CONTENTS

Introduction to NPS Authentication with AD ......................... 2
Registering the NPS in Active Directory Domain Services ...... 4
Adding Stonesoft Components to the Active Directory .......... 9
Creating an Active Directory Server Element .................... 10
Defining a New LDAP Domain ......................................... 12
Configuring the Firewall Policy for Authentication ............... 13
Introduction to NPS Authentication with AD

This document describes how to configure your Windows Server 2008 Network Policy Server (NPS) as the authentication method for Stonesoft Firewall/VPN with Active Directory (AD) as the Directory service. The configuration described in this document is meant for authenticating VPN client users or users of browser-based user authentication. The example scenario below is for browser-based user authentication. For information on configuring browser-based user authentication, see the Stonesoft Administrator's Guide.

AD and NPS are included in most, but not all, editions of Windows Server 2008. Introducing AD and NPS into your organization's network is outside the scope of this document. Consult Microsoft's documentation for further instructions.

The example scenario in this document assumes the following AD integration (connections between Stonesoft components are excluded):

Illustration 1  Example Scenario for Active Directory Integration

The NPS is in the same network as the Management Server. The firewall cluster is included in the scenario to ensure high availability, as a single firewall could be a single point of failure. Because the communications between the firewall engines and the NPS are not encrypted, the network is connected to the firewall cluster through a dedicated communications channel. The example values in the steps and illustrations found throughout this document reflect the scenario above.

We also assume that the AD contains the objects shown in Illustration 2.

Illustration 2  AD Organization in This Scenario
**Configuration Overview**

The general workflow for configuring the NPS as the authentication method with AD is divided into two parts. The first part describes how to configure the Network Policy Server:

1. Register the NPS in your AD. See Registering the NPS in Active Directory Domain Services (page 4).
2. Add a Stonesoft firewall engine as a RADIUS client in the NPS. See Adding a Stonesoft Firewall Engine as a RADIUS Client in the NPS (page 5).
3. Create a Connection Request Policy. See Creating a Connection Request Policy for Stonesoft Engines (page 6).
4. Enable dial-in for the end-users. See Adding a Network Policy for Stonesoft Engines (page 7).
5. Add a user account for the Stonesoft components to allow Bind access to the AD. See Adding Stonesoft Components to the Active Directory (page 9).

The second part describes how to configure user authentication in the Stonesoft Management Client:

2. Create an LDAP Domain element for your AD and select **Network Policy Server** as the default authentication method. See Defining a New LDAP Domain (page 12).
3. Configure the Firewall Policy for Authentication. See Configuring the Firewall Policy for Authentication (page 13).

Start by Registering the NPS in Active Directory Domain Services (page 4).
Registering the NPS in Active Directory Domain Services

**Prerequisites:** The Network Policy and Access Services role is installed on the NPS

The AD does not allow NPS to access the user information by default. Allow this as instructed below.

**To register the NPS in Active Directory Domain Services**

1. On the NPS, select **Start**→**Administrative Tools**→**Network Policy Server**.

2. Right-click **NPS (Local)** and select **Register server in Active Directory**. The Network Policy Server dialog opens.

3. Click **OK** to allow the NPS to access the Active Directory.

Continue by **Adding a Stonesoft Firewall Engine as a RADIUS Client in the NPS** (page 5).
Adding a Stonesoft Firewall Engine as a RADIUS Client in the NPS

To add a Stonesoft firewall engine as a RADIUS client in the NPS

1. Expand the RADIUS Clients and Servers branch.

2. Right-click RADIUS Clients and select New. The New RADIUS Client dialog opens.

3. Enter a Friendly name.

4. Enter the IP address that the engine uses to establish the connection. Use an NDI address of a specific node in a firewall cluster.

5. Enter a Shared Secret and confirm it. You must later enter the same secret for the Active Directory Server element in the Stonesoft Management Client. In this example, the shared secret is Pass1234.

Caution – Do not activate the options on the Advanced tab. The Stonesoft Management Center does not support the Message-Authenticator attribute option available in the NPS and is not NAP-capable.
6. Click **OK**.

7. If your firewall is a firewall cluster, repeat steps 1-6 to add each node as a RADIUS client.

The finished configuration for our example scenario is shown below.

Continue by creating a Connection Request Policy for Stonesoft Engines to allow authentication requests from the firewall nodes that act as RADIUS clients and allow end-users to access the VPN.

**Creating a Connection Request Policy for Stonesoft Engines**

▼ **To create a Connection Request Policy**

1. In the Network Policy Server console, expand **Policies**.

2. Right-click **Connection Request Policies** and select **New**.

3. Give the Connection Request Policy a descriptive name and click **Next**. The **New Connection Request Policy** opens.

4. Click **Add**. The **Select condition** dialog opens.

5. Under the **Connection** category, select **Access Client IPv4 Address** and click **Add**.
6. Type in the IP address that is selected as the IPv4 address of the Access Client requesting access from the RADIUS client and click Next. The **New Connection Request Policy** dialog opens.

