

# BIG-IP LTM+APM PCoIP Proxy

BIG-IP Version 11.4.1

VM Horizon View 5.2

iApp Template:F5.vmware\_view.v1.0.0rc4

2014/2/5



*Networld*

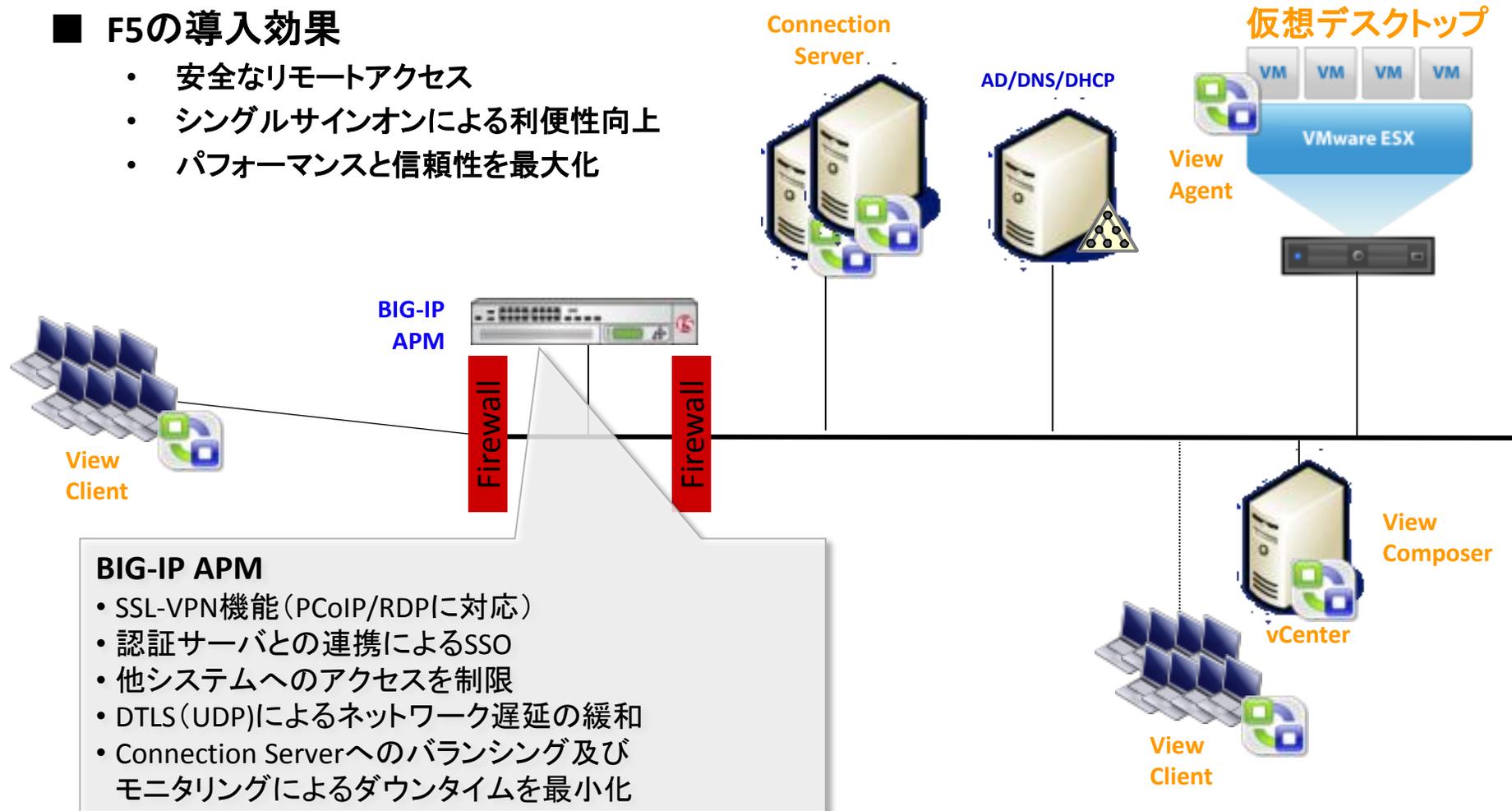
# 安全で便利なVDIの実現

## ■ 課題

- ・ 社外ネットワークからのアクセスに制限
- ・ 認証回数の増加によるユーザの手間
- ・ 遅延によるサービスレベルの低下

## ■ F5の導入効果

- ・ 安全なリモートアクセス
- ・ シングルサインオンによる利便性向上
- ・ パフォーマンスと信頼性を最大化



# PCoIP Proxy

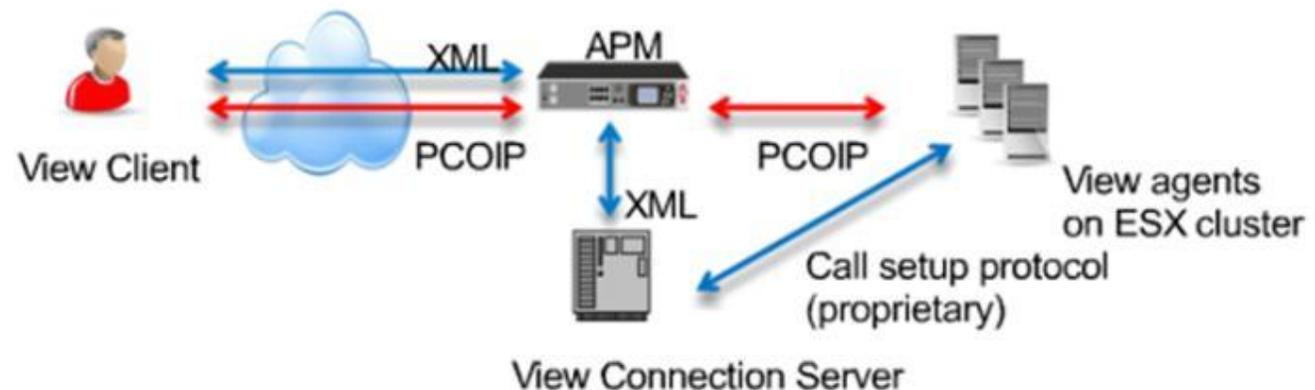
Industry first to offer full proxy support for PCoIP

PC-over-IP (PCoIP) をフルプロキシするPCoIP Proxy機能を実装し、VMware Horizon View アーキテクチャをシンプルに構成しセキュリティとスケーラビリティの向上を実現

