NETGEAR Application Note

SSL312 VPN Concentrator: Integration with Microsoft Active Directory

Summary

The SSL312 is a versatile tool that allows end users to connect to the corporate network from any remote location with internet access. Since SSL is not VPN there is no need for client software. The end user opens the desired application such as email, enters the user name and password to authenticate, and a secure connection is created. This document will discuss how to use Active Directory as the authentication service.

This document provides a step-by-step procedure on how to configure SSL312 for use with Active Directory (AD) to authenticate the users. The document is targeted for users who currently utilize Microsoft Active Directory and want to integrate the SSL312 with AD. The integration of SSL312 with AD will greatly reduce the administration time of having to add users to the SSL by utilizing the user settings existing in AD.

Even though, there are generic references to Active Directory procedures, it is recommended to utilize a Microsoft technical training document for Active Directory configurations. This document is not a good source for settings, configurations, or troubleshooting Active Directory.

This document elaborates on and does not replace the NETGEAR® *ProSafe® SSL VPN Concentrator 25 SSL312 Reference Manual*, sections 3 through 10. Windows Active Directory is one of many authentication options on the SSL VPN concentrator. For more options, please refer to the SSL 312 VPN Concentrator user manual on the NETGEAR support site.

Active Directory is a centralized location for managing services, such as user authentication for your remote SSL VPN users. Since company users and their access information are defined on the AD server, what you need to do on the SSL 312 box is configure the AD domain. This will give access to all your users on the AD server.

Configuring SSL312 for Integration with Active Directory

Active Directory authentication servers support a group and user structure that can be queried when an Active Directory user logs in. This means that you can create Policies and Bookmarks for Active Directory users at the group level without needing to define Active Directory users in the SSL VPN concentrator. Policies and Bookmarks provide end users with access to company resources such as applications and servers. When a user logs in, if no corresponding user name is configured on the local database, then SSL

VPN Concentrator will query the Active Directory server for the list of groups to which the user belongs.

Once you create an Active Directory domain, you can add groups that correspond with groups on your Active Directory server. If the Active Directory user is configured in the SSL VPN concentrator, then the SSL VPN concentrator will ignore the AD group information and, instead, implement policies and bookmarks based on the settings of the group to which the user belongs.

Confirming Connectivity

Before configuring the SSL VPN concentrator to authenticate through Active Directory, it is important to check connectivity, as well as make some preliminary configurations.

To confirm connectivity:

1. Make sure that Active Directory is functioning properly.
2. Ensure that there is IP communication between the AD server and the SSL box. Do a simple ping from the AD server to the SSL and from the SSL box using the Diagnostics menu to ping the AD as well as a DNS lookup, if applicable.

Preliminary Configurations

There are a few procedures to configure in preparation for AD, which are Portal Layouts, Groups, and User configurations. For detailed step-by-step procedures for configuring Portal Layouts, Groups, and Users, please refer to the *Reference Manual* found on the support site at *http://kbserver.netgear.com/main.asp*.

Portal Layouts

Portal Layouts allow you to create a custom page that remote users will see when they log into the portal. Because the page is completely customizable, it provides the ideal way to communicate remote access instruction, support information, technical contact info, or VPN-related news updates to remote users. The page is also well-suited as a starting page for restricted users; if mobile users or business partners are only permitted to access a few files or web URLs, the page you create will only show those links relevant to these users.

Custom Portals are accessed at a different URL than the default portal. For example, if your SSL VPN portal is hosted at https://vpn.company.com, and you created a portal layout named “sales”, then users will be able to access the sub-site at https://vpn.company.com/portal/sales.

Configuring Users and Groups

It is important to understand the policy hierarchy. There are Global Policies that apply to all groups and users accessing the SSL VPN concentrator and Group Policies that apply to all users. The following list describes the hierarchy:

- User Policies take precedence over all Group Policies.
- Group Policies take precedence over all Global Policies.
- If two or more user, group, or global policies are configured, the most specific policy takes precedence.

For using an Active Directory authentication server, you do not need to add individual users into the SSL VPN Concentrator unless you want to define specific policies or bookmarks per user. Configure groups using the same group names as defined in your authentication server.

When configuring Users and Groups, remember that user policies take precedence over all group policies and group policies take precedence over all global policies, regardless of the policy definition. (A user policy that allows access to all IP addresses will take precedence over a group policy that denies access to a single IP address).

