



APC
apcommunications

競合FW構築経験者が語る- Firewall Migration Toolを活用した移行方法

株式会社エーピーコミュニケーションズ
iTOC事業部 MBS部
宮内 一輝 (k_miyauchi@ap-com.co.jp)

2024年10月3日

- 1.会社／自己紹介
- 2.今回の目的
- 3.Firewall Migration Tool (FMT)の概要説明
- 4.検証プロセス
 - a. 検証の概要
 - b. 検証の狙い
 - c. 検証項目
 - d. 検証環境
 - e. 検証手順
- 5.検証結果
 - a. 各機能の移行結果
 - b. 手動移行とFMT使用時の比較
 - c. Optimize ACL(Beta)
- 6.総括
 - a. 所感
 - b. Appendix
 - c. まとめ
- 7.さいごに

1. 会社紹介



会社名 : 株式会社エーピーコミュニケーションズ
URL : <http://www.ap-com.co.jp/>
本社 : 東京都千代田区鍛冶町2丁目9番12号
神田徳カビル 3階
関連会社 : 株式会社APアシスト、
(戦略提携)ミランティス・ジャパン株式会社
代表 : 内田 武志
設立 : 1995年11月16日
資本金 : 9,250万円
従業員数 : 478名 (2024年4月現在)

事業種目	プライバシーマーク	品質マネジメントシステム
届出電気通信 事業者 A-16-7952 認定取得日 2004/11/18	 10821154 認定取得日 2006/4/7	 JQA-QMA14103 091 認定取得日 : 2005/4/25
情報セキュリティマネジメントシステム	【登録事業者】 ● ITソリューション事業本部 ● グローバルビジネス事業部 ● 先進サービス開発事業部 ● システム開発部 ● IT戦略室	
 認定取得日 : 2009/6/5	【登録活動範囲】 ● 顧客要求仕様に基づくアプリケーション、ネット ワークの設計開発・支援・構築・運用・保守業務 ● 上記の人材供給サービスの企画・管理業務 ● 自主開発によるアプリケーション、WEBサービス	





ENGINEER DRIVEN

「エンジニアとお客様を笑顔にする」
というビジョンを掲げ
従来の慣例に捉われずに
工夫と挑戦を行い続けることができる
NeoSIerを目指し、
新しい価値を作り出す会社です。

日本のSI業界は、もっとおもしろくできる。

1. 会社紹介



カプセルトイ

手のひらネットワーク機器

を企画・総合監修した会社です

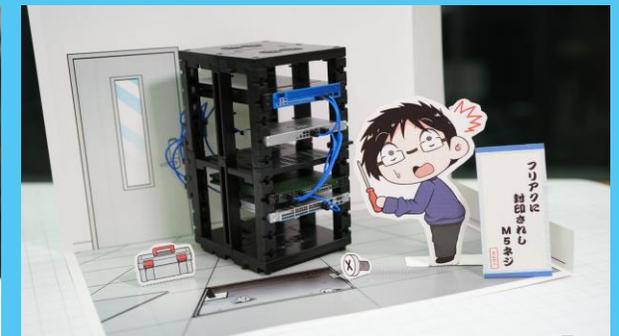
本企画は、総合監修を務める当社が「ITインフラを一般の方にも知ってもらい、業界を盛り上げたい」という思いから立案し、これに共感した A10 ネットワークス様・シスコ様・古河電工様の協力により実現に至りました。

企画・総合監修 ▶▶ APC Communications

※パソコン、ノートパソコンは付属しません。

ネットワーク機器メーカー 監修
手のひらネットワーク機器

※デザインはイメージです。
実際の商品とは異なります。ご了承ください。



1. 自己紹介

氏名： 宮内 一輝 (みやうち かずき)

出身： 神奈川県 大和市

経歴： Palo Alto Networks社製品 運用保守
Palo Alto Firewall構築案件

趣味： 水泳
CTF **NEW**



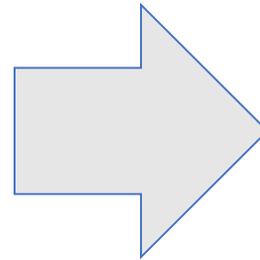
2. 今回の目的

今回は他社ベンダーのFirewall製品からCisco Firewall Threat Defense(FTD)への移行検証を実施

検証にはCisco社が無償で提供しているFirewall Migration Tool(FMT)を使用し、その使用感や手動移行との比較結果を共有することでFMTとはこういった場面で活用できるツールか知ってもらう

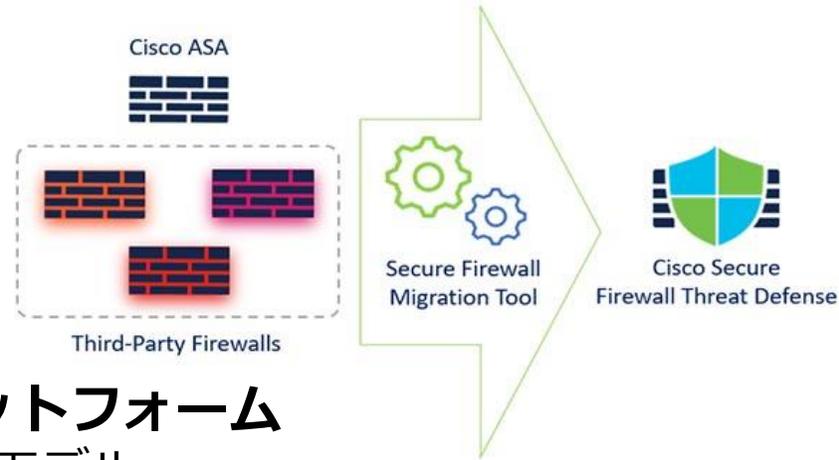


Third-Party Firewall



3. Firewall Migration Tool (FMT)の概要説明

無償で提供される FTDセルフサービス移行ツール

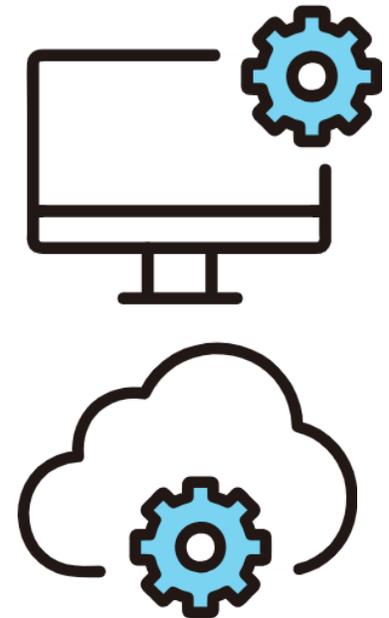


移行元 サポート対象のプラットフォーム

- Cisco Secure Firewall ASA全モデル
- Cisco Secure Firewall Device Manager (FDM) 管理のFTD
- サードパーティ製品：Palo Alto Networks, Fortinet, Check Point

使用方法

- 移行先のFTDはFMC管理（もしくは cdFMC）を用意
- Windows/Mac/CloudベースUI提供
 - Desktop App
 - CDOクラウドサービス



検証プロセス

- Palo Alto Networks社 FirewallからCisco FTDへのマイグレーションを想定した検証を実施
- 移行にはFirewall Migration Tool(FMT)を使用

検証のゴール：FMTを使用した設定ベースでの移行可否の確認

確認すること	確認しないこと
<ul style="list-style-type: none">● FMTを使用した設定移行手順● 各機能毎の移行可否● 移行に伴う考慮事項	<ul style="list-style-type: none">● 移行後の機能検証● 移行前後の動作差分確認

