



BIG-IP Access Policy manager (APM)

SSL VPNリモートアクセス・アクセス管理・認証基盤統合ソリューション



激変するユーザー環境に 最適なソリューションを提供するF5

アプリケーションのWeb化



71% の情報通信業界有識者が2020年までにほぼ全てのビジネスパーソンがweb/モバイル経由で業務に従事すると予測

スマートデバイスの爆発的増加



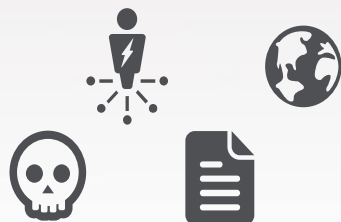
95% のビジネスパーソンが1台以上のモバイル機器を利用

1.3億の企業が2014年までにモバイル・アプリケーションを利用するようになる

進化し続ける外部脅威

58% のインターネット犯罪が思想・活動家の関与するもの

81% インターネット被害がハッカーに関連するもの



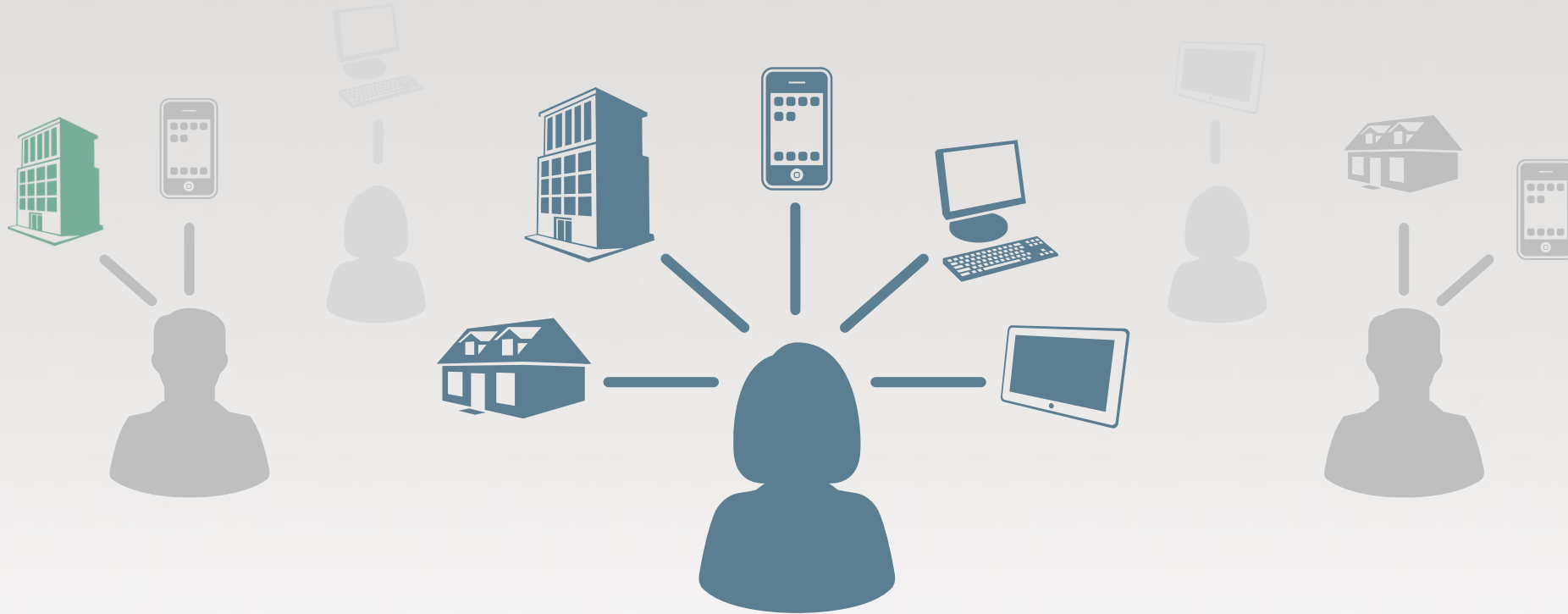
クラウドへの移行が加速

80% の新しいアプリケーションはクラウドベース

72% のCIOはアプリケーションをクラウドに移行・移行予定



ユーザが求めている事とは



エンドユーザは、どのようなアプリケーションに対しても、いつでも、どこでも、自由にアクセスできる事を求めている...

