Identity Aware Proxy

The Evolution of Today's Security Architectures

Presented by

Jason Wilburn
Solutions Engineer

What is Zero Trust?

A Zero Trust Architecture (ZTA) strategy is one where there is no implicit trust granted to systems based on their physical or network location (i.e., local area networks vs. the Internet).

NIST

- The network is always assumed to be hostile.
- External and internal threats exist on the network at all times.
- Network locality is not sufficient for deciding trust in a network.
- Every device, user, and network flow is authenticated and authorized.
- Policies must be dynamic and calculated from as many sources of data as possible.

Gillman and Barth

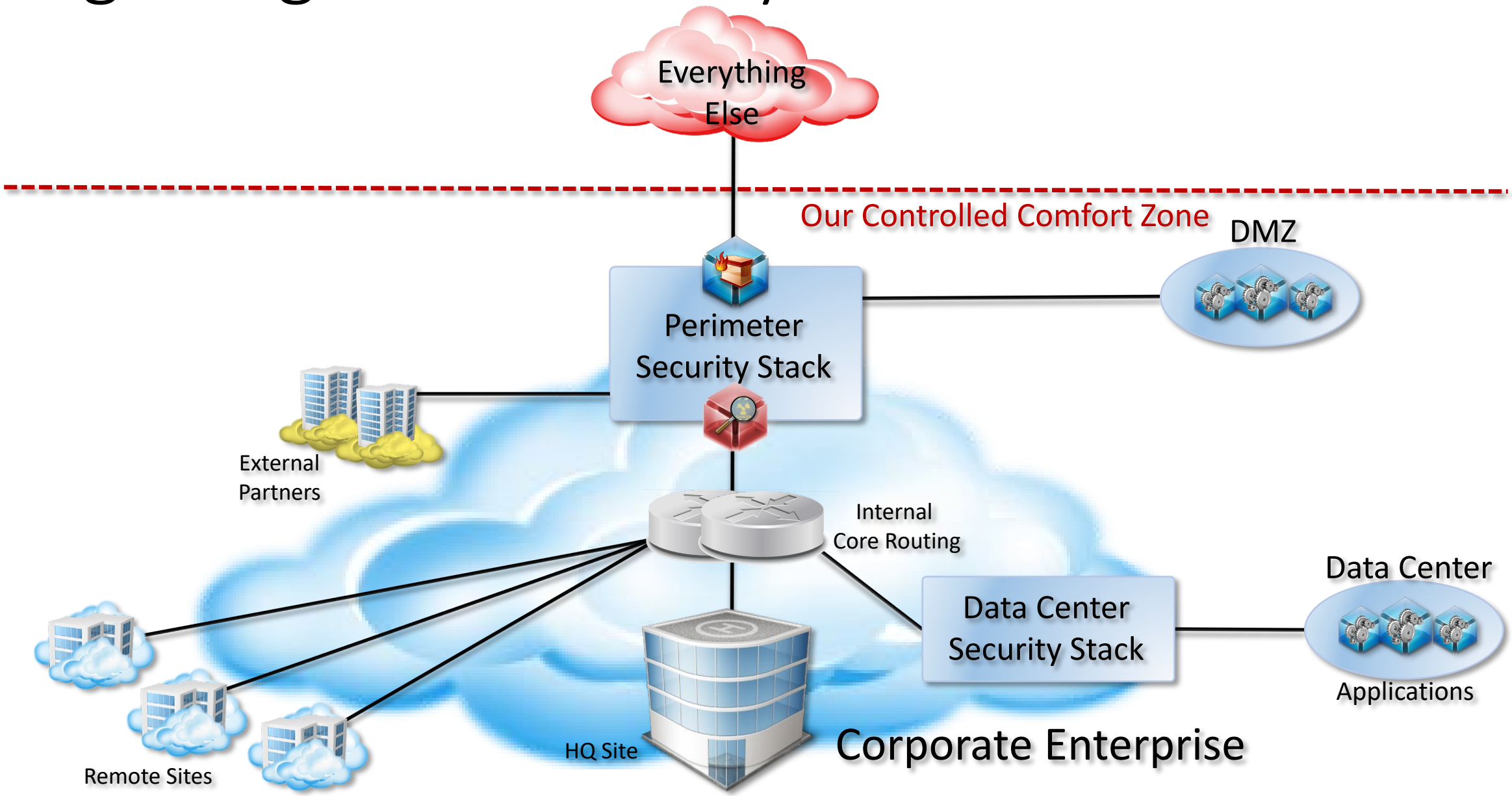
Zero Trust is a data-first framework to achieve security using microperimeters and microsegmentation.

Forrester

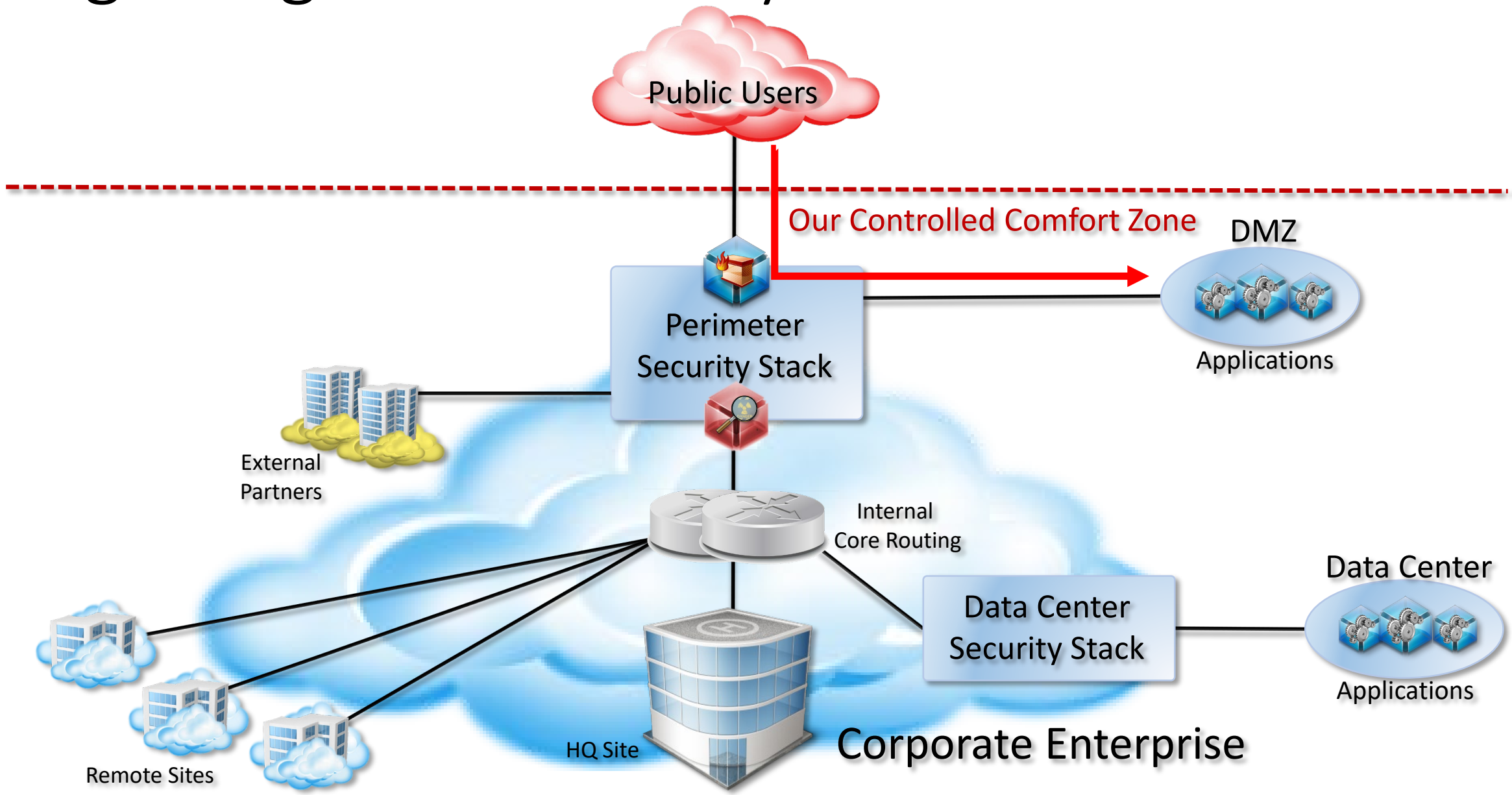
Zero trust networking is a concept for secure network connectivity where the initial security posture has no implicit trust between different entities, regardless of whether they are inside or outside of the enterprise perimeter. Least-privilege access to networked capabilities is dynamically extended only after an assessment of the identity of the entity, the system and the context.