各種設定オブジェクトを作成しなおすのは抜け漏れがありそうで不安

移行前後で差分確認するのは面倒くさい

ツールを使用することで手動移行より楽になるの？

多数あるポリシーを1つずつ手動で移行するのが面倒くさい

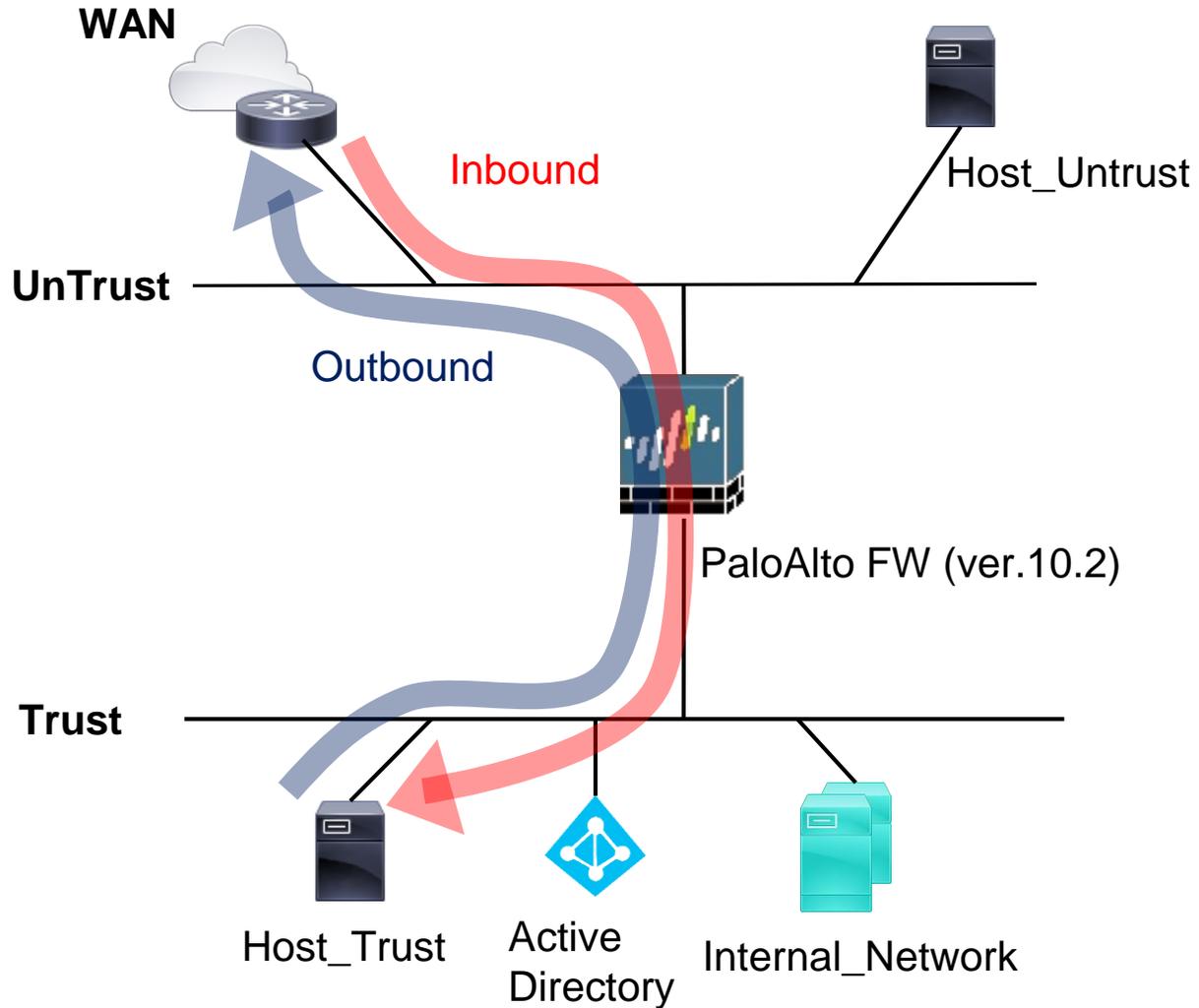


無償のツールをどこまで信用すればいいの？

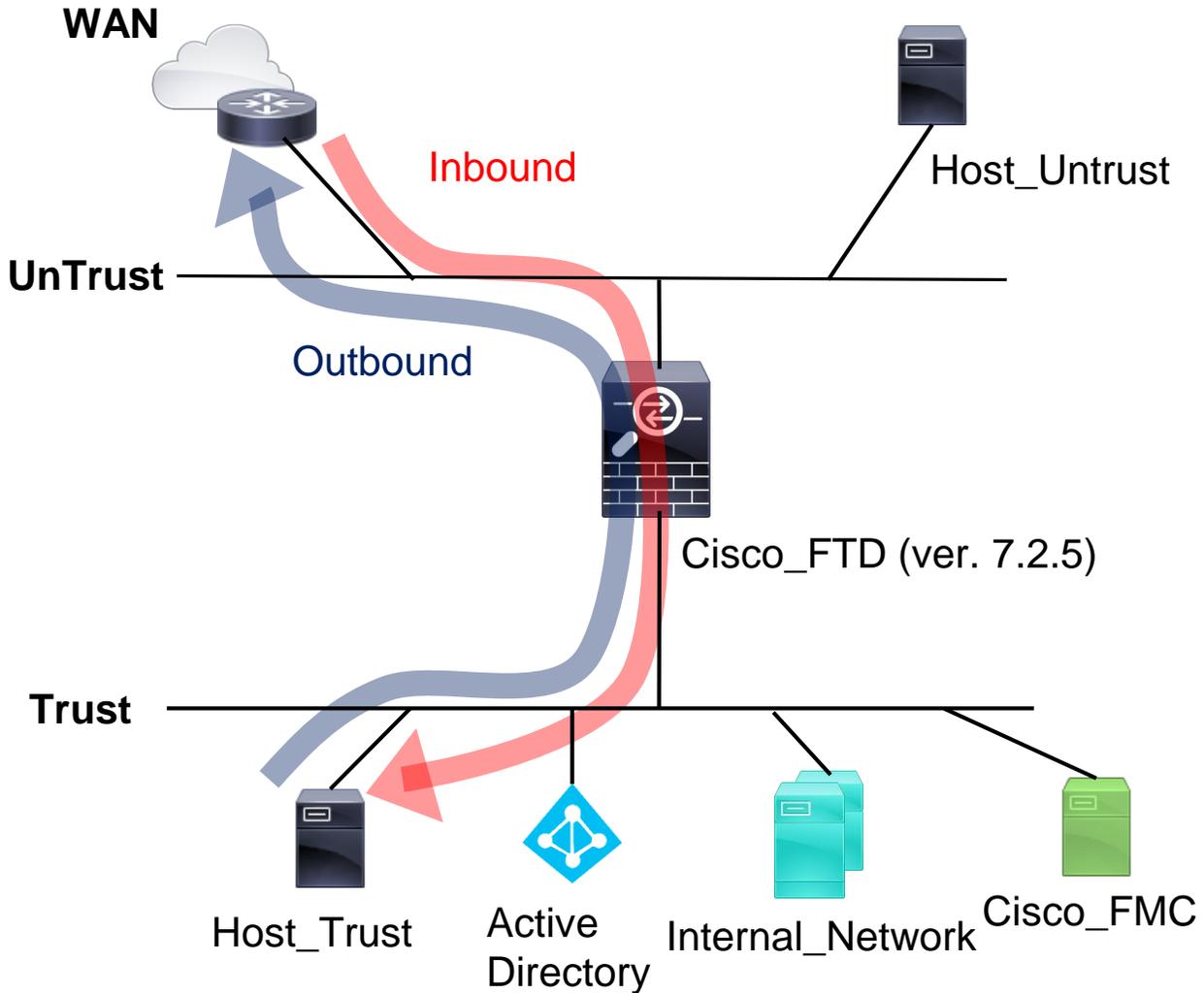
No.	移行元 (PaloAlto)	移行先 (FTD)	結果	備考
1	Interfece	Interfaces		
2	Zone	Security Zones		
3	Static Routing	Static Routes		
4	Dynamic Routes	Dynamic Routes		
5	Address Object	Network Objects		
6	Service Object	Port Objects		
7	Application ID	Applications		
8	Security Policy	Security Rule		
9	NAT Policy	NAT Rule		
10	Security Profile(Threat Prevention)	Intrusion Policy		
11	GlobalProtect	Remote Access VPN		

4-d. 検証環境(概要図)

