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 Firewall
ファイアウォールの設定、DNAT の設定編

第 4.0 版

2023 年 8 月 31 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	2020/4/24	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
3.0	2022/4/20	v18.5 アップグレードに伴う改版	興安計装株式会社
4.0	2023/8/31	v19.5 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 Firewall オンラインヘルプ
https://doc.sophos.com/nsg/sophos-firewall/19.5/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 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

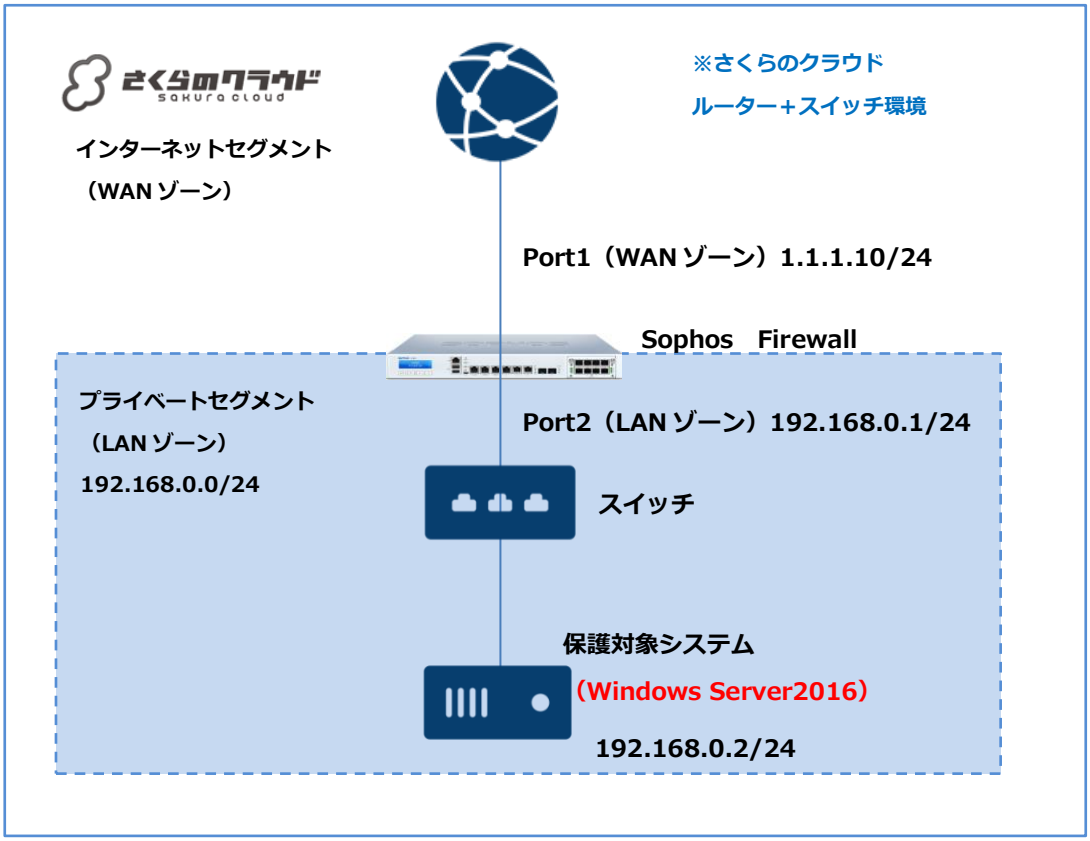
目的:
１．ファイアウォールのデフォルトポリシーの確認（IP マスカレードの設定）
２．DNAT の設定（グローバルから Sophos Firewall を経由して配下のサーバへのリモートデスクトップ接続ができるよう設定）
３．ログビューアを利用した接続確認

本手順書は以下の手順書に沿って Sophos 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。

初期導入手順書
https://www.owlook.jp/public/document/sophos_firewall_intruduction.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 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 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 1.1.1.10 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 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。
- **※IP アドレス等、設定値については、それぞれの環境に読み替えてご参照ください。**