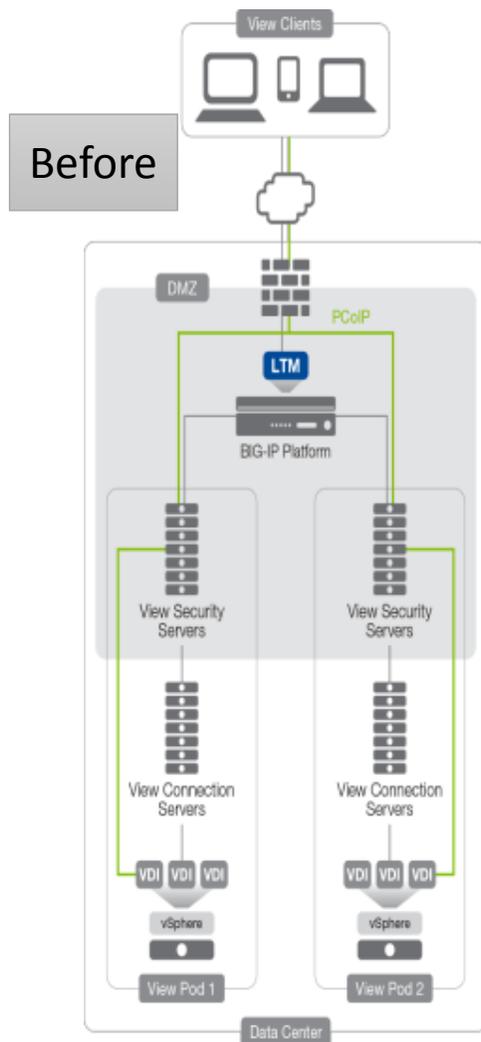
## キーポイント

- PC-over-IPプロトコルをフルプロキシサポート
- VMware Horizon View アーキテクチャをシンプルに
- セキュリティ強化とスケーラビリティに貢献
- 業界で最初の機能実装
- 他のVDI接続もサポート

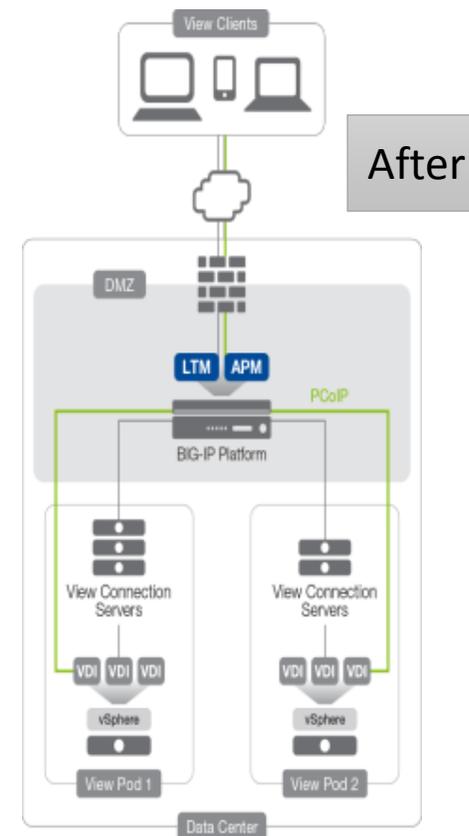
・ **注意事項**  
RDPプロトコル  
USBリダイレクト  
Blast  
はPCoIPでは利用できない



# PCoIP Proxy – Simplify Your Architecture



- F5 Access Policy Manager (APM) でPCoIP プロキシを実現
- 1対1の設置が必要だったSecurityサーバとConnectionサーバのひも付きを分離
- ICSA Labs認定取得のハイパフォーマンスアクセスセキュリティ
- アプリケーション、ロケーションを問わないユニファイドグローバルアクセス