Gartner

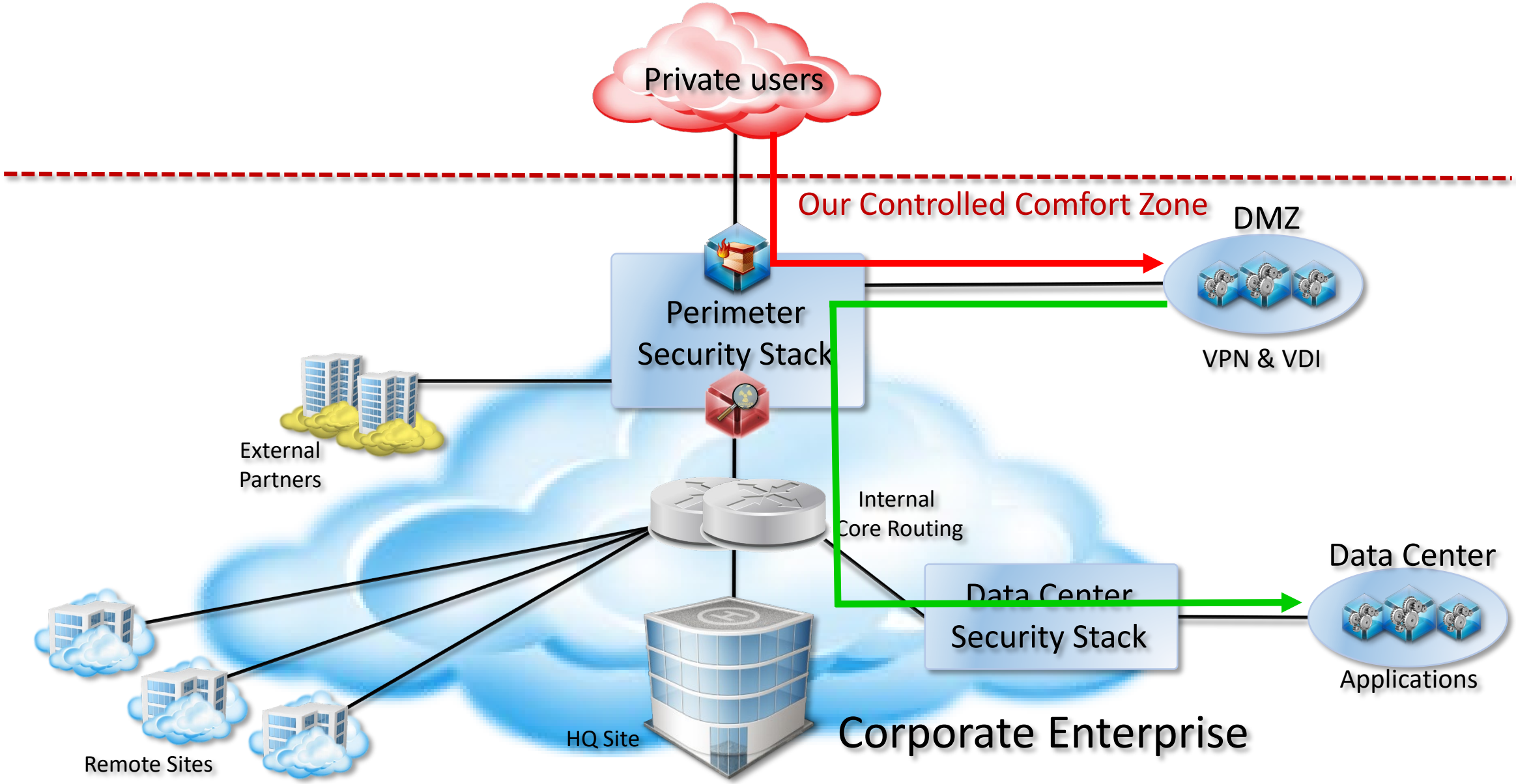
Beginning of the Journey



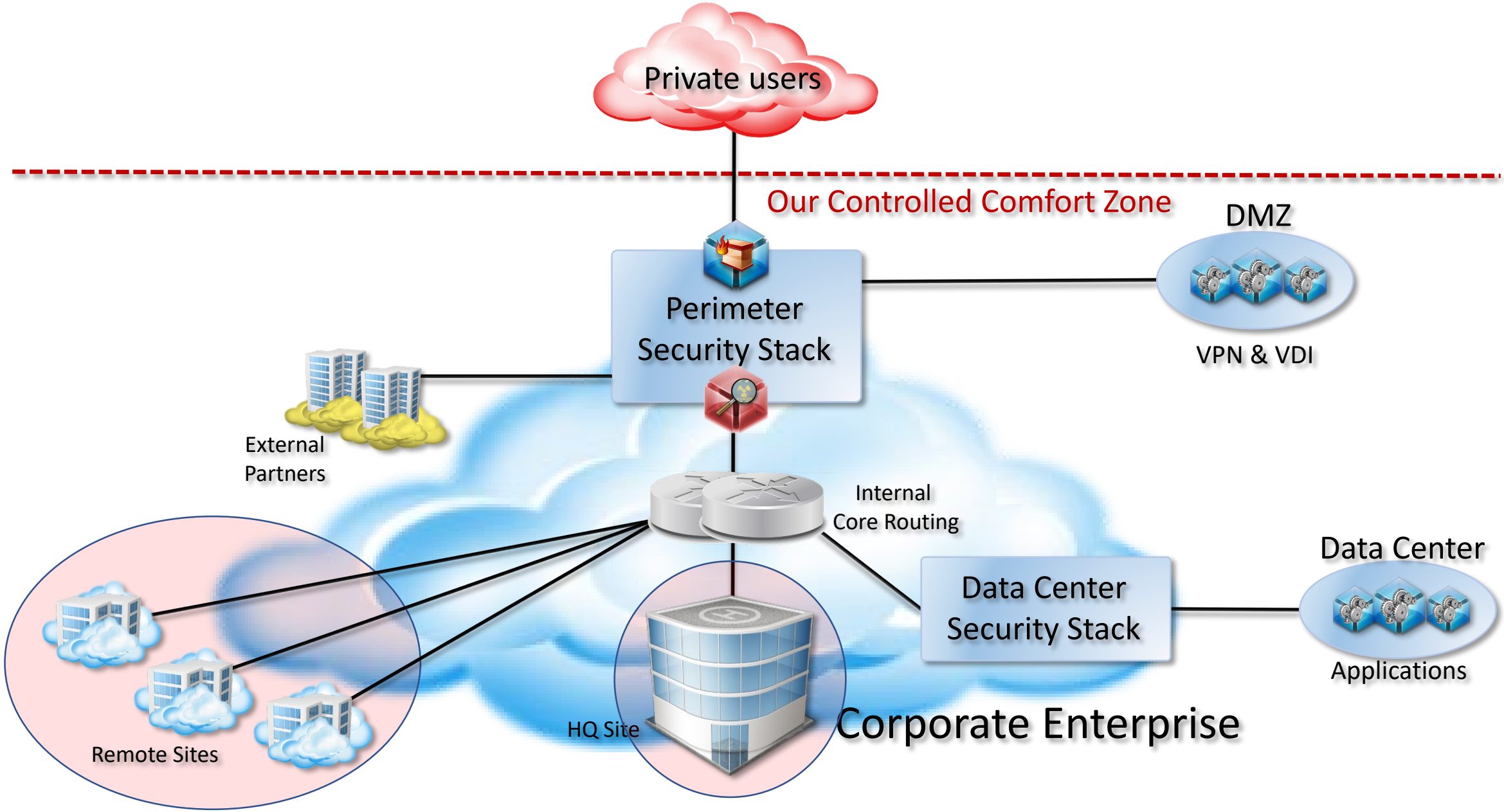
Beginning of the Journey



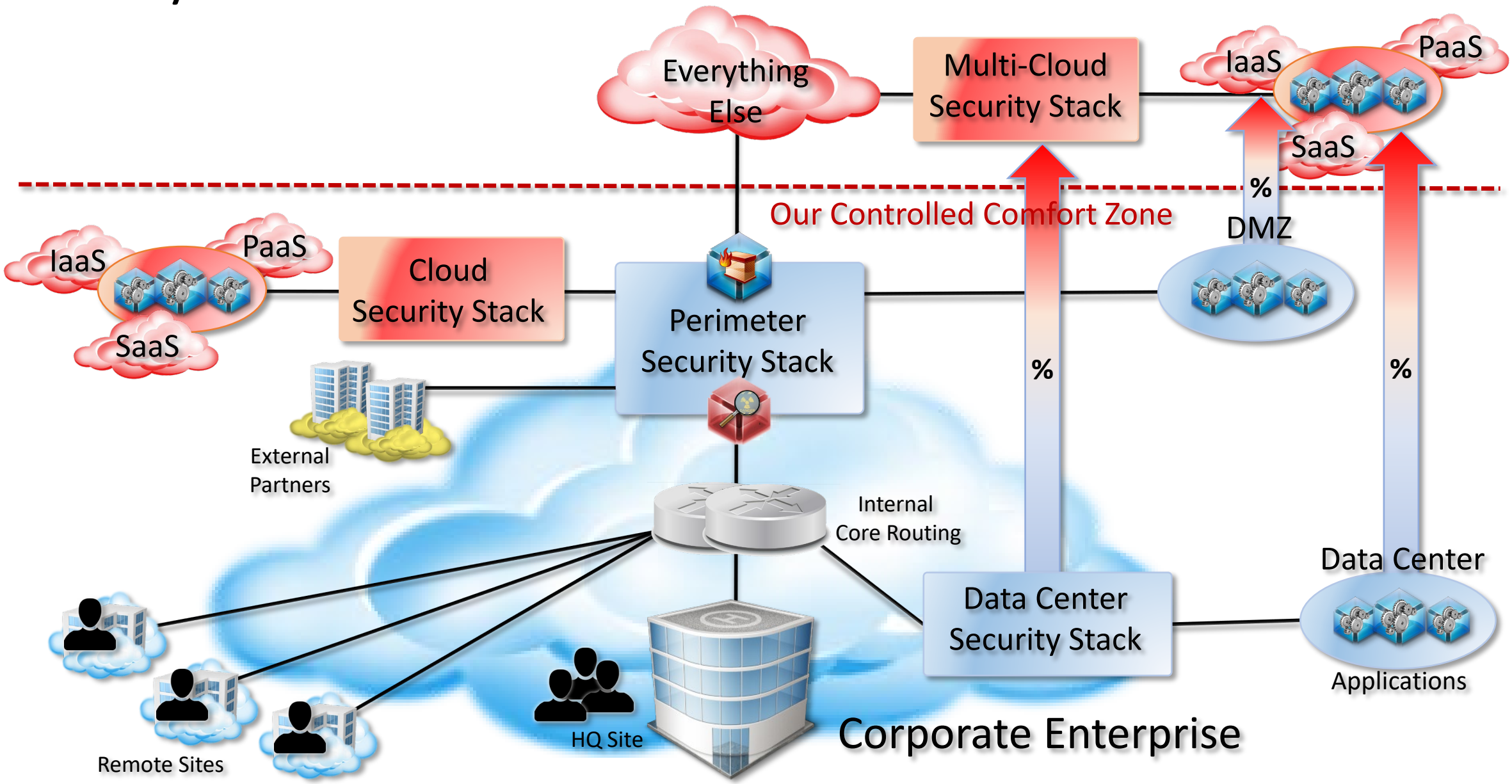
Beginning of the Journey



