さくらのクラウド「Sophos UTM」

Owlook

サービス利用手順書

かんたんネットワークプロテクション編

第 1.0 版

2018 年 1 月 25 日

興安計装株式会社
KOANKEISO

目　次

内容

改訂履歴

版数	更新日	更新内容	更新者
1.0	2018/1/25	初版作成	興安計装株式会社

はじめに

本手順書に関する注意事項

この手順書は、一般的な評価環境を簡単なステップで構築するための補助資料です。導入に際して必要な全てのトピックについての網羅的な解説は意図しておりません。個々のトピックについての詳細は、管理者ガイドをご確認頂くようお願い致します。

本サービスにおけるお問い合わせは、さくらインターネット株式会社が提供するサポート窓口をご利用いただくか、技術情報にて公開されたナレッジをご参照ください。本サービスの製品 SophosUTM9 の開発元であるソフォス株式会社への直接の問い合わせを固く禁じます。

本手順書の目的と位置づけ

目的: Sophos UTM9 の配下に展開された保護対象システム（サーバ若しくはクライアント）をネットワークプロテクションの各機能で保護する基本設定手順をご提供すること。

本手順の順番に沿って設定を進めて頂くことにより、Sophos UTM9 によるシステムの保護に必要な初期構成が可能となります。

本手順書ではサービス利用手順【初期導入編】に従い、セットアップされていることを前提としております。またネットワークプロテクション以外の機能については、本手順書には記載しておりません。

1. サービスについて

（1）サービス提供内容

提供項目	内容
Sophos UTM9 アーカイブイメージ	一部機能を除き、動作検証及び初期設定が完了した状態のアーカイブイメージを提供します。
Sophos UTM9 利用ライセンス	当社が提供したアーカイブイメージから展開したSophosUTM9 のみが適用可能なライセンスを提供します。

（2）サービス提供範囲

本サービスで提供される SophosUTM9 の機能は以下の通りです。

サービス項目	機能
ネットワークサービス	・DNS ・DHCP ・NTP 上記に付随する各種オプション
ユーザポータル	リモートアクセスサービスを提供するブラウザベースアプリケーションと付随する各種オプション
ネットワークプロテクション	・ファイアウォール ・侵入防御(IPS) ・高度な防御機能(ATP) 上記に付随する各種オプション
Web プロテクション	・Web フィルタリング ・アプリケーションコントロール 上記に付随する各種オプション
E メールプロテクション	・SMTP プロキシ ・POP3 プロキシ 上記に付随する各種オプション
高度な防御	よりリスクの高い通信の防御
Web サーバプロテクション	・Web Application Firewall（WAF） 上記に付随する各種オプション

サイト間 VPN	・IPsec ・SSL ・Amazon VPC
リモートアクセス	・SSL ・PPTP ・L2TP over IPsec ・IPsec ・HTML5 VPN ポータル ・Cisco™ VPN クライアント
ログとレポート	・各サービスのログ取得 ・各サービスのレポート作成 ・エグゼクティブサマリーレポートの作成

