - 정책 이름
   - IPv4-TCP
   - IPv4-UDP
   - IPv4-ICMP
   - IPv4-DNS
   - IPv6-TCP
   - IPv6-UDP
   - IPv6-ICMP
   - IPv6-DNS
3. 테이블에 공격 아이콘이 표시되면 아이콘을 클릭하여 해당 공격 트래픽 정보를 표시합니다.

BDoS 트래픽 모니터링

BDoS 보호를 포함하는 네트워크 보호 정책의 트래픽을 모니터링할 수 있습니다. *Statistics Graph(통계 그래프)* 및 *Last Sample Statistics(마지막 샘플 통계)* 테이블에 트래픽 정보가 표시됩니다.

주의: 트래픽이 상태 없음 보호와 여러 네트워크 보호 정책을 일치시키면 APSolute Vision에서 삭제된 총 트래픽에 대해 표시하는 값은 관련된 모든 네트워크 보호 정책에 맞게 삭제된 모든 트래픽의 합계를 나타냅니다. 트래픽이 여러 네트워크 보호 정책을 상태 없음 보호와 일치시키면 해당 네트워크 보호 정책이 모두 삭제된 동일한 트래픽 수를 세기 때문입니다.

BDoS 보호를 포함하는 네트워크 정책의 트래픽 정보를 표시하려면

1. *Security Monitoring(보안 모니터링)* 관점에서 모니터링할 디바이스를 선택합니다.
2. **Protection Monitoring(보호 모니터링) > BDoS Traffic Monitoring Reports(BDOS 트래픽 모니터링 보고)**를 선택합니다.
3. *BDoS Traffic Statistics(BDoS 트래픽 통계)* 그래프 및 *Last Sample Statistics(마지막 샘플 통계)* 테이블의 표시 범위를 구성합니다.

통계 그래프

테이블에는 지정된 매개변수에 따라 선택된 네트워크 보호 정책의 트래픽 비율이 표시됩니다.

표 158: 통계 그래프 및 마지막 샘플 통계 테이블의 범위 매개변수

매개변수	설명
범위	네트워크 보호 정책입니다. 목록은 BDoS 프로필에 만 구성 된 정책을 표시 합니다.
마지막 표시	공격이 종료된 후 그래프에서 공격을 표시하는 기간입니다. 즉, 그래프에서 현재 진행 중이거나 선택한 기간 내에 종료된 모든 공격을 표시합니다. 값: ● 10분 ● 20분 ● 30분 ● 1시간 기본값: 10분
방향	*Statistics Graph(통계 그래프)* 및 *Last Sample Statistics(마지막 샘플 통계)* 테이블에서 표시하는 트래픽의 방향입니다. 값: Inbound(인바운드), Outbound(아웃바운드)
단위	*통계 그래프*와 *마지막 샘플 통계* 테이블에서 트래픽을 표시하는 데 사용하는 단위입니다. 값: ● Kbps—초당 킬로비트입니다. ● 패킷/초—초당 패킷 수입니다.

표 159: 통계 그래프 매개변수

매개변수	설명
IP 버전	그래프에서 표시하는 트래픽의 IP 버전입니다. 값: IPv4, IPv6
보호 유형	모니터링할 보호 유형입니다. 값: ● TCP ACK FIN ● TCP FRAG ● TCP RST ● TCP SYN ● TCP SYN ACK ● UDP ● UDP FRAG ● ICMP ● IGMP
규모	Y축을 따라 정보를 표시하기 위한 눈금입니다. 값: 선형, 로그
공격 상태	(읽기 전용) 공격 상태입니다.

표 160: 통계 그래프 범례

Line	설명
총 트래픽 (진한 파란색)	디바이스에서 특정 보호 유형과 방향에 대해 확인하는 총 트래픽입니다.
합법적 트래픽 (연한 파란색)	DefensePro에서 공격을 차단한 후 실제 전달된 트래픽 비율입니다. 공격이 없으면 총 트래픽과 합법적 트래픽이 같습니다.
일반 에지 (녹색 파선)	통계적으로 계산된 베이스라인 트래픽 비율입니다.
의심스러운 에지 (주황색 파선)	공격의 가능성이 있는 트래픽 변경을 나타내는 트래픽 비율입니다.
공격 에지 (빨간색 파선)	공격을 나타내는 트래픽 비율입니다.

표 161: 마지막 샘플 통계 매개변수

매개변수	설명
트래픽 유형	보호 유형입니다. 특정 트래픽 유형과 방향에는 각각 디바이스에서 자동으로 학습하는 베이스라인이 있습니다.
기본	디바이스에서 예상되는 일반적인 트래픽 비율입니다.
총 트래픽	디바이스에서 특정 트래픽 유형과 방향에 대해 확인하는 총 트래픽 비율입니다.

표 161: 마지막 샘플링 통계 매개변수(계속)

매개변수	설명
베이스라인 부분 %	비율 불변 베이스라인을 표시합니다. 즉, 동일한 방향의 기타 모든 트래픽과 비교하여 특정 트래픽 유형의 정상 백분율입니다.
RT 부분 %	동일한 방향의 기타 모든 트래픽과 비교하여 특정 트래픽 유형의 실제 백분율입니다.
합법적 트래픽	디바이스에서 공격을 차단한 후 실제 전달된 트래픽 비율입니다. 공격이 없으면 RT 비율과 합법적 비율이 같습니다.
합법적 부분 %	디바이스에서 공격을 차단한 후 기타 트래픽 유형과 비교하여 지정된 유형의 트래픽이 실제로 전달된 비율입니다.
공격 수준	현재 공격 레벨을 평가하는 숫자 값입니다. 값이 8 이상이면 공격을 나타냅니다.

DNS 트래픽 모니터링

DNS 플러드 보호를 포함하는 네트워크 보호 정책의 트래픽을 모니터링할 수 있습니다. *Statistics Graph(통계 그래프)* 및 *Last Sample Statistics(마지막 샘플 통계)* 테이블에 트래픽 정보가 표시됩니다.

DNS 보호를 포함하는 네트워크 보호 정책의 트래픽 정보를 표시하려면

1. *Security Monitoring(보안 모니터링)* 관점에서 모니터링할 디바이스를 선택합니다.
2. **Protection Monitoring(보호 모니터링) > BDoS Traffic Monitoring Reports(DNS 트래픽 모니터링 보고)**를 선택합니다.
3. *통계* 그래프 및 *마지막 샘플 통계* 테이블을 표시하는 데 사용하는 필터를 구성합니다.

통계 그래프

그래프에는 지정된 매개변수에 따라 선택된 네트워크 보호 정책의 트래픽 비율이 표시됩니다.

표 162: 통계 그래프 및 마지막 샘플 통계 테이블의 범위 매개변수

매개변수	설명
범위	네트워크 보호 정책입니다. 목록에는 DNS 프로필에만 구성된 규칙이 표시됩니다.
방향	*Statistics Graph(통계 그래프)* 및 *Last Sample Statistics(마지막 샘플 통계)* 테이블에서 표시하는 트래픽의 방향입니다. 값: Inbound(인바운드), Outbound(아웃바운드)
단위	(읽기 전용) *통계 그래프*와 *마지막 샘플 통계* 테이블에서 트래픽을 표시하는 데 사용하는 단위입니다. 값: QPS—초당 쿼리 수

표 163: 통계 그래프 매개변수

매개변수	설명
IP 버전	그래프에서 표시하는 트래픽의 IP 버전입니다. 값: IPv4, IPv6

표 163: 통계 그래프 매개변수(계속)

매개변수	설명
보호 유형	모니터링할 DNS 쿼리 유형입니다. 값: ● 기타 ● 텍스트 ● A ● AAAA ● MX ● NAPTR ● PTR ● SOA ● SRV
규모	Y축을 따라 정보를 표시하기 위한 눈금입니다. 값: 선형, 로그
공격 상태	(읽기 전용) 공격 상태입니다.

표 164: 통계 그래프 범례

Line	설명
총 트래픽 (진한 파란색)	디바이스에서 특정 보호 유형과 방향에 대해 확인하는 총 트래픽입니다.
합법적 트래픽 (연한 파란색)	DefensePro에서 공격을 차단한 후 실제 전달된 트래픽 비율입니다. 공격이 없으면 총 트래픽과 합법적 트래픽이 같습니다.
일반 에지[1] (녹색 파선)	통계적으로 계산된 베이스라인 트래픽 비율입니다.
의심스러운 에지[1] (주황색 파선)	공격의 가능성이 있는 트래픽 변경을 나타내는 트래픽 비율입니다.
공격 에지[1] (빨간색 파선)	공격을 나타내는 트래픽 비율입니다.

1 – 이 라인은 사용 공간 바이패스 또는 수동 트리거를 사용하도록 보호가 구성된 경우에는 표시되지 않습니다.

마지막 샘플 통계 테이블

그래프에 마지막 샘플 통계가 표시됩니다.

표 165: 마지막 샘플 통계 매개변수

매개변수	설명
트래픽 유형	보호 유형입니다. 특정 트래픽 유형과 방향에는 각각 디바이스에서 자동으로 학습하는 베이스라인이 있습니다.
기본	디바이스에서 예상되는 일반적인 트래픽 비율입니다.

표 165: 마지막 샘플 통계 매개변수(계속)

매개변수	설명
총 트래픽	DefensePro 디바이스에서 특정 트래픽 유형과 방향에 대해 확인하는 총 트래픽 비율입니다.
베이스라인 부분 %	비율 불변 베이스라인을 표시합니다. 즉, 동일한 방향의 기타 모든 트래픽과 비교하여 특정 트래픽 유형의 정상 백분율입니다.
RT 부분 %	동일한 방향의 기타 모든 트래픽과 비교하여 특정 트래픽 유형의 실제 백분율입니다.
합법적 트래픽	디바이스에서 공격을 차단한 후 실제 전달된 트래픽 비율입니다. 공격이 없으면 RT 비율과 합법적 비율이 같습니다.
합법적 부분 %	디바이스에서 공격을 차단한 후 기타 트래픽 유형과 비교하여 지정된 유형의 트래픽이 실제로 전달된 비율입니다.
공격 수준	현재 공격 레벨을 평가하는 숫자 값입니다. 값이 8 이상이면 공격을 나타냅니다.

새로운 보안 공격 경고

현재 공격(*Security Monitoring(보안 모니터링)* 관점의 일부) 테이블에 새로운 공격이 표시되면 APSolute Vision에서 경고를 트리거합니다.

Alerts(경고) 창에 있는 *Module(모듈)* 열의 값이 *Security Reporting(보안 보고)*입니다.
각 DefensePro 디바이스에서 개별 보안 경고를 트리거합니다.

보안 경고는 단일 보안 이벤트(즉, 단일 공격 이벤트)용이거나 여러 보안 이벤트에서 집계됩니다. 단일 공격과 다중 공격의 경고 형식은 비슷합니다.

표 166: 보안 경고의 정보

단일 공격용 보안 경고의 문자열	보안 경고 집계 공격 정보의 문자열
공격 유형: <attack category>[1]가 시작되었습니다.	<quantity of attacks> 공격 유형: <attack category>[1]이 <start time of first attack>과(와) <start time of last attack>.[2] 사이에 시작되었습니다.
탐지 규칙: <Network Protection policy>;	탐지 규칙: <Network Protection policy>;[3]
공격 이름: <attack name>;	공격 이름: <attack name>;[3]
소스 IP: <attacker IP address>;	소스 IP: <attacker IP address>;[4]
대상 IP: <attacked IP address>;	대상 IP: <attacked IP address>;
대상 포트: <attacked port>;	대상 포트: <attacked port>;
조치: <action>.	조치: <action>.

1 – 공격 카테고리(가능한 *모든* DefensePro 버전 및 컨피그레이션에 해당).
- ACL
- 스캔 방지
- 동작 기반 DoS(Behavioral DoS)
- DoS
- HTTP 플러드
- 침입
- 서버 크래킹
- SYN 플러드
- 이상 징후
- 상태 저장 ACL
- DNS
- BWM

2 – 시간의 형식은 dd.MM.yy hh:mm입니다.
3 – 공격의 필드 값이 다르면 값은 쉼표로 구분됩니다.
4 – 공격의 필드 값이 다르면 값은 **다중**입니다. 값이 **다중**이면 DefensePro에서 특정 값을 보고할 수 없는 경우도 나타낼 수 있습니다.

APSolute Vision 관리자가 보안 경고에 포함된 매개변수를 제한할 수 있습니다. 종종 이메일을 통해 수신되는 보안 경고를 스마트폰에서 보는 경우가 많으므로 이 옵션이 유용합니다. 작은 화면 크기에 맞도록 관리자가 경고에 포함할 매개변수를 선택할 수 있습니다.

보안 경고에 포함할 매개변수를 선택하려면

1. *APSolute Vision Settings(APSolute Vision 설정)* 보기 *System(시스템)* 관점에서 **General Settings(일반 설정) > Alert Browser(경고 브라우저) > Security Alerts(보안 경고)**를 선택합니다.
2. 경고에 포함할 각 매개변수 옆에 있는 확인란을 선택합니다. 다음 매개변수의 조합을 선택할 수 있습니다.
   - 정책 이름
   - 공격 이름
   - 소스 IP 주소
   - 대상 IP 주소
   - 대상 포트
   - 작업

   기본적으로 모든 확인란이 선택됩니다.
3. **Submit(제출)**을 클릭합니다.

참고: 설정 변경사항은 변경 및 전달 시에 생성된 경고에 적용됩니다.

12장 – DefensePro 관리

이 장에서는 DefensePro 관리에 대해 설명하며 다음 절이 포함되어 있습니다.

- CLI(Command Line Interface), 199페이지
- 웹 서비스, 201페이지
- API 구조, 202페이지
- APSolute API SDK(Software Development Kit), 202페이지

Command Line Interface

CLI(Command Line Interface)에 액세스하려면 직렬 케이블 연결과 터미널 에뮬레이션 애플리케이션이 있어야 합니다.

DefensePro에서는 최대 5개의 동시 텔넷 또는 SSH 세션을 지원합니다.

디버깅을 수행하는 데도 CLI를 사용할 수 있습니다. 디버깅이 필요한 경우 DefensePro에서는 텍스트 형식으로 제공되는 개별 파일을 생성하며, Radware Technical Support에 필요한 모든 CLI 명령을 집계합니다. 파일에는 *클라이언트* 테이블, *ARP* 테이블 등의 인쇄물과 같은 다양한 CLI 명령의 출력도 포함됩니다. APSolute Vision을 사용하여 이 파일을 다운로드한 다음 Radware Technical Support에 보낼 수 있습니다(디바이스 컨피그레이션 파일 다운로드, 61페이지 참조).

