Using MobileIron Sentry for Control and Visibility into ActiveSync Devices

Introduction

With the rising popularity of Apple iOS, Android, Windows Mobile and Symbian devices within the enterprise, organizations are quickly looking for ways to adopt ActiveSync in their environment in a secure manner. Though ActiveSync is increasing in its ubiquity as a de-facto standard for push e-mail, many organizations have faced challenges in adopting it within their enterprise. ActiveSync alone has traditionally not delivered the access control and visibility features demanded by security-conscious enterprises. Specifically, ActiveSync has not met the following enterprise requirements:

- **Access Control**: Administrators face difficulties in restricting unauthorized users from registering their phones and have had to manually allow access on a per-user basis. Even with a manual allow / block policy, organizations have had challenges in enforcing policies that limit the number of phones that can be registered to a mailbox authorized for ActiveSync.

- **Visibility**: There have been limited ways to determine what devices are connecting to what ActiveSync-enabled mailboxes on a global basis without custom-developing scripts. Even Exchange 2010’s tools within Exchange Web Services have been limited to a per-mailbox view as opposed to an enterprise-wide view.

- **Security**: It has been difficult to restrict devices from connecting to ActiveSync based on posture (e.g., OS version, security posture, etc.), beyond the standard policy enforcement criteria offered by the ActiveSync platform. Basic policies, like enforcing password policies on devices, have been problematic in some hosted e-mail environments.

MobileIron Sentry provides the infrastructure needed for enterprises to meet these challenges and enable ActiveSync, and devices like iPhones, with confidence. This whitepaper will discuss the architecture of MobileIron Sentry and concepts for deploying MobileIron Sentry within the enterprise.

**MobileIron Sentry Architecture**

MobileIron Sentry uses two distinct architectural models: MobileIron Sentry Standalone and MobileIron Sentry Integrated. There are no feature differences between the two implementations; both offer the following functionality:

- Ensure only authorized devices are able to connect to ActiveSync
- Ensure that connecting devices meet organizational policy assessments
- Provide visibility into all devices attempting to connect to ActiveSync, regardless of whether those devices are under MobileIron management
- Perform DM commands, such as remote wipe
The model chosen for deployment by a given enterprise depends on the enterprise’s security goals, network topology, and back-end mail infrastructure. Note that Integrated Sentry must be used if only client-certificates will authenticate users to the Exchange infrastructure. Two-factor authentication using certificates plus username and password, when deployed in conjunction with a front-end proxy or load balancer that can handle certificate verification, is supported by either Sentry model.

**MobileIron Sentry Standalone** acts as a proxy between clients and the mail infrastructure, sitting in-line between an ActiveSync client and the organization’s ActiveSync mail server(s). This model supports a variety of back-end mail infrastructures; customers have successfully deployed MobileIron Sentry Standalone connected to Microsoft Exchange, Lotus Notes when used with Notes Traveler, and hosted solutions such as BPOS-S, BPOS-D or Google Gmail.

**MobileIron Sentry Integrated** acts as a policy agent within Exchange 2007 and Exchange 2010 mail clusters. Support is also offered for Microsoft’s BPOS-D hosted mail system. This model is useful for organizations that want to enforce policies on the mail cluster itself, rather than through an appliance that sits within the communication flow for ActiveSync. With MobileIron Sentry Integrated, organizations can also leverage their existing high availability (HA) environment, as the Sentry does not sit directly in the mail flow.

**Policy Enforcement Using MobileIron Sentry Standalone**

When using the MobileIron Sentry Standalone, policy adherence is achieved via network-level enforcement. To reach e-mail, each ActiveSync device will first connect to the MobileIron Sentry appliance. To determine whether a device is allowed to connect to the back-end ActiveSync mailserver, e-mail traffic is inspected by the MobileIron Sentry appliance; from this traffic, the client’s device ID is obtained and passed to the MobileIron Virtual Smartphone Platform (VSP), or management appliance. The VSP uses this client ID to examine the information provided to it by the MobileIron client to determine if a device should connect to ActiveSync. This information includes client type, security state, OS version and other data. When queried, the VSP will respond to the Sentry appliance as to whether or not the queried client device is allowed to connect. If the device is not allowed to connect, then traffic for that particular client will be blocked from connecting to the back-end mail environment.

