

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

目次

内容

| | |
|------------------------------------|----|
| 改訂履歴 | 2 |
| はじめに | 3 |
| 1. ご利用環境の構成 | 4 |
| 2. ファイアウォールの設定 | 5 |
| 3. DNAT の設定（RemoteDesktop 用） | 9 |
| (1) DNAT の設定..... | 9 |
| (2) リモートデスクトップ接続の確認 | 17 |
| 4. 最後に | 20 |

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

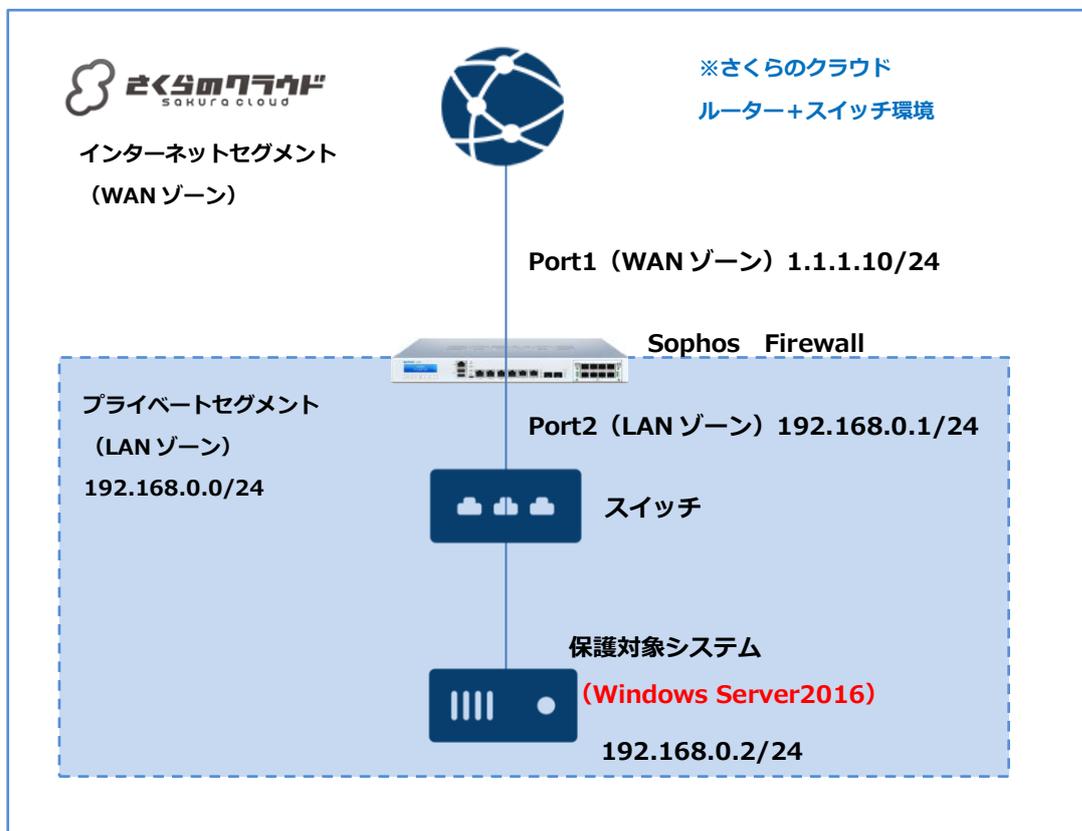
本手順書は以下の手順書に沿って Sophos Firewall が展開されアクティベートされた、状態を前提としております。

