PROTECTING ACTIVESYNC AND OWA WITH FORTIWEB

ActiveSync is a Microsoft technology that has brought data synchronization and server access to hundreds of millions of mobile devices since its introduction. In over 20 years it has evolved to be the foundation of mobile access to today's latest email and server products, including Microsoft Exchange, Office 365, and IBM Notes. Chances are you're using ActiveSync if your organization uses Microsoft Exchange and you're accessing your email on an iOS, Android, Windows Mobile, or BlackBerry device.

Along with ActiveSync, Outlook on the Web is the de facto standard for browser-based access to Exchange and Office 365 for email, contacts, tasks, and other services managed by these servers. Outlook for the Web has had many previous names including Exchange Web Connect, Outlook Web Access, and Outlook Web App. Most people know it as OWA for Outlook Web Access.

Both ActiveSync and OWA are widely used; however, they present a security challenge to IT teams, as the data sent from a mobile device or a web browser could bypass traditional threat detection systems in certain situations.

HIGHLIGHTS

- ActiveSync and OWA not scanned by SEGs
- Threats bypass traditional detection
- Affects Microsoft Exchange, Office 365, and IBM Notes
- FortiWeb provides AV for ActiveSync/ OWA attachments
- Integrated with FortiSandbox and FortiSandbox Cloud

THE SECURITY LOOPHOLE WITH ACTIVESYNC AND OWA

When remote users send and receive emails using ActiveSync or OWA, the server directly communicates with the devices, bypassing email protection services that scan SMTP traffic. Secure Email Gateways (SEGs) only scan inbound and outbound emails from users that are external to the communications server using SMTP.

The ActiveSync protocol is based on XML and uses HTTPS to communicate to the server. OWA is a browser-based method that communicates to the server using HTTP and HTTPS. SEGs have no visibility to this traffic and can't intercept threats that may be hidden inside.

Using Microsoft Exchange as an example, if a remote user sends an email infected with malware using their mobile device or OWA to a recipient outside the organization's Exchange Server, the email would be flagged and acted upon by the SEG. However, recipients on the same Exchange Server as the mobile or OWA user would receive the infected email, spreading the threat or possibly sending it to other users on the Exchange Server.

Many organizations need to control, secure, and protect ActiveSync and OWA communications for many reasons ranging from basic security hygiene to compliance. For example, ActiveSync and OWA email must be scanned for threats as part of ISO 27001 certification.

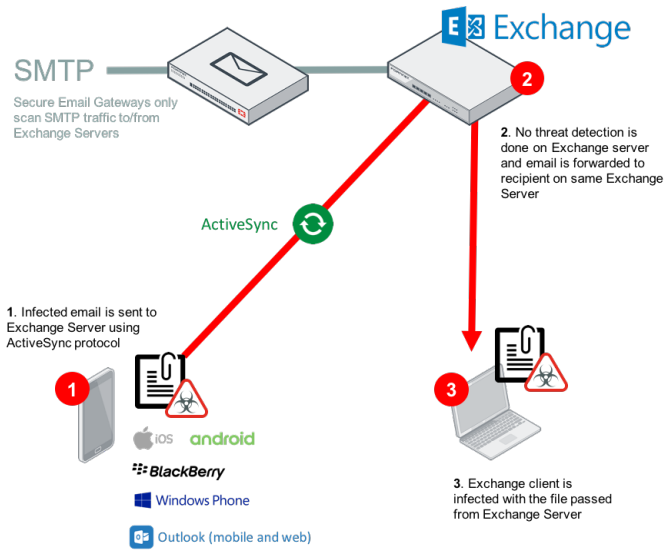

Figure 1: Remote users send email and attachments directly to the Exchange Server, bypassing traditional email security.

FORTIWEB ACTIVESYNC AND OWA SCANNING

In addition to its core web application firewall functionality, FortiWeb can be deployed to publish applications, provide SSO, and manage authentication delegation. Many Fortinet customers use FortiWeb as a replacement for the discontinued Microsoft Threat Management Gateway to publish Microsoft Exchange and other Microsoft applications.

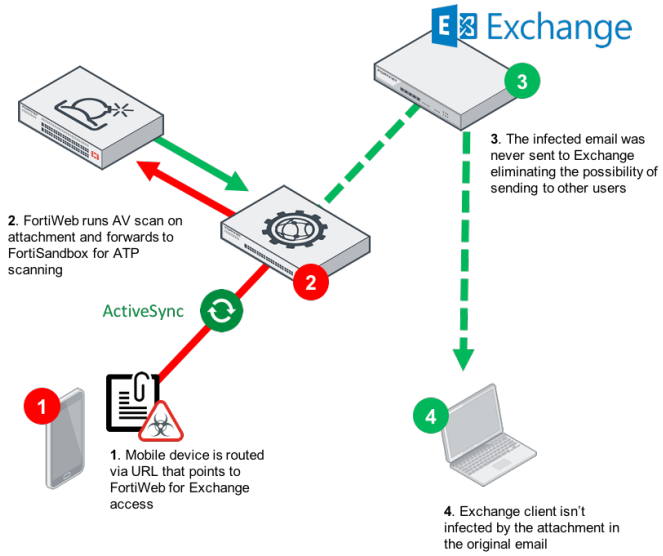

Figure 2: FortiWeb is deployed in front of Exchange Server to intercept email traffic from remote devices to scan for threats.

Using this functionality, FortiWeb can be deployed as a proxy for ActiveSync and OWA. This means that any remote mobile user or email client would be directed to FortiWeb. Here FortiWeb would inspect the traffic and intercept any attachments sent from the device or web browser. These attachments are then processed by FortiWeb's antivirus engine to check for threats. FortiWeb can also be configured to send attachments to Fortinet's sandboxing solutions for additional scans to detect advanced persistent threats or zero-day attacks.

BENEFITS

By using FortiWeb to protect your ActiveSync-based applications and users accessing email with OWA, you get:

- Proven protection against threats hidden in ActiveSync and OWA attachments
- Mobile Attachment Scanning for Office 365
- Flexible deployment options including VMs, Cloud, and Appliances
- Easy-to-deploy antivirus for Exchange, IBM Notes, and other ActiveSync-based applications
- Integration with FortiSandbox and FortiSandbox Cloud for protection from advanced persistent threats
- Integrated single platform for publishing Microsoft Exchange Server applications and services

ABOUT FORTIWEB

When enterprise organizations need to protect their users and systems from advanced application vulnerability threats such as Cross-Site Scripting and SQL Injection, or meet PCI DSS compliance, only Fortinet's high-performance FortiWeb WAF solutions provide industry-leading protected traffic throughputs up to 20 Gbps. With features including third-party vulnerability scanner support and integration with Fortinet's enterprise firewalls and sandboxing products, FortiWeb is unmatched in WAF performance and security effectiveness to protect and defend against threats that target mission-critical web applications.

FortiWeb offers many deployment options including hardware and virtual appliances to meet the needs of on-premises, cloud, and hybrid enterprise environments. Virtual appliances support all major hypervisors including VMware and Microsoft Hyper-V. It is also available for Amazon Web Services and Microsoft Azure.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

119963-A-0-EN September 27, 2017 9:36 AM
Macintosh HD:Users:mbunnell:Documents:Egnyte:Shared:CREATIVE SERVICES:Team:Michael-Bunnell:SB-Proctecting-ActiveSync-OWA-FortiWeb:sb-protecting-activesync-owa-fortiweb_092717_932am