



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.ht ml

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。

		ファイアウォールルール		NAT JU-JU			SSL/T	LS インスペクション	ルール
(Pvq)	IPv6	フィルタの無効化			<i>סדרד</i> כן	オールル	ールの追加	✓ #3	MB
1-	ルの種類	送信元ゾーン	苑先ゾー:	× 💽 :	状態		ルールロ)	Add Filter 💌	フィルタのリセ
		名前	送信元	宛先	対象	ID	アクショ	機能とサービス	
• •		Traffic to Interna in 08,00108 Traffic to WAN in 08,00108	To LAN, WiFi, VPN, DMZ would be added to this Outbound traffic to WA! this group on the first m	Firewall rules with the de roup on the first match b I. Firewall rules with the d atch basis if user selects	stination zone as LAN, 1 asis if user selects auto estination zone as WAN automatic grouping op	WiFi, VPN, I omatic grou would be tion. This is		リシーグ	ループ
• 🗆	D ĝ	Traffic to DMZ in 0.8, OUT 0.8	Inbound traffic to DMZ this group on the first m	Firewall rules with the des atch basis if user selects	长很级 tination zone as DMZ w automatic grouping op	rould be ad	ded to the de	-をグル	ープ化
• •	4	Auto added firewal	Inbound traffic to DMZ this group on the first m すべてのゾーン、すべて の木スト	Firewall rules with the des atch basis if user selects すべてのゾーン、すべて のホスト	smtP, SmtP(S)	tion. This is	ded to the de_ 許可する	-をグル	ープ化
= =	4		Inbound traffic to DMZ this group on the first m すべてのソーン, すべて のホスト LAN, すべてのホスト	Firewall rules with the des atch basis if user selects ずべてのゾーン, すべて のホスト WAN, すべてのホスト	tination 2016 85 DM2 w automatic grouping op SMTP. SMTP(S) すべてのサービス	#1 #5	ded to the de 許可する 許可する	-をグル 単体ホ	ープ化 リシー

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。

設定 VPN	I 🗌 5	#Default Network P in 0 B, OUT 0 B	LAN, すべての木スト	WAN, すべての木スト	すべてのサービス	#5	許可する	IPS AV WEB APPIQOS HB .	
ネットワーク		★ペアたドロップ			totali 12-	#0	融高オス		

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。

	ルー	ル	とす	ペリシー					■ 操作ガイ	(ドログビュー)	r NIJ	admin 🔻
監視 & 分析 Control Center			2	リァイアウォールルール	ſ	N	AT JL—JL		SSL/1	TLS インスペクション	16-16	
現在のアクティビティ レポート	(Pv4)	IPve	5	フィルタの無効化			NAT JL-JL	ファイアウォールル	ールの追加	•	t) [_	削除
रूछ जन्म	16-1	しの種業	R.	🔽 送信元ゾーン		苑先ゾーン	▼ 状態	•	ルールロ	Add Filter 👻	フィルタの	ノセット
ルールとポリシー		#		名前	送信元	和先	ĦB	ID	アクション	機能とサービス		
侵入防御 Web	= 🗆		1	Traffic to Interna in 0 B, OUT 0 B	To LAN, WIF would be ad	FI, VPN, DMZ. Firewall rule ided to this group on the	es with the destination 2 first match basis if use	tone as LAN, WiFi, VPN, r selects automatic gro	DMZ uping			r ^
アプリケーション ワイヤレス	• 🗆		1	Traffic to WAN in 0 B, OUT 0 B	Outbound to this group o	raffic to WAN. Firewall ru on the first match basis if	les with the destination f user selects automatic	zone as WAN would be grouping option. This i	added to is the d		,	~
メール Web サーバー	•	0	1	Traffic to DMZ in 0 B, OUT 0 B	Inbound tra this group o	ffic to DMZ. Firewall rule on the first match basis if	s with the destination zo fuser selects automatic	one as DMZ would be a grouping option. This i	dded to is the de		,	^