2．ファイアウォールの設定

デフォルトで設定されているルールの確認

①画面左側のメニューから、ルールとポリシーをクリックします。

デフォルトで設定されているファイアウォールルールが存在します。

ポリシーグループ

・Traffic to Internal Zones

・Traffic to WAN

・Traffic to DMZ

※グループ内のポリシーはデフォルトで無効になっています。

単体ポリシー

・Auto added firewall policy for MTA

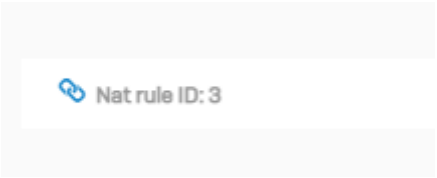
Sophos Firewall から通知メールを許可するためのポリシーです。

・#Default_Network_Policy

デフォルトですべてのトラフィックを拒否するマスカレードポリシーです。

②#Default_Network_Policy をクリックします。

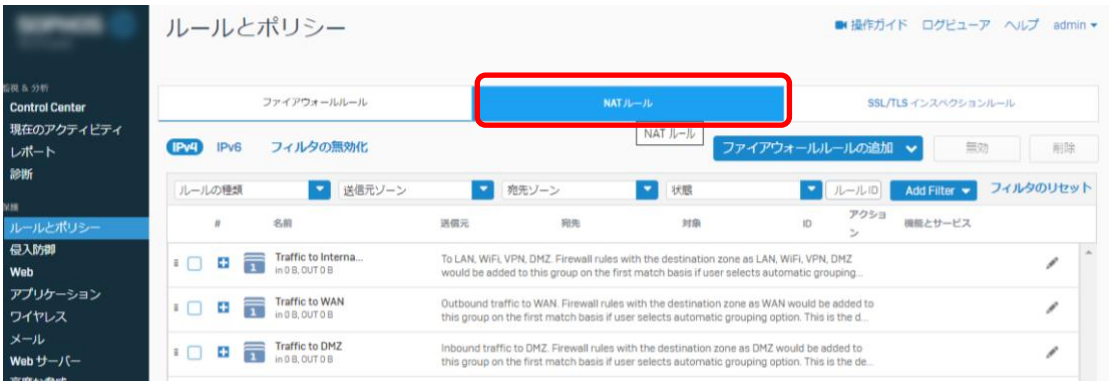
③Nat rule セクションで以下の設定がされていることを確認します。



Nat rule ID:3

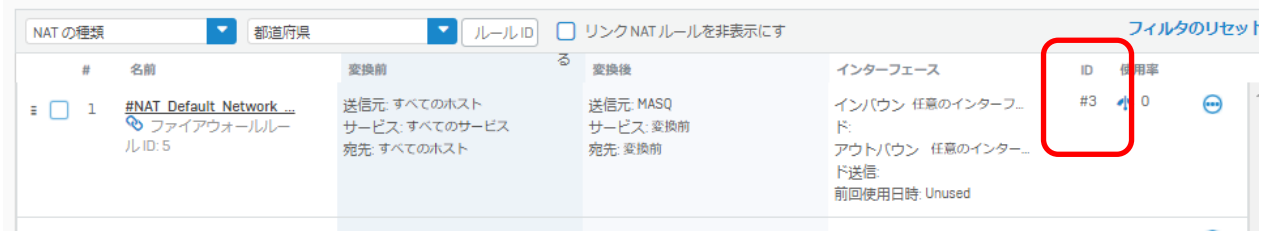
④今回は設定の確認のみのため「キャンセル」で設定画面を閉じます。

⑤NAT ルールタブをクリックします。

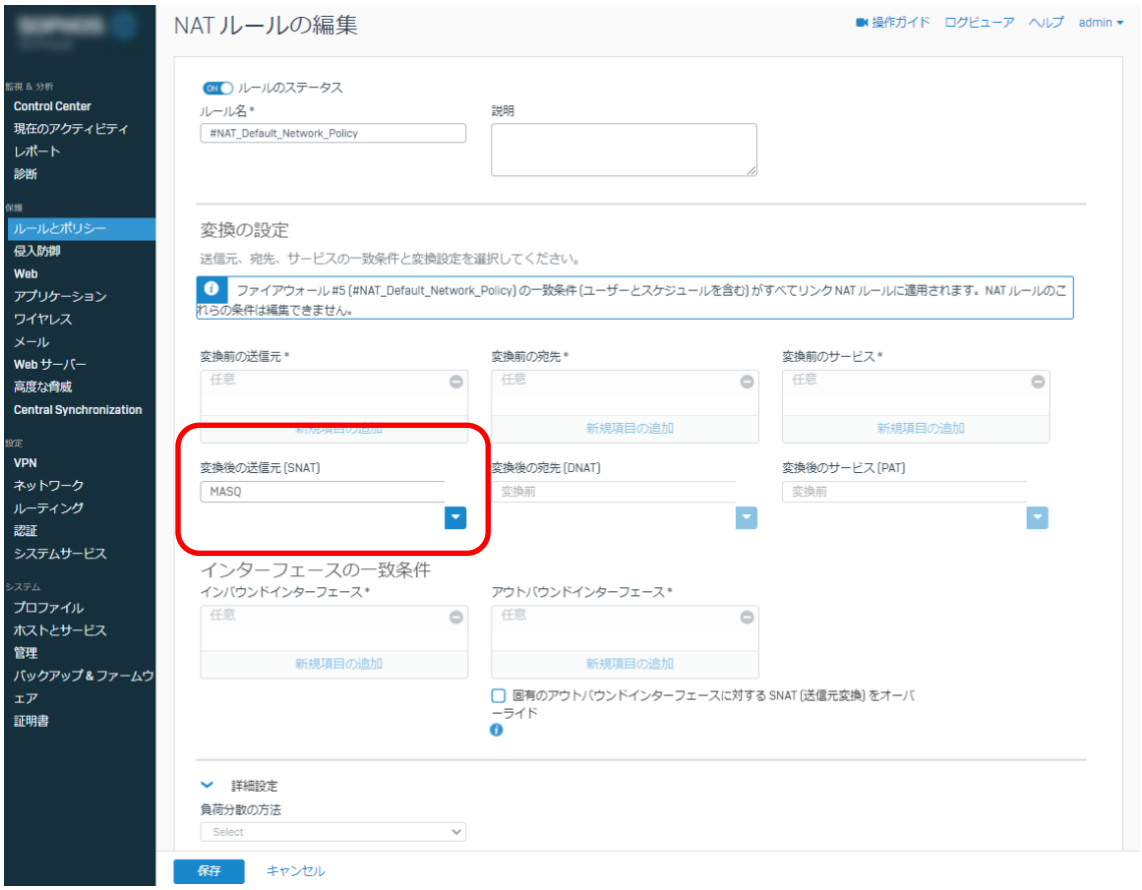


⑥NAT ルール ID３の内容を確認します。

※NAT ルール ID は以下の赤枠内の番号が NAT ルール ID となります。



⑦「変換後の送信元 (SNAT)」が「MASQ」となっています。保護対象クライアントがインターネットに通信する際、自動的にマスカレードされるポリシーがデフォルトで設定されます。



このように Sophos Firewall は「ファイアウォールルール」と「NAT ルール」が独立して存在しており、それぞれのルールをリンクさせる機能があります。デフォルトでは、内部から外部への通信及びメール通知用ポリシー（MTA 許可）、マスカレードポリシーがセットされています。

