KELグループ社内勉強会
Firewallの導入

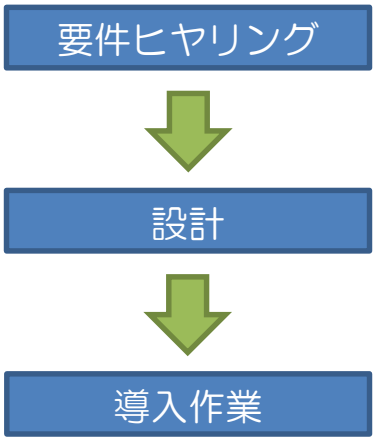
案件について

❖Firewall（以下FW）製品を扱う案件はどんな案件が存在するか

- お客様の既存NWへ新しくFWを導入するケース
- 既存FWのEoLに伴って機器の更改を行うケース
- 新基盤構築プロジェクトにおいてNW構成にFWが含まれているケース

❖お話しする流れ

- 案件スタートからクローズまでの流れを沿う形で説明させて頂きます
- レイヤー3までのベーシックなアクセス制御を行うFWの導入についてお話します



要件ヒアリング①

お客様より実現したい内容を伺う

⑴実現したい内容及び必要な通信要件を受領

- 通信要件を用いた説明、
  もしくは簡易的な構成図を見ながら説明を受ける。

⑵作業によって発生する通信断時間の確認

- 既存業務への影響有無及び、希望リリース日時のご要望、
  既存業務影響が有る場合は停止時間の確認。

⑶当日の作業スケジュール及び作業手順（順序）の確認

- 大枠の当日の流れを確認。

要件とお客様NW構成は可能であれば打ち合わせ前に取得して読み込みを行います。
お客様が実現したい内容をイメージできる様にしておく事で、ヒアリング時の理解度に差がでます。

要件ヒアリング②-1

お客様から提示された内容に対して漏れが無い様にヒアリングを行う

(1)通信要件の漏れが無いかヒアリングする

- お客様からは、通信要件がわかる何らかの資料（通信リストや構成図）が提示される為、
  資料に目を通し明確でない記述があれば「どのような状況」で「どのような通信制御」を
  必要としているのかをお客様に確認します。
  明確な記載がある部分に関しても、通信方向やトラフィック量について確認をしておきます。

  お客様にも「即答できないもの」「即答できるもの」があると思いますが、
  いずれにせよ資料の更新を依頼し、こちらで要望する情報が記載されている資料に
  更新して送っていただく流れにします。
  （資料更新をお客様にお願いする背景にはお客様自身にも通信要件を理解頂く事が狙いです）

(2)通信影響の許容時間を確認

- 既存業務への影響がでることが想定される場合、
  大まかな想定通信断時間をお伝えし、お客様の許容できる断時間がどの程度かを確認します。
  （秒単位での断時間の回答を求められることがよくありますが、
  正確な影響時間を回答出来ない場合は持ち帰りとし後日回答します）

要件ヒアリング②-2

⑶スケジュールと作業手順・時間の確認

・お客様がもっているイメージに合わせ、こちらの作業時間と作業の流れを説明します。

双方の認識にズレがある場合は、この場で双方の感覚を調整しておきますが
特にNW作業に必要となる所要時間はその必要性を丁寧に説明してお客様の感覚を
こちらに寄せてもらいます。
（お客様のご要望に寄り添う事も大事ですが、NW作業に必要な時間を
削ってまで要望を呑んでしまう事は作業品質の低下に繋がる可能性があるので注意が必要です）

設計①-1

◆要件ヒアリング後、得た情報を元に設計を進めます
◆要件ヒアリングの内容は取りまとめて資料に書き出しておきます（認識齟齬を防ぐ為）
◆設計に関する確認事項を取りまとめます、確認ポイントを以下に明記します

