Deployment Options Guide

PrecisionAccess

Executive Summary

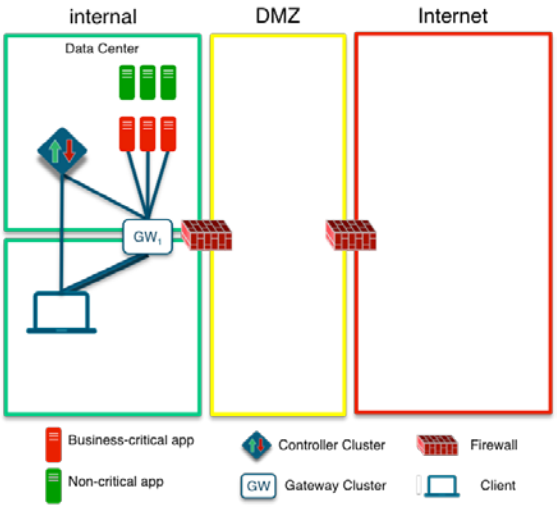
PrecisionAccess consists of a Controller Cluster and one or more Gateway Clusters that can be located in any of the following networking environments: on the internal network, on the DMZ, or on the Internet. In addition, the Controller Cluster interacts with the SAML Identity Provider (IdP), which can also be located in any of those environments. This document discusses the advantages and disadvantages of deploying in each environment.

Table of Contents

Controller Cluster Placement

Controller on the Internal Network

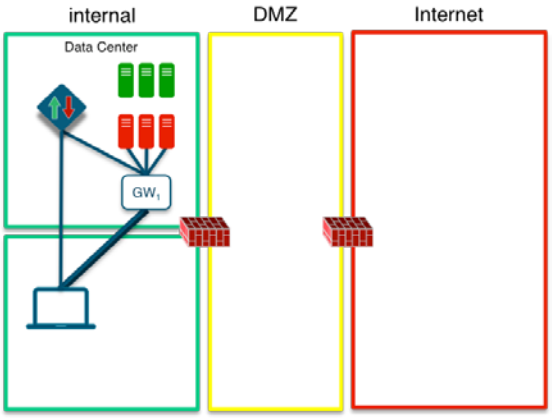
Today, most of the business-critical applications are located in a dedicated data center on the enterprise internal network. Therefore, it is logical to want to put the PrecisionAccess Controller Cluster and Gateway Clusters on the internal network, as well. As pictured at the right, this is a perfectly reasonable deployment option.



As shown in the picture, the business critical applications (in red) can only be accessed via PrecisionAccess. At some point in time, most enterprises want all applications protected by PrecisionAccess. And, PrecisionAccess makes it possible to accomplish this – one or more applications at a time. Therefore, with PrecisionAccess, corporations can begin by greatly increasing the security posture of their most business critical applications. Then, over time, essentially fulfill the entire role of Network Access Control (NAC) in protecting all servers from unauthorized clients, while at the same time providing extensive visibility into each authorized endpoint.

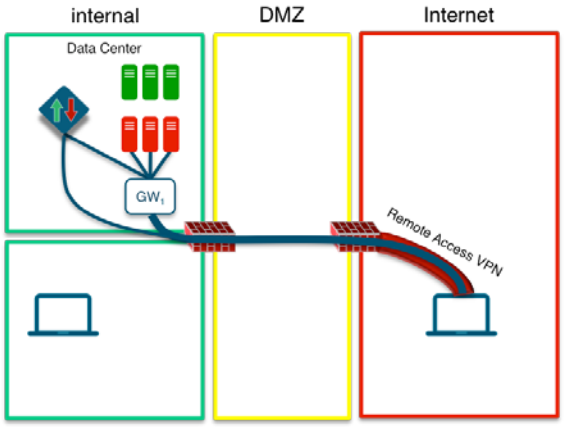
In this implementation, typically, the clients must be a member of the domain to access the network, which provides additional controls on the client. However, network admins should also enable PrecisionAccess posture checking and trust assessment to significantly improve the trust of clients accessing business critical applications.

Also, note, that in the above implementation, the Gateway Clusters are 2-port devices such that the traffic from the user network to the data center bypasses the firewall. This reduces the load on the firewall, and can result in some cost savings. Alternatively, in the picture at the right, all traffic – both to protected applications and unprotected applications – goes through the firewall. Both options work equally as well. And both options make it very easy to implement firewall rules to block users from direct access to the protected applications without first going through PrecisionAccess.