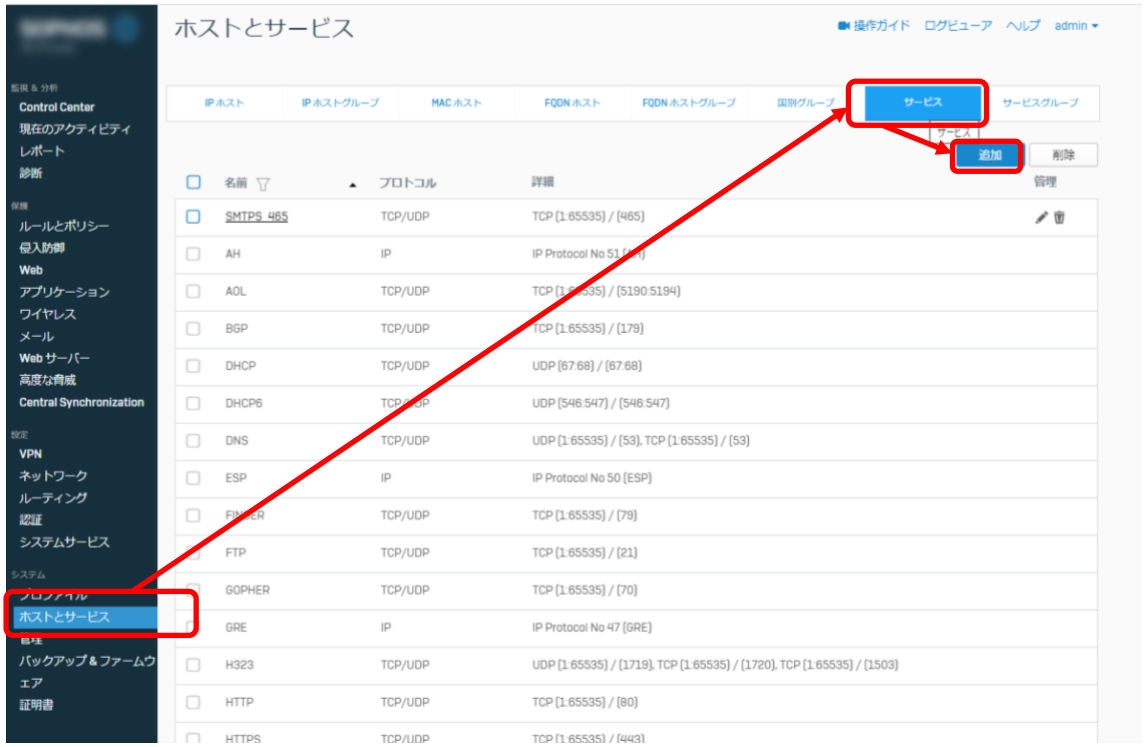
3．DNAT の設定（RemoteDesktop 用）

（1）DNAT の設定

事前準備

ここでは、外部のユーザよりリモートデスクトップで内部の保護対象サーバーへアクセスする為の設定を記載します。ポリシーを設定する前に、以下のサービスを登録します。

ホストとサービス ＞ サービスタブ ＞ 追加をクリックします。



名前：（例として AdvanceRDT63389）

種類：TCP

宛先ポート：63389

保存をクリックします。繰り返し以下のサービスを登録します。

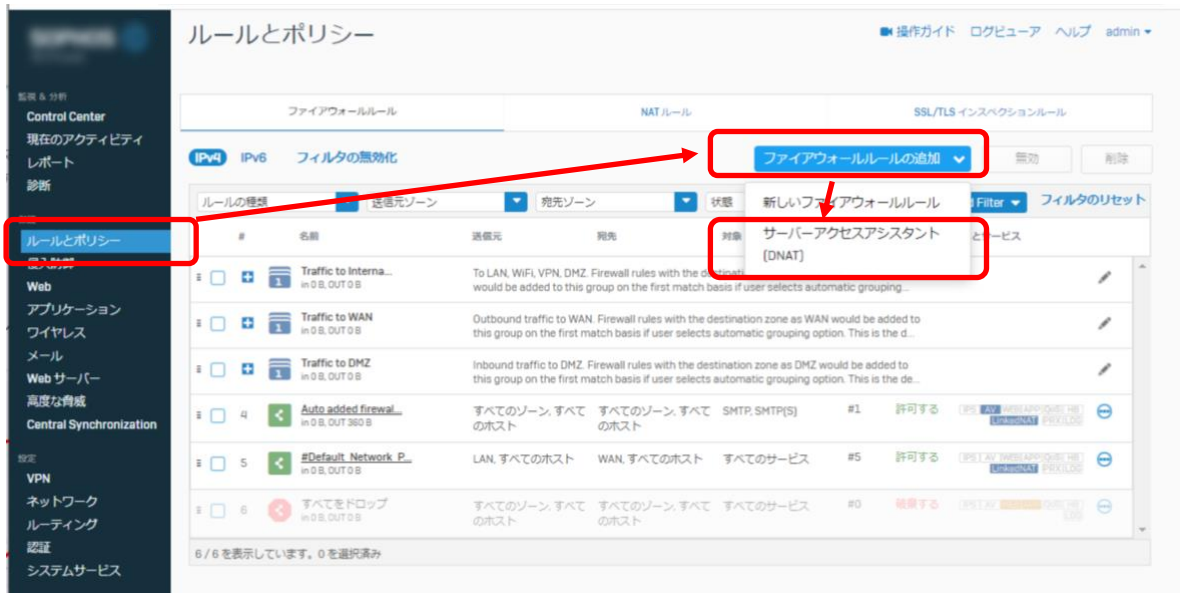
名前：（例として RDT3389）

種類：TCP

宛先ポート：3389

保存をクリックします。ここまでで、AdvanceRDT63389、RDT3389 のサービスを登録しました。

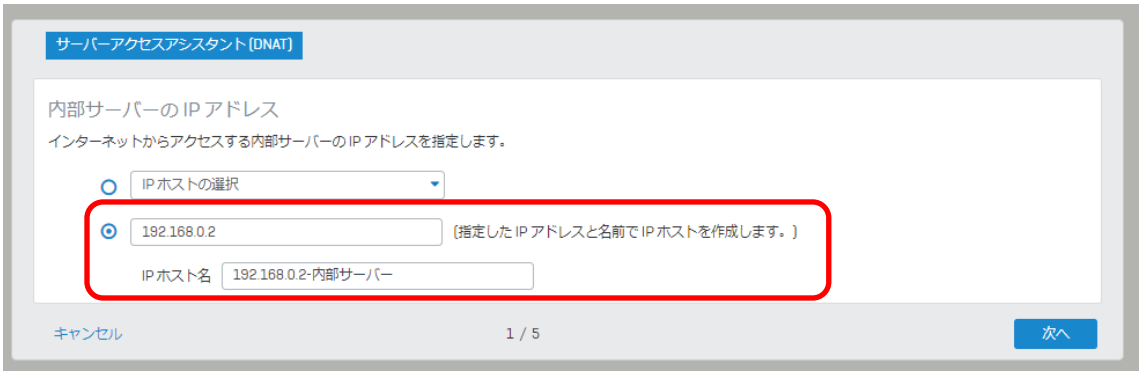
①ルールとポリシー＞ ファイアウォールルールの追加 ＞ サーバアクセスアシスタントのルールをクリックします。



