付録A　相互接続に関わる仕様

試験をはじめるに先立って各製品の設定可能なパラメータや基本的な機能の使用について調査を行なった。それぞれの製品ごとにベンダーから提出されたデータを収集した。

パラメータ確認シート

2000/12/14

記入者会社名： ネットワンシステムズ株式会社
記入者：太田
記入日付： 2001年3月29日
製品名： ContivityVPNSwitch
製造メーカ：NortelNetworks
Version： v02_61.05

1. 製品について

1) 製品形態	
- ハードウェア製品の場合は各シリーズの型番とサポートIF	型番：Contivity1510、Contivity2600、Contivity4500 IF：Ethernet (10M/100M 自動認識) × 2
- ソフトウェア製品の場合は、サポートするプラットフォーム	
2) 製品定価	￥1，980，000－～

2. 鍵管理について

1) サポートしている鍵交換手法	IKE
2) IKEパラメータについて	
①Phase 1パラメータ	
ⅰ) サポートしているモード	Main mode、Aggressive mode (受けのみ)
ⅱ) 相互認証方式	Pre-Shared Key、電子署名
- 電子署名の場合の対応CA局	Entrust (Ready)、Verisign
ⅲ) 暗号アルゴリズム	DES
ⅳ) 認証アルゴリズム	MD5、SHA-1
ⅴ) DHグループ	Group-1
ⅵ) 有効期間	
ｱ)Life Type (Time)	(サポート)
ｲ) Life Duration (Time)	0(無し)～86399s
ｳ) Life Type (KB)	--
ｴ) Life Duration (KB)	--
ⅶ) IDペイロード	送信：ID_IPV4_ADDR, 受信：ID_IPV4_ADDR,
②Phase2 パラメータについて	
ⅰ) サポートしているTransform	ESP, AH
ⅱ) 暗号アルゴリズム	DES、3DES(128bit)
ⅲ) 認証アルゴリズム	HMAC-MD5, HMAC-SHA1
ⅳ) DHグループ	Group-1
ⅴ) 有効期間	
ｱ)Life Type (Time)	(サポート)
ｲ) Life Duration (Time)	0(無し)～86399s
ｳ) Life Type (KB)	(サポート)
ｴ) Life Duration (KB)	1kb～4,294,967,295kb
ⅵ) IDペイロード	ID_IPV4_ADDR, ID_IPV4_SUBNET
③PFSについて	
ⅰ) PFSのサポート	(サポート)
ⅱ) PFSのON/OFFの可否	可

3. 運用管理について

①設定方法について	
ⅰ) 設定方法	Webベース管理ツールより
ⅱ) リモートからの設定変更の可否	可
- 可能な場合は、どの様に行うか？	Webベース管理ツールより
②運用管理について	
ⅰ) SAの状況確認の可否	可
- 可能な場合は、どの様に行うか？	Webベース管理ツールより
ⅱ) SAの削除の可否	可
- 可能な場合は、どの様に行うか？	Webベース管理ツールより
ⅲ) 相手毎のSA削除の可否	可
- 可能な場合は、どの様に行うか？	Webベース管理ツールより
ⅳ) SA削除のリモート操作の可否	可
- 可能な場合は、どの様に行うか？	Webベース管理ツールより
③LOGについて	
ⅰ) IKEのネゴシエーションがLOGに残るか？	残る
- 可能な場合は、LOGの確認方法	Webベース管理ツールより
ⅱ) LOGの保存期間	特に無し (コマンドによるLOGの切替えまで保存されている。)
ⅲ) LOGのExport機能の可否	可
- 可能な場合は、どの形式で可能か？	SYSLOG
④その他	
ⅰ) Decrypt Keyを確認する事は可能か？	不可

パラメータ確認シート

2000/12/14

記入者会社名： 株式会社ディアイティ
記入者：関
記入日付： 2000年12月18日
PERMIT/Gate
製造メーカ：Alcatel
Version： 3.10.010

1. 製品について

1) 製品形態	ハードウェア
- ハードウェア製品の場合は各シリーズの型番とサポートIF	1520,2520,4620(10BaseT)　7520(100Base/TX)
- ソフトウェア製品の場合は、サポートするプラットフォーム	
2) 製品定価	

2. 鍵管理について

1) サポートしている鍵交換手法	IKE
2) IKEパラメータについて	
①Phase 1パラメータ	
ⅰ) サポートしているモード	Main Mode, Aggressive Mode
ⅱ) 相互認証方式	Pre-Shared, 電子署名
- 電子署名の場合の対応CA局	Entrust (Ready), SSH, Baltimore等のPKCS#10発行要求, PKCS#7署名済みファイル発行可能なCA
ⅲ) 暗号アルゴリズム	DES,3DES,CAST,RC5,Blowfish,IDEA(optional)
ⅳ) 認証アルゴリズム	MD5,SHA-1
ⅴ) DHグループ	1,2,5
ⅵ) 有効期間	
ｱ)Life Type (Time)	サポート
ｲ) Life Duration (Time)	5minから252,600min(365days)
ｳ) Life Type (KB)	サポート
ｴ) Life Duration (KB)	300kbyteから1,073,741,824kbytes(1Tbytes)
ⅶ) IDペイロード	ID_IPV4_ADD, ID_IPV4_SUBNET, ID_IPV4_RANGE
②Phase2 パラメータについて	
ⅰ) サポートしているTransform	ESP,AH
ⅱ) 暗号アルゴリズム	DES,3DES,CAST,Blowfish,IDEA(optional)
ⅲ) 認証アルゴリズム	MD5,SHA-1
ⅳ) DHグループ	1,2,5
ⅴ) 有効期間	
ｱ)Life Type (Time)	サポート
ｲ) Life Duration (Time)	5minから252,600min(365days)
ｳ) Life Type (KB)	サポート
ｴ) Life Duration (KB)	300kbyteから1,073,741,824kbytes(1Tbytes)
ⅵ) IDペイロード	ID_IPV4_ADD, ID_IPV4_SUBNET, ID_IPV4_RANGE
③PFSについて	
ⅰ) PFSのサポート	サポート
ⅱ) PFSのON/OFFの可否	可

3. 運用管理について

①設定方法について	
ⅰ) 設定方法	専用ツール(管理用ソフトウェア)
ⅱ) リモートからの設定変更の可否	可
- 可能な場合は、どの様に行うか？	専用ツールで行う。
②運用管理について	
ⅰ) SAの状況確認の可否	可
- 可能な場合は、どの様に行うか？	専用ツールおよびシリアルコンソール
ⅱ) SAの削除の可否	可
- 可能な場合は、どの様に行うか？	専用ツールおよびシリアルコンソール
ⅲ) 相手毎のSA削除の可否	不可
- 可能な場合は、どの様に行うか？	
ⅳ) SA削除のリモート操作の可否	可
- 可能な場合は、どの様に行うか？	専用ツールおよびシリアルコンソール
③LOGについて	
ⅰ) IKEのネゴシエーションがLOGに残るか？	残る
- 可能な場合は、LOGの確認方法	専用ツールおよびシリアルコンソールからの閲覧
ⅱ) LOGの保存期間	特に無し (消去コマンドを実行しなければ300行)
ⅲ) LOGのExport機能の可否	可
- 可能な場合は、どの形式で可能か？	syslogまたはテキストファイル
④その他	
ⅰ) Decrypt Keyを確認する事は可能か？	不可

パラメータ確認シート

2000/12/14

記入者会社名： 新日鉄情報通信システム(株)
記入者：松島
記入日付： 2000/12/15
製品名： VPN-1
製造メーカ： Checkpoint社
Version： v4.1 sp2

1. 製品について

1) 製品形態	ソフトウェア
- ハードウェア製品の場合は各シリーズの型番とサポートIF	
- ソフトウェア製品の場合は、サポートするプラットフォーム	Solaris v2.6, Solaris7, RedHat Linux6.1, RedHat Linux6.2, WinNT v4.1
2) 製品定価	\500,000～