本サービスで提供される SophosUTM9 の詳細機能については Owlook セキュリティマネジメントサービス仕様書内の３．提供機能の詳細をご参照ください。

（3）サービス利用条件

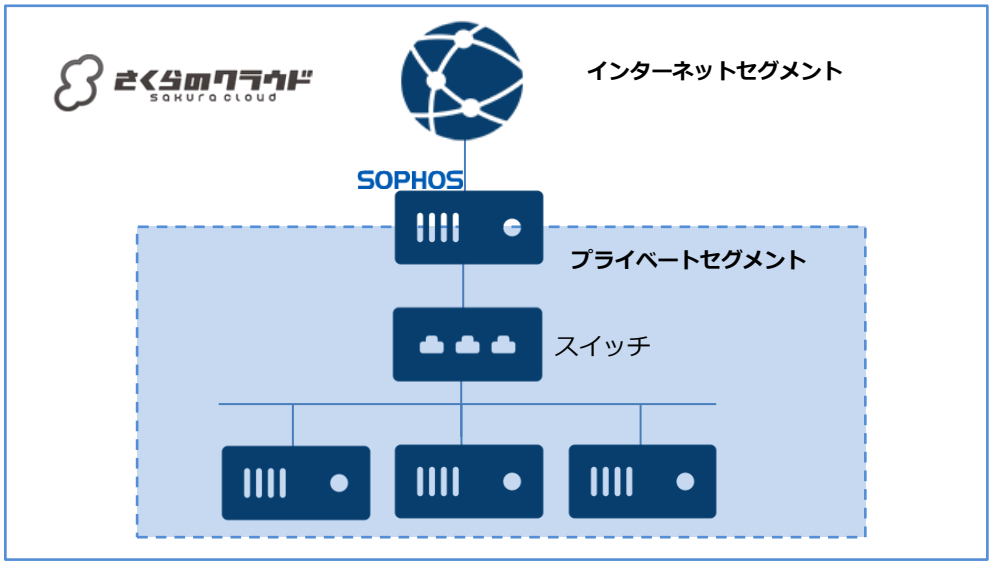
本サービスの利用条件は以下の通りです。

①ご利用環境

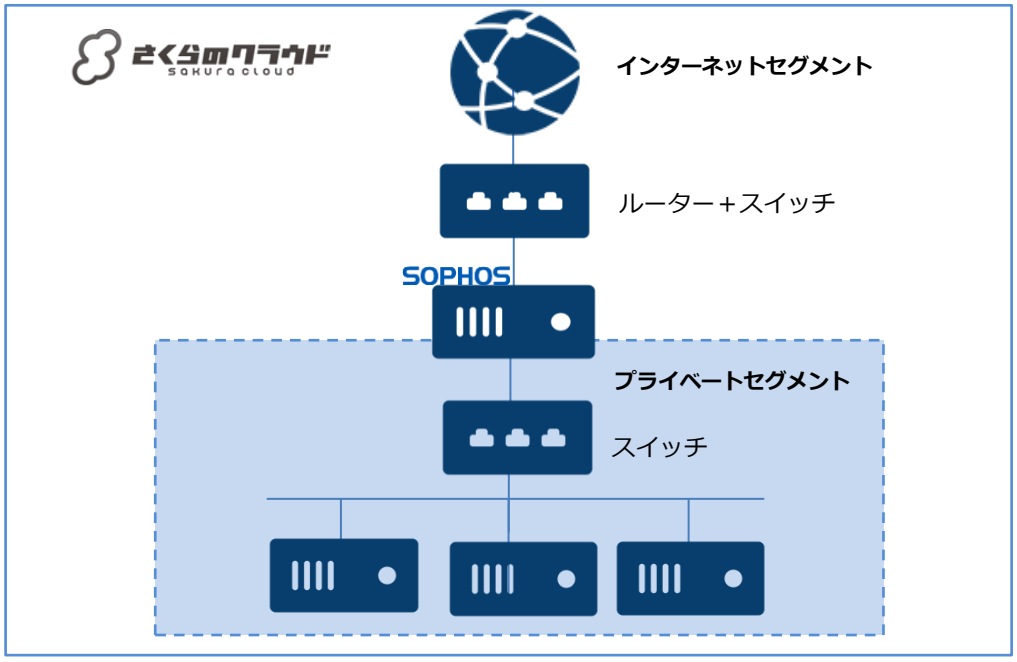
さくらのクラウドサービス内の全てのリージョンよりご利用可能です。

②推奨導入構成

Sophos UTM9 はご利用の環境における外部（インターネット）との接続点への導入し、内部はスイッチを利用しセグメントを構築してください。



また以下のように、ルーター＋スイッチ機能で SophosUTM9 へ任意の IP アドレスを設定することが可能です。



③サイジング

さくらのクラウドサービス環境へ SophosUTM9 を展開した場合のスペック目安は以下の通りです。あくまで目安でありパフォーマンスを保証する数値ではありません。ハイパーバイザーのご利用環境によって最大 10%までのパフォーマンスの低下が予想されます。

vCPU	2	2	4	4	2*6	2*10
メモリ(GB)	4	8	12	16	24	48
HDD(GB)	100※1					
FW 最大※2 (Mbps)	3,100	13,000	20,000	25,000	40,000	60,000
IPS 最大 (Mbps)	750	3,000	6,000	7,000	12,000	16,000
FW + ATP + IPS 最大 (Mbps)	680	2,850	5,890	6,650	11,980	14,600
新規最大 TCP 接続/秒	24,000	70,000	120,000	130,000	160,000	190,000
同時最大 TCP 接続数	2,000,000	4,000,000	6,000,000	8,000,000	12,000,000	20,000,000
同時最大接続 IPsec VPN トンネル数	175	500	1,200	1,600	2,200	2,800
同時接続 SSL VPN トンネル数	75	200	250	280	340	420

※1　Disk サイズの推奨は 100GB です。ログの保持には Syslog サーバへの転送機能を推奨します。

※2　1518 バイトのパケットサイズ、デフォルトのルールセット環境の目安値です。

（4）サービス利用の流れ

本サービスご利用までの流れは以下の通りとなります。実施内容についての詳細手順はさくらインターネットより技術情報として公開されています。

提供ステップ	実施内容
①さくらのクラウドサービスのアカウント取得	本サービスはさくらのクラウドサービス上で提供可能なサービスとなります。その為、利用者はさくらのクラウドサービスが利用できる状態であることが前提となります。
②SophosUTM9 の展開	さくらのクラウドサービスより本サービスより提供される SophosUTM9 のアーカイブイメージをパブリックアーカイブから展開します。
③利用規約へ同意	SophosUTM9 へ初回ログイン時に表示される URL より利用規約を確認し、同意頂きます。

④ライセンスサーバーへの接続	SophosUTM9 へ当社が提供するライセンスサーバへ接続設定を行います。
⑤利用ライセンスの有効化	SophosUTM9 がライセンスサーバへ接続後、利用ライセンスが有効になります。利用ライセンスの有効化処理はご利用環境によって 30 分程お待ちいただく事があります。
⑥利用開始	SophosUTM9 の機能がご利用いただけるようになり、利用者にて設定が可能となります。
⑦利用終了	SophosUTM9 を一定期間停止、または削除した場合、ライセンスは破棄され利用終了となります。

（５）サービス提供範囲外の機能について

本サービスで提供される Sophos UTM9 利用ライセンスはほぼすべての機能をご利用いただく事が可能なライセンスです。その為、本サービス仕様書に記載のない機能も利用ライセンスに含まれます。

