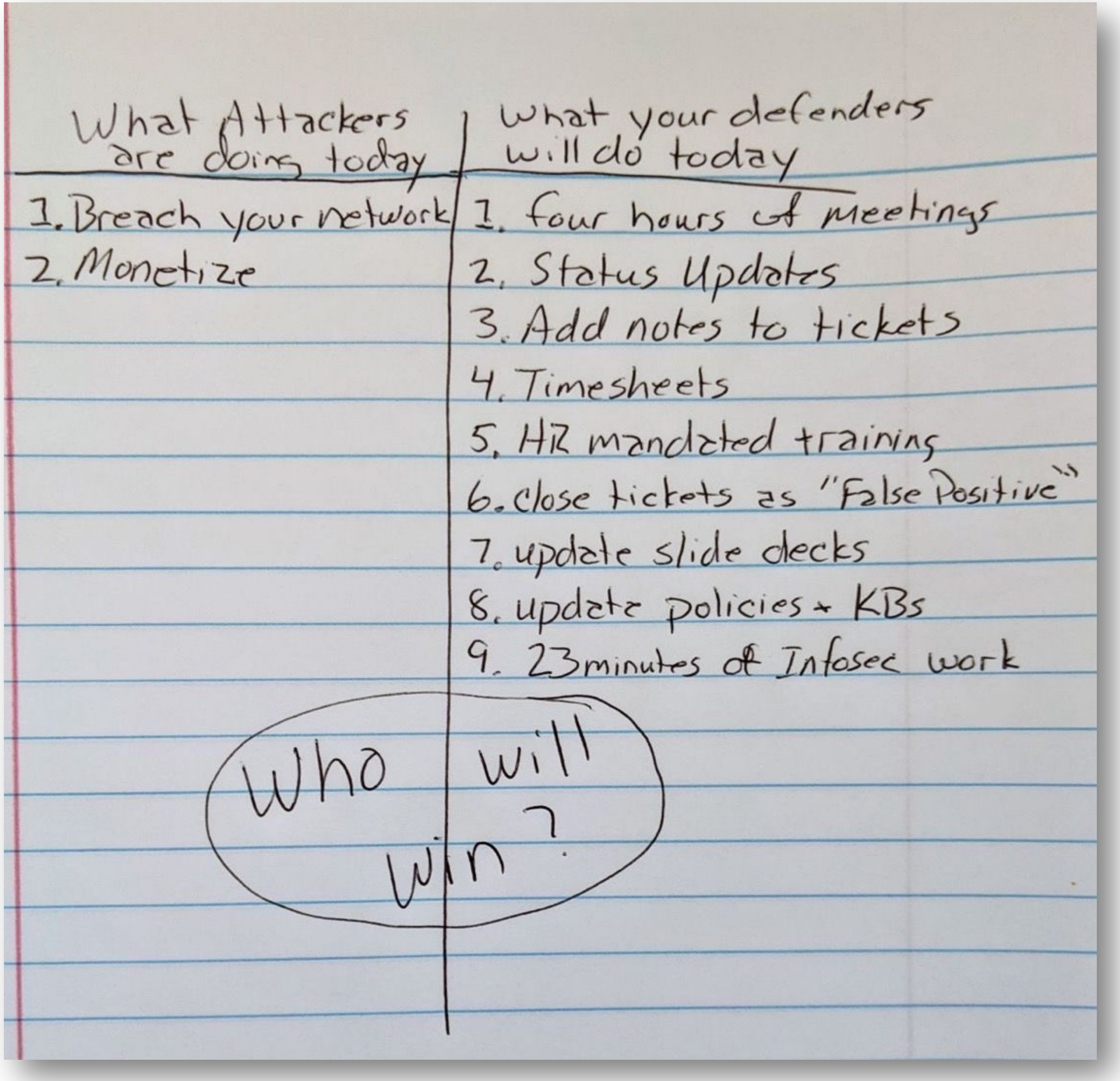
F5 APM

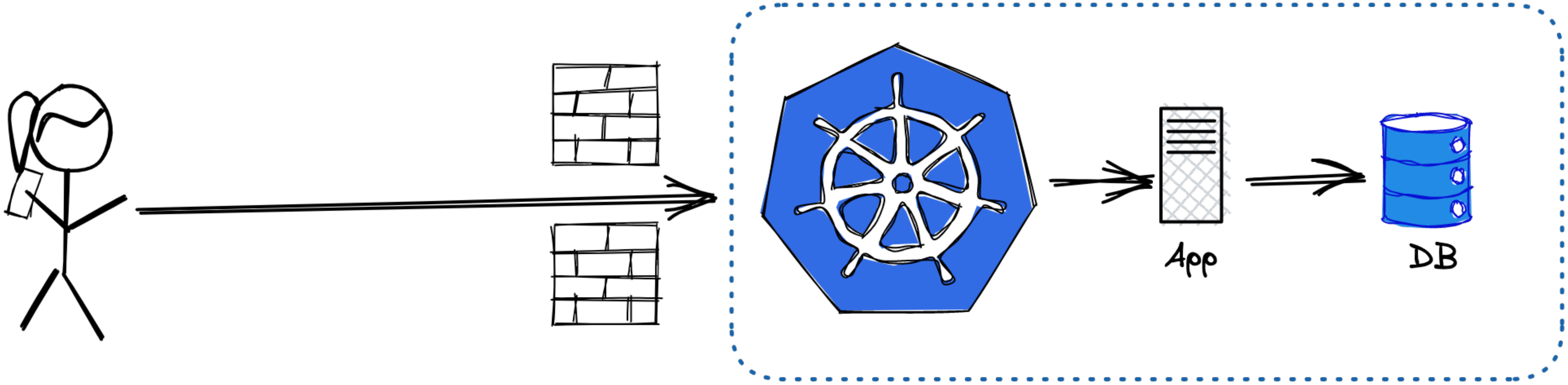
Univerzálny a bezpečný prístup k aplikáciám

