さくらのクラウド向け

Owlook

仮想型 UTM マネジメント

サービス利用手順書

Sophos XG Firewall
ネットワークプロテクション編

第 2.0 版

2021 年 2 月 4 日

興安計装株式会社

目　次

内容

改訂履歴

版数	更新日	更新内容	更新者
1.0	2020/5/1	初版作成	興安計装株式会社
2.0	2021/2/4	v18 アップグレードに伴う改版	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、さくらのクラウド環境において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、ユーザーアシスタントをご確認頂くようお願い致します。

Sophos XG Firewall ユーザーアシスタント
https://docs.sophos.com/nsg/sophos-firewall/18.0/Help/en-us/webhelp/onlinehelp/index.html

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 Sophos XG Firewall 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:
１．IPS 機能を有効にする
２．フラッド防御を有効にする
３．DoS 防御を有効にする
４．高度な脅威防御（ATP）の設定

本手順書は以下の手順書に沿って Sophos XG Firewall が展開されアクティベートされた、状態を前提としております。

初期導入編

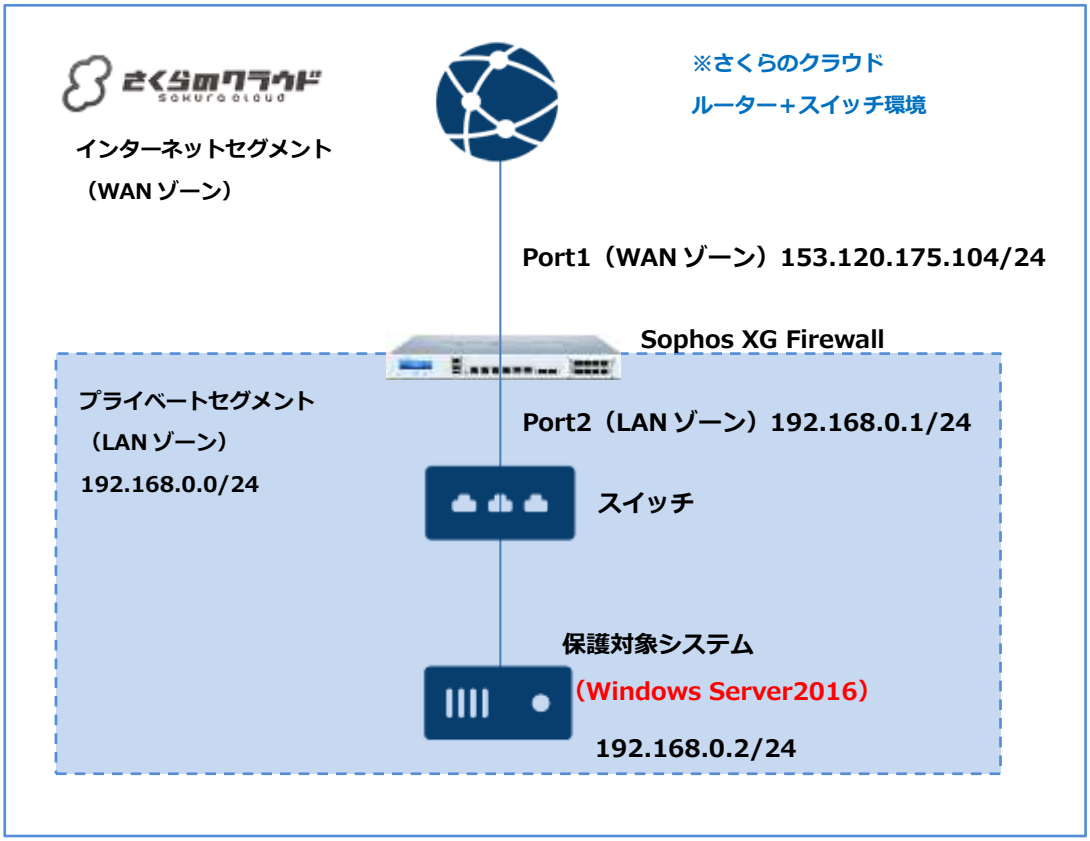
https://www.owlook.jp/public/document/sophos_xg_intruduction.pdf

