IBM Security
Network Intrusion Prevention System

Network Intrusion Prevention System ユーザー・ガイド

バージョン 1 リリース 4.5

発行日: 2012 年 12 月

目次

Homologation statement - regulation notice

This product is not intended to be connected directly or indirectly by any means whatsoever to interfaces of public telecommunications networks.

本製品は、電気通信事業者の通信回線への直接、またはそれに準ずる方法での接続を目的とするものではありません。

Safety, environmental, and electronic emissions notices

Safety notices may be printed throughout this guide. **DANGER** notices warn you of conditions or procedures that can result in death or severe personal injury. **CAUTION** notices warn you of conditions or procedures that can cause personal injury that is neither lethal nor extremely hazardous. **Attention** notices warn you of conditions or procedures that can cause damage to machines, equipment, or programs.

DANGER notices

危險

To prevent a possible shock from touching two surfaces with different protective ground (earth), use one hand, when possible, to connect or disconnect signal cables. (D001)

危險

Overloading a branch circuit is potentially a fire hazard and a shock hazard under certain conditions. To avoid these hazards, ensure that your system electrical requirements do not exceed branch circuit protection requirements. Refer to the information that is provided with your device or the power rating label for electrical specifications. (D002)

危險

If the receptacle has a metal shell, do not touch the shell until you have completed the voltage and grounding checks. Improper wiring or grounding could place dangerous voltage on the metal shell. If any of the conditions are not as described, STOP. Ensure the improper voltage or impedance conditions are corrected before proceeding. (D003)

危險

An electrical outlet that is not correctly wired could place hazardous voltage on the metal parts of the system or the devices that attach to the system. It is the responsibility of the customer to ensure that the outlet is correctly wired and grounded to prevent an electrical shock. (D004)

危險

When working on or around the system, observe the following precautions:

Electrical voltage and current from power, telephone, and communication cables are hazardous. To avoid a shock hazard:

- **Connect power to this unit only with the IBM® ISS provided power cord. Do not use the IBM ISS provided power cord for any other product.**
- **Do not open or service any power supply assembly.**
- **Do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this product during an electrical storm.**
- **The product might be equipped with multiple power cords. To remove all hazardous voltages, disconnect all power cords.**
- **Connect all power cords to a properly wired and grounded electrical outlet. Ensure that the outlet supplies proper voltage and phase rotation according to the system rating plate.**
- **Connect any equipment that will be attached to this product to properly wired outlets.**
- **When possible, use one hand only to connect or disconnect signal cables.**
- **Never turn on any equipment when there is evidence of fire, water, or structural damage.**
- **Disconnect the attached power cords, telecommunications systems, networks, and modems before you open the device covers, unless instructed otherwise in the installation and configuration procedures.**
- **Connect and disconnect cables as described in the following procedures when installing, moving, or opening covers on this product or attached devices.**

To disconnect:

1. **Turn off everything (unless instructed otherwise).**
2. **Remove the power cords from the outlets.**
3. **Remove the signal cables from the connectors.**
4. **Remove all cables from the devices.**

To connect:

1. **Turn off everything (unless instructed otherwise).**
2. **Attach all cables to the devices.**
3. **Attach the signal cables to the connectors.**
4. **Attach the power cords to the outlets.**
5. **Turn on the devices.**

(D005)

CAUTION notices

注意:
Data processing environments can contain equipment transmitting on system links with laser modules that operate at great than Class 1 power levels. For this reason, never look into the end of an optical fiber cable or open receptacle. (C027)

注意:
The battery contains lithium. To avoid possible explosion, do not burn or charge the battery.

Do not:

- **Throw or immerse into water**
- **Heat to more than 100°C (212°F)**
- **Repair or disassemble**

Exchange only with the IBM ISS-approved part. Recycle or discard the battery as instructed by local regulations. In the United States, IBM ISS has a process for the collection of this battery. For information, call 1-800-426-4333. Have the IBM ISS part number for the battery unit available when you call. (C003)

注意:
For 19" rack mount products:

- **Do not install a unit in a rack where the internal rack ambient temperatures will exceed the manufacturer's recommended ambient temperature for all your rack-mounted devices.**
- **Do not install a unit in a rack where the air flow is compromised. Ensure that air flow is not blocked or reduced on any side, front, or back of a unit used for air flow through the unit.**
- **Consideration should be given to the connection of the equipment to the supply circuit so that overloading the circuits does not compromise the supply wiring or overcurrent protection. To provide the correct power connection to a rack, refer to the rating labels located on the equipment in the rack to determine the total power requirement of the supply circuit.**
- *(For sliding drawers)* **Do not pull or install any drawer or feature if the rack stabilizer brackets are not attached to the rack. Do not pull out more than one drawer at a time. The rack might become unstable if you pull out more than one drawer at a time.**
- *(For fixed drawers)* **This drawer is a fixed drawer and must not be moved for servicing unless specified by the manufacturer. Attempting to move the drawer partially or completely out of the rack might cause the rack to become unstable or cause the drawer to fall out of the rack.**

(R001 Part 2 of 2)

Product handling information

One of the following two safety notices may apply to this product. Please refer to the specific product specifications to determine the weight of the product to see which applies.

注意:
This part or unit is heavy but has a weight smaller than 18 kg (39.7 lb). Use care when lifting, removing, or installing this part or unit. (C008)

注意:
The weight of this part or unit is between 18 and 32 kg (39.7 and 70.5 lb). It takes two persons to safely lift this part or unit. (C009)

Product safety labels

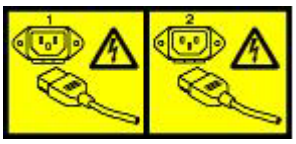
One or more of the following safety labels may apply to this product.

危険

Hazardous voltage, current, or energy levels are present inside any component that has this label attached. Do not open any cover or barrier that contains this label. (L001)

危険

Multiple power cords. The product might be equipped with multiple power cords. To remove all hazardous voltages, cdisconnect all power cords. (L003)



World trade safety information

Several countries require the safety information contained in product publications to be presented in their national languages. If this requirement applies to your country, a safety information booklet is included in the publications package shipped with the product. The booklet contains the safety information in your national language with references to the US English source. Before using a US English publication to install, operate, or service this IBM ISS product, you must first become familiar with the related safety information in the booklet. You should also refer to the booklet any time you do not clearly understand any safety information in the US English publications.

Laser safety information

The following laser safety notices apply to this product:

注意:
This product may contain one or more of the following devices: CD-ROM drive, DVD-ROM drive, DVD-RAM drive, or laser module, which are Class 1 laser products. Note the following information:

- **Do not remove the covers. Removing the covers of the laser product could result in exposure to hazardous laser radiation. There are no serviceable parts inside the device.**
- **Use of the controls or adjustments or performance of procedures other than those specified herein might result in hazardous radiation exposure. (C026)**

注意:
Data processing environments can contain equipment transmitting on system links with laser modules that operate at greater than Class 1 power levels. For this reason, never look into the end of an optical fiber cable or open receptacle. (C027)

Laser compliance

All lasers are certified in the U.S. to conform to the requirements of DHHS 21 CFR Subchapter J for class 1 laser products. Outside the U.S., they are certified to be in compliance with IEC 60825 as a class 1 laser product. Consult the label on each part for laser certification numbers and approval information.

Product recycling and disposal

This unit must be recycled or discarded according to applicable local and national regulations. IBM encourages owners of information technology (IT) equipment to responsibly recycle their equipment when it is no longer needed. IBM offers a variety of product return programs and services in several countries to assist equipment owners in recycling their IT products. Information on IBM ISS product recycling offerings can be found on IBM's Internet site at http:// www.ibm.com/ibm/environment/products/prp.shtml.

Esta unidad debe reciclarse o desecharse de acuerdo con lo establecido en la normativa nacional o local aplicable. IBM recomienda a los propietarios de equipos de tecnología de la información (TI) que reciclen responsablemente sus equipos cuando éstos ya no les sean útiles. IBM dispone de una serie de programas y servicios de devolución de productos en varios países, a fin de ayudar a los propietarios de equipos a reciclar sus productos de TI. Se puede encontrar información sobre las ofertas de reciclado de productos de IBM en el sitio web de IBM http:// www.ibm.com/ibm/environment/products/prp.shtml.

Notice: This mark applies only to countries within the European Union (EU) and Norway.

Appliances are labeled in accordance with European Directive 2002/96/EC concerning waste electrical and electronic equipment (WEEE). The Directive determines the framework for the return and recycling of used appliances as applicable through the European Union. This label is applied to various products to indicate that the product is not to be thrown away, but rather reclaimed upon end of life per this Directive.

In accordance with the European WEEE Directive, electrical and electronic equipment (EEE) is to be collected separately and to be reused, recycled, or recovered at end of life. Users of EEE with the WEEE marking per Annex IV of the WEEE Directive, as shown above, must not dispose of end of life EEE as unsorted municipal waste, but use the collection framework available to customers for the return, recycling, and recovery of WEEE. Customer participation is important to minimize any potential effects of EEE on the environment and human health due to the potential presence of hazardous substances in EEE. For proper collection and treatment, contact your local IBM representative.

注意: このマークは EU 諸国およびノルウェーにおいてのみ適用されます。

この機器には、EU 諸国に対する廃電気電子機器指令 2002/96/EC(WEEE) のラベルが貼られています。この指令は、EU 諸国に適用する使用済み機器の回収とリサイクルの骨子を定めています。このラベルは、使用済みになった時に指令に従って適正な処理をする必要があることを知らせるために種々の製品に貼られています。

Remarque: Cette marque s'applique uniquement aux pays de l'Union Européenne et à la Norvège.

L'etiquette du système respecte la Directive européenne 2002/96/EC en matière de Déchets des Equipements Electriques et Electroniques (DEEE), qui détermine les dispositions de retour et de recyclage applicables aux systèmes utilisés à travers l'Union européenne. Conformément à la directive, ladite étiquette précise que le produit sur lequel elle est apposée ne doit pas être jeté mais être récupéré en fin de vie.

Battery return program

This product contains a lithium battery. The battery must be recycled or disposed of properly. Recycling facilities may not be available in your area. For information on disposal of batteries outside the United States, go to http://www.ibm.com/ibm/environment/products/ batteryrecycle.shtm or contact your local waste disposal facility.

In the United States, IBM has established a return process for reuse, recycling, or proper disposal of used IBM sealed lead acid, nickel cadmium, nickel metal hydride, and other battery packs from IBM equipment. For information on proper disposal of these batteries, contact IBM at 1-800-426- 4333. Please have the IBM part number listed on the battery available prior to your call.

For Taiwan:

Please recycle batteries 廢電池請回收

For the European Union:

Notice: This mark applies only to countries within the European Union (EU).

Batteries or packing for batteries are labeled in accordance with European Directive 2006/66/EC concerning batteries and accumulators and waste batteries and accumulators. The Directive determines the framework for the return and recycling of used batteries and accumulators as applicable throughout the European Union. This label is applied to various batteries to indicate that the battery is not to be thrown away, but rather reclaimed upon end of life per this Directive.

Les batteries ou emballages pour batteries sont étiquetés conformément aux directives européennes 2006/66/EC, norme relative aux batteries et accumulateurs en usage et aux batteries et accumulateurs usés. Les directives déterminent la marche à suivre en vigueur dans l'Union Européenne pour le retour et le recyclage des batteries et accumulateurs usés. Cette étiquette est appliquée sur diverses batteries pour indiquer que la batterie ne doit pas être mise au rebut mais plutôt récupérée en fin de cycle de vie selon cette norme.

バッテリーあるいはバッテリー用のパッケージには、EU 諸国に対する廃電気電子機器指令 2006/66/EC のラベルが貼られています。この指令は、バッテリーと蓄電池、および廃棄バッテリーと蓄電池に関するものです。この指令は、使用済みバッテリーと蓄電池の回収とリサイクルの骨子を定めているもので、EU 諸国にわたって適用されます。このラベルは、使用済みになったときに指令に従って適正な処理をする必要があることを知らせるために種々のバッテリーに貼られています。

In accordance with the European Directive 2006/66/EC, batteries and accumulators are labeled to indicate that they are to be collected separately and recycled at end of life. The label on the battery may also include a symbol for the metal concerned in the battery (Pb for lead, Hg for the mercury, and Cd for cadmium). Users of batteries and accumulators must not dispose of batteries and accumulators as unsorted municipal waste, but use the collection framework available to customers for the return, recycling, and treatment of batteries and accumulators. Customer participation is important to minimize any potential effects of batteries and accumulators on the environment and human health due to potential presence of hazardous substances. For proper collection and treatment, contact your local IBM representative.

For California:

Perchlorate Material - special handling may apply. See http://www.dtsc.ca.gov/ hazardouswaste/perchlorate.

The foregoing notice is provided in accordance with California Code of Regulations Title 22, Division 4.5, Chapter 33. Best Management Practices for Perchlorate Materials. This product, part, or both may include a lithium manganese dioxide battery which contains a perchlorate substance.

Electronic emissions notices

The following statements apply to this IBM product. The statement for other IBM products intended for use with this product will appear in their accompanying manuals.

Federal Communications Commission (FCC) Statement

注: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. this equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions contained in the installation manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

注: Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors, by installation or use of this equipment other than xvi IBM Internet Security Systems as specified in the installation manual, or by any other unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

注: This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Canadian Department of Communications Compliance Statement

This Class A digital apparatus complies with Canadian ICES-003.

Avis de conformité aux normes du ministère des Communications du Canada

Cet appareil numérique de las classe A est conform à la norme NMB-003 du Canada.

European Union (EU) Electromagnetic Compatibility Directive

This product is in conformity with the protection requirements of EU Council Directive 2004/108/ EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM ISS cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM ISS option cards.

This product has been tested and found to comply with the limits for Class A Information Technology Equipment according to European Standard EN 55022. The limits for Class equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

Warning:

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

European Community contact:

IBM Technical Regulations
Pascalstr. 100, Stuttgart, Germany 70569
Telephone: 0049 (0) 711 785 1176
Fax: 0049 (0) 711 785 1283
e-mail: tjahn@de.ibm.com

EC Declaration of Conformity (In German)

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 89/336/EWG zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EUMitgliedsstaaten und hält die Grenzwerte der EN 55022 Klasse A ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung der IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung der IBM gesteckt/eingebaut werden.

EN 55022 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden: "Warnung: Dieses ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funk-Störungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu ergreifen und dafür aufzukommen."

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem “Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)“. Dies ist die Umsetzung der EU-Richtlinie 89/336/EWG in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) vom 18. September 1998 (bzw. der EMC EG Richtlinie 89/336) für Geräte der Klasse A.

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EGKonformitätszeichen - CE - zu führen.

Verantwortlich für die Konformitätserklärung nach Paragraf 5 des EMVG ist die IBM Deutschland GmbH, 70548 Stuttgart.

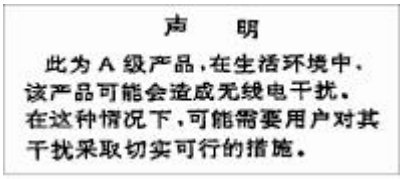
Informationen in Hinsicht EMVG Paragraf 4 Abs. (1) 4:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A

update: 2004/12/07

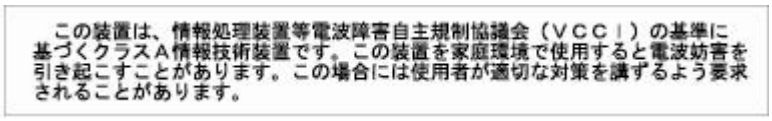
People's Republic of China Class A Compliance Statement:

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may need to perform practical actions.



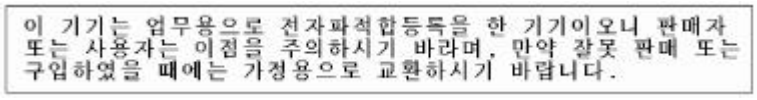
Japan Class A Compliance Statement:

This product is a Class A Information Technology Equipment and conforms to the standards set by the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). In a xviii IBM Internet Security Systems domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.



This product may not be certified in your country for connection by any means whatever to interfaces of public telecommunications networks. Further certification may be required by law prior to making any such connection. Contact an IBM representative or reseller for any questions.
本製品は、電気通信事業者の通信回線との責任分界点への、直接的な接続を想定した認定取得作業を行っていません。そのような接続を行うには、電気通信事業者による事前検査等が必要となる場合があります。ご不明な点については、IBM担当員または販売代理店にお問い合わせください。
本製品およびオプションに電源コード・セットが付属する場合は、それぞれ専用のものになっていますので他の電気機器には使用しないでください。

Korean Class A Compliance Statement:



まえがき

このガイドでは、ご使用の IBM Security Network IPS GX および GV アプライアンス用の IBM Security Network Intrusion Prevention System (IPS) の特色と機能を説明します。

対象読者

このガイドは、ネットワーク環境内の不正侵入防御システムのセットアップ、構成、および管理を担当するネットワーク・セキュリティー・システム管理者を対象としています。ネットワーク・セキュリティー・ポリシーおよび IP ネットワーク構成に関する基礎的な知識があると役立ちます。

サポートされるアプライアンス・モデル

このファームウェア・リリースは、以下のアプライアンス・モデルをサポートします。

- GX3002
- GX4000 シリーズ
- GX5000 シリーズ
- GX6000 シリーズ
- GX7000 シリーズ
- GV200
- GV1000

IBM Security Network IPS アプライアンスの資料

このガイドでは、IBM Security Network Intrusion Prevention System (IPS) の概念と機能を説明します。アプライアンスの構成と管理の手順および方法については、オンライン・ヘルプを参照してください。

最新の資料

最新の資料については、IBM Security 製品のインフォメーション・センター (http://publib.boulder.ibm.com/infocenter/sprotect/v2r8m0/index.jsp) にアクセスしてください。

サポート知識ベース

IBM サポート知識ベースは、有益な情報源です。IBMサポート知識ベースから、この知識ベースにアクセスできます。

ご使用条件

IBM Security 製品のライセンス情報については、http://www.ibm.com/services/us/iss/html/contracts_landing.html から IBM Licensing Agreement をダウンロードしてください。

カスタマー・サポート

IBM セキュリティー・ソリューションでは、サポートを受ける資格をお持ちのお客様に対して技術サポートを提供しています。

カスタマー・サポート

IBM サポート・ホームには、以下の情報が記載されています。

- サポートを受けるための登録および資格要件
- お客様の所在国におけるカスタマー・サポートの電話番号
- カスタマー・サポートにご連絡いただく前に収集しておく必要がある情報

第 1 章 IBM Security Network Intrusion Prevention System の紹介

この章では、IBM Security Network Intrusion Prevention System (IPS) を紹介し、その機能を使用して最小限の構成でネットワークを保護する方法について説明します。また、ネットワーク・セキュリティーをカスタマイズするために実装できる、IBM Security Network IPS のその他の機能についても記述しています。

不正侵入防御

IBM Security Network Intrusion Prevention System (IPS) は、悪意のある攻撃を自動的にブロックする一方で、ネットワーク帯域幅および可用性を維持します。IBM Security Network IPS アプライアンスは、ゲートウェイまたはネットワーク上にデプロイできる専用のレイヤー 2 ネットワーク・セキュリティー・アプライアンスです。広範囲にわたるネットワーク再構成を行わなくても、侵入試行、サービス妨害 (DoS) 攻撃、悪意のあるコード、バックドア、スパイウェア、ピアツーピア・アプリケーション、その他の新たに出現し続ける脅威を防止できます。

これらのアプライアンスは、柔軟なデプロイメント・オプションとすぐに使用可能な機能を備えており、ネットワーク境界ではもちろん、内部ネットワークと内部ネットワーク・セグメントの全域にわたって、正確で高性能なプロテクションを確実に提供できます。

