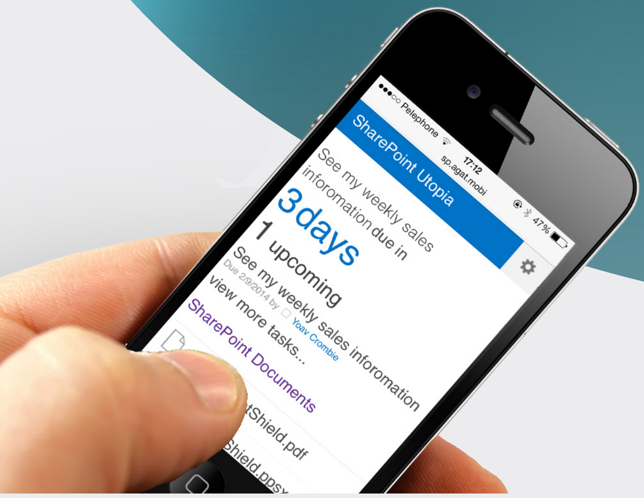
AGAT
Software Development

SharePoint SHIELD

Securing SharePoint mobile Connectivity



Key Features

- Active Directory password protection
- Block Dos & Brute-force attacks
- Smart Card policy solution for mobile
- Two-factor authentication for specific third part clients
- No additional client install
- Available for Microdot TMG/ISA and Bastion on windows or Linux

For today's mobile enterprise, the need to connect smartphones to the corporate network has become a vital business requirement. To protect their sensitive business data, mobile enterprises require easy-to-deploy tools that secure the connectivity of personal mobile devices with corporate SharePoint servers.

Background

The widespread use of smartphones has revolutionized the way we work, play and interact. Mobile devices allow us to be connected 24x7, giving us access to information anytime, anywhere. Whether your company has adopted a Bring Your Own Device (BYOD) strategy or supplies corporate mobile devices to its employees, these devices represent a major information security threat , due to the sensitive data that they often carry.

Using their personal devices, employees commonly connect to the corporate network from home or from public non-managed networks, increasing the risk of data leaks and possible exposure of a user's network credentials. Moreover, since there is no control over the apps employees install on their smartphones, these devices are more prone to malware infection.

Securing SharePoint Connectivity

Smartphones and personal computers can connect to Microsoft SharePoint server using mobile browsers or third parts clients. While connected sensitive information is exposed requiring the organization to take precautions. Companies realize that securing SharePoint mobile connectivity is as important as securing remote access, since smartphones can be used as a tunnel into the corporate network. SharePoint Shield as part of the mobility-shield product suite is specifically designed to address the complex security needs of today's mobile enterprise.

Introducing the SharePoint Shield Product Suite

Unlike most mobile security solutions that focus on protecting the data stored on the mobile device through encryption strategies and containerization, SharePoint Shield offers a new approach that completely eliminates the need to store Active Directory passwords on the device. With SharePoint shield the connection to SharePoint is done by using dedicated SharePoint credentials that are created by the user rather than the regular network Active Directory credentials.

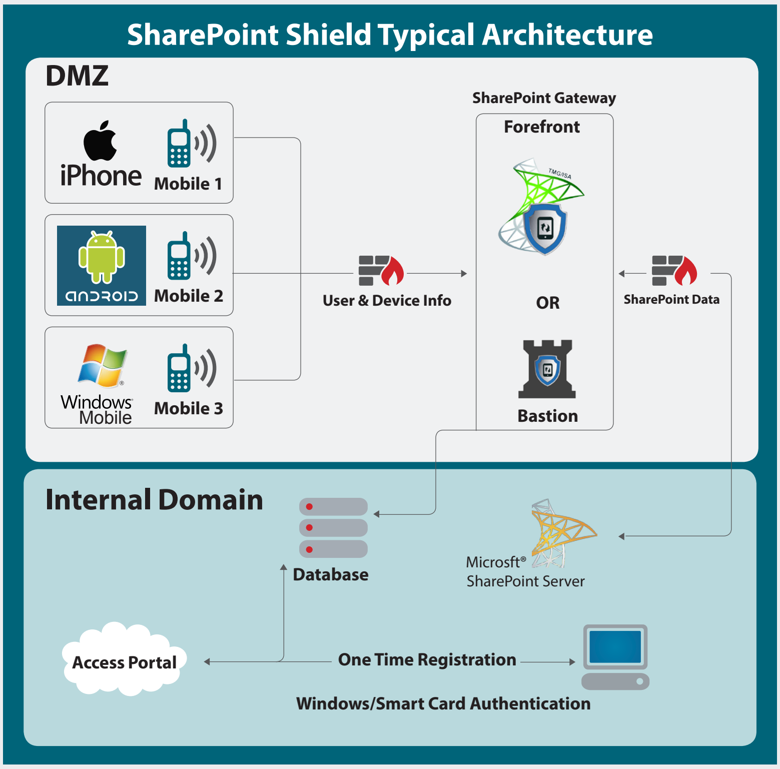
SharePoint Shield interacts directly with the client - server traffic. The solution effectively controls who can connect to the network based not only on credentials but also on the device in use. Since SharePoint Shield does not require any additional client installation, it is ideal for BYOD .