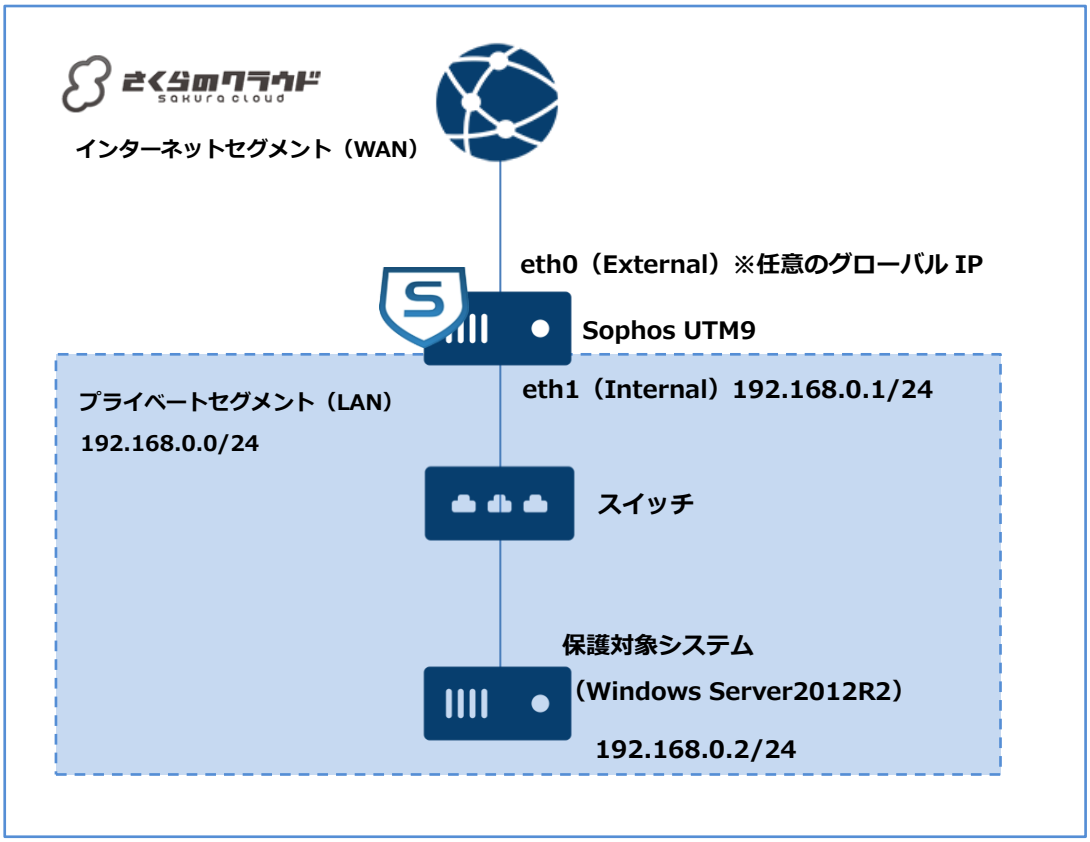
またさくらのクラウドサービス環境では、Sophos UTM9 に搭載された HA クラスタ機能及びブリッジインターフェイスの構成をご利用いただく事ができません。

本サービス仕様書に記載がある機能は、推奨導入構成において動作確認ができている機能となります。

本サービス仕様書に記載のない機能または、推奨外の構成でご利用いただく場合、本サービス内でサポートすることはできません。本サービス仕様書に記載のない機能または、推奨外の構成は、利用者の責任でご利用いただきますようお願いいたします。

2. ご利用環境の構成

本手順書では以下の構成であることを前提に記載いたします。



【構成要件】

- Sophos UTM9 はご利用の環境におけるインターネットとの接続点へ導入します。
- Sophos UTM9 はインターネットセグメント（WAN）側とプライベートセグメント（LAN）側の 2 つの NIC を持ちます。プライベートセグメント（LAN）側の IP アドレスは 192.168.0.1/24 を持ちます。
- プライベートセグメント（LAN）は 192.168.0.0/24 のネットワーク帯域で構成します。
- プライベートセグメント（LAN）はスイッチを利用しセグメントを構築します。
- 保護対象システムの IP アドレスは 192.168.0.2/24 を持ちます。
- 保護対象システムのデフォルトゲートウェイは Sophos UTM9 のプライベートセグメント（LAN）側の IP アドレス 192.168.0.1/24 を向いています。