説明・確認資料の作成（要件まとめ・設計）

⑴物理構成/論理構成の提示
- 機器諸元及び電源ケーブル規格、必要電源ケーブル数を提示
- 物理/論理構成の提出
  （更改案件であれば現在の構成と新FW導入による物理構成の変更点を図に起こし、
  お客様との相互認識を行う）

⑵必要ケーブル数・ケーブルタグ部材
- 必要ケーブル数・ケーブル長・色指定の有無、標準or細径
  ケーブルタグ形状、ケーブルタグ記載内容の認識合わせを行います
  （責任分界点を目安に部材調達内容をリスト化し、
  お客様調達範囲があれば明示的に記載し認識のズレを防止する）

⑶HA構成について
- HA構成の種類（Active/Standby構成又はActive/Active構成）
- フェイルオーバー条件について説明します（復旧時の自動切り戻り機能の実装ついて確認）
- 設定同期、セッション同期について説明します

⑷OSについて
- OSバージョンの選定理由を明確にします
  （お客様指定がある場合はリリースノートを確認し、妥当性を確認する）
- EoL期日を把握しておき、お客様に連携しておきます

設計①-2

KEL TECHNICAL SERVICE LTD.

⑸汎用手順書について

- 弊社作成の汎用手順を事前に確認頂き、他に必要な手順が無いか確認します

⑹スケジュールについて

- リリース作業実施日から逆算し、いつまでに何を実施するか予定を立て合意を頂きます
  （WBSの提出を求められている場合は別途作成し、提出を行う）

⑺検証方針について

- 検証を導入前にKEL技術センター環境で実施する場合、
  NW環境はお客様環境と同様の環境を準備出来ない為、
  疑似的に再現した環境で行う旨を予めお伝えし合意を頂きます

⑻納品物について

- 納品資料について事前に提出内容を一覧化し、納品資料の認識を合わせておきます

- 以上を踏まえて資料作成を行い、お客様と打ち合わせを行います
- 作成した資料とお客様の認識がズレている事もあります。
  その場合は都度ヒアリングを行い後の工程を進める上で手戻りが少ない様にこの段階で設計を固めておく事が重要です

設計②-1

KEL TECHNICAL SERVICE LTD.

パラメータシート作成（通信要件）

(1)新規導入の場合

・要件ヒアリング時に頂いている情報を元にパラメータ表を作成します。

(2)既存FWを更改する場合

・既存コンフィグを確認し重複している設定や、新FWを導入する事で設定不要となるポリシーが無いか確認を行い、Excelで一覧表を作成します。新FWに移植しないポリシーを明示的にお客様に示します。（この際、お客様でも不要ポリシーが他に無いか確認頂きます。）

【SAMPLE】ASA Config精査

Name	ACL	protocols	source				dstination			
	outside_access_in	icmp	any4				any4			
	outside_access_in	tcp	any4				any4			
	outside_access_in	udp	host	xxx.xxx.xxx.001			xxx.xxx.0.0	255.255.0.0	eq	domain
移植不要	outside_access_in	udp	host	xxx.xxx.xxx.002	eq	domain	xxx.xxx.0.1	255.255.0.0		
	outside_access_in	udp	host	xxx.xxx.xxx.003			xxx.xxx.0.2	255.255.0.0	eq	domain
移植不要	outside_access_in	udp	host	xxx.xxx.xxx.004	eq	domain	xxx.xxx.0.3	255.255.0.0		
	outside_access_in	udp	host	xxx.xxx.xxx.005			xxx.xxx.0.4	255.255.0.0	eq	netbios-ns
移植不要	outside_access_in	udp	host	xxx.xxx.xxx.006	eq	netbios-ns	xxx.xxx.0.5	255.255.0.0		
重複ルール(移植不要)	outside_access_in	icmp	any4	any4			**echo-reply**			
	outside_access_in	udp	object	mrelay			host	xxx.xxx.xxx.xxx	eq	25
移植不要	outside_access_in	udp	object	mrelay	eq	25	host	xxx.xxx.xxx.xxx		
同一ゾーン間の制御(移植不要)	outside_access_in	udp	object	mrelay			host	xxx.xxx.xxx.xxx	eq	25
同一ゾーン間の制御(移植不要)	outside_access_in	udp	object	mrelay	eq	25	host	xxx.xxx.xxx.xxx		
	outside_access_in	udp	host	xxx.xxx.xxx.001			host	xxx.xxx.xxx.xxx	eq	domain
同一ゾーン間の制御(移植不要)	outside_access_in	udp	host	xxx.xxx.xxx.002			host	xxx.xxx.xxx.xxx	eq	domain
	outside_access_in	udp	host	xxx.xxx.xxx.003			host	xxx.xxx.xxx.xxx	eq	domain
同一ゾーン間の制御(移植不要)	outside_access_in	udp	host	xxx.xxx.xxx.004			host	xxx.xxx.xxx.xxx	eq	domain
移植不要	outside_acce									
同一ゾーン間の制御(移植不要)	outside_acce									
移植不要	outside_acce									
同一ゾーン間の制御(移植不要)	outside_acce									