プロテクション機能

IBM Security の不正侵入防御機能には、実証済みの検出および防止テクノロジーが最新のセキュリティー更新と共に含まれています。これらのアプライアンスは、トラフィックの論理的な流れと状態を認識し、その結果としてトロイの木馬、バックドア、ワームなどのネットワークの脅威に対する卓越した保護を提供します。

IBM Security Network IPS は、ユーザーのネットワークを脅威から保護するために、以下の機能を提供します。

- **動的ブロッキング**

  IBM Security Network IPS では、ぜい弱性ベースの攻撃識別を使用して、不要なトラフィックへの即時的で信頼性の高いブロッキング・レスポンスを可能にする一方、正当なトラフィックが妨害されずに通過できるようにします。検出ベースのブロッキングを使用する詳細なトラフィック検査プロセスを採用しており、既知の攻撃と以前には不明だった攻撃の両方を停止します。
- **ファイアウォール・ルール**

  アプライアンスが特定の IP アドレス、ポート番号、プロトコル、または VLAN からの着信パケットをブロックできるようにする、ファイアウォール・ルールを作成することができます。これらのルールは、ネットワークに影響を及ぼす前に多くの攻撃をブロックします。
- **最新のセキュリティー調査に基づいた自動セキュリティー・コンテンツ更新**

  更新済みのセキュリティー・コンテンツを自動的にダウンロードしてアクティブ化できます。ユーザーが受け取るセキュリティー更新は、IBM ISS X-Force® 研究開発チームの進行中のコミットメントの成果であり、既知および不明の脅威に対する最新の保護を提供するものです。

- **Quarantine レスポンスおよび Block レスポンス**

  インライン・アプライアンスは、Quarantine レスポンスを使用して、初期攻撃の後に指定した時間だけトラフィックをブロックします。また、Block レスポンスを使用して、イベントが発生した接続をブロックおよびリセットしたり、イベントを引き起こしたパケットをドロップしたりします。
- **Virtual Patch™ プロテクション**

  IBM Security の Virtual Patch® 機能は、貴重な時間バッファーを提供するため、ぜい弱なシステムすべてに即時にパッチを適用する必要がなくなります。システムにパッチを適用して再起動しなくても、手動でサーバーを更新する準備ができるまで待つか、スケジュール済みの更新が発生するまで待つことができます。
- **SNMP および SNMPv3 サポート**

  SNMP ベースのトラップを使用して重要なシステム問題を示す標識をモニターしたり、SNMP および SNMPv3 レスポンスを使用してセキュリティーやその他のアプライアンス・イベントに応答したりすることができます。
- **IPv6**

  Network IPS アプライアンスは、ファイアウォール・ルール、接続イベント、および検疫ルールを含む多くの機能について、IPv6 ネットワークをサポートしています。
- **SNORT**

  Network IPS アプライアンスには、特定の構成コンテンツとルールに従ってパケットの処理、アラートの送信、イベントの記録、およびレスポンスの送信を行う統合 SNORT システムが組み込まれています。

アプライアンス・インターフェース・モード

インライン・アプライアンスには、以下の 3 つのインターフェース・モードがあります。
- インライン・プロテクション
- インライン・シミュレーション
- パッシブ・モニター

アプライアンス設定の構成時に、これらのいずれかの動作モードを選択しています。必要な場合には、構成メニューを使用して、デフォルトの動作モードを使用し、後で別のモードを選択できます。

インターフェース・モード

インライン・プロテクション

インライン・プロテクション・モードでは、アプライアンスをネットワーク・インフラストラクチャーに完全に統合することができます。Block レスポンスと Quarantine レスポンスに加えて、すべてのファイアウォール・ルールが有効になり、適用済みのセキュリティー・ポリシー全体が有効になります。

注: これが、アプライアンスのデフォルト・モードです。

インライン・シミュレーション

インライン・シミュレーション・モードでは、アプライアンスを使用して、トラフィック・パターンに影響を及ぼさずにネットワークをモニターすることができます。従来の Block レスポンスに加えて、アプライ

アンスは Quarantine レスポンスを使用します。これらのレスポンスが起動された場合、パケットは廃棄されず、デフォルトではアプライアンスが TCP 接続をリセットすることもありません。ブロックされるはずのイベントは、「シミュレートされたブロック」状態として報告されます。このモードは、ネットワーク・トラフィックに影響を及ぼさずにセキュリティー・ポリシーのベースライン設定やテストを行う場合に役立ちます。

パッシブ・モニター

パッシブ・モニター・モードでは、モニター・ネットワーク・トラフィックをインラインにせずに、従来の受動的な侵入検知システム (IDS) 機能を複製します。アプライアンスは、疑わしいネットワーク・アクティビティーを検出すると、リセットを送信して TCP 接続をブロックします。このモードは、ご使用のネットワークに必要なインライン・プロテクションのタイプを判別する場合に役立ちます。

アプライアンス・インターフェース・モードの変更

パッシブ・モニター・モードとインライン・シミュレーション・モードまたはインライン・プロテクション・モードとの間で変更を行う場合は、アプライアンスへのネットワーク接続を変更する必要があります。パッシブ・モニター・モードで作動するアプライアンスは、タップ、ハブ、または SPAN ポートに接続している必要があります。

アプライアンス・インターフェース・モードをインライン・シミュレーションからインライン・プロテクションに変更する場合は、一部の拡張パラメーターを変更して、インライン・プロテクションに適した値に設定することが必要な場合があります。

レスポンス

レスポンスは、アプライアンスが侵入やその他の重要なイベントを検出したときにどう対処するかを制御します。アプライアンスには多数の定義済みのレスポンスが用意されています。さらに、ユーザーは独自のレスポンスを構成して、必要に応じてそれらのレスポンスをイベントに適用することができます。

Block レスポンス

Block レスポンスと Ignore レスポンスは、不正侵入に対するレスポンスとして常に使用可能です。**Block レスポンス**はデフォルトのレスポンスで、パケットを廃棄して TCP 接続にリセットを送信することによって攻撃をブロックします。Block レスポンスは、以下のように、アプライアンスの動作モードに応じて異なります。

使用モード	アプライアンス
パッシブ・モニター	リセットを送信して TCP 接続をブロックしますが、それ以上のブロックは実行しません。必要ない場合は、チューニング・パラメーターを使用するか、またはセキュリティー・イベント・ポリシーで Block レスポンスを無効にすることによって、リセットを無効化できます。デフォルトの X-Force ブロック・オプションを「なし」に変更することによって、リセットを無効化することもできます。
インライン・シミュレーション	ネットワーク・トラフィックをモニターして警報を生成しますが、害を与えるトラフィックのブロックは行いません。
インライン・プロテクション	パケットを廃棄して TCP 接続にリセットを送信することによって、攻撃をブロックします。

Ignore レスポンス

Ignore レスポンスは、イベント内部に指定された基準に一致するパケットを無視するようにアプライアンスに通知します。このレスポンスを設定することで、レスポンス・フィルターを通じて指定トラフィックのイベントを無視したり、あるいはこのレスポンスを使用してプロテクション・ドメインの特定のイベントを無視したりすることができます。レスポンス・フィルターまたはセキュリティー・イベントの作成時にこのレスポンスを選択すると、アプライアンスは、一致するパケットを検出してもアクションを実行しません。

Ignore レスポンスは、構成済みの他のすべてのレスポンスに優先されます。「Ignore」を選択すると、特定のイベントに対するその他のレスポンス・アクションは実行されません。

重要: Ignore レスポンスは、ネットワークを脅かさないセキュリティー・イベントをフィルターに掛ける場合にのみ使用してください。

構成可能なレスポンス

追加のレスポンスを作成して、Block レスポンスおよび Ignore レスポンスと連携させて使用できます。以下の表に、構成可能なレスポンスのタイプのリストを示します。

構成可能なレスポンス	説明
メール	イベントが発生したときに個人またはグループに E メール通知を送信するように、アプライアンスを構成できます。また、メッセージに含めるイベント・パラメーターを選択して、検出されたイベントに関する重要な情報を提供することもできます。
証拠のログ記録	イベントを起動した単一パケットのコピーを保存するか、イベントを起動したセッションのすべてのパケットを保存するように、アプライアンスを構成できます。キャプチャー・ログ・ファイルは、イベント名とイベント ID によって識別します。証拠ログには、侵入者がネットワークに何をしようとしたかが示されます。 アプライアンスは、イベントを起動したパケットを `/cache/packetlogger/logevidence` フォルダーに記録します。 IPS ローカル管理インターフェースで、パケット・ファイルをダウンロードまたは削除します。
Quarantine	アプライアンスがセキュリティー・イベント、接続イベント、またはユーザー定義イベントを検出したときに侵入者をブロックするために、Quarantine レスポンスを作成できます。Quarantine レスポンスは、ワームやトロイの木馬をブロックする場合に有効です。Quarantine レスポンスが有効になるのは、アプライアンスをインライン・プロテクション・モードで実行するように構成している場合のみです。 アプライアンスは、検出された侵入者イベントに応じて独自の検疫ルールを生成します。「Quarantined Intrusions (検疫済みの不正侵入)」ページには、手動に作成した検疫ルールに加えて、これらの動的検疫ルールも表示されます。 **注:** 事前定義されたいくつかの Quarantine レスポンスがすでに設定されています。事前定義されたレスポンスの名前変更、変更、または削除はできません。

構成可能なレスポンス	説明
SNMP	接続イベント、セキュリティー・イベント、およびユーザー定義イベントに対して、Simple Network Management Protocol (SNMP) 通知レスポンスを構成できます。SNMP レスポンスは、イベントに関連する値をプルして SNMP マネージャーに送信します。
ユーザー指定	イベントに対する独自のレスポンス (アプリケーションまたはスクリプトの実行など) を構成できます。 Linux のバイナリー・スクリプトまたはシェル・スクリプトを使用でき、任意のコマンド・ライン・オプションまたはコマンド・ライン引数 (イベント名、ソース・アドレスなど) を含めることができます。 レスポンスの作成後に、実行可能ファイルを手動でアプライアンスにコピーする必要があります。

事前定義の Quarantine レスポンス

レスポンス	説明
「Quarantine Intruder (侵入者の検疫)」	特定の侵入者からターゲットへのインバウンド・ネットワーク・トラフィックを停止します。 このレスポンスは、侵入者 IP アドレスからターゲット IP アドレスへの一致プロトコル・トラフィックをブロックする検疫ルールを追加します。 このレスポンスを使用して、既知の悪意のある侵入者がサーバーとの通信を確立するのを防止します。 このレスポンスは、ネットワーク・スイープ・セキュリティー・イベントをブロックするのには適していません。このレスポンスを有効にした場合、侵入者のサブネット・スイープにより非常に多くの検疫ルールが追加されるので、このレスポンスでスイープを効果的にブロックすることはできません。
「Quarantine Trojan (トロイの木馬の検疫)」	感染した可能性のあるホストのすべてのネットワーク通信を停止する方法を提供します。 このレスポンスは、単一の被害者の特定の TCP または UDP ポートへのトラフィックを指定の期間ブロックする検疫ルールを追加します。 このオプションを使用する前に、誤検出のリスクを考慮してください。ゼロデイ型または非常にインパクトの大きいトロイの木馬がインターネット全体に蔓延している場合は、このオプションを使用してください。 **注:** このレスポンスは ICMP トラフィックには適用されません。
「Quarantine Worm (ワームの検疫)」	伝搬して自己増殖しようとするネットワーク・ワームの拡大を最小限に抑える方法を提供します。 このレスポンスは、単一の侵入者から特定の TCP または UDP ポートへのトラフィックを指定の期間ブロックする検疫ルールを追加します。 ゾンビまたは潜在的にぜい弱なネットワーク・サービスとの会話を確立しようとするボットネットをブロックするには、このレスポンスが適しています。 **注:** このレスポンスは ICMP トラフィックには適用されません。

レスポンス	説明
「**Quarantine DDOS (Distributed Denial-of-Service) (DDOS (分散サービス妨害) の検疫)**」	特定の攻撃に関連する侵入者からのトラフィックをブロックします。 このレスポンスは、DDOS イベントをブロックすると同時にレポート・ロードを削減する場合に適しています。同じ侵入者からの一致イベントはサイレントにブロックされ、検疫ルールがアクティブになっている間は再び報告されることはありません。 **注: 「Quarantine DDOS (Distributed Denial-of-Service) (DDOS (分散サービス妨害) の検疫)」**事前定義レスポンスは、セキュリティー・イベントのみに対して機能し、その他のイベント・タイプには機能しません。

SiteProtector™ のレスポンス・オブジェクト

SiteProtector を使用してアプライアンスを管理していて、イベントに対するレスポンスを構成する必要がある場合は、レスポンス・オブジェクトを使用してください。レスポンス・オブジェクトを使用すると、データを一元化することができます。データが変化した場合でも、データの各インスタンスでなく、レスポンス・オブジェクトを変更できます。

注: SiteProtector を使用してアプライアンスを管理している場合は、中央レスポンスを使用してイベントレスポンスを作成できます。詳しくは、SiteProtector のヘルプの『Central Responses の設定 (Configuring Central Responses)』を参照してください。

ポリシーでの手順

IPS ローカル管理インターフェースの場合:

- 「**Secure Protection Settings (セキュア・プロテクション設定)**」 > 「**Response Tuning (レスポンス・チューニング)**」 > 「**レスポンス**」

SiteProtector の場合:

- 「**Shared Objects (共有オブジェクト)**」 > 「**レスポンス・オブジェクト**」

IPv6

IBM Security Network Intrusion Prevention System (IPS) は、IPv6 ネットワークを攻撃から保護します。IPv6 サポートに関連した特殊な考慮事項は、すべてアプライアンスのヘルプに示されています。

IPv6 は、標準インターネット・プロトコルとして IPv4 の代わりに使用するためのものです。IPv6 トラフィックにネットワークを移行する準備段階では、Network IPS アプライアンスは、IPv4 トラフィックのサポートを継続しながら、IPv6 トラフィックをサポートするように構成することができます。

このアプライアンスは、以下の機能について IPv6 アドレスをサポートしています。

- ユーザー定義イベント
- プロテクション・ドメイン
- 接続イベント
- 検疫ルール
- レスポンス・フィルター
- ファイアウォール・ルール
- ハイアベイラビリティ

- 管理インターフェース
- SiteProtector のエージェント・マネージャー
- SNMP 通知 (情報およびトラップ)
- NTP サーバー

第 2 章 アプライアンスの管理

ローカルに、または中央アプライアンス管理システムを使用して、アプライアンスのセキュリティー・ポリシーの作成とデプロイ、アラートの管理、および更新の適用を行うことができます。

IBM Security Network IPS は、次のようなアプライアンス管理ツールを提供します。

- IPS ローカル管理インターフェース (アプライアンスを個別にローカルで管理)
- SiteProtector (アプライアンスを中央管理コンソールから管理)

IPS ローカル管理インターフェース

IPS ローカル管理インターフェースは、ローカルの単一アプライアンスを管理するためのブラウザー・ベースのグラフィカル・ユーザー・インターフェース (GUI) です。IPS ローカル管理インターフェースを使用して、以下の機能を管理できます。

- アプライアンスの状況のモニター
- 動作モードの構成
- ファイアウォール設定の構成
- アプライアンスの設定およびアクティビティーの管理
- アラートの詳細の確認
- ハイアベイラビリティの構成
- プロテクション・ドメインを使用したセキュリティー・ポリシーの管理

SiteProtector

SiteProtector は、IBM ISS 中央管理コンソールです。SiteProtector を使用して、コンポーネントおよびアプライアンスの管理、イベントのモニター、報告のスケジュールを行うことができます。デフォルトでは、アプライアンスは、IPS ローカル管理インターフェースで管理されるようにセットアップされます。アプライアンスのグループを他のセンサーと一緒に管理している場合は、SiteProtector が提供する中央管理機能を選択すると便利です。

アプライアンスを SiteProtector に登録すると、SiteProtector は、アプライアンスの以下の管理機能を制御します。

- ファイアウォール設定
- 不正侵入防御設定
- アラート・イベント
- アプライアンスおよびセキュリティー・コンテンツの更新

アプライアンスを SiteProtector に登録すると、IPS ローカル管理インターフェースでこれらの機能を表示できますが、変更 は SiteProtector からのみ可能です。

参照情報: SiteProtector でのアプライアンスの管理の説明については、SiteProtector のユーザー資料 (http://publib.boulder.ibm.com/infocenter/sprotect/v2r8m0/index.jsp) または SiteProtector のヘルプを参照してください。

SiteProtector または IPS ローカル管理インターフェースの管理対象

いくつかのローカル機能は、アプライアンスで直接管理する必要があります。しかし、その他の機能は、SiteProtector に登録後に、SiteProtector で制御できます。

注: SiteProtector にアプライアンスを登録した後は、IPS ローカル管理インターフェースの一部の領域は読み取り専用になります。SiteProtector からアプライアンスの登録を抹消すると、IPS ローカル管理インターフェースは、また完全に機能するようになります。
以下の表では、SiteProtector または IPS ローカル管理インターフェースを使用して制御する機能をリストしています。

機能	SiteProtector	IPS ローカル管理インターフェース
アラート・イベント	✔	✔
ファイアウォール設定	✔	✔
インストール設定	✔	✔
不正侵入防御設定	✔	
手動更新		✔
検疫ルールの管理		✔
SiteProtector の管理		✔
更新設定	✔	✔

IPS ローカル管理インターフェースの使用

IPS ローカル管理インターフェースは、IBM Security Network IPS アプライアンス用の Web ベースの管理インターフェースです。アプライアンスをローカルに構成して管理する場合に、IPS ローカル管理インターフェースを使用します。

Java™ ランタイム環境

IPS ローカル管理インターフェースを実行するには、アプライアンスに正しいバージョンの Java ランタイム環境 (JRE) をインストールしておく必要があります。サポートされる JRE のバージョン番号を調べるには、README 文書を参照してください。

IPS ローカル管理インターフェースへのアクセス

Web ブラウザーを使用して IPS ローカル管理インターフェースにアクセスします。アプライアンスの IP アドレスを使用してアプライアンスにアクセスするには、**https://**<アプライアンスの *IP アドレス*> を入力します。DNS サーバーを使用している場合は、**https://**<ホスト名> を入力します。

SiteProtector を使用した管理

SiteProtector は、IBM ISS 管理コンソールです。SiteProtector を使用して、コンポーネントおよびアプライアンスの管理、イベントのモニター、報告のスケジュールを行うことができます。デフォルトでは、アプライアンスは、IPS ローカル管理インターフェースで管理されるようにセットアップされます。アプライアンスのグループを他のセンサーと一緒に管理している場合は、SiteProtector が提供する中央管理機能を選択すると便利です。

SiteProtector 管理オプション

アプライアンスを SiteProtector グループに登録すると、以下のことができます。

- アプライアンスがセンサー・グループの設定を継承できるようにする。
- グループ内の単一アプライアンスの設定の一部またはすべてを SiteProtector で個別に管理し、グループ設定にかかわらず個々の設定をアプライアンスが維持できるようにする。

SiteProtector エージェント・マネージャーの仕組み

SiteProtector 管理を有効にする場合は、アプライアンスをエージェント・マネージャーに割り当てます。エージェント・マネージャーは、SiteProtector に登録された各種のエージェントおよびアプライアンスのコマンドおよび制御アクティビティーを管理し、アプライアンスからイベント・コレクターへのデータ転送を容易にします。イベント・コレクターは、アプライアンスから受け取るリアルタイム・イベントを管理します。

エージェント・マネージャーは、ポリシー・サブスクリプション・グループに基づいて、ポリシー更新をアプライアンスに送信します。(サブスクリプション・グループは、単一のポリシーを共有するエージェントまたはアプライアンスのグループです。) アプライアンスを SiteProtector に登録する前に、そのアプライアンスが所属するグループを決定してください。その結果、グループのポリシーがアプライアンス自体に共有されるようになります。