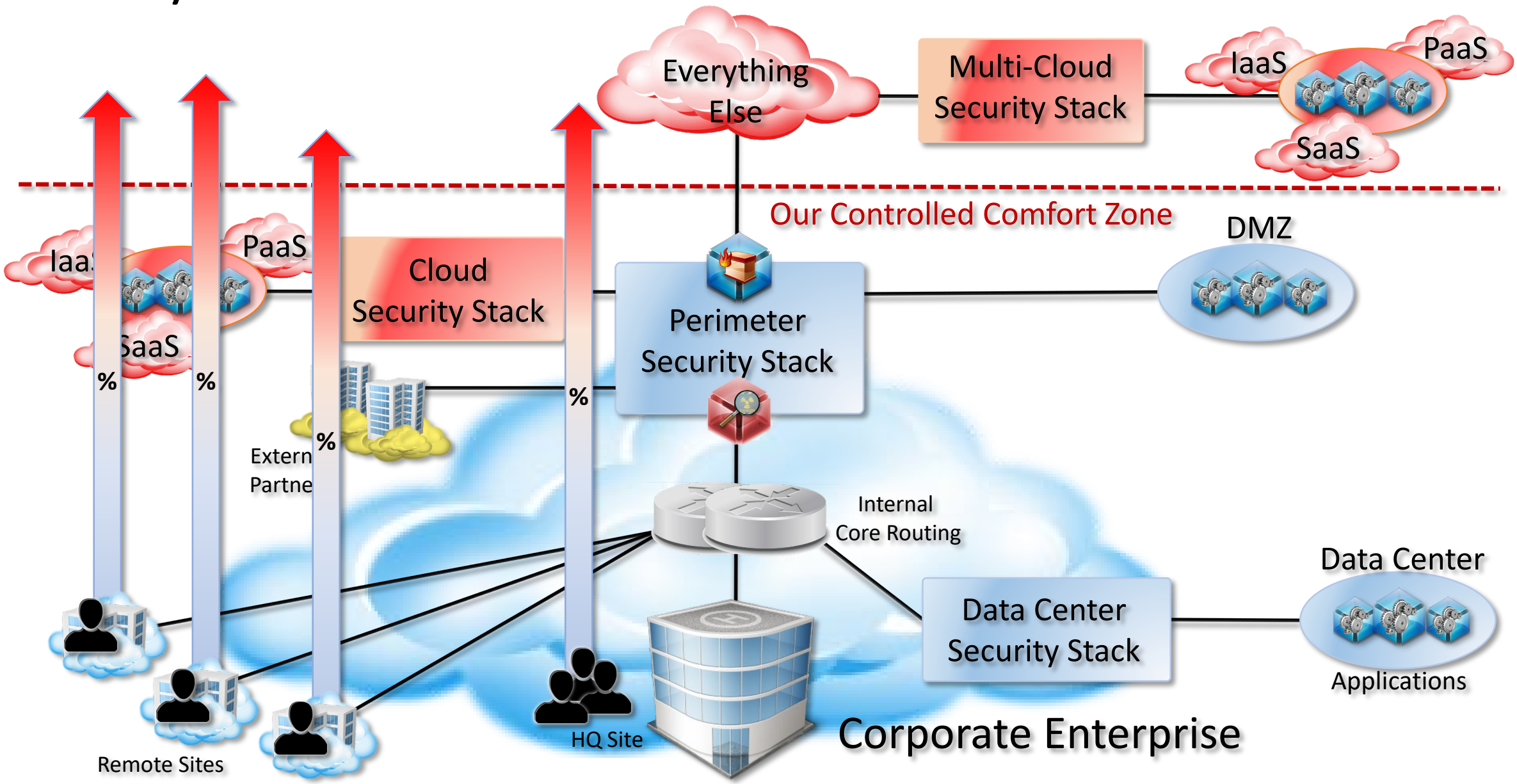
Beginning of the Journey



Today's Architecture

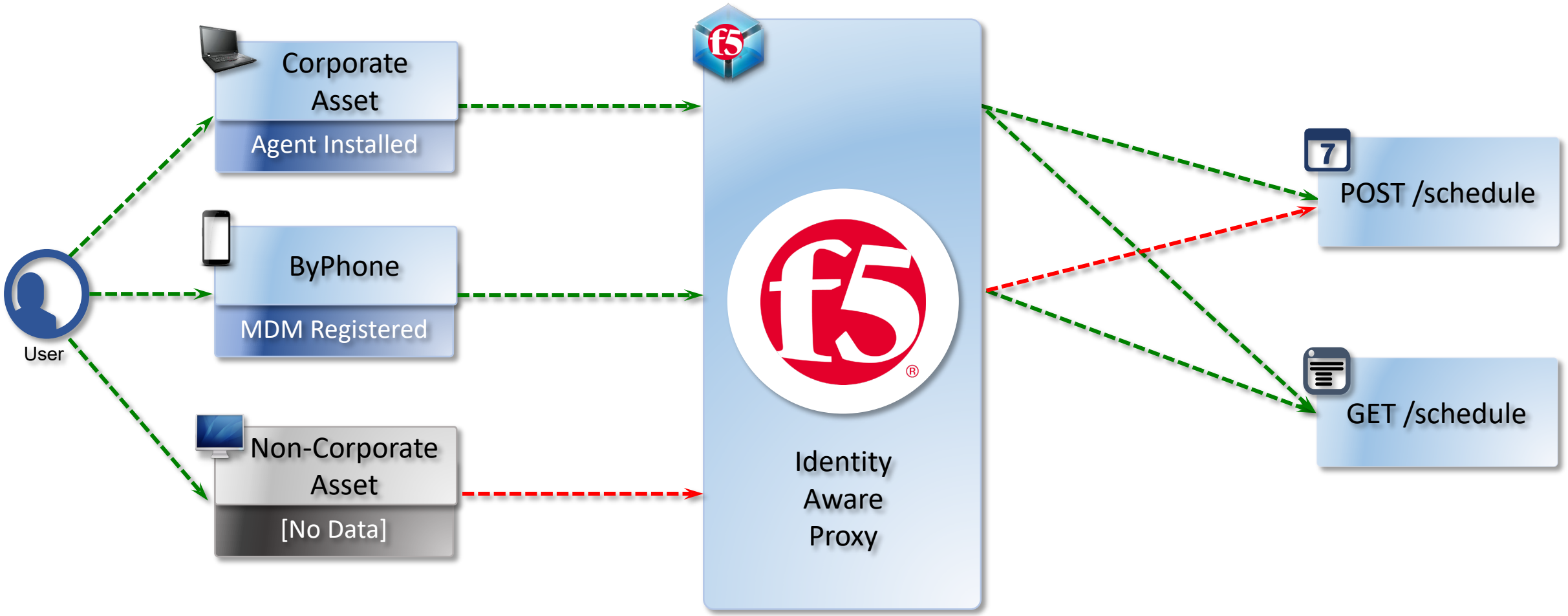


Today's Architecture

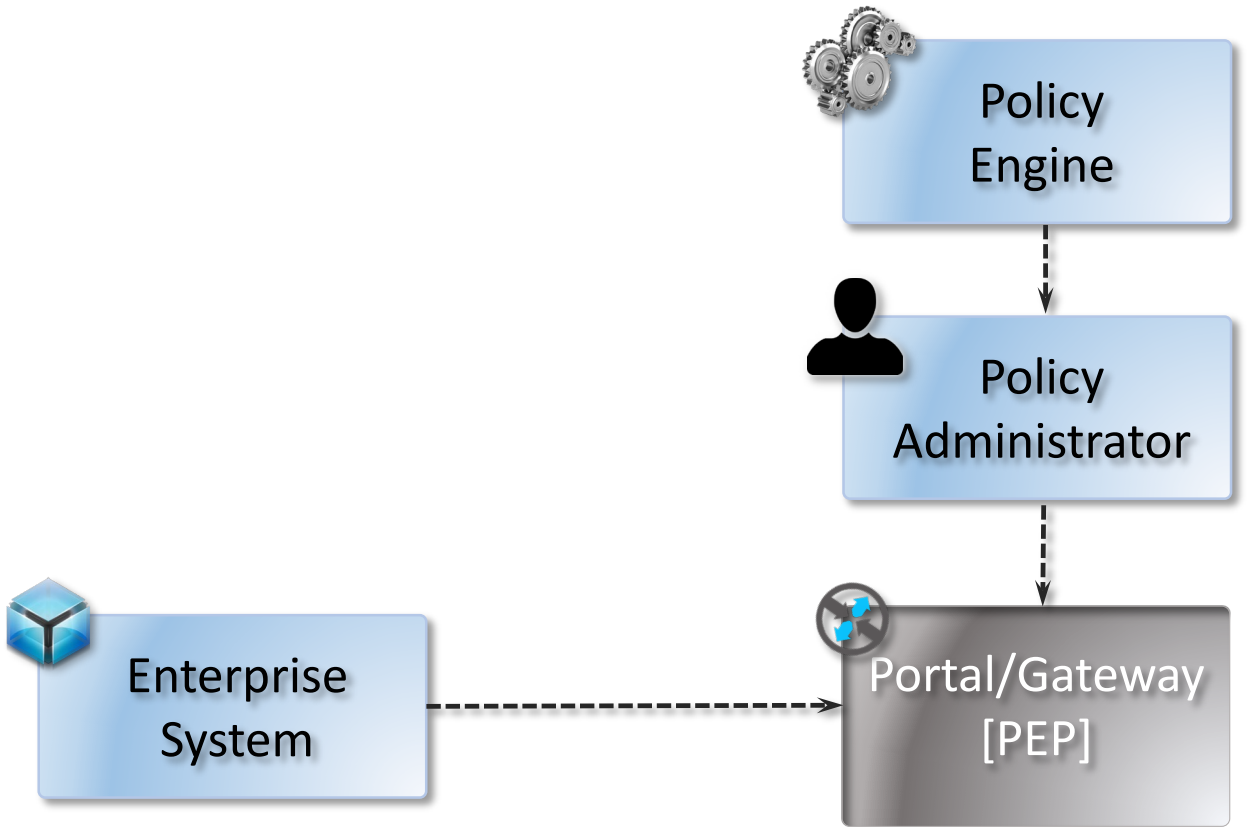


Tomorrow’s Architecture