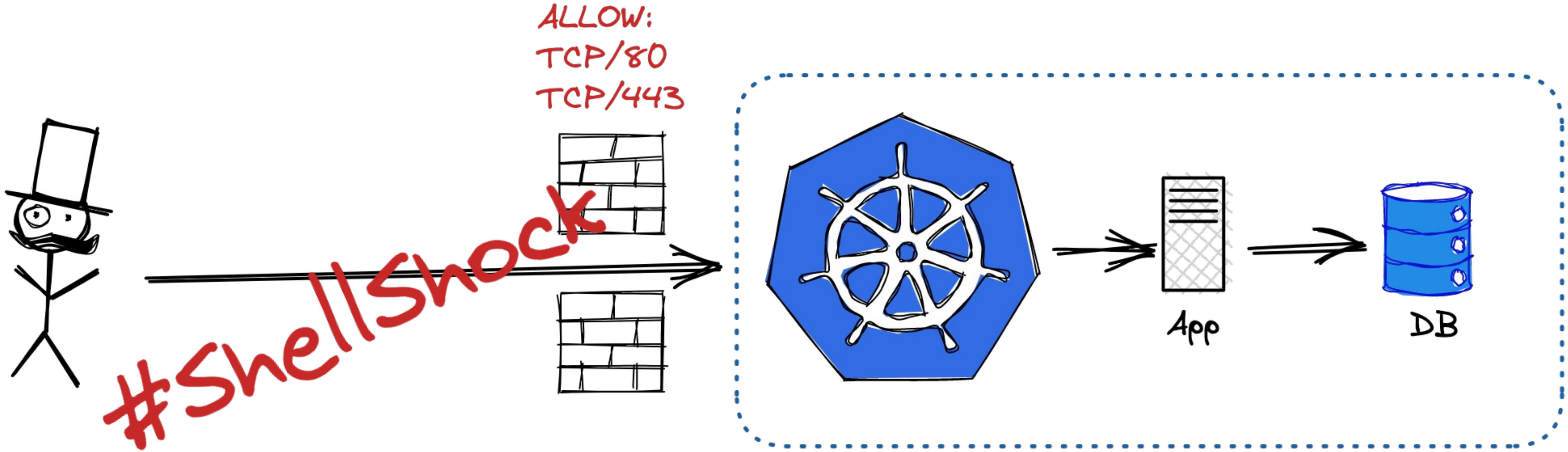
Luboš Klokner | F5 | Sr. Solution Engineer

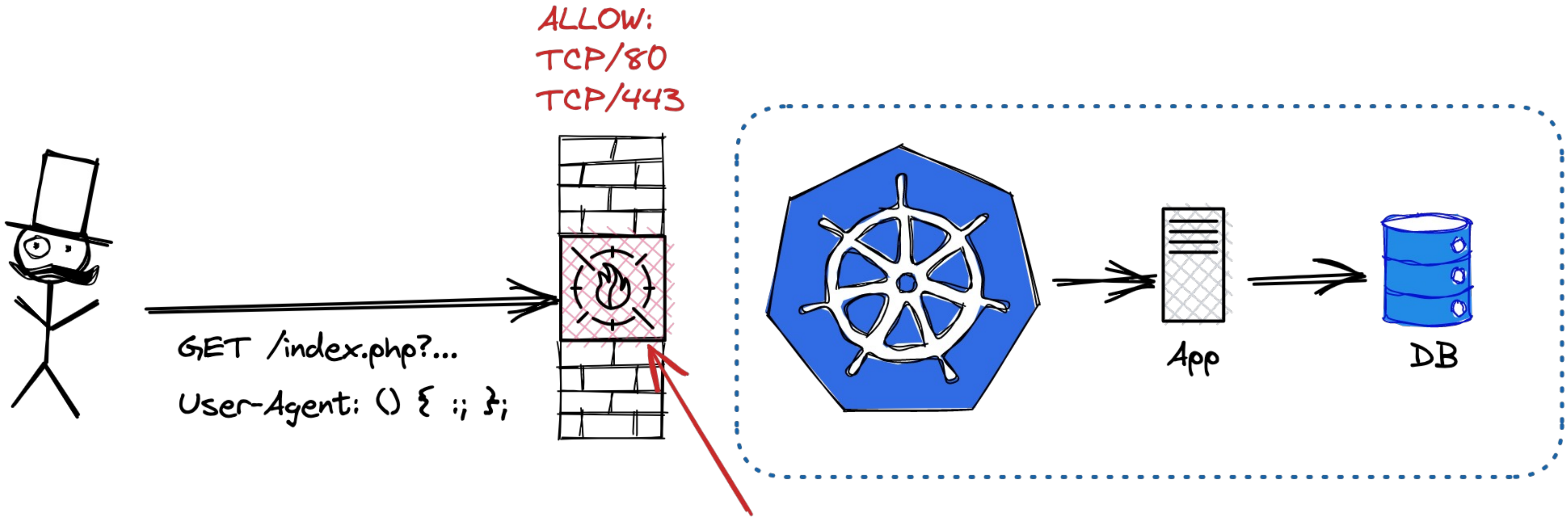


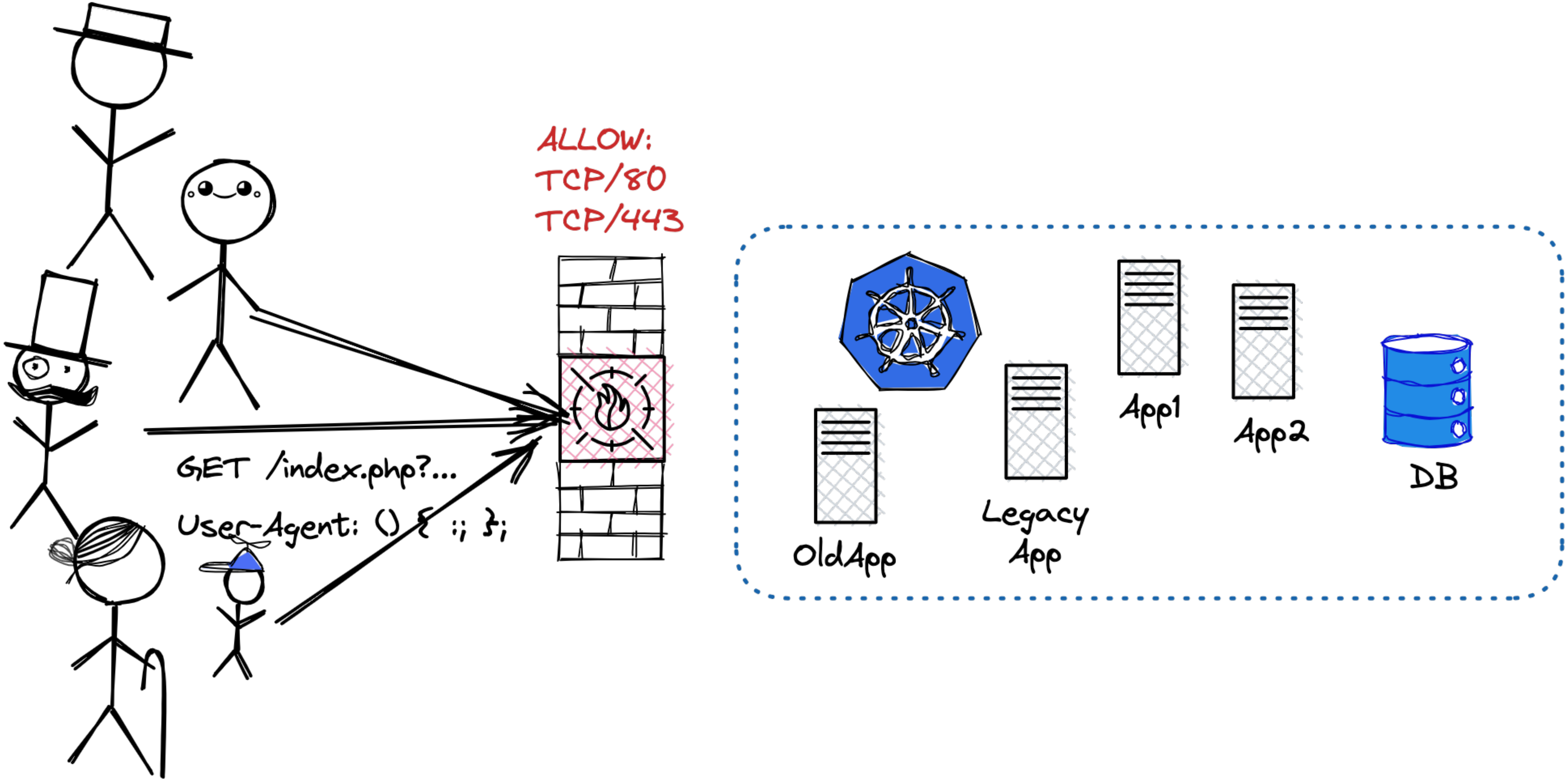
What Attackers are doing today	what your defenders will do today
1. Breach your network	1. four hours of meetings
2. Monetize	2. Status Updates
	3. Add notes to tickets
	4. Timesheets
	5. HR mandated training
	6. close tickets as "False Positive"
	7. update slide decks
	8. update policies + KBs
	9. 23minutes of Infosec work