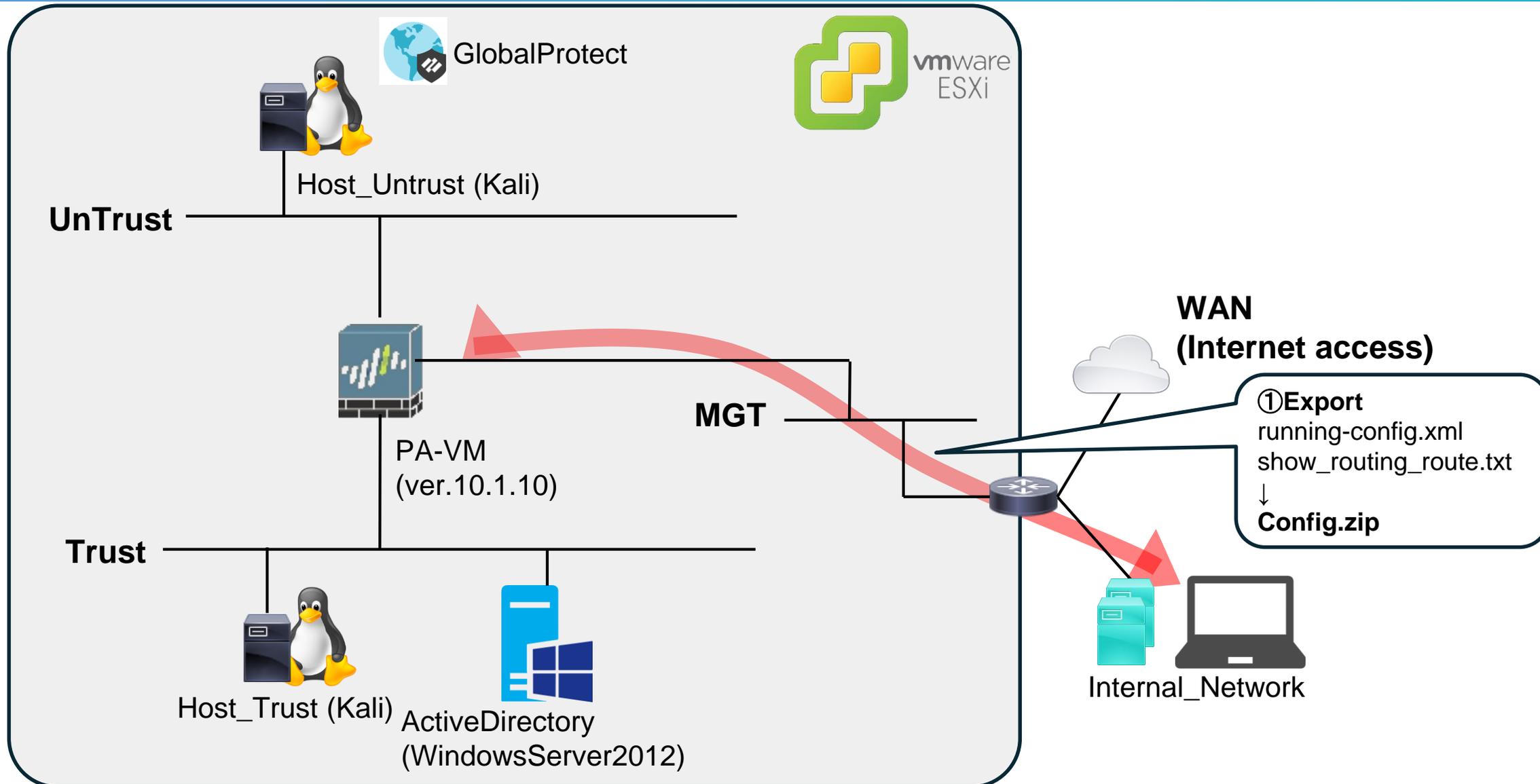
■ PaloAlto Strata Firewall



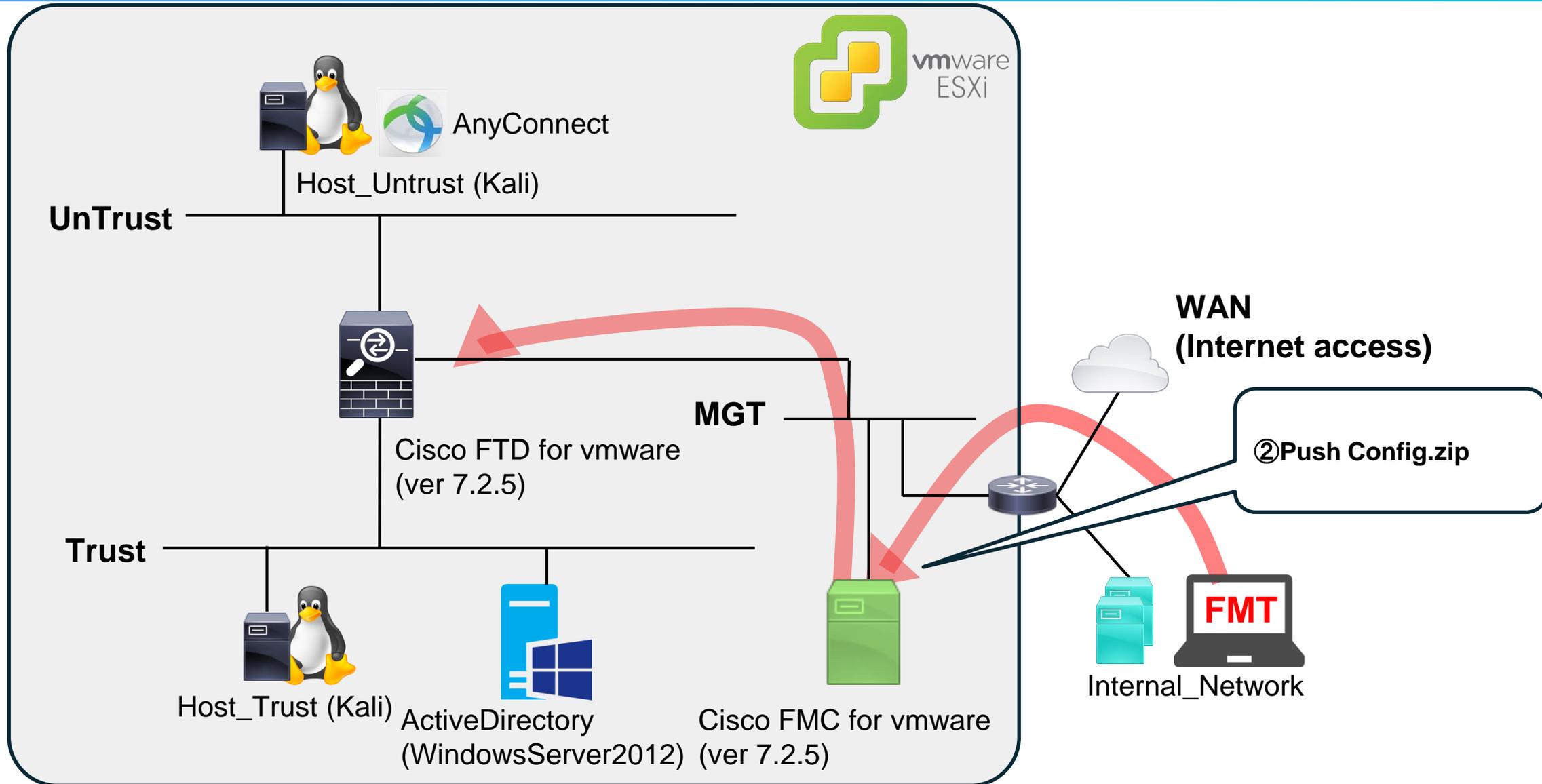
■ Firewall Threat Defense



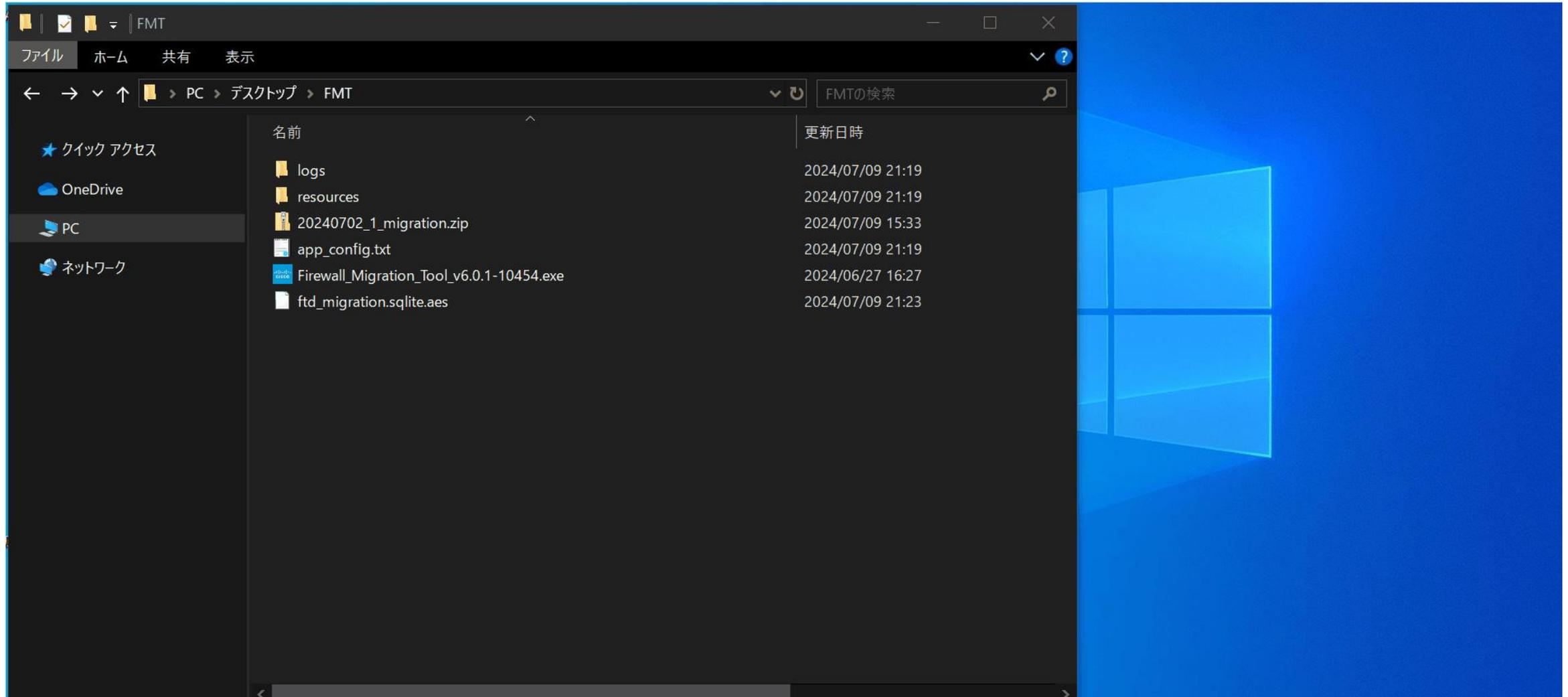
4-e. 検証手順 (PaloAlto)



4-e. 検証手順 (Cisco FTD)



4-e. 検証手順 (FMT)



検証結果

5-a. 検証結果

No.	移行元 (PaloAlto)	移行先 (FTD)	結果	備考
1	Interfece	Interfaces	○	物理インターフェースのみ対応
2	Zone	Security Zones	◎	
3	Static Routing	Static Routes	◎	
4	Dynamic Routes	Dynamic Routes	×	
5	Address Object	Network Objects	◎	
6	Service Object	Port Objects	◎	
7	Application ID	Applications	◎	
8	Security Policy	Security Rule	○	“application-default”使用時は考慮点有
9	NAT Policy	NAT Rule	◎	
10	Security Profile(Threat Prevention)	Intrusion Policy	×	セキュリティ機能は各社独自の為不可
11	GlobalProtect	Remote Access VPN	○	FMCでの事前準備が必要 Tunnel Interfaceは移行不可

◎：移行可能
○：移行可能
(考慮点有)
×：移行不可

5-a. 検証結果（正常に移行できた設定）

No.	移行元 (PaloAlto)	移行先 (FTD)	結果	備考
1	Interfece	Interfaces	○	物理インターフェースのみ対応
2	Zone	Security Zones	◎	
3	Static Routing	Static Routes	◎	
4	Dynamic Routes	Dynamic Routes	×	
5	Address Object	Network Objects	◎	
6	Service Object	Port Objects	◎	
7	Application ID	Applications	◎	
8	Security Policy	Security Rule	○	“application-default”使用時は考慮点有
9	NAT Policy	NAT Rule	◎	
10	Security Profile(Threat Prevention)	Intrusion Policy	×	セキュリティ機能は各社独自の為不可
11	GlobalProtect	Remote Access VPN	○	FMCでの事前準備が必要 Tunnel Interfaceは移行不可

◎：移行可能
○：移行可能
(考慮点有)
×：移行不可

5-a. 検証結果 Security Zones

The screenshot shows the 'Map Security Zones' interface of the Cisco Firewall Migration Tool (Version 6.0.1). The source is Palo Alto Networks (8.0+) and the target is Cisco FTD (v7.2.5). The interface includes 'Add SZ' and 'Auto-Create' buttons. A table maps PAN Zone Names to FMC Security Zones. The 'Trust' and 'Untrust' zones in the PAN column are highlighted with a red box, and the 'Inside_Zone' and 'Outside_Zone' zones in the FMC column are also highlighted with a red box. A callout box points to the 'Inside_Zone' mapping with the text: '移行元のZoneに紐づいたZoneが作成可能なことを確認'.