エージェント・マネージャーについて詳しくは、SiteProtector の資料またはオンライン・ヘルプを参照してください。

アプライアンスと SiteProtector との通信方法

SiteProtector にアプライアンスを登録すると、アプライアンスは、その最初のハートビート をエージェント・マネージャーに送信して、エージェント・マネージャーにアプライアンスの存在を認識させます。ハートビートは、アプライアンスがまだ実行中であることを示すために使用する暗号化された定期的な HTTP 要求です。これにより、アプライアンスは、エージェント・マネージャーから更新を受信することができます。SiteProtector にアプライアンスを登録するときに、ハートビート間の時間間隔 (秒単位) を設定してください。

資産のグループ化

エージェント・マネージャーは、ハートビートを受け取ると、登録のセットアップ時にユーザーが指定したグループにアプライアンスを配置します。グループを指定しなかった場合は、デフォルト・グループ「G-Series」または「Network IPS」(SiteProtector のバージョンによって異なる) にアプライアンスが配置されます。アプライアンスの登録時にグループ・ボックスをクリアすると、アプライアンスは「Ungrouped Assets (グループ化されていない資産)」に配置されます。

ローカル設定またはグループ設定

ローカル・アプライアンスの設定でグループ設定を上書きできるようにした場合、アプライアンスは最初のハートビート時にローカル設定を維持します。ローカル・アプライアンスの設定でグループ設定を上書きできないようにした場合、グループのポリシー設定が未定義であっても、エージェント・マネージャーは即時にグループのポリシー・ファイルをアプライアンスに「プッシュ」します。例えば、アプライアンスにファイアウォール・ルールを設定してから、ファイアウォール・ルールが定義されていないグループにアプライアンスを登録すると、グループ・ポリシーがローカル・ポリシーを上書きし、それ以後はアプライアンスには有効なファイアウォール・ルールがなくなります。

2 回目のハートビート時、およびそれ以降の各ハートビート時に、エージェント・マネージャーはグループ・ポリシーをアプライアンスに「プッシュ」します。ただし、一部のローカル・アプライアンス設定を SiteProtector で変更することができます。アプライアンスに対して変更したローカル・ポリシー設定は、そのアプライアンスについてのみグループ・ポリシー設定よりも優先されます。グループ内の他のすべてのアプライアンスに対しては、グループ・ポリシー設定が有効なままになります。

SiteProtector でのアプライアンスの更新の働き

アプライアンスを SiteProtector に登録した後は、定期的な更新を継続することで最大のパフォーマンスを維持し、アプライアンスが常に最新のファームウェア、セキュリティー・コンテンツ、およびデータベースを実行する状態を確保する必要があります。データベース更新、セキュリティー・コンテンツ更新、およびファームウェア更新のダウンロードとインストールを自動的に実行するようスケジュールすることを検討してください。

注: アプライアンスが SiteProtector に登録されている場合でも、IPS ローカル管理インターフェースでファームウェア更新をダウンロードしてインストールすることができます。

「Update Settings (更新設定)」ページを使用して、以下の自動更新オプションをスケジュールします。

- ファームウェア更新のダウンロードおよびインストール
- セキュリティー・コンテンツ更新のダウンロードおよびインストール
- データベースの更新

SiteProtector でのアプライアンス・イベントの処理方法

アラートを生成して SiteProtector に送信するイベントを指定できます。イベント発生時に、アプライアンスが SiteProtector にアラートを送信します。アラート内のイベント情報を使用することで、有用なレポートを作成できます。アラートがロギング用に構成されている場合、SiteProtector に送信されたアラートは、IPS ローカル管理インターフェースの「Alerts (アラート)」ページにも表示されます。

正常性アラートとセンサー・アラート

「Alerts (アラート)」セクションを使用して、ご使用の Network IPS アプライアンス上のセンサー・アラートおよび正常性アラートを構成します。センサー・アラートおよび正常性アラートを SiteProtector に表示するように構成できます。

センサー・アラート

アプライアンス関連のイベントを通知するアラート・メッセージを構成できます。イベントによりアラートが発生したときにアプライアンスが実行するアクション (イベントに応答して SNMP トラップを送信するなど) を決定してください。

表 1. センサー・アラート

アラート	説明
Sensor Error (センサー・エラー)	センサー・システム・エラーが発生したときにアラートを出します。
Sensor Warning (センサー警告)	システムの問題の可能性がある場合にアラートを出します。
Sensor Informative (センサー情報)	ユーザー・アクション (パスワードの変更、ログのダウンロード、パラメーターの編集など) に関するアラートを出します。

正常性アラート

アプライアンスの正常性を通知するアラート・メッセージを構成できます。イベントによりアラートが発生したときにアプライアンスが実行するアクション (イベントに応答してアプライアンス管理者に E メールを送信するなど) を決定してください。

表 2. 正常性アラート

アラート	説明
Health Error (正常性エラー)	アプライアンス (システム、セキュリティー、ネットワーク、および SiteProtector) の正常性に障害が発生したときにアラートを出します。例えば、内部プロセスが失敗した場合に、正常性エラーのアラートが出ます。
Health Warning (正常性警告)	アプライアンス (システム、セキュリティー、ネットワーク、および SiteProtector) の正常性に障害が発生する可能性があるときにアラートを出します。例えば、ライセンスが期限切れになった場合に、正常性警告のアラートが出ます。
Health Informative (正常性情報)	アプライアンス (システム、セキュリティー、ネットワーク、および SiteProtector) の正常性が正常な場合にアラートを出します。例えば、期限切れのライセンスが更新されたためにアプライアンスが正常になったことを示す、正常性情報のアラートが出ます。

ポリシーでの手順

IPS ローカル管理インターフェースの場合:

- 「**Manage System Settings (システム設定の管理)**」 > 「**アプライアンス**」 > 「**Alerts Settings (アラート設定)**」

SiteProtector の場合:

- 「**Alerts (アラート)**」ポリシー

キャパシティー・プランニング

スループット・グラフ、ドライバー統計、および SNMP GET 要求を使用して、キャパシティー・プランニングの情報を収集します。

スループット・グラフ

スループット・グラフでは、 ネットワークで出入りするトラフィックの合計 (メガビット単位) が表示されます。スループット・グラフには、ネットワーク内を移動する未分析のトラフィックおよびセキュア・トラフィックの合計も表示されます。未分析のトラフィックは、プロトコル分析モジュール (PAM) では検査されていません。セキュア・トラフィックは、PAM で検査されています。ただし、これは必ずしもトラフィックが疑わしいものであったことを意味するわけではありません。これらのグラフは、1 時間、1 日、1 週間、または 1 カ月の統計を表示するようにカスタマイズできます。トラフィックのキャパシティーとご使用のアプライアンスの分析の表示に最も都合のよい時間枠を選択してください。

スループット・グラフを表示するには、「**Monitor Health and Statistics (正常性および統計のモニター)**」 > 「**ネットワーク**」を選択します。

ドライバー統計

ドライバー統計はキャパシティー・プランニングに役立ちます。 ドライバー統計では、ドライバーのセキュア・トラフィック、未分析のトラフィック、受信されたパケット数、および送信されたパケット数の合計が報告されるからです。キャパシティー・プランニングに役立つ 4 つのドライバー統計は、具体的には以下のとおりです。

- **adapter.bytes.secured**: 保護されたバイト数の合計がリストされます。
- **adapter.bytes.unanalyzed**: 未分析のバイト数の合計がリストされます。
- **adapter.0.packets.received**: アダプター 0 (アダプター A) で受信されたパケット数がリストされます。
- **adapter.0.packets.transmitted**: アダプター 0 (アダプター A) で 送信された (インライン・パートナーから転送された、または注入された) パケット数がリストされます。

ドライバー統計を表示するには、「**Monitor Health and Statistics (正常性および統計のモニター)**」 > 「**ネットワーク**」を選択します。

SNMP GET 要求と MIB ファイル

SNMP GET 要求は、キャパシティー・プランニングに役立ちます。この要求を構成して、管理情報ベース (MIB) ファイルから統計を取得できるからです。MIB ファイルには、以下の項目に関する情報が含まれています。

- **network.driver.stats**: 「**Monitor Health and Statistics (正常性および統計のモニター)**」 > 「**ネットワーク**」 > 「**Network Driver Statistics (ネットワーク・ドライバー統計)**」で表示される統計がすべて含まれています。
- **protection.analysis.stats**: 「**Monitor Health and Statistics (正常性および統計のモニター)**」 > 「**セキュリティー**」 > 「**Protection Analysis Statistics (プロテクション分析統計)**」で表示される統計がすべて含まれています。
- **network.protection.stats**: 「**Monitor Health and Statistics (正常性および統計のモニター)**」 > 「**セキュリティー**」 > 「**Network Protection Statistics (ネットワーク・プロテクション統計)**」で表示される統計がすべて含まれています。
- **ipmi.chassis.status** (GX7000 シリーズのアプライアンスの場合のみ): シャーシの状況に関する情報および電源障害とドライバー障害に関する情報が含まれています。この状況は、Intelligent Platform Management Interface (IPMI) で表示できます。

SNMP GET 要求を構成するには、「**Manage System Settings (システム設定の管理)**」 > 「**アプライアンス**」 > 「**SNMP**」を選択します。その後、SNMP ツールを使用して、**MIB: NET-SNMP-EXTEND-MIB:nsExtendOutput1Table** から MIB ファイル内容を取得します。

注: キャパシティー・プランニング機能が有効になるのは、SNMP GET 要求が構成済みで有効になっている場合のみです。

NTP サーバー

Network Time Protocol (NTP) サーバーをご使用の Network IPS アプライアンスに追加できます。NTP サーバーは、指定のソースから正確な時刻を取得し、ネットワーク上にある複数のコンポーネントの時刻を同期化します。

NTP サーバーは、異なるタイム・ゾーンおよび異なる大陸にまたがるネットワーク上で時刻を管理する場合に役立ちます。SiteProtector から NTP ポリシーを構成して管理し、そのポリシーをご使用のすべての

Network IPS アプライアンスに適用することができます。NTP ポリシーは、認証に対称鍵および自動キー交換を使用します。

対称鍵

サーバーおよびクライアントは、共通秘密鍵を認証に使用します。対称鍵交換の利点としては、コンピューターの電力使用量が最小限で済む、処理時間が比較的速い、送信側と受信側の両方に暗号化または暗号化解除を行う機能があるなどの点が挙げられます。対称鍵交換を構成するには、NTP サーバーで鍵識別子 (鍵 ID)、鍵のタイプ、および鍵の値が必要です。このオプションは、NTP バージョン 3 と 4 でのみ使用可能です。

自動キー

サーバーとクライアントの両方がファイアウォールの外部にある場合は、自動キー認証を使用することができます。自動キー認証では、証明書ベースの鍵交換 (「チャレンジ/応答」交換とも呼ばれる) を使用します。この認証方式は、クライアントに対してサーバーを認証する場合に使用すると最適です。この方式は、例えば、ファイアウォールの外側にある中央サーバーが、やはりファイアウォールの外側にある複数の下層サーバーに自己認証する場合に十分に機能します。これらの下層サーバーは、内部ハードウェア部分 (NIC) を使用して、ファイアウォールの内側のクライアントに NTP アクセスを提供します。このオプションは、NTP バージョン 4 でのみ使用可能です。

自動キー交換では ID スキームを使用して、リモート・システムの ID を提供します。ID スキームを使用すると、中間者攻撃の防止に役立ちます。このアプライアンスは、Schnorr (IFF)、Guillou-Quisquater (GQ)、Mu-Varadharajan (MV) の 3 つの ID スキームをサポートしています。

FIPS および NTP ポリシー

NTP ポリシーは、連邦情報処理標準 (FIPS) 140-2 に適合するように作成されています。FIPS オプションを使用するように NTP ポリシーを構成する前に、ファームウェアのバージョンとハードウェアが FIPS で認証済みのものであることを確認してください。ご使用のネットワークが FIPS 140-2 に準拠する必要がない場合は、FIPS オプションを指定して NTP ポリシーを構成しても利点はありません。

対称鍵: FIPS 準拠にするためには、対称鍵の内容に暗号ハッシュ関数 SHA-1 のみを使用してください。MD5 は FIPS 準拠ではありません。

自動キー: FIPS 準拠にするためには、以下のオプションを使用してください。

設定	FIPS 準拠オプション
Message Digest Algorithm (メッセージ・ダイジェスト・アルゴリズム)	SHA-1
Encryption Scheme (暗号化スキーム)	DSA-SHA-1

FIPS 認証された IBM セキュリティー製品の具体的な情報については、IBM セキュリティーの FIPS140 セキュリティー・ポリシーの資料を調べてください。これらの資料は、 米国連邦情報・技術局 (NIST) の Web サイトにある「Module Validation Lists」セクション (http://csrc.nist.gov/groups/STM/cmvp/index.html)にあります。

ポリシーでの手順

IPS ローカル管理インターフェースの場合:

- 「**Manage System Settings (システム設定の管理)**」 > 「**アプライアンス**」 > 「**NTP Configuration (NTP 構成)**」

SiteProtector の場合:

- 「**NTP Configuration (NTP 構成)**」ポリシー

第 3 章 ファイアウォール設定の構成

ルール・ステートメントを使用して、パケット内の各種のソースおよび宛先情報に基づいて攻撃をブロックするためのファイアウォール・ルールを構成することができます。さらに、表示対象としての関心がない場合は、検査不要のトラフィックをフィルタリングして除去することもできます。

ファイアウォール・ルールの構成

ファイアウォール・ルールは、パケット内の各種のソースおよびターゲット情報に基づいて攻撃をブロックします。ファイアウォール・ルールを手動で追加することも、指定する値を使用してアプライアンスがルールを作成できるようにすることもできます。この機能は、ファイアウォール設定の構成時に高い柔軟性を提供します。

ファイアウォール・ルールの動作は、モードごとに異なります。以下の表で、アプライアンスがモニター・モードに従ってファイアウォール・ルールをどのように適用するかを説明します。

表 3. ファイアウォール・ルールとモニター・モード

モード	**ファイアウォール・ルールの動作**
インライン・モード	インライン・モードのアプライアンスは、指定された構成に従って、通過するトラフィックにファイアウォール・ルールを適用します。
パッシブ・モード	パッシブ・モードのアプライアンスは、従来のセンサーと同様に機能し、パケットの直接パス内には入りません。しかし、パッシブ・モードのアプライアンスでは、アプライアンスで検査する必要のないトラフィックをフィルタリングして除去することができます。ファイアウォール・ルールをパッシブ・モードのフィルターとして使用するには、ファイアウォール・ルールで Ignore レスポンスを選択します。
インライン・シミュレーション	インライン・シミュレーション・モードのアプライアンスは、パケットを渡しますが、アクションを実行しません。代わりに、アプライアンスは、インライン・モードになっていた場合に実行したはずのアクションを報告します。

ファイアウォール・ルールの基準

ファイアウォール・ルールは、以下の基準を自由に組み合わせて定義できます。

- インターフェース
- VLAN 範囲
- プロトコル (TCP、UDP、または ICMP)
- ソースまたはターゲットの IP アドレスとポート範囲

ファイアウォール・ルールの順序

アプライアンスは、リストされている順序に従って (上から下に) ファイアウォール・ルールを処理します。正しい順序付けが必須です。接続がファイアウォール・ルールに一致すると、その接続に対する以降の処理は停止します。設定された追加のファイアウォール・ルールがあっても、アプライアンスはすべて無視します。

例:

以下のステートメントを使用すると、特定のホストの特定のポートあてのもの以外、ネットワーク・セグメントに対するすべての接続をブロックできます。

```
adapter any ip src addr any dst addr 1.2.3.4 tcp dst port 80
(Action = "ignore")
adapter any ip src addr any dst addr 1.2.3.1-1.2.3.255
(Action = "drop")
```

説明:
最初のルールでは、ホスト 1.2.3.4 のポート 80 へのすべてのトラフィックは、正当なトラフィックとして通過して Web サーバーに到達できるようにします。そのネットワーク・セグメントのその他のトラフィックはすべてドロップされます。

ルールの順序を逆にすると、セグメントへのすべてのトラフィックが (1.2.3.4 上の Web サーバーへのトラフィックまでも) ドロップされます。

ファイアウォール・ルールの順序の変更

ファイアウォール・ルールの順序を変更するには、 上へ または 下へ アイコンを使用してルールを移動します。

ファイアウォール・ルールおよびアクション

ファイアウォールでは、ルール (つまりステートメント) に一致したパケットにファイアウォールがどう反応するかを記述したいくつかの異なるアクションをサポートしています。以下の表に、これらのアクションを定義します。

ルール	説明
Ignore (Permit)	一致パケットの通過を許可し、そのパケットに対してはこれ以上のアクションまたはレスポンスが実行されないようにします。セッションに対してこれ以上の検査は実行されません。
Protect	このルールに一致するパケットは PAM で処理されます。一致パケットは、ロギング、Block レスポンス、Quarantine レスポンスなど (ただしこれらに限定されません) の通常レスポンスで処理されるようにします。
Monitor	IP ホワイトリストとして機能します。ステートメントに一致するパケットが Quarantine レスポンスおよび Block レスポンスをバイパスできるようにします。ただし、その他のすべてのレスポンスはパケットに適用されます。

ルール	説明
Drop (Deny)	パケットがファイアウォールを通過するときに、パケットをドロップします。このファイアウォールはインラインなので、このアクションによってパケットがターゲット・システムに到達するのが防止されます。接続は、多くの場合は数回再試行し、最終的にはタイムアウトになります。
ドロップおよびリセット	ドロップ・アクションと同様に機能しますが、ソース・システムに TCP リセットを送信します。接続は、(自動的にリセットされるために) ドロップ・アクションの場合より速く終了します。 **注:** TCP 以外のすべてのプロトコルでは、このオプションはドロップ・アクションと同様に機能します。

ポリシーでの手順

IPS ローカル管理インターフェースの場合:

- 「**Secure Protection Settings (セキュア・プロテクション設定)**」 > 「**Firewall (ファイアウォール)**」 > 「**Firewall Rules (ファイアウォール・ルール)**」

SiteProtector の場合:

- 「**Firewall (ファイアウォール)**」ポリシー

ファイアウォール・ルール言語

ファイアウォール・ルールは、ルールが適用されるトラフィックを定義する複数のステートメント (または節) で構成されます。手動でファイアウォール・ルールを作成する場合は、このトピックに示す構文を使用します。

ファイアウォール節

ファイアウォール・ルールは、各パケットの特定の基準に一致するようにチェーニングされた複数の節で構成されます。節は、プロトコル・スタック内の特定の層を表します。個々の節は、条件と式に細分できます。式は、ルールの変数部分で、そこにアドレス、ポート、または数値パラメーターを接続できます。

以下のファイアウォール節を使用できます。

- **アダプター節**

  A から P までのアダプター・セット (「インターフェース」ともいいます) を指定します。このアダプター・セットを使用して、ルールを特定のアダプターに接続します。アダプター節は、ルールが適用される特定のアダプターを示します。サポートされるアダプター式は、any および A から P までの文字です。アダプター節を指定しなければ、そのルールはすべてのアダプターのパケットに一致します。

```
adapter (adapter-id)
adapter A
adapter any
adapter A,C
adapter A-C
```

- **イーサネット節**

802.1 フレームに一致するネットワーク・プロトコル・タイプ または仮想 LAN (VLAN) ID を指定します。イーサネット節を使用して、802.1q VLAN トラフィックをフィルタリングしたり、特定タイプのイーサネット・プロトコルを許可または拒否したりすることができます。プロトコル・タイプのリストは http://www.iana.org/assignments/ethernet-numbers にあります。イーサネット・プロトコル定数は、10 進、8 進、16 進、または別名表記で指定できます。特定タイプのイーサネット・トラフィックをブロックしやすくするには、予約済みの番号の代わりに別名を指定します。場合によっては、別名で複数のポート (例えば IPX と PPPoE) をブロックします。

```
ether proto (protocol-id)
ether proto {arp|aarp|atalk|ipx|mpls|netbui|pppoe|rarp|sna|xns}
ether vid (vlan-number)
ether vid (vlan-number) proto (protocol-id)
```

```
ether proto !arp
ether vid 1 proto 0x0800
ether vid 2 proto 0x86dd
ether vid 3-999 proto 0x0800,0x86dd
```

