

## vGW シリーズ

# インストールおよび管理ガイド

リリース

リリース 5.0



発行: 2011-12-13

改訂 1

Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, California 94089  
USA  
408-745-2000  
www.juniper.net

本製品は、Integrated Systems Inc. の子会社 Epilogue Technology が開発した Envoy SNMP Engine を内蔵しています。Copyright © 1986-1997, Epilogue Technology Corporation. All rights reserved. このプログラムとそのドキュメントは私的な支出により開発されたもので、パブリックドメインには帰属しません。

本製品には、Mark Moraes 氏が開発したメモリ割当てソフトウェアが組み込まれています。Copyright © 1988, 1989, 1993, University of Toronto.

本製品には、カリフォルニア大学、パークレー校とその貢献者が開発した FreeBSD ソフトウェアが組み込まれています。4.4BSD および 4.4BSD-Lite リリースに含まれる全ドキュメントとソフトウェアは、カリフォルニア大学が著作権を所有しています。Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994. The Regents of the University of California. All rights reserved.

GateD software copyright © 1995, the Regents of the University. All rights reserved. Gate Daemon は、コーネル大学とその協力者がリリース 3.0 を基に開発しました。Gated は、Kirtan の EGP、UC パークレー校のルーティング デモン (ruted)、および DCN の HELLO ルーティング プロトコルに基づいています。Gated の開発は、全米科学財団から部分的な援助を受けています。Portions of the GateD software copyright © 1988, Regents of the University of California. All rights reserved. Portions of the GateD software copyright © 1991, D. L. S. Associates.

本製品には Maker Communications, Inc. が開発したソフトウェアが組み込まれています。Copyright © 1996, 1997, Maker Communications, Inc.

Juniper Networks、Junos、Steel-Belted Radius、NetScreen、ScreenOS は、米国およびその他の国における Juniper Networks, Inc. の登録商標です。Juniper Networks ロゴ、Junos ロゴ、および JunosE は Juniper Networks, Inc. の商標です。文書に掲載されているその他の商標、登録商標はすべて各所有者に帰属します。

Juniper Networks は、本文書内の誤りに関する責任を一切負いません。Juniper Networks は事前に通告することなく、本出版物を変更、修正、移譲する権利、あるいはその他の形態で改訂する権利を有します。

Juniper Networks が製造または販売した製品、または同製品の構成部品には、Juniper Networks が所有する、または同社にライセンス供与された以下の特許が 1 つ以上適用されている場合があります。U.S. Patent Nos. 5,473,599、5,905,725、5,909,440、6,192,051、6,333,650、6,359,479、6,406,312、6,429,706、6,459,579、6,493,347、6,538,518、6,538,899、6,552,918、6,567,902、6,578,186、および 6,590,785。

#### vGW シリーズ インストールおよび管理ガイド

##### 改訂履歴

September 2011-R1

本書の情報は、改訂履歴に一覧された日付時点でのものです。

## エンド ユーザー ライセンス契約

本ソフトウェアのダウンロード、インストール、使用の前には本エンド ユーザー ライセンス契約（「契約」）に目を通しておいてください。本ソフトウェアのダウンロード、インストール、使用により、または別の形態での本書内の条件への合意表現により、お客様、またはお客様以外の場合はお客様と正規に提携する代理人/代理店は本契約に従うことに合意します。本書内の条件に合意できない場合、(A) 本ソフトウェアのダウンロード、インストール、使用を行わないでください。また (B) ライセンス条件に関して Juniper Networks にお問い合わせ頂くことも可能です。

1. 当事者。本契約の当事者は、(i) Juniper Networks, Inc.（顧客の当社が米国内にある場合）または Juniper Networks (Cayman) Limited（顧客の当社が米国外にある場合）（かかる該当する事業体をここでは「Juniper」と呼称します）、および (ii) 本ソフトウェアを利用するための当該のライセンスを Juniper または Juniper の正規代理店から購入している個人または団体（「顧客」）です（「当事者」と総称）。
2. ソフトウェア。本契約では、「ソフトウェア」は Juniper または Juniper 供給のソフトウェアのプログラム モジュールと機能で顧客が Juniper または Juniper 正規代理店に当該のライセンス料金はサポート料金を支払っているもの、または Juniper が装置に組み込んだもので顧客が Juniper または Juniper 正規代理店から購入したものを意味します。「ソフトウェア」には、同ソフトウェアのアップデート、アップグレード、および新規リリースも含まれます。「組み込みソフトウェア」は、Juniper が Juniper 製装置に組み込んだかロードしたソフトウェア、およびその後アップデート、アップグレード、追加、または交換する目的で組み込んだかロードしたソフトウェアを意味します。
3. ライセンス付与。当該の料金の支払い、および本書に規定される制限および制約への準拠により、Juniper は以下の使用制限に従うことを条件として、ソフトウェアを実行ファイル形式でのみ使用する非排他的、譲渡不可のライセンスを、サブライセンス権を含めずに顧客に付与します。
  - a. 顧客は Juniper または Juniper 正規代理店から購入したときの状態の Juniper 製装置に組み込まれた状態でのみ、および同装置で実行する目的でのみ組み込みソフトウェアを使用するものとします。
  - b. 顧客は単一処理装置を内蔵する単一のハードウェア シャーシ上で、または顧客がその個数分のライセンス料金を支払っている場合は複数のシャーシまたは処理装置上で、本ソフトウェアを使用するものとします。ただし、Steel-Belted Radius または Odyssey Access Client のソフトウェアに限っては、顧客は物理ランダム アクセス メモリ空間、および複数プロセッサを内蔵する単一のコンピュータ上で本製品を使用するものとします。Steel-Belted Radius または IMS AAA ソフトウェアを複数台のコンピュータまたは仮想マシン（たとえば Solaris ゾーン）で使用するには、コンピュータまたは仮想マシンが単一のシャーシに物理的に内蔵されているかどうかに関係なく、その個数分のライセンスが必要です。
  - c. 顧客が購入した製品購入書類、印刷物または電子媒体によるユーザー マニュアル、および/または特定のライセンスに、顧客のソフトウェア利用の制限が指定されている場合があります。かかる制限により、シート、登録された端点、同時ユーザー、セッション、コール、接続、加入者、クラス、ノード、領域、機器、リンク、ポート、またはトランザクションの使用がそれぞれの最大数に制限される場合があります、あるいは特定の特長、機能、サービス、アプリケーション、操作、性能を利用する場合に別途ライセンスの購入が要求される場合があります、あるいはスループット、パフォーマンス、設定、帯域幅、インターフェース、処理に対して、また一時的、地理的な制限が課せられる場合があります。加えて、かかる制限により、本ソフトウェアをある特定のネットワークの管理のために使用するの禁止されることも、本ソフトウェアを他の特定のソフトウェアと一緒に使用しなければならないこともあります。顧客が本ソフトウェアを使用する場合、かかるすべての制限に従い、当該ライセンスをすべて購入する必要があります。
  - d. 本ソフトウェアを試用する場合、顧客の本ソフトウェアの使用権利はダウンロード、インストール、または使用を開始してから 30 日経過後に期限切れになります。30 日間の試用期限切れ後は、顧客はライセンス料金を支払うことによりのみ本ソフトウェアを使用することができます。30 日間の試用期限切れ後、顧客は本ソフトウェアを再インストールして試用期限を延長または試用開始日を新規に設定することはできません。
  - e. 顧客は自社の企業ネットワークへのアクセスを管理する目的にのみ、Steel-Belted Radius ソフトウェアのエンタープライズ エディションを使用可能です。具体的は、サービス プロバイダ顧客が、商用ネットワーク アクセス サービスをサポートするために Steel-Belted Radius ソフトウェアのグローバル エンタープライズ エディションを使用することは明示的に禁止されます。

上記のライセンスは顧客側で移転あるいは譲渡することはできません。本書内に示されるライセンスは、本ソフトウェアの当該ライセンスをソフトウェア購入時に Juniper または Juniper 正規代理店から購入していないユーザーに対しては付与されません。

4. 使用の禁止。上記が規定されている場合でも、本書内で規定されるライセンスにより顧客が以下を行うことは禁止されます。また顧客も以下を行わないことに合意し、以下を行わないものとします。(a) 本ソフトウェアを修正、アンバンドル化、リバース エンジニアリングすること、または本ソフトウェアから派生品を作成すること、(b) （バックアップ用に必要とされる場合を除き）本ソフトウェアの不正なコピーを作成すること、(c) 形態を問わず本製品のコピーを第三者に貸与、販売、譲渡、または付随する権利を付与すること、(d) 本ソフトウェアのコピー、または本ソフトウェアが組み込まれた製品に記載された Juniper 独自の注意、ラベル、マークを削除すること、(e) 中古市場で販売される Juniper 装置に組み込まれたものを含めて、本ソフトウェアのコピーを第三者に配布すること、(f) 当初、当該ライセンスを購入し有効な鍵を Juniper から取得せずに、「ロックされた」すなわち鍵で制御された機能、関数、サービス、アプリケーション、操作、性能を使用すること、これは、かかる機能、関数、サービス、アプリケーション、操作、または性能が鍵を使用せずに有効になる場合を含む、(g) Juniper が配布したソフトウェア用の鍵を第三者に配布すること、(h) 顧客が Juniper または Juniper 正規代理店から購入した使用法を超える方式で、またはかかる使用法を拡大して本ソフトウェアを使用すること、(i) 非 Juniper 装置で、本組み込みソフトウェアを使用すること、(j) 顧客が元々 Juniper または Juniper 正規代理店から購入していない Juniper 製装置で、本組み込みソフトウェアを使用すること（または使用できるようにすること）、(k) 事前に Juniper の書面による同意を得ずに、

本ソフトウェアに対するテストまたはベンチマークの結果を第三者に開示すること、(I) 本書内で明示的に規定している以外の方法で本ソフトウェアを使用すること。

5. 監査。顧客は本契約への準拠を検証するのに必要とされる精細な記録を維持するものとします。Juniper 側からの要請がある場合、顧客はかかる記録を Juniper に提供し、顧客側の本契約への準拠を証明するものとします。

6. 機密性。当事者は、本ソフトウェアの全機能および関連マニュアルが Juniper の極秘の所有物であることに合意します。この場合、顧客は商業的に妥当なあらゆる努力を払い、本ソフトウェアおよび関連マニュアルを極秘に管理します。これには本ソフトウェアへのアクセスを、顧客の社内的な業務目的で本ソフトウェアを使用する必要がある顧客の従業員および請負業者に制限する内容を最低減含めるものとします。

7. 所有権。Juniper および Juniper のライセンサはそれぞれ、本ソフトウェア、関連マニュアル、本ソフトウェアのすべてのコピーに付随するすべての権利、タイトル、利害関係（著作権を含む）の所有権を有します。本契約のどの部分も、本ソフトウェアまたは関連マニュアルの権利、タイトル、利害関係の譲渡または移譲、あるいは本ソフトウェア、関連マニュアル、本ソフトウェアのコピーの販売として解釈されることはありません。

8. 保証、責任の限度、保証の免責。本ソフトウェアに適用される保証は、本ソフトウェアに添付された保証文書（「Warranty Statement」）に記載されています。本契約のどの部分においても、本製品をサポートする義務を発生させることはありません。サポート サービスは別途購入できます。かかるサポートは、書面による個別のサポート サービス契約で管理されます。法律で許容される範囲を上限に、Juniper は本契約、本ソフトウェア、Juniper 製ソフトウェアまたは Juniper 提供のソフトウェアから生じる利益の損失、データの消滅、代替品、代替サービスの費用または調達に対して、あるいは特殊な、間接的な、付随的な損害に対して責任を負わないものとします。いかなる場合も、Juniper は Juniper 製ソフトウェアまたは Juniper 提供のソフトウェアの不正な使用または誤った使用から生じる損害に対して責任を負わないものとします。Warranty Statement で明示的に規定される場合を除き、法律で許容される範囲で、Juniper は（明示的、暗黙的、法的、その他を問わず）本ソフトウェアに付随するすべての保証から免責され、これには商用性、特定の用途への適合性、非侵害の暗黙的な保証も含まれます。いかなる場合も、Juniper は本ソフトウェア、または本ソフトウェアを実行する装置あるいはネットワークがエラーや中断を起こさずに動作すること、または侵入あるいは攻撃に対する脆弱性がないことを保証しません。いかなる場合も、契約、不法行為（不履行を含む）、保証の違反、その他のいずれで生じたかを問わず Juniper または Juniper のサプライヤまたはライセンサの顧客への法的責任は、申し立ての原因となったソフトウェアに対して顧客が支払った金額、またはソフトウェアが別の Juniper 製品に組み込まれている場合は、かかる他の製品に対して顧客が支払った金額を超えないものとします。顧客は Juniper が保証の免責条項および本書に規定される法的責任の制限に基づいて同社製品の価格を設定し、本契約を締結していること、および価格設定と本契約の締結に、両当事者間のリスク（契約の救済措置で本質的な目的が救済されず、結果的に損失を生じるリスクを含む）の割り振りを反映すること、および価格設定と本契約の締結により、両当事者間の契約の本質的な基礎が形成されることを承認し合意します。

9. 終了。本契約の違反、または顧客による当該料金の未払いが発生した場合、本書の規定により付与されるライセンスは自動的に停止するものとします。かかるライセンスの停止により、顧客は顧客が保有または管理する本ソフトウェアのコピーおよび関連マニュアルをすべて破棄するか、Juniper に返却するものとします。

10. 税。本契約の下に支払いされるすべてのライセンス料金には、税金が含まれません。顧客は本ソフトウェアのライセンスの購入、輸入、または使用から生じる税の支払いに責任を負うものとします。適用できる場合、各税務管轄区域の有効な免税書類は請求書の作成前に Juniper に提出し、当該免税が取り消されるか変更された際には顧客は迅速に Juniper に通知するものとします。顧客が支払うべきすべての金額は、源泉徴収税を差し引いた金額です。かかる源泉徴収税について、顧客は迅速に以下を行い、Juniper に適切に協力するものとします。必要なすべての源泉徴収税を支払いしたことを示す有効な税金徴収証明書および他の必要な書類を Juniper に提出すること、支払うべき源泉徴収税が減額される適切な申告を完了すること、および本契約に基づく取引に関係する監査または税金処理手続きについて Juniper に通知および協力すること。顧客はすべての適用できる税法に従うものとし、また、顧客は本契約に規定される義務の不履行または遅延の結果として Juniper が被った負債に関係するすべての費用と損害賠償金を Juniper に迅速に支払うかまたは返済するものとします。本節に規定する顧客の義務は、本契約の終了または満期後も継続するものとします。

11. 輸出。顧客は米国および当該国の機関または当局で適用されるすべての輸出法および輸出制限および輸出規制に従い、かかる制限、法律または規制に違反して、または必要とされるすべての承認を得ずに本ソフトウェアまたは本ソフトウェアからの直接の生成物を輸出または再輸出しないことに合意します。顧客はかかる違反に対して責任を負うものとします。顧客に提供されたソフトウェアのバージョンには、顧客が輸出ライセンスなしに本ソフトウェアを輸出するのを制限する暗号化またはその他の機能が含まれている場合があります。

12. 商用コンピュータ ソフトウェア。本ソフトウェアは「商用コンピュータ ソフトウェア」であり、提供時に付与される権限は制限されています。米国政府による使用、配布、開示は本契約に規定される制限、および DFARS 227.7201 ~ 227.7202-4、FAR 12.212、FAR 27.405(b)(2)、FAR 52.227-19、FAR 52.227-14(ALT I11) の該当する法律に規定される制限に従って行われます。

13. インターフェース情報。適用される法律で要求される範囲で、および顧客から書面で要求がある場合、Juniper は本ソフトウェアと独自に作成された別のプログラム間の相互運用を達成するのに必要なインターフェース情報を、手数料が発生する場合はその支払い後に顧客に提供するものとします。顧客はかかる情報に関する厳密な守秘義務を遵守し、Juniper がかかる情報の開示に関して規定したすべての当該条件に従ってかかる情報を使用するものとします。

14. サードパーティ ソフトウェア。本ソフトウェアに組み込まれたソフトウェアの Juniper のライセンサ、および本ソフトウェアに組み込まれた製品または技術（または本ソフトウェアからアクセスされるサービス）の Juniper のサプライヤは、本契約のサードパーティ受益者であり、かかるライセンスまたはベンダーは、Juniper と同等に独自に本契約を行使する権限を有するものとします。さらに、特定のサードパーティ ソフトウェア

アが本ソフトウェアに組み込まれる場合があり、かかるソフトウェアは、それぞれの所有者のライセンスが添付されている場合、これに従う必要があります。本ソフトウェアの一部が、かかる一部のソースコードの公開を Juniper に義務付けるオープンソースライセンス（GNU General Public License（「GPL」）または GNU Library General Public License（「LGPL」）など）に基づき配布されることを条件に、Juniper は要求があれば、配布日から最長 3 年間にわたりかかるソースコード部分（適宜 Juniper 側での修正を含む）を開示するものとします。かかる要求は、Juniper Networks, Inc.、1194 N. Mathilda Ave., Sunnyvale, CA 94089, ATTN: General Counsel 宛に書面で行うことができます。GPL のコピーは <http://www.gnu.org/licenses/gpl.html> から、LGPL のコピーは <http://www.gnu.org/licenses/lgpl.html> から入手できます。

15. その他。本契約書は法の原則への抵触とは無関係に、カリフォルニア州の法律により統制されるものとします。国連国際物品売買条約（Convention for the International Sale of Goods）の条項は、本契約に適用されません。本契約の下で生じる紛争については、当事者はここに、カリフォルニア州サンタクララ郡内の州裁判所および連邦裁判所の対人管轄権および専属管轄権、および同所での裁判に合意します。本契約は本ソフトウェアに関して、Juniper と顧客との間の完全なる合意と見なされ、Juniper の正規代理人と顧客との間で個別に締結された書面契約の条件が、本書内の条件と矛盾する、または衝突する限りにおいてのみかかる条件で統制される場合を除き、口頭か書面かを問わず、本契約に関連した事前または同時期の契約すべて（発注書内に記載される矛盾する条件を含める）よりも優先されます。本契約の変更、あるいは本契約内の権利の放棄は、相手側当事者が書面で明示的に同意していなければ有効になりません。本契約の一部が無効な状態にある場合、当事者はかかる無効性によっても本契約の残りの部分の有効性に影響が及ばないことに合意します。本契約および関連マニュアルは英語で記述されており、当事者は英語版で統制されることに合意します。（カナダ: Les parties aux présentes confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattache, soient rédigés en langue anglaise.（翻訳: 当事者は本契約およびすべての関連マニュアルが、現在および将来にわたり英語で記述されることを承認します））。



# 簡略な目次

	このガイドについて .....	xix
第1部	vGW シリーズの概要	
第1章	vGW シリーズの概要 .....	3
第2章	vGW シリーズのリソース要件 .....	11
第3章	vGW シリーズの VMware 環境との統合 .....	15
第2部	vGW シリーズの構成と管理	
第4章	vGW セキュリティ デザイン VM の概要 .....	35
第5章	vGW シリーズのメイン モジュール .....	45
第6章	vGW シリーズ VM のネットワーク モジュール .....	53
第7章	vGW シリーズのファイアウォール モジュール .....	59
第8章	vGW シリーズの IDS モジュール .....	67
第9章	vGW シリーズのアンチウィルス モジュール .....	75
第10章	vGW シリーズのイントロスペクション モジュール .....	93
第11章	vGW シリーズのコンプライアンス モジュール .....	107
第12章	vGW シリーズ VM のレポート モジュール .....	117
第13章	vGW シリーズの設定モジュール .....	125
第14章	vGW シリーズのアプリケーション設定 .....	127
第15章	vGW シリーズのセキュリティ設定 .....	161
第16章	vGW セキュリティ デザインのアプライアンス設定 .....	183
第17章	vGW シリーズのステータス アラート .....	193
第18章	高可用性とフォールト トレランス .....	195
第3部	Juniper Networks 製品の相互運用性	
第19章	vGW シリーズの Juniper Networks 製品との相互運用性 .....	203
第4部	索引	
	索引 .....	213





# 目次

	このガイドについて	xix
	目的	xix
	対象読者	xix
	ドキュメントの表記規則	xx
	ドキュメントの入手	xx
	ドキュメントのフィードバック	xx
	テクニカル サポートのリクエスト	xx
	セルフヘルプ オンライン ツールおよびリソース	xx
	JTAC へのお問い合わせ	xxi
第1部	vGW シリーズの概要	
第1章	vGW シリーズの概要	3
	vGW シリーズの理解	3
	クラウド コンピューティングと vGW シリーズの理解	8
	VMware インフラストラクチャと vGW シリーズの理解	9
	vSphere と vGW シリーズの理解	9
	VMware ESX および ESXi ホストと vGW シリーズの理解	9
	vMotion と vGW シリーズの理解	9
第2章	vGW シリーズのリソース要件	11
	vGW シリーズの前提条件とリソース要件の理解	11
	全体的なリソースおよびアクセス要件の理解	11
	仮想アプライアンス システムの要件の理解	12
	VMware vSwitch の要件の理解	13
	VMware ポート グループの要件の理解	13
	仮想化 NIC の要件の理解	14
第3章	vGW シリーズの VMware 環境との統合	15
	vGW シリーズの VMware 環境との統合の準備	15
	VMSafe ファイアウォールおよび監視モード	16
	vGW シリーズの環境時刻同期の理解	16
	Open Virtualization Format (OVF) OVA テンプレート方法の理解	17
	OVA バンドル方法を使用した vGW シリーズの VMware インフラストラクチャとの統合	18
	OVA 単一ファイル方法を使用した vGW セキュリティ デザイン VM の VMware との統合	26
	OVA 単一ファイル方法を使用した vGW セキュリティ VM の VMware との統合	27
	vGW シリーズのセットアップ	28

第2部	vGW シリーズの構成と管理	
第4章	vGW セキュリティ デザイン VM の概要	35
	vGW セキュリティ デザイン VM の理解	35
	vGW セキュリティ VM の理解	36
	vGW セキュリティ デザイン VM のナビゲーションの理解	37
	vGW セキュリティ デザイン VM のナビゲーション ボタン バーの理解	39
	vGW セキュリティ デザイン VM のツリーについて	40
	VM ツリーの概要	41
	複雑な VM ツリーでの VM の特定	42
第5章	vGW シリーズのメイン モジュール	45
	vGW シリーズのメイン モジュールの理解	45
	Dashboard	45
	[Status] タブ	46
	[Events and Alerts] タブ	49
	Security Alerts	49
	System Status and Events	50
	[Quarantine] タブ	51
第6章	vGW シリーズ VM のネットワーク モジュール	53
	vGW シリーズ VM のネットワーク モジュールの理解	53
	ネットワーク モジュール	53
	表示情報の操作	54
	単一の仮想マシンに関するネットワーク情報の表示	54
	表示情報の時間間隔の変更	55
	詳細オプションの使用	57
	表データの並べ替え	57
第7章	vGW シリーズのファイアウォール モジュール	59
	vGW シリーズのファイアウォール モジュールの理解	59
	[Manage Policy] タブ	60
	[Apply Policy] タブ	62
	[Logs] タブ	64
第8章	vGW シリーズの IDS モジュール	67
	vGW シリーズの IDS モジュールの理解	67
	vGW シリーズの IDS モジュールの理解	68
	[Top Alerts] タブ	68
	[Alert Sources] タブ	69
	[Alert Targets] タブ	69
	[All Alerts] タブ	70
	IDS 設定の構成とアクティビティの表示	71
第9章	vGW シリーズのアンチウイルス モジュール	75
	vGW シリーズのアンチウイルス構成の概要	75
	vGW シリーズのアンチウイルスの理解	77
	アンチウイルス ソフトウェアについて	78
	シグネチャベースの検出	78

	vGW アンチウイルス機能	78
	vGW アンチウイルス ダッシュボード	80
	vGW シリーズ アンチウイルスのオンアクセス スキャンの構成	83
	vGW Endpoint の理解とインストール	86
	vGW Endpoint のインストール	86
	vGW Endpoint の自動更新	86
	VM 上の vGW Endpoint	87
	検疫されたファイル	88
	vGW Endpoint のコンポーネントと表示	88
	vGW シリーズ アンチウイルスのオンデマンド スキャンの構成	89
第10章	vGW シリーズのイントロスペクション モジュール	93
	vGW シリーズのイントロスペクション モジュールの理解	93
	vGW シリーズ イントロスペクションの [Applications] タブの理解	95
	vGW シリーズ イントロスペクションの [VMs] タブの理解	97
	vGW セキュリティ デザイン VM イントロスペクションのイメージ エンフォーサ機能の理解	98
	vGW シリーズの [Image Enforcer] タブの理解	100
	vGW シリーズの [Enforcer Profiles] タブの理解	101
	[Enforcer Profiles] ペインについて	101
	[Add Enforcer Profile] ペイン	102
	vGW シリーズ イントロスペクションのスケジュール機能の理解	104
	vGW シリーズ イントロスペクションのスキャン ステータスの理解	105
	vGW シリーズ イントロスペクションのレジストリ チェック機能の理解	106
第11章	vGW シリーズのコンプライアンス モジュール	107
	vGW シリーズのコンプライアンス モジュールの理解	107
	コンプライアンス モジュール	107
	[Compliance] タブ	108
	[Rules] タブ	109
	コンプライアンス規則の構成	109
	vGW シリーズのハイパーバイザおよび拡張 VM セキュリティの理解	112
	ハイパーバイザのセキュリティの必要性	112
	vGW シリーズのハイパーバイザおよび VM セキュリティと VMware 要塞化ガイドライン	113
	vGW シリーズのハイパーバイザおよび VM セキュリティの概要	113
	修復	114
	構成例	114
第12章	vGW シリーズ VM のレポート モジュール	117
	vGW シリーズのレポート モジュールの理解	117
	vGW シリーズのレポート モジュールを使用した自動レポートの仕様の構成	118
	vGW シリーズのカスタム レポート タイプの理解	120
	vGW シリーズのネットワーク レポートの理解	120
	vGW シリーズのファイアウォール レポートについて	121
	vGW シリーズの IDS レポートについて	121
	vGW シリーズのイントロスペクション レポートについて	121
	vGW シリーズのコンプライアンス レポートの理解	122
	vGW アンチウイルス レポートの理解	122

第13章	vGW シリーズの設定モジュール	125
	vGW シリーズの設定モジュールの理解	125
第14章	vGW シリーズのアプリケーション設定	127
	vGW シリーズのアプリケーション設定の理解	127
	vGW シリーズの設定モジュールを使用したステータスおよびライセンス情報の表示	128
	vGW シリーズのライセンスの理解	129
	ライセンス要件	129
	vGW シリーズのライセンス	129
	評価ライセンス	130
	vGW シリーズのライセンスの取得、インストール、および管理	130
	設定モジュールを使用した vGW シリーズの VMware との統合	131
	スプリットセンター機能の理解	132
	マルチセンター機能の理解	133
	マルチセンター機能	133
	委任 vGW セキュリティ デザイン VM とスタンドアロン vGW セキュリティ デザイン VM を含む vGW シリーズの配備	133
	vGW シリーズのマルチセンター機能の構成	134
	vGW シリーズ マルチセンターの同期オブジェクトの理解	135
	オブジェクトの同期	136
	オブジェクトの命名	136
	委任 vGW セキュリティ VM に対してローカルなオブジェクトの作成	136
	マルチセンター機能とスプリットセンター機能を使用したスケーリングの構成	137
	ESX/ESXi ホストへの vGW セキュリティ VM の配備	143
	vGW シリーズのインストール設定の構成	146
	vGW シリーズの vNIC 毎ポリシー機能の理解	147
	vNIC 毎ポリシーについて	147
	個別のポリシーを持つ vNIC とスマート グループ	147
	個別のポリシーを持つ vNIC の表示	148
	vNIC の命名規則	148
	vGW シリーズの vNIC 毎ポリシー機能の構成	148
	同じ VM 上の個々の vNIC に対する vGW ポリシーの構成と表示	150
	vNIC 毎ポリシーとスマート グループの理解	153
	設定モジュールを使用した vGW シリーズ管理者の定義	155
	vGW シリーズ管理者の認証に関する Active Directory のセットアップ	156
	vGW シリーズ環境で使用する新しいマシンの定義	157
	高可用性の使用	158
	vGW シリーズの E メールおよびレポート アプリケーション設定の構成	158
第15章	vGW シリーズのセキュリティ設定	161
	vGW シリーズのセキュリティ設定の理解	161
	vGW シリーズの設定モジュールを使用したグローバル設定の構成	162
	vGW セキュリティ VM 設定の理解	163
	vGW シリーズのアンチウィルス設定の理解と構成	165
	IDS 設定の理解と構成	166
	IDS シグネチャ設定の理解と構成	168
	vGW シリーズのセキュリティ アラート設定の理解	169
	E メール アラート設定	169
	SNMP トラップ設定	169

	自動構成アラートとマルチキャスト アラート	169
vGW	シリーズでのプロトコルのサポートの理解	170
vGW	シリーズのグループ設定の理解	170
	vGW グループ タイプ	170
	グループのコピー	171
vGW	シリーズのスマート グループの理解と使用	172
	背景	172
	スマート グループ	172
	スマート グループの使用について	172
	スマート グループの作成について	173
	スマート グループの定義例	180
vGW	シリーズのネットワーク 設定の理解	180
vGW	シリーズの SRX ゾーン設定の理解	181
第16章	vGW セキュリティ デザインのアプライアンス設定	183
	vGW シリーズの更新設定の理解	183
	vGW セキュリティ デザイン VM の手動更新	184
	パッチ モードでの vGW セキュリティ VM の更新	185
	vGW シリーズのネットワーク 設定の構成	186
	vGW シリーズのプロキシ設定の構成	186
	vGW シリーズの時刻設定の構成	186
	vGW シリーズのバックアップおよびリストア機能の理解	187
	vGW シリーズのバックアップおよびリストア機能の構成	188
	vGW シリーズのログ収集の理解	189
	ログ収集	190
	ファイルのアップロード	190
	ファイルのダウンロード	190
	vGW シリーズのログの表示	190
	vGW シリーズのサポート設定の理解	190
第17章	vGW シリーズのステータス アラート	193
	vGW シリーズのステータスおよびアラートの理解	193
	ステータス	193
	アラート	193
	E メール アラート設定	194
	SNMP トラップ設定	194
	自動構成アラートとマルチキャスト アラート	194
第18章	高可用性とフォールト トレランス	195
	vGW シリーズの高可用性ソリューションの理解	195
	vGW シリーズの高可用性ソリューションについて	195
	vGW セキュリティ デザイン VM の高可用性について	195
	vGW セキュリティ VM の高可用性について	196
	高可用性のためのセカンダリ vGW セキュリティ デザイン VM のインストール	196
	高可用性のためのセカンダリ vGW セキュリティ VM のインストール	197
	VMware の高可用性と分散リソース スケジュールの理解	198
	vGW シリーズのフォールト トレランスのサポートの理解	198
	vGW シリーズのフォールト トレランスについて	199
	vGW シリーズでの vGW シリーズ フォールト トレランス	199
	仮想マシンに対するフォールト トレランスの有効化	200

第3部	Juniper Networks 製品の相互運用性	
第19章	vGW シリーズの Juniper Networks 製品との相互運用性	203
	vGW シリーズおよび Junos SRX シリーズのセキュリティ ゾーン	203
	SRX シリーズ サービス ゲートウェイのセキュリティ ゾーンについて	203
	SRX シリーズ サービス ゲートウェイのゾーンと vGW シリーズ	204
	関連するアプリケーション ノート	204
	vGW シリーズに対する Junoscript インターフェースの有効化	205
	vGW シリーズと SRX シリーズ デバイスとの相互運用性のための SRX シリーズ ゾーン オブジェクトの構成	206
	SRX シリーズのゾーン アドレス帳への vGW シリーズ VM レコードの登録について	207
	vGW シリーズと SRX シリーズ ゾーンとの相互運用性の検証	207
	vGW シリーズから Juniper Networks STRM への Syslog および Netflow データの送信に関する構成	208
	vGW シリーズと IDP の相互運用の構成	209
第4部	索引	
	索引	213

# 図の一覧

第1部	vGW シリーズの概要	
第1章	vGW シリーズの概要	3
	図 1: メイン モジュール	4
	図 2: ネットワーク モジュール	4
	図 3: ファイアウォール モジュール	5
	図 4: IDS モジュール	5
	図 5: アンチウィルス モジュール	6
	図 6: イン트로スペクション モジュール	6
	図 7: コンプライアンス モジュール	7
	図 8: レポート モジュール	7
	図 9: 設定モジュール	8
第3章	vGW シリーズの VMware 環境との統合	15
	図 10: vGW シリーズ セキュリティ デザイン VM のログイン画面	29
第2部	vGW シリーズの構成と管理	
第4章	vGW セキュリティ デザイン VM の概要	35
	図 11: ボタン バー	37
	図 12: VM ツリー	38
	図 13: vGW セキュリティ デザイン VM のナビゲーション バー	39
	図 14: VM ツリーで VM を選択した例	41
第5章	vGW シリーズのメイン モジュール	45
	図 15: メイン モジュールのダッシュボード	46
	図 16: [Status] タブ	47
	図 17: ボタン バーに表示された正常性ステータス アイコン	48
	図 18: [Events and Alerts] タブの [Security Alerts] ペイン	49
	図 19: メイン モジュールの [Quarantine] タブ	51
第6章	vGW シリーズ VM のネットワーク モジュール	53
	図 20: ネットワーク モジュールの [Summary] タブ	54
	図 21: ネットワーク モジュールの [Summary] タブ	55
	図 22: 異なる時間間隔でのネットワーク データの表示: パート 1	55
	図 23: 異なる時間間隔でのネットワーク データの表示: パート 2	56
	図 24: ネットワーク データに対するフィルタリングの使用	57
第7章	vGW シリーズのファイアウォール モジュール	59
	図 25: ファイアウォール モジュール	59
	図 26: [Manage Policy] タブ	60
	図 27: [Apply Policy] タブ	64
	図 28: ファイアウォール モジュールの [Logs] タブ	65

第8章	vGW シリーズの IDS モジュール .....	67
	図 29: IDS モジュールの [Top Alerts] タブ .....	68
	図 30: IDS モジュールの [Alert Sources] タブ .....	69
	図 31: IDS モジュールの [Alert Targets] タブ .....	70
	図 32: IDS モジュールの [All Alerts] タブ .....	70
	図 33: IDS インバウンド ポリシー規則 .....	73
第14章	vGW シリーズのアプリケーション設定 .....	127
	図 34: ESX/EXSi ホストへの vGW セキュリティ VM の配備 .....	144
第15章	vGW シリーズのセキュリティ設定 .....	161
	図 35: [Signature Details] 画面 .....	168



# 表の一覧

第2部	vGW シリーズの構成と管理	
第4章	vGW セキュリティ デザイン VM の概要	35
	表1: ナビゲーション ボタン	39
	表2: 仮想マシンの状態を表すアイコン	42
第5章	vGW シリーズのメイン モジュール	45
	表3: vGW シリーズのステータス アイコン	47
第6章	vGW シリーズ VM のネットワーク モジュール	53
	表4: 詳細オプション	57
第7章	vGW シリーズのファイアウォール モジュール	59
	表5: ファイアウォールのポリシー構成設定	61
第10章	vGW シリーズのイントロスペクション モジュール	93
	表6: Add Enforcer Profile: ゴールド イメージとその比較対象の VM の選択	102
	表7: エンフォーサ プロファイル編集オプション	103
	表8: 許容されるゴールド イメージからの逸脱	103
	表9: アクション	103
	表10: コンプライアンス規則の指定	103
	表11: エンフォーサ イメージ スキャンの定義	104
第11章	vGW シリーズのコンプライアンス モジュール	107
	表12: コンプライアンス規則の作成パラメータ	110
第14章	vGW シリーズのアプリケーション設定	127
	表13: vNIC 毎ポリシーが有効な場合の vNIC のスマート グループ属性	153
	表14: vGW シリーズ管理者	155
第15章	vGW シリーズのセキュリティ設定	161
	表15: スマート グループ属性	174



# このガイドについて

- 目的 [xixページ](#)
- 対象読者 [xixページ](#)
- ドキュメントの表記規則 [xxページ](#)
- ドキュメントの入手 [xxページ](#)
- ドキュメントのフィードバック [xxページ](#)
- テクニカル サポートのリクエスト [xxページ](#)

## 目的

---

仮想化環境向けの Juniper Networks vGW シリーズは、VMware ESX/ESXi ホスト上の統合されたソフトウェアとして動作します。このガイドでは、vGW シリーズを VMware 環境と統合し、インストール、構成、管理する方法について説明します。また、vGW シリーズの要件を示し、アンチウィルスや IDS サポートなどのセキュリティ デザイン VM コンポーネント、それらのコンポーネントの使用方法、vGW セキュリティ デザイン VM 全体を使用して仮想化環境を管理する方法についても説明します。さらに、ファイアウォール ポリシーを作成する方法と、vGW セキュリティ VM を VMware ESX/ESXi ホストに配備してそれらのホストを保護する方法も示します。

## 対象読者

---

このガイドは以下の読者を対象とします。

- エンタープライズ ネットワークおよびセキュリティ管理者

このグループには、企業のネットワークおよびセキュリティ インフラストラクチャの担当者が含まれます。

これらの管理者は、すでに運用されている仮想化データ センターの管理や、仮想化に向けたデータ センターの整理統合、再構築を業務とします。また、プライベート クラウドやハイブリッド クラウドを使用してデータ センター内に仮想化サービスや仮想化製品を導入することもあります。

- 仮想インフラストラクチャ管理者

このグループには、仮想マシンやその他の仮想化リソースを企業またはその他の事業体に提供するクラウド サービス プロバイダが含まれます。

これらの管理者は、仮想化サーバー、ハイパーバイザ、仮想マシン、およびその他の仮想化インフラストラクチャを管理します。クラウド配置では、仮想化サーバーや仮想マシンが実行される物理リソースの管理も行います。

## ドキュメントの表記規則

---

vGW シリーズ製品の機能はほとんどがグラフィカル ユーザー インターフェースを通じて操作するため、このドキュメントにはアイコン、記号、およびナビゲーション方法に関する説明があります。

## ドキュメントの入手

---

Juniper Networks の技術ドキュメントの最新バージョンはすべて、Juniper Networks の Web サイトにある製品ドキュメント ページ (<http://www.juniper.net/techpubs>) から入手できます。

## ドキュメントのフィードバック

---

ドキュメント サービスのいっそうの充実に向けて、フィードバック、ご意見・感想、ご提案などをお寄せくださるようお願いします。 ご意見・感想は [techpubs-comments@juniper.net](mailto:techpubs-comments@juniper.net) 宛てに E メールでお送りいただくか、<https://www.juniper.net/cgi-bin/docbugreport/> にあるドキュメントのフィードバック フォームに入力できます。 E メールで送付される場合は、必ず以下の情報を記入してください。

- ドキュメントの名前
- ページ番号
- ソフトウェア リリース バージョン

## テクニカル サポートのリクエスト

---

製品のテクニカル サポートは、Juniper Networks 技術支援センター (JTAC) を通じてご利用いただけます。 お客様が現在 J-Care または JNASC のサポート契約を結んでいる場合、または保証の対象である場合は、販売後のテクニカル サポートが必要なときに、弊社のツールやリソースにオンラインでアクセスするか、または JTAC に相談できます。

- JTAC ポリシー – JTAC の利用方法やポリシーの詳細については、『JTAC ユーザー ガイド』を参照してください。このユーザー ガイドは <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf> にあります。
- 製品保証 – 製品保証に関する情報は、<http://www.juniper.net/support/warranty/> を参照してください。
- JTAC 業務時間 – JTAC センターのリソースは、1 年 365 日、週 7 日、1 日 24 時間利用できます。

## セルフヘルプ オンライン ツールおよびリソース

問題を簡単に素早く解決するために、Juniper Networks では、Customer Support Center (CSC) という名前のオンライン セルフサービス ポータルを開設し、次のサービスを提供しています。

- CSC サービスの検索: <http://www.juniper.net/customers/support/>
- 既知のバグの検索: <http://www2.juniper.net/kb/>
- 製品ドキュメントの検索: <http://www.juniper.net/techpubs/>

- 弊社の知識ベースを使用したソリューションおよび質問への回答の検索: <http://kb.juniper.net/>
- ソフトウェアの最新バージョンのダウンロードとリリース ノートの参照:  
<http://www.juniper.net/customers/csc/software/>
- 技術告示での関連するハードウェアおよびソフトウェアの通知の検索:  
<https://www.juniper.net/alerts/>
- Juniper Networks コミュニティ フォーラムへの入会と参加:  
<http://www.juniper.net/company/communities/>
- CSC Case Management ツールを使用したお問い合わせ: <http://www.juniper.net/cm/>

製品シリアル ナンバーによるサービス資格を確認するには、Serial Number Entitlement (SNE) ツール (<https://tools.juniper.net/SerialNumberEntitlementSearch/>) を使用してください。

## JTAC へのお問い合わせ

JTAC へのお問い合わせは Web サイトまたは電話でできます。

- <http://www.juniper.net/cm/> にある、CSC の Case Management ツールを使用してください。
- 電話の場合は、1-888-314-JTAC（米国、カナダ、メキシコからは無料通話サービス 1-888-314-5822 を利用可）におかけください。

通話料無料番号のない国での国別の連絡先またはダイヤル直通電話については、  
<http://www.juniper.net/support/requesting-support.html> を参照してください。



## 第1部

# vGW シリーズの概要

このパートには以下の章があります。

- [vGW シリーズの概要 3ページ](#)
- [vGW シリーズのリソース要件 11ページ](#)
- [vGW シリーズの VMware 環境との統合 15ページ](#)





# vGW シリーズの概要

この章には以下のトピックがあります。

- [vGW シリーズの理解 3ページ](#)
- [クラウド コンピューティングと vGW シリーズの理解 8ページ](#)
- [VMware インフラストラクチャと vGW シリーズの理解 9ページ](#)

## vGW シリーズの理解

---

vGW シリーズは、マルチテナントのパブリックおよびプライベート クラウド、および両者を組み合わせたハイブリッド クラウドに対して完全な仮想化セキュリティを提供します。vGW シリーズは、VMware ESX/ESXi ホスト上の統合されたソフトウェアとして動作します。vGW シリーズは以下の 2 つのメイン コンポーネントから成ります。

- 中央管理サーバーを備えた vGW セキュリティ デザイン VM。この 1 つの VM で複数の vGW セキュリティ VM が管理されます。vGW セキュリティ デザイン VM は、vGW セキュリティ VM のファイアウォール セキュリティ ポリシーの構成や ESX/ESXi ホストへの vGW セキュリティ VM の配備など、さまざまな目的に使用します。vGW セキュリティ デザイン VM の各モジュールを使用して、vGW シリーズの各種機能を構成し、配備に関する情報を表示します。35ページの「[vGW シリーズの vGW セキュリティ デザイン VM の理解](#)」を参照してください。

- 保護する各ホストにインストールされる vGW セキュリティ VM。vGW セキュリティ VM は、ホストのハイパーバイザに挿入される vGW カーネル モジュールへのパイプ役を務めます。

vGW セキュリティ VM は vGW セキュリティ デザイン VM と連携して、指定されたセキュリティ ポリシーを vGW カーネル モジュールに挿入します。仮想化ネットワーク トラフィックは、vGW カーネル モジュール内のセキュリティ ポリシーに従って保護および分析されません。

vGW セキュリティ デザイン VM は、vGW シリーズの機能を実装する以下のモジュールから成ります。画面の一番上にあるボタン バーがアクティブな機能を示します。

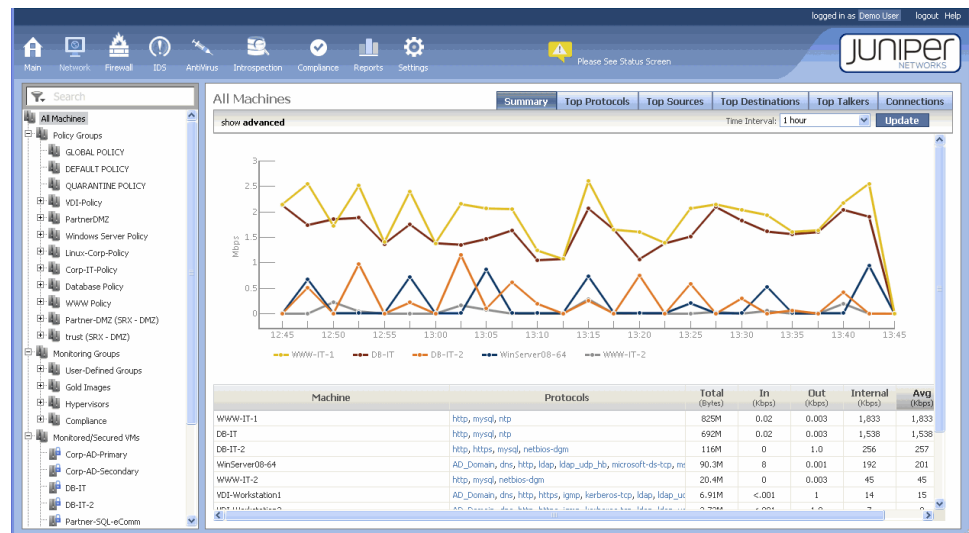
- メイン。45ページの「vGW シリーズのメイン モジュールの理解」および4ページの図1を参照してください。

図 1: メイン モジュール



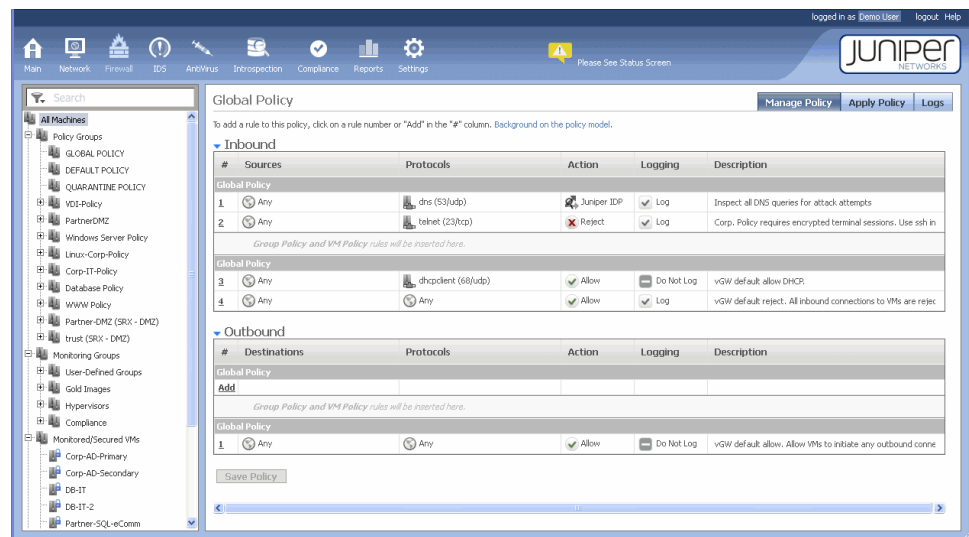
- ネットワーク。53ページの「vGW シリーズ VM のネットワーク モジュールの理解」および4ページの図2を参照してください。

図 2: ネットワーク モジュール



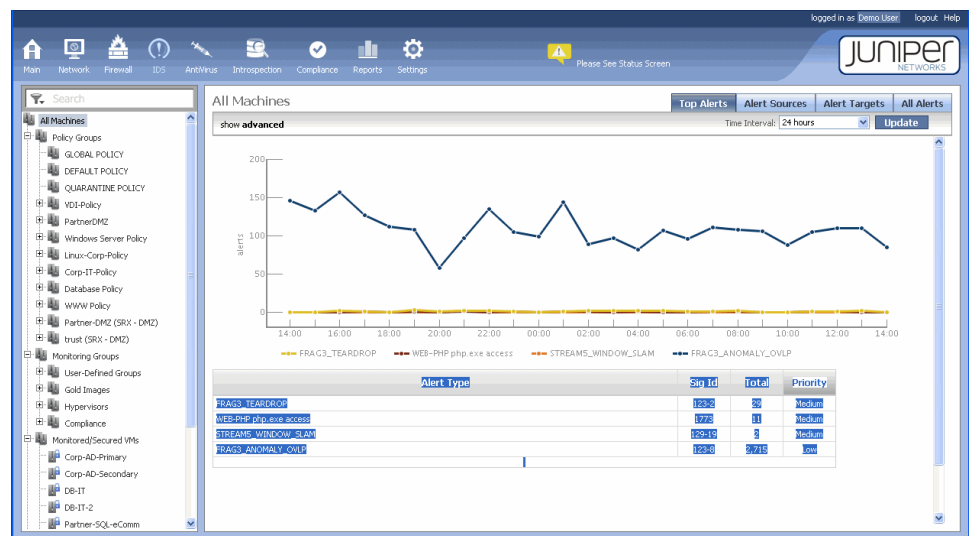
- ファイアウォール。59ページの「vGW シリーズのファイアウォール モジュールの理解」および5ページの図3を参照してください。

図 3: ファイアウォール モジュール



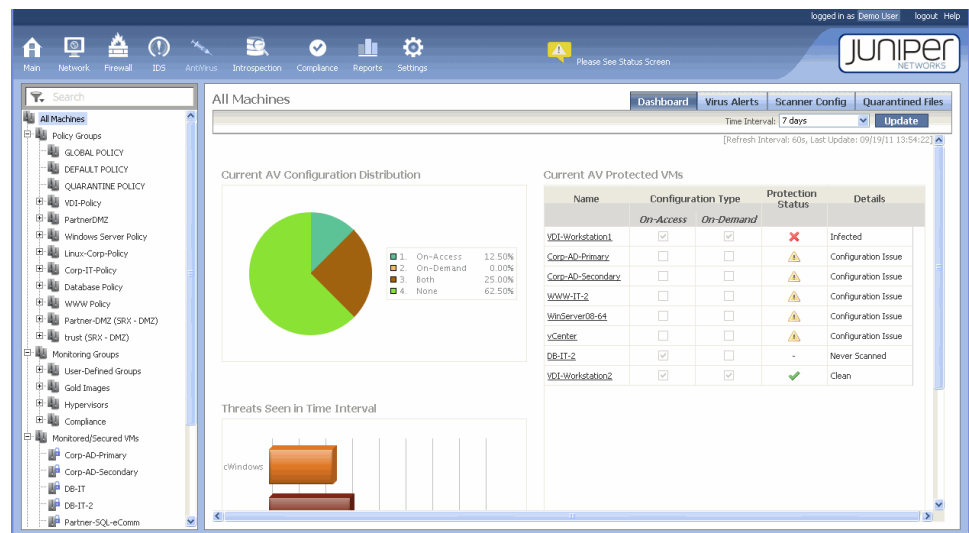
- IDS。67ページの「vGW シリーズの IDS モジュールの理解」および 5ページの図4を参照してください。

図 4: IDS モジュール



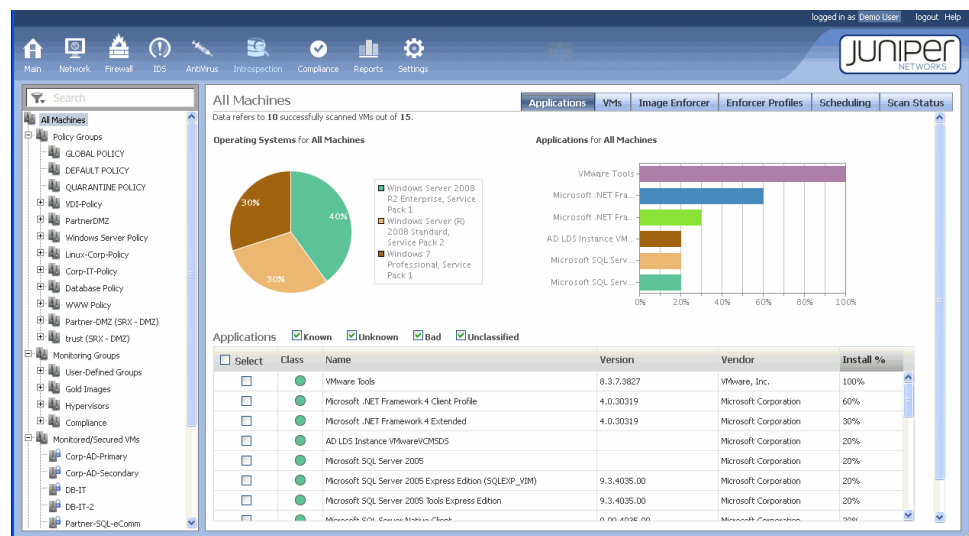
- アンチウィルス。77ページの「vGW シリーズのアンチウィルス モジュールの理解」および 6ページの図5を参照してください。

図 5: アンチウィルス モジュール。



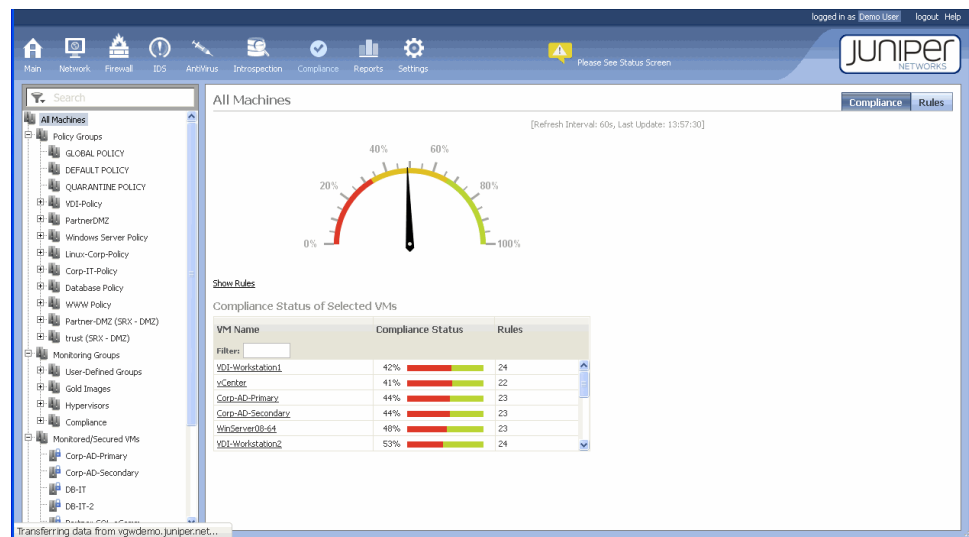
- ・イントロスペクション。93ページの「「vGW シリーズのイントロスペクション モジュールの理解」」および 6ページの図6を参照してください。

図 6: イントロスペクション モジュール



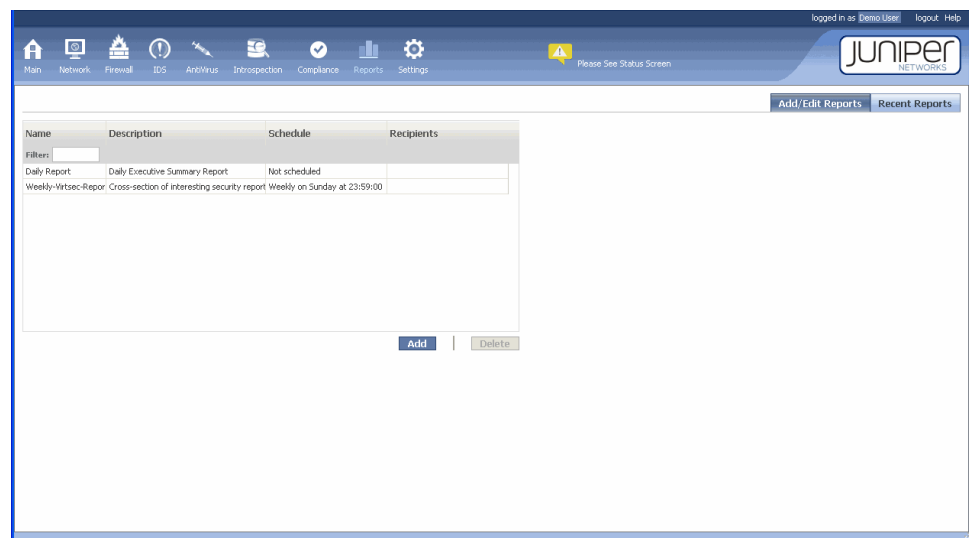
- ・コンプライアンス。107ページの「「vGW シリーズのコンプライアンス モジュールの理解」」および 7ページの図7を参照してください。

図 7: コンプライアンス モジュール



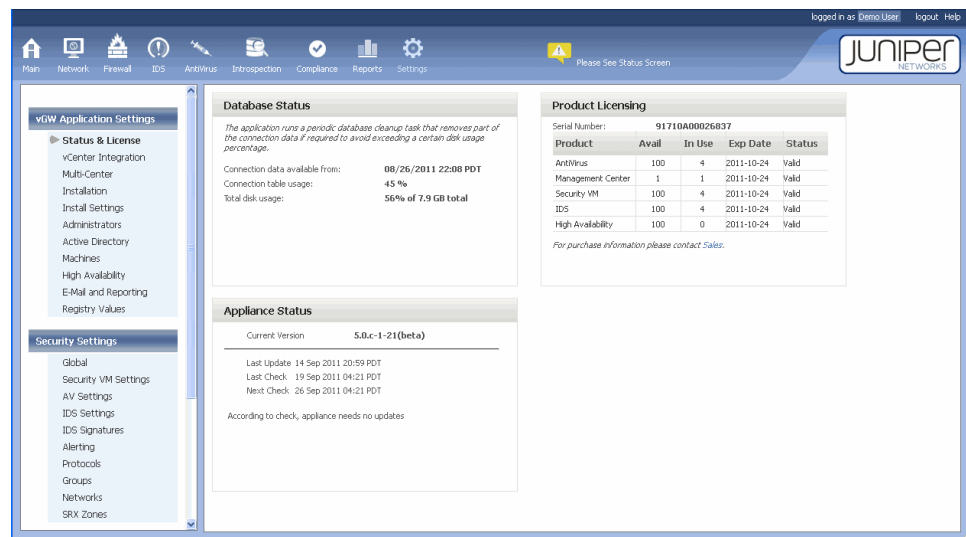
- レポート。117ページの「vGW シリーズのレポート モジュールの理解」および 7ページの図8を参照してください。

図 8: レポート モジュール



- 設定。125ページの「vGW シリーズの設定モジュールの理解」および 8ページの図9を参照してください。

図 9: 設定モジュール



- 関連項目
- 9ページのVMware インフラストラクチャと vGW シリーズの理解
  - 8ページのクラウド コンピューティングと vGW シリーズの理解
  - 16ページのVMSafe ファイアウォールおよび監視モード
  - 35ページのvGW シリーズの vGW セキュリティ デザイン VM の理解
  - 36ページのvGW セキュリティ VM の理解

## クラウド コンピューティングと vGW シリーズの理解

クラウドとは、個人や企業がインターネット接続を通じてアクセスできる、インターネットをベースとしたサーバー、ソフトウェア、アプリケーションなどの仮想化コンピューティング リソースの環境です。顧客（「テナント」と呼びます）は自社ビジネスの運営に必要なリソースにアクセスできます。

クラウドには以下のような特長があります。

- 複数の顧客が同じインフラストラクチャを共有できるため、価格やパフォーマンスの面で優位性が得られます。
- 必要なすべてのハードウェアとソフトウェアをあらかじめ自分で購入する代わりに、サービス利用時にのみ料金を支払うリース方式の投資が可能になります。
- 必要に応じてビジネスを容易に拡張し、より多くのサービスや機能を階層化できます。

仮想化データ センターは、パブリック クラウド、プライベート クラウド、ハイブリッド クラウドのいずれの場合でも、セキュリティ保護された独立した仮想マシン（VM）環境を顧客や組織に提供する必要があります。

vGW シリーズは、物理ネットワークを保護する物理的なセキュリティ メカニズムでは実現できない方法で仮想ネットワークのセキュリティを保護します。物理的なネットワーク セキュリ

ティメカニズムは物理的なハードウェアとそのソフトウェアに制限されており、仮想マシン間のトラフィック伝送や通信は可視化できません。

- 関連項目
- [3ページのvGW シリーズの理解](#)
  - [9ページのVMware インフラストラクチャと vGW シリーズの理解](#)

## VMware インフラストラクチャと vGW シリーズの理解

Juniper Networks の vGW シリーズは、VMware vSphere サーバー上の統合されたソフトウェアとして動作します。

このトピックには以下のセクションがあります。

- [vSphere と vGW シリーズの理解 9ページ](#)
- [VMware ESX および ESXi ホストと vGW シリーズの理解 9ページ](#)
- [vMotion と vGW シリーズの理解 9ページ](#)

### vSphere と vGW シリーズの理解

VMware vSphere は、ソフトウェアやハードウェアを含む仮想化コンピューティング インフラストラクチャの大規模なプールを管理できるクラウド オペレーティング システムです。vGW シリーズのコンポーネントは、VMware vSphere インフラストラクチャと統合されます。vGW シリーズは仮想化のサポートという特定の目的のために設計されているため、VMware vCenter と自動的に同期します。また、VMware の *VMsafe* インターフェースを使用して、ブレイクスルー レベルのセキュリティとパフォーマンスを提供します。

### VMware ESX および ESXi ホストと vGW シリーズの理解

VMware ESX および ESXi ホストは、仮想化 IT 環境を構築、管理するための基盤となります。これらのハイパーバイザー ベースのホストには抽象的なプロセッサ、メモリ、ストレージ、およびネットワーク リソースが含まれ、非改変オペレーティング システムやアプリケーションを実行する複数の仮想マシンの間でこれらのリソースが共有されます。

vGW シリーズは、ESX および ESXi ホストで実行される VM を管理および保護します。

### vMotion と vGW シリーズの理解

VMware には *vMotion* という機能があり、これによってアクティブな（つまり、動作中の）VM をある物理サーバーから別の物理サーバーに移動できます。VM を別のサーバーに移動する場面としては、たとえばホストの保守作業を行うときに挙げられます。また、vMotion を Dynamic Resource Scheduler (DRS) から起動することで、VM を自動的に移動することもできます。これは、システム リソースの使用状況を物理サーバーの間で均等に分散させる場合に使用します。

