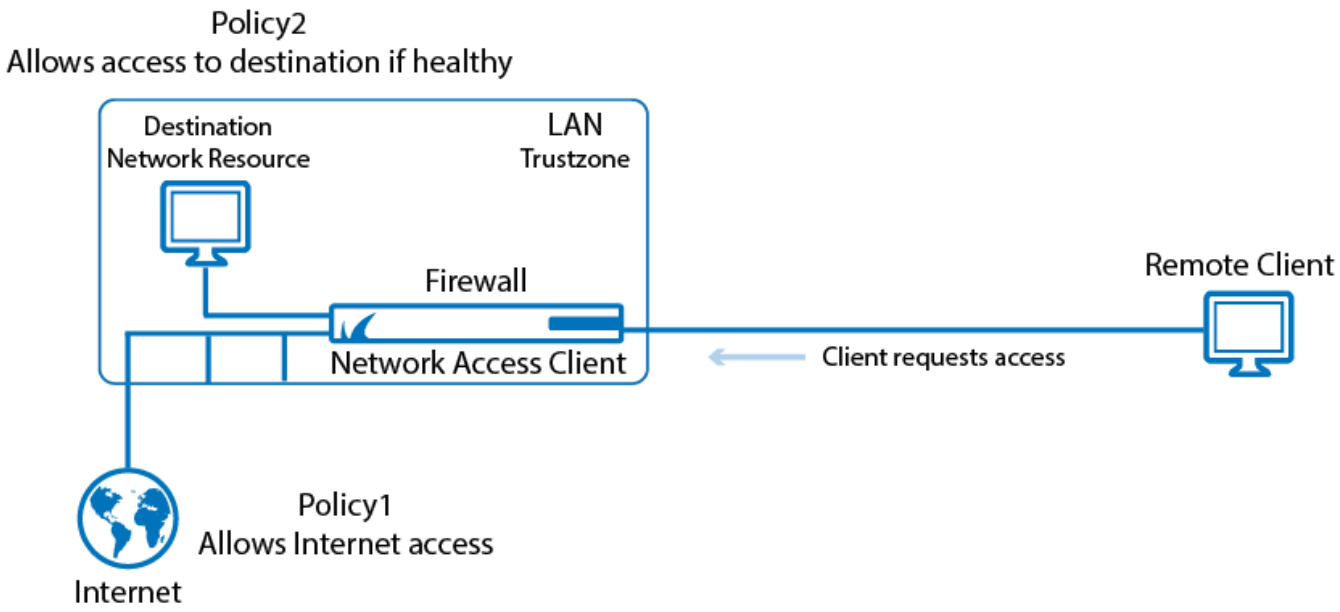
Rules and Policy Matching

https://campus.barracuda.com/doc/46895151/

The Barracuda Network Access Client provides a managed personal firewall solution with periodic health assessments. The outcome of the assessment and the identity of the machine and/or current user will influence the policy applicable to the endpoint. Each Access Control Service belongs to a so-called trust zone. All Access Control Services within the same trust zone share the same set of security policies. In addition, they share a signing key, so that a mutual trust relationship can be established. Within each trust zone, there is a **Local Machine** policy ruleset that is used to determine a policy for a connecting machine. As soon as user authentication is requested by the connecting client, the **Current User** policy ruleset is used for policy matching. If the connection attempt is mediated by an intermittent VPN service, the **VPN** policy ruleset is adopted.



The Policy Ruleset

Up to three firewall rulesets can be assigned to a **secured and monitored** endpoint. A policy ruleset is processed from the top to the bottom in sequential order. Each policy rule consists of three parts:

- An identity-related part that defines the applicable matching policy and criteria.
- A health policy part is used to determine the health state by comparing the status information sent by the client with the specified required status.
- A policy attribute part that contains firewall rulesets, messages, pictures, and network access policies that are **assigned to a healthy client**.

When the endpoint system goes online and connects to the SHV, it will be assigned a **Local Machine**

ruleset and a **Limited Access** ruleset. The **Limited Access** ruleset is the one ruleset that comes into effect when the endpoint is diagnosed as **unhealthy** by the SHV. If no identity match can be found, a **No Rule Exception** policy is assigned. The client system is assumed untrusted, and a configured **Untrusted Access** firewall ruleset and client message applies.

As soon as a user logs into the system, a different policy may apply to the endpoint now, depending on the identity of the user and various other conditions. The assigned policy attributes may cause a different **Current User** ruleset to be assigned. This ruleset is cleared when the user logs off or the system is rebooted.