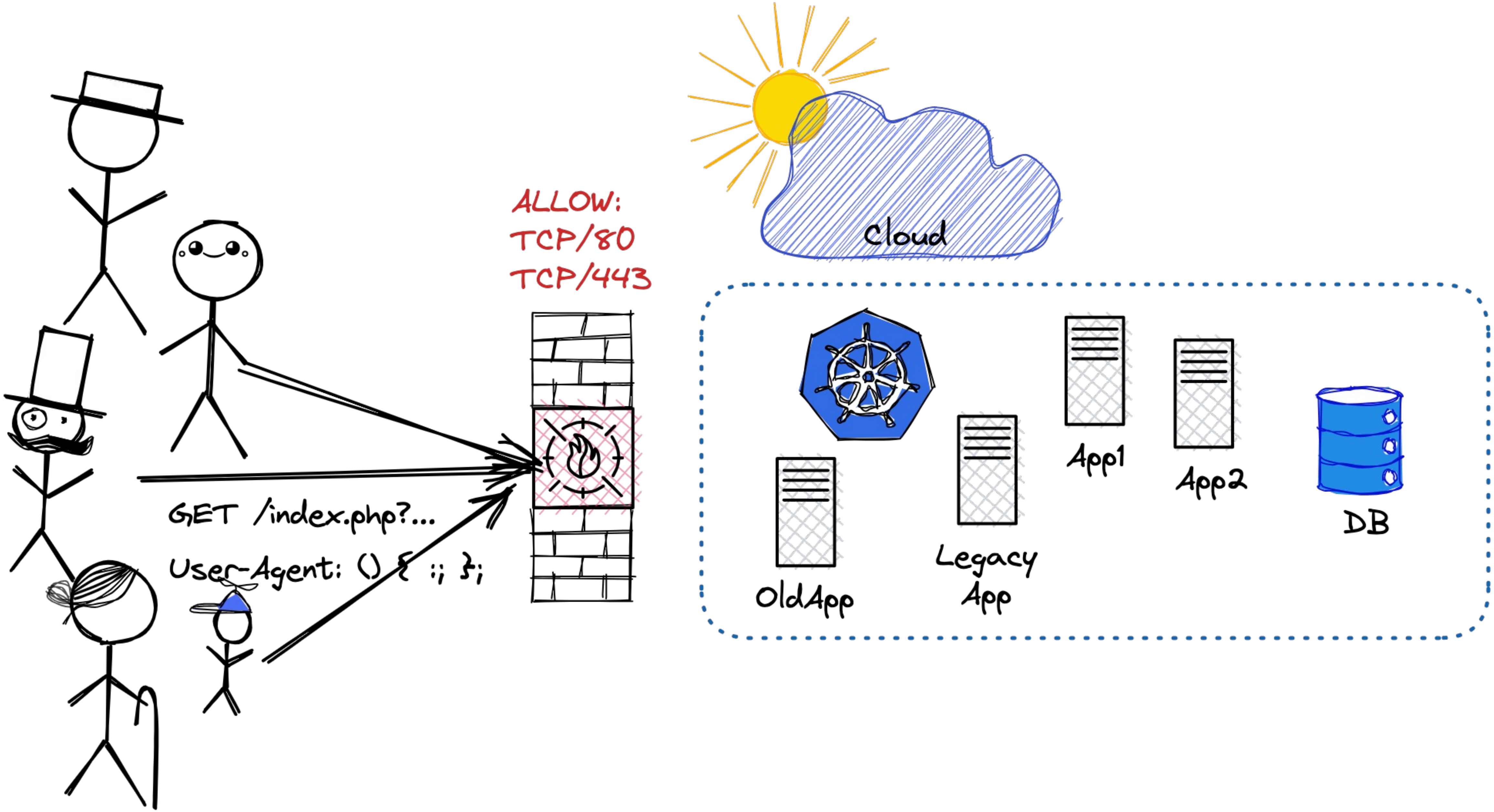
Who will win?

