Configuring Access Control Service Trustzones

https://campus.barracuda.com/doc/48202922/

Each Access Control service is assigned to a trustzone. All Access Control Services within the same trustzone share the same set of security policies and signing key, so that the trust relationship can be established. Each trustzone contains three policy rulesets:

- **Local Machine** – Used to determine a policy for a connecting machine. A connecting machine is an endpoint system that does not request user authentication.
- **Current User** – Used for policy matching when the connecting client requests user authentication.
- **VPN** – Adopted if an intermittent VPN service mediates the connection attempt.

Each policy ruleset contains policy rules that are processed from top to bottom. The policy set in the first matching rule is executed. If none of the rules match, the no-rule-exception policy is applied. The client is then considered to be untrusted. To better control the client-health state, you can also define a catch-all policy rule. This will allow you to receive more information on the client health state and also enable server-side visualization. Each policy rule consists of three parts:

- **Identity Matching** – An identity-related part that defines the applicable matching policy and criteria.
- **Required Health State** – 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. There are only three health states: healthy, unhealthy, and untrusted.
- **Policy Assignments** – Contains firewall rule sets, messages, pictures, and network access policies that are assigned to a healthy client.

Trustzones can be created on a stand-alone NextGen Firewall F-Series or in a global-, range-, or cluster-level configuration in the Control Center.

Create a Policy Rule

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Server > your virtual server > Assigned Services > Access Control Service > Access Control Service Trustzone**.
2. Click **Lock**
3. Click on the **Local Machine**, **VPN**, or **Current User** tab to select the ruleset the policy rule is created in.
4. Right-click in the main area and select **Add**. The **Create Policy Rule** window opens.
5. Configure **Identity Matching**:
    1. Enter a **Policy Name**.
    2. Configure **Basic Identity Matching**:

Client Connection	■ **External** – Effects that this policy rule is ignored for internal connections (connections to an IP address not defined in **Access Control Service Settings > System Health-Validator > External IPs**). ■ **Ignore** – Means that the policy rule is neither ignored for internal nor external connections. ■ **Internal** – Effects that this policy rule is ignored for external connections (connections to an IP address defined in **Access Control Service Settings > System Health-Validator > External IPs**).
Time Restriction	Each policy rule can be assigned with a date and time restriction. The date restriction consists of a **Start Date** and an **End Date**. Outside that time period, this policy rule will be ignored. The granularity of the time restriction is 1 hour on a weekly base. A rule is allowed at all times by default; that is, all check boxes in the **Time Interval** window are cleared. Selecting a check box denies a rule for the given time. Click **the respective icon** to configure allowed and disallowed time intervals simultaneously. Click **the respective icon** to clear selected check boxes. Click **the respective icon** to configure disallowed time intervals. Select **Continue if mismatch** to proceed the health evaluation within the policy ruleset with the next rule (default). Select **Block if mismatch** to stop the health evaluation process and set the client to "unhealthy" immediately.

3. Configure **Basic Matching** settings:

Policy Matching	■ **All-of-following** ■ **One-of-following** Set this to **All-of-following** if all of the identity-matching parameters (basic and advanced), except the empty ones, must match for a successful identity verification. If just one field does not match, the identity is not verified successfully within this policy rule and the health match process will proceed with the next policy rule in the policy ruleset. Set this to **One-of-following** to let the identity verification succeed if just one field matches. Empty fields are ignored. String comparison is case insensitive. For the pattern to match, at least one user group must match at least one defined group pattern.
Group Patterns	At least one user group must match at least one of these patterns for successful identity verification. Ensure that you are using the accurate syntax for the group patterns. For example, MSAD groups must be entered as distinguished name as follows: `CN=group-*, OU=my-unit,CD=mycompany,DC=at`
Net Bios Domain	A NetBIOS domain to match only users belonging to a specific domain. This is only available for the **Current User** and **VPN** rulesets.
User [Login Name]	Username patterns consist of the login name (without leading **DOMAIN**).