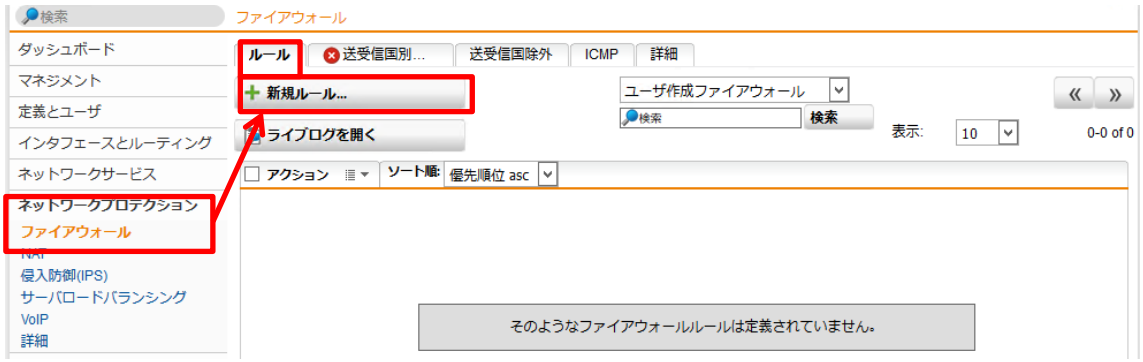
3．ネットワークプロテクション機能の初期設定

3－1．ファイアウォール

（1）初期ポリシーの設定手順

ファイアウォールは初期状態ですべての通信を「拒否」します。その為、通信を許可するポリシーを追加する必要があります。

①ネットワークプロテクション ＞ ファイアウォール ＞ルールタブより、「新規ルール」を押下します。



②「ルールを追加」画面に遷移します。以下の通り、設定を入力し、「＋」ボタンを押下し詳細メニューを展開します。

グループ：グループなし

優先順位：最下位

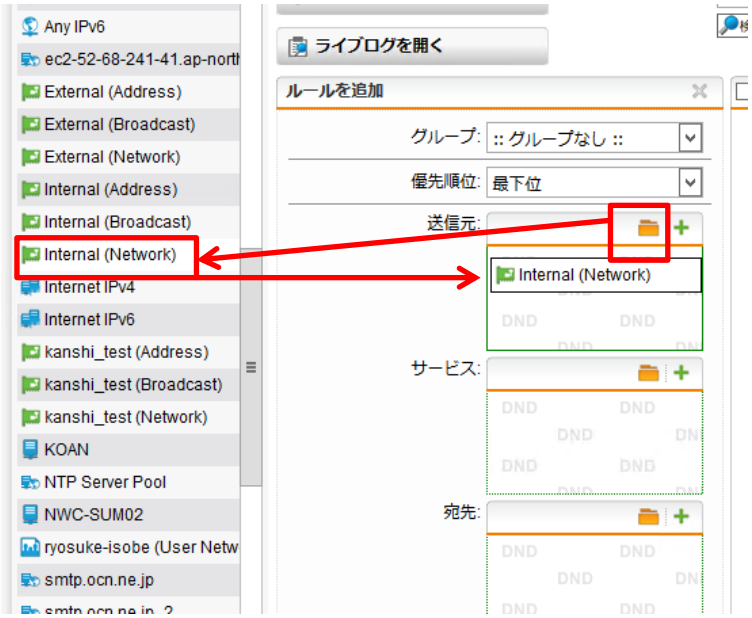
送信元：Internal（Network）

サービス：Any

宛先：Any

アクション：許可

この時、送信元、サービス、宛先のフォルダアイコンを押下すると、左メニューにオブジェクトが転嫁されます。オブジェクトの一覧からドラック&ドロップで設定が可能です。



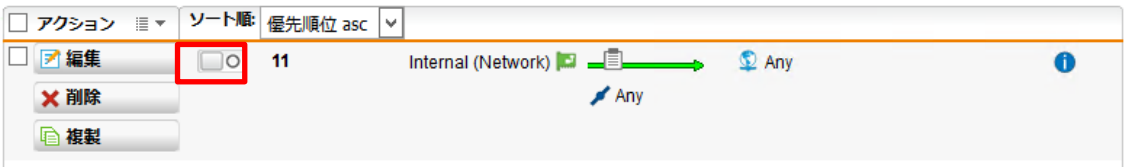
③「詳細」より以下の通り、設定を入力し、「保存」ボタンを押下します。

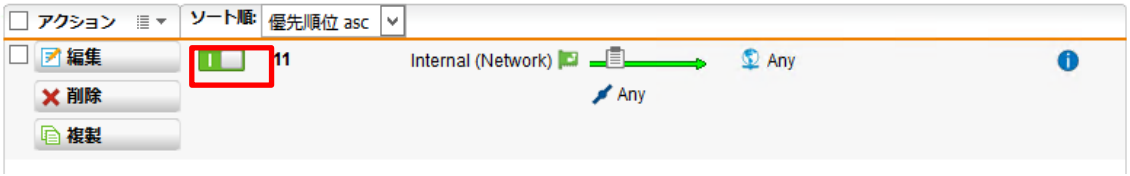
時間帯：常時

トラフィックをログ：チェック

送信元 MAC アドレス：なし

④ポリシー作成直後は、「無効」状態になっているため、有効化ボタンを押下し、ポリシーを有効にします。



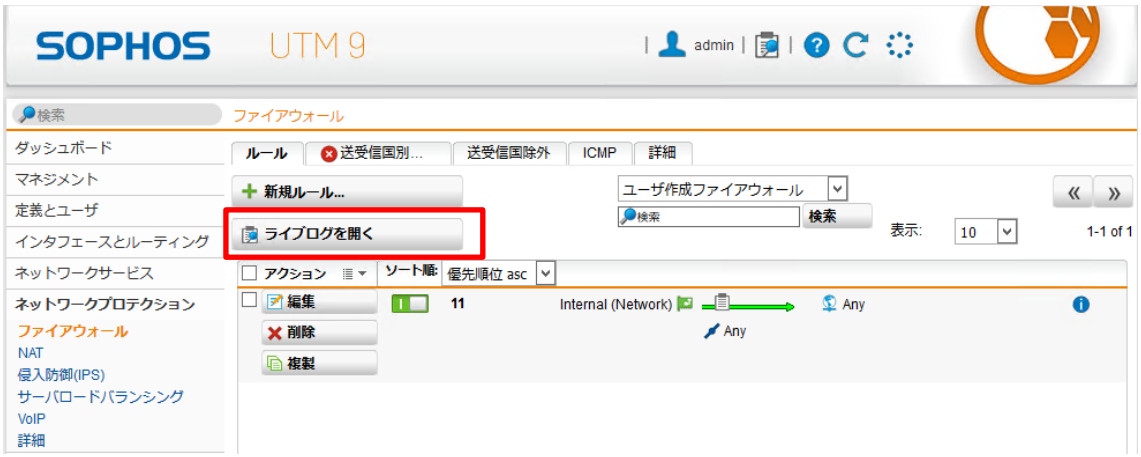


以上で、初期ポリシーの設定手順は完了です。

（2）ライブログの確認手順

ファイアウォールの動作状況をライブログで確認するには、下記の手順を実行します。

①「ライブログを開く」ボタンを押下します。



②別ウィンドウでログ画面が立ち上がります。ルールに一致したもの、拒否したもの等の通信状態をリアルタイムに確認することができます。

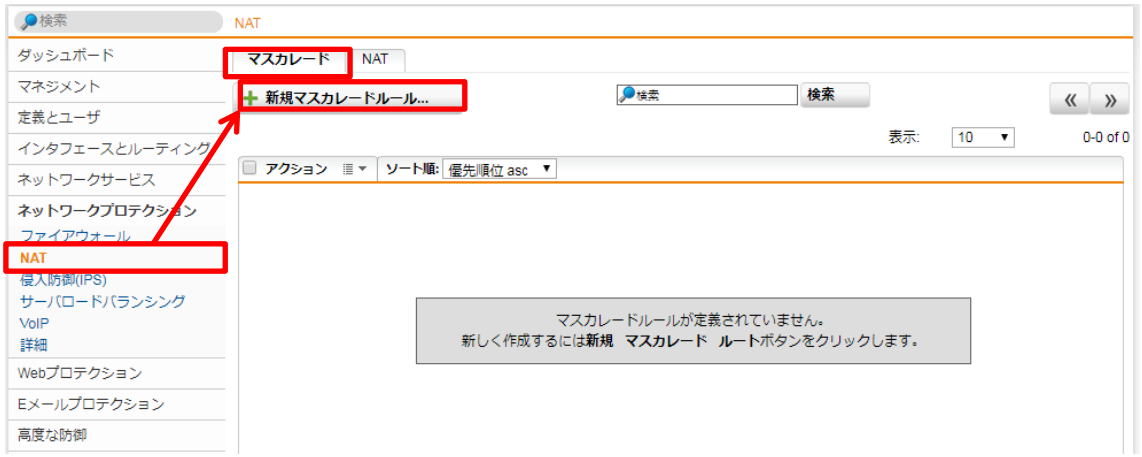
ファイアウォールルールをオンにしたりオフにしたりして通信されているパケットの状態をご確認ください。

