InflectionIT

SharePoint Lookup Table

- Intapp Walls relies on a lookup table to match sites to clients / matters
- This lookup table ideally lives on the same SQL database used by SharePoint
- This table must be populated by the firm either manually or by a custom script.

	SiteUrl	ClientId	MatterId
1	http://sharepoint.firm.com/1000/	1000	NULL
2	http://sharepoint.firm.com/1000/0001/	1000	0001
3	http://sharepoint.firm.com/1000/0002/	1000	0002
4	http://sharepoint.firm.com/1000/0003/	1000	0003
5	http://sharepoint.firm.com/2000/	2000	NULL
6	http://sharepoint.firm.com/2000/0001/	2000	0001
7	http://sharepoint.firm.com/2000/0002/	2000	0002
8	http://sharepoint.firm.com/2000/0003/	2000	0003
9	http://sharepoint.firm.com/3000/	3000	NULL
10	http://sharepoint.firm.com/3000/0001/	3000	0001

InflectionIT

COM Module Only

- Intapp Walls writes security using native SharePoint Client Object Model (COM)
- COM does not support explicit denies
- External users can be configured to be ignored by Intapp Walls using a REGEX

Intapp Walls writes directly to SharePoint native security: Client Object Model (COM)

Intapp Walls Extension Service

SharePoint native security does not support denies, Exclusionary walls must be written as including everyone with access to the site except denied users.

Configurable Access Denied Page

WALLBUILDER by Intapp

Intapp Walls Server

SharePoint

SharePoint IIS Server(s)

COM Module Only

Pros	Cons
3rd party tools that rely on SharePoint native security are automatically supported	**No explicit denies** – performance associated with adding all users except those denied can be unacceptable at larger firms or those with many exclusionary walls.
Uses native SharePoint security – does not require installing anything extra on top of SharePoint.	**Performance** - SharePoint does not allow direct calls to a SQL database, thus applying and repairing security can be slow compared to systems that allow database access like iManage or DM5.

COM Exclusionary Performance

Performance greatly improves if sites are not public by default.

If User A is denied access to a matter:

If Group containing Users A, B, C have access:

Intapp Walls will create new ZZINT SharePoint group to have access adding Users B and C.

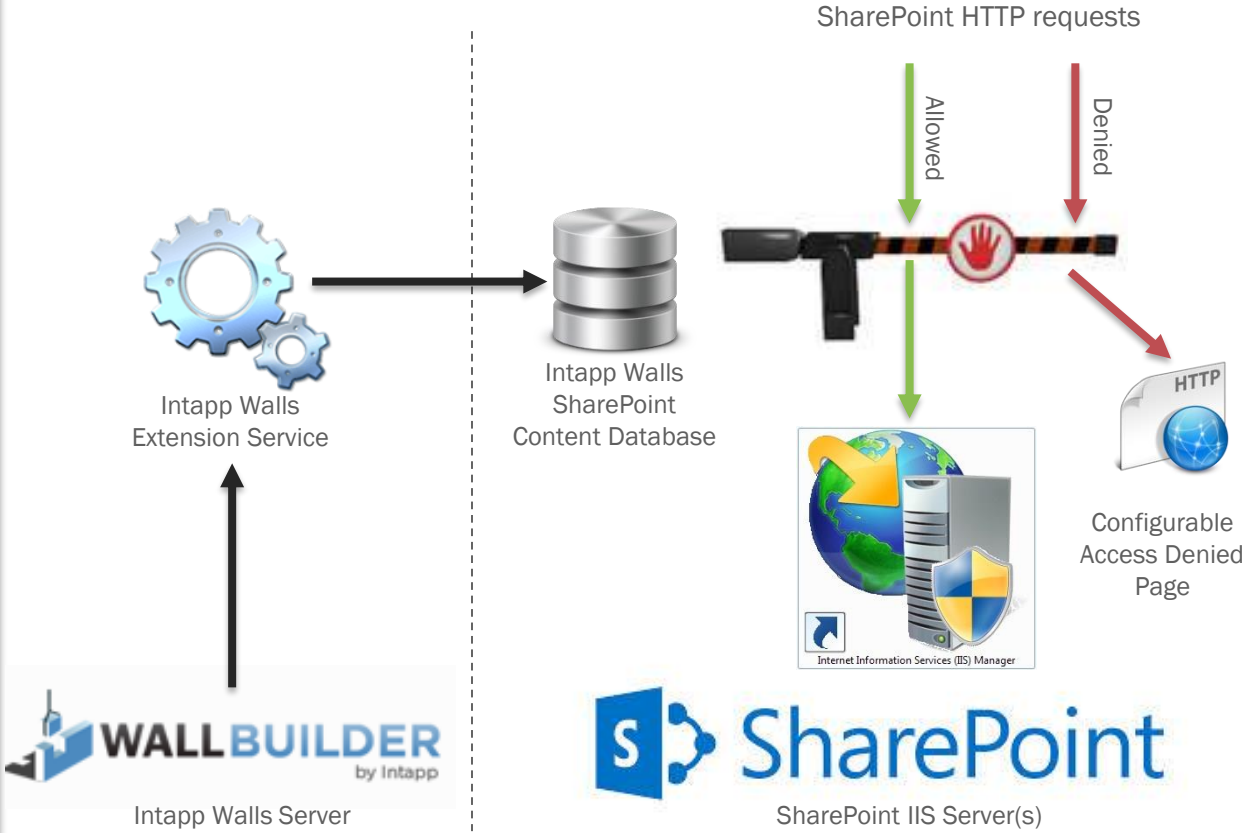
If EVERYONE group containing 1000 users is granted access:

Intapp Walls will create new ZZINT SharePoint group to grant access to 999 users - - **SLOW** - – (all except user A)

InflectionIT

HTTP Module Only

- An HTTP interceptor that sits on top of the SharePoint IIS server. Includes Search Trimmer
- Users making SharePoint requests are validated against Intapp Walls.
- Users without access will be forwarded to a configurable denied page.