VM がサーバー間で移行できることから、そのセキュリティ レベルが損なわれ、新規システムのセキュリティ レベルまで低下するおそれがあります。保護されていないゾーンや信頼レベルの低いゾーンに VM が移行する可能性もあります。

従来のファイアウォールとは異なり、vGW シリーズ ファイアウォールは、開いている接続とセキュリティをイベント全体を通して維持することにより、ライブ移行をサポートします。vGW シリーズがあれば、VM の適切なセキュリティが移行中に損なわれることはありません。

- 関連項目
- [3ページのvGW シリーズの理解](#)
  - [16ページのVMSafe ファイアウォールおよび監視モード](#)
  - [195ページのvGW シリーズの高可用性ソリューションの理解](#)
  - [198ページのvGW シリーズのフォールト トレランスのサポートの理解](#)



## vGW シリーズのリソース要件

この章では、vGW シリーズを VMware 環境にインポートし、インストールして実行するために必要な前提条件とリソースについて説明します。

- [vGW シリーズの前提条件とリソース要件の理解 11ページ](#)

### vGW シリーズの前提条件とリソース要件の理解

このトピックでは、vGW シリーズ製品のインストールを準備する方法について説明します。vGW シリーズを VMware 環境にインポートし、インストールして実行するために必要な前提条件とリソースを示します。このトピックには以下のセクションがあります。

- [全体的なリソースおよびアクセス要件の理解 11ページ](#)
- [仮想アプライアンス システムの要件の理解 12ページ](#)
- [VMware vSwitch の要件の理解 13ページ](#)
- [VMware ポート グループの要件の理解 13ページ](#)
- [仮想化 NIC の要件の理解 14ページ](#)

### 全体的なリソースおよびアクセス要件の理解

以下のリソースが使用できるようにします。

- 1 台以上の vSphere ESX/ESXi 4. xx ホスト。複数のホストを使用することを推奨します。

VMware vSphere Client ソフトウェアを使用して、vGW シリーズを VMware インフラストラクチャと統合します。

- VMware Virtual Center (vCenter) Server、バージョン 2.5。

vCenter VMware 管理サーバーは、仮想化データ センターを監視します。vCenter は物理サーバーでも、MS Windows サーバーを実行している VM でも、どちらでもかまいません。

vGW シリーズは vCenter サーバーを使用して、vGW シリーズを自動的にインポートし、仮想環境に変更が加えられたときに必要に応じてセキュリティを適応させます。

- ネットワーク接続。
  - VMware Virtual Infrastructure API を利用するためには、vGW セキュリティ デザイン VM が HTTPS を通じてこの API にアクセスする必要があります。

VMware Virtual Infrastructure API へのアクセスは、VM リソースの自動検出のためにも必要です。

- VMware Virtual Infrastructure API にアクセスできるかどうかを確認するには、Web ブラウザから Virtual Center ホスト (<https://vCenter-IP-address>) に接続してみます。
- DNS および NTP サーバー（一部のコンポーネント用）。vGW セキュリティ VM には、NTP によってセンターにアクセスすることが必要です。
- 以下のサポートされている Web ブラウザのいずれかが必要です。
  - Microsoft Internet Explorer 6、7、8
  - Mozilla Firefox 2 以降



注：ブラウザのローカライズされている（英語以外の）バージョン（IE7 の日本語版など）は、完全にはサポートされていません。ただし、日本語を含むほとんどの文字セットは正しく表示されます。

## 仮想アプライアンス システムの要件の理解

vGW セキュリティ デザイン VM および vGW セキュリティ VM 仮想アプライアンスはどちらも、ネットワーク接続ストレージ（NAS）デバイスまたはローカル データ ストアを使用するよう構成できます。ただし、以下のようにすることを推奨します。

- vGW セキュリティ デザイン VM は NAS デバイスに格納し、VMotion によって移行できるようにする。

vGW セキュリティ デザイン VM は特定の ESX/ESXi ホストに拘束されないため、ホスト間で移行できます。

vGW セキュリティ デザイン VM は低速の NAS デバイスの影響を受けやすいため、注意深く監視する必要があります。

- 各 vGW セキュリティ VM は、インストール先の ESX/ESXi ホスト上のローカル データストアに格納する。

vGW セキュリティ VM は単一の ESX/ESXi ホスト上にインストールされ、常にそのホストに関連付けられます。vGW セキュリティ VM はその特定のホストに専用なので、VMotion によって移行されないように構成します。vGW セキュリティ VM を移行可能にすると、仮想化環境に問題が生じる場合があります。

前述のように、必要であれば vGW セキュリティ VM を NAS デバイスに配置してもかまいません。この場合は、vGW セキュリティ VM が VMotion によって指定ホストから移動されないようにしてください。



注：読み取り専用データストアは使用しないでください。

- 仮想アプライアンスのサイズ：
  - vGW セキュリティ デザイン VM：
    - メモリ：2 GB
    - ディスク スペース：11 GB

- vGW セキュリティ VM:
  - メモリ: 512 MB
  - ディスク スペース: 1.5 GB

## VMware vSwitch の要件の理解

VMware には、仮想スイッチ (vSwitch) と呼ばれる抽象化ネットワーク デバイスを作成する機能があります。vSwitch は内部で仮想マシン間のトラフィックをルーティングし、外部ネットワークに接続します。vSwitch の機能は物理的なイーサネット スイッチに似ており、トラフィックを正しい仮想マシンに転送するためにどの仮想マシンが vSwitch の仮想ポートに論理的に接続されているかを検出します。

物理イーサネット アダプタ (アップリンク アダプタとも呼びます) を使用して vSwitch を物理スイッチに接続し、仮想ネットワークを物理ネットワークに参加させることができます。このプロセスは、物理スイッチ同士を接続して大きなネットワークを作成するのと似ています。vSwitch は物理スイッチのように機能するとはいえ、物理スイッチの高度な機能は備えていません。

vGW シリーズに関しては、

- vSwitch を ESX/ESXi ホスト サーバー上の 1 つ以上の物理 NIC にマップできます。ただし、これは必須ではありません。
- vSwitch で QoS トラフィック シェーピングなどの機能を構成できます。

vGW シリーズは以下のタイプのスイッチと相互運用できます。

- 標準の VMware 仮想スイッチ
- VMware 分散仮想スイッチ (DVS)
- Cisco Nexus 1000V デバイス

## VMware ポート グループの要件の理解

VMware 仮想化環境では、ポート グループを使用して、複数のポートが共通の構成の下に集約されます。ポート グループは、仮想マシンがラベル付きネットワークに接続するためのアンカー ポイントです。各ポート グループはネットワーク ラベルによって識別されます。ポート グループを構成する場合は VLAN にマップすることが多いですが、これは必須ではありません。

管理者は、VM を vSwitch に接続する仮想ネットワーク インターフェース カード (NIC) をポート グループに割り当てます。

ポート グループには以下の 2 つのタイプがあります。

- 仮想マシン ポート グループ。
- VM カーネル ポート グループ。このタイプのポート グループは、vMotion や ESX/ESXi ホスト管理用のストレージに使用されます。

vGW セキュリティ デザイン VM と各 vGW セキュリティ VM の管理インターフェースとの間の通信用に指定されたポート グループを作成することを推奨します。たとえば、このポート グループに「Juniper Networks vGW Management」という名前を付けます。このポート グループを VLAN に関連付けてもかまいませんが、TCP 443 または TCP 8443 をフィルタリングしないでください。vGW セキュリティ デザイン VM のインターフェース用と各 vGW セキュリティ VM 用の IP アドレス空間が必要です。



注: この目的のために既存の VMware 管理ポート グループを使用できます。

## 仮想化 NIC の要件の理解

vNIC を構成するときは、以下の点を考慮してください。

- vGW セキュリティ VM および vGW セキュリティ デザイン VM の vNIC の構成を変更しないでください。デフォルトでは、vNIC は電源オン時に接続するよう設定されます。
- ゲスト VM (VM) は、VMware でサポートされている任意のタイプの vNIC を使用できます。たとえば、VMXNET3 を使用してパフォーマンスを向上させることが可能です。さらに、vGW シリーズは 1 つの VM に対して複数の vNIC をサポートしています。vNIC 毎ポリシー機能を使用して、これらの vNIC を異なるポリシーによって保護できます。

- 関連項目
- [3ページのvGW シリーズの理解](#)
  - [9ページのVMware インフラストラクチャと vGW シリーズの理解](#)
  - [16ページのvGW シリーズの環境時刻同期の理解](#)
  - [18ページのOVA バンドル方法を使用した vGW シリーズの VMware インフラストラクチャとの統合](#)
  - [26ページのOVA 単一ファイル方法を使用した vGW セキュリティ デザイン VM の VMware との統合](#)

## vGW シリーズの VMware 環境との統合

この章では、vGW シリーズを VMware インフラストラクチャと統合する方法について説明します。また、製品のインストールに使用する 2 つの VMSafe インストール モードについても説明します。どちらのモードでも、vGW セキュリティ デザイン VM から VMware vCenter に対して自動的に構成変更が加えられます。この自動プロセスにより、管理の複雑さが低減し、構成エラーが少なくなります。必要であれば、vGW セキュリティ デザイン VM を使用して、これらの構成変更を後で自動的に削除できます。

この章には以下のセクションがあります。

- [vGW シリーズの VMware 環境との統合の準備 15ページ](#)
- [VMSafe ファイアウォールおよび監視モード 16ページ](#)
- [vGW シリーズの環境時刻同期の理解 16ページ](#)
- [Open Virtualization Format \(OVF\) OVA テンプレート方法の理解 17ページ](#)
- [OVA バンドル方法を使用した vGW シリーズの VMware インフラストラクチャとの統合 18ページ](#)
- [OVA 単一ファイル方法を使用した vGW セキュリティ デザイン VM の VMware との統合 26ページ](#)
- [OVA 単一ファイル方法を使用した vGW セキュリティ VM の VMware との統合 27ページ](#)
- [vGW シリーズのセットアップ 28ページ](#)

### vGW シリーズの VMware 環境との統合の準備

vGW シリーズをインポートして VMware 環境にインストールする前に、以下のことを確認します。

- 運用環境の仮想マシン (VM) が相互に通信できることを確認します。これには ping コマンドを使用します。
- SSH または KVM を使用して ESX/ESXi ホストにアクセスできることを確認します。
- ネットワーク上で NTP と DNS が適切に機能していることを確認します。

- 関連項目
- [11ページのvGW シリーズの前提条件とリソース要件の理解](#)
  - [3ページのvGW シリーズの理解](#)
  - [16ページのvGW シリーズの環境時刻同期の理解](#)

## VMSafe ファイアウォールおよび監視モード

VMSafe ファイアウォールおよび監視モードまたは VMSafe 監視モードを使用して vGW セキュリティ VM を ESX/ESXi ホストにインストールするとき、vGW シリーズは VMSafe ネットワーキング API を使用してセキュリティ エンジンホストのハイパーバイザ内のカーネル モジュールとして構築します。これにより、すべてのゲスト VM (VM) の完全なプロトコル インспекションが可能となります。

VMSafe ファイアウォール モードでは、特定の VM またはポート グループ全体のセキュリティを保護できます。保護対象の各 VM を通過するすべてのトラフィックが可視化されます。VMSafe モードは仮想スイッチング層に依存しません。

VMSafe 監視モードは、セキュリティ ポリシーを vGW ハイパーバイザ カーネル モジュールにロードできない点を除いては、VMSafe ファイアウォールおよび監視インストール モードと同じです。このモードは一般に、不適切に構成されたセキュリティ ポリシーが原因でパケットがブロックされないことを保証する場合に使用します。

- 関連項目
- [3ページのvGW シリーズの理解](#)
  - [9ページのVMware インフラストラクチャと vGW シリーズの理解](#)
  - [36ページのvGW セキュリティ VM の理解](#)
  - [35ページのvGW シリーズの vGW セキュリティ デザイン VM の理解](#)

## vGW シリーズの環境時刻同期の理解

vGW シリーズは、すべてのセキュリティ ポリシーやログなどに適切なタイムスタンプが設定されるように、NTP を使用して環境内 (vCenter、ESX/ESXi ホスト、vGW シリーズ コンポーネント) のすべての時刻を同期します。システムの不適切な構成による時刻の大きなずれは、予期しない結果を招き、環境のトラブルシューティングを困難にする場合があります。

vGW セキュリティ VM の時刻設定は vGW セキュリティ デザイン VM から取得されます。



**警告:** vGW セキュリティ デザイン VM の時刻設定を直接編集しないでください (タイムゾーンを変更しないことも含む)。vGW セキュリティ VM の時刻設定は vGW セキュリティ デザイン VM から取得されます。

vGW シリーズをインストールするとき、NTP の構成に注意してください。すべての VMware コンポーネントで有効な時刻設定が使用されていることを確認します。また、内部 NTP サーバーが稼働中で正しく機能しているか、外部インターネット接続を介してインターネット タイムサーバーにアクセスできることも確認します。

詳細については、[186ページの「vGW シリーズの時刻設定の構成」](#)を参照してください。

- 関連項目
- [15ページのvGW シリーズの VMware 環境との統合の準備](#)
  - [3ページのvGW シリーズの理解](#)
  - [15ページのvGW シリーズの VMware 環境との統合の準備](#)

- [9ページのVMware インフラストラクチャと vGW シリーズの理解](#)

## Open Virtualization Format (OVF) OVA テンプレート方法の理解

vGW シリーズは、仮想マシンのパッケージ化と配信に Open Virtualization Format (OVF) 規格を利用しています。OVF は業界標準の内容検証と完全性チェックをサポートしており、ソフトウェア ライセンスを管理するための基本的な枠組みを提供します。規格で述べられているように、OVF は「仮想マシンで実行するソフトウェアをパッケージ化および配信するためのオープンかつ安全で移植性のある効率的な拡張可能フォーマット」を定義します。OVF 規格では、ソフトウェアを単一のアーカイブにパッケージ化して配信する OVA テンプレート方法もサポートされています。vGW シリーズは OVA を使用して、両方の vGW シリーズ コンポーネントを含む単一ファイルを提供します。この OVA ファイルをロードするには vSphere 4.x クライアントを使用します。

OVA を使用して、vGW シリーズ VM を以下の方法で配備できます。

- vGW セキュリティ デザイン VM と VMSafe vGW セキュリティ VM テンプレートをを含む単一のバンドル OVA パッケージ（「コンボ パッケージ」とも呼びます）。

詳細については、[18ページの「「OVA バンドル方法を使用した vGW シリーズの VMware インフラストラクチャとの統合」](#)を参照してください。

- vGW セキュリティ デザイン VM と vGW セキュリティ VM テンプレートを別々に配備する、バンドルされていない OVA ファイル。

OVA コンボ パッケージは vApp をインストールしますが、VMware は DRS が有効になっていないクラスタには vApp をインストールしません。

バンドルされていない OVA を使用する方法は、初期インストールの後に最新の vGW セキュリティ VM をインストールするためにも役立ちます。こうすると、ESX/ESXi ホストでの自動的な vGW セキュリティ VM のインスタンス化に常に最新バージョンが使用されるようになります。

- 単一の OVA ファイルを使用して vGW セキュリティ デザイン VM を配備する方法の詳細については、[26ページの「「OVA 単一ファイル方法を使用した vGW セキュリティ デザイン VM の VMware との統合」](#)を参照してください。
- 単一の OVA ファイルを使用して vGW セキュリティ VM を配備する方法の詳細については、[27ページの「「OVA 単一ファイル方法を使用した vGW セキュリティ VM の VMware との統合」](#)を参照してください。

- 関連項目
- [3ページのvGW シリーズの理解](#)
  - [15ページのvGW シリーズの VMware 環境との統合の準備](#)
  - [9ページのVMware インフラストラクチャと vGW シリーズの理解](#)

## OVA バンドル方法を使用した vGW シリーズの VMware インフラストラクチャとの統合

このトピックでは、vGW シリーズ アプライアンス - vGW セキュリティ デザイン VM と vGW セキュリティ VM - を VMware 仮想化インフラストラクチャと統合する方法について説明します。

このトピックには以下のセクションがあります。

- [前提条件 18ページ](#)
- [概要 18ページ](#)
- [vGW シリーズ OVA コンボ パッケージのダウンロード 19ページ](#)
- [vGW シリーズの VMware インフラストラクチャとの統合 19ページ](#)

### 前提条件

詳細については、11ページの「[「vGW シリーズの前提条件とリソース要件の理解」](#)」を参照してください。

### 概要

バンドル OVA テンプレートを使用すると、vGW セキュリティ デザイン VM と vGW セキュリティ VM の両方を単一の OVA アーカイブ ファイルによって配備できます。この場合、OVA は単一の vApp を作成し、2 つの vGW シリーズ VM アプライアンスをその中に挿入します。

この vApp は、配備および統合プロセスが完了した後に削除できます。この vApp は vGW シリーズ VM を運ぶためにのみ使用されます。ただし、vGW シリーズ VM の配備と統合が済むまで削除しないよう注意してください。

単一のコンボ パッケージ ファイルでは、OVA テンプレートによって以下が配備されます。

- vGW セキュリティ デザイン VM
- VM Safe vGW セキュリティ VM

vGW シリーズを VMware インフラストラクチャと統合した後に、vGW セキュリティ VM をテンプレートに手動で変換する必要があります。この変換後のテンプレートを使用して、保護する各 ESX/ESXi ホスト上に vGW セキュリティ VM が自動的にインスタンス化されます。

- OVA コンボ パッケージは vApp をインストールしますが、VMware は DRS が有効になっていないクラスタには vApp をインストールしません。この場合は、バンドルされていない OVA を使用して各コンポーネントを別々に配備する必要があります。
- 単一の OVA ファイルを使用して vGW セキュリティ デザイン VM を配備する方法の詳細については、26ページの「[「OVA 単一ファイル方法を使用した vGW セキュリティ デザイン VM の VMware との統合」](#)」を参照してください。
- 単一の OVA ファイルを使用して vGW セキュリティ VM を配備する方法の詳細については、27ページの「[「OVA 単一ファイル方法を使用した vGW セキュリティ VM の VMware との統合」](#)」を参照してください。



## vGW シリーズ OVA コンボ パッケージのダウンロード

ステップごとの手順 ここでは、vGW シリーズ アプライアンスを含む OVA コンボ パッケージを Juniper Networks ダウンロード サイトからダウンロードする手順を示します。

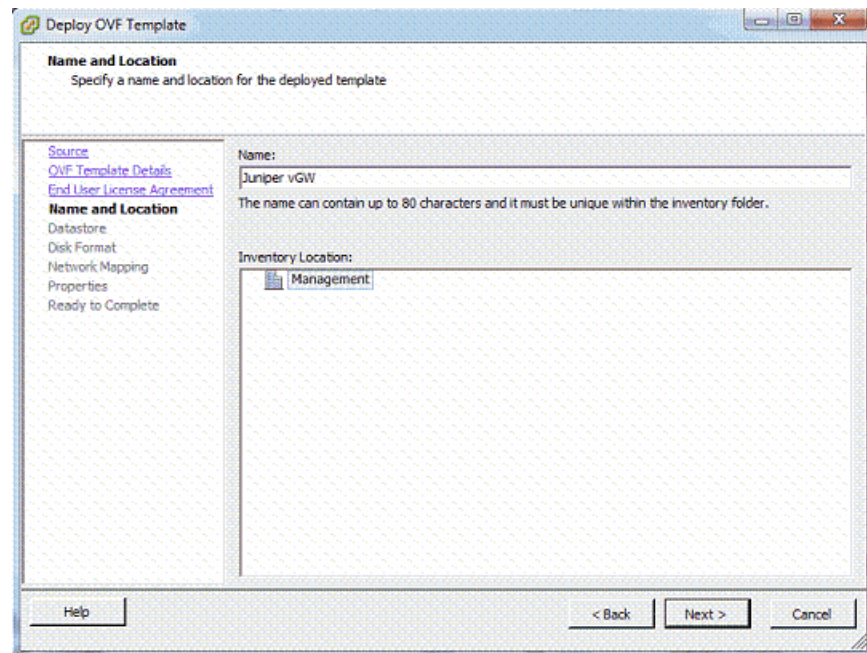
vGW セキュリティ デザイン VM と vGW セキュリティ VM の両方を含む Juniper Networks OVA アーカイブ ファイルをダウンロードするには、以下の手順に従います。

1. Juniper Networks サポート ページに移動します。
  - [Support] ボックスの左列で、[Download Software] を選択します。
  - [Security] セクションで、[vGW (Altor)] を選択します。
  - [Software] タブを選択します。
  - [vGW Series 5.0 Combo Package] をクリックし、サイトにログインしてファイルをダウンロードします。

## vGW シリーズの VMware インフラストラクチャとの統合

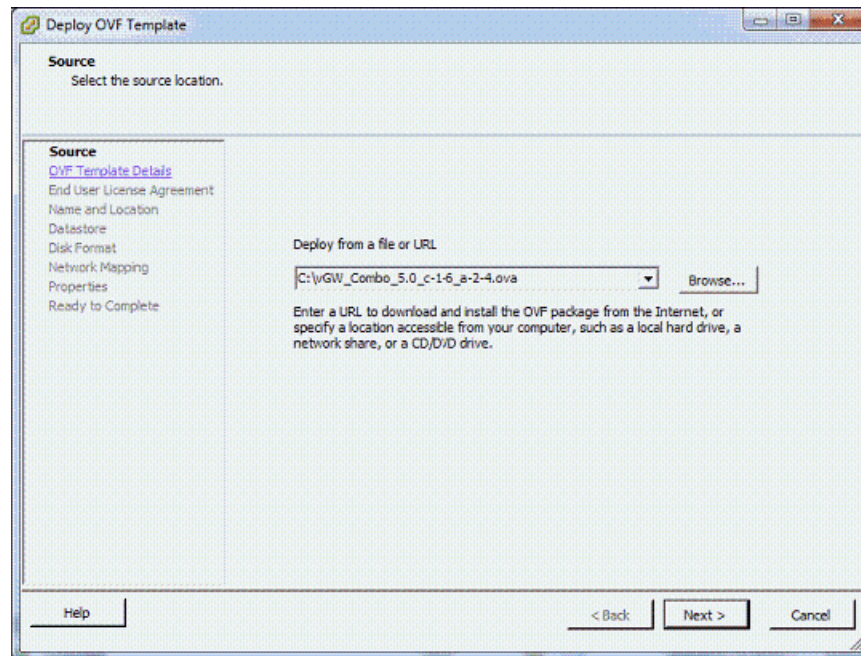
ステップごとの手順 vGW シリーズ仮想アプライアンス - vGW セキュリティ デザイン VM と vGW セキュリティ VM - を配備して VMware インフラストラクチャと統合するには、以下の手順に従います。

1. vSphere 4.x クライアントを使用して、バンドル OVA ファイルをロードします。[File] メニューから [Deploy OVF Template] を選択します。



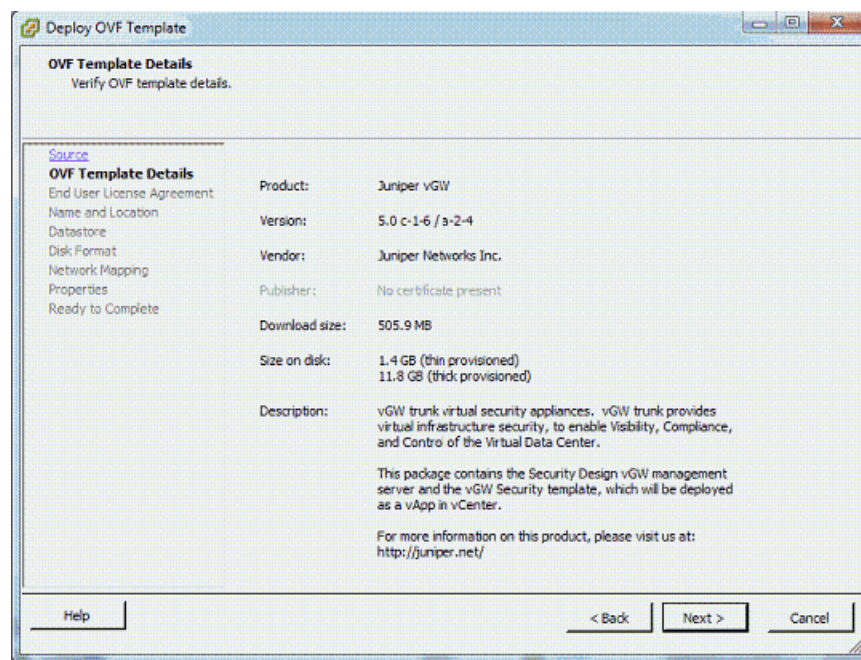
2. [Deploy from File or URL] フィールドにダウンロード ファイルの名前またはその URL (例: c:\temp¥vGW\_Combo\_5.0\_#-#-#-#-#.ova) を入力し、[Next] をクリックします。

OVA ファイルの名前と場所を指定したら、アプライアンス ウィザードに OVA テンプレートの詳細ページが表示されます。

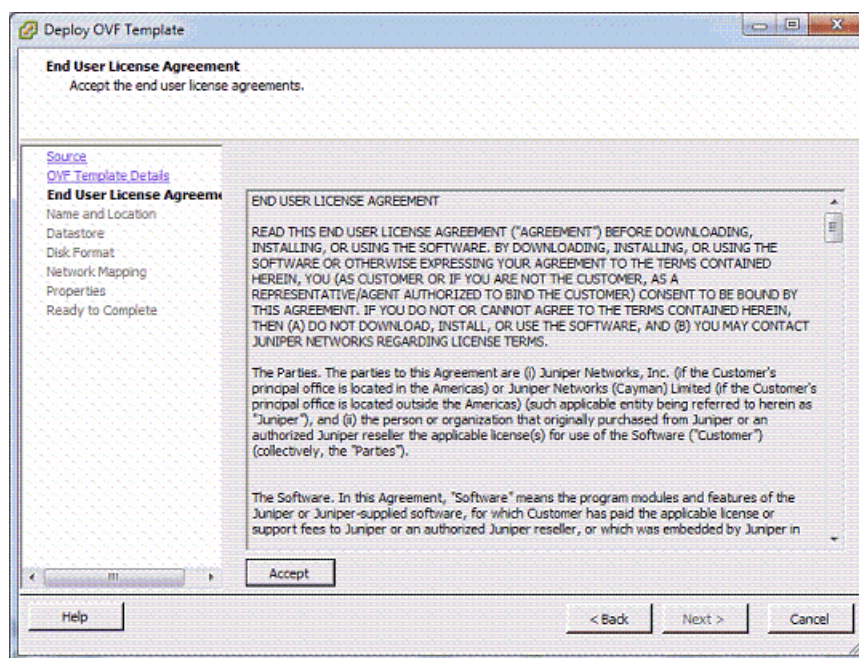


3. OVA パッケージの内容を確認し、[Next] をクリックします。

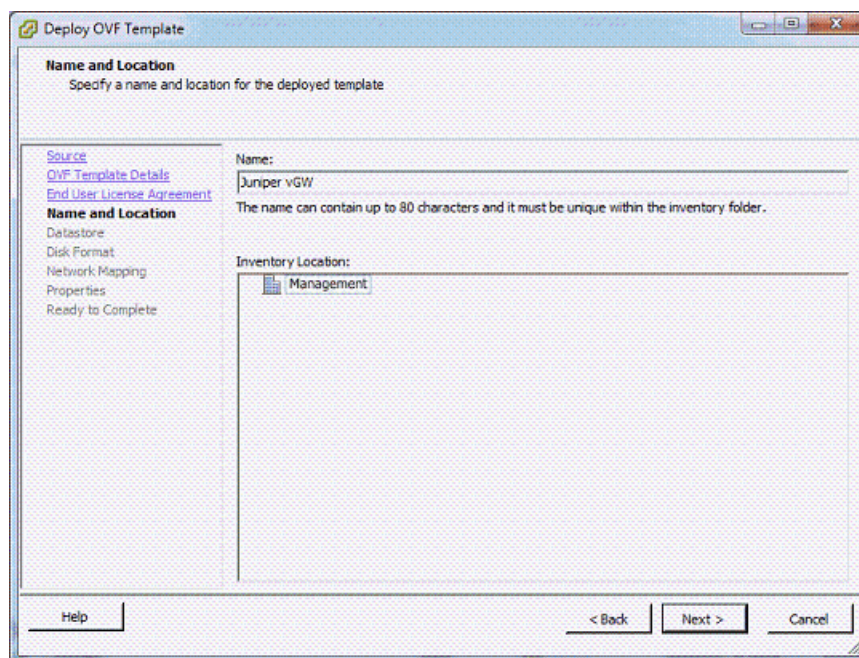
OVA パッケージのバンドルを解除する前に、vGW シリーズ アプライアンスがパッケージに含まれていることを確認します。OVA テンプレートの概要情報には、シック プロビジョニングおよびシン プロビジョニングに必要なディスク容量も示されます。



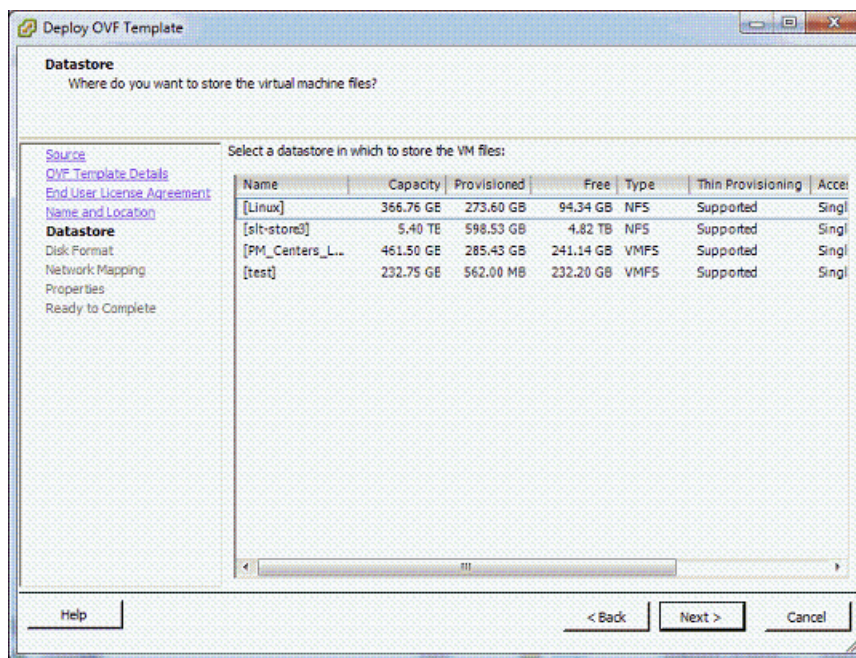
4. vGW シリーズの使用許諾契約に同意し、[Next] をクリックします。



5. 作成する vApp の名前と保存する場所を指定します。

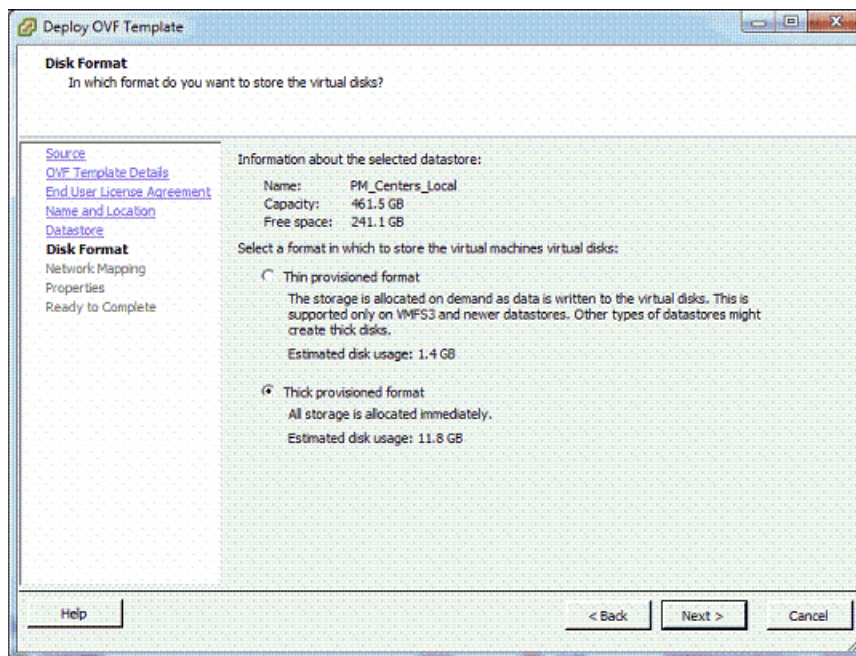


6. 配備したテンプレートを実行するホストまたはクラスタを指定します。

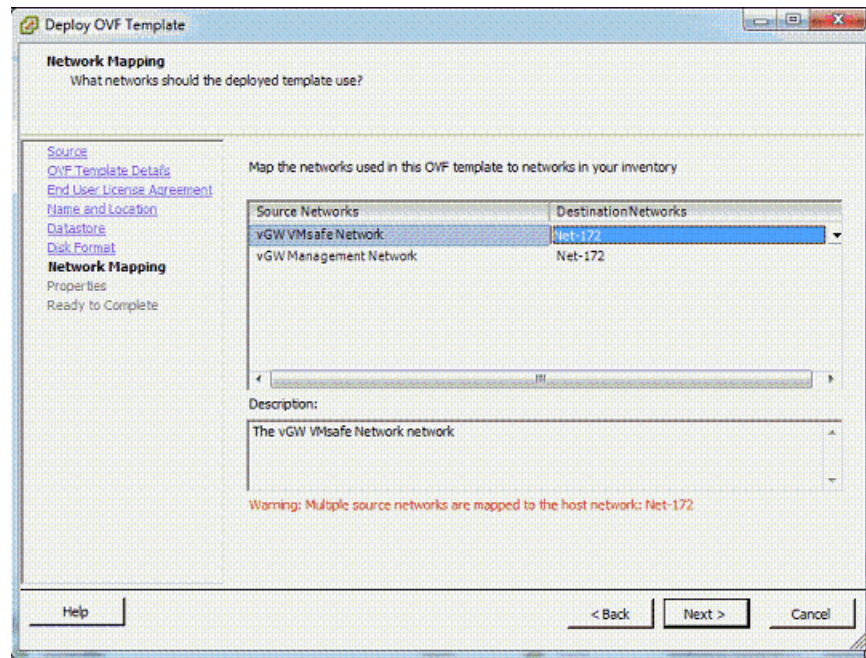


7. ディスク フォーマットを選択します。デフォルトのシック プロビジョン フォーマットをそのまま使用します。

シック プロビジョニングでは、その製品に必要なすべての容量があらかじめ割り当てられます。



8. ネットワークをマップします。vGW 管理ネットワークを、vCenter および vGW セキュリティ デザイン VM にアクセス可能な宛先ネットワークに設定します。



9. vGW シリーズ ファイルの保存に使用するデータベースのサイズを指定します。

このデータベースには、ネットワーク接続レコードやファイアウォール ログが保存されます。データベースの保存にはネットワーク ストレージ デバイス (NAS) を使用することを推奨します。そうすると、領域最適化のために vMotion によってデータベースを移行できます。

デフォルトのディスク サイズは 8.0 GB です。5 ~ 10 台の ESX/ESXi ホストを含む標準的な環境では、このサイズのデータベースで数か月分の累積データを格納できます。ただし、実際の運用環境に合わせてデータベースのサイズを 8.0 GB 以上にしてもかまいません。

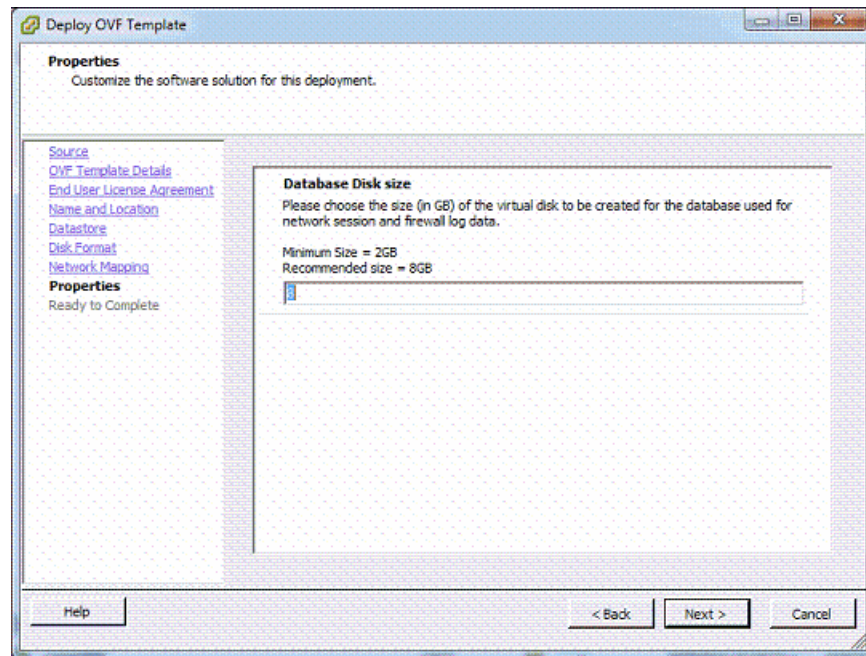
現在の容量が十分でない場合は、後でデータベースのサイズを増やすことができます。ハードコードされた制限はありませんが、75 GB 未満のサイズに抑えることを推奨します。

このディスクはシン プロビジョニングしないでください。





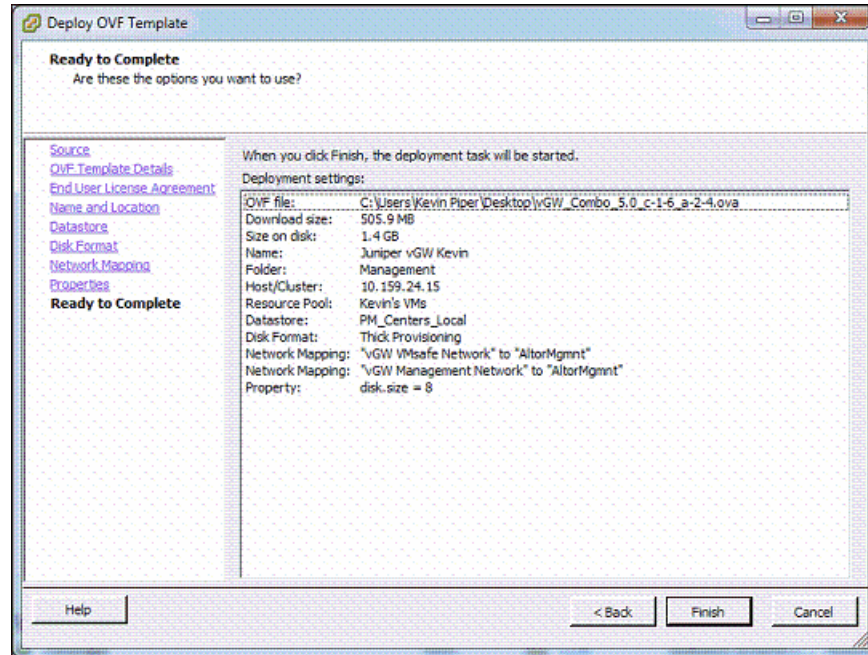
注: 読み取り専用データ ストアは使用しないでください。



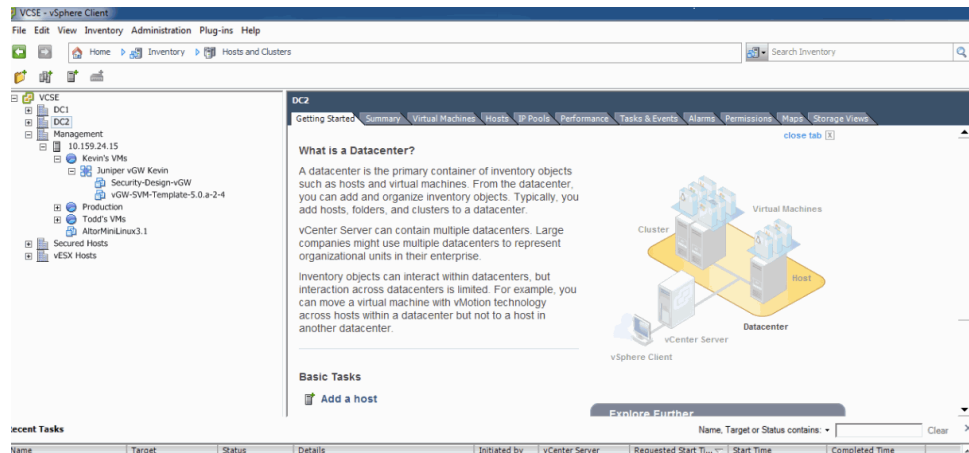
10. 構成が正しいことを確認し、[Finish] をクリックして配備を完了します。

仮想アプライアンス ウィザードによってファイルがダウンロードされ、vGW シリーズ VM が単一の仮想アプライアンス (vApp) として VMware インフラストラクチャに挿入されます。

OVA インポートが完了したら、vCenter に「Juniper vGW」という名前の vApp が追加されます。この vApp には、vGW セキュリティ デザイン VM と vGW セキュリティ VM テンプレート コンポーネントの両方が含まれます。



11. Juniper vGW アプライアンスを展開すると、vGW セキュリティ デザイン VM と vGW セキュリティ VM が表示されます。



これら 2 つの vGW シリーズ VM をここから移動した後、vApp を削除できます。この vApp の名前は「Juniper Networks」であるか、またはインポート プロセス中に指定した名前です（vApp を削除することは必須ではありません）。



注: vGW シリーズ VM を移動する前に vApp を削除しないでください。そうすると、新しく作成された vGW シリーズ VM が削除されます。

- vGW-SVM-Template VM を、保護する各 ESX/ESXi ホスト用の vGW セキュリティ VM をインスタンス化するために vGW セキュリティ デザイン VM およびインストーラが使用できるテンプレートに変換します。テンプレートを右クリックし、[Convert to Template] を選択します。
- vGW セキュリティ デザイン VM を右クリックし、この VM の電源をオンにします。

- 関連項目
- [3ページのvGW シリーズの理解](#)
  - [9ページのVMware インフラストラクチャと vGW シリーズの理解](#)

## OVA 単一ファイル方法を使用した vGW セキュリティ デザイン VM の VMware との統合

このトピックでは、vGW セキュリティ デザイン VM を含む単一の OVA ファイルをダウンロードして配備する方法について説明します。

vGW セキュリティ デザイン VM アプライアンスを含む OVA ファイルをダウンロードするには、以下の手順に従います。

1. Juniper Networks vGW OVA ファイルをダウンロードします。
  - Juniper Networks サポート ページに移動します。
  - [Support] ボックスの左列で、[Download Software] を選択します。
  - [Security] セクションで、[vGW (Altor)] を選択します。
  - [Software] タブを選択します。
  - [Security Design vGW 5.0] をクリックし、サイトにログインしてファイルをダウンロードします。
2. vSphere 4.x クライアントを使用して vGW セキュリティ デザイン VM 用の OVA ファイルをロードし ([File] > [Deploy OVF Template])、[Deploy from File or URL] フィールドに OVA ダウンロード ファイルの名前を入力します。  
たとえば、c:\temp\SecurityDesignvGW.ovf と入力します。
3. 仮想アプライアンス ウィザードの指示に従い、運用環境に適切なオプションを選択します。
4. [Finish] をクリックし、ファイルをダウンロードして vGW セキュリティ デザイン VM を VMware インフラストラクチャと統合します。

vGW セキュリティ デザイン VM のインポート プロセスが完了したら、次にこの VM 用の仮想ハード ディスクを追加する必要があります。



**注:** バンドル方法ではこのステップは自動的に実行されるため、ユーザーが行う必要はありません。

5. データストアとして使用するディスクを追加します。
  - [vGW Security Design VM] を選択します。



- [Summary] タブを選択し、[Edit Settings] > [Add a Hard Disk virtual device] の順にクリックします。

このディスクは、ネットワーク接続レコードやファイアウォール ログを保存するデータベースに使用されます。vMotion を使用してデータ ストアを移行できるように、ネットワーク アクセス ストレージ (NAS) を選択します。

デフォルトのディスク サイズは 8.0 GB です。5 ~ 10 台の ESX/ESXi ホストを含む標準的な環境では、このサイズのデータベースで数か月分の累積データを格納できます。

実際の運用環境に合わせてデータベースのサイズを 8.0 GB 以上にしてもかまいません。現在の容量が十分でない場合は、後でデータベースのサイズを増やすことができます。このディスクはシン プロビジョニングしないでください。

6. vGW セキュリティ デザイン VM の電源をオンにします。

- 関連項目
- [27ページのOVA 単一ファイル方法を使用した vGW セキュリティ VM の VMware との統合](#)
  - [18ページのOVA バンドル方法を使用した vGW シリーズの VMware インフラストラクチャとの統合](#)
  - [15ページのvGW シリーズの VMware 環境との統合の準備](#)
  - [11ページのvGW シリーズの前提条件とリソース要件の理解](#)

## OVA 単一ファイル方法を使用した vGW セキュリティ VM の VMware との統合

このトピックでは、vGW セキュリティ VM を含むバンドルされていない OVA ファイルをダウンロードして配備する方法について説明します。

vGW セキュリティ VM アプライアンスを含む OVA ファイルをダウンロードするには、以下の手順に従います。

1. VMware vSphere Client を使用して vGW セキュリティ VM 用の OVA ファイルをロードし ([File] > [Deploy OVF Template])、[Deploy from File or URL] フィールドにテンプレート名 vGW-SVM-Template を入力します。たとえば、c:\temp\vGW-SVM-Template.ova と入力します。

2. 仮想アプライアンス ウィザードに示された各ステップで、運用環境に適切なオプションを選択します。

運用環境に適切なホスト/クラスターやリソース プールなどを構成します。

ネットワーク マッピング情報を指定するよう求められたら、デフォルトの設定をそのまま使用します。これらの設定は後で自動的に構成されます。

3. 仮想アプライアンス ウィザードが完了したら、作成された VM を右クリックして [Convert to Template] を選択します。

変換後のテンプレートを使用して、仮想ネットワーク上の保護する ESX/ESXi ホストに vGW セキュリティ VM を自動的にインストールできます。vGW セキュリティ デザイン VM およびインストーラは、保護するホスト上で vGW セキュリティ VM をインスタンス化するためにこのテンプレートを必要とします。

- 関連項目
- 26ページのOVA 単一ファイル方法を使用した vGW セキュリティ デザイン VM の VMware との統合
  - 18ページのOVA バンドル方法を使用した vGW シリーズの VMware インフラストラクチャとの統合
  - 15ページのvGW シリーズの VMware 環境との統合の準備
  - 11ページのvGW シリーズの前提条件とリソース要件の理解

---

## vGW シリーズのセットアップ

vGW シリーズをダウンロードして配備し、vGW セキュリティ デザイン VM の電源をオンにした後、vGW セキュリティ デザイン VM の IP アドレスなどの基本的なオペレーティング システム パラメータを構成できます。vGW セキュリティ デザイン VM には Web ブラウザを使用してアクセスします。

vCenter サーバーから IP アドレスを確認するには、vCenter コンソールで [vGW Security Design VM] を選択し、[Summary] タブを選択します。また、[Console] タブを使用して IP アドレスを表示することもできます。

vGW セキュリティ デザイン VM ネットワークで DHCP が使用できない場合は、以下の手順に従います。

1. ユーザー名とパスワードの両方に admin と入力して、コンソールにログインします。図を参照
2. コマンド プロンプトで config network と入力し、IP アドレスを割り当てるオプションを指定します。

IP アドレスが DHCP によって設定されている場合、または静的な IP アドレスが割り当てられている場合は、Web ブラウザを使用して vGW セキュリティ デザイン VM にアクセスできます。

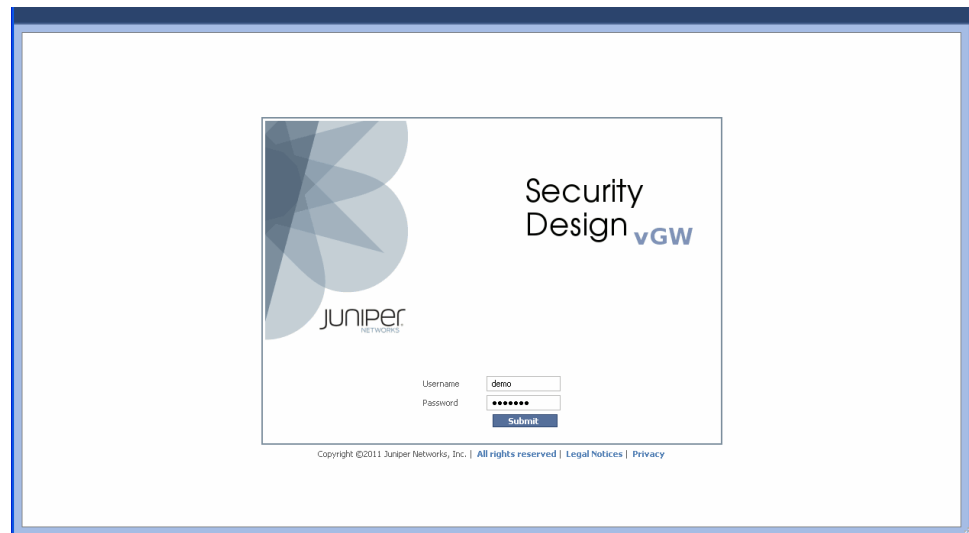
3. サポートされている Web ブラウザを使用し、HTTPS によって vGW セキュリティ デザイン VM 管理インターフェースに接続します。

ユーザー名とパスワードの両方に admin と入力します。29ページの図10を参照してください。

サポートされている Web ブラウザは次のとおりです。

- Internet Explorer 6、7、8
- Firefox 2 以降

図 10: vGW シリーズ セキュリティ デザイン VM のログイン画面



4. 情報メッセージを読み、[Wizard Progress] セクションに表示されたプロセス概要を確認します。
5. ログインに使用したデフォルトの vGW グローバル管理アカウント (admin) を変更します。  
デフォルト パスワードを変更する必要があります。新しいパスワードを安全な場所に保管します。パスワードを紛失または失念した場合、パスワードを回復するのは困難です。



**ヒント:** インストールが完了した後、管理アカウントを vGW セキュリティ デザイン VM と統合できます。

6. vGW セキュリティ デザイン VM のネットワーキング パラメータを構成します。  
vGW 管理ネットワークの正しい宛先ネットワークを設定し、VMsafe ネットワークはそのままにします。
7. IP アドレスを変更した場合は、システムに再度ログインする必要があります。IP アドレスの変更はただちに反映されます。



**注:** このとき、DNS サーバーのエントリが確認されます。警告メッセージは無視して問題ありません。

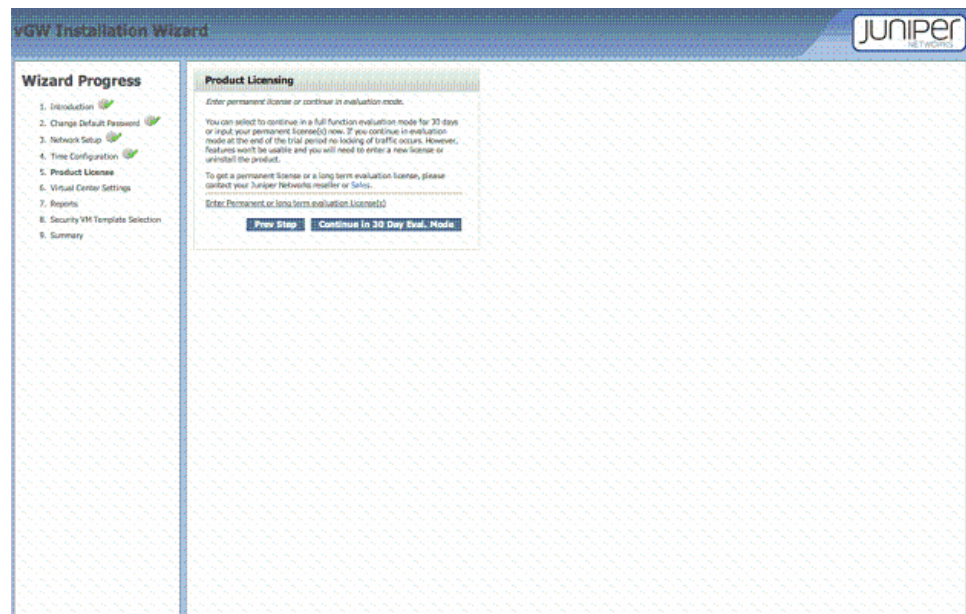
8. システム時刻を設定します。  
正しいタイムゾーンを設定してから、運用環境の NTP サーバーを指定します。  
vGW シリーズ コンポーネントが機能するためには、すべての ESX/ESXi ホストに正しいシステム時刻が設定されている必要があります。  
NTP サーバーがない場合は、事前定義されたサーバーを使用できます。外部インターネット接続を介して NTP サーバーにアクセスできず、内部 NTP サーバーもない場合は、この

ウィンドウに表示されたすべてのエントリをクリアして、時刻を手動で設定する必要があります。

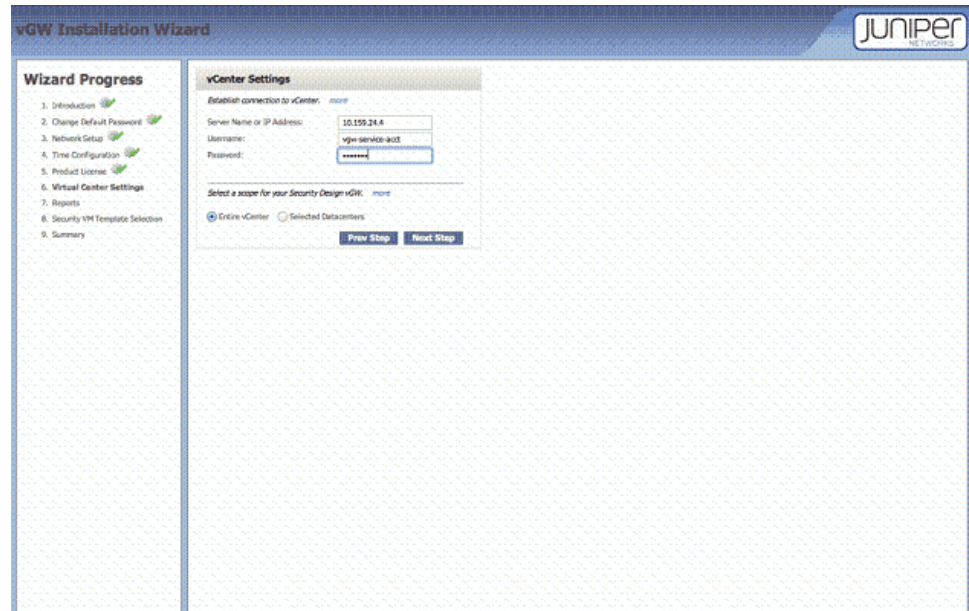
時刻を手動で設定するには、コンソールにログインし、vGW シリーズ コマンドライン ユーティリティを使用します。

この時点で、データベース ディスクが作成済みで適切に初期化されているかどうかを確認されます。データベース ディスクが適切に定義されていない場合は、メッセージが表示されます。

30 日評価ライセンスを使用している場合は、引き続きこのモードで vGW シリーズを使用するか、永続ライセンスを入力するかを選択できます。



9. 適切な認証情報を入力して [Next] をクリックし、認証テストを実行します。



vGW シリーズから vCenter に VM インベントリやその他の操作を照会するには、読み取りおよび書き込みアクセス権のあるアカウントが必要です。

- 適切に接続された場合は、ESX/ESXi ホストと検出された VM の数を示すメッセージが表示されます。
- 接続に問題がある場合は、そのように通知されます。その場合は、使用した資格情報が正しいこと、IP によって vCenter システムに接続できることを確認します。

場合によっては、別の vNIC を vGW セキュリティ デザイン VM に挿入しなければならないことがあります。そのような場合は、その vNIC を使用して、vCenter サーバーに接続するネットワークに接続する必要があります。

10. 必要に応じて、レポートの送信に使用する E メール サーバーを構成します。

このオプションを使用すると、vGW シリーズから E メールによってシステム アクティビティに関するレポートを送信できます。また、レポートで使用する基本情報（標準レポート Eメールの件名や内容など）を構成することもできます。これらのパラメータを構成した後、Eメール接続をテストできます。

この情報は後で構成することも、vGW セキュリティ デザイン VM 設定モジュールの [Application Settings] セクションを使用してインストールの完了後に変更することも可能です。

11. 運用環境を保護する vGW セキュリティ VM を配備するためのテンプレートを定義します。

vGW セキュリティ VM のダウンロードとテンプレートへの変換をまだ行っていない場合は、今すぐ行います。以下を定義できます。

- VMSafe カーネル モジュールをロードできない ESX/ESXi ホスト、または VMSafe カーネル モジュールが存在しない ESX/ESXi ホストに VM が接続しようとしたときに vGW シリーズがどのように反応するか。

- VMSafe 監視モード インストール画面が表示されるかどうか。

vGW シリーズを監視モードで配備する場合を除き、VMSafe の監視のみオプションはオフのままにします。

また、vGW シリーズのロードに失敗したときに VM へのネットワーク トラフィックをドロップする場合を除き、Allow All トラフィックのデフォルト オプションはそのままにします。このオプションは後で、1 つ以上の VM の動作を変更したい場合に変更できます。

12. [Done] をクリックして、vGW セキュリティ デザイン VM のセットアップを完了します。

vGW セキュリティ デザイン VM が表示されます。 このモジュールを使用して、保護する ESX/ESXi ホストへの vGW セキュリティ VM の配備、その他の vGW シリーズ機能の構成、特定の結果や結果の要約を示す情報やレポートの表示を行うことができます。

関連項目    • [3ページのvGW シリーズの理解](#)

## 第2部

# vGW シリーズの構成と管理

このパートには以下の章があります。

- vGW セキュリティ デザイン VM の概要 35ページ
- vGW シリーズのメイン モジュール 45ページ
- vGW シリーズ VM のネットワーク モジュール 53ページ
- vGW シリーズのファイアウォール モジュール 59ページ
- vGW シリーズの IDS モジュール 67ページ
- vGW シリーズのアンチウィルス モジュール 75ページ
- vGW シリーズのイントロスペクション モジュール 93ページ
- vGW シリーズのコンプライアンス モジュール 107ページ
- vGW シリーズ VM のレポート モジュール 117ページ
- vGW シリーズの設定モジュール 125ページ
- vGW シリーズのアプリケーション設定 127ページ
- vGW シリーズのセキュリティ設定 161ページ
- vGW セキュリティ デザインのアプライアンス設定 183ページ
- vGW シリーズのステータス アラート 193ページ
- 高可用性とフォールト トレランス 195ページ





## vGW セキュリティ デザイン VM の概要

この章には以下のトピックがあります。

- [vGW セキュリティ デザイン VM の理解 35ページ](#)
- [vGW セキュリティ VM の理解 36ページ](#)
- [vGW セキュリティ デザイン VM のナビゲーションの理解 37ページ](#)
- [vGW セキュリティ デザイン VM のナビゲーション ボタン バーの理解 39ページ](#)
- [vGW セキュリティ デザイン VM のツリーについて 40ページ](#)

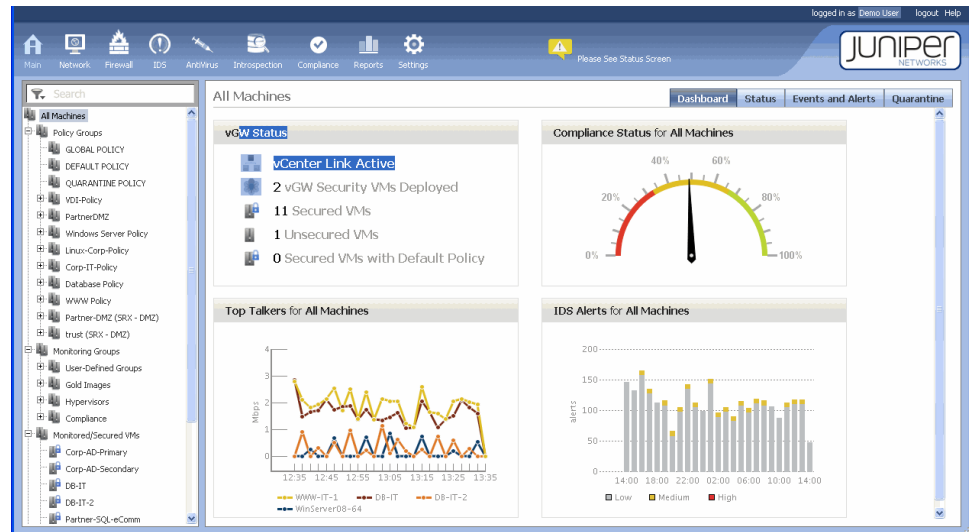
### vGW セキュリティ デザイン VM の理解

vGW シリーズには、vGW セキュリティ デザイン VM という管理サーバーが含まれます。vGW セキュリティ デザイン VM を使用すると、セキュリティ ポリシーの操作やネットワーク トラフィックの分析ができ、管理者が定期的に使用する運用環境に関する詳細情報を表示できます。また、ファイアウォール ポリシーを作成し、保護する ESX/ESXi ホスト上の vGW セキュリティ VM にそれらのポリシーをインストールすることも可能です。

vGW を構成するには、vGW セキュリティ デザイン VM 管理センターを使用します。vGW セキュリティ デザイン VM へのアクセスには Web インターフェース ブラウザを使用する必要があります。vGW セキュリティ デザイン VM へのアクセスに必要な IP アドレスを確認するには、VMware で vGW セキュリティ デザイン VM アプライアンスのサマリ タブをクリックします。

vGW セキュリティ デザイン VM を初めて起動した後、vGW セキュリティ デザイン VM にアクセスするには、ユーザー名に admin と入力し、インストール時に設定したパスワードを入力します。vGW セキュリティ デザイン VM からログアウトするには、vGW セキュリティ デザイン VM 画面の右上隅にある [logout] をクリックします。

vGW セキュリティ デザイン VM にログインすると、メイン モジュール画面とその [Dashboard] タブが表示されます。



この画面には、各種 vGW モジュールから収集された情報が表示されます。以下のトピックで、表示される各 vGW モジュールの情報を制御するためのコンポーネントについて説明します。

