

Microsoft Active Directory Authentication with SonicOS 3.0 Enhanced and SonicOS SC 1.0 (CSM 2100CF)

Introduction

SonicWALL Unified Threat Management (UTM) appliances running SonicOS Enhanced 3.0 support user level authentication (ULA) against a Microsoft Active Directory user database, as does the SonicWALL CSM 2100CF Content Filtering appliance, but the methods in which these two appliances communicate with Active Directory is substantially different.

This Technote explains the communication methods employed by each device, and identifies the differences between them. For a full description of implementing User Level Authentication on either the SonicWALL CSM 2100CF or a SonicWALL security appliance running SonicOS Enhanced 3.0, refer to the following user guides:

- SonicOS SC 1.0 Administrator's Guide
- SonicOS Enhanced 3.0 Administrator's Guide

The most noteworthy difference between the two appliances is that the CSM 2100CF supports 'Single Sign On' integration with Active Directory, while SonicOS Enhanced 3.0 does not support Single Sign On.

Instead, SonicOS Enhanced 3.0 provides an interface for the manual authentication against Microsoft's Active Directory by means of full Lightweight Directory Access Protocol (LDAP) client integration. This allows SonicOS 3.0 Enhanced to provide ULA functions against any implementation of LDAP (e.g. Active Directory, OpenLDAP, Novell eDirectory) while the CSM 2100CF only supports Microsoft's Active Directory.

Single Sign On

The term 'Single Sign On' (SSO) refers to the automated reuse of user credentials across multiple authentication checkpoints. Since most users today begin their computing sessions by logging on to a Microsoft Windows Active Directory (MSAD) domain, the ability to reuse these MSAD credentials is a significant convenience to users in environments where subsequent authentication is required; a prime example of this is Content Filtered environments, where certain users are to be granted access to some content, while other users are to be denied access to said content. Rather than requiring the user to provide his or her credentials a second time for the purpose of authenticating to the Content Filtering system, SSO provides an automated facility to reuse the credentials the user provided when first logging on to the workstation, making the subsequent authentication process transparent to the user.

