FORTINET

White Paper

Securing Mobile Devices

With FortiOS 5

Introduction

Organizations are increasingly dependent on mobile information technology in every activity. Employees rely heavily on more and more portable network devices that allow them critical flexibility to roam for increased productivity. But mobile devices put networks at increased risk of data leaks and exposure to malicious infection.

The BYOD phenomenon

BYOD (bring your own device) started out as an informal trend that saw staff using smartphones and tablets in the workplace to access privileged internal resources. These devices rely heavily on network connectivity for many of their functions and applications.

However, it quickly evolved to include a broader phenomenon of the use of a variety of devices in the workplace that aren't controlled by the corporation that hosts them.

Employees like bringing their own devices for the familiarity, ease of use and, by extension, access to the organization's applications. Companies embrace BYOD because it allows employees increased mobility, higher job satisfaction and greater efficiency and productivity.

Although BYOD brings new advantages to the workforce, it also brings its fair share of challenges. Many of these challenges revolve around security. The most significant problem for IT departments is the lack of visibility and control of these devices.

Unmanaged devices

These are typically wifi devices brought in by employees. Users access the network, logging in on their smartphones, tablets or laptops with their usual credentials, but the devices can evade security policies because they're not a formal part of the enterprise's managed environment. Yet installing a host agent to manage these devices can be unwelcome and intrusive to the owner of the device.

And, unlike corporate equipment, personal mobile devices often run on different operating systems (and many different versions of operating systems), making the installation of a host agent difficult, if not impossible.

Personal devices can also add to network misuse, with applications such as internet radio and video streaming.

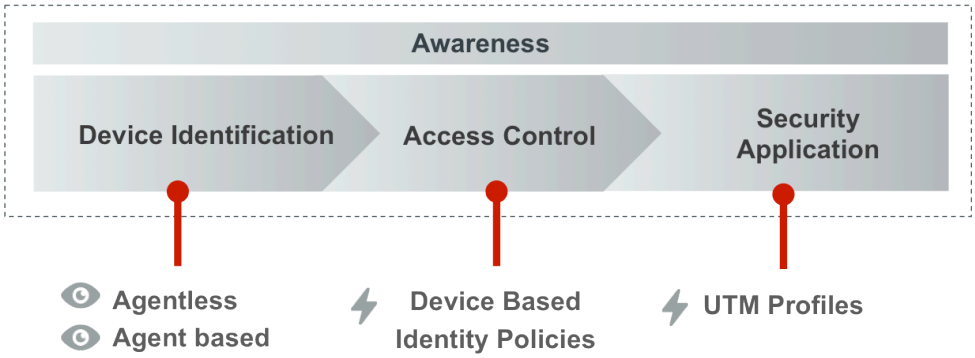
Corporate mobile devices

These are portable devices issued by the corporation, so they're more likely components of the managed network environment than purely personal devices. But when they're out of the corporate network, they're out of the range of the security policy enforced by the security gateway.

In both cases, mobile devices can be lost or stolen. Without proper control, they can also be used to leak corporate data, inadvertently or maliciously.

How FortiOS 5 secures mobile devices

There are three elements to the FortiOS 5 solution for securing mobile devices; identification, access control and security application.



Device identification

FortiOS 5 identifies all devices, wired and wireless, and their operating systems in two ways:

1) Agentless detection

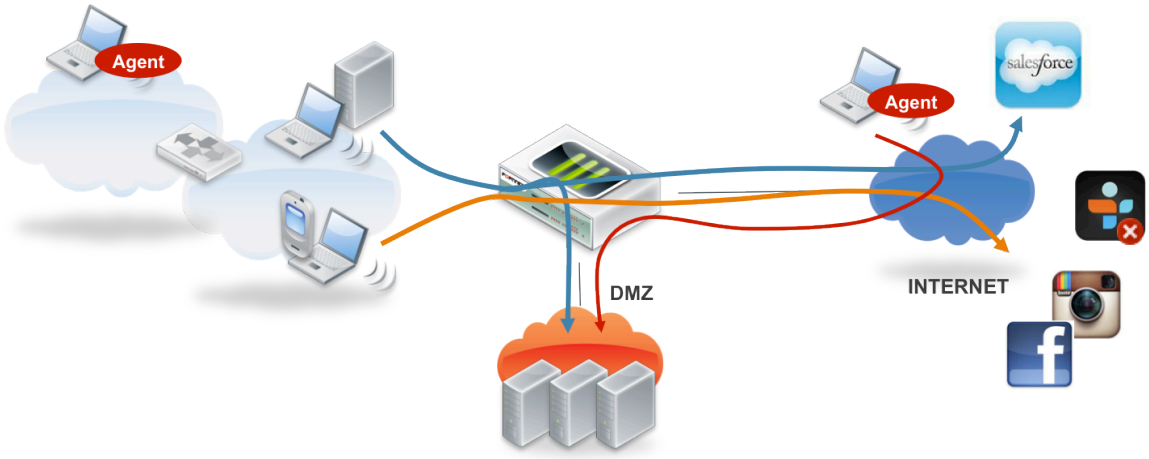
Agentless detection identifies devices that log on to the network without requiring additional software on the devices themselves.