PAN Zone Name	FMC Security Zones
Trust	Inside_Zone
Untrust	Outside_Zone
Internet	Internet
Corp-VPN	Corp-VPN
DMZ	DMZ

10 per page 1 to 5 of 5 Page 1 of 1

Back Next

5-a. 検証結果 Security Zones

 Firewall Migration Tool (Version 6.0.1)

Map Security Zones ⓘ

Source: Palo Alto Networks (8.0+)
Target FTD: CiscoFTD_v7.2.5

Add SZ Auto-Create

PAN Zone Name	FMC Security Zones
Trust	Trust
Untrust	Untrust
Internet	Internet
Corp-VPN	Corp-VPN
DMZ	DMZ

移行元のZoneと同一名称のZoneを自動作成可能

Success
Successfully gathered

10 per page 1 to 5 of 5 Page 1 of 1

Back Next

5-a. 検証結果 Static Routes

仮想ルーター - default

Router Settings

スタティックルート

再配信プロファイル

RIP

OSPF

OSPFv3

BGP

マルチキャスト

IPv4 | IPv6

2 個の項目s → ×

	名前	宛先	インターフェイス	ネクストホップ		管理距離	メトリック	BFD	ルートテーブル
				タイプ	値				
<input type="checkbox"/>	default-route	0.0.0.0/0	ethernet1/3	ip-address	192.168.79.254	default	10	None	unicast
<input type="checkbox"/>	test	20.20.20.20/32	ethernet1/3	ip-address	192.168.79.254	default	10	None	unicast

+ 追加 - 削除 ↺ コピー

OK キャンセル

5-a. 検証結果 Static Routes

Optimize, Review and Validate Configuration ⓘ

Source: Palo Alto Networks (8.0+)
Target FTD: CiscoFTD_v7.2.5

Access Control Objects NAT Interfaces Routes Site-to-Site VPN Tunnels ⓘ Remote Access VPN

Select all 2 entries Selected: 0 / 2

Actions ▾

Save

🔍 Search



<input type="checkbox"/>	#	Interface	IP Type	Network	Gateway
<input type="checkbox"/>	1	ethernet1_3	V4	0.0.0.0/0	192.168.79.254
<input type="checkbox"/>	2	ethernet1_3	V4	20.20.20.20	192.168.79.254

移行元の設定が踏襲
されていることを確認

50 ▾ per page 1 to 2 of 2 ⏪ ◀ Page of 1 ▶ ⏩

Validate

5-a. 検証結果 Network Objects

名前	場所	タイプ	アドレス
<input type="checkbox"/> 172.20.79.100		IP ネットマスク	172.20.79.100/24
<input type="checkbox"/> Kali_TrustHost		IP ネットマスク	10.20.79.1/32
<input type="checkbox"/> test		IP ネットマスク	1.1.1.1
<input type="checkbox"/> test2		IP ネットマスク	2.2.2.2
<input type="checkbox"/> test3		IP ネットマスク	3.3.3.3
<input type="checkbox"/> test_google.com		FQDN	www.google.com
<input type="checkbox"/> Win2012_DNS_Server		IP ネットマスク	10.20.79.10/32

5-a. 検証結果 Network Objects

Firewall Migration Tool (Version 6.0.1)

Optimize, Review and Validate Configuration ⓘ

Access Control **Objects** NAT Interfaces Routes Site-to-Site VPN Tunnels 1 Remote Access VPN

Network Objects Port Objects VPN Objects

Select all 12 entries Selected: 0 / 12 Actions Save

Search

#	Name	Validation State	Type	Value
1	test	Will be created in FMC	Network Object	1.1.1.1
2	test2	Will be created in FMC	Network Object	2.2.2.2
3	Kali_TrustHost	Will be created in FMC	Network Object	10.20.79.1
4	Win2012_DNS_Server	Will be created in FMC	Network Object	10.20.79.10
5	obj_0.0.0.0_0	Will be created in FMC	Network Object	0.0.0.0/0
6	obj_172.20.79.100_32	Will be created in FMC	Network Object	172.20.79.100
7	obj_10.20.79.1_32	Will be created in FMC	Network Object	10.20.79.1
8	obj_192.168.79.196	Will be created in FMC	Network Object	192.168.79.196
9	obj_172.20.79.1	Will be created in FMC	Network Object	172.20.79.1

50 per page 1 to 12 of 12 Page 1 of 1

Validate

Source: Palo Alto Networks (8.0+)
Target FTD: CiscoFTD_v7.2.5

移行元の設定が踏襲されていることを確認

移行元でSecurity Ruleの内容から自動生成される

5-a. 検証結果 Port Objects

名前	場所	プロトコル	宛先ポート	タグ
<input type="checkbox"/> service-dns		TCP	53	
<input type="checkbox"/> service-http	事前定義済み	TCP	80,8080	
<input type="checkbox"/> service-https	事前定義済み	TCP	443	
<input type="checkbox"/> TCP_10002		TCP	10002	
<input type="checkbox"/> TCP_10003		TCP	10003	
<input type="checkbox"/> TCP_10005		TCP	10005	
<input type="checkbox"/> TCP_10006		TCP	10006	
<input type="checkbox"/> TCP_10007		TCP	10007	
<input type="checkbox"/> TCP_10008		TCP	10008	
<input type="checkbox"/> TCP_10010		TCP	10010	
<input type="checkbox"/> TCP_10014		TCP	10014	
<input type="checkbox"/> TCP_10033		TCP	10033	
<input type="checkbox"/> TCP_10080		TCP	10080	
<input type="checkbox"/> TCP_10081		TCP	10081	
<input type="checkbox"/> TCP_110		TCP	110	
<input type="checkbox"/> TCP_25		TCP	25	
<input type="checkbox"/> TCP_3389		TCP	3389	
<input type="checkbox"/> TCP_443		TCP	443	

5-a. 検証結果 Port Objects

Firewall Migration Tool (Version 6.0.1)

Optimize, Review and Validate Configuration ⓘ

Access Control **Objects** NAT Interfaces Routes Site-to-Site VPN Tunnels ⓘ

Network Objects **Port Objects** VPN Objects

Select all 18 entries Selected: 0 / 18 Actions Save Search

#	Name	Validation State	Type	Value
1	UDP_500	Will be created in FMC	Port Object	udp:500
2	UDP_4500	Will be created in FMC	Port Object	udp:4500
3	TCP_10080	Will be created in FMC	Port Object	tcp:10080
4	TCP_110	Will be created in FMC	Port Object	tcp:110
5	TCP_10033	Will be created in FMC	Port Object	tcp:10033
6	TCP_25	Will be created in FMC	Port Object	tcp:25
7	TCP_3389	Will be created in FMC	Port Object	tcp:3389
8	TCP_10002	Will be created in FMC	Port Object	tcp:10002
9	TCP_10003	Will be created in FMC	Port Object	tcp:10003
10	TCP_10005	Will be created in FMC	Port Object	tcp:10005

50 per page 1 to 18 of 18 Page 1 of 1 Validate

Source: Palo Alto Networks (8.0+)
Target FTD: CiscoFTD_v7.2.5

移行元の設定が踏襲されていることを確認

5-a. 検証結果 Applications

名前	送信元		宛先		アプリケーション	サービス	URL カテゴリ	アクション	プロフィール
	ゾーン	アドレス	ゾーン	アドレス					
1 External_Allow_Trusthost	Trust	Kali_TrustHost Win2012_DNS_Server	Internet Untrust	any	dns web-browsing	application-default	any	許可	
2 External_Allow_TrustHost_VPN	Trust	Kali_TrustHost Win2012_DNS_Server	Corp-VPN	any	dns web-browsing	application-default	any	許可	none
3 External_Allow_UntrustHost	Untrust	172.20.79.1	Internet Trust	any	any	application-default	any	許可	none
4 External_Allow_UntrustHost_VPN	Untrust	172.20.79.1	Corp-VPN	any	any	application-default	any	許可	none
5 VPN-to-Untrust	Corp-VPN	any	Untrust	any	any	any	any	許可	none
6 VPN-to-Trust	Corp-VPN	any	Trust	any	any	any	any	許可	none
7 internal_allow	Internet	any	Trust	10.20.79.1	any	any	any	許可	none
8 test_address_object	any	any	any	test	any	any	any	許可	none
9 test_address_object_2	any	any	any	test2	any	any	any	許可	none
10 All-Allow	any	any	any	any	any	any	any	許可	none
11 untrust-to-dmz_001	Untrust	40.1.1.40/32	DMZ	172.15.7.51/32	any	UDP_4500	any	許可	
12 untrust-to-dmz_002	Untrust	40.1.1.40/32	DMZ	172.15.7.51/32	any	UDP_500	any	許可	
13 untrust-to-dmz_003	Untrust	10.1.1.10/32	DMZ	172.15.7.51/32	any	UDP_4500	any	許可	

5-a. 検証結果 Applications

Firewall Migration Tool (Version 6.0.1)

Optimize, Review and Validate Configuration ⓘ

Access Control | Objects | NAT | Interfaces | Routes | Site-to-Site VPN Tunnels ⓘ | Remote Access VPN

Select all 115 entries Selected: 0 / 115 Actions Save

Source: Palo Alto Networks (8.0+) Target FTD: CiscoFTD_v7.2.5

14 ? ⚙️ ↻

移行元の設定が踏襲されていることを確認

■	#	Name	SOURCE				DESTINATION			Application	URLs	State	Action	TIME BASED
			Zone	Network	Port	Zone	Network	Port						
<input type="checkbox"/>	1	External_Allow_Trust...	Inside_Zone	Kali_TrustHost...	ANY	Internet,Out...	ANY	ANY	DNS, HTTP	NA	✓	Allow	None	
<input type="checkbox"/>	2	External_Allow_Trust...	Inside_Zone	Kali_TrustHost...	ANY	Corp-VPN	ANY	ANY	DNS, HTTP	NA	✓	Allow	None	
<input type="checkbox"/>	3	External_Allow_Untr...	Outside_Zone	172.20.79.1	ANY	Internet,Insi...	ANY	ANY	ANY	NA	✓	Allow	None	
<input type="checkbox"/>	4	External_Allow_Untr...	Outside_Zone	172.20.79.1	ANY	Corp-VPN	ANY	ANY	ANY	NA	✓	Allow	None	
<input type="checkbox"/>	5	VPN-to-Untrust_#5	Corp-VPN	ANY	ANY	Outside_Zone	ANY	ANY	ANY	NA	✓	Allow	None	
<input type="checkbox"/>	6	VPN-to-Trust_#6	Corp-VPN	ANY	ANY	Inside_Zone	ANY	ANY	ANY	NA	✓	Allow	None	
<input type="checkbox"/>	7	internal_allow_#7	Internet	ANY	ANY	Inside_Zone	ANY	ANY	ANY	NA	✓	Allow	None	
<input type="checkbox"/>	8	test_address_object...	ANY	ANY	ANY	ANY	test	ANY	ANY	NA	✓	Allow	None	
<input type="checkbox"/>	9	test_address_object...	ANY	ANY	ANY	ANY	test2	ANY	ANY	NA	✓	Allow	None	