₽ ¢	ルールとポリシー			■ 漫作ガイド □	ガビューア ヘル	プadmin 、
^{監視 & 分析} Control Center 現在のアクティビティ レポート	ファイアウォールル・		NATルール	SSL/TLS イン:	スペクションルール	101E2
診断	NAT の種類	道府県	ルID リンク NAT ルールを非表示	C. 7	フィル	タのリセット
ルールとポリシー	# 名前	変換前	る 変換後	インターフェース	ID 使用率	
 侵入防御 Web アプリケーション ワイヤレス メール 	■ □ 1 <u>#NAT Default Netwo</u> ◆ ファイアウォール ルロ:5	IL	送信元 MASQ サービス: 愛換前 宛先: 愛換前	インパウン 任意のインターフ ド: アウトバウン 任意のインター ド送信 前回使用日時: Unused	#3 🏠 O	⊖ ^
Web サーバー 高度な脅威 Central Synchronization	■ 2 Auto added NAT rule f ◆ ファイアウォール ルロ: 1	 送信元:すべての水スト レー サービス: SMTP, SMTP(S) 宛先:すべての水スト 	送信元 MASQ サービス: 変換的 宛先: 変換的	インパウン 任意のインターフ ド: アウトパウン 任意のインター ド送告: 前回使用日時: Unused	#1 🏠 O	Θ
マ PN ネットワーク 「 ルーティング	E 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: 変換的 宛先 変換的	インパウン 任意のインターフ_ ド: アウトパウンド送信 Port1 前回使用日時: Unused	#2 🋧 0	Ξ
認証 システムサービス	3/3を表示しています。0を選択済み					

⑥NAT ルール ID 3 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。

NAT の種類	都道府県			リンク NAT ルールを非表示にす			7-	ィルタのリセッ
#	名前	変換前	5	変換後	インターフェース	ID	俄用3	率
≡ 🗌 1	<u>#NAT Default Network</u> � ファイアウォールルー ルロ: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	インパウン 任意のインターフ ド: アウトパウン 任意のインター ド送信: 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。

NAI ルールの編集				■ 操作カイド	ロクヒューア ^
exe ルールのステータス オーノレール名キー イビティ ポNAT_Default_Network_Policy		說明			
シー 変換の設定					
送信元、宛先、サービスの一致多	そ件と変換設定を選	択してください。			
ファイアウォール #5 [#NAT]	_Default_Network_F	Policy] の一致条件 [ユーザーとスケミ	ジュールを含む)がすべて	Cリンク NAT ルールに適用さ	れます。NAT ルーノ
れらの条件は編集できません。					
変換前の送信元*		変換前の宛先*	变	換前のサービス*	
任意	٥	任意	0	任意	(
nronization					
利用が発展しい通知		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)	奕	換後のサービス (PAT)	
MASQ		変換前		変換前	
	·		•		
	两冬件				
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			
任意	0	任意	0		
&ファームウ		朝7規項目の力量加			
		 固有のアウトバウンドインター ーライド 	-フェースに対する SNA	⊺ (送信元変換) をオーバ	
		0			
 詳細設定 自済分数の方注 					

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(Remote Desktop 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。