・設定情報の棚卸が出来る絶好の機会である為、可能な限り協力頂き設定情報を厳選します
・不要なポリシーが入っている＝セキュリティレベルの低下に繋がります

設計②-2

KEL TECHNICAL SERVICE LTD.

パラメータシート作成（通信要件以外の他設定）

(1)パラメータシートを作成する

- パラメータシートをベースに設定事項をヒアリングします
- ヒアリング箇所を黄色セルとし、お客様に埋めて頂く事は問題ありませんが、
  お客様のレベルに合わせて以下の様に記載内容の意味や補足事項を記載すると親切であり、
  不明点があった際の問い合わせにかかる工数を削減でます

【SAMPLE】PaloAlto Interface Setting

インターフェイス名	インターフェースタイプ	Netflowプロファイル	バーチャルワイヤー(L1の場合) VLAN(L2の場合) 仮想ルーター(L3の場合)	ゾーン名	IP/Prefix	リンク速度	リンク デュプレックス	リンク状態	MTU (値: 576-1500)	TCP MSSの調整	タグのないサブインターフェース
ethernet1/1	Layer1		vsys3	AAA-WAN	-	auto	auto	auto		☐	☐
ethernet1/2	Layer1		vsys3	AAA-LAN	-	auto	auto	auto		☐	☐
ethernet1/3	Layer1		vsys4	OTHER-WAN	-	auto	auto	auto		☐	☐
ethernet1/4	Layer1		vsys4	OTHER-LAN	-	auto	auto	auto		☐	☐
ethernet1/5						auto	auto	auto		☐	☐
ethernet1/6						auto	auto	auto		☐	☐
ethernet1/7						auto	auto	auto		☐	☐
ethernet1/8						auto	auto	auto		☐	☐
ethernet1/9						auto	auto	auto		☐	☐
ethernet1/10						auto	auto	auto		☐	☐
ethernet1/11						auto	auto	auto		☐	☐
ethernet1/12						auto	auto	auto		☐	☐
ethernet1/13	Aggregate(ae1)		default		-	auto	auto	auto		☐	☐
ethernet1/14	Aggregate(ae1)		default		-	auto	auto	auto		☐	☐
ethernet1/15						auto	auto	auto		☐	☐
ethernet1/16						auto	auto	auto		☐	☐
ethernet1/17						auto	auto	auto		☐	☐
ethernet1/18						auto	auto	auto		☐	☐
ethernet1/19						auto	auto	auto		☐	☐
ethernet1/20						auto	auto	auto		☐	☐
ethernet1/21						auto	auto	auto		☐	☐
ethernet1/22										☐	☐
ethernet123										☐	☐
ethernet1/24								auto		☐	☐
ae1	Layer3					auto	auto	auto		☐	☐
ae1.xxx1	Layer3		vsys1	BBB-WAN	xxx.xxx.xxx.xxx/xx					☐	☐
ae1.xxx2	Layer3		vsys1	BBB-LAN	xxx.xxx.xxx.xxx/xx					☐	☐
ae1.yyy1	Layer3		vsys2	HOSPITAL-WAN	yyy.yyy.yyy.yyy/yy					☐	☐
ae1.yyy2	Layer3		vsys2	HOSPITAL-LAN	yyy.yyy.yyy.yyy/yy					☐	☐
vlan										☐	☐
loopback										☐	☐
tunnel											