- [39ページのvGW セキュリティ デザイン VM のナビゲーション ボタン バーの理解](#)
- [40ページのvGW セキュリティ デザイン VM のツリーについて](#)
- [vGW セキュリティ デザイン VM のアイコンについて](#)

関連項目    • [3ページのvGW シリーズの理解](#)

## vGW セキュリティ VM の理解

ネットワーク トラフィックを収集して保護するため、監視および保護対象の各 ESX ホストに vGW セキュリティ VM が配備されます。vGW セキュリティ VM は、自身が実行されている ESX/ESXi ホストを保護および監視し、vGW セキュリティ デザイン VM に情報を報告します。

vGW セキュリティ VM は、vGW セキュリティ デザイン VM を使用して配備します。1 つの vGW セキュリティ デザイン VM で複数の vGW セキュリティ VM が管理されます。管理者はこの管理サーバーにログインし、セキュリティ ポリシーを構成して vGW セキュリティ VM に配備します。

- 関連項目
- [163ページのvGW セキュリティ VM の設定モジュールの理解](#)
  - [197ページの高可用性のためのセカンダリ vGW セキュリティ VM のインストール](#)
  - [143ページのESX/ESXi ホストへの vGW セキュリティ VM の配備](#)

## vGW セキュリティ デザイン VM のナビゲーションの理解

vGW セキュリティ デザイン VM ボタン バーを VM ツリーとともに使用します。これら 2 つを組み合わせることで、使用する vGW モジュールを選択してから、選択した VM の情報を表示したり、VM を構成したりできます。37ページの図11 および 38ページの図12を参照してください。

図 11: ボタン バー

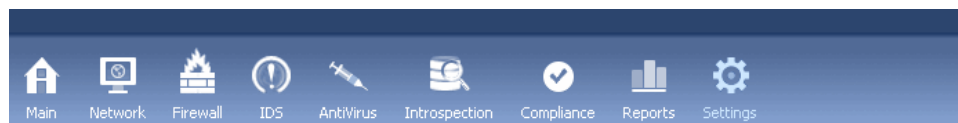
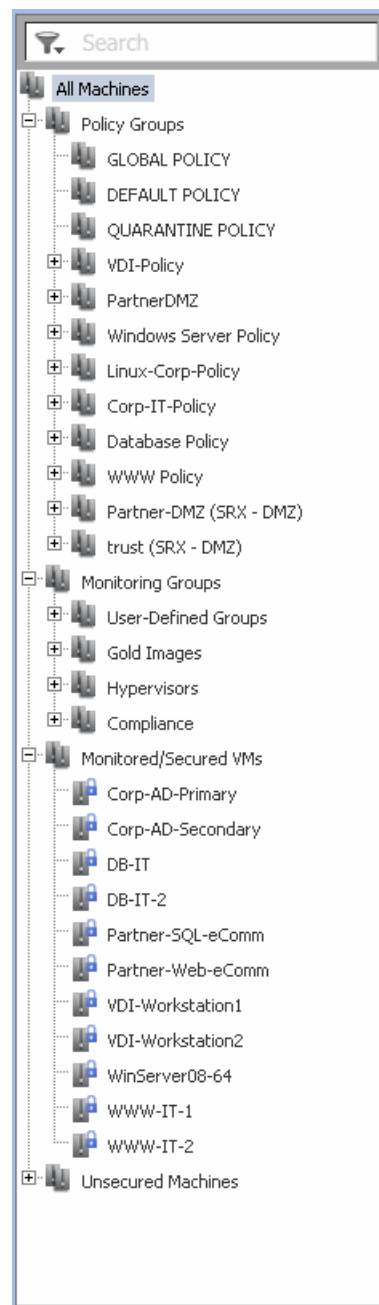


図 12: VM ツリー



詳細については、以下を参照してください。

- [39ページのvGW セキュリティ デザイン VM のナビゲーション ボタン バーの理解](#)
- [40ページのvGW セキュリティ デザイン VM のツリーについて](#)

各種状態を識別するアイコンの詳細については、「vGW セキュリティ デザイン VM のアイコンについて」を参照してください。

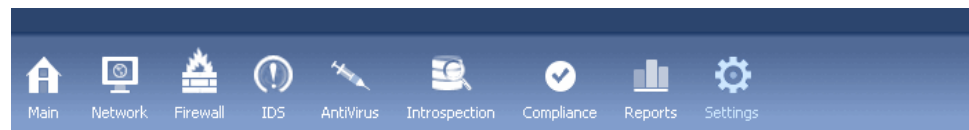
関連項目    • 3ページのvGW シリーズの理解

## vGW セキュリティ デザイン VM のナビゲーション ボタン バーの理解

このトピックでは、使用する vGW セキュリティ デザイン VM モジュールを選択したり、モジュール間を移動したりするためのナビゲーション ボタン バーについて説明します。

vGW セキュリティ デザイン VM は、モジュール式の構成および情報表示構造を備えています。ナビゲーション ボタン バーには、さまざまなモジュールを表すアイコンがあります。

図 13: vGW セキュリティ デザイン VM のナビゲーション バー



39ページの表1 に、各アイコンが表すモジュールを示します。表に示された各モジュールのリンクをクリックすると、該当するモジュールについて説明するトピックに移動します。

表1: ナビゲーション ボタン










アイコン	モジュール	説明	参照先
	メイン	ステータス、アラート、ネットワーク アクティビティを単一のビューに統合します。 検疫された VM を特定し、その VM に対してアクションを実行できます。	45ページの「vGW シリーズのメイン モジュールの理解」
	ネットワーク	ネットワーク アクティビティのサマリ、上位プロトコル、上位送信元、上位宛先、上位トーカー、接続を表示します。	53ページの「vGW シリーズ VM のネットワーク モジュールの理解」
	ファイアウォール	ポリシーを管理およびインストールし、ログを表示します。	59ページの「vGW シリーズのファイアウォール モジュールの理解」
	IDS	すべてのネットワーク トラフィック、または VM またはプロトコルの選択したサブセットを監視します。	67ページの「vGW シリーズの IDS モジュールの理解」
	アンチウィルス	マルウェアを検出することによってゲスト VM を保護し、影響を受けたファイルや VM を検疫します。	77ページの「vGW シリーズのアンチウィルス モジュールの理解」

表1: ナビゲーション ボタン (続き)

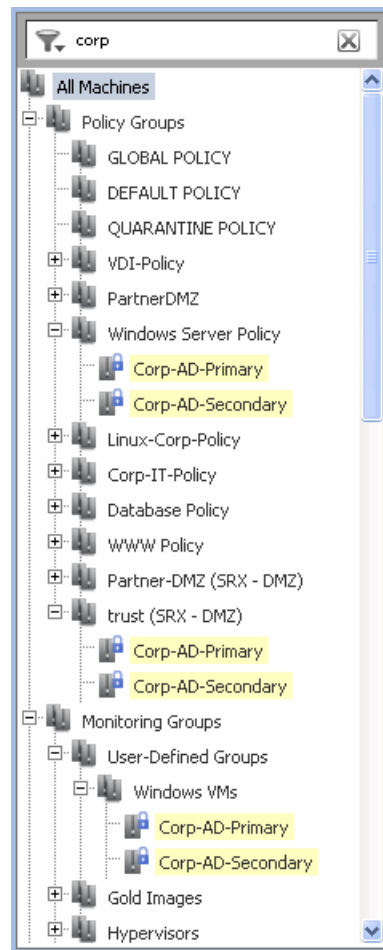
アイコン	モジュール	説明	参照先
 Introspection	イントロスペクション	システムをスキャンし、各 VM で実行されているソフトウェア（オペレーティング システム、パッチレベル、アプリケーション）に関するレポートを表示します。  その構成をゴールド イメージ比較ポイントとして使用する VM テンプレートまたはアクティブな VM を指定できるイメージ エンフォーサ機能が含まれます。 指定したゴールド イメージに対して VM の内容が比較されます。	93ページの「vGW シリーズのイントロスペクション モジュールの理解」
 Compliance	コンプライアンス	事前定義された一連の規則と照合して仮想インフラストラクチャを監視し、すべてのコンポーネントが安全に構成されていることを保証します。	107ページの「vGW シリーズのコンプライアンス モジュールの理解」
 Reports	レポート	詳細なシステムおよびセキュリティ レポートを生成します。	117ページの「vGW シリーズのレポート モジュールの理解」
 Settings	設定	パスワードなどの構成設定を制御します。	125ページの「vGW シリーズの設定モジュールの理解」

- 関連項目
- 40ページのvGW セキュリティ デザイン VM のツリーについて
  - vGW セキュリティ デザイン VM のアイコンについて

## vGW セキュリティ デザイン VM のツリーについて

このトピックでは、注目する仮想マシンを選択するための VM ツリーについて説明します。VM ツリーは、ほとんどの vGW セキュリティ デザイン VM モジュールと組み合わせて使用します。VM のグループまたは個々のグループを VM ツリーで選択します。 ボタン バーで選択したモジュールに応じて、選択した VM に関する情報を表示したり、VM に対してアクションを実行したりできます。 41ページの図14 に、VM ツリーで 3 つの VM グループを選択した例を示します。

図 14: VM ツリーで VM を選択した例



モジュール ボタン バーの詳細については、39ページの「「vGW セキュリティ デザイン VM のナビゲーション ボタン バーの理解」」を参照してください。

- VM ツリーの概要 41ページ
- 複雑な VM ツリーでの VM の特定 42ページ

## VM ツリーの概要

VM ツリー ペインでどの VM を選択するかによって、横の画面に表示される情報が変わります。ツリー内のすべての VM、VM のグループ、または単一の VM を選択できます。 ボタン バーを使用してモジュールを選択すると、そのモジュールの画面に VM ツリーで選択した VM に関する情報が表示されます。

モジュールは表示する情報の種類を制御するのに対して、ツリーは情報を表示する対象の VM を制御します。 これらを組み合わせることで、選択した VM の選択したモジュールに関する情報を構成できます。 たとえば、すべてのマシンのネットワーク トラフィックを表示するには、ツリーで [All Machines] を選択してから、ボタン バーで [Network] アイコンをクリックします。

VM ツリーには以下のメイン グループが含まれます。

- Policy Groups

すべてのセキュリティ ポリシー グループ（グローバル、デフォルト、検疫の各ポリシー グループと、管理者が定義したポリシー グループ）が含まれます。

- Monitoring Groups

[Policy Group] オプションによって作成されたすべてのグループと、ハイパーバイザおよびコンプライアンス状態を監視するためのグループが含まれます。

- Monitored/Secured VMs







vGW シリーズによって監視されている VM、ファイアウォールによってそのネットワークトラフィックが保護されている VM、またはその両方が一覧表示されます。

- Unsecured Machines

vGW シリーズによって現在分析または保護されていないすべての VM が一覧表示されます。

42ページの表2 に、監視されている VM の状態を表すアイコンを示します。

表2: 仮想マシンの状態を表すアイコン

	この VM は完全に監視されていますが、安全ではありません。たとえば、ファイアウォール ポリシーがロードされていません。
	このシステム（VM、または外部で定義されたマシン）は監視されておらず、「セキュリティ保護された」ネットワークに移動されていません。  注：ネットワーク レポートには、監視されていないシステムと監視されている VM 間のセッションを表示できます。
	このシステムの IP アドレスを vGW シリーズが特定できません。システムの電源が入っていない、システムが休止している、VMware Tools がインストールされていない、などが原因として考えられます。  ヒント：IP アドレスを手動で定義するには、[Settings] -> [vGW Application Settings] -> [Machines] の順にクリックします。
	この VM はコンプライアンスに適合しています。
	この VM はコンプライアンスに適合していません。
	これは VMware コンポーネント（ESX ホストなど）です。

## 複雑な VM ツリーでの VM の特定

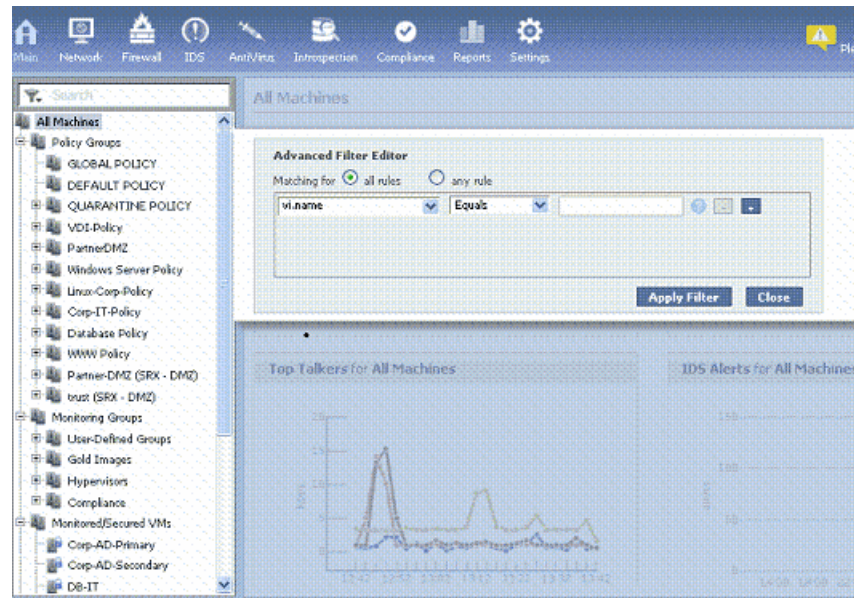
ツリーの複雑さが増すにつれて、VM ツリーで VM を特定することが難しくなります。このプロセスを簡単にするため、VM ツリーの上部にフィルタが用意されています。このフィルタフィールドに、ツリー内の VM 名と照合するテキスト文字列を入力できます。テキストを入力すると、ツリー内の一致する VM が動的に検索されます。一致する VM が含まれないツリー内



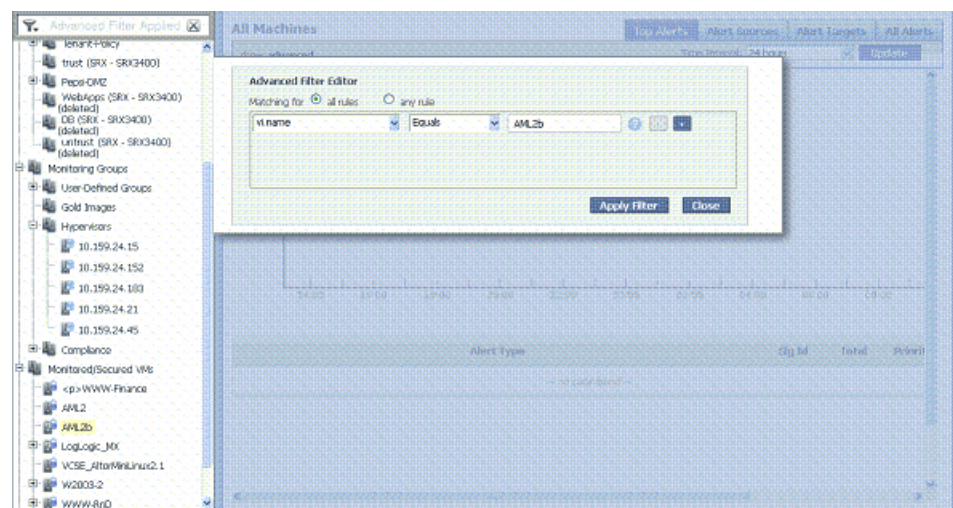
のブランチは折りたたまれ、一致するブランチを示すようにツリーが展開されます。一致する VM を探すためにツリー内のすべてのグループを展開する必要はありません。

VM ツリーの検索機能を強化するため、Advanced Filter Editor が使用できるようになりました。この機能を使用するには、検索フィルタの右側にあるアイコンをクリックします。そうすると、下の図に示すように Advanced Filter Editor が表示されます。

次の図に示すように、すべての VM に対して検索を実行できます。



また、次の図に示すように、名前によって特定の VM を検索することもできます。



フィルタを解除してブランチを折りたたむには、フィルタの右にある [×] アイコンをクリックします。

関連項目 • 39ページのvGW セキュリティ デザイン VM のナビゲーション ボタン バーの理解

- vGW セキュリティ デザイン VM のアイコンについて

## vGW シリーズのメイン モジュール

この章では、vGW セキュリティ デザイン VM のメイン モジュール コンポーネントについて説明します。この章には以下のトピックがあります。

- [vGW シリーズのメイン モジュールの理解 45ページ](#)

### vGW シリーズのメイン モジュールの理解

vGW セキュリティ デザイン VM のメイン モジュールには、多くの vGW セキュリティ デザイン VM モジュールから収集された情報が表示されます。vGW シリーズによって新しいイベントやアラートが検出されると、メイン モジュールの画面に表示されたデータやグラフが自動的に更新されます。

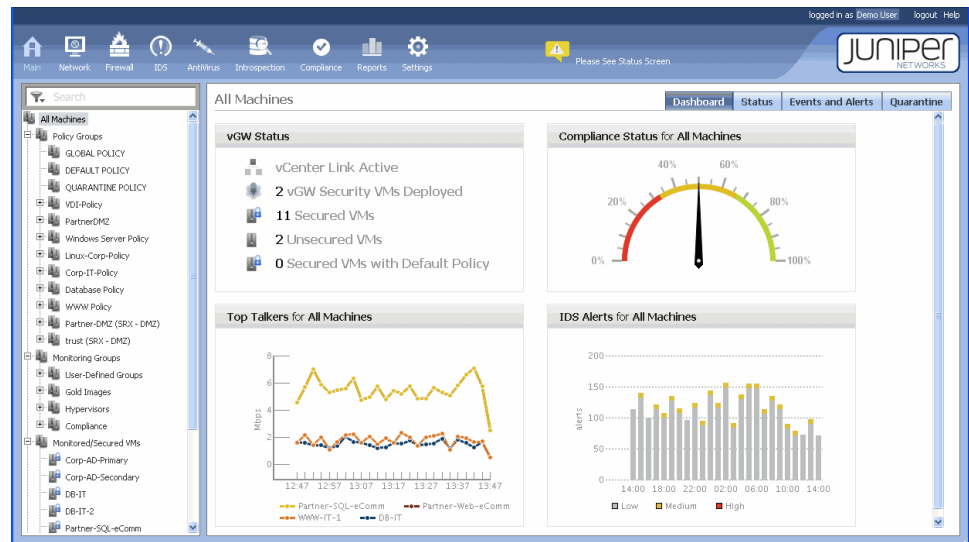
メイン モジュールには以下のタブがあります。

- [Dashboard 45ページ](#)
- [\[Status\] タブ 46ページ](#)
- [\[Events and Alerts\] タブ 49ページ](#)
- [\[Quarantine\] タブ 51ページ](#)

### Dashboard

[Dashboard] タブには、仮想マシン環境の動作が一目でわかるようにグラフと表で示されます。すべてのゲスト仮想マシン (VM) のアクティビティを表示できます。また、VM ツリー ペインで VM のグループまたは個々の VM を選択して、それらのアクティビティのみを表示することもできます。 [46ページの図15](#)を参照してください。

図 15: メイン モジュールのダッシュボード



[Dashboard] タブは以下の部分で構成されています。

**vGW Status**—運用インフラストラクチャの現在の状態の概要を示します。VMware vCenter への vGW の接続状態、ESX/ESXi ホストを保護するために配備されている vGW セキュリティ VM の数、配備している VM の全体的な状態（つまり、それらの VM がセキュリティ保護されているかどうか）が示されます。

**Compliance Status for All Machines**—組織に存在するすべての VM のうちの程度がコンプライアンス規則に違反しているかを示します。規則に違反している VM が多い（ウェイトが高い）ほど、針が赤に近付きます。

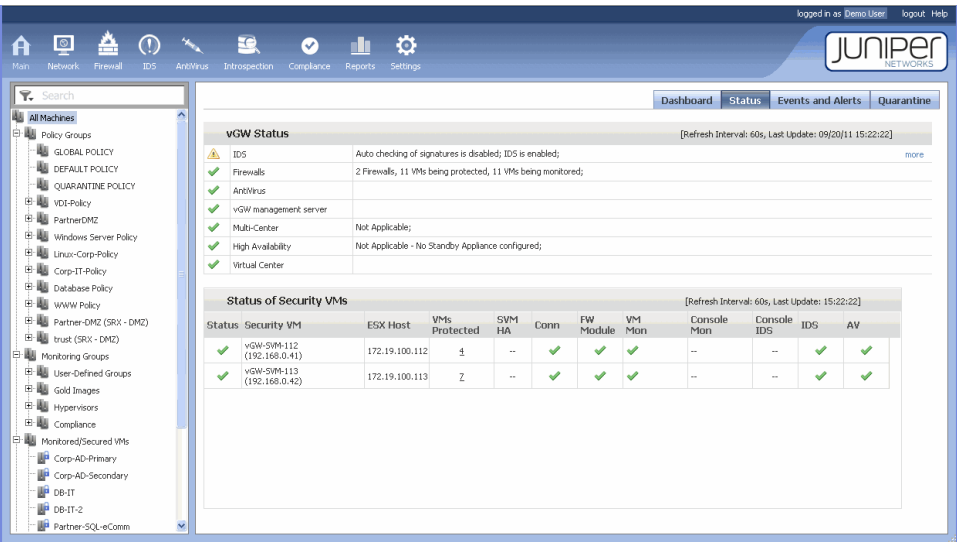
**Top Talkers for All Machines**—過去 1 時間のネットワーク アクティビティが表示されます。

**IDS Alerts for All Machines**—過去 24 時間に発生した優先度が高、中、低のアラートが表示されます。

## [Status] タブ

[Status] タブには、各モジュールの vGW 設定と個々の vGW セキュリティ VM のステータスのサマリが表示されます。この画面は 60 秒ごとに更新されます。47ページの図16を参照してください。

図 16: [Status] タブ



[Status] 画面は以下のペインで構成されています。

vGW Status-ステータス アイコンによって vGW シリーズ コンポーネントの状態が示されます。コンポーネントごとに、47ページの表3に示すステータス アイコンを使用してコンポーネントの現在の状態が示されます。

47ページの表3 に、vGW セキュリティ VM のステータス アイコンを示します。



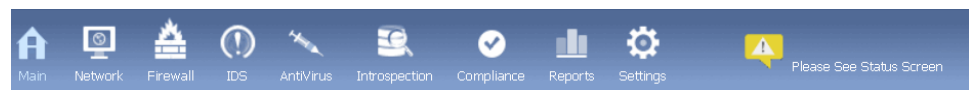
注:

表3: vGW シリーズのステータス アイコン

アイコン	意味
	この vGW シリーズ コンポーネントは適切に機能しています。
	1 つ以上の問題がこのコンポーネントに存在します。問題の例としては、保守設定が矛盾しているか無効になっている、ファイアウォールの更新が必要、などがあります。
	重要な問題がそのコンポーネントに存在します。たとえば、モジュールが正しくロードされていません。

これらのアイコンに加えて、個々のコンポーネントが注意を要するときに全体的な正常性ステータス アイコンが表示されます。48ページの図17 に、ボタン バーの右端に正常性ステータス アイコンが表示されたところを示します。このアイコンは、監視されているコンポーネントの基になる状態に応じて赤または黄色になります。

図 17: ボタン バーに表示された正常性ステータス アイコン



このアイコンの上にマウス ポインタを置くと、現在注意を要する正確なコンポーネント名が表示されます。

Status of Security VMs-このペインでは、個々の vGW セキュリティ VM のステータスが報告されます。vGW セキュリティ VM のステータス アイコンをクリックすると、詳細な情報が表示されます。

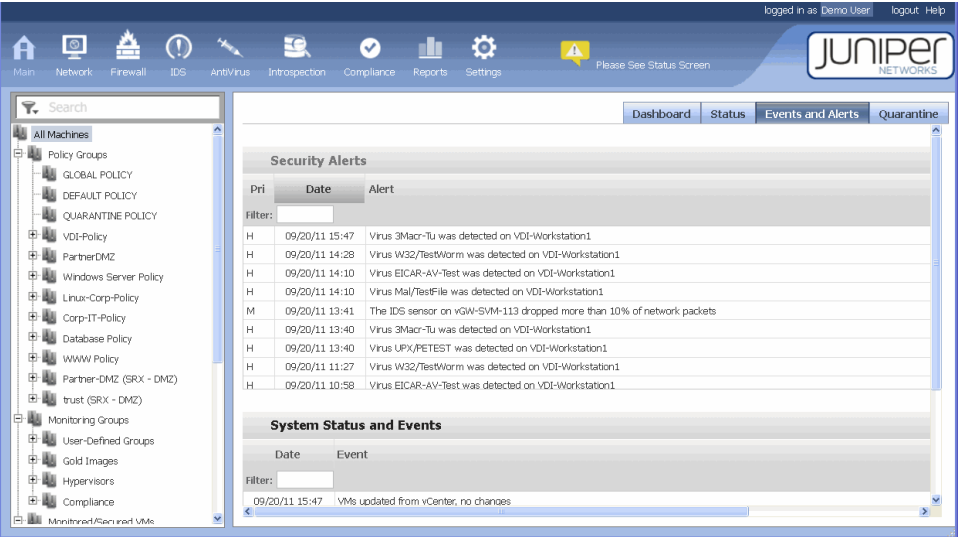
[Status of Security VMs] ペインには以下の情報が表示されます。

- vGW セキュリティ VM の名前
- vGW セキュリティ VM が保護しているホスト
- 保護している VM の数
- vGW シリーズ HA が有効かどうか
- vGW セキュリティ VM が vGW セキュリティ デザイン VM に接続しているかどうか
- ファイアウォール モジュールが有効かどうか
- VM 監視が使用されているかどうか
- その管理コンソールの IP アドレス
- IDS が使用されている場合、IDS コンソールの IP アドレス
- IDS が有効かどうか。IDS が作動している場合は IDS データが表示されます。作動していない場合、チャートは空白になります。
- アンチウィルスが有効かどうか

特定の vGW セキュリティ VM の構成を変更するには、設定モジュールの [Security VM Settings] セクションを使用します。詳細については、[163ページの「vGW セキュリティ VM の設定モジュールの理解」](#)を参照してください。

[Events and Alerts] タブ

[Events and Alerts] タブには 2 つのペインがあります。



- [Security Alerts 49ページ](#)
- [System Status and Events 50ページ](#)

Security Alerts

[Security Alerts] ペインには、vGW シリーズで発生した、IDS アラートとアンチウィルス アラート以外のすべてのアラートが一覧表示されます（IDS アラートとアンチウィルス アラートはそれぞれ固有のモジュールで報告されます）。報告されるアラートは主として vGW シリーズ システムに関連したイベントであり、たとえば vGW シリーズのバージョン更新の発生に関する報告や、コンポーネントの障害発生時のアラートなどです。

アラートはその重大度に応じて高（H）、中（M）、低（L）のいずれかに分類されます。[Priority] または [Date] 列をクリックすると、リストの並び順が変わります。 [49ページの図18](#)を参照してください。

図 18: [Events and Alerts] タブの [Security Alerts] ペイン

Security Alerts		
Pri	Date	Alert
Filter: <input type="text"/>		
H	09/20/11 18:00	Virus 3Macr-Tu was detected on VDI-Workstation1
H	09/20/11 17:31	Virus W32/TestWorm was detected on VDI-Workstation1
H	09/20/11 17:10	Virus EICAR-AV-Test was detected on VDI-Workstation1
H	09/20/11 17:09	Virus Mal/TestFile was detected on VDI-Workstation1
H	09/20/11 15:47	Virus 3Macr-Tu was detected on VDI-Workstation1
H	09/20/11 14:28	Virus W32/TestWorm was detected on VDI-Workstation1
H	09/20/11 14:10	Virus EICAR-AV-Test was detected on VDI-Workstation1
H	09/20/11 14:10	Virus Mal/TestFile was detected on VDI-Workstation1
M	09/20/11 13:41	The IDS sensor on vGW-SVM-113 dropped more than 10% of network packets

## System Status and Events

多くの企業では、コンプライアンス標準やセキュリティ ベスト プラクティスに準拠するため、管理およびポリシー操作の完全な監査証跡が必要となります。 詳細な監査証跡は、セキュリティ管理者が頼りにするセキュリティ インフラストラクチャの重要な部分です。

vGW シリーズはイベントに関する情報を収集し、管理およびポリシー操作が行われたときにその情報を [System Status and Events] ペインに書き込みます。 以下のイベントに関するイベント アラートが書き込まれます。

- 管理者アクティビティ イベント:
  - 管理者がログインまたはログアウトしたとき、およびログイン試行が失敗したときにイベント アラートが書き込まれます。
  - 管理者が以下のような vGW セキュリティ デザイン VM の設定変更を行ったとき、イベント アラートが書き込まれます。
  - 一般的なシステム設定（ログ接続、システム再起動、ライセンス変更、アクティブ ディレクトリなど）が変更されたとき。
  - 手動で VM が更新されたとき。
  - vGW シリーズ オブジェクト（ネットワーク、マシン、グループ、プロトコル、管理者の設定など）が変更されたとき。
  - vGW セキュリティ デザイン VM または vGW セキュリティ VM のソフトウェアが更新されたとき。
  - ファイアウォール構成が変更されたとき。
  - Syslog、Netflow、外部検査デバイス、およびインフラストラクチャ増強の構成が変更されたとき。
- 自動的に保護される VM の構成が変更されたとき。
- IDS シグネチャが変更されたとき、新しいシグネチャが追加されたとき。
- [Scan Now] 要求によってイントロスペクション スキャンが開始されたとき、スケジュールされたイベントが発生したとき、スケジュールされたスキャンの構成が変更されたとき。
- コンプライアンス規則が変更されたとき。
- レポートが作成されたとき、レポートの構成設定が変更されたとき。
- イメージ エンフォーサが構成されたとき、イメージ エンフォーサの構成設定が変更されたとき、イメージ エンフォーサ スキャンが実行されたとき。
- アンチウィルスが構成されたとき、アンチウィルスの構成が変更されたとき、アンチウィルス スキャンが実行されたとき。
- SRX 統合が変更されたとき。
- マルチセンターおよびスプリットセンターの設定が構成または変更されたとき。
- バックアップおよびリストアが構成されたとき、バックアップおよびリストアの構成が変更されたとき。



- ライセンス設定が変更されたとき。
- レジストリ値が変更されたとき。

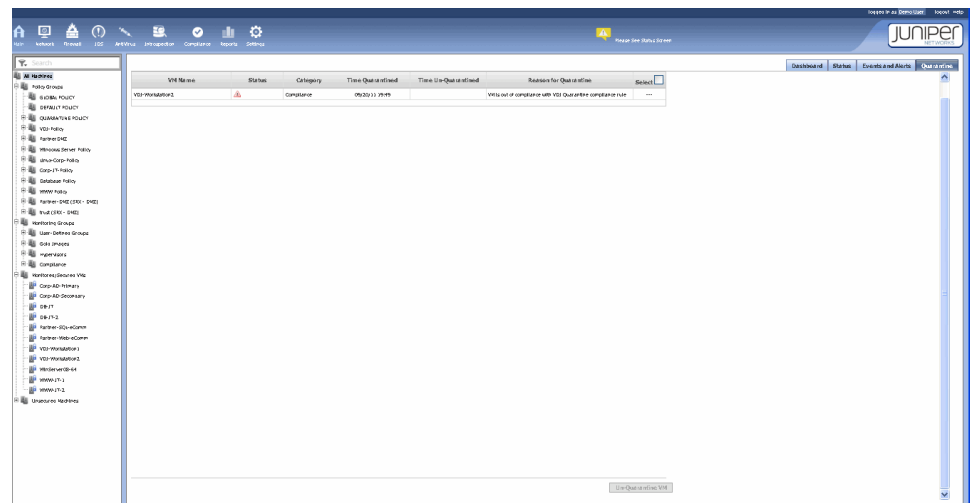
イベントは時系列順に並んでおり、最も最近に発生したイベントが表の一番上に表示されます。追加のイベントを表示するには、vGW セキュリティ デザイン VM データベースにアクセスします。

設定モジュールの [Alerting] セクションで、E メールによって管理者にアラートを送信するよう設定することもできます。

## [Quarantine] タブ

メイン モジュールの [Quarantine] タブには、アンチウイルス、コンプライアンス、またはイメージ エンフォーサ スキャンの結果として検疫された VM に関する情報が表示されます。このタブを使用して、VM が検疫された日時、検疫から解放された日時、および検疫された理由を確認できます。

図 19: メイン モジュールの [Quarantine] タブ



メイン モジュールの [Quarantine] タブでは、以下のことができます。

- 1 つまたは複数の機能について、検疫された VM に関する情報を表示できます。

アンチウイルス、コンプライアンス、またはイメージ エンフォーサの前のチェックボックスをオンにすると、その機能のスキャンの結果検疫された VM に関する情報のみが個別に表示されます。

また、複数の機能を選択すると、それらの検疫された VM に関する情報がまとめて表示されます。

これらの選択した機能について、

- 現在検疫されている VM に関する情報を表示できます。
- これまでに検疫された VM に関する履歴情報を表示できます。

検疫された VM を解放するには、VM を選択して [Un-Quarantine VM] ボタンをクリックします。



注: アンチウイルス モジュールを使用して、ウイルスまたはその他のマルウェアに感染したファイルを検疫できます。詳細については、[77ページの「vGW シリーズのアンチウイルス モジュールの理解」](#)を参照してください。

- 関連項目
- [39ページのvGW セキュリティ デザイン VM のナビゲーション ボタン バーの理解](#)
  - [40ページのvGW セキュリティ デザイン VM のツリーについて](#)

# vGW シリーズ VM のネットワーク モジュール

この章では、ネットワーク トラフィックに関する情報を表示する、vGW セキュリティ デザイン VM のネットワーク モジュールについて説明します。この章には以下のトピックがあります。

- [vGW シリーズ VM のネットワーク モジュールの理解 53ページ](#)

## vGW シリーズ VM のネットワーク モジュールの理解

vGW セキュリティ デザイン VM のネットワーク モジュールには、VM ツリー ペインで選択したゲスト仮想マシン (VM) のネットワーク トラフィックが表示されます。すべての VM または選択した VM のネットワーク トラフィックを表示できます。

このトピックでは、ネットワーク モジュール コンポーネントについて説明します。このトピックには以下のセクションがあります。

- [ネットワーク モジュール 53ページ](#)
- [表示情報の操作 54ページ](#)

## ネットワーク モジュール

ネットワーク モジュールには、VM ツリー ペインで選択した VM のネットワーク トラフィックが表示されます。すべての VM または選択した VM のネットワーク トラフィックを表示できます。

ネットワーク モジュールには以下の 6 つのタブがあります。

- Summary
- Top Protocols
- Top Sources
- Top Destinations
- Top Talkers
- Connections

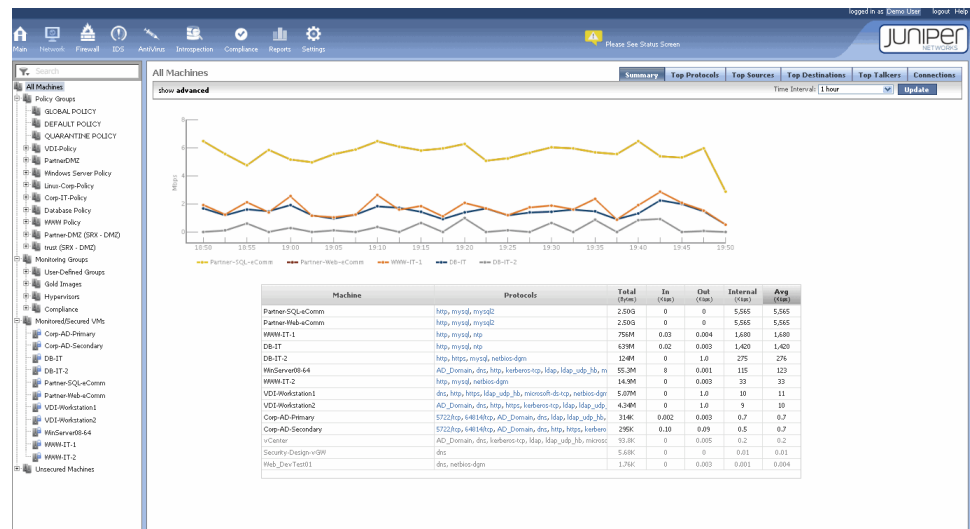
VM の情報を表示するには、その VM が既知の IP アドレスを持っている必要があります。VMware Tools が VM にインストールされている場合、IP アドレスは自動的に決定されます。IP アドレスが自動的に設定されない場合は、設定モジュールの [vGW Application Settings] セクションの [Machines] セクションを使用して、IP アドレスを手動で設定できます。

## 表示情報の操作

ネットワーク モジュールの [Summary] タブには、すべての VM に関する情報（54ページの図20を参照）、または特定の VM に関する情報（55ページの図21を参照）を表示できます。

画面上部の折れ線グラフは、レポートの上位 VM の帯域幅使用状況を示します。グラフの下は、VM ツリーで選択した VM の詳細なネットワーク データを示します。この場合は、1 時間のデータが表示されます。

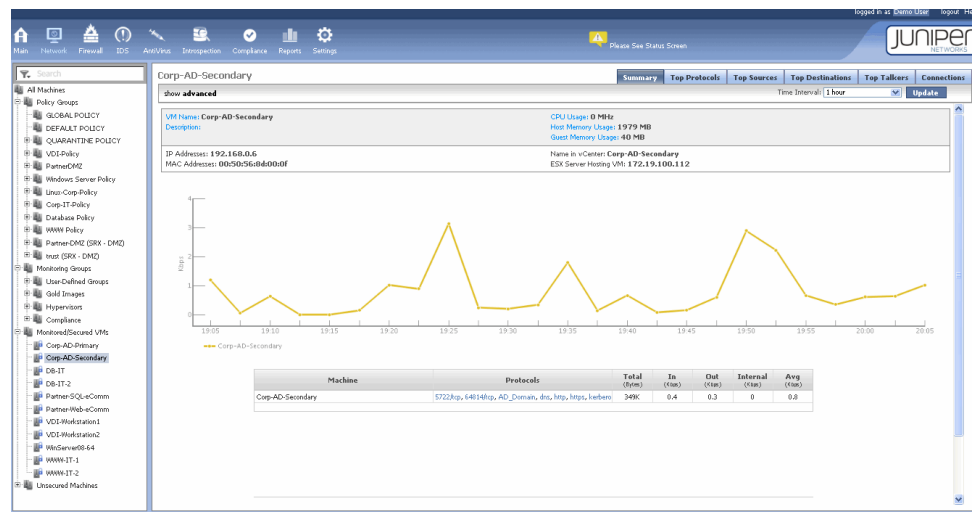
図 20: ネットワーク モジュールの [Summary] タブ



## 単一の仮想マシンに関するネットワーク情報の表示

単一の VM に関する情報を表示するには、対象の VM を VM ツリーで選択します。55ページの図21に、Corp-AD-Secondary VM の情報を表示した例を示します。

図 21: ネットワーク モジュールの [Summary] タブ



VM の接続を表示するには、グラフの個々の線をクリックします。 プロトコルのフィルタを表示するには、プロトコル フィールドをクリックします。

### 表示情報の時間間隔の変更

ネットワーク データをグラフ化する期間を変更するには、[Time Interval] メニューを使用します。 別の間隔を選択して [Update] をクリックします。 時間間隔を選択するか、カスタムの期間を指定できます。 この時間間隔機能は、他の vGW セキュリティ デザイン モジュールでも使用できます。

55ページの図22 および 56ページの図23 に、すべてのマシンの情報を時間間隔を変えて表示した例を示します。

図 22: 異なる時間間隔でのネットワーク データの表示: パート 1

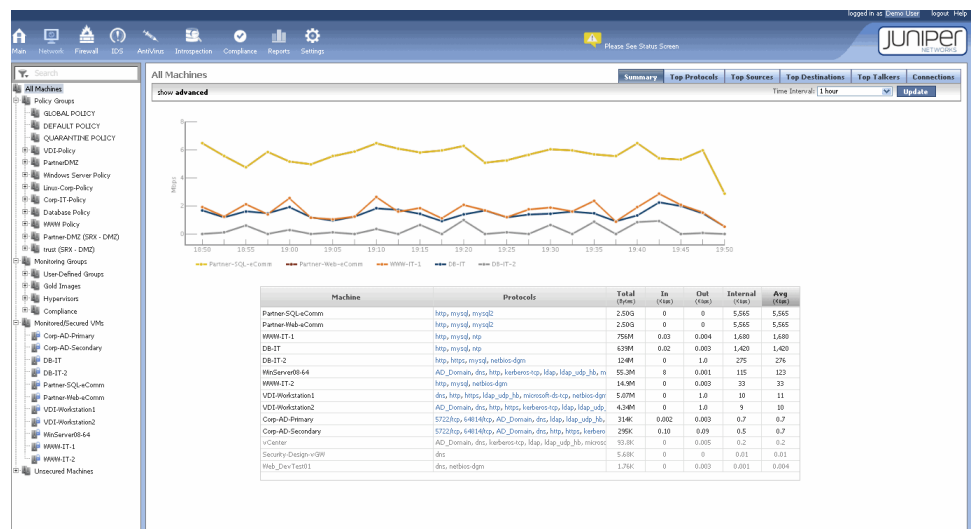
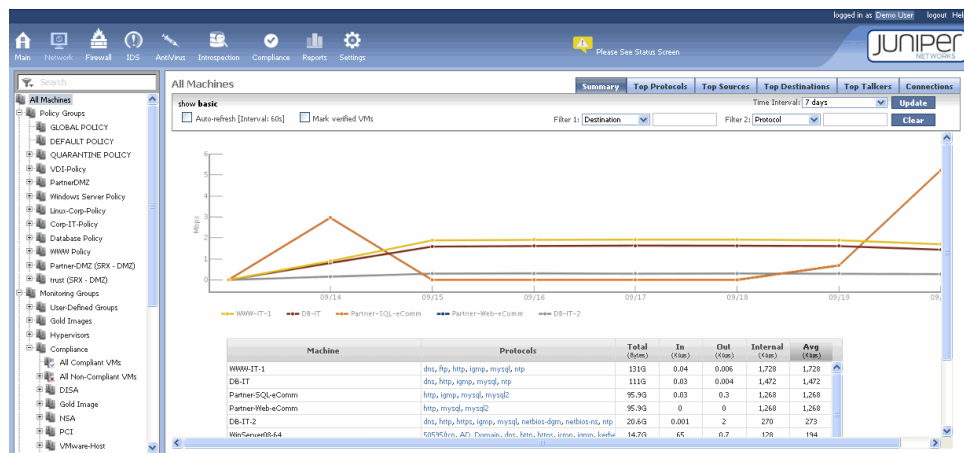
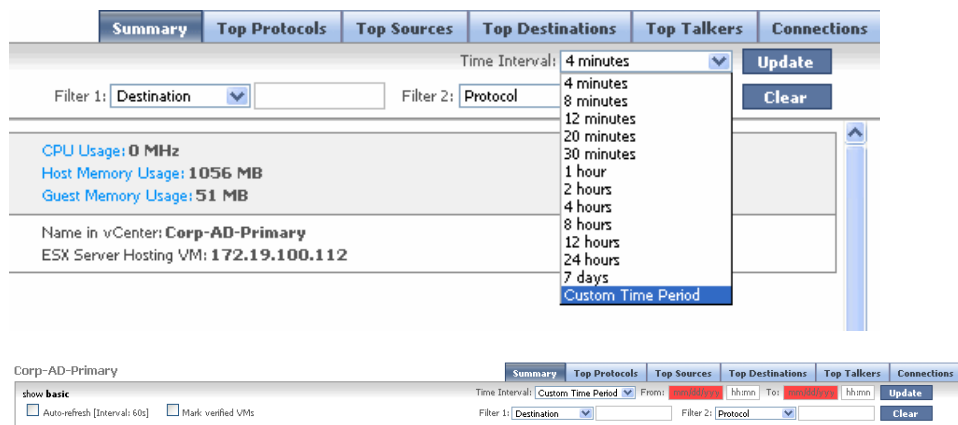


図 23: 異なる時間間隔でのネットワーク データの表示: パート 2



直近のトラフィック間隔からのリアルタイム データが表の [Total]、[In]、[Out]、[Internal] の各列に反映されます。プロトコル、送信元、宛先、または上位トークナーをグラフ化している場合は、選択した時間間隔を使用して最小値、最大値、および平均値が計算され、グラフの下 の表に表示されます。

カスタムの期間を指定して履歴データを表示できます。[Time Interval] メニューで、[Custom Time Period] を選択します。[From] フィールドと [To] フィールドに日付を入力するか、カレンダー ポップアップ ウィンドウを使用します。時刻を指定しない場合、時刻フィールドはデフォルトで 00:00 に設定されます。



注: データベースのサイズと使用可能なリソースによっては、カスタムの期間を指定したときに、グラフ化したデータが表示されるまでに 30 分以上かかる場合があります。1 か月以上の期間のデータなど、大きなデータ セットを調べる場合は、レポート モジュールを使用することを推奨します。

詳細オプションの使用

表示する情報をフィルタによって絞り込むことができます。フィルタリング オプションを表示するには、時間間隔バーにある [show advanced] をクリックします。57ページの図24 に、ネットワーク接続データに対して使用される詳細なフィルタリング オプションを示します。

図 24: ネットワーク データに対するフィルタリングの使用



[Filter 1] メニューと [Filter 2] メニューをクリックしてフィルタリング オプションを選択し、各フィールドの設定を入力して [Update] をクリックすると、入力した設定に基づいてグラフとデータの表示が更新されます。フィルタ フィールドをリセットするには [Clear] をクリックします。



注: 設定したフィルタはグラフと表のすべてのデータに影響します。

その他の詳細オプションは、表示しているタブによって若干異なります。57ページの表4 に、詳細オプションの説明を示します。

表4: 詳細オプション

選択	アクション
Auto-refresh	60 秒ごとにデータを自動的に更新します。
Mark verified VMs	IP アドレスに加えて一意の VMware ID/UUID も使用して、その接続が実際に識別されたサーバーから来ているかどうかを自動的に検証します。両方の値を使用することで、IP スプーフィングなどの問題から保護されます。この追加検証が行われる VM をインターフェースに表示できます。
Multicast in table	<p>マルチキャスト パケットを監視対象に含めます。マルチキャスト パケットは特定のホスト宛てではなく、ネットワーク上のすべてのマシンで見られるため、すべての VM の接続セッション リストに含まれます。</p> <p>しかし、マルチキャスト トラフィックは量が非常に多くなることがあり、マルチキャスト トラフィックを含めると選択した VM に固有のセッションがわかりにくくなる可能性があります。このビューからマルチキャストを除去するには、[Multicast in table] チェックボックスをオフにします。</p>

詳細ビューを終了するには、[show basic] をクリックします。

表データの並べ替え

[Network] 画面の表データは列を基準に並べ替えることができます。ポインタを列見出しの上に置き、ポインタが「指差す手」の形に変わったら、列見出しをクリックして並べ替えます。

関連項目   • 3ページのvGW シリーズの理解





## 第7章

# vGW シリーズのファイアウォール モジュール

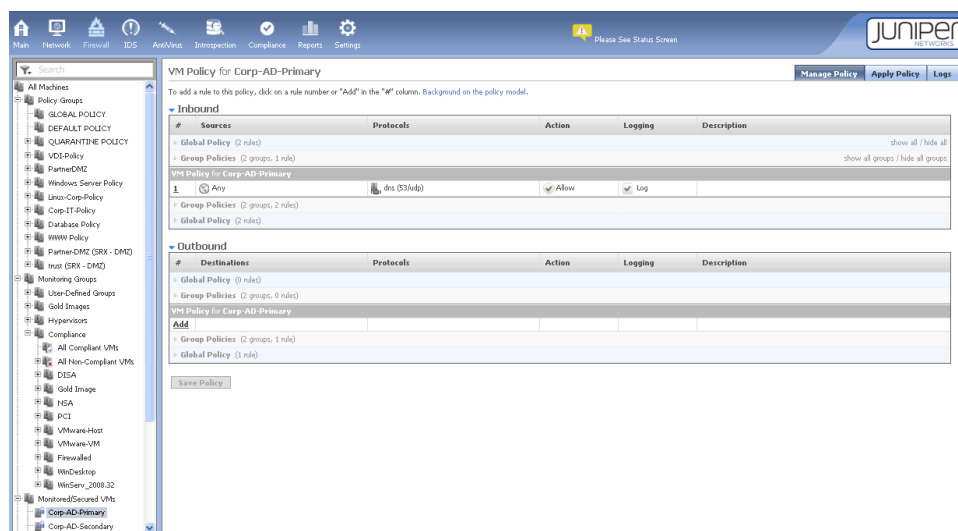
この章には以下のトピックがあります。

- vGW シリーズのファイアウォール モジュールの理解 59ページ

## vGW シリーズのファイアウォール モジュールの理解

vGW セキュリティ デザイン VM のファイアウォール モジュールでは、セキュリティ ポリシーを定義、適用し、監視できます。ファイアウォール モジュールのタブ画面に表示されるデータを変更するには、VM ツリー ペインですべての VM、1 つの VM、または複数の VM を選択します。すべての VM ではなく、1 つまたは複数の VM を選択した場合は、それらの VM のみに関連する情報が表示されます。59ページの図25 に、1 つの VM のみに関連する情報を示します。

図 25: ファイアウォール モジュール



このトピックには以下のセクションがあります。

- [Manage Policy] タブ 60ページ
- [Apply Policy] タブ 62ページ
- [Logs] タブ 64ページ

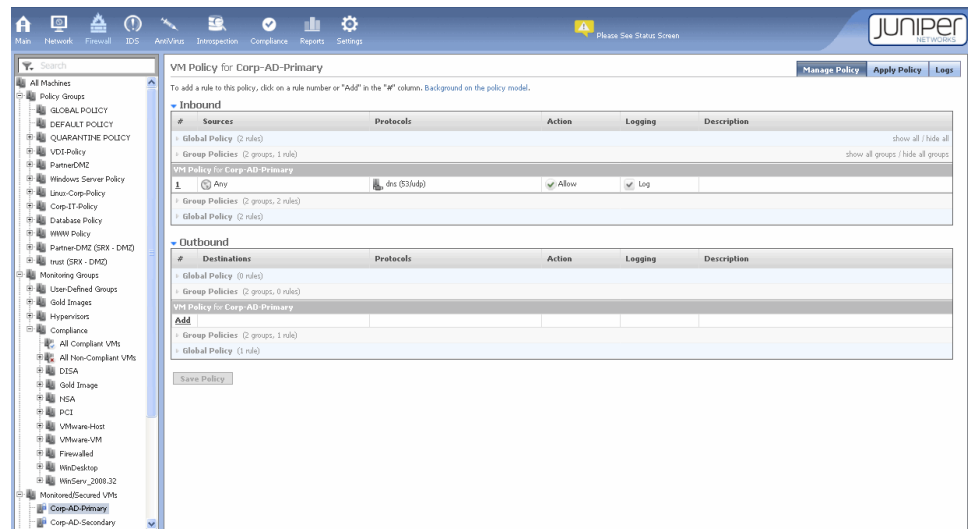
## [Manage Policy] タブ

ファイアウォール モジュールの [Manage Policy] タブでは、セキュリティ ポリシーを定義および編集できます。60ページの図26を参照してください。

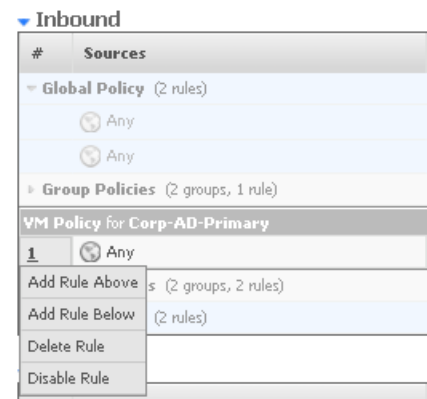
新しいポリシー規則を作成するには、以下の手順に従います。

1. [#] 列の規則番号をクリックします。この例では、Corp-AD-Primary VM 用のアウトバウンド規則を追加します。

図 26: [Manage Policy] タブ

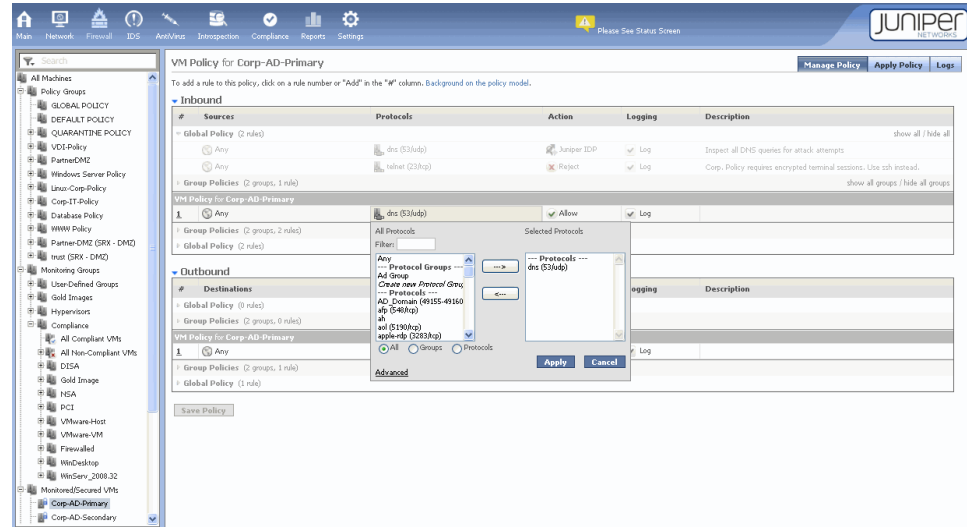


2. [Add Rule Above] または [Add Rule Below] を選択します。



規則は上から順に適用されます。

- ・ポリシー設定を構成するには、表のセルをクリックし、ポップアップ ダイアログ ボックスを使用して情報を編集します。
- ・ダイアログ ボックスのメニューをすばやく選択するには、選択する項目の最初の文字を入力します。たとえば、[All Protocols] メニューで文字 **t** を入力すると、リスト内の telnet にスクロールします。



- ・項目をただちに選択するには、フィルタ ボックスに直接入力します。

一部を除くすべてのプロトコルを含むポリシーを定義するには、以下の手順に従います。

1. [Advanced] をクリックします。
2. [Selected Protocols] リストで [All protocols except:] を入力します。
3. 除外するプロトコルを 1 つ以上選択し、それらをリストに移動します。

61ページの表5 に、ポリシー構成設定の説明を示します。

表5: ファイアウォールのポリシー構成設定

フィールド	説明
Sources	接続の発生元のオブジェクトを定義します。
Protocols	規則で使用するプロトコルを定義します。  該当するオプションを選択することで、新しいプロトコルまたはプロトコル グループを動的に作成することもできます。
Action	接続を許可、ドロップ（サイレント ドロップ）、または拒否（トラフィックをドロップして送信元に通知を送る）します。  また、パケットをサードパーティ製デバイスにリダイレクトまたは複製することもできます。 [Settings]-> [Security Settings] -> [Global] -> [External Inspection Devices] を参照してください。

表5: ファイアウォールのポリシー構成設定 (続き)

フィールド	説明
Logging	<p>規則に一致する接続をログに記録する、この接続のログへの記録をスキップする、この接続が規則に一致するときにアラートを送信する、のいずれかを選択します。</p> <p>[Alert] オプションを選択すると、E メール メッセージまたは SNMP トラップが送信されます。</p> <p>アラートの構成の詳細については、80 ページの「アラート」を参照してください。</p>
説明	ポリシーの説明を入力します。

ポリシー設定の入力または編集が済んだら、[Save] をクリックして変更を vGW セキュリティ デザイン VM データベースに保存します。








**注意:** 新しい規則を有効にするためには、[Apply Policy] タブを使用してポリシーの変更を適用する必要があります。規則はただちに適用できるほか、保守中に適用することもできます。

既存の規則を削除または無効/非アクティブにするには、規則番号をクリックして該当するメニュー項目を選択します。無効にした規則は灰色で表示され、取り消し線が付きま

## [Apply Policy] タブ

[Apply Policy] タブでは、セキュリティ ポリシーをファイアウォールに適用して運用インフラストラクチャ内の VM を保護できます。

画面左側の VM ツリー ペインを使用して、ポリシーを適用する VM を選択します。たとえば、単一のゲスト VM (VM) にポリシーをインストールする場合は、[Apply Policy] タブを表示し、対象の VM を VM ツリー ペインで選択します。

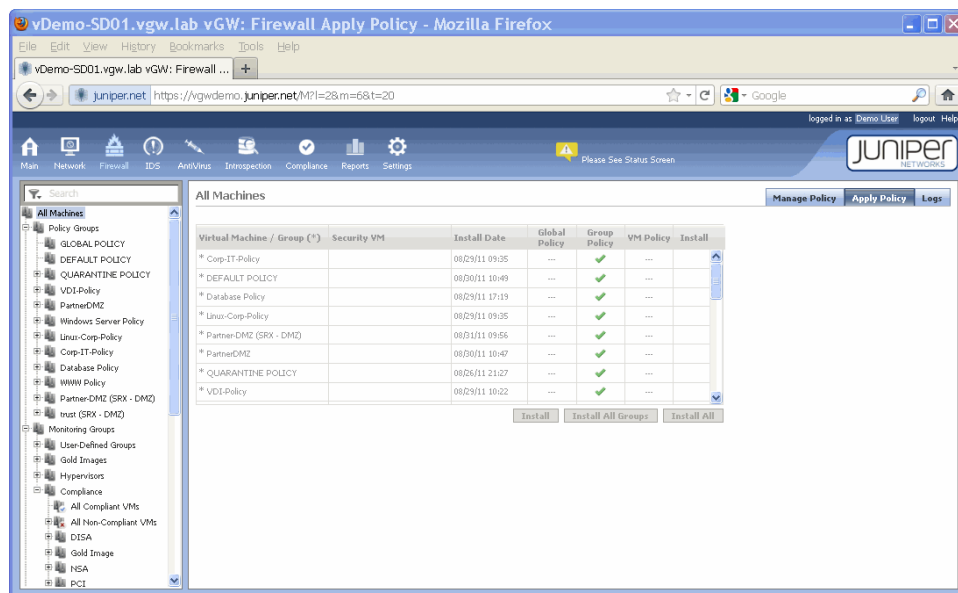
アイコン	意味
	このポリシーは最新状態であり、さらなるアクションは必要ありません。
	対象の VM はポリシー グループに含まれていますが、vGW セキュリティ VM ファイアウォールによって保護されていないため、ポリシーを取得できません。これは通常、調査が必要なエラー状態を示します。
	このポリシー タイプは対象の VM には存在しません。たとえば、その VM 用の個別の VM ポリシーが構成されていません。  VM ごとに個別の VM ポリシーを作成する必要はありません。
	このポリシーは変更されており、VM に配備する必要があります。
	ポリシーのインストールを妨げるエラー状態が存在します。ポリシーの配布に問題があるものの、古いポリシーが適切に機能している場合は、チェックマーク アイコンが表示されます。



**ヒント:** ポリシー ステータス アイコンの上にポインタを置くと、アイコンの説明を示すツール ヒントが表示されます。

ポリシーを実装する準備ができたなら、[Install] または [Install All] をクリックして、ポリシーをファイアウォールに適用します。そうすると、ポリシーが選択した VM に配備されるか、vNIC 毎ポリシー機能を使用している場合は VM の vNIC に配備されます。

図 27: [Apply Policy] タブ

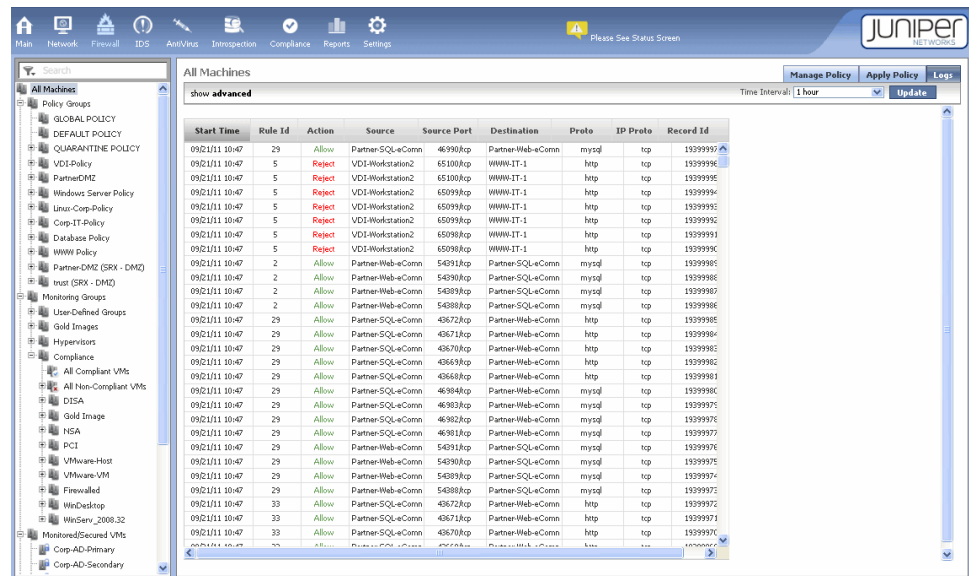


## [Logs] タブ

ファイアウォール規則を定義するとき、[Log]、[Don't Log]、および [Alert] 通知オプションを指定できます。ある規則に対して [Log] または [Alert] を選択すると、その規則に一致するトラフィックがログに記録されます。65ページの図28 に [Logs] タブを示します。

