Cloud Access Manager 8.1.3

SonicWALL Integration Overview

The information in this document is provided in connection with One Identity 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 One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES 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 ONE IDENTITY 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 ONE IDENTITY HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity 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. One Identity do not make any commitment to update the information contained in this document.

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

One Identity LLC.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

Refer to our Web site (http://www.OneIdentity.com) for regional and international office information.

Patents

One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at http://www.OneIdentity.com/legal/patents.aspx.

Trademarks

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.OneIdentity.com/legal. All other trademarks are the property of their respective owners.

Legend

⊗ **WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.**

⚠ **CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**

ℹ IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

Cloud Access Manager SonicWALL Integration Overview
Updated - October 2017
Version - 8.1.3

Contents

Introduction

The following guide explains how to integrate SonicWALL with Cloud Access Manager.

Overview

Support for SonicWALL malware detection in the Security Analytics Engine, provided with a One Identity Cloud Access Manager installation, requires coordinated configuration with SonicWALL Next Generation Firewall (NGFW), Single Sign-On (SSO), Security Analytics Engine and Cloud Access Manager user authentication.

This guide describes how to implement a typical deployment highlighting the required configuration to fully enable SonicWALL malware detections for Security Analytics Engine user access evaluations, when users access Cloud Access Manager applications.

Functional highlights

In the following example a typical corporate network is used to illustrate how SonicWALL, the Security Analytics Engine and Cloud Access Manager products are configured to enable Security Analytics Engine risk scoring. This is for Cloud Access Manager users who may have malware detections indicated by a SonicWALL Next Generation Firewall (NGFW), this environment includes:

1. A Cloud Access Manager installation configured for internal and external corporate user access.
2. Security Analytics Engine enabled for Cloud Access Manager step-up authentication, with the following:
    - Security Analytics Engine policy for Cloud Access Manager configured to enable the Associated w/ Malware condition.
    - The optional Security Analytics Engine SonicWALLProcessor service installed and configured to process malware detection information from the firewall.
3. At least one SonicWALL NGFW configured to monitor user Internet access, with the following enabled:

- Single Sign-On enabled for user identification Gateway.
- Anti-Virus, Anti-Spyware and Intrusion Prevention features enabled.
- AppFlow configured to send malware detection flow information to the SonicWALLProcessor service.

The following is a high level overview of the user actions and information flow; this is illustrated in Figure 1 with further details provided in Functional details:

1. An internal corporate network user, User1 in the MyCorp domain accesses the internet and encounters some malware. The user is authenticated using the firewall SSO feature; the malware is detected by the NGFW, and optionally blocked.
2. The firewall forwards the malware detection information to the Security Analytics Engine installation, including the IP address and SSO-provided domain and user name, for example:

   IP: 10.6.100.102

   User: MyCorp\User1
3. Later, User1 accesses a Cloud Access Manager application from either inside the corporate network, or from the Internet.
4. Cloud Access Manager authenticates the user, detects the IP address and evaluates if the user is authorized to access the application.
5. As part of the authorization determination, Cloud Access Manager queries Security Analytics Engine to determine the user's risk score, and forwards the user name and IP information for processing by Security Analytics Engine. During the risk score evaluation, Security Analytics Engine will search for malware records received from the firewall and match them on either a user name or IP address, for example:

   Internal Access

   IP: 10.6.100.102

   User: MyCorp\User1

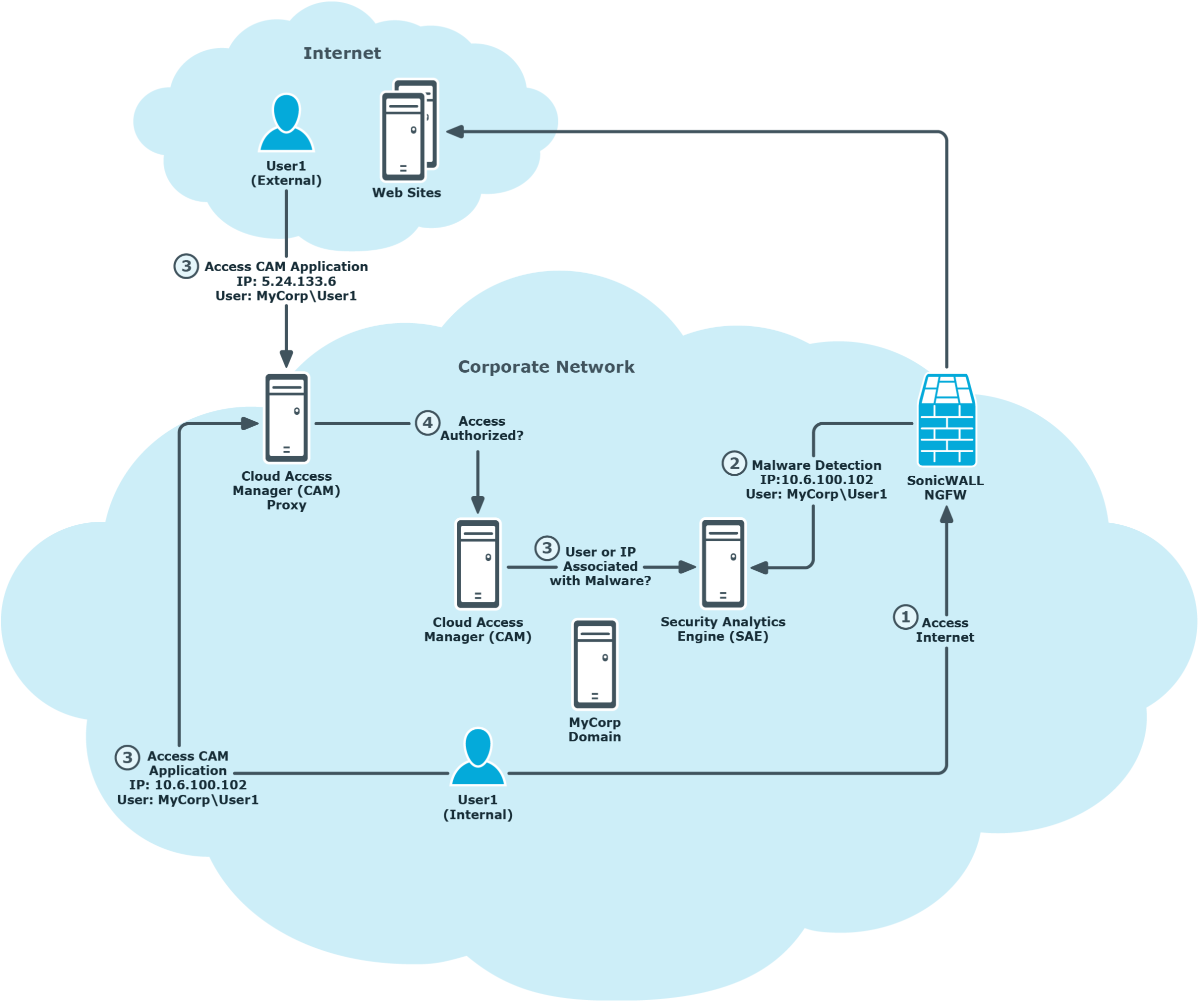
   or

   Internet Access

   IP: 5.24.133.6

   User: MyCorp\User1

Figure 1: Cloud Access Manager and SonicWALL deployment overview


Internet
User1 (External)
Web Sites
3 Access CAM Application IP: 5.24.133.6 User: MyCorp\User1
Corporate Network
Cloud Access Manager (CAM) Proxy
4 Access Authorized?
2 Malware Detection IP:10.6.100.102 User: MyCorp\User1
SonicWALL NGFW
Cloud Access Manager (CAM)
3 User or IP Associated with Malware?
Security Analytics Engine (SAE)
1 Access Internet
MyCorp Domain
3 Access CAM Application IP: 10.6.100.102 User: MyCorp\User1
User1 (Internal)

Functional details

The following sections provide a detailed breakdown of functionality related to the user authentication, malware detection and risk assessment steps highlighted in Functional highlights, this includes:

- SonicWALL Single Sign-On
- The Security Analytics Engine SonicWALLProcessor service
- Cloud Access Manager user authentication
- Using split DNS to forward internal IP addresses to the Security Analytics Engine

SonicWALL Single Sign-On

A key component of the malware detection information that enables Cloud Access Manager and Security Analytics Engine risk score evaluations to associate users with malware detections is user identification by firewall. Without this feature, only IP address matches would function, which would limit the malware association capabilities of Security Analytics Engine and prevent external Cloud Access Manager users being associated with malware detection records.

