

さくらのクラウド「仮想型 UTM マネジメント」サービス利用手順書 Sophos Web サーバープロテクション(WAF)編



内容

改訂履歴	2
はじめに	3
1. ご利用環境の構成	4
2.バックエンド Web サーバーの作成	5
3. 保護ポリシーの作成	8
4. 証明書の作成	11
(1)Default の証明機関を設定する。	11
(2)SSL 証明書を Sophos Firewall で作成する。(自作 SSL 証明書)	13
(2)発行済の SSL 証明書をアップロードする。	14
5. ユーザーポータルの HTTPS ポート設定変更	16
6 .WAF ポリシーの作成	17
7.WAFのアクセスログ確認とフィルタルールのスキップ設定	19
(1)サイトへの正常系アクセスログを確認	19
(2)出力されたルール ID を確認	23
(3)「フィルタルールのスキップ」へ、誤検出のルール ID を追加	23
(4)インフラストラクチャルールについて	25
8.WAFの動作確認	26
9. 設定のまとめ	28
10. 詳細の機能と設定を知りたい時	28

さくらのクラウド「仮想型 UTM マネジメント」サービス利用手順書 Sophos Web サーバープロテクション(WAF)編

改訂履歴

版数	更新日	更新内容	更新者
1.0	2020/5/25	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定	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定	興安計装株式会社
3.1	2023/8/29	OS バージョン差分修正	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 ユーザーアシスタント

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. バックエンド(保護対象の Web サーバー)の作成
- 2. 保護ポリシーの作成※モニターモード
- 3. HTTPS 証明書の作成
- 4. ユーザポータルのポート変更
- 5. WAF ポリシーの作成
- 6. Web サイトへのアクセスログを確認
- 7. ルール ID を抽出
- 8. スキップルールの設定と、ポリシーを拒否モードで動作

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

ネットワークプロテクション編

https://www.owlook.jp/public/document/sophos_nrtworkprotection.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 Port1 を接続したルーター+スイッチの保持するグローバル IP アドレスを設定します。
- > 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 192.168.0.8/24 を持ちます。
- ▶ 保護対象システムのリッスンポートは HTTP(80)です。
- ▶ 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。
- > 保護対象システムは Wordpress5.4.16 です。
- 保護対象システムの FQDN は webserver.koan-eng.be です。

2. バックエンド Web サーバーの作成

※今回の手順では「1.ご利用環境の構成」に基づき記載します。

①ホストとサービス > IPホストタブ > 追加をクリックします。

	ホフ	ストとサービス			■ 操作ガイド ログビューア ヘルプ admin • koan keiso
BRASH Control Center 現在のアクティビティ レポート	Ŀ	P#25	Z HAC#21	FOONホスト FOONホストグループ 開始グループ	サービス サービスグループ
が出 ルールとポリシー な入野者	0	88 V -	811	FFLADIM V	2000 NB株 Pバージョン V 信理
Web アプリケーション ワイヤレス メール	7	##ALL_IPSEC_RW ##ALL_IPSEC_RW6	システムホスト システムホスト	NA.	IPv6
Web サーバー 高度な用い Central Synchronization		##ALL_RW	システムホスト	NA	IPv4
RE VPN	0	WALL_RW6	システムホスト	NA.	IPv6
ネットワーク ルーティング 御屋		##ALL_SSLVPN_RW	システムホスト	NA	IPv9
52969-22		#RALL_SSLVPN_RW6	システムホスト	NA	IPv6
プロファイル ポストとサービス		#Port1-0	システムホスト		IPvil
10日 10日 10日 11日 11日 11日 11日 11日 11日 11日	0	#Port1:1	システムホスト		IPv9

②今回は名前を「web_host」、IP アドレスを「192.168.0.8」とし保存をクリックします。

507405 0	IPホストの編集				■ (R)	ゆめイド ログビュー	ーア ヘルプ admin • koan keiso
Bill ト Stil Control Center 現在のアクティビティ レポート JIM	ゆホスト タホストグループ	HACRON	FORMAR	FQDN:#21-0%-7	戦制クループ	9 -82	サービスグループ
62	名前*	web_host					
ルールとポリシー 住入的間	IPパージョン*	IPv4					
Web アプリケーション	環境・	p.					
ワイヤレス	ドアドレス*	19216808					
Marg 9-7/- Alt v # 4 Cartral Synchronization 部 2 マントワーク トーティンク 記録 システムサービス システムサービス	ゆホストクループ		E規項目の追加				
プロファイル ホストとサービス 警理 パックアップ&ファームウェア 足利者	407 17-226						

③web_host が生成されていることを確認します。

ホストとサービス	D	<u>19216812199</u>	IPアドレス	19216812199/255255.255.255	IPv4	A* 1
官兵 バックアップ&ファームウ		192168128	IPアドレス	192.168.12.8/255.255.255.255	IPv4	A 1
エア 証明書	C	web host	IPアドレス	192168128/255255255255	IPv4	A 🛈