# iApp テンプレートのインポート

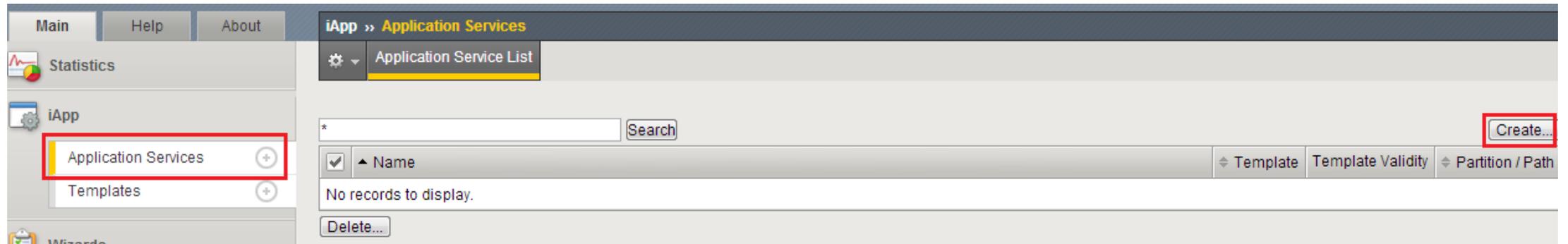
<input type="checkbox"/>	Name	Validity	Associated Application Services	Verification	Certificate	System-supplied	Partition / Path
<input type="checkbox"/>	f5.oracle_as_10g			F5 Verified	f5-irule	Yes	Common
<input type="checkbox"/>	f5.oracle_ebs			F5 Verified	f5-irule	Yes	Common
<input type="checkbox"/>	f5.peoplesoft_9			F5 Verified	f5-irule	Yes	Common
<input type="checkbox"/>	f5.radius			F5 Verified	f5-irule	Yes	Common
<input type="checkbox"/>	f5.replication			F5 Verified	f5-irule	Yes	Common
<input type="checkbox"/>	f5.sap_enterprise_portal			F5 Verified	f5-irule	Yes	Common
<input type="checkbox"/>	f5.sap_erp			F5 Verified	f5-irule	Yes	Common
<input type="checkbox"/>	f5.vmware_view			F5 Verified	f5-irule	Yes	Common
<input checked="" type="checkbox"/>	f5.vmware_view.v1.0.0rc4			None			Common
<input type="checkbox"/>	f5.vmware_vmotion			F5 Verified	f5-irule	Yes	Common

F5 DevCentralからiApp Template f5.vmware\_view.v1.0.0rc4をダウンロードしインポート

<https://devcentral.f5.com/>

本iAppはLTMモジュールが必須

# iApp テンプレートから設定



iApp Application ServicesからCreateをクリック

# iApp テンプレートから設定

iApp >> Application Services >>

Template Selection: Basic

Name	<input type="text"/>
Template	f5.vmware_view.v1.0.0rc4

Welcome to the iApp template for VMware View 5.0 and 5.1, and Horizon View 5.2

NAMEにポリシー名を入力  
Templateのプルダウンメニューからf5.vmware\_view.v1.0.0rc4を選択

Check for updates	<a href="https://devcentral.f5.com/wiki/iApp.VMware-Applications.ashx">https://devcentral.f5.com/wiki/iApp.VMware-Applications.ashx</a> .
Software Support	While this iApp template officially supports only View 5.0 and 5.1, and Horizon View 5.2, you can use it with View 4.6 with no modifications.
Prerequisites	Before using this iApp you must ensure that the following prerequisites are met:  The View environment must be fully configured and tested to verify clients are able to access the available Desktops via each Connection or Security Server that will be a part of this deployment.  Ensure that your Active Directory server is properly configured and all View Clients have the appropriate credentials to access the View environment.  Ensure that DNS and NTP servers are properly configured on the BIG-IP system. See the deployment guide or BIG-IP documentation for instructions
Additional features available	If you plan on using this template to configure the BIG-IP system for processing encrypted web traffic (HTTPS), you need to import an SSL certificate and key that correspond to all fully-qualified DNS names that you are using for the HTTPS traffic. Importing SSL certificates and keys is not a part of this template; see Local Traffic >> SSL Certificate List.  You do not currently have the BIG-IP Application Visibility Reporting Module (AVR) provisioned on the BIG-IP system. Provisioning AVR (also called Analytics) provides rich application statistics and reporting for your application deployments.