Identity Aware Proxy (IAP)

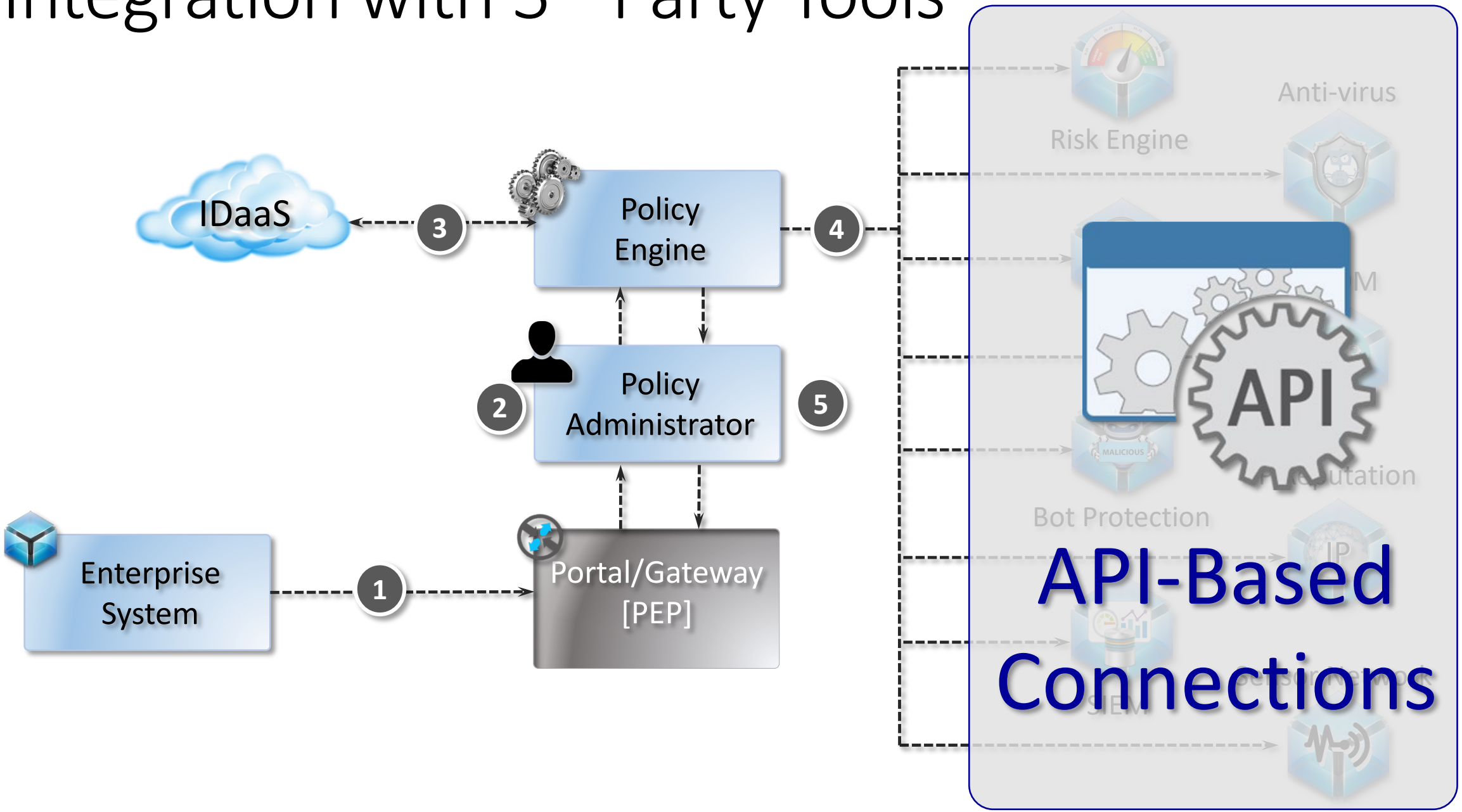


Posture Assessments



- Firewall
- Anti-Virus
- Patch Management
- Machine Certificate
- Hard Disk Encryption
- File
- Process
- Public File Sharing