507405 ©	Web サーバー			■ 操作ガイド	ログビューア ヘルブ admin・ koan keiso
ER 5 198 Control Center	1940 サーバー	保護シング	問題ポリシー	間目テンプレート	\$492
現在のアクティビティ レポート 診断			۰ ۸,۲,۲	被加	ADM Hills Sing
*** ファイアウォール Q.3.800 Web アプリケーション ワイヤレス	レコードが見つかりません				
メール Web サーバー Put Gran					

④Web サーバー > web ポリシータブ > 追加をクリックします。

⑤名前は任意ですが、今回は「web-server」、ポート「80」とします。ホストは①~③で作成し

	Web サーバーの編	鏶		● 論作の-(1)	5 ログビューア へらブ admin・ iconitatio
ERLON	Web 27-75-	885.15-	885/3-	間接をしていート	2497
Control Cantar 現在のアウティビティ					
Loff-F					
28	9 E .	102,1010			
611 Dire (1999)	20.48				
97479x-16 93.88					
Web	ホスト・	web_host	•		
アプリケーション	18:0	プレインデキストン	110		
3-5	#->*	80			
Web サーバー	8-72547				
ARUAN		٠.			
Central Synchronization	945791.	300			
UTN CON	パックエンド療徳プーリングを	MBCY D			
ネットワーク					
1-7420					
システムサービス					
1.374					
707746					
ホストとサービス					
11日本 バックアップトファールウ					
17					
248					
					
	60 (HD-10)				

た「web_host」を選択し、他の項目はデフォルトのまま保存をクリックします。

⑥web-server が作成されていることを確認します。

507405 0	Web サーバー			■ 操作ガイド	ログビューア へルプ admin + koan keiso
Control Center	Web #-/(保護ポリシー	御田ポリシー	間経テンプレート	2002
現在のアクティビティ レポート 2015	_				izho Hille
82		 木スト 		後知	管理
ファイアウォール 収入的制	U web server	web_host		プレインテキスト(HTTP)	× 8
Web					
ワイヤレス					

※Web サーバーについては、実サーバーのリッスンしているポートが HTTP (80) か HTTPS (443) かで、設定を適宜変更してください。今回の手順では「1.ご利用環境の構成」に基 づき記載します。

3. 保護ポリシーの作成

①Web サーバー > 保護ポリシータブ > 追加をクリックします。

	Web サーバ	_			■ 操作力イド	ログビューア ヘルプ edmin・ koan keiso
ER & 96 Control Center 現在のアクティビティ レポート	Web 17-/(-	Ģ	保護ポリシー	自己ポリシー	ロロテンプレート	
27M	C 88 7					- <u><u><u></u></u></u>
◎Ⅲ ファイアウォール	Excharge.Aut	2 ALCOVER				/
经入时期 Web	Exchange Der	secal.				/
アプリケーション ワイヤレス	Arvantere	look				/
x-1	 Hicrosoft Lyn 					/
100 9-70- ALE URM	 Microsoft RD 	Web.2008				/
Central Synchronization	 Microsoft RDC 	2008				/

②任意で名前を入力します。今回は「waf_policy」と入力します。

	保護ポリシーの編集	EC.		■ 操作力イド	ログビューア ヘルプ admin・ koan keise
ER 5 20日 Control Center 現在のアクティビティ レポート	Web th-PC-	保護ポリシー	間目ポリシー	間ビアンプレート	2022
2155	名明•	waf_policy			
5回 ファイアウォール 収入的部	20.01				
Web	Outlook Anywhere の非監視				
アプリケーション ワイヤレス	€-κ.	₹ = 9-	•		
×-16	Cookie 署名				
Aguna	スタティック URL ハードニング				
Central Synchronization	フォームハードニング				

このポリシー設定ではさまざまなセキュリティ検査ポリシーを設定することができます。 保護機能の詳細は Sophos Firewall ユーザーアシスタントをご覧いただくか、本サービスの 仕様書をご覧ください。

Sophos Firewall ユーザーアシスタント

https://doc.sophos.com/nsg/sophos-firewall/19.5/help/en-us/webhelp/onlinehelp/index.html Sophos Firewall イメージ提供の仕様書 https://www.owlook.jp/public/document/sophos xg shiyou.pdf

or stell	Web #t _ If _	@lanf112	10013
ontrol Center	Web 5 -71-	1440/11/2/2/-	REAL PROPERTY SHOW
在のアクティビティ			
*	久前 *	Domain States	
N),	3400	-wat "bolicy	
	說明		
ルとポリシー			
(約30)		1	
b	Outlook Anywhere の非監視		
プリケーション			12
TPUZ	246-0014-001	t=9-	Ŷ
-JL	Cookie署名	OFF	
bサーバー	スタティック UPL ハードニング		
にな僧族		OFF	
ntral Synchronization	フォームハードニング		
	and the second second		
N	マルウェア対策		
ットワーク	低レビュテーションのクライアントをブ		
ーティング	ロック		
Œ	共通の脅威フィルタ	ON	
ステムサービス	フィルタの弾度	Local a reading of	225
τ Δ .	A STATE A SAME	レベル1(銀石橋い)	*
コファイル	フィルタルールのスキップ		
(トとサービス			
I.		検索/追加	+
クアップ&ファームウ			
	アプリケーション攻撃		

