Important Information

Latest Software

We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Latest Documentation

The latest version of this document is at:
http://supportcontent.checkpoint.com/documentation_download?ID=12297

For additional technical information, visit the Check Point Support Center (http://supportcenter.checkpoint.com).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>05 June 2011</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>

Feedback

Check Point is engaged in a continuous effort to improve its documentation.

Please help us by sending your comments (mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on How to Configure Client Authentication  Technical Reference Guide).
Objective

This document explains how to configure VPN client authentication with a Check Point R70 firewall. Client Authentication permits multiple users and connections from the authorized IP address or host. Authorization is performed per machine, so client authentication is best enabled on single-user machines.

For example, authorize FINGER for a client machine. All users on this machine are authorized to use FINGER. The VPN client does not ask them to enter a password during the authorization process.

The main advantage of client authentication is that it can be used on a number of connections for any service. Authentication can be set to valid for a time period. These authentication methods can also be used for unencrypted communication.

Authentication is required for Remote Access communication using SecuRemote or SecureClient.

Details

Supported Versions

- Check Point NGX R65 to Check Point R70

Supported OS

- Operating Systems supported by NGX R65 up to R70, and all HFA levels
- IPSO 4.2 – 6.2
- SecurePlatform 2.4/2.6

Supported Appliances

- All IPSO appliances
- All SecurePlatform models

Assumed Knowledge:

- Use of SecuRemote or SecureClient
- Configuration of R70 Security Gateways for Remote Access users

Related Documentation

- sk44460: Client Authentication does not work when restricted with an Address Range object http://supportcontent.checkpoint.com/solutions?id=sk44460
- sk43957: Client authentication with https http://supportcontent.checkpoint.com/solutions?id=sk43957
- sk35018: How to enable client authentication for http traffic that does not run on port 80 http://supportcontent.checkpoint.com/solutions?id=sk35018

Impact on the Environment and Warnings

Port 259 and 900 must be open on the gateway.
Creating Users and Groups

Authentication rules are defined by user groups rather than individual users. To define authentication rules, you must first define users and groups. You can define users with the Check Point user database, or with an LDAP server. To learn more about LDAP in Check Point, see *Smart Directory (LDAP) and User Management* in the *R70 Security Management Server Administration Guide* (http://supportcontent.checkpoint.com/documentation_download?ID=8745).

You can update users and groups without re-installing the Rule Base. To install the user database, click **Policy > Install Database**.

If you have a user database or LDAP server, define the user accounts first, and then define groups to add the accounts to. If you will create user accounts one by one, you can first define a user template. User accounts based on a template inherit group association and other properties.

These procedures are done in the SmartDashboard.

Creating User Groups

To create a user group:
1. Click **Network Objects** tree > **Users and Administrators** tab > **User Groups**.
2. Right-click and select **New Group**.
   The Group Properties window opens.
3. Assign the group a name.
4. Add users to the group.
Creating User Templates

Define user templates to make it faster to create individual user accounts. After you create a template, user accounts based on it inherit the properties of the template, including membership in groups. User accounts are not dynamically updated with template changes. If you change the properties of a template, those changes affect only future user accounts.

To create a user template:
1. Click Network Objects tree > Users and Administrators tab > Users.
2. Right-click Templates and select New Template.
   The User Template Properties window opens.
   ![User Template Properties window](image)
3. Enter a name for the template.
   ![Template name](image)
4. In the Groups tab, add the user template groups.
   When you create a user account based on this template, the user is assigned to these groups automatically.
5. In the Authentication tab, select an authentication scheme.

6. In the remaining tabs, enter properties for the user template.

Creating User Accounts

To create user accounts:
1. In the Users branch of the Network Objects tree, right-click and select an account template. The User Properties window opens.
2. Enter the user data.
   You can change the properties that the user inherited from the template, without changing the template.
Authentication Schemes

Authentication schemes use usernames and passwords to identify valid users. Some schemes are maintained locally. The usernames and passwords are stored on the gateway. Other schemes are maintained externally, and the user authentication data is stored on an external authentication server. Some schemes, such as SecurID, are based on a one-time password. All of the schemes can be used with users defined on an LDAP server.