SSL VPN concentrator groups are also defined using the Users and Groups menu.

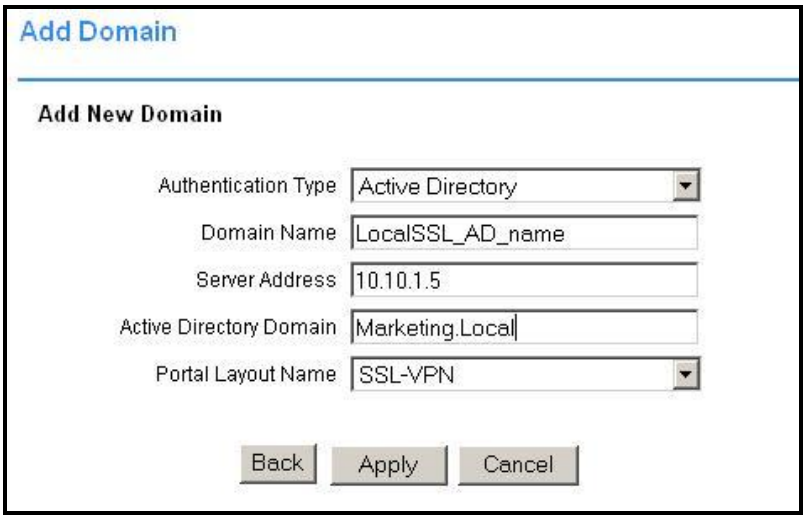
To configure a group:

1. Under the Access and Administration menu in the left navigation pane, click **Users and Groups**. The Add Group window displays for you to add your group.
2. In the **Group Name** field, enter the group name.
3. Select a domain from the **Domains** drop-down menu.
4. When you are finished, click **Apply**.

Configuring Windows Active Directory Authentication

To configure Windows Active Directory authentication:

1. Under the Access and Administration menu in the left navigation pane, click **Domains** then click **Add Domain**. The Add Domain window displays.



2. From the **Authentication Type** drop-down menu, select **Active Directory**. Fields for Active Directory configuration display.
3. In the **Domain Name** field, enter a descriptive name for the authentication domain. This is the same value as the Server Address field or the Active Directory Domain field, depending on your network configuration.
4. In the **Server Address** field, enter the IP address or host name of the Active Directory server.
5. In the **Active Directory Domain** field, enter the Active Directory domain name.
6. From the **Portal Layout Name** drop-down menu, select the name of the portal layout. The default layout is SSL-VPN. You can define additional layouts in the Portal Layouts screen.
7. To force users to supply a valid digital certificate before granting access, select the **Require Client Digital Certificates** radio button. The CNAME of the client certificate must match the user name that the user supplies to log in, and the certificate must be generated by a certificate authority (CA). That is trusted by the SSL VPN concentrator.
8. Click **Apply** to update the configuration. Once the domain has been added, the domain displays in the table on the Domains screen.

Troubleshooting Tips

The time settings between the Active Directory server and the SSL VPN concentrator must be synchronized. Kerberos authentication, used by Active Directory to authenticate clients, permits a maximum of a 15-minute time difference between the Windows server and client (the SSL VPN concentrator). The Easiest way to solve this issue is to configure Network Time Protocol (NTP) on the Date and Time screen, and make sure that the server's time settings are also correct.

To properly set up Active Directory, NTP must be configured in both the SSL312 and the Windows 2000 or Windows 2003 server. Active Directory uses Kerberos5 protocol for

authentication. For Kerberos to work, the clock skew between the server (Windows) and the client (SSL312) must be less than 60 minutes.

For NETGEAR FAQs please refer to the following links:

http://kbserver.netgear.com/kb_web_files/n101641.asp

http://kbserver.netgear.com/kb_web_files/n101642.asp

For additional information on NETGEAR SSL VPN product information, please refer to the following links:

- SSL VPN concentrator at

http://tools.netgear.com/landing/2006/SSLVPN/index_eu.aspx?cid=70130000000GqmP

- Support and documents at *http://kbserver.netgear.com/main.asp*

Conclusions

SSL312 VPN Concentrator can easily integrate with a wide variety of pre-existing authentication methods, such as AD. Integration with AD saves the administrator time and money by having a centralized location to manage all users. The SSL312 VPN Concentrator allows end users to easily access company resources such as email and file share. Since SSL is not VPN it is not necessary to install client VPN software which greatly reduces administration cost.

February 15, 2007