②今回はグループに含めず、単体のポリシーとして設定します。まず以下の通りに設定します。

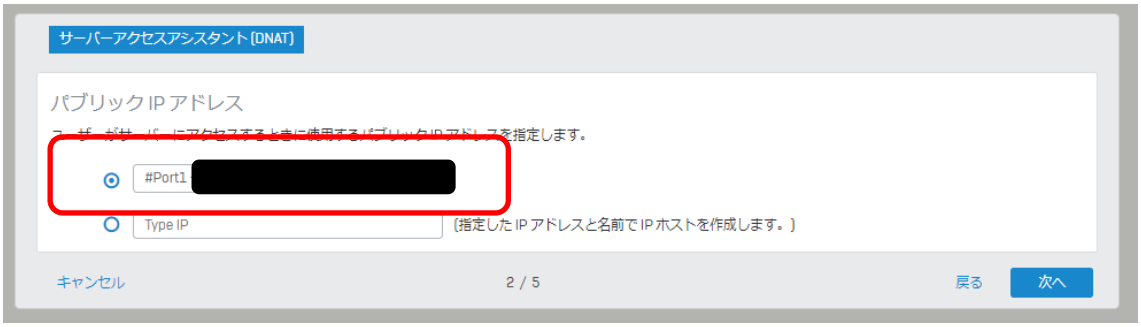
Type IP：192.168.0.2

IP ホスト名：192.168.0.2-内部サーバー



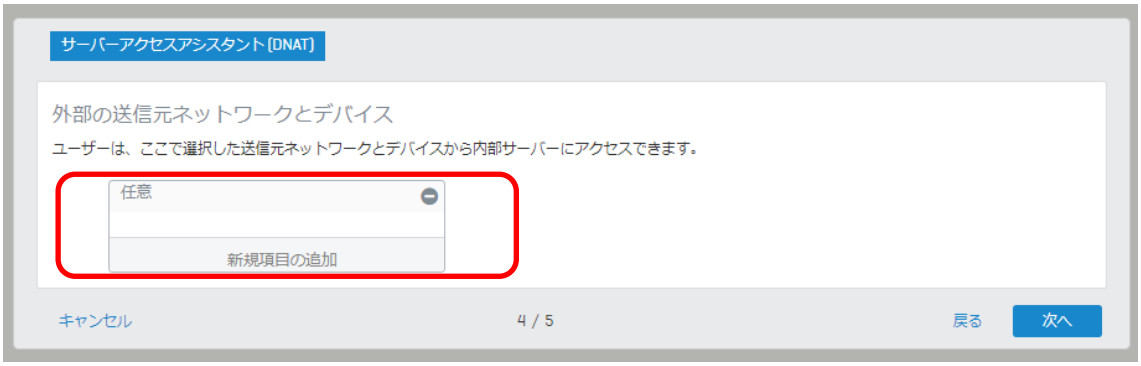
③ユーザがサーバにアクセスるパブリック IP アドレスに Port1（グローバルアドレス）を選択します。

