

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 Firewall ネットワークプロテクション編



内容

改訂履歴	2
はじめに	3
1. ご利用環境の構成	4
2. ネットワークプロテクションの設定	5
(1)ネットワークプロテクション機能の適用範囲	5
(2)侵入防御(IPS)の設定	5
(3)スプーフ防御を有効にする	9
(4)DoS 防御を有効にする	.10
(5)高度な脅威検知の設定	.11
3. 最後に	. 12

改訂履歴

版数	更新日	更新内容	更新者
1.0	2020/5/1	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. IPS 機能を有効にする
- 2. フラッド防御を有効にする
- 3. DoS 防御を有効にする
- 4. 高度な脅威防御(ATP)の設定

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_firewall_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 firewall fw dnat.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. ネットワークプロテクションの設定

(1) ネットワークプロテクション機能の適用範囲

ネットワークプロテクション機能には以下の機能があります。機能と適用範囲は以下の通りで

す。

機能	説明	適用範囲
侵入防御(IPS)	シグネチャベースの検知機能です。	ファイアウォール
		ポリシー単位
スプーフ防御	IP アドレスのスプーフィング攻撃を防止する機能です。	各ゾーン全体
DoS 防御	ネットワークホストへのフラッド攻撃を防止する機能です。	Sophos Firewall全
		体

(2)侵入防御 (IPS) の設定

①侵入防御 > IPS ポリシー タブをクリックします。

	侵入	、防御	■ 操作ガイド ログビューア へい	ルプ admin ▼ koan keiso
監視 & 分析 Control Center 現在のワクティビティ		DoS 攻撃	IPSポリシー カスタム IPS シグネチャ Dos/スプーフ防衛	1
レホート 診断			Ditak	削除
保護 ルールとハリンー		石前 🔹	說明	管理
侵入防御 Web アプリケーション		DMZ TO LAN	A default IPS policy template to scan the traffic flowing from DMZ to LAN; Primarily intended to secure server(s) hosted in the LAN zone	
ワイヤレス メール		DMZ TO WAN	A default IPS policy template to scan the traffic flowing from DMZ to WAN; Primarily intended to secure the DMZ-based client(s)	<i>M</i> ²
Web サーバー 高度な骨威 Central Synchronization		LAN TO DMZ	A default IPS policy template to scan the traffic flowing from LAN to DMZ; Primarily intended to secure the LAN-based client(s) and DMZ-based server(s)	. Mar
設定 VDN		LAN TO WAN	A default IPS policy template to scan the traffic flowing from LAN to WAN; Primarily intended to secure LAN-based client(s)	
ネットワーク ルーティング		WAN TO DMZ	A default IPS policy template to scan the traffic flowing from WAN to DMZ; Primarily intended to secure server(s) hosted in the DMZ	
認証 システムサービス		WAN TO LAN	A default IPS policy template to scan the traffic flowing from WAN to LAN; Primarily intended to secure server(s) hosted in the LAN	1
システム プロファイル オストとサービス		dmzpolicy	A General policy to scan traffic flowing to DMZ	1
10、11とリーとス 管理 パックアップ&ファームウェア	, 🗆	generalpolicy	A General Policy	A* 1
証明書		lantowan general	A General policy for LAN to WAN Traffic	
		lantowan strict	A Strict policy for LAN to WAN Traffic	× 1

IPS ポリシーはカスタマイズが可能ですが、今回は推奨されている「generalpolicy」を適用する手順を記載します。※手順の中では適用されているポリシールールの確認方法のみ記載します。

