お客様各位

株式会社日立ソリューションズ Fortinet 製品ユーザサポート

FortiGate で特定サイトへのアクセス不可事象について

拝啓、平素は Fortinet 製品サポートをご利用下さいまして誠にありがとうございます。

現在、FortiGate をご利用のお客様より、特定サイトへのアクセスが不可となる事象が発生している とのご申告を複数頂いています。

詳細は調査中となりますが、お客様におかれましては、当該事象が発生している場合は、下記に示す 「2. 一時的な回避策」実施の検討をお願いいたします。

敬具

記

1. 申告頂いている事象

6/27 より、FortiOS (現状 v6.2 系での発生のみを確認しています)で SSL インスペクション機能を利 用している場合、一部の HTTPS サイトへのアクセスがブロックされる。

2. 一時的な回避策

現在、詳細は調査中で明確な回避策は確認できていませんが、「無効な SSL 証明書を許可」することで 事象が解消された旨の報告を受けています。

事象が発生した場合は、付録記載の手順を参考に「無効な SSL 証明書を許可」し、事象が解消するか ご確認ください。

3. その他

本件の追加でご案内できる情報が確認できましたら、弊社サポートサイトで順次ご案内します。 本事象は現在、FortiOS v6.2 系でのみ確認しています。v6.2 系は 2023/09/28 に EOS(End of

Support:メーカサポート終了)を迎えます。v6.4 系以降の OS を搭載可能な製品をご利用のお客様は v6.4 系以降へのアップグレードも合わせてご検討いただきますようお願いします。

v6.4 系以降のリリース OS 及び、搭載できるモデルについては、以下、弊社サポートサイトをご覧 ください。尚、以下サイトは弊社から製品出荷時に同梱していますアカウントが必要となります。

FortiGate / FortiWiFi / FortiAP リリース OS https://csps.hitachi-solutions.co.jp/fortinet/cer/fortigate/release.html

以上

以下に従い SSL インスペクションプロファイルに「無効な SSL 証明書を許可」を設定します。 尚、以下画像は表示言語を日本語にしている場合の画面例です。表示言語、ご利用の OS バージョン によって画面が異なる場合があります。

(1) 管理 GUI ヘログインします

(2) GUI 表示機能のセキュリティプロファイルが有効であることを確認

左メニューの[システム] – [表示機能設定] を選択し、 [複数セキュリティプロファイル] が有効 になっていることを確認します。

(チェックボックスが入っていない場合はチェックを入れ、有効にします)

FortiGate 50E						д 🖲 🕗 admin 🗝
🚳 ダッシュボード	> 🏦	表示機能設定				
セキュリティファブリ ※ ック	>	③ ポリシーベース IPsec VPN	0		変更 🜖	í í
■ FortiView	\rightarrow	● マルチキャストポリシー	٥			ヹキュリティプロ
• > 7	, v	■ ロードバランス	٥]		
管理者 管理者プロファイル		ワイヤレスオープンセキュリティ	٥]		
ファームウェア	- 1	③ 脅威ウェイトトラッキング	٥	Ĵ		
設定	_	● 差し替えメッセージグループ	٥	Ĵ		
HA SNMP		● 証明書	0	Ĵ		
差し替えメッセージ	- 1	● 複数インターフェースポリシー	٥			
FortiGuard 表示機能設定	☆	● 複数セキュリティプロファイル	٥	j		
証明書		○ 名前なしポリシー許可	۵]		
ポリシー & オブジェク ▶	>					ļ
ヤキュリティブロファ				適用		

(3) 対象のファイアウォールポリシーを開きます

左メニューの[ポリシー&オブジェクト] – [IPv4 ポリシー] を選択し、対象のポリシーを選択、 編集します。

FortiGate 50E									Q + >_	[] @+ 🗘 🖲 🌏 ad	lmin *
	> •	+新	規作成 🥒 編集	會 削除	Q 7	ポリシーのルックア	'ップ 検索			Q	
ホリシー&オフシェク ト	~	イン	ターフェースペアも	21- 2-	ケンス別						
IPv4ポリシー	☆	ID	名前	送信元	宛先	スケジュール	サービス	アクション	NAT	セキュリティプロファイル	
認証ルール	1	ㅁ 쟈	lan → 🔛 wan1 (1)							
アドレス		1	テストポリシー	🗉 all	🔳 all	o always	🖸 ALL	 ACCEPT 	● 有効化済み	wca default	U
インターネット サービ スデータベース										ss. test	
サービス	- JI	0 暗	K 1								
スケジュール											
パーチャルIP											

(4) SSL インスペクションポリシーを変更

[セキュリティプロファイル項]の SSL インスペクション項の"ペン"アイコンをクリックします。

FortiGate 50E		Q + >_ []
システム	Edit Policy	
^{ポリシー&オプジェク} ▶	IPブール設定 発信インターフェースのアドレスを使用 ダイナミックIPブールを使う	ID 1
IPv4ポリシー	☆ 送信元ポートの保持 ③	旱漁の利用
認証ルール	プロトコルオプション 🔤 default 🔹 🖋	4時間前
アドレス	セキュリティプロファイル	最初の利用
インターネットサービ スデータベース	Webフィルタ 🜑 WEB default 🔹 🖋	18時間前
サービス	DNSフィルタ ③ IPS	ヒット数 11,650
スケジュール	SSLインスペクション MyInspection ・	総パイト数 551.63 MB
IPプール	ロギングオブション	
プロトコルオプション	許可トラフィックをログ	
● セキュリティブロファ イル	・ コメント コメント記入 01023	
I VPN	>	■ ビデオチュートリアル ピ
🛔 ユーザ&デバイス	このポリシーを有効化 〇	
■ ログ&レポート	>	
● モニタ	OK =+v>t	2)レ