표 167: DefensePro CLI 명령 및 메뉴

명령	설명
ACL	액세스 제어 목록입니다.
classes	분류에 사용되는 트래픽 특성을 구성합니다.
device	디바이스 설정입니다.
dp	DefensePro 보안 설정입니다.
help	지정된 명령의 도움말을 표시합니다.
login	디바이스에 로그인합니다.
logout	디바이스에서 로그아웃합니다.
manage	디바이스 관리 컨피그레이션입니다.
net	네트워크 컨피그레이션입니다.
ping	원격 호스트를 Ping합니다.
reboot	장비를 재부팅합니다.
security	디바이스 보안입니다.
services	일반 네트워킹 서비스입니다.
shutdown	종료합니다.
ssh	SSH를 통해 원격 호스트에 연결합니다.
statistics	디바이스 통계 컨피그레이션입니다.
system	시스템 매개변수를 설정합니다.
telnet	텔넷을 통해 원격 호스트에 연결합니다.
trace-route	지정된 대상의 홉과 레이턴시를 측정합니다.

CLI 세션 시간 초과

텔넷 또는 SSH를 통해 CLI에 로그온하면 인증 절차를 완료하도록 미리 정의된 시간 초과가 있습니다. 디바이스와 CLI 세션을 설정한 후 *Authentication Time-out(인증 시간 초과)* 매개변수에 정의된 기간 내에 사용자 이름과 비밀번호를 삽입해야 합니다. 로그인을 세 번 잘못 시도하고 나면 터미널이 10분 간 잠기며 해당 IP 주소에서 더 이상 로그인이 허용되지 않습니다.

텔넷 또는 SSH 세션의 경우, 세션 시간 초과 매개변수로 세션이 비활성화되어도 디바이스와의 연결이 유지관리되는 기간을 정의합니다. 미리 정의된 기간이 종료되어도 세션이 여전히 비활성이면 세션이 자동으로 종료됩니다.

세션 시간 초과 매개변수로 세션이 비활성화되어도 콘솔을 통해 디바이스와의 연결이 계속 열려 있는 기간을 지정할 수 있습니다. 미리 정의된 시간이 지나고 나면 세션이 자동으로 종료됩니다.

세션 시간 초과를 구성하려면

> 콘솔의 경우 다음 명령을 사용합니다.

Manage terminal session-timeout

> SSH 세션의 경우 다음 명령을 사용합니다.

Manage ssh session-timeout

> 텔넷 세션의 경우 다음 명령을 사용합니다.

Manage telnet session-timeout

> SSH 인증의 경우 다음 명령을 사용합니다.

Manage ssh auth-timeout

> 텔넷 인증의 경우 다음 명령을 사용합니다.

Manage telnet auth-timeout

CLI 기능

콘솔 액세스, 텔넷 또는 SSH를 통해 DefensePro CLI를 사용할 수 있습니다.

CLI에서는 다음과 같은 기능을 제공합니다.

- 일관되고 논리적으로 구성된 직관적인 명령 구문.
- 현재 디바이스 컨피그레이션을 볼 수 있으며, CLI 명령행으로 형식화된 system config 명령.
- system config 설정 명령을 사용하여 system config의 출력 또는 일부를 다른 디바이스의 CLI에 붙여넣기. 이 옵션은 쉬운 컨피그레이션 복제에 사용할 수 있습니다.
- 도움말 및 명령 완료 키.
- 명령행 편집 키.
- 명령 기록.
- 구성 가능한 프롬프트.
- 텔넷 및 SSH에 대해 구성 가능한 배너.
- Ping—네트워크의 다른 호스트를 Ping하여 다른 호스트의 가용성 테스트.
- Traceroute—다음 명령을 사용합니다.

  trace-route <destination IP address>

  출력 형식:

  DP#trace-route www.radware.com

trace-route to host 209.218.228.203:

```
1:      50ms     50ms     50ms  212.150.43.130
2:      50ms     50ms     50ms  80.74.101.129
3:      50ms     50ms     50ms  192.116.214.2
4:      *        *        *
5:      50ms     50ms     50ms  80.74.96.40
```

- 텔넷 클라이언트—원격 호스트에 대한 텔넷 세션을 시작하려면 다음 CLI 명령을 사용합니다.
  telnet <IP address>
- SSH 클라이언트—원격 호스트에 대한 SSH 세션을 시작하려면 다음 CLI 명령을 사용합니다.
  ssh <IP address>

CLI 트랩

직렬 케이블을 통해 물리적 DefensePro 플랫폼에 연결하면 이벤트 발생 시 디바이스에서 트랩을 생성합니다.

CLI, 텔넷 및 SSH를 통해 트랩을 보내는 명령은 다음과 같습니다.

manage terminal traps-outputs set-on

콘솔 전용:

manage terminal traps-outputs set normal

모든 CLI 사용자에게 트랩 전송

이 옵션을 사용하면 트랩을 직렬 터미널에만 보내거나 SSH와 텔넷 클라이언트에도 보낼지 구성할 수 있습니다.

웹 서비스

DefensePro Radware 디바이스는 SNMP, 직렬 포트, 텔넷, SSH, HTTP(내부 웹 애플리케이션 사용) 및 HTTPS를 통해 관리할 수 있습니다. 고객에게 향상된 애플리케이션 모니터링, 맞춤 설정된 애플리케이션 전달 네트워크 관리 애플리케이션 및 고급 자동화 툴을 개발하는 기능을 제공하기 위해 Radware에서는 개방형 표준 기반 SOAP(XML) API인 APSolute API를 사용하는 DefensePro의 웹 서비스 인터페이스를 제공합니다.

APSolute API와 통합하면 고객이 디바이스 성능을 포괄적으로 볼 수 있습니다. 여기에는 이력 데이터 분석 및 트렌드 분석, 성능 진단, 가용성 보고서 및 외부 매개변수에 따라 최적으로 애플리케이션을 전달하기 위한 DefensePro 미세 조정 및 유지관리 작업 자동화 등이 포함됩니다.

주요 기능:

- 외부 애플리케이션에서 Radware 제품 기능 제어.
- API 사용 네트워크 디바이스가 애플리케이션의 소프트웨어로 표시되므로, 진정한 소프트웨어 고유 통합이 가능.
- 여러 개발 플랫폼과 언어용 포괄적인 SDK.
- 광범위한 샘플 애플리케이션 코드, 문서 및 컨피그레이션 가이드.
- 웹 서비스 기반 API를 통해 사용 가능한 1,700개 이상의 방법.
- HTTPS를 통한 SOAP/XML 지원을 통해 유연하고 안전한 통신이 가능.

API 구조

APSolute API는 Java, Visual Basic/C# 및 Perl 등의 일반적인 개발 언어를 사용하여 서드파티 애플리케이션의 DefensePro 디바이스에 대한 전체 액세스를 제공하는 SOAP/XML 인터페이스입니다. 이 인터페이스를 사용하면 디바이스 컨피그레이션과 모니터링 상태 및 성능 통계가 가능합니다.

APSolute API에서는 DefensePro 디바이스와 상호 작용하는 다음 두 가지 방법을 제공합니다.

1. CLI 명령 실행:

   이 인터페이스에서는 다음을 지원하지 않습니다.

   - ping, telnet 및 trace-route와 같이 컨피그레이션 명령 또는 모니터링이 아닌 명령.
   - 비동기 출력이 있는 명령(예: accelerator 관련 CLI 명령).
   - CLI 명령의 응답은 처음 1000개의 행으로 제한됩니다.

2. Radware의 SNMP MIB를 미러링하는 SOAP 명령을 통해 디바이스 구성 및 모니터링. 다음 유형의 명령을 사용할 수 있습니다.
   - 스칼라 MIB 매개변수의 경우, 값을 검색(가져오기)하고 값을 변경(설정)합니다.
   - MIB 테이블 항목의 경우, 항목을 생성하고 항목을 삭제하며 항목의 매개변수를 하나 이상 업데이트하고, 항목을 검색(가져오기)하며, 전체 테이블을 검색(가져오기)하고 테이블을 단계별로 확인(첫 번째 항목을 가져온 후 다음 항목 가져오기)합니다.

DefensePro 웹 서비스는 일반 웹 브라우저와 같이 HTTP 또는 HTTPS 요청을 통해 작동합니다. 웹 서비스는 기본적으로 DefensePro에서는 사용하지 않습니다.

다음을 사용하여 DefensePro 웹 서비스를 사용하도록 설정할 수 있습니다.

- CLI—웹 서비스 상태 관리
- WBM—웹 서비스 창(서비스 > 웹 > *웹 서비스* 창)
- APSolute Vision—*설정* 창의 *액세스* 탭

디바이스에서 웹 또는 보안 웹 관리 인터페이스가 사용되는 경우에만 웹 서비스를 사용할 수 있습니다.

APSolute API SDK(Software Development Kit)

APSolute API SDK에는 커스텀 개발 애플리케이션에서 제어 및 모니터링 기능을 신속하게 개발하는 데 사용할 수 있는 필수 구성 요소와 문서가 모두 제공됩니다. 여기에는 다음이 포함됩니다.

- 모든 인터페이스와 모듈의 WSDL(Web Service Description Language)
- API 참조
- 제품 개요
- 일부 기본 디바이스 컨피그레이션/모니터링 기능의 샘플 코드

APSolute API SDK에 대한 작업을 시작하기 위해 SOAP 클라이언트 툴킷(SOAP 버전 1.1 이상 지원)과 워크스테이션의 툴킷용 개발 환경을 설치합니다.

부록 A – 사용 공간 바이패스 필드 및 값

이 부록에서는 BDoS 보호 및 DNS 보호의 ***footprint bypass(사용 공간 바이패스)*** 필드에 대해 설명하고 다음과 같은 기본 절이 포함되어 있습니다.

- BDoS 사용 공간 바이패스 필드 및 값, 204페이지
- DNS 사용 공간 바이패스 필드 및 값, 210페이지

BDoS 사용 공간 바이패스 필드 및 값

이 절에는 다음 표가 포함되어 있습니다.

- UDP, ICMP 및 IGMP 컨트롤러의 BDoS 사용 공간 바이패스 필드 및 값, 204페이지
- 모든 TCP 컨트롤러의 BDoS 사용 공간 바이패스 필드 및 값, 206페이지

자세한 내용은 BDoS 사용 공간 바이패스 구성, 106페이지를 참조하십시오.

표 168: UDP, ICMP 및 IGMP 컨트롤러의 BDoS 사용 공간 바이패스 필드 및 값

컨트롤러	필드	기본 상태	기본값 또는 “N/A”[1]	설명
UDP ICMP IGMP	체크섬	Accept	UDP의 경우: 0 ICMP 및 IGMP의 경우: N/A	패킷의 UDP 헤더에 있는 체크섬 값입니다.
UDP ICMP IGMP	id-num	Accept	UDP의 경우: 0 ICMP 및 IGMP의 경우: N/A	IP 패킷 헤더의 ID 번호입니다.
UDP ICMP IGMP	id-num-ipv6	Accept	UDP의 경우: 0 ICMP 및 IGMP의 경우: N/A	IPv6 패킷 헤더의 ID 번호입니다.
UDP ICMP IGMP	dns-id-num	Accept	UDP의 경우: 0 ICMP 및 IGMP의 경우: N/A	DNS 쿼리의 ID 번호입니다.
UDP	dns-qname	Accept	해당 없음	DNS 쿼리에서 요청한 도메인 이름입니다.
UDP	dns-qcount	Accept	1	단일 DNS 세션의 DNS 쿼리 수입니다.
UDP	source-port	Accept	해당 없음	공격의 소스 포트입니다.
UDP ICMP IGMP	frag-offset	Accept	0,185	데이터그램에서 이 프래그먼트가 속한 위치를 표시합니다. 프래그먼트 옵셋은 8바이트(64비트) 단위로 측정됩니다.

표 168: UDP, ICMP 및 IGMP 컨트롤러의 BDoS 사용 공간 바이패스 필드 및 값(계속)

컨트롤러	필드	기본 상태	기본값 또는 “N/A”[1]	설명
UDP ICMP	frag-offset-ipv6	Accept	0,181	데이터그램에서 이 IPv6 프래그먼트가 속한 위치를 표시합니다. IPv6 프래그먼트 옵셋은 8바이트(64비트) 단위로 측정됩니다.
UDP ICMP	flow-label	Accept	0,181	IPv6 라우터에서 특별히 처리되도록 요청하는 제품의 라벨을 지정하기 위해 소스에서 사용합니다. 플로우는 소스 주소와 0이 아닌 플로우 라벨을 조합하여 고유하게 식별합니다.
UDP ICMP IGMP	source-ip	Accept	해당 없음	공격의 소스 IP 주소입니다.
UDP ICMP	source-ip-ipv6	Accept	해당 없음	공격의 소스 IPv6 주소입니다.
UDP ICMP IGMP	tos	Accept	해당 없음	IP 패킷 헤더의 서비스 값 유형입니다.
UDP ICMP IGMP	packet-size	Accept	UDP 및 IGMP의 경우: N/A ICMP의 경우: 74	데이터 링크 헤더를 포함하는 패킷의 크기(바이트)입니다.
UDP ICMP	packet-size-ipv6	Accept	UDP의 경우: N/A ICMP의 경우: 118	데이터 링크 헤더를 포함하는 IPv6 패킷의 크기(바이트)입니다.
UDP	destination-port	Accept	해당 없음	패킷 헤더의 대상 포트입니다.
UDP ICMP IGMP	destination-ip	Accept	해당 없음	대상 IP 주소입니다.
UDP ICMP	destination-ip-ipv6	Accept	해당 없음	대상 IPv6 주소입니다.

표 168: UDP, ICMP 및 IGMP 컨트롤러의 BDoS 사용 공간 바이패스 필드 및 값(계속)

컨트롤러	필드	기본 상태	기본값 또는 “N/A”[1]	설명
UDP ICMP IGMP	fragment	Accept	해당 없음	프로토콜 프레그먼트 패킷입니다.
UDP ICMP IGMP	ttl	Accept	해당 없음	IP 패킷 헤더의 TTL(Time-To-Live) 값.
UDP ICMP IGMP	vlan-tag	Accept	해당 없음	VLAN 태그 값(외부).
ICMP IGMP	icmp-igmp-message-type	Accept	해당 없음	프로토콜 메시지 유형 값입니다.
ICMP	icmp-message-type-ipv6	Accept	해당 없음	ICMP IPv6 메시지 유형 값입니다.