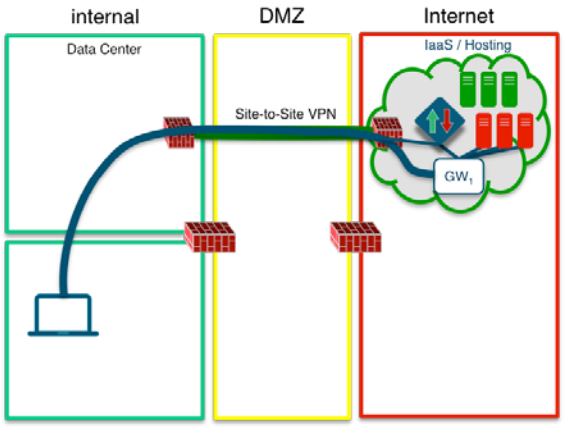
VPN Access for Remote Users

With the Controller on the internal network, remote users will have to VPN into the internal network to access the protected applications in the same way they do today for all internal applications. PrecisionAccess is unique in that it is one of the few implementation of the Software Defined Perimeter (SDP) that works over a remote access VPN. As shown in the picture at the right, the client on the Internet is connected to the firewall via a remote access VPN tunnel (shown in red). Then, access to both the Controller Cluster and to the Gateway Clusters is provided over that tunnel. This is a great way to greatly increase the security of business-critical applications without changing the users' workflow.



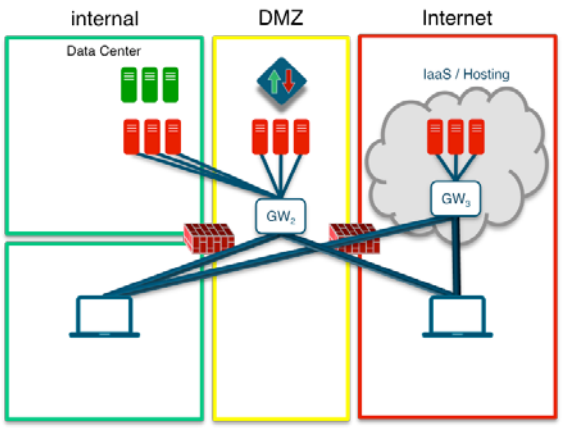
PrecisionAccess Hosted in a Hybrid Cloud

Today, many corporations are moving to a hybrid cloud model in which they extend their existing data center to Infrastructure as a Service (IaaS) providers such as Amazon AWS, Microsoft Azure, Google Compute Engine, and IBM SoftLayer by creating a site-to-site VPN connection to those services as shown in the picture to the right.



The hybrid cloud architecture effectively extends the internal network into the virtual private cloud of the IaaS provider. Therefore, one can put the PrecisionAccess Controller Cluster and the Gateway Clusters in those locations, too, if desirable. Changes to the networking infrastructure are not needed. Basic switching and routing will inherently provide the appropriate access to the PrecisionAccess infrastructure, as needed.

Controller on the DMZ



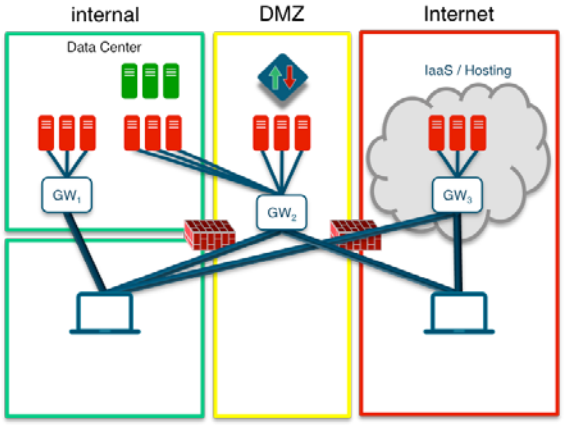
A very common alternative to the Controller Cluster on the internal network is to put the Controller Cluster on the DMZ. This still locks down business-critical applications and scales to encompass all applications like one would get from NAC, but also adds transparent access to remote users and the ability for remote users to directly access applications in the cloud without having to backhaul through the corporate network.