2. 鍵管理について

1) サポートしている鍵交換手法	IKE, SKIP, ManualIPSEC
2) IKEパラメータについて	
①Phase 1パラメータ	
ⅰ) サポートしているモード	Main Mode, Aggressive Mode
ⅱ) 相互認証方式	Pre-Shared, 電子署名
- 電子署名の場合の対応CA局	Entrust (Ready), SSH, Baltimore等のPKCS#10発行要求, PKCS#7署名済みファイル発行可能なCA
ⅲ) 暗号アルゴリズム	DES, 3DES
ⅳ) 認証アルゴリズム	MD5, SHA-1
ⅴ) DHグループ	Group-1, Group-2
ⅵ) 有効期間	
ｱ)Life Type (Time)	サポート
ｲ) Life Duration (Time)	5min ～ 365日
ｳ) Life Type (KB)	---
ｴ) Life Duration (KB)	---
ⅶ) IDペイロード	送信 ID_IPV4_ADDR, 受信 ID_IPV4_ADDR,
②Phase2 パラメータについて	
ⅰ) サポートしているTransform	ESP, AH
ⅱ) 暗号アルゴリズム	DES, 3DES
ⅲ) 認証アルゴリズム	HMAC-MD5, HMAC-SHA1
ⅳ) DHグループ	Group-1, Group-2
ⅴ) 有効期間	
ｱ)Life Type (Time)	サポート
ｲ) Life Duration (Time)	2min ～ 24h
ｳ) Life Type (KB)	---
ｴ) Life Duration (KB)	---
ⅵ) IDペイロード	ID_IPV4_ADDR, ID_IPV4_SUBNET
③PFSについて	
ⅰ) PFSのサポート	サポート
ⅱ) PFSのON/OFFの可否	可

3. 運用管理について

①設定方法について	
ⅰ) 設定方法	専用ツール
ⅱ) リモートからの設定変更の可否	可
- 可能な場合は、どの様に行うか？	専用ツールで行う。
②運用管理について	
ⅰ) SAの状況確認の可否	可
- 可能な場合は、どの様に行うか？	VPN-1がインストールされているマシン上でコマンド実行
ⅱ) SAの削除の可否	可
- 可能な場合は、どの様に行うか？	VPN-1がインストールされているマシン上でコマンド実行
ⅲ) 相手毎のSA削除の可否	可
- 可能な場合は、どの様に行うか？	VPN-1がインストールされているマシン上でコマンド実行
ⅳ) SA削除のリモート操作の可否	可
- 可能な場合は、どの様に行うか？	VPN-1がインストールされているマシンにLOGONした上でコマンド実行
③LOGについて	
ⅰ) IKEのネゴシエーションがLOGに残るか？	残る
- 可能な場合は、LOGの確認方法	専用ツールでLOGを確認
ⅱ) LOGの保存期間	特に無し (コマンドによるLOGの切替えまで保存されている。)
ⅲ) LOGのExport機能の可否	可
- 可能な場合は、どの形式で可能か？	テキストファイル
④その他	
ⅰ) Decrypt Keyを確認する事は可能か？	可

パラメータ確認シート

2000/12/19

記入者会社名： (株)ネットマークス
記入者：荻野
記入日付： 2000/12/19
製品名： Nokia IP シリーズ
製造メーカ： Nokia社
Version： v4.1 sp2

1. 製品について

1) 製品形態	組込一体型（ハードウェア、ソフトウェア）
- ﾊｰﾄﾞｳｪｱ製品の場合は各ｼﾘｰｽﾞの型番とｻﾎﾟｰﾄIF	Nokia IP330 , Nokia IP440 , Nokia IP650, (Ethernet , Fast Ethernet)
- ｿﾌﾄｳｪｱ製品の場合は、ｻﾎﾟｰﾄするﾌﾟﾗｯﾄﾌｫｰﾑ	IPSO-3.2.1-fcs1
2) 製品定価	\1,300,000～

2. 鍵管理について

1) サポートしている鍵交換手法	IKE, SKIP, ManualIPSEC
2) IKEパラメータについて	
①Phase 1パラメータ	
ⅰ) サポートしているモード	Main Mode, Aggressive Mode
ⅱ) 相互認証方式	Pre-Shared, 電子署名
- 電子署名の場合の対応CA局	Entrust (Ready), SSH, Baltimore等のPKCS#10発行要求, PKCS#7署名済みファイル発行可能なCA
ⅲ) 暗号アルゴリズム	DES, 3DES
ⅳ) 認証アルゴリズム	MD5, SHA-1
ⅴ) DHグループ	Group-1, Group-2
ⅵ) 有効期間	
ｱ)Life Type (Time)	サポート
ｲ) Life Duration (Time)	5min ～ 365日
ｳ) Life Type (KB)	---
ｴ) Life Duration (KB)	---
ⅶ) IDペイロード	送信 :ID_IPV4_ADDR, 受信 :ID_IPV4_ADDR,
②Phase2 パラメータについて	
ⅰ) サポートしているTransform	ESP, AH
ⅱ) 暗号アルゴリズム	DES, 3DES
ⅲ) 認証アルゴリズム	HMAC-MD5, HMAC-SHA1
ⅳ) DHグループ	Group-1, Group-2
ⅴ) 有効期間	
ｱ)Life Type (Time)	サポート
ｲ) Life Duration (Time)	2min ～ 24h
ｳ) Life Type (KB)	---
ｴ) Life Duration (KB)	---
ⅵ) IDペイロード	ID_IPV4_ADDR, ID_IPV4_SUBNET
③PFSについて	
ⅰ) PFSのサポート	サポート
ⅱ) PFSのON/OFFの可否	可

3. 運用管理について

①設定方法について	
ⅰ) 設定方法	専用ツール
ⅱ) リモートからの設定変更の可否	可
- 可能な場合は、どの様に行うか？	専用ツールで行う。
②運用管理について	
ⅰ) SAの状況確認の可否	可
- 可能な場合は、どの様に行うか？	VPN-1がインストールされているマシン上でコマンド実行
ⅱ) SAの削除の可否	可
- 可能な場合は、どの様に行うか？	VPN-1がインストールされているマシン上でコマンド実行
ⅲ) 相手毎のSA削除の可否	可
- 可能な場合は、どの様に行うか？	VPN-1がインストールされているマシン上でコマンド実行
ⅳ) SA削除のリモート操作の可否	可
- 可能な場合は、どの様に行うか？	VPN-1がインストールされているマシンにLOGONした上でコマンド実行
③LOGについて	
ⅰ) IKEのネゴシエーションがLOGに残るか？	残る
- 可能な場合は、LOGの確認方法	専用ツールでLOGを確認
ⅱ) LOGの保存期間	特に無し (コマンドによるLOGの切替えまで保存されている。)
ⅲ) LOGのExport機能の可否	可
- 可能な場合は、どの形式で可能か？	テキストファイル
④その他	
ⅰ) Decrypt Keyを確認する事は可能か？	可

パラメータ確認シート

2000/12/14

記入者会社名： アライドテレシス株式会社
記入者：藁谷　哲也
記入日付： 2001/3/7
製品名： CentreCOM AR720 + AR010
製造メーカ：Allied Telesis
Version： 2.0.2.pl1

1. 製品について

1) 製品形態	
- ﾊｰﾄﾞｳｪｱ製品の場合は各ｼﾘｰｽﾞの型番とｻﾎﾟｰﾄIF	AR720: (10/100_Port1) , (AsyncPort) AR020(PRI_Port)　2)AR021(BRI_Port) 3)AR022(10BT_Port) 4)AR023(SYNC_Port)
- ｿﾌﾄｳｪｱ製品の場合は、ｻﾎﾟｰﾄするﾌﾟﾗｯﾄﾌｫｰﾑ	N/A
2) 製品定価	\306,000～