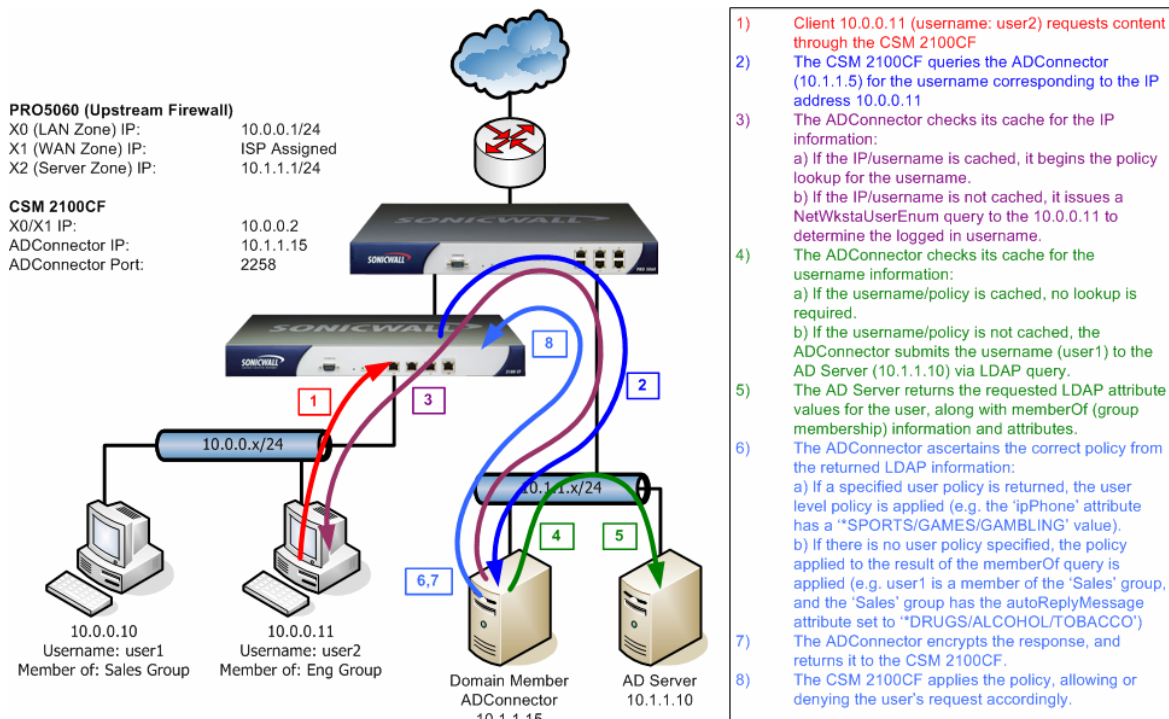
The SonicWALL ADConnector

The SonicWALL CSM 2100CF achieves this level of transparency, through automated Single Sign On integration by means of the SonicWALL ADConnector. The ADConnector is an installable agent that runs as a service on a Microsoft Win32 workstation or server that is either a domain member or domain controller for the target (authenticating) domain.

▷ SONICWALL TECH NOTE :

After successful installation, and upon the service being started, the ADConnector will query its configured DNS server to locate a Domain Controller (DC) Resource Record. If there are multiple DCs available, it will use the first DC returned in the DNS response. The ADConnector will then send all queries to this DC.

The following diagram illustrates the process and flow of information employed by the SSO Active Directory integration of the CSM 2100CF and the ADConnector:



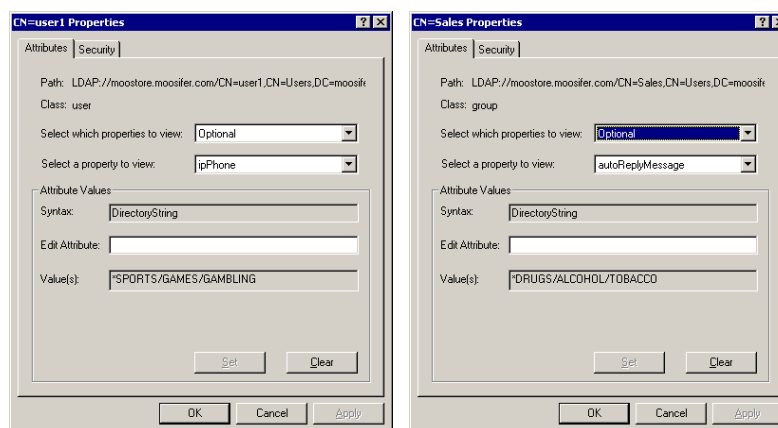
- 1) A workstation with an IP address of 10.0.0.11, configured with a default gateway of 10.0.0.1 requests content (e.g. <http://www.sonicwall.com>) through the CSM 2100CF. The user logged on to the workstation is a member of the local AD domain, has logged on with username 'user1', and is a member of the 'Sales' group.
- 2) The CSM 2100CF detects the request, and queries the ADConnector (residing on domain member server 10.1.1.5) for the username corresponding to the IP address 10.0.0.10.
- 3) Since the ADConnector caches information to speed responses to queries, it first checks its cache to see if it's previously resolved this IP address to the corresponding username.
 - a. If the cache contains the information, move to step 4.
 - b. If the cache does not contain the information (e.g. this is the first request from IP address 10.0.0.10) the ADConnector uses the Microsoft dotNet framework to issue a NetWkstaUserEnum Lib call from netapi32.dll to 10.0.0.10 to determine the username logged on to the current session. This function call is complete in its result, returning all logon information for local, terminal service, impersonated users, and interactive logons.

▷ SONICWALL TECH NOTE :

- 4) Upon receiving the logged on username information ('user1'), the ADConnector checks its cache again to see if it has the applicable policy associated with the username 'user1'.
 - a. If the cache contains the information, move to step 7.
 - b. If the cache does not contain the information the ADConnector issues an LDAP query to the AD Server (10.1.1.10) to retrieve the correct attribute information for the user, as well as group membership (memberOf) information, and relevant group attribute information.
 - c. The Active Directory server returns the response to the LDAP query. This includes the pertinent* attribute information for the user, the memberOf (group) information for the user, and the pertinent* attribute information for the group.