Because access control is established at a network level using MobileIron Sentry Standalone, it is natural to ask how users can be prevented from circumventing security by connecting directly to the ActiveSync server. In these cases, our recommendation to customers is to establish firewall rules that mandate incoming connections to the corporate ActiveSync server come only from the source IP address of the Sentry appliances in the network. This ensures that all traffic destined for ActiveSync servers within the enterprise will first connect through the organization’s Sentry appliances.

In addition to providing access control over the corporate e-mail environment, policies can be applied using the ActiveSync conduit established between the MobileIron Sentry and an ActiveSync client. These policies include remote wipe of the phone, defining password complexity and other policies. Note that, in many cases, these policies can be established independently of ActiveSync using the MobileIron VSP and client.
Deployment Concepts for MobileIron Sentry Standalone

Network Placement

Security-conscious customers generally place the MobileIron Sentry appliance within the Demilitarized Zone (DMZ), in-line with the MobileIron VSP. In this scenario, customers would connect through the perimeter firewall over port 443 or port 80 for mail. Traffic would be passed either to a front-end ActiveSync server within the DMZ, behind the corporate firewall, or back out to the Internet.

The MobileIron Sentry and VSP do not have to be in line with one another; the MobileIron VSP can sit behind the corporate firewall while the Sentry sits in the DMZ, or both appliances can live behind the corporate firewall. In the case where the Sentry is behind the corporate firewall, customers generally will deploy in conjunction with a reverse proxy or security gateway such as Microsoft Internet Security and Acceleration (ISA) server. Guidance for these environments is described below.

Use of SSL Certificates

Generally, customers will want to ensure that a trusted SSL certificate, such as one from Verisign or Thawte, is used to establish secure connections between client handsets and the MobileIron Sentry appliance. When installing these certificates, two options exist:
1. **Without a load balancer:** When deploying without a load balancer, the CN of the SSL certificate should match the hostname of the Sentry appliance. The certificate should then be installed directly onto the appliance.

2. **Behind a load balancer:** When deploying behind a load balancer, if the load balancer is terminating SSL connections, the CN of the SSL certificate should match the DNS name of the virtual IP (VIP) assigned to the load balancer. The SSL certificate should then be assigned to the load balancer itself. Customers can choose to ensure encrypted connections between the load balancer and Sentry appliances by using the pre-installed self-signed certificates on each appliance or by installing trusted certificates on each appliance. Another option is to simply not mandate encrypted traffic between the load balancer and each Sentry appliance; to accomplish this, simply disable the “Require Client TLS” option in the Sentry configuration.

**Load Balancing & High Availability**

There are key concepts to understand when deploying MobileIron Sentry Standalone within the corporate environment. First, organizations will need to determine the level of availability that will be needed for mobile mail. MobileIron Sentry appliances are designed to work behind load balancers; multiple Sentry appliances can be connected to a single VSP. In this case, ActiveSync clients would first connect to the virtual IP of the enterprise load balancer, and the load balancer would route traffic appropriately, either in a round-robin or priority fashion.
The MobileIron Sentry appliances are designed to be resilient in the case that a VSP fails. If the failure of a VSP occurs, then each MobileIron Sentry appliance is designed to fail open. The Sentry appliance will mandate a simple passcode using the ActiveSync DM conduit to ensure that any new devices that connect to the Sentry meet a basic security policy. All ActiveSync traffic will be allowed through until connection between the VSP and Sentry is restored; when this occurs, any devices out of policy will be blocked.

**Deployment in Highly Distributed ActiveSync Environments**

MobileIron Sentry can also handle highly distributed / available ActiveSync mail environments where multiple ActiveSync servers handle transactions for mail. Depending on the organization’s network topology, each MobileIron Sentry may point to a load balancer, which will route traffic to the appropriate ActiveSync server. An alternative method is to configure each MobileIron Sentry to point at multiple, individual ActiveSync front-end servers. In this case, the Sentry would distribute connections to the defined ActiveSync servers on either a round-robin or priority basis for load balancing and high availability purposes.