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。

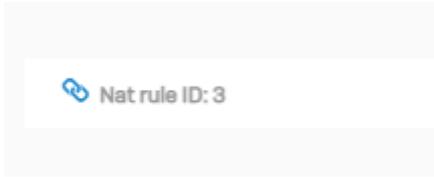
単体ポリシー

- 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。

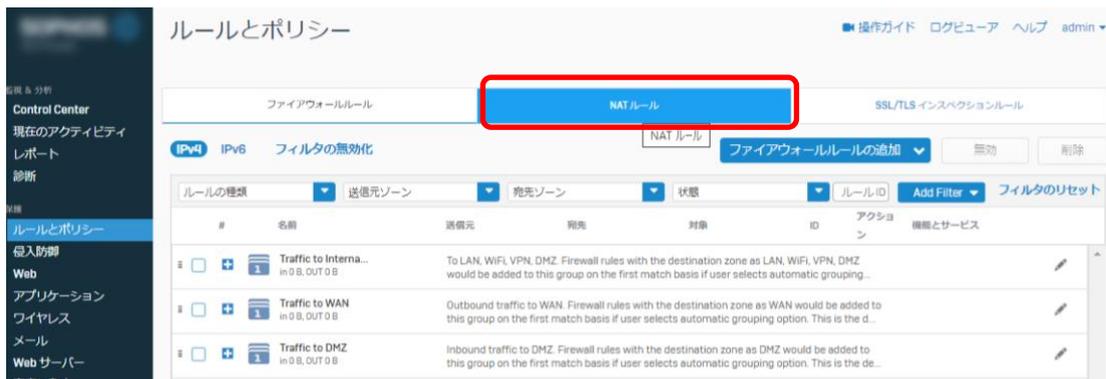


Nat rule ID:3

④今回は設定の確認のためのため「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。



⑥ NAT ルール ID 3 の内容を確認します。

The screenshot shows the 'Rules and Policies' (ルールとポリシー) page in the Sophos Firewall management console. The 'NAT Rules' (NAT ルール) tab is selected. A table lists NAT rules with columns for ID, Name, Before (変換前), After (変換後), and Interface (インターフェース). Rule #3, 'Default SNAT IPv4', is highlighted with a red box.

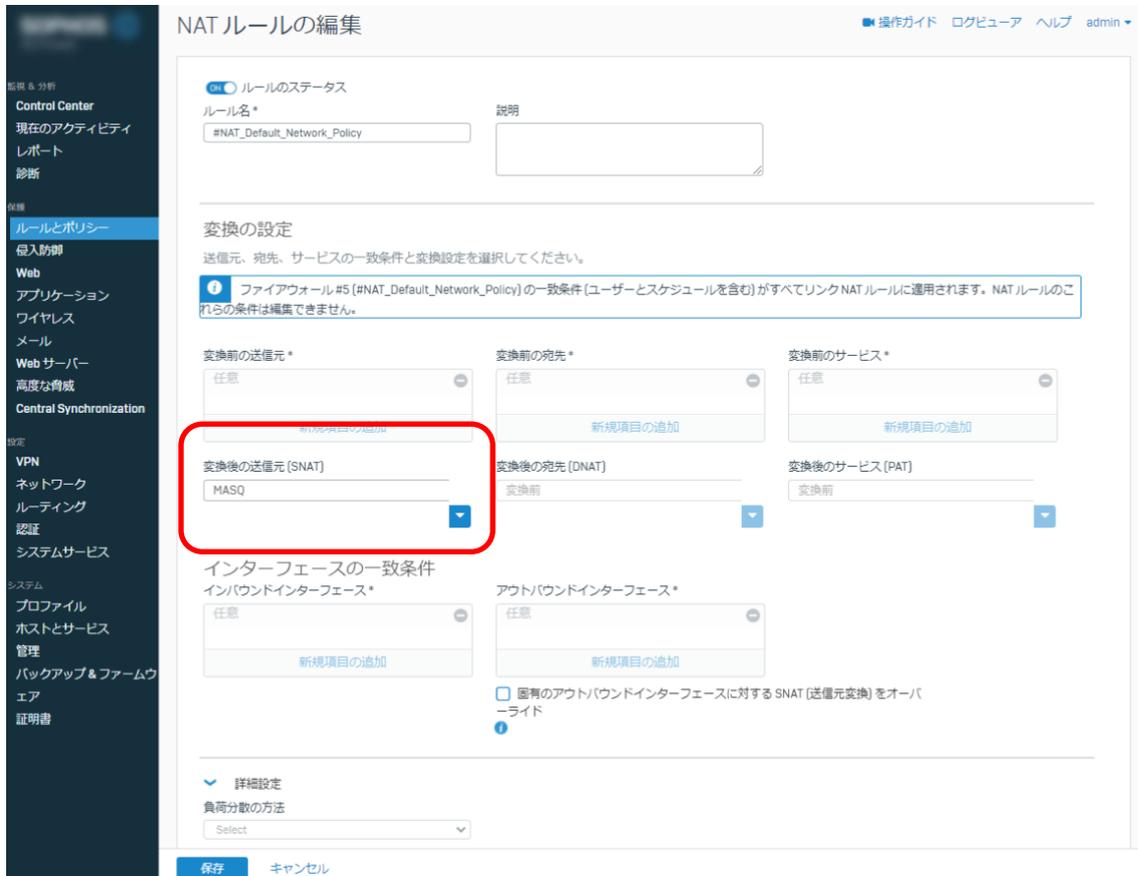
| # | 名前 | 変換前 | 変換後 | インターフェース | ID | 利用率 |
|---|---|--|-----------------------------------|---|----|-----|
| 1 | #NAT_Default_Network... ファイアウォールルール ID: 5 | 送信元: すべてのホスト サービス: すべてのサービス 宛先: すべてのホスト | 送信元: MASQ サービス: 変換前 宛先: 変換前 | インバウン 任意のインターフェース アウトバウン 任意のインターフェース 送信: 前回使用日時 Unused | #3 | 0 |
| 2 | Auto added NAT rule f... ファイアウォールルール ID: 1 | 送信元: すべてのホスト サービス: SMTP, SMTP(S) 宛先: すべてのホスト | 送信元: MASQ サービス: 変換前 宛先: 変換前 | インバウン 任意のインターフェース アウトバウン 任意のインターフェース 送信: 前回使用日時 Unused | #1 | 0 |
| 3 | Default SNAT IPv4 | 送信元: すべてのホスト サービス: すべてのサービス 宛先: すべてのホスト | 送信元: MASQ サービス: 変換前 宛先: 変換前 | インバウン 任意のインターフェース アウトバウン 送信 Port1 前回使用日時: Unused | #2 | 0 |