ファイアウォールの設定、DNAT の設定編

https://www.owlook.jp/public/document/sophos_xg_fw_dnat.pdf

1．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 XG Firewall 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 XG Firewall は WAN ゾーン側と LAN ゾーン側の 2 つの NIC を持ちます。LAN 側の IP アドレスは 192.168.0.1/24 を持ちます。
- WAN ゾーンは 153.120.175.104 の IP アドレスを持ちます。
- LAN ゾーンは 192.168.0.0/24 のネットワーク帯域で構成します。
- LAN ゾーン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 XG Firewall の LAN ゾーン側の IP アドレス 192.168.0.1/24 を向いています。

2．ネットワークプロテクションの設定

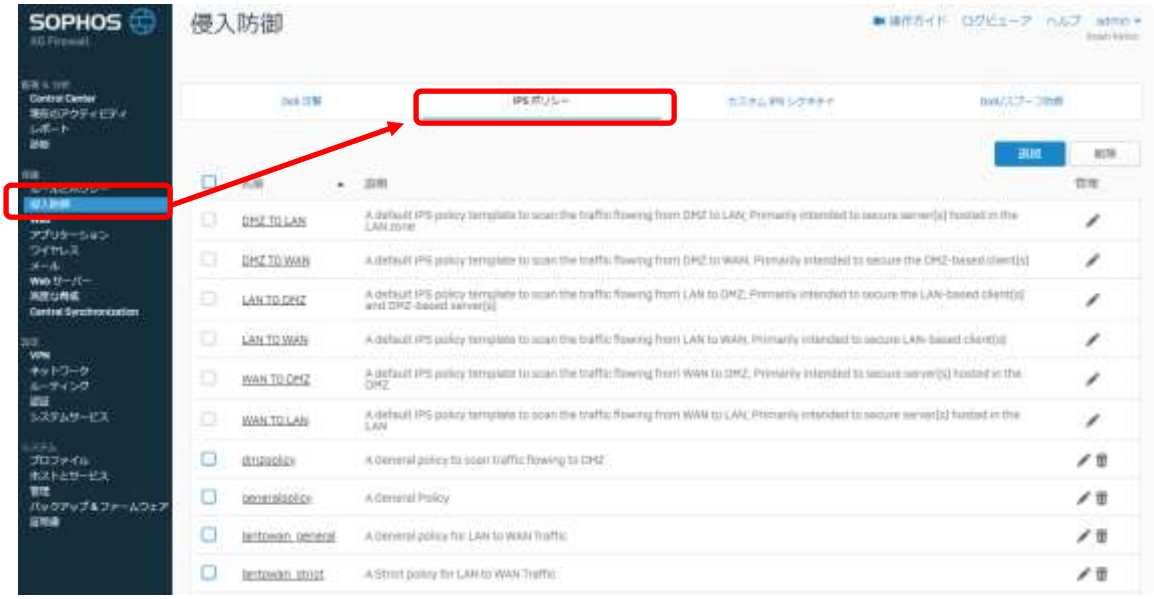
（1）ネットワークプロテクション機能の適用範囲

ネットワークプロテクション機能には以下の機能があります。機能と適用範囲は以下の通りです。

機能	説明	適用範囲
侵入防御（IPS）	シグネチャベースの検知機能です。	ファイアウォールポリシー単位
スプーフ防御	IP アドレスのスプーフィング攻撃を防止する機能です。	各ゾーン全体
DoS 防御	ネットワークホストへのフラッド攻撃を防止する機能です。	SophosXGFirewall 全体