②「generalpolicy」をクリックします。

	侵入防御	フィードバック 🖬 操作ガイド ログ	ビューア ヘルプ admin・ Koankeiso
監視&分析 Control Center 現在のアクティビティ	DoS攻擊	IPSポリシー カスダムIPSシグネチャ ロ	loS/スプーフ防御
レホート ゼロデイ対策 診断 ^{保護}	IPS 保護 🚺 IPS を使用するファイアウォ		
ルールとポリシー	シグネチャの更新日時	21.41.58, 4月 14 2022	
ワイヤレス メール Web ttーバー	□ 名前 ▲	影明	追加 削除 管理
web リーハー 高度な防御	DMZ TO LAN	A default IPS policy template to scan the traffic flowing from DMZ to LAN; Primarily intended to secure server(s) host the LAN zone	ied in
設定 VPN	DMZ TO WAN	A default IPS policy template to scan the traffic flowing from DMZ to WAN; Primarily intended to secure the DMZ-bas client(s)	ed 🥒
ネットワーク	LAN TO DMZ	A default IPS policy template to scan the traffic flowing from LAN to DMZ, Primarily intended to secure the LAN-base client(s) and DMZ-based server(s)	d 🇨
認証	LAN TO WAN	A default IPS policy template to scan the traffic flowing from LAN to WAN, Primarily intended to secure LAN-based of	lient(s)
SAFAJ-EA	WAN TO DMZ	A default IPS policy template to scan the traffic flowing from WAN to DMZ, Primarily intended to secure server(s) hos the DMZ	ited in
Sophos Central プロファイル	WAN TO LAN	A default IPS policy template to scan the traffic flowing from WAN to LAN, Primarily intended to secure server(s) hos the LAN	ted in 🖋
ホストとサービス	dmzpolicy	A General policy to scan traffic flowing to DMZ	1
■4 バックアップ&ファームウ ー	generalpolicy	A General Policy	* U
エア	Iantowan_general	A General policy for LAN to WAN Traffic	1
	lantowan strict	A Strict policy for LAN to WAN Traffic	1

③適用されているフィルタが表示されます。今回はデフォルトの「Migrate_def_filter_1」をク リックします。

	侵入防御			■ 操作ガイド ログビューア へ	ルプ admin ▼ koan keiso
監視 & 分析 Control Center 現在のアクティビティ レポート 診断	DoS 攻擊	IPS ポリシー	カスタム IPS シグネチャ	DoS/スプーフ防御	
 # ハールとポリシー 保入的参 Web アプリケーション ワイヤレス メール Web サーバー 満皮な角成 	名前 • 說明	generalpolicy A General Policy 係存 キャンセ	تال		
Central Synchronization 設定 VPN ネットワーク ルーティング 認証 システムサービス	□ 冬前 □ Migrate def filter 1	シグネチャ すべて	シグネチャフィルタの条件 カテゴリ = すべてのカテゴリ 単要国 = すべて重要記 ブラットフォー人を考えてブラットフォーム	<u>追加</u> アクション 推奨	削除 管理 ✔ 面
システム プロファイル ホストとサービス 管理 バックアップ&ファームウェア 証明書			対象 = すべて 対象		

④IPS ポリシールールの編集画面が表示されます。デフォルトの「Migrate_def_filter_1」では 推奨のシグネチャーリストが設定されています。※今回は内容の編集は行いません。