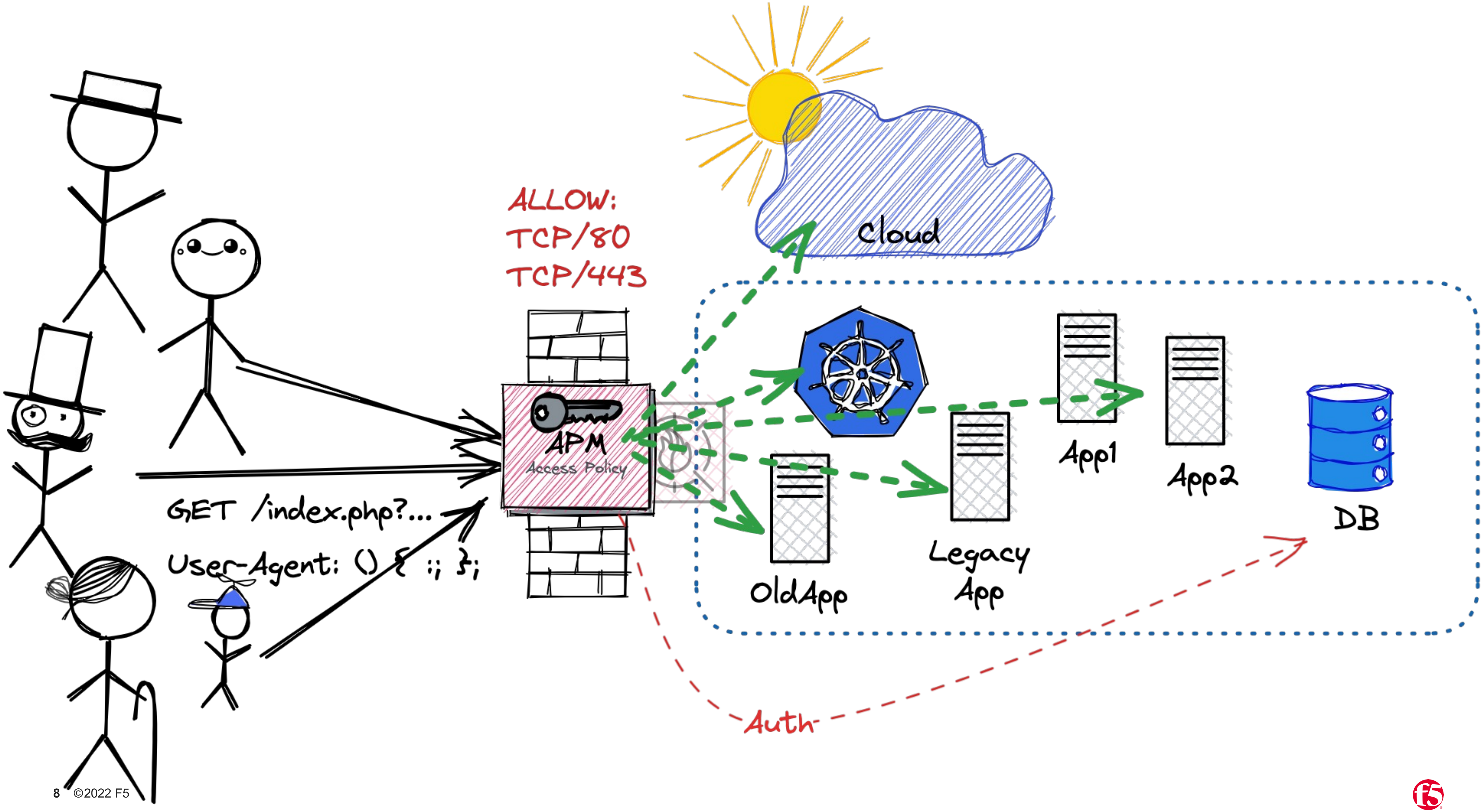

App
DB


ALLOW:
TCP/80
TCP/443
#ShellShock
App
DB


ALLOW:
TCP/80
TCP/443
GET /index.php?...
User-Agent: () { :; };
App
DB


ALLOW:
TCP/80
TCP/443
GET /index.php?...
User-Agent: () { :; };
OldApp
Legacy App
App1
App2
DB


ALLOW:
TCP/80
TCP/443
Cloud
GET /index.php?...
User-Agent: () { :; };
OldApp
Legacy App
App1
App2
DB


ALLOW:
TCP/80
TCP/443
Cloud
APM
Access Policy
GET /index.php?...
User-Agent: () { :; };
OldApp
Legacy
App
App1
App2
DB
Auth

The challenges of managing access today

Need to manage access based on identity and context

Rapidly expanding, changing mobile workforce

Explosion in number of users, use cases, in-use devices

Increased virtualization and multi-cloud

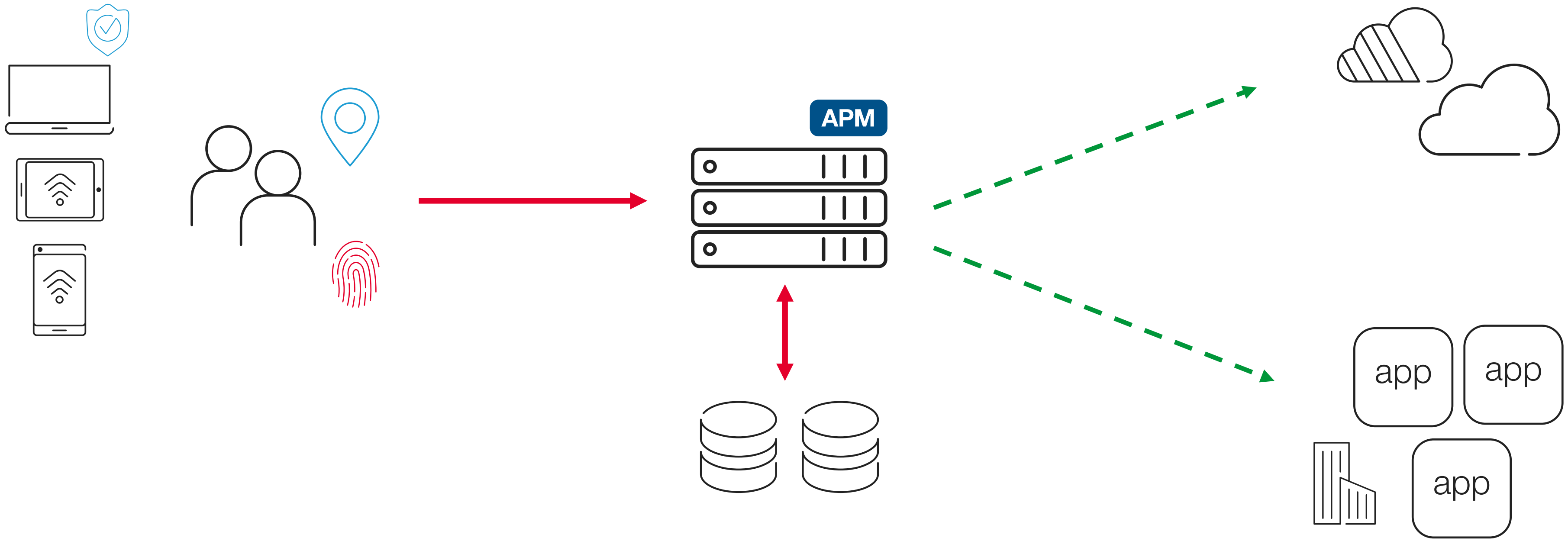
Fast rising number of security threats and attacks