3－2．NAT

（1）マスカレード設定手順

マスカレードの機能を利用して内部ネットワークから外部のネットワークへアクセスするには、下記の手順を実行します。

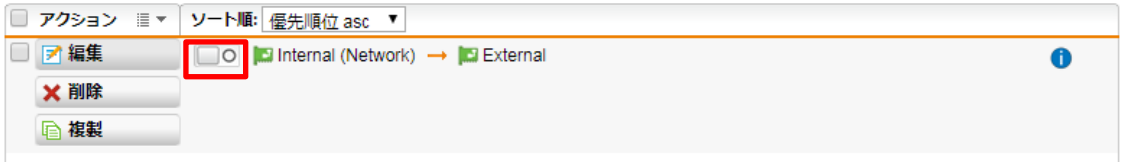
①ネットワークプロテクション　＞　NAT ＞　マスカレードタブより「新規マスカレードルール」ボタンを押下します。

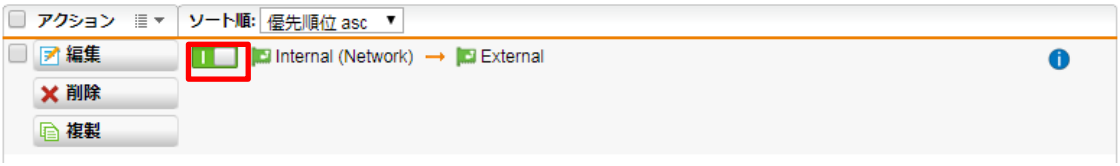


②「マスカレードルール」を追加より、以下の通り入力し、「保存」ボタンを押下します。

ネットワーク：Internal（Network）
優先順位：最下位
I/F：External
使用アドレス：プライマリアドレス

③有効化ボタンを押下しマスカレードルールを有効にします。





（2）DNAT の設定手順

DNAT(Destination NAT)ルールを設定するには、以下の手順を実行します。
ここではインターネット上の任意のユーザから、保護対象システム（Windows Server2012R2）にカスタマイズしたポート番号でリモートデスクトップ接続する想定の手順となります。

①ネットワークプロテクション　＞ NAT ＞ NAT タブより「新規マスカレードルール」ボタンを押下します。

②「NAT ルールを追加」より、以下の通り入力します。

グループ：グループなし
優先順位：最下位
ルールタイプ：DNAT（宛先）

③マッチング条件の欄は以下の通り入力します。

トラフィック送信元：Any
サービス：53389
トラフィック宛先： External（Address）

この時、サービスについては新たにサービスを定義する必要があります。「＋」ボタンを押下して「サービス定義の追加」を開き以下の通り入力し「保存」を押下します。

名前：53389　※任意

定義タイプ：TCP

宛先ポート：53389

送信元ポート：1:65535

④アクションの欄、詳細は以下の通り入力します。

変換後の宛先：192.168.0.2

サービス：Microsoft Remote Desktop

自動ファイアウォールルール：チェック

初期パケットのログ：チェック

この時、変換後の宛先については新たにネットワークオブジェクトを追加する必要があります。「＋」ボタンを押下して「ネットワークオブジェクトを追加」を開き以下の通り入力し「保存」を押下します。

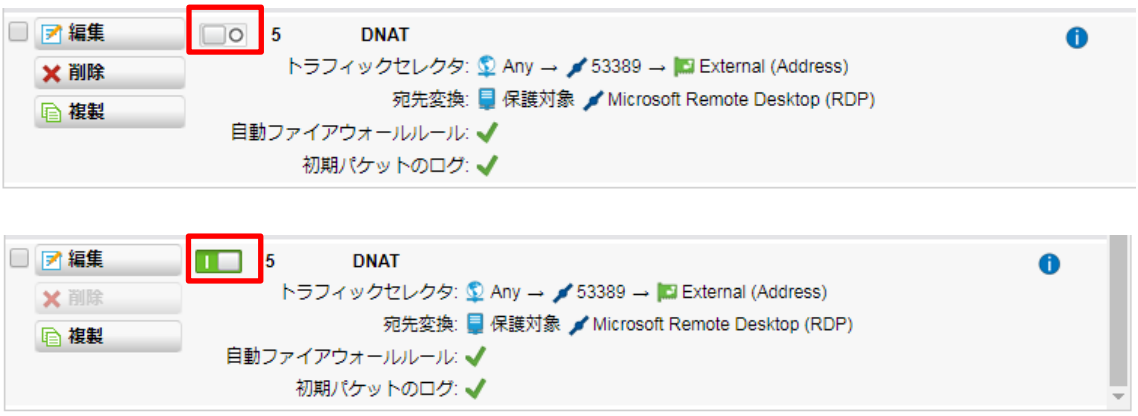
名前：保護対象　※任意

タイプ：ホスト

IPv4 アドレス：192.168.0.2

⑤入力が完了したら「保存」ボタンを押下します。

⑥有効化ボタンを押下し DNAT ルールを有効にします。



⑦設定をテストします。WAN 側クライアント PC から Sophos UTM9 の WAN 側インタフェースの公開用 IP アドレスに 53389 ポートでアクセスすることで、保護対象システム（Windows Server2012R2）にアクセスすることができます。