As one can see from the picture, clients on the internal network connect to a Controller on the DMZ and are then directed to Gateways in one or more Gateway Clusters such that they can access applications on the internal network, DMZ, and/or on the Internet. Similarly, clients on the Internet (at home, hotels, coffee shops, etc.) can do the same.

Internet Applications Become Invisible

One of the advantages of this deployment is that enterprise applications in hosting centers and in IaaS providers can be accessed directly by users, but which “don’t exist” on the Internet for unauthorized users. The applications “don’t exist” because the PrecisionAccess Gateways provide access to authorized users on authorized devices, only.

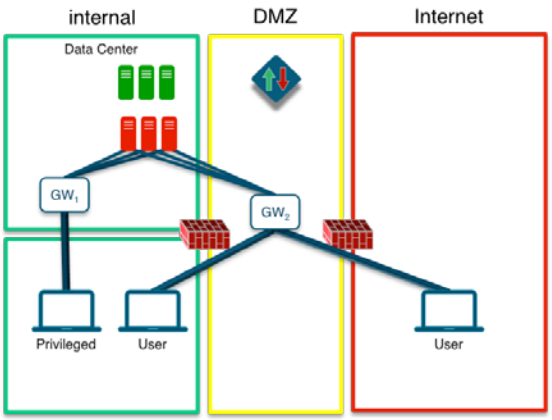
Access from the Internal Network, Only



With the Controller Cluster in the DMZ, it’s still possible to require the client to be on the internal network to access certain applications. This can be done by putting a Gateway Cluster that can only be accessed from the internal network, as shown on the left hand side of this picture.

Therefore, the “Controller in the DMZ” implementation provides the best of both worlds, it can lock down critical applications such that they can only be accessed from the internal network, and provide access to other applications from both the internal network and the Internet.

Privileged Access from Internal Only

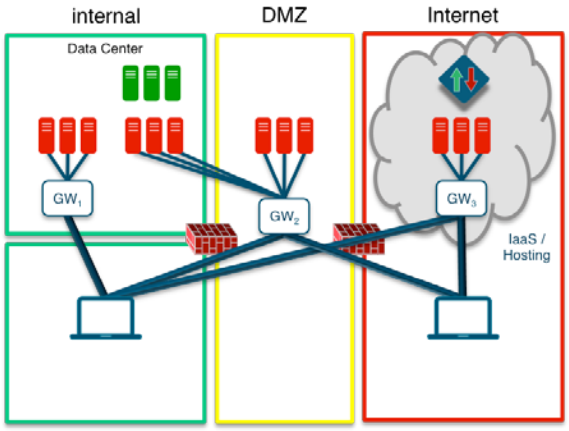


Continuing with the thought above, the corporation may have some applications where users should receive access from anywhere, but application owners and IT admins must be on the corporate network to access the servers. As shown at the right, this is easily implemented with PrecisionAccess.

An example of this split access methodology would arise if application owners and IT admins were required to be on the internal network to access FTP and RDP, respectively. However, users could access the web application (i.e., http/s) on those servers from anywhere. As shown in the picture, only GW_1 would be allowed to access the FTP and RDP services of the servers, where as GW_2 would provide all users (including application owners and IT admins, as appropriate) access the web application.

Controller on the Internet

The third major option is to put the Controller Cluster on the Internet. The picture on the right shows this implementation. This deployment option looks almost identical to the DMZ-based controller above, and it implements all the same use cases – including protecting applications in the data center, on the DMZ, and on the Internet (i.e., in the cloud and at hosting centers).



Same as Controller on the DMZ, Almost

In comparing the this deployment option with the Controller on the DMZ, we see customers who have a "Cloud First" policy selecting this path, where as more traditional security professionals prefer the latter option.

However, there is one minor differentiating factor between the two, and that is, "What happens if the WAN link goes down?" For many organizations, business productivity depends on WAN access to such an extent, that the question is moot – if the WAN link goes down, productivity is lost.