	ホス	くトとサ	ービス				■ 操	作ガイド ログビュー	-ア ヘルプ admin ▼
監視 & 分析 Control Center 現在のアクティピティ	IP	カホスト	IPホストグループ	MAC/KZF	FQDNホスト	FQDN ホストグループ	国別グループ	サービス	サービスグループ
レポート		名前 ▽	. 7	עבאם	计相				追加 管理
^{保護} ルールとポリシー	0	SMTPS 465	тс	P/UDP	TCP (1:65535) / (4	65)			1
侵入防御 Web		AH	IP		IP Protocol No 51 (-1			
アプリケーション		AOL	тс	P/UDP	TCP (1:52535) / (5	190:5194)			
ウイヤレス メール		BGP	тс	P/UDP	TCP (1:65535) / (1	79)			
Web サーバー 高度な脅威		DHCP	тс	P/UDP	UDP [67:68] / [67:6	88]			
Central Synchronization		DHCP6	тс	PAUP	UDP (546:547) / (5	46:547)			
BOE VPN		DNS	τι	P/UDP	UDP (1:65535) / (5	3), TCP (1:65535) / (53)			
ネットワーク		ESP	IP		IP Protocol No 50 (ESP)			
ルーティング 認証		FINDER	тс	P/UDP	TCP (1:65535) / (7	9]			
システムサービス	/	FTP	то	P/UDP	TCP (1:65535) / (2	1)			
5274 JUJF1N	-	GOPHER	тс	P/UDP	TCP (1:65535) / (7	0)			
ホストとサービス = 4		GRE	IP		IP Protocol No 47 (GRE)			
バックアップ&ファームウ エフ		H323	тс	P/UDP	UDP (1:65535) / (1	719), TCP (1:65535) / (17	20), TCP (1:65535) / (1503)	
正明書		HTTP	то	P/UDP	TCP (1:65535) / (8	0)			
		HTTPS	TC	P/UDP	TCP (1:65535) / (4	43]			

XG Firewall	サービスの	追加				■ 漫 (ドガイド ログビュ・	ーア ヘルプ admin ▼
 監視 & 分析 Control Center 現在のアクティビティ レポート 診断 	IP#ZF	IP ホストグループ	MACホスト	FQDNホスト	FQDN ホストグループ	国別グループ	サービス	サービスグループ
 単語 パールとポリシー (常入防御) Web アプリクーション アプリクーション アプリクーション マイヤレス メール Web サーバー 海底な外間 Carl Synchronization 設定 	名前* 種類*		AdvanceRDT633	89)IP O ICMP O 送信元ポート 165535	ICMPv6 宛先ポート 63389	0		
VPN ネットワーク マーク	保存 キャ	ッンセル						

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。

SOPHOS 🕀 XG Firewall	サービス	の追加				■ 操作ガ	イド ログビュー	アーヘルプ admin 🔻
監視 & 分析 Control Center 現在のアクティビティ レポート 診断	IP ホスト	IPホストグループ	MACホスト	FQDNホスト	FQDN ホストグループ	国別グループ	サービス	サービスグループ
保護 ルールとポリシー 使入防御 Web アプリケーション ウイヤレス メール Web サーパー 高校領統 Central Synchronization	名前* 種類*		RDT3389 ・ TCP/UDP プロトコル 「TCP マー	 IP O ICMP 送信元ポート 1.65535 	O ICMPv6 宛先ボート 3389	0		
VPN ネットワーク □ = へんが	保存	キャンセル						

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。

	ルールと	ポリシー						■ 操作ガイ	ドログビュー	P ~113	admin
監視 & 分析 Control Center		ファイアウォールルール		NAT JU-JU				SSL/TL	Sインスペクション	n-n	
現在のアクティビティ レポート	IPv4 IPv6	フィルタの無効化				ファイアウ	ォールル	ールの追加		t [相除
1915 	ルールの種類	送信元ゾーン	マ 宛先ゾーン	> 🔽 🛛	伏服	新しいファ	イアウォ	-1414-14	Filter 👻	フィルタ	のリセッ
ルールとポリシー		88	送信元	宛先	対象	サーバーア	クセスア	シスタント	とアービス		
Web	· 🗆 🖬 🖥	Traffic to Interna in 0 B, OUT 0 B	To LAN, WIFI, VPN, DMZ. would be added to this g	Firewall rules with the d group on the first match b	stinati asis if use	r selects auto	matic grou	ping_			/
アプリケーション ワイヤレス		Traffic to WAN	Outbound traffic to WAM this group on the first m	N. Firewall rules with the d match basis if user selects	lestination automatic	zone as WAN c grouping opt	l would be tion. This is	added to the d			/
メール Web サーバー	· 🗆 🖬 🖥	Traffic to DMZ	Inbound traffic to DMZ. I this group on the first m	Firewall rules with the des atch basis if user selects	itination z automatio	one as DMZ w c grouping op	ould be ad	ded to the de			/
高度な 角威 Central Synchronization	I 🗆 4	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 の木スト	SMTP, S	MTP(S)	#1	許可する			Θ
VPN	I D 5	#Default Network P in 08,00T08	LAN. すべての木スト	WAN, すべてのホスト	すべての	のサービス	#5	許可する			Θ
ネットワーク ルーティング	¥ 🗆 6 🄇	すべてをドロップ inde_outos	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	TATO	のサービス	#0				Θ
認証	6/6を表示してい	ます。0 を選択済み									