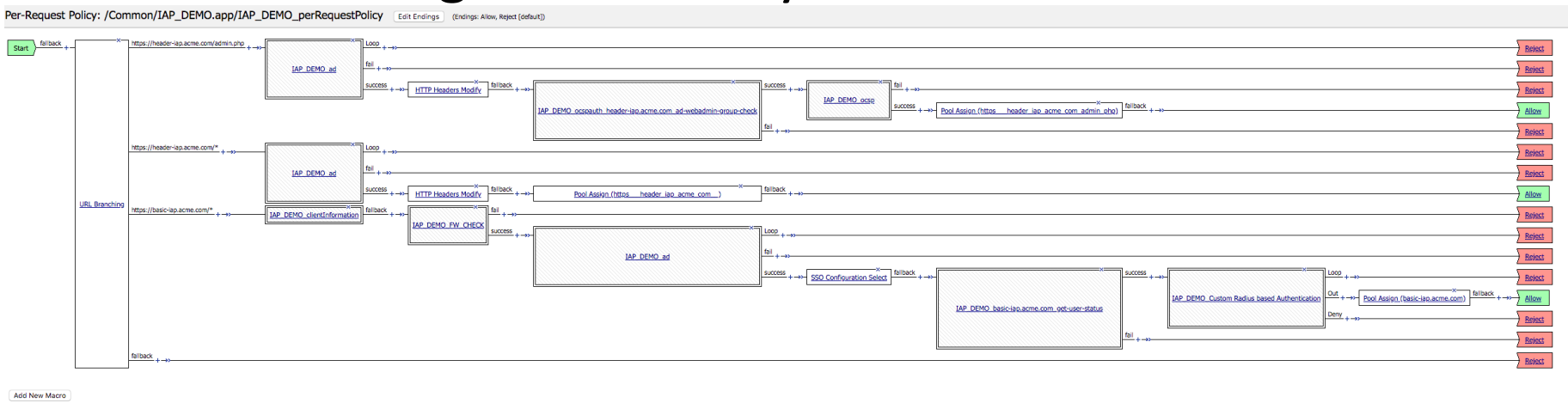
Integration with 3rd Party Tools



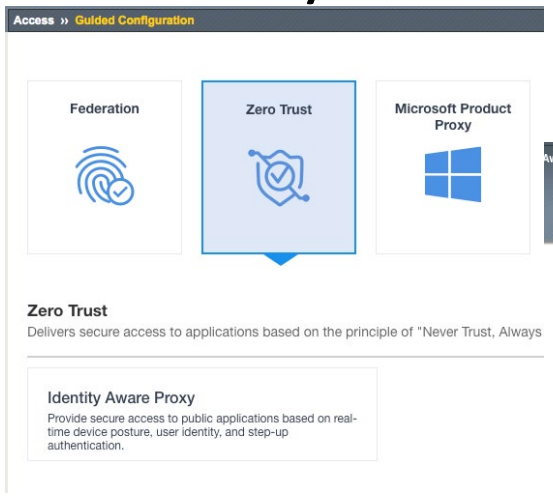
Credential Protection

Two ways to implement IAP

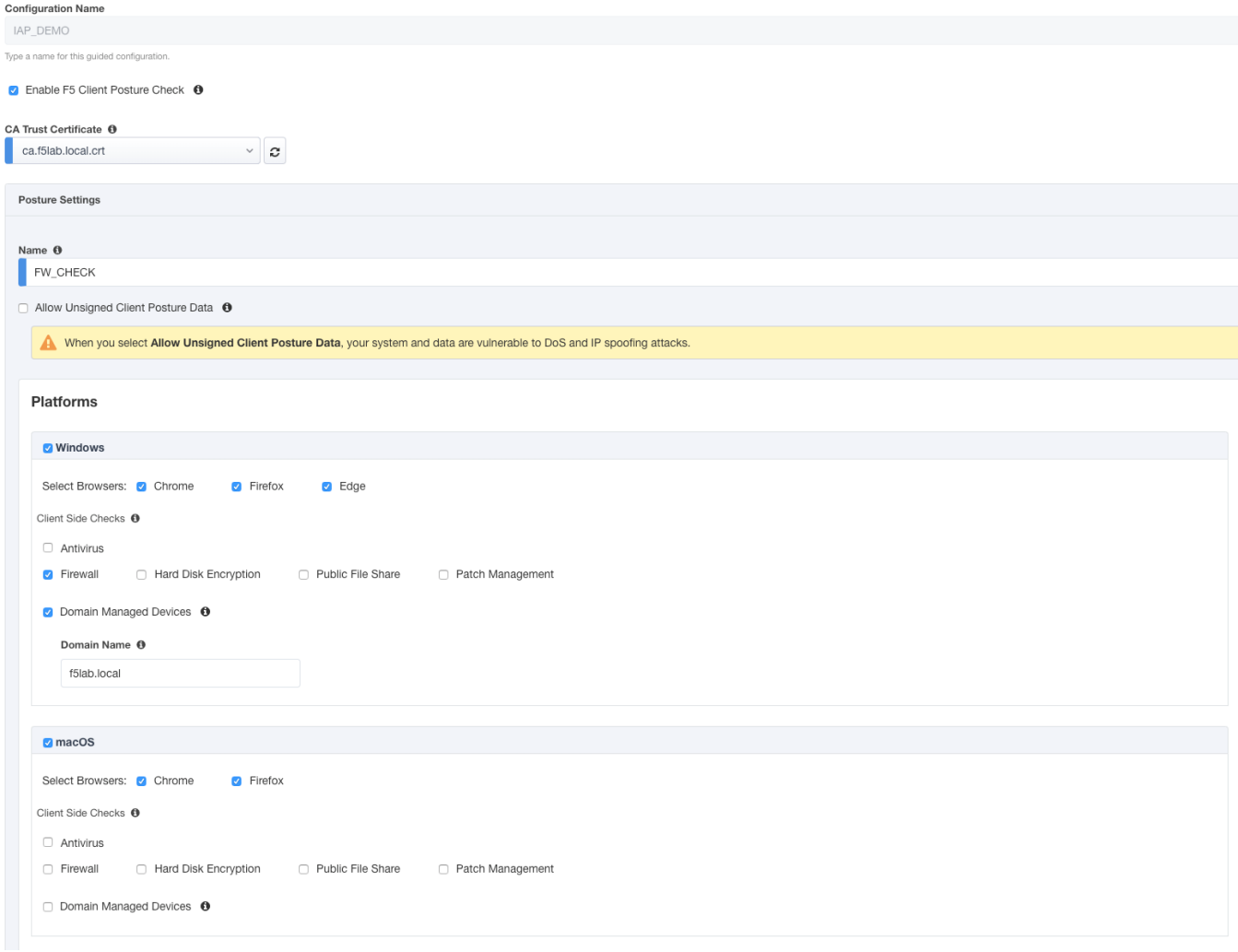
- Per-Request Policies using Visual Policy Editor



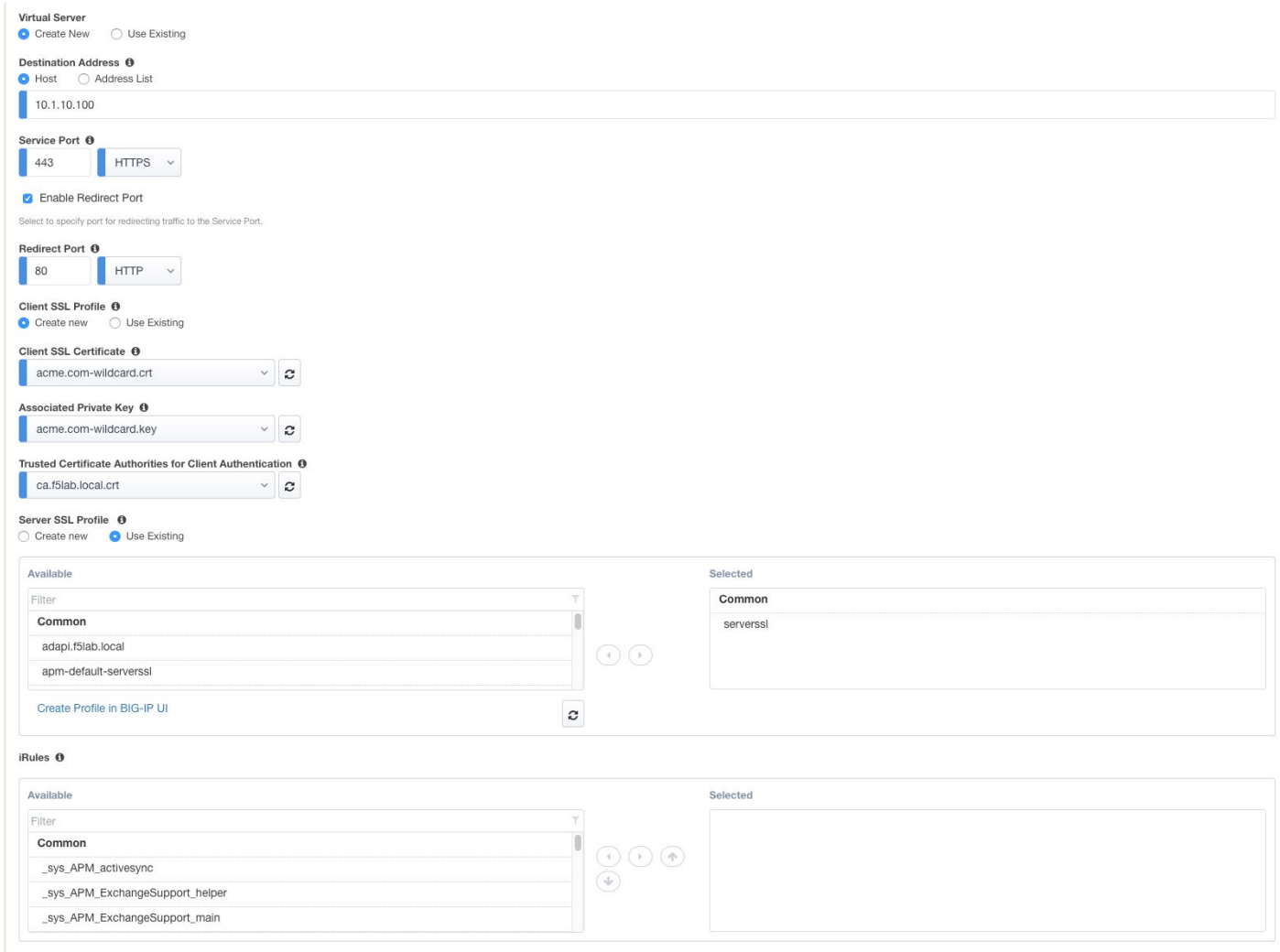
- Identity Aware Proxy Guided Configuration