1 – N/A”(즉, “해당 없음”)는 필드에서 특정 값을 사용할 수 없음을 나타냅니다. 일반 상태인 **Accept(수락)** 또는 **바이패스**만 적용됩니다.

표 169: 모든 TCP 컨트롤러의 BDoS 사용 공간 바이패스 필드 및 값

컨트롤러	필드	기본 상태	기본값 또는 “N/A”[1]	설명
TCP-SYN TCP-RST TCP-ACK-FIN TCP-SYN-ACK TCP-Frag	sequence-num	Accept	해당 없음	관련 TCP 패킷 헤더의 시퀀스 번호 값.

표 169: 모든 TCP 컨트롤러의 BDoS 사용 공간 바이패스 필드 및 값(계속)

컨트롤러	필드	기본 상태	기본값 또는 “N/A”[1]	설명
TCP-SYN TCP-RST TCP-ACK-FIN TCP-SYN-ACK TCP-Frag	id-num	Accept	해당 없음	IP 패킷 헤더의 ID 번호입니다.
TCP-SYN TCP-RST TCP-ACK-FIN TCP-SYN-ACK TCP-Frag	source-port	Accept	해당 없음	생성된 공격의 소스 포트입니다.
TCP-SYN TCP-RST TCP-ACK-FIN TCP-SYN-ACK TCP-Frag	source-ip	바이패스		생성된 공격의 소스 IP 주소입니다.
TCP-SYN TCP-RST TCP-ACK-FIN TCP-SYN-ACK TCP-Frag	source-ip-ipv6	바이패스		생성된 공격의 소스 IPv6 주소입니다.
TCP-SYN TCP-RST TCP-ACK-FIN TCP-SYN-ACK TCP-Frag	tos	Accept		IP 패킷 헤더의 서비스 값 유형입니다.

표 169: 모든 TCP 컨트롤러의 BDoS 사용 공간 바이패스 필드 및 값(계속)

컨트롤러	필드	기본 상태	기본값 또는 “N/A” [1]	설명
TCP-SYN TCP-RST TCP-ACK-FIN TCP-SYN-ACK TCP-Frag	packet-size	Accept	TCP-SYN, TCP-SYN- ACK의 경우: 60, 62, 66, 74 TCP-RST, TCP-ACK- FIN의 경우: 60 TCP-Frag의 경우: N/A	데이터 링크 헤더를 포함하는 패킷의 크기(바이트)입니다.
TCP-SYN TCP-RST TCP-ACK-FIN TCP-SYN-ACK TCP-Frag	packet-size-ipv6	Accept	TCP-SYN, TCP-SYN- ACK의 경우: 80, 82, 86, 94 TCP-RST, TCP-ACK- FIN의 경우: 74 TCP-Frag의 경우: N/A	데이터 링크 헤더를 포함하는 IPv6 패킷의 크기(바이트)입니다.
TCP-SYN TCP-RST TCP-ACK-FIN TCP-SYN-ACK TCP-Frag	destination-port	Accept		공격의 대상 TCP 포트입니다.
TCP-SYN TCP-RST TCP-ACK-FIN TCP-SYN-ACK TCP-Frag	destination-ip	Accept		공격의 대상 IP 주소입니다.
TCP-SYN TCP-RST TCP-ACK-FIN TCP-SYN-ACK TCP-Frag	destination-ip-ipv6	Accept		공격의 대상 IPv6 주소입니다.

표 169: 모든 TCP 컨트롤러의 BDoS 사용 공간 바이패스 필드 및 값(계속)

컨트롤러	필드	기본 상태	기본값 또는 “N/A”[1]	설명
TCP-SYN TCP-RST TCP-ACK-FIN TCP-SYN-ACK TCP-Frag	ttl	Accept		IP 패킷 헤더의 TTL(Time-To-Live) 값.
TCP-SYN TCP-RST TCP-ACK-FIN TCP-SYN-ACK TCP-Frag	vlan-tag	Accept		VLAN 태그 값(외부).
TCP-FRAG	frag-offset	Accept	0, 185	데이터그램에서 이 프래그먼트가 속한 위치를 표시합니다. 프래그먼트 옵셋은 8바이트(64비트) 단위로 측정됩니다.
TCP-FRAG	frag-offset-ipv6	Accept	0, 181	데이터그램에서 이 IPv6 프래그먼트가 속한 위치를 표시합니다. IPv6 프래그먼트 옵셋은 8바이트(64비트) 단위로 측정됩니다.
TCP-SYN TCP-RST TCP-ACK-FIN TCP-SYN-ACK TCP-Frag	flow-label	Accept	0	IPv6 라우터에서 특별히 처리되도록 요청하는 제품의 라벨을 지정하기 위해 소스에서 사용합니다. 플로우는 소스 주소와 0이 아닌 플로우 라벨을 조합하여 고유하게 식별합니다.

1 – “N/A”(즉, “해당 없음”)는 필드에서 특정 값을 사용할 수 없음을 나타냅니다. 일반 상태인 **Accept(수락)** 또는 **바이패스**만 적용됩니다.

DNS 사용 공간 바이패스 필드 및 값

DNS 사용 공간 바이패스 유형은 모두 동일한 필드, 기본 상태 및 기본값을 지원하는 다음 컨트롤러와 연관됩니다.

- A
- AAAA
- MX
- NAPTR
- 기타
- PTR
- SOA2
- SRV
- 텍스트

표 170: DNS 사용 공간 바이패스 필드 및 값

필드	기본 상태	기본값 또는 "N/A"[1]	설명
checksum	Accept	UDP의 경우: 0 ICMP 및 IGMP의 경우: N/A	패킷의 UDP 헤더에 있는 체크섬 값입니다.
id-num	Accept	UDP의 경우: 0 ICMP 및 IGMP의 경우: N/A	IP 패킷 헤더의 ID 번호입니다.
id-num-ipv6	Accept	UDP의 경우: 0 ICMP 및 IGMP의 경우: N/A	IPv6 패킷 헤더의 ID 번호입니다.
dns-id-num	Accept	UDP의 경우: 0 ICMP 및 IGMP의 경우: N/A	DNS 쿼리의 ID 번호입니다.
dns-qname	Accept	해당 없음	DNS 쿼리에서 요청한 도메인 이름입니다.
dns-qcount	Accept	1	단일 DNS 세션의 DNS 쿼리 수입니다.
source-port	Accept	해당 없음	공격의 소스 포트입니다.
flow-label	Accept	0,181	IPv6 라우터에서 특별히 처리되도록 요청하는 제품의 라벨을 지정하기 위해 소스에서 사용합니다. 플로우는 소스 주소와 0이 아닌 플로우 라벨을 조합하여 고유하게 식별합니다.

표 170: DNS 사용 공간 바이패스 필드 및 값(계속)

필드	기본 상태	기본값 또는 “N/A”[1]	설명
source-ip	Accept	해당 없음	공격의 소스 IP 주소입니다.
source-ip-ipv6	Accept	해당 없음	공격의 소스 IPv6 주소입니다.
tos	Accept	해당 없음	IP 패킷 헤더의 서비스 값 유형입니다.
packet-size	Accept	UDP 및 IGMP의 경우: N/A ICMP의 경우: 74	데이터 링크 헤더를 포함하는 패킷의 크기(바이트)입니다.
packet-size-ipv6	Accept	UDP의 경우: N/A ICMP의 경우: 118	데이터 링크 헤더를 포함하는 IPv6 패킷의 크기(바이트)입니다.
destination-ip	Accept	해당 없음	대상 IP 주소입니다.
destination-ip-ipv6	Accept	해당 없음	대상 IPv6 주소입니다.
fragment	Accept	해당 없음	프로토콜 프레그먼트 패킷입니다.
ttl	Accept	해당 없음	IP 패킷 헤더의 TTL(Time-To-Live) 값.
vlan-tag	Accept	해당 없음	VLAN 태그 값(외부).
dns-ancount	Accept	0	단일 DNS 세션의 DNS 응답 수입니다.
flags	Accept	해당 없음	DNS 헤더 플래그 필드(AA, TC, RD 등).

1 – N/A”(즉, “해당 없음”)는 필드에서 특정 값을 사용할 수 없음을 나타냅니다. 일반 상태인 **Accept(수락)** 또는 **바이패스**만 적용됩니다.

부록 B – 미리 정의된 기본 필터

목록은 제품 버전에 따라 달라집니다.

표 171: 미리 정의된 기본 필터

이름	설명	프로토콜	OMPC Offset (OMPC 옵셋)	OMPC Mask (OMPC 마스크)
000	루틴	IP	1	e0000000
001	우선순위	IP	1	e0000000
010	즉시	IP	1	e0000000
011	플래시	IP	1	e0000000
100	ToS 플래시 재정의	IP	1	e0000000
101	CRITIC/ECP	IP	1	e0000000
110	인터네트워크 제어	IP	1	e0000000
111	네트워크 제어	IP	1	e0000000
aim-aol-any	AIM/AOL 인스턴트 메신저	TCP	0	ffff0000
aol-msg	AOL 인스턴트	TCP	0	0
ares_ft_udp_0	Ares_FT_udp	UDP	36	ffffffff
ares_ft_udp_1	Ares_FT_udp	UDP	40	ff000000
bearshare_download_tcp_0	BearShare_Download_tcp	TCP	0	ffffffff
bearshare_download_tcp_1	BearShare_Download_tcp	TCP	4	ffffffff
bearshare_request_file_udp_0	BearShare_Request_File_udp	UDP	0	ffffffff
bearshare_request_file_udp_1	BearShare_Request_File_udp	UDP	4	00ffffff
bittorrent_command_1_0	BitTorrent	TCP	0	ffffffff
bittorrent_command_1_1	BitTorrent	TCP	4	ffffffff
bittorrent_command_1_2	BitTorrent	TCP	8	ffffffff
bittorrent_command_1_3	BitTorrent	TCP	12	ffffffff
bittorrent_command_1_4	BitTorrent	TCP	16	ffffffff
bittorrent_command_2_0	BitTorrent	TCP	0	ffffffff
bittorrent_command_2_1	BitTorrent	TCP	4	ffffffff
bittorrent_command_2_2	BitTorrent	TCP	8	ffffffff
bittorrent_command_2_3	BitTorrent	TCP	12	ffffffff

표 171: 미리 정의된 기본 필터(계속)

이름	설명	프로토콜	OMPC Offset (OMPC 옵셋)	OMPC Mask (OMPC 마스크)
bittorrent_command_2_4	BitTorrent	TCP	16	ffffffff
bittorrent_command_2_5	BitTorrent	TCP	20	ffffffff
bittorrent_command_3_0	BitTorrent	TCP	0	ffffffff
bittorrent_command_3_1	BitTorrent	TCP	4	ffffffff
bittorrent_command_3_2	BitTorrent	TCP	8	ffffffff
bittorrent_command_3_3	BitTorrent	TCP	12	ffffffff
bittorrent_command_3_4	BitTorrent	TCP	16	ffffffff
bittorrent_command_3_5	BitTorrent	TCP	20	ffff0000
bittorrent_command_4_0	BitTorrent	TCP	8	ffffff00
bittorrent_command_4_1	BitTorrent	TCP	11	ff000000
bittorrent_command_4_2	BitTorrent	TCP	11	ff000000
bittorrent_udp_1_0	BitTorrent_UDP_1	UDP	8	ffffff00
bittorrent_udp_1_1	BitTorrent_UDP_1	UDP	12	ffff0000
citrix-admin	Citrix 관리자	TCP	0	0
citrix-ica	Citrix ICA	TCP	0	0
citrix-ima	Citrix IMA	TCP	0	0
citrix-ma-client	Citrix MA 클라이언트	TCP	0	0
citrix-rtmp	Citrix RTMP	TCP	0	0
diameter	배율	TCP	0	0
directconnect_file_transfer_0	DirectConnect_File_transfer	TCP	0	ff000000
directconnect_file_transfer_1	DirectConnect_File_transfer	TCP	21	ffffffff
directconnect_file_transfer_2	DirectConnect_File_transfer	TCP	25	ffffffff
dns	DNS 세션	UDP	0	0
emule_tcp_file_request_0	eMule	TCP	0	ff000000
emule_tcp_file_request_1	eMule	TCP	4	ffff0000
emule_tcp_hello_message_0	eMule	TCP	0	ff000000

표 171: 미리 정의된 기본 필터(계속)

이름	설명	프로토콜	OMPC Offset (OMPC 옵셋)	OMPC Mask (OMPC 마스크)
emule_tcp_hello_message_1	eMule	TCP	4	ffff0000
emule_tcp_secure_handshake_0	eMule	TCP	0	ff000000
emule_tcp_secure_handshake_1	eMule	TCP	4	ffff0000
ftp-session	FTP 세션	TCP	0	0
gnutella_tcp_1_0	Gnutella_TCP_1	TCP	0	ffffff00
gnutella_tcp_2_0	Gnutella_TCP_2	TCP	0	ffffffff
gnutella_tcp_2_1	Gnutella_TCP_2	TCP	4	ffffffff
gnutella_tcp_3_0	Gnutella_TCP_3	TCP	0	ffffff00
googletalk_ft_1_0	GoogleTalk_FT_1	UDP	24	ffffffff
googletalk_ft_1_1	GoogleTalk_FT_1	UDP	28	ffffffff
googletalk_ft_1_2	GoogleTalk_FT_1	UDP	32	ffffffff
googletalk_ft_1_3	GoogleTalk_FT_1	UDP	36	ffff0000
googletalk_ft_2_0	GoogleTalk_FT_2	UDP	24	ffffffff
googletalk_ft_2_1	GoogleTalk_FT_2	UDP	28	ffffffff
googletalk_ft_4_0	GoogleTalk_FT_4	UDP	67	ffffffff
googletalk_ft_4_1	GoogleTalk_FT_4	UDP	71	ffffffff
groove_command_1_0	Groove	TCP	6	ffffffff
groove_command_1_1	Groove	TCP	10	ffffffff
groove_command_1_2	Groove	TCP	14	ffffffff
groove_command_2_0	Groove	TCP	6	ffffffff
groove_command_2_1	Groove	TCP	10	ffff0000
groove_command_3_0	Groove	TCP	7	ffffffff
groove_command_3_1	Groove	TCP	11	ffffffff
groove_command_3_2	Groove	TCP	15	ffffffff
groove_command_3_3	Groove	TCP	19	ffffffff
h.225-session	H225 세션	TCP	0	0

표 171: 미리 정의된 기본 필터(계속)