Networks	The user's peer address must be part of at least one of these networks.
Allowed OS Versions	■ **Name** ■ **OS Versions** – must be one of the listed Microsoft Windows Versions. ■ **Service Pack Major Number** ■ **Service Pack Minor Number** ■ **Minimum Build Number** – needs to be the OS build number and is checked only if Policy on OS was set to This-One-Or-Newer. ■ **Policy on OS** Possible values for **Policy on OS** are: ■ **Exact-This-One** – The client OS must match **OS Versions**, **Service Pack Major Number**, and **Service Pack Minor Number**. ■ **Explicit-Deny** – If the client OS matches **OS Versions**, **Service Pack Major Number**, and **Service Pack Minor Number**, the current policy rule will be ignored for the current match, and health evaluation processing proceeds with the next policy rule in the policy ruleset. ■ **This-One-Or-Newer** – The client OS must be identically equal to **OS Versions**. The client **Service Pack Major Number** and **Service Pack Minor Number** need to be equal or greater than those defined here.
Hostnames	Enter hostnames here. Patterns may be used.

4. (optional) In the **Identify** section of the left menu, click **Advanced** and configure the following settings:

Advanced Identity Matching	
MAC Addresses	Patterns may be used.
Microsoft Machine SIDs	A SID is a globally unique machine identifier generated by Microsoft operating systems. It is visualized in the Access Control Server's access cache. Patterns may be used.
Certificate Conditions	
x509 Subject	The X.509 subject of the client's authentication certificate must match at least one of these patterns. For example: **CN=name-*, O=my-company**. Certificate authentication is only possible in local machine and basic user authentication.
x509 Issuer	The subject of the issuer of the client's certificate must match at least one of these patterns. For example: **CN=name-*, O=my-company**. Certificate authentication is only possible in local machine and basic user authentication.
x509 Altnames	The subject alternative name of the client's authentication certificate must match at least one of these patterns. For example: **IP:10.0.10.***. Certificate authentication is only possible in local machine and basic user authentication. The subject alternative name must be prefixed with its type (for example, **email:** or **IP:**)

6. Configure **Required Health State** criteria:
   1. (optional) To use the **Legacy Health Check** features, select **Legacy Health Check**. A legacy **SSL VPN and NAC** license is required.
   2. Configure **Service Settings**:

Service Settings	
Personal Firewall On	■ **Required** ■ **Required** ■ **Not Required** (default) Set to **Required** if a client must have the Personal Firewall up and running to be healthy. If the client does not meet this requirement, the user will be advised to turn on the firewall.
Antivirus Scanner On (Legacy Health Check only)	■ **Required** ■ **Required** ■ **Not Required** (default) Set to **Required** if a client must have the Virus Scanner up and running to be healthy. If the client does not meet this requirement, the user will be advised to turn on the Virus Scanner. The **Required** option only takes effect as long as the **Antivirus** check box is activated (see the figure above).
Antispyware Scanner On (Legacy Health Check only)	■ **Required** ■ **Required** ■ **Not Required** (default) Set to **Required** if a client must have the Spyware Scanner up and running to be healthy. If the client does not meet this requirement, the user will be advised to turn on the Spyware Scanner. The **Required** option only takes effect as long as the **Antispyware** check box is activated (see the figure above).
Miscellaneous	
Continue Match	■ **STOP on Health Mismatch** (default) ■ **Continue on Health Mismatch** Set this to **Continue on Health Mismatch** if the health validation should continue with the next policy rule in the policy ruleset in cases where the health evaluation in the current rule returned that the client is **not healthy**. Set this to **STOP on Health Mismatch** if health validation should not continue with the next policy rule in the policy ruleset if the client is **not healthy**. In this case, the policy attributes of the current rule are assigned to the client and the client is advised to heal itself.
Registry Check Rules	Select a registry check object. The client's registry entries must match those of the selected registry check object to be healthy.