2. 鍵管理について

1) サポートしている鍵交換手法	IKE, ManualIPSEC
2) IKEパラメータについて	
①Phase 1パラメータ	
ｉ) サポートしているモード	Main Mode, Aggressive Mode
ii) 相互認証方式	Pre-Shared
- 電子署名の場合の対応CA局	なし
iii) 暗号アルゴリズム	DES
iv) 認証アルゴリズム	MD5, SHA-1
ｖ) DHグループ	Group-1, Group-2
vi) 有効期間	
ｱ)Life Type (Time)	サポート
ｲ) Life Duration (Time)	600～3144960秒（デフォルト:86400秒）
ｳ) Life Type (KB)	サポート
ｴ) Life Duration (KB)	1～1000KB(デフォルト:1000KB)
vii) IDペイロード	送信：ID_IPV4_ADDR, 受信：ID_IPV4_ADDR,
②Phase2 パラメータについて	
ｉ) サポートしているTransform	ESP, AH
ii) 暗号アルゴリズム	DES
iii) 認証アルゴリズム	HMAC-MD5, HMAC-SHA1
iv) DHグループ	Group-1, Group-2
ｖ) 有効期間	
ｱ)Life Type (Time)	サポート
ｲ) Life Duration (Time)	600～3144960秒（デフォルト:28800秒）
ｳ) Life Type (KB)	サポート
ｴ) Life Duration (KB)	1～2000000000KB(デフォルト:有効期間なし)
vi) IDペイロード	ID_IPV4_ADDR, ID_IPV4_SUBNET
③PFSについて	
ｉ) PFSのサポート	サポート
ii) PFSのON/OFFの可否	可

3. 運用管理について

①設定方法について	
ｉ) 設定方法	コマンド入力、TextEDIT機能付き
ii) リモートからの設定変更の可否	可
- 可能な場合は、どの様に行うか？	TELNET or SSH
②運用管理について	
ｉ) SAの状況確認の可否	可
- 可能な場合は、どの様に行うか？	ConsoleまたはTelnet/SSHにてコマンド実行
ii) SAの削除の可否	可
- 可能な場合は、どの様に行うか？	ConsoleまたはTelnet/SSHにてコマンド実行
iii) 相手毎のSA削除の可否	否
- 可能な場合は、どの様に行うか？	
iv) SA削除のリモート操作の可否	可
- 可能な場合は、どの様に行うか？	ConsoleまたはTelnet/SSHにてコマンド実行
③LOGについて	
ｉ) IKEのネゴシエーションがLOGに残るか？	残る
- 可能な場合は、LOGの確認方法	ConsoleまたはTelnet/SSHにてコマンドにてLOGを確認
ii) LOGの保存期間	ルーター内部はDefault300行(設定により変更可能)
iii) LOGのExport機能の可否	可
- 可能な場合は、どの形式で可能か？	SyslogServer
④その他	
ｉ) Decrypt Keyを確認する事は可能か？	可

パラメータ確認シート

2000/12/14

記入者会社名： マイクロソフト株式会社
記入者：藤本浩司
記入日付： 2001/03/07
製品名： Windows 2000 Server
製造メーカ：Microsoft Co., Ltd.
Version： 5.0

1. 製品について

1) 製品形態	
- ﾊｰﾄﾞｳｪｱ製品の場合は各ｼﾘｰｽﾞの型番とｻﾎﾟｰﾄIF	
- ｿﾌﾄｳｪｱ製品の場合は、ｻﾎﾟｰﾄするﾌﾟﾗｯﾄﾌｫｰﾑ	Windows 2000
2) 製品定価	オープンプライス

2. 鍵管理について

1) サポートしている鍵交換手法	IKE
2) IKEパラメータについて	
①Phase 1パラメータ	
ⅰ) サポートしているモード	メインモード
ⅱ) 相互認証方式	Pre-shared, 電子署名,Kerberos
- 電子署名の場合の対応CA局	Windows 2000 Certificate Services、PKCS#10発行要求, PKCS#7署名済みファイル発行可能なCA
ⅲ) 暗号アルゴリズム	DES, 3DES
ⅳ) 認証アルゴリズム	MD5, SHA-1
ⅴ) DHグループ	
ⅵ) 有効期間	
ｱ)Life Type (Time)	サポート
ｲ) Life Duration (Time)	
ｳ) Life Type (KB)	
ｴ) Life Duration (KB)	
ⅶ) IDペイロード	
②Phase2 パラメータについて	
ⅰ) サポートしているTransform	ESP, AH
ⅱ) 暗号アルゴリズム	DES, 3DES
ⅲ) 認証アルゴリズム	HMAC-MD5, HMAC-SHA1
ⅳ) DHグループ	
ⅴ) 有効期間	
ｱ)Life Type (Time)	サポート
ｲ) Life Duration (Time)	
ｳ) Life Type (KB)	
ｴ) Life Duration (KB)	
ⅵ) IDペイロード	
③PFSについて	
ⅰ) PFSのサポート	サポート
ⅱ) PFSのON/OFFの可否	可

3. 運用管理について

①設定方法について	
ⅰ) 設定方法	専用ツール
ⅱ) リモートからの設定変更の可否	可
- 可能な場合は、どの様に行うか？	専用ツールにておこなう
②運用管理について	
ⅰ) SAの状況確認の可否	可
- 可能な場合は、どの様に行うか？	IPSECMON で確認
ⅱ) SAの削除の可否	可
- 可能な場合は、どの様に行うか？	IP セキュリティーポリシーの管理（スナップイン）で作成したポリシーの割り当て解除
ⅲ) 相手毎のSA削除の可否	可
- 可能な場合は、どの様に行うか？	相手毎にポリシーを作成する必要がある。そのポリシーの割り当て解除
ⅳ) SA削除のリモート操作の可否	可
- 可能な場合は、どの様に行うか？	IP セキュリティーポリシーの管理をスナップインするさい、別のコンピュータを選択
③LOGについて	
ⅰ) IKEのネゴシエーションがLOGに残るか？	
- 可能な場合は、LOGの確認方法	
ⅱ) LOGの保存期間	
ⅲ) LOGのExport機能の可否	
- 可能な場合は、どの形式で可能か？	
④その他	
ⅰ) Decrypt Keyを確認する事は可能か？	

パラメータ確認シート

2000/12/14

記入者会社名： 株式会社ヒューコム
記入者： 加納
記入日付： 2000/12/18
製品名： FireboxII
製造メーカ： WatchGuard
Version： 4.5

1. 製品について

1) 製品形態	ハードウェア
- ﾊｰﾄﾞｳｪｱ製品の場合は各ｼﾘｰｽﾞの型番とｻﾎﾟｰﾄIF	FireboxⅡ、FireboxⅡ Plus、Firebox Ⅱ Fast VPN いずれも、10/100M Ethernet Interface×3）
- ｿﾌﾄｳｪｱ製品の場合は、ｻﾎﾟｰﾄするﾌﾟﾗｯﾄﾌｫｰﾑ	
2) 製品定価	878,000円

2. 鍵管理について

1) サポートしている鍵交換手法	IKE, ManualIPSEC
2) IKEパラメータについて	
①Phase 1パラメータ	
ⅰ) サポートしているモード	Main Mode
ⅱ) 相互認証方式	Pre-Shared
- 電子署名の場合の対応CA局	
ⅲ) 暗号アルゴリズム	DES, 3DES
ⅳ) 認証アルゴリズム	MD5 (Responderの場合のみ), SHA-1
ⅴ) DHグループ	Group-1
ⅵ) 有効期間	
ｱ)Life Type (Time)	サポート
	0時間～32000時間
ｳ) Life Type (KB)	サポート
ｴ) Life Duration (KB)	0Kbyte～32000Kbyte
ⅶ) IDペイロード	送信 :ID_IPV4_ADDR, 受信 :ID_IPV4_ADDR,
②Phase2 パラメータについて	
ⅰ) サポートしているTransform	ESP, AH
ⅱ) 暗号アルゴリズム	DES, 3DES
ⅲ) 認証アルゴリズム	HMAC-MD5, HMAC-SHA1
ⅳ) DHグループ	Group-1
ⅴ) 有効期間	
ｱ)Life Type (Time)	サポート
ｲ) Life Duration (Time)	0時間～32000時間
ｳ) Life Type (KB)	サポート
ｴ) Life Duration (KB)	0Kbyte～32000Kbyte
ⅵ) IDペイロード	ID_IPV4_ADDR, ID_IPV4_SUBNET
③PFSについて	
ⅰ) PFSのサポート	Responderの場合のみサポート
ⅱ) PFSのON/OFFの可否	否