# iApp テンプレートから設定

Template Options	
Do you want to see inline help?	Show inline help text
	This template offers extensive inline assistance, notes, and configuration tips. We strongly recommend reading the inline help presented in the template until you are familiar with the functionality and implications of the deployment options. Important notes are always shown no matter which selection you make here.
Which configuration mode do you want to use?	Basic - use F5's recommended settings
	This template supports two configuration modes. Basic mode automatically configures many options, such as load balancing method or profile types, on the BIG-IP system using F5 recommended settings without user intervention. Advanced mode allows you to review and edit the F5 recommended settings before configuring the system.
BIG-IP Access Policy Manager	
Do you want to deploy BIG-IP Access Policy Manager?	Yes, deploy BIG-IP Access Policy Manager
NOTE	You can use the BIG-IP Access Policy Manager (APM) as a full PCoIP secure gateway proxy, or a DTLS Network Access VPN. Deploying BIG-IP APM as a full PCoIP proxy requires the View Clients to be using Horizon View 5.2 or later and the BIG-IP system must be running version 11.4 or later.
	You must have fully licensed the BIG-IP APM to use the APM features in this template.
How should the BIG-IP system	
Support RSA SecurID two-factor authentication?	No, do not support RSA SecurID two-factor authentication
IMPORTANT	You must have an existing SecurID AAA Server object on this BIG-IP APM to support RSA SecurID two-factor authentication.
	Choosing Yes enables support for two-factor authentication using SecurID. You must have already created a SecurID AAA Server object prior to configuring this portion of the iApp. Creating an AAA Server object for SecurID is not a part of this template, see Access Policy > AAA Servers > SecurID. Choosing No disables the ability to authenticate via SecurID.

Do you want to deploy BIG-IP Access Policy Manager?のプルダウンメニューから  
Yes, deploy BIG-IP Access Policy Managerを選択

# iApp テンプレートから設定

Should the BIG-IP system show a message to View users during logon?	<input type="text" value="No, do not add a message during logon"/>	View Clientでアクセス時に指定したメッセージを表示可能。 ただし今回は設定しない
	The BIG-IP system can display a message to users during the logon process. The BIG-IP APM refers to this as a 'Disclaimer' message. Select whether you want to display a disclaimer message to users during logon.	
What is your public-facing IP address?	<input type="text"/>	Firewall等でGlobalIPアドレスとPrivateIPアドレスをNATされている場合GlobalIPアドレスを入力
	You may not be translating your public address, however, if you are, enter the public NAT IP address View Clients resolve to for initial connections.	
What is the NetBIOS domain name for your environment?	<input type="text"/>	
	Specify the NetBIOS domains for this View environment. For example, if the FQDN is 'my.example.com', the NetBIOS domain is 'my'. If you have multiple domains, enter each domain separated by a space. The Active Directory servers you are using for authentication (that you will specify later) need to trust all the domains you enter here.	
Create a new AAA Server object or select an existing one?	<input type="text" value="Create a new AAA Server object"/>	
Which Active Directory servers (IP and host name) are used for user credential authentication?	Host name <input type="text"/> IP <input type="text"/> <input type="button" value="X"/>	
	<input type="button" value="Add"/>	
	Specify each of your Active Directory domain controllers, both FQDN and associated IP address, used for this View environment. Click the Add button for additional rows.	
What is your Active Directory domain name?	<input type="text"/>	
	Specify the fully qualified domain name (FQDN) used for this View environment, for example, my.example.com	

NetBIOSやActiveDirectory関連の設定を入力  
既に登録されている場合はプルダウンメニューから指定可能

Create a new monitor for the Active Directory servers?	<input type="text" value="Yes, create a simple ICMP monitor"/>
--	--

# iApp テンプレートから設定

SSL Encryption	
How should the BIG-IP system handle encrypted traffic?	Terminate SSL for clients, re-encrypt to View servers (SSL bridging) ▼
	SSL is a cryptographic protocol used to secure client to server communications. Select how you want the BIG-IP system to handle encrypted traffic.
	If your environment requires clients use SSL and session persistence (which ensures requests from a single user are always distributed to the

Connection Serverがデフォルトhttpsで処理となるため、SSL bridgingを指定

	system uses the SSL ID or Client/Server IP to enforce session persistence. Because these parameters are less granular, you may experience inconsistent distribution of client requests.
Which SSL certificate do you want to use?	default.crt ▼
	To establish encrypted communication, a client and server negotiate security parameters that are used for the session. As part of this handshake, a certificate is provided by the server to the client to identify itself. The client can then validate the certificate with an authority for authenticity before sending data. When the BIG-IP system is decrypting communication between the client and server, an SSL certificate and key pair for each fully-qualified DNS name related to this application instance must be configured on the system.
	Select the SSL certificate you imported for this deployment. Importing certificates and keys is not a part of this template, see Local Traffic >> SSL Certificate List. To select any new certificates and keys you import, you need to restart or reconfigure this template.
Which SSL private key do you want to use?	default.key ▼
	Select the associated SSL key.
CRITICAL	You have selected a default BIG-IP certificate and/or key. This application service configuration is incomplete and will not be secure until you import and assign a trusted certificate and key that are valid for all fully qualified domain names used to access the application. See Local Traffic >> SSL Certificate List for importing certificates and keys. To select any new certificates and keys you import, you need to restart or reconfigure this template.