and the second s	侵入防御					■ 操作ガイド	ログビューア ヘルプ adm koan k	nin 🝷 keiso
監視 & 分析 Control Center 現在のアクティビティ	DoS 攻擊		IPS ポリシー		カスタム IPS シグネチャ		DoS/スプーフ防御	
レポート 診断 のま	IPS ポリシールールの編集							
ルールとポリシー 侵入防御 Web	ルール名 * Migrate_def_filter_1							
アプリケーション ワイヤレス メール Web サーバー	(カテゴリ *) (重	要度	▼ 〕 プラットフォーĿ	▲ ▼ 対象	<u>ب</u>	スマートフィルタ	フィルタのクリン	P
高度な脅威 Central Synchronization	 ● すべてを選択 ● 個別のシク ● 金曲 ▽ 	ブネチャを選択 sın ▽	カテゴル	金要座	プラットフォーム	初先	#考⇒カスアクミ,ョ`,	
設定 VPN ネットワーク ルーティング 認証 システムサービス	SERVER-ORACLE Oracle WebLogic Server CVE- 2018-2894 Web Service Config Arbitrary File Upload	1180717040	server-oracle	3 - Moderate	Windows, Linux, Mac,	Client	パケットの切断	Î
システム プロファイル ホストとサービス 管理	APP-DETECT EFS Software Easy File Sharing Web Server vfolder.ghp Stack Buffer Overflow	1170627020	app-detect	2 - Major	Windows	Client	パケットの切断	
 バックアップ&ファームウェア 証明書	BROWSER-CHROME Data race in ExtensionsGuestView	2302984	browser-chrome	1 - Critical	Windows, Linux, Mac	Client	パケットの切断	
	BROWSER-CHROME Google Chrome Blink CVE-2020-6549 Renderer MediaElementEventLis memory corruption atternot	2304641	browser-chrome	2 - Major	Windows, Linux, Unix	Client	パケットの切断	

IPS ポリシールールは「カテゴリ」、「重要度」、「プラットフォーム(OS)」、「対象(Server か Client か)」でフィルタリングが可能です。もし、シグネチャを追加・削除したい場合、条 件をフィルタリング後に選択したシグネチャが適用されます。※推奨としてはデフォルト設定 のご利用を推奨しております。

「保存」はせずに「キャンセル」をクリックします。

⑤ファイアウォール > #Default_Network_Policy をクリックします。

	ル	,—	ル	ر ح	ドリシー			-				▶ 操作ガイ	ドログ	ビューア	ヘルプ	admin 👻 koan keiso
 ・ ・ ・				5	ファイアウォールルール			NATルール				SSL/T	LS インス^	ペクションルー	JL	
レポート 診断		v4)	IPv	8	フィルタの無効化					ファイアウ	ォールル	ールの追加	~	無効		削除
ルールとポリシー	Л	レール	の種;	ā.	送信元ゾーン		宛先ゾーン	/	状態			ルールロ	Add Filt	er 👻 フ	ィルタの	リセット
Web アプリケーション ワイヤレス			#		名前	送信元		宛先	対象		ID	アク ショ ン	機能とサー	ービス		
メール Web サーバー 高度な脅威	Ξ		5	<	DNAT Advanced RDT in 7.22 KB, OUT 10 53 KB	すべての のホスト	ゾーン, すべて	LAN, #Port1	Adva	nceRDT	#6	許可する	IPS /	V (WEB ABB Q UnkedNAT) P	os (HB) RX Illog	⊡
Central Synchronization			6	â	waf_rule in 0 B, OUT 0 B	すべての のホスト	ゾーン, すべて	#Port1	web: eng.	server.koan- be	#7	中継				⊡
VPN ネットワーク ルーティング	Ξ	9	Ð	2	Traffic to Interna in 0 B, OUT 0 B	To LAN, W would be	/iFi, VPN, DMZ. added to this g	Firewall rules with the group on the first mate	destination h basis if t	on zone as LAN, V user selects auto	ViFi, VPN, matic gro	DMZ uping				1
NGAIL システムサービス	=			1	Traffic to WAN in 0 B, OUT 0 B	Outbound this group	l traffic to WAN o on the first m	I. Firewall rules with th atch basis if user sele	ne destinat cts autom	ion zone as WAN atic grouping opt	I would be tion. This i	added to is the d				/
^{システム} プロファイル ホストとサービス 管理	=		E	1	Traffic to DMZ in 0 B, OUT 0 B	Inbound t this group	raffic to DMZ. I o on the first m	Firewall rules with the atch basis if user sele	destinatio cts autom	n zone as DMZ w atic grouping opt	ould be a tion. This i	dded to is the de				/
ら <u>ユ</u> バックアップ&ファームウェア 証明書	=		11	<	Auto added firewal in 0 B, OUT 118 KB	すべての のホスト	ゾーン, すべて	すべてのゾーン, すべ のホスト	SMT	P, SMTP(S), PS_465	#1	許可する	IPS A	V WEB APP Q LinkedNAT PI		⊡
	=	ſ	12	<	#Default Network P in 0 B, OUT 0 B	LAN, すべ	てのホスト	WAN, すべての木スト	トすべ	てのサービス	#5	許可する	IPS A	V WEB APP Q LinkedNAT P	OS HB RX LOG	⊖