50 per page 1 to 50 of 115 Page 1 of 3

Optimize ACL (Beta) Validate

5-a. 検証結果 NAT Rule



		元の packets					変換済み packets			
名前		送信元ゾーン	宛先ゾーン	宛先インターフェイス	送信元アドレス	宛先アドレス	サービス	送信元変換	宛先変換	ヒット数
1	NAT1_source_nat	Corp-VPN Trust	Untrust	any	any	any	any	dynamic-ip-and-port ethernet1/2 172.20.79.254/24	なし	903
2	NAT2_destination_nat	Untrust	Untrust	any	any	172.20.79.100/32	any	none	destination-translation アドレス: 10.20.79.1/32	330
3	NAT2_destination_nat_Kali	Internet	Internet	any	any	192.168.79.196	any	none	destination-translation アドレス: 10.20.79.1/32	12
4	InternetNAT_source_nat	Trust	Internet	any	any	any	any	dynamic-ip-and-port ethernet1/3 192.168.79.196/24	なし	50637
5	InternetNAT_source_nat_Install_GPClient_Untr...	Untrust	Internet	any	172.20.79.1	any	any	dynamic-ip-and-port ethernet1/3 192.168.79.196/24	なし	2286

5-a. 検証結果 NAT Rule

Firewall Migration Tool (Version 6.0.1)

Optimize, Review and Validate Configuration ⓘ

Source: Palo Alto Networks (8.0+) Target: CiscoFTD_v7.2.5

Access Control Objects **NAT** Interfaces Routes Site-to-Site VPN Tunnels ⓘ Remote Access VPN

Select all 6 entries Selected: 0 / 6 Actions Save

	NAT		ZONE		ORIGINAL PACKET				TRANSLATED PACKET				Dynamic IP / Port-Fallback
	Type	Method	Source	Destination	ADDRESS		PORT		ADDRESS		PORT		
<input type="checkbox"/>	<input type="text"/>												
<input type="checkbox"/>	MANUAL	dynamic	Corp-VPN	Outside_Zone	any	obj_0.0.0.0_0	ANY	ANY	interface	obj_0.0.0.0_0	ANY	ANY	Not Applicable
<input type="checkbox"/>	MANUAL	dynamic	Inside_Zone	Outside_Zone	any	obj_0.0.0.0_0	ANY	ANY	interface	obj_0.0.0.0_0	ANY	ANY	Not Applicable
<input type="checkbox"/>	MANUAL	static	Outside_Zone	Inside_Zone	any	obj_172.20.79...	ANY	ANY	obj_0.0.0.0_0	obj_10.20.79.1_32	ANY	ANY	Not Applicable
<input type="checkbox"/>	MANUAL	static	Internet	Inside_Zone	any	obj_192.168.7...	ANY	ANY	obj_0.0.0.0_0	obj_10.20.79.1_32	ANY	ANY	Not Applicable
<input type="checkbox"/>	MANUAL	dynamic	Inside_Zone	Internet	any	obj_0.0.0.0_0	ANY	ANY	interface	obj_0.0.0.0_0	ANY	ANY	Not Applicable
<input type="checkbox"/>	MANUAL	dynamic	Outside_Zone	Internet	obj_172.20.79.1	obj_0.0.0.0_0	ANY	ANY	interface	obj_0.0.0.0_0	ANY	ANY	Not Applicable

50 per page 1 to 6 of 6 Page 1 of 1

Note: Dynamic IP/Port Fall-back option will create a pool that will perform IP and Port Translation and will be used if the primary pool "Translated - Source Address" runs out of IP

Validate

移行元の設定が踏襲されていることを確認

5-a. 検証結果（移行にあたり一部考慮点のあった設定）▶▶ APCommunications

No.	移行元 (PaloAlto)	移行先 (FTD)	結果	備考
1	Interfece	Interfaces	○	物理インターフェースのみ対応
2	Zone	Security Zones	◎	
3	Static Routing	Static Routes	◎	
4	Dynamic Routes	Dynamic Routes	×	
5	Address Object	Network Objects	◎	
6	Service Object	Port Objects	◎	
7	Application ID	Applications	◎	
8	Security Policy	Security Rule	○	“application-default”使用時は考慮点有
9	NAT Policy	NAT Rule	◎	
10	Security Profile(Threat Prevention)	Intrusion Policy	×	セキュリティ機能は各社独自の為不可
11	GlobalProtect	Remote Access VPN	○	FMCでの事前準備が必要 Tunnel Interfaceは移行不可

◎：移行可能
○：移行可能
(考慮点有)
×：移行不可

5-a. 検証結果 Interface

DASHBOARD ACC MONITOR POLICIES OBJECTS **NETWORK** DEVICE Commit

Ethernet | VLAN | ループバック | トンネル | SD-WAN

9 個

インターフェイス	インターフェイスタイプ	管理プロファイル	リンク状態	IP アドレス	仮想ルーター	タグ	VLAN / バーチャルワイヤー	セキュリティゾーン
ethernet1/1	Layer3	ping		10.20.79.254/24	default	Untagged	none	Trust
ethernet1/2	Layer3	ping		172.20.79.254/24	default	Untagged	none	Untrust
ethernet1/3	Layer3	ping		192.168.79.196/24	default	Untagged	none	Internet

Ethernet | **VLAN** | ループバック | トンネル | SD-WAN

インターフェイス	管理プロファイル	IP アドレス	仮想ルーター
vlan		none	none

Ethernet | VLAN | **ループバック** | トンネル | SD-WAN

インターフェイス	管理プロファイル	IP アドレス	仮想ルーター
loopback		none	none

Ethernet | VLAN | ループバック | **トンネル** | SD-WAN

インターフェイス	管理プロファイル	IP アドレス	仮想ルーター	セキュリティゾーン	機能	コメント
tunnel		none	none	none		
tunnel.1		none	default	Corp-VPN		

5-a. 検証結果 Interface

Map FTD Interface ⓘ

Source: Palo Alto Networks (8.0+)
Target FTD: CiscoFTD_v7.2.5

Refresh

PAN Interface Name	FTD Interface Name	Mapped Nameif
<input type="text"/>		
ethernet1/1	GigabitEthernet0/0 ▾	ethernet1_1
ethernet1/2	GigabitEthernet0/1 ▾	ethernet1_2
ethernet1/3	GigabitEthernet0/2 ▾	ethernet1_3

以下Interfaceが含まれていない

- VLAN Interface
- Loopback Interface
- Tunnel Interface

5-a. 検証結果 Security Rule

名前	送信元		宛先		アプリケーション	サービス	URL カテゴリ	アクション	プロファイル	オプション
	ゾーン	アドレス	ゾーン	アドレス						
1 External_Allow_Trusthost	Trust	Kali_TrustHost Win2012_DNS_Server	Internet Untrust	any	dns web-browsing	application-default	any	許可		
2 External_Allow_TrustHost_VPN	Trust	Kali_TrustHost Win2012_DNS_Server	Corp-VPN	any	dns web-browsing	application-default	any	許可	none	
3 External_Allow_UntrustHost	Untrust	172.20.79.1	Internet Trust	any	any	application-default	any	許可	none	
4 External_Allow_UntrustHost_VPN	Untrust	172.20.79.1	Corp-VPN	any	any	application-default	any	許可	none	
5 VPN-to-Untrust	Corp-VPN	any	Untrust	any	any	any	any	許可	none	
6 VPN-to-Trust	Corp-VPN	any	Trust	any	any	any	any	許可	none	
7 internal_allow	Internet	any	Trust	10.20.79.1	any	any	any	許可	none	
8 test_address_object	any	any	any	test	any	any	any	許可	none	
9 test_address_object_2	any	any	any	test2	any	any	any	許可	none	
10 All-Allow	any	any	any	any	any	any	any	許可	none	
11 untrust-to-dmz_001	Untrust	40.1.1.40/32	DMZ	172.15.7.51/32	any	UDP_4500	any	許可		
12 untrust-to-dmz_002	Untrust	40.1.1.40/32	DMZ	172.15.7.51/32	any	UDP_500	any	許可		

移行元で「application-default」を使用している場合は考慮が必要

5-a. 検証結果 Security Rule

Firewall Migration Tool (Version 6.0.1)

Source: Palo Alto Networks (8.0+)

Select Target ⓘ

Firewall Management >

FMC IP Address/Hostname/FQDN: 192.168.79.118

Choose FTD >

Selected FTD: CiscoFTD_v7.2.5

Select Features ▾

Device Configuration

- Interfaces
- Routes
- Site-to-Site VPN Tunnels (no data)
 - Policy Based (Unsupported) ⓘ
 - Route Based (VTI)

Shared Configuration

- Access Control
 - Migrate policies with Application-default as Enabled ⓘ
- NAT
- Network Objects
- Port Objects
- Remote Access VPN

Optimization

- Migrate Only Referenced Objects

Proceed

Back Next

無 : 「Disabled」 Ruleとして移行される
有 : Service 「Any」 として移行される

By default, policies with service as "application-default" will be migrated as service "Any". If this is not an acceptable behavior, uncheck the box. All policies with "application-default" will be migrated as "Disabled". Refer FMT User Guide for a workaround.

5-a. 検証結果 Security Rule

Firewall Migration Tool (Version 6.0.1)

Optimize, Review and Validate Configuration

Access Control | Objects | NAT | Interfaces | Routes | Site-to-Site VPN Tunnels | Remote A...