# iApp テンプレートから設定

Virtual Servers and Pools	
What IP address do you want to use for the virtual server?	<input type="text"/>
	This IP address, combined with the port you specify below, becomes the BIG-IP virtual server address and port, which clients use to access the application. The system intercepts requests to this IP:Port and distributes them to the View servers. If you are using BIG-IP APM, this is the address to which the BIG-IP APM sends traffic after authenticating it.
What is the associated service port?	<input type="text" value="443"/>
	Specify the service port you want to use for the virtual server. The default value displayed here is based your answer to the question asking how the system should handle SSL traffic.
	Because you are using BIG-IP APM, the BIG-IP APM first authenticates the user, and then uses this virtual server address to transparently connect the user to the View environment.
What FQDN will clients use to access the View environment?	<input type="text"/>
	The FQDN entered here will be used by the View Client to resolve to the virtual IP entered above.
Which servers should be included in this pool?	Node/IP address: <input type="text"/> Port: <input type="text" value="443"/> Conn limit: <input type="text" value="0"/> <input type="button" value="X"/>
	<input type="button" value="Add"/>
	Specify the IP address(es) of your View servers. If you have multiple servers, you can enter multiple addresses. Depending on your previous selections, you may be able to use a range of addresses.
Client Optimization	
Which HTTP compression profile do you want to use?	<input type="text" value="Use F5's recommended compression profile"/>
	Compression improves performance and end user experience for Web applications that suffer from WAN latency and throughput bottlenecks. Compression reduces the amount of traffic sent to the client to complete a transaction.
Application Health	
Create a new health monitor or use an existing one?	<input type="text" value="https"/>

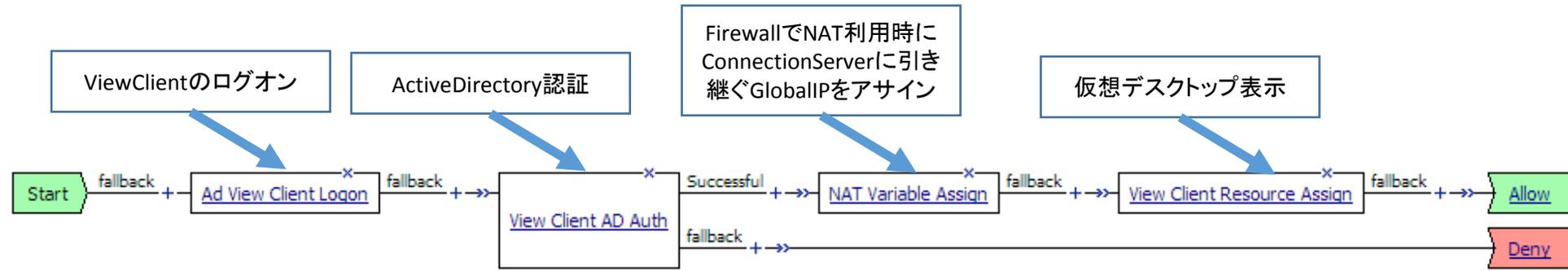
Virtual ServerのIPアドレスを入力

Virtual ServerのFQDNを入力

Connection ServerのIPアドレスを入力

Connection Serverのヘルスチェックを設定

# 仮想デスクトップ表示までのシーケンス



# Connection Server設定



対象のConnection ServerのView接続サーバ設定を編集で  
本項目のすべてのチェックボックスを外す

# Virtual Server

Local Traffic » Virtual Servers : Virtual Server List

Virtual Server List | Virtual Address List | Statistics

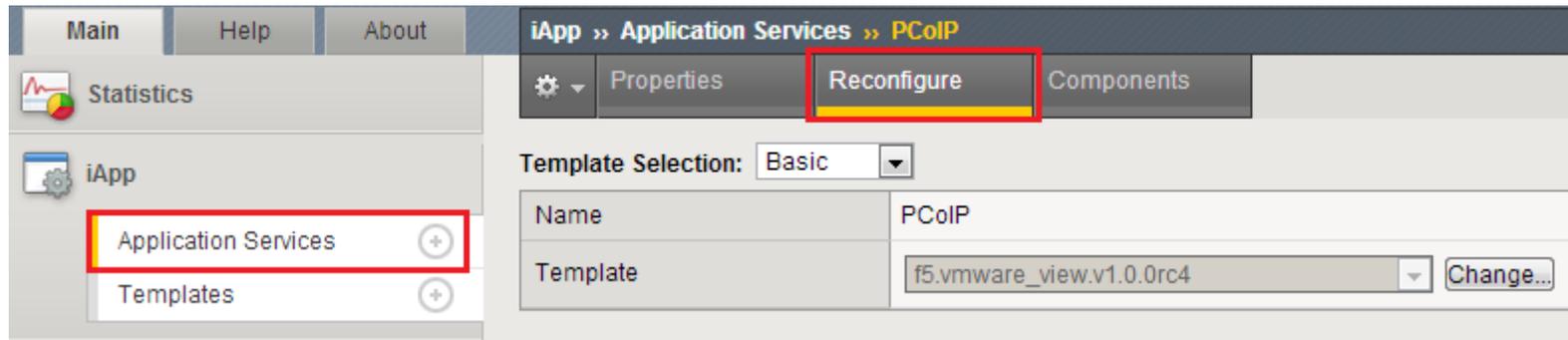
\*  Search

<input checked="" type="checkbox"/>	Status	Name	Application	Destination	Service Port	Type	Resources	Partition / Path
<input type="checkbox"/>		PCoIP_apm_redirect	PCoIP	10.21.1.171	80 (HTTP)	Standard	<a href="#">Edit...</a>	Common/PCoIP.app
<input type="checkbox"/>		PCoIP_pcoip_udp	PCoIP	10.21.1.171	4172	Standard	<a href="#">Edit...</a>	Common/PCoIP.app
<input type="checkbox"/>		PCoIP_proxy_https	PCoIP	10.21.1.171	443 (HTTPS)	Standard	<a href="#">Edit...</a>	Common/PCoIP.app