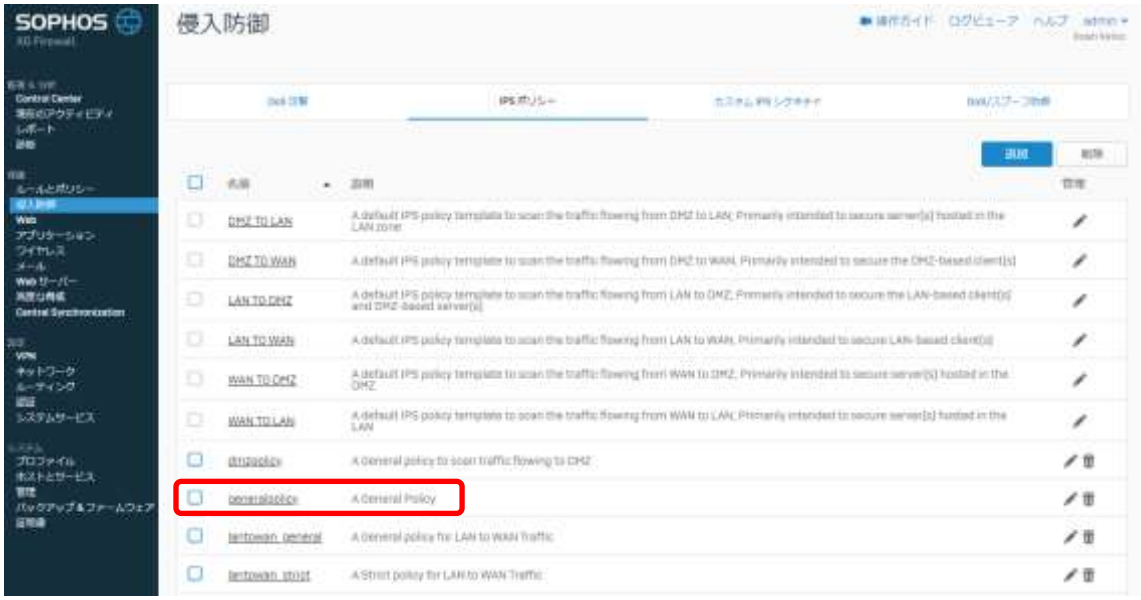
（2）侵入防御（IPS）の設定

①侵入防御　＞　IPS ポリシー　タブをクリックします。



IPS ポリシーはカスタマイズが可能ですが、今回は推奨されている「generalpolicy」を適用する手順を記載します。※手順の中では適用されているポリシールールの確認方法のみ記載します。

②「generalpolicy」をクリックします。



③適用されているフィルタが表示されます。今回はデフォルトの「Migrate_def_filter_1」をクリックします。

④IPS ポリシールールの編集画面が表示されます。デフォルトの「Migrate_def_filter_1」では推奨のシグネチャーリストが設定されています。※今回は内容の編集は行いません。

IPS ポリシールールは「カテゴリ」、「重要度」、「プラットフォーム（OS）」、「対象（Server か Client か）」でフィルタリングが可能です。もし、シグネチャを追加・削除したい場合、条件をフィルタリング後に選択したシグネチャが適用されます。※推奨としてはデフォルト設定のご利用を推奨しております。

「保存」はせずに「キャンセル」をクリックします。

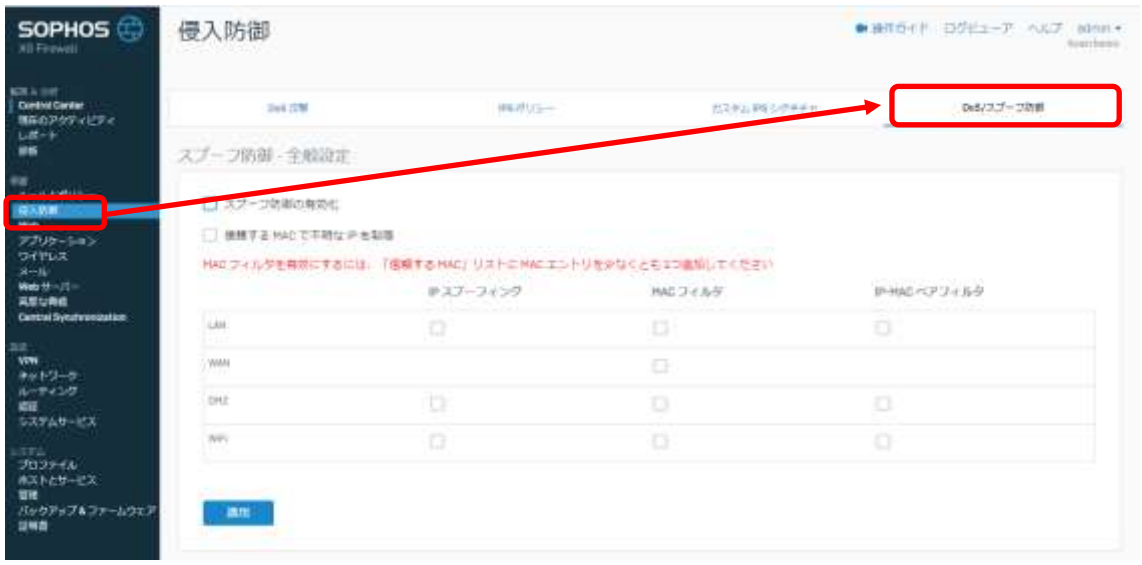
⑤ファイアウォール ＞ #Default_Network_Policy　をクリックします。

