SONICWALL

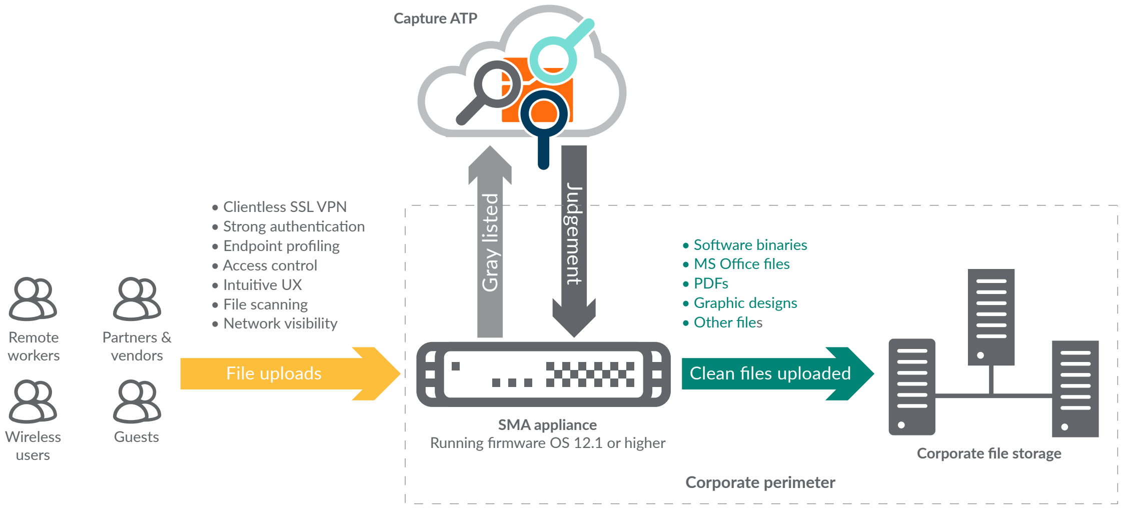
TECH BRIEF: HOW SONICWALL SMA STOPS MALICIOUS FILES FROM ENTERING YOUR NETWORK

Introduction

This technical brief discusses how SonicWall's Secure Mobile Access (SMA) stops malicious files from entering your network. SMA integrates with Capture ATP, a cloud-based multi-engine sandbox, and extends automated real-time breach detection and prevention capabilities beyond the traditional corporate perimeter. This ensures that an organization gets the same level of protection for remote workers, vendors and contractors from any location.

How SonicWall SMA stops malicious files from entering your network

SonicWall SMA provides a secure file share mechanism that utilizes multiple security components to block malicious files while allowing only trusted users and endpoints, and clean files into the network.



Components of a secure file share mechanism

SMA integrates with Capture ATP, a cloud-based multi-engine sandbox, and extends automated real-time breach detection and prevention capabilities beyond the traditional corporate perimeter.