- **IPv4 データグラム節**

IPv4 アドレスと、トランスポート・レベルのフィルタリング・フィールド (TCP/UDP ソースまたは宛先ポート、ICMP タイプまたはコード、または特定の IP プロトコル番号など) を指定します。IP データグラム節は、IP データグラム内部に存在しているプロトコルと、ステートメントが一致するためには満たさなければならないプロトコル固有の条件を判別します。現在は、ICMP、TCP、および UDP の各条件のみがサポートされていますが、任意の IP プロトコルに基づいてフィルターを指定できます。IP データグラム節を指定しないと、ステートメントはすべての IP データグラム・プロトコルに一致します。

以下に示す 1 番目と 2 番目のステートメントは、IP アドレス式に一致する IP パケットに一致します。3 番目のステートメントは、IP アドレス式に一致する IP パケットに一致します。4 番目のステートメントは、プロトコル・タイプに一致する IP パケットに一致します。5 番目のステートメントは、1 番目と 2 番目のステートメントの組み合わせです 6 番目のステートメントは、1 番目、2 番目、および 4 番目のステートメントの組み合わせです。

```
1. ip src addr <IPv4-addr>
2. ip dst addr <IPv4-addr>
3. ip addr <IPv4-addr>
4. ip proto <protocol-type>
5. ip src addr <IPv4-addr> dst addr <IPv4-addr>
6. ip src addr <IPv4-addr> dst addr <IPv4-addr> proto <protocol-type>
```

例:

```
ip addr 192.168.10.1/24
ip addr 192.168.10.0-192.168.10.255
```

- **IPv6 データグラム節**

IPv6 データグラム節は、IPv6 データグラム内部に存在しているプロトコルと、ステートメントが一致するためには満たさなければならないプロトコル固有の条件を判別します。現在は、ICMPv6、TCP、および UDP の各条件のみがサポートされていますが、任意の IPv6 プロトコルに基づいてフィルターを指定できます。IPv6 データグラム節を指定しないと、ステートメントはすべての IPv6 データグラム・プロトコルに一致します。以下に示す 1 番目と 2 番目のステートメントは、IPv6 アドレス式に一致するソースおよび宛先の IPv6 パケットをブロックします。3 番目のステートメントは、IPv6 アドレス式に一致するソースおよび宛先 IPv6 パケットをブロックします。4 番目のステートメントは、プロトコル・タイプに一致する IPv6 パケットをブロックします。5 番目のステートメントは、1 番目と 2 番目のステートメントの組み合わせです 6 番目のステートメントは、1 番目、2 番目、および 4 番目のステートメントの組み合わせです。

```
ipv6 src addr <ipv6-addr>
ipv6 dst addr <ipv6-addr>
ipv6 addr <ipv6-adr>
ipv6 proto <protocol-type>
ipv6 src addr <ipv6-addr> dst addr <ipv6-addr>
ipv6 src addr <ipv6-addr> dst addr <ipv6-addr> proto <protocol-type>
```

例:

```
ipv6 addr FF01:0:0:0:0:0:0:101
ipv6 addr 12AB:0:0:CD30::/60
ipv6 addr FF01::101-FF01:0:0:0:0:0:0:200
```

ファイアウォール条件

TCP および UDP 条件

TCP および UDP ポート番号は 10 進、8 進、または 16 進表記で指定できます。ポート値の範囲は 0 から 65535 です。

```
tcp src port <TCP-UDP-port>
tcp dst port <TCP-UDP-port>
tcp dst port <TCP-UDP-port> src port <TCP-UDP-port>
udp src port <TCP-UDP-port>
udp dst port <TCP-UDP-port>
udp dst port <TCP-UDP-port> src port <TCP-UDP-port>
```

ICMPv4 条件

ICMP 条件は 10 進、8 進、または 16 進表記で指定できます。タイプおよびコードの有効な番号は http://www.iana.org/assignments/icmpparameters に示されています。

```
icmp type (protocol-type)
icmp code (message-code)
icmp type (protocol-type) code (message-code)
```

ICMPv6 条件

ICMPv6 条件は 10 進、8 進、または 16 進表記で指定できます。タイプおよびコードの有効な番号は http://www.iana.org/assignments/icmpparameters に示されています。

```
icmpv6 type <protocol-type>
icmpv6 code <message-code>
icmpv6 type <protocol-type> code <message-code>
```

式

式では、節のプロトコル・パーサーが一致する必要のあるヘッダー値のリストを記述します。それぞれの節が直接的な原因となって、プロトコル・スタックの特定の層に一致します。構文および値の受け入れ範囲は、節によって制御します。式は、単一値、コンマ区切りの値のリスト、または範囲セットのいずれかにすることができます。現在、式はアダプター番号、IPv4 アドレス、IPv6 アドレス、TCP および UDP のポート番号、ICMP のメッセージ・タイプとコード、および IP データグラム・プロトコル番号を指定するための存在です。

```
(value)
(value), (value)
(value)-(value)
```

感嘆符 (!) で始まる式は、*NOT 式* と呼ばれます。NOT 式は、指定した値以外のすべての値に一致します。一致する値がまったくない NOT 式の場合は、エラーが生成されます。

IPv4 アドレス式の例

<n> は、0 から 255 までの範囲の 16 進数または 10 進数です。すべての 16 進数には、0x というプレフィックスが付いていなければなりません。

単一アドレス

```
n.n.n.n
```

アドレス・リスト

```
n.n.n.n, n.n.n.n
```

CIDR フォーマットを使用する特定アドレス (ネットマスク値は 1 から 32 までの範囲内になければなりません)

```
n.n.n.n/<netmask>
```

アドレス範囲 (最初の値が最後の値より小さい場合)

```
n.n.n.n - n.n.n.n
```

IPv6 アドレス式の例

<n> の値は 16 進数字 (0 から F) でなければなりません。IPv6 アドレス内の 4 桁のゼロのグループは、単一のゼロに縮小されるか、または省略されます。

単一アドレス

```
nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn
```

アドレス・リスト

```
nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn, nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn
```

CIDR フォーマットを使用する特定アドレス (ネットマスク値は 1 から 128 までの範囲内になければなりません)

```
nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn/<prefix>
```

アドレス範囲 (最初の値が最後の値より小さい場合)

```
nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn - nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn
```

TCP/UDP ポート、プロトコル ID、または番号

どの定数にリストする値も、フィールドに必要な範囲内になければなりません。そうでない場合は、パーサーが解析節を拒否します。

```
0xFFFF
65535
0, 1, 2
0 - 2
! 3 - 65535
```

完全なファイアウォール・ルールの例

以下のステートメントは、完全なファイアウォール・ルールの例です。プロトコルを指定しない場合、ルールはすべての *(any)* プロトコルを使用します。

- `adapter A ip src addr <ip_address>`
- `adapter A ip src addr <ip_address> dst addr any tcp src port 20 dst port 80`

- adapter any ip src addr any dst addr <ip_address>
- adapter any ip src addr any dst addr any icmp type 8
- tcp
- adapter B icmp
- udp
- adapter A ipv6 src addr <ipv6_addr>
- adapter A ipv6 src addr <ipv6_addr> dst addr any tcp src port 20 dst port 80
- adapter any ipv6 src addr any dst addr <ipv6_addr>
- adapter any ipv6 src addr any dst addr any icmpv6 type 128
- ipv6 tcp
- adapter B icmpv6

第 4 章 セキュリティー・イベントの操作

この章では、セキュリティー・イベントおよびレスポンス・フィルターの構成方法を説明します。これらの機能を使用して、ネットワークで発生するセキュリティー・イベントについて、アプライアンスが応答する方法および報告する方法を制御できます。

セキュリティー・イベントの構成

「セキュリティー・イベント」ページには、攻撃タイプ別および監査別に数百に及ぶイベントがリストされています。セキュリティー・イベントは、攻撃やその他の疑わしいアクティビティーを示すことができる内容を持つネットワーク・トラフィックです。ネットワーク・トラフィックがアクティブ・セキュリティー・ポリシー内のいずれかのイベントに一致すると、セキュリティー・イベントが起動されます。ネットワークの必要性に合わせてセキュリティー・ポリシー内のイベントを編集できます。

複数のセキュリティー・イベントの編集

以下の方法で、複数のセキュリティー・イベントを選択できます。

- Ctrl キーを押して複数イベントを選択することを示してから、各イベントを選択する。
- Shift キーを押してイベント範囲を選択することを示してから、範囲内の最初と最後のイベントを選択する。

注: 編集した各項目は、選択済みのイベントすべてで変更されます。

変更の表示

選択済みイベント内の異なる値を持つ項目の横に、青色の三角形のアイコンが表示されます。このアイコンのあるフィールドの値を変更すると、選択済みのすべてのイベントで、値が新規設定に変更され、フィールドの横に表示されていた青い三角形のアイコンが消えます。

例えば、ブロックするものとしてマークしていない 2 つのイベントがあるとします。片方のイベントで Block レスポンスを有効にするとします。編集済みイベントの「ブロック」の横に青い三角形のアイコンが表示されます。もう 1 つのイベントに対しても Block レスポンスを有効にすると、両方のイベントでブロックが有効になり、青い三角形が消えます。

ポリシーでの手順

IPS ローカル管理インターフェースの場合:

- **「Secure Protection Settings (セキュア・プロテクション設定)」 > 「Advanced IPS (拡張 IPS)」 > 「セキュリティー・イベント」**

SiteProtector の場合:

- **セキュリティー・イベント**

セキュリティー・イベント情報の表示

「セキュリティー・イベント」ページには、攻撃タイプと監査に従って、数百に及ぶセキュリティー・イベントがリストされています。イベントの表示方法をカスタマイズすると、表示と検索が行いやすくなります。

フィルターおよび正規表現について

セキュリティー・イベント・フィルターでは、正規表現を使用してイベントの表示数を制限します。

正規表現 (regex ともいう) は、指定のパターンに一致するテキストを検索する場合に使用できる記号と構文の集合です。

最も基本的なレベルでは、以下のようなワイルドカード検索のタイプがサポートされています。

検索値	リターン
.*	すべてのイベント
http.*	「http」で始まるすべてのイベント
.*http	「http」で終わるすべてのイベント
.*http.*	「http」を含むすべてのイベント

正規表現は、「セキュリティー・イベント」リスト内のすべての列を検索します。例えば http* を検索した場合、その検索では、http プロトコル列に一致するすべてのイベントと、http で始まるすべてのイベントが返されます。

セキュリティー・イベントの表示とグループ化

セキュリティー・イベントの選択またはグループ化を行う前に、該当のアイコンをクリックしてください。このアクションによって、表示またはグループ化する列を決定するためのウィンドウが表示されます。

セキュリティー・イベントの表示

「フィルター」機能を使用することで、最も関心のあるセキュリティー・イベントに焦点をあてることができます。「フィルター」チェック・ボックスをクリックして、フィルターに使用する正規表現を入力します。

第 5 章 その他の不正侵入防御設定の構成

この章では、ユーザー定義イベント、接続イベント、OpenSignature イベントなど、その他の不正侵入防御設定を構成および管理する方法について説明します。検疫対象の不正侵入の管理方法、アプライアンスのグローバル・チューニング・パラメーターの表示方法、および X-Force ブロッキングのモニター方法について説明します。

検疫済み不正侵入の管理

「Quarantine Rules (検疫ルール)」ページには、検出された侵入者イベントへのレスポンスとして動的に生成された検疫ルールが表示されます。Quarantine レスポンスが有効になっている場合、ルールにより、ブロック対象のパケットとそのパケットをブロックする時間が指定されます。これによりワームの拡散が防止され、バックドアまたはトロイの木馬に感染したシステムへのアクセスが拒否されます。独自の検疫ルールを手動で追加および削除できます。ただし、既存のルールを編集することはできません。

シングルクリック・ブロッキング

「Security Alerts Logs (セキュリティー・アラート・ログ)」ページから、イベントをクリックして「**Block Intruder (侵入者のブロック)**」を選択できます。これにより、イベントで報告された送信元 IP アドレスのルールが「Quarantine Rules (検疫ルール)」ページに追加されます。アプライアンスは、ルールで指定された時間だけ、その IP アドレスでのトラフィックをすべてブロックします。シングルクリック・ブロッキング機能で追加された検疫ルールは、適用する必要がなくなったら削除してください。削除しなかった場合、ルールの期限が切れたときに、アプライアンスが自動的にそのルールを削除します。

ポリシーでの手順

IPS ローカル管理インターフェースの場合:

- 「**Secure Protection Settings (セキュア・プロテクション設定)**」 > 「**Response Tuning (レスポンス・チューニング)**」 > 「**Quarantine Rules (検疫ルール)**」

重要: 検疫済み不正侵入の表示または削除は、IPS ローカル管理インターフェースを使用した場合のみ可能です。

接続イベントの構成

接続イベントは、特定のアドレスまたはポートで出入りするオープン接続についてのユーザー定義通知です。アプライアンスが指定ポートでのネットワーク・アクティビティーを検出すると、アクティビティーのタイプや交換されたネットワーク・パケットの内容に関係なく、接続イベントが生成されます。

「Connection Events (接続イベント)」ページには、事前定義の接続イベントが、WWW、FTP、または IRC など、さまざまな接続タイプ別にリストされます。このページを使用して、モニターが必要なトラフィックに対応するために、これらのイベントのカスタマイズやユーザー独自のイベントの作成ができます。

例えば、誰かが FTP を使用してネットワークに接続するたびに接続イベントがコンソールにアラートを送るように、ルールを定義できます。

注: 接続は常に、ユーザーが指定する宛先ポートに対して登録されます。そのため、FTP 接続をモニターするには、FTP ポートを使用する必要があります。1 接続に 1 項目を指定すれば各方向のトラフィックに十分です。

接続イベントの仕組み

ネットワーク・トラフィックが特定のポートを通じて、特定のアドレスから、特定のネットワーク・プロトコルを使用してモニター対象ネットワークに接続すると、接続イベントが発生します。アプライアンスは、パケット・ヘッダー値を使用してこれらの接続を検出します。接続イベントは必ずしも攻撃やその他の疑わしいアクティビティーを構成するわけではありませんが、セキュリティー管理者の関心を引く可能性のあるネットワーク・オカレンスです。

注: 接続イベントは、特定の攻撃シグネチャーについてネットワークをモニターするわけではありません。これらのタイプの攻撃をモニターするには、セキュリティー・イベントを使用します。詳しくは、25 ページの『セキュリティー・イベントの構成』を参照してください。

接続イベントの削除

リストから任意の接続イベントを削除できます。ただし、事前定義の接続イベントを編集し、後でそれを削除することに決めた場合、そのイベントは事前定義された状態には戻らないことに注意してください。イベントはリストから完全に削除されます。このイベントを再度使用する必要があっても、使用できなくなります。

削除でなく無効化するためのベスト・プラクティス

イベントを無効化して、リストに残しておくことを検討してください。この方法をとれば、後で再度使用する必要が生まれた場合、イベントは何らかの形でまだ使用可能です。

ポリシーでの手順

IPS ローカル管理インターフェースの場合:

- 「**Secure Protection Settings (セキュア・プロテクション設定)**」 > 「**Advanced IPS (拡張 IPS)**」 > 「**Connection Events (接続イベント)**」

SiteProtector の場合:

- 「**Connection Events (接続イベント)**」ポリシー

ユーザー定義イベントの構成

ポリシーで有効にされるイベントは、アプライアンスで何を検出するかを制御します。コンテキストを囲んでユーザー定義イベントを作成して、アプライアンスがイベント確認のスキャンを行う必要のあるネットワーク・パケットのタイプと部分を指定します。

新規のユーザー定義イベント

ユーザー定義イベントを追加すると、新規イベントはリストの下部に表示されます。

ポリシーでの手順

IPS ローカル管理インターフェースの場合:

- 「**Secure Protection Settings (セキュア・プロテクション設定)**」 > 「**Advanced IPS (拡張 IPS)**」 > 「**User Defined Events (ユーザー定義イベント)**」

SiteProtector の場合:

- 「**User Defined Events (ユーザー定義イベント)**」ポリシー

ユーザー定義イベントのコンテキスト

ユーザー定義イベントを作成する場合、イベントについてモニターするネットワーク・パケットのタイプと特定部分をアプライアンスに指示するコンテキストを選択します。コンテキストを指定した後で、パケットをスキャンするときに厳密に何を検索するのかについて、アプライアンスに指示するストリングを追加します。詳しくは、32 ページの『ユーザー定義イベントの正規表現』を参照してください。

以下のユーザー定義イベントのコンテキストを使用できます。

- DNS_Query コンテキスト
- Email_Receiver コンテキスト
- Email_Sender コンテキスト
- Email_Subject コンテキスト
- File_Name コンテキスト
- News_Group コンテキスト
- Password コンテキスト
- SNMP_Community コンテキスト
- URL_Data コンテキスト
- User_Login_Name コンテキスト
- User_Probe_Name コンテキスト

以下の表に、各ユーザー定義イベントのコンテキストをリストし、各コンテキストのモニター対象について説明し、例を示します。

コンテキスト	例
DNS_Query。DNS 照会の DNS 名と、UDP および TCP 経由の DNS 応答パケットをモニターします。アプライアンスは、「ストリング」ボックス内の情報を、これらのパケット内の拡張バージョン (人が読んで理解できる形) のドメイン名と比較します。ユーザーが IP アドレスを使用して直接サイトにアクセスした場合、DNS ルックアップが発生しないため、アプライアンスはイベントを検出できません。 **注:** 特定の URL をモニターする場合、ドメイン名は最初の要素でしかないことに留意してください。例えば、//www.news.com は、http://www.news.com/stories における最初の要素です。URL の残りを検出するには、URL_Data コンテキストを使用します (「URL_Data コンテキスト」を参照)。	DNS_Query コンテキストを `www.microsoft.com` というストリング値と一緒に使用すると、Microsoft Web サイトにアクセスするユーザーをモニターすることができます。 サイト内でインターネット上のハッカー関連の資料にアクセスするユーザーについて懸念している場合は、次のようなドメインへのアクセスをモニターすることができます。 • hackernews.com • rootshell.com