Please note that a minimum of one Sentry appliance must be deployed for each unique mail organization / ActiveSync environment. Connecting a Sentry to multiple mail organizations is not supported.
**Deployment behind Load Balancers & Network Appliances**

When deploying MobileIron Sentry behind load balancers or other network appliances, the load balancer should be configured in an active/passive mode where there is one MobileIron Sentry as the primary appliance and another appliance is available as a standby unit. Alternatively, enterprises can deploy in an active/active configuration, where traffic is evenly split between two online Sentry appliances.

It is important that these upstream appliances do not modify the source port of connection threads destined for the Sentry appliance. To examine individual clients’ traffic and block it accordingly, the MobileIron Sentry relies on its ability to examine unique connection threads, which are defined by an IP address and a TCP source port that is unique to the source IP. In some cases, network appliance features, such as “TCP Connection Pooling” or “TCP Optimization,” will place traffic on the same TCP source port and IP address. While this may help optimize traffic for back-end infrastructure like web servers, it breaks the ability for the Sentry to inspect unique connection threads for each device. Therefore, these features are not supported when used in conjunction with the MobileIron Sentry.

**Use in Conjunction with Outlook Web Access / Webmail**

In some cases, organizations will have both ActiveSync and webmail services such as Outlook Web Access (OWA) deployed on the same back-end server. If an organization decides to use firewall rules to tunnel all ActiveSync traffic through a Sentry appliance, it should be noted that tunneling Outlook Web Access or other Webmail traffic through the MobileIron Sentry is not supported. While both ActiveSync and webmail applications like OWA are HTTP-based, the Sentry appliance will not pass OWA traffic. Customers can employ methods such as Microsoft ISA Server or other application firewalls to help bifurcate this traffic or separate webmail and ActiveSync servers from each other.

**Policy Enforcement using MobileIron Sentry Integrated**

When using MobileIron Sentry Integrated, policy adherence is achieved via policy enforcement at the mailbox level on an Exchange 2007, 2010 or BPOS-D mailserver. No changes are made to the network topology. The MobileIron VSP will connect to a MobileIron Sentry agent, a lightweight piece of software that sits in the Exchange mail cluster. The first policy written by the MobileIron Sentry agent is that only devices within a mailbox’s allowed device list can establish a connection to Exchange. As clients are registered with the MobileIron VSP, the VSP will write the client ID to the allowed devices list for ActiveSync. This prevents any unauthorized or unregistered devices from connecting. If a device is found to be out of policy, for instance, the phone is found to be modified, then the client’s device ID will be removed from the allowed device list and the client will no longer be allowed to connect. The connection between the VSP and Sentry agent can be used for sending ActiveSync DM commands, such as remote wipe, to clients as well.

Policy enforcement is handled by the MobileIron Sentry agent’s ability to set policies directly at the individual mailbox level within the Exchange cluster. Visibility over every device attempting to connect to ActiveSync is provided by querying the mail cluster directly.

In addition to policy controls, the MobileIron Sentry agent will periodically gather inventory information from the Exchange or BPOS-D cluster. This provides a near real-time inventory of devices that are connected to Exchange or BPOS-D for inventorying purposes.
Deployment Concepts for MobileIron Sentry Integrated

Network Placement & Service Account Credentials

The Sentry Agent can be installed on any Windows server in the cluster; the only requirement is that the server has Exchange Management Tools installed. Generally, either customers will install the Sentry agent on a dedicated management cluster, or a separate server with Exchange Management Tools will be installed.

Communications between the MobileIron VSP and the Sentry Integrated agent occur over port 9090. For best performance, the connection between the MobileIron VSP and the Windows server hosting the Sentry agent should be a reliable, low-latency (<250ms) broadband (>1Mb/s) link. The MobileIron Sentry Integrated agent also requires a service account with which to access Exchange Management Tools. This service account must have Exchange Administrator rights, as only this account type has the proper privileges with which to set Exchange policies.
**Conclusion**

Securing the enterprise ActiveSync e-mail environment is critical for successful deployments of iPhone, Windows Mobile, Symbian and Android. MobileIron Sentry provides the tools needed to gain visibility over devices connecting, prohibit unauthorized devices from gaining access to ActiveSync, and blocking devices that either do not meet requirements or have fallen out of compliance from connecting to corporate e-mail. Virtually any ActiveSync environment is supported, either via a network-based approach or integrated mailbox-based approach, ensuring that the right model is available for any organization.