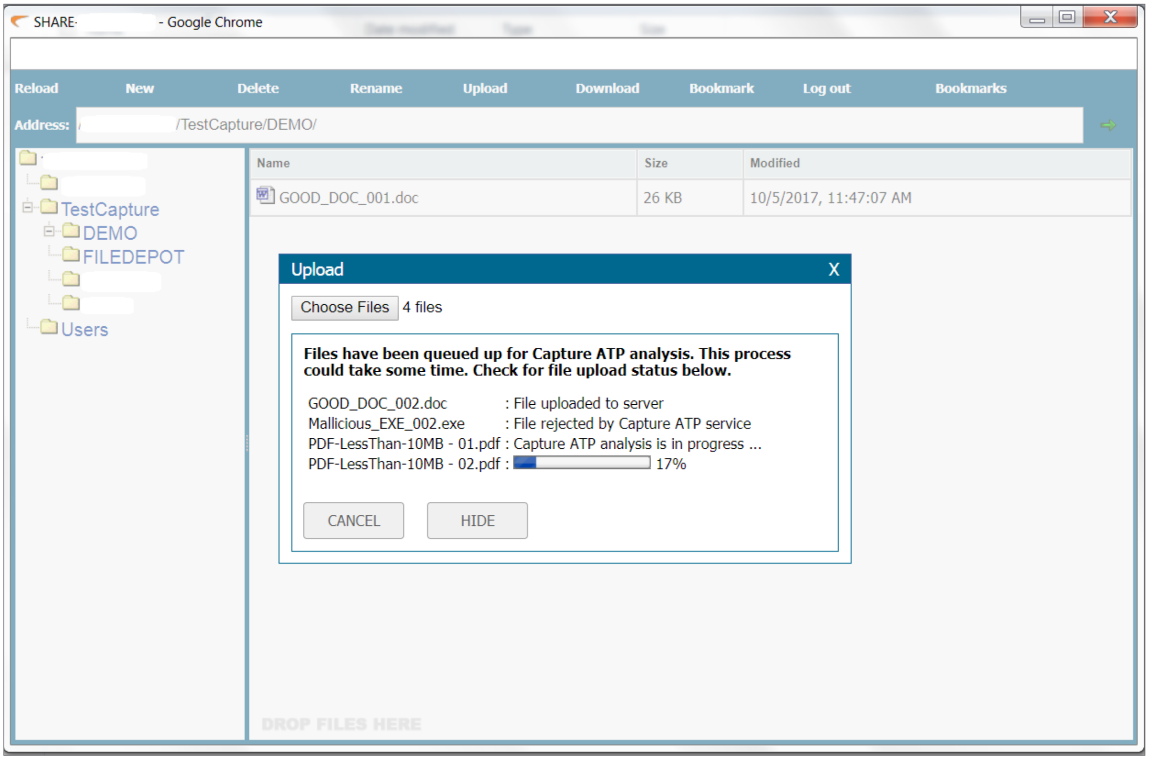
Clientless Access: Installing clients on every endpoint device is an IT overhead and not a viable policy in a BYOD environment. Users also get frustrated when a client or an agent needs to be installed in order to perform routine tasks. This becomes a challenge when those users do not have the admin rights on their devices. With browser-based HTML5 clientless access, users do not need to install any client. Users simply open their choice of web browser and login to a secure access portal, which encrypts the session with strong SSL/TLS.

Strong Authentication: SonicWall SMA supports industry standard authentication methods that use RADIUS and Kerberos for campus-hosted applications, and SAML 2.0 for cloud-hosted SaaS applications. In addition, the solution can be configured to integrate with user directories such as LDAP and a SAML IdP to provide federated single sign-on from a single URL to both on-campus and cloud applications. For added security, the solution can chain authentication methods and seamlessly integrate with leading multi-factor authentication technologies. The login event into the secure access portal ensures that the user has gone through strong authentication mechanisms.

Endpoint Profiling: The endpoint control feature for SMA allows the administrator to enforce granular access control rules based on the health status of the connecting device. Prior to granting access, mobile devices are interrogated for essential security information such as jailbreak or root status, device ID, certificate status and OS versions. Laptops and PCs are also interrogated for the presence or absence of security software, client certificates, and device ID. Devices that do not meet policy requirements are not allowed network access, and the user is notified of non-compliance.

Access Control: With SMA, IT can enforce granular access control policies based on the type of user (employee, contractor, partner or vendor), device being used, application being accessed and location of access. When the user logs in, SMA checks the groups and attributes to present the network share and the applications the user has access to. To provide network file share access to remote users, IT can configure a dedicated network drive that is segmented from other part of the network.

Intuitive UX: User experience is a critical component when it comes to security and productivity. SMA utilizes a modern HTML5 file browser that provides users with an intuitive experience that is similar to popular public cloud file share services. This familiarity enables productivity with ease of use.