Device Posture

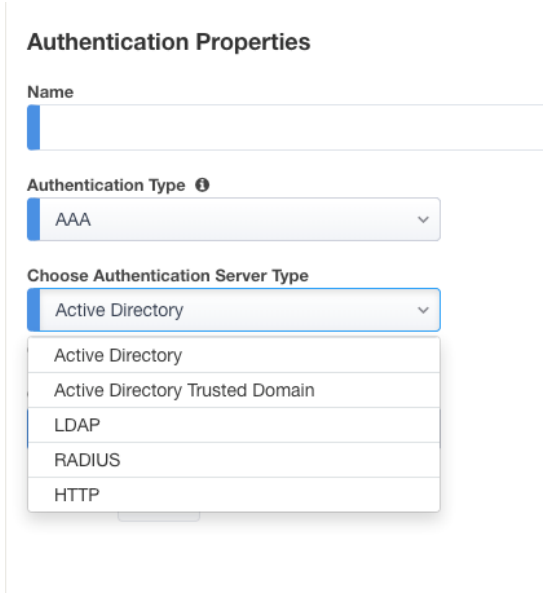


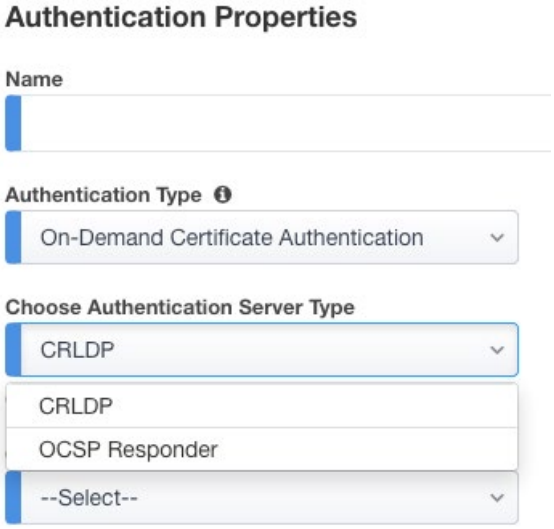
Virtual Server

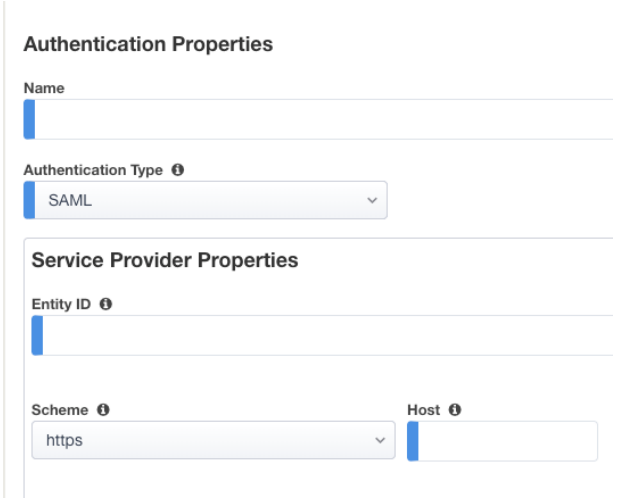


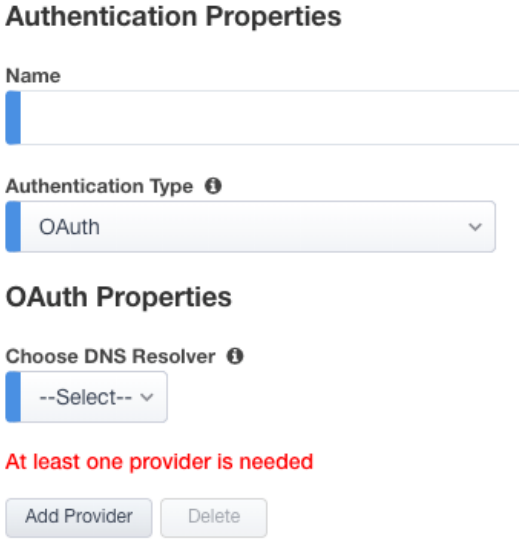
User Identities

- Active Directory
- LDAP
- RADIUS
- HTTP
- SAML
- CRDLP
- OCSP
- OAuth

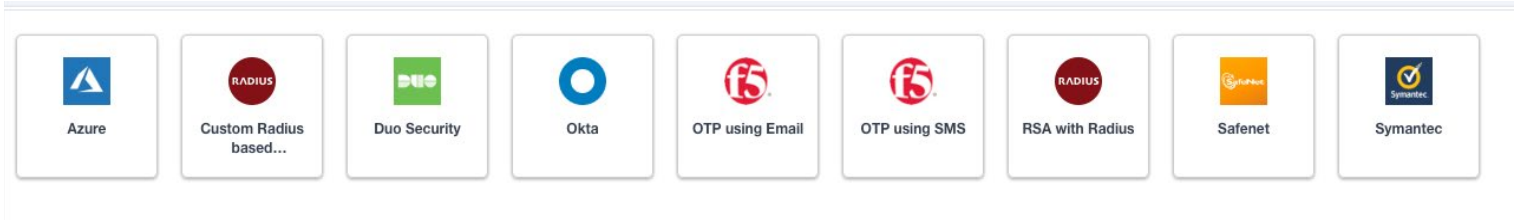




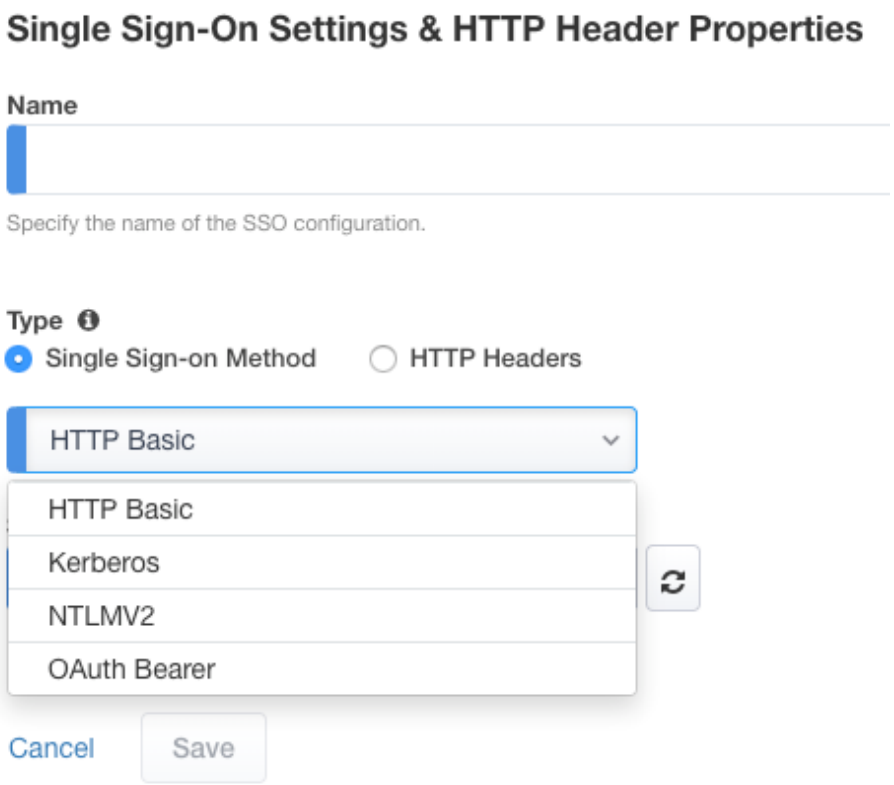


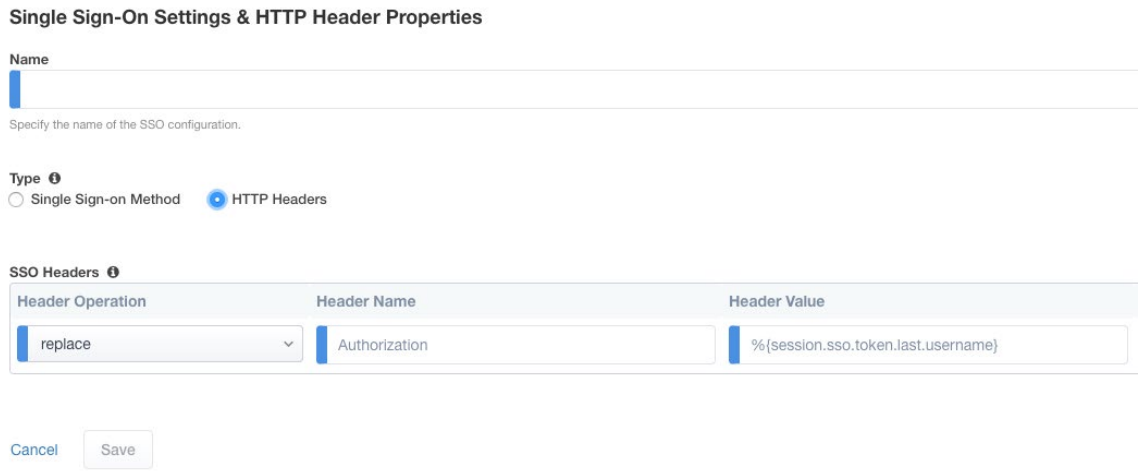


MFA

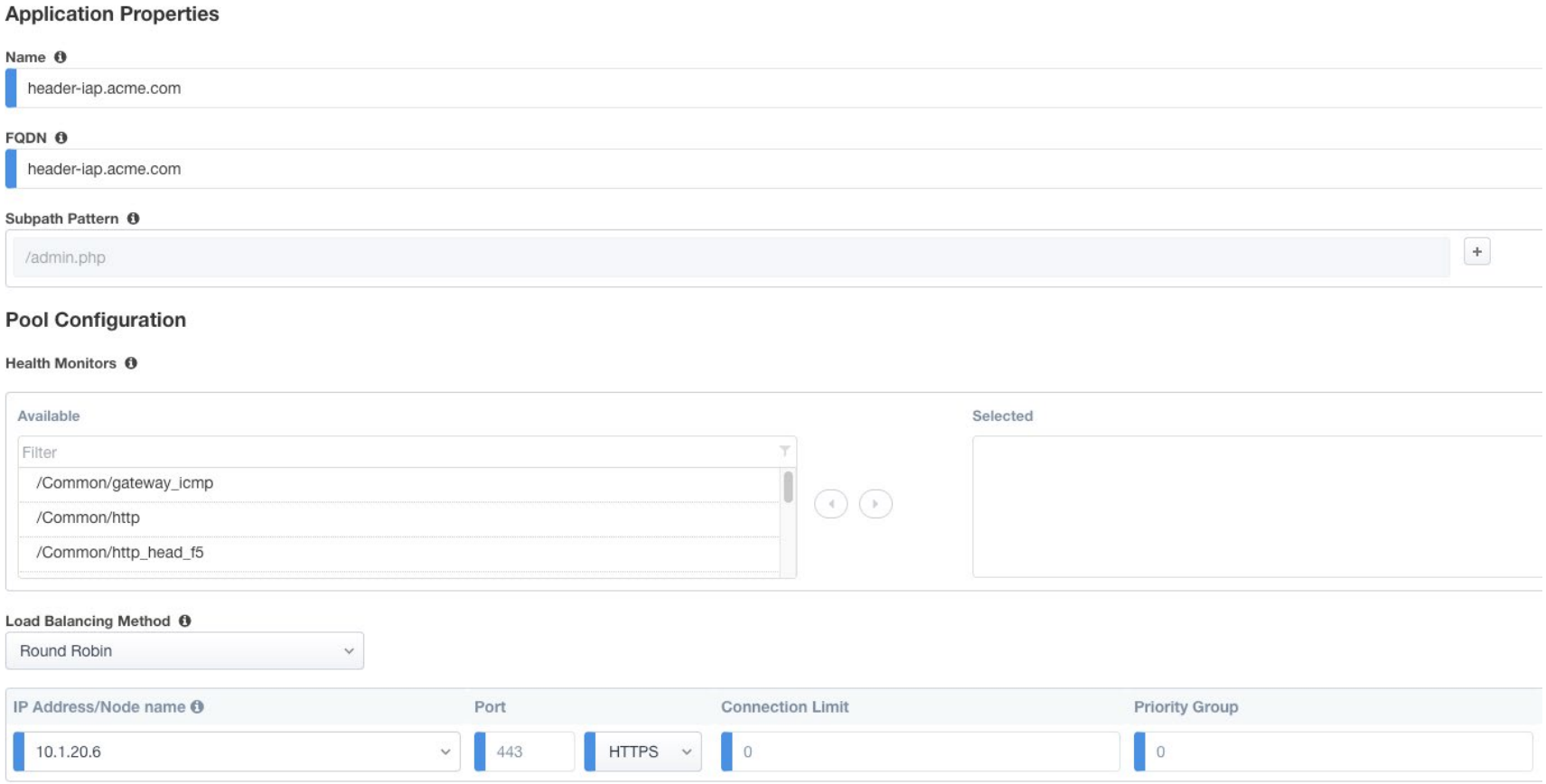

Azure
Custom Radius based...
Duo Security
Okta
OTP using Email
OTP using SMS
RSA with Radius