   3. In the **Windows Security Center Settings** section select which Windows Security Center states to query:
      - **Network Firewall**
      - **Windows Update**

- **Virus Protection**
- **Spyware Protection**
- **User Account Control**
- **Internet Security Settings**

4. (Legacy Health check only) Configure **Antivir** and **Antispyware** settings:

Antivirus	
AV Real Time Protection	■ **Required** ■ **Required** ■ **Not Required** (default) Set to **Required** if a client must have enabled the real-time protection of the Virus Scanner to be healthy. If the client does not meet this requirement, it will be advised to turn on the real-time protection of the Virus Scanner.
Last AV Scan Not Older Than	■ **Ignore** ■ **6-Hours > 1-Month** ■ **24-Hours** (default) Set to a value other than **Ignore** to ensure that the client's last full virus scan is not older than to be healthy. If the client does not meet this requirement, it will be advised to perform a full virus scan.
Last AV Scan Action	■ **Manual** ■ **Auto Remediation** Depending on this parameter, the user gets informed either to manually perform a full virus scan, or that the client tries to execute a full system scan automatically.
AV Engine Required	■ **Ignore** ■ **Latest** (default) ■ **Previous** ■ **Last-2** Set to **Ignore** if the client's Virus Scanner version should not be checked. Set to **Latest** if the client must not have an older version of the Virus Scanner to return a **healthy** state. Set to **Previous** if the latest and the previous version of the Virus Scanner are accepted to return a **healthy** state. Set to **Last-2** if the latest, the previous, and the second-to-last Virus Scanner versions are accepted to return **a healthy** state. If the client does not meet the chosen requirement, it will be advised to perform a Virus Scanner engine update.

AV Patterns Not Older Than (h)	■ **Ignore** ■ **6-Hours > 1-Month** ■ **24-Hours** (default) Set this to a value other than **Ignore** to require Virus Scanner patterns to be not older than to be healthy. This value will be ignored if the latest Virus Scanner pattern is older than . For example, if this option is set to **6-Hours** but the latest pattern was released 8 hours ago, the client's state will be set to **unhealthy** due to this option. Release cycles of Virus Scanner patterns depend on the Virus Scanner vendor.
AV Engine/Pattern Action	■ **Manual** ■ **Auto Remediation** Depending on this parameter, either the user gets informed to manually update the AV system, or the client tries to trigger AV updates automatically.
Allowed Vendors	Choose one or more out of this list of Virus Scanner vendors in order to enforce a specific Virus Scanner product to be installed on the client. Virus Scanner products not listed here are ignored in the health validation process. This option is helpful especially to exclude certain Virus Scanner products from the health validation process. The list of available Virus Scanner vendors is created dynamically.
Antispyware	
AS Real Time Protection	■ **Required** ■ **Required** ■ **Not Required** (default) Set to **Required** if a client must have enabled the real-time protection of the Spyware Scanner to be healthy. If the client does not meet this requirement, it will be advised to turn on the real-time protection of the Spyware Scanner.
Last AS Scan Action	■ **Manual** ■ **Auto Remediation** Depending on this, the user either gets informed to manually perform a full spyware scan, or the client tries to execute a full system scan automatically.
Last AS Scan Not Older Than	■ **Ignore** ■ **6-Hours > 1-Month** ■ **24-Hours** (default) Set to a value other than **Ignore** to ensure that the client's last full spyware scan is not older than for validly returning the **healthy** state. If the client does not meet this requirement, it will be advised to perform a full spyware scan.

AS Engine Required	■ **Ignore** ■ Latest (default) ■ **Previous** ■ **Last-2** Set to **Ignore** if the client's anti-spyware engine version should not be checked. Set to **Latest** if the client must not have an older version of the Spyware Scanner engine to validly return the **healthy** state. Set to **Previous** if the latest and the previous version of the Spyware Scanner engine can validly return the **healthy** state. Set to **Last-2** if the latest, the previous, and the second-to-last Spyware Scanner engine versions are allowed to validly return the **healthy** state. If the client does not meet the chosen requirement, it will be advised to perform a Spyware Scanner engine update.
AS Pattern Definitions Required	■ **Ignore** ■ **Latest** (default) ■ **Previous** ■ **Last-2** Set to **Ignore** if the client's spyware pattern definitions should not be verified. Be aware that, in this case, the client may be healthy without having any spyware patterns installed. Set to **Latest** if the client's spyware patterns must be up-to-date to validly return the **healthy** state. Set to **Previous** if the client's spyware patterns must either be up-to-date or of the previous version to validly return the **healthy** state. Set to **Last-2** if the client's spyware patterns must either be up-to-date or of the previous or the second-to-last version to validly return the **healthy** state. If the client does not meet the chosen requirement, it will be advised to perform a spyware patterns update.
AS Patterns Not Older Than (h)	■ **Ignore** ■ **6-Hours > 1-Month** ■ **24-Hours** (default) Set this to a value other than Ignore to require spyware patterns to be not older than to validly return the **healthy** state. The setting will be ignored if the latest spyware pattern is older than . For instance, if the value is set to **6-Hours** but the latest spyware pattern was released 8 hours ago, the client's state will be set to **unhealthy** due this setting. Release cycles of spyware patterns depend on the Spyware Scanner product vendor.
AV Engine/Pattern Action	■ **Manual** ■ **Auto Remediation** Depending on this setting, the user either gets informed to manually update the Spyware Scanner, or the client tries to trigger such an update automatically.