⑥その他のセキュリティ機能 > エクスプロイトの検出・防止 (IPS) > generalpolicy を 選択し保存をクリックします。

	ファイアウォールルールの編集	耒	■ 操作ガイド ログビューア ヘルプ admin マ koan keiso
■満葉 も分析 Control Carter 現在のカクライビティ レポート 参数 レールとれりシー 会入わ时 Web アプリケーション フイヤレス メール.	 Web フィルタリング Webポリシー なし Webカテゴリペースのトラフィックシェービング の適用 QUIC プロトコルのプロック ▲ 	マルウェアスキャンとコンテンツスキャン ✓ HTTP および復号化した HTTPS をスキャン Sandstorm でゼロディ脅威を検出 ✓ FTP のマルウェアをスキャン	 一般的な Web ボートをフィルタリング DPI エンジンではなく Web プロキシを使用する OPI エンジンまたは Web プロキシの選択 Web プロキシでのフィルタリング中に HTTPS を 選号化する
Web サーバー 高度な脅威 Central Synchronization 設定	▶ Synchronized Security ハートピートの設定		
SEE VPN Aットワーク ルーティング 認証 システムサービス フロファイル プロファイル ポストとサービス 管理 パックアップをファームウェア 証明書	その他のセキュリティ機能 アブリケーションの特定・新御(アブリケーションコン トロール) なし アブリクーションペースのトラフィックシェーピ ングポリシーや適用 エクスプロイトの検出・防止(PS) 【generalpolicy	トラフィックシェービング なし なし 	DSCP マーキング DSCP マーキングの選択
	保存 キャンセル		

以上で設定は完了です。#Default_Network_Policy を通過するトラフィックに対し、IPS ポリ シー「generalpolicy」が有効になります。

(3) スプーフ防御を有効にする

①侵入防御 > DoS/スプーフ防御 タブをクリックします。

	侵入防御			■ 操作ガイド ログビューア ヘルプ admin ▼ koan keiso
 監視 & 分析 Control Center 現在のアクティビティ レポート 診断 	DoS 攻撃 フプ つれない 今 405-50 r字	IPSポリシー	カスタム IPS シグネチャ	DoS/スプーフ防御
代達 日、1 とが115 日 日 日 マゴリケーション ワイヤレス メール	 スプーフ防御の有効化 信頼する MAC で不明な IP を制限 MAC フィルタを有効にするには、「信! 	積する MAC」リストに MAC エントリを少な	くとも1つ追加してください	
Web サーバー 高度な脅威 Central Synchronization		IPスプーフィング	MAC フィルタ	IP-MAC ペアフィルタ
设定	LAN			
VPN ネットワーク	WAN			
ルーディンク 認証 システムサービス	DMZ			
システム プロファイル ポストとサービス 管理 パックアップ&ファームウェア 証明書	WiFi 波 用			

②今回は IP スプーフィングを有効にします。スプーフ防御の有効化をクリックします。 また防御対象とする、ゾーンを選択し適用をクリックします。今回は LAN ゾーンで有効にし