![New Connection Request Policy dialog](image)

7. Select **Override network policy authentication settings** and click Next.

Continue by **Adding a Network Policy for Stonesoft Engines** to define which users can access the network.

## Adding a Network Policy for Stonesoft Engines

You can define users that are allowed to access the Active Directory either through user properties in the AD or through the Network Policy in the NPS. The section below explains how the users are defined through the Network Policy in the NPS.

**To add a Network Policy for Stonesoft engines**

1. In the Network Policy Server console, expand **Policies**.

2. Right-click **Network Policy** and select **New**. The **New Network Policy** dialog opens.

![New Network Policy dialog](image)
3. Click Add. The Select condition dialog opens.

4. Select User Groups under the Groups category and click Add. The User Groups dialog opens.

5. Click Add Groups. The Select Group dialog opens.

6. Type in the name of the group.
   • Alternatively, type in the beginning of the name, click Check Names, and select the group.

7. Click OK twice to return to the New Network Policy dialog.

8. Make sure Access Granted is selected and click Next.
9. Select **Unencrypted authentication (PAP, SPAP)** as the authentication method. This is the only method that Stonesoft firewalls support.

Note – PAP is only used between the firewall engines and the NPS. Within this connection, authentication data is sent in cleartext form. Make sure the connection is otherwise secure (for example, by using a dedicated network link).

10. Click **Next**. A message related to using unencrypted authentication is displayed. To continue with the configuration, click **No**.

11. Click **Next** twice, then click **Finish**.

12. Move the new condition you created into the first position (one position at a time) by selecting **Move Up** in the right-click menu for the Network Policy.

13. *(Optional)* Enable the users in the selected user group to authenticate regardless of user-specific settings:
   13a. Double-click the new Network Policy to open its properties.
   13b. Select **Ignore user account dial-in properties**.
   13c. Click **OK**.

Continue by Adding Stonesoft Components to the Active Directory.

**Adding Stonesoft Components to the Active Directory**

**Prerequisites:** Registering the NPS in Active Directory Domain Services

The Stonesoft Management Server performs an LDAP BIND operation using a user account in the AD to retrieve the user information. This makes the information available for use in Stonesoft configurations. In this example, the account only requires read access to the user database and the AD domain is **support.com**. Illustration 3 shows the Stonesoft account defined in the AD. It is stored in the “Admins” Organizational Unit (OU).

**Illustration 3  Example Stonesoft Account in the Active Directory Users and Computers Panel**
Illustration 4 shows the end-user accounts defined in the AD. Users Lisa and Bob are members of the “VPN Client Users” user group. “Sales” is an Organizational Unit (OU).

Illustration 4  Example Users in the Active Directory Users and Computers Panel

To successfully authenticate, the end-user accounts must be allowed dial-in access in the User properties in the AD or in the Network Policy. In this example, the Network Policy was set to override the Users’ properties.

Continue by Creating an Active Directory Server Element.

Creating an Active Directory Server Element

You must next create in the Management Client an Active Directory Server element that contains the user database and authentication options needed to use an Active Directory server to store and authenticate users. This scenario assumes that there is no NAT between the Stonesoft components and the NPS. When NAT is applied, the Location and Contact Address must be defined.

▼ To create an Active Directory Server element

1. In the Stonesoft Management Client, select Configuration → Configuration → User Authentication. The User Authentication Configuration view opens.


3. Specify a unique Name and IP Address. In this example, we use Win2008_AD and 192.168.1.210.
4. Switch to the **Connection** tab.

5. In the **Base DN** field, enter the path to the end-user accounts. In this example, this is `ou=sales,dc=support,dc=com`. The value has a limit of 160 characters.

6. In the **Bind User ID** field, define the user account that the firewall and Management Server use to connect to the AD. In this example, this is `cn=stonesoft,ou=admins,dc=support,dc=com`.

7. In the **Bind Password** field, enter the password for the Stonesoft user account. In this example, this is the password for the user account `stonesoft`.

8. Make sure that the **LDAP on Port** number is correct for your Network Policy Server's AD. The default port in Stonesoft is the default port that AD uses for LDAP.

9. *(Recommended)* Select **LDAP Start TLS** to enable Transport Layer Security (TLS) for the AD connections. TLS is only used if the AD server supports it.

10. Switch to the **Authentication** tab.

11. Make sure that the **Port Number** is correct for your NPS.
- The default port in Stonesoft is the default port the NPS uses for RADIUS. Only the default port is allowed in the predefined Firewall Template Policy. You must allow a non-standard port yourself.

12. Enter the **Shared Secret** that you defined for the RADIUS clients that you defined for the Stonesoft engines on the NPS. In our example, this was `Pass1234`.