※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。

This is a close-up view of the NAT rule table from the previous screenshot. A red box highlights the 'ID' column, showing the value '#3' for the first rule.

| # | 名前 | 変換前 | 変換後 | インターフェース | ID | 利用率 |
|---|--|---|-----------------------------------|---|----|-----|
| 1 | #NAT_Default_Network... ファイアウォールルール ID: 5 | 送信元: すべてのホスト サービス: すべてのサービス 宛先: すべてのホスト | 送信元: MASQ サービス: 変換前 宛先: 変換前 | インバウン 任意のインターフェース アウトバウン 任意のインターフェース 送信: 前回使用日時 Unused | #3 | 0 |

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。

The screenshot shows the 'Hosts and Services' page in the Sophos Firewall management console. The 'Services' tab is selected, and the 'Add' button is highlighted with a red box. A red arrow points from the 'Add' button to the 'Hosts and Services' menu item in the left sidebar, which is also highlighted with a red box.

| 名前 | プロトコル | 詳細 | 管理 |
|------------------------------------|---------|--|----|
| <input type="checkbox"/> SMTPS_465 | TCP/UDP | TCP [1.65535] / [465] | |
| <input type="checkbox"/> AH | IP | IP Protocol No 51 [51] | |
| <input type="checkbox"/> AOL | TCP/UDP | TCP [1.65535] / [5190.5194] | |
| <input type="checkbox"/> BGP | TCP/UDP | TCP [1.65535] / [179] | |
| <input type="checkbox"/> DHCP | TCP/UDP | UDP [67.68] / [67.68] | |
| <input type="checkbox"/> DHCP6 | TCP/UDP | UDP [546.547] / [546.547] | |
| <input type="checkbox"/> DNS | TCP/UDP | UDP [1.65535] / [53], TCP [1.65535] / [53] | |
| <input type="checkbox"/> ESP | IP | IP Protocol No 50 [ESP] | |
| <input type="checkbox"/> FINRGR | TCP/UDP | TCP [1.65535] / [79] | |
| <input type="checkbox"/> FTP | TCP/UDP | TCP [1.65535] / [21] | |
| <input type="checkbox"/> GOPHER | TCP/UDP | TCP [1.65535] / [70] | |
| <input type="checkbox"/> GRE | IP | IP Protocol No 47 [GRE] | |
| <input type="checkbox"/> H323 | TCP/UDP | UDP [1.65535] / [1719], TCP [1.65535] / [1720], TCP [1.65535] / [1503] | |
| <input type="checkbox"/> HTTP | TCP/UDP | TCP [1.65535] / [80] | |
| <input type="checkbox"/> HTTPS | TCP/UDP | TCP [1.65535] / [443] | |