[Logs] タブには [Mark verified VMs] などの詳細オプションがあります。この設定をオンにすると、IP アドレスに加えて一意の VMware ID/UUID も使用して、その接続が実際に識別されたサーバーから来ているかどうかを検証されます。この機能は、IP スプーフィングや DHCP 変更などの問題からネットワークを守ります。この追加検証が可能な VM にはアスタリスク (\*) が付きます。[Mark verified VMs] の設定をオン/オフすると、それに応じてアイコンが表示または非表示になります。[Auto-refresh] をクリックすると、60 秒ごとに自動的にログの表示が更新されます。

図 28: ファイアウォール モジュールの [Logs] タブ



フィルタを使用して、表示するログ エントリを絞り込むことができます。特定の VM に関連するログのみを表示するには、その VM を VM ツリーで選択します。

関連項目    • 3ページのvGW シリーズの理解





## vGW シリーズの IDS モジュール

この章には以下のトピックがあります。

- [vGW シリーズの IDS モジュールの理解 67ページ](#)
- [vGW シリーズの IDS モジュールの理解 68ページ](#)
- [IDS 設定の構成とアクティビティの表示 71ページ](#)

### vGW シリーズの IDS モジュールの理解

---

vGW シリーズには IDS エンジンが完全に統合されており、すべての仮想ネットワーク トラフィックの監視にこのエンジンを使用できます。 また、ゲスト VM (VM) または使用されたプロトコルのサブセットのトラフィックを選択的に監視することもできます。 選択したトラフィックがシグネチャ データベースと照合され、不審なアクティビティに対して優先度が高、中、低のアラート フラグが設定されます。

- IDS モジュールの各タブの詳細と、返されたデータの解釈方法については、[68ページの「vGW シリーズの IDS モジュールのタブの理解」](#)を参照してください。
- IDS 設定の構成の詳細については、[166ページの「IDS 設定の理解と構成」](#)を参照してください。
- IDS 機能の使用方法の詳細については、[71ページの「IDS 設定の構成とアクティビティの表示」](#)を参照してください。

vGW セキュリティ デザイン VM では、運用環境の IDS を構成するために以下の情報を設定できます。

- IDS 設定
- IDS 更新
- 更新ステータス
- アップロードする IDS シグネチャ

- 関連項目
- [3ページのvGW シリーズの理解](#)
  - [125ページのvGW シリーズの設定モジュールの理解](#)

## vGW シリーズの IDS モジュールの理解

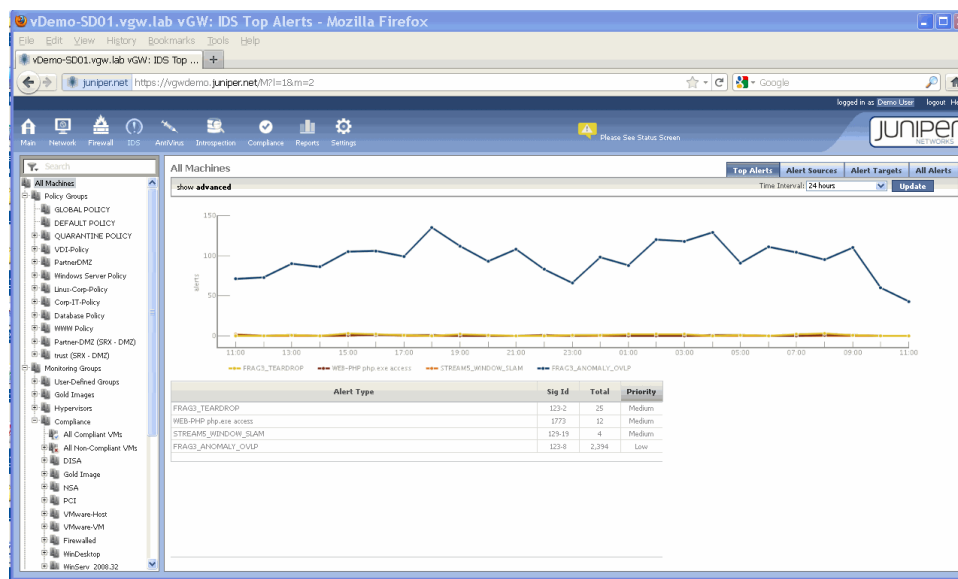
このトピックでは、vGW シリーズの IDS モジュールについて説明します。IDS エンジン、ゲスト仮想マシン (VM) によって生成された攻撃、または VM を攻撃している物理サーバーによって生成された攻撃を明らかにします。IDS エンジン、攻撃の一方の側が VM であるときに攻撃を識別できます。IDS モジュールには以下の 4 つのタブがあります。

- [Top Alerts] タブ 68ページ
- [Alert Sources] タブ 69ページ
- [Alert Targets] タブ 69ページ
- [All Alerts] タブ 70ページ

### [Top Alerts] タブ

[Top Alerts] タブには、指定した期間（たとえば 24 時間など）に発生したアラートを示すグラフが表示されます。異なる時間間隔を指定すると、その期間内に発生したアラートが表示されます。グラフを見ると、各アラート オプションの発生頻度が一目わかります。このタブにはグラフの他にアラートのタイプとそのシグネチャ ID を表す表があり、異なる時間間隔を指定した場合にはその間隔内に発生したアラートが表示されます。

図 29: IDS モジュールの [Top Alerts] タブ



各アラートは高、中、低に分類され、総数（[Total] 列）の多い順に並べられます。

各アラートの詳細を表示するには、[Alert Type] 列見出しをクリックします。そうすると、アラートの説明とそのシグネチャ ID を含む画面が表示されます。アラートを発生させたトラフィックの生成元、またはそのトラフィックの宛先を知りたい場合は、アラートの詳細画面の上部にある [Alert Sources] または [Alert Targets] をクリックします。特定のアラートの優先レベルを変更する場合、またはそのアラートに関する情報を表示しない場合は、設定モジュールの [Security Settings] セクションにある [IDS Signatures] 画面を使用します。

アラートの詳細には、説明とシグネチャ ID が含まれます。

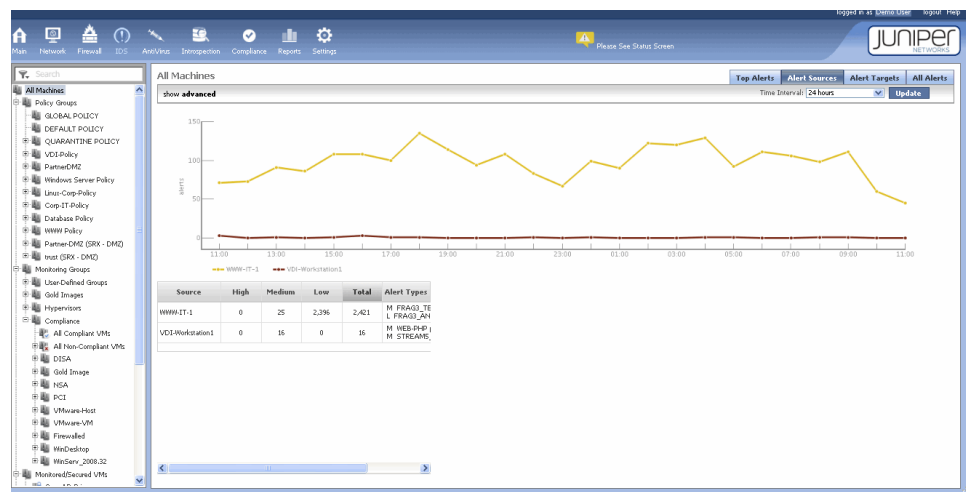
- [IDS Signatures] 設定画面の [Sig Id]、または自由形式のテキストを使用して、シグネチャリストを検索できます。
- 表示されたアラートに関する詳細（トラフィックの生成元や宛先など）が知りたい場合は、詳細画面の上部にある [Alert Sources] または [Alert Targets] をクリックします。

## [Alert Sources] タブ

[Alert Sources] タブには、vGW シリーズによって IDS シグネチャと一致すると見なされたトラフィックの生成元システムが表示されます。これらのシステムはゲスト VM (VM) か、仮想ネットワーク上で通信している物理システムのどちらかです。高アラート、中アラート、低アラートの発生回数とアラートの総数を示す列があります。69ページの図30を参照してください。

総数の最も多いシステムがリストの一番上に表示されます。[High]、[Medium]、[Low] の各列をクリックして表示を並べ替えることができます。また、[Alert Type] 列のアラート名をクリックすると、特定の攻撃に関する情報（トラフィックの生成元や宛先など）が得られます。

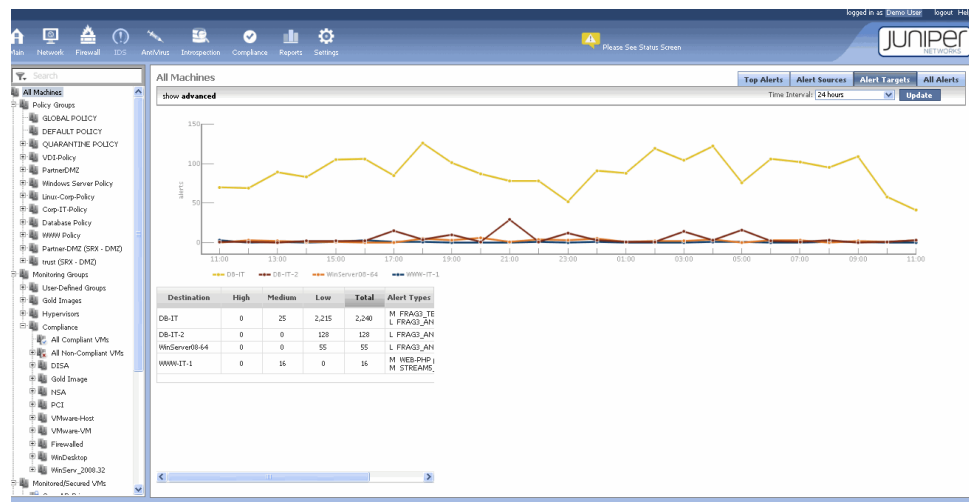
図 30: IDS モジュールの [Alert Sources] タブ



## [Alert Targets] タブ

[Alert Targets] タブは、最も多くの攻撃を受けているシステムが表示される点以外は [Alert Sources] タブと同じです。70ページの図31を参照してください。

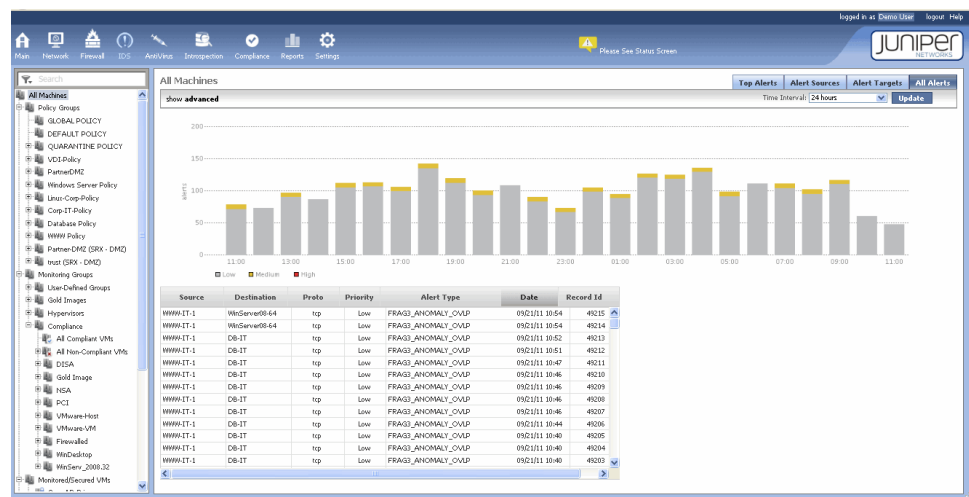
図 31: IDS モジュールの [Alert Targets] タブ



## [All Alerts] タブ

[All Alerts] タブには、[Time Interval] で設定した期間（デフォルトは 24 時間）内にシステムによって捕捉された各アラートをすべて含むリストが表示されます。 特定のアラートの詳細を表示するには、アラート タイプをクリックします。 デフォルトでは、最も最近発生したイベントが画面の一番上に表示され、下に行くほど発生日時が古くなります。 各アラートは [Time] 列の順に並べられます。 70ページの図32を参照してください。

図 32: IDS モジュールの [All Alerts] タブ



- 関連項目
- 166ページのIDS 設定の理解と構成
  - 168ページのIDS シグネチャ設定の理解と構成
  - 71ページのIDS 設定の構成とアクティビティの表示

## IDS 設定の構成とアクティビティの表示

---

このトピックでは、vGW セキュリティ デザイン VM を構成して、IDS エンジンによって生成された結果を各タブに表示する方法について説明します。

1. IDS を有効にしてその設定を指定するには、以下のトピックを参照してください。

- [166ページのIDS 設定の理解と構成](#)

**IDS Settings**

*Intrusion Detection System base settings*

☒ Enable IDS

---

**IDS Parameters**

*Port numbers for protocols to be treated as HTTP*

HTTP ports:

*Port numbers for protocols to be treated as SSL*

SSL ports:

- [168ページのIDS シグネチャ設定の理解と構成](#)

**IDS Updates**

*IDS signatures are updated frequently. The settings below control the behavior of the update processing.*

---

**Auto Update (Hourly Check)**

☒ Disabled

☐ Download Automatically, Manually Apply Updates

☐ Download and Apply Update Automatically

---

**Update Status**

Currently Installed Signatures: **20110823.6366-1-1**

Signatures Available for Update: **20110902.6366-1-1**

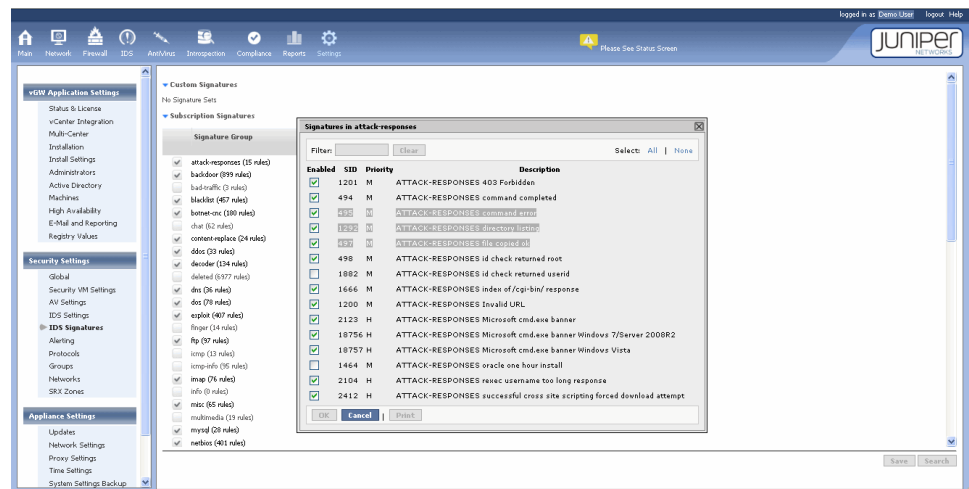
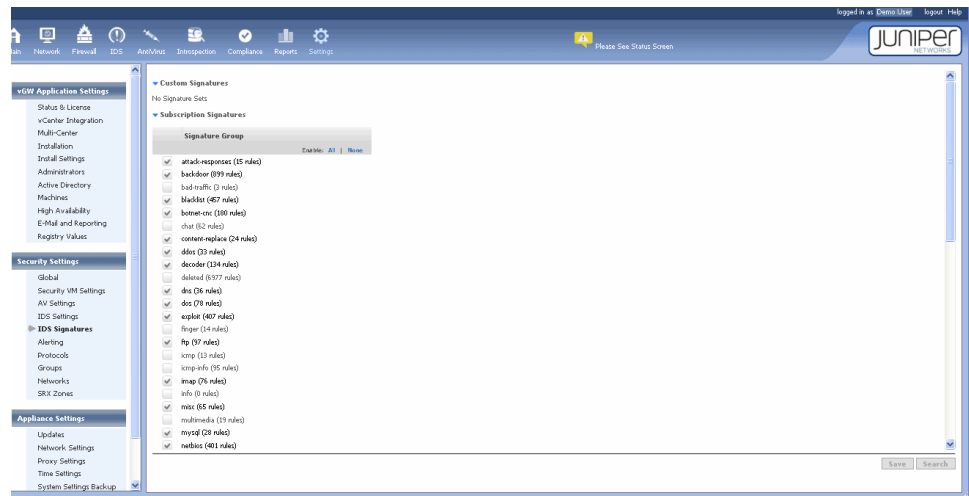
Last Update Check:

Next Update Check:

---

**Upload Signatures File**

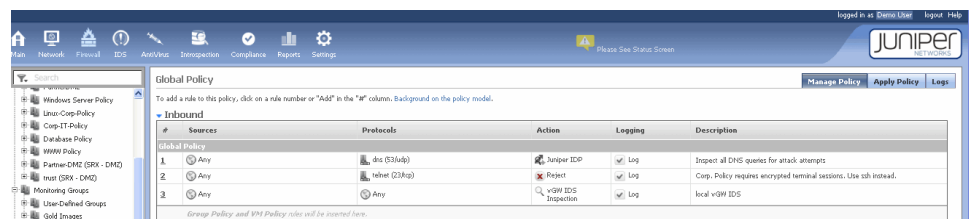
2. 運用環境に関連するシグネチャを有効にするには、[168ページの「IDS シグネチャ設定の理解と構成」](#)を参照してください。設定モジュールの [Security Settings] セクションの [IDS Signatures] セクションを使用します。



3. トラフィックを IDS エンジンにオフロードするファイアウォール規則を作成して適用します。vGW シリーズでは、スキャンするトラフィックを細かい粒度で指定できます。たとえば、特定の VM へのトラフィックや特定の VM からのトラフィックをスキャンしたり、特定のプロトコルを使用したトラフィックをスキャンすることが可能です。

次の図は、すべてのインバウンド トラフィックを IDS によって検査してログに記録するよう指定するインバウンド ファイアウォール規則を示します。

図 33: IDS インバウンド ポリシー規則



4. [Apply Policy] タブを使用して IDS 規則を適用します。

この構成が完了すると、仮想ネットワークで不審なトラフィックが発生したときに IDS エンジンによってアラート フラグが設定されます。

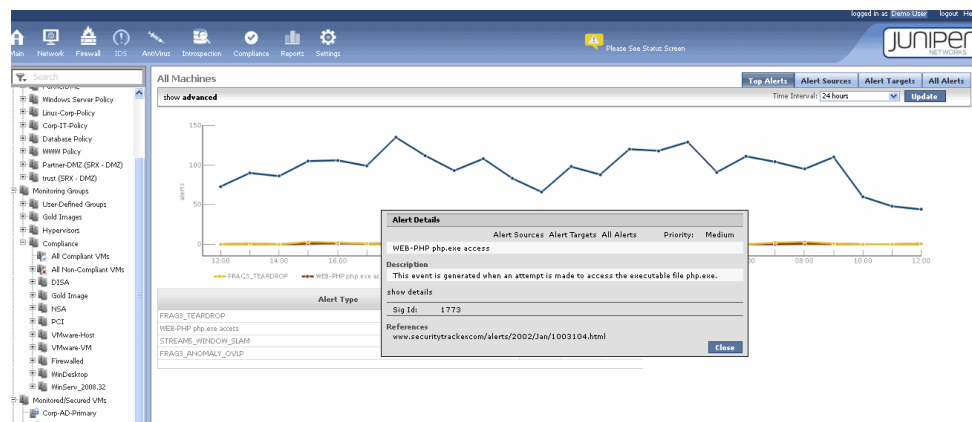
IDS エンジンが適切に機能していることを確認するには、以下の手順に従います。

1. 保護されている VM への HTTP 接続を開き、リクエストを送信します。

たとえば、`http://10.10.10.10/php.exe` と入力します。VM がポート 80 をリッスンしている場合、この `php.exe` のリクエストはシグネチャ ID 1773 (WEB-PHP `php.exe` access) に違反します。

2. 画面に書き込まれた規則違反をクリックし、そのアラートに関する詳細情報を確認します。

次の [Alert Details] 画面は、WEB-PHP アラートの詳細を示します。



- 関連項目
- 67ページのvGW シリーズの IDS モジュールの理解
  - 68ページのvGW シリーズの IDS モジュールのタブの理解
  - 121ページのvGW シリーズの IDS レポートについて
  - 168ページのIDS シグネチャ設定の理解と構成



## vGW シリーズのアンチウィルス モジュール

この章には以下のトピックがあります。

- vGW シリーズのアンチウィルス構成の概要 75ページ
- vGW シリーズのアンチウィルスの理解 77ページ
- vGW シリーズ アンチウィルスのオンアクセス スキャンの構成 83ページ
- vGW Endpoint の理解とインストール 86ページ
- vGW シリーズ アンチウィルスのオンデマンド スキャンの構成 89ページ

### vGW シリーズのアンチウィルス構成の概要

---

このトピックでは、vGW シリーズのアンチウィルス機能による仮想化環境の保護を構成する手順の概要を示します。



注: vGW シリーズのアンチウィルス機能にはライセンスが必要です。

vGW シリーズのアンチウィルス機能の詳細については、77ページの「[vGW シリーズのアンチウィルス モジュールの理解](#)」を参照してください。

vGW シリーズのアンチウィルスには、マルウェアおよびウィルスから運用環境を守るために以下の 2 つの手段が用意されています。

- オンアクセス スキャナ

オンアクセス スキャナは、ゲスト VM (VM) を悪意のあるコンテンツのダウンロードや実行からリアルタイムで守ります。このスキャナは、ファイルにアクセスしたとき、またはファイルが送信されたときに VM がウィルスに感染するのを防ぎます。

- オンデマンド スキャナ

オンデマンド スキャナは、VM のディスク全体をオフラインで定期的にスキャンし、仮想ディスク ファイルに悪意のあるコンテンツが含まれていないかどうかを調べます。スキャンをいつ実行するかを指定するスケジュールを設定します。



注: オンデマンド スキャナを使用するときは、ファイルまたは VM を検疫できません。

オンアクセス スキャンの結果として検疫された VM は、メイン モジュールの [Quarantine] タブを使用して管理します。45ページの「[vGW シリーズのメイン モジュールの理解](#)」を参照してください。

[On-Access Scanning] と [On-Demand Scanning] の両方を単一の vGW アンチウイルス スキャナ構成で設定できます。

オンアクセス スキャナ構成の範囲で選択した VM グループのいずれにも含まれない VM は、vGW アンチウイルスによって保護されません。

運用環境の vGW オンアクセス スキャンを構成するには、以下の手順に従います。

1. 以下に示す必須の準備手順を実行します。

システムのこれらの部分を構成すると、VM がウイルスに感染したときに検疫ポリシーに従って VM 全体を検疫できます。VM を検疫すると、その VM へのネットワーク トラフィック およびその VM からのネットワーク トラフィックが完全に制限されます。

また、vGW Endpoint との通信に使用される通信メカニズムが起動します。オンアクセス スキャンによって保護する VM には vGW Endpoint をインストールする必要があります。

以下のことを行います。

- a. ESX/ESXi ホストをセキュリティ保護します。運用環境の ESX/ESXi ホストに vGW セキュリティ VM を配備します。この作業には、設定モジュールの [vGW Applications Settings] の [Installation] セクションを使用します。143ページの「[ESX/ESXi ホストへの vGW セキュリティ VM の配備](#)」を参照してください。
- b. VM をセキュリティ保護します。オンアクセス スキャンによって保護する VM に対して vGW ファイアウォールを構成します。ファイアウォール モジュールの [Manage Policy] タブを使用してファイアウォール ポリシーを作成し、ファイアウォール モジュールの [Apply Policy] タブを使用してそれらのポリシーを適用します。59ページの「[vGW シリーズのファイアウォール モジュールの理解](#)」を参照してください。



注意: vGW セキュリティ VM を配備しなければ、上記の手順に従って vGW ファイアウォールで VM を保護しても、オンアクセス スキャンは機能しません。上記の必須の構成を行わず、オンアクセス スキャナのみを構成して vGW アンチウイルスを有効にしても、効果はありません。

2. VM のオンアクセス スキャナ構成を作成します。

83ページの「[vGW シリーズ アンチウイルスのオンアクセス スキャンの構成](#)」を参照してください。

3. vGW アンチウイルス機能を有効にし、vGW Endpoint をダウンロードします。

165ページの「[vGW シリーズのアンチウイルス設定の理解と構成](#)」を参照してください。

4. 保護する VM に vGW Endpoint をインストールします。

86ページの「[vGW Endpoint の理解とインストール](#)」を参照してください。このトピックでは、VM への vGW Endpoint のインストール方法と、脅威が検出されたときなどの各種状況を通知する vGW Endpoint のポップアップについて説明しています。



注: オンアクセス スキャンによって保護するすべての VM に vGW Endpoint をインストールする必要があります。

オンデマンド スキャンは、以下の点がオンアクセス スキャンとは異なります。

- オンデマンド スキャンの使用時にファイルまたは VM を検疫することはできません。
- オンデマンド スキャンは、vGW セキュリティ VM によって保護されていない ESX/ESXi 上の VM でも実行できます。この場合は、vGW セキュリティ デザイン VM、または別のホスト上の vGW セキュリティ VM によってスキャンが実行されます。TCP 902 が必要です。
- VM に vGW Endpoint をインストールする必要はありません。
- オンデマンド スキャンでは、スキャンする VM を vGW ファイアウォールによって保護できますが、それは必須ではありません。

vGW ファイアウォールによって VM を保護する必要がなく、VM に vGW Endpoint をインストールする必要もないことから、オンデマンド スキャンは、セキュリティ上の危険のない保護された場所から仮想ディスク ファイルに対して実行できます。この利点により、vGW アンチウイルスの rootkit を検出および特定する能力が向上します。mal.exe や simpletroj.exe などの怪しい名前を持つファイルを検出できます。

オンデマンド スキャンを構成するには、以下の手順に従います。

1. VM のオンデマンド スキャナ構成を作成します。

89ページの「[vGW シリーズ アンチウイルスのオンデマンド スキャンの構成](#)」を参照してください。

2. vGW アンチウイルス機能を有効にします。

165ページの「[vGW シリーズのアンチウイルス設定の理解と構成](#)」を参照してください。

- 関連項目
- [3ページのvGW シリーズの理解](#)
  - [36ページのvGW セキュリティ VM の理解](#)

## vGW シリーズのアンチウイルスの理解

このトピックでは、vGW シリーズのアンチウイルス機能について説明します。詳しい説明に入る前に、アンチウイルス技術に関する背景情報を示します。



注: vGW シリーズのアンチウイルス機能にはライセンスが必要です。

このトピックを読む前に、75ページの「[vGW シリーズのアンチウイルス構成の概要](#)」をお読みください。このトピックでは、事前に必要な構成を含む詳しい vGW アンチウイルス構成プロセスの概要を示しています。ステップごとに、詳細な手順を説明するトピックへのリンクがあります。

このトピックには以下のセクションがあります。

- [アンチウイルス ソフトウェアについて 78ページ](#)
- [シグネチャベースの検出 78ページ](#)
- [vGW アンチウイルス機能 78ページ](#)

## アンチウイルス ソフトウェアについて

アンチウイルス ソフトウェアは、ウイルス、ワーム、スパイウェアなどのマルウェアの活動を防ぎ、その存在を検出します。アンチウイルス ソフトウェアの実装には通常、シグネチャベースの検出や rootkit 検出の採用など、さまざまな手段が関与します（vGW アンチウイルスはこれらの検出機能を両方ともサポートしています）。

仮想化環境は物理ネットワークとまったく同じようにマルウェアの脅威や増殖の危険に絶えずさらされています。物理ネットワークの管理者が運用環境を仮想化した場合、ハードウェアデスクトップで使用していたのと同じアンチウイルス ソフトウェアを仮想マシンにもインストールすることが少なくありません。物理環境用に設計されたアンチウイルス ソフトウェアは、仮想システムにインストールした場合には極度に制限を受け、さまざまな問題を引き起こします。たとえば、メモリを過剰に使用したり（1 つのゲスト VM あたりのメモリ使用量が 100 MB を超えることもよくあります）、CPU を使用し尽くしてシステム パフォーマンスを極度に低下させ、*brownout*と呼ばれる状況を生み出したりします。

アンチウイルス ソフトウェアは多くの場合マルウェアに対する防御の最前線ですが、仮想環境ではシステム パフォーマンスを犠牲にしてアンチウイルス ソフトウェアを使用する必要はありません。

## シグネチャベースの検出

シグネチャとは、ある特定のウイルスまたはウイルスのグループの特徴を示す、ウイルスの一部を構成する固有のビット列（ビット パターン）です。vGW アンチウイルス機能は、ウイルス スキャンの実行中に、スキャンするリソースやファイルの内容をウイルス シグネチャ データベースと照合します。

シグネチャ パターンが検出されると、スキャンの構成時に管理者が指定した修復アクションが実行されます。この構成には、vGW アンチウイルス モジュールの [Scanner Config] タブを使用します。複数のアクションを指定できます。たとえば、[Alert when a virus is detected] をアクションとして選択すると、vGW アンチウイルスによってウイルスが検出されたときにそのイベントに関する詳細が [Virus Alerts] タブに表示されます。[Virus Alerts] タブでは、見つかった脅威のタイプ（worm.exe など）、脅威が特定された場所（ワークステーション名など）、およびその他の関連情報を確認できます。

vGW アンチウイルス機能は、2 種類の方法を使用してウイルスやマルウェアを検出するという点で確実性があります。まず、シグネチャ データベースを使用して特定のウイルスを検出します。さらに、不審なコード部分をヒューリスティックに検出する方法によってこのアプローチが補完されます。

## vGW アンチウイルス機能

従来から今日に至るまで、アンチウイルス ソフトウェアは、ホスト（デスクトップ、サーバー、およびその他のローカル デバイス）またはネットワーク（ホストに到達する前にマルウェアや攻撃試行を捕捉できるようにするため）を保護することを目的に開発されてきました。

デスクトップおよびその他のホスト用のソフトウェアは、エージェント（またはエンドポイント）ソフトウェアと考えられています。 エンドポイント ソフトウェアを使用するにはスキャン エンジンと攻撃シグネチャ データベースをすべてのマシンにインストールする必要があります。 デバイスでのシステムの起動速度とパフォーマンスの低下をもたらします。 デバイスのスキャンが実行されると、メモリが消費されてパフォーマンスが影響を受けます。 仮想化環境向けのセキュリティ製品が登場し始めたときは、このモデルが仮想化環境に導入されました。つまり、仮想化ネットワークと仮想化ホストは別々の製品によって別々に保護されていました。

vGW アンチウイルス機能は、どちらのケースにおいても、スキャン エンジンとシグネチャ データベースを各 VM にインストールするのではなく、vGW アンチウイルスを構成する対象の各 ESX/ESXi ホスト上でインスタンス化された vGW セキュリティ VM ファイアウォールにスキャン エンジンとシグネチャ データベースを一元化することにより、VM に対するパフォーマンスの影響を抑えます。 VM がファイルにアクセスするとき、またはファイルを送信しようとするときに、VM にインストールした「軽量な」vGW Endpoint がそのファイル（場合によってはウイルスの検出に必要なファイルの一部分のみ）を検査のために仮想化ネットワークを通じて vGW セキュリティ VM に渡します。

vGW アンチウイルス機能は、vMotion が使用されているときにも有効です。 vGW アンチウイルスによって保護された VM が vMotion によって別の ESX/ESXi ホストに移行された場合も、その VM は引き続き保護されます。 移動先のホスト上の vGW セキュリティ VM が、vGW アンチウイルスによる保護操作を引き継ぎます。

vGW アンチウイルス機能は VM を保護するため、マルウェアを検出し、感染したファイルまたは VM そのものを検疫します（オンアクセス スキャンの場合）。また、管理者が修復方法を定義することもできます。

vGW アンチウイルスの実装は、以下の機能や手段によって、エージェントだけでは実現できないセキュリティや柔軟性の向上をもたらします。

- ESX/ESXi ホスト ハイパーバイザにインストールされたカーネル モジュールの使用
- 管理の統合
- 軽量な vGW Endpoint をインストールした VM に対してオンアクセス スキャンを実行する機能
- オンデマンド機能を使用して、何も追加インストールせずに VM 全体をスキャンする機能

vGW アンチウイルス機能を有効にすると、vGW セキュリティ VM で vGW セキュリティ デザイン VM のスキャン エンジンがアクティブになります。 このアプローチはスキャン エンジンを一元化してディスク、ディスク IO、メモリ、および CPU の使用量を抑え、仮想化インフラストラクチャ全体に負荷を分散させます。

vGW アンチウイルス データベースとそれに対する更新も vGW セキュリティ VM に配備されます。

vGW アンチウイルスは主に以下の 3 つのコンポーネントを利用します。

- vGW セキュリティ デザイン VM
  - vGW セキュリティ デザイン VM を使用して、vGW アンチウイルスの有効化、スキャンの構成、レポートやアラートの表示、新しいバージョンのシグネチャのダウンロード、vGW Endpoint のダウンロードを行います。

- vGW セキュリティ VM

vGW セキュリティ VM はオンデマンド スキャンを実行します。 オンアクセス スキャンでは、vGW Endpoint によって不審なファイルが vGW セキュリティ VM に送信され、そこで分析されます。

オンデマンド スキャンは、vGW セキュリティ VM がインストールされていない ESX/ESXi 上の VM に対しても実行できます。 この場合は、vGW セキュリティ デザイン VM、または別のホスト上の vGW セキュリティ VM によってスキャンが実行されます。TCP 902 が必要です。vGW アンチウィルスは、VM が vMotion によって別の分析対象のホストに移行されたときにも引き続き有効です。 移行先のホスト上の vGW セキュリティ VM が vGW アンチウィルスの機能を実行します。

- vGW Endpoint

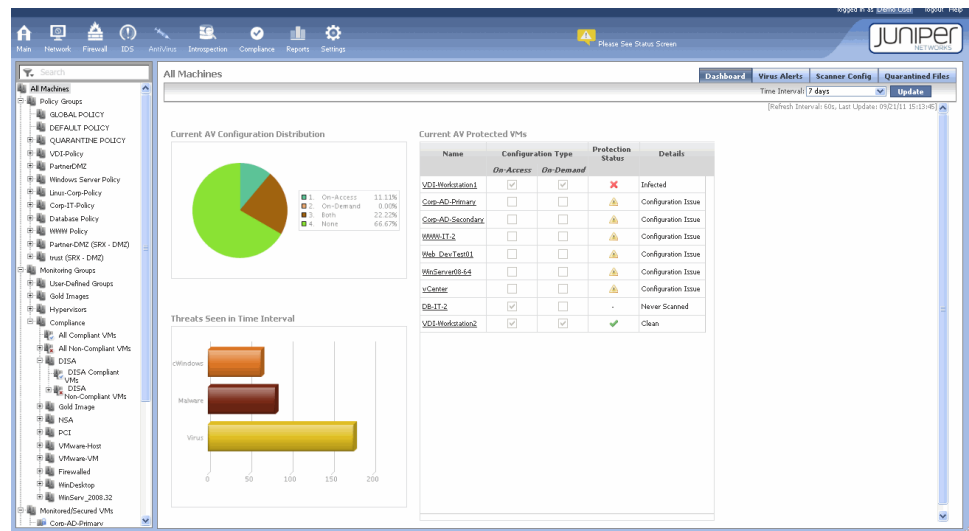
vGW Endpoint はオンアクセス スキャンに使用されます。 これは、ファイルにアクセスするとき、またはファイルが送信されたときに、感染ファイルから VM を守ります。vGW Endpoint によってファイルが vGW セキュリティ VM に送信され、そこで分析されます。 感染したファイルが見つかり、オンアクセス スキャナ構成で検疫アクションが指定されていた場合、そのファイルは VM 上の vGW Endpoint に隔離され、管理者が検疫から解放するか、削除するか、取得するまで、そこにとどまります。 検疫から解放したファイルは VM で再び使用できます。

オンデマンド スキャンでは、vGW Endpoint をインストールする必要はありません。

## vGW アンチウィルス ダッシュボード

vGW アンチウィルス ダッシュボードには、運用環境で保護されているすべての VM の現在の状態の全体像が表示されます。

運用環境内のすべての VM の情報を表示できるほか、VM ツリーで特定の VM を選択してその情報を表示することもできます。 また、時間間隔を変更して、より広い期間または狭い期間内に発生した脅威を表示することも可能です。 さらに、VM の vGW アンチウィルス イベントに関する情報（ウィルスが検出された、シグネチャが更新された、など）も表示できます。

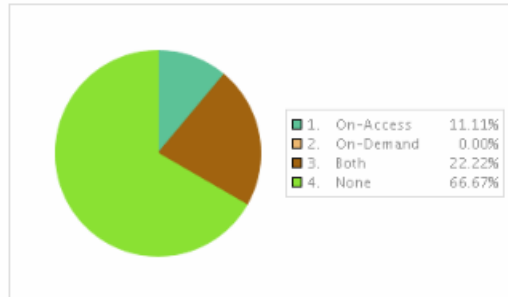


vGW アンチウィルス ダッシュボードは以下のペインで構成されています。

- Current AV Configuration Distribution

この円グラフは、オンアクセス スキャナによって保護されている VM、オンデマンド スキャナによって保護されている VM、その両方によって保護されている VM、および vGW アンチウィルスによって保護されていない VM の数の比率を示します。

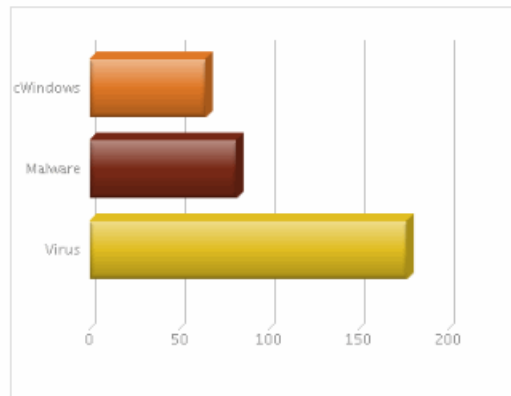
Current AV Configuration Distribution



- Threats Seen in Time Interval

この棒グラフには、選択した時間間隔内に見つかった脅威の種類と割合が表示されます。

Threats Seen in Time Interval

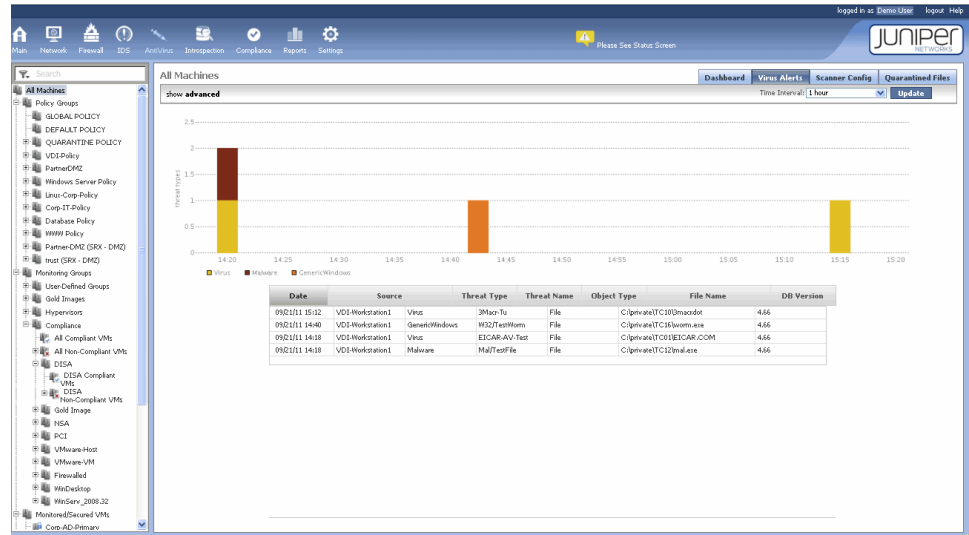


- Current AV Protected VMs

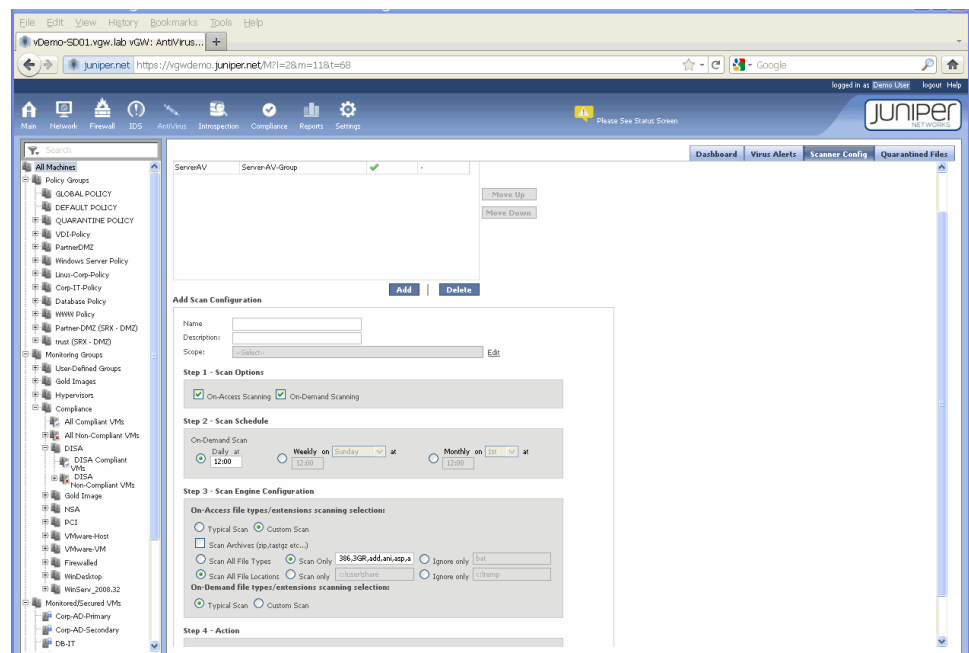
この表は、vGW アンチウィルスによって保護されている VM、それらの VM を保護するスキャナ構成のタイプ、および保護ステータスとその詳細を示します。保護ステータスが問題を示している場合は、その VM の行をクリックして詳細情報を表示できます。図 Xx を参照してください。

たとえば、ある VM の保護ステータスが感染状態を示している場合は、その行をクリックして VM の詳細を表示します。そうすると、該当する VM のスキャン統計（スキャンされたファイルの数や検疫されたファイルの数など）、VM のスキャナ構成、VM の脅威タイプ棒グラフが表示され、企てられたウィルス感染、その発生日時、および vGW アンチウィルスによる対処を表す表が表示されます。

[Virus Alerts] タブには、[Time Interval] フィールドで指定した期間内に発生した脅威のタイプを示すグラフと、脅威のタイプに関する詳細（イベントの日時、発生場所、ファイル名）が表示されます。

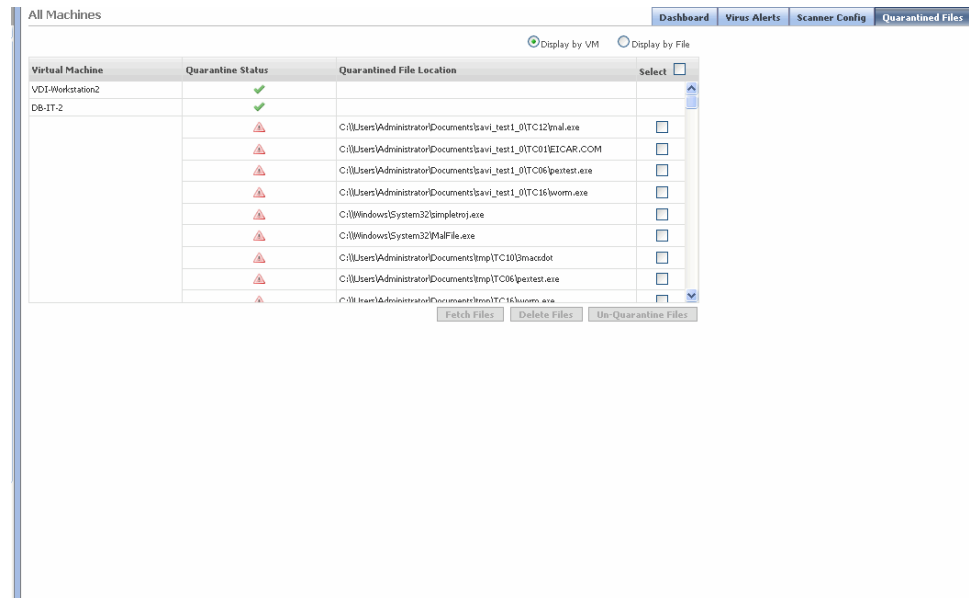


[Scanner Config] タブでは、オンアクセス スキャンとオンデマンド スキャンを定義できます。[Add] をクリックして [Add Scan Configuration] ペインを表示したときは、両方のスキャン タイプが選択されています。各スキャン タイプを別々に設定することも、1 つの構成でまとめて設定することもできます。標準スキャンとカスタム スキャンのどちらかを選択します。次の図は、両方のスキャン タイプをまとめてカスタム スキャンとして定義した例を示します。各スキャン タイプを別々に設定する方法の詳細については、83ページの「vGW シリーズ アンチウィルスのオンアクセス スキャンの構成」および89ページの「vGW シリーズ アンチウィルスのオンデマンド スキャンの構成」を参照してください。





[Quarantined Files] タブには、検疫されたファイルのリストが表示されます。検疫できるのは、オンアクセス スキャンによって見つかった感染ファイルのみです。検疫されたファイルは VM 上の vGW Endpoint に隔離され、それに関する情報がこの画面に表示されます。検疫されたファイルを含む VM、そのファイルの場所、およびステータスが示されます。



1 つ以上のファイルを選択して、以下のアクションを実行できます。

- ファイルを取得できます。この場合は、さらに分析するためにファイルがハッシュされ、VM から転送されます。
- ファイルを検疫解除できます。この場合は、隔離されたファイルが再び VM で使用できるようになります。

場合によっては、誤検出によってファイルが検疫されることがあります。これは、ファイルがマルウェアである、または感染している疑いがあるものの、実際はそうではないことを意味します。シグネチャ データベースを更新してスキャンを再度実行すると、この問題が解決する場合があります。

- そのファイルが間違いなくマルウェアであるか感染していることが確認された場合は、VM から削除できます。

VM がウイルスに感染していて、スキャン構成で [Quarantine the VM] が指定されている場合、その VM は検疫ポリシー グループに配置されます。検疫ポリシー グループから VM を移動するには、メイン モジュールの [Quarantine] タブを使用します。該当する VM を選択し、[Un-quarantine] をクリックします。

関連項目 • [86ページのvGW Endpoint の理解とインストール](#)

## vGW シリーズ アンチウイルスのオンアクセス スキャンの構成

このトピックでは、vGW アンチウイルスのオンアクセス スキャナの構成方法について説明します。この構成には、vGW セキュリティ デザイン VM のアンチウイルス モジュールを使用しま

す。オンアクセス スキャンが構成されている場合は、ファイルにアクセスするたび、またはファイルが送信されるたびに、vGW アンチウイルスが割り込んでそのファイルをシグネチャデータベースと照合し、マルウェアやウイルスが含まれていないことを確認します。vGW アンチウイルスのオンアクセス スキャンは、ゲスト VM (VM) への感染ファイルのダウンロードをブロックすることにより、損害を受ける前に大元の段階でネットワークを悪意ある攻撃から守ります。

vGW アンチウイルス構成プロセス全体の概要については、[75ページの「vGW シリーズのアンチウイルス構成の概要」](#)を参照してください。このトピックには、vGW アンチウイルス構成のその他の部分について説明するトピックへのリンクがあります。

オンアクセス スキャンを構成する前に、以下のことを行います。

- 運用環境の ESX/ESXi ホストに vGW セキュリティ VM を配備します。
- ファイアウォール ポリシーを構成し、保護する VM にインストールします。

vGW アンチウイルスのオンアクセス構成を作成、または新規に追加するには、以下の手順に従います。

1. アンチウイルス モジュールを選択します。アンチウイルス モジュールのメイン画面で、[Scanner Config] タブを選択します。
2. [Add] をクリックします。
3. vGW アンチウイルス スキャナ構成の名前を指定します。
4. 必要に応じて、後でわかりやすいように定義の簡単な説明を入力します。
5. [Scope] フィールドで、スキャンする VM メンバーを含む VM グループを指定します。リストから VM グループを選択して [Selected Groups] に移動します。

スキャンを定義した後、そのスキャンは [Scanner Config] 表の構成リストに追加されます。



注:

ある VM グループが複数のスキャナ構成のメンバーである場合は、その VM グループが属する一番上のスキャン定義が使用されます。表でのスキャナ構成の順序は変更できます。

6. [Step 1 Scan Options] セクションで、[On-Access Scanning] チェックボックスをオンにします。



注: スキャナ構成画面の [Step 2] はオンデマンド スキャンの場合にのみ必須なので、ここでは省略します。

7. [Step 3 Scan Engine Configuration] セクションの [On-Access file types/extensions scanning selection] で、実行するスキャンのタイプとして [Typical Scan] と [Custom Scan] のどちらかを選択します。この例では、[Typical Scan] チェックボックスをオンにします。

カスタム スキャンの作成方法の詳細については、この後に示す手順を参照してください。

8. [Step 4 Action] セクションで、スキャンによってウイルスが検出されたときに実行するアクションを以下の中から 1 つ以上選択します。

- Alert when a virus is detected – 感染した VM またはファイルの情報を [Virus Alerts] タブに表示します。
- Quarantine the VM – 感染した VM を検疫ポリシー グループに含めます。

アンチウイルス スキャンの結果として検疫された VM のリストを表示するには、メインモジュールの [Quarantine] タブを使用します。VM を検疫から解放するには、このタブで VM を選択して [Un-Quarantine VM] ボタンをクリックします。詳細については、XXX を参照してください。

- Quarantine infected files – 感染したファイルを検疫します。

検疫されたファイルのリストを表示するには、アンチウイルス モジュールの [Quarantined Files] タブを使用します。オプション ボタンを使用して情報の表示方法を指定します。検疫されたファイルを VM 別に分類して表示するか、フラットで包括的なファイル リストとして表示するかを選択できます。

[Quarantine Files] 画面では、感染したファイルを削除、または検疫から解放できます。また、感染したファイルを取得し、独自のプロセスに従って修復することもできます。

- Suspend the VM – VM 全体を一時停止します。

スキャンするファイルを指定できるカスタム スキャンを作成するには、以下の手順に従います。

1. [Step 3 Scan Engine Configuration] セクションの [On-Access file types/extensions scanning selection] で、[Custom Scan] オプション ボタンを選択します。
2. スキャンするファイルを選択します。



**注:** このセクションで指定したファイル タイプとファイルの場所は、スキャンするファイルを明確に特定するために組み合わせて働きます。たとえば、[Scan All File Types] と [Scan Only] (場所としてたとえば c:\user\share を指定) を選択した場合は、その場所にあるすべてのファイルだけがスキャンされます。

- a. 各種フォーマットでアーカイブされたすべてのファイルをスキャンする場合は、[Scan Archives] チェックボックスをオンにします。

パフォーマンスを向上させる場合は、アーカイブ ファイルをスキャンしないでください。

- b. スキャンするファイルのタイプを選択します。以下のいずれかを選択します。

- Scan All File Types – 選択したファイルの場所にあるすべてのタイプのファイルをスキャンします。
- Scan Only – 選択したファイルの場所にある、指定したタイプのファイルのみをスキャンします。デフォルトで入力されているリストから、スキャンしないファイル タイプを削除できます。

- Ignore only – 指定したタイプを除くすべてのタイプのファイルをスキャンします。
- c. スキャンするファイルが存在する場所を選択します。
  - Scan All Locations – すべての場所の、選択したタイプのファイルをスキャンします。
  - Scan only – 指定した場所にある、選択したタイプのファイルをスキャンします。
  - Ignore only – 指定した場所に存在するファイルを除くすべてのファイルをスキャンします。

関連項目

## vGW Endpoint の理解とインストール

このトピックでは、vGW Endpoint とその使用方法について説明します。vGW アンチウイルス構成の全体的コンテキストにおける vGW Endpoint のダウンロードおよびインストール手順を理解するには、75ページの「vGW シリーズのアンチウイルス構成の概要」を参照してください。

- [vGW Endpoint のインストール 86ページ](#)
- [vGW Endpoint の自動更新 86ページ](#)
- [VM 上の vGW Endpoint 87ページ](#)
- [検疫されたファイル 88ページ](#)
- [vGW Endpoint のコンポーネントと表示 88ページ](#)

### vGW Endpoint のインストール

vGW シリーズのオンアクセス スキャンを VM で実行するためには、オンアクセス スキャナ構成の範囲で指定した VM グループに属する各 VM に vGW Endpoint をインストールする必要があります。vGW Endpoint はバイナリ形式の実行可能ファイル（.exe ファイル）で、さまざまな方法でインストールできます。たとえば、ネットワーク共有にバイナリを配置している場合は、ログイン スクリプトによってドライブをマップしてバイナリを実行できます。また、Web サーバーにバイナリを掲載し、必要に応じてダウンロードして実行する方法もあります。この場合は、Microsoft Server and Cloud Platform System Center や Manage Engine Desktop Central ソフトウェアなどのソフトウェア パッケージを使用してもかまいません。この目的では、どれでも好きなツールを使用できます。

### vGW Endpoint の自動更新

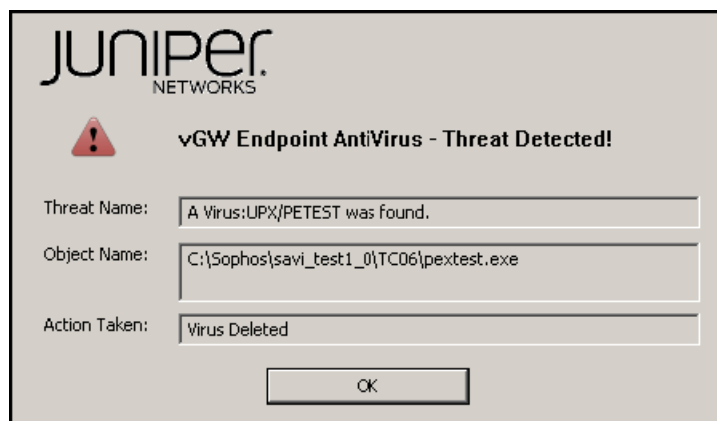
vGW Endpoint をダウンロードし、オンアクセス スキャナ構成で指定した運用環境の保護 VM に配布した後は、vGW Endpoint を更新する必要はありません。vGW セキュリティ デザイン

VM を更新するとき、すべての VM 上の vGW Endpoint も自動的に更新されます。つまり、vGW Endpoint は一度インストールすれば、後は自動的に更新が配備されます。

## VM 上の vGW Endpoint

vGW Endpoint が vGW シリーズに接続しているとき、次の画面が VM に表示されます。

vGW アンチウイルスによって VM への脅威が検出されると、それを通知するために次のアラート画面が表示されます。



### 検疫されたファイル

オンアクセス スキャンの結果として検疫されたファイルは、保護 VM 上の vGW Endpoint に隔離されます。検疫されたファイルは VM からアクセスできませんが、VM 上にローカルに残ります。検疫されたファイルはアンチウイルス モジュールの [Quarantine] タブを使用して管理します。これらのファイルは以下のように扱うことができます。

- ファイルを取得できます。この場合は、さらに分析するためにファイルがハッシュされ、VM から転送されます。
- ファイルを検疫解除できます。この場合は、隔離されたファイルが再び VM で使用できるようになります。

場合によっては、誤検出によってファイルが検疫されることがあります。これは、ファイルがマルウェアである、または感染している疑いがあるものの、実際はそうではないことを意味します。シグネチャ データベースを更新してスキャンを再度実行すると、この問題が解決する場合があります。

- そのファイルが間違いなくマルウェアであるか感染していることが確認された場合は、VM から削除できます。

### vGW Endpoint のコンポーネントと表示

vGW Endpoint には以下のコンポーネントが含まれます。

- ファイルの監視やスキャン ポリシーの強制を行うフィルタ ドライバ。
- vGW セキュリティ VM との通信を処理するサービス。これは状態の報告や vGW アンチウイルス ポリシーの強制（オンアクセス スキャン時のファイルの検疫など）を行います。
- vGW セキュリティ デザイン VM のサービスにとって既知の状態を示すトレイ アプリケーション。このアプリケーションは、以下の 3 つのアイコンによって 3 種類の主な状態を表します。

- 赤い警告三角形アイコン - 脅威が検出されたとき、赤い警告三角形アイコンが付いたポップアップ ウィンドウが表示されます。 脅威がなくなると、赤い三角形アイコンは消えます。
- 透明のバースト アイコン - すべてのコンポーネントが実行され、vGW セキュリティ VM に接続しています。
- 黄色の三角形が付いたバースト アイコン - サービスとドライバは実行されていますが、vGW セキュリティ VM との通信がまだ完全には確立されていません。
- 赤い x が付いたバースト アイコン - サービスまたはドライバがロードされていません。この状態では、vGW アンチウイルス ポリシーを強制できません。 問題が解決すると、透明のバースト アイコンが表示されます。

関連項目    • [3ページのvGW シリーズの理解](#)

## vGW シリーズ アンチウイルスのオンデマンド スキャンの構成

このトピックでは、オフラインの完全ディスク スキャンをスケジュールできるオンデマンド vGW アンチウイルス スキャン機能を構成する方法について説明します。 スキャン フットプリントを小さくするため、ディスクの特定の部分のみをスキャンするよう指定したり、全体スキャンから一部を除外したりできます。 オンデマンド スキャンでは、VM に何らかのソフトウェアをインストールする必要はありません。 オンアクセス スキャンでは vGW Endpoint をインストールする必要がありますが、オンデマンド スキャンではこれは不要です。

このトピックを読む前に、[75ページの「vGW シリーズのアンチウイルス構成の概要」](#)を読んでプロセス全体を理解してください。



注: [On-Access Scanning] と [On-Demand Scanning] の両方を単一のアンチウイルス スキャナ構成で設定できます。

オンデマンド スキャンでは、

- 日次、週次、または月次のスキャンをスケジュールできます。
- vGW Endpoint エージェントは必要ないため、VM にインストールする必要はありません。
- rootkit 検出が実行されます。

vGW ファイアウォールによって VM を保護する必要がなく、VM に vGW Endpoint をインストールする必要もないことから、オンデマンド スキャンは、セキュリティ上の危険のない保護された場所から仮想ディスク ファイルに対して実行できます。 この利点により、vGW アンチウイルスの rootkit を検出および特定する能力が向上します。 vGW アンチウィル

ス エンジンには、rootkit ファイルの検出に役立つシグネチャが含まれています。mal.exe や simpletroj.exe などの怪しい名前を持つファイルを検出できます。

vGW アンチウィルスのオンデマンド構成を作成、または新規に追加するには、以下の手順に従います。

1. vGW アンチウィルス モジュールを選択します。vGW アンチウィルス モジュールのメイン画面で、[Scanner Config] タブを選択します。

The screenshot shows the 'Scanner Config' tab in the vGW interface. It contains the following sections:

- Name:** A text input field.
- Description:** A text input field.
- Scope:** A dropdown menu with '--Select--' and an 'Edit' button.
- Step 1 - Scan Options:** Contains two checkboxes: 'On-Access Scanning' (unchecked) and 'On-Demand Scanning' (checked).
- Step 2 - Scan Schedule:** Contains three radio buttons for scheduling: 'Daily at 12:00' (selected), 'Weekly on Sunday at 12:00' (unchecked), and 'Monthly on 1st at 12:00' (unchecked).
- Step 3 - Scan Engine Configuration:** Contains two sections:
  - 'On-Access file types/extensions scanning selection:' with 'Typical Scan' (selected) and 'Custom Scan' (unchecked).
  - 'On-Demand file types/extensions scanning selection:' with 'Typical Scan' (selected) and 'Custom Scan' (unchecked).
- Step 4 - Action:** Contains four checkboxes: 'Alert when a virus is detected' (checked), 'Quarantine VM' (checked), 'Quarantine infected files' (checked), and 'Suspend VM' (unchecked).
- Buttons:** 'Save' and 'Cancel' buttons at the bottom right.

2. [Add] をクリックします。
3. vGW アンチウィルス オンデマンド構成スキャンの名前を指定します。
4. [On-Demand Scan] オプション ボタンを選択します。
5. 必要に応じて、後でわかりやすいように定義の簡単な説明を入力します。
6. [Scope] フィールドで、スキャンする VM グループを指定します。

This screenshot shows the same 'Scanner Config' interface as before, but with a modal dialog open for selecting VM groups. The dialog has two panes: 'All Groups' and 'Selected Groups'.

- All Groups:** A list of VM groups including 'Corp-IT-Policy', 'Database Policy', 'Firewalled\_compliant', 'Hypervisors', 'Linux-Corp-Policy', 'Partner-DMZ (SRX - DMZ)', 'PartnerDMZ', 'Poomima-Test Group', 'Server-AV-Group', and 'trust (SRX - DMZ)'.
- Selected Groups:** An empty list box.
- Buttons:** 'Apply' and 'Cancel' buttons at the bottom right of the dialog.