HTTP Module Only

InflectionIT

Pros	Cons
Very fast performance	SharePoint in the Cloud not supported
Allows explicit denies	3rd party tools not supported
Allows securing individual objects using custom Client/Matter labels	User must have access to underlying site to be granted access (this is a pro to some firms)

Notes Intapp Walls SharePoint Support

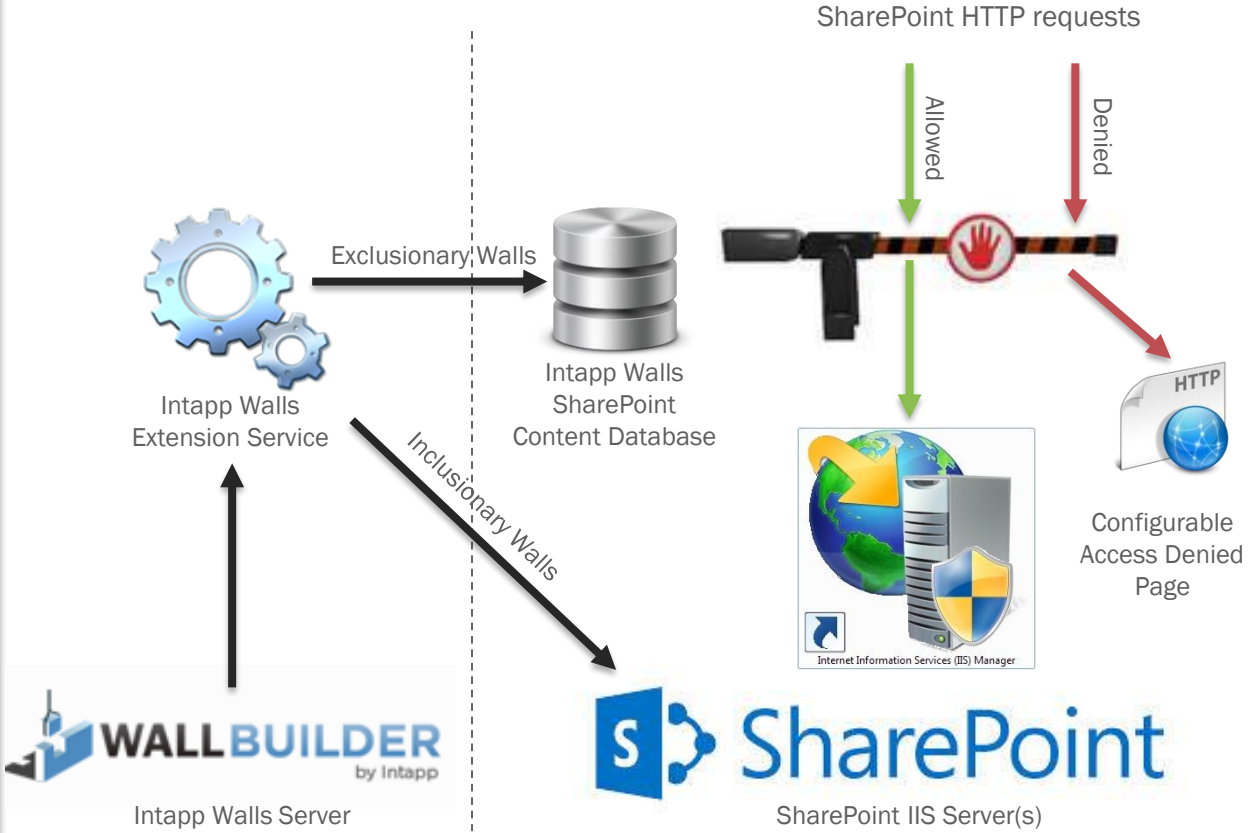
InflectionIT

- Supported SharePoint versions: 2010, 2013 and SharePoint Online
- Intapp Walls 6.1 added:
  - **Created assemblies** – Added support for the various SharePoint COM API versions: COM API v14 for SharePoint 2010, COM API v15 for SharePoint 2013 and COM API v16 for SharePoint Online.
  - **Office365 SharePoint Online** – Added support for securing SharePoint Online in Office365 using the COM model. As a prerequisite, the **SharePoint Server 2013 Client Components SDK** must be installed on the Intapp Walls Extension Service server. The extension uses the UPN (user principal name) to identify users in SharePoint Online.
- COM on hosted SharePoint was supported prior to Intapp Walls 6.1 without the above improvements
- HTTP Module security is only supported on premise due to Microsoft cloud security restrictions.

InflectionIT

HTTP for Exclusionary, COM for Inclusionary

- **Intapp best practice for on premise installs**
- Inclusionary walls will be written using native Client Object Model
- Exclusionary walls will be enforced using the HTTP module



HTTP for Exclusionary, COM for Inclusionary

InflectionIT

Pros	Cons
3rd party tools respect inclusionary walls	3rd party tools do not support exclusionary walls
Good performance	
Exclusionary walls don't require adding everyone except those denied	
Inclusionary walls will grant a user access regardless of whether they had prior access to the site.	