Controlling access through identity

User Identity and Device Information + Network / Connection + Application Health and Risk

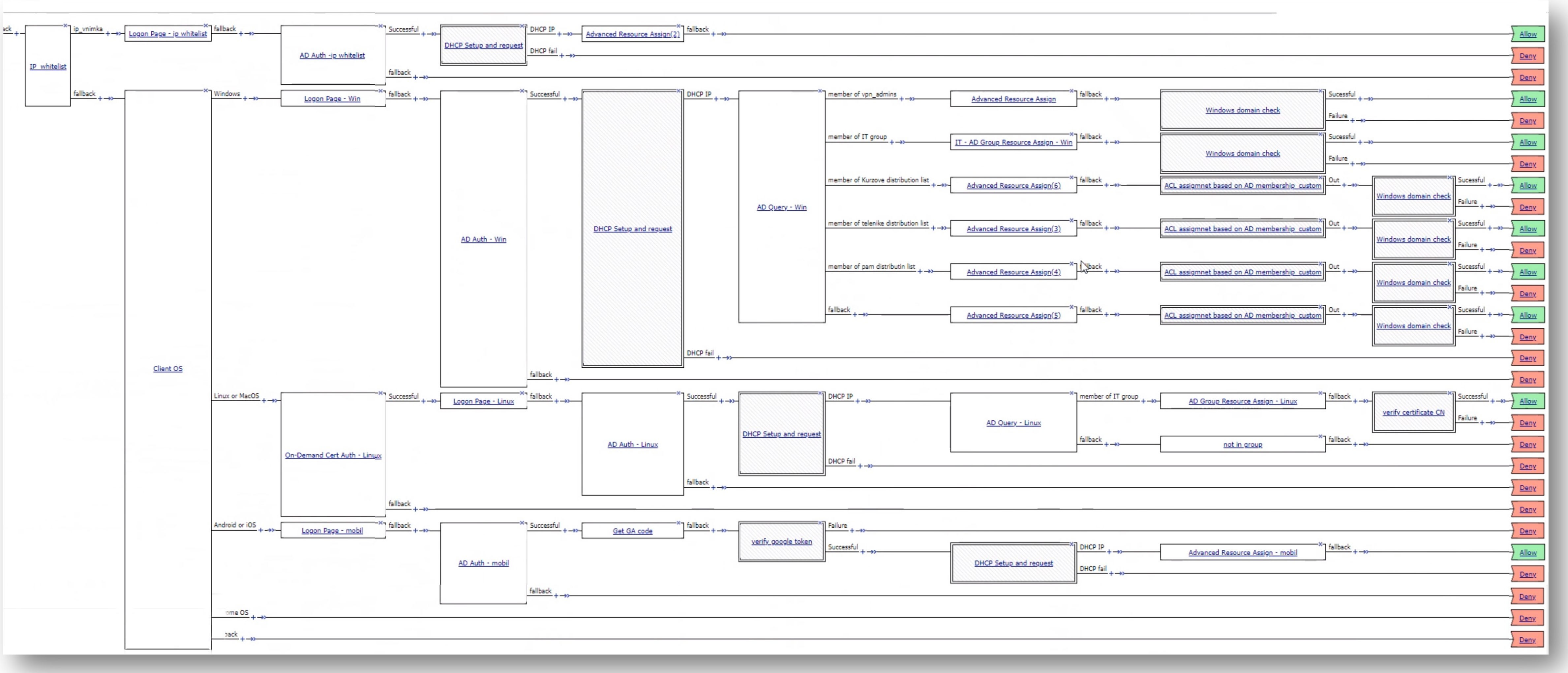
Access Policy

Reference Architecture



Access Policy Design

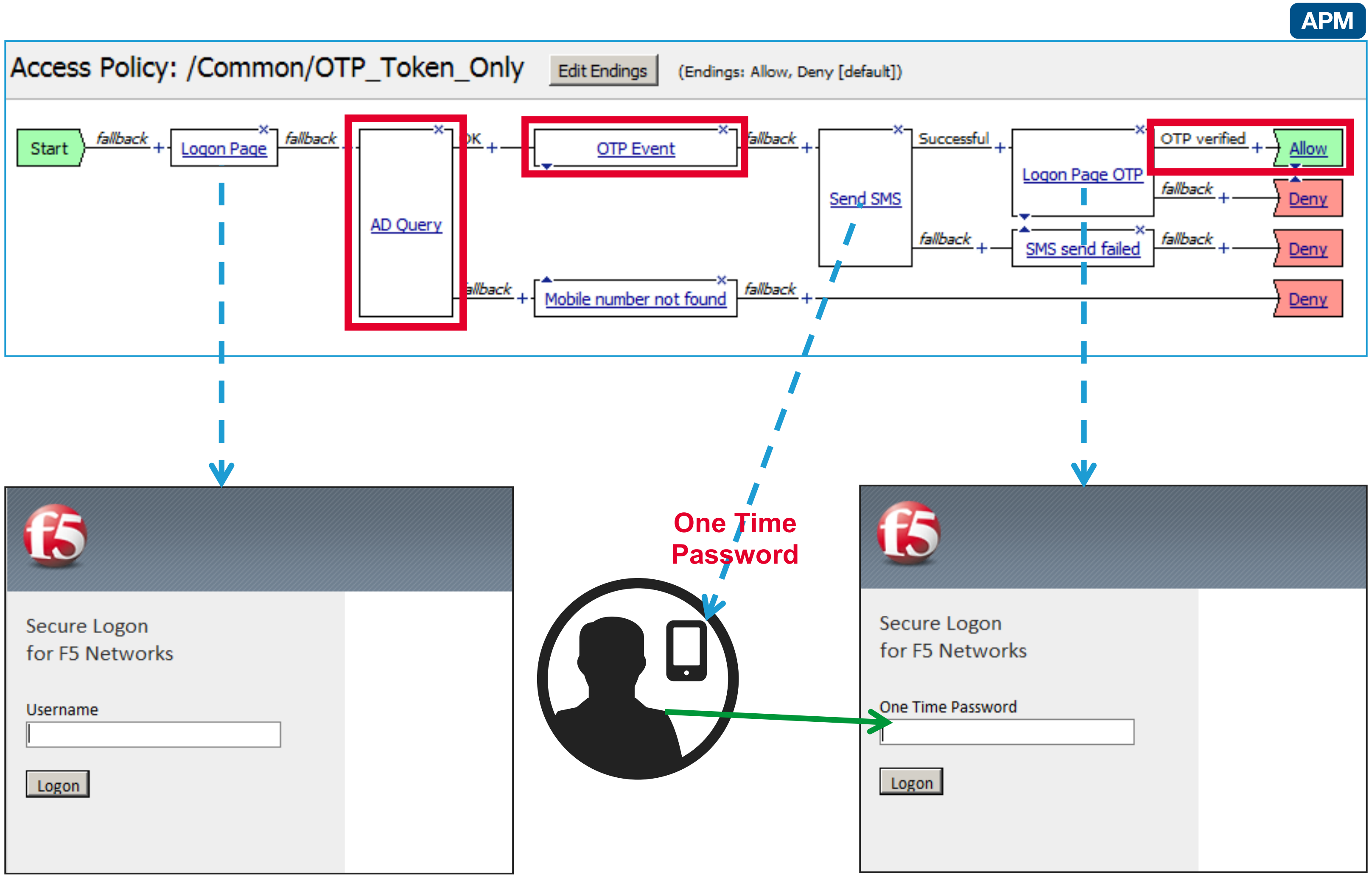
APM



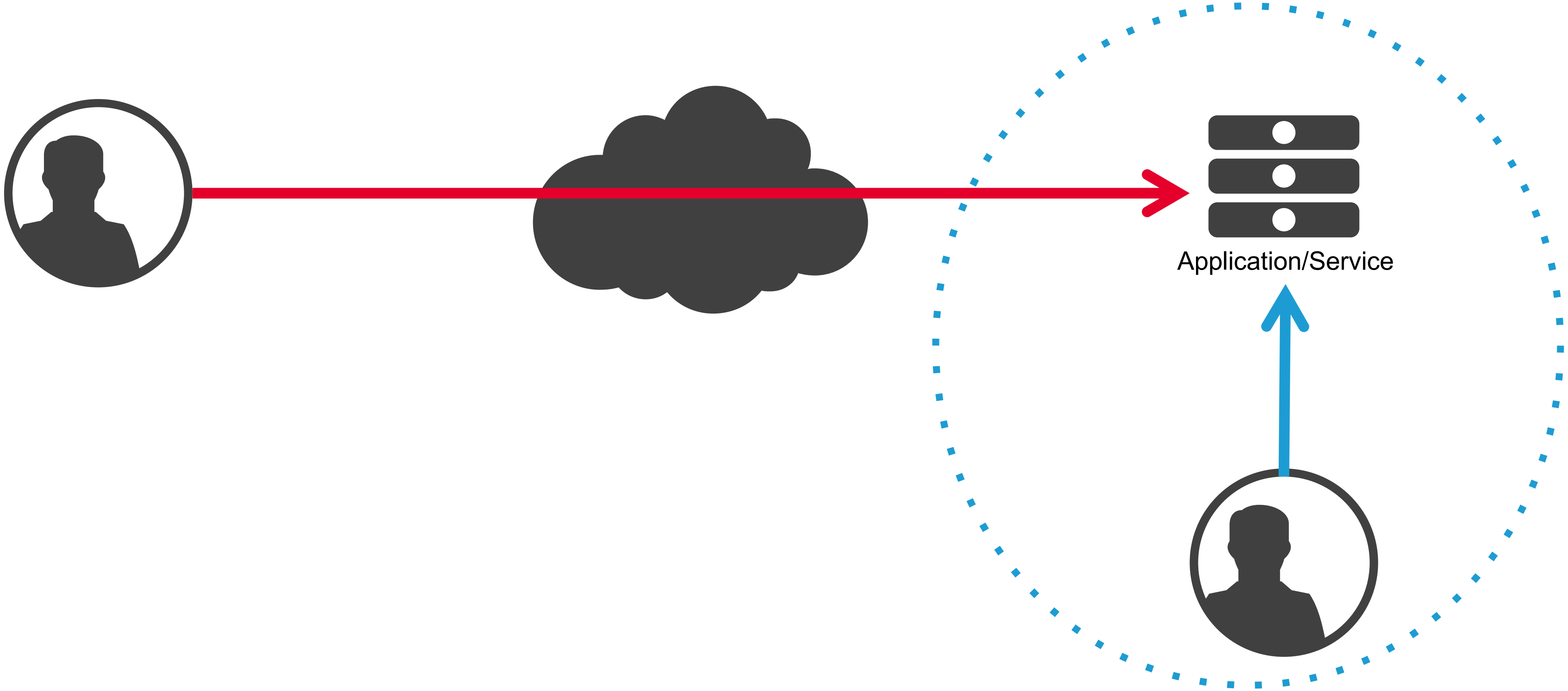
Examples

1. SMS One Time Password
2. Internal vs. External User
3. Step-up Authentication
4. Client Posture Check

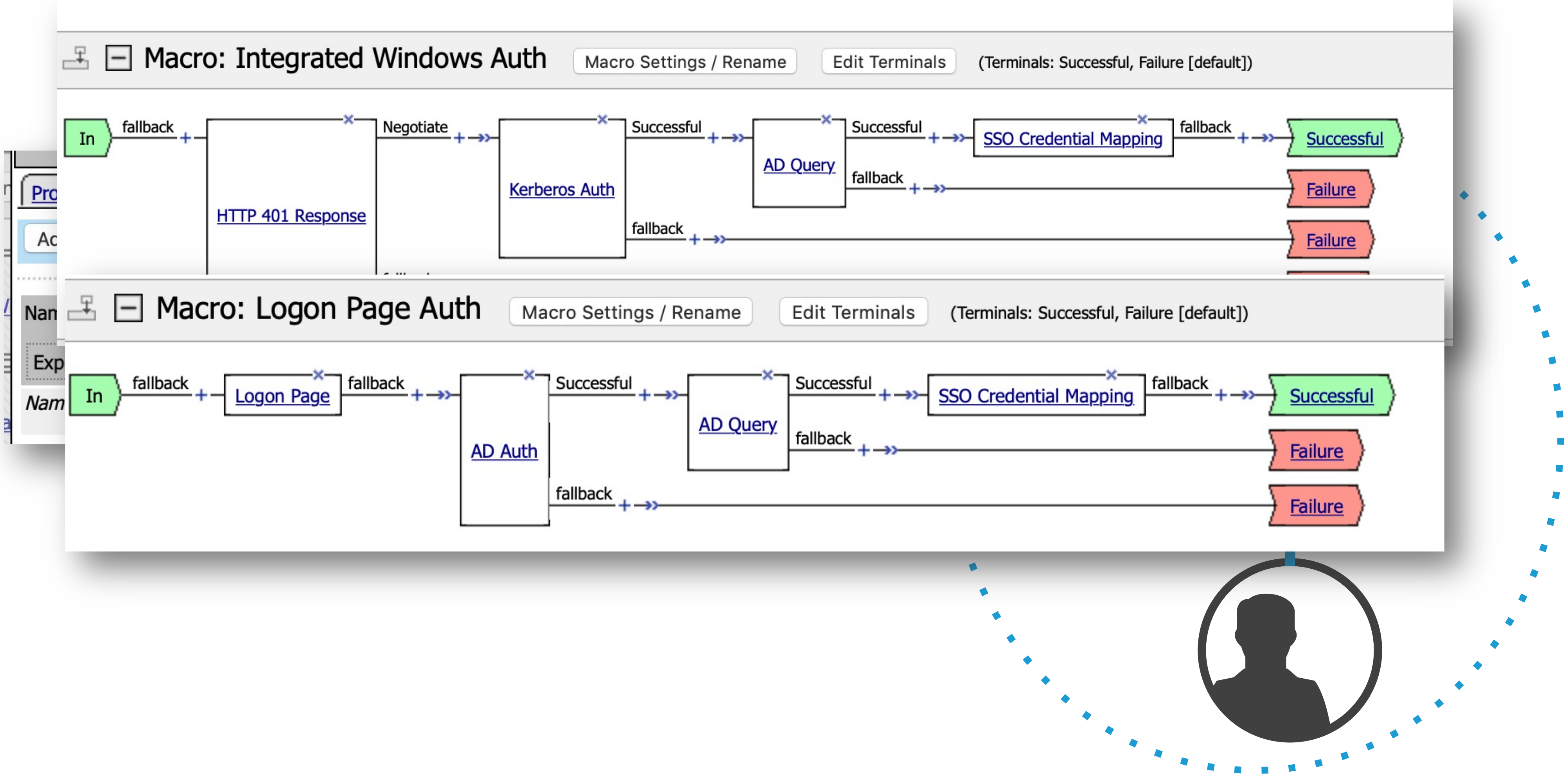
Access Policy using SMS OTP



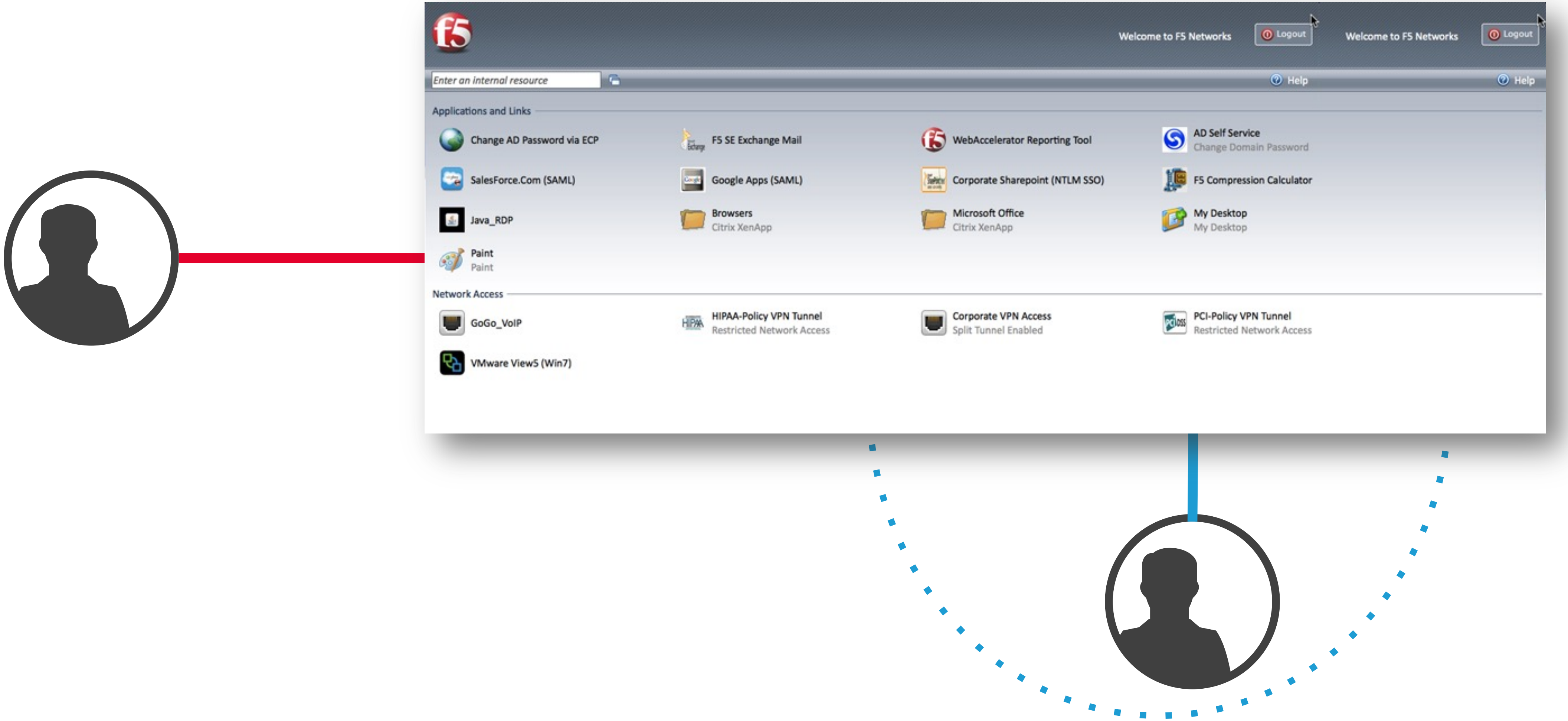
Internal vs. External Network