F5はアプリケーション、ユーザー・アクセス端末 情報への高度な可視化と管理性をご提供します

Users



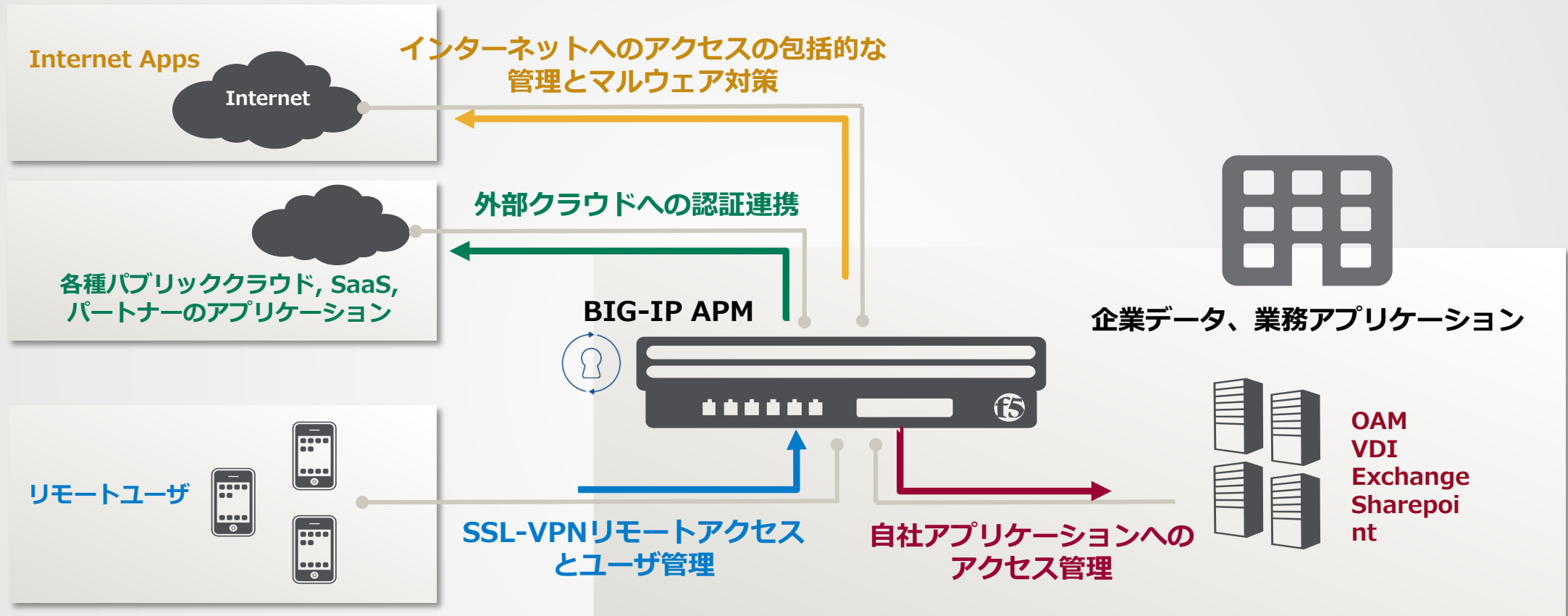
どこからのアクセスに対しても
セキュアな環境をご提供

Resources



ユーザーのアプリケーションを、
ロケーションを問わず守る

F5のアクセスセキュリティ、認証基盤連携



リモートアクセス、ユーザアクセス管理、シングルサインオン、フェデレーション。そして、ユーザデバイスからウェブアクセスまで全て一元管理。

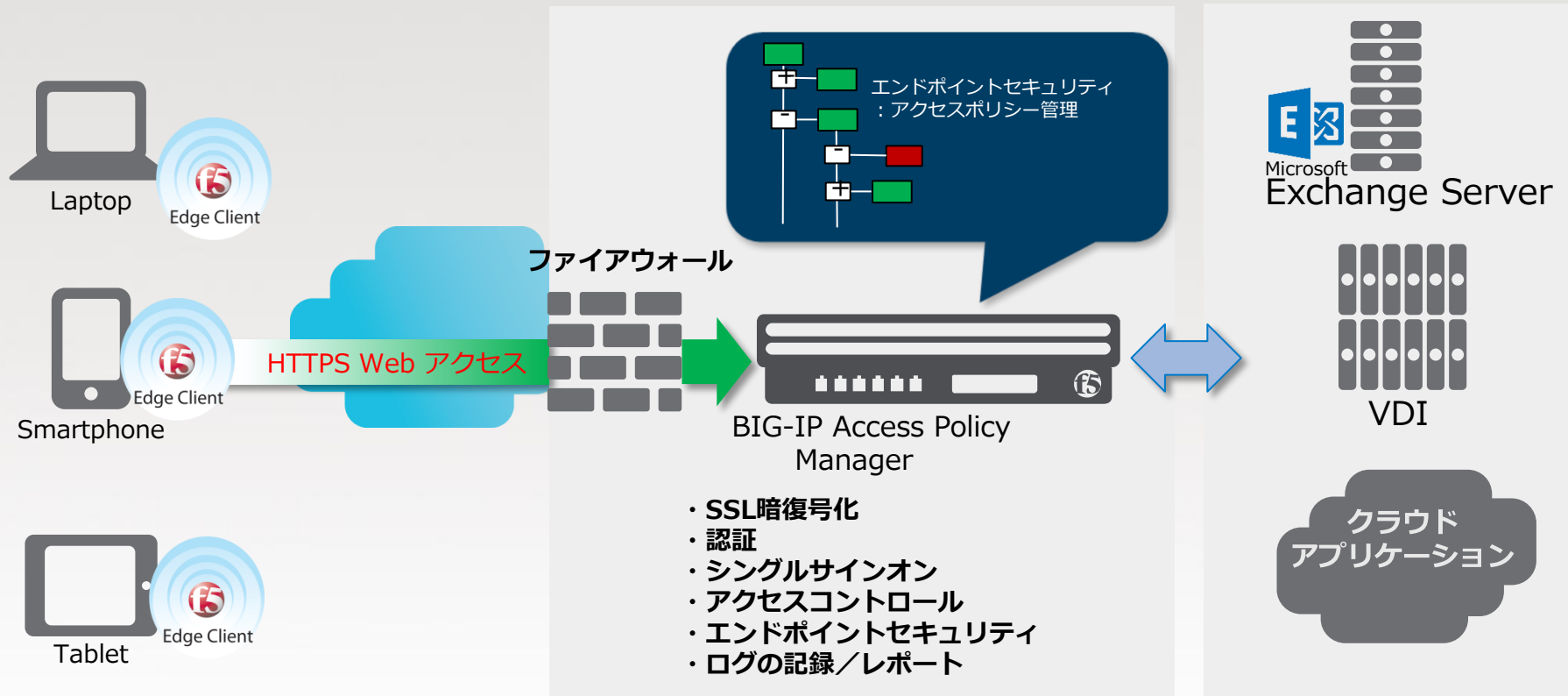
主要機能紹介



SSL-VPNによるセキュアなリモートアクセス

BIG-IP Access Policy Manager (APM)

- ✓ セキュリティポリシーは強制するが、ユーザビリティを損なわない
- ✓ 運用管理の負荷を低減



高いユーザビリティ/セキュリティ/運用管理性を実現

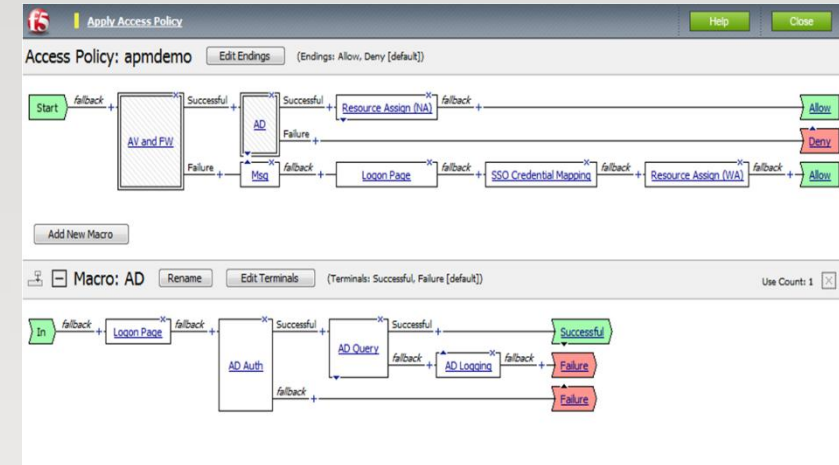


アクセス管理の統合

BIG-IP Access Policy Manager (APM)

BIG-IP® APM によるメリット:

- 最大10万ユーザという大規模環境にもアプライアンス一台で対応
- 認証基盤の統合、リモートアクセス、ウェブアクセス、アプリケーションへのアクセスを効率化



BIG-IP® APMの特徴:

- Webシングルサインオンおよび認証・アクセスコントロールサービスを中央で集中管理
- BIG-IPのスピードでのフルプロキシL4 – L7アクセス制御
- アクセスポリシーにエンドポイントチェックを追加
- ビジュアルポリシーエディタ (VPE)により、ポリシーベースのアクセスコントロールを提供
- VPEルール – カスタムのアクセスポリシーのためのプログラムインターフェース



エンドポイントのアクセスを制御

BIG-IP Access Policy Manager (APM)



許可、拒否、もしくは下記のようなエンドポイントの属性に基づいた制御を実施

- アンチウィルスソフトウェアのバージョンやアップデート状況
- ファイアウォールソフトウェアのステータス
- 特定アプリケーションのインストール
- 証明書の有無