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

サーバーアクセスアシスタント(DNAT)		
内部サーバーの IP アドレス インターネットからアクセスする内部サーバーの IF	アドレスを指定します。	
 Pホストの選択 	•	
I92.168.0.2	(指定した IP アドレスと名前で IP ホストを作成します。)	
IPホスト名 192.168.0.2-内部サー	-/(
キャンセル	1/5	次へ

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。)

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		
 ● #Port1 	使用するパブレックロファドレスを指定します。	
О Туре IP	(指定した IP アドレスと名前で IP ホストを作成します。)	
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 ユーザーは、内部サーバートの選択済みサードスにア		
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	デバイスから内部サーバー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

サーバーアクセスアシスタント(DNAT)				
キャンセル	5 / 5		戻る 保	存して完了する

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。

-	ルールとポリシー			■ 操作ガイド ログ	ビューア	, <i>い</i> ぱ	admin 👻
^{監視 & 分析} Control Center 現在のアクティビティ レポート	ファイアウォールルール	REA: NAT	NATルール の使用方法	SSL/TLS インス NAT JLールの追加 🗸	ペクショ 無効	>//-//	削除
診断 	NATの種類	a レールロ	 リンク NAT ルールを非表示(<u>ਟਰ</u>		フィルタの	のリセット
ルールとポリシー			変換後	インターフェース	ID	使用率	
日1時間 Web アプリケーション ワイヤレス	目 1 DNAT to 192.168.0.2-内	送信7: すべての木スト サーヒス: AdvanceRDT63389 ウナーPort1:153120168.88	送信元: 変換前 サービス: 変換前 宛 192168.0.2-内部サーバー:1. 先:	インパウンド: Port1 アウトパウン 任意のインター ド送信 前回使用日時: Unused	#4	^ 0	•
メール Web サーバー 高度な脅威 Central Synchronization	E 2 Loopback NAT#4 DNATt	送信元 すべてのホスト サービス: AdvanceRDT63389 宛先 #Port1:153120.168.88	送信元: MASQ サービス: 変換前 宛 192168.02-内部サーバー:1. 先:	インパウン 任意のインターフ ド: アウトパウン 任意のインター ド送信: 前回使用日時: Unused	#6	^ 0	Θ
8定 VPN ネットワーク ルーティング	E 3 Reflexive NAT#4 DNAT	送信 192168.02-内部サーバー 元: 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	インパウン 任意のインターフ_ ド: アウトパウン 任意のインター_ ド送信: 前回使用日時: Unused	#5	小 О	Θ
認証 システムサービス ^{システム} プロファイル	E 4 <u>#NAT Default Network</u> や 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	インパウン 任意のインターフ_ ド: アウトパウン 任意のインター_ ド送信: 前回使用日時: Unused	#3	* 0	Θ
がストとリーとス 管理 バックアップ&ファームウ ェア 証明書	■ 5 <u>Auto added NAT rule f</u>	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	インパウン 任意のインターフ ド: アウトパウン 任意のインター_ ド送信: 前回使用日時: Unused	#1	* 0	Θ
	E 6 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	インパウン 任意のインターフ ド: アウトパウンド送信: Port1 前回使用日時: Unused	#2	^ 0	•