コンテキスト	例
Email_Receiver。SMTP、POP、IMAP の各プロトコルを使用する E メール・ヘッダーの受信側アドレス部分をモニターすることで、特定の受信者に対する着信 E メールまたは発信 E メールをモニターします。アプライアンスが Email_Receiver コンテキストを使用してシグネチャーに一致するイベントを検出した場合は、イベントの詳細を調べることによって、その E メールが使用したプロトコルを判別することができます。 **注:** このコンテキストでは、MAPI プロトコルで送信された E メールはモニターしません。	誰かが「ソーシャル・エンジニアリング」を使用して特定の社員を操作していると思われる場合は、その社員のアドレスへの着信 E メールをモニターし、送信元 IP を記録することができます。また、誰かが社内の専有情報を特定の外部 E メール・アドレスにリークしていると思われる場合は、そのアドレスへの E メールを追跡することができます。
Email_Sender。特定の差出人の着信または発信 E メールをモニターするには、Email_Sender コンテキストを使用します。Email_Sender コンテキストは、SMTP、POP、IMAP の各プロトコルを使用している E メール・ヘッダーの差出人アドレス部分をモニターします。アプライアンスが Email_Sender コンテキストを使用してシグネチャーに一致するイベントを検出した場合は、イベントの詳細を調べることによって、その E メールが使用したプロトコルを制御することができます。 **注:** このコンテキストでは、MAPI プロトコルで送信された E メールはモニターしません。	ソーシャル・エンジニアリングまたはその他の社員操作のインスタンス (インバウンド) を検出する場合、または会社からの情報漏えい (アウトバウンド) を検出する場合に、Email_Sender コンテキストを使用します。
Email_Subject。SMTP、POP、および IMAP の各プロトコルを使用するメッセージの E メール・ヘッダーにある件名行をモニターします。 **注:** このコンテキストでは、MAPI プロトコルで送信された E メールはモニターしません。	重要なプロジェクト名またはファイル名をモニターすることによって情報漏えいを検出するためのイベントを作成できます。 Email_Subject を使用して、「ILOVEYOU」ウィルスなどのウィルスを検出できます。 **ヒント:** ウィルスおよびその他の攻撃には、件名行を系統的に変更する開発プログラムが含まれているため、これらのタイプのウィルスを追跡する場合は Email_Content コンテキストを使用してください。
File_Name。File_Name コンテキストは、ユーザーまたはプログラムが以下のいずれかのプロトコルを使用してリモート側でファイルの読み取りまたはファイルへの書き込みを試みたときに、それを検出します。 • TFTP • FTP • Windows ファイル共有 (CIFS または Samba) • NFS **注:** NFS は、ファイル名を直接参照せずにファイルを開くことができます。このコンテキストを使用してファイルへの NFS アクセスをモニターしても、100% 有効とは言えない可能性があります。	1999 年の Explorer ワームが Windows ネットワーク全体に伝搬したとき、このワームはリモートの Windows 共有上の特定ファイルへの書き込みを試みました。このようなワームの場合、ファイルへのアクセス試行をモニターし、ローカルでのワームの伝搬を止めることができます。
News_Group。社員がアクセスするニュース・グループ名をモニターするには、News_Group コンテキストを使用します。News_Group コンテキストは、NNTP プロトコルを使用してニュース・グループにアクセスしている人をモニターします。	このコンテキストを使用して、社内のインターネット使用ポリシーに照らして不適切なニュース・グループ (ハッカー・グループやポルノ・グループなど) へのサブスクリプションを検出できます。

コンテキスト	例
Password。ネットワーク上で平文で渡されたパスワードを識別するには、Password コンテキストを使用します。パスワードが暗号化されていないと、アタッカーは、別のサイトからスニファー・プログラムを使用してトラフィックをモニターし、簡単にパスワードを盗むことができます。Password コンテキストは、FTP、POP、IMAP、NNTP、または HTTP プロトコルを使用して平文でパスワードを送信しているプログラムまたはユーザーをモニターします。Password コンテキストを使用すると、以下のことができます。 • 暗号漏えいアカウントをモニターしてフォレンジック・データを取得する。 • 退職した社員のアカウントをモニターする。 • デフォルト・パスワードの使用を検出する。 **注:** このコンテキストでは、暗号化パスワードをモニターしません。	• **暗号漏えいアカウントのモニター:** 暗号漏えいアカウントを取り消した後で、そのアカウントを使用しようとする外部からの試みをモニターするイベントを作成して、暗号漏えいデータにアクセスした人を検出することができます。 • **退職した社員のアカウントのモニター:** 退職した社員のパスワードの検索を追加して、閉鎖したアカウントへの無許可のリモート・アクセス試行を検出できます。 • **デフォルト・パスワードの使用の検出:** 一般的なぜい弱性を探り出そうとしているアタッカーを検出するには、サイトに関連するデフォルト・パスワードを検索するイベントをセットアップします。 **注:** X-Force データベースには、このようなアカウント名の詳細を示すレコードが多数含まれます。デフォルト・パスワードについて詳しくは、X-Force データベース (http://xforce.iss.net) でパスワードを検索してください。
SNMP_Community。SMNP コミュニティー・ストリングの使用と、悪用の可能性をモニターします。SNMP_Community コンテキストは、SNMP コミュニティー・ストリングを含むすべてのパケットをモニターします。SNMP コミュニティー・ストリングは、SNMP メッセージ内の平文パスワードです。このパスワードは、各メッセージを認証します。パスワードが有効なコミュニティー名でない場合、メッセージは拒否されます。 認証されていない個人がコミュニティー・ストリングを知ってしまうと、その個人はその情報を使用して、ご使用の装置から重要な構成データを取得したり、さらには装置を再構成したりできるようになります。 **重要:** 非常に固有性の高いコミュニティー・ストリングを使用し、それを定期的に再構成することを検討してください。	• **旧ストリングの使用を試みる個人の検出:** SNMP コミュニティー・ストリングを変更する場合は、このコンテキストを使用してイベントを作成し、アプライアンスが旧ストリングの使用を試みる個人を検索するようにします。 • **デフォルト・ストリングの使用の検出:** X-Force データベースには、一般的な装置上でのデフォルト・コミュニティー・ストリングに関わるさまざまなぜい弱性に関する情報が含まれます。アタッカーは、これらのデフォルト・パスワードを使用してお客様の装置にアクセスしようとする場合があります。このアクティビティーをアプライアンスに検出させるには、このコンテキストを使用して、ご使用のサイトにある装置に関連するデフォルト・パスワードをモニターするイベントを作成します。これらのイベントは、これらの一般的なぜい弱性を探ろうとするアタッカーを検出することができます。 **注:** Internet Scanner を使用してネットワークをスキャンする場合、このコンテキストを使用して SNMP コミュニティー・ストリングを検査するためのルールで、SNMP スキャンへの応答として、このイベントのインスタンスが数多く検出される場合があります。 **参照情報:** デフォルト・パスワードについて詳しくは、X-Force データベース (http://xforce.iss.net) で SNMP を検索してください。

コンテキスト	例
URL_Data。HTTP GET 要求に関連したさまざまなセキュリティー問題またはポリシー問題をモニターします。HTTP GET 要求が発生するのは、クライアント (Web ブラウザーなど) が Web サーバーからのファイルを要求したときです。HTTP GET 要求は、Web サーバーにあるファイルを取得するための最も一般的な方法です。URL_Data コンテキストは、HTTP GET 要求によるアクセスの際に、特定ストリングの URL の内容 (ドメイン名またはアドレス自体を除去したもの) をモニターします。**注:** このコンテキストは、HTTP GET 要求に関連付けられているドメイン名をモニターしません。	ぜい弱な CGI スクリプトに関する攻撃をアプライアンスでモニターするには、このコンテキストを使用してください。IBM ISS のアドバイザリー #32 (1999 年 8 月 9 日リリース) に、このコンテキストを使用して Microsoft Internet Information Server コンポーネントのぜい弱性を利用する試みを検索する方法の説明があります。**参照情報:** 詳しくは、『Vulnerabilities in Microsoft Remote Data Service』(http://xforce.iss.net/alerts/advise32.php) を参照してください。社員がコンピューターを使用して社内禁止サイト (ポルノ・サイトなど) にアクセスしているかどうかを全体的に検索する場合、このコンテキストを使用することができます。
User_Login_Name。認証要求中に平文で公開されたユーザー名を検出します。このコンテキストは多くのプロトコルに対応するので、このコンテキストを使用して、アタッカーが使用するプロトコルに関わらず、特定のアカウントを使用しようとする試みを追跡できます。User_Login_Name コンテキストは、FTP、POP、IMAP、NNTP、HTTP、Windows、または R* プロトコルを使用した認証要求での平文のユーザー名をモニターします。	暗号漏えいアカウントを使用しようとする試みを追跡する場合や、最近解雇した社員が旧アカウントにオンラインでアクセスしようとしたと思われる場合に、このコンテキストを使用します。攻撃によりアカウント名「FredJ」に暗号漏えいが起きたことがわかっている場合は、このコンテキストを使用して、そのアカウントへのアクセス試行を検索するイベントを構成します。
User_Probe_Name。ご使用のネットワーク上のコンピューターへの、デフォルト・プログラム・パスワードを使用したアクセス試行を識別します。User_Probe_Name コンテキストは、FINGER、SMTP、VRFY、および SMTP EXPN に関連付けられているユーザー名をモニターします。アタッカーがこれらのデフォルト・アカウントを使用して、将来、ご使用のサーバーまたはその他のコンピューターにアクセスする可能性があります。	Password および SNMP_Community コンテキストの場合と同様に、X-Force データベースを使用して、ご使用のネットワークのシステムおよびソフトウェアに関連付けられているデフォルト・アカウントとデフォルト・パスワードのリストを作成できます。**参照情報:** デフォルト・パスワードについて詳しくは、X-Force データベース (http://xforce.iss.net) で SNMP を検索してください。

ユーザー定義イベントの正規表現

正規表現 (ストリング) は、ユーザー定義イベントに対してユーザーが指定したネットワーク・パケット (コンテキスト) 内のパターンを検出するためにアプライアンスが使用する、静的テキストと変数の組み合わせです。アプライアンスが単一の静的テキスト・ストリングより多くの項目を検出するようにするには、正規表現を使用します。

正規表現の制限

ユーザー定義の式には、いくつかの制限が適用されます。

- 正規表現の限度は 128 バイトです。
- 1 つのコンテキストの正規表現の数は 16 に制限されます。

これらの値は変更される可能性があります。最新の値については、IBM サポート・ポータル (http://www.ibm.com/support/entry/portal) を参照してください。技術情報 1435274 を検索してください。

正規表現ライブラリー

アプライアンスは、決定性有限オートマトンまたは DFA 正規表現と呼ばれる IBM Security のカスタム正規表現ライブラリーを使用します。

優先順位の変更

これらの正規表現では、括弧を使用して優先順位の標準的な順序を変更することができます。

例: 自然順の優先順位では、4+2*4 を 12 と解釈します。これは、自然順の優先順位では、掛け算が足し算より優先されるためです。しかし、括弧を使用してこの優先順位を変更することができます。例えば、(4+2)*4 を使用すると、答えは 12 ではなく 24 になります。この例では優先順位の数学的な用法を示していますが、ほかにも多くの非数値的用法があります。

参照情報: 優先順位の順序や、正規表現を使用する場合のその他の情報について詳しくは、「*詳説 正規表現 (オライリー・ジャパン)*」(編集者 Jeffrey E. Friedl および Andy Oram) を参照してください。

正規表現構文

以下の正規表現構文をユーザー定義イベントで使用できます。

メタ文字	説明
(r)	r に一致
x	x に一致
xr	x の後に r が続くものに一致
¥s	スペースかタブのどちらか (改行ではない) に一致
¥d	10 進数字に一致
¥"	二重引用符に一致
¥'	単一引用符に一致
¥¥	バックスラッシュに一致
¥n	改行 (ASCII NL または LF) に一致
¥r	キャリッジ・リターン (ASCII CR) に一致
¥t	水平タブ (ASCII HT) に一致
¥v	垂直タブ (ASCII VT) に一致
¥f	改ページ (ASCII FF) に一致
¥b	バックスペース (ASCII BS) に一致
¥a	ベル (ASCII BS) に一致
¥ooo	指定の 8 進数文字コードに一致
¥xhhh	指定の 16 進数文字コードに一致
.	改行以外の文字に一致
¥@	一致なし (受け入れ位置を示す)
“‘“	一致なし
[xy-z]	x、または y から z までの (x および y を含む) 何にでも一致 (文字クラス)

メタ文字	説明
[^xy-z]	x 以外、および y から z まで (x および y を含む) 以外に一致 • キャレットは先頭文字でなければなりません。先頭でない場合は、キャレット自体が文字の集合の一部になります。 • ダッシュを含める場合は、先頭文字としてダッシュを入力してください。
『テキスト』	内部にメタ文字があるかどうかに関係なく、文字通りにテキストに一致。テキストは全体で 1 単位としては扱われません。
r?	r に一致するか、一致なし (オプション演算子)
r*	ゼロ個以上の r が現れるものに一致 (クリーネ閉包)
r+	1 個以上の r が現れるものに一致 (正クリーネ閉包)
r{m,n}	少なくとも m 回、最大 n 回の r に一致 (反復演算子)
r|l	r または l のどちらかに一致 (代替演算子)
r/l	後に l が続く r にのみ一致 (先読み演算子)
^r	行頭の r にのみ一致 (bol アンカー)
r$	行末の r にのみ一致 (eol アンカー)
r, l	任意の正規表現に一致
m, n	整数に一致
x,y,z	任意の印刷可能 ASCII 文字またはエスケープ ASCII 文字に一致
テキスト	印刷可能 ASCII 文字またはエスケープ ASCII 文字のシーケンスに一致
ooo	3 文字までの 8 進数字のシーケンスに一致
hhh	16 進数字のシーケンスに一致

DNS 名検索のヒント

ピリオドはいかなる文字にも一致するワイルドカード文字であるため、DNS 名検索では円記号を使用して、ピリオドをエスケープしてください。**例**: www¥.ibm¥.com

チューニング・パラメーターの構成

チューニング・パラメーターは、グループ・レベルおよびサイト・レベルの不正侵入防御設定に影響を及ぼします。

SiteProtector で管理するアプライアンス・グループのチューニング・パラメーターを編集および構成します。IPS ローカル管理インターフェースを使用すると、特定のアプライアンスにサイト・レベルで影響を及ぼすパラメーターを表示できます。

アプライアンス・グループについては、以下のコンポーネントを調整できます。

- 不正侵入防御レスポンス
- 不正侵入防御セキュリティー・リスク
- ファイアウォール・ロギング

- 更新

デフォルト値

チューニング・パラメーターは、名前/値のペアで構成されます。名前/値のペアごとに、デフォルト値があります。例えば、パラメーター **np.firewall.log** は、有効にしたファイアウォール・ルールに一致するパケットの詳細を、ログに記録するかどうかを決定するパラメーターです。このパラメーターのデフォルト値は **on** です。

一般的に使用されるチューニング・パラメーターは、「Tuning Parameters (チューニング・パラメーター)」ページにリストされます。このページのリスト、および「Update Settings (更新設定)」ページの拡張パラメーターのリストに、チューニング・パラメーターを追加できます。どちらかのページでチューニング・パラメーターがリストされていない場合または有効になっていない場合でも、そのチューニング・パラメーターの動作は、そのパラメーターに定義されているデフォルト値によって制御されます。チューニング・パラメーターの動作を変更するには、そのチューニング・パラメーターを構成し、有効にして、目的の動作を含むデフォルト値を適用する必要があります。

OpenSignature の構成

OpenSignature の柔軟なルール言語を使用することにより、カスタマイズされ、パターン・マッチングのとれた IDS シグネチャーを作成し、IPS 製品でまだ先制対処の対象になっていない特定の脅威を検出することができます。この機能は、ルール・インタープリターとして IBM プロトコル分析モジュール (PAM) に組み込まれています。

OpenSignature 関連のリスク

カスタム・シグネチャー開発の機能は非常に広範囲に及びます。この柔軟性のゆえにリスクも加わります。作成されたルールまたはシグネチャーの品質が低いと、センサーのパフォーマンスに影響が出たり、その他のさまざまな結果をもたらす可能性があります。ユーザー独自のカスタム・シグネチャーを使用する場合のリスクには、以下のようなものがありますが、これに限られるわけではありません。

- アプライアンスのパフォーマンスが許容できないものになる。
- PAM が無限ループに陥る。
- 特定セグメントへのすべてのネットワーク・トラフィックがブロックされる (バイパスの有無に関係なく、インライン・モードの場合)。

注意:
OpenSignature を使用することにした場合、IBM Security ではアプライアンスのパフォーマンスを保証しません。この機能の有効化は、お客様の責任で行ってください。IBM カスタマー・サポートでは、ご使用の環境のカスタム・ルール作成またはトラブルシューティングのサポートはしておりません。カスタム・シグネチャーの作成についてサポートが必要な場合は、IBM プロフェッショナル・サービスにご連絡ください。

OpenSignature の構文

各カスタム・ルールの構文オプションは以下のとおりです。

(アクション): alert

(プロトコル): tcp、udp、icmp、ip

(IP およびネットマスク): 単一 IP アドレス (a.b.c.d)、IP アドレスの範囲 (a.b.c.d-w.x.y.z)、CIDR 表記を使用したネットワーク・アドレス (a.b.c.0/24)

重要: 不適切なフォーマット設定の OpenSignature ルールを使用すると、PAM 構成エラー・レスポンスを受け取る場合があります。ただし、PAM 構成エラー・レスポンスはデフォルトでは有効になっていません。この機能をセキュリティー・イベント・ポリシーで有効にすることを検討してください。それによって、OpenSignature ルールに不適切な構文があった場合に、必ず通知を受け取れるようになります。

否定演算子

否定演算子は、以下のように「!」で示されます。

alert tcp ! 192.168.1.0/24

「!」で指示されているもの以外が使用されると、アラートのプロンプトが出されます。

OpenSignatures パーサーの有効化

OpenSignature パーサーを有効にするには、以下の表に示す設定を使用してください。

設定	説明

名前	OpenSignature を有効にするには、以下のいずれかを入力します。
	
	`engine.opensignature.enabled`
	
	`pam.trons.enabled`

値	以下を入力します。 `true`

OpenSignature のデフォルト・レスポンス

すべての OpenSignature イベントのデフォルト・レスポンスは **DISPLAY** です。このデフォルト・レスポンスがあるため、IPS ローカル管理インターフェースと SiteProtector の両方が OpenSignature イベントを報告します。デフォルト・レスポンスを編集するには、チューニング・パラメーターを使用します。チューニング・パラメーターを使用すると、通知レスポンスやプロテクション・レスポンスなどの機能を構成することができます。

例:

```
np.opensignature.user.response=DISPLAY:WithoutRaw;EMAIL:admin,Block:Default
np.opensignature.response=block-connection'
```

ポリシーでの手順

IPS ローカル管理インターフェースの場合:

- 「**Secure Protection Settings (セキュア・プロテクション設定)**」 > 「**OpenSignatures**」

SiteProtector の場合:

- 「**OpenSignature Events (OpenSignature イベント)**」ポリシー

SNORT の構成

SNORT は、Network IPS アプライアンスに統合されているオープン・ソースの不正侵入防御および検出システムです。この統合システムをアプライアンスのネイティブのプロトコル分析モジュール (PAM) と併用して、ネットワークを不正侵入から保護することができます。

Network IPS 上の SNORT

注: 統合 SNORT システムに関する固有の構成情報については、IPS ローカル管理インターフェースまたは SiteProtector のヘルプ・システムを参照してください。

統合システムは、その独自の機能を提供するほか、SNORT アクティビティーに対する応答の送信も行います。統合システムでは、SNORT のイベント情報をリストし、それらのイベントの検疫ルールを生成します。システムは、TCP リセット・コマンドを使用した SNORT ルールをサポートします。これには、SNORT ルールのパフォーマンス・メトリックを報告するルール・プロファイル機能も含まれています。.