이름	설명	프로토콜	OMPC Offset (OMPC 옵셋)	OMPC Mask (OMPC 마스크)
hdc1	높은 삭제 클래스 1	IP	1	fc000000
hdc2	높은 삭제 클래스 2	IP	1	fc000000
hdc3	높은 삭제 클래스 3	IP	1	fc000000
hdc4	높은 삭제 클래스 4	IP	1	fc000000
HTTP	World Wide Web HTTP	TCP	0	0
http-alt	HTTP 대체	TCP	0	0
https	HTTP over SSL	TCP	0	0
icecast_1	IceCast_Stream	TCP	0	ffffffff
icecast_2	IceCast_Stream	TCP	4	ffffffff
icecast_3	IceCast_Stream	TCP	8	ffff0000
icmp	ICMP	ICMP	0	0
icq	ICQ	TCP	0	0
icq_aol_ft_0	ICQ_AOL_FT	TCP	0	ffffffff
icq_aol_ft_1	ICQ_AOL_FT	TCP	0	ffffffff
icq_aol_ft_2	ICQ_AOL_FT	TCP	2	ffff0000
imap	인터넷 메시지 액세스	TCP	0	0
imesh_download_tcp_0	iMesh_Download_tcp	TCP	0	ffffffff
imesh_download_tcp_1	iMesh_Download_tcp	TCP	4	ffffffff
imesh_request_file_udp_0	iMesh_Request_File_udp	UDP	0	ffffffff
imesh_request_file_udp_1	iMesh_Request_File_udp	UDP	4	00ffffff
ip	IP 트래픽	IP	0	0
itunesdaap_ft_0	iTunesDaap_FT	TCP	0	ffffffff
itunesdaap_ft_1	iTunesDaap_FT	TCP	4	ffffffff
itunesdaap_ft_2	iTunesDaap_FT	TCP	8	ffffff00
itunesdaap_ft_3	iTunesDaap_FT	TCP	2	ffff0000
kazaa_request_file_0	Kazaa_Request_File	TCP	0	ffffffff

표 171: 미리 정의된 기본 필터(계속)

이름	설명	프로토콜	OMPC Offset (OMPC 옵셋)	OMPC Mask (OMPC 마스크)
kazaa_request_file_1	Kazaa_Request_File	TCP	4	ffffffff
kazaa_request_file_2	Kazaa_Request_File	TCP	8	ffff0000
kazaa_udp_packet_0	Kazaa_UDP_Packet	UDP	6	ffffffff
kazaa_udp_packet_1	Kazaa_UDP_Packet	UDP	4	ffff0000
ldap	LDAP	TCP	0	0
ldaps	LDAPS	TCP	0	0
ldc1	낮은 삭제 클래스 1	IP	1	fc000000
ldc2	낮은 삭제 클래스 2	IP	1	fc000000
ldc3	낮은 삭제 클래스 3	IP	1	fc000000
ldc4	낮은 삭제 클래스 4	IP	1	fc000000
lrp	로드 보고서 프로토콜	UDP	0	0
manolito_file_transfer_0_0	Manolito	TCP	0	ffffffff
manolito_file_transfer_0_1	Manolito	TCP	0	ffffffff
manolito_file_transfer_0_2	Manolito	TCP	0	ffffffff
manolito_file_transfer_1_0	Manolito	TCP	4	ff000000
manolito_file_transfer_1_1	Manolito	TCP	4	ff000000
manolito_file_transfer_2_0	Manolito	TCP	4	ff000000
manolito_file_transfer_2_1	Manolito	TCP	4	ff000000
mdc1	중간 삭제 클래스 1	IP	1	fc000000
mdc2	중간 삭제 클래스 2	IP	1	fc000000
mdc3	중간 삭제 클래스 3	IP	1	fc000000
mdc4	중간 삭제 클래스 4	IP	1	fc000000
meebo_get_0	MEEBO_GET	TCP	0	ffffffff
meebo_get_1	MEEBO_GET	TCP	4	ffffffff
meebo_get_2	MEEBO_GET	TCP	8	ffffffff
meebo_get_3	MEEBO_GET	TCP	12	ffffffff

표 171: 미리 정의된 기본 필터(계속)

이름	설명	프로토콜	OMPC Offset (OMPC 옵셋)	OMPC Mask (OMPC 마스크)
meebo_get_4	MEEBO_GET	TCP	16	ffffffff
meebo_get_5	MEEBO_GET	TCP	20	ffffffff
meebo_get_6	MEEBO_GET	TCP	24	ffffffff
meebo_get_7	MEEBO_GET	TCP	28	ffffffff
meebo_get_8	MEEBO_GET	TCP	32	ff000000
meebo_post_0	MEEBO_POST	TCP	0	ffffffff
meebo_post_1	MEEBO_POST	TCP	4	ffffffff
meebo_post_2	MEEBO_POST	TCP	8	ffffffff
meebo_post_3	MEEBO_POST	TCP	12	ffffffff
meebo_post_4	MEEBO_POST	TCP	16	ffffffff
meebo_post_5	MEEBO_POST	TCP	20	ffffffff
meebo_post_6	MEEBO_POST	TCP	24	ffffffff
meebo_post_7	MEEBO_POST	TCP	28	ffffff00
msn-any	MSN 메신저 채팅	TCP	0	ffffffff
msn-msg	MSN 메신저 채팅	TCP	0	0
msn_msgr_ft_0	MSN_MSGR_FT	TCP	0	ffffffff
msn_msgr_ft_1	MSN_MSGR_FT	TCP	48	ffffffff
mssql-monitor	Microsoft SQL traffic-monitor	TCP	0	0
mssql-server	Microsoft SQL Server 트래픽	TCP	0	0
nntp	네트워크 뉴스	TCP	0	0
nonip	비IP 트래픽	NonIP	0	0
oracle-server1	Oracle 서버	TCP	0	0
oracle-server2	Oracle 서버	TCP	0	0
oracle-server3	Oracle 서버	TCP	0	0
oracle-v1	Oracle SQL *Net 버전 1	TCP	0	0
oracle-v2	Oracle SQL *Net 버전 2	TCP	0	0

표 171: 미리 정의된 기본 필터(계속)

이름	설명	프로토콜	OMPC Offset (OMPC 옵셋)	OMPC Mask (OMPC 마스크)
POP3	포스트 오피스 프로토콜 3	TCP	0	0
prp	PRP	UDP	0	0
radius	RADIUS 프로토콜	TCP	0	0
rexec	원격 프로세스 실행	TCP	0	0
rshell	원격 쉘	TCP	0	0
rtp_ft_0	RTP_FT	UDP	0	ffff0000
rtp_ft_1	RTP_FT	UDP	0	ffff0000
rtp_ft_2	RTP_FT	UDP	16	ffff0000
rtsp	RTSP	TCP	0	0
sap	SAP	TCP	0	0
sctp	SCTP 트래픽	SCTP	0	0
skype-443-handshake	포트 443의 Skype 시그니처	TCP	0	ff000000
skype-443-s-hello	포트 443의 Skype 시그니처	TCP	11	ffffffff
skype-80-l-56	포트 80의 Skype 시그니처	TCP	2	ffff0000
skype-80-proxy	포트 80의 Skype 시그니처	TCP	0	ffffffff
skype-80-pshack	포트 80의 Skype 시그니처	TCP	13	ff000000
skype-ext-l-54	Skype 시그니처	TCP	2	ffff0000
skype-ext-pshack	Skype 시그니처	TCP	13	ff000000
smtp	Simple Mail Transfer	TCP	0	0
snmp	SNMP	UDP	0	0
snmp-trap	SNMP 트랩	UDP	0	0
softethervpn443	SoftEther 이더넷 시스템	TCP	0	ffffff00
softethervpn8888	SoftEther 이더넷 시스템	TCP	0	ffffff00
soulseek_pierce_fw_0	SoulSeek_Pierce_FW	TCP	0	ffffffff
soulseek_pierce_fw_1	SoulSeek_Pierce_FW	TCP	4	ff000000
soulseek_pierce_fw_2	SoulSeek_Pierce_FW	TCP	2	ffff0000

표 171: 미리 정의된 기본 필터(계속)

이름	설명	프로토콜	OMPC Offset (OMPC 옵셋)	OMPC Mask (OMPC 마스크)
ssh	SSH(Secure Shell)	TCP	0	0
tcp	TCP 트래픽	TCP	0	0
telnet	텔넷	TCP	0	0
tftp	Trivial File Transfer	UDP	0	0
udp	UDP 트래픽	UDP	0	0
voip_sign_1	VOIP 시그니처	UDP	28	c03f0000
voip_sign_10	VOIP 시그니처	UDP	28	c03f0000
voip_sign_11	VOIP 시그니처	UDP	28	c03f0000
voip_sign_12	VOIP 시그니처	UDP	28	c03f0000
voip_sign_13	VOIP 시그니처	UDP	28	c03f0000
voip_sign_2	VOIP 시그니처	UDP	28	c03f0000
voip_sign_3	VOIP 시그니처	UDP	28	c03f0000
voip_sign_4	VOIP 시그니처	UDP	28	c03f0000
voip_sign_5	VOIP 시그니처	UDP	28	c03f0000
voip_sign_6	VOIP 시그니처	UDP	28	c03f0000
voip_sign_7	VOIP 시그니처	UDP	28	c03f0000
voip_sign_8	VOIP 시그니처	UDP	28	c03f0000
voip_sign_9	VOIP 시그니처	UDP	28	c03f0000
yahoo_ft_0	YAHOO_FT	TCP	0	ffffffff
yahoo_ft_1	YAHOO_FT	TCP	10	ffff0000
yahoo_get_0	YAHOO_GET	TCP	0	ffffffff
yahoo_get_1	YAHOO_GET	TCP	4	ffffffff
yahoo_get_2	YAHOO_GET	TCP	8	ffffffff
yahoo_get_3	YAHOO_GET	TCP	12	ffffffff
yahoo_get_4	YAHOO_GET	TCP	16	ff000000
yahoo_post_0	YAHOO_POST	TCP	0	ffffffff

표 171: 미리 정의된 기본 필터(계속)

이름	설명	프로토콜	OMPC Offset (OMPC 옵셋)	OMPC Mask (OMPC 마스크)
yahoo_post_1	YAHOO_POST	TCP	4	ffffffff
yahoo_post_2	YAHOO_POST	TCP	8	ffffffff
yahoo_post_3	YAHOO_POST	TCP	12	ffffffff
yahoo_post_4	YAHOO_POST	TCP	16	ffff0000

부록 C – DefensePro 공격 보호 ID

이 부록에서는 DefensePro 공격 보호 ID에 대해 설명합니다.

참고: 이 릴리스에서는 다음 표에 나열된 일부 보호는 지원하지 않습니다.

표 172: DefensePro 공격 보호 ID

ID 번호 또는 범위	공격 보호 이름	카테고리 (보고용)	기본 위험	기본 조치	보고 조치	설명
8	White List	해당 없음				허용 목록 발생은 보안 이벤트로 보고되지 않습니다.
9	차단 목록	액세스				차단 목록 액세스 위반입니다.
70	네트워크 플러드 IPv4 UDP	동작 기반 DoS				네트워크 플러드 IPv4 UDP입니다.
71	네트워크 플러드 IPv4 ICMP	동작 기반 DoS				네트워크 플러드 IPv4 ICMP입니다.
72	네트워크 플러드 IPv4 IGMP	동작 기반 DoS				네트워크 플러드 IPv4 IGMP입니다.
73	네트워크 플러드 IPv4 TCP-SYN	동작 기반 DoS				SYN 플래그가 있는 네트워크 플러드 IPv4 TCP입니다.
74	네트워크 플러드 IPv4 TCP-RST	동작 기반 DoS				RST 플래그가 있는 네트워크 플러드 IPv4 TCP입니다.
75	네트워크 플러드 IPv4 TCP-ACK	동작 기반 DoS				ACK 플래그가 있는 네트워크 플러드 IPv4 TCP입니다.
76	네트워크 플러드 IPv4 TCP-PSH	동작 기반 DoS				PSH 플래그가 있는 네트워크 플러드 IPv4 TCP입니다.
77	네트워크 플러드 IPv4 TCP-FIN	동작 기반 DoS				FIN 플래그가 있는 네트워크 플러드 IPv4 TCP입니다.
78	네트워크 플러드 IPv4 TCP-SYN-ACK	동작 기반 DoS				SYN 및 ACK 플래그가 있는 네트워크 플러드 IPv4 TCP입니다.
79	네트워크 플러드 IPv4 TCP-FRAG	동작 기반 DoS				FRAG 플래그가 있는 네트워크 플러드 IPv4 TCP입니다.
80	네트워크 플러드 IPv6 UDP	동작 기반 DoS				네트워크 플러드 IPv6 UDP입니다.
81	네트워크 플러드 IPv6 ICMP	동작 기반 DoS				네트워크 플러드 IPv6 ICMP입니다.
82	네트워크 플러드 IPv6 IGMP	동작 기반 DoS				네트워크 플러드 IPv6 IGMP입니다.
83	네트워크 플러드 IPv6 TCP-SYN	동작 기반 DoS				SYN 플래그가 있는 네트워크 플러드 IPv6 TCP입니다.
84	네트워크 플러드 IPv6 TCP-RST	동작 기반 DoS				RST 플래그가 있는 네트워크 플러드 IPv6 TCP입니다.