Address: /TestCapture/DEMO/

Name	Size	Modified
GOOD_DOC_001.doc	26 KB	10/5/2017, 11:47:07 AM

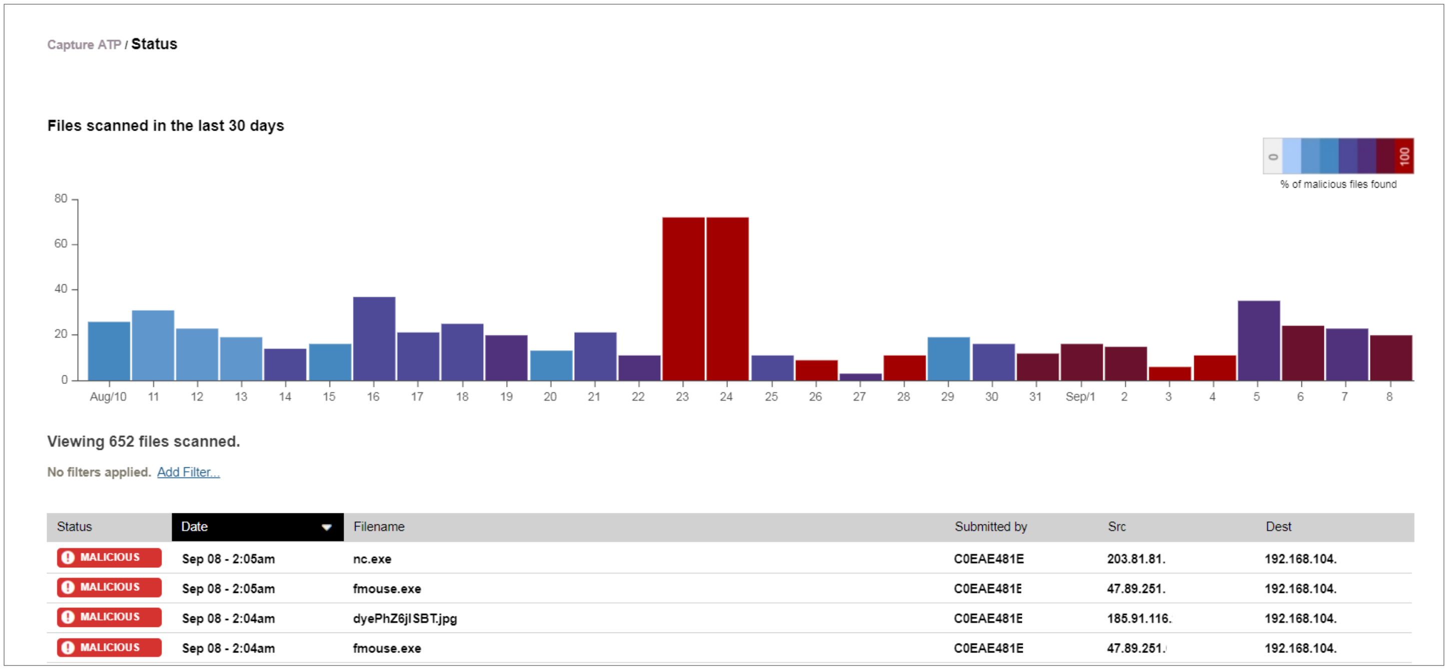
Choose Files 4 files

Files have been queued up for Capture ATP analysis. This process could take some time. Check for file upload status below.

```
GOOD_DOC_002.doc           : File uploaded to server
Mallicious_EXE_002.exe     : File rejected by Capture ATP service
PDF-LessThan-10MB - 01.pdf : Capture ATP analysis is in progress ...
PDF-LessThan-10MB - 02.pdf :                 17%
```

Files uploaded using HTML5 file browser are scanned by Capture ATP for ransomware and 0-day threats.

File Scanning: When the user clicks on the share drive, the HTML5 file browser allows the user to navigate the folder structure. SMA provides a drag-and-drop experience to upload files into the network share drive. When the user uploads a file into a particular folder, the file is scanned by our cloud-based multi-engine Capture ATP sandbox for malware and zero-day threats. The verdict is delivered in near real-time, and suspicious files are rejected.