13. Click **OK**.

Continue by **Defining a New LDAP Domain** (page 12).
Defining a New LDAP Domain

Each LDAP server has its own LDAP Domain in the Stonesoft Management Center. One LDAP Domain can be selected as the default, so that end-users can leave out the domain information when they authenticate (they can type “username” instead of “username@LDAP Domain”). Users stored under non-default LDAP domains must always include the LDAP Domain in the username.

To define a new LDAP Domain

1. In the Stonesoft Management Client, select Configuration→Configuration→User Authentication. The User Authentication Configuration view opens.

2. Right-click Users and select New LDAP Domain.

3. Enter a Name. In this example, we use support.com.

4. Select Default LDAP Domain if this LDAP Domain is used for all or most authentications.

5. Select the AD Server element (in our example, Win2008_AD) and click Add.
6. Switch to the **Default Authentication** tab.

7. Click **Select** and double-click **Network Policy Server**.

8. Click **OK**.

9. Expand the branch of the new LDAP Domain and its subfolders until you see the user accounts retrieved from the AD.
   - If no error messages appear, the AD integration with your Management Server is successful.
   - Most frequently, problems are either authentication-related (such as wrong username/password), connectivity-related, or the result of an incorrect Base DN path for retrieving the user information.
   - You can use the `ldp` tool on the NPS to manually test Bind operations against the AD.

Continue by Configuring the Firewall Policy for Authentication.

## Configuring the Firewall Policy for Authentication

The end-user's authentication connection to the firewall and the firewall engines' LDAP and RADIUS connections to the NPS are allowed in the predefined Firewall Template Policy using the default ports. If your configuration is non-standard in some way, add corresponding Access rules to the Firewall Policy.

Successful authentication is recorded by the firewall so that the information can be used as matching criteria in Access rules when the user accesses services.

You can use browser-based user authentication with AD server authentication. For information on enabling browser-based user authentication, see the *Stonesoft Administrator's Guide*. In this section, we first test user authentication and then change the Access rules to allow secure access in a production environment. The following scenario assumes that browser-based user authentication is enabled on the firewall and that a rule that allows browser-based user authentication has been added to the Firewall Policy.

### To configure Access rules for testing authentication

1. Add the following IPv4 Access rules to the Firewall Policy and install the Policy.
   - The first IPv4 Access rule allows anyone to ping.
   - The second IPv4 Access rule allows user Lisa with the login name “lisay” to access web pages after authentication.

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Users</th>
<th>Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANY</td>
<td>ANY</td>
<td>Ping</td>
<td>Allow</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Testing Client</td>
<td>ANY</td>
<td>HTTP</td>
<td>Allow</td>
<td>User “lisay” in AD</td>
<td>Network Policy Server authentication method</td>
</tr>
</tbody>
</table>
2. Open a web browser and connect to the firewall's CVI address. In our example, we use 192.168.1.1.

3. Log in as user “lisay”. The username syntax is either username@LDAP Domain or just username for the default LDAP domain. In this example, these are lisay@support.com or lisay, respectively. The password is the account password in the AD.
   - Everything you type is case sensitive.
   - The domain you enter when authenticating is the name of the LDAP Domain in the Stonesoft Management Center, not the domain in the AD.
   - Most frequently, errors at this point are due to a lack of connectivity or to an authentication failure on the NPS.

4. After successful authentication, test HTTP connectivity through the firewall.

In this example, user Bob with the login name “bobt” can also successfully authenticate, as his account is stored in the AD alongside Lisa’s account. However, Bob does not gain HTTP access after authentication because his account is not included in the IPv4 Access rule.

Considerations for Access rules in production environments:

- Use User Group elements (such as “VPN Client Users” in our example) to allow access to all users included in that user group, so that any changes in the contents of the user group do not require any changes in the Access rules. If you add an individual User element to a rule, the user name is recorded in the policy and is not removed until you manually remove it.
- Set the Action to Use IPsec VPN (the Enforce option) to make the rule apply specifically to VPN client access within a specific (separately configured) VPN. This also activates the VPN in the policy.

Depending on the IP address that the DHCP server gives to the VPN clients’ virtual adapters, additional Access rules may be needed to handle that address range. However, existing rules match both authenticated and unauthenticated users as well as VPN and non-VPN traffic, unless the Access rule explicitly states something different.
Stonesoft Guides

Administrator’s Guides - step-by-step instructions for configuring and managing the system.

Installation Guides - step-by-step instructions for installing and upgrading the system.

Reference Guides - system and feature descriptions with overviews to configuration tasks.


For more documentation, visit
www.stonesoft.com/support/

Stonesoft Corporation
Itälahdenkatu 22 A
FI-00210 Helsinki
Finland
Tel. +358 9 476 711
Fax +358 9 476 1349

Stonesoft Inc.
1050 Crown Pointe Parkway
Suite 900
Atlanta, GA 30338
USA
Tel. +1 770 668 1125
Fax +1 770 668 1131

Copyright 2012 Stonesoft Corporation. All rights reserved. All specifications are subject to change.