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。



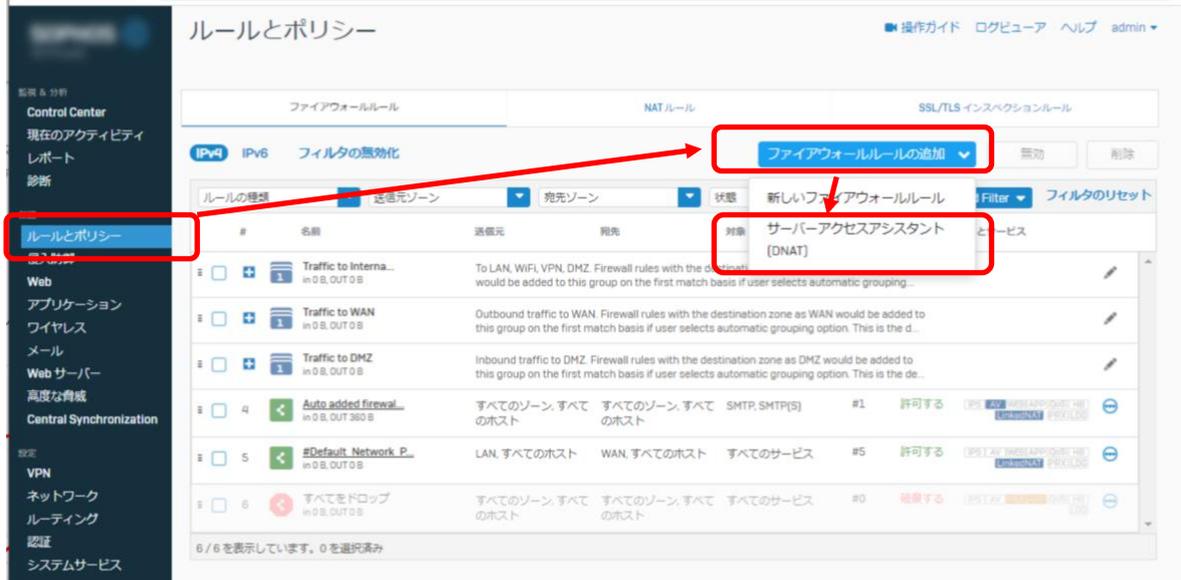
名前：(例として RDT3389)

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。

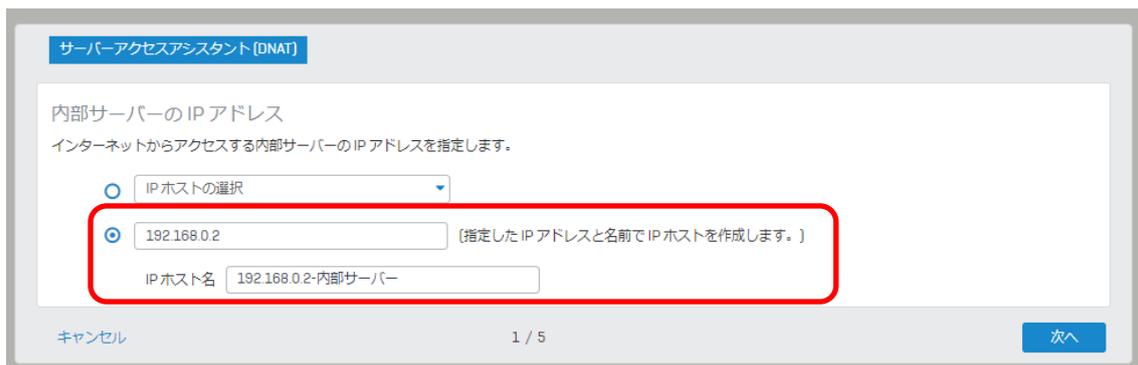
④ルールとポリシー> ファイアウォールルールの追加 > サーバアクセスアシスタントのルールをクリックします。



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するパブリック 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。)



サーバーアクセスアシスタント [DNAT]

パブリック IP アドレス

ユーザがサーバにアクセスするときに使用するパブリック IP アドレスを指定します。

#Port1 [REDACTED]

Type IP [指定した IP アドレスと名前で作成します。]

キャンセル 2 / 5 戻る 次へ

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。



サーバーアクセスアシスタント [DNAT]

サービス

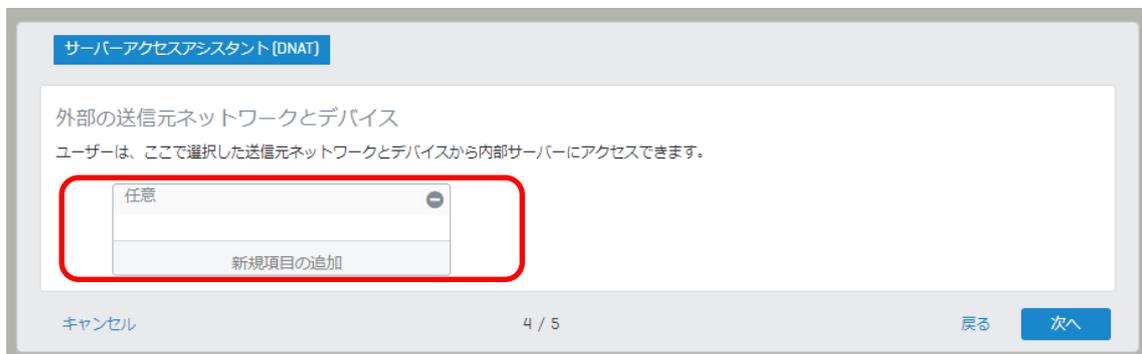
ユーザは、内部サーバ上の選択済みサービスにアクセスできます。

AdvanceRDT63389

新規項目の追加

キャンセル 3 / 5 戻る 次へ

⑤送信元の設定を行います。今回は任意 (Any) で設定します。



サーバーアクセスアシスタント [DNAT]