Internal vs. External Network



Internal vs. External Network



Welcome to F5 Networks Logout Welcome to F5 Networks Logout

Enter an internal resource

Help Help

Applications and Links

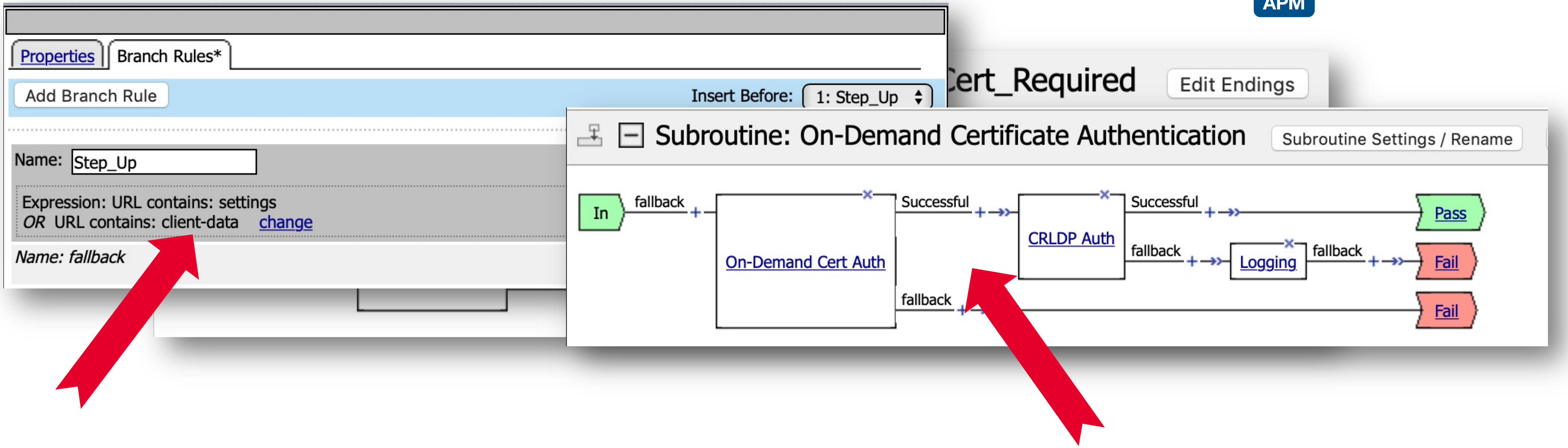
Change AD Password via ECP	F5 SE Exchange Mail	WebAccelerator Reporting Tool	AD Self Service Change Domain Password
SalesForce.Com (SAML)	Google Apps (SAML)	Corporate Sharepoint (NTLM SSO)	F5 Compression Calculator
Java_RDP	Browsers Citrix XenApp	Microsoft Office Citrix XenApp	My Desktop My Desktop
Paint Paint			

Network Access