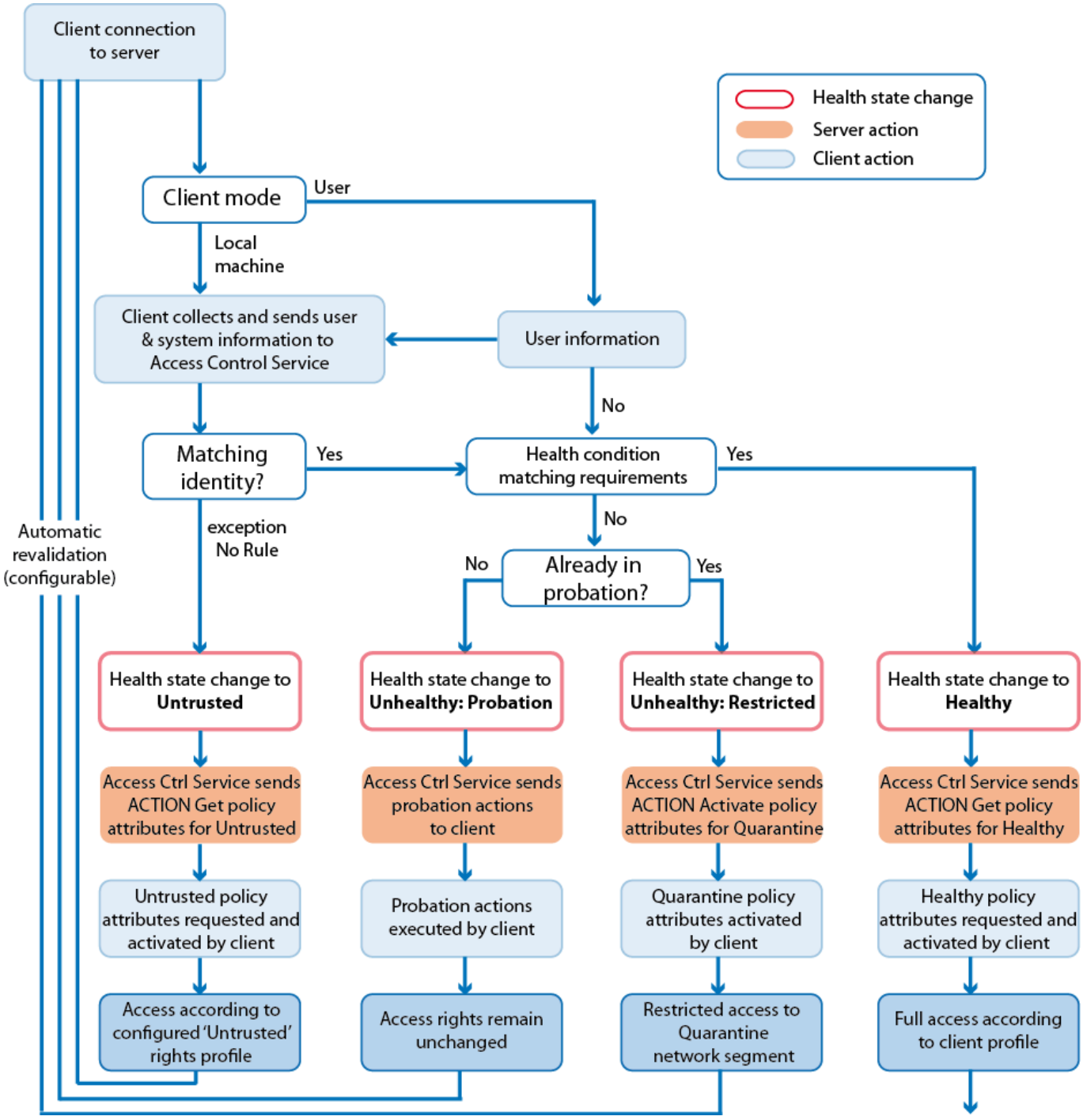
Consequently, a notebook that has been used in the office environment and is taken home in the evening will operate at home with the most recently installed **Local Machine** ruleset.

Any endpoint whose system state is assessed as unhealthy will have the most recently installed **Limited Access** ruleset activated by the client after a configurable grace period. The **quarantine** state is not entered immediately because there is a configurable period of time during which the client is given a chance to recover from the current condition, for example, by successfully starting a disabled antivirus (AV) scanner service or updating an obsolete AV pattern file.