■黄色セル： お客様にて記載
■緑色セル： KELで修正
□白色セル： デフォルト値

IPアドレス/サブネットの記載をお願いします

設計③-1

KEL TECHNICAL SERVICE LTD.

検証

(1)検証項目の作成

- 試験項目には確認方法と判定基準を記載します
- 前提条件、全試験項目について共通する周知内容があれば記載します
- 試験内容作成後、お客様へ提出し実施内容について合意を頂きます

KEL技術センタで行う試験項目及び、
現地で行う試験項目を明確にしましょう

FW冗長化　検証計画兼結果報告書

事前検証・導入時検証

事前の検証環境は、疑似環境で実施する。
疑似環境ではすべての通信を再現することはできないため、機能確認は可能な範囲で実施する。
障害試験実施時は、端末間で継続PingとTCPセッションを確立し、通信断時間とセッション維持機能を確認する。
基本#1をActive、#2をPassiveの状態を正常として検証する。#2がActiveとなった場合は、都度切り戻す。

試験を進めるうえでの前提条件を記載し、
試験実施内容の判定基準に曖昧な箇所を無くしましょう。

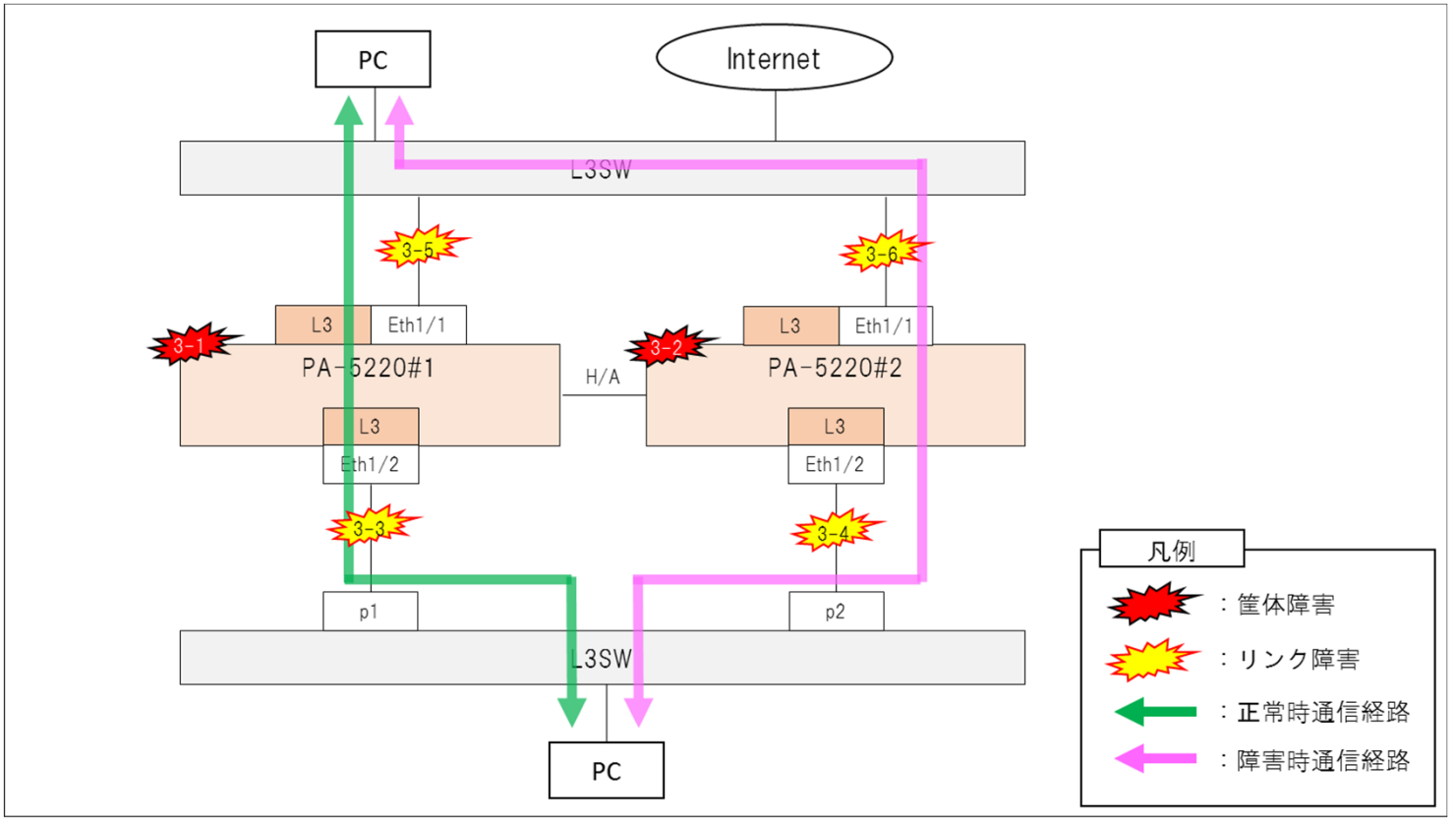
カテゴリ	対象機器	項番	項目	確認方法	判定基準	事前検証結果 断時間	導入時検証結果 断時間
2.結合（正常系）	PA-3260#1系	2-1	HA構成確認	GUI：Dashboard > 高可用性　のステータスを確認する。	以下ステータスであること。 Mode：Active-passive Local：Active 実行コンフィグ：Synchronized 各バージョン：Match　※Mismatchが無いこと HA1・2・バックアップ全て：Up		
		2-2	インタフェースステータス確認	GUI：Network>インタフェース を確認する。	接続ポートがすべて想定されるLink速度でupしていること。		
		2-3	ルーティング確認	CLI：show routing route の出力を確認する。	設定したStatic Routeがroutingがテーブルにのっていること。		