GoGo_VoIP	HIPAA-Policy VPN Tunnel Restricted Network Access	Corporate VPN Access Split Tunnel Enabled	PCI-Policy VPN Tunnel Restricted Network Access
VMware View5 (Win7)			

Step-up Authentication

APM



Properties | Branch Rules*

Add Branch Rule

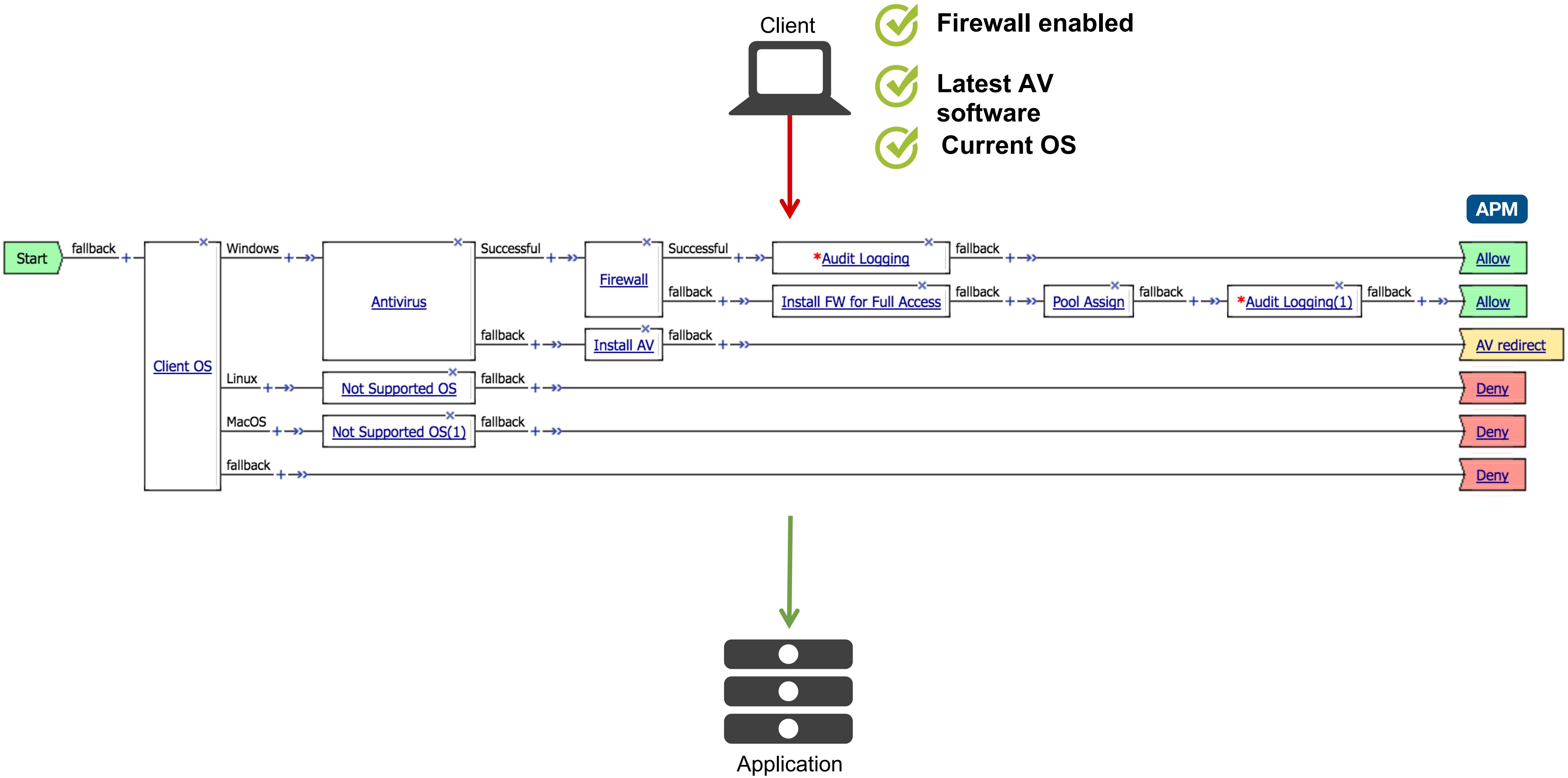
Insert Before: 1: Step_Up

Name: Step_Up

Expression: URL contains: settings
OR URL contains: client-data change

Name: fallback

Client security check



✓ Firewall enabled

✓ Latest AV software

✓ Current OS

Challenge: Enforcing Zero Trust for app access

NEVER TRUST

- How should users trust be tested?
- Will users inside the network need to login to apps?
- Will users who have already accessed apps need to re-login?

ALWAYS VERIFY

- Will users need to be re-verified when attempting to access any app?
- Will users' devices and their security need to be verified?
- Will users' locations need to be checked?
- Will apps need to be verified for security and access?

CONTINUOUSLY MONITOR

- Will users' devices need to be continuously checked? How, and how often?
- Will users' locations need to be monitored continuously?
- Will users' network access need to be watched for its security?