さくらのクラウド
Sophos UTM設定代行サービス　設定値説明
（サイト間VPN）

最終更新：2018年7月26日

お客様入力項目

No	提供サービス	作業完了条件	No	設定箇所（大項目）	設定箇所（詳細）	入力値	条件
1	サイト間VPN SSL ※SophosUTM同士の接続	・ヒアリング項目及びデフォルト項目が手順書通りに設定されていること。	1-1		WebAdminのURL	IPもしくはURL	Server拠点とClient拠点の2拠点分の情報が必要
			1-2		WebAdminのアカウントとパスワード	アカウントとパスワード	Server拠点とClient拠点の2拠点分の情報が必要
			1-3	サイト間VPN > SSL >コネクションタブ	ローカルネットワーク	ネットワークアドレス	Server拠点のInternalネットワーク（プライベートセグメント）であること
			1-4		リモートネットワーク	ネットワークアドレス	Client拠点のInternalネットワーク（プライベートセグメント）であること
			1-5	サイト間VPN > SSL >コネクションタブ	コネクションタイプ	サーバ	
			1-6		コネクション名	Externalアドレス	
			1-7		自動ファイアウォールルール	ON	
			1-8	サイト間VPN > SSL >設定タブ	インタフェースアドレス	すべて	
			1-9		プロトコル	TCP	
			1-10		ポート	60443	※デフォルト443では多くのサービスと重複する可能性があるため
			1-11		ホスト名を上書き	Externalアドレス	リモートアクセスユーザが到達可能であること
			1-12		プールネットワーク	VPNプール（SSL）10.242.2.0/24	
			1-13		Duplicate（重複）CN	ON	
			1-14	リモートアクセス > SSL > 詳細タブ	暗号化アルゴリズム	AES-128-CBC	
			1-15		認証アルゴリズム	SHA1	
			1-16		鍵サイズ	2048ビット	
			1-17		サーバ証明書	Local X509 Cert	
			1-18		鍵ライフタイム	28800	
			1-19		圧縮設定	ON	
			1-20		デバックモード	ON	
			1-21	サイト間VPN > SSL >コネクションタブ	コネクションタイプ	クライアント	
			1-22		設定ファイル	サーバ側で作成した.apcファイル	
			1-23		自動ファイアウォールルール	ON	

お客様入力項目

No	提供サービス	作業完了条件	No	設定箇所（大項目）	設定箇所（詳細）	入力値	条件
2	サイト間VPN　IPsec ※Sophosと他ベンダー製品との接続時に推奨	・ヒアリング項目及びデフォルト項目が手順書通りに設定されていること。	2-1		WebAdminのURL	IPもしくはURL	
			2-2		WebAdminのアカウントとパスワード	アカウントとパスワード	
			2-3	サイト間VPN > Ipsec >リモートゲートウェイタブ	ゲートウェイ	接続先グローバルIP	対向拠点のExternalアドレスであること
			2-4		VPN IDタイプ	Sophos、Cisco、YAMAHAはIPアドレス Juniperはホスト名	
			2-5		VPN IDタイプ（オプション）	Sophos:不要 RTX１２００：リモートローカル（RTX1200のLAN側）のIPアドレス Cisco：不要 Juniper：ホスト名	
			2-6		リモートネットワーク	ネットワークアドレス	対向拠点のInternalネットワーク（プライベートセグメント）であること
			2-7	サイト間VPN > Ipsec >　コネクションタブ	ローカルネットワーク	ネットワークアドレス	設定対象UTMのInternaolネットワーク（プライベートセグメント）であること
			2-8	サイト間VPN > Ipsec >リモートゲートウェイタブ	名前	ゲートウェイで設定するIPアドレス	
			2-9		ゲートウェイタイプ	イニシエートを行う	
			2-10		認証タイプ	事前共有鍵	
			2-11		キー	英数大小文字8文字	
			2-12	サイト間VPN > Ipsec >　ポリシータブ	名前	ゲートウェイで設定するIPアドレス	
			2-13		IKE暗号化アルゴリズム	AES-256	RTX1200:AES-256 Cisco:AES-256 Juniper:3DES
			2-14		KE認証アルゴリズム	SHA2-256	RTX1200:SHA2-256 Cisco:SHA2-256 Juniper:SHA1
			2-15		IKE SAライフタイム	28800	RTX1200:28800 Cisco:86400 Juniper:28800
			2-16		IKE DHグループ	5：MODP 1536	RTX1200:グループ14：MODP 2048 Cisco:グループ5：MODP 1536 Juniper:グループ2：MODP 1024
			2-17		IPsec暗号化アルゴリズム	AES-256	RTX1200:AES-256 Cisco:AES-256 Juniper:AES-128
			2-18		IPsec認証アルゴリズム	SHA2-256	RTX1200:SHA2-256 Cisco:SHA2-256 Juniper:SHA1
			2-19		IPsec SAライフタイム	28800	RTX1200:28800 Cisco:86400 Juniper:3600
			2-20		IPsecDHグループ	5：MODP 1536	RTX1200:グループ14：MODP 2048 Cisco:グループ5：MODP 1536 Juniper:グループ2：MODP 1024
			2-21		厳密ポリシー	設定なし	
			2-22		圧縮	設定なし	
			2-23	サイト間VPN > Ipsec >　コネクションタブ	名前	接続先グローバルIP	
			2-24		リモートゲートウェイ	PN > IPsec > リモートゲートウェイタブで設定したもの	
			2-25		ローカルインタフェース	Externalインターフェース	
			2-26		ポリシ	イト間VPN > IPsec > ポリシタブで定義したもの	
			2-27		自動ファイアウォールルール	ON	