Select all 115 entries Selected: 0 / 115 Actions Save Search

■	#	Name	SOURCE			DESTINATION			Application	URLs	State	Action	TIME BASED Objects
			Zone	Network	Port	Zone	Network	Port					
<input type="checkbox"/>	1	External_Allow_Trust...	Inside_Zone	Kali_TrustHost,W...	ANY	Internet,Out...	ANY	ANY	HTTP, DNS	NA	✓ [icons]	Allow	None
<input type="checkbox"/>	2	External_Allow_Trust...	Inside_Zone	Kali_TrustHost,W...	ANY	Corp-VPN	ANY	ANY	HTTP, DNS	NA	✓ [icons]	Allow	None
<input type="checkbox"/>	3	External_Allow_Untr...	Outside_Zone	172.20.79.1	ANY	Internet,Insi...	ANY	ANY	ANY	NA	✓ [icons]	Allow	None
<input type="checkbox"/>	4	External_Allow_Untr...	Outside_Zone	172.20.79.1	ANY	Corp-VPN	ANY	ANY	ANY	NA	✓ [icons]	Allow	None
<input type="checkbox"/>	5	VPN-to-Untrust_#5	Corp-VPN	ANY	ANY	Outside_Zone	ANY	ANY	ANY	NA	✓ [icons]	Allow	None
<input type="checkbox"/>	6	VPN-to-Trust_#6	Corp-VPN	ANY	ANY	Inside_Zone	ANY	ANY	ANY	NA	✓ [icons]	Allow	None
<input type="checkbox"/>	7	internal_allow_#7	Internet	ANY	ANY	Inside_Zone	ANY	ANY	ANY	NA	✓ [icons]	Allow	None
<input type="checkbox"/>	8	test_address_object...	ANY	ANY	ANY	ANY	test	ANY	ANY	NA	✓ [icons]	Allow	None
<input type="checkbox"/>	9	test_address_object...	ANY	ANY	ANY	ANY	test2	ANY	ANY	NA	✓ [icons]	Allow	None

200 per page 1 to 115 of 115 Page 1 of 1

Optimize ACL (Beta) Validate

Application 「any」 / Service 「application-default」
→サポートされていないため、Disabledとして移行

Application 「xyz」 / Service 「application-default」
→Application 「xyz」 / Service 「any」 として移行

※application-defaultに関するFAQ
https://www.cisco.com/c/en/us/td/docs/security/firepower/migration-tool/migration-guide-pan/pan2threat-defense-with-the-migration-tool/m_migration_tool_faqs.html

5-a. 検証結果 RAVPN(Remote Access VPN)

 Firewall Migration Tool (Version 6.0.1) 🔔⁷ ? ⚙️ ↻

Optimize, Review and Validate Configuration ⓘ Source: Palo Alto Networks (8.0+)
Target FTD: CiscoFTD_v7.2.5

Access Control Objects NAT Interfaces Routes Site-to-Site VPN Tunnels ⓘ Remote Access VPN

Policy Assignment IKEV2 Connection Profile AnyConnect Packages ⓘ Trustpoints

Select all 1 entries Selected: 0 / 1 Actions ▾ Save ⌵

<input type="checkbox"/>	#.	Connection Profile Name	VPN Protocols	Targeted Devices	VPN Interface	Validation State
<input type="checkbox"/>	1	External-Gateway	SSL	CiscoFTD_v7.2.5	ethernet1_2	Will be created in FMC

50 ▾ per page 1 to 1 of 1 |< < Page of 1 > >|

Validate

5-a. 検証結果 RAVPN(Remote Access VPN)

Firewall Migration Tool (Version 6.0.1)

Optimize, Review and Validate Configuration ⓘ

Source: Palo Alto Networks (8.0+)
Target FTD: CiscoFTD_v7.2.5

Access Control Objects NAT Interfaces Routes Site-to-Site VPN Tunnels ⓘ Remote Access VPN

Policy Assignment IKEV2 Connection Profile ⓘ AnyConnect Packages ⓘ Trustpoints

AAA Address Pool Group-Policy

Select all 3 entries Selected: 0 / 3 Actions Save

#	Name	Type	IP address	Hostname/Domain/Entity ID ⓘ	AD Primary... ⓘ	Key/Passw... ⓘ	Certificate ⓘ	Validation State
1	migrationTestPr...	LOCAL_REALM	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Will be created in FMC
2	Auth-Profile01	AD(LDAPS)	10.20.79.10		tac-test		Not Applicable	Will be created in FMC
3	migrationtestGr...	LOCAL_USER	Not Applicable	Not Applicable	Not Applicable		Not Applicable	Will be created in FMC

50 per page 1 to 3 of 3 Page 1 of 1

Validate

移行元で設定済の場合においても手動で設定が必要となる

5-a. 検証結果 RAVPN(Remote Access VPN)

Firewall Migration Tool (Version 6.0.1)

Optimize, Review and Validate Configuration ⓘ

Access Control Objects NAT Interfaces Routes Site-to-Site VPN Tunnels ⓘ Remote Access VPN

Policy Assignment IKEV2 Connection Profile **AnyConnect Packages ⓘ** Trustpoints

Select all 1 entries Selected: 0 / 1 Actions Save Refresh

Search

#	RAVPN Feature	File Type	File Name (Source : FMC)	Validation State
1	Anyconnect Package	Anyconnect Client Image	<div style="border: 2px solid red; padding: 2px;">Select File anyconnect-linux64-4.10.08029-webdeploy-k9.pkg anyconnect-win-4.10.08029-webdeploy-k9.pkg</div>	Will be created in FMC

50 per page 1 to 1 of 1 Page 1 of 1

Validate

AnyConnectのPackagesを選択
事前にFMCにUploadしておく必要有

5-a. 検証結果 RAVPN(Remote Access VPN)

Firewall Migration Tool (Version 6.0.1)

Optimize, Review and Validate Configuration ⓘ

Source: Palo Alto Networks (8.0+)
Target FTD: CiscoFTD_v7.2.5

Access Control Objects NAT Interfaces Routes Site-to-Site VPN Tunnels ⓘ Remote Access VPN

Policy Assignment IKEV2 Connection Profile AnyConnect Packages ⓘ Trustpoints

Remote Access Interface SAML

Select all 1 entries Selected: 0 / 1 Actions Save

#	Certificate Type	Trustpoint (Certificate from Source Config)	Trustpoint (Requires Certificate from FMC)
1	SSL Global Identity Certificate	GP-External	

50 per page 1 to 1 of 1 Page 1 of 1

Validate

**FMCの証明書を選択
事前にFMC側で設定しておく必要有**

5-a. 検証結果（現時点では移行できなかった設定）

No.	移行元 (PaloAlto)	移行先 (FTD)	結果	備考
1	Interfece	Interfaces	○	物理インターフェースのみ対応
2	Zone	Security Zones	◎	
3	Static Routing	Static Routes	◎	
4	Dynamic Routes	Dynamic Routes	×	
5	Address Object	Network Objects	◎	
6	Service Object	Port Objects	◎	
7	Application ID	Applications	◎	
8	Security Policy	Security Rule	○	“application-default”使用時は考慮点有
9	NAT Policy	NAT Rule	◎	
10	Security Profile(Threat Prevention)	Intrusion Policy	×	セキュリティ機能は各社独自の為不可
11	GlobalProtect	Remote Access VPN	○	FMCでの事前準備が必要 Tunnel Interfaceは移行不可

◎：移行可能
○：移行可能
(考慮点有)
×：移行不可

- FMTでは移行対象外

参考 : PaloAlto側のマイグレーションツールであるExpeditionでも同様に移行対象外

仮想ルーター - default

Router Settings 有効化 デフォルトルートの拒否

スタティックルート ルーター ID 2.2.2.2

再配信プロファイル BFD None

RIP エリア | 認証プロファイル | ルールのエクスポート | 詳細

<input type="checkbox"/>	エリア ID	タイプ	範囲	インターフェイス
<input type="checkbox"/>	0.0.0.0	normal		ethernet1/1 ethernet1/2

マルチキャスト

+ 追加 - 削除

OK キャンセル

5-a. 検証結果 Dynamic Routes

- FMTでは移行対象外

参考 : PaloAlto側のマイグレーションツールであるExpeditionでも同様に移行対象外

Firewall Migration Tool (Version 6.0.1)

Optimize, Review and Validate Configuration ⓘ

Source: Palo Alto Networks (8.0+)
Target FTD: CiscoFTD_v7.2.5

Access Control Objects NAT Interfaces **Routes** Site-to-Site VPN Tunnels ⓘ Remote Access VPN

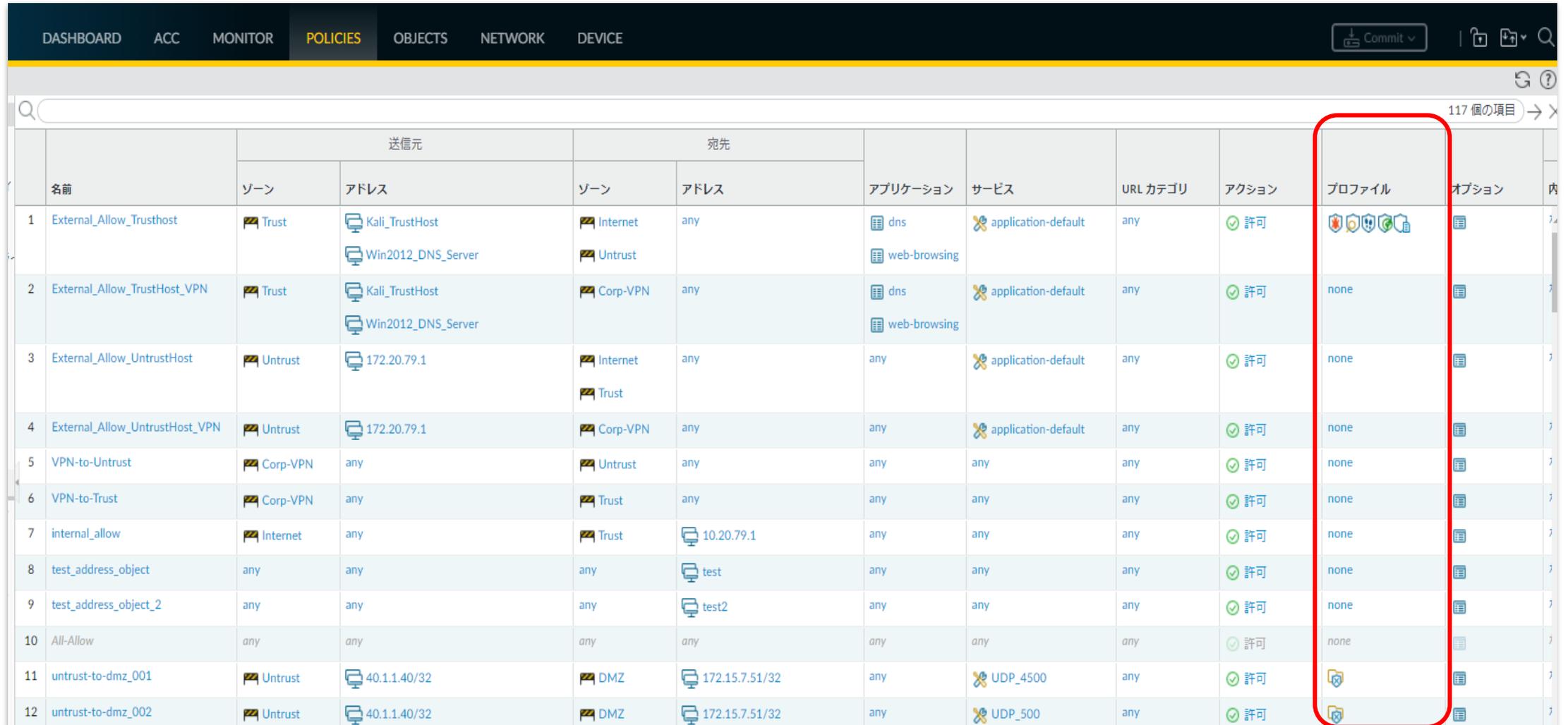
Select all 2 entries Selected: 0 / 2 Actions Save Search