Network IPS アプライアンス上の統合 SNORT システムには、コマンド・ライン関数、構成コンテンツ、およびルールという 3 つのセクションがあります。

セクション	説明
コマンド・ライン	これにより、SNORT エンジンが実行可能になり、コマンド・ライン・オプション (ルール順序の処理、式、パケット・キャプチャー機能など) を指示できるようになります。
構成コンテンツ	構成コンテンツと、変数定義、プリプロセッサー、出力モジュール、および操作を制御するその他のオブジェクトが入っている構成ファイルが含まれています。この部分には、ルール・プロファイル・オプションも含まれています。
ルール	ルール・ファイルが含まれていて、ネットワーク上のぜい弱性を保護するために設計された SNORT ルールをリストしています。

リスク

SNORT の使用方法を理解していれば、システムは広範囲にわたる脅威に対抗するためのカスタマイズされた保護を提供するものとなります。しかし、正しく使用しないと、SNORT システムが原因でアプライアンスにエラーの負荷がかかり、パフォーマンスの妨げとなる場合があります。SNORT について十分な知識がない場合は、統合 SNORT システムを使用しないでください。IBM カスタマー・サポートでは、カスタム SNORT ルールと構成コンテンツの作成やトラブルシューティングのサポートはしておりません。

本書の情報を使用して、Network IPS アプライアンスの統合 SNORT システムを管理します。SNORT 自体の最新情報 (ルール、資料、およびコミュニティー・フォーラムを含む) については、https://www.snort.org にアクセスしてください。

考慮すべき事項

SNORT ルール

- 統合システムではルールの構文検査を実行しないので、適切な SNORT ルール構文チェッカーを使用して、ルールの整合性を確認してください。
- 1 つのルール・ファイルからインポートする SNORT ルールの数は 9000 以下にしてください。これより多くのルールを一度にインポートすると、IPS ローカル管理インターフェースおよび SiteProtector コンソールのパフォーマンスに影響します。

- インポートする SNORT ルール・ファイルのサイズは 5 MB 以下にしてください。. これより大きい SNORT ルール・ファイルをインポートすると、IPS ローカル管理インターフェースおよび SiteProtector コンソールのパフォーマンスに影響します。
- Network IPS アプライアンスは、SNORT の動的ルールの使用をサポートしていません。
- 統合システムは検疫ルールをサポートしているため、不要なトラフィックにアクティブに応答できます。また、SNORT TCP リセット・ルールの使用もサポートしているため、不要なトラフィックにアクティブに応答できます。
- 統合システムは、重複する SID と改訂番号を持つルールを処理する場合、最後に入力されたルールを用いてトラフィックを検査する方法を取ります。システムは、それより前のルールを無視します。
- 過剰な数のアラートを生む SNORT ルールを管理するには、構成ファイルでイベント・フィルターを使用します。

SNORT 構成

- Network IPS アプライアンスは、サード・パーティーのプリプロセッサーの使用をサポートしていません。
- 構成ファイル (デフォルトの構成ファイル、またはインポートされた構成ファイル) の設定とディレクトリーを確認して、ファイルがご使用の環境に適した機能を提供するように調整してください。
- SNORT.conf ファイルをインポートする場合は、ルール・パス変数を削除してください。ルール・パス変数の例:
  - `var PREPROC_RULE_PATH ../preproc_rules`
  - `var WHITE_LIST_PATH /etc/snort/rules`

パフォーマンス

- **重要:** SNORT ルール・プロファイルは SNORT エンジンのパフォーマンスに影響を及ぼす場合があるため、必要なときのみ使用するようにしてください。
- SNORT ルール・アクティビティーが高くなると、アプライアンスに負荷がかかる場合があります。セキュアで未分析のスループット統計を使用して、ご使用の SNORT ルール・アクティビティーのキャパシティーを判別してください。これらのスループット統計は、「ネットワーク・ダッシュボード」に表示されます。セキュア・トラフィックの値が低い場合と未分析のトラフィックの値が高い場合は、SNORT ルール・アクティビティーが高くなっている可能性を示します。

一般

- 統合 SNORT システムがインラインではないため、統合システムは Block レスポンスをサポートしていません。このシステムは IDS モードです。
- SNORT システムは、不要な TCP 接続に応答して、TCP リセット・ポートを通じて TCP リセットを送信します。
- SNORT システムは、不要な UDP 接続に応答して、TCP リセット・ポートを通じて ICMP ポート到達不能メッセージを送信します。

SNORT および PAM

SNORT および PAM (プロトコル分析モジュール) は、同じデータ・パケットをそれぞれ無関係に分析します。この設計により、それぞれのシステムから予期せぬ動作が起こる場合があります。

アプライアンスは、パケットの単一キューを PAM および統合 SNORT システムに配信します。アプライアンスは、このキューには処理順序を適用しません。最初にパケットを取得したシステムがそのパケットを最初に分析します。最初のシステムがパケットを変更するかまたはパケットに応答すると、次に 2 番目の

システムが変更されたパッケージを分析するか、すでに応答されているパケットに対して応答します。この関係の結果、予期しないイベントまたは検疫ルールが表示される場合があります。

アクション	結果
PAM の分析が先の場合	PAM が SNORT より先にパケットを分析し、PAM がパケットを除去します。SNORT が同じパケットを後で分析し、イベントを生成します。予期しない結果として、PAM がすでに除去したパケットから SNORT が不必要なイベントを生成することになります。
SNORT の分析が先の場合	SNORT が PAM より先にパケットを分析し、SNORT がイベントを生成します。このイベントから、検疫ルールが作成されます。このパケットは、後で PAM が分析後に除去するパケットですが、PAM はまだこのパケットを取得していません。SNORT は、PAM がまだ応答していないために、同じパケットを検出します。SNORT が別のイベントを生成し、別の検疫ルールが作成されます。後になって、PAM がこのパケットを分析し、トラフィックを除去します。予期しない結果として、PAM がパケットに応答する前に、SNORT が重複イベントを生成し、重複する検疫ルールが作成されることになります。

SNORT とハイアベイラビリティ (HA) モード

SNORT システムの構成オプションとして、HA モードでミラーリングされたポートを検査するか検査しないかを選択できます。 以下の表に、各オプションの動作の概略を示します。

オプション	アクション
検査 (有効)	HA ペア内のアプライアンスで稼働中の SNORT システムは、ミラーリングされたポートからのパケットを検査します。この動作は、インライン・プロテクション・モードまたはインライン・シミュレーション・モードで稼働中のペアに適用されます。このオプションでは、グローバル・レスポンスと SiteProtector アラートの重複の可能性が増大します。 ただし、システムはミラーリングされたポートからのパケットも含めてすべてのパケットを分析することになるため、このオプションでは、SNORT システムが攻撃を見落とす可能性が減少します。
検査しない (無効)	HA ペア内のアプライアンスで稼働中の SNORT システムは、ミラーリングされたポートからのパケットを検査しません。この動作は、インライン・プロテクション・モードまたはインライン・シミュレーション・モードで稼働中のペアに適用されます。このオプションでは、グローバル・レスポンスと SiteProtector アラートの重複の可能性が最小になります。 ただし、このオプションでは、SNORT システムがすべてのトラフィックを分析するための機能が制限されます。 **重要:** このオプションを無効にすると、SNORT システムのどれかが攻撃を見落とす可能性が生まれます。また、SNORT イベントから生成された検疫ルールは、HA ペア内のアプライアンス上で非同期となっている可能性があります。

SNORT エラーのトラブルシューティング

統合 SNORT システムは、一度に 1 つずつ、エラーを識別します。このプロセス・フローのため、SNORT ポリシーを正常に適用するには個々のエラーをトラブルシューティングして修正する必要があります。

エラー: SNORT エラーは、統合システムが無効とみなした構成コンテンツまたはルールを検出したときに発生します。IPS ローカル管理インターフェースおよび SiteProtector では、ユーザーがエラーのある設定を実行依頼した場合に、アプライアンスは、ポリシーの適用に失敗したことを示すメッセージを「**SNORT Configuration (SNORT 構成)**」タブまたは「**SNORT Rules (SNORT ルール)**」タブに表示します。このエラー・メッセージには、問題の修正に役立つように、SNORT からの情報も含まれています。SNORT ルール・エラーの場合、メッセージには SID およびメッセージ・ストリングがリストされます。システムは、ポリシー障害を重要イベントとして報告します。

ヒント: SNORT ルールに対して構文チェッカーを使用すると、無効なルールの数を減らすのに役立ちます。

トラブルシューティング: 統合 SNORT システムのトラブルシューティングは、 統合 SNORT システムが一度に 1 エラーずつ識別するため、反復プロセスです。システムは、エラーを検出すると、ポリシー設定の適用に失敗し、障害を報告します。ポリシー設定を正常に適用するには、その前にエラーのトラブルシューティングを行う必要があります。エラーを修正した後で、設定を再適用する必要があります。システムは、構成コンテンツまたはルールにそれ以上のエラーがないことを確認すると、ポリシー設定を正常に再適用します。しかし、別のエラーを検出すると、システムは個々のエラーについてこのプロセスを繰り返します。

注: SNORT エンジンの正常性状況を調べるには、「**Monitor Health and Statistics (正常性および統計のモニター)**」 > 「**セキュリティー**」 > 「**ダッシュボード**」に進みます。

SnEP

SNORT イベント処理プログラム (SnEP) は、SNORT システムからエラーを拾い出して、SNORT エラーを以下の方法で報告します。

- SnEP が重要イベントを生成します。SnEP は、そのイベントを [SNORT ERROR] として識別し、SNORT がエラー・メッセージ・ストリングを指示します。
- SnEP がエラーをシステムのログに記録します。
- SnEP が SiteProtector にアラートを送信します。

SNORT および検疫機能

検疫ルールを構成し、統合 SNORT システムによって識別された疑わしいアクティビティーから生成されたイベントに対して、Quarantine レスポンスを送信します。Quarantine レスポンスは、システムがイベントを検出すると、ワームやトロイの木馬などの侵入者をブロックします。検疫ルールは手動で追加され、検出された侵入者イベントに応答して動的に生成されます。このルールにより、ワームの拡散が防止され、バックドアやトロイの木馬に感染したシステムへのアクセスが拒否されます。このルールは、攻撃後のデータ漏えいの防止にも役立ちます。

SNORT ルールのインポートと削除

Network IPS アプライアンスは、カスタマイズされた設定とプログラムされた動作に従って、ルール・ファイルから SNORT ルールをインポートして管理します。

インポート済みルールの属性のカスタマイズ: ルール・ファイルから SNORT ルールをインポートすると、アプライアンスはそれらのルールをファイル名別にグループ化します。インポート済みのルールの以下の属性をカスタマイズできます。

- 有効
- ルール・ストリング

  注: ルール・ストリング属性を変更できます。ただし、更新済みバージョンのルール・ファイルをインポートした場合、アプライアンスは変更を再適用しません。この属性への変更は失われます。
- コメント
- 表示
- 重要度
- レスポンス (メール、検疫、SNMP、ユーザー指定)

Network IPS アプライアンスは、これらのカスタマイズ済み属性を保管して、更新済みファイルをインポートした後で (ルール・ストリング以外の) すべてを再適用できるようにします。

更新または変更済みのルール・ファイルの再インポート: 特定の状況では更新および変更を含むルール・ファイルの再インポートが必要になるため、アプライアンスはカスタマイズ済みの属性を保管します。アプライアンスは、再インポートされたファイルのルールを以下の方法で処理します。

- 更新済みファイルに対してルールが新規であれば、アプライアンスはそのルールをグループに追加します。
- 更新済みファイルからルールが削除されていれば、アプライアンスはそのルールをグループから削除します。そのルールがまだ必要な場合は、「追加」アイコンを使用してルールを追加する必要があります。
- ルールが更新済みファイルにも継続して存在していれば、アプライアンスはカスタマイズ済みの属性を更新バージョンのルールに適用します。

注: 統合システムは、重複する SID と改訂番号を持つルールを処理する場合、最後に入力されたルールを用いてトラフィックを検査する方法を取ります。システムは、それより前のルールを無視します。

SNORT ルールの削除: アプライアンスでは、過去のルールおよび削除済みルールの記録を保持しません。. ルールを削除した後、その削除済みルールが入ったルール・ファイルを再インポートすると、アプライアンスはそのルールを再び SNORT ポリシーに追加します。

SNORT ルール・プロファイル

重要: SNORT ルール・プロファイル機能は、SNORT エンジンのパフォーマンスに影響を及ぼす可能性があるため、必要なときのみ使用するようにしてください。

SNORT ルール・プロファイルを使用して、SNORT ルールのパフォーマンスを分析し、発生する可能性のあるパフォーマンスの問題をトラブルシューティングします。これを有効にすると、アプライアンスはユーザーが表示またはダウンロード可能な SNORT ルール・プロファイル・ファイルを作成します。このファイルには、最も攻撃数が多いルールのパフォーマンス統計が含まれています。SNORT ルール・プロファイルに関する考慮事項をいくつか以下に示します。

- この機能には、IPS ローカル管理インターフェースを使用した場合のみアクセスできます。
- この機能を実行するには、SNORT エンジンと SNORT ルール・プロファイルを有効にする必要があります。
- この機能には、コンテンツやプリプロセッサーを入力する必要はありません。 Network IPS アプライアンスに、この機能がすでに含まれています。

SNORT ルール・プロファイル・ファイルは以下の統計別にソートできます。

統計	説明
検査	SNORT エンジンが初期分析を実行してトラフィックをグループ化および事前選別した後で、SNORT エンジンがルール・オプションを検査した回数。
一致	SNORT エンジンがすべてのルール・オプションに一致したトラフィックを検出した回数。
一致なし	SNORT エンジンがどのルール・オプションにも一致するトラフィックがないことを検出した回数。
平均ティック (平均/検査)	SNORT エンジンがリストされたルールに照らして各パケットを検査するのに要した平均時間。

統計	説明
一致当たりの平均ティック (平均/一致)	SNORT エンジンがすべてのルール・オプションに一致する各パケットを検査するのに要した平均時間。
一致なし当たりの平均ティック (平均/一致なし)	SNORT エンジンがイベントを生成しなかった各パケットを検査するのに要した平均時間。 **注:** この統計は、クリーン・トラフィックの検査に費やされた浪費時間を表します。
合計ティック	最も多い処理時間を使用したルール。

SNORT ルール・プロファイル統計について詳しくは、https://www.snort.org を参照してください。

サポートされない SNORT 構成オプション

Network IPS アプライアンスは、SNORT 構成の以下のオプションをサポートしていません。

config alert_with_interface_name
config alertfile
config chroot
config daemon
config daq
config daq_dir
config daq_list
config daq_mode
config daq_var
config interface
config logdir
config no_promisc
config nolog
config pkt_count
config policy_mode
config profile_rules
config quiet
config response
config snaplen
config umask
config min_ttl
config new_ttl
include
output
preprocessor normalize_ip4
preprocessor normalize_ip6
preprocessor normalize_icmp4
preprocessor normalize_icmp6
preprocessor normalize_tcp

SNORT 式の例

コマンド・ライン領域 (「**SNORT Execution (SNORT 実行)**」タブにあります) で、SNORT 式を設定します。 SNORT 式は TCPDump 式に似ています。式には 1 つ以上のプリミティブがあります。プリミティブには、1 つ以上の修飾子が前に付いた ID (名前または番号) が含まれています。式の主要な 3 つの修飾子は、**type**、**dir**、および **proto** です。

修飾子	タイプ
type	ID 名または番号の参照先を識別します。例: • **host**: IP アドレスに基づきトラフィックを探します。**host 1.2.3.4** • **net**: CIDR 表記を使用してネットワーク全体をキャプチャーします。**net 1.2.3.0/24** • **port**: 特定のポートで出入りするトラフィックを検査します。**port 3389** • **portrange**: ある範囲内のすべてのポートのトラフィックを検査します。**portrange 21-23**
dir	方向を指定します。例: • **src**: ソースからのトラフィックのみを検出し、ホスト会話の片側を除去します。**src 2.3.4.5** • **dst**: 宛先からのトラフィックのみを検出し、ホスト会話の片側を除去します。**dst 3.4.5.6**
proto	マッチングを特定のプロトコルに制限します。**proto** と入力する必要はありません。例: • **tcp**: マッチングを TCP トラフィックに制限します。**tcp** • **icmp**: マッチングを ICMP トラフィックに制限します。**icmp** • **udp**: マッチングを UDP トラフィックに制限します。**udp**

3 つの修飾子をすべて組み合わせた例:

- **src port 1025 and tcp**
- **udp and src port 53**

ポリシーでの手順

IPS ローカル管理インターフェースの場合:

- 「**Secure Protection Settings (セキュア・プロテクション設定)**」 > 「**Advanced IPS (拡張 IPS)**」 > 「**SNORT Configuration and Rules (SNORT 構成およびルール)**」
- 「**Review Analysis and Diagnostics (分析および診断の確認)**」 > 「**診断**」 > 「**SNORT Rule Profiling (SNORT ルール・プロファイル)**」

SiteProtector の場合: 「**SNORT Configuration and Rules (SNORT 構成およびルール)**」ポリシー

レスポンス・フィルターの構成

レスポンス・フィルターを使用して、アプライアンスがレスポンスするイベントの数および管理コンソールに報告されるイベントの数を制御します。

レスポンス・フィルターを使用して以下を行うことができます。

- フィルターに指定されたネットワーク基準に基づき起動するセキュリティー・イベントのレスポンスを構成する。
- アプライアンスがコンソールに報告するセキュリティー・イベントの数を減らす。

例

セキュアで信頼できるネットワーク上のホスト、または他の何らかの理由でアプライアンスで無視したいホストがある場合は、Ignore レスポンスを有効にしたレスポンス・フィルターを使用できます。

レスポンス・フィルターの属性

レスポンス・フィルターには以下の構成可能な属性があります。

- インターフェース
- 仮想 LAN (VLAN)
- ソースまたはターゲットの IP アドレス
- ソースまたはターゲットのポート番号 (全ポートまたは特定のサービスに関連付けられた個別ポート) またはICMP タイプ/コード (いずれか片方が使用されます)。

フィルターおよびその他のイベント

アプライアンスは、レスポンス・フィルターに一致するトラフィックを検出すると、そのフィルターに指定されたレスポンスを実行します。それ以外の場合は、アプライアンスはイベント自体に指定されたレスポンスを実行します。

注: セキュリティー・イベントを無効にすると、それに対応するレスポンス・フィルターも無効になります。

レスポンス・フィルターの順序

レスポンス・フィルターはルール順序に従います。例えば、複数のフィルターを同じセキュリティー・イベントに追加した場合、アプライアンスは最初に一致にしたものに対してレスポンスを実行します。アプライアンスは、フィルターのリストを上から下への順に読み取ります。

ポリシーでの手順

IPS ローカル管理インターフェースの場合:

- 「**Secure Protection Settings (セキュア・プロテクション設定)**」 > 「**Response Tuning (レスポンス・チューニング)**」 > 「**Response Filters (レスポンス・フィルター)**」

SiteProtector の場合:

- 「**Response Filters (レスポンス・フィルター)**」ポリシー

LEEF システム・ログの構成

ご使用のネットワークで異なるコンポーネントを統合する際に役立つように、このアプライアンスでは、ログ・イベント拡張フォーマット (LEEF) を使用してセキュリティー・インシデント・イベント・マネージャー (SIEM) にイベント情報を送信することができます。

このタスクについて

この機能を有効にすると、アプライアンスは IPS イベント、SNORT イベント、正常性アラート・イベント、およびシステム・アラート・イベントを SIEM に送信するため LEEF に変換します。「**Review Analysis and Diagnostics (分析および診断の確認)**」 > 「**ダウンロード**」 > 「**Logs and Packet Captures (ログおよびパケットのキャプチャー)**」で、IPS ローカル管理インターフェースからログ・ファイルを取得することができます。

注: IPS イベントには、セキュリティー・イベント、接続イベント、ユーザー定義イベント、および OpenSignatures ポリシーのイベントが含まれます。

この機能は、Q1 Labs で開発された QRadar SIEM を使用してテストされています。詳しくは、http://q1labs.com を参照してください。Q1 Labs のお客様は、http://partners.q1labs.com にアクセスして DocCentral にサインインすることで、資料を表示できます。