③今回はモードを「モニター」、「共通の脅威フィルタ」を ON にします。

④共通の脅威フィルタを ON にすると、画面下部に脅威フィルタのカテゴリが表示されます。今回はすべてのカテゴリが ON の状態で保存をクリックします。またフィルタの強度をレベル1 (最も緩い)からレベル4(最も厳しい)まで設定可能です。今回はレベル1で設定ます。

ワイヤレス	共通の脅威フィルタ	
メール		
Web サーバー	フィルタの強度	レベル1(最も緩い) ・
高度な脅威	フィルタルールのスキップ	
Central Synchronization	5 170 700 70000 (199	
設定		
VPN		枝繁/追加 中
ネットワーク	マプリケーションが酸	_
ルーティング	テラリケーション攻撃	
認証	SQL インジェクション攻撃	
システムサービス	XSS 攻擊	
システム	プロトコル強化	
プロファイル	フキャナ検出	
ホストとサービス		
管理	データ流出	
バックアップ & ファームウ		
ェア		
証明書	保存キャンセル	

⑤waf_policyが生成されていることを確認します。

	Web	サーバー			■ 操作ガイド	ログビューア ヘルプ admin・ koan keiso
ER 5 11年 Control Center 現在のアクティビティ		Web 19-7(-	保護ポリシー	間目ボリシー	認証テンプレート	2022
Lult-h						2030 HDR
	0	88 V				 管理
sa ファイアウォール		Exchange AutoDiscover				/
包入150回 Web		Exchange General				/
アプリケーション		Exchange Outlook Acrosomer				/
X-1		Microsoft Lanc				/
Webサーバー 高度な発展	0	Microsoft RD Web 2008				/
Central Synchronization		Microsoft RDG 2008				/
NE VEN	0	waf_colicy				/ 8

4. 証明書の作成

HTTPS サーバー証明書は、Web サイトの実在性を確認し、ブラウザとウェブサーバー間で通 信データの暗号化を行うための電子証明書です。認証機関から発行されます。HTTPS サーバー 証明書には、Web サイトの所有者の情報や、暗号化通信に必要な鍵、発行者の署名データが含 まれています。

ローカル署名した証明書を生成する際は、Default の証明機関の設定を先に行う必要があります。 証明書 > 証明機関(CA)タブ > Default のオブジェクトをクリックします。

-	証明	月書			 MARK 	WF DØEs	-7 ^	ルブ admin • Ktanketst
Control Center		1288	azimmet toka		Dertificat	e Revocation List ()	en n ez.	ан
ME0/974074 レポート 認問		北田 立	1	MINT	878	88 77	10.50	H(1a
na ルールとポリシー	0	Default		2020-02-03	2030-12-01	内部		/
423,3588 Web		SecurityAppMance_SSL_CA	C=06.0T=0utoretree/0=Septex/0U=8/GG/CH=Septex 502 CA_CETOD/XCU/FR054Kemathateses-support@reption on m	2015-08-01	2037-02-03	BERT	٩	0 č
97192-282 971922 X-11	0	AAAGerLifeateGervices	/C+GE/S1+Greater Manchester L+Saflad/O+Carrols CA United OI+AUL Certificate Services	2004-01-01	2028-12-31	Enter S		× 8
Web 19-11-	0	ACA ROOT	C+ESharahunbar-02963086/0+CONSEJO GENERAL DE LAABOGACIA/CN+AGA/R007	2010-05-27	2041-05-27	5rt-r		10
ALE Grant	0	ACCVRAZI	CN+ACCVR821/OU+INGACCV/O+ACCV/C+EE	2011-05-05	2030-12-91	Britis		/ 8
NE VEN	0	AGEDICOM, Not	ICN-ACEDICON ROMOU-PRIG-EDICONIC-ES	2008-04-18	2028-04-13	Exper-		/ 8
ネットワーク	0	ADNUB	IC+SIO+ACRAB	2003-05-15	2029-05-15	5rtor		10
10-94 222 1011	0	AC MAIL DAVE	IC-REVIG-DIRECCION DENERAL DE LA POLICIA/OU-DIRECN-AC RAIZ DIRE	2006-02-18	2036-02-06	BRH		/ 8
57577-FX	0	AC Rolz Certicemera S A	IC+CO/G+Gociettiel Cameral de Cartiticación Digital - Carticianara S.A./ON+AC Raiz Carticianara S.A.	2010-05-24	2031-05-24	Erekt		18
707744	1	ANCERT Certificados CON V2	IC=ES/O=Agencia Notestal de Cestificacion S.L.U CIP 853395805/CN=ARCERT Cestificacion CGN V2	2010-05-25	2030-05-25	BRAN		/ 11
III	0	ANCERT Certificados Notariales	/C+ES/O+Agencia Notacat de Certificación S.L.U CIF EUX/995855/CH+ANCERT Certificados Notacates V2	2010-05-25	2030-05-25	EN.M.		18
149793839-169	0	ANE Global Root CA	IC-4557-BaccelotaX-Banatora (see surrant address at http://www.adf.educatores.dov/clas.ttml.y0+A00F Autombed at Certificacon/OLI+A00F Class.	2013-06-10	2033-08-05	yard.		× 11