3－3．侵入検知（IPS）

ここでは、外部ネットワークから内部ネットワークに対する不正アクセスに対する防御機能である、「侵入防御（IPS）」について説明します。

（1）グローバル設定手順

①ネットワークプロテクション　＞　侵入検知（IPS）　＞　グローバルタブより「IPS ステータス」ボタンを押下します。

②IPS の検知を有効にするネットワーク及び、インターフェイスを指定します。

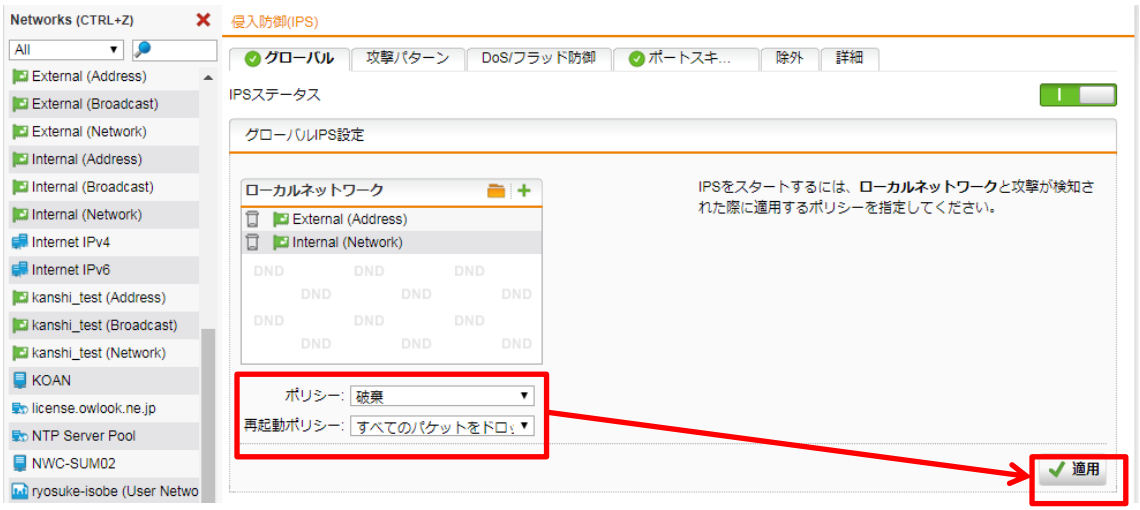
今回は、外部からの不正アクセス及び内部ネットワークの不正アクセスに対する防御を有効にするため、以下のポリシーを適用します。

External（Address）

Internal（Network）

フォルダアイコンをクリックし該当のオブジェクトをドラックアンドドロップします。

③ポリシー及び再起動ポリシーはデフォルトのまま、「適用」ボタンを押下し設定を保存します。



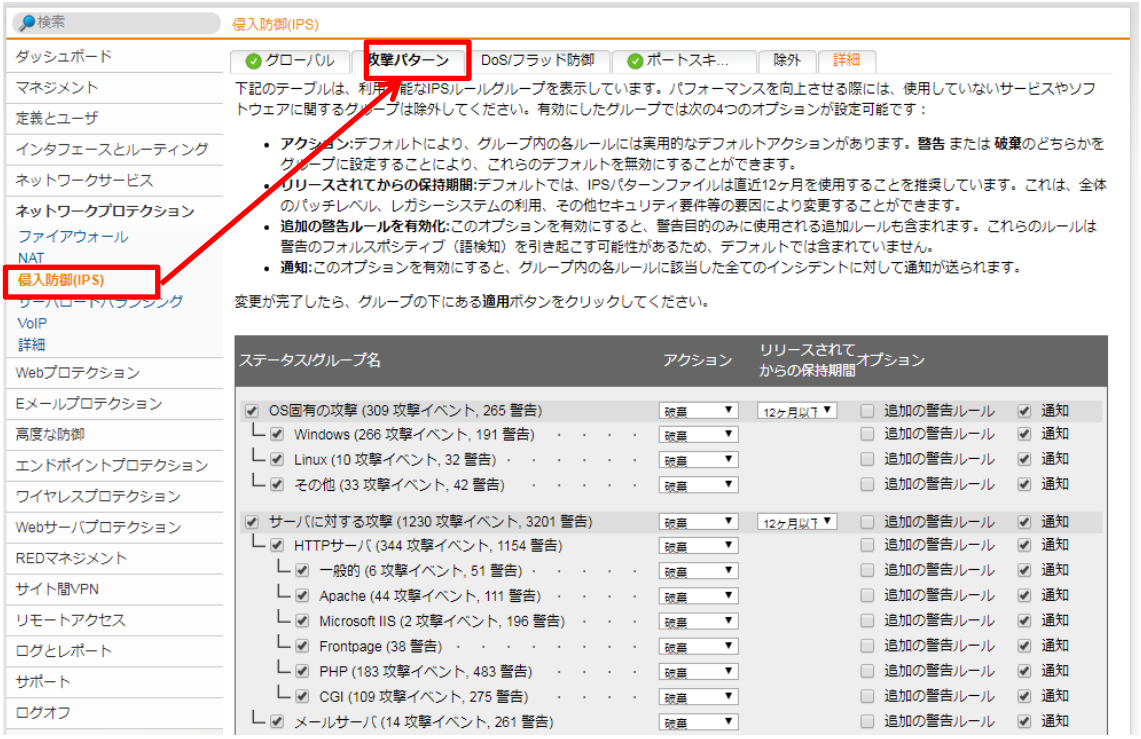
以上で、グローバル設定手順は完了です。

（2）攻撃パターン設定手順

①ネットワークプロテクション ＞ [侵入防御（IPS） ＞ 攻撃パターンタブを開きます。

攻撃の種類は大きく分けて以下の 6 種類があり、それらに対する詳細な攻撃パターンに対して個別に設定できます。

・ OS 固有の攻撃
・ サーバに対する攻撃
・ クライアントソフトウェアに対する攻撃
・ プロトコルアノマリー
・ マルウェア



②アクションの設定が完了したら、「適用」ボタンを押下します。

以上で、攻撃パターン設定手順は完了です。デフォルトでは全ての攻撃を検知する設定になっています。細かいチューニングについては管理者ガイドを参考に環境に合わせチューニングしてみてください。