手順

1. LEEF システム・ログ機能を有効にします。
   a. IPS ローカル管理インターフェースで、「**Secure Protection Settings (セキュア・プロテクション設定)**」 > 「**Advanced IPS (拡張 IPS)**」 > 「**Tuning Parameters (チューニング・パラメーター)**」に進みます。「SiteProtector Management (SiteProtector 管理)」で、「**Tuning Parameters (チューニング・パラメーター)**」ポリシーを選択します。
   b. チューニング・パラメーター **crm.leef.enabled** を追加して、それを「**True**」に設定します。
2. オプション: LEEF システム・ログ・ファイルのサイズを設定します。
   a. IPS ローカル管理インターフェースで、「**Secure Protection Settings (セキュア・プロテクション設定)**」 > 「**Advanced IPS (拡張 IPS)**」 > 「**Tuning Parameters (チューニング・パラメーター)**」に進みます。「SiteProtector Management (SiteProtector 管理)」で、「**Tuning Parameters (チューニング・パラメーター)**」ポリシーを選択します。
   b. チューニング・パラメーター **crm.leef.logsize** を追加して、それを **1 から 100** MB の間の数値に設定します。デフォルトは **10** MB です。
3. SIEM と通信するには Secure Shell (SSH) プロトコルを使用します。アプライアンスから LEEF システム・ログを取得するには、セキュア・コピー (SCP) コマンドを使用するように SIEM を構成します。ログ・ファイルは `/var/iss/leef.log` にあります。QRadar SIEM は、15 分ごとに LEEF システム・ログを取得します。

第 6 章 X-Force プロテクション・モジュール

IBM X-Force の研究開発チームは、最新の脅威の傾向を調査し、監視しています。チームでは、お客様のネットワークを脅威から保護するために、ご使用のアプライアンスと連携するセキュリティー・モジュールおよびコンテンツを配信しています。

PAM

PAM (Protocol Analysis Module: プロトコル分析モジュール) は、ネットワークを不正侵入から保護するためにアプライアンスが使用する情報を提供します。PAM は、包括的な不正侵入リストに対する処理仕様を格納したデータベースです。 IBM Security は、X-Press Update (XPU) を使用して PAM 情報を最新状態に保ちます。X-Press Update は、IPS ローカル管理インターフェースまたは SiteProtector の X-Press Update Server を介して適用できます。PAM を制御するには、チューニング・パラメーター構成を使用します。

X-Force デフォルト・ブロッキングの使用

X-Force デフォルト・ブロッキングを使用すると、X-Force 推奨のイベントに対して Block レスポンスおよび Quarantine レスポンスが自動的に有効になります。アプライアンスは、「X-Force Virtual Patch」ページで構成されたオプションに応じて、推奨設定を有効または無効にします。以下のオプションがあります。

表 4. X-Force のオプションおよびアクション

オプション	有効な場合のアクション
常時	X-Press Update (XPU) を適用する際、アプライアンスは XPU で定義されている新規イベントに対して Block レスポンスおよび Quarantine レスポンスを有効にします。
Through XPU (この XPU まで)	XPU を適用する際に、アプライアンスは指定の XPU バージョン (そのバージョンを含む) までに定義された新規イベントに Block レスポンスおよび Quarantine レスポンスを設定します。 XPU コンテンツ更新の適用を制御するには、このオプションを使用します。テスト済みの XPU バージョンにこのオプションを設定すると、アプライアンスがそれより後の XPU バージョンを適用することはありません。まず最初に、このオプションを使用して X-Force の推奨事項を検討し、新規イベントに適用するかしないかを決定することができます。
なし	XPU を適用する際に、アプライアンスは XPU で定義されている新規イベントに対して、Block レスポンスおよび Quarantine レスポンスを設定しません。

ポリシーでの手順

IPS ローカル管理インターフェースの場合:

- 「**Secure Protection Settings (セキュア・プロテクション設定)** > 「**セキュリティー・モジュール**」 > 「**X-Force Virtual Patch**」

SiteProtector の場合:

- 「**Shared Objects (共有オブジェクト)**」 > 「**X-Force Virtual Patch**」ポリシー

データ損失の防止シグネチャーの使用

個人識別可能情報 (Personal Identifiable Information: PII) やその他の、ネットワーク内で移動したりネットワーク外部に移動している機密情報のパケットを検査および分析するには、「データ損失の防止」機能を使用します。ご使用のアプライアンスの定義済みイベント、ユーザー組み合わせイベント、およびユーザー定義イベントで、この機能を使用できます。

「データ損失の防止」の仕組み

データ損失の防止では、データ・パケットがネットワーク上を移動するときにそれらのパケットを検査し、それによって、多くのタイプの機密情報の送信を検出します。この機能では、さまざまなプロトコルおよびコンテンツ内のパターン (クレジット・カード番号、名前、日付、金額、E メール・アドレス、社会保障番号、アメリカ合衆国の電話番号、およびアメリカ合衆国の住所など) のパターンを識別できます。

さらに、事前設定シグネチャーに加えて、ユーザー定義のカスタム・シグネチャーを 8 つまで作成できます。また、事前設定シグネチャーとユーザー定義シグネチャーを組み合わせてグループ化することで、ユーザー組み合わせシグネチャーを 8 つまで作成できます。ユーザー組み合わせシグネチャーは、単一データ・セットとして機能します。

パフォーマンスとチューニング

すべてのデータ損失の防止シグネチャーおよびプロトコルをオンにすると、ネットワーク・パフォーマンスに何らかの影響が発生する可能性があります。このレベルのプロテクションを必要とする企業はほとんどなく、ユーザーが必要なシグネチャーおよびプロトコルのサブセットを識別するにつれて、パフォーマンスの数値は一般に向上します。

データ損失の防止は、監査またはブロッキングのために使用できます。ほとんどの企業は、ポリシーのチューニング中に監査モードを使用します。この方法は、セキュリティー・マネージャーが事業運営を中断せずにブロックできる*可能性のある* データの種類を理解するために役立ちます。別の企業では、監査モードで十分であると感じているため、ブロッキング・モードのデプロイは計画していない場合もあります。

特定のシグネチャーやコンテンツ・タイプに基づく大量のイベントが現れることがあります。「データ損失の防止」ポリシーを変更して、イベント数を削減できます。

注: ポリシーに関する支援が必要な場合は、専門のセキュリティー・コンサルタントがお手伝いします。

ポリシーでの手順

IPS ローカル管理インターフェースの場合:

- 「**Secure Protection Settings (セキュア・プロテクション設定)** > 「**セキュリティー・モジュール**」 > 「**データ損失の防止**」

SiteProtector の場合:

- 「**データ損失の防止**」ポリシー

Web アプリケーション・プロテクションの使用

Web アプリケーション・プロテクション (WAP) は、IBM Security プロトコル分析モジュール (PAM) エンジンからの攻撃、監査、およびパラメーター名 (キーワード) を使用して、Webアプリケーション・セキュリティー攻撃に対する全体的な保護を提供します。

WAP は、以下のタイプの Web アプリケーション・セキュリティー攻撃からネットワークを保護するために役立ちます。

攻撃	説明
注入攻撃	アタッカーがプログラムまたは照会にコードを注入したり、コンピューターにマルウェアを注入できるようにして、データベースの読み取りまたは変更、または Web サイトのデータの変更を可能にするリモート・コマンドを実行できるようにします。
悪意のあるファイル実行	PHP スクリプト言語の SMB ファイル・ラッパーを使用して、リモート側でのコードの実行、リモート側でのルート・キットのインストール、システム全体のセキュリティー侵害、Windows システムの内部システムのセキュリティー侵害をアタッカーが実行できるようにします。
クロスサイト要求偽造 (CSRF)	Web サイトが信頼するユーザーから、無許可のコマンドを送信します。
情報開示攻撃	Web サイトに関するシステム固有の情報 (ソフトウェア配布、バージョン番号、パッチ・レベルなど) を取得しようとします。取得される情報には、バックアップ・ファイルまたは一時ファイルがある場所なども含まれる場合があります。
パス・トラバーサル攻撃	Web 文書のルート・ディレクトリーまたは CGI ルート・ディレクトリーの外部にあるファイル、ディレクトリー、およびコマンドへの強制アクセスを実行します。
認証	Web サイトがユーザー、サービス、またはアプリケーションの ID の検証に使用する認証プロセスをターゲットとして、それを利用しようとします。
バッファー・オーバーフロー	バッファーのオーバーフローを引き起こすために、ターゲットを過剰なデータであふれさせます。その後、アタッカーは、コンピューターに対してリモート・シェルを実行し、攻撃対象のアプリケーションに付与されているものと同じシステム特権を取得します。
ブルート・フォース	試行錯誤方式を使用して、個人のユーザー名、パスワード、クレジット・カード番号、または暗号鍵をプログラムで推測します。
ディレクトリー索引付け攻撃	通常の基本ファイルが存在していない場合に要求されたディレクトリー内のすべてのファイルをリストする Web サーバーの機能を不正利用します。
各種攻撃	キャッシュ・サーバーまたは Web ブラウザーに、重要で機密の可能性のあるユーザー固有の情報の開示を強制することによって、ぜい弱な Web サーバーを不正利用します。

PAM 制御のセキュリティー・イベントおよびレスポンス・フィルター

プロトコル分析モジュール (PAM) は、X-Force Virtual Patch 推奨事項を制御します。これは、PAM が多くのセキュリティー・イベントを制御することを意味します。PAM は、Web アプリケーション・プロテクション (WAP) ポリシー内にある一部のセキュリティー・イベントに構成された設定をオーバーライドします。PAM が制御するセキュリティー・イベントの WAP ポリシー設定をオーバーライドするには、レスポンス・フィルターを使用します。 レスポンス・フィルターは PAM 設定をオーバーライドするので、WAP ポリシーはネットワークの必要性に従ってアクティビティーに応答するようになります。

重要: PAM が制御するWAP ポリシー設定を、「Web Application Protection (Web アプリケーション・プロテクション)」ページまたは「セキュリティー・イベント」ページから変更することはできません。レスポンス・フィルターを使用する必要があります。

例: ブロックから無視への変更

PAM では、**HTTP_Unknown_Protocol** イベント・パラメーターが Block レスポンスを使用するように構成されていますが、このイベントが Ignore レスポンスを使用するようにしたいとします。「セキュリティー・イベント」ページに進み、**HTTP_Unknown_Protocol** パラメーターを探してそれを変更しようとしたところ、このパラメーターがありません。そこで、「Response Filter (レスポンス・フィルター)」ページに進んで、このイベント名のレスポンス・フィルターを作成します。次に、「**イベントを無視**」チェック・ボックスを選択します。レスポンス・フィルター設定により PAM 設定がオーバーライドされ、**HTTP_Unknown_Protocol** イベント・パラメーターが今度は「イベントの無視」を使用するようになります。

例: 有効から無効への変更

PAM では **HTTP_Get_CreateTable** パラメーターが有効になっていますが、これはご使用のネットワークの必要性に合わないので、無効にしたいとします。「セキュリティー・イベント」ページに進み、**HTTP_Get_CreateTable** パラメーターを探してそれを再構成しようとしたところ、このパラメーターがありません。そこで、「Response Filter (レスポンス・フィルター)」ページに進んで、このイベント名のレスポンス・フィルターを作成します。次に、「**有効**」 チェック・ボックスをクリアします。このレスポンス・フィルター設定により、PAM 設定がオーバーライドされ、**HTTP_Get_CreateTable** パラメーターが無効になりました。

ポリシーでの手順

IPS ローカル管理インターフェースの場合:

- 「**Secure Protection Settings (セキュア・プロテクション設定)**」 > 「**セキュリティー・モジュール**」 > 「**Web Application Protection (Web アプリケーション・プロテクション)**」

SiteProtector の場合:

- 「**Web Application Protection (Web アプリケーション・プロテクション)**」ポリシー

第 7 章 プロテクション・ドメインの使用

カスタム・プロテクション・ドメインを使用すると、1 つのアプライアンスで複数のネットワーク・セグメントをモニターすることができます。これは、これらのネットワーク・セグメントが異なるセキュリティー設定を必要とする場合でも可能です。プロテクション・ドメインは、仮想センサーのように、まるで複数のアプライアンスがネットワークをモニターしているかのように機能します。カスタム・プロテクション・ドメインを使用することで、異なるネットワーク・セグメントに異なるセキュリティー設定を定義することができます。

グローバル・プロテクション・ドメイン

各アプライアンスにはグローバル・プロテクション・ドメインがあり、これは削除できません。イベントはすべて、グローバル・プロテクション・ドメインの下にリストされます。ネットワークの全セグメントにわたって適用するイベントを構成する場合は、グローバル・ポリシーを使用してください。アプライアンスでグローバル・ポリシーを使用する場合、アプライアンスは、ネットワークの全領域について同じ方法でイベントを処理します。

ネットワーク上の特定のセグメントに対するポリシーを構成する場合は、各セグメントにプロテクション・ドメインを作成します。

注: グローバル・プロテクション・ドメインでは、フラッディング・イベントおよびスイープ・イベントに対するルールを常に有効にしてください。フラッディングおよびスイープ攻撃は複数のターゲットを対象にするのが一般的であり、これらのターゲットは複数のプロテクション・ドメインにわたって分散している可能性があります。これらのルールをグローバル・プロテクション・ドメインで有効にしておくことで、この種の攻撃を確実に検出して正しく報告するのに役立ちます。

プロテクション・ドメインの追加

単一アプライアンスを使用して、さまざまなセキュリティー要件を持つ複数のネットワーク・セグメントをモニターするには、カスタム・プロテクション・ドメインを作成してください。これらのプロテクション・ドメインを使用して、異なるネットワーク・セグメントに異なるセキュリティー・ポリシーを適用します。

ポート、VLAN、または IP アドレス範囲を使用して、プロテクション・ドメインを定義できます。

ポリシーでの手順

IPS ローカル管理インターフェースの場合:

- **「Secure Protection Settings (セキュア・プロテクション設定)」 > 「Advanced IPS (拡張 IPS)」 > 「プロテクション・ドメイン」**

SiteProtector の場合:

- **「Shared Objects (共有オブジェクト)」 > 「プロテクション・ドメイン」**

プロテクション・ドメインの操作

プロテクション・ドメインを使用して、単一アプライアンスでモニターするさまざまなネットワーク・セグメントのセキュリティー・ポリシーおよびユーザー定義ポリシーを定義します。

プロテクション・ドメインを使用するポリシー

グローバル・プロテクション・ドメインまたはカスタム・プロテクション・ドメインを、以下のポリシーで使用できます。

- セキュリティー・イベント
- ユーザー定義イベント
- データ損失の防止
- Web アプリケーション・プロテクション
- レスポンス・フィルター

プロテクション・ドメインおよびイベント

デフォルトでは、アプライアンスはグローバル・プロテクション・ドメインを使用してセキュリティーを管理します。ご使用のネットワークで、さまざまなセグメント用に異なるセキュリティー設定が必要な場合は、カスタム・プロテクション・ドメインを定義し、必要に応じて各ドメインにセキュリティー設定を割り当ててください。

注:

- 異なるコンテキストおよび照会ストリングを持つイベントに同じ名前を使用しないでください。同じ名前を使用すると、発生したイベントの判別が難しくなります。
- 同じ名前のイベントが 2 つあり、一方をグローバル・プロテクション・ドメインに割り当て、もう一方をカスタム・プロテクション・ドメインに割り当てた場合、定義済みのネットワーク・セグメント内でアラート詳細が発生すると、カスタム・ドメインに割り当てられたイベントのみがアラートを生成します。それ以外の場合は、アプライアンスはグローバル・プロテクション・ドメインに割り当てられたイベントを報告します。
- 同一のユーザー定義イベントが 2 つあってそれらの名前が異なる場合、各イベントが独自のアラートを生成します。

プロテクション・ドメインと IPv6 サポート

IPv6 アドレスまたはアドレス範囲を指定して、プロテクション・ドメインを定義することができます。プロテクション・ドメインは、IPv6 環境で完全にサポートされていますが、使用しにくくなる可能性があります。例えば、ラップトップ・コンピューターなどの携帯用の資産は、ネットワークに接続する場所に応じて、複数の IPv6 アドレスを持つ可能性があります。

プロテクション・ドメインのベスト・プラクティス

プロテクション・ドメインは、それを理解して正しく使用すると、ネットワークの保護を拡張する貴重なツールとなります。

グローバル・プロテクション・ドメインの使用を推奨

単一アプライアンスによって保護されたすべてのネットワーク・セグメントにセキュリティー設定を適用するには、グローバル・プロテクション・ドメインを使用します。この方法は、同じポリシーを複数のプロテクション・ドメインに設定するより早くて簡単です。

フラッディング攻撃およびスイープ攻撃からの保護

ある種のフラッディング攻撃およびスイープ攻撃は、カスタム・プロテクション・ドメインでは認識されない場合があります。これらの攻撃は複数のターゲットを対象にするのが一般的であり、それらのターゲットは複数のプロテクション・ドメイン間に分散している可能性があります。これらのイベントをグローバル・プロテクション・ドメインで有効にしておくことで、この種の攻撃を確実に検出して正しく報告するのに役立ちます。

プロテクション・ドメインの削除

プロテクション・ドメインを削除しても、そのプロテクション・ドメインに割り当てられたユーザー定義イベント、セキュリティー・イベント、およびレスポンス・フィルターはアクティブなまま残り、削除されたプロテクション・ドメインに関連付けられたイベントは起動されたままになることがあります。プロテクション・ドメインを削除する前に、そのプロテクション・ドメインに関連付けられているすべてのユーザー定義イベント、セキュリティー・イベント、およびレスポンス・フィルターを削除または再割り当てしてください。

第 8 章 ハイアベイラビリティのためのアプライアンスの構成

ハイアベイラビリティ (HA) サポートは、2 つの連携するアプライアンスの間の構成配置です。HA モードを使用すると、2 つの同等のアプライアンスが既存のハイアベイラビリティ環境で連携して、ネットワークに追加のプロテクションを提供することができます。接続されて HA モードで動作するように構成された 2 つのアプライアンスを HA パートナーまたは HA ペアと呼びます。

HA と SiteProtector の管理

HA 構成は IPS ローカル管理インターフェースで表示できますが、インライン HA 構成のアプライアンスを管理するには SiteProtector を使用する必要があります。HA ペアの両方のアプライアンスは同一の SiteProtector グループに入っていなければなりません。それにより、SiteProtector は、XPU およびポリシー更新も含め、アプライアンス更新を同期化できます。

コンテンツ更新とファームウェア更新を順次に適用できるので、両方のアプライアンスがフェイルクローズに構成されている場合は特に、ネットワーク接続性を維持できるように片方のアプライアンスを常に作動可能な状態にしておくことができます。

各アプライアンスは固有の ID を使用して SiteProtector に報告を送ります。

ライセンス登録

HA 構成のライセンスは、非 HA アプライアンスのライセンスと同様です。個別アプライアンスごとに、専用のライセンスが必要です。SiteProtector を使用して HA アプライアンスを管理している場合、各アプライアンスが SiteProtector からのライセンスを要求します。

制限

HA モードでは、ファイアウォール・ルールの一部としてインターフェース・パラメーターを使用することができません。プロテクション・ドメインをインターフェースに基づいて定義することはできません。HA 環境では同じトラフィックが異なるインターフェース上を流れる場合があるため、インターフェース・パラメーターを使用すると、HA パートナー・アプライアンスが非同期になる可能性があります。

重要: プロテクション・ドメインおよび構成済みのファイアウォール・ルールを定義するときは、すべてのインターフェースを選択する必要があります。ファイアウォール・ルール定義を作成する場合、インターフェース・キーワードを使用しないでください。

HA に関する考慮事項

- 単一の HA 環境でモデルを混用することはできません。例えば、GX5208 アプライアンスと GX6116 アプライアンスを HA ペアとして使用することはできません。
- 同じ HA ペア内のアプライアンスのファームウェア・レベルと X-Press Update (XPU) レベルは必ず一致するようにしてください。
- 同じ HA ペア内のアプライアンスは、同じ SiteProtector グループで管理してください。

ポリシーでの手順

IPS ローカル管理インターフェースの場合:

- 「**Manage System Settings (システム設定の管理)**」 > 「**ネットワーク**」 > 「**Security Interfaces (セキュリティー・インターフェース)**」