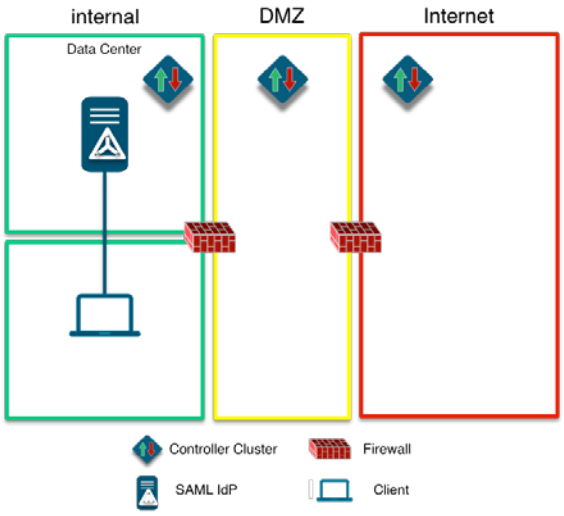
However, in some companies, this dependency on the WAN link may not exist yet. With the Controller on the Internet, if the WAN link goes down, no additional internal connections will be created.

Later, we will see that if the SAML Identity Provider is deployed through Microsoft Azure AD, Okta, or any of the other identity-as-a-service providers, then the company already has the dependency on the WAN link, and, therefore, this issue goes away.

SAML IdP Deployment

Just like the Controller Cluster, the SAML Identity Provider (IdP) can be deployed on the internal network, on the DMZ, and/or on the Internet.

IdP on the Internal Network



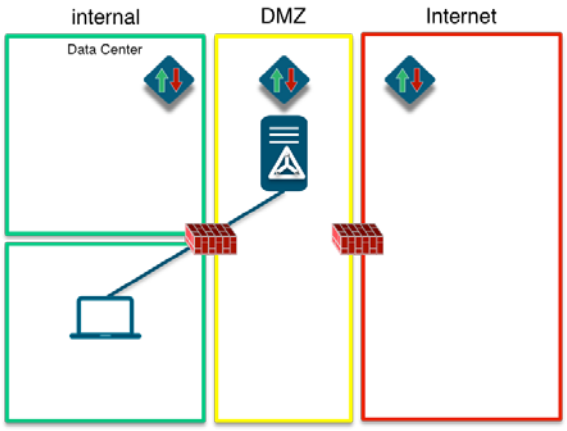
While it is more common to deploy the IdP on the DMZ or on the Internet, a number of organizations have deployed the IdP on the internal network to provide Single Sign On (SSO) across computer platforms. Two key benefits of this deployment are: 1) the IdP is not exposed to the Internet and 2) it is easy to take an existing Active Directory (AD) server and turn it into an IdP by enabling the Active Directory Federation Service (AD FS).

Note that if the IdP is only exposed to the internal network, then the users will have to be on the internal network to access it. Therefore, remote users will have to VPN in before connecting to the IdP.

Note, also, that as shown with the Controller Cluster on the internal network above, the IdP can be placed in a hybrid cloud with site-to-site VPN connecting the VPC of the hybrid cloud to the existing data center of the internal network.

With the IdP on the internal network, often, the Controller Cluster will be placed on the internal network, too. However, that does not need to be the case. Rather, the Controller Cluster can be deployed on the internal network, on the DMZ, or in a hosting center or IaaS – as shown in the picture by depicting the Controller Cluster in all three environments.

IdP on the DMZ

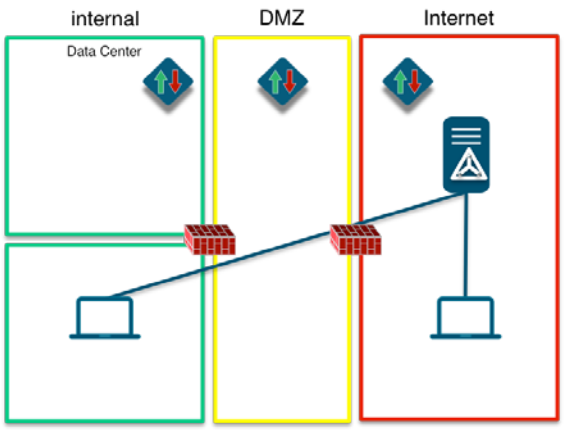


When the SAML IdP is created using an enterprise product such as CA SiteMinder, it is typically deployed on the DMZ with access from both the internal network and from the Internet such that it can provide SSO for both Internal applications and Cloud-based applications. Usually, this also means that the IdP will have a different DNS entry for the internal network vs. the Internet. And, sometimes, it will even involve different authentication policies such as Integrated Window Authentication (IWA) for internal users, but some less automated log in for external users.

Again, the Controller Cluster can be anywhere.

IdP on the Internet

Many companies are now moving to SSO as a service via Microsoft Azure AD, Okta, or many of the other SAML-based services. This places the IdP on the Internet.