The ability to intercept the authentication process also enabled the product to block Dos / DDos and brute force attacks.

SharePoint Shield Architecture

The SharePoint Shield was specifically developed for Microsoft environments and is naturally integrated with the Forefront TMG/ ISA server family. As a server side software solution, the SharePoint Shield can be easily and quickly installed on the relevant gateway and does not require any client side software.

SharePoint Shield is also available as a standalone gateway (Bastion server) that can be located behind firewalls such as F5 or others. Using Bastion can be done either on Windows or on Linux.



Active Directory Protection

Key Features

- Avoid using Active Directory credentials on mobile device / laptop.
- Block DoS attacks.
- Block Brute force attacks.
- Avoid account lockout.
- Solution for Smart card login policy.

Mobile devices represent a security threat to your corporate network. User credentials are stored and used on the device in public networks, while users install apps on their devices without knowing the source. This raises a few issues:

1. Your Active Directory username and password can be hacked and used to provide access to many core business applications.
2. Potentially allowing someone else to access your SharePoint information.
3. Exposing your Active Directory to Dos and brute-force attacks.

For these reasons, securing access control is essential sharePoint Shield offers a new approach to solve these issues by defining dedicated SharePoint credentials.
Following are a few examples of how your organization can improve SharePoint connectivity security using the dedicated login feature in the SharePoint Access Control module:

Avoid Storing Active Directory Credentials on Device

Using the Active Directory credentials in the non-secure environment of a mobile device introduces risk. The exposed credentials could be hacked and used to either get access to your SharePoint information like docuents or login to other corporate applications.

Hacking is typically done in two ways in the mobile world: "Eavesdropping" on public networks, or hostile applications installed by users or received by SMS.

SharePoint shield offers a new approach for protecting the Active directory credentials by defining dedicated SharePoint credentials that are different from the network Active Directory credentials. The dedicated login option offers a higher level of security as AD credentials are not stored on the mobile device.
In this scenario, the user creates dedicated SharePoint credentials on the Access Portal self service web site. Only the dedicated credentials are used with the mobile device and the Active directory credentials are now fully protected as they do not leave the network.

Smart Card Solution

Many organizations with high security requirement use smart card or token for network login. In these networks, users do not have a username and password for Active Directory. SharePoint Access Control allows the usage of SharePoint without the need to manage Active Directory credentials. With the dedicated login solution, the user logs into the Access Portal, authenticates with his smart card from his network computer and creates dedicated SharePoint credentials for use on the mobile device/ external laptop / desktops.

Active Directory Account Lockout Guard

Account lockout can be a result of two scenarios:

- User has changed the Active Directory password but did not change the device settings, so the device keeps trying to authenticate with the old password.
- An attacker that has the username (without the password) tries to login several times SharePoint Shield solves this issue by blocking false attempts at the gateway level.

Block DoS attacks and brute force attacks

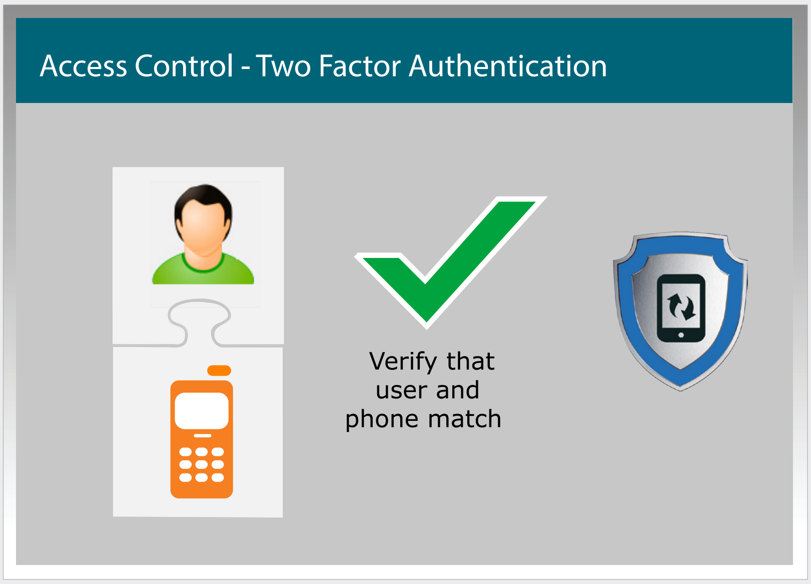
Publishing SharePoint to the internet exposes your network to Dos (denial-of-service) and brute force attacks. These can cause your network to become unavailable and cause significant business damage. The SharePoint Shield blocks these attacks on the gateway level by configuring a block failed login policy thus blocking the attack attempts from reaching the Active Directory.