Rulesets should always mirror a company's overall abstract security policy. To implement CloudGen Firewalls at a clear network perimeter, such as. an internal-Internet transition, the ruleset should be built according to SAEM:

1. **S**trictly Enforce
2. **A**nalyze
3. **E**nforce
4. **M**onitor

The Client-Server Interaction Process



The following client-server interactions are processed by the the various components of the Barracuda Network Access Client when connecting, validating health, and assigning network access:

Step 1. The Applicable Ruleset is Determined

The Barracuda Network Access Client determines which context it is started in and which method it uses to connect to the Access Control Service.

- **Local Machine context** – The local machine context applies during the startup of a Windows computer as well as after user logout. Since the Windows system distinguishes between **Current User** and **Local Machine** context, it is necessary to handle the local machine context separately, e.g., no pop-ups are allowed if no user is logged in. Certificate-based authentication is available for both **Local Machine** and **Current User Authentication;** however, different Microsoft certificate stores are available to get the certificates from. A **Local Machine** certificate must not be password protected because dialog boxes to request the password will not be available.
- **Current User context** – As soon as a user has logged in successfully, the client switches to the **Current User** context. Now, additional information like the username and the password (or Kerberos ticket in case of NTLM authentication) can be used to perform identity matching. Because the user context allows pop-up and client windows to be opened, the client can notify the user about the current health state or request additional information. For example: Basic Authentication: popup requests username and password.
- **VPN context** – The VPN context is an extension of the **Current User** context. The client can determine if a Barracuda VPN connection was initiated as well as if the VPN server has Access Control Service capabilities. If the client mode is VPN, all possibilities available in user mode are available as well. Additionally, an online and offline ruleset can be assigned to the client.

Step 2. The Client connects to the Access Control Service

The client connects to the configured Access Control Service. The IP address of the Access Control Service is either configured manually (during installation) or is assigned by the DHCP server. The connection is based on TCP and uses port 44000 to communicate between client and server. The connection is always initiated by the client.

During the handshake, the Access Control Service notifies the client of its capabilities (e.g., 'NTLM authentication is available'). As a response, the client collects all available system information and sends this information back to the Access Control Service together with authentication credentials. This response contains details about the computer's network (e.g., IP address, MAC-address), the computer's operating system (e.g., OS version, hostname, domain name, user and certificates) as well as details about installed health suite, and antivirus or anti-spyware products.

Further policy matching on the Access Control Service depends on the data collected and sent from the client.

Step 3. The Client Identity is Determined

Depending on the client mode (**Local Machine**, **Current User**, **VPN**), the Access Control Server determines the applicable policy ruleset, which is then used to perform identity matching. The available identity information is sequentially matched from top to bottom with the identity conditions of the individual policies. Each policy can be configured to match if all configured identity criteria apply or if only one of the configured criteria applies.

Matching Criteria	Local Machine	Current User	VPN

Client Connection Type	Yes	Yes	Yes
Current Date and Time	Yes	Yes	Yes
NetBIOS Domain	No	Yes	Yes
Group Patterns	No	Yes	Yes
User (Log-in Name)	No	Yes	Yes
Network	Yes	Yes	Yes
OS Version	Yes	Yes	Yes
Hostname	Yes	Yes	Yes
MAC Address	Yes	Yes	Yes
X.509 Certificate Conditions	Yes	Yes	Yes

If a match is found, the comparison of the health information sent by the client with the stated health requirements of the policy rule continues. In case no rule matches, you can configure a **No Rule Exception** that notifies clients even if they cannot be identified. A better way to control clients is to manually apply a **Catch-All** rule at the end of the policy ruleset.

Health Matching

At the beginning of the client-server communication, the health state of the client is **Uninitialized**. If the quarantine ruleset is already available on the client, the client activates this ruleset, but remains in the **Uninitialized** state. This state triggers an immediate connection to the configured Access Control Service. As soon as the communication between the client and the Access Control Service is established and policy matching is performed, a health state is assigned. Usually, Access Control Service and VPN client have the same health state. The only exception is the **Uninitialized** state. In this case, the Access Control Service is not aware of the existence of the client.

Untrusted Health State

When the identity match is finished and the client's identity cannot be validated, the health state changes to **Untrusted**. Untrusted does not necessarily mean that the client may be a guest client, but only that the Access Control Service cannot determine the client's identity. Nevertheless, the **Access Control Service Trustzone > Settings > No Rule Exception** configuration parameter allows you to assign a set of client attributes.