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check Point Password</td>
<td>The gateway stores a static password in the local user database of each user configured in Security Management Server. No additional software is required.</td>
</tr>
<tr>
<td>Operating System Password</td>
<td>The gateway authenticate using the username and password stored on the client OS. You can also use passwords that are stored in a Windows domain. No additional software is required.</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Remote Authentication Dial-In User Service (RADIUS) - an external authentication scheme for security and scalability that separates the authentication function from the access server. Using RADIUS, the Security Gateway forwards authentication requests from remote users to the RADIUS server. The RADIUS server authenticates users with the user account data that is stored on it. The RADIUS protocol uses UDP to communicate with the gateway. RADIUS servers and RADIUS server group objects are defined in SmartDashboard.</td>
</tr>
<tr>
<td>SecurID</td>
<td>With SecurID, users have a token authenticator and a PIN or password. Token authenticators generate one-time passwords that are synchronized to an RSA ACE/server and change approximately every minute. Token authenticators can be hardware or software. Hardware tokens are key-ring or credit card-sized devices. Software tokens are on the PC or device from which the user authenticates. When a user authenticates, the one-time use code is validated by the ACE/server. The gateway acts as an ACE/Agent 5.0 and forwards authentication requests from remote users to the ACE/server. ACE manages the database of RSA users and their assigned tokens.</td>
</tr>
<tr>
<td>TACAS</td>
<td>Terminal Access Controller Access Control System (TACACS) - an access control for routers, network access servers and other networked devices through centralized servers. TACACS is an external authentication scheme that provides verification services. Using TACACS, the gateway forwards authentication requests from remote users to the TACACS server. The TACAS server authenticates users with the user account data that is stored on it. The system supports physical card key devices (token cards) and Kerberos secret key authentication. TACACS encrypts the username, password, authentication services and accounting data of authentication requests.</td>
</tr>
<tr>
<td>Undefined</td>
<td>If a user with an undefined authentication scheme is matched to a Security Rule with some form of authentication, access is always denied.</td>
</tr>
</tbody>
</table>

Client Authentication and Sign On

Client Authentication can be used to authenticate any service. It enables access from a specific IP address for an unlimited number of connections. The client user requests authentication, but it is the client machine that is granted access.
Client Authentication is less secure than user authentication, because it permits access for multiple users and connections from authorized IP addresses or hosts. Authorization is given per machine, for services that do not have an initial login procedure.

The advantages of Client Authentication are that it can be used for an unlimited number of connections, for any service, and is valid for any length of time.

Note - When configuring user objects, you can set the locations that users can access. But this can cause problems with security rules that require some form of authentication

Client Authentication works with all sign on methods. For sign on methods other than Manual Client Authentication, the Security Gateway is transparent to the users. They authenticate directly to the destination host.

Manual Sign On

To connect:

- Telnet to port 259 on the gateway.
- HTTP connection to the gateway on port 900 and a web browser.

The requested URL must include the gateway name and the port number. For example: http://gateway:900

Standard Manual Sign On

In this example of a Standard Manual Sign On method, before opening a connection to the destination host, the user msmith first authenticates to fw1, the Security Gateway.

```
Pc1% telnet fw1 259
Trying 191.23.45.67 ...  
Connected to fw1.
Escape character is '^[].'
CheckPoint FireWall-1 Client Authentication Server running on fw1
Login: msmith
FireWall-1 Password: ********
User authenticated by FireWall-1 auth.
Choose:
(1) Standard Sign On
(2) Sign Off
(3) Specific Sign On
Enter your choice: 1
User authorized for standard services (1 rules)
Connection closed by foreign host.
```

Specific Manual Sign On

In this example of a Specific Manual Sign On method, two services are specified: rstat and finger (each one to a different host).
Partially Automatic Sign On

Partially Automatic Sign On is available for authenticated services (Telnet, FTP, HTTP and RLOGIN) only if they are defined in the client authentication rule. If the user attempts to connect to a remote host using one of the authenticated services, they must authenticate with User Authentication.

