How do I configure my WSA to do LDAP Authentication Group Policy?

Document ID: 117937

Contributed by Kei Ozaki and Siddharth Rajpathak, Cisco TAC Engineers.
Jul 15, 2014

Contents

Question:

Environment: Cisco Web Security Appliance (WSA), all versions of AsyncOS

This Knowledge Base article references software which is not maintained or supported by Cisco. The information is provided as a courtesy for your convenience. For further assistance, please contact the software vendor.

For "Authentication Group" to work, first we need to configure an authentication realm under "GUI > Network > Authentication".

1. First set "Authentication Protocol" as 'LDAP' and navigate to "Group Authorization" (with other section correctly configured).
2. Specify your "Group Name Attribute". This is the attribute which holds the value that is displayed under "Web Security Manager" > "Web Access Policies" > "Click Add Group" > "Select Group Type to Authentication Group" > "Directory Lookup" table. This attribute needs to be unique and the leaf node represented by this attribute needs contain a list of users in its group.
3. Next, specify the "Group Filter Query". This is the search filter which WSA uses to locate all the GROUP in LDAP directory.
4. Now, specify "Group Membership Attribute" which is the attribute in the leaf node that would hold the members unique value. Since this attribute is holding the member of this GROUP, you would see multiple entries. Please make sure that value included in this attribute corresponds to the value included in "User Name Attribute" located on the same page.

Below is an example of how WSA would use the LDAP realm configuration to match a username against a LDAP group:

1. Let's say we set "Group Filter Query" to "objectClass=group"
2. WSA would first use this filter and search through the LDAP directory, and find the result.
3. Then, using the result, WSA will look for the attribute specified in "Group Membership Attribute". Let's say this is an attribute called "member".
4. Now if a user logs in as 'USERNAME_A' through the WSA proxy, WSA would look up the user's account in LDAP server, and if there was a match it would use the attribute specified under "User Name Attribute" (example: uid) and checks if "uid" matches against users listed in "member" attribute collected above.

5. If there was a match the user would use the policy configured and if not, then WSA would evaluate the next policy in line.

To see what attributes need to be configured using your LDAP server, please refer to "Softerra LDAP Browser" http://www.ldapbrowser.com

---

Updated: Jul 15, 2014 Document ID: 117937