		2-4	NTP時刻同期確認	CLI：show ntp の出力を確認する。	statusがsynchedであること。reachableがyesであること。		
		2-5	リモートアクセス確認	疑似監視端末からssh, HTTPS で機器にログインする。	所定のパスワードでssh, HTTPSアクセスができること。		
		2-6	CPU使用率確認	GUI：Dashboard > システムリソース を確認する。	平均でCPU使用率80%以下であること。		
		2-7	ログ確認	GUI：Monitor > システム を確認する。	異常なエラーメッセージがないこと。		
	PA-3260#2系	2-8	HA構成確認	GUI：Dashboard > 高可用性　のステータスを確認する。	以下ステータスであること。 Mode：Active-passive Local：Passive 実行コンフィグ：Synchronized 各バージョン：Match　※Mismatchが無いこと HA1・2・バックアップ全て：Up		
		2-9	インタフェースステータス確認	GUI：Network>インタフェース を確認する。	接続ポートがすべて想定されるLink速度でupしていること。		
		2-10	ルーティング確認	CLI：show routing route の出力を確認する。	設定したStatic Routeがroutingがテーブルにのっていること。		
		2-11	NTP時刻同期確認	CLI：show ntp の出力を確認する。	statusがsynchedであること。reachableがyesであること。		
		2-12	リモートアクセス確認	疑似監視端末からssh, HTTPS で機器にログインする。	所定のパスワードでssh, HTTPSアクセスができること。		
		2-13	CPU使用率確認	GUI：Dashboard > システムリソース を確認する。	平均でCPU使用率80%以下であること。		
		2-14	ログ確認	GUI：Monitor > システム を確認する。	異常なエラーメッセージがないこと。		