7. [Step 2 Scan Schedule] セクションで、いつスキャンを実行するかを指定します。

日次、週次、または月次のスキャンをスケジュールできます。

8. [Step 3 Scan Engine Configuration] セクションで、実行するスキャンのタイプとして [Typical Scan] と [Custom Scan] のどちらかを選択します。この例では、[Typical Scan] チェックボックスをオンにします。

カスタム スキャンの作成方法の詳細については、この後に示す手順を参照してください。

**Step 3 - Scan Engine Configuration**

**On-Access file types/extensions scanning selection:**

☒ Typical Scan ☐ Custom Scan

**On-Demand file types/extensions scanning selection:**

☐ Typical Scan ☐ Custom Scan

**Step 4 - Action**

☒ Alert when a virus is detected ☒ Quarantine VM ☒ Quarantine infected files ☐ Suspend VM

**Save** **Cancel**

9. [Step 4 Action] セクションで、スキャンによってウイルスが検出されたときに実行するアクションを以下の中から選択します。



**注意:** オンデマンド スキャンでは、ファイルまたは VM を検疫することはできません。

- Alert when a virus is detected – 感染した VM またはファイルの情報を [Virus Alerts] タブに表示します。
- Suspend the VM – VM 全体を一時停止します。

スキャンするファイルを指定できるカスタム スキャンを作成するには、以下の手順に従います。

1. [Step 3 Scan Engine Configuration] セクションの [On-Demand file types/extensions scanning selection] で、[Custom Scan] オプション ボタンを選択します。

**Step 3 - Scan Engine Configuration**

**On-Access file types/extensions scanning selection:**

☐ Typical Scan ☒ Custom Scan

☐ Scan Archives (zip, tar, gz etc...)

☐ Scan All File Types ☒ Scan Only  ☐ Ignore only

☒ Scan All File Locations ☐ Scan only  ☐ Ignore only

**On-Demand file types/extensions scanning selection:**

☐ Typical Scan ☐ Custom Scan

2. スキャンするファイルを選択します。



注: このセクションで指定したファイル タイプとファイルの場所は、スキャンするファイルを明確に特定するために組み合わせて働きます。たとえば、[Scan All File Types] と [Scan Only] (場所としてたとえば c:\user\share を指定) を選択した場合は、その場所にあるすべてのファイルだけがスキャンされます。

- a. 各種フォーマットでアーカイブされたすべてのファイルをスキャンする場合は、[Scan Archives] チェックボックスをオンにします。  
  
パフォーマンスを向上させる場合は、アーカイブ ファイルをスキャンしないでください。
- b. スキャンするファイルのタイプを選択します。以下のいずれかを選択します。
  - Scan All File Types – 選択したファイルの場所にあるすべてのタイプのファイルをスキャンします。
  - Scan Only – 選択したファイルの場所にある、指定したタイプのファイルのみをスキャンします。デフォルトで入力されているリストから、スキャンしないファイル タイプを削除できます。
  - Ignore only – 指定したタイプを除くすべてのタイプのファイルをスキャンします。
- c. スキャンするファイルが存在する場所を選択します。
  - Scan All Locations – すべての場所の、選択したタイプのファイルをスキャンします。
  - Scan only – 指定した場所にある、選択したタイプのファイルをスキャンします。
  - Ignore only – 指定した場所に存在するファイルを除くすべてのファイルをスキャンします。

関連項目    • [3ページのvGW シリーズの理解](#)

## vGW シリーズのイントロスペクション モジュール

この章には以下のトピックがあります。

- [vGW シリーズのイントロスペクション モジュールの理解 93ページ](#)
- [vGW シリーズ イントロスペクションの \[Applications\] タブの理解 95ページ](#)
- [vGW シリーズ イントロスペクションの \[VMs\] タブの理解 97ページ](#)
- [vGW セキュリティ デザイン VM イントロスペクションのイメージ エンフォース機能の理解 98ページ](#)
- [vGW シリーズの \[Image Enforcer\] タブの理解 100ページ](#)
- [vGW シリーズの \[Enforcer Profiles\] タブの理解 101ページ](#)
- [vGW シリーズ イントロスペクションのスケジュール機能の理解 104ページ](#)
- [vGW シリーズ イントロスペクションのスキャン ステータスの理解 105ページ](#)
- [vGW シリーズ イントロスペクションのレジストリ チェック機能の理解 106ページ](#)

### vGW シリーズのイントロスペクション モジュールの理解

vGW セキュリティ デザイン VM のイントロスペクション モジュールを使用すると、RPM パッケージ マネージャをサポートするすべての MS Windows および Linux ゲスト仮想マシン (VM) にインストールされた仮想インフラストラクチャ内のソフトウェアを監視できます。vGW シリーズでは、ゲスト VM にエンドポイント ソフトウェアをインストールせずに、インストールされているアプリケーション、オペレーティング システムのタイプ (MS Windows XP や Windows 2003 など)、レジストリ値、および適用されている更新 (ホットフィックス) を特定できます。

MS Windows システムにインストールされているアプリケーションをスキャンするとき、レジストリ情報もスキャンされます。大部分は vGW セキュリティ VM がスキャンを実行します。vGW セキュリティ VM がスキャンのほとんどを実行するため、スケーラビリティの問題が軽減され、プロセスが高速になるとともに、新しいセキュリティ リスクの導入を回避できます。

vGW シリーズのイントロスペクションは、スキャン エンジンを一元化してディスク、ディスク IO、メモリ、および CPU の使用量を抑え、システムのすべての部分に負荷を分散させます。vGW セキュリティ デザイン VM と vGW セキュリティ VM の両方がこのプロセスに関与します。つまり、vGW セキュリティ VM がデフォルトでスキャンを実行しますが、vGW セキュリティ VM がインストールされていない VM もスキャンできます。この場合は、vGW セキュリティ デ

ザイン VM によってスキャンが実行され、ESX/ESXi ホストにアクセスするため TCP ポート 902 が必要となります。

イントロスペクション モジュールは、VM のスナップショットをとってそれを分析します。これにより、スキャン中にアクティブな VM への悪影響が生じないことが保証されます。スキャンが完了した後、スナップショットはただちに削除されます。

スキャンによって VM のアプリケーションを調べる際、ネットワーク パケットは使用されません。その代わりに、ネイティブの VMware インフラストラクチャを使用してディスクの内容が確認されます。そのため、高速かつ正確なスキャンが可能です。長くても数秒で、インストールされているアプリケーションの分析が終わります。

インストールされているアプリケーションを正確に特定できることから、それらの VM のセキュリティ ポリシーが厳密になり、セキュリティ ポリシーを動的に適用できます。たとえば、VM を分析して Apache Web サーバーが実行されている VM を特定し、それらの VM をスマート グループに配置して「webservers」などのグループ名を付けます。このポリシー グループに対して、HTTP/HTTPS による通信を許可するよう設定します。

イントロスペクション モジュールを使用すると、運用環境にインストールされているアプリケーションを評価して、セキュリティ保護されているアプリケーションや必須ではあるが見つからないアプリケーションを確認することが可能です。たとえば、vGW Endpoint が必要な場合に vGW Endpoint がない VM をすばやく特定し、これらの VM を限定的なファイアウォールポリシーによって検疫できます。

イントロスペクション機能はパッチ管理ソリューションの代わりとなることを意図したものではありませんが、この目的でイントロスペクション機能を使用して特定のホットフィックスが適用されているどうかを確認し、必要なホットフィックスが適用されていないホストを、パッチ管理ソリューションによって適切な更新が配備されるまで検疫しておくことができます。

イントロスペクションの結果はタイプ（アプリケーション、オペレーティング システム、ホットフィックス）別に分類され、インストールされているソフトウェアに関するグラフィカルなサマリ比較と詳細な統計情報の表によって表されます。



**警告：** イントロスペクションを適切に機能させるには、vGW セキュリティ デザイン VM と ESX/ESXi ホストの間で TCP ポート 902 を開く必要があります。

イントロスペクション画面には以下のタブがあります。

- Applications

詳細については、95ページの「[「vGW シリーズ イントロスペクションの \[Applications\] タブの理解」](#)」を参照してください。

- VMs

詳細については、97ページの「[「vGW シリーズ イントロスペクションの \[Applications\] タブの理解」](#)」を参照してください。

- Image Enforcer

詳細については、「[vGW セキュリティ デザイン VM イントロスペクションのイメージ エンフォース レポート機能の理解](#)」を参照してください。

- Enforcer Profiles

詳細については、101ページの「「vGW シリーズの [Enforcer Profiles] タブの理解」」を参照してください。

- Scan Status

詳細については、105ページの「「vGW シリーズ イントロスペクションのスキャン ステータス機能の理解」」を参照してください。

- Scheduling

詳細については、104ページの「「vGW シリーズ イントロスペクションのスケジュール機能の理解」」を参照してください。

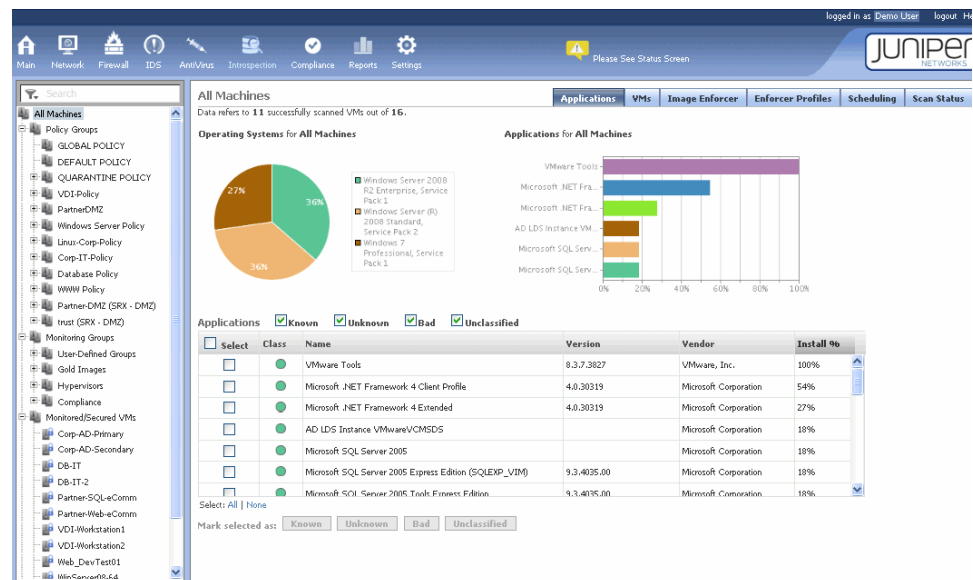
- Scheduling

詳細については、104ページの「「vGW シリーズ イントロスペクションのスケジュール機能の理解」」を参照してください。

関連項目

## vGW シリーズ イントロスペクションの [Applications] タブの理解

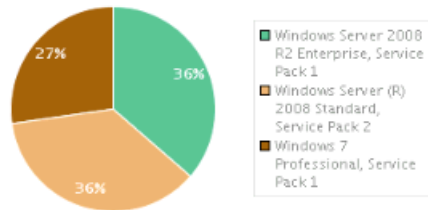
vGW セキュリティ デザイン VM のイントロスペクション モジュールの [Applications] タブには、ゲスト VM (VM) に現在インストールされているソフトウェアに関する以下の情報が表示されます。調べる VM を VM ツリーで選択します。



[Applications] タブには以下のものが含まれます。

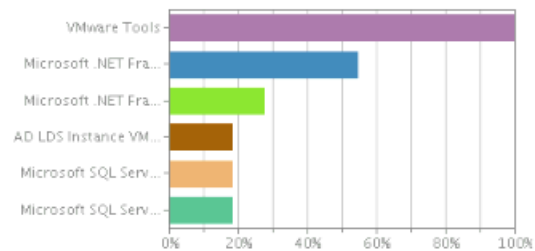
- オペレーティング システムの各タイプの割合を比較する円グラフ。

Operating Systems for All Machines



- アプリケーションの各タイプの割合を比較する棒グラフ。

Applications for All Machines



- 各アプリケーションの詳細なリスト。

Applications ☒ Known ☒ Unknown ☒ Bad ☒ Unclassified

Select	Class	Name	Version	Vendor	Install %
<input type="checkbox"/>		VMware Tools	8.3.7.3827	VMware, Inc.	100%
<input type="checkbox"/>		Microsoft .NET Framework 4 Client Profile	4.0.30319	Microsoft Corporation	54%
<input type="checkbox"/>		Microsoft .NET Framework 4 Extended	4.0.30319	Microsoft Corporation	27%
<input type="checkbox"/>		AD LDS Instance VMwareVCMSDS		Microsoft Corporation	18%
<input type="checkbox"/>		Microsoft SQL Server 2005		Microsoft Corporation	18%
<input type="checkbox"/>		Microsoft SQL Server 2005 Express Edition (SQLEXP_VIM)	9.3.4035.00	Microsoft Corporation	18%
<input type="checkbox"/>		Microsoft SQL Server 2005 Tools Express Edition	9.3.4035.00	Microsoft Corporation	18%

Select: All | None

Mark selected as:



**注:** VM ツリーで VM のグループを選択した場合は、円グラフと棒グラフのデータが集計されます。単一の VM を選択した場合は、詳細な情報が表形式で表示されます。

[Applications] タブは以下の目的で使します。

- 運用環境にインストールされているソフトウェアに関する情報を確認する。これにより、以下のことがわかります。
- ソフトウェアの全体的な評価。インストールされているソフトウェアのタイプを、どの VM にインストールされているかにかかわらず一目で確認できます。

- 特定のソフトウェアが実行されている VM の割合。 特定のアプリケーション、サービスパック、またはオペレーティング システムが実行されている運用環境内の VM の割合がわかります。
- 特定の VM または VM グループに固有の情報。 どのアプリケーションが VM または VM のグループにインストールされているかがわかります。
- インストールされているソフトウェアを運用環境全体にわたって分類する。 この分類体系を使用して VM のソフトウェアの状態を監視し、VM で不正なソフトウェアや不適切なソフトウェアが実行されていないかどうかを管理者の指定に基づいて判定できます。

表で 1 つ以上のアプリケーションを選択し、以下のいずれかに分類できます。

- Known – 運用中の仮想化環境で使用してもよいアプリケーションにはこの分類を使用します。
- Unknown – アプリケーションは存在するものの、これが運用環境にとって適切かどうか不明な場合は、この分類を使用します。
- Bad – 運用環境で使用が許可されていないアプリケーションにはこの分類を使用します。
- Unclassified – まだ調べていないアプリケーションにはこの分類を使用します。 新しくインストールされたアプリケーションは、初期状態では [Unclassified] に分類されます。

表示情報を操作するには、以下のようになります。

- 選択した VM で実行されているすべてのアプリケーションを選択するには、[Select All] をクリックします。
- 選択されているすべてのアプリケーションをクリアするには、[None] をクリックします。
- アプリケーションを名前またはベンダーによって並べ替えるには、表の列見出しをクリックします。

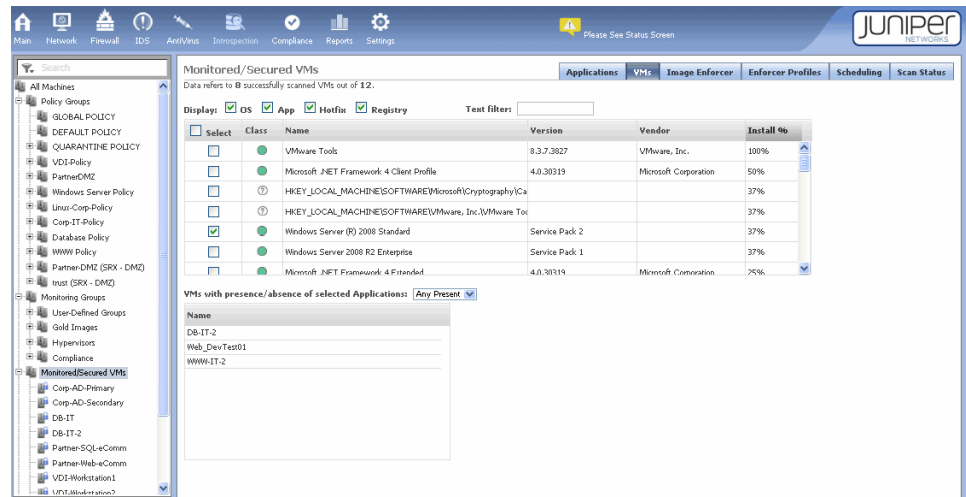
選択を変更すると、アプリケーションの棒グラフが自動的に更新されます。

関連項目

## vGW シリーズ イントロスペクションの [VMs] タブの理解

vGW セキュリティ デザイン VM のイントロスペクション モジュールの [VMs] タブを使用すると、選択した VM または VM のグループにインストールされているソフトウェアを監視できます。 VM で実行されているオペレーティング システムやアプリケーションに関する情報（インストールされているサービス パックやホットフィックスの詳細など）を表示または非表示にすることが可能です。 [VMs] タブは、どの VM に特定のタイプのソフトウェアがインストールされているかを確認する際に役立ちます。 この機能を使用して、1 つ以上の VM でソフトウェアが存在するかどうかを確認できます。

次の図では、VM ツリーで選択した User-Defined Groups 内の VM をスキャンし、Microsoft .NET Framework 4 クライアント プロファイルが含まれているかどうかを確認しています。



この機能はさまざまな用途に使用できます。たとえば、以下のような用途が挙げられます。

- MS Windows Server 2003 オペレーティング システムが実行されているすべての VM、または特定のホットフィックスがインストールされたすべての VM を表示する。
- Kazaa や Skype などの特定のアプリケーションが実行されている VM を確認する。
- 必要なソフトウェアが存在しない VM を確認する。

リスト内の特定の項目を名前またはベンダーによって検索するには、詳細表の [Name] または [Vendor] 列見出しをクリックし、[Text filter] ボックスにソフトウェアの名前またはベンダーを入力します。そうすると、リストが更新されて入力したテキストと一致する項目が表示されます。

また、VM ツリーのグループ設定によって絞り込んだ VM の中で、特定のソフトウェアを含むものを検索することもできます。そのためには、VM ツリーでグループを選択してから、表でソフトウェアのタイプを 1 つ以上選択します。たとえば、[VMs with presence/absence of select Applications] フィルタをクリックし、メニューから [All Present]、[Any Present]、[All Absent]、[Any Absent] のいずれかを選択します。そうすると、指定した条件を満たす VM のリストが下の表に表示されます。

vGW シリーズのイントロスペクション機能は、ファイアウォール設定にかかわらず、インストールされているソフトウェアを検出できます。vGW セキュリティ デザイン VM のインスタンス化には依存しません。

関連項目    • [3 ページの vGW シリーズの理解](#)

## vGW セキュリティ デザイン VM イントロスペクションのイメージ エンフォーサ機能の理解

vGW セキュリティ デザイン VM のイントロスペクション モジュールは、MS Windows および Linux ゲスト仮想マシン (VM) にインストールされているソフトウェアを監視するためのさまざまな情報を提供します。これにより、VM の状態や VM 間のアプリケーションのフロー、お



よびアプリケーションの使用方法について深い理解が得られます。また、VM にインストールされているオペレーティング システムのバージョンやサーバー パッチのバージョンもわかります。この情報は、インストールされているソフトウェアに関するグラフィカルなサマリ比較と詳細な統計情報の表によって表されます。この大量の情報の管理を容易にし、アプリケーションを事前対応的に分類できるようにするため、vGW シリーズにはイメージ エンフォーサというイントロスペクション機能が用意されています。

イメージ エンフォーサ機能の中核を成すのは「ゴールド イメージ」という概念です。ゴールド イメージとは VM を生成する元となるテンプレートのことですが、アクティブなゲスト VM (VM) を指すこともあります。このテンプレートまたは VM は有効かつ望ましい構成を備えています。ゴールド イメージとして認定された VM は、モデル VM 構成のレベルに昇格します。

ゴールド イメージを選択するためのプロファイルを作成するには、[Enforcer Profiles] タブを使用します。このプロファイルでは、ゴールド イメージに対して比較する VM や、比較に条件を付けるパラメータも指定できます。VM のゴールド イメージからの逸脱を許容することも可能です。

テンプレートをゴールド イメージとして使用するときは通常、そのテンプレートから生成した VM を比較対象とします。そうすると、たとえばそれらの VM の構成がどのような点でどの程度変更されているかを確認できます。ただし、比較する VM を任意に指定してもかまいません。

比較の結果に基づいて特定のアクションを実行することもできます。たとえば、不適合の VM を検疫することが可能です。検疫された VM は、[Image Enforcer] 画面とメイン モジュールの [Quarantine] 画面に表示されます。[Quarantine] 画面から検疫された VM を解放し、たとえばその VM を修正して有効な VM に回復したり、その他の種類の修復を実行したりできます。メイン モジュールの [Quarantine] タブの詳細については、[45ページの「vGW シリーズのメイン モジュールの理解」](#)を参照してください。

[Image Enforcer] タブを使用して、比較結果のサマリを表示し、比較した VM が全体的にゴールド イメージとどの程度一致しているかを確認できます。また、特定の VM に固有の棒グラフから、その VM の適合度もわかります。

イメージ エンフォーサ機能には、以下のようにさまざまな用途があります。

- SQL Server のゴールド イメージを作成して、適合していないサーバーをチェックできます。
- デスクトップのゴールド イメージを作成し、それに対してデスクトップ ソフトウェアを比較できます。

別のケースについて考えてみます。たとえば、PCI コンプライアンスについて監査担当者が承認した構成を含むテンプレートをゴールド イメージとし、そのゴールド イメージの名前を「PCI-Win-Template」にしたとします。Win-PCI-Servers および PCI-Desktop VMs グループに属する VM を PCI-Win-Template ゴールド イメージに対して比較するとき、比較条件の一部として、「known」として分類されたアプリケーションを許容することを指定できます。ゴールド イメージ構成にはこれらのアプリケーションは含まれていませんが、比較する VM の構成にこれらの既知のアプリケーションが含まれていても、比較条件に違反することにはなりません。

テンプレートのゴールド イメージにはそれぞれ、コンプライアンス規則が自動的に作成されます。デフォルトでは、ゴールド イメージから生成された VM が検査され、コンプライアンス状態が変わるとアラートが生成されます。

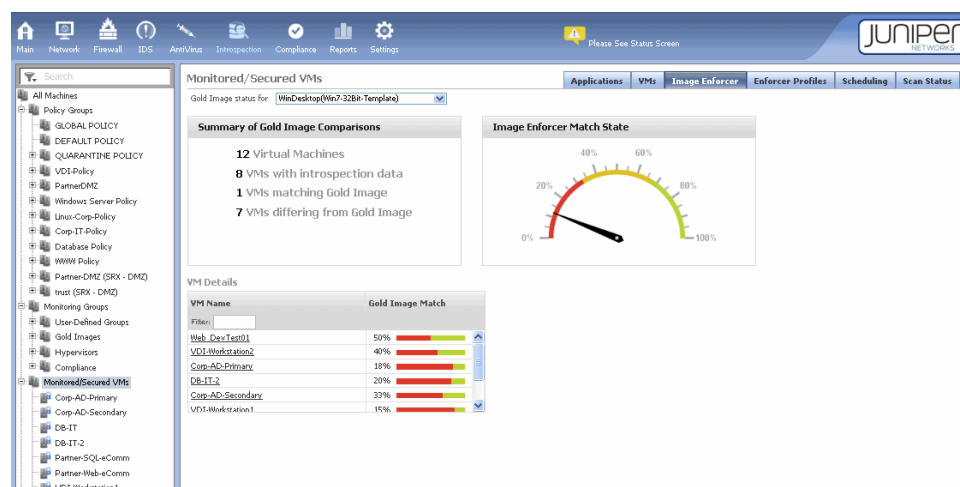
VM のスキャンをいつ実行するかを指定できます。たとえば、特定のイベントが発生したときや、[Scheduling] タブを使用して作成した明確なスケジュールに従って、スキャンを実行できます。また、同時スキャンの数を制限することも可能です。

- 関連項目
- vGW セキュリティ デザイン VM のイントロスペクション モジュールの理解
  - 101ページのvGW シリーズの [Enforcer Profiles] タブの理解

## vGW シリーズの [Image Enforcer] タブの理解

イントロスペクション モジュールの [Image Enforcer] タブでは、「ゴールド イメージ」と呼ぶモデル テンプレートまたはアクティブな仮想マシン (VM) に対するゲスト VM の比較結果が報告されます。[Enforcer Profile] タブで、ゴールド イメージとその比較対象の VM、および比較条件を指定します。

次の図は、VM ツリーで選択した Monitored/Secured VMs グループに属する VM をスキャンして WinDesktop(Win7-32bit-Template) ゴールド イメージと比較した結果を表示する [Image Enforcer] 画面を示します。



[Image Enforcer] タブには以下の比較結果が表示されます。

- 一致を識別します。つまり、VM にインストールされているソフトウェアのうち、ゴールド イメージ構成のソフトウェアと一致するものが識別されます。
- VM にインストールされているアプリケーションのうち、ゴールド イメージ構成に含まれていないものが識別されます。
- ゴールド イメージ構成に含まれているアプリケーションのうち、VM にインストールされていないものが識別されます。
- ソフトウェアのバージョンがチェックされ、VM のバージョンのうちゴールド イメージのバージョンと一致していないものが識別されます。

- 関連項目
- 98ページのvGW セキュリティ デザイン VM イントロスペクションのイメージ エンフォーサー機能の理解

- 101ページのvGW シリーズの [Enforcer Profiles] タブの理解

## vGW シリーズの [Enforcer Profiles] タブの理解

このトピックでは、vGW シリーズのイントロスペクション モジュールの [Enforcer Profiles] タブについて説明し、このタブを使用してプロファイルを作成する方法を示します。また、プロファイルを作成または変更するために管理者が選択または指定する情報についても説明します。

イメージ エンフォーサを使用すると、有効かつ望ましい構成を備え、ゴールド イメージのステータスに昇格した VM テンプレートまたはアクティブな VM に対して VM を比較できます。比較スキャンの結果に基づいて、ゴールド イメージから逸脱した VM を検疫する、アプリケーションを VM に追加または VM から削除して VM を適合させる、といったアクションを実行できます。

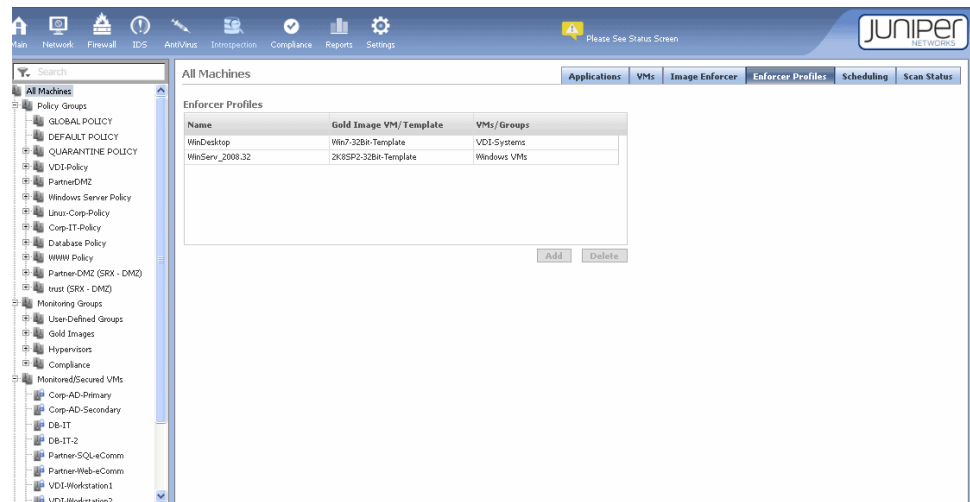
このトピックを読む前に、98ページの「vGW セキュリティ デザイン VM イントロスペクションのイメージ エンフォーサ機能の理解」をお読みください。

このトピックには以下のセクションがあります。

- [Enforcer Profiles] ペインについて 101ページ
- [Add Enforcer Profile] ペイン 102ページ

### [Enforcer Profiles] ペインについて

イントロスペクション モジュールの [Enforcer Profiles] タブを選択すると、[Enforcer Profiles] ペインが表示されます。このペインに表示される情報は、すでに構成済みのプロファイル（存在する場合）を反映します。



新しいプロファイルを追加して名前を付けると、そのプロファイルがプロファイル リストに表示されます。このリストには、各プロファイルで選択したゴールド イメージとその比較対象の VM が示されます。

## [Add Enforcer Profile] ペイン

新しいプロファイルを追加するには、[Enforcer Profiles] ペインの下にある [Add] をクリックします。[Add Enforcer Profile] ペインが表示されます。このペインを使用してエンフォースャ プロファイルを構成し、比較スキャンのパラメータを指定します。このペインでは、比較に使用するゴールド イメージを選択します。また、比較を定義する一致条件と、スキャンの完了後に実行するアクションも指定できます。VM をある特定の要件から免除する条件や、不適合の VM を検疫するかどうかを指定することが可能です。

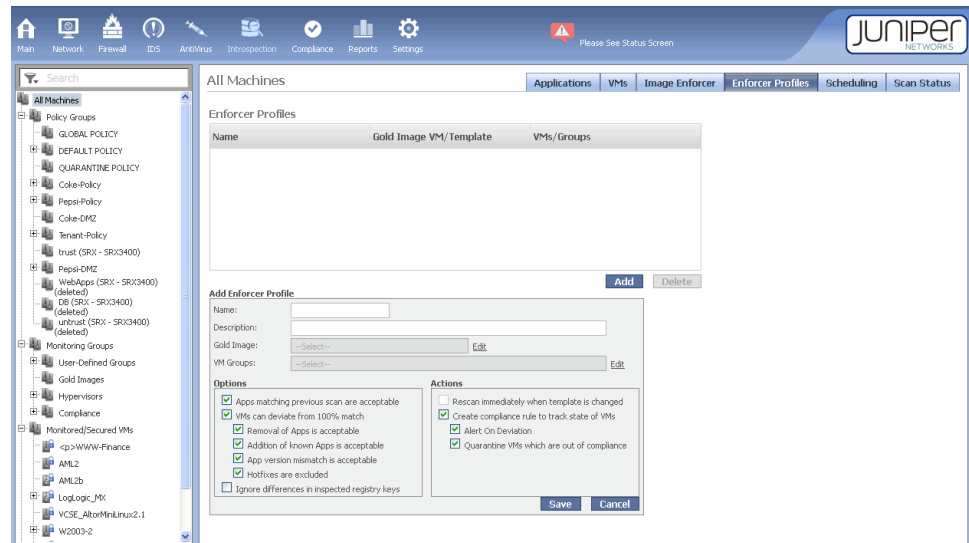


表6: Add Enforcer Profile: ゴールド イメージとその比較対象の VM の選択

フィールド	指定
Name	プロファイルの内容を示す名前。
説明	プロファイルの使用目的の説明。
Gold Image	<p>この比較においてゴールド イメージとして使用する VM テンプレートまたは VM。[Gold Image] 選択リストを使用して、既存のテンプレートまたは VM を選択します。</p> <p>選択リストの下部にあるオプション ボタンを使用して、すべてのゴールド イメージ候補を表示するか、テンプレートまたは VM のみを表示するかを選択できます。</p> <p><b>注:</b> テンプレートまたは VM をゴールド イメージのステータスに昇格させると、そのテンプレートまたは VM は VM ツリーの [Monitoring Group] セクションにある Gold Images グループに移動します。</p>
VM Groups	<p>選択したゴールド イメージに対してその構成を比較する VM グループまたは VM。</p> <p>矢印ボタンを使用して、VM グループまたは VM をプロファイルに追加またはプロファイルから削除できます。</p>

表7: エンフォーサ プロファイル編集オプション

オプション	このチェックボックスをオンにした場合の意味
Apps matching previous scan are acceptable	このプロファイルのゴールド イメージに対する以前のスキャンで一致していた VM が現在は一貫しない場合、その VM は許容されます。  この場合は、ゴールド イメージが更新されて再スキャンされている可能性があります。Enforcer Profile グループで指定された VM の更新には時間がかかるため、これらの VM は移行中で一致しているものとして許容されます。
VMs can deviate from 100% match	このプロファイルのゴールド イメージに対して比較された VM が、 <a href="#">103ページの表8</a> に示すオプションによって指定された点でゴールド イメージから逸脱していた場合、その VM は許容されます。
Ignore differences in inspected registry keys	レジストリ キーのアプリケーション設定がゴールド イメージと異なっても許容します。

表8: 許容されるゴールド イメージからの逸脱

オプション	このチェックボックスをオンにした場合の意味
Removal of apps is acceptable	ゴールド イメージに存在しないアプリケーションが VM から削除されている場合、それを許容します。
Additions of known apps is acceptable	あるアプリケーションがゴールド イメージの一部である場合、そのアプリケーションは「known」として分類されます。
App version mismatch is acceptable	VM に含まれるアプリケーションのバージョンがゴールド イメージに存在するバージョンよりも古いか新しい場合、それを許容します。
Hot fixes are excluded	ホットフィックスが比較から除外され、VM で許容されます。

[103ページの表9](#) に、比較スキャンの後に実行できるアクションを示します。

表9: アクション

オプション ボタン	このチェックボックスをオンにした場合の意味
Rescan immediately when template is changed	ゴールド イメージとして使用しているテンプレートを VM に変換し、修正してから再びテンプレートに変換した結果、テンプレートが変更された場合、常にそのゴールド イメージに対して VM の比較を自動的に実行します。
Create compliance rule to track state of VMs	ゴールド イメージ構成から生成されたコンプライアンス規則を自動的に定義し、 <a href="#">103ページの表10</a> に示す管理者が選択したアクションを実行します。

表10: コンプライアンス規則の指定

Alert On Deviation	VM がゴールド イメージから逸脱したときに通知します。
--------------------	------------------------------

表10: コンプライアンス規則の指定 (続き)

Quarantine VMs which are out of compliance	VM の構成がゴールド イメージの構成と一致していない場合、その VM を検疫します。一致を判定する際、103ページの表8に示す管理者が指定した許容条件が考慮されます。
--	--

関連項目    • 3ページのvGW シリーズの理解

## vGW シリーズ イントロスペクションのスケジュール機能の理解

vGW セキュリティ デザイン VM のイントロスペクション モジュールの [Scheduling] タブでは、VM をスキャンするスケジュールを定義できます。

ピーク期間のパフォーマンスを向上させるため、同時スキャン メニューで最大数を選択して同時スキャン数を制限できます。同時に実行するスキャンの数は 2 つまでにすることを推奨します。スキャンのスケジュールを定義するには、[Add] をクリックし、このスキャンのオプションを選択して、[Save] をクリックします。104ページの表11を参照してください。

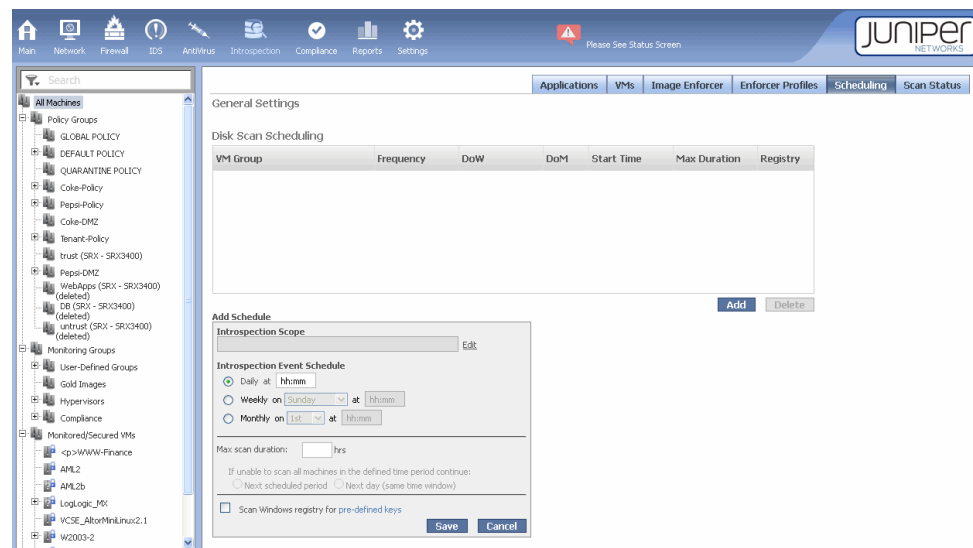


表11: エンフォース イメージ スキャンの定義

オプション	選択または入力
Introspection Scope	[All Machines] または [Selected Group] を選択してから、リストからグループを選択します。
Introspection Event Schedule	[Daily] を選択し、スキャンを開始する時刻を入力します。  [Weekly] を選択し、曜日を選択して、スキャンを開始する時刻を入力します。  [Monthly] を選択し、月の日にちを選択して、スキャンを開始する時刻を入力します。
Max scan duration	スキャンの最長の継続時間。[max scan duration] オプションを使用することで、スキャンが保守時間帯を超えないようにすることができます。そのとき実行中のスキャンは完了しますが、リスト内の後続のスキャンは開始されません。保留中のスキャンは [Scan Status] タブに一覧表示されます。これらは次のスケジュール時刻になると再開されます。

表11: エンフォーサ イメージ スキャンの定義 (続き)

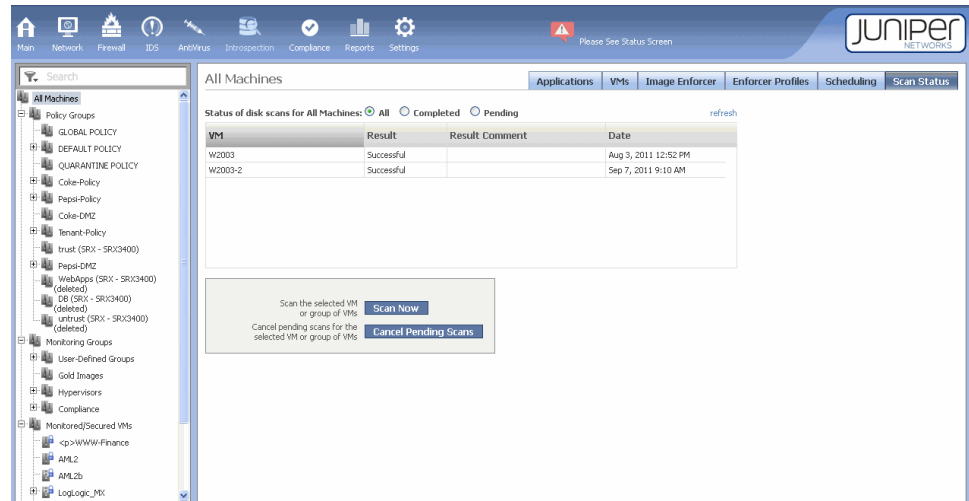
オプション	選択または入力
If unable to scan...	<p>次回のスケジュールされた間隔でスキャンを続行する場合は、[Next scheduled period] を選択します。</p> <p>翌日の同じ時刻にスキャンを続行する場合は、[Next Day] を選択します。</p>

スケジュールを削除するには、リストでスケジュールを選択して [Delete] をクリックします。

関連項目

## vGW シリーズ イントロスペクションのスキャン ステータスの理解

vGW セキュリティ デザイン VM のイントロスペクション モジュールの [Scan Status] タブでは、1 つ以上の VM のディスク スキャンを監視できます。vGW シリーズはゲスト VM のディスクの完全な分析を実行します。VM システムに複数のディスクが存在する場合は、それぞれのディスクが分析されます。この分析により、インストールされているアプリケーション、オペレーティング システム、および VM で実行されているサービス パック/パッチ レベルが検出されます。



vGW シリーズで採用されているスキャン技術は単なるネットワーク プローブではなく、非常に正確です。ハイパーバイザからディスク ファイルの実際の読み取りが行われます。また、スキャン速度も非常に高速です。標準的な VM のスキャンには 5 分かかりません。スキャンはシステムのスナップショットに対して実行されるため、VM の運用状態には影響しません。スキャンが完了すると、スナップショットは削除されます。

すべてのスキャン（完了したスキャンと保留中のスキャン）、完了したスキャン、または保留中のスキャンに関する現在の情報を表示できます。また、スキャンを手動で実行したり、進行中のスキャンをキャンセルすることもできます。

すべてのスキャン、完了したスキャン、または保留中のスキャンのリストを表示するには、表の上のオプション ボタンを選択します。VM ツリーで選択した VM または VM のグループに対

してスキャンを実行するには、[Scan Now] をクリックします。 進行中のスキャンをキャンセルするには、[Cancel Pending Scans] をクリックします。

関連項目   • [3ページのvGW シリーズの理解](#)

---

## vGW シリーズ イントロスペクションのレジストリ チェック機能の理解

vGW セキュリティ デザイン VM のイントロスペクション モジュールを使用して Microsoft Windows VM 内のレジストリを検査し、ユーザー定義のレジストリ キーとその値を検出することもできます。

このレジストリ検査機能は以下のために使用します。

- アプリケーション構成の属性を確認する。たとえば、ディスク暗号化アプリケーションによって重要なディレクトリが保護対象として構成されているかどうかを確認できます。
- 構成のバージョン（たとえば、ゲスト VM 内の DLP アプリケーションのシグネチャ バージョンなど）を確認する。
- レジストリ キーを内部タグとして使用して MS Windows ビルドを特定する、またはレジストリ キーをセキュリティ ポリシー自動化の識別子として使用する。

レジストリ検査の設定は、設定モジュールの [Registry Values] セクションで構成します。各構成要素は、regedit で表示されるレジストリ値に対応します。構成値は以下のとおりです。

- Name – vGW 管理内でレジストリ値を識別する名前。
- Key – レジストリ キーのパス。たとえば、HKEY\_LOCAL\_MACHINE¥SOFTWARE¥VMware, Inc.¥VMware Tools など。レジストリ キーの名前を確認するには、次の図に示すように、MS Windows の regedit を使用します。
- Data – データ フィールドには、選択したレジストリ名に関連付けられた内容を指定します。

関連項目   • [3ページのvGW シリーズの理解](#)



# vGW シリーズのコンプライアンス モジュール

この章では、vGW セキュリティ デザイン VM のコンプライアンス モジュールについて説明します。

- [vGW シリーズのコンプライアンス モジュールの理解 107ページ](#)
- [コンプライアンス規則の構成 109ページ](#)
- [vGW シリーズのハイパーバイザおよび拡張 VM セキュリティの理解 112ページ](#)

## vGW シリーズのコンプライアンス モジュールの理解

---

このトピックでは、vGW セキュリティ デザイン VM のコンプライアンス モジュールについて説明します。このモジュールを使用すると、業界標準のベスト プラクティスに関するシステム全体のコンプライアンス状態を監視できます。また、自組織のベスト プラクティスを反映する規則を定義することもできます。つまり、単に業界のベスト プラクティスや標準ガイドライン（PCI や HIPAA など）を使用するだけでなく、ユーザー独自のコンプライアンス要件を定義することが可能です。

このトピックには以下のセクションがあります。

- [コンプライアンス モジュール 107ページ](#)
- [\[Compliance\] タブ 108ページ](#)
- [\[Rules\] タブ 109ページ](#)

## コンプライアンス モジュール

コンプライアンス モジュールは規則エディタを基盤とします。このエディタでは、VMware インフラストラクチャや関連する VM に関する複数の属性を使用して、作成する各規則の条件を設定できます。

コンプライアンス規則を使用して主要な構成パラメータを監視することにより、仮想セキュリティ システムの全体的な状態を迅速に把握できます。たとえば、非管理 VM に特定のポートグループへの接続を許可しないというコンプライアンス規則を作成することが可能です。

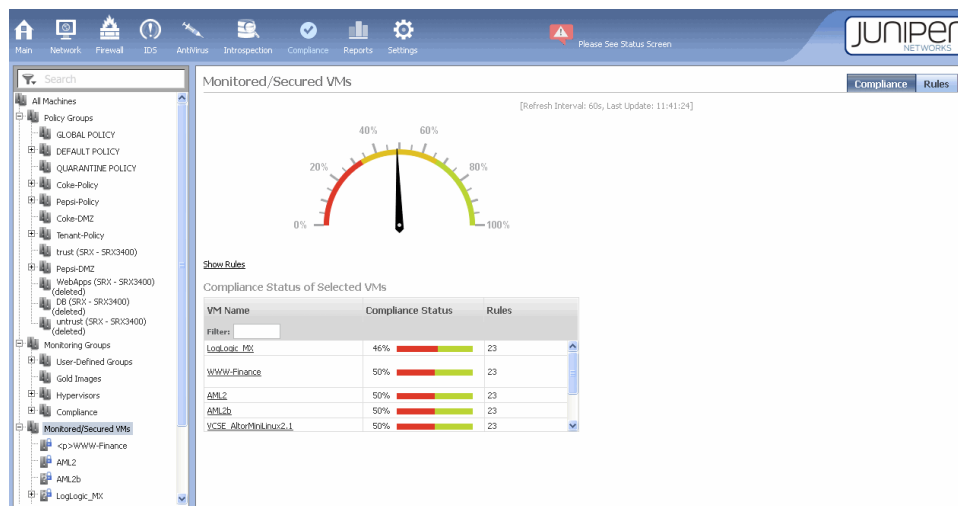
指定した規則の違反は全体的なコンプライアンス状態に影響します。違反に関する詳細をレポートやステータス画面で確認できます。

コンプライアンス モジュールには以下の 2 つのタブがあります。

- Compliance
- Rules

## [Compliance] タブ

[Compliance] タブには、VM ツリーで選択した VM または VM のグループの現在のコンプライアンス レベルを示すコンプライアンス メーターと、 全体的なコンプライアンス レベルの計算に使用された統計データが表示されます。



現在のコンプライアンス レベルを反映するため、コンプライアンス メーターは 60 秒ごとに自動的に更新されます。

VM ツリーで VM グループを選択した場合、コンプライアンス メーターには、グループ内のすべての VM の全体的なコンプライアンス パーセントが表示されます。メーターの下には、各 VM の名前とその個々のコンプライアンス レベルが表示されます。

グループに関連付けられたコンプライアンス規則を表示するには、[Show Rules] をクリックします。そうすると、各規則の一覧を示す表が表示されます。この表には、名前、ウェイト、規則が適用される VM の数、規則のコンプライアンス ステータスが含まれます。

- 規則を無効にするには、そのチェックボックスをオフにします。

コンプライアンス メーターが更新され、調整した規則セットに基づく現在のコンプライアンス レベルが表示されます。

- 表の規則をダブルクリックすると、その規則に関する詳細が表示されます。

VM ツリーで単一の VM を選択した場合は、その VM の現在のコンプライアンス レベルを示すコンプライアンス メーターと、その VM を保護している規則が表示されます。

## [Rules] タブ

[Rules] タブでは、コンプライアンス規則を作成して管理できます。このタブには、規則の名前、そのウェイト、およびその規則に関連付けられたラベルを含む定義済み規則のリストがあります。各規則はラベルによって分類されます。

				Compliance	Rules
Rule Name	Weight	Labels	Quarantine		
Filters: <input type="text"/>		Filter by: VMware-VM			
Backdoor Communications	1	VMware-VM	off		
Clipboard enabled	1	VMware-VM	off		
Disk shrink on	1	VMware-VM	off		
Editable devices	1	VMware-VM	off		
Forged MAC Addresses	1	DISA,NSA,VMware-VM	off		
Guest MAC Address Change	1	DISA,NSA,VMware-VM	off		
				Add Rule from Pre-defined List   Add   Disable   Delete	

表示される規則のリストを絞り込むには、[Filter by] メニューを使用します。



**注:** vGW シリーズには、仮想インフラストラクチャを VMware のセキュリティおよび要塞化ガイドラインに対して評価するコンプライアンス規則とテンプレートが組み込まれています。これらの規則は、コンプライアンス モジュールの機能を学習するための良い例でもあります。

関連項目   •

## コンプライアンス規則の構成

このトピックでは、コンプライアンス規則の作成方法について説明します。コンプライアンスモジュールの概要については、を参照してください。

コンプライアンス モジュールの [Rules] タブからコンプライアンス規則を作成するには、以下の手順に従います。

1. [Add] をクリックします。[Add Rule] ダイアログ ボックスが表示されます。

**Add Rule**

Name:

Comment:

Remediation:

Compliance Scope:  [Edit](#)

Weight:

☐ Generate Alert when compliance state changes

☐ Quarantine non-compliant VMs

Compliance Groupings:  [Edit](#)

Create Groups For:

☐ Compliant VMs

☐ Non-Compliant VMs

**Advanced**

Matches: ☒ All ☐ Any

[?](#) [-](#) [+](#)

[Test](#) [Save](#) [Cancel](#)

2. 規則を定義します。110ページの表12 に、使用可能なオプションの説明を示します。

表12: コンプライアンス規則の作成パラメータ

オプション	アクション
Compliance Scope	[All Machines] または [Selected Group] を選択してから、リストからグループを選択します。
Name	規則の名前を入力します。文字と数字を使用した、わかりやすくシンプルな名前を付けます。必要に応じて、[Comment] フィールドに規則の詳細を入力します。
Weight	コンプライアンス レベルの計算時に使用するウェイトを入力します。
Generate Alert when compliance state changes	コンプライアンス レベルが変わったときに警告を書き込むよう指定します。
Compliance Groupings	[Edit] をクリックして 1 つ以上のラベルを [Selected Labels] リストに移動し、[Apply] をクリックします。

表12: コンプライアンス規則の作成パラメータ (続き)

オプション	アクション
Create Groups	<p>指定した一致条件 ([Matches] フィールドで定義) を満たすメンバー、またはその条件に違反するメンバーで構成されたグループを作成します。</p> <p>グループを作成することは必須ではありませんが、どちらか一方のオプションを選択した場合、非ポリシーのスマート グループがデフォルトで作成されます。このグループをポリシー グループに変更するには、[Settings] -&gt; [Security Settings] -&gt; [Groups] を使用します。コンプライアンスに基づくグループを自動的に作成する利点は、この条件を使用して VM ツリーで簡単に VM を見つけられることと、vGW シリーズ全体でこのグループを使用できることです。110ページの表12を参照してください。</p>
Matches	<p>VM が下のフィールドで定義したすべての条件を満たす必要がある場合は [All] を選択し、下のフィールドで定義した条件のいずれかを満たしていればよい場合は [Any] を選択します。次に属性と演算子を選択し、値を入力します (たとえば、vi.datacenter Equals HQ)。この規則に別の条件を追加する場合は [+] をクリックし、この規則から条件を除外する場合は [-] をクリックします。</p>
Advanced	<p>定義ではなく選択クエリを入力します。クエリの構文の詳細については、172ページの「vGW シリーズのスマート グループの理解と使用」を参照してください。</p>

## 3. [Test] をクリックします。

入力した条件がチェックされ、指定した条件を適用した場合にグループに含まれる VM (存在する場合) を示すメッセージが [Edit Rule] ダイアログ ボックスに表示されます。

The screenshot shows the 'Add Rule' dialog box with the following details:

- Name:** uTorrent
- Comment:** Compliance policy for bit-torrent application
- Remediation:** (Empty text area)
- Compliance Scope:** All Machines
- Weight:** 3
- Generate Alert when compliance state changes:** ☒
- Quarantine non-compliant VMs:** ☐
- Compliance Groupings:** (Empty list)
- Create Groups For:**
  - ☐ Compliant VMs
  - ☐ Non-Compliant VMs
- Advanced** tab is selected.
  - Matches:** ☒ All ☐ Any
  - Condition:** vf.application **Operator:** Equals **Value:** uTorrent, 3.0.0

The 'Compliance Test' window shows the following results:

- Compliance Test Results:** 0 Compliant VMs, 42 Non-Compliant VM
- Compliant VMs:** (Empty list)
- Non-Compliant VMs:**
  - 10.159.24.15
  - 10.159.24.152
  - 10.159.24.183
  - 10.159.24.21
  - 10.159.24.45

## 4. [Save] をクリックします。



注：表 10 に説明した項目に加えて、コンプライアンス チェック時に VM をネットワークから切り離すオプションもあります。デフォルトでは、このオプションは表示されないようになっています。その理由は、これを誤って使用した場合、意図しない深刻なネットワーク ダウンタイムが発生する可能性があるためです。たとえば、このアクションを指定したコンプライアンス規則を誤って作成した場合、vCenter を含むすべての VM がオフラインになるおそれがあります。このコンプライアンス アクションを有効にするには、vGW セキュリティ デザイン VM の Web インターフェースから次を実行します。これを実行すると、“[Disconnect from the network when non compliant]” という選択ボックスが表示されます。

`http:///compDisconnect?disconnect=true`（または `false`）

事前定義された規則を選択することもできます。規則を簡単に検索するには、フィルタを指定します。

Compliance Rules			
Rule Name	Weight	Labels	Quarantine
Filters		Filter by: VMware-VM	
Backdoor Communications	1	VMware-VM	off
Clipboard enabled	1	VMware-VM	off
Disk shrink on	1	VMware-VM	off
Editable devices	1	VMware-VM	off
Forged MAC Addresses	1	DISA,NSA,VMware-VM	off
Guest MAC Address Change	1	DISA,NSA,VMware-VM	off

Add Rule from Pre-defined List

Add

Disable

Delete

## vGW シリーズのハイパーバイザおよび拡張 VM セキュリティの理解

このトピックでは、VMware 要塞化ガイドラインと一致する vGW シリーズのハイパーバイザおよび VM に関するセキュリティについて説明します。



注：このトピックの内容を活用するには、VMware 要塞化ガイドラインを全般的に理解する必要があります。

- ハイパーバイザのセキュリティの必要性 112ページ
- vGW シリーズのハイパーバイザおよび VM セキュリティと VMware 要塞化ガイドライン 113ページ
- vGW シリーズのハイパーバイザおよび VM セキュリティの概要 113ページ
- 修復 114ページ
- 構成例 114ページ

### ハイパーバイザのセキュリティの必要性

ハイパーバイザでは、仮想化インフラストラクチャによって、マルウェアの攻撃を受ける可能性のある新しい抽象層が導入されます。ハイパーバイザを攻撃対象として開拓しようとする試

みが近年増加しており、今後もそのような試みの頻度や種類は増加し続けるものと予想されます。ハイパーバイザへの攻撃は、機密データの漏洩やサービス拒否 (DoS) などの深刻な混乱を引き起こすおそれがあります。ハイパーバイザが危険にさらされると、多数の異なるテナントに属するゲスト仮想マシン (VM) も危険にさらされます。ハイパーバイザは仮想化環境における極めて重要なリソースなので、その保護は包括的なセキュリティにとって不可欠です。

vGW シリーズでは、セキュリティ保護するハイパーバイザ ホストが安全な環境に必要とされるセキュリティおよびコンプライアンス標準を満たしているかどうかを検証できます。組み込みのハイパーバイザ コンプライアンス チェックは、VMware 要塞化ガイドラインに基づきます。また、独自に追加のハイパーバイザ コンプライアンス チェックを作成して、必要なセキュリティ コンプライアンス チェックを自動化できます。

### vGW シリーズのハイパーバイザおよび VM セキュリティと VMware 要塞化ガイドライン

vGW シリーズのハイパーバイザ セキュリティは、可能な限りすべての点で VMware 要塞化ガイドラインと一致しています。ある特定の理由から、一部のガイドラインは実装されていません。たとえば、

- 「NCN12 - document VLANs used on vSwitches」などのガイドラインは、さまざまな方法で実装可能な動作に関係します。実装が多様であることから、vGW シリーズでその違反をチェックできません。
- 「HST02 - Ensure uniqueness of CHAP auth secret」などのガイドラインは、vGW シリーズがアクセスできないコンポーネントに関係します。したがって、vGW はこれらに関するチェックを実行できません。

### vGW シリーズのハイパーバイザおよび VM セキュリティの概要

VMware の推奨と一致する vGW シリーズのコンプライアンス チェックを表示するには、コンプライアンス モジュールの [Rules] タブにあるフィルタ ボックスで [VMware-VM] および [VMware-host] を選択します。<[Filter] ボックスで [VMware-VM] が選択されている [Rules] タブ画面を示す図>を参照してください。

規則を選択すると、その規則と、コンプライアンス違反に応じて実行される修復アクションを説明するペインが表示されます。<[Edit Rule] 画面 ([Compliance] > [Rules]) を示す図>を参照してください。

[Edit Rule] ペインから、規則の定義を以下のように変更できます。以下を変更できます。

- 規則を適用するグループの範囲 ([Compliance Scope] リスト)。構成済みの VM およびグループのリストを表示するには、[Edit] をクリックします。
- 規則のウェイト ([Weight] フィールドで 1 ~ 5 の範囲)。5。
- グループに属するハイパーバイザまたは VM のコンプライアンス状態が変わったときにアラートを生成するかどうか。
- 不適合の VM およびハイパーバイザを検疫するかどうか。
- [Compliant VMs] および [Non-Compliant VMs] に対応するハイパーバイザ グループを自動的に作成するかどうか。

## 修復

各コンプライアンス チェック（規則）に対して具体的な修復方法が提案されます。VMware 要塞化ガイドラインを参照して詳細な情報を得ることもできます。

## 構成例

ハイパーバイザのコンプライアンス要件を構成し、それらに関する情報を表示するには、VM ツリーとコンプライアンス モジュールを組み合わせて使用します。

1. VM ツリーの [Monitoring Groups] で、[Hypervisors] グループを選択して [Hypervisor] 画面を表示します。

[Hypervisors] 画面には以下の情報が表示されます。

- 運用中の仮想化環境にある ESX/ESXi ホストの全体的なコンプライアンス ステータス。
- [Compliance Status of Selected VMs] 表に、Hypervisors 監視グループに属する個々のハイパーバイザの IP アドレス、コンプライアンス ステータス、およびそのハイパーバイザに対して構成されたコンプライアンス規則の数が表示されます。

2. グループ内のハイパーバイザに対して構成された規則に関する情報を表示するには、[Show Rules] をクリックします。

[Hypervisors] 画面が展開して以下の情報が表示されます。

- [Compliance Rules for Selected VMs] 表。この表には、ハイパーバイザに対して構成された一連の規則がすべて表示されます。各規則について以下の情報が表示されます。
  - 規則名。
  - 規則に設定されたウェイト。
  - 規則が適用される VM（この場合はハイパーバイザ）。
  - 規則に対して検疫が有効になっているかどうかを示す検疫状態。
  - 規則が適用されているハイパーバイザの全体的なコンプライアンス ステータス。
- [Compliance Status of Selected VMs] 表には以下の情報が表示されます。
  - ハイパーバイザの IP アドレス。
  - ハイパーバイザに適用されているすべての規則に関する、ハイパーバイザのコンプライアンス ステータス。
  - ハイパーバイザに適用されている規則の数。

3. 規則の構成を表示するには、[Compliance Rules for Selected VMs] 表で規則名をクリックします。

[Edit Rule] ペインが表示されます。このペインには以下の情報が表示されます。

- 規則名の下に [Comment] フィールドに、規則の簡単な説明が表示されます。
- [Remediation] フィールドに、ハイパーバイザをこの規則に準拠させるための修復アクションの案が提示されます。



[Edit Rule] ペインから、規則の定義を以下のように変更できます。 以下を変更できます。

- 規則を適用するグループの範囲 ([Compliance Scope] リスト)。 リストを表示するには [Edit] をクリックします。
  - 規則のウェイト ([Weight] フィールドで 1 ~ 5 の範囲)。 5.
  - グループに属するハイパーバイザのコンプライアンス状態が変わったときにアラートを生成するかどうか。
  - 不適合のハイパーバイザを検疫するかどうか。
  - [Compliant VMs] および [Non-Compliant VMs] に対応するハイパーバイザ グループを自動的に作成するかどうか。
4. 規則の構文をカスタマイズするには、その規則の [Edit Rule] ペインから [Advanced] をクリックします。 スマート グループ定義の構成の詳細については、「vGW シリーズのスマート グループの理解」を参照してください。
  5. 規則を構成した後で [Test] をクリックし、選択した範囲に含まれるハイパーバイザに対して規則をテストします。
  6. 規則の定義に間違いがない場合は、[Save] をクリックします。

関連項目    • [3ページのvGW シリーズの理解](#)



## vGW シリーズ VM のレポート モジュール

この章には以下のトピックがあります。

- vGW シリーズのレポート モジュールの理解 117ページ
- vGW シリーズのレポート モジュールを使用した自動レポートの仕様の構成 118ページ
- vGW シリーズのカスタム レポート タイプの理解 120ページ
- vGW シリーズのネットワーク レポートの理解 120ページ
- vGW シリーズのファイアウォール レポートについて 121ページ
- vGW シリーズの IDS レポートについて 121ページ
- vGW シリーズのイントロスペクション レポートについて 121ページ
- vGW シリーズのコンプライアンス レポートの理解 122ページ
- vGW アンチウィルス レポートの理解 122ページ

### vGW シリーズのレポート モジュールの理解

vGW セキュリティ デザイン VM のレポート モジュールでは、自動レポートを作成および変更し、レポートが生成されたときの結果を表示できます。

レポート モジュールには以下のタブがあります。

- Add/Edit Reports

このタブを使用してレポートを作成します。 デフォルトでは、[Add/Edit Reports] タブ画面の表は空です。 レポートを作成すると、作成したレポートがこの表に表示されます。

- Recent Reports

[Recent Reports] タブには、作成済みのレポートを含む表が表示されます。 レポートを開くには、リストで目的のレポートをダブルクリックします。 PDF ファイルとして開くか、ハード ドライブに保存できます。



注: レポートを PDF ファイルとして表示するには、PDF ビューアをシステムにインストールする必要があります。

各レポートには、レポート名とレポートの作成日を含む高レベルのヘッダが付いています。

レポートの仕様を作成するとき、以下のタイプのレポートを [Report Selection] セクションで選択して作成できます。

- エグゼクティブ サマリ

エグゼクティブ サマリ レポートは、すべての vGW セキュリティ デザイン VM モジュールにわたるセキュリティおよびパフォーマンス レポートに対する広範な視点を提供します。

- ファイアウォール

ファイアウォール レポートには、vGW シリーズ ファイアウォールによって処理された上位の許可接続と拒否接続が含まれます。

- ネットワーク アクティビティ

ネットワーク アクティビティ レポートは、最もアクティブな VM や仮想ネットワークで最もよく観察されるプロトコルなど、ネットワーク使用状況の概要を示します。

- セキュリティ

セキュリティ レポート

- イントロスペクション

イントロスペクション レポートは、選択した VM にインストールされているアプリケーションの詳細や、使用されているオペレーティング システムの明細を示します。また、VM がゴールド イメージ（有効かつ望ましいテンプレートまたは VM）と比較されたときに生成されるイメージ エンフォーサ レポートも提供します。