Connectionサーバアクセス用 on port 443  
(アクセスポリシーやSSL処理のプロファイルを関連付けます)  
PCoIPアクセス用 on port 4172  
port 80はport 443リダイレクト用

# Appendix 1

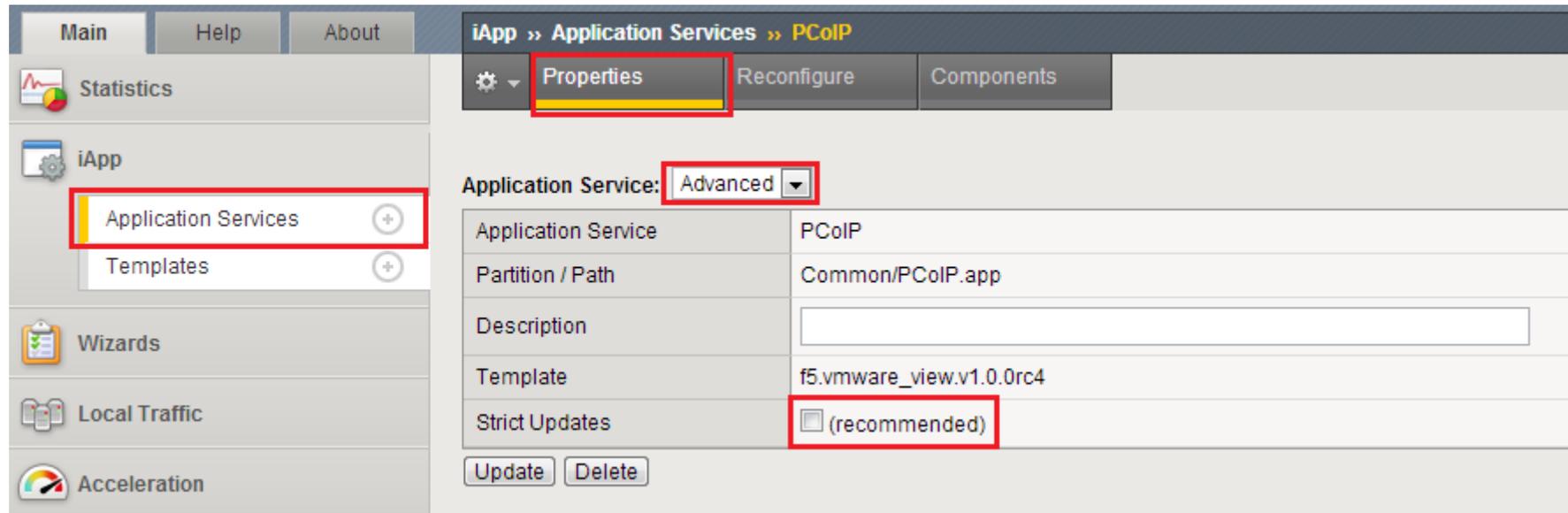
## (iAppテンプレート設定後の再設定)