＃Port1（設定されているグローバル IP アドレスが表示されます。）

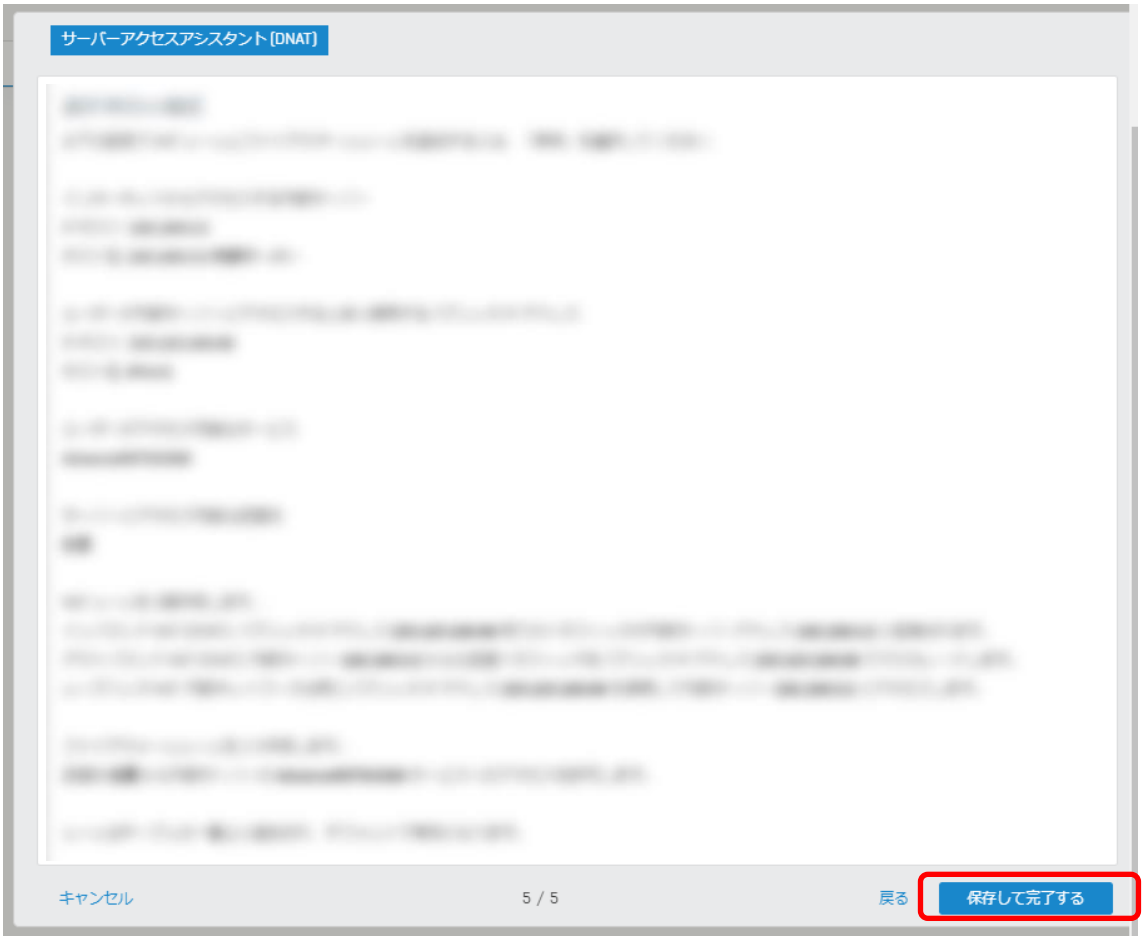


④ここでサービスは事前準備で作成した AdvanceRDT63389 を選択します。

⑤送信元の設定を行います。今回は任意（Any）で設定します。



⑥設定の概要が表示されるので内容を確認し、保存して完了するをクリックします。



このウィザードで 3 つの NAT リンクルールが自動的に生成されます。

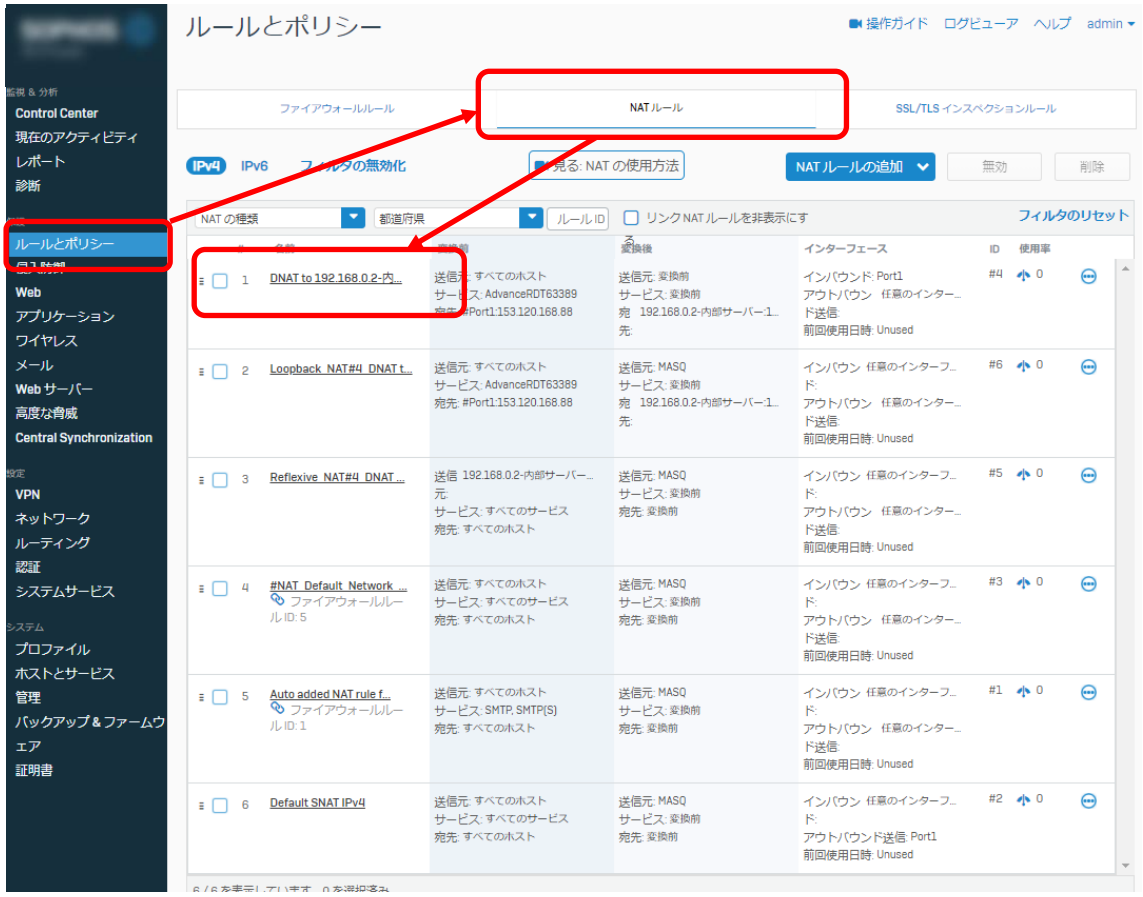
・インバウンド NAT (DNAT): パブリック IP アドレス宛てのトラフィックが内部サーバーアドレス 192.168.0.2 に変換されます。