3. 運用管理について

①設定方法について	
ⅰ) 設定方法	専用ツール
ⅱ) リモートからの設定変更の可否	可
- 可能な場合は、どの様に行うか？	専用ツールで行う
②運用管理について	
ⅰ) SAの状況確認の可否	可
- 可能な場合は、どの様に行うか？	専用ソフトで行う
ⅱ) SAの削除の可否	可
- 可能な場合は、どの様に行うか？	専用ソフトで行う
ⅲ) 相手毎のSA削除の可否	可
- 可能な場合は、どの様に行うか？	専用ソフトで行う
ⅳ) SA削除のリモート操作の可否	可
- 可能な場合は、どの様に行うか？	専用ソフトで行う
③LOGについて	
ⅰ) IKEのネゴシエーションがLOGに残るか？	残る
- 可能な場合は、LOGの確認方法	専用ソフトでLOGを確認
ⅱ) LOGの保存期間	特に無し
ⅲ) LOGのExport機能の可否	可
- 可能な場合は、どの形式で可能か？	テキストファイル、Web Trend形式
④その他	
ⅰ) Decrypt Keyを確認する事は可能か？	否

パラメータ確認シート

2000/12/14

記入者会社名： 株式会社ヒューコム
記入者： 加納
記入日付： 2000/12/18
製品名： Shiva VPN Gateway
製造メーカ： Intel
Version： 6.8P3

1. 製品について

1) 製品形態	ハードウェア
- ﾊｰﾄﾞｳｪｱ製品の場合は各ｼﾘｰｽﾞの型番とｻﾎﾟｰﾄIF	Shiva VPN Gateway、Shiva VPN Express、INTEL Netstructure VPN 3110、3120（いずれも、10/100M Ethernet Interface×2）
- ｿﾌﾄｳｪｱ製品の場合は、ｻﾎﾟｰﾄするﾌﾟﾗｯﾄﾌｫｰﾑ	
2) 製品定価	1,980,000円

2. 鍵管理について

1) サポートしている鍵交換手法	IKE, ESP V1, ManualIPSEC、L2TP Over IPSec、SST
2) IKEパラメータについて	
①Phase 1パラメータ	
ⅰ) サポートしているモード	Main Mode, Aggressive Mode
ⅱ) 相互認証方式	Pre-Shared, 電子署名、Radius、SecurID
- 電子署名の場合の対応CA局	Entrust (Ready), Shiva CA
ⅲ) 暗号アルゴリズム	DES, 3DES
ⅳ) 認証アルゴリズム	MD5, SHA-1
ⅴ) DHグループ	Group-1, Group-2
ⅵ) 有効期間	
ｱ)Life Type (Time)	サポート
ｲ) Life Duration (Time)	3分～22日
ｳ) Life Type (KB)	サポート
ｴ) Life Duration (KB)	10000Kbyte～2147483647Kbyte
ⅶ) IDペイロード	送信 ID_IPV4_ADDR, 受信 ID_IPV4_ADDR,
②Phase2 パラメータについて	
ⅰ) サポートしているTransform	ESP, AH
ⅱ) 暗号アルゴリズム	DES, 3DES
ⅲ) 認証アルゴリズム	HMAC-MD5, HMAC-SHA1
ⅳ) DHグループ	Group-1, Group-2
ⅴ) 有効期間	
ｱ)Life Type (Time)	サポート
ｲ) Life Duration (Time)	3分～22日
ｳ) Life Type (KB)	サポート
ｴ) Life Duration (KB)	10000Kbyte～2147483647Kbyte
ⅵ) IDペイロード	ID_IPV4_ADDR, ID_IPV4_SUBNET
③PFSについて	
ⅰ) PFSのサポート	サポート
ⅱ) PFSのON/OFFの可否	可

3. 運用管理について

①設定方法について	
ⅰ) 設定方法	専用ツール、コマンド
ⅱ) リモートからの設定変更の可否	可
- 可能な場合は、どの様に行うか？	専用ツール、コンソール、Telnetのいずれか
②運用管理について	
ⅰ) SAの状況確認の可否	可
- 可能な場合は、どの様に行うか？	専用ツール、コンソール、Telnetのいずれか
ⅱ) SAの削除の可否	可
- 可能な場合は、どの様に行うか？	専用ツール、コンソール、Telnetのいずれか
ⅲ) 相手毎のSA削除の可否	可
- 可能な場合は、どの様に行うか？	専用ツール、コンソール、Telnetのいずれか
ⅳ) SA削除のリモート操作の可否	可
- 可能な場合は、どの様に行うか？	専用ツール、コンソール、Telnetのいずれか
③LOGについて	
ⅰ) IKEのネゴシエーションがLOGに残るか？	残る
- 可能な場合は、LOGの確認方法	コンソールかSyslogでLOGを確認
ⅱ) LOGの保存期間	特に無し
ⅲ) LOGのExport機能の可否	可
- 可能な場合は、どの形式で可能か？	テキストファイル
④その他	
ⅰ) Decrypt Keyを確認する事は可能か？	可

パラメータ確認シート

2000/12/14

記入者会社名：(株)PFU
記入者：川渕
記入日付：２００１/３/１６
製品名：NetShelter/FW
製造メーカ：(株)PFU
Version：Ｅ１１Ｌ１１

1. 製品について

1) 製品形態	ハードウェア
- ﾊｰﾄﾞｳｪｱ製品の場合は各ｼﾘｰｽﾞの型番とｻﾎﾟｰﾄIF	型番：LSF100A　IF：LAN(10/100自動認識)×3
- ｿﾌﾄｳｪｱ製品の場合は、ｻﾎﾟｰﾄするﾌﾟﾗｯﾄﾌｫｰﾑ	
2) 製品定価	600,000円

2. 鍵管理について

1) サポートしている鍵交換手法	IKE、およびManual IPsec
2) IKEパラメータについて	
①Phase 1パラメータ	
ｉ) サポートしているモード	MainおよびAggressive
ii) 相互認証方式	Pre-Shared-Key
- 電子署名の場合の対応CA局	---
iii) 暗号アルゴリズム	DESおよび3DES
iv) 認証アルゴリズム	MD5およびSHA1
ｖ) DHグループ	Group1(768MODP)、Group2(1024MODP)
vi) 有効期間	
ｱ)Life Type (Time)	サポート
ｲ) Life Duration (Time)	10分～24時間
ｳ) Life Type (KB)	サポート
ｴ) Life Duration (KB)	0～110592000KB
vii) IDペイロード	送信：ID_IPV4_ADDR, 受信：ID_IPV4_ADDR
②Phase2 パラメータについて	
ｉ) サポートしているTransform	ESP
ii) 暗号アルゴリズム	DESおよび3DES
iii) 認証アルゴリズム	MD5およびSHA1
iv) DHグループ	Group1(768MODP)、Group2(1024MODP)
ｖ) 有効期間	
ｱ)Life Type (Time)	サポート
ｲ) Life Duration (Time)	10分～24時間
ｳ) Life Type (KB)	サポート
ｴ) Life Duration (KB)	0～110592000KB
vi) IDペイロード	ID_IPV4_ADDR, ID_IPV4_ADDR_SUBNET
③PFSについて	
ｉ) PFSのサポート	サポート
ii) PFSのON/OFFの可否	可