iAppにて設定した内容で再設定を行う場合はReconfigureから設定

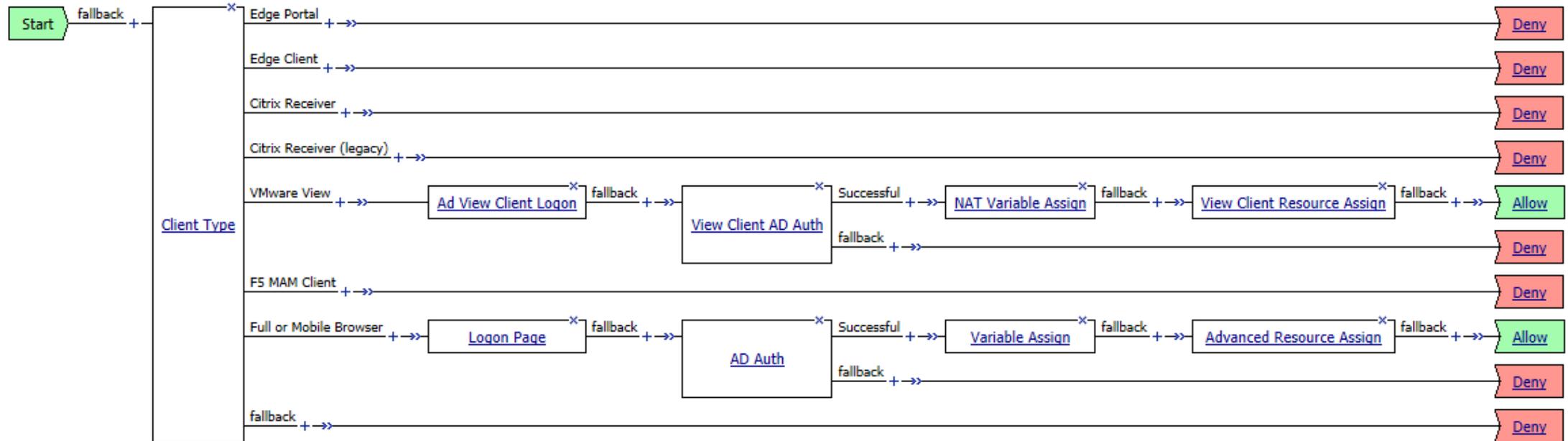
# Appendix2

## (iAppテンプレート設定後のパラメータ調整)



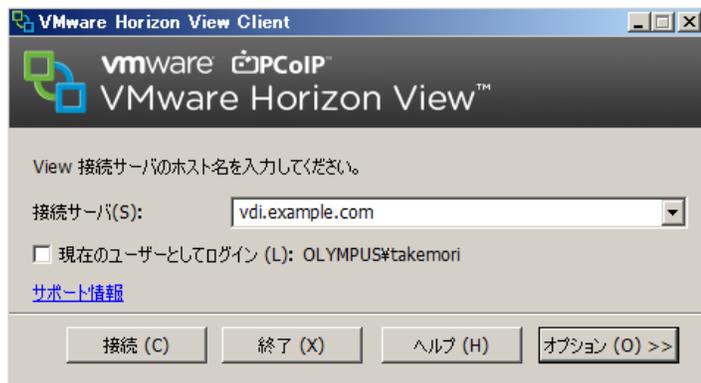
iAppを使用して設定した場合、デフォルトではパラメータ等はiAppからのみの変更となるが Strict Updatesのチェックボックスを外すとパラメータを個別に変更可能  
ただし、Reconfigureから設定を行うと上書きされる為、注意が必要。

# Appendix3-1(ブラウザからのアクセス)

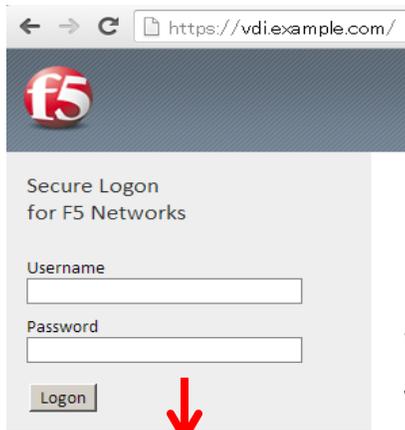


ViewClientからのアクセスとシーケンスを分けることでブラウザからアクセスさせることも可能  
ブラウザからアクセスする場合はEdgeClient動作可能端末であればエンドポイントチェックが可能

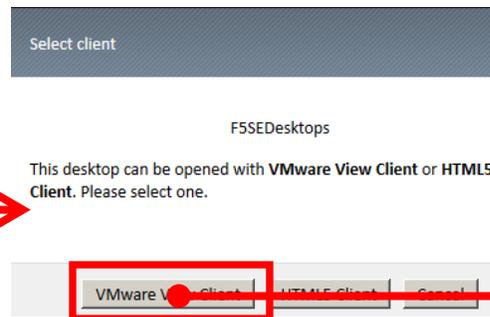
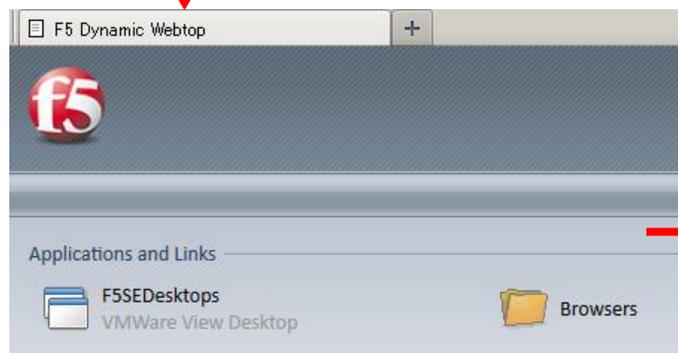
# Appendix3-2(ブラウザからのアクセス)