外部の送信元ネットワークとデバイス

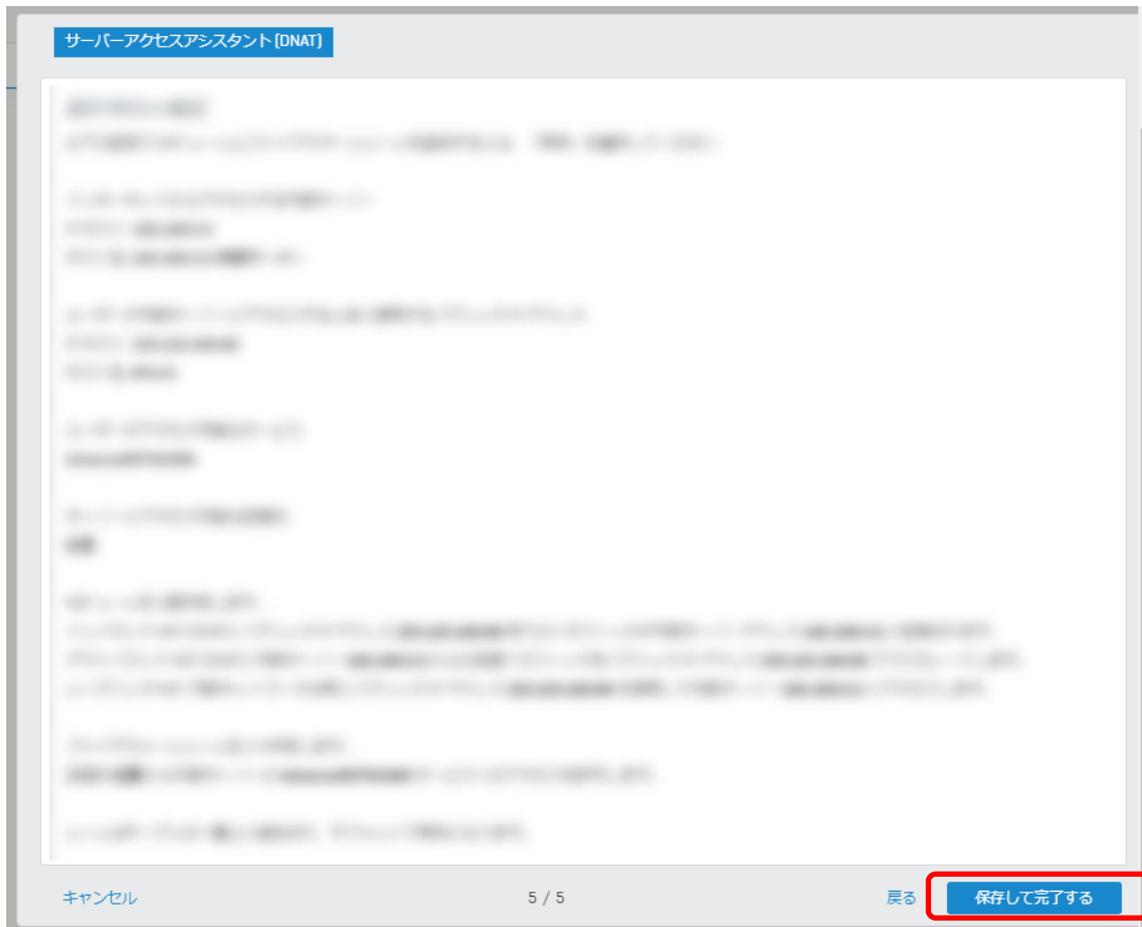
ユーザは、ここで選択した送信元ネットワークとデバイスから内部サーバにアクセスできます。

任意

新規項目の追加

キャンセル 4 / 5 戻る 次へ

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。

The screenshot shows the 'Rules and Policies' (ルールとポリシー) configuration page in the Sophos Firewall management interface. The 'NAT Rules' (NAT ルール) tab is active. A table lists several NAT rules. Rule 1, titled 'DNAT to 192.168.0.2-内部サーバー_1609294219283', is highlighted with a red box. A red arrow points from the 'NAT Rules' tab to this rule. The left sidebar shows the navigation menu with 'Rules and Policies' (ルールとポリシー) highlighted.