표 172: DefensePro 공격 보호 ID(계속)

ID 번호 또는 범위	공격 보호 이름	카테고리 (보고용)	기본 위험	기본 작업	보고 조치	설명
85	네트워크 플러드 IPv6 TCP-ACK	동작 기반 DoS				ACK 플래그가 있는 네트워크 플러드 IPv6 TCP입니다.
86	네트워크 플러드 IPv6 TCP-PSH	동작 기반 DoS				PSH 플래그가 있는 네트워크 플러드 IPv6 TCP입니다.
87	네트워크 플러드 IPv6 TCP-FIN	동작 기반 DoS				FIN 플래그가 있는 네트워크 플러드 IPv6 TCP입니다.
88	네트워크 플러드 IPv6 TCP-SYN-ACK	동작 기반 DoS				SYN 및 ACK 플래그가 있는 네트워크 플러드 IPv6 TCP입니다.
89	네트워크 플러드 IPv6 TCP-FRAG	동작 기반 DoS				FRAG 플래그가 있는 네트워크 플러드 IPv6 TCP입니다.
100	인식되지 않은 L2 형식	이상 징후	Low	보고하지 않음	프로세스	인식되지 않는 L2 형식입니다.
103	잘못된 IPv4 체크섬	이상 징후	Low	Block	바이패스	잘못된 IPv4 체크섬입니다.
104	유효하지 않은 IPv4 헤더 또는 총 길이	이상 징후	Low	Block	바이패스	올바르지 않은 IPv4 헤더 또는 총 길이입니다.
105	TTL Less Than or Equal to 1(TTL이 1 이하)	이상 징후	Low	보고서	프로세스	TTL이 1 이하
107	Inconsistent IPv6 Headers(일치하지 않는 IPv6 헤더)	이상 징후	Low	Block	바이패스	일치하지 않는 IPv6 헤더입니다.
108	IPv6 Hop Limit Reached(IPv6 홉 제한 도달)	이상 징후	Low	보고서	프로세스	IPv6 홉 제한에 도달했습니다.
110	Unsupported L4 Protocol(지원되지 않는 L4 프로토콜)	이상 징후	Low	보고하지 않음	프로세스	지원되지 않는 L4 프로토콜입니다.
112	올바르지 않은 TCP 헤더 길이	이상 징후				(이 이상 징후 보호는 DefensePro 5.11 및 5.12에서만 사용할 수 있습니다.) 올바르지 않은 TCP 헤더 길이입니다.
113	Invalid TCP Flags(올바르지 않은 TCP 플래그)	이상 징후	Low	Block	바이패스	올바르지 않은 TCP 플래그입니다.
116	올바르지 않은 UDP 헤더 길이	이상 징후				올바르지 않은 UDP 헤더 길이입니다.
119	로컬 호스트와 동일한 소스 또는 대상 주소	이상 징후	Low	Block	바이패스	로컬 호스트와 동일한 소스 또는 대상 IP 주소입니다.

표 172: DefensePro 공격 보호 ID(계속)

ID 번호 또는 범위	공격 보호 이름	카테고리 (보고용)	기본 위험	기본 작업	보고 조치	설명
120	대상 주소와 동일한 소스 주소(랜드 공격)	이상 징후	Low	Block	바이패스	대상 IP 주소와 동일한 소스 IP 주소(랜드 공격)입니다. 이 시그니처의 CVE(Common Vulnerability Enumerator)는 CVE-1999- 0016입니다.
125	L4 소스 또는 대상 포트 0	이상 징후	Low	Block	바이패스	레이어 4 소스 또는 대상 포트가 0입니다.
131	Invalid L4 Header Length(유효하지 않은 L4 헤더 길이)		Low	Block	바이패스	유효하지 않은 L4 헤더 길이
150	HTTP 페이지 플러드 공격	HttpFlood				HTTP 페이지 플러드 공격입니다.
240	TCP 상태 없음	DoS				TCP 상태 없음 플러드입니다.
350	SCAN_TCP_SCAN	스캔 방지				TCP 스캔을 시도합니다.
351	SCAN_UDP_SCAN	스캔 방지				UDP 스캔을 시도합니다.
352	SCAN_ICMP_SCAN	스캔 방지				ICMP 스캔을 시도합니다.
400	무작위 대입 웹					무작위 대입 웹 공격은 기본 HTTP 인증으로 보호되는 사이트의 제한된 영역을 침입하려는 시도입니다.
401	웹 스캔					웹 취약성 스캔은 일반적으로 스캔된 웹 서버에서 수행하는 침입 공격의 사전 작업으로 실행되는 정보 수집 공격입니다. 공격자가 여러 유형의 HTTP 요청을 전송하고 서버 응답을 분석하여 웹 서버에 대한 정보를 수집하려고 합니다. 이 경우 자동 툴이 자주 사용됩니다.

표 172: DefensePro 공격 보호 ID(계속)

ID 번호 또는 범위	공격 보호 이름	카테고리 (보고용)	기본 위험	기본 작업	보고 조치	설명
402	무작위 대입 SMTP					무작위 대입 SMTP 공격은 사용자 이름과 비밀번호 인증으로 보호되는 SMTP 메일 서버에서 제한된 계정에 침입하려는 시도입니다.
403	무작위 대입 FTP					무작위 대입 FTP 공격은 사용자 이름과 비밀번호 인증으로 보호되는 FTP 서버에서 제한된 계정에 침입하려는 시도입니다.
404	무작위 대입 POP3					무작위 대입 POP3 공격은 사용자 이름과 비밀번호 인증으로 보호되는 POP3 메일 서버에서 제한된 계정에 침입하려는 시도입니다.
405	무작위 대입 SIP(UDP)					무작위 대입 SIP(UDP) 공격은 사용자 이름과 비밀번호 인증으로 보호되는 SIP 서버에서 UDP를 통해 제한된 계정에 침입하려는 시도입니다. 이 유형의 공격은 SIP 서버에 등록 플러드도 초래할 수 있습니다.
406	무작위 대입 SIP(TCP)					무작위 대입 SIP(TCP) 공격은 사용자 이름과 비밀번호 인증으로 보호되는 SIP 서버에서 TCP를 통해 제한된 계정에 침입하려는 시도입니다. 이 유형의 공격은 SIP 서버에 등록 플러드도 초래할 수 있습니다.

표 172: DefensePro 공격 보호 ID(계속)

ID 번호 또는 범위	공격 보호 이름	카테고리 (보고용)	기본 위험	기본 작업	보고 조치	설명
407	무작위 대입 MySQL					무작위 대입 MySQL 공격은 사용자 이름과 비밀번호 인증으로 보호되는 MySQL 데이터베이스 서버에서 제한된 데이터베이스 계정에 침입하려는 시도입니다.
408	무작위 대입 MSSQL					무작위 대입 MSSQL 공격은 사용자 이름과 비밀번호 인증으로 보호되는 MSSQL 데이터베이스 서버에서 제한된 데이터베이스 계정에 침입하려는 시도입니다.
409	SIP 스캔(UDP)					SIP 스캔 공격에서는 취약성을 발견하거나 서버에서 기존 가입자 전화번호(SIP 사용자 또는 SIP URI라고도 함)를 채취하기 위해 SIP 서버를 식별하려고 합니다. 전화번호는 나중에 SPIT(SPAM over IP Telephony) 공격을 실행하는 데 사용할 수 있습니다.
410	SIP 스캔(TCP)					SIP 스캔 공격에서는 취약성을 발견하거나 서버에서 기존 가입자 전화번호(SIP 사용자 또는 SIP URI라고도 함)를 채취하기 위해 SIP 서버를 식별하려고 합니다. 전화번호는 나중에 SPIT(SPAM over IP Telephony) 공격을 실행하는 데 사용할 수 있습니다.

표 172: DefensePro 공격 보호 ID(계속)

ID 번호 또는 범위	공격 보호 이름	카테고리 (보고용)	기본 위험	기본 작업	보고 조치	설명
414	SIP 스캔 DST(TCP)					SIP 스캔 공격에서는 취약성을 발견하거나 서버에서 기존 가입자 전화번호(SIP 사용자 또는 SIP URI라고도 함)를 채취하기 위해 SIP 서버를 식별하려고 합니다. 전화번호는 나중에 SPIT(SPAM over IP Telephony) 공격을 실행하는 데 사용할 수 있습니다.
416	무작위 대입 SIP DST(TCP)					무작위 대입 SIP DST(TCP) 공격은 사용자 이름과 비밀번호 인증으로 보호되는 SIP 서버에서 TCP를 통해 제한된 계정에 침입하려는 시도입니다. 특정 공격은 서버에서 시작된 세션에서 발견한 오류 응답에서 탐지되었습니다. 이 유형의 공격은 SIP 서버에 등록 플러드도 초래할 수 있습니다.
417	무작위 대입 SMB					무작위 대입 SMB 공격은 사용자 이름과 비밀번호 인증으로 보호되는 SMB(파일 공유) 서버에서 제한된 계정에 침입하려는 시도입니다.
418	무작위 대입 SIP DST(UDP)					무작위 대입 SIP DST(UDP) 공격은 사용자 이름과 비밀번호 인증으로 보호되는 SIP 서버에서 UDP를 통해 제한된 계정에 침입하려는 시도입니다. 특정 공격은 서버에서 시작된 세션에서 발견한 오류 응답에서 탐지되었습니다. 이 유형의 공격은 SIP 서버에 등록 플러드도 초래할 수 있습니다.

표 172: DefensePro 공격 보호 ID(계속)

ID 번호 또는 범위	공격 보호 이름	카테고리 (보고용)	기본 위험	기본 작업	보고 조치	설명
419	SIP 스캔 DST(UDP)					SIP 스캔 공격에서는 취약성을 발견하거나 서버에서 기존 가입자 전화번호(SIP 사용자 또는 SIP URI라고도 함)를 채취하기 위해 SIP 서버를 식별하려고 합니다. 전화번호는 나중에 SPIT(SPAM over IP Telephony) 공격을 실행하는 데 사용할 수 있습니다.
450	DNS 플러드 IPv4 DNS-A	DNS 보호				IPv4를 통한 DNS A 쿼리 플러드입니다.
451	DNS 플러드 IPv4 DNS-MX	DNS 보호				IPv4를 통한 DNS MX 쿼리 플러드입니다.
452	DNS 플러드 IPv4 DNS-PTR	DNS 보호				IPv4를 통한 DNS PTR 쿼리 플러드입니다.
453	DNS 플러드 IPv4 DNS-AAAA	DNS 보호				IPv4를 통한 DNS AAAA 쿼리 플러드입니다.
454	DNS 플러드 IPv4 DNS-Text	DNS 보호				IPv4를 통한 DNS 텍스트 쿼리 플러드입니다.
455	DNS 플러드 IPv4 DNS-SOA	DNS 보호				IPv4를 통한 DNS SOA 쿼리 플러드입니다.
456	DNS 플러드 IPv4 DNS-NAPTR	DNS 보호				IPv4를 통한 DNS NAPTR 쿼리 플러드입니다.
457	DNS 플러드 IPv4 DNS-SRV	DNS 보호				IPv4를 통한 DNS SRV 쿼리 플러드입니다.
458	DNS 플러드 IPv4 DNS-Other	DNS 보호				IPv4를 통한 DNS 기타 쿼리 플러드입니다.
459	DNS 플러드 IPv4 DNS-ALL	DNS 보호				IPv4를 통한 DNS 쿼리 플러드입니다.
460	DNS 플러드 IPv6 DNS-A	DNS 보호				IPv6을 통한 DNS A 쿼리 플러드입니다.
461	DNS 플러드 IPv6 DNS-MX	DNS 보호				IPv6을 통한 DNS MX 쿼리 플러드입니다.
462	DNS 플러드 IPv6 DNS-PTR	DNS 보호				IPv6을 통한 DNS PTR 쿼리 플러드입니다.
463	DNS 플러드 IPv6 DNS-AAAA	DNS 보호				IPv6을 통한 DNS AAAA 쿼리 플러드입니다.
464	DNS 플러드 IPv6 DNS-Text	DNS 보호				IPv6을 통한 DNS 텍스트 쿼리 플러드입니다.
465	DNS 플러드 IPv6 DNS-SOA	DNS 보호				IPv6을 통한 DNS SOA 쿼리 플러드입니다.
466	DNS 플러드 IPv6 DNS-NAPTR	DNS 보호				IPv6을 통한 DNS NAPTR 쿼리 플러드입니다.
467	DNS 플러드 IPv6 DNS-SRV	DNS 보호				IPv6을 통한 DNS SRV 쿼리 플러드입니다.
468	DNS 플러드 IPv6 DNS-Other	DNS 보호				IPv6을 통한 DNS 기타 쿼리 플러드입니다.

표 172: DefensePro 공격 보호 ID(계속)

ID 번호 또는 범위	공격 보호 이름	카테고리 (보고용)	기본 위험	기본 작업	보고 조치	설명
469	DNS 플러드 IPv6 DNS-ALL	DNS 보호				IPv6을 통한 DNS 쿼리 플러드입니다.
720	SYN 플러드 보호		High	정책 조치에 따름		보호 정책당 공격 시작, 진행 및 종료입니다.
721	SYN 플러드 사용 보호		High	정책 조치에 따름		첫 번째 ACK/데이터 패킷 비율에 대한 SYN 비율이 초당 1000패킷을 넘으면 진행 중인 메시지입니다.
722	SYN 플러드 보호 전체 테이블		Medium	정책 조치에 따름		(이 이벤트는 버전 5.10 이상에서는 생성되지 않습니다.) DefensePro의 세션 테이블 보호에 사용합니다.
723	SCRP(SYN ACK Reflection Protection)		High	정책 조치에 따름		(이 이벤트는 버전 5.10 이상에서는 생성되지 않습니다.) SARP(SYN ACK Reflection Protection)에 사용합니다.
724	SYN 보호 삭제 프래그멘테이션		정보	정책 조치에 따름		인증 프로세스 중에 프래그멘테이션된 패킷이 도착하면 사용합니다. 패킷을 버립니다.
725	SYN 보호 삭제 재설정		정보	정책 조치에 따름		인증 프로세스 중에 기존 세션과 일치하지 않는 RESET 패킷이 도착하면 사용합니다. 패킷을 버립니다.
726	SYN 보호 상황에 맞지 않음		정보	정책 조치에 따름		(이 이벤트는 버전 5.10 이상에서는 생성되지 않습니다.) 인증 프로세스 중에 기존 세션과 일치하지 않는 패킷이 도착하면 사용합니다. 패킷이 삭제되고 소스에 RESET이 전송됩니다.

표 172: DefensePro 공격 보호 ID(계속)

ID 번호 또는 범위	공격 보호 이름	카테고리 (보고용)	기본 위험	기본 작업	보고 조치	설명
727	SYN 보호 가득 찬 테이블		Medium	정책 조치에 따름		SYN 보호 테이블이 가득 차고 모듈에서 동시 인증 프로세스를 더 이상 처리할 수 없는 경우 사용합니다. 테이블이 가득 찬 경우 새로 확인된 ACK(또는 데이터) 패킷은 폐기합니다.
729	SYN 보호 상황에 맞지 않음		정보	정책 조치에 따름		인증 프로세스 중에 기존 세션과 일치하지 않는 패킷이 도착하면 사용합니다. 패킷이 삭제되고 소스에 RESET이 전송됩니다.
730	SYN 보호 확인되지 않은 쿠키		정보	Drop		ACK 패킷이 DefensePro 디바이스에서 보낸 쿠키와 일치하지 않는 SYN 쿠키를 포함하여 도착한 경우 사용합니다. 이 오류는 정책이 차단 및 보고로 구성된 경우에만 생성됩니다.
731	SYN 보호 불완전		정보	Drop		(이 이벤트는 버전 5.1x에는 해당하지 않습니다.) 인증 프로세스 중, 첫 번째 데이터 패킷이 도착하기 전에 새 세션이 에이징될 때 사용합니다.
732	SYN 보호 잘못된 tcp 삭제		정보	Drop		인증 프로세스 중에 예상치 못한 패킷 또는 잘못된 TCP 플래그가 있는 패킷이 도착하면 사용합니다. 패킷을 버립니다.
740	TCP 세션 삭제	상태 저장 ACL	High	Drop		ACL 정책과 일치하는 트래픽에 대해 보고합니다.
741	TCP 세션 허용	상태 저장 ACL	정보	Forward		ACL 정책과 일치하는 트래픽에 대해 보고합니다.