HA 構成オプション

IBM Security Network IPS は、ハイアベイラビリティ (HA) 構成する方法として、標準 HA と地理的 HA の 2 つの方式を提供しています。

標準 HA 構成では、2 つのアプライアンスのプロテクション・ポートをケーブル接続して、それぞれのアプライアンスが他方のアプライアンスからのトラフィックをミラーリングするようにします。各アプライアンス上で使用可能なポートの半分が「インライン・ポート」として使用され、半分が他方のアプライアンスへの「ミラー・ポート」として使用されます。この構成はネットワークの可用性とプロテクションを最大化する助けとなりますが、制約がいくつかあります。HA ペアを形成するアプライアンスは、相互にケーブル接続可能な距離に配置する必要があり、各アプライアンスのプロテクション・ポートの半分はミラー・ポートとしてのサービスに提供する必要があります。

地理的 HA 構成では、2 つのアプライアンスは検疫状態を共有しますが、トラフィックのミラーリングは行いません。ペアの一方のアプライアンスで作成された検疫ルールは、他方のアプライアンスに転送されます。HA ペアを形成するアプライアンスは、管理ポートを通じて通信し、通信に管理ネットワークを使用します。ケーブル配線のために近接しているかどうかは問題ではありません。

ハイアベイラビリティ・モード

HA 構成では、アプライアンスはインライン・シミュレーション・モードまたはインライン・プロテクション・モードのいずれかでのみ動作可能です。パッシブ・モニター・モードはサポートされていません。HA モードを選択すると、すべてのインライン・インターフェースが該当のインターフェース・モードに自動的に設定されます。

HA では、アプライアンス自体の可用性または耐障害性は取り扱いません。パッシブ・モニター・モード用に構成されて配線されているアプライアンスに対する別個のハイアベイラビリティ・ソリューションはありません。以下の表に示すように、以下のハイアベイラビリティ・モードを使用してアプライアンスを構成できます。

設定	説明
通常モード (HA オフ)	HA は無効にされ、各アプライアンスは単独に動作します。アプライアンスは、インライン・プロテクション、インライン・シミュレーション、およびパッシブ・モニターの各モードで、インターフェース・レベルのみで実行するように構成できます。
HA シミュレーション・モード (標準 HA)	両方の HA パートナー・アプライアンスが、トラフィックをインラインでモニターしますが、トラフィックのブロックは行いません。代わりに、両方のアプライアンスがトラフィックをモニターし、パッシブ通知レスポンスを提供します。アプライアンスは、ミラー・リンクを通じて互いのセグメント上のトラフィックをモニターし、ネットワーク・フェイルオーバーが発生した場合にはいつでも通知を引き継げる状態です。

設定	説明
HA プロテクション・モード (標準 HA)	両方の HA パートナー・アプライアンスがトラフィックをインラインでモニターし、Block レスポンス、Quarantine レスポンス、およびファイアウォール・ルールで構成された攻撃を、それぞれのアプライアンスが報告し、ブロックします。アプライアンスは、ミラー・リンクを使用して互いのセグメント上のトラフィックをモニターし、ネットワーク・フェイルオーバーが発生した場合にはいつでも報告とプロテクションを引き継げる状態です。
地理的 HA	HA ペアの各アプライアンスは、自己のトラフィックをモニターし、新規検疫ルールをパートナーに渡します。

標準的なハイアベイラビリティのためのデプロイメント

IBM Security Network IPS ハイアベイラビリティ (HA) 機能では、*既存の* ハイアベイラビリティ・ネットワーク環境でアプライアンスを活用できるようにします。アプライアンスは、相互間のすべてのトラフィックをミラーリング・リンクを介して受け渡し、それによって両方のアプライアンスはネットワークを経由するすべてのトラフィックを確実に認識でき、したがって状態を維持できます。この方式により、アプライアンスは非対称的に経路指定されたトラフィックを把握でき、ネットワークを完全に保護することができます。

HA サポートは、2 つの連携するアプライアンスに限定されます。両方のアプライアンスが、パケットをインラインで処理し、インライン・プロテクション・ポートに到着する攻撃トラフィックをブロックし、インライン・ポートで受信したイベントを管理コンソールに報告します。

サポートされるアプライアンス

既存の HA 環境で以下のアプライアンス・モデルを使用できます。

- GX5000 シリーズのアプライアンス
- GX6000 シリーズのアプライアンス
- GX7000 シリーズのアプライアンス

重要: 単一の HA 環境でモデルを*混用*する ことはできません。例えば、GX5208 アプライアンスと GX6116 アプライアンスを HA ペアとして使用することはできません。

サポートされるネットワーク構成

ハイアベイラビリティ・ネットワークは、通常、以下の 2 つの方法のいずれかで構成されます。

既存の HA 構成	説明
1 次 / 2 次	この構成では、トラフィックは冗長ネットワーク・セグメントの片方のみを流れ、ネットワーク上の 1 次デバイスが、そのデバイスのいずれかに障害が発生するまで、すべてのトラフィックを処理します。障害が発生した時点で、トラフィックは 2 次冗長ネットワーク・セグメントにフェイルオーバーし、2 次デバイスが処理を引き継ぎます。
クラスタリング	この構成では、トラフィックのロード・バランスがとられ、両方のデバイス・セットがアクティブになって、常時トラフィックを監視します。

IBM Security Network IPS の HA 機能は、これらのネットワーク構成を両方ともサポートしています。これを達成するには、両方の IBM Security アプライアンスが同一の状態を維持する必要があります。両方のアプライアンスは、複数のポートを介した複数の接続で構成されるミラー・リンクで接続されます。これらのミラー・リンクは、アプライアンスがそのインライン・ポートで受信するすべてのトラフィックを他方のアプライアンスに渡し、両方のアプライアンスのプロトコル分析モジュールがネットワーク・トラフィックをすべて確実に処理できるようにします。さらに、アプライアンスは非対称的に経路指定されたトラフィックを処理します。この方式により、フェイルオーバー時にプロテクションのギャップが生じるのを確実に防ぎます。

注: HA 機能が有効になっているときに IPS Setup を実行する場合、ネットワーク設定を変更することはできません。

HA でのレスポンスの処理、ブロック、報告、および生成

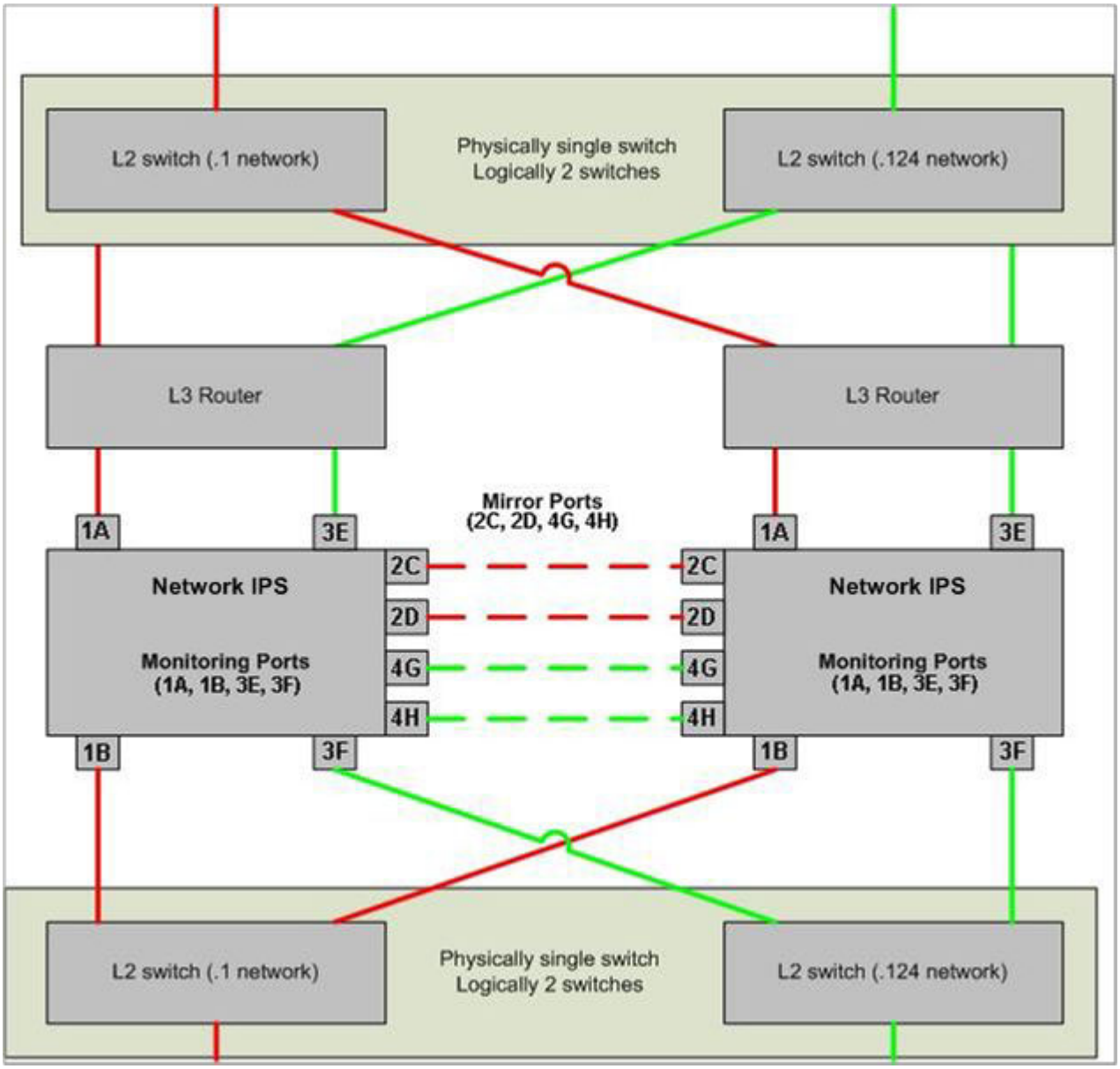
HA ペアのアプライアンスは、インライン・ポートおよびミラー・ポートから受信したすべてのパケットを処理します。ただし、アプライアンスは、インライン・ポートで発生するイベントに対してのみ、攻撃をブロックし、イベントを報告し、レスポンスを生成します。ミラー・ポートで発生するトラフィックに対しては、ブロックも報告も、レスポンスの生成も行いません。ミラー・ポート・トラフィックに関しては、アプライアンスは処理のみを行います。

両方のアプライアンスがトラフィック全体を常に監視しています。フェイルオーバーが発生した場合も、セキュリティーに途切れはありません。両方のアプライアンスが最新状態を維持するので、1 つの HA ネットワーク・セグメントに障害が発生しても、他方のアプライアンスがそのインライン・ポートですべてのパケットを受信します。ネットワークは保護された状態のままで、中断が生じることはありません。

注: 少数の攻撃、特に Port Scan などのスイープ攻撃の場合は、重複イベント (クラスター構成の各アプライアンスから 1 つずつ) が生成される場合があります。

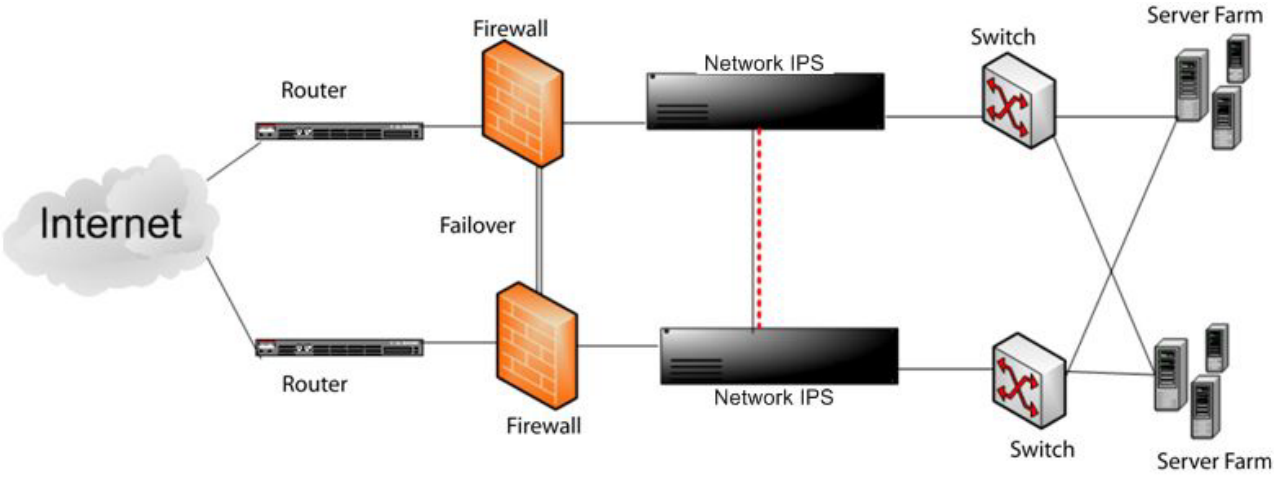
標準 HA デプロイメント: 論理図

SiteProtector を使用してアプライアンスを管理する場合、SiteProtector Agent Manager から HA クラスターを管理できます。 HA の論理図を以下に示します。


L2 switch (.1 network)
Physically single switch
Logically 2 switches
L2 switch (.124 network)
L3 Router
L3 Router
Mirror Ports
(2C, 2D, 4G, 4H)
1A
3E
1A
3E
Network IPS
Monitoring Ports
(1A, 1B, 3E, 3F)
2C
2D
4G
4H
2C
2D
4G
4H
Network IPS
Monitoring Ports
(1A, 1B, 3E, 3F)
1B
3F
1B
3F
L2 switch (.1 network)
Physically single switch
Logically 2 switches
L2 switch (.124 network)

標準 HA デプロイメント: 物理図

典型的な HA デプロイメント・シナリオの物理ネットワーク図を以下に示します。



地理的なハイアベイラビリティのためのデプロイメント

地理的 HA 構成では、2 つのアプライアンスが検疫状態を共有しますが、トラフィックのミラーリングは行いません。HA ペアを形成するアプライアンスは、それぞれの管理ポートを通じて通信します。ペアの片方のアプライアンスで作成された検疫ルールは、管理ポートを通じてもう一方のアプライアンスに転送されます。HA ペアは通信に管理ネットワークを使用するので、ケーブル接続の接近性は問題ではありません。

サポートされるアプライアンス

既存の HA 環境で以下のアプライアンス・モデルを使用できます。

- GX3000 シリーズのアプライアンス
- GX4000 シリーズのアプライアンス
- GX5000 シリーズのアプライアンス
- GX6000 シリーズのアプライアンス
- GX7000 シリーズのアプライアンス
- GV シリーズの仮想アプライアンス

重要: 単一の HA 環境でモデルを*混用*する ことはできません。例えば、GX5208 アプライアンスと GX6116 アプライアンスを HA ペアとして使用することはできません。

HA パートナー間の通信

地理的 HA 構成では、HA パートナーは管理ネットワークを通じて相互に通信します。パートナー・アプライアンス間のすべての通信は暗号化されます。通信を有効にするには、証明書が必要です。

以下の通信オプションを使用できます。

- **初回のみ信頼:** 各アプライアンスがオンラインになったときに、それぞれがパートナー・アプライアンスからの必要な暗号化証明書を要求します。
- **明示的な信頼:** 手動で両方のアプライアンスに暗号鍵をコピーして、通信を有効にする必要があります。

地理的 HA ペアのホスト名または時刻/日付の設定の変更

初回のみ信頼: ホスト名または時刻/日付の設定を変更する前に、パートナー・アプライアンスの地理的 HA モードを無効にしてください。このステップにより、アプライアンスは、地理的 HA を再び有効にしたときに「初回のみ信頼」構成で起動され、新しい暗号鍵を自動的にダウンロードします。

明示的な信頼: HA ペアが明示的な信頼を使用するように設定されている場合、通信を有効にするには、変更されたアプライアンスから HA パートナーにユーザーが鍵をコピーする必要があります。

地理的 HA ペアでのアプライアンスの再イメージ化

初回のみ信頼: アプライアンスの再イメージ化を行う場合、またはアプライアンスを出荷時のデフォルト値にリセットする場合は、その前にパートナー・アプライアンスの地理的 HA モードを無効にしてください。このステップにより、アプライアンスは、地理的 HA を再び有効にしたときに「初回のみ信頼」構成で起動され、新しい暗号鍵を自動的にダウンロードします。

明示的な信頼: HA ペアが明示的な信頼を使用するように設定されている場合、通信を有効にするには、再イメージ化したアプライアンスから HA パートナーにユーザーが鍵をコピーする必要があります。

システム時刻

地理的 HA を有効にする前に、両方のアプライアンスのシステム時刻が正しいことを確認してください。そうしないと、暗号鍵が正しく作成されない場合があります。

第 9 章 一般情報

このセクションには、IBM Security Network IPS アプライアンスに関する一般情報が含まれています。

互換性

以下のトピックに、アプライアンスで現在サポートされる Web ブラウザーおよび Java ランタイム環境 (JRE) のバージョンのリストを示します。

Web ブラウザーの互換性

以下のブラウザーがサポートされています。

- Internet Explorer 8
- Internet Explore 9
- Firefox 13

Java ランタイム環境の互換性

JRE 1.6 および 1.7 がサポートされています。JRE の使用時には、以下のいずれかを実行してください。

重要: JRE 1.7 は、32 ビットの Windows システムの場合のみ機能します。64 ビットの Windows システムでは使用できません。

- Java キャッシュを頻繁にクリアしてください。
- Java コンソールが一時ファイルをコンピューター上に保持しないようにしてください。
- Java キャッシュの最大スペースをゼロに設定してください。

アプライアンス・パーティション

以下の表に、パーティションとファイル・システムのリストを示します。

パーティション	ファイル・システム
/ *ルート・パーティション*	• オペレーティング・システム • 不正侵入防御システム・モジュール • データベース
/boot	• オペレーティング・システム
/rboot	• オペレーティング・システム
/cache	• ログ・ファイル
/restore	• バックアップ・イメージ • 出荷時のデフォルト・イメージ

累積更新およびロールバック

更新をインストールした後でアプライアンスが更新パッケージを削除するので、ダウンロードしたパッケージはアプライアンスにはもうありません。更新をロールバックした場合、アプライアンスがダウンロードおよびインストールに使用可能な更新を検出するのは、次回ユーザーが更新を検出したとき、または次回に予定された自動更新のときです。

特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒103-8510
東京都中央区日本橋箱崎町19番21号
日本アイ・ビー・エム株式会社
法務・知的財産
知的財産権ライセンス渉外

以下の保証は、国または地域の法律に沿わない場合は、適用されません。 IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。 IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Corporation
Project Management
C55A/74KB
6303 Barfield Rd.,
Atlanta, GA 30328
U.S.A

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、またはそれと同等の条項に基づいて、IBM より提供されます。

IBM の将来の方向または意向に関する記述については、予告なしに変更または撤回される場合があり、単に目標を示しているものです。

商標

IBM、IBM ロゴおよび ibm.com は、世界の多くの国で登録された International Business Machines Corporation の商標です。他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。現時点での IBM の商標リストについては、http://www.ibm.com/legal/copytrade.shtml をご覧ください。

Linux は、Linus Torvalds の米国およびその他の国における商標です。

UNIX は The Open Group の米国およびその他の国における登録商標です。

Microsoft および Windows は、Microsoft Corporation の米国およびその他の国における商標です。

索引

日本語, 数字, 英字, 特殊文字の順に配列されています。なお, 濁音と半濁音は清音と同等に扱われています。

[ア行]

[カ行]

[サ行]

[タ行]

[ハ行]

［マ行］

［ヤ行］

［ラ行］

B

E

F

I

J

L

M

N

O

P

Q

S

T

U

W

X

Printed in Japan

日本アイ・ビー・エム株式会社
〒103-8510 東京都中央区日本橋箱崎町19-21