- コンプライアンス

コンプライアンス レポートは、すべてのコンプライアンス ラベル分類の詳細なステータス状況を示します。

- アンチウィルス

アンチウィルス レポート

これらのレポート タイプに加えて、カスタム レポートも作成できます。

関連項目   • [3ページのvGW シリーズの理解](#)

## vGW シリーズのレポート モジュールを使用した自動レポートの仕様の構成

このトピックでは、レポートで生成する情報の種類やレポートをいつ生成するかを決定するパラメータを構成する方法について説明します。このトピックを読む前に、[117ページの「vGW シリーズのレポート モジュールの理解」](#)をお読みください。

レポート データをさらに役立てるため、[Report Selection] セクションを使用して内容のフィルタを指定できます。送信元 IP、宛先 IP、またはプロトコルを使用してレポートをフィルタリングできます。また、高優先度、中優先度、低優先度のアラートを除外することも可能です。フィルタリングを行うと、正確に必要な情報のみが得られます。

レポートの仕様を追加するとき、エグゼクティブ サマリ、ファイアウォール、ネットワーク アクティビティ、セキュリティ、イントロスペクション、コンプライアンス、スマート グループなどの事前定義レポートを選択できます。また、カスタム レポートも作成できます。

レポートを定義するには、以下の手順に従います。

1. [Add] をクリックします。
2. レポートを作成するマシンを選択します。仮想化インフラストラクチャ全体のレポートを作成する場合は [All Machines] を選択します。
3. レポートの名前 (Report1 など) と説明を入力します。



注: レポート名にスペースまたは特殊文字を使用しないでください。

4. レポートの最大エントリ数を指定します。
5. レポートを作成する期間を指定します。
6. レポートの出力形式として PDF または CSV を選択します。



注: レポートを PDF ファイルとして表示するには、PDF ビューアをシステムにインストールする必要があります。

7. レポートを現在のハード ディスクに保存するか、E メールで受信者に送信するかを指定します。



注: レポートを E メールで送信する場合は、レポートの送信先として、単独の E メール アカウント、E メール エイリアス、またはコロンで区切った複数のアカウントを指定できます。また、Eメールの「差出人」フィールドに表示される E メール アドレスを指定することもできます。

8. レポートをいつ生成するかを選択します。レポートをただちに生成するか、特定の日にレポートを実行するようスケジュールできます。

レポートは就業時間外などの利用率が低い時間帯に実行するようスケジュールすることを推奨します。レポートの生成はシステム リソースを著しく消費する場合があります。レポートのスケジュール設定の詳細については、「vGW セキュリティ デザイン VM のレポート モジュールを使用したレポート生成のスケジュール」を参照してください。

9. レポート タイプを選択します。エグゼクティブ サマリ、ファイアウォール、ネットワーク アクティビティ、セキュリティ、イントロスペクション、コンプライアンス、アンチウィルスなど、いくつかの事前定義レポートが用意されています。また、カスタム レポートも作成できます。

レポート作成プロセス中に選択されたレポートには、タイトル、グラフ、および関連する表データが含まれます。複数のタイプのレポートを選択すると、各レポートが同じ PDF 出力ファイルに順番に追加されます。



ヒント: レポート タイプを選択すると、そのレポートの説明が表示されます。

10. [Generate Now] または [Save] をクリックして、レポートを作成します。

関連項目   • [3ページのvGW シリーズの理解](#)

## vGW シリーズのカスタム レポート タイプの理解

このトピックでは、vGW セキュリティ デザイン VM のレポート モジュールを使用して作成できるカスタム レポートの種類について説明します。 カスタム レポートを作成するとき、ネットワーク、ファイアウォール、IDS、イントロスペクション、コンプライアンスの各レポート用の特定のパラメータを選択できます。 また、[Add Report] 画面の [Report Selection] セクションを使用して、事前定義されたレポートを選択することもできます。 これらのレポートタイプの基本的属性は、事前定義レポートで設定されています。 レポート モジュールの概要については、[117ページの「vGW シリーズのレポート モジュールの理解」](#)を参照してください。

以下のトピックで、管理者が定義できるカスタム レポートの種類について説明します。

- [120ページのvGW シリーズのネットワーク レポートの理解](#)
- [121ページのvGW シリーズのファイアウォール レポートについて](#)
- [121ページのvGW シリーズの IDS レポートについて](#)
- [121ページのvGW シリーズのイントロスペクション レポートについて](#)
- [122ページのvGW シリーズのコンプライアンス レポートの理解](#)
- [アンチウィルス レポート](#)

関連項目   • [3ページのvGW シリーズの理解](#)

## vGW シリーズのネットワーク レポートの理解

このトピックでは、vGW セキュリティ デザイン VM のレポート モジュールを使用して定義できるネットワーク レポートの種類について説明します。 このトピックを読む前に、[117ページの「vGW シリーズのレポート モジュールの理解」](#)をお読みください。

- Top Talkers: 最も多くのトラフィック（トラフィック フローの生成元と宛先の合計）を生成しているマシンを示します。
- Top Destinations: システムが最も頻繁に通信している相手を示します。
- Top Protocols: 仮想ネットワークで最もよく使用されているプロトコルを示します。
- Top Sources: どのシステムが最も多くのトラフィックを生成しているかを示します。
- Total Bytes: Top Talkers レポートと似ていますが、使用されているプロトコルも示します。

関連項目   • [3ページのvGW シリーズの理解](#)

## vGW シリーズのファイアウォール レポートについて

ファイアウォール レポートは、ファイアウォール モジュールによって収集された情報に基づいて生成されます。VM のファイアウォール セキュリティ規則を定義できます。リソースへの接続またはリソースからの接続が行われるとき、ファイアウォールはそのアクティビティをログに記録し、レポート モジュールから使用できるようにします。

以下のファイアウォール セキュリティ レポートを作成できます。

- Top Accepted Destinations: 宛先フィールドのどのマシンが最も多くの数の接続（各ファイアウォール ログ イベントの送信元フィールドと宛先フィールドを含む）を受け入れているかを示します。
- Top Accepted Sources: 送信元フィールドのどのマシンが最も多くの数の接続を受け入れているかを示します。
- Top Dropped or Rejected Destinations: 宛先フィールドのどのマシンが最も多くの数の接続をドロップまたは拒否しているかを示します。ファイアウォール規則のアクション規則として指定できるのは、許可、ドロップ、拒否のいずれかです。
- Top Dropped or Rejected Sources: 送信元フィールドのどのマシンが最も多くの数の接続をドロップまたは拒否しているかを示します。

関連項目   • [3ページのvGW シリーズの理解](#)

## vGW シリーズの IDS レポートについて

IDS レポートは、IDS モジュールによって収集された情報に基づいて生成されます。これらのレポートには、仮想ネットワークで見られたすべての悪意あるトラフィックまたは不審なトラフィックを含むリストが表示されます。

- Top Alerts: 仮想ネットワークで見られたアラートを示します。
- Alter Sources: 攻撃の送信元を示します。

このレポートに含まれるシステムの [Maximum] 数は、報告される攻撃の数を決定します。たとえば、値 20 を指定した場合に、指定したレポート期間に 40 回の攻撃が発生したときは、20 回の攻撃のみが報告されます。

関連項目   • [3ページのvGW シリーズの理解](#)

## vGW シリーズのイントロスペクション レポートについて

イントロスペクション レポートは、イントロスペクション モジュールによって収集された情報に基づいて生成されます。これらのレポートには以下の情報が表示されます。

- Known Applications: 管理者がイントロスペクション モジュールで [Known] として定義したアプリケーションを示します。通常、これらは仮想化環境で最適なアプリケーションと見なされ、使用が許可されます。
- Unknown Applications: さらなる調査が必要と管理者が判断したアプリケーションを示します。
- Bad Applications: 仮想化環境で不適であり使用を許可しないと管理者が定義したアプリケーションを示します。
- Unclassified Applications: 管理者がまだ分類していないアプリケーションを示します。デフォルトでは、Unclassified という状態は、vGW シリーズによって認識されないアプリケーションが VM で検出されたことを示します。
- Operating Systems: 運用環境内の VM にインストールされているオペレーティング システムを示します。オペレーティング システム情報は自動的に収集されるため、運用環境内のすべてのオペレーティング システムに対してレポートを実行できます。

関連項目    • [3ページのvGW シリーズの理解](#)

## vGW シリーズのコンプライアンス レポートの理解

コンプライアンス レポートは、コンプライアンス モジュールによって収集された情報に基づいて生成されます。これらのレポートには、以下のコンプライアンス グループからの情報が表示されます。

- DISA: Defense Information Systems Agency のベスト プラクティスに関連する情報を示します。
- NSA: National Security Agency のベスト プラクティスに関連する情報を示します。
- PCI: Payment Card Industry のベスト プラクティスに関連する情報を示します。
- VMware: VMware のセキュリティ ベスト プラクティスに関連する情報を示します。

生成されたレポートには、これらのコンプライアンス グループのいずれか、またはすべてに関連する情報を含む 3 つのサマリ表が表示されます。たとえば、PCI と VMware のみを選択した場合は、これら 2 つのコンプライアンス グループの値を示す 3 つの表が表示されます。最初の表は、選択したグループに存在するすべての規則を示します。2 番目の表は、各グループの規則、VM の数、およびステータスに関するサマリ情報を示します。3 番目の表は、各グループに関連付けられたすべての VM を示します。

関連項目    • [3ページのvGW シリーズの理解](#)

## vGW アンチウイルス レポートの理解

vGW セキュリティ デザイン VM のレポート モジュールを使用して vGW アンチウイルス レポートを定義し、その実行をスケジュールできます。以下の情報をレポートに含めるよう指定できます。

- AntiVirus Alerts



- AntiVirus Quarantine
- AntiVirus Summary

レポート データは脅威タイプ、脅威名、または VM を基準に並べ替えることができます。

アンチウィルスに適用される標準のレポート構成情報の詳細については、[117ページの「vGW シリーズのレポート モジュールの理解」](#)を参照してください。

関連項目   • [3ページのvGW シリーズの理解](#)



## vGW シリーズの設定モジュール

- [vGW シリーズの設定モジュールの理解 125ページ](#)

### vGW シリーズの設定モジュールの理解

vGW セキュリティ デザイン VM の設定モジュールは、vGW シリーズの中核的な操作を制御します。設定モジュールは、幅広い情報を 3 つのサブセクションに分けて扱います。これらのサブセクションから、システムのさまざまな部分に関する情報を構成または表示できます。

設定モジュールの 3 つの主要セクションは以下のとおりです。

- vGW Application Settings
- Security Settings
- Appliance Settings

- 関連項目
- [127ページのvGW シリーズのアプリケーション設定の理解](#)
  - [161ページのvGW シリーズのセキュリティ設定の理解](#)



## vGW シリーズのアプリケーション設定

- vGW シリーズのアプリケーション設定の理解 127ページ
- vGW シリーズの設定モジュールを使用したステータスおよびライセンス情報の表示 128ページ
- vGW シリーズのライセンスの理解 129ページ
- vGW シリーズのライセンスの取得、インストール、および管理 130ページ
- 設定モジュールを使用した vGW シリーズの VMware との統合 131ページ
- スプリットセンター機能の理解 132ページ
- マルチセンター機能の理解 133ページ
- vGW シリーズのマルチセンター機能の構成 134ページ
- vGW シリーズ マルチセンターの同期オブジェクトの理解 135ページ
- マルチセンター機能とスプリットセンター機能を使用したスケーリングの構成 137ページ
- ESX/ESXi ホストへの vGW セキュリティ VM の配備 143ページ
- vGW シリーズのインストール設定の構成 146ページ
- vGW シリーズの vNIC 毎ポリシー機能の理解 147ページ
- vGW シリーズの vNIC 毎ポリシー機能の構成 148ページ
- 同じ VM 上の個々の vNIC に対する vGW ポリシーの構成と表示 150ページ
- vNIC 毎ポリシーとスマート グループの理解 153ページ
- 設定モジュールを使用した vGW シリーズ管理者の定義 155ページ
- vGW シリーズ管理者の認証に関する Active Directory のセットアップ 156ページ
- vGW シリーズ環境で使用する新しいマシンの定義 157ページ
- 高可用性の使用 158ページ
- vGW シリーズの E メールおよびレポート アプリケーション設定の構成 158ページ

### vGW シリーズのアプリケーション設定の理解

---

設定モジュールの [Applications] セクションでは、vGW シリーズ製品のライセンスの付与、vGW セキュリティ デザイン VM のステータスのチェック、VMware へのアクセスの制御、管理者情報の追加と変更を行うことができます。また、マシン、高可用性、E メール、およびレポートの設定を構成することもできます。

以下のトピックで、特定のアプリケーション設定について説明します。

- 128ページのvGW シリーズの設定モジュールを使用したステータスおよびライセンス情報の表示
- 129ページのvGW シリーズのライセンスの理解
- 130ページのvGW シリーズのライセンスの取得、インストール、および管理
- 131ページの設定モジュールを使用した vGW シリーズの VMware との統合
- 132ページのスプリットセンター機能の理解
- 133ページの「「マルチセンター機能の理解」」および134ページの「vGW シリーズのマルチセンター機能の構成」
- 137ページのマルチセンター機能とスプリットセンター機能を使用したスケーリングの構成
- 143ページのESX/ESXi ホストへの vGW セキュリティ VM のインストールとアンインストール
- 146ページのvGW シリーズのインストール設定の構成
- 148ページのvGW シリーズの vNIC 毎ポリシー機能の構成
- 155ページの設定モジュールを使用した vGW シリーズ管理者の定義
- 156ページのvGW シリーズ管理者の認証に関する Active Directory のセットアップ
- 133ページのマルチセンター機能の理解
- 134ページのvGW シリーズのマルチセンター機能の構成
- 137ページのマルチセンター機能とスプリットセンター機能を使用したスケーリングの構成
- 158ページのvGW シリーズの E メールおよびレポート アプリケーション設定の構成

- 関連項目
- 3ページのvGW シリーズの理解
  - 36ページのvGW セキュリティ VM の理解
  - 35ページのvGW シリーズの vGW セキュリティ デザイン VM の理解

## vGW シリーズの設定モジュールを使用したステータスおよびライセンス情報の表示

設定モジュールの [Applications] セクションでは、基本的なシステム ステータスを表示し、ライセンス情報を表示および構成できます。 このセクションには以下の部分があります。

- Database Status - ネットワーク セッション データを保存する内部データベースのステータスが表示されます。 データベース ディスクがいっぱいになると、最も古いセッションのセッション データが削除されます。 このセクションから、どれくらい過去のセッション データをデータベースに保存できるかがわかります。

デフォルトでは、vGW シリーズ データベースを含むディスクは 8 GB に設定されます。 データベースが小さくて運用環境の情報を十分に保存できない場合は、サイズを増やすことができます。

データベースのサイズを増やすには、以下の手順に従います。

1. vGW セキュリティ デザイン VM の電源をオフにします。

2. VMware で vGW セキュリティ デザイン VM の設定を編集し、2 番目のディスクのサイズを増やします。

3. vGW セキュリティ デザイン VM を起動します。

vGW セキュリティ デザイン VM が起動すると、新しいディスク サイズが認識され、データベースが新しく定義した容量に拡張します。

- Product Licensing – このエリアには、Juniper Networks vGW シリーズの有効なライセンスをまとめた表が表示されます。このライセンス体系は「マルチキー」です。つまり、各種機能のライセンスと機能の数をシステムに付与できます。

少なくとも、vGW セキュリティ デザイン VM 管理センターの有効なライセンスが必要です。

ライセンスの詳細とその指定方法については、以下を参照してください。

- [129ページのvGW シリーズのライセンスの理解](#)
- [130ページのvGW シリーズのライセンスの取得、インストール、および管理](#)

- Appliance Status – このエリアには、vGW セキュリティ デザイン VM のバージョンと最後の更新情報が表示されます。更新を開始する方法の詳細については、76 ページの「システムの更新」を参照してください。

関連項目 • [3ページのvGW シリーズの理解](#)

## vGW シリーズのライセンスの理解

このトピックには以下のセクションがあります。

- [ライセンス要件 129ページ](#)
- [vGW シリーズのライセンス 129ページ](#)
- [評価ライセンス 130ページ](#)

### ライセンス要件

vGW シリーズを使用可能にするには、以下のことを行う必要があります。

- vGW セキュリティ デザイン VM のライセンスと、必要に応じて各種機能の個別ライセンスを購入する。
- ライセンスの資格付与ライセンス キーを取得する。
- vGW シリーズ コンポーネントと機能のライセンス キーを必要に応じてインストールし、それらのキーを管理する。

資格付与ライセンス キーの存在によって、機能を使用できるかどうかが決まります。vGW シリーズ機能のソフトウェア ライセンスの購入方法の詳細については、Juniper Networks の営業担当者にお問い合わせください。

### vGW シリーズのライセンス

以下の vGW シリーズ コンポーネントのライセンスをご購入いただけます。

- vGW セキュリティ デザイン VM – vGW セキュリティ デザイン VM のライセンスを購入する必要があります。このコンポーネントは vGW シリーズの管理センターとして機能します。
- 各 ESX/ESXi ホストは物理的な CPU ソケット数を持ちます。保護するホストごとに、その CPU ソケットの数に対応するライセンスを別途購入する必要があります。この要件は以下のコンポーネントと機能に適用されます。
  - vGW セキュリティ VM – vGW セキュリティ VM は、自身が実行されている ESX/ESXi ホストを保護および監視し、vGW セキュリティ デザイン VM に情報を報告します。
  - 高可用性 (HA) – プライマリおよびセカンダリの vGW セキュリティ VM と vGW セキュリティ デザイン VM を配備することで、単一コンポーネント障害が発生したときのソリューション回復力を維持します。
- アンチウィルス -- マルウェアの検出と感染した VM の特定、および管理者による修復方法の定義によって、VM を保護します。vGW アンチウィルス機能は、これらの処理がパフォーマンスやリソースに与える影響を最小限に抑えるため、vGW セキュリティ VM にスキャンを一元化し、必要な場合に各 VM で EndPoint と呼ばれる微小のエージェントを使用します。
- 侵入検知システム (IDS) – 仮想ネットワーク トラフィックを調べて悪意のあるコンテンツやアクティビティ (Web 攻撃や分散サービス拒否 (DDOS) 攻撃など) を検出します。

購入できるライセンスの数は 2 つから始まり、ライセンス パッケージに従って増加します。セキュリティ VM、HA、IDS、およびアンチウィルスのライセンスは、2 個、10 個、20 個、およびそれ以上のパッケージで販売されています。また、各機能の CPU ソケット数が無制限のライセンスも用意されています。

IDS とアンチウィルスを除くすべての機能では、ライセンスは永続的です。IDS とアンチウィルスのライセンスは申し込みに基づきます。1 年間と 3 年間のライセンスがあります。

ライセンス管理システム (LMS) における vGW シリーズの特権が得られたら、ライセンスを生成できます。vGW シリーズのライセンス キーは無作為な長いテキスト文字列で、等号 (=) で終わります。

## 評価ライセンス

評価ライセンスを使用して vGW シリーズ製品の機能を試すことができます。評価製品はフル機能を備えており、30 日間のライセンスが埋め込まれています。評価ライセンスで vGW シリーズのすべての機能を使用できます。もっと長期のライセンスが必要な場合は、営業担当者にお問い合わせください。

- 関連項目
- [3ページのvGW シリーズの理解](#)
  - [11ページのvGW シリーズの前提条件とリソース要件の理解](#)

## vGW シリーズのライセンスの取得、インストール、および管理

vGW セキュリティ デザイン VM の電源をオンにした後、vGW シリーズ インストール ウィザードを実行します。このプロセス中に製品ライセンス情報を入力するよう求められます。vGW シリーズをご購入いただいた場合は、vGW セキュリティ デザイン VM のライセンス キーを入



力します。ライセンス キーをインストールしたら、シリアル番号が表示されます。このシリアル番号は製品サポートに使用します。

ライセンスが必要な使用するコンポーネントおよび機能ごとに、vGW セキュリティ デザイン VM を使用して資格付与ライセンス キーをインストールする必要があります。適切なライセンス キーが存在しない場合、その機能を作動させることはできず、更新をインストールすることもできません。

ライセンス キーは設定モジュールの [Application Settings] セクションに入力します。[Status & License] セクションの [Product Licensing] セクションでライセンスのインストールと管理を行います。また、このセクションを使用して既存のライセンスを表示することもできます。

関連項目 • [3ページのvGW シリーズの理解](#)

## 設定モジュールを使用した vGW シリーズの VMware との統合

このトピックでは、vGW シリーズを VMware インフラストラクチャと統合する方法について説明します。

vGW シリーズと VMware との連携は、[vCenter Integration] セクションの設定によって制御されます。[vCenter Integration] 画面では、以下のパラメータを構成できます。

- vCenter Settings - vGW セキュリティ デザイン VM が VMware Virtual Center サーバー (vCenter) と通信するために必要なログイン情報。vGW セキュリティ デザイン VM は VMware Virtual Infrastructure API を使用して以下のことを行います。

- VM インベントリ情報の取得
- リソース利用状況の確認
- VM に影響を与えるイベントの確認

vCenter で使用されるアカウントには VMware インフラストラクチャへの読み取りおよび書き込みアクセス権が必要です。VMware で作成したカスタム アカウントを使用できます。そのようなアカウントを使用すると、変更アクティビティを特定および監視するのが容易になります。どちらの場合も、アカウントには管理者特権が必要です。

- Scope - vGW セキュリティ デザイン VM の管理者が、この vGW セキュリティ デザイン VM によって管理する vCenter のデータ センターを指定できます。スプリット センター機能を使用する場合は、[Selected Datacenters] オプション ボタンを選択します。そうすると、すべての vCenter データ センターが表示されます。スプリット センター機能を使用しない場合は、[Entire vCenter] オプション ボタンを選択します。
- スプリット センター機能の概要については、75 ページの「スプリット センター機能の理解」を参照してください。
- Deleted VMs - vGW シリーズでは、ある期間にわたって遭遇していた任意の仮想マシンに関する情報を表示できます。これには VMware の vCenter システム リポジトリから削除されたものも含まれます。この機能により、過去のトラフィック レコードが保持されるので、vGW シリーズ管理者は VMware で発生したすべてのアクティビティを確認できます。このように、vGW シリーズのインターフェースに VM の情報を持続的に表示させることで、悪質な

管理者やハッカーが VM を呼び出して不正なアクティビティを実行した後、その VM を削除して証拠を消し去るような試みを明らかにすることが可能です。ただし、削除された VM を vGW シリーズ インターフェースに表示させたくない場合は、このメニュー項目をオフにして、削除された VM が表示されないようにすることができます。このメニュー項目を再びオンにした場合、削除された VM が再び表示されます。

- vGW Series management enter Plugin – このボタンは、vGW シリーズ プラグインを vCenter インターフェースにインストールする場合に使用します。プラグインをインストールするには、[Register] をクリックします。このプラグインを表示して使用するには、vSphere Client インターフェースで [Home] -> [Solutions and Applications] の順に選択します。vGW シリーズ管理プラグインを削除するには、[Unregister] をクリックします。
- Automatic Startup – この設定を使用して、ESX システムの起動時に vGW シリーズの vGW セキュリティ デザイン VM とファイアウォールも起動するかどうかを指定できます。これらの vGW シリーズ コンポーネントは、デフォルトで自動的に起動するように設定されます。
- Synchronize machine name – デフォルトでは、vCenter で VM の名前が変更されると、vGW セキュリティ デザイン VM 上の対応する VM オブジェクトの名前が同じ値に変更されます。この設定を無効にするには、この項目をオフにします。

たとえば、VM チームと同じ命名規則を使用しない場合は、この設定を無効にできます。また、VM の名前を使用した動的なセキュリティ ポリシーを作成していて、vCenter での単純な名前の変更によってそれらのポリシーが影響を受けないようにする場合にも、このデフォルト動作の無効化は役立ちます。

関連項目    • [3ページのvGW シリーズの理解](#)

## スプリットセンター機能の理解

vGW シリーズには、VMware vCenter のキャパシティ拡張に伴うスケーラビリティの制限を排除する「スプリットセンター」という機能があります。スプリットセンター機能を使用すると、大規模な vCenter を 2 つ以上のデータ センターから成る複数の管理ドメインに分割し、各管理ドメインを別々の vGW セキュリティ デザイン VM によって管理できます。

管理ドメインには 1 つ以上のデータ センターを含めることができます。スプリットセンター機能を使用すると、運用環境の拡張に合わせて、必要な数の vGW セキュリティ デザイン VM を配備できます。

vCenter に関連付けられた個々の vGW セキュリティ デザイン VM は全体として、その vCenter の ESX/ESXi ホストと VM すべてを保護しますが、各 vGW セキュリティ デザイン VM が管理するのは特定のデータ センターのセットのみです。ある vGW セキュリティ デザイン VM からは、他の vGW セキュリティ デザイン VM の情報は見えず、他の vGW セキュリティ デザイン VM によって保護されている仮想化環境の部分も見えません。単一の vGW セキュリティ デザイン VM の立場では、自身が管理するデータ センターの範囲外にあるオブジェクトはすべて、存在しないも同然です。

スプリットセンター機能を構成するには、[Select a scope for your Security Design vGW] という vCenter 範囲選択メニューを使用します。その vGW セキュリティ デザイン VM で vCenter のすべてのデータベースを管理するか、管理する対象のデータ センターを選択できます。

複数の vGW セキュリティ デザイン VM を使用して仮想化環境を管理する場合は、他の vGW セキュリティ デザイン VM の管理者との間でどのデータ センターを管理するかを分担します。どの vGW セキュリティ デザイン VM にも、vCenter のすべてのデータ センターが選択肢として表示されます。

複数の vGW セキュリティ デザイン VM の間で vCenter データベースのセキュリティ管理を分担する方法の詳細については、「マルチセンター機能とスプリットセンター機能を使用した vGW 仮想ゲートウェイ スケーリングの構成」を参照してください。

関連項目   • [3ページのvGW シリーズの理解](#)

## マルチセンター機能の理解

このトピックには、vGW シリーズのマルチセンター機能について説明する以下のセクションがあります。

- [マルチセンター機能 133ページ](#)
- [委任 vGW セキュリティ デザイン VM とスタンドアロン vGW セキュリティ デザイン VM を含む vGW シリーズの配備 133ページ](#)

### マルチセンター機能

データ センターの地理的分離やスケーリング要件、異なる管理ドメインの使用といったさまざまな理由から、vGW シリーズを配備する企業の中には、複数の VMware vCenter を使用して運用環境を管理しているケースがあります。このような企業は、あたかも単一の配備から展開されたかのように、すべてのデータ センターに対して同一またはほぼ同じ vGW セキュリティ デザイン VM 構成を使用することを望みます。異なる場所にある別々の vGW セキュリティ デザイン VM を同じ情報によって手動で構成することは時間がかかって煩雑であり、間違いが起りがちです。

このような要件を持つ企業や、自社の環境を拡張したい企業に対応するため、vGW シリーズには「マルチセンター」という機能が用意されています。マルチセンター機能を使用すると、ある 1 か所の vCenter に接続する vGW セキュリティ デザイン VM をマスターとして指定できます。

データベース レプリケーション モデルに従って、マスター vGW セキュリティ デザイン VM で構成を行い、その構成を 1 つ以上の委任 vGW セキュリティ デザイン VM センター（それぞれが別々の vCenter に接続している）に同期できます。マスター vGW セキュリティ デザイン VM があるグローバル オブジェクトの構成が、マスター vGW セキュリティ デザイン VM の管理者が委任センターの定義を作成するときに選択したオブジェクトに基づいて、委任 vGW セキュリティ デザイン VM センターに自動的に伝播されます。

### 委任 vGW セキュリティ デザイン VM とスタンドアロン vGW セキュリティ デザイン VM を含む vGW シリーズの配備

マルチセンター機能構成に参加する vGW セキュリティ デザイン VM と参加しない vGW セキュリティ デザイン VM を仮想化環境に含めることができます。ある特定の vCenter のリソースを管理する 1 つの vGW セキュリティ デザイン VM で一意の構成を設定し、異なる vCenter に接続する他の vGW セキュリティ デザイン VM でそれとほとんど同じ構成を使用したい場合があります。

たとえば、6 つのデータ センターを含む仮想化環境があり、各データ センターはサイズがさまざま、それぞれ別々の vCenter に接続しているとします。これらのデータ センターのうち 5 つで同じ全体的構成を使用し、残り 1 つでは異なる構成を使用する場合、同様に構成する 5 つのデータ センターに対してマルチセンター機能を使用し、残り 1 つの vGW セキュリティ デザイン VM は個別に構成することができます。

- 関連項目
- [134ページのvGW シリーズのマルチセンター機能の構成](#)
  - [135ページのvGW シリーズ マルチセンターの同期オブジェクトの理解](#)

## vGW シリーズのマルチセンター機能の構成

このトピックでは、マルチセンター機能を使用して、マスター センターの vGW セキュリティ デザイン VM の構成を、異なる vCenter に接続する他の vGW セキュリティ デザイン VM インストールに同期する方法について説明します。マスターに従属する vGW セキュリティ デザイン VM インストールのことを「委任センター」と呼びます。

委任センターは 1 つ以上構成できます。マスターから委任センターに構成を同期するオブジェクトを選択できます。

委任センターを作成するには、OVA をインポートし、vGW セキュリティ デザイン VM を管理対象の vCenter に接続します。OVA のインポートの詳細については、[18ページの「「OVA バンドル方法を使用した vGW シリーズの VMware インフラストラクチャとの統合」](#) および [27ページの「「OVA 単一ファイル方法を使用した vGW セキュリティ VM の VMware との統合」](#) を参照してください。

マルチセンター機能を構成するには、設定モジュールの [Application Settings] セクションを使用します。委任センターに同期するオブジェクトは、委任センターの観点からはグローバル オブジェクトと見なされます。マスター vGW セキュリティ デザイン VM の管理者は、新しい委任センター構成を追加するとき、同期するオブジェクトを指定します。

このトピックを読む前に、[133ページの「「マルチセンター機能の理解」](#)」をお読みください。

委任センターをマルチセンター構成に追加するには、以下の手順に従います。

1. マスター（プライマリ）センターで、設定モジュールの [Application Settings] セクションを選択し、[Multi-Center] を選択します。
2. 下部の [Multi-Center Configuration] ペインで、[Add] をクリックします。  
[Delegate Center Configuration (Add)] ペインが表示されます。
3. [Name] フィールドで、委任センターを表す構成の名前を指定します。
4. [Hostname/IP] フィールドに、委任センターのホスト名または IP アドレスを入力します。
5. [User ID] フィールドと [Password] フィールドに、委任センターの認証情報を入力します。
6. 同期するオブジェクトを選択します。
  - リストにあるすべてのオブジェクトの状態をマスター vGW セキュリティ デザイン VM から定義中の委任センターに同期する場合は、[Select All] をオンにします。

- 一部のオブジェクトだけをマスター vGW セキュリティ デザイン VM から委任センターに同期する場合は、[Synchronize Objects] セクションで、同期する各オブジェクトの前にあるチェックボックスをオンにします。
  - Global Policy
  - Default Policy
  - Quarantine Policy
  - Policy Groups
  - Monitoring Groups
  - Networks
  - External Machines
  - IDS Signatures
  - Compliance
  - AntiVirus Settings

最初に委任センターを構成するとき、その委任センターの証明書を認証する必要があります。



**警告:** 委任センターがすでに構成されているときにバックアップ ファイルが作成された場合、次の条件とアクションが適用されます。マスター vGW セキュリティ デザイン VM をバックアップ ファイルからリストアする場合、バックアップ ファイルがリストアされた後に、マスター vGW セキュリティ デザイン VM のマルチセンター表に表示された委任 vGW セキュリティ デザイン VM センターのエントリを保存する必要があります。 そのためには、各委任センターの行エントリを選択して [Save] をクリックします。

委任センターのエントリを保存する前、そのエントリは委任センターとマスター vGW セキュリティ デザイン VM とが一度も通信していないことを示します。 ただし、マスター vGW セキュリティ デザイン VM には委任センターの正しい IP アドレスが設定されており、マスターと委任センターの両方が互いの証明書を持っています。

- 関連項目
- [133ページのマルチセンター機能の理解](#)
  - [135ページのvGW シリーズ マルチセンターの同期オブジェクトの理解](#)

## vGW シリーズ マルチセンターの同期オブジェクトの理解

このトピックでは、プロトコルおよびコンプライアンス規則オブジェクトがマスター vGW セキュリティ デザイン VM から委任 vGW セキュリティ デザイン VM センターにどのように同期されるかについて説明します。 委任センターの [Settings] ペインには、同期されたオブジェクトに関するステータスやその他の情報が表示されます。

委任センターの観点からは、同期オブジェクトは読み取り専用のグローバル オブジェクトと見なされ、変更できません。

このトピックには以下のセクションがあります。

- [オブジェクトの同期 136ページ](#)
- [オブジェクトの命名 136ページ](#)
- [委任 vGW セキュリティ VM に対してローカルなオブジェクトの作成 136ページ](#)

## オブジェクトの同期

新しく同期されたグローバル オブジェクトが名前も内容も委任センターにあるローカル オブジェクトと同一である場合があります。 この場合、グローバル オブジェクトにプロトコルやコンプライアンス規則などのデフォルト値が含まれるときは、ローカル オブジェクトがグローバル オブジェクトに変換されます。 委任センター vGW セキュリティ デザイン VM にあるグローバル版のローカル オブジェクトは、変換済みとしてマークされます。 このローカル オブジェクトへの参照はすべて保持されますが、変換後、それらの参照はグローバル オブジェクトに関係します。 変換されたオブジェクトはグローバル オブジェクトなので、委任センター vGW セキュリティ デザイン VM 上で読み取り専用オブジェクトとしてアクセスされます。 つまり、委任センター vGW セキュリティ デザイン VM の管理者はこのオブジェクトを変更できません。

もはやミラーリングされなくなったオブジェクトは、ローカル オブジェクトによって使用されている場合を除き、委任センターから削除されます。 つまり、そのオブジェクトがプロトコルなどのローカル オブジェクトから変換されたものである場合は、その時点でローカル オブジェクトに逆変換されます。

## オブジェクトの命名

命名の問題とスマート グループのロジックの問題を避けるため、同じ名前を持つグローバル オブジェクトとローカル オブジェクトが同じコンテキストで存在する場合は、グローバル オブジェクトが優先され、グローバル オブジェクトにその名前が使用されます。 そのオブジェクトには、委任センターから見てグローバルとマークされます。 競合する名前を持つオブジェクトは名前が変更され、末尾に「local」という語が付加されます。

マスター vGW セキュリティ デザイン VM の管理者は、委任センターに対して選択されているオブジェクトを削除できます。 この場合、そのオブジェクトは委任センター上でグローバルでなくなります。 それに対応するローカル オブジェクトが存在する場合、そのオブジェクトは元の状態に戻り、委任センター管理者が編集できるようになります。

## 委任 vGW セキュリティ VM に対してローカルなオブジェクトの作成

委任 vGW セキュリティ デザイン VM センターの管理者は、自分が管理するシステムのローカル オブジェクトを今までどおり構成できます。 これらのローカル オブジェクトはローカルのまま存続し、一部の例外を除き、マスター vGW セキュリティ デザイン VM 構成には影響しません。 たとえば、ローカル ポリシー グループの優先度は常にグローバル ポリシー グループよりも低くなります。

関連項目    • [133ページのマルチセンター機能の理解](#)



## マルチセンター機能とスプリットセンター機能を使用したスケーリングの構成

このトピックでは、マルチセンター機能とスプリットセンター機能を組み合わせて拡張する仮想化環境を保護する方法について説明します。

これらの機能は通常、以下のことを実現するために組み合わせて使用します。

- 単独の vCenter にある複数の vGW セキュリティ デザイン VM の間でリソースを分割して管理する。

スプリットセンター機能を使用すると、単独の vCenter にあるリソースを分割し、各部分に対する責任を複数の vGW セキュリティ デザイン VM の間で分担できます。各 vGW セキュリティ デザイン VM は、あたかも別々の vCenter に接続しているかのように見えます。この機能では、分割の単位はデータ センターです。

スプリットセンター機能の背景については、[132ページの「スプリットセンター機能の理解」](#)を参照してください。

- すべての vGW セキュリティ デザイン VM 委任センター（単一の vCenter について責任を分担しているものも含む）にほとんど同じ構成を配備する。

マルチセンター機能を使用すると、運用環境の拡張に合わせた構成管理が容易になります。

異なる vCenter にある vGW セキュリティ デザイン VM、および同じ vCenter でリソースのセキュリティ管理責任を分担している vGW セキュリティ デザイン VM に対してほとんど同じ構成を作成することが可能です。それらの vGW セキュリティ デザイン VM に同じ構成を効果的に配備し、リアルタイムで自動的に更新できます。

マルチセンター機能の背景については、[133ページの「マルチセンター機能の理解」](#)を参照してください。

このトピックには以下のセクションがあります。

- [vGW シリーズのスプリットセンターマルチセンター構成の要件 137ページ](#)
- [例について 138ページ](#)
- [vGW セキュリティ デザイン VM に対するスプリットセンターおよびマルチセンターの構成 140ページ](#)

### vGW シリーズのスプリットセンターマルチセンター構成の要件

以下の例に示す会社の仮想化インフラストラクチャでは、3 つの個別の VMware vCenter でデータ センターを管理しています。

- 最初の vCenter (vCenter1) には 5 つのデータ センターが含まれます。vCenter1 はテキサス州ダラスにあります。1 つのデータ センターが他のデータ センターよりかなり大規模です。

vCenter1 データ センターの管理は、スプリットセンター機能によって、以下のように 2 つの vGW セキュリティ デザイン VM の間で分割します。

- vGW セキュリティ デザイン VM-1 は、大規模なデータ センターである vCenter1-data-center-1 を管理します。
- vGW セキュリティ デザイン VM-2 は、以下の残り 4 つのデータ センターを管理します。

- vCenter1-data-center-2
  - vCenter1-data-center-3
  - vCenter1-data-center-4
  - vCenter1-data-center-5
- 2 番目の vCenter (vCenter2) には 2 つのデータ センターが含まれます。vCenter2 はミネソタ州ミネアポリスにあります。vGW セキュリティ デザイン VM-3 によって以下の両方のデータ センターを管理します。
    - vCenter2-data-center-1
    - vCenter2-data-center-2
  - 3 番目の vCenter (vCenter3) には 2 つのデータ センターが含まれます。vCenter3 はノースカロライナ州ローリーにあります。vGW セキュリティ デザイン VM-4 によって以下の両方のデータ センターを管理します。
    - vCenter3-data-center-1
    - vCenter3-data-center-2

## 例について

この会社の仮想化環境は、地理的に離れた 3 つの vCenter にまたがります。そのうち 1 つの vCenter にあるリソースのセキュリティ管理責任を、スプリットセンター機能によって 2 つの vGW セキュリティ デザイン VM の間で分割します。

この会社では、すべての vGW セキュリティ デザイン VM にほとんど同じ構成を配備することを計画しています。それぞれの構成を同じパラメータを使用して手動で別々に作成するのは時間がかかるうえに間違いが起りやすいので、マルチセンター機能を使用してこの問題を解決することにしました。

マルチセンター機能では、ある 1 つの vGW セキュリティ デザイン VM をマスター センターとして使用します。そのマスター センターの構成が、すべてのスレーブ（委任）vGW セキュリティ デザイン VM にコピーされます。

この例では、vGW セキュリティ デザイン VM-3 をマスター センターとします。vGW セキュリティ デザイン VM-3 の管理者が、すべての委任センターのマルチセンター機能を構成します。

各委任 vGW セキュリティ デザイン VM センターのエントリを定義するには、設定モジュールの [Application Settings] セクションにある [Multi-Center] セクションを使用します。この例の委任センターは以下のとおりです。

- vGW セキュリティ デザイン VM-1
  - すべてのオブジェクトがコピーされるよう指定します。
- vGW セキュリティ デザイン VM-2
  - すべてのオブジェクトがコピーされるよう指定します。
- vGW セキュリティ デザイン VM-4



監視グループと IDS 以外のすべてのオブジェクトがコピーされるよう指定します。

設定モジュールの [Multi-Center] セクションにある [Delegate Center Configuration (Add)] ペインを使用して、委任 vGW セキュリティ デザイン VM センターのエントリを作成します。そのために、以下の情報を入力します。

- Name - 委任センターの名前を入力します。
- Hostname/IP - 委任センターのホスト名または IP アドレスを入力します。これにより、マスター vGW セキュリティ デザイン VM と委任センター vGW セキュリティ デザイン VM が通信できるようになります。  
  
委任センターに対して選択したオブジェクトに基づいて、マスター構成が委任センターで自動的に更新されます。
- User ID および Password - 委任 vGW セキュリティ デザイン VM センターの資格情報を入力します。
- Synchronize Objects - すべてのオブジェクトを選択する場合は [Select All] チェックボックスをオンにし、コピーして自動的に更新するオブジェクトを個別に選択する場合はそのオブジェクトの前にあるチェックボックスをオンにします。以下のオブジェクトを選択できます。
  - Global Policy - グローバル ポリシーと、そのポリシーが依存するすべてのオブジェクトを同期します。特に、ポリシー内の規則の送信元と宛先、およびプロトコルの構成がコピーされます。
  - Default Policy - デフォルト ポリシーと、そのポリシーが依存するすべてのオブジェクトを同期します。特に、ポリシー内の規則の送信元と宛先、およびプロトコルの構成がコピーされます。
  - Quarantine Policy - 検疫ポリシーと、そのポリシーが依存するすべてのオブジェクトを同期します。特に、ポリシー内の規則の送信元と宛先、およびプロトコルの構成がコピーされます。
  - Policy Groups - すべてのポリシー グループと各グループに関連するポリシー、および各ポリシーが依存するすべてのオブジェクトを同期します。特に、グループに含まれるポリシー内の規則の送信元と宛先、プロトコル、ネットワーク、およびマシンがコピーされます。
  - Monitoring Groups - すべての監視グループと各グループに関連するポリシー、および各ポリシーが依存するすべてのオブジェクトを同期します。特に、グループに含まれるポリシー内の規則の送信元と宛先、プロトコル、ネットワーク、およびマシンがコピーされます。
  - Networks - すべてのネットワークを同期します。
  - External Machines - すべての外部マシンを同期します。
  - IDS Signatures - IDS シグネチャと設定を同期します。

- Compliance - コンプライアンス規則と、各規則が依存するすべてのオブジェクト（グループなど）を同期します。
- Antivirus Settings - すべてのアンチウイルス スキャン構成と、各構成が依存するすべてのオブジェクト（グループなど）を同期します。

## vGW セキュリティ デザイン VM に対するスプリットセンターおよびマルチセンターの構成

### 最初の vGW セキュリティ デザイン VM に対するスプリットセンターの構成

ステップごとの手順 ここでは、スプリットセンター機能を使用して、vCenter1 にあるリソースの一部の管理責任を vGW セキュリティ デザイン VM-1 に与える方法を示します。

1. vGW セキュリティ デザイン VM-1 から、設定モジュールを選択します。
2. ナビゲーション ツリーで、[vGW Application Settings] の下にある [vCenter Integration] を選択します。
3. [vCenter Settings] ペインで、以下の情報を入力します。
  - vCenter のサーバー名または IP アドレス。この例では、vCenter1 と入力します。
  - vCenter1 に対して認証する vGW セキュリティ デザイン VM-1 のユーザー名とパスワード。この例では、admin-1 および talk#321 と入力します。
4. [vCenter Settings] ペインで、vGW セキュリティ デザイン VM-1 の管理範囲を選択します。vCenter1 に属するデータ センターを表示するには、[Selected Datacenters] オプション ボタンを選択します。

vCenter1 に属する以下のデータ センターが表示されます。

- vCenter1-data-center-1
- vCenter1-data-center-2
- vCenter1-data-center-3
- vCenter1-data-center-4
- vCenter1-data-center-5

デフォルトでは、その vGW セキュリティ デザイン VM がすべてのデータ センターを管理するよう構成されます。

5. vCenter1-data-center-1 の前のチェックボックスをオンにして [Save] をクリックし、vGW セキュリティ デザイン VM-1 にこのデータ センターの管理を任せます。

これで、vGW セキュリティ デザイン VM-1 によって管理される範囲が vCenter1 の vCenter1-data-center-1 にある VM とその他のリソースのみになりました。



注: 選択した内容が保存される前に、管理者が指定した認証資格情報が vCenter1 によって検証されます。 次のメッセージが表示されます。

Checking vCenter login credentials. This may take up to 15 seconds depending on server loads.

指定した資格情報が無効な場合、選択したデータ センター管理範囲は確定されません。

6. 構成を確定する場合は、[Okay] をクリックします。

## 2 番目の vGW セキュリティ デザイン VM に対するスプリットセンターの構成

ステップごとの手順 ここでは、スプリットセンター機能を使用して、vCenter1 にあるリソースの一部の管理責任を vGW セキュリティ デザイン VM-2 に与える方法を示します。

1. vGW セキュリティ デザイン VM-2 から、設定モジュールを選択します。
2. ナビゲーション ツリーで、[vGW Application Settings] の下にある [vCenter Integration] を選択します。
3. [vCenter Settings] ペインで、以下の情報を入力します。
  - vCenter のサーバー名または IP アドレス。 この例では、vCenter1 と入力します。
  - vCenter1 に対して認証する vGW セキュリティ デザイン VM-2 のユーザー名とパスワード。 この例では、admin-2 および talk#4\*5#6 と入力します。
4. [vCenter Settings] ペインで、vGW セキュリティ デザイン VM-2 の管理範囲を選択します。 vCenter1 に属するデータ センターを表示するには、[Selected Data centers] オプション ボタンを選択します。

vCenter1 に属する以下のデータ センターが表示されます。

- vCenter1-data-center-1
- vCenter1-data-center-2
- vCenter1-data-center-3
- vCenter1-data-center-4
- vCenter1-data-center-5

デフォルトでは、その vGW セキュリティ デザイン VM がすべてのデータ センターを管理するよう構成されます。

5. vCenter1-data-center-2、vCenter1-data-center-3、vCenter1-data-center-4、vCenter1-data-center-5 の前のチェックボックスをオンにして [Save] をクリックし、vGW セキュリティ デザイン VM-2 にこれらのデータ センターの管理を任せます。



注: 選択した内容が保存される前に、管理者が指定した認証資格情報が vCenter1 によって検証されます。次のメッセージが表示されます。

Checking vCenter login credentials. This may take up to 15 seconds depending on server loads.

指定した資格情報が無効な場合、選択したデータ センター管理範囲は確定されません。

6. 構成を確定する場合は、[Okay] をクリックします。

### マルチセンター機能を使用した 3 つの委任センターのエントリの定義

#### ステップごとの手順

ここでは、3 つの vGW セキュリティ デザイン VM を委任センターにして、マスターである vGW セキュリティ デザイン VM-3 の構成の大部分を継承するためのエントリを定義する方法を示します。

この例では、以下のエントリを構成する方法を示します。

- vGW セキュリティ デザイン VM-1 と vGW セキュリティ デザイン VM-2 のエントリ。これらの VM には、すべての構成オブジェクトがコピーされるようにします。
- vGW セキュリティ デザイン VM-4 のエントリ。この VM には、監視グループと IDS 以外のすべての構成オブジェクトがコピーされるようにします。

vGW セキュリティ デザイン VM-3 マスターから vGW セキュリティ デザイン VM-1 の委任センター エントリを定義するには、以下の手順に従います。

1. 設定モジュールの [Applications Settings] セクションを選択し、[Multi-Center] を選択します。
2. 委任センター エントリの名前として、mc-delegate-1 と入力します。
3. 委任センターのユーザー ID およびパスワード資格情報として、admin-1 および talk#321 と入力します。
4. [Synchronize Objects] で、[Select All] をクリックします。
5. 構成に間違いがない場合は、[Save] をクリックします。間違いがある場合は [Cancel] をクリックします。

#### ステップごとの手順

vGW セキュリティ デザイン VM-3 マスターから vGW セキュリティ デザイン VM-2 の委任センター エントリを定義するには、以下の手順に従います。

1. 設定モジュールの [Applications Settings] セクションを選択し、[Multi-Center] を選択します。
2. 委任センター エントリの名前として、mc-delegate-2 と入力します。
3. 委任センターのユーザー ID およびパスワード資格情報として、admin-2 および talk#4\*5#6 と入力します。

4. [Synchronize Objects] で、[Select All] をクリックします。
5. 構成に間違いがない場合は、[Save] をクリックします。間違いがある場合は [Cancel] をクリックします。
6. 選択したオブジェクトをマスターから委任 vGW セキュリティ デザイン VM-2 センターにただちに同期するには、[Synchronize] をクリックします。

ステップごとの手順 vGW セキュリティ デザイン VM-3 マスターから、監視グループと IDS 以外のすべてのオブジェクトをコピーする vGW セキュリティ デザイン VM-4 の委任センター エントリを定義するには、以下の手順に従います。

1. 設定モジュールの [Applications Settings] セクションを選択し、[Multi-Center] を選択します。
2. 委任センター エントリの名前として、mc-delegate-4 と入力します。
3. 委任センターのユーザー ID およびパスワード資格情報として、admin-4 および eadf2#\$4 と入力します。
4. [Synchronize Objects] で、監視グループと IDS 以外のすべてのオブジェクトについて、前にあるチェックボックスをオンにします。
5. 構成に間違いがない場合は、[Save] をクリックします。間違いがある場合は [Cancel] をクリックします。
6. 選択したオブジェクトをマスターから委任 vGW セキュリティ デザイン VM-4 センターにただちに同期するには、[Synchronize] をクリックします。

結果 以下のエリアで委任センターのステータスを確認できます。

- マスター vGW セキュリティ デザイン VM 上の [Multi-Center Configuration] 表。この表には、構成の同期に関するサマリ情報が示されます。

マスター vGW セキュリティ デザイン VM の設定モジュールで、[vGW Application Settings] の [Multi-Center] を選択します。

- 委任 vGW セキュリティ デザイン VM 上の [Multi-Center Status and Information] ペイン。このペインには、マスターから同期された構成に関する詳細情報が示されます。

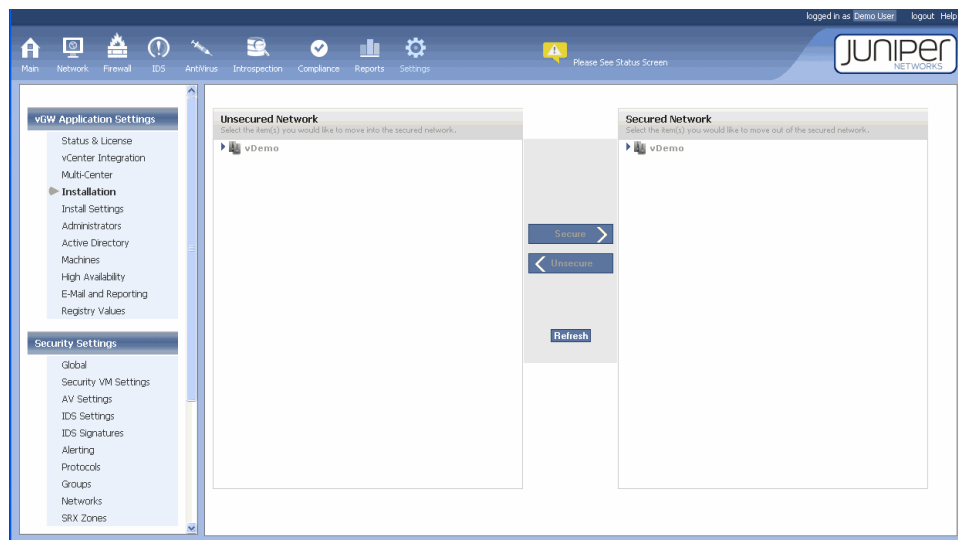
委任 vGW セキュリティ デザイン VM センターの設定モジュールで、[vGW Application Settings] の [Multi-Center] を選択します。

関連項目 • [3ページのvGW シリーズの理解](#)

## ESX/ESXi ホストへの vGW セキュリティ VM の配備

情報を収集してネットワーク トラフィックを保護するため、監視および保護対象の各 ESX/ESXi ホストに vGW セキュリティ VM を配備します。vGW セキュリティ VM をホストにインストールすると、カーネル モジュールがロードされ、ポリシーとログ情報が維持されます。すべての接続は vGW VMsafe カーネル モジュールで行われます。 [144ページの図34](#)を参照してください。

図 34: ESX/EXSi ホストへの vGW セキュリティ VM の配備



vGW セキュリティ VM をホストにインストールするには、以下の手順に従います。

1. vGW セキュリティ デザイン VM の設定モジュールの [vGW Application Settings] セクションで、[Installation] を選択します。
2. [Unsecured Network] ペインで、vGW セキュリティ VM をインストールするホストの前のチェックボックスをオンにして選択します。
3. vGW セキュリティ VM ファイアウォールの名前を指定します。
4. [Secure] をクリックします。

vGW カーネル コンポーネントをホストにインストールしてよいか確認するメッセージが表示されます。

[Secure] をクリックすると、関連する VM のすべての仮想 NIC (vNIC) が vGW シリーズ VMsafe カーネル モジュールに関連付けられます。デフォルトでは、各 vNIC には非常に限定的なセキュリティ ポリシーが設定されています。ファイアウォール モジュールの [Manage Policy] タブを使用して、このポリシーの制限を緩和できます。また、たとえばあるストレージ ネットワーク デバイスに接続している vNIC にセキュリティを実装しない場合など、VM の特定の vNIC を vGW セキュリティ ポリシーの適用および強制から除外することもできます。

vGW シリーズには vNIC 毎ポリシーという機能があり、同じ VM 上の個々のインターフェース、つまり仮想 NIC (vNIC) に対して別々のファイアウォール ポリシーを構成できます。この機能の詳細については、147ページの「[vGW シリーズの vNIC 毎ポリシー機能の理解](#)」および148ページの「[vGW シリーズの vNIC 毎ポリシー機能の構成](#)」を参照してください。

5. [OK] をクリックします。

[Security VM Parameters] ウィンドウが表示されます。

以下のパラメータの値を指定または選択します。

- a. vGW セキュリティ VM の名前を入力します。
- b. セキュリティ管理対処モードを選択します。
- c. vGW セキュリティ VM から vGW セキュリティ デザイン VM への接続に使用するポートグループを指定します。
- d. vGW セキュリティ VM のデータ ストアを指定します。
- e. ハイパーバイザ通信コンソールを監視するかどうかを指定します。 ハイパーバイザ コンソールの監視を有効にする方法の詳細については、[163ページの「vGW セキュリティ VM の設定モジュールの理解」](#)の構成情報を参照してください。
- f. [Secure] をクリックします。

vGW セキュリティ デザイン VM をホストからアンインストールするには、以下の手順に従います。

1. [vGW Application Settings] の [Installation] セクションにある [Secured Network] ペインで、保護ネットワークから移動する vGW セキュリティ VM を持つホストを選択します。
2. [Unsecure] 矢印ボタンをクリックします。
3. [VMsafe Firewall Uninstall] ステータス ウィンドウが表示されます。 選択したホストからファイアウォールが削除される処理 (VM を選択した場合は特定の VM が保護ネットワークから移動される処理) の進行状況がステータス ウィンドウに表示されます。

保護ネットワークから削除する単一の VM を選択して [Unsecure] ボタンをクリックすると、その VM の VMsafe 保護に関連するすべての VMX エントリが削除され、vGW シリーズによる保護を適用する前の状態に戻ります。

仮想化環境から vGW シリーズをアンインストールする場合は、この方法ですべての VM の保護を解除します。 その後で、各 ESX/ESXi ホストのチェックボックスをオンにして [Unsecure] をクリックし、vGW シリーズによる保護の対象から除外します。 そうすると、カーネル モジュールと、関連する VMservice vSwitch およびポート グループが削除されます。

ホストの VM を削除する前にホストを保護対象から除外しても VM に悪影響はありません。 ただし、その VM の、vGW シリーズに関連する不要な VMsafe VMX エントリが削除されずに残ります。



**注:** vGW シリーズのカーネル モジュールだけを特定のホストから削除し、VM は保護対象の別の ESX/ESXi ホストに移動する場合、または後で vGW シリーズを再インストールする場合には、VM の VMsafe VMX エントリを削除しない方が望ましいことがあります。

関連項目 • [3ページのvGW シリーズの理解](#)

## vGW シリーズのインストール設定の構成

このトピックでは、管理者が vGW セキュリティ デザイン VM を使用して構成するファイアウォール インストール設定について説明します。この構成には、設定モジュールの [Install Settings] セクションを使用します。

[VMSafe installation] ペインで以下の情報を構成します。以下のことができます。

- ESX/ESXi ホスト上での vGW セキュリティ VM (ファイアウォール) のインスタンス化に使用する vGW セキュリティ VM テンプレートを選択します。[VMSafe Template] ポップアップメニューから、使用するテンプレートを選択します。
- VM が vGW シリーズ VMSafe カーネル モジュールに接続できない場合、または vGW セキュリティ デザイン VM からファイアウォール ポリシーを取得できない場合のセキュリティ動作を指定します。
  - VM へのトラフィックまたは VM からのトラフィックをセキュリティ制御なしで許可します。
  - VM へのトラフィックまたは VM からのトラフィックをすべて停止します。この場合、VMware からその VM の vNIC への接続は切断されます。
- vGW セキュリティ VM および vGW セキュリティ デザイン VM によって VM のアクティビティの監視のみを行い、VM を保護しないことを指定します。

この場合、その VM 用の vGW セキュリティ VM にファイアウォール ポリシーはロードされません。監視モードを使用すると、セキュリティ ポリシーによってトラフィックがブロックされないよう気を配らずに vGW セキュリティ VM を配備できます。

自動保護機能を有効にして、指定した VM を自動的に保護し、それらの VM にセキュリティ ポリシーを付加できます。

VM を保護することを選択した場合、必要に応じて、選択したグループ内の特定のグループを自動的に保護する対象から除外できます。

以下のことができます。

- 自動的に保護する VM を選択します。以下を指定できます。
  - VM を指定しない。
  - フィールドのポップアップ リストから選択した特定のグループに属する VM。
  - VM ポリシーが付与された VM、またはポリシー グループに含まれる VM。
  - すべての VM。
- 自動的に保護しない VM のグループを選択します。ポップアップ メニューを使用してグループを選択します。

vNIC ごとに別々のポリシーを割り当てるオプションを設定できます。詳細については、[148ページの「vGW シリーズの vNIC 毎ポリシー機能の構成」](#)を参照してください。

- [Policy-per-vNIC] ペインを使用して、以下の情報を構成します。



- 同じ VM 上の vNIC ごとに別々のポリシーを構成できるようにするかどうか。
- 別々の vNIC ポリシーを許可する VM で、1 つ以上の vNIC を対象外にできるかどうか。  
つまり、それらの vNIC にはセキュリティ ポリシーは付加されず、vGW シリーズによって保護されません。

関連項目    • [3ページのvGW シリーズの理解](#)

## vGW シリーズの vNIC 毎ポリシー機能の理解

このトピックでは、vGW シリーズの vNIC 毎ポリシー機能について説明します。この機能を使用すると、同じゲスト VM (VM) 上の個々のインターフェース、つまり仮想 NIC (vNIC) に対して別々のファイアウォール ポリシーを構成できます。

- [vNIC 毎ポリシーについて 147ページ](#)
- [個別のポリシーを持つ vNIC とスマート グループ 147ページ](#)
- [個別のポリシーを持つ vNIC の表示 148ページ](#)
- [vNIC の命名規則 148ページ](#)

### vNIC 毎ポリシーについて

vNIC 毎ポリシー機能は、vGW セキュリティ デザイン VM を使用して構成します。vNIC 毎ポリシー機能を有効にするか、VM 上のすべての vNIC を同じように保護するか（デフォルトの動作）を選択できます。vNIC 毎ポリシーを有効にした場合でも、vNIC が 1 つしかない VM では単一の vNIC に対するポリシーを構成できます。

vNIC 毎ポリシーを有効にしない場合、VM 上のいずれかの vNIC に対して個別のポリシーを構成することはできません。VM 上のすべての vNIC が同じポリシーを継承します。選択した vNIC の構成方法は、配備環境にグローバルに適用されます。つまり、同じ vGW セキュリティ デザイン VM を使用して構成されたすべての VM に適用されます。

vNIC 毎ポリシー機能を有効にした場合、同じ VM 上の 1 つ以上の vNIC にファイアウォール ポリシーを付加しないことを許可するオプションを有効にできます。そうすると、ファイアウォール セキュリティを効果的に回避できます。このオプションを有効にすると、一部の vNIC をそれぞれ固有のポリシーによって保護し、同じ VM 上の残りのポリシーを保護対象から除外することが可能です。

### 個別のポリシーを持つ vNIC とスマート グループ

vNIC 毎ポリシー機能が使用されている VM をスマート グループに含めることができます。スマート グループのメンバーシップを VM 全体（つまり、VM のすべてのインターフェース）に適用するか、スマート グループのロジックが当てはまる vNIC のみに適用するかを選択できます。たとえば、インターフェースがあるポート グループに属していること、またはある特定の VLAN に接続していることをスマート グループに含める条件にすることが可能です。vNIC 毎ポリシーを構成した場合の vNIC とスマート グループとの関係の詳細については、[153ページ](#)の「[vNIC 毎ポリシーとスマート グループ](#)」を参照してください。