・アウトバウンド NAT (SNAT): 内部サーバー 192.168.0.2 からの送信トラフィックをパブリック IP アドレスでマスカレードします。

・ループバック NAT: 内部ネットワークは同じパブリック IP アドレスを使用して内部サーバー 192.168.0.2 にアクセスします。

ここで作成されたインバウンド NAT について、サービスを AdvanceRDT から標準の RDT へ変換する設定を追加します。

⑦ルールとポリシー ＞ NAT ルール から自動生成された「DNAT to 192.168.0.2-内部サーバー_1609294219283」をクリックします。



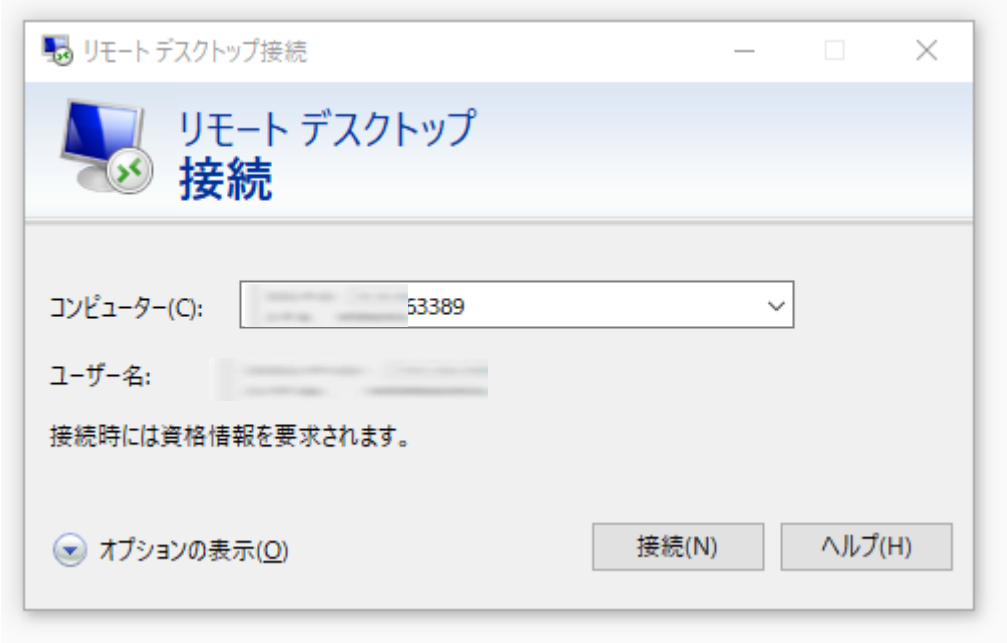
⑧変換後のサービス（PAT）に事前準備で作成した RDT3389 を選択し保存をクリックします。

