Usage guide for vpnsync.exe

Vpnsync is a utility which will list all members of a selected AD security group, ensure that those user accounts exist on a chosen XG firewall, and set ensure that the selected users are granted rights to connect using Sophos Connect IPsec VPN client. This utility may be scheduled to run periodically, to automatically add new users to the firewall, with correct VPN access rights.

Requirements

The vpnsync utility requires the following information and access:

- API access to your XG firewall
- XG Firewall credentials with rights to create user accounts
- Access to a domain account. No increased privileges are necessary
- Access to Active Directory over LDAP port 389
- The script must be run from a Windows host that is a domain member
- The windows host should have a static IP address

Installation instructions

The utility does not require installation, it is provided in a zipped archive, that contains all files necessary to execute

1. Extract the archive to the location you wish to run the script from.
2. Choose where to place the script on your windows host. The script will attempt to log results to the same folder it is run from, so be sure that it will be able to write to the folder when run by an unprivileged domain account

XG Configuration

Configuring API access

1. Login to the XG firewall WebAdmin interface
2. Navigate to Backup & Firmware > API
3. Add the IP address of your windows host to the Allowed IP address list
4. Enable API configuration if it is not
5. Click Apply to save the changes

Creating an administrator role with minimal privileges (optional, but recommended)

1. When logged into the WebAdmin interface, Navigate to Profiles > Device Access
2. Click Add
3. Enter **vpnsync API Access** in the Profile Name field
4. Scroll down, and locate the Identity group, then click the + icon to expand it
5. Locate Users, then select Read-Write permissions
6. Ensure all other editable columns are set to None
7. Click Save

Creating an administrator account for use with the vpnsync utility (optional, but recommended)

1. When logged into the WebAdmin interface, Navigate to Authentication > Users
2. Click Add
3. In the **User name** and **Name** fields, enter **vpnsync**
4. Choose a strong password, and enter it in the **Password** field
5. Set the user type to **Administrator**
6. Set the profile to **vpnsync API Access**
7. Enter an email address in the email field. It does not need to be a real email address, just be a value in the form of an email address
8. Set the group to **Open Group**
9. Click Save

Vpnsync configuration

Creating the configuration file

All configuration for the vpnsync executable file should be stored in the file: vpnsync.yml, located in the same folder as the application. It should be opened in a text editor such as notepad.exe, to make configuration changes.

When editing the file, do not add extra lines, or change the indentation of any lines. When changing values, such as the username on line 3 ("user: vpnsync") be sure to leave a single space between the colon(:) and the start of the value you enter.

1. Copy the file vpnsync-default.yml, and rename the copy to vpnsync.yml, and open it in the text editor of your choice.
2. Follow the comments on lines starting with # to set the correct values for your environment
3. AD is accessed via LDAP currently. LDAPS is not supported in this version.
4. The userDN value must be in correct LDAP syntax. If you are unsure of the correct syntax to use, run ADSI Edit on a domain controller. After connecting to your domain, the first folder listed under "Default naming context" will show the correct syntax for this value.
5. The vpngroupDN value must be in correct LDAP syntax. If you are unsure of the correct syntax to use, run ADSI Edit on a domain controller. After connecting to your domain, expand the folders below "Default naming context" to locate the the desired security group. The Distinguished Name field will reveal the correct value to enter for this parameter.

Testing

Once XG API access is enabled and vpnsync.yml is configured, simply run vpnsync.exe. Results will be written to the vpnsync.log in the same folder as the application. If there are any errors, please reference this file as a first troubleshooting step. If working as expected, you should see members of the chosen AD group listed on the console window while it is executing, and once it is complete, you should see all current members of the AD group added to the firewall, and given permission to connect to Sophos Connect.

Scheduling

This script does not install and auto-start, or run as a service. It must be scheduled using an application such as the windows task scheduler. When using the windows task scheduler, it is recommended to keep the recurrence to the minimum amount necessary (Daily is recommended). If a large number of users are created at one time, it may put unexpected load on your firewall. Task Scheduler will ask you to supply a user account to run the task. A privileged user is not needed, only a domain account with permission to list users is needed. It is recommended to create an account specifically for this task, and to set the permissions of any folders that vpnsync.yml files are located in to be accessible by only select users, including the user created to execute the commands, as the yml files will contain username and password information, for both the firewall and your AD environment.

How to schedule using Task Scheduler:

- On the server you've chosen to run the script, click Start, then begin typing Task Scheduler. When you see the Task Scheduler application presented, launch it
- Click on the Task Scheduler Library
- Click Create Task
- On the General tab, click Change User or Group, and select the user created for this task
- Select **Run whether user is logged in or not**
- On the Triggers tab, add a new trigger
- Set the schedule to **Daily**
- Set the desired start time
- Optionally, for more frequent updates, select **Repeat task every** and choose a more frequent time interval
- Click **OK** to save the trigger
- On the Actions tab, add a new Action
- Select Start a program, then in the **program/script** field, browse for the location of vpnsync.exe
- If you are syncing multiple groups with multiple yml config files, enter the path of the first one in the **Start in** field
- Click **OK** to save the Action
- Click OK to save the task
- Select the task in the list, and select Run, to test that the task is functioning correctly, and view the vpnsync.log file in the same folder as the vpnsync.yml file.

Limitations

- Vpnsync does not support nested user groups. Only direct members of the chosen AD group will be synchronized.
- Users removed from the AD group will not be removed from Sophos Connect access rights on XG, though disabled or deleted AD users will no longer be able to connect
- Only one group may be specified in the vpnconfig.yml file
- The filename vpnconfig.yml is hardcoded, and cannot be named differently
- The vpnconfig.yml file is expected to reside in the present working directory, when vpnsync.exe is executed

- Synchronizing multiple groups is possible, but requires separate vpnconfig.yml files to be located in separate directories, and when executed, that the working directory for vpnconfig.exe be set to the location of the selected config file.
- Vpnsync does not come with any support or warranty. It is provided as-is, and free of charge. If you require support in using this utility, it is recommended that you consult with other Sophos users on the Sophos Community Forums.