Allowed Vendors	Choose one or multiple entries from the list of Spyware Scanner vendors in order to enforce specific Spyware Scanner vendor products to be installed on the client. Spyware Scanner products not listed here are ignored during the health validation process. This setting is helpful especially for excluding certain Spyware Scanner products from the health validation process. The list of available Spyware Scanner vendors is dynamically created.

5. Configure the **Allowed Health Suite** policies:

Allowed Health Suite Versions	
Name	Specify a name.
Major Release	The client's health suite major release version number must match **Major Release**.
Minor Release	The client's health suite minor release version number must match **Minor Release**.
Service Pack Number	The **Service Pack Number** must match the service pack number of the client's health suite.
Policy on OS	■ **Exact-This-On** – The client's health suite version must match all three number values. ■ **Explicit-Deny** – If the client's health suite version matches all three number values, the health state will be set to a value different than **healthy** and the clients will be advised to update the health suite. ■ **This-One-Or-Newer** – The client's health suite major version must equal **Major Version**. The minor release version number and the service pack number need to be equal or greater than those defined here.

6. In the the **Required Security Updates** section, click **+** to add IDs for the required Microsoft hotfixes in **KB123456** format

7. Configure **Policy Assignments**:
   1. Configure the **Policy Assignment Attributes**:

Policy Assignment Attributes	
Personal Firewall Settings	■ **Ruleset Name** – Select one of the created **Personal Firewall Rule** objects. If the client does not already have this ruleset installed, the health state will be set to a value other than **healthy** and the client will be advised to update the personal firewall ruleset from the remediation server.
Message of the Day	Select one of the created **Welcome Message** objects. If the client does not already have this message, it will be advised to get the message from the remediation server.

Limit Access	■ **Ruleset Name** ■ **Message** ■ **Client Emerg. Quarantine Time (s)** Configure the quarantine ruleset. Assignment of **Limited Access** rulesets and messages is only available for the **Local Machine** ruleset. The quarantine ruleset (**Limited Access**) is stored on the local machine. This means that the quarantine ruleset can only be updated if the current user logs off or the client is rebooted. If a client changes its state to **unhealthy,** the local machine quarantine ruleset is activated.

2. (optional) Configure **Policy Assignment Exceptions**:

Exceptions	
Software Update Required	■ **Yes** ■ **No** (default) ■ **Yes-Even-Major** Change this to **Yes** for the client to automatically perform software updates if a new software minor version is available on the CC. **Yes-Even-Major** will cause the client to also perform major version updates.
User Authentication Required	■ **Yes** ■ **No** ■ **Like Service Settings** (default) Only available for the local machine ruleset. If this is set to **No**, user authentication is not performed even if a user logs in.