(1) Default の証明機関を設定する。

Sophos Firewall 内部で SSL 証明書を生成する場合に、証明機関として参照する設定を行いま

す。

- ① 証明機関の詳細を以下の例示を参考に設定します。
 - ・国名: Japan
 - ・都道府県: Tokyo
 - ・地域名: Chiyoda-ku
 - ・組織名:koan keiso ※会社名等
 - ・組織単位名:sales ※部署名等
 - ・一般名(CN): koan keiso ※会社名等
 - ・メールアドレス:任意のメールアドレス

さくらのクラウド「仮想型 UTM マネジメント」サービス利用手順書

Sophos Web サーバープロテクション(WAF)編

・秘密鍵のパスワード:任意のパスワード

・鍵の種類:デフォルトのまま使用します。※デフォルトは RSA です。

・鍵長:デフォルトのまま使用します。※デフォルトは2048です。

・セキュアハッシュ:デフォルトのまま使用します。※デフォルトは SHA-256 です。

下部の保存ボタンをクリックします。

5 × .		
名則 *	Default	
国名 *	Japan	~
都道府県*	Tokyo	
地域名*	Chiyoda-ku	[例:市名]
組織名 *	koan keiso	[例:会社名]
組織単位名 *	sales	[例:部署名]
一般名 [CN] *	koan keiso	[例: サーバーの木スト
メールアドレス *	sample@example.com	
秘密鍵のパスワード*		
鍵の種類 *	● RSA ● 楕円曲線暗号	
鏈長 *	2048	~
ヤキュアハッシュ*	OLLA DER	

続いて、ローカル署名した証明書の作成を行います。

-	証明書					■ 操作ガイド ログビューア へ	ルブ admin • koan kelso
ERA 26 Control Center 現在のアクティビティ		298		ESTERNI (CA)		Certificate Revocation List(亚明鲁夫阶)	(2 N)
レポート	□ 名前 ▽	L	脑目	H78	1216.4	8640 V	16128 5572
5回 ファイアウォール 伝入的制	Appliance.ert	ficate 2	015-08-01	2037-01-01	×	アップロード	٥
Web アプリケーション							
メール Web サーバー							
消息をな作品 Central Synchronization							
^{田田} VPN ネットワーク							
ルーティング 障壁 システムサービス							
5374 プロファイル	/						
ホストとサービス 管理 パックアップ& ファールウ							
iina]						

(2) SSL 証明書を Sophos Firewall で作成する。(自作 SSL 証明書)

Sopohos Firewall 内部で SSL 証明書を生成する場合の手順です。今回はこの手順で生成する証明書を利用して設定を行います。

① ローカル署名した証明書の生成を選択します。

-	証明書	3	フィードバック	■ 最初初一个下	09Ea-7	へんプ admin・ 観史計算用式会社
Control Center	1118	(Ethink ICA)		Certificate Revo	oeten Let (正明書)	HE CAR
単世のアクティビティ レポート ゼロディ対策 副前	79585+	○ 証明書のアップロート ◎ ローカル署名した証明書の主成	Ошнина	編束(CSP)の生	a	

- ② 証明書の詳細セクションを以下の通り設定します。
 - ・名前:webserver.koan-eng.be ※Web サーバーの FQDN を使用します。
 - ・開始日、終了日:デフォルトのまま使用します。※デフォルトは1年です。
 - ・鍵長:デフォルトのまま使用します。※デフォルトは2048です。

・セキュアハッシュ:デフォルトのまま使用します。※デフォルトは SHA-256 です。 証明書の詳細

名前*	webserver.koan-eng.be	
開始日*	2022-04-08) 🏥
終了日 *	2023-04-08	
鍵の種類*	● RSA ● 楕円曲線暗号	
雄長*	2048 🗸	
セキュアハッシュ *	SHA - 256 🗸	

③ サブジェクト名の属性セクションは、Default 認証機関から引用されている部分はそのま ま利用し、不足箇所について設定を行います。

・一般名	(CN): webserver.koan-eng.be	※Web サーバーの FQDN を使用します。
サブジェクト名の	D属性	
国名	Japan	v
都道府県	Токуо	
地域名	Chiyoda-ku	(例:市名)
組織名	koan keiso	[例: 会社名]
組織単位名	sales	(例:部署名)
一般名 [CN] *	webserver.koan-eng.be	(例:サーバーのホスト名)
メールアドレス	sample@example.com	

④ サブジェクト代替名(SAN)セクションは、詳細設定を開き、証明書 ID に DNS を選択して
 Web サーバーの FQDN を設定します。

サブジェクト代替名	(SAN)
-----------	-------

DNS 名			
	検索 / 追加		
IPアドレス			
	検索 / 追加		
詳細設定 ▼			
証明書ID	DNS	webserver.koan-eng.be)