○ / ○ を事売しています ○ を深切落み

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

ルール名* DNAT to 192 168.0.2-内部サーバー_16092	説明 DNAT rule created using DNAT wizard. D 192.168.0.2-内郎サーバー	NAT to	
変換の設定 送信元、宛先、サービスの一致条件と	を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*	
任意	#Port1	AdvanceRDT63389	/ 0
新規項目の追加	新規項目の追加	新規項	间の追加
変換後の送信元 (SNAT)	変換後の宛先 [DNAT]	変換後のサービス (PAT)	
変換前	192.168.0.2-内部サーバー	RDT3389	
インターフェースの一致条 インパウンドインターフェース* Port1	牛 アウトバウンドインターフェース ● 任意	•	
新規項目の追加	新規項目の追加		
	□ 適有のアウトバウンドインターフェ オーバーライド ●	:ースに対する SNAT (送信元変換) を	

00000				0,00					
	ルールとポリシー					■ 操作ガー	イド ログビューア ヘノ	ける	admin 👻
監視 & 分析									
Control Center	ファイアウォールルール		NAT JL-JL			S	SL/TLS インスペクションルール	~	
現在のアクティビティ									
レポート	[Pv4] IPv6 Jイルタの無効化			ノアイアウォー	/_////	しの近辺	▶ 無効	削除	
診断		->	カキゾーン	▼ 状能				- Hzy	۷Þ
保機						アクショ		<u> </u>	-
ルールとポリシー	# 名前	送信元	宛先	建筑	ID	>>>>	機能とサービス		
侵入防御	- D 1 DNAT to 192.168.0	WAN. すべてのホ	Z WAN. #Port1	AdvanceRDT63389	#6	許可す	AV WEB APP QoS HB	—	
Web	= ± in 0 B, OUT 0 B	F				3	LinkedNAT PRX LOG IPS	Ŭ	
アプリケーション	= 🗖 🖪 🧮 Traffic to Interna	To LAN, WiFi, VPI	I, DMZ. Firewall rules with	the destination zone a	s LAN, W	iFi, VPN,			
ワイヤレス	- 🛄 🖬 🖬 in 0 B, OUT 0 B	DMZ would be ad	ded to this group on the f	irst match basis if user	selects			<i>a</i>	
メール									
Web サーバー	E Traffic to WAN in 0 B, OUT 0 B	Outbound traffic added to this gro	to WAN. Firewall rules wit	h the destination zone	as WAN	would be			
局度な肖威 October I October State									
Central Synchronization	- 🗖 🖪 Traffic to DMZ	Inbound traffic to	DMZ. Firewall rules with	the destination zone as	DMZ wo	uld be		0	
設定	= 🛄 🖬 🖬 in 0 B, OUT 0 B	added to this gro	up on the first match basi	s if user selects autom	atic grou	iping		144	
VPN									
ネットワーク	E 5 5 Auto added firewal	すべてのゾーン。 べてのホスト	す すべてのゾーン,す ペアのホスト	SMTP, SMTP(S)	#1	許可す る	AV WEB APP QoS HB LinkedNAT PRX_LOG IPS	\odot	
ルーティング		A COMAR	A COMAT						
認証	6 6 B.OUT 0 B	LAN, すべての木;	ス WAN, すべての木ス	すべてのサービス	#5	許可す る	AV WEB APP QoS HB LinkedNAT PRX LOG IPS	\odot	
システムサーヒス		1.	1.						
システム	■ 7 3 5 5 5 5 5 5 5 5 5 5 5 5	すべてのゾーン, べてのホスト	す すべてのゾーン,す ペアのホフト	すべてのサービス	#0				
プロファイル									*
ホストとサービス	7/7を表示しています。0を選択済み								