(5) 無効な SSL 証明書を許可 を有効にします

画面下部[共通オプション]にある「無効な SSL 証明書を許可」にチェックを入れ、OK ボタンを 押します。

FortiGate 50E								۵۵	💽 admin •
🚯 ダッシュボード	> î	Edit Policy	SSL/SSHインスペクションプロファイルの編集		_				×
☆ セキュリティファブリ ※ ック	>		SSLサーバ保護 インスペクション方式 SS証明書のインスペクション フ	ULSSLイン	スペク	ション			•
📥 FortiView	>		CA証明書 Fortinet_CA_SSL	• ± 4	オウンロ	⊐- ŀ			
🖶 ネットワーク	>		ブラックリストされた証明書 🜖 許可 ブロック 🗮 ブラックリス	ストされた	証明書	を表え	7		
• システム	>	セキュリティ	信頼されないSSL証明書 許可 プロック 無視する項目	■ 信頼さ	れるひ	AIJス	トを表	示	- I
ポリシー&オプジェク ▶	~	Webフィル	プロトコルポートマッピング						
IPv4ポリシー	☆		すべてのポートを検査する 🕥						
認証ルール		SSLインスペ	HTTPS C 443						
アドレス			cci イン・フ ペ ケシ・コン・ナプシ・コン・						_
インターネットサービ	- 1	ロギングオン							_
スデータベース	- 1	許可トラフィ	SSHティーフスキャン						
サービス	- 1		共通オプション						
スケジュール			möh+>ccit5的業友推可 ●						_
バーチャルIP		このポリシ-	SSLアノマリのログを記録する 3 ●						
IPプール									I
プロトコルオプション									*
			OK キャンセル	·					

(6) IPv4 ポリシーを閉じる

「(4) SSL インスペクションポリシーを変更」の画面に戻りますので、画面下部の OK ボタンを押 し、ポリシー設定を更新します。

以上で手順は終了ですが、「(4) SSL インスペクションポリシーを変更」の画面で、SSL インスペクシ ョン項が、以下、何れかになっている場合は、デフォルトで定義されている読込専用のプロファイルの 為、「無効な SSL 証明書を許可」を有効にすることが出来ません。

この場合は、後続手順でプロファイルをコピー(クローンを作成)し、コピーしたプロファイルを利用 下さい。

- certificate-inspection
- deep-inspection
- no-inspection

(7) プロファイルのクローン(コピー)を作成

左メニューの[SSL/SSH インスペクション]を選択し、対象のプロファイルを選択し、画面上部の クローンボタンをクリックします。

FortiGate 50E				Q+ >_ [] @+	斗 🕘 admin •
• システム	>	+ 新規作成 ● 編集 ● クロ	ーン 自 削除 検索	Q	
ポリシー&オブジェク		名前≑	リードオンリー 🌣	⇒ オくメロ	参照≑
[□] ト	Ĺ	ss. MyInspection			1
セキュリティブロファ ● ノリ	~ 1	ss. certificate-inspection	₽	Read-only SSL handshake inspection profile.	0
1/2		ss. custom-deep-inspection		Customizable deep inspection profile.	0
Webフィルタ		ss. deep-inspection	₽	Read-only deep inspection profile.	0
DNSフィルタ		ss. no-inspection	•	Read-only profile that does no inspection.	0
 侵入防止 SSL/SSHインスペクション IPS Signatures Webレーティングオー パーライド 	☆	対象のプロファ	イルを選択		_

(8) プロファイルのクローン(コピー)を作成

名前項目に、プロファイルの任意の名前を入力し、OK ボタンを押します。

FortiGate 50E		Q + ≻_ []	0• 40	🔝 admin •
・システム	▲ 新規作成 クローン*certificate-inspection*			×
♪ ポリシー &オプジェク ト	クローンの名前を入力してください: 104 My/inspe			
● セキュリティプロファ ● イル	★ 名前 certificate-inspectionのクローン			
Webフィルタ	OK Cancel			
DNSフイルタ	ss no-inspe			
SSL/SSH-(),7/2/2/2/				
ヨン	★			
IPS Signatures				

(9) プロファイルの割り当て

「(4) SSL インスペクションポリシーを変更」の画面に戻り、プロファイル名を「(8) プロファ イルのクローン(コピー)を作成」で作成したプロファイルに変更します。

その後、「(5) 無効な SSL 証明書を許可 を有効にします」及び「(6) IPv4 ポリシーを閉じる」の 手順を実施します。

FortiGate 50E		Q 🔹 >_ [] 🔞 र 🗘 🛛 admin र
システム	Edit Policy	
^{ポリシー&オプジェク} ▶	。 IPプール設定 発信インターフェースのアドレスを使用 ダイナミックIPプールを使う	ID 1
IPv4ポリシー ⊰	≥ 送信元ポートの保持 ①	豊後の利用
認証ルール	プロトコルオプション 📧 default 🔹 🖋	4時間前
アドレス	セキュリティプロファイル	最初の利用
インターネットサービ スデータベース	Webフィルタ 🜑 wm default 🔹 🌶	Tondial bi
サービス	IPS C Is default	11,650
スケジュール パーチャルIP	SSLインスペクション MyInspection 🔹	総バイト数 551.63 MB
IPブール	ロギングオプション	
プロトコルオプション	許可トラフィックをログ ● セキュリティイベント すべてのセッション	⑦ ドキュメント
■ セキュリティプロファ イル	- コメント コメント記入 erio23	
III VPN		• ビデオチュートリアル ひ
▲ ユーザ&デバイス		
■ ログ&レポート :	· · · · · · · · · · · · · · · · · · ·	
モニタ	ОК <i></i>	セル