#	Interface	IP Type	Network	Gateway
1	ethernet1_3	V4	0.0.0.0/0	192.168.79.254
2	ethernet1_3	V4	20.20.20.20	192.168.79.254

50 per page 1 to 2 of 2 Page 1 of 1 Validate

RoutesにDynamic Routesが追加されていないことを確認

5-a. 検証結果 Intrusion Policy



The screenshot shows a web-based interface for managing intrusion policies. The top navigation bar includes 'DASHBOARD', 'ACC', 'MONITOR', 'POLICIES', 'OBJECTS', 'NETWORK', and 'DEVICE'. A search bar and a 'Commit' button are also visible. The main content area displays a table with 12 rows of policy entries. The columns are: '名前' (Name), '送信元' (Source) with sub-columns 'ゾーン' (Zone) and 'アドレス' (Address), '宛先' (Destination) with sub-columns 'ゾーン' (Zone) and 'アドレス' (Address), 'アプリケーション' (Application), 'サービス' (Service), 'URL カテゴリ' (URL Category), 'アクション' (Action), 'プロファイル' (Profile), and 'オプション' (Options). The 'Profile' column for the last two rows (11 and 12) is highlighted with a red box.

名前	送信元		宛先		アプリケーション	サービス	URL カテゴリ	アクション	プロファイル	オプション
	ゾーン	アドレス	ゾーン	アドレス						
1 External_Allow_Trusthost	Trust	Kali_TrustHost Win2012_DNS_Server	Internet Untrust	any	dns web-browsing	application-default	any	許可		
2 External_Allow_TrustHost_VPN	Trust	Kali_TrustHost Win2012_DNS_Server	Corp-VPN	any	dns web-browsing	application-default	any	許可	none	
3 External_Allow_UntrustHost	Untrust	172.20.79.1	Internet Trust	any	any	application-default	any	許可	none	
4 External_Allow_UntrustHost_VPN	Untrust	172.20.79.1	Corp-VPN	any	any	application-default	any	許可	none	
5 VPN-to-Untrust	Corp-VPN	any	Untrust	any	any	any	any	許可	none	
6 VPN-to-Trust	Corp-VPN	any	Trust	any	any	any	any	許可	none	
7 internal_allow	Internet	any	Trust	10.20.79.1	any	any	any	許可	none	
8 test_address_object	any	any	any	test	any	any	any	許可	none	
9 test_address_object_2	any	any	any	test2	any	any	any	許可	none	
10 All-Allow	any	any	any	any	any	any	any	許可	none	
11 untrust-to-dmz_001	Untrust	40.1.1.40/32	DMZ	172.15.7.51/32	any	UDP_4500	any	許可		
12 untrust-to-dmz_002	Untrust	40.1.1.40/32	DMZ	172.15.7.51/32	any	UDP_500	any	許可		

5-a. 検証結果 Intrusion Policy

Firewall Migration Tool (Version 6.0.1)

Optimize, Review and Validate Configuration ⓘ

Access Control | Objects | NAT | Interfaces | Routes | Site-to-Site VPN Tunnels ⓘ | Remote Access VPN

Select all 115 entries Selected: 0 / 115 Actions ▾ Save

■	#	Name	SOURCE			DESTINATION			Application	URLs	Status	Action	TIME BASED
			Zone	Network	Port	Zone	Network	Port					Objects
<input type="checkbox"/>	1	External_Allow_Trust...	Inside_Zone	Kali_TrustHost,W...	ANY	Internet,Out...	ANY	ANY	HTTP, DNS	NA	✓	Allow	None
<input type="checkbox"/>	2	External_Allow_Trust...	Inside_Zone	Kali_TrustHost,W...	ANY	Corp-VPN	ANY	ANY	HTTP, DNS	NA	✓	Allow	None
<input type="checkbox"/>	3	External_Allow_Untr...	Outside_Zone	172.20.79.1	ANY	Internet,Insi...	ANY	ANY	ANY	NA	✓	Allow	None
<input type="checkbox"/>	4	External_Allow_Untr...	Outside_Zone	172.20.79.1	ANY	Corp-VPN	ANY	ANY	ANY	NA	✓	Allow	None
<input type="checkbox"/>	5	VPN-to-Untrust_#5	Corp-VPN	ANY	ANY	Outside_Zone	ANY	ANY	ANY	NA	✓	Allow	None
<input type="checkbox"/>	6	VPN-to-Trust_#6	Corp-VPN	ANY	ANY	Inside_Zone	ANY	ANY	ANY	NA	✓	Allow	None
<input type="checkbox"/>	7	internal_allow_#7	Internet	ANY	ANY	Inside_Zone	ANY	ANY	ANY	NA	✓	Allow	None
<input type="checkbox"/>	8	test_address_object...	ANY	ANY	ANY	ANY	test	ANY	ANY	NA	✓	Allow	None
<input type="checkbox"/>	9	test_address_object...	ANY	ANY	ANY	ANY	test2	ANY	ANY	NA	✓	Allow	None

200 per page 1 to 115 of 115 Page 1 of 1

Optimize ACL (Beta) Validate

Intrusion PolicyやFile Policyが移行されていないことが確認できる

5-a. 検証結果 Intrusion Policy

- FMTでは移行対象外
 - セキュリティ機能に関しては各ベンダーによって機能差分があるため慎重に行う必要有
- 参考：PaloAlto側のマイグレーションツールであるExpeditionでも同様に移行対象外

Security Ruleを選択することで、FMT上で一括設定変更が可能

設定可能な場合

設定不可能な場合

#	Name	Zone	Network	Port	Zone	Network	Port	Allow	Deny	Log	Count
1	External_Allow_Trusthost_#1	Internet,O...	ANY	ANY	Internet,O...	ANY	ANY	✓			2
2	External_Allow_TrustHost_VPN...	Corp-VPN	ANY	ANY	Corp-VPN	ANY	ANY	✓			1
3	External_Allow_UntrustHost_#3	Internet,In...	ANY	ANY	Internet,In...	ANY	ANY	✓			1
4	External_Allow_UntrustHost_V...	Corp-VPN	ANY	ANY	Corp-VPN	ANY	ANY	✓			1
5	VPN-to-Untrust_#5	Outside_Z...	ANY	ANY	Outside_Z...	ANY	ANY				1

Blocked
No File policy available on the FMC

5-b. 手動移行とFMT使用時の比較

- 今回は最も時間を要するSecurity Rule（計115件）の移行時間を比較
- Intrusion Policyはいずれも手動設定となるため対象外
- 移行の際は移行元のSecurity Policyを踏襲する
- Security Rule作成に伴う各種ObjectsやZones設定の作成時間は考慮範囲外

項目	手動移行	FMT使用時
設定方法	GUI ※CLIは非対応	GUI ※FMTのインストール有
事前準備	FTD + FMCの初期設定	+ FMTのインストール
総所要時間	約180分	約7分
備考	ObjectsやZonesを作成する必要有	7/17時点では軽微な不具合有 ※

※不具合に関してはTAC経由で不具合報告済

5-c. Optimize ACL(Beta)について

- 冗長なSecurity RuleやShadowルールを最適化可能な機能
- Optimize ACLを実行した段階で分析結果を表示
- 「移行せず削除」するか「無効化して移行」するか2通りのActionを実行可能

Overview: ACL Analysis

Total ACL rules - 115

- Disabled ACL rules - 1

ACL rules considered for optimization - 114

- Redundant ACL rules - 29
- Shadowed ACL rules - 7
- Unique ACL rules - 78

Note - Some ACLs may overlay between redundant and shadow rules, refer detailed excel reporting available under ACL optimization section.

Click on **Yes** to proceed ahead with ACL optimization.

(New Interface will provide the ability to Review, Select and Optimize the original ACL rules)

Yes **No**

移行元Ruleの
分析結果を表示

ACL Optimization(Beta)

Redundant ACLs Shadow ACLs

Select all 29 entries Selected: 29 / 29

Actions Save

	ACL Name	Zone	Network	Migration Actions	Destination	Port	Application	Status	Redundant to
<input checked="" type="checkbox"/>	dmz-to-untrust...	DMZ	172.15.7.5...	Do not migrate	netwc	udp:4500	AF		
<input checked="" type="checkbox"/>	dmz-to-untrust...	DMZ	172.15.7.5...	Migrate as disabled		udp:4500	AF		
<input checked="" type="checkbox"/>	dmz-to-untrust...	DMZ	172.15.7.5...			udp:4500	AF		dmz-to-untrust_001...
<input checked="" type="checkbox"/>	dmz-to-untrust...	DMZ	172.15.7.5...			udp:4500	ANY	✓	dmz-to-untrust_001...
<input checked="" type="checkbox"/>	dmz-to-untrust...	DMZ	172.15.7.5...			udp:4500	ANY	✓	dmz-to-untrust_001...
<input checked="" type="checkbox"/>	dmz-to-untrust...	DMZ	172.15.7.5...			udp:4500	ANY	✓	dmz-to-untrust_002...
<input checked="" type="checkbox"/>	dmz-to-untrust...	DMZ	172.15.7.5...			udp:500	ANY	✓	dmz-to-untrust_002...
<input checked="" type="checkbox"/>	dmz-to-untrust...	DMZ	172.15.7.5...			udp:500	ANY	✓	dmz-to-untrust_002...
<input checked="" type="checkbox"/>	dmz-to-untrust...	DMZ	172.15.7.5...			udp:500	ANY	✓	dmz-to-untrust_002...
<input checked="" type="checkbox"/>	dmz-to-untrust...	DMZ	172.15.7.5...			udp:500	ANY	✓	dmz-to-untrust_002...