Safenet
Symantec

SSO & HTTP Header

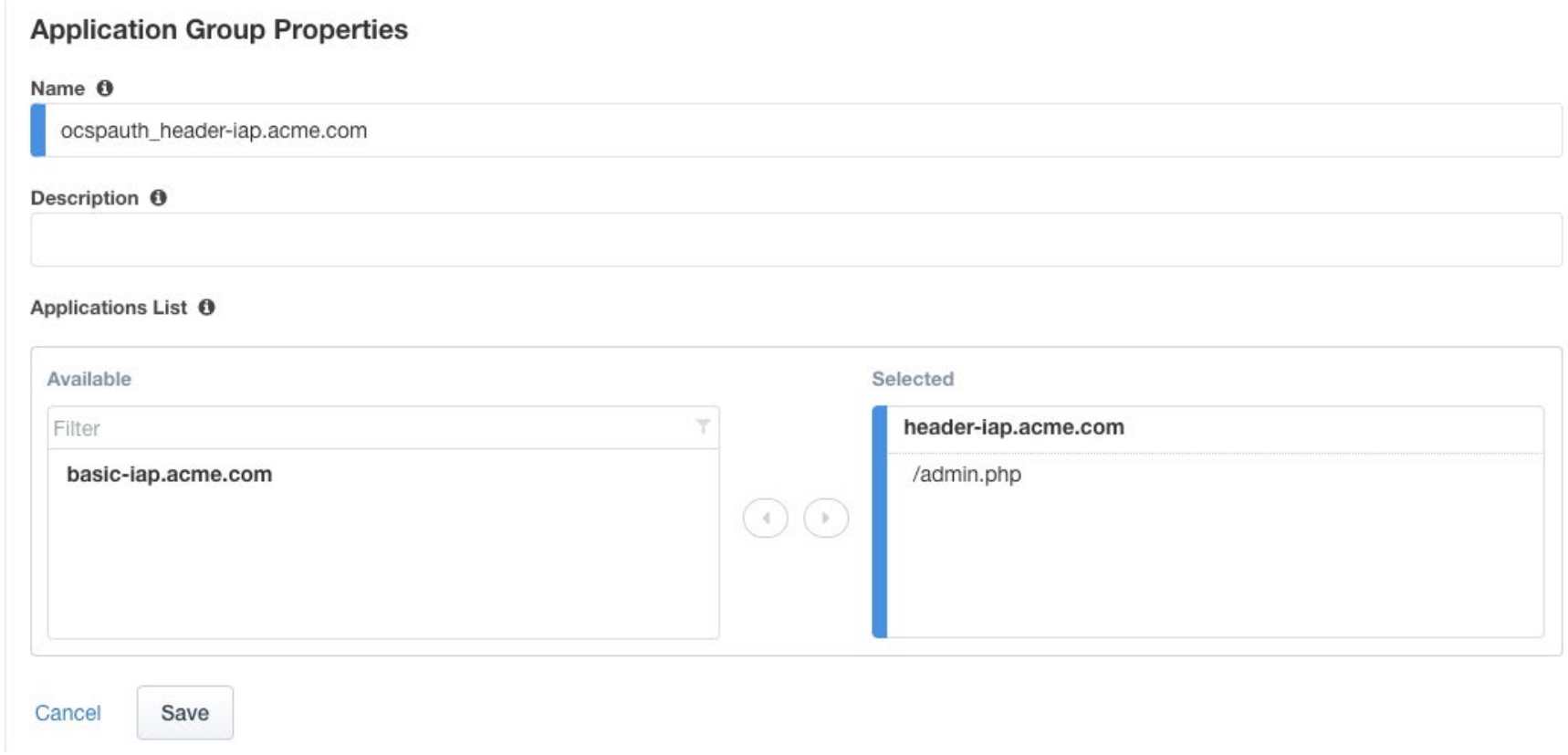




Applications



Application Groups



Contextual Access

Contextual Access Properties

Name

basic-iap.acme.com

Resource Type ⓘ

Application

Resource ⓘ

basic-iap.acme.com

Device Posture ⓘ

FW_CHECK

Primary Authentication ⓘ

ad

HTTP Header ⓘ

--Select--

Single Sign-On ⓘ

basic_sso

☑ **Enable Additional Checks** ⓘ

Trigger Rules

Trigger rules are executed in the order they appear. If trigger rules are not defined, then the default fallback rule is executed.