표 172: DefensePro 공격 보호 ID(계속)

ID 번호 또는 범위	공격 보호 이름	카테고리 (보고용)	기본 위험	기본 작업	보고 조치	설명
742	UDP 세션 삭제	상태 저장 ACL	High	Drop		ACL 정책과 일치하는 트래픽에 대해 보고합니다.
743	UDP 세션 허용	상태 저장 ACL	정보	Forward		ACL 규칙과 일치하는 트래픽에 대한 정책.
744	ICMP 세션 삭제	상태 저장 ACL	High	Drop		ACL 정책과 일치하는 트래픽에 대해 보고합니다.
745	ICMP 세션 허용	상태 저장 ACL	정보	Forward		ACL 정책과 일치하는 트래픽에 대해 보고합니다.
746	IP 세션 삭제	상태 저장 ACL	High	Drop		ACL에서 명시적으로 지원되지 않는 ACL 정책과 일치한 IP 트래픽에 대해 보고합니다(즉, TCP, UDP, ICMP, IGMP, SCTP 또는 지원되는 터널링 프로토콜 등이 *아닌* 트래픽).
747	IP 세션 허용	상태 저장 ACL	정보	Forward		ACL에서 명시적으로 지원되지 않는 ACL 정책과 일치한 IP 트래픽에 대해 보고합니다(즉, TCP, UDP, ICMP, IGMP, SCTP 또는 지원되는 터널링 프로토콜 등이 *아닌* 트래픽).
748	TCP 중간 플로우 패킷	상태 저장 ACL	Medium	Drop		ACL 정책과 일치하는 트래픽에 대해 보고합니다.
749	TCP 잘못된 재설정	상태 저장 ACL	Medium	Drop		ACL 정책과 일치하는 트래픽에 대해 보고합니다.
750	TCP 핸드쉐이크 위반	상태 저장 ACL	Medium	Drop		ACL 정책과 일치하는 트래픽에 대해 보고합니다.
751	ICMP Smurf 패킷	상태 저장 ACL	Medium	Drop		ACL 정책과 일치하는 트래픽에 대해 보고합니다.
752	ICMP 패킷 이상	상태 저장 ACL	Medium	Drop		ACL 정책과 일치하는 트래픽에 대해 보고합니다.

표 172: DefensePro 공격 보호 ID(계속)

ID 번호 또는 범위	공격 보호 이름	카테고리 (보고용)	기본 위험	기본 작업	보고 조치	설명
753	GRE 세션 삭제	상태 저장 ACL	High	Drop		ACL 정책과 일치하는 트래픽에 대해 보고합니다.
754	GRE 세션 허용	상태 저장 ACL	정보	Forward		ACL 정책과 일치하는 트래픽에 대해 보고합니다.
755	SCTP 세션 삭제	상태 저장 ACL	High	Drop		ACL 정책과 일치하는 트래픽에 대해 보고합니다.
756	SCTP 세션 허용	상태 저장 ACL	정보	Forward		ACL 정책과 일치하는 트래픽에 대해 보고합니다.
1,000–100,000	DoS 실드 시그니처 또는 침입 보호 시그니처	DoS				SOC(Security Operations Center) 시그니처 파일의 시그니처 범위입니다. 홀수 ID 번호는 DoS 실드 시그니처입니다. 짝수 ID 번호는 침입 시그니처입니다.
200,000	HTTP	SynFlood	Medium	정책 조치에 따름		미리 정의된 HTTP-SYN-flood 공격 보호입니다.
200,001	HTTPS	SynFlood	Medium	정책 조치에 따름		미리 정의된 HTTPS-SYN-flood 공격 보호입니다.
200,002	RTSP	SynFlood	Medium	정책 조치에 따름		미리 정의된 RTSP-SYN-flood 공격 보호입니다.
200,003	FTP_CTRL	SynFlood	Medium	정책 조치에 따름		미리 정의된 FTP_CTRL-SYN-flood 공격 보호입니다.
200,004	POP3	SynFlood	Medium	정책 조치에 따름		미리 정의된 POP3-SYN-flood 공격 보호입니다.
200,005	IMAP	SynFlood	Medium	정책 조치에 따름		미리 정의된 IMAP-SYN-flood 공격 보호입니다.
200,006	SMTP	SynFlood	Medium	정책 조치에 따름		미리 정의된 SMTP-SYN-flood 공격 보호입니다.
200,007	TELNET	SynFlood	Medium	정책 조치에 따름		미리 정의된 TELNET-SYN-flood 공격 보호입니다.

표 172: DefensePro 공격 보호 ID(계속)

ID 번호 또는 범위	공격 보호 이름	카테고리 (보고용)	기본 위험	기본 작업	보고 조치	설명
200,008	RPC	SynFlood	Medium	정책 조치에 따름		미리 정의된 RPC-SYN-flood 공격 보호입니다.
300,000-449,999	사용자 정의 맞춤형 시그니처	DoS				사용자 정의 보호 범위입니다. 사용자가 시그니처를 생성하면 디바이스에서 순차적으로 ID 번호를 생성합니다.
450,000– 475,000	사용자 정의 연결 제한 보호	DoS				사용자 정의 연결 제한 보호 범위입니다. 사용자가 보호를 생성하면 디바이스에서 순차적으로 ID 번호를 생성합니다.
500,000-599,999	사용자 정의 SYN 플러드 보호	SYNFlood	Low	정책 조치에 따름		사용자 정의 SYN 플러드 보호 범위입니다. 사용자가 보호를 생성하면 디바이스에서 순차적으로 ID 번호를 생성합니다.
600,000-675,000	사용자 정의 연결 PPS 제한 보호	DoS				사용자 정의 연결 PPS 제한 보호 범위입니다. 사용자가 보호를 생성하면 디바이스에서 순차적으로 ID 번호를 생성합니다.

부록 D – DefensePro에서 지원되는 프로토콜

이 부록에는 DefensePro 시그니처에서 보호할 수 있는 프로토콜과 운영 체제가 나열되어 있습니다. DefensePro 시그니처를 통해 보호할 수 있는 프로토콜은 다음과 같습니다.

- BGP
- BOOTP
- Borland Interbase Protocol
- CA 라이센스 클라이언트 프로토콜
- CVS
- DHCP
- DNP3(SCADA)
- DNS
- EIGRP
- Finger
- FTP
- HTTP
- HTTPS
- ICCP(SCADA)
- ICMP
- Ident
- IGAP
- IGMP
- IP
- IPP
- IRC
- ISAKMP
- LDAP
- LPR
- MaxDB
- MODBUS(SCADA)
- Motorola Timbuktu
- NBT
- NDAP
- NDMP
- NetBIOS
- NetFlow
- NFS
- NHRP
- NMAP
- NNTP
- Ntalk
- NTP
- ORACLE
- Overnet
- PCAnywhere
- POP2
- POP3
- PP
- RADIUS
- RDP
- Retrospect
- RFB(VNC)
- RIP
- Rlogin
- RTSP
- SCCP(SKINNY)
- SCTP
- SIP
- SMB
- SMS 원격 제어
- SMTP
- SNMP
- SOAP
- SOCKS4
- SOCKS5
- SQL
- SSH
- SSL
- SUN-RPC
- TACACS
- TCP
- TELNET
- TFTP
- UDP
- UPNP
- WebDAV
- WHOIS
- Winny
- WINS
- XDMCP
- 보안 IMAP
- 보안 SMTP

DefensePro 시그니처를 통해 보호할 수 있는 운영 체제는 다음과 같습니다.

- 3COM
- Cisco
- Juniper
- Linux
- Mac OS
- MS Windows

DefensePro에서 지원되는 프로토콜

- MS Windows Server
- Unix

부록 E – 문제 해결

디바이스가 예상대로 작동하지 않으면 시스템을 진단하거나 Radware Technical Support에 관련 정보를 제공할 수 있습니다.

하드웨어 관련 문제를 해결하려면 Cisco Technical Support에 문의하십시오. 이 부록에는 다음 절이 포함되어 있습니다. 기술 지원 파일, 239페이지.

기술 지원 파일

DefensePro 디바이스에서 기술 지원 파일을 생성할 수 있습니다. 그러면 지정된 위치에 저장한 다음 문제를 진단하는 데 도움이 되도록 Radware Technical Support에 보낼 수 있습니다.

CLI를 사용하는 기술 지원 파일에는 다음이 포함됩니다.

- **Radware Technical Support에서 DefensePro 디바이스의 문제점을 진단하는 데 일반적으로 필요한 데이터**—이 데이터는 다양한 CLI 명령에서 수집한 출력으로 구성됩니다.
- **디바이스에 대한 각 컨피그레이션 변경 레코드(임의의 관리 인터페이스를 통해 수행)**— 디바이스에서 첫 번째 명령을 수신하면 이러한 레코드를 저장하기 시작합니다. 레코드는 날짜별로 오름차순으로 정렬됩니다. 데이터 크기가 허용된 최대 크기(2MB)를 초과하면 가장 오래된 레코드를 덮어 씁니다. 디바이스 컨피그레이션을 지우지 않는 한, 전체 데이터는 절대 지우지 않습니다.
- **dp_support.txt**—Radware Technical Support에서 DefensePro 디바이스의 문제를 진단하는 데 일반적으로 필요한 데이터가 포함되어 있습니다. 데이터는 다양한 CLI 명령에서 수집한 출력으로 구성됩니다.
- **auditLog.log**—디바이스의 각 컨피그레이션 변경 레코드를 포함합니다(임의의 관리 인터페이스를 통해 수행). 디바이스에서 첫 번째 명령을 받으면 이 레코드를 저장하기 시작합니다. 레코드는 날짜별로 오름차순으로 정렬됩니다. 데이터 크기가 허용된 최대 크기(2MB)를 초과하면 가장 오래된 레코드를 덮어 씁니다. 디바이스 컨피그레이션을 지우지 않는 한, 전체 데이터는 절대 지우지 않습니다.

  auditLog.log 파일의 각 레코드 구조는 다음과 같습니다.

  <dd>-<MM>-<yyyy> <hh>:<mm>:<ss> <Event description>

  예:

  06-12-2009 19:16:11 COMMAND: “logout” by user radware via Console
- HTTPFLD.tar—HTTP 플러드에 대한 데이터를 포함합니다.
- NTFLD.tar—네트워크 플러드에 대한 데이터를 포함합니다.

CLI를 사용하여 터미널에서 기술 지원 파일의 출력을 생성 및 표시하려면

> 다음 명령을 입력합니다.

  manage support display

CLI를 사용하여 기술 지원 파일을 생성한 후 TFTP 서버에 전송하려면

> 다음 명령을 입력합니다.

manage support tftp put <file name> <TFTP server IP address> [-v]

여기서 각 항목은 다음을 나타냅니다.

-v는 명령 출력도 표시합니다.

웹 기반 관리를 사용하여 기술 지원 파일을 생성 및 다운로드하려면

1. **File(파일) > Support(지원)**를 선택합니다. *Download Tech Support Info File(기술 지원 정보 파일 다운로드)* 창이 표시됩니다.
2. **Set(설정)**를 클릭합니다. *File Download(파일 다운로드)* 대화 상자가 열립니다.
3. **Open(열기)** 또는 **Save(저장)**을 클릭하고 필수 정보를 지정합니다.

부록 F – 용어집

이 용어집은 Radware 기술 환경에서 사용하는 용어와 정의 목록입니다. 일부 단어는 공용 도메인에 속하며, 다른 일부는 Radware에 고유하지만, 모두 Radware 문서에서 사용됩니다.

Radware 용어집은 Radware 기술 환경에서 사용되는 정의가 포함된 특수 단어 목록입니다. 일부 단어는 공용 도메인에 속하며, 다른 일부는 Radware에 고유하지만, 모두 하드카피나 온라인으로 된 Radware 문서에서 사용됩니다.

표 173: 용어

용어	정의
이상	이상 징후는 트래픽 패턴 및 프로토콜의 비정상적이거나 예상치 않은 동작입니다.
공격 대상	대문자 “A”를 사용하는 공격(Attack)은 네트워크, 호스트 또는 서비스에 대해 수행된 악의적인 조치인 위협을 나타냅니다.
공격 목록	공격 목록은 시그니처 데이터베이스에 정의된 대로 알려진 공격자의 데이터베이스입니다.
공격 시그니처 데이터베이스	Radware의 공격 시그니처 데이터베이스에는 알려진 공격의 시그니처가 포함되어 있습니다. 이 시그니처는 연결 및 보호 테이블에 보호 정책을 생성하기 위해 Radware에서 제공하는 미리 정의된 그룹 및 프로필에 포함되어 있습니다. 각 공격 그룹은 특정 애플리케이션 또는 IP 주소 범위를 보호하는 공통 특성이 포함된 공격 시그니처로 구성됩니다.
동작 기반 DoS(BDoS)	동작 기반 DoS(행동 기반 서비스 거부) 보호에서는 가짜 트래픽으로 인해 사용 가능한 네트워크 대역폭이 체증되게 하여, 합법적인 사용자가 네트워크 리소스를 사용하지 못하게 하는 제로 데이 네트워크 플러드 공격으로부터 네트워크를 방어합니다. BDoS 프로필에서는 이례적인 트래픽 공간을 식별하여 이 작업을 수행합니다. 네트워크 플러드 보호 유형은 다음과 같습니다. ● SYN 플러드 ● TCP Fin + Ack 플러드, TCP 재설정 플러드를 포함하는 TCP 플러드 ● TCP Syn + Ack 플러드, TCP 프래그멘테이션 플러드 ● UDP 플러드 ● ICMP 플러드 ● IGMP 플러드

표 173: 용어(계속)