3. 運用管理について

①設定方法について	
ｉ) 設定方法	Webブラウザを使用
ii) リモートからの設定変更の可否	可
- 可能な場合は、どの様に行うか？	Webブラウザを使用
②運用管理について	
ｉ) SAの状況確認の可否	可
- 可能な場合は、どの様に行うか？	Webブラウザを使用
ii) SAの削除の可否	不可（装置リセットのみ）
- 可能な場合は、どの様に行うか？	---
iii) 相手毎のSA削除の可否	不可
- 可能な場合は、どの様に行うか？	---
iv) SA削除のリモート操作の可否	不可
- 可能な場合は、どの様に行うか？	---
③LOGについて	
ｉ) IKEのネゴシエーションがLOGに残るか？	残る（ただし、エラーログ（ネゴの失敗結果）のみ）
- 可能な場合は、LOGの確認方法	Webブラウザを使用
ii) LOGの保存期間	31日
iii) LOGのExport機能の可否	可
- 可能な場合は、どの形式で可能か？	バイナリファイル
④その他	
ｉ) Decrypt Keyを確認する事は可能か？	不可

パラメータ確認シート

2000/12/20

記入者会社名： 古河電気工業株式会社
記入者：宮坂
記入日付： 2000/12/20
製品名： INFONET－VP１００
製造メーカ：古河電気工業株式会社
Version： V０３．０１

1. 製品について

1) 製品形態	
- ﾊｰﾄﾞｳｪｱ製品の場合は各ｼﾘｰｽﾞの型番とｻﾎﾟｰﾄIF	ハードウエア　10base-T×２（別セグメント）
- ｿﾌﾄｳｪｱ製品の場合は、ｻﾎﾟｰﾄするﾌﾟﾗｯﾄﾌｫｰﾑ	
2) 製品定価	498，000円

2. 鍵管理について

1) サポートしている鍵交換手法	IKE
2) IKEパラメータについて	
①Phase 1パラメータ	Main Mode, Aggressive Mode, Quick Mode
ⅰ) サポートしているモード	Pre-Shared, 電子署名
ⅱ) 相互認証方式	
- 電子署名の場合の対応CA局	Entrust, SSH, Baltimore等のPKCS#10発行要求, PKCS#7署名済みファイル発行可能なCA
ⅲ) 暗号アルゴリズム	DES, 3DES
ⅳ) 認証アルゴリズム	MD5, SHA-1
ⅴ) DHグループ	Group-1, Group-2
ⅵ) 有効期間	
ｱ)Life Type (Time)	サポート
ｲ) Life Duration (Time)	60sec～2147483647sec
ｳ) Life Type (KB)	未サポート
ｴ) Life Duration (KB)	
ⅶ) IDペイロード	送受信：ID_IPV4_ADDR, user@FQDN, FQDN
②Phase2 パラメータについて	
ⅰ) サポートしているTransform	ESP
ⅱ) 暗号アルゴリズム	DES, 3DES
ⅲ) 認証アルゴリズム	HMAC-MD5, HMAC-SHA1
ⅳ) DHグループ	Group-1, Group-2
ⅴ) 有効期間	
ｱ)Life Type (Time)	サポート
ｲ) Life Duration (Time)	60sec～2147483647sec
ｳ) Life Type (KB)	サポート
ｴ) Life Duration (KB)	100KB～2147483647KB
ⅵ) IDペイロード	ID_IPV4_ADDR, ID_IPV4_SUBNET
③PFSについて	
ⅰ) PFSのサポート	サポート
ⅱ) PFSのON/OFFの可否	可

3. 運用管理について

①設定方法について	
ⅰ) 設定方法	コマンド, WWW
ⅱ) リモートからの設定変更の可否	可
- 可能な場合は、どの様に行うか？	TELNET端末もしくはWWWブラウザより
②運用管理について	
ⅰ) SAの状況確認の可否	可
- 可能な場合は、どの様に行うか？	コンソール, TELNET端末もしくはWWWブラウザより
ⅱ) SAの削除の可否	可
- 可能な場合は、どの様に行うか？	コンソール, TELNET端末もしくはWWWブラウザより
ⅲ) 相手毎のSA削除の可否	可
- 可能な場合は、どの様に行うか？	コンソール, TELNET端末もしくはWWWブラウザより
ⅳ) SA削除のリモート操作の可否	可
- 可能な場合は、どの様に行うか？	コンソール, TELNET端末もしくはWWWブラウザより
③LOGについて	
ⅰ) IKEのネゴシエーションがLOGに残るか？	残る
- 可能な場合は、LOGの確認方法	コンソールもしくはTELNET端末
ⅱ) LOGの保存期間	ログの容量がいっぱいになったあと古いものから上書きされるので、それまで
ⅲ) LOGのExport機能の可否	可
- 可能な場合は、どの形式で可能か？	syslog
④その他	
ⅰ) Decrypt Keyを確認する事は可能か？	不可

パラメータ確認シート

2000/12/14

記入者会社名： 株式会社ネットマークス
記入者：丸山
記入日付： 2000/12/15
製品名： VPN-1
製造メーカ： VPNet社
Version： 3.0.52

1. 製品について

1) 製品形態	ソフトウェア
- ﾊｰﾄﾞｳｪｱ製品の場合は各ｼﾘｰｽﾞの型番とｻﾎﾟｰﾄIF	VSU-100, VSU-2000, , VSU-5000, VSU-7500
- ｿﾌﾄｳｪｱ製品の場合は、ｻﾎﾟｰﾄするﾌﾟﾗｯﾄﾌｫｰﾑ	
2) 製品定価	\ 350, 000～

2. 鍵管理について

1) サポートしている鍵交換手法	IKE, SKIP, ManualIPSEC
2) IKEパラメータについて	
①Phase 1パラメータ	
ｉ) サポートしているモード	Main Mode, Aggressive Mode(メーカのClient Softのみ対応)
ii) 相互認証方式	Pre-Shared, 電子署名（certificate mode）
- 電子署名の場合の対応CA局	CA局(Not Ready) :Entrust, RSA, Baltimore, VeriSign, IBM, Microsoft, Netscape / PKCS# :7/10/11/12
iii) 暗号アルゴリズム	Any（動的に暗号化アルゴイズムを選択）, DES, 3DES,
iv) 認証アルゴリズム	Any（動的に暗号化アルゴイズムを選択）, MD5, SHA-1
ｖ) DHグループ	Group-1, Group-2
vi) 有効期間	
ｱ)Life Type (Time)	サポート
ｲ) Life Duration (Time)	60sec ～
ｳ) Life Type (KB)	サポート
ｴ) Life Duration (KB)	1KB ～
vii) IDペイロード	送信 :ID_IPV4_ADDR, ID_IPV4_SUBNET受信 :ID_IPV4_ADDR, ID_IPV4_SUBNET
②Phase2 パラメータについて	
ｉ) サポートしているTransform	ESP, AH
ii) 暗号アルゴリズム	Null, Any（動的に暗号化アルゴイズムを選択）, DES, 3DES, RC5
iii) 認証アルゴリズム	Null, Any（動的に暗号化アルゴイズムを選択）, HMAC-MD5, HMAC-SHA
iv) DHグループ	Group-1, Group-2
ｖ) 有効期間	
ｱ)Life Type (Time)	サポート
ｲ) Life Duration (Time)	30sec ～
ｳ) Life Type (KB)	サポート
ｴ) Life Duration (KB)	1KB ～
vi) IDペイロード	ID_IPV4_ADDR, ID_IPV4_SUBNET
③PFSについて	
ｉ) PFSのサポート	サポート
ii) PFSのON/OFFの可否	可