Add | Delete

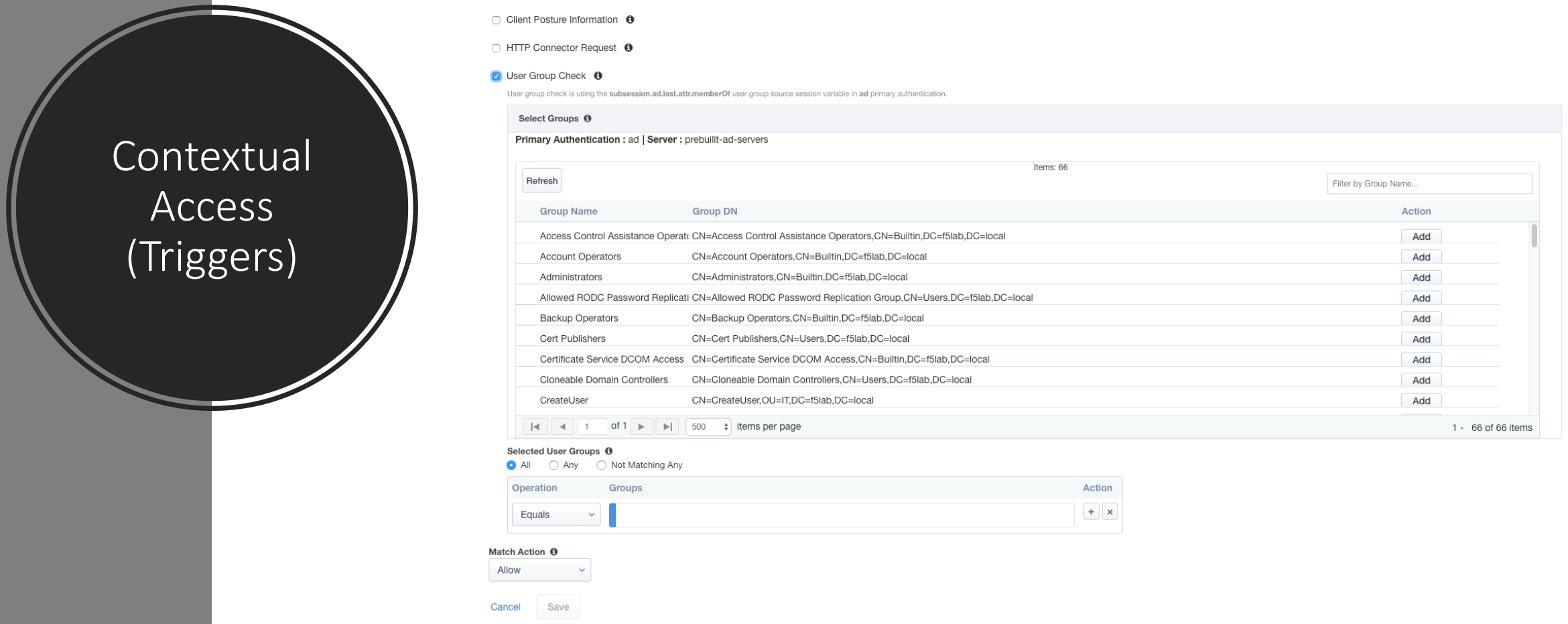
Items: 1

Filter Type by Name...

☐	Name	Trigger Types	Match Action	Sequence
☐	get-user-status	**HTTP Connector Request** ⓘ	**Step Up** ⓘ	
	Default Fallback ⓘ		Reject	

Cancel | Save

Contextual Access (Triggers)



Customization

Logon Page

Form Header Text

Secure Logon
 for F5 Networks

Type the text to display for the form header.

Logon Page Input Field #1

Type the text to display for the first field on the logon page. Usually, it's **Username**.

Logon Page Input Field #2

Password

Type the text to display for the second field on the logon page. Usually, it's **Password**.

Logon Button

This is the label for the logon button. It defaults to **Logon**.

Remediation Page

Software download URL

https://iap1.acme.com/epi/downloads

Error Messages

Invalid client data

Endpoint Inspection error. Please contact your system administrator for assistance.

Network Firewall check failed

Network Firewall check failed.

Antivirus software check failed

Antivirus software check failed.

Patch management check failed

Patch management check failed.

Hard disk encryption check failed

Hard disk encryption check failed.

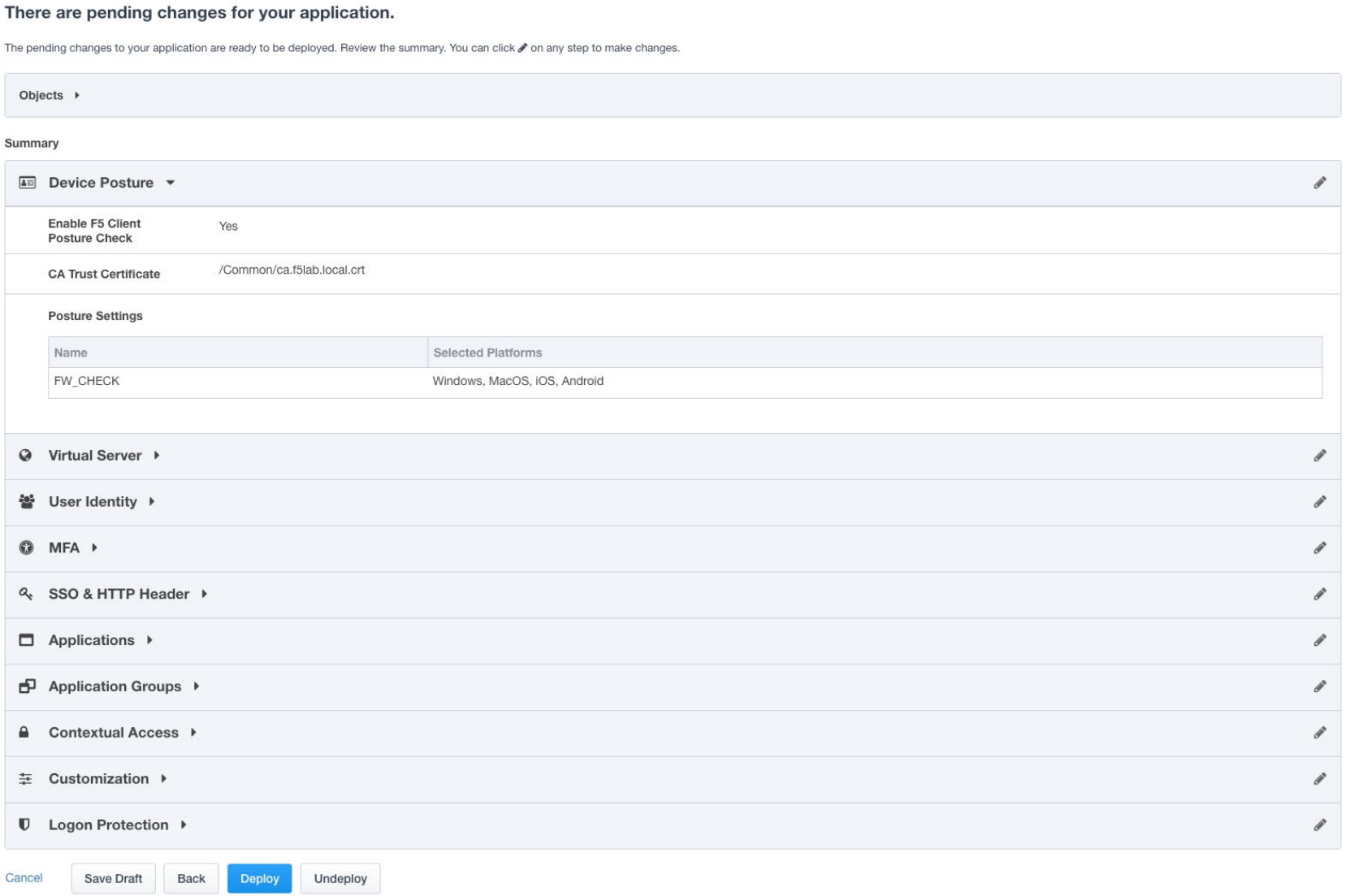
File check failed

File check failed.

Health Agent check failed

Health Agent check failed.

Summary


There are pending changes for your application.
The pending changes to your application are ready to be deployed. Review the summary. You can click on any step to make changes.
Objects
Summary
Device Posture
Enable F5 Client Posture Check
Yes
CA Trust Certificate
/Common/ca.f5lab.local.crt
Posture Settings
Name
Selected Platforms
FW_CHECK
Windows, MacOS, iOS, Android
Virtual Server
User Identity
MFA
SSO & HTTP Header
Applications
Application Groups
Contextual Access
Customization
Logon Protection
Cancel
Save Draft
Back
Deploy
Undeploy

LAB TIME