下部の保存ボタンをクリックします。

⑤ 証明書の一覧から自己証明書が生成されていることを確認します。

証明	書				■ 操作ガイド ログビュー:	ア へいプ admin ▼ koan keiso
	証明書		認証局 (CA)		Certificate Revocation List (証明	書失効リスト)
					i	訪加 削除
	名前 🖓 🔹	開始日	終了日	認証局	種類	管理
	ApplianceCertificate	2015-08-01	2037-01-01	~	アップロード	۵
	webserver.koan-eng.be	2020-05-21	2021-05-21	~	自己署名	تْ 💌 单

(2)発行済の SSL 証明書をアップロードする。

パブリックな認証局より発行された証明書等、既に発行済の HTTPS 証明書を設定する場合の 手順です。※今回の手順では使用しません。参考までに記載します。

①証明書アップロードを選択します。必須項目として名前、証明書ファイルの形式を選択し、 HTTPS 証明書ファイルをアップロードします。HTTPS 証明書の形式により、任意で秘密鍵、パ スフレーズを入力し保存をクリックします。 さくらのクラウド「仮想型 UTM マネジメント」サービス利用手順書 Sophos Web サーバープロテクション(WAF)編

5.96 vital Deter 第07-09-4 ビディ ポート	臣时妻		EILLIN (CA)	Centrate Resocution Lat (道理書系句(以及))
新 アイアウォール 入方数 約 ブリケーション イヤリース	アウション・ 証明書の詳細	◎ 証明書のアップロード 🔘 自己	鼻名した症時暮き生!	成する 🚫 証明書審名表示 (CSP) を注成する
-/L dr Y-/L- EURA Intel Synchronization	名前・ 証明書のファイル形式・ 証明書・	「 「FEH [pain] 「ファイルを編成」編成されていません。	• PEH (Jan) TUR	必須項目
177-9 7425 1 18749-22 17744 17744	10日期 17スフレーズ/P5K	27イルを選択 通知されていません 「パスフレーズ/PSK	Ney 形式のファイ	必要な場合のみ設定

5. ユーザーポータルの HTTPS ポート設定変更

Sophos Firewall はユーザ向けのリモートアクセス等の機能提供用にユーザポータル機能があります。デフォルトでは、HTTPS ポートを使用している設定になっているため、今回設定する手順とポートが重複するため以下の通り、変更が必要です。

管理 > 管理者とユーザの設定 > 管理コンソールとエンドユーザ間の操作セクション より

ユーザポータルの HTTPS ポートを、今回は 443 から 4443 へ変更し適用をクリックします。



6.WAF ポリシーの作成

ここまで、以下のコンポーネントと関連項目の設定をしてきました。

- ・バックエンド(保護対象)Web サーバー
- ・保護ポリシー
- ・SSL 証明書
- ・ユーザポータルの HTTPS ポート変更

これらのコンポーネントを使用して、ファイアウォールのルールに WAF ポリシーを追加します。

①ルールとポリシー > ファイアウォールルールの追加 > 新しいファイアウォールルールをクリックします。

-	ルールと	ポリシー				■ 18075111	ログビューア へルブ edmin - koat keine
BIR & Set Control Center	1	271228-66-6		NAT (L-)	ь.	196/718	f23/105425-5
現在のアクティビティ レポート	633 IPv6	フィルタの無効化				ファイアウォールルールの危険	82 83
	16-160848	anara a	10.8.V-	5 I	112	新しいファイアウォールルール	1 w • 2+69000v+
ルールとポリシー		4.8	885.	88	HB	サーバーアクセスアシスタント (DNAT)	29-63
Web	10 1 3	DNAT to 192 168 12.	WAN FRIDRAN	LAN, APOPUL	Advise	Namus data and a to	
アプリターション	10.1	DNAT Advanced RDT	WWW.WASTINERS	LAN REGIST	All of	CARDY MARKET CARD	DE L'ANDER DE LA CAL

アクション > 承認のプルダウンメニューで「Web サーバープロテクションで保護する」を選択します。今回はルール名を waf_rule とし、ルールの位置を最上位を選択します。

-	ファイアウォールルールの	追加	■ ■#5+ド ロ	ビューア ヘルプ admin - kean heres
BELSON Control Center 現在のアクティビティ		201 3 73 700	A-A002	
ыл-н ВМ	アクション Webサーバープロテクションで保護する		A-A7A-7	
ルールとポリシー 42入的(99	40	1	05-7C 080	CC-ORENOTT.