（3）DoS フラッド防御設定手順

②アクションの設定が完了したら、「適用」ボタンを押下します。

ネットワークプロテクション ＞　侵入防御（IPS）　＞DoS フラッド防御タブを開きます。

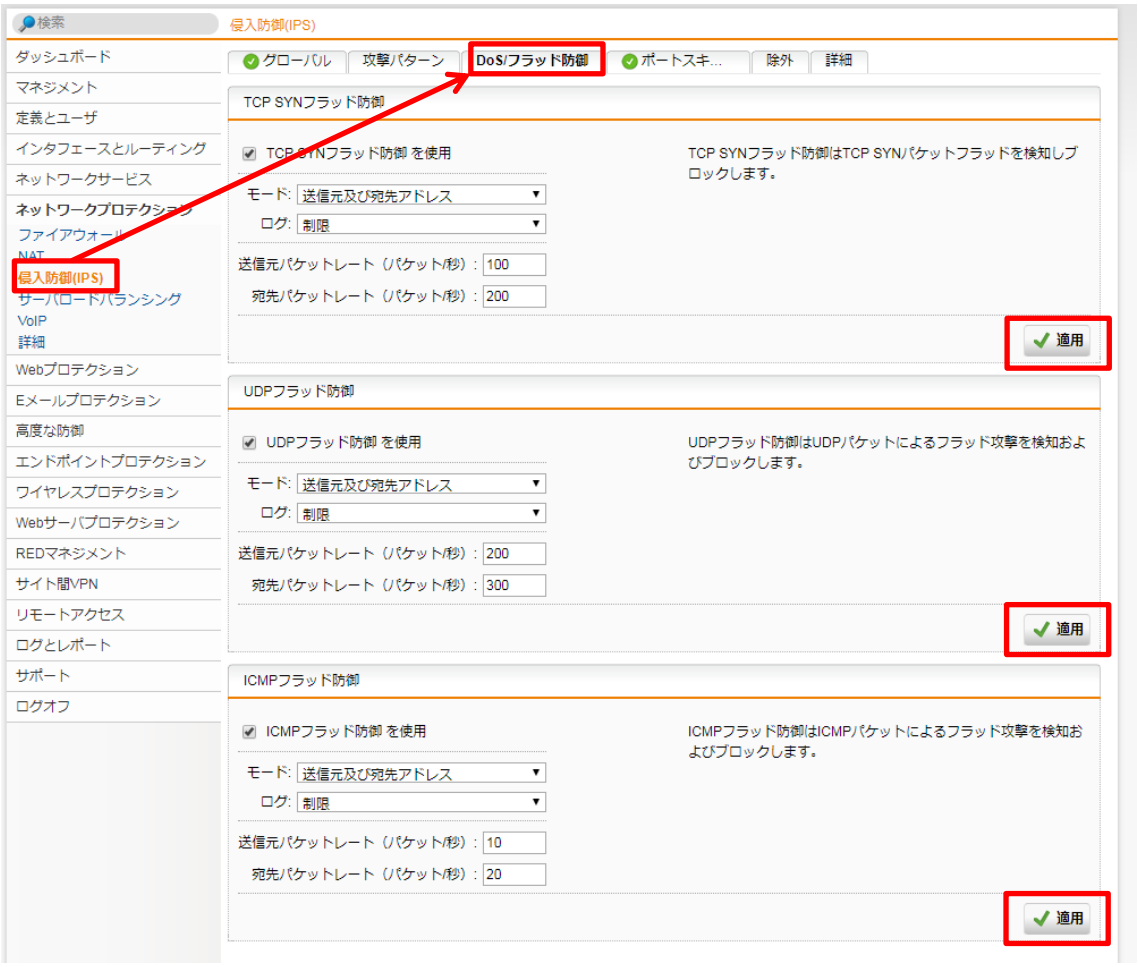
DoS フラッド防御の種類は以下の 3 種類があり、それぞれ個別の設定を行うことができます。