=	7	
ъ	9	0

	侵入防御			■ 操作方イド ログビューア ヘルプ admin マ koan keiso
監視 & 分析 Control Center 現在のアクティビティ レポート	DoS 攻撃	IPS ポリシー	カスタム IPS シグネチャ	DoS/スプーフ的例
 	スプーフ防御 - 全般設定 マスプーフ防御の有効化 ・ 信頼する MAC で不明な IP をみぼ MAC フィルタを有効にするには、 「信 LAN WAN DH2 WFI 	■ a MACJ リストに MAC エントリを少なく IP スプーフィング ■	とも1つ追加してください MACフィルタ	IP-MACペアフィルタ

以上で設定は完了です。パケットの送信元 IP アドレスがファイアウォールのルーティングテ ーブルのいずれのエントリとも一致しなかった場合や、パケットが直接サブネットから送信され たものでない場合は、パケットを破棄します。※より厳密に管理する場合、MAC アドレスを IP アドレスと紐づけて管理することも可能です。

(4) DoS 防御を有効にする

①侵入防御 > DoS/スプーフ防御 タブをクリックします。

	侵入防御			■ 操作ガイド ログビューア ヘルプ admin ▼ koan keiso
 監視&分析 Control Center 現在のアクティピティ レポート 診断 	DoS 攻撃 スプーフ防御 - 全船設定	IPSポリシー	カスタム IPS シグネチャ	DoS/スプーフ防衛
登進 日、日、レガリン 日本 マブリケーション ワイヤレス メール	 スノーフ防御の有効化 信頼する MAC で不明な IP を制 MAC フィルタを有効にするには、 	限 「信頼する MAC」リストに MACエント!	」を少なくとも1つ遺加してください	
Web サーパー 高度な育威 Central Synchronization	LAN	IP スプーフィング	MAC フィルタ	IP-MAC ペアフィルタ
設定 VPN ネットワーク	WAN			
ルーティング 認証 システムサービス	DMZ			
システム プロファイル ホストとサービス 管理 バックアップ&ファームウェア 証明書	WIFI			

②DoSの設定セクションで適用フラグをチェックし適用をクリックします。

nter ティビティ	DoS 攻擊	IP	3ポリシー		カスタム	IPS シグネチャ		DoS/スプ	ーフ防御
Dos	の設定								
リシー ション :	攻撃の維強	送信元 パケットレート: 送信元 [パケット/分]	バーストレート 送信元 [パケット/秒]	適用 フラグ	送信元 トラフィック 破棄	宛先 パケットレート: 宛先 [パケット/分]	バーストレート 宛先 [バケット/秽]	適用 フラグ	宛先 トラフィ ツ破 菜
chronization	SYN フラッド	12000	100		0	12000	100		116
'n	UDP フラッド	12000	100		0	18000	100		0
<i>7</i>	TCPフラッド	12000	100		69391	12000	100		3962
-ビス	ICMP/ICMPv6 フラッド	120	100		0	300	100		0
ル ービス	送信元ルートが指定された破棄パケット	-	-						-
プ&ファームウェア	ICMP/ICMPv6 リダイレクトパケットの無効化	-	-				-		-
	ARP ハードニング								

以上で設定は完了です。今回は SYN フラッド、UDP フラッド、TCP フラッド、ICMP/ICMPv6 フラッドを、送信元、宛先それぞれに対しデフォルトのレートで設定しました。このレートを超 えるパケットを破棄します。

(5) 高度な脅威検知の設定

①高度な脅威 > ATP (Advanced Threat Protection) タブをクリックします。

	高度な脅威		■ 操作ガイド ログビューア ヘルプ admin - koan keiso
協規 8.分析 Control Center 現在のアクティビティ レポート 参断	ATP (Avanced Threat Protection) 全般設定	脅威インテリジェンス	Sandatorm වඩාදී
Rial ルールとポリシー 受入防算 Web アプリケーション ワイヤレス メール	Advance: Threat Protection の有効化 プリシー * ネットワーク / ホスト 例外	D ログしてドロップ マ	
Web ワーハー 高速の負担 VPN ネットワーク ルーディング 超圧 システムサービス 	脅威の例外	新規項目の追加 負責 / 追加	
^{以ステム} プロファイル ホストとサービス 管理 バックアップ&ファームウェア 託明書	セキュリティの詳細設定	いないコンテンツのみを検査してください。 ・テンツと信頼されていないコンテンツの両方を検査してく	ださい。