⑨ファイアウォールルールの最上位にルールが設定されました。

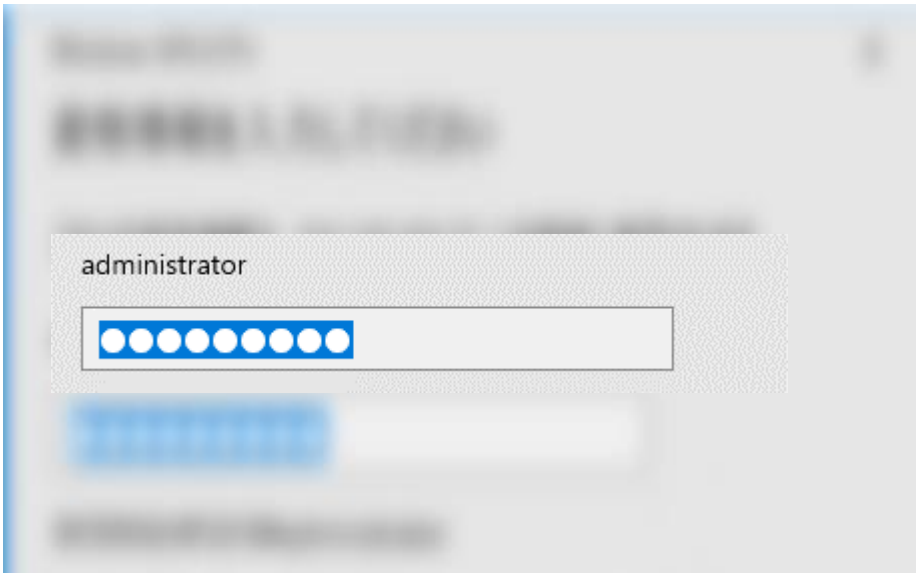
（2）リモートデスクトップ接続の確認

①Sophos Firewall 配下のサーバへ、リモートデスクトップ接続の確認をします。

ここでは WAN 側のグローバル IP アドレスに、63389 ポートを指定します。



認証画面が表示されます。ここではパスワード認証を行い保護対象サーバへアクセスします。



③Sophos Firewall のログ機能を使用し、DNAT のルールが正しく適用されていることを確認します。画面上部のログビューアをクリックします。

ログビューアが表示されます。

④ログを確認するためにログビューアの表示に対しフィルタを追加をクリックします。今回は TCP63389 を利用しているので、以下のように入力し AddFilter をクリックします。