⑥その他のセキュリティ機能 ＞ エクスプロイトの検出・防止（IPS）＞ generalpolicy を選択し保存をクリックします。

以上で設定は完了です。#Default_Network_Policy を通過するトラフィックに対し、IPS ポリシー「generalpolicy」が有効になります。

（3）スプーフ防御を有効にする

①侵入防御 ＞ DoS/スプーフ防御 タブをクリックします。



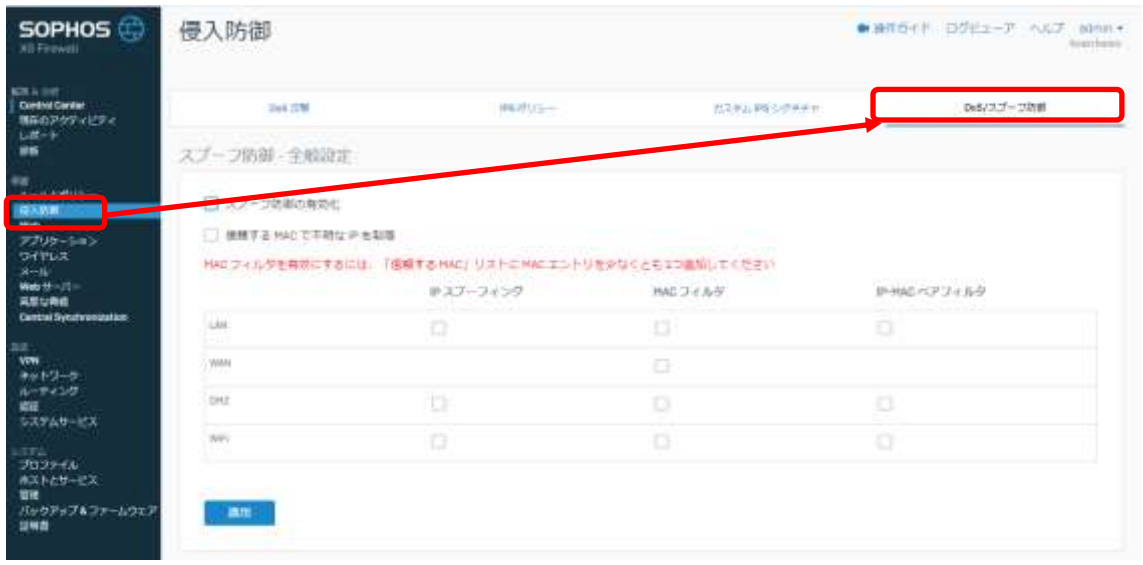
②今回は IP スプーフィングを有効にします。スプーフ防御の有効化をクリックします。

