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 synchronization of personal mobile devices with the Exchange server.

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 ActiveSync Connectivity

Smartphones synchronize with your Microsoft Exchange server using the ActiveSync data protocol. While synchronization enables your employees to access email, email attachments, calendar, tasks and contact lists from anywhere, this process must be absolutely secure in order to prevent loss of confidential information. Companies realize that securing ActiveSync is as important as securing remote access, since smartphones can be used as a tunnel into the corporate network. ActiveSync Shield is specifically designed to address the complex ActiveSync security needs of today’s mobile enterprise. Featuring several powerful modules, ActiveSync Shield effectively controls mobile access and data synchronization when employees connect to an Exchange server with their mobile phones.
Introducing the ActiveSync Shield Product Suite

Unlike most mobile email solutions that focus on protecting the data stored on the mobile device through encryption strategies and containerization, ActiveSync Shield offers a new approach that completely eliminates the need to store data and Active Directory passwords on the device. ActiveSync Shield interacts directly with the ActiveSync protocol on the server side. This solution effectively controls who can synchronize data from the network and what data can be synchronized when users connect to an Exchange server with their mobile phones. Since there is no client installation, ActiveSync Shield is ideal for BYOD implementations since it supports any mobile device including iOS (iPhone, iPad), Android, Windows Phone or Symbian device.

ActiveSync Shield is a comprehensive secure mobile email product suite that includes the following modules:

- **ActiveSync Protector** – Rule-based content filtering and antivirus inspection of email traffic between the Exchange server and the mobile device
- **Mobile Access Control** – Two-factor authentication solution based on device identification together with credentials. The module also features Active Directory password protection and a self-service access portal.
- **ActiveSync WebMail** – DLP solution that enables emails to be read as an online web page within the native mail client, so that no data is stored on the device.
- **Bastion Reverse Proxy Server** – Scalable HTTP gateway solution designed to enable organizations that do not use Microsoft Forefront servers to take advantage of the ActiveSync Shield secure mobile email product suite.

**ActiveSync Shield Architecture**

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

ActiveSync Shield is also available as a standalone gateway (Bastion server).

On the user side, it inspects the request details and verifies access control. On the Exchange side, ActiveSync Shield filters the content published according to the rules defined by the organization.
ActiveSync Protector for Content Filtering

Key Features

- Configure content publishing rules according to different parameters such as device type, Active Directory group membership, mail client and more
- Filtering Exchange content by one or more of the following objects:
  - Mail
  - Attachments
  - Events
  - Tasks
  - Contacts
- Allowing or blocking synchronization of attachments in mail messages or events
- Managing white list of attachment file types
- Filtering based on text search in email and calendar events content
- Allowing meeting requests to be published even when mail is blocked
- Filtering by the sender's domain name
- Transferring content to antivirus service

Dynamic Content Filtering

Securing mobile email has become a business-critical requirement. Organizations need to be able to limit the content leaving their networks to the absolute minimum and to permit such content only for users who really need it. Such an approach significantly reduces security risks as compared to solutions that try to protect the data on the smartphone itself.

The ActiveSync Protector module does this by defining dynamic content rules based on group membership, device types, device clients (e.g., Touchdown) or device ownership (personal or corporate). The rules are used to allow or block all Exchange objects (mail, attachments, contacts, task, and calendar). ActiveSync Protector also supports more complex content inspection rules based on text search, specific attachment types, specific sender domain and more.

Rules can be applied for both directions: from Exchange to device (most common for DLP) or from device to Exchange (for malware / anti-virus reasons).

Anti-Virus Protection

ActiveSync Protector also supports sending content to leading anti-virus services (e.g., eSafe, TrendMicro) via standard ICAP protocol.

This feature is extremely important due to the low security level of most mobile devices and the fact that mobile users are exposed to non-secure public (WiFi) networks. Moreover, implementing BYOD exposes users to a wide variety of non-secure applications installed on personal devices.

Similar to content filtering, anti-virus scanning is performed in both directions - from and to the device.

As ActiveSync Protector inspects all content coming from the device on the mail gateway (e.g., Forefront, Bastion), it detects and blocks malware before it enters the corporate network and reaches your Exchange server.
Mobile Access Control for Strong Email Authentication

Key Features

- Two-factor authentication using the smartphone as something you have and the password as something you know
- Custom login protects corporate password by defining custom login credentials exclusively for ActiveSync
- Self-service access portal to support two-step registration of users
- Strong device authentication not relaying only on device ID
- Admin auditing and control tools for approving devices
- Multiple enrollment options

Strong identification of device

Unlike other solutions in the market, the Mobile Access Control module does not depend only on device ID (IMEI) for identifying the device, but generates an application key that is set on the device during the registration process. This ensures that the user and mobile device to be synchronized always match. This is an important feature because device ID can be easily faked. Some devices allow the user to manually change the device ID sent by the device. Another reason is that corporate phones provided in bulk using a replication process often all have the same device ID.