非管理デバイスのために保護された仮想デスクトップ (Protected Work Space) を提供

- USBへアクセスを制限
- キャッシュクリーナーによる情報の消去
- マルウェアの進入を防御

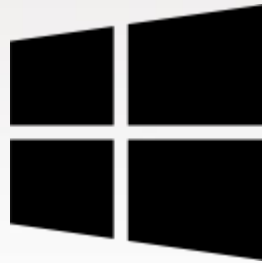
幅広い対応プラットフォーム

F5は、モバイルデバイスにおいてセキュアかつ高速にリモートアクセスを提供する唯一のADCベンダ

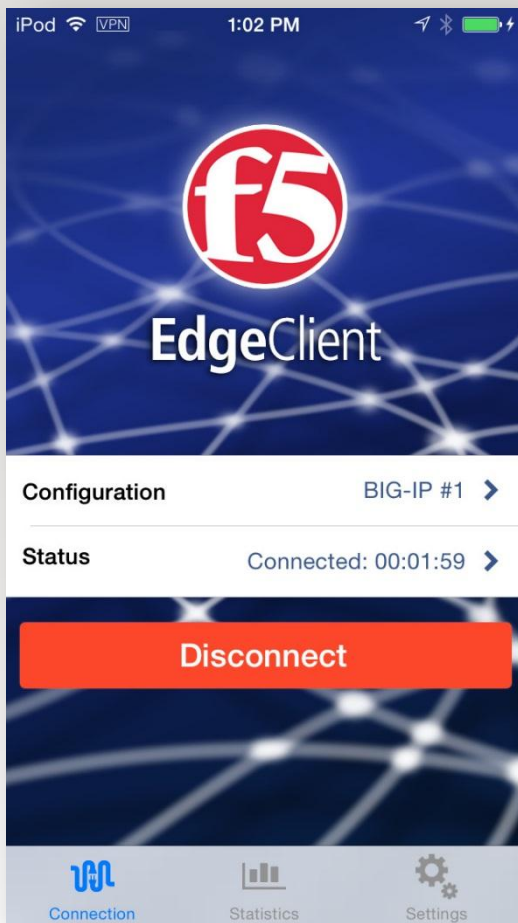
- モバイルデバイス



- Desktop/Laptop



🔒 専用クライアントアプリケーション



各種アプリケーションストア・マーケット
プレイスよりダウンロード可能



アプリケーションに簡単にアクセス

シングルサインオン (SSO)