Probation Health State

If the health match fails, the client still receives a cookie containing the unhealthy assessment as well as the detailed outcome of the health matching procedure. The client software may take appropriate action and try to self-remedy the situation, e.g., by starting the virus scanner. In any case, the user is informed of the current state of their system by an appropriate message. After performing the

requested actions, the client reconnects to the Access Control Service. The Access Control service verifies the health conditions again and changes the client health state to **Healthy** if the client complies with the assigned health policy from now on. Should the client fail to self-remedy the situation or does not reconnect in a reasonable amount of time, its status changes to **Unhealthy** and the quarantine rules are enabled.
A client will never stay in **Probation** state for more than one connect cycle. If the client does not respond within the configurable **Health State Probation Time**, configurable in **Access Control Service Settings > System Health-Validator > General**, the Access Control Service automatically changes the client's health state to **Unhealthy**.

Healthy Health State

Depending on the configuration, the health policy could require an up-to-date Barracuda Personal Firewall installed and enabled, or active antivirus software including up-to-date Virus Scanner patterns. Should all required criteria match, the client is deemed healthy and receives a signed cookie listing the applicable policy attributes. This signed cookie may be further used to authenticate against external trust zones.

Unhealthy Health State

If a client does not comply with the company's health policy, they can perform either manual or automated actions in order to fulfill all health requirements before being put into quarantine. If the client fails during a specific interval, the state is changed to **Unhealthy**, which means that the client is put into quarantine. The latest quarantine ruleset will be activated. On the Barracuda CloudGen Firewall, the proper state is propagated to the firewall engine, where limited access can be enforced.

Health State Requirements

Beside Barracuda Networks-specific information, where health state requirements primarily depend on antivirus or anti-spyware settings, a range of available health state requirements can be specified. Failing a health state requirement might either trigger automatic self-remediation or require a manual action by the user. The desired behavior is configurable because certain antivirus or anti-spyware tools do not fully support auto-remediation. In case of manual action, the user is informed of the required actions via the Barracuda Access Monitor.

The following health state requirements can be specified:

- **Service Settings**
  - Is the installed Barracuda Personal Firewall active?
  - Is the installed Virus Scanner active?
  - Is the installed Spyware Scanner active?
- **Antivirus Settings**
  - Which virus scanner vendors are allowed?
  - Is AV Real Time Protection enabled?
  - When was the last AV scan performed?

    - When was the AV engine updated?
    - When were the AV pattern definitions updated?
- **Anti-spyware Settings**
    - Which spyware scanner vendors are allowed?
    - Is AS Real Time Protection enabled?
    - When was the last AS scan performed?
    - When was the AS engine updated?
    - When were the AS pattern definitions updated?
- **Advanced Health State**
    - Which versions of the health suite are allowed?
- **Miscellaneous**
    - Are specific registry keys set?
    - Which Microsoft hotfixes or service packs are present?

Barracuda Networks provides an online update service helping clients to recognize and activate antivirus and anti-spyware products. Even the quarantine ruleset must at least enable the client to connect to the Access Control Service, to Microsoft Active Directory, and to the remediation servers. The update service provides the information necessary to diagnose whether the client's signature databases and engine versions. are up-to-date As a prerequisite, either the Access Control Service (stand-alone Barracuda CloudGen Firewall) or the Firewall Control Center (for managed units) must have access to the Internet.

For example: A user wants to access a corporate resource and has a virus scanner installed that is not up-to-date. When logging into the network, the user is denied access to the resource and is offered to update the antivirus software. To do so, the user needs access to the Internet. The client state is now **Probation**. Because the Network Access Client continuously checks the client`s health state, after the antivirus software is updated, the policy allows the client not only to access the Internet, but also to the corporate resource. The client state is now **Healthy**. If the client does not manage to update the antivirus software, the status changes to **Unhealthy**.

Depending on the company's infrastructure, more connections should be available to restore the client's health state to **Healthy** again.

Mobile Desktop Connectons

If mobile desktops connect to the corporate LAN through the Internet, the Network Access Monitor communicates through the VPN tunnel with the responsible SHV. In the LAN context, certain policy attributes are assigned together with a **Current User** ruleset. This setup supports a maximum of up to three different firewall rulesets. The **Limited Access** and the **Local Machine** firewall rulesets and policies need to be provided together with the actual **VPN** ruleset.

Policy

VPN Assign-ment	Healthy	Limited Access	VPN Offline
	Firewall Ruleset	Firewall Ruleset	Firewall Ruleset (= **Local Machine** ruleset)
	Message of the Day	Message	
	Welcome Picture		
	Network Access Policies		

The **Local Machine** ruleset acts as a VPN offline ruleset that can be used to centrally control the network access rights of mobile users even when they are not connected to the corporate LAN.

Figures