②Advanced Threat Protection のトグルスイッチを ON、ポリシーを「ログしてドロップ」

に設定し適用をクリックします。

1110 0	高度な脅威		■ 操作ガイド ログビューア ヘルレプ admin ▼ koan keiso
監視 & 分析 Control Center 現在のアクティピティ レポート 診断	ATP (Avanced Threat Protection) 全般設定	育成インテリジェンス	Sandstorm の設定
保護 ルールとポリシー 会入防御	Advanced Threat Protection の有効化 ので		
web アプリケーション	ログ有効	<u>ログ設定の変更</u>	
ワイヤレス メール	ホリシー*	ブレてドロップ 🗸	
Web サーバー 高度な育威	ネットワーク / ホスト 例外		
Central Synchronization 意定 VPN ネットワーク ルーティング 総証 ジステムサービス システム プロファイル	育成の例外 検3	新規項目の追加 発/逾加	
ハストとリーヒス 管理 パックアップをファームウェア	セキュリティの詳細設定		
バックアップ&ファームウェア 証明書	 ● 信頼されていない、シテンツを検査 パフォーマンスを高速化するには、信頼されていな ● すべてのコン・プンツを検査 セキュリティを支付のるには、信頼されているコンテ 注用 	いコンテンツのみを検査してください。 ンツと信頼されていないコンテンツの両方を検査してください	h _e

以上で設定は完了です。高度な脅威防御(Advanced Threat Protection)の機能は、内部から不正な通信を検出します。例えば、何らかの理由でマルウェアに感染してボット化したサーバが内部にあり、外部の C&C サーバ(ボット化したコンピュータ群へ指令を送り攻撃制御の中心

となるサーバ)へ接続を行おうとした場合に、ボット化したサーバからの通信を遮断してくれます。

3. 最後に

本手順書では、ネットワークプロテクションの設定について記載しました。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。

	Corner D	-			■ 操作ガイド ログビ	ミューア へルプ admin ▼
監視 & 分析	システム		Traffic Insight		ユーザーとデバイスの詳細	B
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	1777-722		30 24 18 12	itti 0 Apps ≓ 0 B In	0 0 0 0 リスクあ 不明 置告 接続満 り	ði
診断	インターフェース	VPN	6 0 5分母にヒット	# 0 B Out 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 0 0 ### 9%88829 @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。

ソフォスファイアウォール ☆				
管理者ヘルプ ユーザーボータル	ヘルレブ 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			
	 入門 ソフォスファ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、ソフォスファ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示えたおよび検証する方法、そして最後に、快適に感じたら稼働する方法を学びます。 ソフオスファイアウオールへの安全な管理者アクセス 1. 複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。 2. サインインセキュリティを構成します。 ギロンインセキュリティを構成します。 第日者セッションからサインアウトする:管理者の非アクティブ期間を指定します。 ブルートフォースサインイン攻撃の防止:同じPアドレスからの時間枠内でのサインインの失敗回数を指定します。ブロックされたアクセスの期間を指定します。 オロノクセスなど、すべての推奨事項をデフォルト段定として指定しました。 管理者アカウントのデフォルトのパスワードを使用する場合、次の制限が適用されます。 1. LANおよびWANゾーンでセキュアコピープロトコル (SCP)を使用することはできません。 2. LANゾーンからSSH経由でサインインすると、パスワードを変更するためのプロンプトが表示されます。すでにウィザードを実行している場合は、パスワードの変更メニューが表示されます。 			
システムサービス > ソフォソセントラル > プロファイル > ホストとサービス > 管理 >	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