SharePoint Access Control for Two Factor Authentication

Key Features

- Two-factor authentication using the smartphone as something you have and the password as something you know.
- Self-service access portal to support two-step registration of users.
- Admin auditing and control tools for approving devices.
- Multiple enrollment options

Remark:
The Two Factor Authentication is available for specific third party SharePoint clients



Access Control - Two Factor Authentication

Verify that user and phone match

Device Registration Options

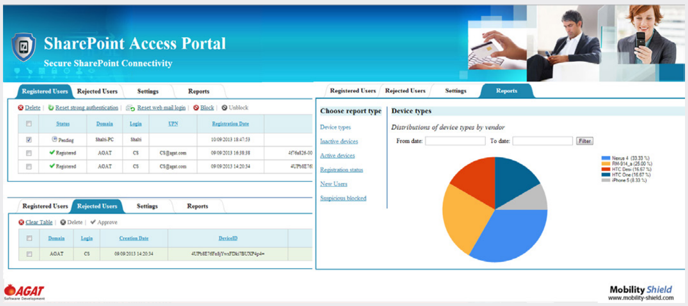
SharePoint Access Control supports various enrollment options:

- Automatic Registration - A device is registered the first time a user connects to SharePoint. Once registered, SharePoint Access Control then verifies during subsequent synchronizations that the operation is in fact performed from the registered device. Any attempt to connect with the user’s credentials from a different device will be blocked.
- Two Step Registration - This option employs a tighter security approach that requires the user to first register on a dedicated Access Portal and then connect within a short period of time (defined in portal configuration) in order to complete registration.

Admin User Management and Auditing

LyncSharePoint Shield includes an admin website “Access Portal” for tracking the user registration process, approving blocked users, deleting users, changing registration site settings and more.

For enterprise installations with multiple domains, the admin site can be managed separately for each domain, allowing each helpdesk to manage the users in its domain.



SharePoint Access Portal

Secure SharePoint Connectivity

Registered Users | Rejected Users | Settings | Reports

Delete | Reset strong authentication | Reset web mail login | Block | Unblock

□	Status	Domain	Login	UPN	Registration Date	
☑	Pending	Shalti-PC	Shalti		10/09/2013 18:47:53	
□	✓ Registered	AGAT	CS	CS@agat.com	09/09/2013 16:38:38	4f76a826-00
□	✓ Registered	AGAT	CS	CS@agat.com	09/09/2013 14:20:34	4UPb8E76

Registered Users | Rejected Users | Settings | Reports

Clear Table | Delete | Approve

□	Domain	Login	Creation Date	DeviceID
□	AGAT	CS	09/09/2013 14:20:34	4UPb8E76Fn8jYwxFDki7BUXP4p4=

Registered Users | Rejected Users | Settings | Reports

Choose report type

- Device types
- Inactive devices
- Active devices
- Registration status
- New Users
- Suspicious blocked

Device types

Distributions of device types by vendor

From date: To date: Filter

Bastion Reverse Proxy Server

Key Features

- Secure remote access to corporate resources without Microsoft Forefront
- Fully compatible with mobility- Shield product suite and SharePoint shield
- High scalability and throughput Available for both Windows and Linux

Standalone Gateway for Mobility - Shield

Bastion is a lightweight, extensible and highly scalable reverse proxy server solution, focused on content filtering for HTTP(S) traffic. Bastion is designed to enable organizations that do not use Microsoft Forefront gateways to take advantage of the Mobility Shield product suite.

Bastion forwards traffic to the configured backend servers (e.g. SharePoint or internal website). However, by employing a pluggable filtering architecture, it can be easily extended to support any kind of filtering through filter modules. Many of AGAT Software’s security products (including the SharePoint Shield suite) are already available as Bastion filters.

Scalable Event-Driven Architecture

Bastion is designed as an event-driven server using asynchronous I/O which uses multithreading to respond to requests. This significantly reduces the overhead as opposed to thread-driven synchronous I/O architectures. Accordingly, the event-driven architecture greatly enhances scalability, allowing Bastion to handle a higher number of concurrent TCP connections compared to process or thread-driven reverse proxy servers.

Bastion can operate on both HTTP requests and responses. Requests and responses can be blocked, modified or left as is (if no filtering is needed). Since Bastion offers maximum HTTP protocol compatibility (beyond the common web usage subset), it can be used to filter almost any HTTP-based protocol, such as SharePoint traffic .

About AGAT

AGAT founded in 1999, began its operations as a Microsoft software development consulting firm. Today, the company focuses most of its efforts on web development, with special expertise in security applications and digital signature solutions.

Over the past few years, AGAT has developed three lines of products: AGSecurity suite, AGForms (web forms development and management infrastructure) and AGSign (digital signature solutions).

AGSecurity suite includes several security products that address the complex network requirements of enterprises and large organizations. Many of the products in this suite are offered as an extension for Microsoft Forefront servers (ISA/IAG/TMG/UAG).
AGAT's customers consist of government offices, banks, insurance companies and large industrial corporations (including Fortune 500 companies).

AGAT
Software Development

Please visit our sites:
Company site: www.agatdev.com
Product site: www.mobility-shield.com

For more information
Contact us:

Agat Software Development
info@agatsolutions.com
57 Hagefen Street, Asseret, Israel
Tel/Fax: 972-8-8598456