용어	정의
DDoS	DNS 서버의 Distributed Denial of Server 공격입니다. 일반적인 공격에서는 “합법적” 요청을 처리하고 도용된 피해자에게 응답을 보내는 DNS 서버에 도용된 도메인 이름 요청을 전송하는 손상된 좀비 시스템(봇넷)을 사용합니다. 반복을 제공하도록 DNS 서버를 구성하면, 요청된 도메인 이름을 로컬에서 사용할 수 없는 경우 DNS 서버에서 IP 주소의 루트 이름 서버를 쿼리합니다. 그러면 트래픽이 인터넷 백본을 횡단하므로, 인터넷 서비스 제공자와 업스트림 제공자가 원하는 대상에 도달하는 데 영향을 미칩니다. Radware의 조정 가능 동작 기반 DoS 보호에서는 DNS 트래픽의 특성을 학습하며 정상 트래픽 동작 베이스라인을 다시 설정합니다. 퍼지 로직을 기반으로 하는 임베디드 의사결정 엔진에서 지속적으로 DNS 트래픽을 분석하고 정상 베이스라인에서 이탈이 발생하면 이를 탐지합니다. 탐지하면 시스템에서 패킷 헤더와 페이로드에 있는 비정상적인 매개변수를 식별하기 위해 의심스러운 DNS 패킷을 자세히 분석합니다.
DPI(Deep Packet Inspection)	헤더만 조사하는 것이 아니라 패킷의 페이로드를 조사합니다. 그러면 보안 디바이스를 통해 애플리케이션 레벨에서 조사를 수행할 수 있습니다.
DoS	서비스 거부는 시스템 리소스를 사용하고 임시적으로 서비스를 유실하게 만드는 공격입니다.
익스플로잇	익스플로잇은 소프트웨어 취약성을 이용하는 프로그램 또는 기술입니다. 프로그램을 사용하여 보안을 붕괴하거나 네트워크를 통해 호스트를 공격할 수 있습니다.
휴리스틱 분석	휴리스틱 분석은 비정상적인 현상을 차단하는 필터를 제공하기 위한 동작 기반 분석입니다. 휴리스틱 분석은 알려진 바이러스 시그니처를 검색하는 대신 프로그램의 동작을 분석하여 잠재적인 바이러스를 식별하는 바이러스 스캐너 기능입니다.
검사 포트	검사 포트는 트래픽을 수신, 검사 및 전송하도록 구성할 수 있는 DefensePro 디바이스의 포트입니다.
침입	침입은 무단으로 시스템 리소스에 액세스하려는 시도하거나 성공적으로 액세스하는 것입니다.
IDS(Intrusion Detection System)	Radware의 IDS(Intrusion Detection System)에서는 상당히 많은 양의 합법적 활동에서 잠재적으로 파괴적/악의적인 이벤트를 필터링하여 제거하도록 최신 보안 및 공격 전문 기술을 적용합니다. 시스템 모니터링 접근 방식은 다음 두 가지가 있습니다. ● 네트워크 기반 IDS인 NIDS에서는 에이전트가 설치된 세그먼트에 전달되는 모든 네트워크 트래픽을 모니터링하여, 의심스러운 이상 징후 또는 시그니처 기반 활동에 대해 조치를 취합니다. ● 호스트 기반 IDS인 HIDS는 로컬 호스트에 한정되며, 명령 실행, 파일 액세스 또는 시스템 호출과 같은 활동을 자세히 모니터링합니다. 일반적으로 조직에서는 알려진 취약성을 기반으로 이러한 접근 방식의 조합을 선택합니다.
침입 방지	침입 방지는 시스템 보안을 손상시키는 실시간 시도를 스캔, 탐지 및 방지하는 보안 서비스입니다.

표 173: 용어(계속)

용어	정의
IP 인터페이스	DefensePro의 IP 인터페이스는 두 개의 구성 요소, 즉 IP 주소와 관련 인터페이스로 구성됩니다. 관련 인터페이스는 물리적 인터페이스 또는 가상 인터페이스(VLAN)일 수 있습니다. IP 라우팅은 DefensePro IP 인터페이스 간에 수행되는 반면 브리징은 VLAN과 연관된 IP 주소를 포함하는 IP 인터페이스 내에서 수행됩니다. DefensePro는 HTTP 요청을 감청하여 콘텐츠 검사 서버 팜에 리디렉션하도록 설계되었습니다. DefensePro 네트워크를 설계할 때 DefensePro 디바이스가 인터넷과 콘텐츠 검사 서버 둘 다와 클라이언트 사이의 경로에 있다는 점을 첫 번째로 가정합니다. DefensePro에서 인터넷으로 이동하는 클라이언트의 요청을 감청하여 콘텐츠 검사 서버에서 클라이언트로 반환되는 패킷을 조작해야 하므로 이와 같이 가정해야 합니다. 로컬 삼각 측량을 사용하는 경우를 제외하고, 모든 트래픽은 물리적으로 DefensePro 디바이스를 통과하여 이동해야 합니다. 여기에는 사용자로부터 인터넷으로 향하는 트래픽과 콘텐츠 검사 서버 팜에서 다시 사용자로 돌아가는 트래픽이 포함됩니다. 콘텐츠 검사 서버를 사용하도록 정적으로 구성된 사용자가 있으면 DefensePro 가상 주소를 사용하도록 구성되어야 합니다. 이 주소는 콘텐츠 검사 서버의 액세스 IP 주소입니다. 이 주소는 정적으로 구성된 사용자만 사용할 수 있습니다.
NHR	NHR(Next-Hop Router)은 트래픽이 라우팅되는 IP 주소를 사용하는 네트워크 요소입니다.
서버, 보고	보고 서버는 최종 사용자에게 보고서를 표시하는 필수 서비스를 실행할 책임이 있는 구성 요소입니다. 여기에는 웹 서버가 포함되며 Eclipse와 웹 인터페이스 모두에 대해 서비스를 제공할 수 있습니다.
서비스	공격 집합에 대한 보호를 제공하는 기능입니다.
시그니처	시그니처는 패턴 기반 분석이며, 알려진 공격 툴을 통해 생성된 패킷을 검색하는 데 사용합니다.
도용	도용은 한 시스템 엔티티가 다른 엔티티의 ID를 가장할 때 발생합니다.

표 173: 용어(계속)

용어	정의
SYN 쿠키	SYN 쿠키는 TCP 서버에서 선택하는 초기 TCP 시퀀스 번호입니다. 서버의 초기 시퀀스 번호와 클라이언트의 초기 시퀀스 번호의 차이점은 다음과 같습니다. ● 상위 5비트: t mod 32, 여기서 t는 64초마다 증가하는 32비트 시간 카운터입니다. ● 다음 3비트: 클라이언트의 MSS에 응답하여 서버에서 선택한 MSS의 인코딩입니다. ● 하위 24비트: 서버에서 선택한 클라이언트 IP 주소와 포트 번호, 서버 IP 주소와 포트 번호 및 t의 비밀 기능입니다. 이와 같이 선택한 시퀀스 번호는 기본 TCP 요구사항을 준수합니다. 즉, 시퀀스 번호가 점진적으로 증가합니다. 서버의 초기 시퀀스 번호는 클라이언트의 초기 시퀀스 번호보다 약간 더 빠르게 늘어납니다. SYN 큐가 가득 차도 SYN 쿠키를 사용하는 서버에서 연결을 삭제하지 않아도 됩니다. 대신 SYN 큐가 큰 경우와 똑같이 SYN+ACK를 다시 보냅니다. (예외: 서버에서 대형 창과 같은 TCP 옵션을 거부해야 하며, 인코딩할 수 있는 8개의 MSS 값 중 하나를 사용해야 합니다.) 서버에서 ACK를 받으면 최신 t 값에 비밀 기능이 작동하는지 확인한 다음 인코딩된 MSS에서 SYN 큐 항목을 다시 빌드합니다. SYN 플러드는 위조된 IP 주소에서 입력되는 일련의 SYN 패킷입니다. IP 주소는 무작위로 선택되며 공격자의 위치에 대한 힌트를 제공하지 않습니다. SYN 플러드로 인해 서버의 SYN 큐가 계속 가득 찹니다. 따라서 대개의 경우 서버에서 연결을 삭제하게 됩니다. 그러나 SYN 쿠키를 사용하는 서버는 계속 정상적으로 작동합니다. SYN 플러드가 미치는 가장 큰 영향은 대형 창을 비활성화하는 것입니다.
SYN 플러드	SYN 공격/플러드는 DoS(Denial of Service) 공격의 유형입니다. 단일 패킷 공격이라고 하는 TCP 3-way 핸드쉐이크를 완료하지 않고 SYN 패킷을 전송하여 SYN 플러드 공격을 수행합니다. 또는 TCP 3-way 핸드쉐이크는 완료하지만, 그 후에 데이터 패킷은 전송하지 않을 수 있습니다. 이러한 공격은 연결 플러드 공격이라고 합니다. SYN 패킷에서 서버에 새 연결을 알립니다. 그런 다음 서버에서 입력되는 연결을 처리하기 위해 메모리를 할당한 다음, 수신 확인을 다시 전송하고, 클라이언트에서 연결을 완료하고 데이터 전송을 시작할 때까지 기다립니다. 공격자가 다수의 SYN 요청을 도용하여, 도착하지 않을 추가 데이터를 기다리는 서버의 메모리를 가득 채울 수 있습니다. 메모리가 가득 차면 서버에서 합법적 클라이언트의 연결을 수락할 수 없습니다. 따라서 서버가 비활성화됩니다. 중요 사항: SYN 플러드는 TCP/IP 기술 핵심에 있는 약점을 악용합니다. 즉, 이 공격에 대한 완벽한 방어가 없습니다. 그러나 부분적으로는 방어할 수 있습니다. 추가 메모리를 예약하고 연결이 완료될 때까지 기다리는 시간을 줄이도록 서버를 구성할 수 있습니다. 마찬가지로 라우터와 방화벽에서 도용된 일부 SYN 패킷을 필터링하여 제거할 수 있습니다. 마지막으로, 양호한 SYN과 잘못된 SYN을 구분하는 데 도움이 되도록 프로토콜을 속일 수 있는 기술(예: “SYN 쿠키”)이 있습니다.

표 173: 용어(계속)

용어	정의
SYN-ACK Reflection 공격 방지	SYN-ACK Reflection 공격 방지는 SYN 공격 반영을 방지하도록 고안되었으며, DoS 공격에 응답하여 생성된 SYN-ACK 패킷 스톰을 줄입니다. 디바이스에 SYN 공격이 발생한 경우 클라이언트에 세션을 계속하도록 메시지를 보내기 위해 임베디드 쿠키가 포함된 SYN-ACK 패킷을 보냅니다.
위협	인터넷 보안 용어로 위협은 자산에 위험을 제기하는 사람, 사물, 이벤트 또는 아이디어입니다. 기본 위협은 정보 누출, 서비스 거부, 무결성 위반 및 불법 사용이 될 수 있습니다.
트로이 목마	트로이 목마(*트로이*라고도 함)는 정상적으로 보이지만 실제로는 시스템을 손상시키기 위해 설계된 컴퓨터 프로그램입니다. 일반적으로 내부 시스템에 대한 무제한 액세스를 제공하여, 보안 모니터링 및 감사 정책을 건너뛰도록 설계됩니다.
바이러스	바이러스는 컴퓨터 시스템을 손상시키고 가능한 손상을 확대할 의도로 작성된 악의적 프로그램 코드입니다.
웜	웜은 사본을 다른 호스트에 보내 자체 확산되기 위해 인터넷이나 로컬 네트워크를 사용하는 일종의 컴퓨터 바이러스입니다.
제로 데이 공격	제로 데이 공격(0day)은 발견한 사람을 제외하고는 누구도 알지 못하는 취약성에 대한 공격입니다. 제로 데이 익스플로잇은 비공개의 알 수 없는 취약성에 대한 공격입니다. 알려진 시그니처가 없으므로 모든 시그니처 기반 보안 방어를 뚫을 수 있습니다. 익스플로잇이 일반 포트를 통과하고 동작 기반 또는 영향 기반 기술과 같은 다른 방어가 없는 경우 중지하기가 어렵거나 불가능합니다.

Radware Ltd. End User License Agreement

By accepting this End User License Agreement (this “License Agreement”) you agree to be contacted by Radware Ltd.’s (“Radware”) sales personnel.

If you would like to receive license rights different from the rights granted below or if you wish to acquire warranty or support services beyond the scope provided herein (if any), please contact Radware’s sales team.

THIS LICENSE AGREEMENT GOVERNS YOUR USE OF ANY SOFTWARE DEVELOPED AND/OR DISTRIBUTED BY RADWARE AND ANY UPGRADES, MODIFIED VERSIONS, UPDATES, ADDITIONS, AND COPIES OF THE SOFTWARE FURNISHED TO YOU DURING THE TERM OF THE LICENSE GRANTED HEREIN (THE “SOFTWARE”). THIS LICENSE AGREEMENT APPLIES REGARDLESS OF WHETHER THE SOFTWARE IS DELIVERED TO YOU AS AN EMBEDDED COMPONENT OF A RADWARE PRODUCT (“PRODUCT”), OR WHETHER IT IS DELIVERED AS A STANDALONE SOFTWARE PRODUCT. FOR THE AVOIDANCE OF DOUBT IT IS HEREBY CLARIFIED THAT THIS LICENSE AGREEMENT APPLIES TO PLUG-INS, CONNECTORS, EXTENSIONS AND SIMILAR SOFTWARE COMPONENTS DEVELOPED BY RADWARE THAT CONNECT OR INTEGRATE A RADWARE PRODUCT WITH THE PRODUCT OF A THIRD PARTY (COLLECTIVELY, “CONNECTORS”) FOR PROVISIONING, DECOMMISSIONING, MANAGING, CONFIGURING OR MONITORING RADWARE PRODUCTS. THE APPLICABILITY OF THIS LICENSE AGREEMENT TO CONNECTORS IS REGARDLESS OF WHETHER SUCH CONNECTORS ARE DISTRIBUTED TO YOU BY RADWARE OR BY A THIRD PARTY PRODUCT VENDOR. IN CASE A CONNECTOR IS DISTRIBUTED TO YOU BY A THIRD PARTY PRODUCT VENDOR PURSUANT TO THE TERMS OF AN AGREEMENT BETWEEN YOU AND THE THIRD PARTY PRODUCT VENDOR, THEN, AS BETWEEN RADWARE AND YOURSELF, TO THE EXTENT THERE IS ANY DISCREPANCY OR INCONSISTENCY BETWEEN THE TERMS OF THIS LICENSE AGREEMENT AND THE TERMS OF THE AGREEMENT BETWEEN YOU AND THE THIRD PARTY PRODUCT VENDOR, THE TERMS OF THIS LICENSE AGREEMENT WILL GOVERN AND PREVAIL. PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE OPENING THE PACKAGE CONTAINING RADWARE’S PRODUCT, OR BEFORE DOWNLOADING, INSTALLING, COPYING OR OTHERWISE USING RADWARE’S STANDALONE SOFTWARE (AS APPLICABLE). THE SOFTWARE IS LICENSED (NOT SOLD). BY OPENING THE PACKAGE CONTAINING RADWARE’S PRODUCT, OR BY DOWNLOADING, INSTALLING, COPYING OR USING THE SOFTWARE (AS APPLICABLE), YOU CONFIRM THAT YOU HAVE READ AND UNDERSTAND THIS LICENSE AGREEMENT AND YOU AGREE TO BE BOUND BY THE TERMS OF THIS LICENSE AGREEMENT. FURTHERMORE, YOU HEREBY WAIVE ANY CLAIM OR RIGHT THAT YOU MAY HAVE TO ASSERT THAT YOUR ACCEPTANCE AS STATED HEREINABOVE IS NOT THE EQUIVALENT OF, OR DEEMED AS, A VALID SIGNATURE TO THIS LICENSE AGREEMENT. IF YOU ARE NOT WILLING TO BE BOUND BY THE TERMS OF THIS LICENSE AGREEMENT, YOU SHOULD PROMPTLY RETURN THE UNOPENED PRODUCT PACKAGE OR YOU SHOULD NOT DOWNLOAD, INSTALL, COPY OR OTHERWISE USE THE SOFTWARE (AS APPLICABLE). THIS LICENSE AGREEMENT REPRESENTS THE ENTIRE AGREEMENT CONCERNING THE SOFTWARE BETWEEN YOU AND RADWARE, AND SUPERSEDES ANY AND ALL PRIOR PROPOSALS, REPRESENTATIONS, OR UNDERSTANDINGS BETWEEN THE PARTIES. “YOU” MEANS THE NATURAL PERSON OR THE ENTITY THAT IS AGREEING TO BE BOUND BY THIS LICENSE AGREEMENT, THEIR EMPLOYEES AND THIRD PARTY CONTRACTORS. YOU SHALL BE LIABLE FOR ANY FAILURE BY SUCH EMPLOYEES AND THIRD PARTY CONTRACTORS TO COMPLY WITH THE TERMS OF THIS LICENSE AGREEMENT.