Step 1
VPNへの認証

Step 2
アプリケーション起動

Step 3
アプリケーションの認証



BIG-IP APM



SharePoint
ORACLE®

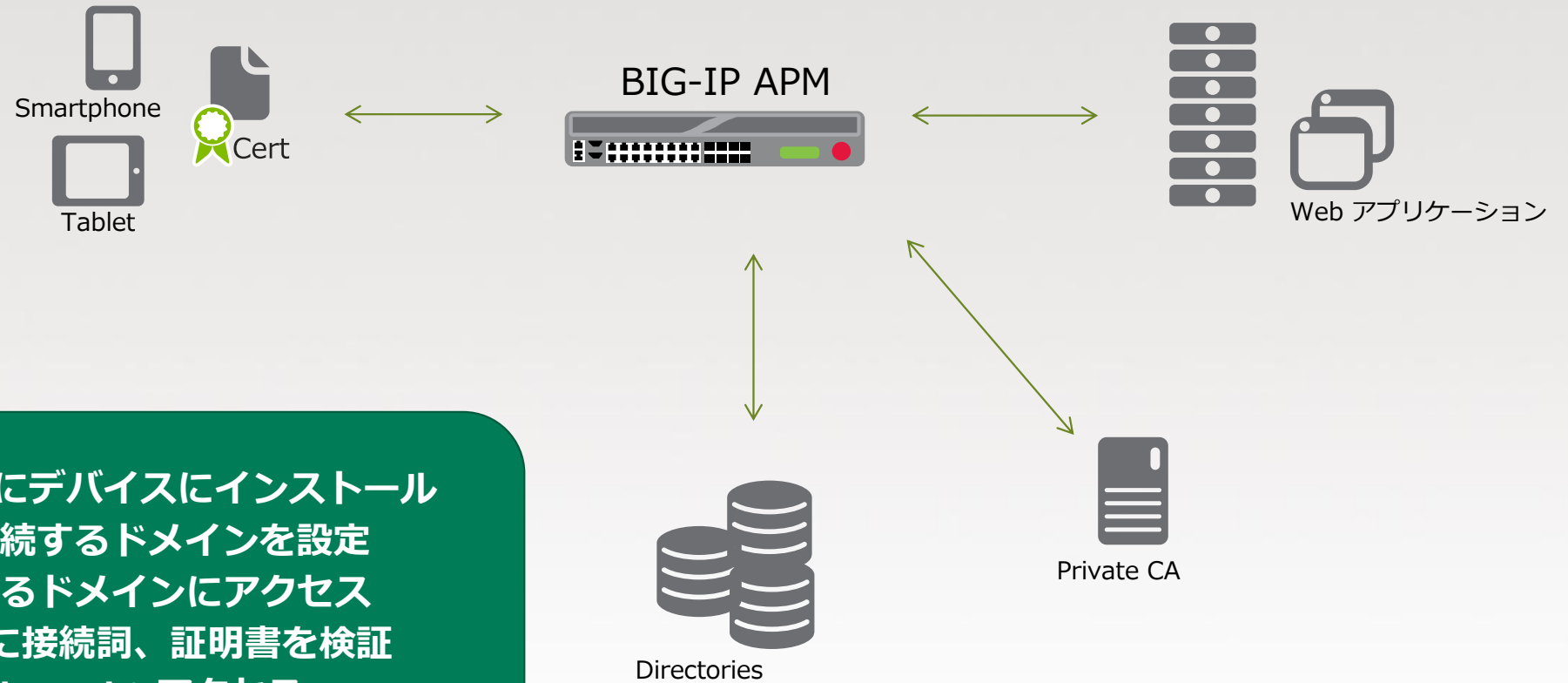
ビジネスアプリケーション

1ステップでアプリケーションへアクセス
アプリ自動起動+シングルサインオン



オンデマンド VPN

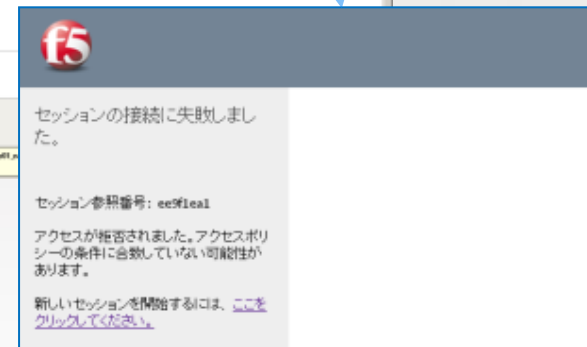