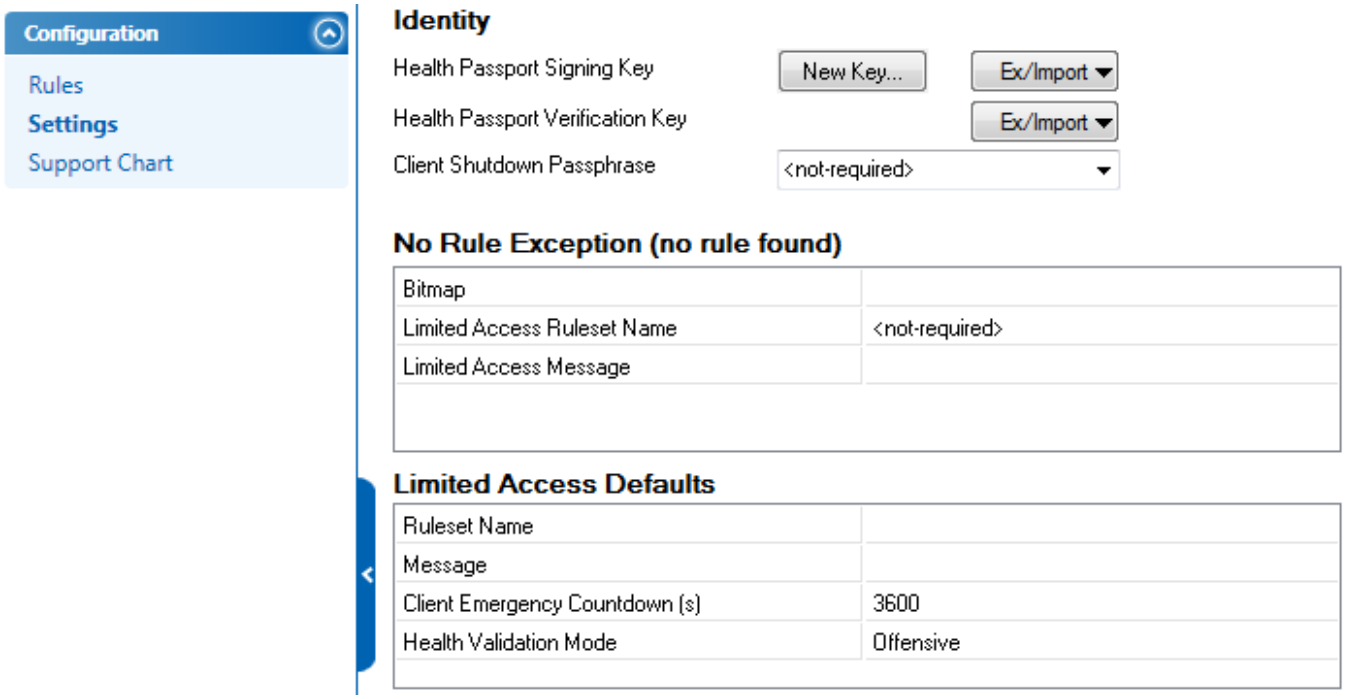
3. (optional) Configure **Policy Assignment Radius Attributes:**

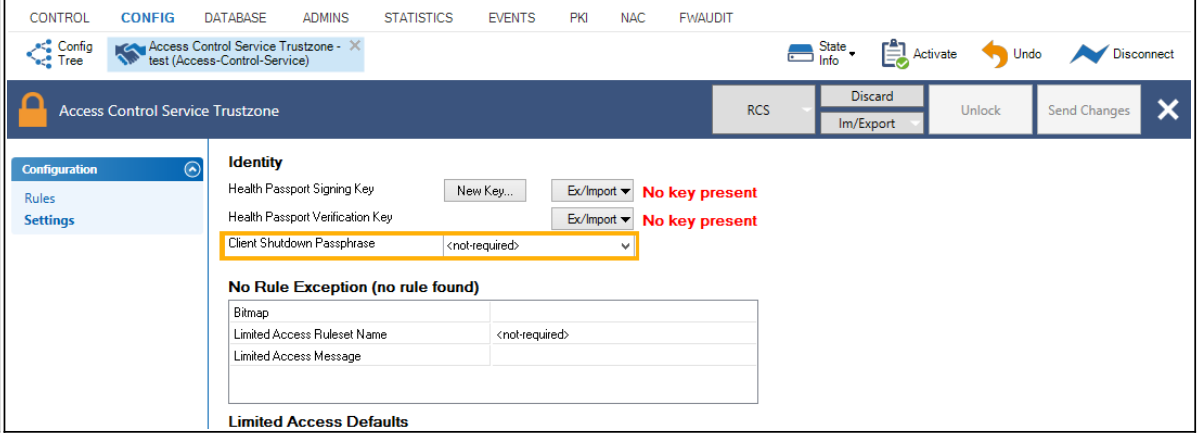
Radius Attributes	
Healthy Attribute Assignments	RADIUS attribute assignments passed to a RADIUS server as key-and-value pairs if the client meets the health requirements.
Unhealthy Attribute Assignments	RADIUS attribute assignments passed to a RADIUS server as key-and-value pairs if the client does not meet the health requirements.