Sophos Web サーバープロテクション(WAF) 編

③ホスト型サーバーセクションを以下の通り設定します。

- ・ホスト型アドレス:#Port1
- ・HTTPS、HTTP のリダイレクト:チェック
- ・リスニングポート:443
- ・HTTPS 証明書:webserver.koan-eng.be
- ・ドメイン:webserver.koan-eng.be ※HTTPS 証明書の内容を読み取るため自動的に設定

されます。

リスニングポート*	ドメイン*	
443	webserver.koan-eng.be	ø •
HTTPS		
-	検索/追加	+
HTTPS 証明書 *		
webserver.koan-eng.be	*	
	▼ Uスニングポート・ 443 ✓ HTTPS HTTPS 証明書・ webserver.koan-eng.be	Vスニングポート・ ドメイン・ webserver.koan-eng.be webserver.koan-eng.be webserver.koan-eng.be webserver.koan-eng.be webserver.koan-eng.be

④保護されたサーバーセクションを以下の通り設定します。

・Web サーバー:web_server ※選択してチェックします。

保護されたサーバー

Web サーバーのリスト		選択した Web サーバー	
入力して検索	作成する	web_server	×
✓ web_server			

⑤詳細設定セクションを以下の通り設定します。

・ポリシー保護対策:waf_policy を選択

・ホストヘッダをパス:チェック

画面下部の保存をクリックします。

詳細設定				
保護対策	侵入防御 🛕		トラフィックシェーピング	
waf_policy	なし	-	なし	-
追加オプション				
 圧縮サポートの無効化 				
 HTMLの書き換え 				
✔ ホストヘッダをパス				
保存キャンセル				

7.WAFのアクセスログ確認とフィルタルールのスキップ設定

Sophos Firewall の保護ポリシーはデフォルト設定が厳格なため、誤検知を防ぐために下記の 作業が必要になります。

- 1. 保護ポリシーでモニターモードで設定
- 2. Web サイトへ正常系アクセス試験を一通り実施しアクセスログを確認
- 3. 検出されたルール ID を「フィルタルールをスキップ」リストへ設定

※今回の手順では「1.ご利用環境の構成」に基づき記載します。

(1) サイトへの正常系アクセスログを確認

アクセスログの確認は GUI で提供されるログビューア一機能では、ルール ID を確認すること ができません。SSH でアクセスし、Advance Shell 機能を利用する必要があります。本手順では、 AdvancedShell によるログ確認方法を記載します。

尚、Advance Shell(CLI)の操作方法についてはサポート対象外となるため、ご利用者様の責 任において操作いただくようお願いします。

①アクセスログの確認準備をします。

本手順では一時的に WAN 側の SSH アクセスを許可しアクセス方法を記載します。

※安全の為、LAN 側からのアクセスを推奨します。



管理 > デバイスアクセス > WAN > SSH にチェックを入れ適用をクリックします。

②任意のターミナルソフトから SSH でログインします。

この時のアカウントは Webadmin へのアクセスアカウントと同様です。

● TCP/IP	ホスト(T): webserver.koan-eng.be	`
	図ヒストリ(0) サービス: O Telnet TCPボート#(P): 22	2
	● SSH SSHバージョン(V): SSH	2 \
	○その他 プロトコル(C): UNSP	EC 、
	#	

③ログイン後メニューが表示されます。 5. Device Management > 3. Advanced Shell を 選択します。



ophos Firmware Version SFOS 17.5.10 MR-10.HF052220.1
evice Management
 Reset to Factory Defaults Show Firmware(s) Advanced Shell Flush Device Reports Exit
Select Menu Number [0-4]: [

④ログイン後、以下のコマンドでリアルタイム出力をキャプチャする準備をします。この時、以下のキーワードを指定します。

- ・Web サーバーの FQDN: webserver.koan-eng.be
- ・ModSecurity による Pattern match : security2:erro

tail -f /log/reverseproxy.log | grep "webserver.koan-eng.be" | grep "security2:error"

⑤Web サーバーヘアクセスし、一通り正常にアクセスできることを確認します。

https://webserver.koan-eng.be/



https://webserver.koan-eng.be/wp-login.php

ユーザー各またはメールアドレス パスワード
/CCワードを出版れてすか! = Sophea UTM で、Webで中ユ UFイー対策 に課意

⑥ログ出力の内容を確認します。

~ 一部抜粋 ~

[Mon May 25 17:24:20.627329 2020] [security2:error] [pid 18358:tid 140426983933696] [client XXX.XXX.XXX.XXX:42914] [client XXX.XXX.XXX.XXX] ModSecurity: Warning. Operator TX:inbound_anomaly_score. LT matched 5 at [file "/content/waf/2.7.3/modsecurity_crs_correlation.conf"] [line "33"] [id "981203" [msa "Inbound Anomaly Score (Total Inbound Score: 3, SQLi=1, XSS=): Restricted SQL Character Anomaly Detection Alert - Total # of special characters exceeded"] [hostname [unique_id "webserver.koan-eng.be"] "/wp-admin/load-styles.php"] [uri "XsuAs38AAAEAAEe2opYAAAAa"], referer: https://webserver.koan-eng.be/wp-admin/