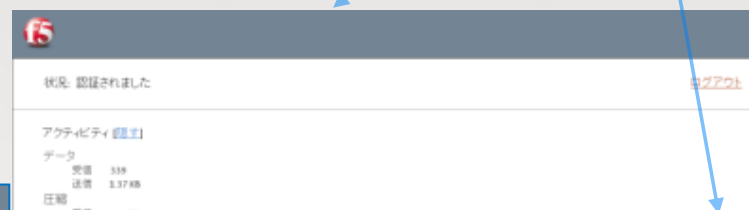
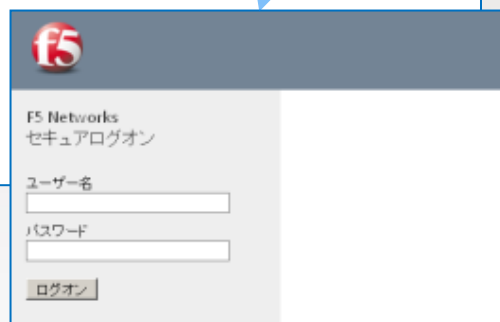
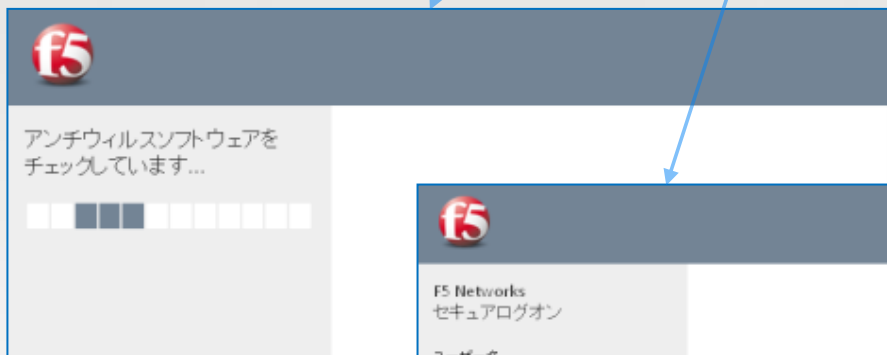
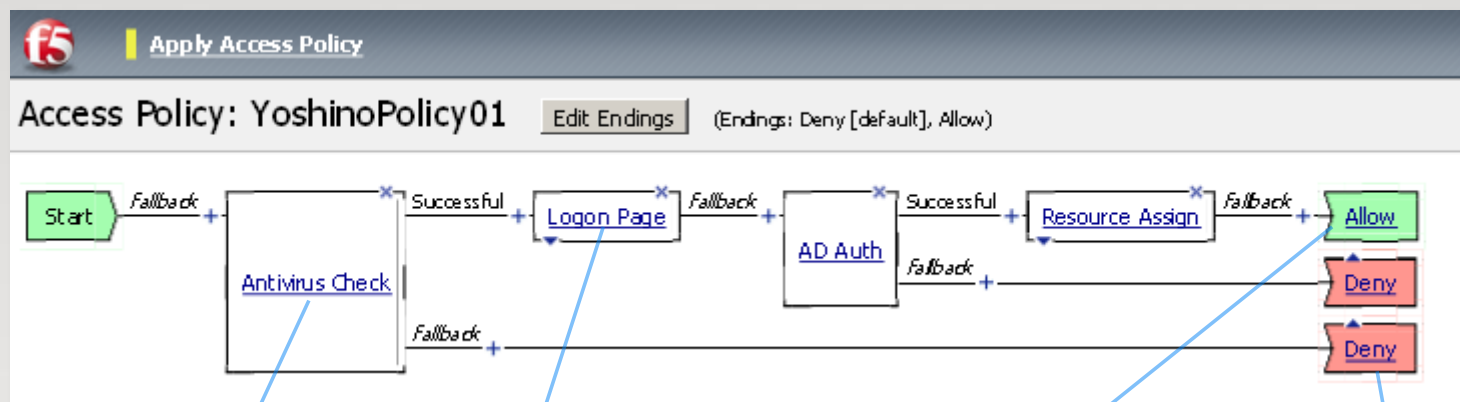
モバイルデバイスにクライアント証明書をインストールし、特定のドメインへのアクセスの場合自動的にVPN接続が可能。(iOSのみ)