3. 運用管理について

①設定方法について	
ｉ) 設定方法	Serial Console 及び 専用ツール(VPNmanager)
ii) リモートからの設定変更の可否	可
- 可能な場合は、どの様に行うか？	専用ツール(VPNmanager)で行う。
②運用管理について	
ｉ) SAの状況確認の可否	可
- 可能な場合は、どの様に行うか？	Serial Console を接続し、Terminal上でコマンド実行
ii) SAの削除の可否	可
- 可能な場合は、どの様に行うか？	Serial Console を接続し、Terminal上でコマンド実行
iii) 相手毎のSA削除の可否	可
- 可能な場合は、どの様に行うか？	Serial Console を接続し、Terminal上でコマンド実行
iv) SA削除のリモート操作の可否	不可
- 可能な場合は、どの様に行うか？	
③LOGについて	
ｉ) IKEのネゴシエーションがLOGに残るか？	残る
- 可能な場合は、LOGの確認方法	Serial Console を接続し、Terminal上でコマンド実行（表示させる）
ii) LOGの保存期間	Te mコンソールでのLOG取得のため、LOG取得は取りっぱなし。
iii) LOGのExport機能の可否	可
- 可能な場合は、どの形式で可能か？	Serial Console を接続し、Terminal上に表示される（テキストファイル）
④その他	
ｉ) Decrypt Keyを確認する事は可能か？	不可(VSUのVersionによっては可)

パラメータ確認シート

2000/12/14

記入者会社名： SSHコミュニケーションズ・セキュリティ(株)
記入者：ヴィッレ・サルメンスー
記入日付： 2001/3/22
製品名： SSH IPSec Express Tookit
製造メーカ： SSHコミュニケーションズ・セキュリティ(株)
Version： 4.0

1. 製品について

1) 製品形態	ソフトウェア・ツールキット
- ハードウェア製品の場合は各シリーズの型番とサポートIF	
- ソフトウェア製品の場合は、サポートするプラットフォーム	NetBSD, VxWorks, Windows(Me,NT,2000,95,98), Solaris, FreeBSD, Linux
2) 製品定価	Open

2. 鍵管理について

1) サポートしている鍵交換手法	IKE
2) IKEパラメータについて	
①Phase 1パラメータ	
ⅰ) サポートしているモード	Main Mode, Aggressive Mode, NewGroup Mode, Config Mode
ⅱ) 相互認証方式	Pre-Shared, 電子署名（RSA/DSA), RSA暗号
- 電子署名の場合の対応CA局	PKCS#11, OCSP, CMPv2
ⅲ) 暗号アルゴリズム	DES, 3DES, Rijndael, Blowfish, CAST128
ⅳ) 認証アルゴリズム	SHA-1, MD5,
ⅴ) DHグループ	Group-1, Group-2, Group-5
ⅵ) 有効期間	
ｱ)Life Type (Time)	サポート
ｲ) Life Duration (Time)	1秒～約136年(2^32)
ｳ) Life Type (KB)	サポート
ｴ) Life Duration (KB)	1KB ～ 4GB
ⅶ) IDペイロード	IPv4, IPv4_SUBNET, IPv4_RANGE, FQDN, USR@FQDN, IPv6, IPv6_SUBNET, IPv6RANGE
②Phase2 パラメータについて	
ⅰ) サポートしているTransform	AH, ESP, IPIP, IPCOMP, PMTU, NAT_TRAVERSAL
ⅱ) 暗号アルゴリズム	DES, 3DES, Rijndael, Blowfish, Towfish, CAST128
ⅲ) 認証アルゴリズム	HMAC-MD5, HMAC-SHA
ⅳ) DHグループ	Group-1, Group-2, Group-5
ⅴ) 有効期間	
ｱ)Life Type (Time)	サポート
ｲ) Life Duration (Time)	1秒～約136年(2^32)
ｳ) Life Type (KB)	サポート
ｴ) Life Duration (KB)	1KB ～ 4GB
ⅵ) IDペイロード	IPv4, IPv4_SUBNET, IPv4_RANGE, FQDN, USR@FQDN, IPv6, IPv6_SUBNET, IPv6RANGE
③PFSについて	
ⅰ) PFSのサポート	サポート
ⅱ) PFSのON/OFFの可否	可

3. 運用管理について

①設定方法について	
ⅰ) 設定方法	コンソール, HTTP
ⅱ) リモートからの設定変更の可否	可
- 可能な場合は、どの様に行うか？	telnet, ssh, Webブラウザ
②運用管理について	
ⅰ) SAの状況確認の可否	可
- 可能な場合は、どの様に行うか？	Webブラウザ
ⅱ) SAの削除の可否	可
- 可能な場合は、どの様に行うか？	Webブラウザ，コンソール
ⅲ) 相手毎のSA削除の可否	不可
- 可能な場合は、どの様に行うか？	
ⅳ) SA削除のリモート操作の可否	可
- 可能な場合は、どの様に行うか？	Webブラウザ，コンソール
③LOGについて	
ⅰ) IKEのネゴシエーションがLOGに残るか？	残る
- 可能な場合は、LOGの確認方法	Webブラウザ，コンソール
ⅱ) LOGの保存期間	制限無し
ⅲ) LOGのExport機能の可否	可
- 可能な場合は、どの形式で可能か？	テキストファイル
④その他	
ⅰ) Decrypt Keyを確認する事は可能か？	可

パラメータ確認シート

2000/12/14

記入者会社名：(株)東陽テクニカ
記入者：安食
記入日付：2001/3/6
製品名：clPro-5000
製造メーカ：RADGUARD社
Version：4.50

1. 製品について

1) 製品形態	ハードウェア
- ﾊｰﾄﾞｳｪｱ製品の場合は各ｼﾘｰｽﾞの型番とｻﾎﾟｰﾄIF	最大スループット、SAのセッション数の違いにより、2000（28Kbps)、2500（512Kbps)、2600(2Mbps)、3000(6Mbps)、5000(100Mbps)とシリーズがあります。オプションでFW機能搭載可能。全シリーズ100M Fast Ethernet(FDX)。全シリーズ必ず専用のCA局を必要とします。
- ｿﾌﾄｳｪｱ製品の場合は、ｻﾎﾟｰﾄするﾌﾟﾗｯﾄﾌｫｰﾑ	
2) 製品定価	\550,000～

2. 鍵管理について

1) サポートしている鍵交換手法	IKE
2) IKEパラメータについて	
①Phase 1パラメータ	
ⅰ) サポートしているモード	Main Mode
ⅱ) 相互認証方式	Pre-Shared, 電子署名
- 電子署名の場合の対応CA局	clProシリーズ同士の接続には、専用のCAを利用、外部CA局を利用する場合は、Entrust, SSH, Baltimore等のPKCS#10発行要求, PKCS#7署名済みファイル発行可能なCA
ⅲ) 暗号アルゴリズム	DES, 3DES
ⅳ) 認証アルゴリズム	MD5, SHA-1
ⅴ) DHグループ	Group-1, Group-2
ⅵ) 有効期間	
ｱ)Life Type (Time)	サポート
ｲ) Life Duration (Time)	15min ～ 24h
ｳ) Life Type (KB)	---
ｴ) Life Duration (KB)	---
ⅶ) IDペイロード	送信 ID_IPV4_ADDR, 受信 ID_IPV4_ADDR,
②Phase2 パラメータについて	
ⅰ) サポートしているTransform	ESP, AH
ⅱ) 暗号アルゴリズム	DES, 3DES
ⅲ) 認証アルゴリズム	HMAC-MD5, HMAC-SHA, DES-MAC
ⅳ) DHグループ	Group-1, Group-2
ⅴ) 有効期間	
ｱ)Life Type (Time)	サポート
ｲ) Life Duration (Time)	10min ～ 24h
ｳ) Life Type (KB)	サポート
ｴ) Life Duration (KB)	1Mbyte ～ 100MByte
ⅵ) IDペイロード	ID_IPV4_ADDR, ID_IPV4_SUBNET
③PFSについて	
ⅰ) PFSのサポート	サポート
ⅱ) PFSのON/OFFの可否	可