[Mon May 25 17:27:50.489546 2020] [security2:error] [pid 18358:tid 140426849650432] [client XXX.XXX.XXX.XXX:33583] [client XXX.XXX.XXX.XXX] ModSecurity: Warning. Pattern match "¥¥¥¥W{4,}" ARGS:submit. ſfile at "/content/waf/2.7.3/modsecurity_crs_generic_attacks.conf"] [line "37"] id "960024"] [rev "2"] [msg "Meta-Character Anomaly Detection Alert - Repetative Non-Word Characters"] [data "Matched Data: ¥¥xe3¥¥x82¥¥xb3¥¥xe3¥¥x83¥¥xa1¥¥xe3¥¥x83¥¥xb3¥¥xe3¥¥x83¥¥x88¥¥xe3¥¥x82¥¥x92¥¥ xe9¥¥x80¥¥x81¥¥xe4¥¥xbf¥¥xa1 within found ARGS:submit: ¥¥xe3¥¥x82¥¥xb3¥¥xe3¥¥x83¥¥xa1¥¥xe3¥¥x83¥¥xb3¥¥xe3¥¥x88¥¥xe3¥¥x82¥¥x82¥¥x92¥¥ xe9¥¥x80¥¥x81¥¥xe4¥¥xbf¥¥xa1"] [ver "OWASP_CRS/2.2.7"] [maturity "9"] [accuracy "8"] [hostname "webserver.koan-eng.be"] [uri "/wp-comments-post.php"] [unique id "XsuBhn8AAAEAAEe2orkAAAAq"], referer:

https://webserver.koan-eng.be/2020/05/13/hello-world/

~ 一部抜粋 ~

[id "9XXXXX"]セクションが、WAF のルールにマッチした ID です。

※AdvancedShell(CLI)による確認方法を、WAN 側からのアクセス方法で記載しましたが、安全の為、LAN 側からのアクセスを推奨します。または目的とする行為が完了後に WAN 側の SSH アクセスを無効化するようお願いします。

(2) 出力されたルール ID を確認

ログに出力されたルール ID は、下記の2つです。 ルール ID にはインフラストラクチャルール というルールが含まれます。

[id "981203"] ←インフラストラクチャルール [id "960024"]

検出されたルール ID のうちインフラストラクチャールール以外の ID を「フィルタルールのス キップ」 リストに追加します。

[id "960024"]

(3)「フィルタルールのスキップ」へ、誤検出のルール ID を追加

①Web サーバー> 保護ポリシー > waf_policy タブをクリックし3. 保護ポリシーで作成したwaf_policy を編集します。

-	Web	b サーバー			■ 操作力イド	ログビューア ヘルプ admin * koan keiso
SEL 5 21F Centrel Center 現在のアクティビティ		Web #-/(-	保護ポリシー	間形ポリシー	間目をシブレート	24222
レポート 2016	0	8M 7				2010日 第13年 第19世
9月 ファイアウォール	0	Exchange sutoDiscover				1
经入防御 Web		Exchange General				/
アプリケーション ワイヤレス	1	Exchange Outlook Acrostere				/
X-12	0	Microsoft Lyne				/
Aguns		Microsoft RD Web 2008				/
Central Synchronization		Microsoft RDG 2008				/
VPN	0	waf_qolicy				/ 8

②フィルターのスキップセクションから id を入力し、+マークをクリックします。

フィルタルールのスキップ		
	960024	

フィルターのスキップに id が追加されました。

さくらのクラウド「仮想型 UTM マネジメント」サービス利用手順書 Sophos Web サーバープロテクション(WAF)編

フィルタルールのスキップ	960024	<i>I</i> O
	検索/追加	+

※本手順はサンプルの為、id を一つのみ記載しましたが、実際の環境に合わせて検出されたフィルターのスキップ id を追加してください。

③フィルターのスキップリストの入力が完了したら、モードを「モニター」から「拒否する」に 変更し画面下部の保存をクリックします。

説明		
		11
Outlook Anywhere の非監視	OFF	
モード*	拒否する	•
Cookie署名	OFF	

※保存をクリックした時点で、Web サーバーに対する防御機能がオンになります。

(4) インフラストラクチャルールについて

インフラストラクチャルールと呼ばれる特定のルールがあります。それらは WAF ModSecurity の中核となるルールです。これらのルールに基づいて他のルールは構築されています。インフラ ストラクチャルールがフィルタールールのスキップリストに追加されている場合、関連するルー ルが無効となり潜在的な攻撃に対して脆弱になるため、以下に記載されたインフラストラクチャ ールールは無効にしないことを推奨します。

- 901100
- 901110
- 949100
- 949190
- 949110
- · 959100
- · 980100
- · 980110
- 980120
- 980130
- 980140

8.WAF の動作確認

簡易的な攻撃を実行し実際の検知を確認します。トップページに意図的なクエリを含め Web サーバーヘリクエストします。※具体的な攻撃方法の解説は省略します。

https://webserver.koan-eng.be/?auth=1'



不正なクエリを検出し、「You don't have permission to access this resource.」(403)と表示されました。ブラウザの表示は下記になります。