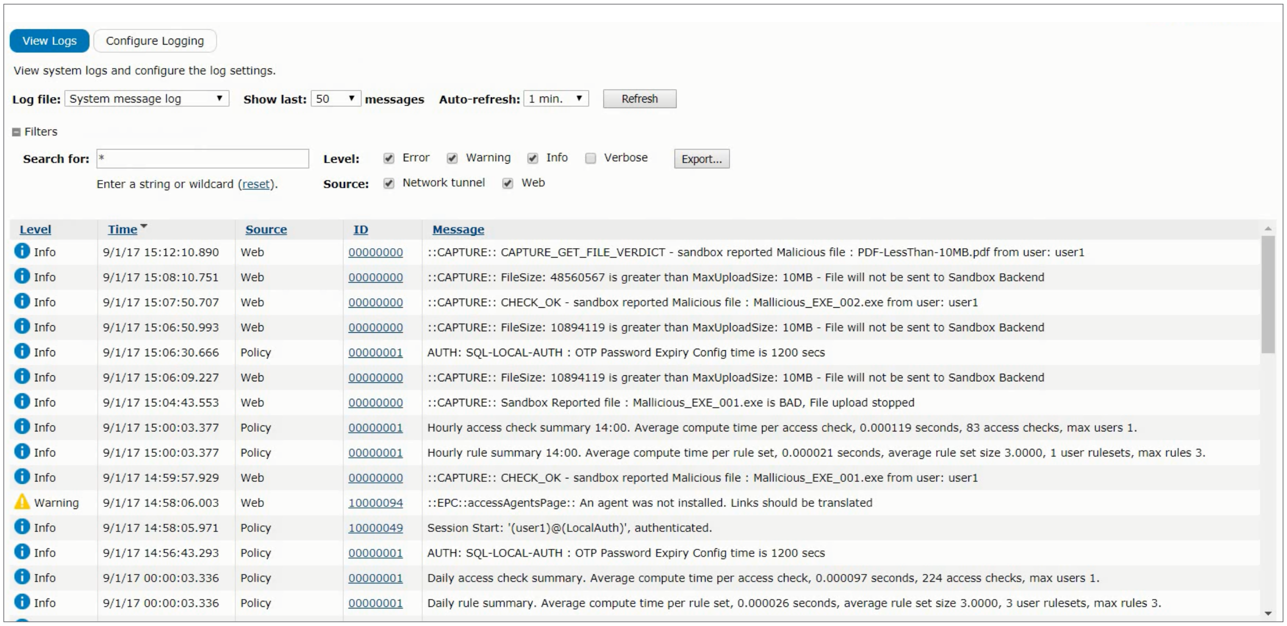
Viewing 652 files scanned.

No filters applied. Add Filter...

Status	Date	Filename	Submitted by	Src	Dest
MALICIOUS	Sep 08 - 2:05am	nc.exe	C0EAE481E	203.81.81.	192.168.104.
MALICIOUS	Sep 08 - 2:05am	fmouse.exe	C0EAE481E	47.89.251.	192.168.104.
MALICIOUS	Sep 08 - 2:04am	dyePhZ6jlSBT.jpg	C0EAE481E	185.91.116.	192.168.104.
MALICIOUS	Sep 08 - 2:04am	fmouse.exe	C0EAE481E	47.89.251.	192.168.104.

Capture ATP file scan reports are available with detailed user session information.

Network Visibility: The central management server (CMS) for SMA provides reporting and monitoring capabilities including Capture ATP test results and session information (such as user ID and IP address). In addition, when the solution is deployed with SonicWall NGFW, SMA shares the session information with the firewall. This provides end-to-end network visibility, and enables audit trail for reporting and compliance.



View system logs and configure the log settings.

Log file: System message log ▾ **Show last:** 50 ▾ **messages** **Auto-refresh:** 1 min. ▾

Filters

Search for: *

Enter a string or wildcard (reset).