3. 運用管理について

①設定方法について	
ⅰ) 設定方法	初期設定はハードウェア本体で、その他の設定は専用CAに接続されている専用マネージャソフトより設定を行う。すべてのVPN装置はこのマネージャから設定を行う。 VPN装置ごとに設定を行うときはSLIP接続にて行う。
ⅱ) ﾘﾓｰﾄからの設定変更の可否	可
- 可能な場合は、どの様に行うか？	専用クライアントソフトにより接続し、専用ソフトにてコントロール
②運用管理について	
ⅰ) SAの状況確認の可否	可
- 可能な場合は、どの様に行うか？	専用マネージャソフトにより確認可能、VPN装置にシリアル接続でも可能
ⅱ) SAの削除の可否	可
- 可能な場合は、どの様に行うか？	VPN装置にシリアルで接続し、コマンド実行
ⅲ) 相手毎のSA削除の可否	可
- 可能な場合は、どの様に行うか？	VPN装置にシリアルで接続し、コマンド実行
ⅳ) SA削除のﾘﾓｰﾄ操作の可否	不可
- 可能な場合は、どの様に行うか？	
③LOGについて	
ⅰ) IKEのネゴシエーションがLOGに残るか？	残る
- 可能な場合は、LOGの確認方法	専用マネージャよりFTPにてダウンロード
ⅱ) LOGの保存期間	ログ保存用メモリに保存（古いものから削除）
ⅲ) LOGのExport機能の可否	可
- 可能な場合は、どの形式で可能か？	専用ログアナライザ形式
④その他	
ⅰ) Decrypt Keyを確認する事は可能か？	不可

パラメータ確認シート

2000/12/14

記入者会社名： アクセントテクノロジーズ(株)
記入者：野々下
記入日付： 2000/12/15
製品名： Raptor PowerVPN
製造メーカ： Axent Technologies
Version： v6.5

1. 製品について

1) 製品形態	ソフトウェア
- ﾊｰﾄﾞｳｪｱ製品の場合は各ｼﾘｰｽﾞの型番とｻﾎﾟｰﾄIF	
- ｿﾌﾄｳｪｱ製品の場合は、ｻﾎﾟｰﾄするﾌﾟﾗｯﾄﾌｫｰﾑ	Solaris v2.6, Solaris7, WinNT v4.1
2) 製品定価	\500,000～

2. 鍵管理について

1) サポートしている鍵交換手法	IKE, SKIP, ManualIPSEC
2) IKEパラメータについて	
①Phase 1パラメータ	
ⅰ) サポートしているモード	Main Mode, Aggressive Mode
ⅱ) 相互認証方式	Pre-Shared, 電子署名
- 電子署名の場合の対応CA局	Entrust
ⅲ) 暗号アルゴリズム	DES, 3DES
ⅳ) 認証アルゴリズム	MD5, SHA-1
ⅴ) DHグループ	Group-1, Group-2
ⅵ) 有効期間	
ｱ)Life Type (Time)	指定無し
ｲ) Life Duration (Time)	---
ｳ) Life Type (KB)	---
ｴ) Life Duration (KB)	---
ⅶ) IDペイロード	送信 ID_IPV4_ADDR, 受信 ID_IPV4_ADDR,
②Phase2 パラメータについて	
ⅰ) サポートしているTransform	ESP, AH
ⅱ) 暗号アルゴリズム	DES, 3DES
ⅲ) 認証アルゴリズム	HMAC-MD5, HMAC-SHA1
ⅳ) DHグループ	Group-1, Group-2
ⅴ) 有効期間	
ｱ)Life Type (Time)	サポート
ｲ) Life Duration (Time)	1min ～ 4200000 min
ｳ) Life Type (KB)	サポート
ｴ) Life Duration (KB)	1 KB ～ 2100000 KB
ⅵ) IDペイロード	ID_IPV4_ADDR, ID_IPV4_SUBNET
③PFSについて	
ⅰ) PFSのサポート	サポート
ⅱ) PFSのON/OFFの可否	可

3. 運用管理について

①設定方法について	
ⅰ) 設定方法	専用ツール
ⅱ) リモートからの設定変更の可否	可
- 可能な場合は、どの様に行うか？	専用ツールで行う。
②運用管理について	
ⅰ) SAの状況確認の可否	可
- 可能な場合は、どの様に行うか？	RMCのGUI上で確認
ⅱ) SAの削除の可否	可
- 可能な場合は、どの様に行うか？	RMCのGUI上で削除
ⅲ) 相手毎のSA削除の可否	可
- 可能な場合は、どの様に行うか？	RMCのGUI上で削除
ⅳ) SA削除のリモート操作の可否	可
- 可能な場合は、どの様に行うか？	リモートのマシンでRMCを実行
③LOGについて	
ⅰ) IKEのネゴシエーションがLOGに残るか？	残る(ログをデバッグモードにすることにより可能)
- 可能な場合は、LOGの確認方法	RMCでLOGを確認
ⅱ) LOGの保存期間	configファイルにて指定
ⅲ) LOGのExport機能の可否	可
- 可能な場合は、どの形式で可能か？	テキストファイル
④その他	
ⅰ) Decrypt Keyを確認する事は可能か？	不可

パラメータ確認シート

2000/12/14

記入者会社名： 日新電機㈱
記入者：小山
記入日付： 2000/12/20
製品名： Ravlin１０
製造メーカ：RedCreek
Version： 3.47

1. 製品について

1) 製品形態	ハードウエア
- ﾊｰﾄﾞｳｪｱ製品の場合は各ｼﾘｰｽﾞの型番とｻﾎﾟｰﾄIF	PersonalRavlin Ⅱ, 3200, 10 （10M-Ethernetインタフェース X2）, Ravlin7150, 7160, 7200 （10M/100M-Ethernetインタフェース X2 7200はX3）
- ｿﾌﾄｳｪｱ製品の場合は、ｻﾎﾟｰﾄするﾌﾟﾗｯﾄﾌｫｰﾑ	
2) 製品定価	\200,000.～

2. 鍵管理について

1) サポートしている鍵交換手法	IKE, Manua lIPSEC
2) IKEパラメータについて	
①Phase 1パラメータ	
ⅰ) サポートしているモード	Main Mode, Aggressive Mode
ⅱ) 相互認証方式	Pre-Shared, 電子署名
- 電子署名の場合の対応CA局	Netscape
ⅲ) 暗号アルゴリズム	DES, 3DES
ⅳ) 認証アルゴリズム	MD5, SHA-1
ⅴ) DHグループ	Group1, Group2
ⅵ) 有効期間	
ｱ)Life Type (Time)	サポート
ｲ) Life Duration (Time)	3分～365日23時間59分
ｳ) Life Type (KB)	
ｴ) Life Duration (KB)	
ⅶ) IDペイロード	ID_IPV4_ADDR, ID_IPV4_SUBNET
②Phase2 パラメータについて	
ⅰ) サポートしているTransform	ESP, AH
ⅱ) 暗号アルゴリズム	DES, 3DES
ⅲ) 認証アルゴリズム	HMAC-MD5, HMAC-SHA1
ⅳ) DHグループ	Group1, Group2
ⅴ) 有効期間	
ｱ)Life Type (Time)	サポート
ｲ) Life Duration (Time)	2分～365日23時間59分
ｳ) Life Type (KB)	
ｴ) Life Duration (KB)	
ⅵ) IDペイロード	ID_IPV4_ADDR, ID_IPV4_SUBNET
③PFSについて	
ⅰ) PFSのサポート	サポート
ⅱ) PFSのON/OFFの可否	可

3. 運用管理について

①設定方法について	
ⅰ) 設定方法	専用ツール（Ravlin NodeManager）
ⅱ) リモートからの設定変更の可否	可
- 可能な場合は、どの様に行うか？	専用ツール（Ravlin NodeManager）から
②運用管理について	
ⅰ) SAの状況確認の可否	可
- 可能な場合は、どの様に行うか？	専用ツール（Ravlin NodeManager）から
ⅱ) SAの削除の可否	可
- 可能な場合は、どの様に行うか？	専用ツール（Ravlin NodeManager）から
ⅲ) 相手毎のSA削除の可否	可
- 可能な場合は、どの様に行うか？	専用ツール（Ravlin NodeManager）から
ⅳ) SA削除のリモート操作の可否	可
- 可能な場合は、どの様に行うか？	専用ツール（Ravlin NodeManager）から
③LOGについて	
ⅰ) IKEのネゴシエーションがLOGに残るか？	残る
- 可能な場合は、LOGの確認方法	ツールSyslogViewerによる
ⅱ) LOGの保存期間	制限なし
ⅲ) LOGのExport機能の可否	有り
- 可能な場合は、どの形式で可能か？	syslog形式
④その他	
ⅰ) Decrypt Keyを確認する事は可能か？	不可