Advanced Shell による確認(CLI)は先に記載した通りですので、ここではログビューア―に よる確認(GUI)を記載します。

①画面右上のログビューア一をクリックします。

	Cartinal Cartar		■ 操作ガイト ログビューア ^ ルプ admin ▼
			NUBI KESU
	2- 2-		
-			

③ ログビューアーを開き、Web サーバープロテクションでフィルタをかけます。

0921-7							#25-72.1					
	c 🛓								-	<u>⊅</u> 779 <i>x−b</i>	Search.	٩
フィルタ:	アクティブなフィルタはあ 時間	りません フィルクをめ ログのコンボーネント	アクション ユーザ&	ファイアウォールウルール	受信インターフェース	送薪インターフェース	送信元 P 送信先 P 送信元ポー	4一次成品版	701-3	ATP (Avanced Threat Protection) アプリケーションフィルタ	にいたいのうアルタイム情報	セット メッ
77479 77479	2020-05-25 15:03:59	Firewall Rule	Allowed	4	Portà	Port2		63389	TCP	結証 電子メール コーノマウォード	<u>HCAP を聞く</u>	
29-170 #=10	2020-05-25 15:03:51	Firewall Rule	Allowed	8	Port1	Port2		63389	TCP	IPS RIVDIP	BCAP BERK	
27-170	2020-05-25 15:03:48	Firewall Rule	Allowed	4	Portà	Port2		63309	TOP	Sandstorm セキュリティハートビート システム	BCAP ENEX	
D 27-770 2-10	2020-05-25 15:03:43	Invalid Traffic	Denied	•				43332	TOP	Web コンテンツポリシー Web フィルタ Web Server Protection	CAP 登職 <	Col ast pac am cor
											-	

③該当の通信が WAF Anormaly として検知されていることが確認できます。

	075	2-7					ポリシー	92.Þ			
11 C ±								To Note	rver Protection	•	SearchQ
フィルタ:アクティブなフィルタはありません 時間 サーバー	マルクを追	URL		理由	メッセージ	秋田のコード	受机バイト政	医肌代化酶	メッセージロ	ポリシーロ	リセット PCAP のリアルタイム情報
With Server 2020-05-25 18:15:38 webserver Protection eng be	cen-					200	809	242	17071	z	<u>PCAP を聞く</u>
No Server Protection	can-			WAF Anomaly	Inbound Anomaly Score Exceeded (Total Score: 10, SQL=6, XSS=) Last Matched Message: 981242-Detects classic SQL injection probings 1/2	403	1557	3505	17071	z	PCAP を聞く
Web 2020-05-25 18:14:53 Webserver Server Protection	-					1	809	242	17071	z	PCAP を開く
		WAF Anomaly	Inbound Anomaly Score: 10, SQLI=6 Message: 981242 injection probings	Score XSS= 2-Dete 1/2	Exceeded (Total): Last Matched cts classic SQL						

9. 設定のまとめ

WAFを設定するために、以下に記すコンポーネントを WAF のポリシーに関連付けます。

- 1. バックエンド(保護対象の Web サーバー)の作成
- 2. 保護ポリシーの作成※モニターモード
- 3. HTTPS 証明書の作成
- 4. ユーザポータルのポート変更
- 5. WAF ポリシーの作成

ポリシーを作成したら、以下に記すステップでポリシールールのチューニング行います。

- 6. Web サイトへのアクセスログを確認
- 7. ルール ID を抽出
- 8. スキップルールの設定と、ポリシーを拒否モードで動作

これらを段階的に実施することで、最適な WAF ポリシーを構築することが可能です。

10. 詳細の機能と設定を知りたい時

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。

	Control C	artar			■ 操作ガイド ログビューア へいに admin v koan keiso			
監視 & 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 Heartbeal			
現在のアクティビティ	パフォーマンス	サービス	30 24	NO Apps	0 0	0 0		
レポート		0.	18	#08h	0,000 mm	10 10 10 10 10 10 10 10 10 10 10 10 10 1		
診断	インターフェース	VPN	6 0 5分母にヒット	≓ 0 8 0ut 0% 50% 100%	アプリケーション	同期と制御™		
保護	0/0 RED	0/0 ワイヤレスAP	許可されたアプリカテゴリ	ネットワーク攻撃	0 9710 591	0 0 882 (St		

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。

		ユーザーアシスタント
**	4	RF69550-F152X388-F
 ● #載 > Hu 単立シントルの使用 > Hu モランシールの使用 > Butoma Convert > Subma Convert > Subma Convert > Butoma Convert > Subma Convert		2014-00142-0 15:324-0000-010-01-0 15-324-0000-010-0 15-324-0000-010-01-0 12-324-000-01-01-0 12-324-000-01-01-0 001-01-01-01-0 001-01-01-01-0 001-01-01-01-0 001-01-01-01-0 001-01-01-01-0 001-01-01-01-0 001-01-01-01-0 001-01-01-01-0 001-01-01-01-0 001-01-01-01-0 001-01-01-0 001-01-01-0 001-01-01-0 001-01-01-0 001-01-0 001-01-0 001-01-0 001-01-0 001-01-0 001-01-0 001-01-0 001-01-0 001-01-0 001-01-0 001-01-0 001-01-0 001-01-0 0 0 0