8. Click **OK**.
9. Click **Send Changes** and **Activate**.

Settings

If no policy rule matched the identity for a client, or at least one matched but the **Continue Match** parameter was set on that/those policy rule(s), the client's state will be **untrusted** and it will be assigned the **No Rule Exception** attributes.



Identity	
Health Passport Signing Key	The RSA key for digital passport signing. The Health Validator returns a digital passport to the client as result of the health validation. The passport contains all information required for the remediation server. To ensure authenticity, the passport is digitally signed. Since all Access Control services of the same trustzone share the same credentials, the remediation server instances can verify whether a passport was issued by a health validator of the same trustzone.
Health Passport Verification Key	The RSA public key for verifying a digital passport signature. If one Access Control Server instance acts exclusively as a remediation server, it is not necessary to set the **Health Passport Signing Key.** However, the **Health Passport Verification Key** must be set.
Client Shutdown Passphrase	If a passphrase is set here, the Access Control service will lock the **Advanced Settings** locally on the clients unless the local user enters the correct passphrase. In addition, the client can only be terminated on the workstation after the passphrase has been entered. The default setting disables these restrictions and enables the local user to administer and terminate the client. 

Access Control Service Trustzone > Settings > No Rule Exception

Bitmap	Select one of the **Picture** objects. The client will then be advised to get the respective bitmap from the remediation server.
Limited Access Ruleset Name	For more information on these two parameters, see Limit Access.
Limited Access Message	
Access Control Service Trustzone > Settings > Limited Access Defaults	
Client Emergency Quarantine Time (s)	If the Access Control Server is not reachable anymore for the client, it switches automatically to the **Unhealthy r**estricted state. Entering a value of **0** disables this. For more information, see Limit Access. If no Access Control Server IP address is available, this parameter does not have any effect. For more information, see How to Configure the Barracuda Access Monitor, **Access Control Server IPs from Registry** and **Access Control Server IPs from DHCP** sections.
Quarantine Ruleset Name	Select one of the **Personal Firewall Rules** objects. The client will be advised to get the respective bitmap from the remediation server.
Quarantine Message	Select one of the **Welcome Messages** objects. The client will be advised to get the respective bitmap from the remediation server.
Health Validation Mode	• **Moderate** Health checks are executed after connection establishment. • **Offensive** Health checks are executed during connection establishment.

The **Health Validation Mode** parameter can also be configured on the client via the following registry key:

Path	`.DEFAULT\Software\Phion\phionha\settings\`
Key	SpeedVPNValidation
Value	• Moderate • Offensive

The **Client Emergency Quarantine Time (s)** parameter can also be configured on the client using the following registry key:

Path	`.DEFAULT\Software\Phion\phionha\settings\`
Key	QuarantineCountDown
Value	[Default: **3600000** (= 1 hour in milliseconds)]

Access Control Service Trustzone > Settings > Radius Attribute Assignments	
With this feature, it is possible to send additional attributes to the switch, depending on the health state of the client. **VLAN Change** attributes are already hardcoded.	
Healthy	For a description of these two parameters, see the radatt.
Unhealthy	

Support Chart

This view provides information concerning the supported Virus Scanner and Spyware Scanner vendors and versions.

The **Support Chart** is automatically downloaded from the Barracuda Networks update service mentioned above and distributed to Barracuda NextGen Admin upon connection. Thus, the **Support Chart** reflects the current capabilities of the Access Control service.

The following restrictions apply to Microsoft Windows 7 64-bit:

- Enabling and disabling of Virus and Spyware Scanner functionality cannot be done automatically for some vendors (see support charts).
- Auto-remediation for Virus Scanner and Spyware Scanner engine and pattern updates is disabled in the 64-bit client.

Figures

1. image2012-11-13 15-29-15.png
2. ac2.png