Viewクライアントから  
そのままアクセス



もしくは、ブラウザでログオン後、  
Webtopのリンクをクリックして  
Viewクライアント起動

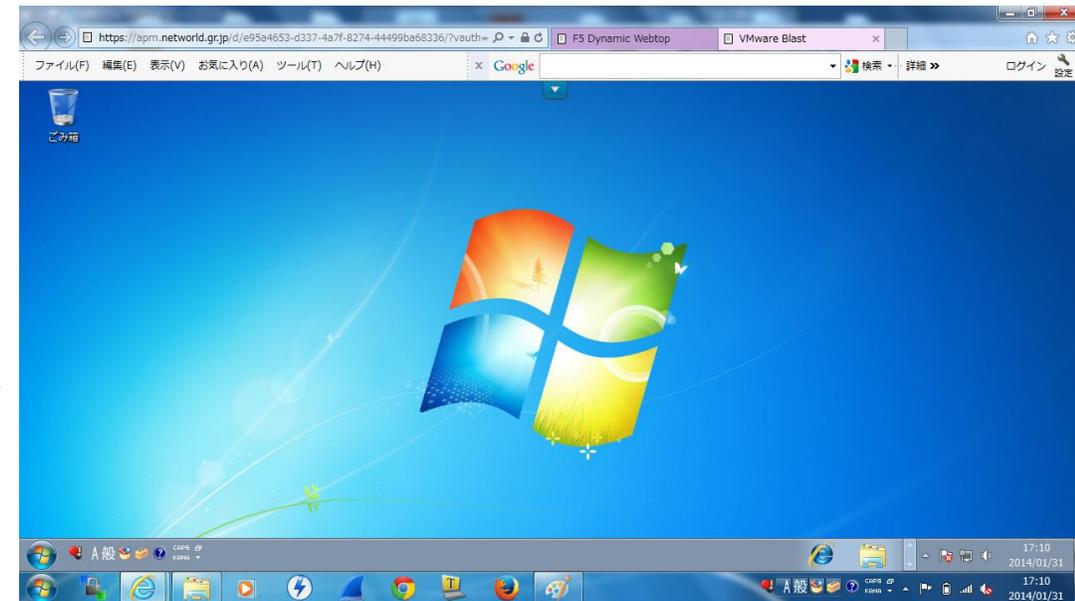
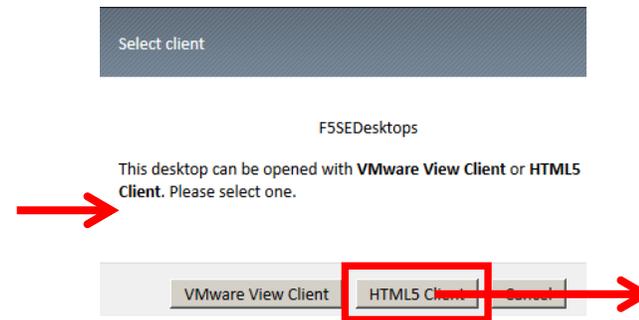
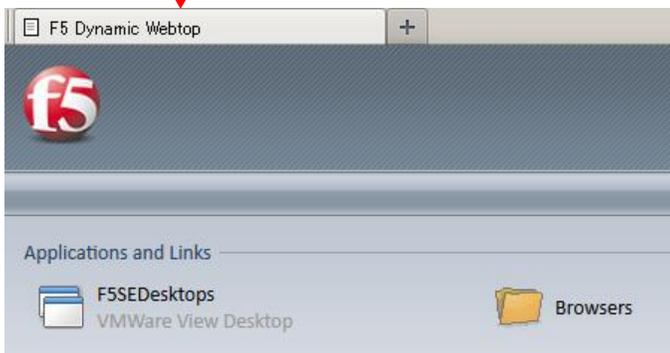


# Appendix3-3(HTML5対応ブラウザからのアクセス)

1. 11.4.1HF2にてHorizon View デスクトップへのHTMLアクセスに対応(HTML5対応ブラウザのみ)
2. Horizon View Client、BIG-IP Edgeclientのインストール不要でデスクトップにアクセス可能
3. PCoIP Proxyでは無い為、SSL処理をBIG-IP/View Connection Serverにて実施する必要あり、BIG-IPではバックエンドSSLも必要
4. TCPベースの通信となり暗号化もPCoIPでは無い為、速度はPCoIPの方が高いと思われる



HTML5対応ブラウザでログオン後、  
Webtopのリンクをクリック



BIG-IP Version 11.4.1HF2

VM Horizon View 5.3

iApp Template:F5.vmware\_view.v1.0.0rc7

にて確認

設定はAppendix3-1と同じ

# Appendix4(同時接続ユーザライセンス)

PCoIP proxyの場合、App tunnelでは無く、Remote Desktopという部類に分けられます。Remote DesktopではCCU(同時接続ユーザ)ライセンスは不要となります。  
※11.4～

- 11.4でCCUが必要な項目は、
  1. Full Network Access(SSL-VPN)
  2. App Tunnel
  3. Portal Access(Reverse proxy)
    - Web-based app link (OWA,SharePoint,XenApp等)
    - Citrix portal modeの3つとなります。



# Appendix5(最大同時セッション数)

CCU(同時ユーザ)ライセンスは不要だが、筐体により  
最大同時セッション数が異なるため考慮する必要がある

## ハードモデルでの目安

500セッションまで: BIG-IP 2000

5000セッションまで: BIG-IP 2200

## VE版の目安

200セッションまで: 200Mbps

1000セッションまで: 1Gbps

1000セッション以上: 3 or 5Gbps

最大2500セッション

※他モジュールと組み合わせる場合は性能劣化に注意