・ TCP SYN フラッド防御

・ UDP フラッド防御

・ ICMP フラッド防御

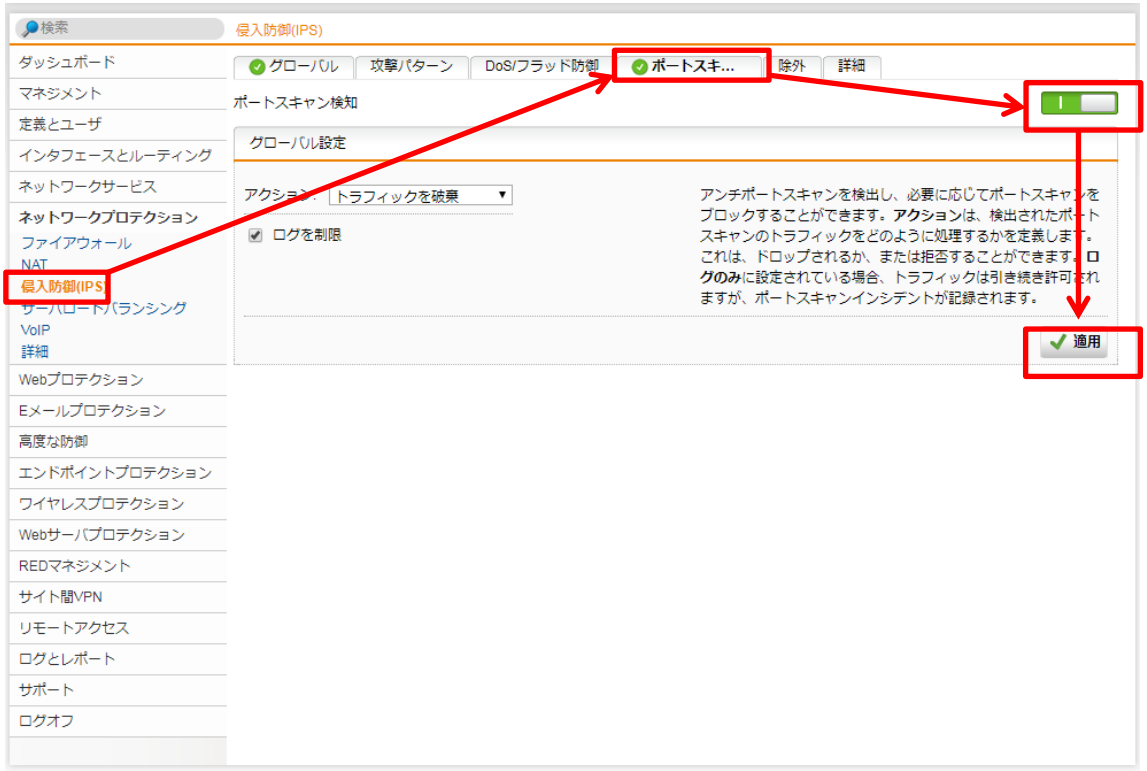
設定が終了したら、項目ごとに「適用」ボタンを押下し設定内容を反映させてください。



以上で、DoS フラッド防御設定手順は完了です。デフォルトではこの機能は無効になっています。細かいチューニングについては管理者ガイドを参考に環境に合わせチューニングしてみてください。

（4）ポートスキャン防御設定手順

①ネットワークプロテクション ＞ 侵入防御（IPS） ＞ ポートスキャン防御]タブを開きます。
デフォルトでは、機能はオフの状態ですのでをクリックして機能をオンにします。
アクションのプルダウンリストから、ポートスキャンに対するアクションを選択し 「適用」を押下します。



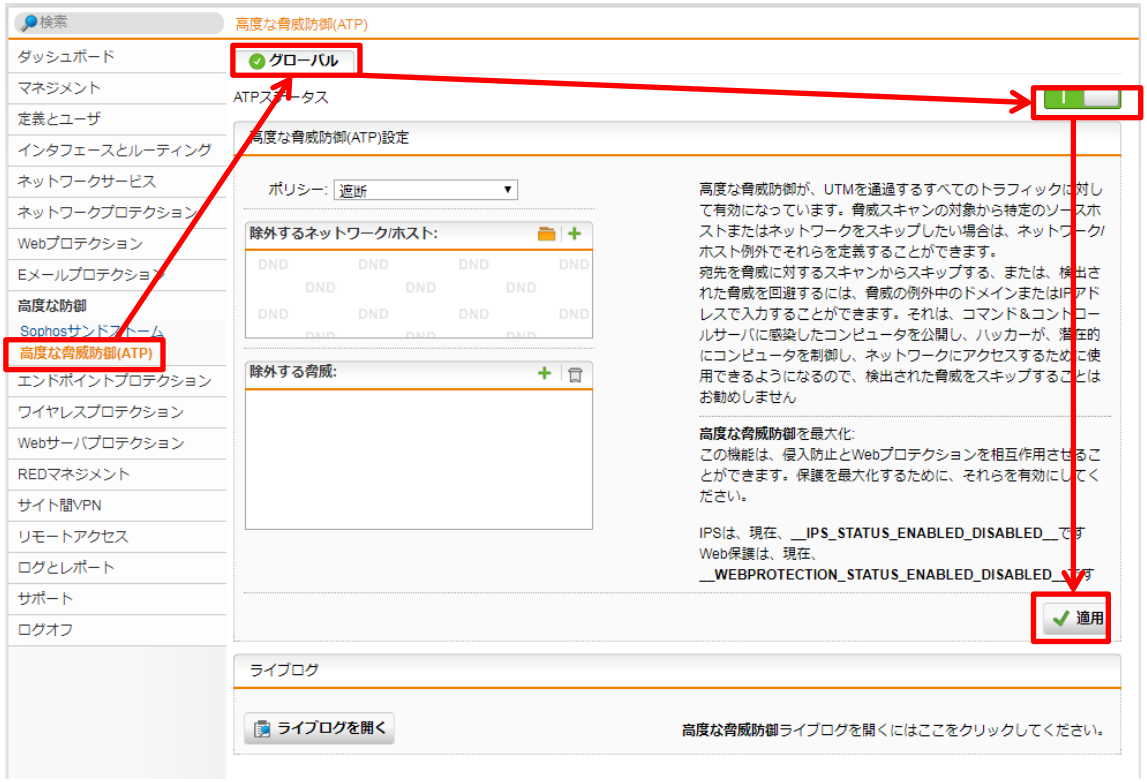
以上で、ポートスキャン設定手順は完了です。デフォルトではこの機能は無効になっています。細かいチューニングについては管理者ガイドを参考に環境に合わせチューニングしてみてください。

３－４．高度な防御（Advanced Threat Protection）

高度な防御（Advanced Threat Protection）機能を有効にすることでより、高度な検知が可能となります。侵入検知と合わせて有効にすることを推奨します。

（１）高度な防御（Advanced Threat Protection）設定手順

①高度な防御 ＞ 高度な脅威防御（ATP） ＞ グローバルタブを開きます。デフォルトでは、機能はオフの状態ですのでをクリックして機能をオンにし「適用」を押下します。



以上で、高度な防御（Advanced Threat Protection）設定手順は完了です。