Level: ☑ Error ☑ Warning ☑ Info ☐ Verbose

Source: ☑ Network tunnel ☑ Web

```
Level     Time                   Source   ID         Message
Info      9/1/17 15:12:10.890    Web      00000000   ::CAPTURE:: CAPTURE_GET_FILE_VERDICT - sandbox reported Malicious file : PDF-LessThan-10MB.pdf from user: user1
Info      9/1/17 15:08:10.751    Web      00000000   ::CAPTURE:: FileSize: 48560567 is greater than MaxUploadSize: 10MB - File will not be sent to Sandbox Backend
Info      9/1/17 15:07:50.707    Web      00000000   ::CAPTURE:: CHECK_OK - sandbox reported Malicious file : Mallicious_EXE_002.exe from user: user1
Info      9/1/17 15:06:50.993    Web      00000000   ::CAPTURE:: FileSize: 10894119 is greater than MaxUploadSize: 10MB - File will not be sent to Sandbox Backend
Info      9/1/17 15:06:30.666    Policy   00000001   AUTH: SQL-LOCAL-AUTH : OTP Password Expiry Config time is 1200 secs
Info      9/1/17 15:06:09.227    Web      00000000   ::CAPTURE:: FileSize: 10894119 is greater than MaxUploadSize: 10MB - File will not be sent to Sandbox Backend
Info      9/1/17 15:04:43.553    Web      00000000   ::CAPTURE:: Sandbox Reported file : Mallicious_EXE_001.exe is BAD, File upload stopped
Info      9/1/17 15:00:03.377    Policy   00000001   Hourly access check summary 14:00. Average compute time per access check, 0.000119 seconds, 83 access checks, max users 1.
Info      9/1/17 15:00:03.377    Policy   00000001   Hourly rule summary 14:00. Average compute time per rule set, 0.000021 seconds, average rule set size 3.0000, 1 user rulesets, max rules 3.
Info      9/1/17 14:59:57.929    Web      00000000   ::CAPTURE:: CHECK_OK - sandbox reported Malicious file : Mallicious_EXE_001.exe from user: user1
Warning   9/1/17 14:58:06.003    Web      10000094   ::EPC::accessAgentsPage:: An agent was not installed. Links should be translated
Info      9/1/17 14:58:05.971    Policy   10000049   Session Start: '(user1)@(LocalAuth)', authenticated.
Info      9/1/17 14:56:43.293    Policy   00000001   AUTH: SQL-LOCAL-AUTH : OTP Password Expiry Config time is 1200 secs
Info      9/1/17 00:00:03.336    Policy   00000001   Daily access check summary. Average compute time per access check, 0.000097 seconds, 224 access checks, max users 1.
Info      9/1/17 00:00:03.336    Policy   00000001   Daily rule summary. Average compute time per rule set, 0.000026 seconds, average rule set size 3.0000, 3 user rulesets, max rules 3.
```

CMS records all Capture ATP related activity to event logs

With all these components in place, SMA with Capture ATP delivers a secure file share mechanism that allows only fully trusted users and clean files into the network.

Conclusion

It is important to enable and empower the mobile workforce. The ability to collaborate and share files is a key use case for remote teams comprised of mobile workers and external contractors. Providing everyone with full VPN access into corporate network is not a good security practice. And any restrictive security policies gives rise to bad security practices and shadow IT. Organizations need to deploy security solutions and define policies that enable workforce productivity. SonicWall SMA with Capture ATP enables organizations to provide the same level of protection for remote workers, vendors and contractors from any location.

To learn more, visit: www.sonicwall.com/sma

The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON- INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

About Us

SonicWall has been fighting the cyber-criminal industry for over 25 years, defending small, medium size businesses and enterprises worldwide. Our combination of products and partners has enabled a real-time cyber defense solution tuned to the specific needs of the more than 500,000 global businesses in over 150 countries, so you can do more business with less fear.

If you have any questions regarding your potential use of this material, contact:

SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

Refer to our website for additional information.
www.sonicwall.com