Many user authentication options are available with SonicWALL firewalls, but enabling integrated Single Sign-On (SSO) capabilities that do not prompt the user for authentication credentials include a combination of the following SonicWALL user authentication options:

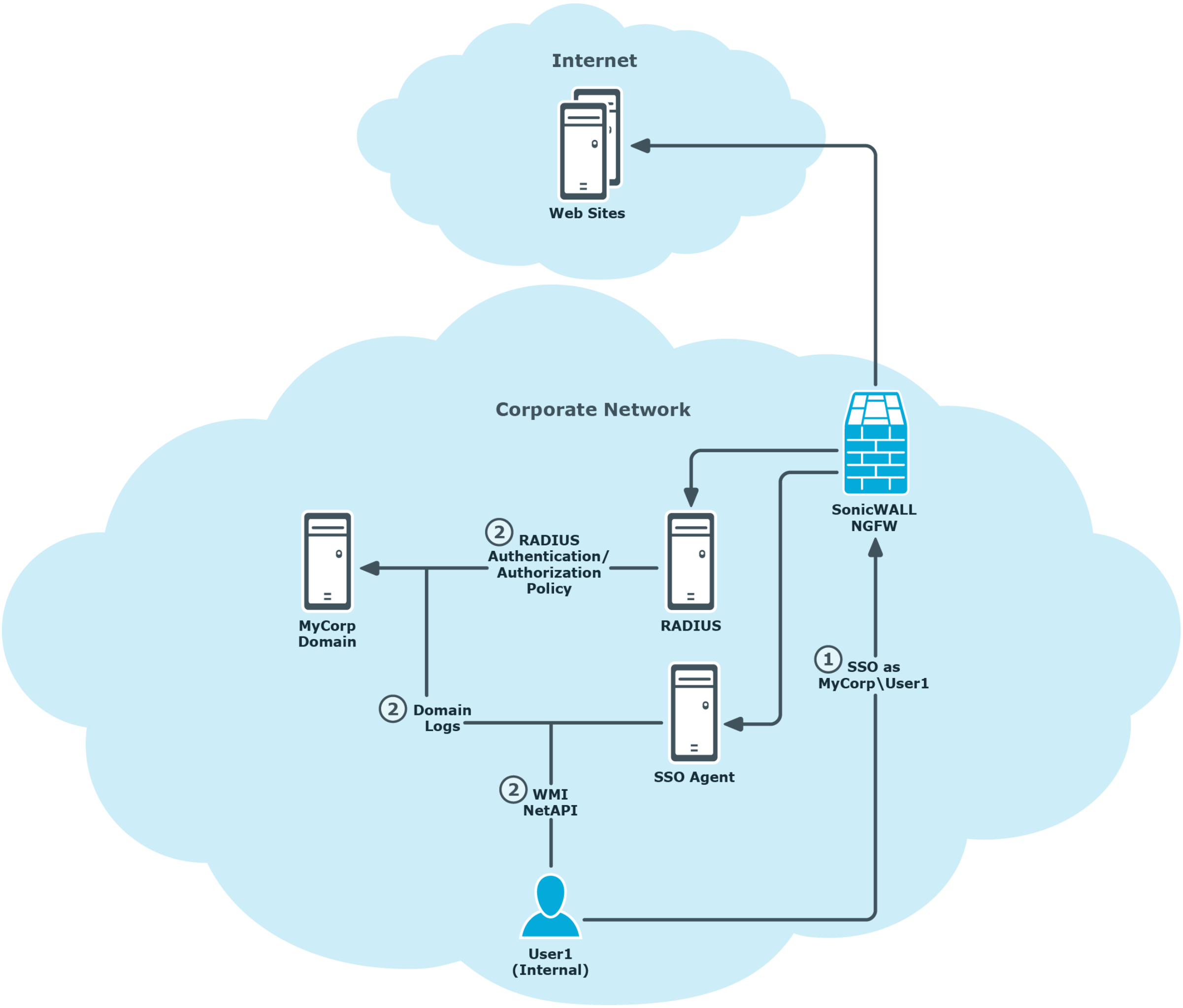
- Browser-based NTLM authentication using RADIUS to authenticate the users.
- Single Sign-On agent deployments provided by installing and configuring the SonicWALL Directory Services Connector.