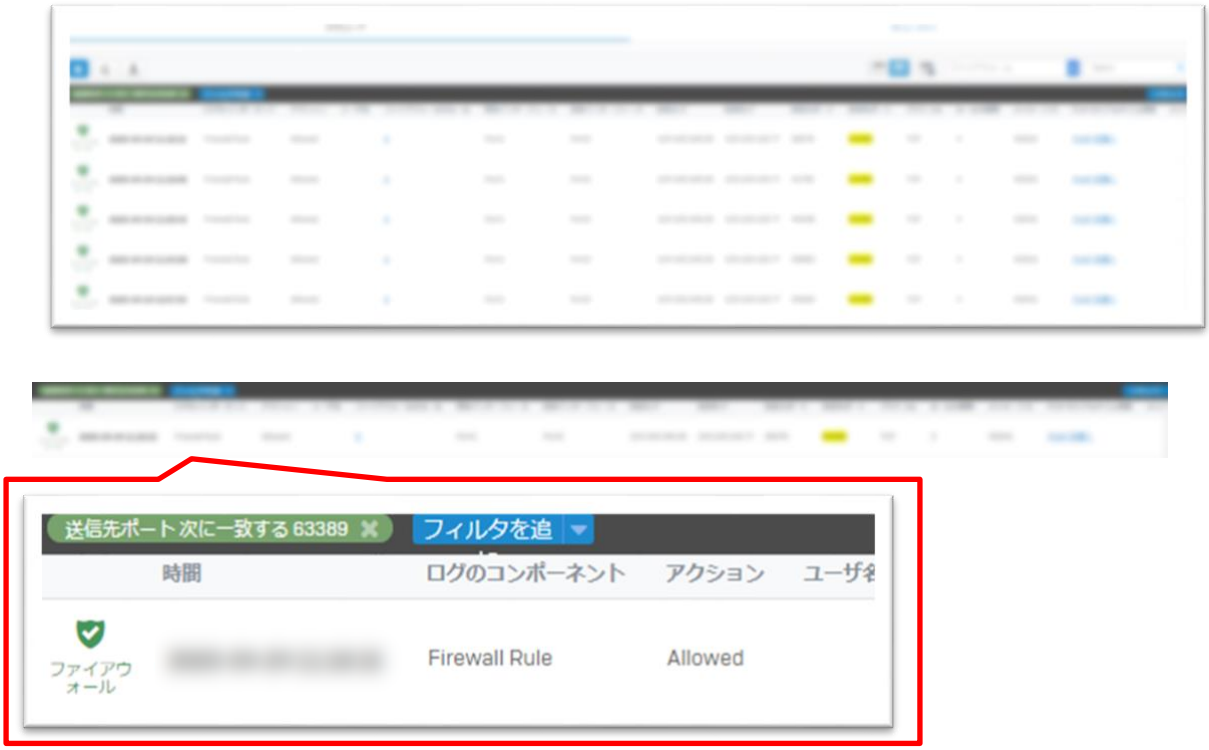
フィールド：送信先ポート

条件：次に一致する

値：63389

---

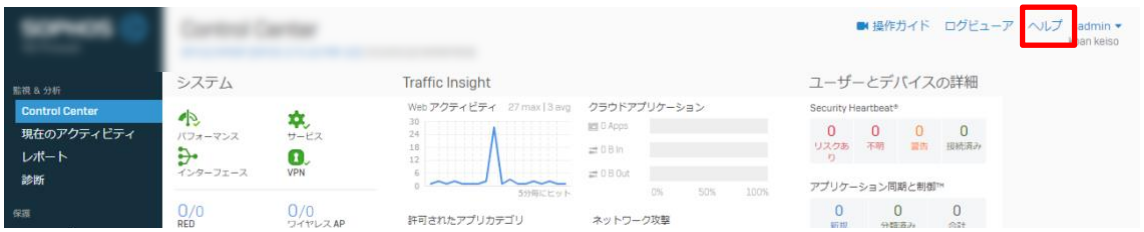
⑤該当のルールを通過しているポリシーが表示されます。



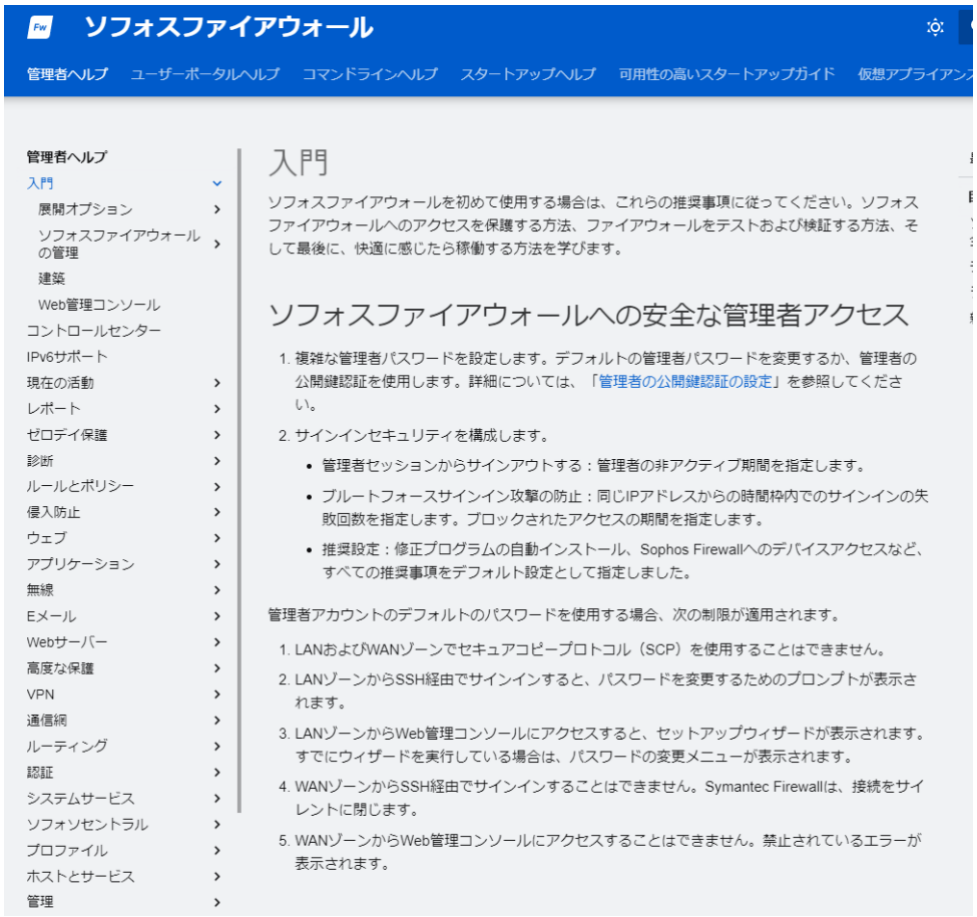
表示されたルールが Allowed されていることを確認します。

４．最後に

本手順書では、ファイアウォールのポリシーについて、マスカレードの設定について、DNAT の設定とログビューアによる確認方法を記載しました。Sophos 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