Device Registration Options

Mobile Access Control supports various enrollment options:

- **Automatic Registration** - A device is registered the first time a user syncs via ActiveSync Protector. Once registered, ActiveSync Protector then verifies during subsequent synchronizations that the sync operation is in fact performed from the registered device. Any attempt to sync 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 synchronize within a short period of time (defined in portal configuration) in order to complete registration. Authentication can be performed against the user’s AD credentials or by using custom credentials that the user creates on the Access Portal (different than their AD credentials). The custom login option offers a higher level of security as AD credentials are not stored on the mobile device, and is useful for supporting organizations that use smartcards for network access rather than username/password credentials.
Admin User Management and Auditing

ActiveSync Shield includes an admin website 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.

Active Directory Password Protection

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 two issues:

1. Your Active Directory username and password can be hacked and used to provide access to many core business applications.
   Even if only mail is published to an external network- a hacker can use your credentials to receive your mails with anyone else noticing.
2. 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.
These scenarios cause help desk overhead and may even cause denial of service in case of an attack. Using the Mobile Access Control custom login, all failed attempts are blocked on the gateway level (Forefront/Bastion) before reaching the Active Directory, thus avoiding account lockout and denial of service.

**ActiveSync Webmail for Data Leak Prevention (DLP)**

**Key Features**
- Email content never resides on user device
- Content immediately blocked in case of stolen or lost device
- No remote wipe technical issues and personal data issues
- Integrated with Mobile Access Control for secure authentication
- No client installation, local encryption or remote wipes
- Revolutionary DLP approach minimizes risk of data loss

**Focus on the Data, Not the Device**
The most significant source of data loss comes from lost or stolen mobile devices containing sensitive business e-mails, which are automatically downloaded to the device from the organization’s internal Exchange servers.

Common mobile security solutions try to solve this problem by concentrating on securing and encrypting data on the device itself. While encrypted data is better protected than unencrypted data, not all devices support encryption. Even for those that do, encrypted data on a stolen device can be decrypted given sufficient time and effort. Remote wipes are also not sufficiently reliable against data loss since they depend on the device being connected to the Exchange server upon synchronization and receiving the remote wipe signal.

**No Email Content Stored on Mobile Device**
In contrast with common solutions, the ActiveSync Webmail module offers a new approach for the problem of data loss. ActiveSync Webmail changes the email body to an online web page and leaves the mail header as expected by the device mail client. The result is that the only data stored on the device is the sender’s name and subject. When authenticated user opens the message on his device, he sees a dynamically generated webpage containing the mail body. If a device is lost or stolen, the user is blocked on the server side and the web page can no longer be retrieved.

By dynamically changing the content sent by Exchange to the mobile device, your sensitive business data is never stored on the mobile device. When the device is lost, no sensitive data can be lost, since it wasn’t there in the first place. Moreover, there is no need to ensure that your users’ devices support data encryption or to install specialized clients on each device to enhance data security. This allows ActiveSync Webmail to work with virtually any device using its native mail client.

It should also be noted that no web page content is stored on the ActiveSync Shield servers. The content is generated on the fly as the user opens the mail message.

To allow offline usage of mails, mail can be saved locally on device for a limited time. After time expiration, ActiveSync Shield deletes the mail from the device and offers opening it via web option through the ActiveSync Webmail.
Bastion Reverse Proxy Server

Key Features
- Secure remote access to corporate resources without Microsoft Forefront
- Fully compatible with ActiveSync Shield product suite
- High scalability and throughput
- Filters any HTTP-based protocol

Standalone Gateway for ActiveSync 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 ActiveSync Shield secure mobile email product suite.

Bastion forwards traffic to the configured backend servers (e.g., Microsoft Exchange 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 ActiveSync 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 Exchange ActiveSync.

About AGAT Software Solutions
AGAT Software Solutions, 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). The most recent addition to the AGSecurity suite, ActiveSync Shield is designed to meet the complex ActiveSync security needs of today’s mobile enterprise. AGAT’s customers consist of government offices, banks, insurance companies and large industrial corporations (including Fortune 500 companies).

For more information
Contact us:
Agat Software Solutions
support@agatsolutions.com
57 Hagefen Street, Asseret, Israel
Tel/Fax: 972-8-8598456
Business development: 972-52-520-9860

Please visit our sites:
Company site: www.agatSolutions.com
Product site: www.SecureMobileEmail.com