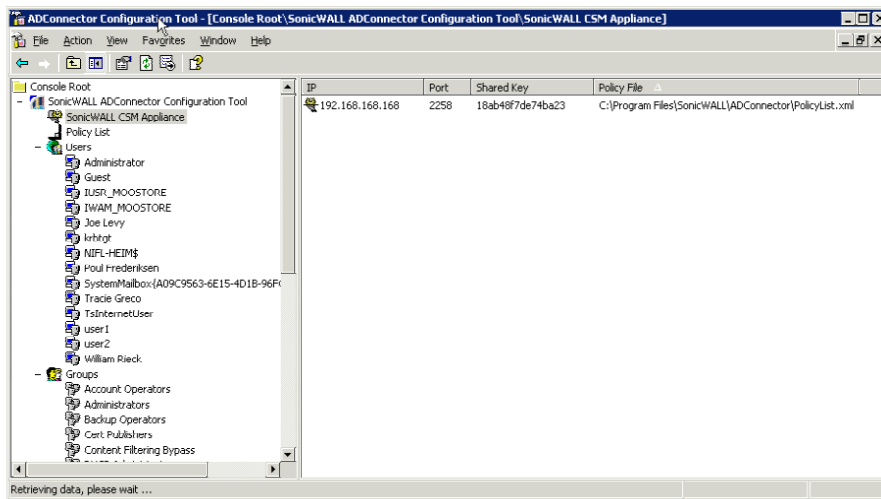
*During installation of the ADConnector, AD attributes are selected as the 'containers' for the user and group policy applications. These are optional attributes within AD, so as to reduce the potential of collisions. In our example, we have selected 'ipPhone' as the user attribute, and 'autoReplyMessage' as the group attribute.

Note: It is possible to view the actual policy information stored within Active Directory with such tools as Microsoft's ADSI Edit (Active Directory Services Interface). ADSIEdit is a part of the Microsoft support tools, which is located in the Support directory of the Windows 2000/2003 Server installation media. ADSIEdit and other such tools should be used with extreme discretion and caution, as it has the ability to directly manipulate Active Directory content.



- 5) The ADConnector processes the information returned to the LDAP query to ascertain the actual effective policy.
 - a. If the user has a policy specified, that policy will be used as the effective policy. In our example, the user 'user1' has the '*SPORTS/GAMES/GAMBLING' value set in the 'ipPhone' attribute, resulting in that policy being the effective policy for 'user1'.
 - b. If the user did not have a specific policy applied, the ADConnector will apply the policy set belonging to the response to the memberOf (group membership) query. In our example, since 'user1' has a specific policy, the policy applied to the 'Sales' group will not be applied to 'user1'. If there was another user (e.g. 'user3') who was also a member of the 'Sales' group, but who did not have a specific policy assigned, that user would inherit the '*DRUGS/ALCOHOL/TOBACCO' policy as the value from the 'autoReplyMessage' attribute for the 'Sales' group.

▷ SONICWALL TECH NOTE :



6) The ADConnector validates and correlates the response to its current (and constantly synchronized) policyList.xml file. It then 3DES encrypts the response, and returns it to the CSM 2100CF. The following is a sample excerpt from a policyList.xml file, and the meaning of the status codes:

| <pre> <CFAPOLICY> <INDEX>1</INDEX> <STATUS>0</STATUS> <NAME>*ADULT CONTENT</NAME> </CFAPOLICY> <CFAPOLICY> <INDEX>2</INDEX> <STATUS>0</STATUS> <NAME>*DRUGS/ALCOHOL/TOBACCO</NAME> </CFAPOLICY> <CFAPOLICY> <INDEX>3</INDEX> <STATUS>0</STATUS> <NAME>*RACISM/HATE/VIOLENCE/WEAPONS</NAME> </CFAPOLICY> </pre> | <table border="1"> <thead> <tr> <th>Status Code</th> <th>Meaning</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>Policy OK</td> </tr> <tr> <td>1</td> <td>Policy deleted</td> </tr> <tr> <td>2</td> <td>Policy assigned</td> </tr> <tr> <td>4</td> <td>Policy synchronization error</td> </tr> <tr> <td>8</td> <td>Policy only found in agent</td> </tr> </tbody> </table> | Status Code | Meaning | 0 | Policy OK | 1 | Policy deleted | 2 | Policy assigned | 4 | Policy synchronization error | 8 | Policy only found in agent |
|--|--|-------------|---------|---|-----------|---|----------------|---|-----------------|---|------------------------------|---|----------------------------|
| Status Code | Meaning | | | | | | | | | | | | |
| 0 | Policy OK | | | | | | | | | | | | |
| 1 | Policy deleted | | | | | | | | | | | | |
| 2 | Policy assigned | | | | | | | | | | | | |
| 4 | Policy synchronization error | | | | | | | | | | | | |
| 8 | Policy only found in agent | | | | | | | | | | | | |