1. ユーザは証明書を事前にデバイスにインストール
2. Edge ClientにVPN接続するドメインを設定
3. ユーザはVPN接続をするドメインにアクセス
4. 自動的にAPM/EDGEに接続詞、証明書を検証
5. 検証された場合のみIntranetへアクセス



強力かつ柔軟なセキュリティポリシー



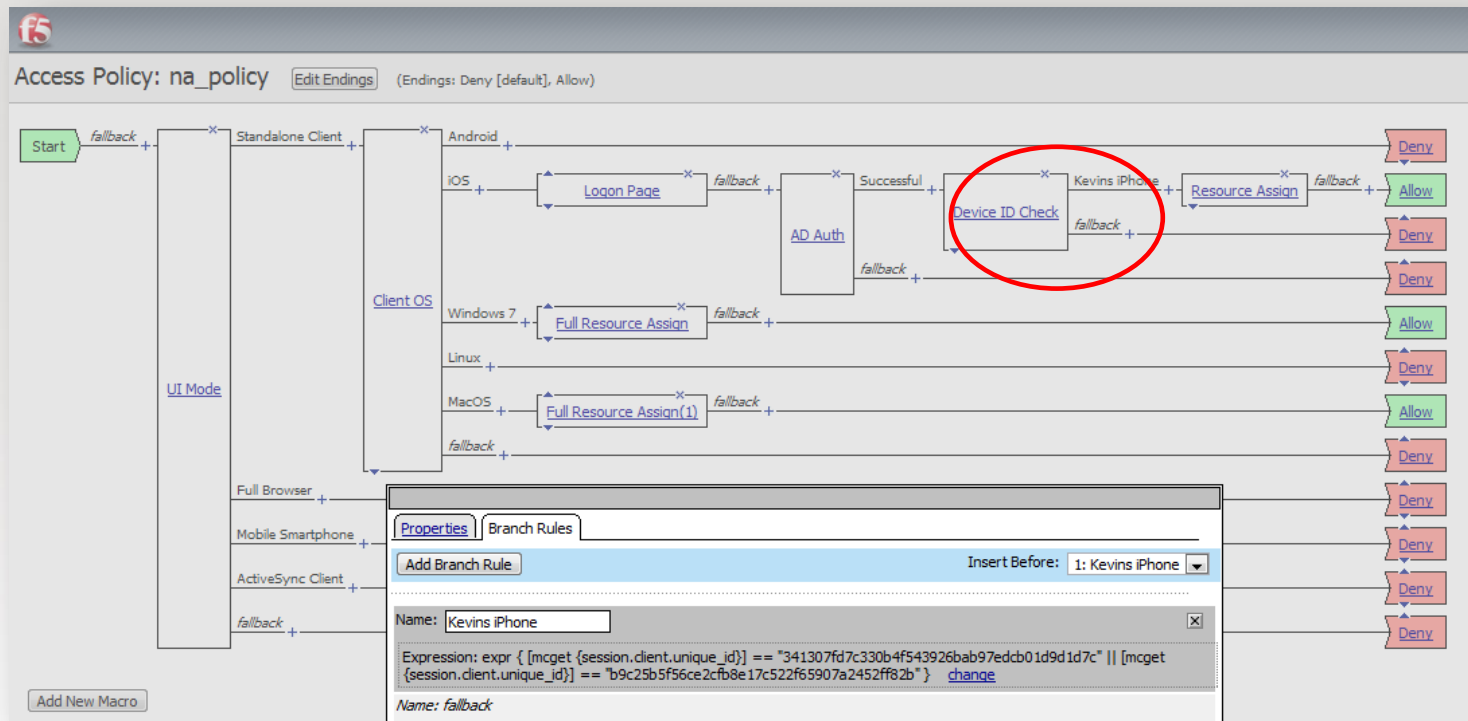
上記設定例：

接続 → クライアントのチェック → ログオン画面が現れ → AD認証 → SSL-VPN



IDと端末の紐付きを特定

- 誰が、いつ、どこから、どんな端末からアクセスしたのかを判定可能なポリシーエディタ
 - 利用者の状況に合わせたアクセスコントロールを柔軟に実現



例： Yamadaというアカウント名で、 iPad利用時に、
XXXXXというデバイスIDというアクセスでなければ拒否する



モバイルデバイスの識別

モバイルデバイスでは、デバイスのインスペクションができないため
クライアントソフトから取得できる情報が重要となる。

	例
<ul style="list-style-type: none">• iOS<ul style="list-style-type: none">• プラットフォーム情報• MACアドレス(WiFi)• モデル名• バージョン情報• ユニークID(UUID)	<p>iOS 90:21:55:07:4A:32 iPhone 4 4.3 8ccaf965e51e3077</p>
<ul style="list-style-type: none">• Android<ul style="list-style-type: none">• プラットフォーム情報• MACアドレス(WiFi)• モデル名• バージョン情報• ユニークID• シリアルナンバ• IMEI番号	<p>Android 90:21:55:07:4A:32 Galaxy Nexus 4.0.2 8ccaf965e51e3077 016BEB2097AF1456 354569041052233</p>



アクセスレポート機能による運用管理

充実で柔軟なレポート機能（認証失敗理由、ライセンス使用率など）

The screenshot displays the 'Reports Browser' interface with a table of session data and a detailed log view.

Local Time	Session ID	Logon	Active	State	Country	Continent	Virtual IP
2012-06-30 22:14:34	3B93E0EE	test1	N				172.28.15.134
2012-06-30 20:01:53	C3A37957	test1	N				172.28.15.134
2012-06-30 19:58:05	BC3BB988	test1	N				172.28.15.134
2012-06-30 19:56:25	43E3EBEB		N				
2012-06-30 19:53:38	870E15BA		N				
2012-06-30 19:50:24	234E7219		N				
2012-06-30 19:50:05	79B0E076	test1	N				
2012-06-30 19:46:04	6E46BDD7	test1	N				
2012-06-30 19:28:20	BF7F6530	test1	N				
2012-06-30 19:26:20	A06AFEA3		N				
2012-06-30 09:59:43	BD949573	test1	N				
2012-06-30 09:58:23	456F8D1F	test1	N				
2012-06-30 09:56:17	8C7AE476	test1	N				
2012-06-30 09:55:26	35C57FF6	test1	N				
2012-06-30 02:57:57	BE0B905A	test1	N				

Local Time	Log Message
2012-06-01 10:12:10	: Received User-Agent header: Mozilla%2f4.0%20(compatible%3b%20MSIE%208.0%3b%20Windows%...
2012-06-01 10:12:10	: Received client info - Type: IE Version: 8 Platform: Win7 CPU: WOW64 UI Mode: Full Javascript Support:...
2012-06-01 10:12:10	: New session from client IP 192.168.200.48 (ST=/CC=/C=) at VIP 172.28.15.139 Listener /Common/apm-vs
2012-06-01 10:12:15	: Username 'test2'
2012-06-01 10:12:15	: Logging Agent
2012-06-01 10:12:15	: session.radius.last.attr.class is 0x3737
2012-06-01 10:12:15	: session.radius.last.attr.filter-id is group2
2012-06-01 10:12:15	: session.radius.last.attr.framed-mtu is 1500
2012-06-01 10:12:15	: session.radius.last.attr.login-service is 0
2012-06-01 10:12:15	: session.radius.last.attr.service-type is 3
2012-06-01 10:12:15	: session.radius.last.errmsg is
2012-06-01 10:12:15	: session.radius.last.result is 1
2012-06-01 10:12:15	: Webtop /Common/full-wf assigned
2012-06-01 10:12:15	: Following rule 'fallback' from item 'Full Resource Assign(1)' to ending 'Allow'

クライアント証明書によるログの例

```

2012-06-26 04:28:09 : Following rule 'fallback' from item 'Logon Page' to item 'Client Cert Inspection(1)'
2012-06-26 04:28:09 : Following rule 'fallback' from item 'Client Cert Inspection(1)' to ending 'Deny'
2012-06-26 04:28:09 : Access policy result: Logon_Deny