1. **License Grant**. Subject to the terms of this Agreement, Radware hereby grants to you, and you accept, a limited, nonexclusive, nontransferable license to install and use the Software in machine-readable, object code form only and solely for your internal business purposes (“Commercial License”). If the Software is distributed to you with a software development kit (the “SDK”), then, solely with regard to the SDK, the Commercial License above also includes a limited, nonexclusive, nontransferable license to install and use the SDK solely on computers within your organization, and solely for your internal development of an integration or interoperation of the Software and/or other Radware Products with software or hardware products owned, licensed and/or controlled by you (the “SDK Purpose”). To the extent an SDK is distributed to you together with code samples in source code format (the “Code Samples”) that are meant to illustrate and teach you how to configure, monitor and/or control the Software and/or any other Radware Products, the Commercial License above further includes a limited,

nonexclusive, nontransferable license to copy and modify the Code Samples and create derivative works based thereon solely for the SDK Purpose and solely on computers within your organization. The SDK shall be considered part of the term “Software” for all purposes of this License Agreement. You agree that you will not sell, assign, license, sublicense, transfer, pledge, lease, rent or share your rights under this License Agreement nor will you distribute copies of the Software or any parts thereof. Rights not specifically granted herein, are specifically prohibited.

2. **Evaluation Use**. Notwithstanding anything to the contrary in this License Agreement, if the Software is provided to you for evaluation purposes, as indicated in your purchase order or sales receipt, on the website from which you download the Software, as inferred from any time- limited evaluation license keys that you are provided with to activate the Software, or otherwise, then You may use the Software only for internal evaluation purposes (“Evaluation Use”) for a maximum of 30 days or such other duration as may specified by Radware in writing at its sole discretion (the “Evaluation Period”). The evaluation copy of the Software contains a feature that will automatically disable it after expiration of the Evaluation Period. You agree not to disable, destroy, or remove this feature of the Software, and any attempt to do so will be a material breach of this License Agreement. During or at the end of the evaluation period, you may contact Radware sales team to purchase a Commercial License to continue using the Software pursuant to the terms of this License Agreement. If you elect not to purchase a Commercial License, you agree to stop using the Software and to delete the evaluation copy received hereunder from all computers under your possession or control at the end of the Evaluation Period. In any event, your continued use of the Software beyond the Evaluation Period (if possible) shall be deemed your acceptance of a Commercial License to the Software pursuant to the terms of this License Agreement, and you agree to pay Radware any amounts due for any applicable license fees at Radware’s then-current list prices.

3. **Subscription Software**. If you licensed the Software on a subscription basis, your rights to use the Software are limited to the subscription period. You have the option to extend your subscription. If you extend your subscription, you may continue using the Software until the end of your extended subscription period. If you do not extend your subscription, after the expiration of your subscription, you are legally obligated to discontinue your use of the Software and completely remove the Software from your system.

4. **Feedback**. Any feedback concerning the Software including, without limitation, identifying potential errors and improvements, recommended changes or suggestions (“Feedback”), provided by you to Radware will be owned exclusively by Radware and considered Radware’s confidential information. By providing Feedback to Radware, you hereby assign to Radware all of your right, title and interest in any such Feedback, including all intellectual property rights therein. With regard to any rights in such Feedback that cannot, under applicable law, be assigned to Radware, you hereby irrevocably waives such rights in favor of Radware and grants Radware under such rights in the Feedback, a worldwide, perpetual royalty-free, irrevocable, sub-licensable and non-exclusive license, to use, reproduce, disclose, sublicense, modify, make, have made, distribute, sell, offer for sale, display, perform, create derivative works of and otherwise exploit the Feedback without restriction. The provisions of this Section 4 will survive the termination or expiration of this Agreement.

5. **Limitations on Use**. You agree that you will not: (a) copy, modify, translate, adapt or create any derivative works based on the Software; or (b) sublicense or transfer the Software, or include the Software or any portion thereof in any product; or (b) reverse assemble, disassemble, decompile, reverse engineer or otherwise attempt to derive source code (or the underlying ideas, algorithms, structure or organization) from the Software, in whole or in part, or in any instance where the law permits any such action, you agree to provide Radware at least ninety (90) days advance written notice of your belief that such action is warranted and permitted and to provide Radware with an opportunity to evaluate if the law’s requirements necessitate such action; or (c) create, develop, license, install, use, or deploy any software or services to circumvent, enable, modify or provide access, permissions or rights which violate the technical restrictions of the Software; (d) in the event the Software is provided as an embedded or bundled component of another Radware Product, you shall not use the Software other than as part of the combined Product and for the purposes for which the combined Product is intended;
(e) remove any copyright notices, identification or any other proprietary notices from the Software (including any notices of Third Party Software (as defined below); or (f) copy the

Software onto any public or distributed network or use the Software to operate in or as a time- sharing, outsourcing, service bureau, application service provider, or managed service provider environment. Notwithstanding Section 5(d), if you provide hosting or cloud computing services to your customers, you are entitled to use and include the Software in your IT infrastructure on which you provide your services. It is hereby clarified that the prohibitions on modifying, or creating derivative works based on, any Software provided by Radware, apply whether the Software is provided in a machine or in a human readable form. It is acknowledged that examples provided in a human readable form may be modified by a user.

6. **Intellectual Property Rights**. You acknowledge and agree that this License Agreement does not convey to you any interest in the Software except for the limited right to use the Software, and that all right, title, and interest in and to the Software, including any and all associated intellectual property rights, are and shall remain with Radware or its third party licensors. You further acknowledge and agree that the Software is a proprietary product of Radware and/or its licensors and is protected under applicable copyright law.

7. **No Warranty**. The Software, and any and all accompanying software, files, libraries, data and materials, are distributed and provided "AS IS" by Radware or by its third party licensors (as applicable) and with no warranty of any kind, whether express or implied, including, without limitation, any non-infringement warranty or warranty of merchantability or fitness for a particular purpose. Neither Radware nor any of its affiliates or licensors warrants, guarantees, or makes any representation regarding the title in the Software, the use of, or the results of the use of the Software. Neither Radware nor any of its affiliates or licensors warrants that the operation of the Software will be uninterrupted or error-free, or that the use of any passwords, license keys and/or encryption features will be effective in preventing the unintentional disclosure of information contained in any file. You acknowledge that good data processing procedure dictates that any program, including the Software, must be thoroughly tested with non-critical data before there is any reliance on it, and you hereby assume the entire risk of all use of the copies of the Software covered by this License. Radware does not make any representation or warranty, nor does Radware assume any responsibility or liability or provide any license or technical maintenance and support for any operating systems, databases, migration tools or any other software component provided by a third party supplier and with which the Software is meant to interoperate.

   This disclaimer of warranty constitutes an essential and material part of this License.

   In the event that, notwithstanding the disclaimer of warranty above, Radware is held liable under any warranty provision, Radware shall be released from all such obligations in the event that the Software shall have been subject to misuse, neglect, accident or improper installation, or if repairs or modifications were made by persons other than by Radware's authorized service personnel.

8. **Limitation of Liability**. Except to the extent expressly prohibited by applicable statutes, in no event shall Radware, or its principals, shareholders, officers, employees, affiliates, licensors, contractors, subsidiaries, or parent organizations (together, the "Radware Parties"), be liable for any direct, indirect, incidental, consequential, special, or punitive damages whatsoever relating to the use of, or the inability to use, the Software, or to your relationship with, Radware or any of the Radware Parties (including, without limitation, loss or disclosure of data or information, and/or loss of profit, revenue, business opportunity or business advantage, and/or business interruption), whether based upon a claim or action of contract, warranty, negligence, strict liability, contribution, indemnity, or any other legal theory or cause of action, even if advised of the possibility of such damages. If any Radware Party is found to be liable to You or to any third- party under any applicable law despite the explicit disclaimers and limitations under these terms, then any liability of such Radware Party, will be limited exclusively to refund of any license or registration or subscription fees paid by you to Radware.

9. **Third Party Software**. The Software includes software portions developed and owned by third parties (the "Third Party Software"). Third Party Software shall be deemed part of the Software for all intents and purposes of this License Agreement; provided, however, that in the event that a Third Party Software is a software for which the source code is made available under an open source software license agreement, then, to the extent there is any discrepancy or inconsistency between the terms of this License Agreement and the terms of any such open source license agreement (including, for example, license rights in the open source license agreement that are

broader than the license rights set forth in Section 1 above and/or no limitation in the open source license agreement on the actions set forth in Section 5 above), the terms of any such open source license agreement will govern and prevail. The terms of open source license agreements and copyright notices under which Third Party Software is being licensed to Radware or a link thereto, are included with the Software documentation or in the header or readme files of the Software. Third Party licensors and suppliers retain all right, title and interest in and to the Third Party Software and all copies thereof, including all copyright and other intellectual property associated therewith. In addition to the use limitations applicable to Third Party Software pursuant to Section 5 above, you agree and undertake not to use the Third Party Software as a general SQL server, as a stand-alone application or with applications other than the Software under this License Agreement.

10. **Term and Termination**. This License Agreement is effective upon the first to occur of your opening the package of the Product, purchasing, downloading, installing, copying or using the Software or any portion thereof, and shall continue until terminated. However, sections 4-14 shall survive any termination of this License Agreement. The Licenses granted under this License Agreement are not transferable and will terminate upon: (i) termination of this License Agreement, or (ii) transfer of the Software, or (iii) in the event the Software is provided as an embedded or bundled component of another Radware Product, when the Software is un-bundled from such Product or otherwise used other than as part of such Product. If the Software is licensed on subscription basis, this Agreement will automatically terminate upon the termination of your subscription period if it is not extended.
11. **Export**. The Software or any part thereof may be subject to export or import controls under applicable export/import control laws and regulations including such laws and regulations of the United States and/or Israel. You agree to comply with such laws and regulations, and, agree not to knowingly export, re-export, import or re-import, or transfer products without first obtaining all required Government authorizations or licenses therefor. Furthermore, You hereby covenant and agree to ensure that your use of the Software is in compliance with all other foreign, federal, state, and local laws and regulations, including without limitation all laws and regulations relating to privacy rights, and data protection. You shall have in place a privacy policy and obtain all of the permissions, authorizations and consents required by applicable law for use of cookies and processing of users' data (including without limitation pursuant to Directives 95/46/EC, 2002/58/EC and 2009/136/EC of the EU if applicable) for the purpose of provision of any services.
12. **US Government**. To the extent you are the U.S. government or any agency or instrumentality thereof, you acknowledge and agree that the Software is a "commercial computer software" and "commercial computer software documentation" pursuant to applicable regulations and your use of the is subject to the terms of this License Agreement.
13. **Governing Law**. This License Agreement shall be construed and governed in accordance with the laws of the State of Israel.
14. **Miscellaneous**. If a judicial determination is made that any of the provisions contained in this License Agreement is unreasonable, illegal or otherwise unenforceable, such provision or provisions shall be rendered void or invalid only to the extent that such judicial determination finds such provisions to be unreasonable, illegal or otherwise unenforceable, and the remainder of this License Agreement shall remain operative and in full force and effect. In any event a party breaches or threatens to commit a breach of this License Agreement, the other party will, in addition to any other remedies available to, be entitled to injunction relief. This License Agreement constitutes the entire agreement between the parties hereto and supersedes all prior agreements between the parties hereto with respect to the subject matter hereof. The failure of any party hereto to require the performance of any provisions of this License Agreement shall in no manner affect the right to enforce the same. No waiver by any party hereto of any provisions or of any breach of any provisions of this License Agreement shall be deemed or construed either as a further or continuing waiver of any such provisions or breach waiver or as a waiver of any other provision or breach of any other provision of this License Agreement.

IF YOU DO NOT AGREE WITH THE TERMS OF THIS LICENSE YOU MUST REMOVE THE SOFTWARE FROM ANY DEVICE OWNED BY YOU AND IMMIDIATELY CEASE USING THE SOFTWARE.

미주 지역 본부
Cisco Systems, Inc.
San Jose CA

아시아 태평양 지역 본부
Cisco Systems (USA) Pte. Ltd.
싱가포르

유럽 지역 본부
Cisco Systems International BV Amsterdam,
네덜란드

Cisco는 전 세계에 200여 개 이상의 지사가 있습니다. 각 지사의 주소, 전화 번호 및 팩스 번호는 Cisco 웹 사이트 **www.cisco.com/go/offices**에서 확인하십시오.