When using Partially Automatic Client Authentication, make sure that port 80 is accessible on the gateway.

Fully Automatic Sign On

Fully Automatic Sign On is available for any service only if the required service is defined in the client authentication rule. If the user attempts to connect to a remote host using an authenticated service (Telnet, FTP, HTTP, and RLOGIN), they must authenticate with User Authentication. If the user attempts to connect to a remote host using any other service, they must authenticate through a properly installed Session Authentication agent.

When using Fully Automatic Client Authentication, make sure that port 80 is accessible on the gateway.

Agent Automatic Sign On

Agent Automatic Sign On is available only if the required service is defined in the Client Authentication rule, and the Session Authentication agent is properly installed. If a user attempts to connect to a remote host using any service, they must authenticate through a Session Authentication agent.

Single Sign On

Single Sign On is available for any service only if the required service is defined in the client authentication rule and UserAuthority is installed. Single Sign On is a Check Point address management feature for transparent network access.

The gateway looks at the user IP address records to see which users are logged on to a given IP address. When a connection matches a Single Sign On enabled rule, the gateway queries UserAuthority with the packet's source IP. UserAuthority returns the name of the user who is registered to the IP address. If the user's name is authenticated, the packet is accepted. If not, it is dropped.
Enabling Client Authentication Wait Mode

When using Manual Sign On and the user authenticates with a Telnet session to port 259 on the gateway, *Wait* mode eliminates the need to open a new Telnet session to sign off and withdraw client authentication privileges.

**To enable Wait mode:**

1. In SmartDashboard, open the properties of the Check Point Gateway object that represents the VPN gateway.
2. Select **Authentication > Enable Wait Mode for Client Authentication**. The gateway monitors the Telnet connection to port 259 of the gateway by pinging the user's host.
3. Define rules to enable pinging:
   - Enable the echo-request service from the gateway to the user's host.
   - Enable the echo-reply service from the user’s host to the gateway.

Configuring Basic Client Authentication

1. Configure the required users and groups for authentication and install the User Database.
2. From the Check Point Gateway object properties > **Authentication**, enable the authentication schemes. The gateway must support all the user defined authentication schemes. For example, if some users must provide a Check Point password, and others RADIUS authentication, select both schemes.
3. Define a Client Authentication access rule:
   a) Right-click in the **Source** column, select **Add User Access**, and then select the group. Do not close the window.
   b) To restrict the location of authenticating users, in the **Location** section of the same window, select **Restrict To** and select the host, group of hosts, network or group of networks that users can access.
   c) In **Service**, select the services you want to authenticate.
   d) In **Action**, select **Client Auth**.

4. For Partially or Fully Automatic Client Authentication, make sure that port 80 is accessible on the gateway machine.
6. Put all Client Authentication Rules above the rule that prevents direct connections to the gateway (the Stealth Rule). This makes sure that clients have access to the gateway.

7. If necessary, open Global Properties > Authentication, and change the Failed Authentication Attempts settings for Client Authentication.

8. Install the security policy.

Authorizing All Standard Sign On Rules

By default, the Partially or Fully Automatic sign on methods open one rule following successful authentication (the rule for which the sign on was initiated). For example, if a user successfully authenticates according an automatic sign on rule, the user can work with the services and destinations permitted only by that rule.

You can configure the gateway to automatically open all Standard Sign On rules following successful authentication using Partially or Fully Automatic Sign On. If a user successfully authenticates according to an automatic sign on rule, then all Standard Sign On rules that define that user and source are available. The user can then work with all the services and destinations permitted by the relevant rules. The gateway knows which user is on the client, and additional authentication is not necessary.

To authorize all relevant Standard Sign On rules following successful Partially or Fully Automatic authentication, use the GUIDbedit Database Tool to change a setting in the gateway database.

To authorize all standard sign on rules:
1. Access the GUIDbedit Database Tool from the directory where SmartConsole is installed.
2. Open GUIDbedit.
3. Search for automatically_open_ca_rules.
4. Set the value to true.