Note that this also makes connectivity to protected applications dependent on a reliable WAN connection – just like with the Controller on the Internet.

And, as with the other two IdP deployment options, the Controller Cluster can be on the internal network, on the DMZ, or in a hosting provider of IaaS.

Independently Deployed

As discussed above, the Controller Cluster can be deployed in any of the environments independently of where the IdP is located because the communication between the Controller Cluster and the IdP is via the browser on the client. Therefore, the only requirement is that the Client can connect to both the Controller Cluster and the IdP. Hence, if either the Controller Cluster or the IdP is only accessible from the internal network, then the users must be on the internal network. Otherwise, the users can be anywhere.

Integrity and Confidentiality

To maintain the integrity of both the SAML Request (from a Controller to the IdP) and the SAML Assertion (from the IdP to the requesting Controller), both the SAML Request and SAML Assertion must be signed. In addition, the contents of the Request and Assertion may be, optionally, encrypted. The cryptographic key pairs and certificates for signing and encryption are exchanged out-of-band via the exchange of SAML Meta Files.

Authentication vs. Authorization

After the user completes the authentication process, the SAML Identity Provider sends a SAML Assertion to the Controller. The Assertion will always state whether or not the user is an authenticated member of the domain. In addition, the Assertion can return the list of applications the user is authorized to access. This is typically done by returning the “groups the user is a member of,” where the groups represent one or more applications the user is authorized to access.

Vidder highly recommends SAML Assertions that include the list of authorized applications. Recall that the method by which security is obtained is by limiting access to only authorized users. PrecisionAccess is unique in that it is the only security control that limits access to authorized users on trusted, authorized devices in a scalable way.

Limiting access is even more important for the most business-critical applications of the company, and, typically, those applications will be the first ones a company chooses to protect with PrecisionAccess. Therefore, if business-critical applications need to be protected, Vidder highly recommends having a group in LDAP (e.g., in AD) that represents authorized access to each application on a per user basis, and that each group name be returned in the SAML Assertion.

However, two other methods of determining authorized users are supported by PrecisionAccess. The simplest is to allow all authenticated users of the domain access to all protected applications. When PrecisionAccess receives the Assertion that the user is an authenticated user of the domain, PrecisionAccess will provide connectivity to all protected applications. This may work initially when the number of protected applications is small, but it clearly does not provide the very high level of security that PrecisionAccess is know for.

The second method is to supply Vidder with the list of all of the authorized user ID’s prior to enabling PrecisionAccess. Then, when PrecisionAccess receives the Assertion that the user is an authenticated user of the domain, PrecisionAccess will compare the user’s ID to the list of authorized ID’s. If the user is authorized for one of more applications, then PrecisionAccess will provide the appropriate connectivity. Again, this may work for a relatively small number of users on a small number of

applications, but it does not scale to tens or hundreds of thousands of users on tens to hundreds to thousands of applications.

Adding a SAML IdP

If a company does not have a SAML IdP, probably the easiest thing to do is to create one by enabling the Active Directory Federation Service (AD FS) on any Active Directory Domain Controller. This can be done in under 15 minutes by an experienced admin. The scope of access can easily be limited to the PrecisionAccess Controller Cluster with simple firewall rules.

Alternatively, Vidder can provide a “Directory Connector” that provides the SAML IdP function to the Controller Cluster by connecting to one of the corporate LDAP servers.

Summary Table

Controller Cluster *	Comments
Internal corporate network	A reasonable choice for network admins who believe the internal network is more secure than the Internet. Requires remote users to VPN into the network before accessing protected applications. PrecisionAccess is uniquely capable of running over remote access VPN connections.
DMZ	Enables the full transparent user experience, where users can access protected applications from anywhere with transparent MFA and an “always on” connection. It is safe to put the Controller Cluster and Gateway Clusters on the DMZ because both are protected from all network-based attacks by Single Packet Authorization (SDP) and mutual TLS.
Hosting / IaaS	The likely choice for corporations with a “Cloud First” policy. A minor concern if the reliability of the WAN connection – unless the IdP is on the Internet, too, in which case there is already that dependency.

* The deployment of the IdP is independent of the deployment of the Controller Cluster. The IdP can be deployed on the internal network, the DMZ, or on the Internet for each of scenarios above. If the company does not have a SAML IdP, Vidder can provide a Directory Connector to the corporate LDAP directory.