また防御対象とする、ゾーンを選択し適用をクリックします。今回は LAN ゾーンで有効にします。

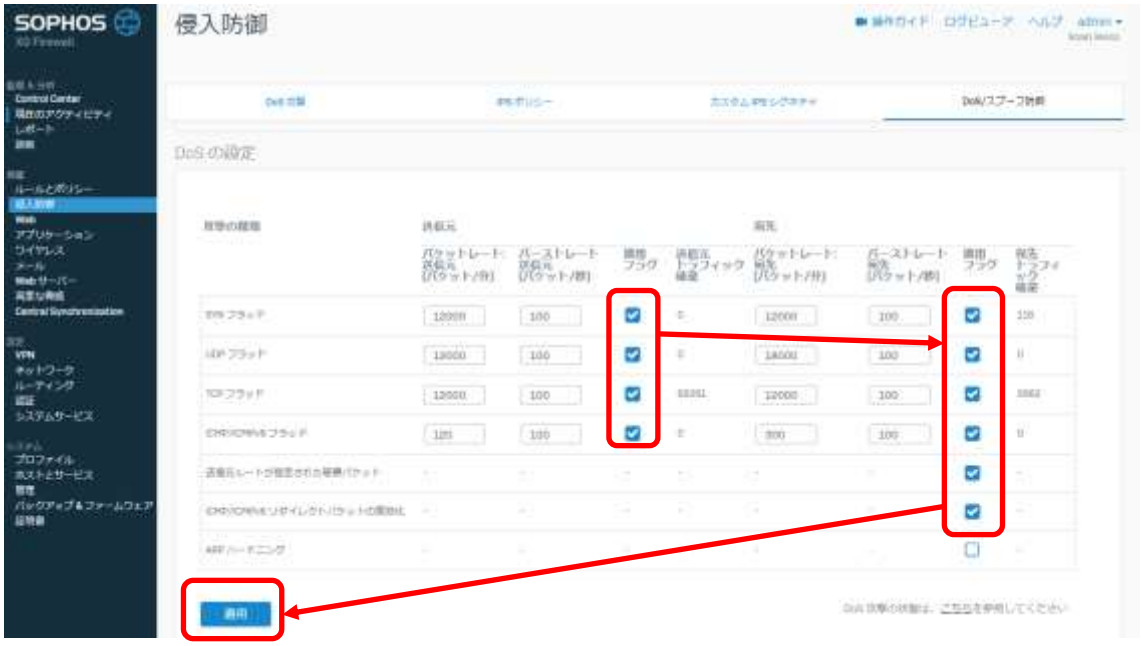
以上で設定は完了です。パケットの送信元 IP アドレスがファイアウォールのルーティングテーブルのいずれのエントリとも一致しなかった場合や、パケットが直接サブネットから送信されたものでない場合は、パケットを破棄します。※より厳密に管理する場合、MAC アドレスを IP アドレスと紐づけて管理することも可能です。

（4）DoS 防御を有効にする

①侵入防御 ＞ DoS/スプーフ防御 タブをクリックします。



②DoS の設定セクションで適用フラグをチェックし適用をクリックします。



以上で設定は完了です。今回は SYN フラッド、UDP フラッド、TCP フラッド、ICMP/ICMPv6 フラッドを、送信元、宛先それぞれに対しデフォルトのレートで設定しました。このレートを超えるパケットを破棄します。

（５）高度な脅威検知の設定

①高度な脅威 ＞ ATP（Advanced Threat Protection） タブをクリックします。

②Advanced Threat Protection のトグルスイッチを ON、ポリシーを「ログしてドロップ」に設定し適用をクリックします。

以上で設定は完了です。高度な脅威防御（Advanced Threat Protection）の機能は、内部から不正な通信を検出します。例えば、何らかの理由でマルウェアに感染してボット化したサーバが内部にあり、外部の C&C サーバ（ボット化したコンピュータ群へ指令を送り攻撃制御の中心

となるサーバ）へ接続を行おうとした場合に、ボット化したサーバからの通信を遮断してくれます。

3．最後に

本手順書では、ネットワークプロテクションの設定について記載しました。Sophos XG Firewall はヘルプより各画面ごとにユーザーアシスタントへリンクされており、必要なときに必要な個所を閲覧することが可能です。画面の上部フレーム内のヘルプを押下します。

以下のようなユーザーアシスタント（オンラインヘルプ）が別タブで開きます。

以上