| NATの種類 | 都道府県 | ルールID | リンク NAT ルールを非表示にする | フィルタのリセット | | |
|--------|------|--|---|--|---|------------------|
| 1 | | DNAT to 192.168.0.2-内部サーバー_1609294219283 | 送信元: 全てのホスト サービス: AdvanceRDT63389 宛先: #Port1:153.120.168.88 | 送信元: 変換前 サービス: 変換前 宛先: 192.168.0.2-内部サーバー_1609294219283 | インターフェース: インバウンド: Port1 アウトバウンド: 任意のインターフェース ド送信: 前回の使用日時: Unused | ID: #4 使用率: 0 |
| 2 | | Loopback NAT#4 DNAT to 192.168.0.2-内部サーバー_1609294219283 | 送信元: 全てのホスト サービス: AdvanceRDT63389 宛先: #Port1:153.120.168.88 | 送信元: MASQ サービス: 変換前 宛先: 192.168.0.2-内部サーバー_1609294219283 | インターフェース: インバウンド: 任意のインターフェース アウトバウンド: 任意のインターフェース ド送信: 前回の使用日時: Unused | ID: #6 使用率: 0 |
| 3 | | Reflexive NAT#4 DNAT to 192.168.0.2-内部サーバー_1609294219283 | 送信元: 192.168.0.2-内部サーバー_1609294219283 宛先: 全てのホスト | 送信元: MASQ サービス: 変換前 宛先: 変換前 | インターフェース: インバウンド: 任意のインターフェース アウトバウンド: 任意のインターフェース ド送信: 前回の使用日時: Unused | ID: #5 使用率: 0 |
| 4 | | #NAT_Default_Network_1609294219283 | 送信元: 全てのホスト サービス: 全てのサービス 宛先: 全てのホスト | 送信元: MASQ サービス: 変換前 宛先: 変換前 | インターフェース: インバウンド: 任意のインターフェース アウトバウンド: 任意のインターフェース ド送信: 前回の使用日時: Unused | ID: #3 使用率: 0 |
| 5 | | Auto added NAT rule for SMTP(S) | 送信元: 全てのホスト サービス: SMTP(S) 宛先: 全てのホスト | 送信元: MASQ サービス: 変換前 宛先: 変換前 | インターフェース: インバウンド: 任意のインターフェース アウトバウンド: 任意のインターフェース ド送信: 前回の使用日時: Unused | ID: #1 使用率: 0 |
| 6 | | Default SNAT IPv4 | 送信元: 全てのホスト サービス: 全てのサービス 宛先: 全てのホスト | 送信元: MASQ サービス: 変換前 宛先: 変換前 | インターフェース: インバウンド: 任意のインターフェース アウトバウンド: 送信: Port1 前回の使用日時: Unused | ID: #2 使用率: 0 |

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。

NAT ルールの編集 操作ガイド ログビューア ヘルプ admin

ルールのステータス

ルール名* 説明

変換の設定

送信元、宛先、サービスの一致条件と変換設定を選択してください。

| 変換前の送信元* | 変換前の宛先* | 変換前のサービス* |
|---------------------------------|-------------------------------------|--|
| <input type="text" value="任意"/> | <input type="text" value="#Port1"/> | <input type="text" value="AdvanceRDT63389"/> |
| 新規項目の追加 | 新規項目の追加 | 新規項目の追加 |

変換後の送信元 (SNAT)

変換後の宛先 (DNAT)

変換後のサービス (PAT)

インターフェースの一致条件

| インバウンドインターフェース* | アウトバウンドインターフェース* |
|------------------------------------|---------------------------------|
| <input type="text" value="Port1"/> | <input type="text" value="任意"/> |
| 新規項目の追加 | 新規項目の追加 |