Note: The policyList.xml file should never be manually edited. For reference, it resides, by default, in the C:\program files\SonicWALL\ADConnector\ directory on ADConnector agent server. It is an XML file that contains all the policies retrieved from the CSM 2100CF, along with a corresponding index number, and status information.

7) The CSM 2100CF applies the policy and allows the request from 'user1'.

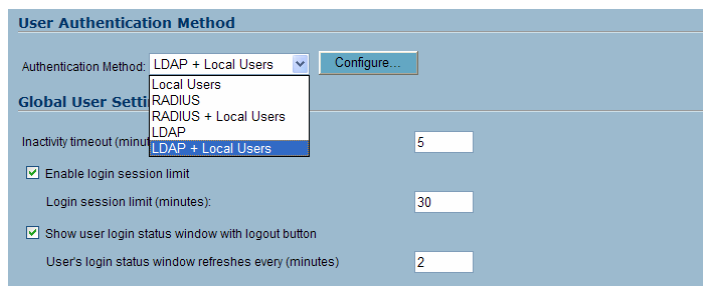
SonicOS 3.0 Enhanced Active Directory / LDAP Client

Active Directory support on SonicOS Enhanced is not a single-sign on mechanism, but rather the ability for SonicOS Enhanced to act as an LDAP client against an Active Directory's LDAP interface using Microsoft's implementation of an LDAP schema. SonicOS Enhanced provides extremely flexible schema interoperability, with support for the Microsoft AD schema, the LDAP core schema, the RFC2798 inetOrgPerson schema, and even user-defined schemas. Connectivity to LDAP servers is also flexible, with support for following protocols:

- LDAPv2 (RFC3494)
- LDAPv3 (RFC2251-2256, RFC3377)
- LDAPv3 over TLS (RFC2830)
- LDAPv3 with STARTTLS (RFC2830)
- LDAP Referrals (RFC2251)

▷ SONICWALL TECH NOTE :

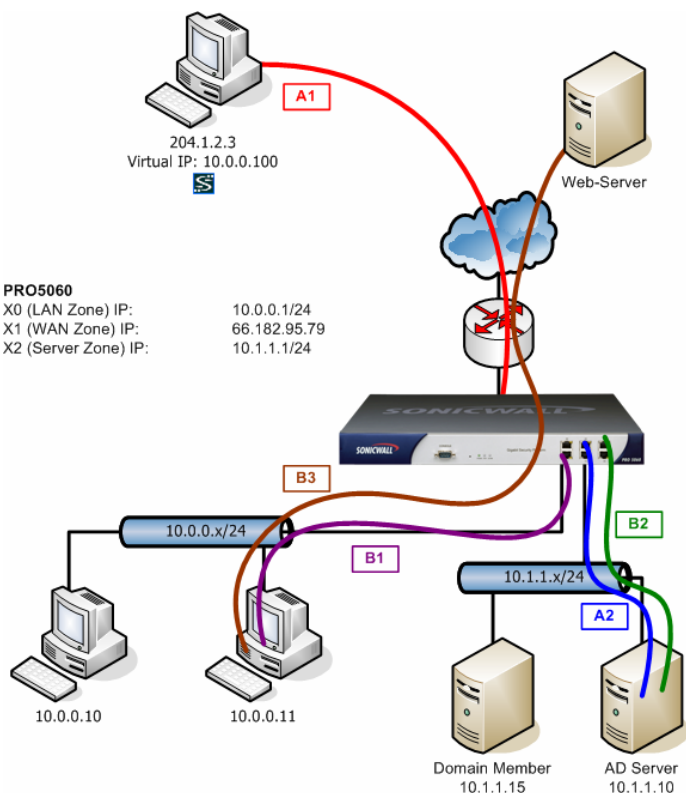
LDAP / AD Configuration is performed from the 'Users>Settings' page on the SonicWALL management UI. The 'User Authentication Method' provides a drop-down list of options:



Selecting either 'LDAP' or 'LDAP+Local Users' and clicking 'Apply' at the top of the page will enable LDAP support, the former using an LDAP directory server exclusively, and the latter using a combination of the LDAP server and the local user database. Please refer to the SonicOS 3.0 Enhanced Admin Guide for information on completing the LDAP/AD client configuration.

After the LDAP authentication method has been configured, it can be used for User Level Authentication for many purposes within SonicOS Enhanced, including:

- GlobalVPN remote access (XAUTH) authentication
- Firewall Access Rules authentication
- Content Filtering Service (CFS) authentication



Remote VPN (GVC) Client

A1) GVC Client (ISP assigned IP address 204.1.2.3) initiates a remote access connection to PRO 5060 at 66.182.95.79.

PRO 5060 has WAN GroupVPN configured for XAUTH against LDAP/AD server 10.1.1.10. Presents XAUTH challenge to GVC Client 204.1.2.3

A2) Credentials are passed to AD server 10.1.1.10. If credentials are valid, an Accept message is received and processed by the PRO 5060, and the GVC session is established. VPN access can be granularly controlled by the user's group membership.

Internal User – CFS Enabled

B1) Internal client (10.0.0.11) requests web-page http://www.sonicwall.com through CFS enabled PRO 5060.

PRO 5060 redirects the request to the internal authentication page, prompting the user to enter username and password.

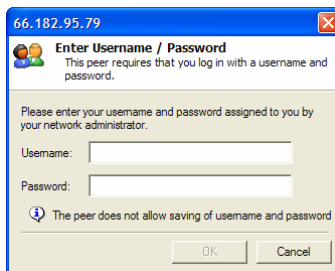
B2) The provided credentials are pass to AD server 10.1.1.10. If the credentials are valid, an Accept message is received and processed by the PRO 5060, and the user session is permitted.

B3) The client is automatically redirected to the originally requested resource, http://www.sonicwall.com, and a session status window is presented to the user.

▷ SONICWALL TECH NOTE :

Two scenarios are presented in the illustration above. The first shows remote user (GVC Client) authentication against an AD/LDAP server, and the second shows Content Filtering Service (CFS) authentication against an AD/LDAP server.

- A1) A remote user (ISP assigned IP address 204.1.2.3) running the SonicWALL GVC client initiates a remote access connection to the PRO 5060's WAN GroupVPN at 66.182.95.79. The WAN GroupVPN is configured to use XAUTH against the LDAP/AD server 10.1.1.10, and also has the virtual adapter enabled.



The client is presented with the 'Enter Username / Password' window, and enters their AD username and password.

- A2) The provided credentials are presented to the AD server via LDAP. If the credentials are valid, the AD server presents an accept message, and the GVC negotiation proceeds. The client will have access VPN access according to the default LDAP group privileges, or to the specific memberOf (group membership) VPN privileges assigned to analogously configured local user groups (refer to the SonicOS Enhanced 3.0 Admin Guide for details).

The second scenario has more similarities to a CSM 2100CF deployment, but it significantly different. The key difference is that the CSM 2100CF does not require manual authentication as is required by SonicOS Enhanced's AD/LDAP client method:

- B1) Internal client (10.0.0.11) requests a web page (<http://www.sonicwall.com>) through the CFS enabled PRO 5060. The client is a member of the local domain, and has already logged on to the workstation as 'user1'.

The PRO 5060 cannot automatically derive the user information (as can the CSM 2100CF). Instead, it redirects the user to its local auth.html page so that the user may present a username and password.

- B2) The provided credentials are presented to the AD server via LDAP. If the credentials are valid, the AD server presents an accept message, and the PRO 5060 CFS system validates the session.
- B3) The client is automatically redirected to the originally requested resource, <http://www.sonicwall.com>, and a session status popup window is presented to user to govern the session, and to provide session status information.

Date: 12-17-04
Version 1.1