50 per page 1 to 29 of 29 Page 1 of 1

Please click on [feedback](#) to provide inputs/suggestions on any aspect of feature relating to ACL Optimization, we'd love to hear it.

Download Report

Confirm Actions Cancel

移行せずに削除する

移行して無効化する

総括

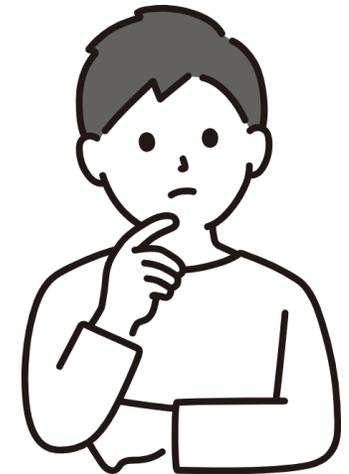
<良い点>

- ソフトウェア自体に堅牢性がある
 - 作業中断、長時間放置しても動作に支障がない
 - 作業中に前項目に戻っても入力内容が保持されている
- 本番環境での使用を考慮した設計になっている
 - Push前後でPDFのレポートが出力される
 - Push後にFMCで詳細内容を確認可能
- ツールを使用することによる人的ミスを防ぐことが可能
- 多量の設定が必要な項目において、大幅な工数削減が見込める



<気になる点>

- 通常のEthernetIF以外のインターフェイスが移行できない
- BGP/OSPF等のダイナミックルーティングに関する設定が移行できない
- RAVPNにおいて事前／事後にFMCの追加設定が必要

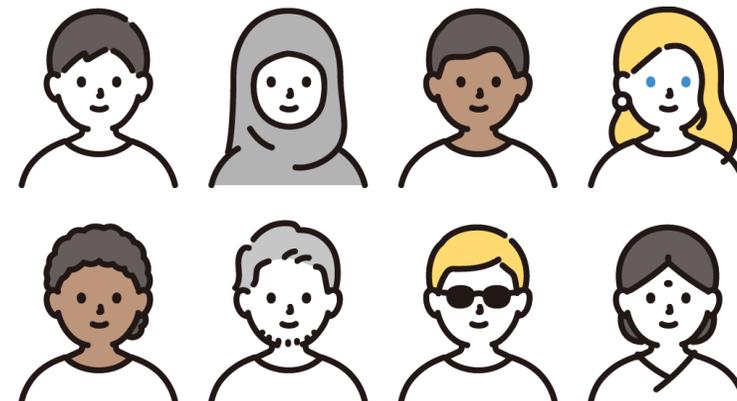


FMTの全世界統計データ（2023/6/9時点）

Total Download 50,000

Device Migration Success Rate 94%+

Net Promoter Score 60



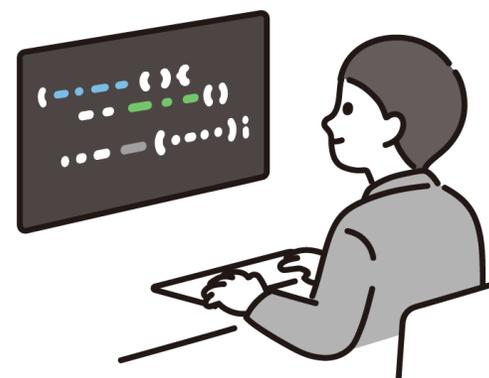
FMTのアップグレードサイクル

概ね2,3か月に一度最新バージョンがリリースされている

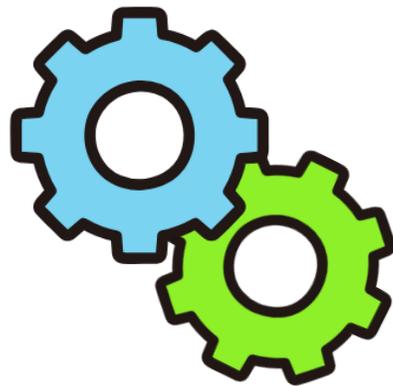
FMT 7.0.0 2024年7月

FMT 6.0.1 2024年5月

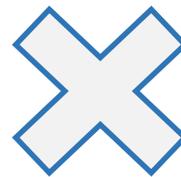
FMT 6.0.0 2024年2月



- ソフトウェア自体が使いやすい
- 移行前後のレポート機能で証跡管理
- 複数のSecurity Rule／各Objectsの移行が便利
- 2,3か月周期でアップデートされている
- 一部設定は移行未対応
- セキュリティ機能は手動移行を視野に
- 一部機能はFMCで追加設定が必要



Firewall Migration Tool



エンジニア

さいごに

7. ネットワークテスト自動化プロダクト「NEEDLEWORK」

FW/UTMのセキュリティポリシーのテスト等、
ネットワーク構築におけるテスト作業を自動化するプロダクトを提供

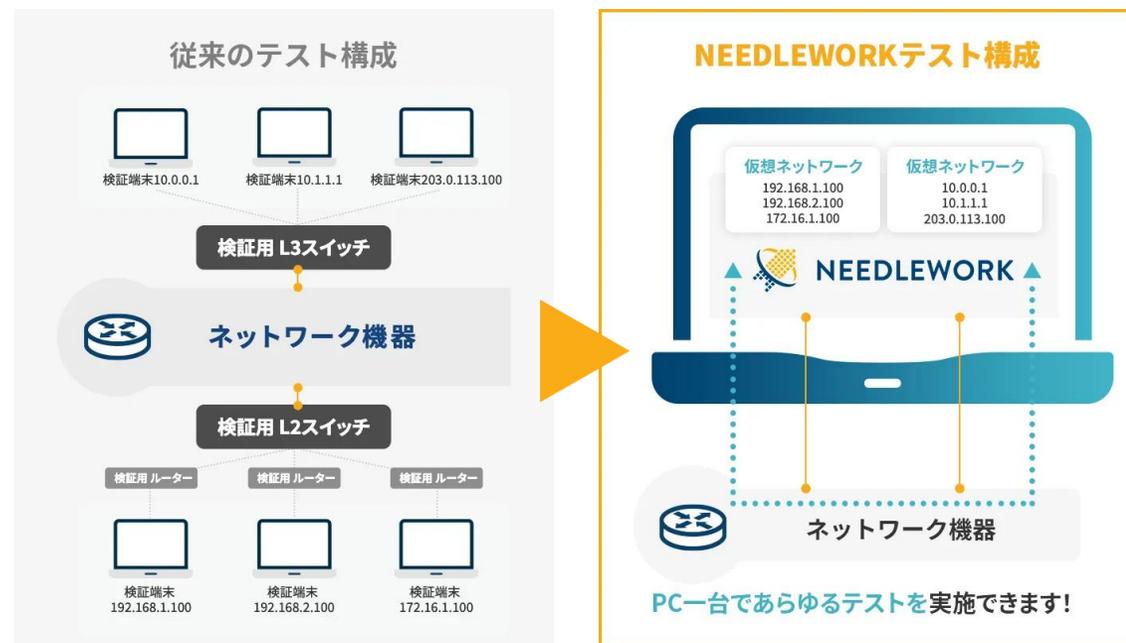


ネットワークインテグレータ様を中心に
94社 135ライセンスの導入実績

■主な機能

- FW/UTMのポリシー通信テスト自動化
- ネットワークの通信テスト (Ping/Traceroute) 自動化
- ネットワーク負荷テストを簡単に実施

特徴：仮想ネットワークを自動生成



InteropTokyo Best of Show Award

[セキュリティ部門]

ファイナリストにノミネートされました



InteropTokyo Best of Show Award

[テスティング部門]

ファイナリストにノミネートされました



無償ライセンス
発信中

NEEDLEWORK 公式Webサイト

<http://www.ap-com.co.jp/ja/needlework/>

7. ネットワーク自動化サービス

大手導入実績多数

Automation Coordinator

オートメーションコーディネーター

ネットワークにおける自動化の高度な課題を解決し

自動化のみならず、**攻めの業務**に取り組み始める体制の構築を

経験豊富なエンジニアチームが実現致します



Redhat社のAnsibleを用いた
ネットワーク自動化の導入とトレーニングを
組み合わせた自動化自律支援サービス



1, 自動化導入サービス

⇒ 自動化導入のスタートアップ



2, プロフェッショナルサービス

⇒ エンジニアが専属でコンサルティングや
高度な自動化導入を並走型で支援



3, クライアントワーク

⇒ お客様企業へリモートワークで常駐し
継続的な自動化推進支援



4, チケットサポート

⇒ チケット制のサポート契約、トラブルシ
ューティングや技術支援を提供



5, 自動化トレーニング

⇒ 個社向けに自動化研修を提供
個社別カリキュラムの作成も支援可能

エンジニアが自ら育てる自動化へ

私たちが最終的に目指すのは、ネットワーク運用の自動化をお客様自身で進めていただける状態です。

ベンダー主導ではなく、現場エンジニア主導の継続的改善サイクルを回せるようになることは、
ベンダー委託コストの削減だけではなく、現場エンジニアのモチベーション向上にもつながります。



PaloAltoチケットサービス

パロアルトネットワークス公認サービスプロバイダーによる

チケット型 技術支援サービス

for パロアルトネットワークス PA-Series

自動化支援サービス

大手導入実績多数

ITインフラ **自動化** 支援サービス



内製化支援サービス for Microsoft Azure

モノリシックからのリフト

マイグレーションサービス
for Microsoft

Azure
ADサーバ クラウド移行支援サービス

VDI/DaaSソリューション

クラウドネイティブへのシフト

クラウドネイティブ内製化支援サービス
for Microsoft Azure

「攻めのDX」内製化・準内製化人材
育成コンサルティングサービス