## 個別のポリシーを持つ vNIC の表示

このセクションでは、vNIC とその情報が vGW セキュリティ デザイン VM によってどのように表示されるかの概要を示します。vNIC のポリシー情報の構成および表示方法の詳細については、150ページの「同じ VM 上の個々の vNIC に対する vGW ポリシーの構成と表示」を参照してください。

vNIC 毎ポリシー機能が有効な場合、

- vNIC は、VM ツリー内のそれぞれの VM の下に表示されます。VM を展開すると、その VM が持つ個々の vNIC が表示されます。たとえば、VM1 を展開すると VM1.nic1 と VM1.nic2 が表示されます。
- VM に関する操作（イントロスペクションやコンプライアンスなど）については、個々の vNIC は表示されません。個々の vNIC は、それらが属する VM と同じように扱われます。VM に含まれるいずれかの vNIC が適合していない場合、その VM は不適合と見なされます。



注: vNIC 毎ポリシー機能を使用しない場合は、同じポリシーがすべての vNIC に適用され、VM は VM ツリー内で単一ノードとして表示されます。

## vNIC の命名規則

vGW シリーズでの vNIC の命名規則は、関連する vCenter 内の VMware で使用されている規則に整合します。

- VMware では、vNIC の名前は Network adapter 1、Network adapter 2 のようになります。vNIC の番号は 0 ではなく 1 から始まります。
- vGW シリーズでは、vNIC の名前は VMx.nic1、VMx.nic2 のようになります。

関連項目    • 3ページのvGW シリーズの理解

## vGW シリーズの vNIC 毎ポリシー機能の構成

このトピックでは、vGW シリーズの vNIC 毎ポリシー機能を有効にして構成する方法について説明します。この機能を使用すると、同じゲスト仮想マシン (VM) に装備された個々の vNIC に対して別々のポリシーを定義できます。この作業には、vGW セキュリティ デザイン VM を使用します。

このトピックを読む前に、「vGW シリーズの vNIC 毎ポリシー機能の理解」をお読みください。

デフォルト構成を引き続き使用し、VM 上のすべての vNIC に対して同じポリシーを使用することもできます。

同じ VM 上の vNIC のポリシーを以下のように構成できます。

- VM 上のすべての vNIC で別々のポリシーを使用する。

- 同じ VM 上の一部の vNIC で別々のポリシーを使用し、同じ VM 上の残りの vNIC は保護されないままにする。
- 単一の VM 上のすべての vNIC で同じポリシーを使用する（デフォルト）。



注: VM で vNIC 毎ポリシー機能を使用し、一部の VM に対して別々のポリシーを定義した場合、同じ VM 上の残りの vNIC に適用する追加の単一ポリシーを定義することはできません。

vNIC 毎ポリシーを有効にするには、以下の手順に従います。

1. vGW セキュリティ デザイン VM の設定モジュールを選択します。
2. [vGW Application Settings] セクションで、[Install Settings] を選択します。
3. vNIC 毎ポリシー機能をグローバルに有効にするには、[Policy Per vNIC] セクションで、[Enable policy at the vNIC level] の前のチェックボックスをオンにします。
4. 必要に応じて、VM 上の一部の vNIC のみを保護し、残りの vNIC は保護しないように構成できます。このオプションを有効にするには、[Enable opt-out of firewalling per vNIC] の前のチェックボックスをオンにします。

保護されない vNIC を含む VM に新しいインターフェースを追加すると、その新しいインターフェースは自動的に保護されます。新しいインターフェースを保護しない場合は、手動で保護対象から除外する必要があります。以下に、vNIC を保護対象から除外する手順を示します。

vNIC に対して個別のポリシーを定義する方法の詳細については、150ページの「[同じ VM 上の個々の vNIC に対する vGW ポリシーの構成と表示](#)」を参照してください。

vNIC からセキュリティ ポリシーを削除する、つまりその vNIC を保護対象から除外するには、以下の手順に従います。

1. vGW セキュリティ デザイン VM の設定モジュールを選択します。
2. [vGW Applications Settings] セクションで、[Installation] を選択します。
3. vNIC を保護対象から除外する前に、その vNIC に適用されているポリシーを削除します。
4. [Secured Network] ペインで、保護対象から除外する vNIC を選択して [Unsecure] 矢印をクリックします。

vNIC または VM 全体を保護対象から除外してよいかどうかを確認するメッセージが表示されます。



注: 保護されない vNIC を含む VM に新しい vNIC を追加した場合、その vNIC は自動的に保護されます。新しい vNIC を保護しない場合は、上記の手順に従って手動で保護対象から除外する必要があります。

インストール UI でポート グループから vNIC を接続解除した場合（vNIC の選択をオフにした場合）、その vNIC は保護されなくなります。 インストーラのダイアログに vNIC の状態を示す警告メッセージが表示されます。

関連項目    • 3ページのvGW シリーズの理解

## 同じ VM 上の個々の vNIC に対する vGW ポリシーの構成と表示

このトピックでは、vNIC 毎ポリシー機能を有効にした場合に同じゲスト仮想マシン（VM）に属する個々の vNIC に対してポリシー規則を構成する方法について説明します。 また、VM ツリーに vNIC がどのように表示されるかについても説明します。 ポリシーを構成して vNIC に適用するには、vGW セキュリティ デザイン VM のファイアウォール モジュールを使用します。

vNIC 毎ポリシーが有効で、同じ VM に複数の vNIC が構成されている場合、それらの vNIC は VM ツリーで、所属する VM の下にネスト表示されます。

- VM ツリーには vNIC の状態が以下のように表示されます。
  - 無効な vNIC は、その vNIC 上のトラフィックが vGW セキュリティ VM ファイアウォールによって保護されていないことを示すアイコンで示されます。
  - VM に個別のファイアウォール ポリシーを持つ vNIC が含まれていて、その VM がグループに属している場合、そのグループのメンバーである vNIC はアクティブとして表示されます。 そのグループに属していない vNIC は、表示はされますが、グループに属していないことを示すために灰色になります。



**注：** vNIC を削除したときに vNIC の番号が変わることがあります。 たとえば、vNIC1 と vNIC2 を含む VM から vNIC1 を削除した場合、vNIC2 が vNIC1 になります。 vNIC1 と vNIC2 の両方に対してポリシーを手動で作成していた場合は、正しいポリシーが vNIC に維持されるように、強制されるポリシーも変更されます。

- vNIC は、以下の場合に VM ツリーに表示されます。
  - VM に対して複数の vNIC が構成されている場合。
  - VM に対して構成された vNIC が 1 つ残っていて、その vNIC にポリシーが適用されている場合。

これは、当初は VM に対して複数の vNIC が構成されていて、それぞれに固有のポリシーが設定されていましたが、そのうち 1 つを除くすべての vNIC が削除されたことを示します。 このような状況でも引き続き、残りの vNIC のポリシーを編集または削除できます。

vNIC ポリシーは、所属する VM のポリシーより上に、定義した順に表示されます。

- vNIC ポリシーは、所属する VM のポリシーの後に強制されます。
- VM ツリーで VM を選択すると、その VM に属する vNIC のポリシーが読み取り専用として表示されます。

- VM ツリーで vNIC を選択すると、その vNIC のポリシーが表示され、そのポリシーを編集できます。その他のポリシーはすべて読み取り専用として表示されます。他の vNIC のポリシーは表示されません。
- 規則ベースの観点から見ると、vNIC ポリシーは他のポリシー タイプと同じように動作します。
- VM ツリーで vNIC が選択されている場合、その vNIC のポリシーを編集できます。VM が選択されている場合、vNIC ポリシーは灰色表示になり、編集できないことを示します。
- 保護されていない vNIC については、vNIC ヘッダが表示されます。規則情報の代わりに次のメッセージが表示されます。“This interface is configured to bypass firewall enforcement.”

vNIC 毎ポリシーが有効な場合、[Apply Policy] 表では vNIC 構成が以下のように表されます。

- vNIC は [Apply Policy] 表の行として表示されます。vNIC 毎ポリシーが無効な場合、または VM に複数の vNIC が含まれない場合、表には VM の情報が通常どおり表示されます。[Apply Policy] 表の詳細については、59ページの「[vGW シリーズのファイアウォール モジュールの理解](#)」を参照してください。
- VM ツリーで VM を選択すると、その VM のポリシーが表示されます。各 vNIC の表エントリはありますが、“(no rules)” と表示されます。
- 各 vNIC はそれぞれ固有のポリシーを持ちます。1 つを除くすべての vNIC が VM から削除された場合は、残りの vNIC が表に表示されます。そのポリシーを編集または削除できます。



**注:** いずれかの vNIC、または vNIC を含むグループに対して構成されたポリシーがある場合、vNIC 毎ポリシー機能を無効にできません。まずそれらのポリシーを削除する必要があります。

個々の vNIC に対する規則は、ファイアウォール モジュールの [Manage Policy] タブを使用して、他のポリシー規則と同じように追加します。

以下に示す手順では、次の例のポリシーを定義する方法について説明します。ファイアウォール ポリシー規則の構成方法の詳細については、59ページの「[vGW シリーズのファイアウォール モジュールの理解](#)」を参照してください。

この例は、vNIC 毎ポリシー機能が有効であることを前提とします。vNIC 毎ポリシーを有効にする方法の詳細については、148ページの「[vGW シリーズの vNIC 毎ポリシー機能の構成](#)」を参照してください。この例では、MIS-Fileserver という VM をファイル サーバーとして使用していて、その VM 上にある次の 3 つの vNIC のそれぞれに対して異なるポリシーを構成しようとしています。

- vNIC1 (MIS-Fileserver-vNIC1) はネットワーク接続専用の vNIC で、そのポリシーではプロトコル指定によって HTTPS および SSH トラフィックを許可する必要があります。
- vNIC2 (MIS-Fileserver-vNIC2) はデータ ストレージ機能のリンクに使用するため、そのポリシーでは iSCSI プロトコルを許可します。
- vNIC3 (MIS-Fileserver-vNIC3) は管理に使用し、SNMP プロトコルのトラフィックを許可します。

これらの vNIC のポリシーを構成するには、以下の手順に従います。

1. vGW セキュリティ デザイン VM で、ファイアウォール モジュールを選択します。
2. VM ツリーで MIS-Fileserver VM を探し、展開して vNIC を表示します。
3. vNIC1 を選択します。

vNIC を選択すると、そのポリシーの画面が表示されます。このポリシーの名前は「vNIC Policy for MIS-Fileserver-vNIC1」です。

4. [Global Policy] 行の下に [vNIC Policy for MIS-Fileserver-vNIC1] というラベルの付いた行があり、そこにこの vNIC のポリシー規則を入力できます。

[Add] をクリックします。

5. 規則の [Sources] 列は [Any] のままにします。
6. 規則の [Protocols] 列で、[Any] をクリックしてプロトコルのリストを表示します。[Filter] ボックスに https と入力します。リストが「https (443/tcp)」までスクロールします。これを選択して右向き矢印をクリックし、[Selected Protocols] ボックスに移動します。

- a. [Filter] ボックスに https と入力します。

[Filter] ボックスに ssh と入力します。リストが「ssh (22/tcp)」までスクロールします。

- a. [ssh (22/tcp)] を選択して右向き矢印をクリックし、[Selected Protocols] ボックスに移動します。

7. [Filter] ボックスに ssh と入力します。リストが「ssh (22/tcp)」までスクロールします。これを選択して右向き矢印をクリックし、[Selected Protocols] ボックスに移動します。

vNIC 毎ポリシーが有効な場合は、[Apply Policy] 表に、vNIC のポリシー状態を示す追加の列が表示されます。

関連項目    • 3ページのvGW シリーズの理解

## vNIC 毎ポリシーとスマート グループの理解

vGW セキュリティ デザイン VM の設定モジュールの [Installation] セクションによって vNIC 毎ポリシー機能を有効にした場合、個々の vNIC をスマート グループに追加できます。スマート グループを構成すると、そのグループのメンバーシップを VM 全体（つまり、VM のすべてのインターフェース）に適用するか、ロジックが当てはまる vNIC（たとえば、そのインターフェースがポート グループに属するか、または VLAN に関連付けられているか）のみに適用するかを指定できます。この情報を構成するには、[Advanced Attributes] を選択します。vNIC のスマート グループを構成するオプションは、vNIC 毎ポリシー機能が有効な場合にのみ表示されます。XREF を参照してください。

グループを構成した後、そのグループをテストできます。[Test] をクリックすると、テスト結果として VM 名だけでなく vNIC 拡張子も示されます。

以下のスマート グループ属性を使用して、vNIC を含むグループを構成できます。これらの属性は全体として VM に関係しません。

表13: vNIC 毎ポリシーが有効な場合の vNIC のスマート グループ属性

スマート グループ属性の定義	コメント
vf.firewall	
vf.group	
vf.has_installed_group_policy	
vf.has_installed_policy	
vf.monitored	
vf.secured	
vf.secured_active	
vf.vmsafeconfig	
vi.host.vmkernel.isolated.vlan	
vi.host.vmkernel.isolated.vswitch	
vi.ip4	
vi.numvnic	
vi.pg_security.forgedtransmits	
vi.pg_security.macchanges	

表13: vNIC 毎ポリシーが有効な場合の vNIC のスマート グループ属性 (続き)

vi.pg_security.promiscuous
vi.portgroup
vi.portgroup.all
vi.pvlan
vi.pvlan.all
vi.vlan
vi.vlan.all
vi.vmsafe_configured
vi.vmsafe_dvfilter
vi.vmsafe_initfailmode
vi.vswitch

174ページの表15 に示す属性を使用して、スマート グループを定義します。スマート グループ エディタには基本と詳細の 2 つのモードがあります。基本モードでは、一対多の属性を選択し、[All] または [Any] の制約を割り当てることができます。規則を追加するには、[+] 記号をクリックします。詳細モードでは、vNIC のスマート グループを構成できます。

1. vGW セキュリティ デザイン VM の設定モジュールの [Security Settings] セクションで、[Groups] サブセクションを選択します。
2. 表示画面で [Add Smart Group] をクリックします。
3. 画面の上部にある [Advanced] をクリックして、vNIC グループ オプションを表示します。
4. [Add Group definition] ペインで、スマート グループの名前を入力します。この例では、Apache Web Servers と入力します。
5. [Enable vNIC membership] をクリックして、グループのメンバーシップが VM ではなく vNIC に関係することを指定します。
6. [Matches] セクションで、[All] オプション ボタンを選択します。
7. 下向き矢印をクリックして、属性のリストを表示します。属性として [vi.name] を選択し、[Contains] を選択して、www と入力します。
8. 行の最後にある [+] 記号をクリックして、別の行を表示します。
9. 属性として [vf.application] を選択し、[Contains] を選択して、www. と入力します。
10. [Group Attributes] で [Policy Group] を選択し、このグループにポリシーを関連付けできるようにします。



- 11. [Priority] レベルとして [Medium] を選択し、[Precedence within Level] で 2 の優先度を割り当てます。
- 12. [Manual] を選択します。

これにより、ファイアウォール モジュールの [Apply Policy] タブを使用してこのグループにポリシーを適用できます。

- 1. グループの名前を指定し、その属性を構成します。
- 2. [Enable vNIC membership] をクリックして、グループのメンバーシップが VM ではなく vNIC に関係することを指定します。
- 3. [Test] をクリックし、作成した構成の結果を表示します。

スマート グループ ロジックが当てはまる vNIC が、VM 名 + vNIC の形式で表示されます。

VM ツリーでスマート グループを表示し、ネストされた vNIC を含む VM を表示したとき、そのグループに属する vNIC (そのグループのロジック条件を満たす vNIC) は通常どおり表示されます。 そのグループに属さない vNIC は灰色表示されます。

vNIC が保護されているかどうかは、VM のすべての vNIC について通常どおり示されます。

関連項目   • [3ページのvGW シリーズの理解](#)

設定モジュールを使用した vGW シリーズ管理者の定義

異なるカテゴリの IT スタッフ メンバーがさまざまな目的で vGW セキュリティ デザイン VM のインターフェースにアクセスできるようにしなければならない場合があります。たとえば、ネットワーク エンジニアがネットワーク統計情報を利用し、セキュリティ エンジニアがポリシーを配備するような場合がその一例です。このような要件に対応するため、vGW シリーズには組み込みのユーザー タイプがいくつか用意されています。

管理者アカウントを作成するには、設定モジュールの [vGW Application Settings] セクションにある [Administrators] を選択します。ユーザーの名前、タイプ、権限、および認証を指定します。

システムにログインしたユーザーのタイプに基づいて、この画面には異なるメニューが表示されます。Global Admin ユーザーがログインしたときは、新しいユーザーを追加できます。その他のユーザーは、新しい管理者を追加しようとすると、単に [Change My Password] ダイアログ ボックスが表示されます。このダイアログで、自分自身の新しいパスワードを入力できます。 各種特権レベルについては、 [155ページの表14](#)を参照してください。

表14: vGW シリーズ管理者

Global Admin	最も高いシステム特権レベル (新しい管理者の追加権限など) を持つ管理者。 グローバル管理者は、ファイアウォールのインストールやアンチウィルスの構成など、製品のすべての操作を実行できます。 たとえば、ポート グループや VM を選択して保護ネットワークに追加または削除できます。
--------------	---

表14: vGW シリーズ管理者 (続き)

VM Admin	<p>ポリシーおよび設定の変更権限を持つ管理者。このタイプの管理者には、IDS を含むファイアウォール セキュリティ ポリシーの変更、アンチウィルスの構成、および VM イントロスpekションおよびコンプライアンスの構成が許可されます。</p> <p>また、VM 間トラフィックのミラーリングを構成することもできます。これは、外部検査デバイスを使用した規則を構成できることを示します。</p> <p>さらに、VM Admin 管理者にファイアウォール ポリシーのインストール特権を与えることも可能です。そうすると、セキュリティ ポリシーを変更する特権を持った管理者がポリシーを変更して保存した後に、VM Admin 管理者がそのポリシーを配布できます。</p>
Network Monitoring	<p>すべてのネットワーク関連画面（たとえば、統計情報やグラフなど）、メイン モジュールのすべてのタブ（[Status] や [Events and Alerts] など）、およびログを表示できる管理者。このタイプの管理者は、設定モジュールの画面は変更できませんが、IDS のアラート（IDS が構成されている場合）とアンチウィルス スキャンは表示できます。また、VM イントロスpekションとコンプライアンスについては、結果の表示はできますが変更はできません。</p>

関連項目    • [3ページのvGW シリーズの理解](#)

## vGW シリーズ管理者の認証に関する Active Directory のセットアップ

vGW シリーズの管理者認証に必要な情報を vGW セキュリティ デザイン VM データベースにローカルに保存する代わりに、Active Directory (AD) を使用して管理者を認証できます。この場合、管理者は自分の Active Directory 資格情報を使用して vGW セキュリティ デザイン VM にログインします。vGW シリーズは Active Directory にその資格情報を照会し、設定に基づいて、vGW セキュリティ デザイン VM へのログインを許可するか、そのユーザーのアクセスを拒否します。

[Default Search Base] は顧客のインストールごとに固有であり、dc=domain-section-1, dc=domain-section-2（たとえば、dc=corp, dc=com など）の形式をとります。

vGW シリーズが Active Directory と連携するようセットアップするには、以下の手順に従います。

- Active Directory サーバーの名前（または IP アドレス）を定義します。
- 適切なポートを設定します。デフォルトでは、ポート TCP 636 (LDAPS) が使用されます。ただし、389 LDAP+STARTTLS を使用したり、カスタム ポートを構成することもできます。  
vGW セキュリティ デザイン VM からサーバーまでのこのポートのアクセスがネットワークで有効になっていることを確認します。
- 名前または IP アドレス、ポート、およびデフォルト検索ベースを選択したら、[Test] または [Save] をクリックして、通信相手の検証と今後すべての暗号化通信に使用されるフィンガープリントを表示します。
- 構成したサーバーのルックアップ プロセスによって認証されるユーザーまたはグループを作成します。
  - 設定モジュールの [vGW Application Settings] セクションを選択し、[Administrators] を選択します。

- b. 管理者を追加します。認証タイプを [Internal]、[AD Individual User]、[AD Group] のいずれかに設定します。
- [AD Individual User] の場合、そのアカウントは AD 資格情報によって認証され、定義された vGW シリーズの設定に従ってすべての特権が適用されます。
  - [AD Group] の場合は、AD 内の既存のグループの名前が使用され、それに特権が割り当てられます。ルックアップによってユーザーが認証され、AD グループのメンバーであるかどうかを確認されます。AD グループのメンバーである場合、vGW シリーズの適切な特権が付与されます。

関連項目    • 3ページのvGW シリーズの理解

## vGW シリーズ環境で使用する新しいマシンの定義

このトピックでは、設定モジュールの [Applications Settings] セクションの [Machines] セクションを使用して vGW シリーズ システムに新しいマシンを定義する方法について説明します。[Machines] セクションでは、自動的に検出された VM に対して使用される設定も編集できます。

vGW シリーズでトラフィック情報を関係付けるには、ホストの IP アドレスが必要です。通常は、VMware Tools を使用して IP アドレスを取得できます。システムに VMware Tools がインストールされていない場合は、マシンをクリックして IP アドレス フィールドを編集することにより、手動で IP アドレスを定義できます。

[Unmonitored Machines] は、手動で追加された外部物理マシンであるか、または vCenter インベントリには表示されるものの vGW シリーズによって直接監視/保護される vSwitch 上にはない仮想マシンです。

このエリアで重要な物理ホストを追加すると、それらがネットワーキング レポートに表示されるので、便利です。このセクションで定義したホストは、ネットワーク表で、IP アドレスではなくホスト名によって識別されます。また、このセクションで定義したホストをファイアウォール ポリシー エディタで使用することもできます。監視対象外マシンをユーザー定義グループに含めることも可能です。

ネットワーク レポートのために VM ツリーで外部マシンを選択した場合は、その外部マシンのトラフィックのみが報告されます。これは、それが vGW シリーズからアクセスできる唯一のトラフィックであるためです。



注: マシン名をクリックして選択すると、[Edit Machine] ダイアログ ボックスにそのホストに関する詳細 (VMsafe 保護ステータスなど) が表示されます。カーネルへの接続に失敗したときの vGW シリーズの動作を変更できます (failopen または failclosed)。

関連項目    • 3ページのvGW シリーズの理解

## 高可用性の使用

---

vGW シリーズは、vGW セキュリティ デザイン VM と vGW セキュリティ VM の両方について高可用性をサポートしています。 詳細については、以下のトピックを参照してください。

- [195ページのvGW シリーズの高可用性ソリューションの理解](#)
- [196ページの高可用性のためのセカンダリ vGW セキュリティ デザイン VM のインストール](#)
- [197ページの高可用性のためのセカンダリ vGW セキュリティ VM のインストール](#)
- [198ページのvGW シリーズのフォールト トレランスのサポートの理解](#)

関連項目    • [3ページのvGW シリーズの理解](#)

## vGW シリーズの E メールおよびレポート アプリケーション設定の構成

---

設定モジュールの [vGW Applications Settings] の [E-Mail and Reporting] セクションを使用して、E メール サーバーとアカウントの情報を構成できます。 この情報は、ステータス メッセージ、ログ メッセージ、およびレポートを配信するために vGW シリーズ全体で使用されます。

vGW セキュリティ デザイン VM のインストール中に、自動レポートを生成するために必要なパラメータを構成できます。

これらのパラメータをまだ構成していない場合、または設定を変更したい場合には、以下の手順に従います。

1. 設定モジュールから、[vGW Application Settings] の [E-Mail and Reporting] を選択します。
2. 新しい設定を入力します。

E メール設定と構成パラメータの説明を以下に示します。

SMTP Server-E メールを送信するサーバーのホスト名または IP アドレス。

SMTP Port-メール サーバーによって使用されるポート（一般に使用されるのは 25、暗号化の場合は 465）。

Authenticate-メール サーバーへの認証が必要な場合は、このオプションを選択します。

TLS Authenticate-メール サーバーで TLS 暗号化が使用される場合は、このオプションを選択します。

SMTP-認証が必要な場合は、このユーザー アカウントを使用します。

E-mail From-E メール メッセージの差出人フィールドに表示されるテキスト。

E-mail To-E メール メッセージの宛先フィールドに表示されるテキスト。



ヒント: パラメータの変更を保存する前に [Test Mail Server] をクリックして、メール サーバー構成のエラーをトラブルシューティングできます。

レポート モジュール設定の構成パラメータは以下のとおりです。

Default e-mail From-デフォルトで E メール メッセージの差出人フィールドに表示されるテキスト。

Mail Subject -レポート モジュールによって送信されるメッセージの件名行に挿入するテキスト。

Mail Content -メッセージの本文に挿入するテキスト (レポート自体は PDF ファイルとして添付されます)。

- 関連項目
- [3ページのvGW シリーズの理解](#)
  - [35ページのvGW シリーズの vGW セキュリティ デザイン VM の理解](#)
  - [36ページのvGW セキュリティ VM の理解](#)



## vGW シリーズのセキュリティ設定

- [vGW シリーズのセキュリティ設定の理解 161ページ](#)
- [vGW シリーズの設定モジュールを使用したグローバル設定の構成 162ページ](#)
- [vGW セキュリティ VM 設定の理解 163ページ](#)
- [vGW シリーズのアンチウィルス設定の理解と構成 165ページ](#)
- [IDS 設定の理解と構成 166ページ](#)
- [IDS シグネチャ設定の理解と構成 168ページ](#)
- [vGW シリーズのセキュリティ アラート設定の理解 169ページ](#)
- [vGW シリーズでのプロトコルのサポートの理解 170ページ](#)
- [vGW シリーズのグループ設定の理解 170ページ](#)
- [vGW シリーズのスマート グループの理解と使用 172ページ](#)
- [vGW シリーズのネットワーク設定の理解 180ページ](#)
- [vGW シリーズの SRX ゾーン設定の理解 181ページ](#)

### vGW シリーズのセキュリティ設定の理解

---

vGW セキュリティ デザイン VM の設定モジュールの [Security Settings] セクションでは、配備した vGW シリーズの中核機能を制御します。セキュリティ ポリシーに使用する各種オブジェクト（グループやネットワークなど）を定義し、IPv6 や非 IP トラフィックなどの情報を処理するときの動作を指定できます。また、[Security Settings] セクションで IDS 設定を制御することもできます。[Security Settings] セクションには配備した vGW シリーズのさまざまな部分の構成がまとめて表示されるため、それらを 1 か所で構成または変更することが可能です。

- 設定モジュールの [Security Settings] セクションには、以下のセクションがあります。
- Global

[162ページの「vGW シリーズの設定モジュールを使用したグローバル設定の構成」](#)を参照してください。

- Security VM Settings

[125ページの「vGW シリーズの設定モジュールの理解」](#)を参照してください。

- AV Settings

165ページの「vGW シリーズのアンチウィルス設定の理解と構成」を参照してください。

- IDS Configuration

166ページの「IDS 設定の理解と構成」を参照してください。

- IDS Signatures

166ページの「IDS 設定の理解と構成」を参照してください。

- Alerting

169ページの「vGW シリーズのセキュリティ アラート設定の理解」を参照してください。

- Protocols

「vGW シリーズのプロトコル設定の理解」を参照してください。

- Groups

170ページの「vGW シリーズのグループ設定の理解」を参照してください。

- Networks

180ページの「vGW シリーズのネットワーク設定の理解」を参照してください。

- SRX Zones

203ページの「vGW シリーズおよび Junos SRX シリーズのセキュリティ ゾーン」を参照してください。

関連項目    • 3ページのvGW シリーズの理解

## vGW シリーズの設定モジュールを使用したグローバル設定の構成

vGW セキュリティ デザイン VM の [Global] 設定画面では、外部検査デバイス、外部ログイン、グローバル設定規則、および NetFlow 構成を定義できます。

[Global] 設定画面には以下のペインがあります。

- External Inspection Devices – このペインには、さらなる分析のためにトラフィックを送信する宛先のデバイス（侵入検知システムやネットワーク アナライザなど）の名前と IP アドレスを入力できます。この外部検査デバイスでは、GRE トンネルを終端できる必要があります。デバイスにトラフィックを送信するには、ポリシー規則を定義する必要があります。

この構成はトラフィックを外部デバイスにミラーリングします。つまり、トラフィックが許可されるか拒否されるかは関係しません。トラフィックを許可するか拒否するかはポリシーの後続の規則で決定する必要があります。アクション フィールドで [duplicate] が指定されていて、ログへの記録も構成されている場合、ミラーリングされたトラフィックはログに表示されます。

サードパーティ製品を使用する場合は、検査およびリダイレクトするトラフィックのタイプに対して異なる規則を作成します。

- Global Settings Rules – 4 種類のトラフィックについて、vGW セキュリティ VM ファイアウォールでの処理方法を指定できます。デフォルトのファイアウォール構成では、IPv6 および非 IP トラフィック（IPX など）はドロップされます。マルチキャストとブロードキャ



ストは、グローバルに許可するか（デフォルト）、このペインでの構成に従ってドロップできます（トラフィックをログに記録するオプションもあります）。マルチキャストのログオプションの設定によってログトラフィックがグラフから排除されることはありません。この設定は、該当するトラフィックの接続ログを [Logs] 画面に表示するかどうかを制御します。

- External Logging - vGW シリーズは、サードパーティ製 Syslog サーバーへのログの送信をサポートしています。外部サーバーへのログ送信機能はこのペインで有効または無効にします。この機能を有効にした場合、ログファイアウォール規則と一致するすべてのトラフィックが vGW シリーズのログに書き込まれます。また、送信先の Syslog サーバーにも書き込まれます。Syslog 形式をカスタマイズすることも可能です。



**ヒント:** 設定モジュールの [Security VMs] セクションを使用して、ホストの個別の vGW セキュリティ VM でグローバル構成をオーバーライドできます。

- NetFlow Configuration - このペインの設定を有効にして IP アドレスとポートを選択することにより、すべての接続フロー情報を NetFlow バージョン 9 によって送信できます。ポート 2055 と 9990 ~ 9999 が一般に使用されます。NetFlow と Syslog はどちらも、Juniper Networks STRM と互換性があります。



**ヒント:** 設定モジュールの [Security VMs] セクションを使用して、ホストの個別の vGW セキュリティ VM でこの構成をオーバーライドできます。

- Infrastructure Configuration Enforcement -- vGW セキュリティ VM と VMware VMsafe 間の通信には特殊なネットワークが必要となります。このネットワークには、VMsafe 通信プロセスの一部でないゲスト VM (VM) は接続しないことが望まれます。このオプションを使用すると、誰かがこのネットワークに VM を接続した場合、セキュリティ強化のためにその VM を切断できます。

関連項目    • [3ページのvGW シリーズの理解](#)

## vGW セキュリティ VM 設定の理解

vGW セキュリティ デザイン VM の設定モジュールの [Security VMs Settings] セクションでは、配備したすべての vGW セキュリティ VM の設定を 1 か所に表示できます。

この画面から、個々の vGW セキュリティ VM を選択してその構成を変更したり、高可用性のためのセカンダリ vGW セキュリティ VM を作成したり、グローバル設定をオーバーライドしたりすることも可能です。



**ヒント:** メイン モジュールの [Status] セクションからこの画面に移動することもできます。そのためには、[Status of Security VMs] ペインで vGW セキュリティ VM の行をクリックします。

この画面の上の部分にある [Security VMs] ペインには、配備された各セキュリティ VM を行とする表があり、以下の情報が表示されます。

- セキュリティ VM が配備されている ESX/ESXi ホストのアドレス
- セキュリティ VM が保護している VM の数
- 高可用性が構成されているかどうか
- ネットワーク監視が有効かどうか
- NetFlow が構成されているかどうか
- Syslog が構成されているかどうか
- vGW アンチウィルスが有効かどうか
- vGW セキュリティ VM のバージョン

vGW セキュリティ デザイン VM の構成に関する詳細情報を表示してその設定を再構成できるペインを表示するには、vGW セキュリティ VM の行をクリックします。

表示されたペインにある以下のタブを使用して vGW セキュリティ VM の固有の設定を構成することにより、グローバル設定をオーバーライドできます。

- VM Settings - このペインには、この vGW セキュリティ VM の構成情報（IP アドレス、管理インターフェース モード、ネットワーク マスク、デフォルト ゲートウェイなど）が表示されます。

また、高可用性ペインも表示されます。このペインから、高可用性のためのセカンダリ vGW セキュリティ VM を構成できます。詳細については、[197ページの「高可用性のためのセカンダリ vGW セキュリティ VM のインストール」](#)を参照してください。

- Network Monitoring.



注: [Network Traffic Monitoring] と [NetFlow Configuration] の設定は互いに無関係です。

- Network Traffic Monitoring -- デフォルトでは、すべての vGW セキュリティ VM から vGW セキュリティ デザイン VM にネットワーク トラフィック監視データが送信されます。ほとんどの場合、ネットワーク トラフィック情報を収集することは有用です。この情報は vGW シリーズのネットワーク モジュールに表示されます。

ファイアウォールによる VM の保護を実装することだけを目的とする場合は、この画面でネットワーク監視を無効にすることにより、全体的なシステム パフォーマンスを向上させることができます。他の vGW セキュリティ VM でこのオプションを有効のままにすると、それらの vGW セキュリティ VM に関するトラフィック統計情報の収集は続行され、ネットワーク モジュールの画面に引き続きその情報が表示されます。

- NetFlow Configuration - この vGW セキュリティ VM の NetFlow を有効または無効にできます（これらの設定は、NetFlow がグローバルに有効にされていない場合には変更できません）。

NetFlow が有効な場合、この vGW セキュリティ VM から、設定モジュールの [Global] セクションで指定したものと異なる NetFlow コレクタに NetFlow データを送信するよう

指定できます。異なる NetFlow コレクタにレコードを送信するには、[Override global netflow configuration] をオンにして NetFlow コレクタのアドレス情報を指定します。

- Console Monitoring - このオプションを有効にすると、vGW シリーズをハイパーバイザ コンソールに接続してシステムの入出力トラフィックを監視し、不適切なアクティビティが発生していないことを確認できます。
- IDS - この vGW セキュリティ VM の IDS エンジンを実効または無効にできます また、コンソールの IDS 検査をオンにすることもできます。
- Syslog - NetFlow と同様に、グローバルな Syslog 構成をオーバーライドして、使用する送信先 Syslog サーバーを選択できます。そのためには、この vGW セキュリティ VM で使用するサーバーの IP アドレス、ポート、およびトランスポート プロトコルを指定します。
- AntiVirus - この vGW セキュリティ VM の vGW アンチウイルスを実効または無効にできます この vGW セキュリティ VM によって保護されているすべての ESX/ESXi ホストを vGW アンチウイルス保護の対象外にする場合は、このタブを使用して個々の ESX/ESXi ホストの vGW アンチウイルス保護を実効にできます。
- Updates - このタブを使用して vGW セキュリティ VM を更新できます。更新の詳細については、183ページの「[vGW シリーズの更新設定の理解](#)」を参照してください。
- Support - このタブでは、デバッグ メッセージを生成するデバッグ フラグを実効にし、診断目的で Juniper Networks サポート チームに送信するログを収集できます。また、このタブから vGW セキュリティ VM を再起動することもできます。

- 関連項目
- [3ページのvGW シリーズの理解](#)
  - [35ページのvGW シリーズの vGW セキュリティ デザイン VM の理解](#)

## vGW シリーズのアンチウイルス設定の理解と構成

このトピックでは、vGW アンチウイルス設定とその構成方法について説明します。このトピックを読む前に、75ページの「[vGW シリーズのアンチウイルス構成の概要](#)」をお読みください。

vGW セキュリティ デザイン VM では、vGW アンチウイルス機能 (vGW Endpoint など) の構成やインストールが簡便に行えるようになっています。

vGW アンチウイルスの設定を構成するには、設定モジュールの [AntiVirus Settings] セクションを使用します。[AntiVirus Settings] 画面では、アンチウイルスの有効化、シグネチャ データベースの更新頻度の設定、vGW Endpoint のダウンロードを行うことができます。

また、ステータス画面に詳細情報が表示され、[About Juniper vGW Endpoint] ボックスにバージョンとビルドの情報が表示されます。

vGW Endpoint は保護される各 VM で実行されます。このソフトウェアは、vGW セキュリティ VM との通信、ファイルへのアクセスの監視、アンチウイルス ポリシーの強制、ユーザーへのステータスの表示を担当します。

アンチウイルスを実効にすると、新しいシグネチャ ファイルはダウンロードされなくなり、オンデマンド スキャンも実行されません。また、vGW セキュリティ VM によってアンチウィル

ス モジュールはロードされず、vGW セキュリティ VM と vGW Endpoint との通信も行われません。

vGW アンチウイルス設定を有効にして構成するには、以下の手順に従います。

1. [AntiVirus Enabled] ボックスをオンにします。
2. vGW アンチウイルス シグネチャ データベースの自動更新を有効にするには、[Auto Update] セクションで以下のように操作します。
  - a. [Enabled] を選択します。
  - b. アンチウイルス シグネチャ データベースを自動的に更新する間隔を分単位で指定します。

このセクションには、現在インストールされているアンチウイルス シグネチャ データベースの日付とバージョンが報告されます。

vGW Endpoint とアンチウイルス スキャン設定を構成するには、以下の手順に従います。

1. vGW セキュリティ デザイン VM が vGW Endpoint との接続が失われたと判断する時間を指定します。
2. 最後に実行したアンチウイルス スキャンが最新と見なされなくなる日数を指定します。

このペインから vGW アンチウイルスを無効にできます。vGW アンチウイルスは有効なままにして、アンチウイルス シグネチャ データベースの自動更新を停止する場合は、自動更新を無効にします。

vGW Endpoint の最新バージョンをダウンロードするには、[Download] をクリックします。ダウンロード セクションには最新の vGW Endpoint のバージョンと日付が示されるので、初期ダウンロード以降に再びダウンロードする必要があるかどうかを判断できます。

ダウンロードした vGW Endpoint を起動スクリプトから起動したり、組織で使用するソフトウェア配布パッケージに含めたいことがあります。また、場合によっては、vGW Endpoint をファイル サーバーに配置したいこともあります。vGW Endpoint の詳細については、[86ページの「vGW Endpoint の理解とインストール」](#)を参照してください。

- 関連項目
- [89ページのvGW シリーズのオンデマンド アンチウイルス スキャンの構成](#)
  - [83ページのvGW シリーズのオンアクセス アンチウイルス スキャンの構成と VM への vGW Endpoint のインストール](#)
  - [3ページのvGW シリーズの理解](#)

## IDS 設定の理解と構成

vGW セキュリティ デザイン VM の設定モジュールの [Security Settings] セクションでは、IDS 設定と IDS 更新を構成できます。IDS 更新を取得するには、IDS ライセンスを購入してインストールする必要があります。

IDS 情報は以下のペインで構成します。

- IDS Settings - IDS サポートを有効にするには、[Enable IDS] チェックボックスをオンにします。IDS パラメータも指定できます。各種ポートを使用して HTTP および SSL トラフィックを通過させることができます。運用環境に基づいて、どのポートを HTTP または SSL として分析するかを指定できます。

- IDS Updates - IDS シグネチャの更新を以下のように構成できます。
  - [Auto Update] を有効にして vGW シリーズ サーバーからの更新をローカル環境に自動的に適用するか、更新をダウンロードした後に手動で適用するかを選択できます。

- カスタム シグネチャを作成または定義して vGW シリーズに手動でインポートすることも可能です。

関連項目 [71ページのIDS 設定の構成とアクティビティの表示](#)

- vGW セキュリティ デザイン VM を使用した vGW シリーズの IDS カスタム シグネチャの構成
- [168ページのIDS シグネチャ設定の理解と構成](#)

## IDS シグネチャ設定の理解と構成

このトピックでは、IDS シグネチャをどのように管理するかを制御する設定の構成方法について説明します。この構成には、設定モジュールの [IDS Signatures] セクションを使用します。

カテゴリ名の横にあるアイコンをクリックして緑のチェックマークまたは赤の x を選択することにより、カテゴリ全体を有効または無効にできます。

カテゴリ内の個々のシグネチャを有効または無効にする場合は、カテゴリをクリックしてから関連するシグネチャを有効または無効にします。また、規則のカテゴリをクリックして規則をクリックすることにより、シグネチャの優先度レベル（高、中、低）を変更することもできます。ここには、使用される特定のシグネチャも表示できます（[Show Raw Signature] を選択）。

vGW セキュリティ デザイン VM の設定モジュールの [IDS Signatures] セクションを使用して、IDS カスタム シグネチャを手動でアップロードできます。[IDS Signatures] 画面には以下の情報が表示されます。

- [Custom Signatures]（すでにアップロードされている場合）。[Custom Signatures] セクションには、カスタム シグネチャを手動でアップロードするまでエントリはありません。
- [Subscription Signatures] には、標準の vGW シリーズ IDS 構成に含まれるすべてのシグネチャ カテゴリが表示されます。
  1. カテゴリを有効または無効にするには、カテゴリ名の前のチェックボックスをクリックします。
  2. カテゴリ内の個々のシグネチャを有効または無効にするには、カテゴリ名をクリックします。そのカテゴリに属するすべてのシグネチャを示す画面が表示されます。  
有効にするシグネチャの前のチェックボックスをクリックします。
  3. 個々のシグネチャの情報を提供する [Signature Details] 画面を表示し、それを構成する（たとえば、シグネチャの優先度レベルを変更する）には、以下の手順に従います。
    - a. [Priority] 列で、シグネチャの優先度（[H]、[M]、[L]）をクリックします。[Signature Details] 画面が表示されます。

図 35: [Signature Details] 画面



関連項目 •

## vGW シリーズのセキュリティ アラート設定の理解

このトピックでは、E メールおよび SNMP トラップのアラート設定の構成方法について説明します。このトピックには以下のセクションがあります。

- [E メール アラート設定 169ページ](#)
- [SNMP トラップ設定 169ページ](#)
- [自動構成アラートとマルチキャスト アラート 169ページ](#)

### E メール アラート設定

メール中継サーバーの IP アドレスと送信元および宛先の E メール アドレスを指定することで、E メール アラートを有効にできます。集約時間は、連続する通知の間隔です。

複数の E メール受信者を構成する必要はありません。ただし、4 つのカスタム E メール アラート タグを作成し、それぞれ異なる E メール エイリアスまたは個々の E メール アカウント、またはそれら 2 つの組み合わせを指し示すことができます。これらのカスタム タグはセキュリティ ポリシー エディタで指定できます。

E メール アラートと SNMP トラップの両方を単一の規則で送信するには、標準アラート アイコンを使用します。この場合は、[Recipients Addresses] にリストされた E メール アドレスのみが使用されます。つまり、E メール アラートと SNMP アラートを送信するときにはカスタム タグは使用できません。

### SNMP トラップ設定

SNMP トラップは、バージョン 1 またはバージョン 2 によって設定できます。SNMP サーバーアドレスとコミュニティ文字列を入力する必要があります。ここでも、必要に応じて集約時間（連続するイベント間の遅延）を設定できます。

### 自動構成アラートとマルチキャスト アラート

デフォルトの構成では、自動構成アドレスが検出されたときにアラートが送信されます（[Settings] 画面 -> [Security Settings] -> [Alerting]）。マルチキャストが観察されたときには、アラートは自動的に送信されません（ただし、これは有効にできます）。

- Autoconfig addresses - マシンに IP アドレスが設定されていない場合、またはマシンが DHCP リースを取得できない場合は、デフォルトで 169.254.\*.\* の範囲の自動構成アドレスが使用されます。この設定は多くの場合、構成または DHCP サービスに問題があることを意味します。
- Multicast - 多くのホストがマルチキャスト パケットを使用して自身の存在をネットワーク上にアドバタイズします。また、各ホストが提供しているサービスに関するブロードキャスト情報や構成データも送信されます。この情報は必要でないことが多く、サーバーがこの情報を提供するのとは望ましくない場合があります。また、セキュリティの観点から見て、マシンで使用可能なサービスをアドバタイズすることについても問題があります。

関連項目    • [3ページのvGW シリーズの理解](#)



## vGW シリーズでのプロトコルのサポートの理解

デフォルトでは、プロトコル表には IANA に登録されたすべてのプロトコルが表示されます。この表に、IANA に登録されていないカスタム プロトコルまたはその他のアプリケーション プロトコルを追加できます。追加したプロトコルは、ポートまたはプロトコルではなく名前によってネットワーク レポートに示されます。

また、独自の非 TCP プロトコルや非 UDP プロトコル（GRE や IPsec プロトコルなど）を定義することもできます。カスタム アプリケーション/TCP/8000 ～ 8005 などのプロトコル範囲を定義できます。

プロトコル表には、プロトコルの名前、タイプ（TCP や UDP など）、使用されるポート番号が表示されます。

いくつかのプロトコルをプロトコル グループにまとめて、ファイアウォール ポリシーの作成に使用できます（たとえば、グローバル用、グループ用、個々の VM 用など）。そのためには、[Add] をクリックしてグループの名前を入力し、適切なプロトコルを選択して [Save] をクリックします。

関連項目   • [3ページのvGW シリーズの理解](#)

## vGW シリーズのグループ設定の理解

設定モジュールの [vGW Security Settings] セクションの [Groups] 設定を使用して、各種 vGW セキュリティ デザイン VM モジュールで使用されるリソースのグループを作成できます。グループをコピーすることもできます。

- [vGW グループ タイプ 170ページ](#)
- [グループのコピー 171ページ](#)

### vGW グループ タイプ

vGW シリーズには、以下の 2 つの主要グループ タイプが用意されています。

- 静的グループ。このグループは管理者が手動で作成します。静的グループは、定義された任意のタイプの vGW オブジェクト（ネットワーク、VM、外部物理システムなど）のコレクションとして作成できます。
- スマート グループ。このグループは、管理者が定義した一連のパラメータに基づいて自動的に作成され、vGW シリーズによって動的に維持管理されます。vGW シリーズは、管理者が構成したパラメータに基づいて、vGW シリーズと VMware の両方のオブジェクト データベースを継続的に分析します。定義されたパラメータに一致するオブジェクトがこれらのグループに自動的に挿入（またはグループから自動的に削除）されます。

スマート グループの詳細については、[172ページの「vGW シリーズのスマート グループの理解と使用」](#)を参照してください。

これらのどちらかのタイプのグループをセキュリティ ポリシーに関連付けることができます。ポリシーの関連付けは、グループを定義するときに構成できる [Policy Group] オプションに



よって制御されます。ポリシーが関連付けられていないグループは、VM ツリーの [Monitoring Groups] セクションに表示されます。

グループは以下の場合に使用できます。

- グループに属する VM がネットワーク上でどのように交信しているかは把握しておきたいものの、そのトラフィックは保護しない場合。
- ポリシー グループに自動的にポリシーを適用したい場合。

グループを構成するとき、[Automatic] と [Manual] のどちらかを選択します。どちらを選択するかによって、そのグループをポリシーに割り当てる際のモードが決まります。[Automatic] を選択すると、そのグループのメンバーに対するポリシーの変更が管理者の介入なしに（たとえば、管理者がファイアウォール モジュールの [Apply Policy] タブを使用しなくても）プッシュされます。

適切なグループ構造を作成すると、多くのセキュリティ タスクを自動化できます。詳細については、[172ページの「vGW シリーズのスマート グループの理解と使用」](#)を参照してください。

## グループのコピー

さまざまな理由から（たとえば、既存のグループに関連付けられたポリシーを複製するためなど）、グループを複製したい場合があります。[Security Settings] の [Group] 画面にある [Groups] 表で、既存のグループを選択してコピーできます。

1. vGW セキュリティ デザイン VM で、設定モジュールの [Security Settings] セクションを選択し、[Global] サブセクションを選択します。
2. 表でグループの名前をクリックして、コピーするグループを選択します。
3. [Copy Group] をクリックします。
4. 表示されたダイアログ ボックスで、新しいグループ名を指定します。
5. コピーするグループがポリシー グループの場合に、コピー元グループのポリシーを新しいグループに関連付けるときは、[Keep Policy] をクリックします。
6. スマート グループの場合は、コピー元のスマート グループのロジックを新しいグループに複製するかどうかを選択できます。VM メンバシップを静的グループに変換することも可能です。
  - ロジックを複製する場合は、[Duplicate Smart Group logic] をクリックします。
  - コピーするスマート グループのメンバーを含む静的グループを作成する場合は、[Convert VM membership to static group] をクリックします。
7. [Save] をクリックします。

[Save] をクリックすると、新しいグループが [Groups] 表に追加されます。

コピーとして作成された新しいグループは、コピー元の自動プッシュ プロパティを継承します。ただし、これは実質的に新しいグループなので、最初は手動でプッシュする必要があります。

関連項目    • [3ページのvGW シリーズの理解](#)

## vGW シリーズのスマート グループの理解と使用

- [背景 172ページ](#)
- [スマート グループ 172ページ](#)
- [スマート グループの使用について 172ページ](#)
- [スマート グループの作成について 173ページ](#)
- [スマート グループの定義例 180ページ](#)

### 背景

ほとんどの組織では、仮想化環境は非常に動的です。新しい仮想マシンはテンプレートから簡単に作成でき、仮想スイッチの構成を変更することも可能で、システムが物理ホスト間で移動されることもよくあります。物理的なデータ センターであれば数日または数週間かかる環境変化のサイクルも、仮想データ センターではほんの短時間で起こります。仮想マシン (VM) のクローンの作成、テンプレートからの新しい VM の作成、既存の VM への新しい仮想ハードウェアの追加、既存の VM のネットワーク間の移動などにかかる時間は、仮想化データ センターでは数秒からせいぜい数分です。

このような環境の動的な性質と、IT チームは多くの場合人員不足が常態化しているという事実から、自動的に適応できるセキュリティ ソリューションが求められています。当然のことながら、すべての組織が自社のすべてのセキュリティ ポリシーを自動的に変更したいわけではなく、一部の変更については明示的な承認を得ることが不可欠の要件となります。

### スマート グループ

自動化された動的なアプローチの要求に応えるため、vGW シリーズにはスマート グループ機能が用意されています。スマート グループを使用すると、

- 完全に制御された状態が維持されます。つまり、セキュリティの変更を自動的にかつ即時に適用するか、手動での介入の必要性を知らせるシンプルなアラートを生成することが可能です。
- セキュリティ ポリシーを仮想データ センターの変更に即時に適応させることができます。
- コンプライアンス チェックにより、セキュリティが確実に維持され、リスクがただちに軽減されます。

### スマート グループの使用について

スマート グループを作成するには、1 つ以上の式を定義します。VM がグループに所属するためには、その式の条件を満たす必要があります。スマート グループは動的なので、そのメンバーは急速に変わる場合があります。VM の構成は常に、スマート グループの条件に一致するよう変更される可能性があります。数秒のうちに、VM がスマート グループに追加、またはスマート グループから削除されることもあります。vGW シリーズは、管理者が定義した式に基づいて、vGW シリーズと VMware の両方のオブジェクト データベースを継続的に分析します。指定されたパラメータに一致する VM がスマート グループに自動的に挿入（またはスマート グループから自動的に削除）されます。

スマート グループの定義に使用される動的メンバーシップ パラメータは、以下の 2 か所から取得されます。

- vGW シリーズのスマート グループ属性

vGW シリーズの属性はカテゴリに分類されており、*vf* という接頭辞が付いています。

たとえば、vGW シリーズのイントロスペクション機能を使用して、VM にインストールされているアプリケーションなどの項目を検出できます。

- vCenter の属性

VMware の vCenter は、仮想ネットワーク インターフェースの接続先のポート グループなどの属性を識別します。VMware vCenter 属性には *vi* という接頭辞が付いています。

スマート グループをセキュリティ ポリシーに関連付けることができます。ポリシーの関連付けは、グループを定義するときに使用できる [Policy Group] オプションによって制御されます。

VM を自動的に保護してポリシーの適用を効率化することにより、仮想インフラストラクチャ全体のセキュリティを効率的に確保できます。以下の 2 つの例について考えます。

- VM 管理者が VM の仮想ネットワーク インターフェースを企業の実運用ネットワークに関連付けた結果、その VM があるスマート グループの *vi.portgroup* 属性に一致したとします。この場合、VM はそのグループのメンバーになり、グループのファイアウォール規則が自動的に適用されます。
- 管理者が、特定の VMware リソース プール (*vi.resourcepool* から取得されます) に接続された VM を監視するスマート グループを定義したとします。ある VM 管理者によってこのリソース プールに VM が追加されると、vGW シリーズ管理者の介入なしにセキュリティ ポリシーがただちにインストールされます。

## スマート グループの作成について

スマート グループを作成するには、設定モジュールの [Security Settings] の [Groups] 画面を使用します。〈図を参照してください〉。以下のプロセスは、高いレベルから見たスマート グループの定義方法を示します。

- スマート グループを定義できる [Add Group] ペインを表示します。このペインを表示するには、[Add a Smart Group] ボタンをクリックします。〈図を参照してください〉。
- [Advanced] モードでは、スマート グループの条件を定義する行を必要だけいくつでも追加できます。各行に 1 つの式を設定します。



**ヒント:** 属性の意味、または属性から取得できる値が分からない場合は、行の末尾にある疑問符 ([?]) をクリックします。そうすると、その属性について説明するポップアップ ウィンドウが表示され、データ タイプと有効な値が示されます。

行ごとに以下のものを選択します。

- 属性

属性の一覧については、[174ページの表15](#)を参照してください。

- 比較演算子

たとえば、属性の指定と一致する VM をグループに含めたり、グループから除外したりできます。

- 値

- グループの定義を保存する前に、[Test] ボタンをクリックして、目的の VM がグループに含まれるかどうかを確認します。

[Type] フィールドに応じて以下の値が返されます。

- Boolean: True または False
- Integer: 数値
- String: 自由形式のテキスト文字列
- Multi String: 複数の文字列値がコンマ、セミコロン、スラッシュなどの区切り文字で連結されたもの
- Multi Value: 有効な選択肢をプルダウンから選択

表15: スマート グループ属性

属性名	データ タイプ	説明
vf.antivirus.database.version	文字列値	この VM で使用されているアンチウイルス データベースのバージョン (VM が接続している中央アンチウイルス データベースにインストールされているバージョン)。
vf.antivirus.endpoint.connected	ブール値	この VM が中央アンチウイルス スキャン エンジンに適切に接続しているか。
vf.antivirus.endpoint.enabled	ブール値	この VM に動作可能なアンチウイルス エージェントがインストールされているか。
vf.antivirus.endpoint.version	文字列値	VM にインストールされている Endpoint のバージョン。
vf.antivirus.onaccess.enabled	ブール値	この VM でオンアクセス アンチウイルス スキャンが有効になっているか。
vf.antivirus.quarantine.enabled	ブール値	この VM が、ウイルス ファイルを検疫するよう構成されているか。
vf.app_count_bad	整数	VM 上のアプリケーションのうち「Bad」として分類されているものの数。
vf.app_count_known	整数	VM 上のアプリケーションのうち「Known」として分類されているものの数。
Vf.app_count_unclassified	整数	VM 上のアプリケーションのうち分類されていないものの数。
vf.app_count_unknown	整数	VM 上のアプリケーションのうち「Unknown」として分類されているものの数。

表15: スマート グループ属性 (続き)

属性名	データ タイプ	説明
vf.app.gi.compliant	文字列値	この VM が、選択したゴールド イメージに適合しているか。
vf.app.is.gold.image	ブール値	この VM が、イメージ エンフォーサ比較用のマスター イメージとして定義されているか。
vf.app.matches.gold.image	ブール値	この VM が、設定したゴールド イメージに適合しているか。
vf.app.registry	文字列値	VM のイントロスペクションによって検出された Windows レジストリのレジストリ値。
vf.application	文字列値	VM にインストールされているアプリケーション。
vf.description	文字列	vGW セキュリティ デザイン VM の設定モジュールの [Machines] セクションで定義された、テキスト文字列での VM の説明。
vf.firewall	文字列	この VM が vGW セキュリティ VM であるか。
vf.group	複数文字列	VM が属するすべての vGW グループをコンマで区切って列挙した文字列。
vf.has_installed_group_policy	ブール値	VM にデフォルトでないグループ ポリシーがインストールされているか。
vf.has_installed_policy	ブール値	VM にセキュリティ ポリシーがインストールされているか。
vf.hotfix	複数文字列	VM にインストールされているホットフィックス。
vf.monitored	ブール値	VM が現在 vGW セキュリティ デザイン VM によって監視されているか。
vf.name	文字列	vGW セキュリティ デザイン VM で定義されている名前。
vf.os	文字列	VM にインストールされているオペレーティングシステム。
vf.quarantined	ブール値	この VM が検疫された状態にあるか (つまり、Quarantine Policy グループに属しているか)。
vf.secured	ブール値	VM が現在 vGW セキュリティ デザイン VM によって保護されているか。
vf.secured_active	ブール値	VM が vGW によってアクティブに保護されているか。

表15: スマート グループ属性 (続き)

属性名	データ タイプ	説明
vf.tag	文字列	この VM に関連付けられたタグ (セミコロン区切り)。
vf.type	列挙	マシン オブジェクト タイプ。
vf.virus.infected	ブール値	文字列値
vi.attribute	文字列値	VI の注釈ボックスで定義された属性値。
vi.cluster	文字列	VM を含むクラスター。
vi.datacenter	文字列	VM が収容されている vCenter 内のデータ センター。
vi.deleted	ブール値	この VM がすでに削除されているか。
vi.excfg.copy.disable	ブール値	リモート コンソール機能へのコピー アンド ペーストがこの VM で無効になっているか。
vi.excfg.deviceconnectable.disable	ブール値	この VM が、デバイスを接続できるよう構成されているか。
vi.excfg.deviceedit.disable	ブール値	この VM が、デバイスを接続および削除できるよう構成されているか。
vi.excfg.diskshrink.disable	ブール値	この VM が、仮想ディスクの縮小を禁止するよう構成されているか。
vi.excfg.diskwiper.disable	ブール値	この VM が、仮想ディスクの縮小を禁止するよう構成されているか。
vi.excfg.dragndrop.disable	ブール値	リモート コンソール機能へのコピー アンド ペーストがこの VM で無効になっているか。
vi.excfg.hostinfo.disable	ブール値	この VM がホストのパフォーマンス情報にアクセスできるか。
vi.excfg.log.disable	ブール値	この VM の VM ログ ファイルのサイズが制限されているか。
vi.excfg.log.keep.old	数値	この VM の保存されるログ ファイルの数が制限されているか。
vi.excfg.log.rotatesize	数値	この VM の VM ログ ファイルのサイズが制限されているか。
vi.excfg.paste.disable	ブール値	リモート コンソール機能へのコピー アンド ペーストがこの VM で無効になっているか。

表15: スマート グループ属性 (続き)

属性名	データ タイプ	説明
vi.excfig.remotedisplay.max	数値	この VM のために使用できるリモート コンソールの数。VMware 要塞化ガイドラインでは 1 つに制限することが推奨されています。
vi.excfig.remoteop.disable	ブール値	このゲストでリモート操作が無効になっているか。
vi.excfig.setguiopts.disable	ブール値	リモート コンソール機能へのコピー アンド ペーストがこの VM で無効になっているか。
vi.excfig.vmxfilesize.limit	数値	VM から VMX ファイルへの情報メッセージを制限するために VMX ファイルのサイズが制限されているか。
vi.folder	複数文字列	vCenter 内の VM を含むフォルダ。
vi.host	文字列	VM を収容している ESX/ESXi ホスト。
vi.host.console.ids	ブール値	このハイパーバイザのサービス コンソールに対して vGW IDS 検査が有効になっているか。
vi.host.console.monitor	ブール値	このハイパーバイザのサービス コンソールに対して vGW ネットワーク監視が有効になっているか。
vi.host.lockdown	ブール値	このハイパーバイザ ホストでロックダウン モードが有効になっているか。
vi.host.ntp.enabled	ブール値	このハイパーバイザで Network Time Protocol (NTP) が構成されて有効になっているか。
vi.host.techsupportmode.disable	ブール値	このハイパーバイザ ホストでテック サポート モードが有効になっているか。
vi.host.vmkernel.isolated.vlan	ブール値	このハイパーバイザの vmkernel 管理ネットワークが分離された VLAN 上に存在するか。
vi.host.vmkernel.isolated.vswitch	ブール値	このハイパーバイザの vmkernel 管理ネットワークが分離された vSwitch 上に存在するか。
vi.indep.nonpersist.disk.ct	数値	この VM によって使用される、independent-nonpersistent として構成された（したがって、イントロスペクション スキャンできない）仮想ディスクの数。
vi.ipv4	IPv4 (複数値)	VM 上の既知の IP アドレス。
vi.memory_inspection	ブール値	この VM で VMsafe メモリおよび CPU API が有効になっているか。
vi.name	文字列	vCenter で定義されたこの VM の名前。

表15: スマート グループ属性 (続き)

属性名	データ タイプ	説明
vi.notes	文字列	vCenter でこの VM に添付された自由形式テキストによる注釈。
vi.os	文字列値	vCenter でこの VM に対して定義されたオペレーティング システム。
vi.pg.security.forgedtransmits	ブール値	VM が、偽装 MAC アドレス (VMX で定義されている以外の MAC) を許可するポート グループに接続しているか。
vi.pg.security.macchanges	ブール値	VM が、未知の MAC アドレス (VMX で定義されている以外の MAC) の受け入れを許可するポート グループに接続しているか。
vi.pg.security.promiscuous	ブール値	VM がプロミスキュス ポート グループに接続しているか。
vi.portgroup	文字列値	この VM がアクティブに接続している、仮想スイッチ上のポート グループ。切断されている vNIC のポート グループは含まれません (実行中または一時停止している VM では、これは実際に接続されているポート グループになります。停止している VM では、電源オン時に接続されるポート グループです)。
vi.portgroup.all	文字列値	この VM が接続するよう構成されている、仮想スイッチ上のポート グループ。このリストには、切断されている vNIC のポート グループも含まれます (実行中または一時停止している VM では、これは実際に接続されているポート グループになります。停止している VM では、電源オン時に接続されるポート グループです)。
vi.powerstate	列挙	この VM の現在の電力状態。
vi.pvlan	数値	接続しているポート グループのプライベート VLAN の値。
vi.pvlan.all	数値	この VM で使用されているすべてのプライベート VLAN のリスト。接続状態の vNIC と切断状態の vNIC の両方が含まれます。
vi.numvnic	整数	接続している vNIC の数。
vi.os	文字列	vCenter でこの VM に対して定義されたオペレーティング システム。
vi.pg_security.forgedtransmits	ブール値	VM が、偽装 MAC アドレス (VMX で定義されている以外の MAC) を許可するポート グループに接続しているか。