設計③-2

検証

(2)検証構成図の作成

- 図中に障害試験箇所及び通信経路を書き込み、お客様に試験実施項目を理解頂きます



設計③-3

検証

⑶検証実施

- 検証項目に沿って検証作業を実施します。

- お客様納品物に検証時のログが含まれる場合、作業ログは試験項目頃に纏めて保管します。

- 事前に想定している結果と異なる結果が生じた場合、
  お客様に状況を連携し必要に応じて設計変更を行います。
  対処後に対象試験項目の試験を再実施します。

- お客様先の本番環境でないと再現出来ないケースも存在します。
  KEL技術センター環境で実施できない試験項目は現地でテストする旨、お客様に了承を頂きます。

⑷検証結果報告

- 検証結果をお客様に報告します。

- 検証作業は設計内容に妥当性があるかを確認する最後の手段でもあります。
- 導入するFWに合わせた機能確認および障害ポイントの試験を
  網羅する事は導入時のトラブルを可能な限り最小に留める為に必須の作業です。

導入作業①

作業時の確認ポイント

⑴作業前

- 作業開始前に作業の流れ（手順）の読み合わせを現地担当のお客様と行います。
- 現場環境を確認して、ファシリティ面で想定と異なる部分がないかを確認します。

⑵作業中

- 作業中に想定していないこと（手順に無い事）を行う必要がある場合は、
  必ずお客様担当者に了承を得てから実施します。
- タイムスケジュールから外れそうな場合も、その前にお客様に状況を説明し了承を得ておきます。

⑶作業後

- 作業時のログやチェックした手順書はとっておき、証跡とします。
- 忘れ物など現場でのやり残しが無い事を確認し、お客様に了承を頂いて現場から退館します。

導入作業②

作業後の立ち合いについて

(1)翌営業日立ち合い

・リリース作業後や翌日立ち合い時に業務通信が思うようにいかず、
急遽その場で確認や変更を求められることがあります。

切り分けを行う為、自身でFWの設定変更（セキュリティポリシーの追加・変更・削除）は
いつでも実施できる様に操作を把握しておく必要があります。

また通信不通の要件がある際はFWでブロックしていないか聞かれる状況もあります。
ブロックしている通信のログを確認する方法を事前に把握しておく様にします。

・トラブル時に構築範囲外の機器（お客様管理）のステータスも合わせて確認して欲しい等、
要望を頂く事もありますが、ステータス確認する為、協力する事は良いかと思いますが、
設定変更を求められた場合は、自身で判断せず上長に相談する様にします。

導入後

納品物の提出

⑴ 提出する資料は以下が一般的に求められます
- 事前に送付出来る資料もあるが、
  最終系として最後に一括して送付を求められるケースも多いです

#	資料・内容	備考
1	詳細設計書（パラメータシート）	リリース後の設定値が記載されている最終形の資料
2	機器のConfigファイル、 バックアップファイル	リリース作業時、作業終了時に取得したConfigファイル、 バックアップファイル
3	構成図（物理・論理）	作成フォーマットは事前に会話すること 既存ドキュメントを修正する場合、事前に構成図を連携頂くこと
4	検証項目書	結果記載済みであること
5	作業手順書	結果記載済みであること
6	汎用手順書	お客様の必要とする操作手順が全て手順化されていること

⑵ お客様の日々の運用の中で想定される設定変更方法や、各ログの確認方法などの操作説明
- セキュリティポリシーの作成・削除・変更方法や、トラフィックログ確認方法、
  HA構成であればフェイルオーバー方法について聞かれる事が多いです
- 実際の設定画面を見ながらお客様に操作方法を説明し理解頂くこと

ご清聴ありがとうございました
参考になれば幸いです