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。

😼 リモート デスクトップ接続			×
↓ リモート デスクトップ 接続			
コンピューター(C): 53389 ユーザー名: 接続時には資格情報を要求されます。	~		
★プションの表示(<u>O</u>) 接続(N)	ヘルプ	(H)

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。

administrator		
administrator	 	

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。

-	ファイアウォール	■ 提作ガイト ログビューア ヘルプ admin マ koan kelso

ログビューアが表示されます。

			-							
							1	1.5		1
	-	-		 	 -	 	 		 -	
•										
*										10.00
*										
۰.										
۰.										
-										

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。

フィルタを追	
ンポーネント アクション	フーザ名 ファイアウォー
ノイルタを追加	×
フィールド: 送信先ポート	•
条件:	
(人に一致9る)	•
值:	
03363]
	Add Filter

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。

										-		-		1
-		-	-						-	-	-			
										-				
										-				
										-				
										-				
										-				
_				-										
信先ポー	- ト 次(こ一致す	<u>ර</u> 63389	• • X)	フィルタを追	1					1			-
信先术 2	-ト次(時間	こ一致す	S 63389		フィルタを追 ログのコンポ	■ ▼ ーネント	アクシ	·Ξン	2-	- 1 72			-	-

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ヘリンクされており、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。

	Corelina C	-			■ 操作ガイド ログビューア へい	ルプ admin マ inan keiso
點視 & 分析	システム		Traffic Insight		ユーザーとデバイスの詳細	
Control Center	ab	-	Web アクティビティ 27 max 3 avg	クラウドアプリケーション	Security Heartbeat®	
現在のアクティビティ レポート	1737-752		30 24 18 12	na GApps at 08 in	0 0 0 0 リスクあ 不明 置告 接続済み	
診断	インターフェース	VPN	6	# 0 8 Out 0% 50% 100%	アプリケーション問題と制御™	
保護	0/0 RED	0/0 24702 AP	許可されたアプリカテゴリ	ネットワーク攻撃	0 0 0 1910	

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。

📨 ソフォスファ	イアウォール 🎄
管理者ヘルプ ユーザーボータ	レヘルプ コマンドラインヘルプ スタートアップヘルプ 可用性の高いスタートアップガイド 仮想アプライアンス
	 入門見 プリススアイアウォールを初めて使用する場合は、これらの推奨事項に従ってください。ソフィス アイアウォールへのアクセスを保護する方法、ファイアウォールをテストおよび快延する方法、そこでアイアウォールへのアクセスやおよび快延する方法、そこの 第後後に、快速に感じたら稼働する方法を学びます。 リクロスクワイクワウスールへの安全な管理者アクセス 集雑な管理者パスワードを設定します。デフォルトの管理者パスワードを変更するか、管理者の公開鍵認証を使用します。詳細については、「管理者の公開鍵認証の設定」を参照してください。 ・ 4 たいとれていたり、「管理者の公開鍵認証の設定」を参照してください。 ・ 5 たいとれていたり、「管理者の公開鍵認証の設定」を参照してください。 ・ 5 たいとれていたり、「管理者の公開鍵認証の設定」を参照してください。 ・ 6 たいとれていたり、「管理者の公開鍵認証の設定」を参照してください。 ・ 5 たいとれていたりたいたり、「管理者の公開鍵認証の設定」を参照してください。 ・ 6 たいとれていたいたいたいたいたいたいたいたいたいたいたいたいたいたいたいたいたいたいた
システムサービス >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	 A. MAN シリン Soon Media C ジ ドン ドン ジ ひとしょ とうや。 Symantice Finewania () シル と ジ ドレントに閉じます。 5. WANゾーンからWeb管理コンソールにアクセスすることはできません。禁止されているエラーが表示されます。

以上