表15: スマート グループ属性 (続き)

属性名	データ タイプ	説明
vi.pg_security.macchanges	ブール値	VM が、未知の MAC アドレス (VMX で定義されている以外の MAC アドレス) の受け入れを許可するポート グループに接続しているか。
vi.pg_security.promiscuous	ブール値	VM がプロミスキュス ポート グループに接続しているか。
vi.portgroup	複数文字列	接続しているポート グループ。
vi.portgroup.all	複数文字列	VM が使用するよう構成されているすべてのポート グループ。
vi.powerstate	複数值	この VM の現在の電力状態。
vi.resourcepool	文字列	VM がメンバーである、vCenter のリソース プール。
vi.vapp	複数文字列	VM がメンバーである、vCenter の vApp グループ。
vi.vlan	複数值、整数	接続しているポート グループの VLAN。
vi.vlan.all	複数值、整数	すべてのインターフェースの VLAN。
vi.vmci_enabled	ブール値	この VM で VMCI (共有メモリ通信) が有効になっているか。
vi.vmsafe_configured	ブール値	この VM で VMSafe ファイアウォール セキュリティが有効になっているか。
vi.vmsafe_dvfilter	複数文字列	この VM を保護している dvfilter。
vi.vmwaretools.running	ブール値	この VM で VMware Tools が実行されているか。
vi.vmwaretools.uptodate	ブール値	この VM にインストールされている VMware Tools のバージョンが最新であるか。
vi.vnic.count	数値	接続している vNIC の数。
vi.vswitch	複数文字列	VM が接続している vSwitch。

## スマート グループの定義例

スマート グループを定義するには、[174ページの表15](#)に示す属性を使用します。設定モジュールの [Groups] 画面で、[Add Smart Group] をクリックします。〈図〉を参照してください。

エディタには 2 つのモードがあります。デフォルトは基本モードです。基本モードでは、一対多の属性を選択し、[All] または [Any] の制約を割り当てることができます。規則を追加するには、[+] 記号をクリックします。

以下の例では詳細モードを使用します。

1. 設定モジュールの [Security Settings] セクションで、[Groups] サブセクションを選択します。
2. [Add Smart Group] をクリックします。
3. [Add Group] ペインで、スマート グループの名前を入力します。この例では、Apache Web Servers と入力します。
4. [Matches] セクションで、[All] オプション ボタンを選択します。
5. 下向き矢印をクリックして、属性のリストを表示します。属性として [vi.name]、比較演算子として [Contains] を選択し、値として www と入力します。

属性の意味がわからない場合は、行の末尾にある [?] をクリックします。属性のデータタイプと有効な値を示すポップアップ ウィンドウが表示されます。

6. セクションの最後にある [+] 記号をクリックして、別の行を表示します。

この簡単なスマート グループの例では属性を 2 つ使用しますが、行はスマート グループの定義に必要なだけいくつでも追加できます。

7. 属性として [vf.application] を選択し、[Contains] を選択して、www と入力します。
8. [Group Attributes] の下で、[Policy Group] を選択します。
9. [Priority] レベルとして [Medium] を選択し、[Precedence within Level] で 2 の優先度を割り当てます。

関連項目    • [3ページのvGW シリーズの理解](#)

## vGW シリーズのネットワーク設定の理解

設定モジュールの [Networks] セクションを使用して、vGW シリーズのセキュリティ ポリシーで使用するネットワーク オブジェクトを定義できます。ネットワークは IP 範囲またはサブネット マスクによって定義できます。

関連項目    • [3ページのvGW シリーズの理解](#)

## vGW シリーズの SRX ゾーン設定の理解

---

vGW セキュリティ デザイン VM の設定モジュールの [SRX Zones] セクションを使用して、物理 SRX システムとの相互運用性を確立できます。詳細については、[203ページの「vGW シリーズおよび Junos SRX シリーズのセキュリティ ゾーン」](#)を参照してください。

関連項目   • [3ページのvGW シリーズの理解](#)



# vGW セキュリティ デザインのアップライアンス設定

- [vGW シリーズの更新設定の理解 183ページ](#)
- [vGW セキュリティ デザイン VM の手動更新 184ページ](#)
- [バッチ モードでの vGW セキュリティ VM の更新 185ページ](#)
- [vGW シリーズのネットワーク設定の構成 186ページ](#)
- [vGW シリーズのプロキシ設定の構成 186ページ](#)
- [vGW シリーズの時刻設定の構成 186ページ](#)
- [vGW シリーズのバックアップおよびリストア機能の理解 187ページ](#)
- [vGW シリーズのバックアップおよびリストア機能の構成 188ページ](#)
- [vGW シリーズのログ収集の理解 189ページ](#)
- [vGW シリーズのログの表示 190ページ](#)
- [vGW シリーズのサポート設定の理解 190ページ](#)

## vGW シリーズの更新設定の理解

---

vGW シリーズには、アーキテクチャのコンポーネントを更新して新しい保護、バグ修正、およびその他の拡張機能を追加するメカニズムが組み込まれています。設定モジュールの [Appliances Settings] セクションの [Updates] セクションを使用して、vGW セキュリティ デザイン VM および vGW セキュリティ VM を更新します。

- [Security Design vGW Update] ペインには、vGW セキュリティ デザイン VM の更新がチェックされてインストールされた最後の日時が表示されます。更新を手動でチェックするには、[Check for Updates] をクリックします。
- [Update Preferences] ペインを使用すると、Juniper Networks インターネット更新サーバーにある最新のソフトウェアを自動的にチェックできます。
- [Security VM Batch Updates] ペインでは、複数の vGW セキュリティ VM をただちに更新したり、それらの更新スケジュールを設定できます。

関連項目   • [3ページのvGW シリーズの理解](#)

## vGW セキュリティ デザイン VM の手動更新

このトピックでは、vGW セキュリティ デザイン VM をオンラインおよびオフラインで手動更新する方法について説明します。

ここでは、vGW セキュリティ デザイン VM をオンラインで手動更新する手順を示します。この手順を実行するには、vGW セキュリティ デザイン VM から Juniper Networks 更新サーバー (HTTPS - TCP 443) に接続する必要があります。

vGW セキュリティ デザイン VM を手動で更新するには、以下の手順に従います。

1. 適切な資格付与キーが vGW セキュリティ デザイン VM にインストールされていることを確認します。

資格付与キーがなければ、更新を自動でインストールすることはできません。資格付与キーは、製品およびソフトウェア サブスクリプション契約をご購入いただいたときに与えられます。詳細については、を参照してください。

[Settings] -> [vGW Application Settings] -> [Status & License] セクションの順に選択し、資格付与キーを入力します。このエリアでは、vGW セキュリティ デザイン VM の更新ステータスを確認することもできます。

2. 設定モジュールの [Appliance Settings] の [Updates] セクションに移動します。
  - a. [Check for Updates] をクリックして、Juniper Networks 更新サーバーに照会します。  
更新サーバーによって、コンポーネントに必要な更新の有無がチェックされます。
  - b. 更新が存在する場合は、[Update Now] をクリックして変更を適用します。

必要な更新が Juniper Networks サーバーからダウンロードされます。場合によっては、vGW セキュリティ デザイン VM の再起動が必要になります。

コンポーネントの更新はオフラインでも実行できます。Juniper Networks サポートから更新 ISO を入手し、その ISO を仮想マシンにマウントしてから、[Offline Update] を選択します。

オフラインで手動更新を実行するには、以下の手順に従います。

- a. [Security Design vGW Update] ペインの [Available upgrades] セクションで、[Advanced] をクリックします。
- b. Juniper Networks サポート チームから更新 ISO を入手し、その ISO を vGW セキュリティ デザイン VM にマウントします。
- c. [Offline Update] チェックボックスをオンにします。
- d. [Connect Update Media] をクリックします。
- e. [Update Now] をクリックします。先に更新をチェックするには、[Check for Updates] をクリックします。

関連項目    • [3ページのvGW シリーズの理解](#)

## バッチ モードでの vGW セキュリティ VM の更新

このトピックでは、vGW セキュリティ VM をグループとしてバッチ モードで更新する方法について説明します。

vGW セキュリティ VM をバッチ モードで更新するときは、更新をただちに実行するか、スケジュールを設定して後で実行するかを選択できます。

vGW セキュリティ VM をバッチ モードで更新するようセットアップするには、以下の手順に従います。

1. vGW セキュリティ デザイン VM の設定モジュールで、[Application Settings] セクションに移動します。 [Updates] セクションを選択します。
2. [Security VM Batch Updates] ペインで、[Custom Product version] を入力します。
3. 更新する vGW セキュリティ VM のチェックボックスをオンにします。  
すべての vGW セキュリティ VM を一度に選択できます。
4. ESX/ESXi ホストがメンテナンス モードのときに更新を実行する場合は、以下の条件を選択します。
  - Always - この場合、ログは失われません。
  - As needed - カーネル ドライバの更新のみの場合。
  - Never
5. [Start Time] オプション ボタンを使用して、バッチ更新プロセスをいつ実行するかを指定します。
  - バッチ更新プロセスをただちに開始するには、[Now] を選択します。 [Schedule Update] をクリックします。
  - バッチ更新をスケジュールするには、[Later] を選択します。
    - a. 開始日時を入力します。
    - b. 必要に応じて、終了時刻を入力します。  
終了時刻を指定した場合、終了時刻に達したときに実行中の更新は最後まで行われません。 しかし、新しい vGW セキュリティ VM の更新は開始されません。
    - c. 必要に応じて、更新が完了または中止されたときに更新ステータス メッセージを送信する宛先の E メール アカウントを入力します。  
ステータス Eメールの E メール アドレスを指定した場合は、更新済みおよび更新待ちの vGW セキュリティ VM について報告するメッセージが受信者に送信されます。

関連項目    • [3ページのvGW シリーズの理解](#)

## vGW シリーズのネットワーク設定の構成

設定モジュールの [Network Settings] セクションでは、vGW セキュリティ デザイン VM のホスト名を変更できます。また、DHCP と静的アドレス方式のどちらを使用するかも指定できます。どちらの場合でも、このセクションを使用して該当する IP アドレスを構成します。

デフォルトでは、vGW セキュリティ デザイン VM が持っている仮想 NIC (vNIC) は 1 つだけです。場合によっては（たとえば、VMware vCenter システムが分離されたネットワーク上に存在する場合など）、追加のインターフェースを vGW セキュリティ デザイン VM に追加しなければならないことがあります。追加の vNIC を vGW セキュリティ デザイン VM に追加するには、VMware を使用して vNIC を追加し、この画面でそのインターフェースを構成します。



注: vGW セキュリティ VM との通信には最初のインターフェース (Interface 1) を使用する必要があります。さらに、そのインターフェースを適切なデフォルト ゲートウェイに通じるよう定義する必要があります。

関連項目   • [3ページのvGW シリーズの理解](#)

## vGW シリーズのプロキシ設定の構成

設定モジュールの [Proxy Settings] セクションでは、アウトバウンド HTTP/HTTPS 接続にプロキシが必要な場合に、プロキシに関する情報を入力します。プロキシ サーバーの IP アドレス、ポート、およびユーザー資格情報をこの画面に入力します。vGW シリーズは、提供されている最新のソフトウェアを取得する際、HTTPS (TCP 443) リクエストを Juniper Networks vGW インターネット更新サーバーに送信します。

関連項目   • [3ページのvGW シリーズの理解](#)

## vGW シリーズの時刻設定の構成

vGW セキュリティ デザイン VM の設定モジュールの [Time Settings] セクションでは、vGW シリーズの適切な動作にとって不可欠な時刻設定と、NTP サーバーの設定を指定します。vGW セキュリティ デザイン VM は正しいタイムゾーンを持ち、NTP サーバーにアクセスできる必要があります。すべてのシステム ログ、セキュリティ ログ、セキュリティ ポリシー配備、およびその他のデータにはタイムスタンプが付きます。時刻設定が間違っている場合、これらのデータには間違った日時が付けられます。ESX/ESXi ホストにインストールされた vGW セキュリティ VM は、自身の時刻設定を vGW セキュリティ デザイン VM の設定と同期します。

内部 NTP サーバーがない場合は、事前設定された NTP サーバーまたはその他のインターネット上の NTP サーバーを使用できます。また、不要なエントリを削除することもできます。

関連項目   • [3ページのvGW シリーズの理解](#)



## vGW シリーズのバックアップおよびリストア機能の理解

多くの会社のネットワークおよびセキュリティ グループでは、自社のハードウェア デバイス システムの構成をバックアップおよびリストアすることが習慣化しています。実際に多くの組織で、構成のバックアップが必須の構成管理業務の一部となっています。

仮想化デバイスに関するこの要件に対処するため、vGW シリーズには、vGW セキュリティ デザイン VM の構成をファイル ストアにバックアップする機能が用意されています。必要なときに、バックアップ バージョンのいずれかを簡単にリストアできます。

インストール ウィザードには、バックアップされている構成設定をスキップできる修正版があります。

この修正版のインストール ウィザードを実行した後に vGW セキュリティ デザイン VM にログインし、使用する vGW セキュリティ デザイン VM バックアップ構成をバックアップ場所からインポートすれば、最小限の労力でバックアップをリストアできます。この作業には、vGW セキュリティ デザイン VM 設定モジュールの [System Settings Backup] セクションにある [Restore] 機能を使用します。

バックアップおよびリストア機能の設定を構成する方法の詳細については、[188ページの「vGW シリーズのバックアップおよびリストア機能の構成」](#)を参照してください。

バックアップした vGW セキュリティ デザイン VM の構成で静的 IP アドレスが使用されていた場合、その構成をリストアしたバージョンでも IP アドレスが同じになります。この場合、エージェントは、リストアした vGW セキュリティ デザイン VM が起動した後ただちにその VM との通信を開始できます。

vGW シリーズでバックアップおよびリストアされる内容は以下のとおりです。

- 管理者が vGW セキュリティ デザイン VM を使用して構成した、以下のすべての構成情報
  - マシン
  - ネットワーク
  - グループ
  - プロトコル
  - セキュリティ ポリシー オブジェクト
  - グループに関連付けられたポリシー
  - スマート グループのメンバーシップとロジック

- 静的グループの VM メンバーシップ。VM-ID/UUID はバックアップおよびリストア プロセスによって変更されることに注意してください。
- 管理者アカウント。 管理者パスワードは安全かつセキュリティ保護された方法でエクスポートされます。



**注:** ソース テーブルは、connections、alerts、idp\_alerts を除くすべてがバックアップされます。 この情報は、他の vGW セキュリティ デザイン VM 機能を使用してバックアップできます。

vGW セキュリティ デザイン VM のバックアップおよびリストア機能では、以下のことができます。

- ファイルのバックアップ場所を指定する。
- 保持するバックアップ ファイルの数を指定する。 必要に応じていつでも、すべてのバックアップ コピーを削除できます。
- 複数のバックアップ バージョンの中からリストアする構成を選択する。
- 構成をバックアップするスケジュールを設定する。

関連項目    • [3ページのvGW シリーズの理解](#)

## vGW シリーズのバックアップおよびリストア機能の構成

vGW シリーズのバックアップおよびリストア機能を使用すると、vGW セキュリティ デザイン VM 構成のバックアップを複数作成して保存し、ある特定のバージョンのバックアップを簡単にリストアできます。 このトピックでは、その設定の構成方法について説明します。 このトピックを読む前に、[187ページの「vGW シリーズのバックアップおよびリストア機能の理解」](#)をお読みください。



**警告:** ベータ カスタマー: この機能の vGW B2 インターフェースは、このドキュメントの記述内容と完全には一致していません。 今後ドキュメントが更新され、バックアップおよびリストアに関する新しい vGW セキュリティ デザイン VM インターフェースの変更点が反映される予定です。

vGW セキュリティ デザイン VM のバックアップおよびリストア方法を決定する設定を定義するには、以下の手順に従います。

1. vGW セキュリティ デザイン VM の設定モジュールの [Appliances Settings] セクションで、[System Settings Backup] を選択します。
2. 表示された画面の [Backup Settings] ペインで、[Enable Backup Settings] チェックボックスをオンにして設定を有効にします。
3. [Backup Location] セクションで、構成情報を保存する場所を指定します。
  - ネットワーク ファイル システム共有 (NFS)

- Windows ファイル システム共有 (CIFS または SMB)

Windows ファイル システム (CIFS (Common Internet File System) または SMB (Server Message Block) ) をファイル ストアとして使用する場合は、以下の情報を指定します。

- ホストの名前とそのパス。
  - ファイル共有へのアクセスに使用するユーザー名とパスワード。
  - vGW シリーズ ソフトウェアが更新される前 (たとえば、バージョン  $x$  からバージョン  $x$ , SP $x$  に更新される前) に構成のバックアップを開始したい場合は、[Backup before software update] をクリックして選択します。
4. ファイル共有に保存する構成のバックアップ バージョンの数を [Number of backups to keep] ボックスに入力します。
  5. 必要に応じて、[Enabled Backup Scheduling] チェックボックスをオンにして構成のバックアップ スケジュールを設定します。
    - a. [Daily] を選択した場合は、時刻を指定します。
    - b. [Weekly] を選択した場合は、曜日と時刻を指定します。
    - c. [Monthly] を選択した場合は、月の日にちと時刻を指定します。
  6. [Save] をクリックして、バックアップ機能の定義を保存します。
  7. 構成をただちにバックアップするには、[Backup Now] をクリックします。



**注:** vGW セキュリティ デザイン VM 構成のバックアップ スケジュールを設定しなかった場合は、バックアップおよびリストアを構成した後ただちにバックアップが実行されます。

構成をリストアするには、[Restore Settings] ペインを使用して以下の手順に従います。

1. [Browse] をクリックして、バックアップ バージョンのリストを表示します。 バージョンを選択して [Restore] をクリックします。  
[Backup Location] セクションで指定したファイル共有情報に基づいて、ファイル共有から取得されたバックアップ済み構成がリストアされます。
2. すべてのバックアップ済みバージョンを削除するには、[Clear] をクリックします。

関連項目    • [3ページのvGW シリーズの理解](#)

## vGW シリーズのログ収集の理解

このトピックでは、設定モジュールの [Log Collection] セクションについて説明します。このセクションは、vGW セキュリティ デザイン VM の問題をトラブルシューティングするための

ログを収集する場合に使用します。個々の vGW セキュリティ VM のログを収集する方法の詳細については、「XXX」を参照してください。

- [ログ収集 190ページ](#)
- [ファイルのアップロード 190ページ](#)
- [ファイルのダウンロード 190ページ](#)

## ログ収集

何らかの理由で、vGW セキュリティ デザイン VM 自体のトラブルシューティングが必要となる問題が発生する場合があります。問題の解決に役立てるため、Collection Tool を使用して Juniper Networks サポート チームに提供する情報を生成できます。

[Start New Collection] をクリックすると、Collection Tool によって関連するログとシステム ファイルが生成され、TGZ ファイルに圧縮されます。このファイルをサポート センターにアップロードするか、ファイルのコピーを手動で提出できます。ファイルをアップロードすることを推奨します。

## ファイルのアップロード

[Upload Log Collection] ペインの [Upload] をクリックすると、圧縮ログ ファイルがアップロードされて ID が返されます。ファイルはアップロード時に (AES-256 によって) 暗号化され、保護サーバーに転送されます。返された ID を使用して、Juniper Networks サポート への提出を追跡できます。トラブル チケット、または当該問題に関するサポート チームとのやり取りにおいても、この ID を提示/参照してください。ファイルをアップロードする前に、問題に関する簡単な説明をコメント フィールドに入力する必要があります。

## ファイルのダウンロード

[Download Log Collection] ペインの [Download] をクリックしてファイルをダウンロードすると、そのファイルを E メールによって随時送信したり、収集したログをサーバーに投稿したりできます。

関連項目   • [3ページのvGW シリーズの理解](#)

---

## vGW シリーズのログの表示

vGW セキュリティ デザイン VM の設定モジュールの [Log Viewer] を使用して、基本的なシステム アクティビティの監視やトラブルシューティングのために各種システム ログおよびアプリケーション ログを選択できます。また、ビューアに表示する行数を選択することもできます。

関連項目   • [3ページのvGW シリーズの理解](#)

---

## vGW シリーズのサポート設定の理解

vGW セキュリティ デザイン VM の設定モジュールのサポート セクションでは、以下のことができます。

- vGW セキュリティ デザイン VM を再起動する。
- vGW シリーズのサービスを再起動する。
- トラブルシューティングに使用するデバッグ フラグを有効または無効にする。

デバッグ フラグを有効にした場合は、ログ ファイルを収集した後でこの画面に戻り、[Debugging OFF] をクリックします。デバッグ設定を有効にしたままにすると、多数のログ ファイルが生成されてディスク領域の使用に関する問題が生じる場合があります。

- vGW セキュリティ デザイン VM への SSH リモート アクセスを有効または無効にする。

SSH を有効にすると、PUTTY などの SSH クライアントから vGW シリーズを管理できます。これにより、vSphere Client を使用せずに vGW セキュリティ デザイン VM や vGW セキュリティ VM コンポーネントの vGW コマンド ラインにアクセスできます。

SSH によって vGW セキュリティ デザイン VM または vGW セキュリティ VM にアクセスすると、コマンドライン インターフェースが表示されます。このコマンドライン インターフェースはさまざまなシステム オプションをサポートします。コマンドライン プロンプトで ? または help と入力すると、サポートされている vGW シリーズ コマンドの一覧が表示されます。

関連項目    • [3ページのvGW シリーズの理解](#)



## vGW シリーズのステータス アラート

- [vGW シリーズのステータスおよびアラートの理解 193ページ](#)

### vGW シリーズのステータスおよびアラートの理解

---

vGW シリーズでは、ユーザー インターフェースにさまざまなステータス アイコンが表示され、アラートを送信するメカニズムも用意されているので、仮想ネットワークで何が起きているかを正確に知ることができます。

- [ステータス 193ページ](#)
- [アラート 193ページ](#)
- [E メール アラート設定 194ページ](#)
- [SNMP トラップ設定 194ページ](#)
- [自動構成アラートとマルチキャスト アラート 194ページ](#)

### ステータス

vGW シリーズのインターフェースには、注意を要するイベントや構成の問題を示す黄色または赤のステータス アイコンが表示されます。 図を参照してください。

ステータス アイコンをクリックすると、メイン モジュール画面の [Status] タブが表示されます。

ステータス変更を引き起こした製品のセクションが表示され、最も重要なステータス変更が一番上に赤で示されます。 ステータスの問題の詳細については、ステータス サマリ行の横にある [more] リンクをクリックします。 図 60 を参照してください。

### アラート

vGW シリーズでは、セキュリティ ポリシー内の規則のログ フィールドが [Alert] またはカスタム E メール アラート タグに設定されていて、この規則に一致する接続がネットワーク上で見つかった場合、アラートが送信されます。

図 xx に示す規則 3 には、カスタム E メール アラート タグ (MIS 部門に E メールを送信する) が設定されています。 規則 2 は、E メール アラートに加えて SNMP トラップも送信するように設定されています。

vGW シリーズは、セキュリティ規則によって生成されるアラートに加えて、優先度が高、中、低のセキュリティ イベントを監視し (これらはメイン モジュールの [Events and Alerts] タ

ブに表示されます)、設定された手段 (E メール、SNMP トラップ、またはその両方) によってそれらのアラートを報告します。

どちらの場合も、[Settings] -> [Security Settings] -> [Alerting] で指定された設定が使用されます。図 62 を参照してください。

E メール アラートと SNMP トラップの両方を送信するか、E メール アラートのみを送信するか、SNMP トラップのみを送信するかを選択できます。

## E メール アラート設定

メール中継サーバーの IP アドレスと送信元および宛先の E メール アドレスを指定することで、E メール アラートを有効にします。集約時間は、連続する通知の間隔です。図 63 を参照してください。

複数の E メール受信者を構成する必要はありません。ただし、4 つのカスタム E メール アラート タグを作成し、それぞれ異なる E メール エイリアスまたは個々の E メール アカウント (またはそれら 2 つの組み合わせ) を指し示すことができます。これらのカスタム タグはセキュリティ ポリシー エディタで指定できます。図 62 では、MIS というタグが 1 つ作成されています。

E メール アラートと SNMP トラップの両方を単一の規則で送信する場合は、標準アラート アイコンを使用します。ただしこの場合は、[Recipients Addresses] にリストされた E メール アドレスのみが使用されます。つまり、E メール アラートと SNMP アラートを送信するときにはカスタム タグは使用できません。

## SNMP トラップ設定

SNMP トラップは、バージョン 1 またはバージョン 2 によって設定できます。SNMP サーバー アドレスとコミュニティ文字列を入力する必要があります。ここでも、必要に応じて集約時間 (連続するイベント間の遅延) を設定できます。

## 自動構成アラートとマルチキャスト アラート

デフォルトの構成では、自動構成アドレスが検出されたときにアラートが送信されます ([Settings] -> [Security Settings] -> [Alerting])。マルチキャストが観察されたときには、アラートは自動的に送信されません (ただし、これは有効にできます)。

- Autoconfig addresses: マシンに IP アドレスが設定されていない場合、またはマシンが DHCP リースを取得できない場合は、デフォルトで 169.254.\*.\* の範囲の自動構成アドレスが使用されます。この設定は多くの場合、構成または DHCP サービスに問題があることを意味します。
- Multicast: 多くのホストがマルチキャスト パケットを使用して自身の存在をネットワーク上にアドバタイズし、提供しているサービスに関するブロードキャスト情報や構成データを送信します。この情報は必要でないことが多く、サーバーがこの情報を提供するのはいらない場合があります。また、セキュリティの観点から見て、マシンで使用可能なサービスをアドバタイズすることについても問題があります。

関連項目    • [3ページのvGW シリーズの理解](#)



## 高可用性とフォールト トレランス

- [vGW シリーズの高可用性ソリューションの理解 195ページ](#)
- [高可用性のためのセカンダリ vGW セキュリティ デザイン VM のインストール 196ページ](#)
- [高可用性のためのセカンダリ vGW セキュリティ VM のインストール 197ページ](#)
- [VMware の高可用性と分散リソース スケジュールの理解 198ページ](#)
- [vGW シリーズのフォールト トレランスのサポートの理解 198ページ](#)

### vGW シリーズの高可用性ソリューションの理解

- [vGW シリーズの高可用性ソリューションについて 195ページ](#)
- [vGW セキュリティ デザイン VM の高可用性について 195ページ](#)
- [vGW セキュリティ VM の高可用性について 196ページ](#)

### vGW シリーズの高可用性ソリューションについて

VMware の高可用性機能は、プライマリおよびセカンダリの vGW セキュリティ VM と vGW セキュリティ デザイン VM を配備することで、VMSafe モード環境に障害が発生したときのソリューション回復力を維持します。

vGW セキュリティ VM は単一ホストに関係しているため、新しい ESX/ESXi ホストに移動しないようにすることが重要です。各 vGW セキュリティ VM は、そのホスト上の VM のみを保護します。ホストがダウンした場合、保護する対象がなくなります。障害復旧後に vGW セキュリティ VM が障害前と同じ場所に復元されなかった場合は、問題が生じる可能性があります。VMware の高可用性および分散リソース スケジュール (DRS) の設定は自動的に、高可用性または DRS によって vGW セキュリティ VM が移動されないように構成されます。

### vGW セキュリティ デザイン VM の高可用性について

vGW セキュリティ デザイン VM は、vGW シリーズ インフラストラクチャ全体の主要な制御点です。vGW セキュリティ デザイン VM は、ユーザー インターフェースの表示、vGW シリーズの各モジュールへのポリシーの配布、ログの整理統合、ネットワーク監視データベースのホスティング、およびその他の重要な機能を担当します。vGW セキュリティ デザイン VM が、たとえば電源がオフになっていたりクラッシュしたりといった理由で使用できない場合、管理者はインフラストラクチャの構成を変更できません。

vGW シリーズ システムのプライマリまたはセカンダリ管理オプションを使用すると、プライマリ vGW セキュリティ デザイン VM がオンラインに復帰するまでの間、セカンダリ vGW セキュ

リティ デザイン VM が代わりにポリシーを提供できます。そのため、通常のすべてのネットワーク アクティビティを中断なしに継続できます。具体的には、ESX/ESXi ホスト上の新しく電源がオンにされた VM は、デフォルトの VMsafe 障害モードにならずにポリシーを取得できます。

セカンダリ vGW セキュリティ デザイン VM の構成方法の詳細については、196ページの「[高可用性のためのセカンダリ vGW セキュリティ デザイン VM のインストール](#)」を参照してください。

## vGW セキュリティ VM の高可用性について

セカンダリ管理センターを準備することに加えて、vGW セキュリティ VM のレベルで冗長性を確保することも重要です。VMsafe により、プライマリおよびセカンダリの vGW セキュリティ VM をセットアップできます。vGW セキュリティ VM は各 ESX ホストにインストールされ、ハイパーバイザと直接やり取りするよう設計されています。IDS とアンチウィルスが動作するためには、vGW セキュリティ VM がアクティブであることが前提となります。

セカンダリ vGW セキュリティ VM をインストールするには、元の vGW セキュリティ VM から別の仮想マシンを構築する必要があります。セカンダリ管理センター（vGW セキュリティ デザイン VM）を作成する場合とは異なり、新しい vGW セキュリティ VM を作成するときは単に既存の vGW セキュリティ VM のクローンが作成されます。

VMware の高可用性および分散リソース スケジュール（DRS）の設定は自動的に、高可用性または DRS によって vGW セキュリティ VM が移動されないように構成されます。vGW セキュリティ VM は新しい ESX/ESXi ホストに移動しないようにすることが重要です。

各 vGW セキュリティ VM は、そのホスト上の VM のみを保護します。ホストがダウンした場合、保護する対象がなくなります。

vGW セキュリティ VM のインストール方法の詳細については、197ページの「[高可用性のためのセカンダリ vGW セキュリティ デザイン VM のインストール](#)」を参照してください。

関連項目   • [3ページのvGW シリーズの理解](#)

## 高可用性のためのセカンダリ vGW セキュリティ デザイン VM のインストール

このトピックでは、メイン vGW セキュリティ デザイン VM に障害が発生したときに使用するセカンダリ vGW セキュリティ デザイン VM を構成する方法について説明します。

セカンダリ vGW セキュリティ デザイン VM をインストールするには、vGW セキュリティ デザイン VM OVF/OVA（または TGZ ファイル）から 2 つ目の vGW セキュリティ デザイン VM を構築する必要があります。高可用性のためのセカンダリ vGW セキュリティ デザイン VM を作成するには、以下の手順に従います。

1. vGW セキュリティ デザイン VM をインポートします。VMware VirtualCenter/vSphere Client によって vGW セキュリティ デザイン VM の OVF/OVA ファイルをロードします（[File] -> [Virtual Appliance] -> [Import]）。
2. 仮想アプライアンス インポートのデフォルト値をそのまま使用します。



**注意:** OVF インポート プロセスでは、データベース ディスクを指定するよう求められます。デフォルト サイズの 8 GB をそのまま使用できます（プライマリ vGW セキュリティ デザイン VM に対して構成されているサイズがこれより大きい場合でも、8 GB でかまいません）。セカンダリ vGW セキュリティ デザイン VM には、プライマリと同じタイプの情報は保存されないため、8 GB を超える容量は必要ありません。インポートが完了した後、新しく作成されたセカンダリ vGW セキュリティ デザイン VM の電源をオンにしないでください。

3. プライマリ管理センター（vGW セキュリティ デザイン VM）を開き、[High Availability] セクションでセカンダリ vGW セキュリティ デザイン VM を選択します。[Settings] -> [vGW Application Settings] -> [High Availability] の順に選択します。



**注:** まだ vGW インターフェースから VM の更新を実行していない場合は ([Settings] -> [vGW Application Settings] -> [vCenter Integration] -> [Update VMs])、vGW 仮想ゲートウェイ ソリューションによって vGW セキュリティ デザイン VM が認識される前にその VM を更新する必要があります。

4. IP アドレスとして DHCP または静的アドレスを入力します。
5. [Save] をクリックします。

セカンダリ vGW セキュリティ デザイン VM の電源が自動的にオンになり、VM が構成されます。このプロセスにはおよそ 10 分かかります。これらの操作が完了したら、この構成で指定した IP アドレスによってセカンダリ vGW セキュリティ デザイン VM にログインできます。

vGW シリーズは 2 つの vGW セキュリティ デザイン VM 管理ステーション間の接続を監視し、プライマリ vGW セキュリティ デザイン VM からの応答が 3 分間ない場合、セカンダリ システムの昇格を開始します。プライマリ vGW セキュリティ デザイン VM が回復するか、その導入先のホストの修理が完了してプライマリ vGW セキュリティ デザイン VM がオンラインに復帰すると、再びプライマリ vGW セキュリティ デザイン VM が自動的にプライマリの役割を担います。vGW シリーズの高可用性は通常のバックアップ操作に置き換わるものではありません。むしろ、プライマリが早急にオンラインに復帰することが期待されます。プライマリ vGW セキュリティ デザイン VM がセカンダリから自動的に再構築されることはないため、vGW セキュリティ デザイン VM をバックアップする際は注意する必要があります。

- 関連項目
- [198ページのVMware の高可用性と分散リソース スケジュールの理解](#)
  - [197ページの高可用性のためのセカンダリ vGW セキュリティ VM のインストール](#)

## 高可用性のためのセカンダリ vGW セキュリティ VM のインストール

セカンダリ vGW セキュリティ VM をインストールするには、元の vGW セキュリティ VM から別の仮想マシンを構築します。セカンダリ vGW セキュリティ デザイン VM 管理センターを作成する場合とは異なり、新しい vGW セキュリティ VM を作成するときは既存の vGW セキュリティ VM のクローンが作成されます。

既存のプライマリ vGW セキュリティ VM のクローンを作成するには、以下の手順に従います。

1. [Settings]、[Security Settings]、[Security VM Settings] の順に選択します。
2. 複製する vGW セキュリティ VM の行をクリックします。
3. [High Availability] ペインで、[Configure] をクリックします。
4. セカンダリ vGW セキュリティ VM の情報を入力します。適切な IP アドレス情報、管理ネットワーク、およびデータ ストアの場所を指定します。
5. [Configure] をクリックします。



注: vGW セキュリティ デザイン VM の場合とは異なり、vGW セキュリティ VM のバックアップを取ることはそれほど重要ではありません（必要であれば、新しい vGW セキュリティ VM をテンプレートから配備することもできます）。

- 関連項目
- [198ページのVMware の高可用性と分散リソース スケジュールの理解](#)
  - [196ページの高可用性のためのセカンダリ vGW セキュリティ デザイン VM のインストール](#)

## VMware の高可用性と分散リソース スケジュールの理解

VMware の高可用性機能は、プライマリおよびセカンダリの vGW セキュリティ VM と vGW セキュリティ デザイン VM を配備することで、VMSafe モード環境に障害が発生したときのソリューション回復力を維持します。

VMware の高可用性および分散リソース スケジュール (DRS) の設定は自動的に、高可用性または DRS によって vGW セキュリティ VM が移動されないように構成されます。vGW セキュリティ VM は新しい ESX/ESXi ホストに移動しないようにすることが重要です。

- 各 vGW セキュリティ VM は、そのホスト上の VM のみを保護します。ホストがダウンした場合、保護する対象がなくなります。
- 障害復旧後に vGW セキュリティ VM が障害前と同じ場所に復元されなかった場合は、問題が生じる可能性があります。

- 関連項目
- [3ページのvGW シリーズの理解](#)

## vGW シリーズのフォールト トレランスのサポートの理解

このトピックには以下のセクションがあります。

- [vGW シリーズのフォールト トレランスについて 199ページ](#)
- [vGW シリーズでの vGW シリーズ フォールト トレランス 199ページ](#)
- [仮想マシンに対するフォールト トレランスの有効化 200ページ](#)

## vGW シリーズのフォールト トレランスについて

仮想化環境では、仮想マシン (VM) が存在するホストに障害が発生した場合に備えて、フォールト トレランス (FT) によって VM の継続的なサポートを確保します。

VMware vCenter 内の VM で FT を有効にすると、セカンダリ VM と呼ばれる VM のコピーが別のホストに自動的に作成されます。元の VM (プライマリ VM) とそのコピー (セカンダリ VM) は並行して実行されます。プライマリ VM のホストで障害が発生すると、セカンダリ VM がただちに実行を引き継ぎ、接続、トランザクション、またはデータが失われることはありません。この引き継ぎを行うためには、プライマリ VM が、同じ構成を持つ同じ種類のホストのクラスターに属している必要があります。また、クラスターを構成するホストで高可用性が有効になっている必要があります。

FT 機能を有効にすると、DRS によって選択されたホスト (DRS が有効な場合)、またはクラスター内の使用可能な任意のホストから選択されたホストにセカンダリ VM が作成されます。プライマリ VM とセカンダリ VM は同じ名前と BIOS uuid を持ちますが、vc\_uuid と vi\_id は互いに異なります。

セカンダリ VM は固有の .vmx ファイルを持ちます。プライマリ VM の .vmx ファイルとセカンダリ VM の .vmx ファイルはどちらも同じデータ ストア ディレクトリに存在します。

プライマリ VM のホストで障害が発生してセカンダリ VM に制御が移行した場合、外部から見ると、あたかも vMotion によってプライマリ VM がセカンダリ VM のホストに移動し、その後元に戻った (つまり、セカンダリ VM が、プライマリ VM が存在していたホストに移動した) のように見えます。

## vGW シリーズでの vGW シリーズ フォールト トレランス

このセクションでは、vCenter で FT が有効にされている VM を vGW シリーズがどのように扱い、全体的に FT がどのようにサポートされるのかについて説明します。

vGW シリーズは、FT が有効にされている VM をユーザーに見せるかどうかについて、以下のよう to 扱います。

- セカンダリ VM は VM ツリーに表示されません。
- セカンダリ VM は設定モジュールの [Machines] セクションに表示されません。
- 設定モジュールの [Installation] セクションでは、プライマリ VM とセカンダリ VM の両方が [Secured Network] ファイアウォール ツリーに表示されます。vSphere Client でホスト上の VM がマークされるのと同じように、セカンダリ VM 名の後に「secondary」という語が付加されます。

たとえば、host1 と host2 の 2 台のホストを含むクラスターがあるとします。vCenter で host1 に my-test-vm という VM を作成したとき、FT を有効にしました。プライマリ my-test-vm VM は host1 にとどまります。FT をサポートするため、「my-test-vm (secondary)」という名前のセカンダリ VM が host2 に作成されます。これらの 2 つの VM が設定モジュールの [Installation] セクションに表示されます。

- セカンダリ VM に対してポリシーを定義することはできません。

vGW が vNIC を再接続すること、およびこの VM を自動的に一時停止または再開することは禁じられています。これらを行うと、望ましくない効果が生じます。この理由から、以下のようになります。

- FT が構成されている VM の電源がオンになっている場合、設定モジュールの [Installation] セクションでその VM を選択して保護することはできません。該当するチェックボックスは灰色表示になります。VM のツールヒントには、「この VM を保護するためにはまず VM を一時停止するか FT を無効にする必要がある」と表示されます。
- FT が有効にされている VM は、vGW シリーズの自動保護機能によって保護されません。vGW でその VM を保護するためには VM の FT を無効にするか VM を一時停止する必要があることを伝えるアラートが生成されます。

自動保護機能は、FT が有効にされている VM を監視し、FT が無効にされたか、または VM が一時停止して電源がオフにされたかをチェックします。VM が Auto Secure グループに属した場合、vGW はその VM を保護します。

すでに VMsafe によって保護されている VM で FT を有効にすると、セカンダリ VM が作成され、その VMsafe param0 は不正確な値になります。これは、このパラメータがセカンダリ VM に固有の VC\_uuid ではなくプライマリ VM の VC\_uuid を反映するためです。ただし、セカンダリの .vmx は読み取り専用であり、再構成操作はすべて失敗するため、vCenter はこのパラメータを再構成しようとしません。

## 仮想マシンに対するフォールトトレランスの有効化

VM に対して FT を有効にする前に、クラスタの高可用性を有効にする必要があります。

vCenter 内の VM に対して FT を有効にするには、以下の手順に従います。

1. vSphere Client を使用して vCenter にアクセスし、対象の VM が存在するホストを特定します。
2. VM の名前を右クリックします。
3. 表示されたメニューから、[Fault Tolerance] を選択します。
4. [Turn On Fault Tolerance] を選択します。
5. DRS 自動化が無効になること、および VM のメモリ予約が VM のメモリ サイズに変更されることを知らせるメッセージを確認したら、[Yes] をクリックして変更を確定します。

You c

画面の下部にある [Recent Tasks] ウィンドウで、VM のフォールトトレランスがオンになったことを確認します。

関連項目 • [3ページのvGW シリーズの理解](#)

## 第3部

# Juniper Networks 製品の相互運用性

このパートには以下の章があります。

- [vGW シリーズの Juniper Networks 製品との相互運用性](#) 203ページ





## vGW シリーズの Juniper Networks 製品との相互運用性

この章では以下のトピックについて説明します。

vGW シリーズと他の Juniper Networks 製品との統合の詳細 (STRM、SRX のゾーン同期、および SRX-IDP を含む) については、セキュリティ仮想化のアプリケーション ノート (<http://www.juniper.net/us/en/solutions/enterprise/data-center/secure>) を参照してください。

- vGW シリーズおよび Junos SRX シリーズのセキュリティ ゾーン 203ページ
- vGW シリーズに対する Junoscript インターフェースの有効化 205ページ
- vGW シリーズと SRX シリーズ デバイスとの相互運用性のための SRX シリーズ ゾーン オブジェクトの構成 206ページ
- SRX シリーズのゾーン アドレス帳への vGW シリーズ VM レコードの登録について 207ページ
- vGW シリーズと SRX シリーズ ゾーンとの相互運用性の検証 207ページ
- vGW シリーズから Juniper Networks STRM への Syslog および Netflow データの送信に関する構成 208ページ
- vGW シリーズと IDP の相互運用の構成 209ページ

### vGW シリーズおよび Junos SRX シリーズのセキュリティ ゾーン

このトピックには以下のセクションがあります。

- SRX シリーズ サービス ゲートウェイのセキュリティ ゾーンについて 203ページ
- SRX シリーズ サービス ゲートウェイのゾーンと vGW シリーズ 204ページ
- 関連するアプリケーション ノート 204ページ

### SRX シリーズ サービス ゲートウェイのセキュリティ ゾーンについて

セキュリティ ゾーンとは、ポリシーによるインバウンドおよびアウトバウンド トラフィックの調整を必要とする、SRX シリーズ デバイス上の 1 つ以上のネットワーク セグメントを集めたものです。

セキュリティ ゾーンは、SRX シリーズ デバイスの 1 つ以上のインターフェースが結び付けられる論理的なエンティティです。

1 つの SRX シリーズ デバイス上で複数のセキュリティ ゾーンを構成し、ネットワークをセグメントに分割してそれぞれのニーズに応じたさまざまなセキュリティ オプションを各セグメントに適用できます。多数のセキュリティ ゾーンを定義し、物理ネットワークのセキュリティ デザインを適切に細分化することが可能です。そのために複数のセキュリティ アプライアンスを配備する必要はありません。

セキュリティ ポリシーの観点から見ると、トラフィックはあるセキュリティ ゾーンに入り、別のセキュリティ ゾーンから出ていきます。この入口ゾーンと出口ゾーンの組み合わせがコンテキストとして定義されます。各コンテキストにはポリシーの順序付きリストが含まれます。

SRX シリーズ デバイスはさまざまなタイプのセキュリティ ゾーンをサポートしています。

### SRX シリーズ サービス ゲートウェイのゾーンと vGW シリーズ

vGW シリーズのゾーン同期機能は、vGW シリーズの仮想化セキュリティ層を SRX シリーズ サービス ゲートウェイの物理デバイスおよびネットワーク セキュリティと自動的に結び付ける手段となります。

vGW シリーズのゾーン機能は、SRX シリーズ デバイスで構成されたゾーンを仮想化環境にインポートすることで、VM とゾーンを容易にマッピングします。

これらのゾーン割り当てを使用して、以下のことができます。

- VM 間で使用するゾーン ポリシーを適用する。
- ゾーンをコンプライアンス チェックと統合して、VM が許可されたゾーンのみに接続されるようにする。

SRX シリーズのゾーンを VM と同期するために vGW シリーズが実行するプロセスでは、以下のものが定義されます。

- SRX オブジェクト。このプロセスは、SRX シリーズ デバイスからのゾーン構成情報の取得、vGW シリーズ インターフェースへのゾーンのマッピング、各ゾーンとの VLAN またはネットワーク範囲の関連付けを伴います。
- 各ゾーンに関連付けられた VLAN とネットワークに基づく、vGW シリーズ内のスマート グループとしてのゾーン。

また、各 VM に動的に関連付けられたスマート グループが適切なゾーンに関連付けられていることも検証されます。このプロセスにより、vGW シリーズ VM 間のポリシーの強制と、SRX シリーズ ゾーンのコンプライアンス検証が可能となります。

### 関連するアプリケーション ノート

vGW シリーズと他の Juniper Networks 製品との統合の詳細 (STRM、SRX のゾーン同期、および SRX-IDP を含む) については、セキュリティ仮想化のアプリケーション ノート (<http://www.juniper.net/us/en/solutions/enterprise/data-center/secure>) を参照してください。

関連項目    • [3ページのvGW シリーズの理解](#)

## vGW シリーズに対する Junoscript インターフェースの有効化

ゾーン同期のために vGW シリーズが SRX シリーズ デバイスにアクセスできるようにするには、Junoscript XML スクリプティング API を有効にする必要があります。 そのためには、以下の手順に従います。

1. デジタル Secure Sockets Layer (SSL) 証明書を生成し、SRX シリーズ デバイスにインストールします。

- a. openssl がインストールされている BSD または Linux システムで、SSH コマンドライン インターフェースに次の openssl コマンドを入力します。 これにより、自己署名 SSL 証明書が Privacy-Enhanced Mail (PEM) 形式で生成されます。 指定したファイルに証明書と暗号化されていない 1024 ビット RSA 秘密鍵が書き込まれます。

```
% openssl req -x509 -nodes -newkey rsa:1024 -keyout mycert.pem -out mycert.pem
```

- b. プロンプトが表示されたら、適切な情報を識別形式で入力します。 たとえば、国名に対して US と入力します。
- c. 作成したファイルの内容を表示します。

```
cat mycert.pem
```

- d. SSL 証明書を SRX シリーズ デバイスにインストールします。 証明書を含むファイルを BSD または Linux システムから SRX シリーズ デバイスにコピーします。 CLI を使用して証明書をインストールするには、構成モードで次のステートメントを入力します。

```
[edit]
user@host# set security certificates local mycert load-key-file mycert.pem
```

2. mycert 証明書を使用して HTTPS web-management を構成します。

```
[edit]
user@host# set system services web-management https local-certificate mycert
user@host# set system services web-management https interface ge-0/0/0.0
user@host# set system services web-management https port 443
```

3. まだ構成していない場合は、このインターフェースの IP アドレスを構成します。
4. 新しく作成した証明書を使用して Junoscript 通信を有効にします。

```
[edit]
user@srx# set system services xnm-ssl local-certificate mycert
[edit]
user@srx# set system services xnm-ssl local-certificate mycert
```

関連項目    • [3ページのvGW シリーズの理解](#)

## vGW シリーズと SRX シリーズ デバイスとの相互運用性のための SRX シリーズ ゾーン オブジェクトの構成

vGW セキュリティ デザイン VM インターフェースを使用して新しい SRX シリーズ ゾーン オブジェクトを作成するには、以下の手順に従います。

### 1. 設定モジュールを選択します。

- a. 左ペインの [Security Settings] ボックスで、[SRX Zones] を選択します。

- b. 画面の右下にある [Add] ボタンをクリックします。

[Add SRX Zone] ペインが表示されます。

- c. [Add SRX Zone] ペインで、SRX ゾーンに関する以下の情報を指定します。

- Name: SRX ゾーン オブジェクトの簡潔で分かりやすい名前。 この名前は VM ゾーン のラベルに使用されます。
- Host: vGW セキュリティ デザイン VM への接続に使用される、SRX シリーズ デバイス上のデバイス管理 IP アドレス。
- Port: Junoscript インターフェースを介した SRX シリーズ デバイスへの接続に使用される TCP ポート。
- Login と Password: SRX シリーズ デバイスへの認証に使用される資格情報。

SRX ゾーン オブジェクトのアカウントには、SRX シリーズ デバイスのゾーン、インターフェース、ネットワーク、およびルーティング構成の読み取りアクセス権が必要です。 必要に応じて、VM エントリを書き込むために各ゾーンのアドレス帳への書き込みアクセス権が必要になります。

SRX シリーズ デバイスのアドレス帳に VM オブジェクトを登録しない場合には、書き込みアクセス権は必要ありません。

- VMs associated with this SRX: このパラメータは VM の範囲を指定します。 SRX シリーズ デバイスに関連する VM を定義します。

### 2. 同期間隔と関連インターフェースを定義するには、SRX ゾーン オブジェクトの定義を保存した後に [Load Zones] をクリックします。

ゾーン同期プロセスが完了した後、vGW シリーズによって取得されたゾーンのリストが表示されます。 VM ゾーン グループとして vGW シリーズにインポートするゾーンを選択できます。

SRX シリーズ デバイスを自動的にポーリングしてゾーンを更新するよう設定することもできます。

vGW シリーズの自動ゾーン同期プロセスによって同期更新を制御するには、以下の情報を指定します。

- Update Frequency: SRX シリーズ デバイスに更新を問い合わせる頻度（間隔）。

- Relevant Interfaces: vGW シリーズで監視する SRX シリーズ デバイスのインターフェースを選択します。これにより、関連インターフェースに新しく割り当てられたゾーンが検出され、vGW シリーズの監視対象としてそれらのゾーンが追加されます。

同期プロセスに参加している SRX シリーズ ゾーンは、vGW シリーズの VM スマート グループとして自動的に作成されます。スマート グループは以下のパラメータに基づいて作成されます。

- SRX シリーズ デバイスのインターフェースに関連付けられた VLAN。
- SRX シリーズ デバイスのインターフェースで定義されたサブネットと、ゾーン内で定義されたルート。

ゾーン同期構成で、関連付ける VM が選択されている場合は、選択したグループがスマート グループに追加されます。

関連項目    • [3ページのvGW シリーズの理解](#)

## SRX シリーズのゾーン アドレス帳への vGW シリーズ VM レコードの登録について

vGW シリーズと SRX シリーズのゾーン同期機能では、VM が属するゾーンの SRX シリーズ アドレス帳に VM のレコードを登録できます。そうすると、SRX シリーズ デバイス管理のコンテキスト内で VM とゾーンのマッピングを検証できます。

SRX シリーズ デバイスのゾーン アドレス帳に追加される VM レコードは、vCenter で定義された VM の名前で作成されます。アドレス帳エントリの VM 名の前に、それが自動生成された VM レコードであることを示す文字列が付加されます。デフォルトでは「VM-」という文字列が使用されますが、この名前は同期ダイアログ ボックスで変更できます。

関連項目    • [3ページのvGW シリーズの理解](#)

## vGW シリーズと SRX シリーズ ゾーンとの相互運用性の検証

VM ゾーン関連付け情報に vGW シリーズの管理範囲内からアクセスできるときは、それをポリシー自動化およびコンプライアンス チェック手順に組み込むことができます。

コンプライアンス要件を満たしていない VM に対して、ただちにアクションを実行できます。不適合グループとグループ ポリシーを作成して、不適合の VM をネットワークから排除することが可能です。不適合の VM はすべてこのグループに追加されます。

次の図に示す構成例では、評価する VM の範囲として、DMZ にある SRX シリーズ デバイスの DB ゾーンを使用しています。さらに、そのゾーンの必須条件として、VM に DMZ 承認済みのタグが付いている、VM 名がデータベース命名要件に従っている、などを定義しています。

この図では、範囲を DB ゾーンに設定し、不適合の VM は [Non-Compliant VMs] グループに追加して検疫すること、およびアラートを発行することを指定しています。

関連項目    • [3ページのvGW シリーズの理解](#)

## vGW シリーズから Juniper Networks STRM への Syslog および Netflow データの送信に関する構成

Juniper Network の vGW シリーズを Security Threat Response Manager (STRM) と統合すると、仮想化サーバー環境の多層防御が可能となります。

vGW シリーズを Security Threat Response Manager (STRM) と統合すると、

- ログやイベントの集中管理、ネットワーク全体にわたる脅威検出、コンプライアンス レポートの作成などの STRM の利点が仮想化データ センターにもたらされます。
- vGW シリーズから STRM に、ログ、イベント、および仮想マシン間のトラフィックに関する統計情報を送信できます。

さらに、物理インフラストラクチャと仮想インフラストラクチャを単一ペインから包括的に概観できる一貫したビューが得られます。

vGW シリーズと STRM の実装には 2 つの統合ポイントがあります。

vGW シリーズは、

- ファイアウォールのログとイベントを Syslog を通じて STRM にエクスポートします。
- 仮想マシン間のトラフィックに関する統計情報を Netflow を通じてエクスポートします。

Syslog および Netflow 情報を STRM に送信するよう vGW セキュリティ デザイン VM を構成するには、以下の手順に従います。

1. vGW セキュリティ デザイン VM の設定モジュールで外部ロギングを構成します。
  - a. [Settings] -> [Global] -> [External Logging] の順に選択します。
  - b. [External Inspection Devices] ペインで、STRM の IP アドレスを指定します。
2. 同じ画面で Netflow を構成します。〈図〉に示すように、[NetFlow Configuration] セクションに STRM の IP アドレスを入力します。

vGW シリーズの Syslog および NetFlow データを受信するよう STRM を構成するには、以下の手順に従います。

1. vGW 用の STRM デバイス機能拡張をダウンロードします。
  - a. Juniper Networks サポート ページに移動します。Juniper Networks メイン ページから、[Support] タブを選択します。
  - b. 左の列で、[Download Software] を選択します。
  - c. [Security] ボックスで、[vGW (Altor)] を選択します。
  - d. [Software] タブを選択します。
  - e. [XML Specification for STRM] というファイルを右クリックして保存します。

この XML ファイルをブラウザで開いて表示しないでください。このファイルをブラウザで開くと、ファイルが破損する可能性があります。

2. STRM ユーザー インターフェースにログインします。
3. [Config] -> [Sensor Device Extensions] -> [Add a Device Extension] に移動します。
4. vGW シリーズ用のデバイス機能拡張を追加します。
5. [Browse] をクリックし、ダウンロードしたファイル (XML Specification for STRM) を選択します。
6. [Upload] をクリックし、デバイス機能拡張をアップロードします。デバイス機能拡張が [Extension Document] リストに表示されます。
7. [Save] をクリックして続行します。
8. Administration Console で、[Sensor Devices] を選択して vGW シリーズをセンサー デバイスとして追加します。  
これにより、Syslog レコードのソースが定義されます。
9. [Add a sensor device] を選択し、センサー デバイスを汎用 DSM として追加します。
  - a. [Device Hostname/IP] フィールドで、vGW セキュリティ デザイン VM の IP アドレスを指定します。
  - b. [Device Hostname/IP] フィールドで、vGW セキュリティ デザイン VM の IP アドレスを指定します。
  - c. 先ほど指定した、Juniper Networks vGW シリーズ用のデバイス機能拡張を選択します。
  - d. 残りのオプションを構成します。任意の名前を指定し、説明を入力できます。
10. STRM の [Event Viewer] 画面で、[Raw Events Display] オプションを選択します。
  - a. Juniper Networks vGW によって生成された、「action=allow」を含むログ レコードを探し、ダブルクリックして [Event Details] 画面を表示します。
  - b. [Map Event] ” アイコンを選択してマップします。
11. 「action=reject」および「action=drop」を含む vGW レコードに対して同じ手順を繰り返し、STRM QID 11750269 にマップします。

この手順が完了すると、vGW シリーズのログが STRM で使用できるようになります。

関連項目    • [3ページのvGW シリーズの理解](#)

## vGW シリーズと IDP の相互運用の構成

Juniper Networks の IDP シリーズ侵入検知防御アプライアンスは、幅広い攻撃からネットワークを守る機能を備えています。ステートフルな侵入検知防御技術を使用して、ワーム、トロイの木馬、スパイウェア、キーロガー、およびその他のマルウェアを防ぎます。その機能セットには、ステートフル シグネチャ検知、プロトコル異常検知、QoS/DiffServ マーキング、VLAN

対応ルール、ロールベースの管理、ドメインおよび管理アクティビティの分離、IDP レポーター、トラフィック パターン プロファイリングなどが含まれます。

vGW シリーズと IDP の相互運用性を構成する前に、侵入検知システムを外部検査デバイスとして構成し、設定モジュールの [Security Settings] の [Global] セクションを使用してそのデバイス用の適切なリダイレクション規則を設定する必要があります。

[External Inspection Devices] 画面では、さらなる分析のためにトラフィックを送信する宛先のデバイスの名前と IP アドレスを入力できます。

vGW シリーズと IDP の相互運用を構成するには、以下の手順に従います。

1. 運用環境の NSM にログインします。
2. VM 間通信のセキュリティ ポリシーを作成します。
  - a. ポリシーの通知セクションで、[Logging] を選択します。
  - b. 任意の送信元と宛先間のトラフィックに対してポリシーを有効にします。
  - c. アクションを [None] に設定します。

このセキュリティ ポリシーを使用して、VM 間のトラフィック異常を検査できます。
3. セキュリティ ポリシーを作成した対象の IDS システムで、GRE カプセル化解除のサポートを有効にします。
4. [Device Manager] -> [Security Devices] の順に選択します。
5. [Sensor Settings] -> [Run-Time Parameters] の順に選択します。
6. [Enable GRE decapsulation support] をオンにします。

パラメータが正しく設定されたことを確認するため、IDP デバイスのコマンド ラインに次のコマンドを入力します。

```
user@host# scio const -s s0 get sc_gre_decapsulation
```

これらの手順が完了したら、構成をテストできます。 上記の手順が完了した後（vGW セキュリティ デザイン VM での外部検査デバイスと関連するセキュリティ ポリシーの作成を含む）、Juniper Networks データベースで攻撃を引き起こして構成をテストします。

関連項目   • [3ページのvGW シリーズの理解](#)



## 第4部

# 索引

- [索引 213ページ](#)



# 索引

## C

カスタマー サポート.....	xx
JTAC へのお問い合わせ.....	xx

## D

DNS サービス.....	11
ドキュメント	
についてのご意見・感想.....	xx

## E

ESX/ESXi ホスト.....	9
-------------------	---

## M

マニュアル	
についてのご意見・感想.....	xx

## N

NTP サービス.....	11
---------------	----

## O

Open Virtualization Format (OVF) .....	17
OVA.....	17
OVA テンプレート方法	
vGW セキュリティ VM 用の単一方法.....	27
vGW セキュリティ デザイン VM 用の単一方法.....	26
OVA バンドル方法.....	18
パッケージのダウンロード.....	19

## S

サポート、テクニカル 参照 テクニカル サポート	
--------------------------	--

## T

テクニカル サポート	
JTAC へのお問い合わせ.....	xx

## V

vGW アンチウィルス	
オンアクセス スキャン.....	83
vGW セキュリティ VM.....	36

vGW セキュリティ デザイン VM	
イントロスペクション モジュール.....	104, 105
Applications feature.....	95
VMs feature.....	97
vGW セキュリティ デザイン VM モジュール	
コンプライアンス モジュール.....	107
ファイアウォール モジュール.....	59
vMotion.....	9
VMsafe	
インターフェース.....	9
VMSafe .....	16
VMSafe ファイアウォールおよび監視モード.....	16
VMSafe モード	
VMSafe ファイアウォールおよび監視モード.....	16
VMware	
ESX/ESXi ホスト.....	9
vGW シリーズの統合	
preparation.....	15
vMotion.....	9
vSphere.....	9
インフラストラクチャと vGW.....	9
VMware Virtual Center (vCenter) .....	11
vNIC.....	11
vSphere.....	9, 11
vSwitch.....	11

## W

Web ブラウザ.....	11
---------------	----

## ア

アンチウィルス.....	77
概要.....	77

## イ

イベントとアラート.....	45
インストール	
前提条件とリソース要件.....	11
インストール モード	
VMSafe ファイアウォールおよび監視モード.....	16
イントロスペクション モジュール	
VM 機能.....	97
アプリケーション機能.....	95
スキャン ステータス機能.....	105
スケジュール機能.....	104

## ク

クラウド コンピューティング.....	8
---------------------	---

コ		分	
コンプライアンス モジュール.....	107	分散リソース スケジュール.....	198
シ		委	
システム コンポーネントの更新.....	183	委任センター.....	133
vGW セキュリティ VM.....	183	概	
vGW セキュリティ デザイン VM.....	183	概要.....	3
ス		設	
ステータスとステータス アイコン.....	45	設定モジュール	
スマート グループ.....	172	マルチセンター.....	133
ナ		高	
ナビゲーション ボタン バー.....	39	高可用性.....	195, 198
ネ		分散リソース スケジュール.....	195, 198
ネットワーク接続.....	11		
フ			
ファイアウォール モジュール.....	59		
ポ			
ポート グループ.....	11		
マ			
マルチセンター機能.....	133		
メ			
メイン モジュール.....	45		
リ			
リソース要件			
DNS サービス.....	11		
NTP サービス.....	11		
VMware Virtual Center (vCenter) .....	11		
vNIC.....	11		
vSphere.....	11		
vSwitch.....	11		
Web ブラウザ.....	11		
ネットワーク接続.....	11		
ポート グループ.....	11		
仮想アプライアンス.....	11		
仮想デバイス.....	11		
仮			
仮想アプライアンス.....	11		
仮想デバイス			
サイズ.....	11		