固有のアウトバウンドインターフェースに対する SNAT (送信元変換) をオーバーライド

▼ 詳細設定

負荷分散の方法

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。

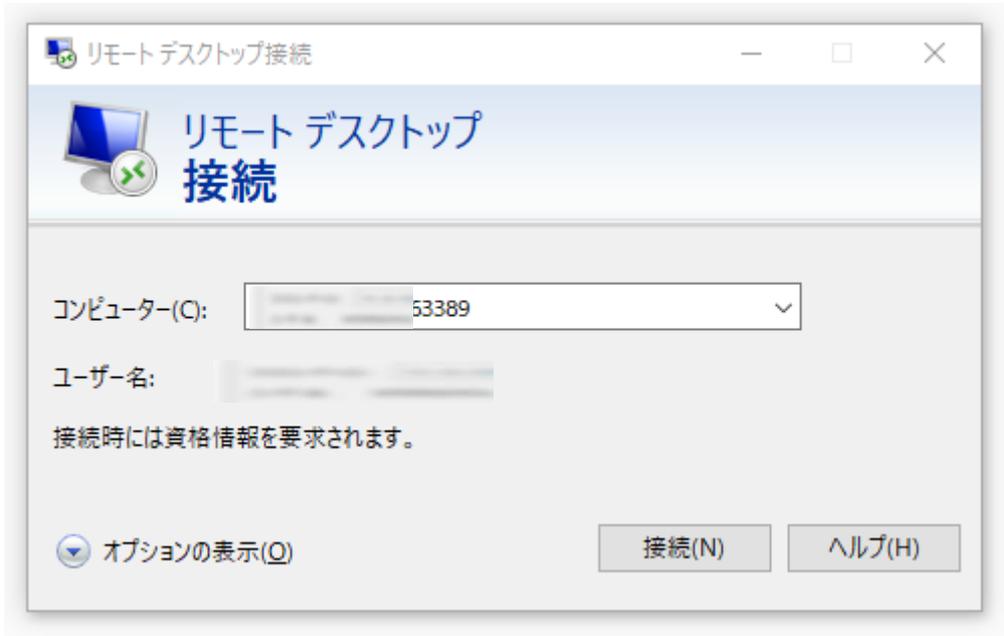
The screenshot shows the 'ルールとポリシー' (Rules and Policies) section of the Sophos Firewall management console. The 'ファイアウォールルール' (Firewall Rules) tab is selected. The rule list is sorted by priority, and the rule 'DNAT to 192.168.0...' is at the top (ID #6), highlighted with a red box. Below it are other rules like 'Traffic to Intern...', 'Traffic to WAN', 'Traffic to DMZ', 'Auto added firewal...', '#Default Network P...', and 'すべてをドロップ'.

| # | 名前 | 送信元 | 宛先 | 対象 | ID | アクション | 機能とサービス |
|---|-----------------------|--|------------------|-----------------|----|-------|--|
| 1 | DNAT to 192.168.0... | WAN, すべてのホスト | WAN, #Port1 | AdvanceRDT63389 | #6 | 許可する | [AV] [WEBAPP] [QoS] [HB] [LinkedNAT] [PRX] [LOG] [IPS] |
| | Traffic to Intern... | To LAN, WiFi, VPN, DMZ. Firewall rules with the destination zone as LAN, WiFi, VPN, DMZ would be added to this group on the first match basis if user selects... | | | | | |
| | Traffic to WAN | Outbound traffic to WAN. Firewall rules with the destination zone as WAN would be added to this group on the first match basis if user selects automatic grouping... | | | | | |
| | Traffic to DMZ | Inbound traffic to DMZ. Firewall rules with the destination zone as DMZ would be added to this group on the first match basis if user selects automatic grouping... | | | | | |
| 5 | Auto added firewal... | すべてのゾーン, すべてのホスト | すべてのゾーン, すべてのホスト | SMTP, SMTP(S) | #1 | 許可する | [AV] [WEBAPP] [QoS] [HB] [LinkedNAT] [PRX] [LOG] [IPS] |
| 6 | #Default Network P... | LAN, すべてのホスト | WAN, すべてのホスト | すべてのサービス | #5 | 許可する | [AV] [WEBAPP] [QoS] [HB] [LinkedNAT] [PRX] [LOG] [IPS] |
| 7 | すべてをドロップ | すべてのゾーン, すべてのホスト | すべてのゾーン, すべてのホスト | すべてのサービス | #0 | 拒否する | [AV] [WEBAPP] [QoS] [HB] [LinkedNAT] [PRX] [LOG] [IPS] |