```

ハイブリッドクラウド・アプリケーション 利用における課題

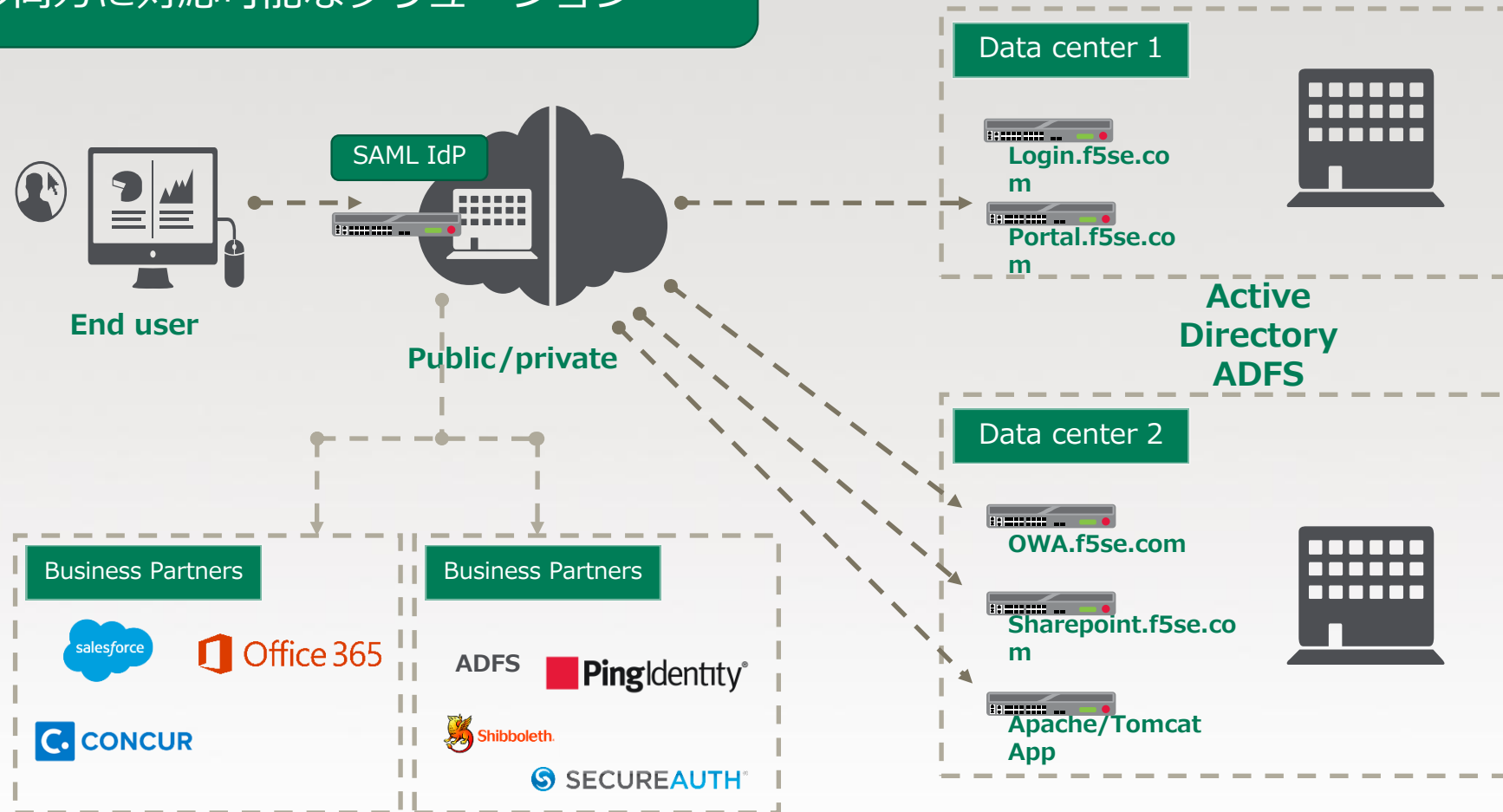
- ✓ Salesforceなどクラウドアプリケーションへのアカウント/アクセス管理の問題
- ✓ 企業買収やグループ企業などビジネス活動では統合されているが認証管理システムが追いついていけない
- ✓ アプリ毎の認証機能開発のコスト



SAML対応によるクラウド相互認証連携

クラウドや複数データセンター間連携を実現

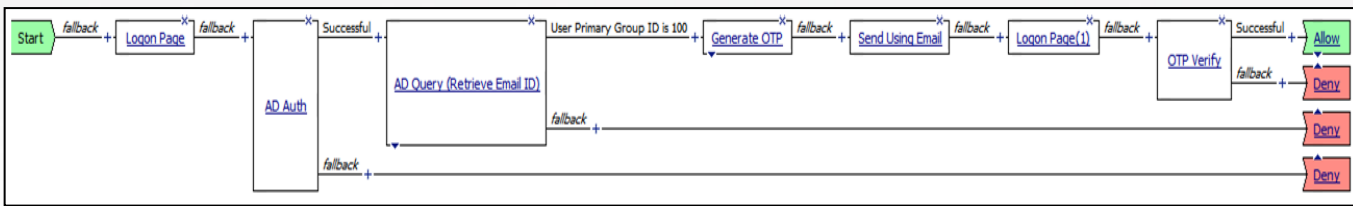
SAML 2.0に対応し、且つSPプロファイル及びIdPプロファイル両方に対応可能なソリューション





APM ワンタイムパスワード

- ワンタイムパスワードの精製・解読をサポート
 - パスワード長、タイムアウト値などは柔軟に設定可能
- OTPをEメール / SMSで送信
 - ユーザーEメール情報をAD queryから抽出
 - Eメール、SMS GatewayまたはHTTP認証と統合
- 認証失敗後の追加認証などの使用用途も有用



Properties Branch Rules	
Name:	OTP Generate
OTP Generate	
OTP length	6
OTP timeout in seconds	300



Solutions for an application world.