> NOTE: We recommend you review the configuration options outlined in the SonicOS Administrator Guide as each option should be evaluated for compatibility requirements and potential limitations.

The following example includes a combination of NTLM and SSO Agent configurations, where NTLM is preferred but SSO Agent fallback is used to seamlessly authenticate user access to web sites. The process of authenticating the user is illustrated in Figure 2 and described as follows:

1. An internal corporate network user, User1 in the MyCorp domain for example, accesses the internet and is authenticated using the firewall SSO feature.
2. Based on the Next Generation Firewall (NGFW) SSO configuration, one or more of the following SSO authentication steps is performed to identify the user as MyCorp\User1:
    a. NTLM negotiation is attempted with User1's browser. The browser supplied credentials are forwarded to a configured RADIUS server for authentication and authorization policy evaluations.
    b. Alternatively, the NGFW may query an installed and configured SonicWALL SSO Agent (Directory Services Connector) for information related to the authenticated user on the source computer IP address. The SSO Agent can be configured with various options for determining the authenticated user, this includes:
        - Parsing Domain Controller logs.
        - Querying the computer in question using NetAPI or WMI protocols.

Figure 2: SonicWALL Single Sign-On



The Security Analytics Engine SonicWALLProcessor service

In order to process malware detection information forwarded by the SonicWALL Next Generation Firewall (NGFW) in AppFlow details, the optional Security Analytics Engine SonicWALLProcessor Service must be installed and configured to receive AppFlow information and forward malware detection records to the Security Analytics Engine web site. Once received by the Security Analytics Engine web site, the malware detection records are stored for subsequent risk score evaluations when users access Cloud Access Manager applications.

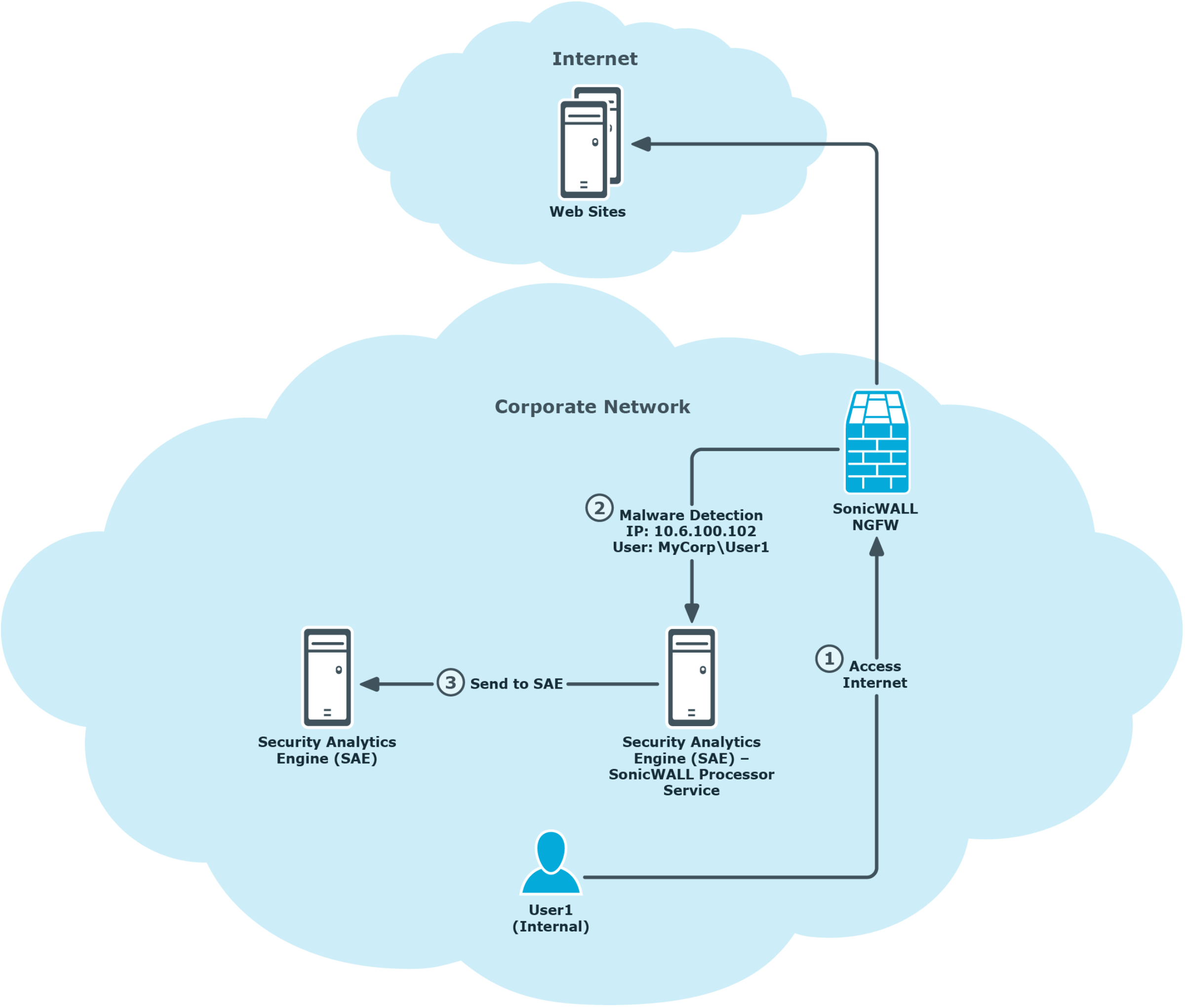
The process of malware detection information flowing from the SonicWALL NGFW through the Security Analytics Engine SonicWALLProcessor Service to the Security Analytics Engine web site is illustrated in Figure 3 and described as follows:

1. An internal corporate network user, User1 in the MyCorp domain for example, accesses the internet and the NGFW detects malware during the browsing activity.
2. Based on the AppFlow configuration in the NGFW, the malware detection details, including the IP address and SSO user details, are sent to the Security Analytics Engine SonicWALLProcessor Service as follows:

   IP: 10.6.100.102

   User: MyCorp\User1
3. The Security Analytics Engine SonicWALLProcessor Service receives the malware detection details and forwards malware detection records to the Security Analytics Engine web site.

Figure 3: Security Analytics Engine malware detection



Cloud Access Manager user authentication

Cloud Access Manager provides several user authentication options through configured Front-End Authenticators (FEA) that you can use to provide user identification details for Security Analytics Engine to match SonicWALL malware detection records. In the following example, both Active Directory and LDAP authenticator configuration details are provided that will support Security Analytics Engine and the SonicWALL malware record provided domain\user user name format:

- Active Directory Authenticator - User attributes that support the domain\user user name format are retrieved automatically.
- LDAP Authenticator – Utilize LDAP user attributes that will enable user name correlation to SonicWALL malware records by correlating to the user attributes in the directory used for SonicWALL authentication, for example:
  - Unique Id – canonicalName (Active Directory) or distinguishedName (OpenLDAP).
  - Login Name – sAMAccountName (Active Directory) or Uid (OpenLDAP).
  - Mail – mail (Active Directory or OpenLDAP).

The process of Cloud Access Manager authenticating internal and external users and forwarding IP address and user identification information to Security Analytics Engine for risk policy evaluation, including finding records associated with malware, is depicted in Figure 4 and described below:

1. User1 accesses a Cloud Access Manager application from either inside the corporate network, or optionally from the Internet.
2. Cloud Access Manager performs evaluations to determine whether the user's access to the application is authorized.
3. When the user is authenticated using either an Active Directory or LDAP FEA, user identification attributes are retrieved that detail the user identity and are used as part of the authorization evaluation, these include:

   Active Directory FEA

   Upn: MyCorp\User1

   UniqueId: 0A2524D3-352D-4025-B6EE-7AC868D7A3D4

   Mail: user1@mycorp.com

   or

   LDAP FEA

   Upn: User1

   UniqueId: CN=Corp User1,CN=Users,DC=mycorp,DC=com

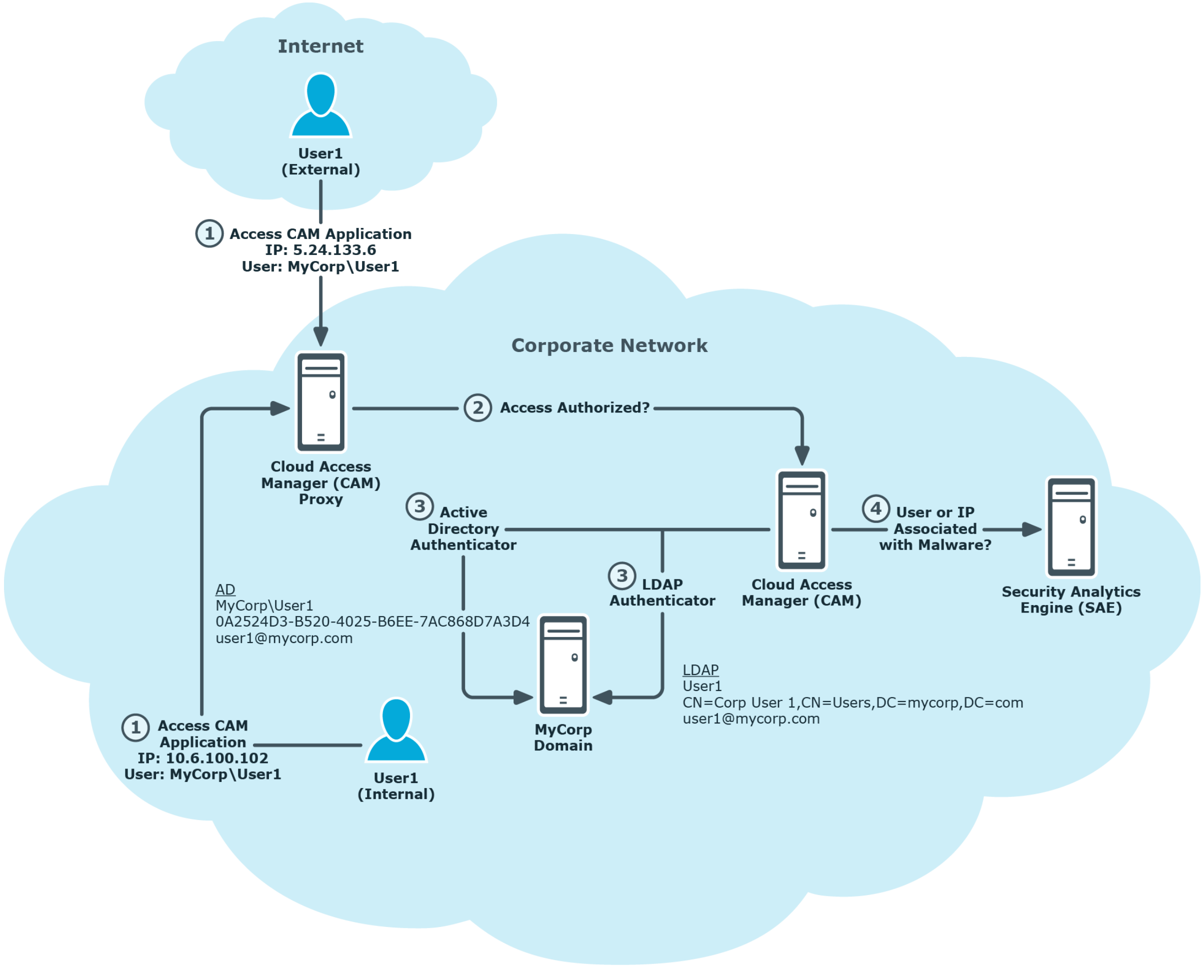
   Mail: user1@mycorp.com

4. While determining authorization, Cloud Access Manager queries Security Analytics Engine to determine the user's risk score, and forwards the IP address and user attribute information for processing by Security Analytics Engine. During the risk

score evaluation, Security Analytics Engine will search for malware records received from the firewall and match on either a user name or IP address.

In the case where an LDAP FEA is used, the Security Analytics Engine evaluation will correlate the LDAP provided attributes to the mycorp\User1 format.

Figure 4: Cloud Access Manager Front-end Authenticators and user identification



Using split DNS to forward internal IP addresses to the Security Analytics Engine

When Cloud Access Manager notifies the Security Analytics Engine of a security event, it includes, as part of the contextual information, the IP address of the end-user’s machine. Since users can access Cloud Access Manager from the internal network, as well as from the Internet, Cloud Access Manager must ensure that the correct IP address (internal or external) is reported. To ensure that the internal address is reported for connections coming from the internal network, split DNS must be configured for the Cloud Access Manager proxy hostname.

About us

Contacting us

For sales or other inquiries, visit https://www.oneidentity.com/company/contact-us.aspx or call +1-800-306-9329.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product