The new value takes effect after you install the security policy.
Changing the Client Authentication Port

To change the Client Authentication port number:
1. Stop the gateway services: `cpstop`
2. Change the port number in the Manage > Service > Show > TCP Services window for these services:
   - To change the port number for Telnet sign on, change the port number of the `FW1_clntauth_telnet` service.
   - To change the port number for HTTP sign on, change the port number of the `FW1_clntauth_http` service.
   These are Check Point gateway services, provided as part of the Client Authentication.
3. Use a simple text editor to edit the `$FWDIR/conf/fwauthd.conf` file. Change the port number of the Client Authentication application to the port number defined in the service, with one of these:
   - For Telnet Sign On, change the first column in the `in.aclientd` line.
   - For HTTP Sign On, change the first column in the `in.ahclientd` line.

Example of an `$FWDIR/conf/fwauthd.conf` file:
```
21fwssd in.aftpd wait 0
80 fwssd in.ahtpd wait 0
513 fwssd in.arlogindwait 0
25 fwssd in.asmtpd wait 0
23 fwssd in.atelnetd wait 0
259 fwssd in.aclientd wait 259
10081 fwssd in.lhtpd wait 0
900 fwssd in.ahclientdwait 900
0 fwssd in.pingd respawn 0
0 fwssd in.ahclientdwait 900
0 fwssd in.ahclientdwait 900
0 vpn vpnd respawn 0
0 fwssd mdq respawn 0
0 xrm xrmdrespawn0 -pr
```

⚠️ Important - Do not change anything else in these lines.

4. Make sure that there is no rule that blocks the connection to the new port.
5. Restart the gateway: `cpstart`

Allowing Encrypted Client Authentication

You can configure the gateway to allow connections over HTTPS.

To configure encrypted Client Authentication:
1. Stop the gateway services: `cpstop`
2. Open `$FWDIR/conf/fwauthd.conf` and change
   ```
   900 fwssd in.ahclientd wait 900
to
   901 fwssd in.ahclientd wait 901 ssl:Cert_Nickname
   ```
   Note - `Cert_Nickname` is taken from VPN Certificate List. To find the nickname of your gateway, open Gateway Properties > VPN and see Certificates List.
3. Save and close the file.
4. Run: `cpstart`
5. Open SmartDashboard.
6. Create this rule:

```
NewGroup@Any, Internal_LAN, Any Traffic, TCP https, Client Auth, Log
```
This rule also allows HTTPS traffic between the client and the Web server after successful authentication.

7. Install the policy.

8. In the client's browser, do:
   a) Enter the URL of the gateway: https://<FireWall-1_name_or_IP_address>:901
   b) Click Yes to trust the VPN-1 gateway certificate.
   c) Enter the VPN user name.
   d) Click OK.
   e) Click Yes.
   f) Enter the VPN password.
   g) Click Submit.
   h) Enter the URL of the Web server: https://<Internal_Web_Server_IP_address>
   i) Click Yes.

The client is authenticated to the gateway and to the internal Web server.

### Tracking Authentication

You can track successful and unsuccessful authentication attempts in SmartView Tracker, or you can use other tracking options, for example, email and alerts. You can configure authentication tracking for different types of authentication attempts.

**Failed authentication attempts:**

Can be tracked for all forms of authentication.

To track failed authentication attempts:

a) Open Gateway Properties > Authentication.

b) Select the tracking option in Authentication Failure Track.

**Successful authentication attempts:**

Can be tracked for Client Authentication.

To track successful authentication attempts:

a) In the Client Auth rule, right-click Action.

   The Client Authentication Action Properties window opens.

b) Select the Successful Authentication Tracking option. The default setting is Log.

**All Authentication attempts:**

Can be tracked for all forms of authentication.

To track all authentication attempts, in a rule that uses authentication, select an option in Track.

The Set by Rule tracking option can only be added to the tracking policy set in the gateway object. For example, if the gateway object is set to log all failed authentication attempts, setting a rule to None has no effect and failed authentication attempts are still logged in SmartView Tracker. But setting the rule to Alert causes an Alert to be sent for each failed authentication attempt.

### Verifying the Procedure

1. Select an authentication scheme.
2. Login with the authentication scheme and necessary credentials.
   Test also for credentials that should fail.