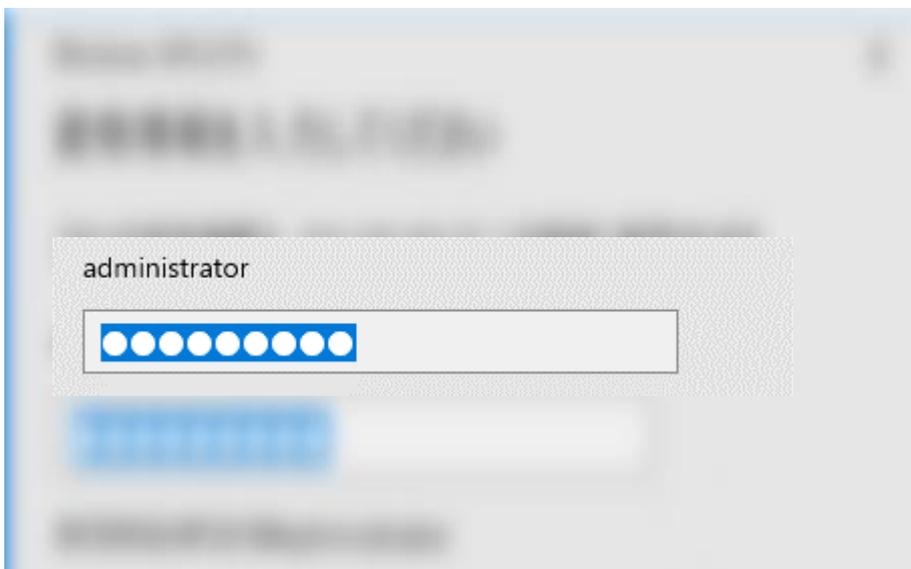
(2) リモートデスクトップ接続の確認

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

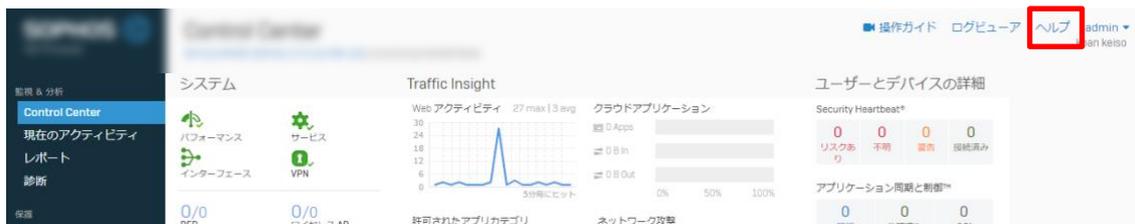
⑤該当のルールを通過しているポリシーが表示されます。



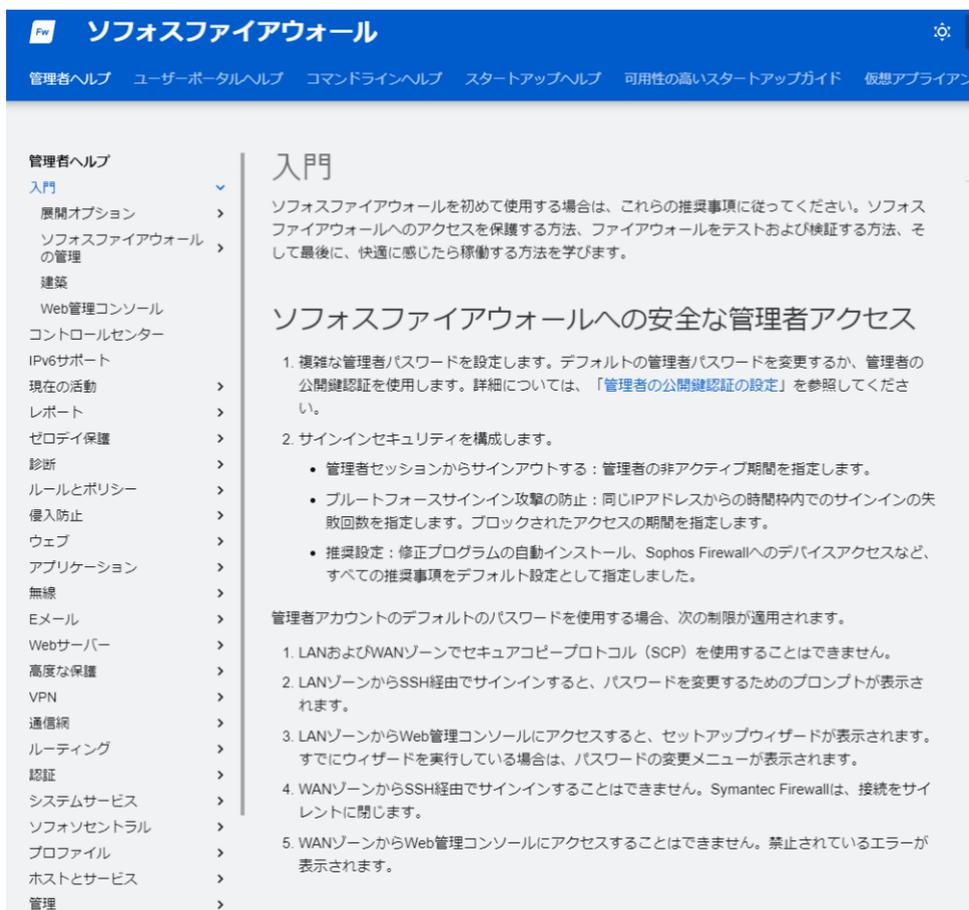
表示されたルールが Allowed されていることを確認します。

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箇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