パラメータ確認シート

記入者会社名：㈱フジクラ
記入者：相馬
記入日付：２００１/０３/０６
製品名：FNX0531
製造メーカ：㈱フジクラ
Version：V2.1.03

1. 製品について

1) 製品形態	ハードウェア
- ﾊｰﾄﾞｳｪｱ製品の場合は各ｼﾘｰｽﾞの型番とｻﾎﾟｰﾄIF	WAN BRI 1ポート(ISDN or HSD or Frame Relay)、LAN 2ポート(10/100M, 10M)
- ｿﾌﾄｳｪｱ製品の場合は、ｻﾎﾟｰﾄするﾌﾟﾗｯﾄﾌｫｰﾑ	---
2) 製品定価	\148,000

2. 鍵管理について

1) サポートしている鍵交換手法	IKE、Manual IPsec
2) IKEパラメータについて	
①Phase 1パラメータ	
ⅰ) サポートしているモード	Main Mode, Aggressive Mode
ⅱ) 相互認証方式	Pre-Shared
- 電子署名の場合の対応CA局	---
ⅲ) 暗号アルゴリズム	DES
ⅳ) 認証アルゴリズム	MD5, SHA-1
ⅴ) DHグループ	Group-1
ⅵ) 有効期間	
ｱ)Life Type (Time)	サポート
ｲ) Life Duration (Time)	120 ～ 4294967295 (2の32乗-1) [sec]
ｳ) Life Type (KB)	---
ｴ) Life Duration (KB)	---
ⅶ) IDペイロード	送信 :ID_IPV4_ADDR, 受信 :ID_IPV4_ADDR
②Phase2 パラメータについて	
ⅰ) サポートしているTransform	ESP, AH
ⅱ) 暗号アルゴリズム	DES, 3DES, ESP-NULL
ⅲ) 認証アルゴリズム	HMAC-MD5, HMAC-SHA1
ⅳ) DHグループ	Group-1
ⅴ) 有効期間	
ｱ)Life Type (Time)	サポート
ｲ) Life Duration (Time)	120 ～ 4294967295 (2の32乗-1) [sec]
ｳ) Life Type (KB)	---
ｴ) Life Duration (KB)	---
ⅵ) IDペイロード	ID_IPV4_ADDR, ID_IPV4_SUBNET
③PFSについて	
ⅰ) PFSのサポート	未サポート
ⅱ) PFSのON/OFFの可否	否

3. 運用管理について

①設定方法について	
ⅰ) 設定方法	コンソール、telnet、web、ftp
ⅱ) リモートからの設定変更の可否	可
- 可能な場合は、どの様に行うか？	telnet or web or ftp で行う
②運用管理について	
ⅰ) SAの状況確認の可否	可
- 可能な場合は、どの様に行うか？	"key list" コマンドで使用 (Phase2 SA のみ確認可、コンソールでのみ使用可)
ⅱ) SAの削除の可否	可
- 可能な場合は、どの様に行うか？	リブートor 電源OFF
ⅲ) 相手毎のSA削除の可否	否
- 可能な場合は、どの様に行うか？	---
ⅳ) SA削除のリモート操作の可否	否
- 可能な場合は、どの様に行うか？	---
③LOGについて	
ⅰ) IKEのネゴシエーションがLOGに残るか？	残る (ただし、エラーイベントのみ)
- 可能な場合は、LOGの確認方法	"log sys" コマンドで確認
ⅱ) LOGの保存期間	特になし (ログ領域が一杯になると古いものから順に上書きされる)
ⅲ) LOGのExport機能の可否	可
- 可能な場合は、どの形式で可能か？	リモートホストにログを転送するようにあらかじめ設定しておく (デフォルトは転送しない)
④その他	
ⅰ) Decrypt Keyを確認する事は可能か？	IPsec SA のDecrypt key は確認可、IKE SA は不可

パラメータ確認シート

2000/12/14

記入者会社名： 工学院大学
記入者： 松木・高野
記入日付： ２０００/１２/１９
製品名： Cisco IOS
製造メーカ： Cisco Systems
Version： 12.1(4)

1. 製品について

1) 製品形態	ソフトウェア
- ﾊｰﾄﾞｳｪｱ製品の場合は各ｼﾘｰｽﾞの型番とｻﾎﾟｰﾄIF	
- ｿﾌﾄｳｪｱ製品の場合は、ｻﾎﾟｰﾄするﾌﾟﾗｯﾄﾌｫｰﾑ	Cisco7120等ルータ製品
2) 製品定価	

2. 鍵管理について

1) サポートしている鍵交換手法	IKE, CET, IPSEC-Manual
2) IKEパラメータについて	
①Phase 1パラメータ	
ｉ) サポートしているモード	Main Mode, Aggressive Mode
ii) 相互認証方式	Pre-Shared, CA, Public-Key
- 電子署名の場合の対応CA局	Entrust, Verisign, Boltimore, Microsoft等SCEPサポートCA
iii) 暗号アルゴリズム	DES, 3DES
iv) 認証アルゴリズム	MD5, SHA-1
ｖ) DHグループ	Group-1,2,5
vi) 有効期間	
ｱ)Life Type (Time)	サポート
ｲ) Life Duration (Time)	120sec - 86400sec (2min - 1day)
ｳ) Life Type (KB)	None
ｴ) Life Duration (KB)	―
vii) IDペイロード	送信 :ID_IPv4_ADDR,受信 :ID_IPv4_ADDR
②Phase2 パラメータについて	
ｉ) サポートしているTransform	ESP, AH
ii) 暗号アルゴリズム	DES, 3DES
iii) 認証アルゴリズム	HMAC-MD5, HMAC-SHA1
iv) DHグループ	Group1,2,5
ｖ) 有効期間	
ｱ)Life Type (Time)	サポート
ｲ) Life Duration (Time)	60sec - 86400sec (1min - 1day)
ｳ) Life Type (KB)	サポート
ｴ) Life Duration (KB)	2560KB ～ 536870912KB
vi) IDペイロード	ID_IPv4_ADDR, ID_IPv4_SUBNET
③PFSについて	
ｉ) PFSのサポート	サポート
ii) PFSのON/OFFの可否	可

3. 運用管理について

①設定方法について	
ｉ) 設定方法	Console又はTelnet, SSH, 管理ツール
ii) リモートからの設定変更の可否	可
- 可能な場合は、どの様に行うか？	Console又はTelnet, SSH, 管理ツール
②運用管理について	
ｉ) SAの状況確認の可否	可
- 可能な場合は、どの様に行うか？	Console又はTelnet, SSH, 管理ツール
ii) SAの削除の可否	可
- 可能な場合は、どの様に行うか？	Console又はTelnet, SSH, 管理ツール
iii) 相手毎のSA削除の可否	可
- 可能な場合は、どの様に行うか？	Console又はTelnet, SSH, 管理ツール
iv) SA削除のリモート操作の可否	可
- 可能な場合は、どの様に行うか？	Console又はTelnet, SSH, 管理ツール
③LOGについて	
ｉ) IKEのネゴシエーションがLOGに残るか？	残る
- 可能な場合は、LOGの確認方法	Console又はSyslogで確認
ii) LOGの保存期間	特に無し
iii) LOGのExport機能の可否	可
- 可能な場合は、どの形式で可能か？	テキストファイル
④その他	
ｉ) Decrypt Keyを確認する事は可能か？	可