It utilizes a broad range of measures to accurately determine device type, with traditional TCP and MAC vendor code fingerprinting, the use of DHCP attributes, and application layer analysis including HTTP user agent and SIP message parsing. These measures can be updated via our FortiGuard network as the device landscape evolves.

2) Agent-based identification

For agent-based identification, FortiClient is installed on devices to feed information directly to FortiOS. This technique is the most reliable and allows identification even when the devices are on remote networks.

Access control



After devices are identified, they're automatically assigned to device groups according to type and OS. Administrators also have the ability to create custom groups for policy enforcement.

Security Application

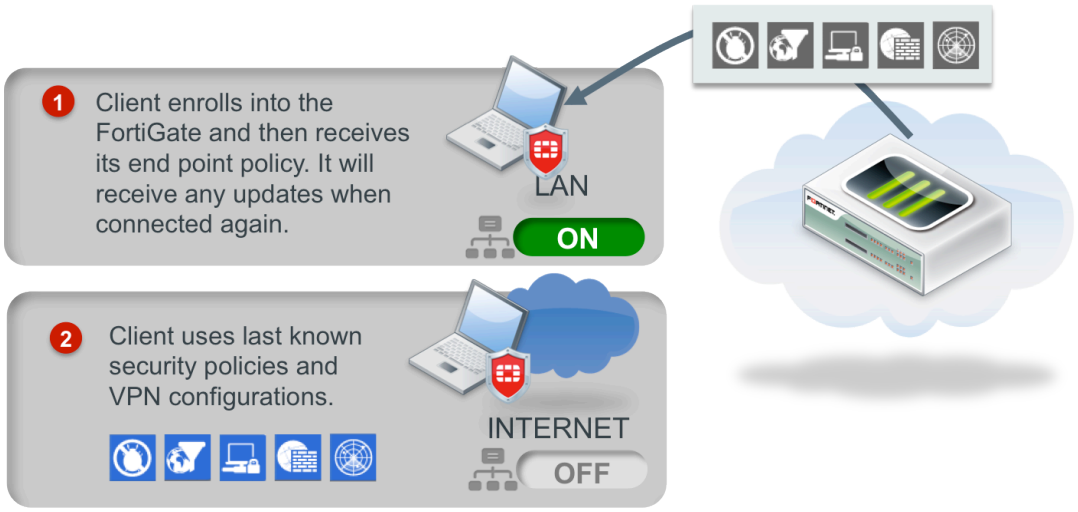
The administrator can then control access and assign security profiles based on device groups or individual devices. These profiles include web content filtering and application control.

For example, a school can set policies where teachers can access server resources, while students only access permitted areas of the Internet, avoiding plagiarism sites and other inappropriate content. In addition, to prevent bandwidth abuse, students are blocked from streaming multimedia. Or a corporation that uses contractors on its guest network can allow their devices access to project-specific resources while allowing only internet access to other guests.

Device contextual information for visibility

Device identification also allows the FortiGate to provide new contextual information in status widgets and logs. This allows administrators to better understand their network posture and identify problem spots quickly.

Endpoint control with off-net protection



When mobile devices leave the local network and go “off-net”, they’re no longer protected by a security gateway. The tight integration between FortiClient and FortiOS provides off-net protection, reducing corporate vulnerability to malware infection and data leaks and enforcing corporate access policies. Adopting endpoint control allows users not only to bring their own devices, but to take their security policy home.

Web filtering, for example, can block malicious and phishing sites even when the user is telecommuting or web browsing. The user can access the Internet safely anywhere without needing a VPN. When a VPN is required to connect to corporate resources, FortiOS distributes new VPN configurations to roaming devices.

Synchronizing fixed and mobile security policies allows the simple implementation of updates and modifications to ensure up-to-date protection.

Conclusion

The combination of FortiClient and FortiOS 5 provides a powerful solution ensuring the most appropriate level of security is present on all devices, at all times, in all places.

FORTINET

GLOBAL HEADQUARTERS
Fortinet Inc.
1090 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
Fax: +1.408.235.7737
www.fortinet.com/sales

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia
Antipolis, France
Tel: +33.4.8987.0510
Fax: +33.4.8987.0501

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730
Fax: +65.6223.6784

LATIN AMERICA SALES OFFICE
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480

Copyright© 2012 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, and FortiGuard®, are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance metrics contained herein were attained in internal lab tests under ideal conditions, and performance may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet’s General Counsel, with a purchaser that expressly warrants that the identified product will perform according to the performance metrics herein. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet’s internal lab tests. Fortinet disclaims in full any guarantees. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.