Client-to-Site Group Policy Settings

https://campus.barracuda.com/doc/73719157/

The following sections provide additional details on the client-to-site VPN server parameter settings.

Group Policy Tab

The **VPN Group Policy** specifies the network IPsec settings. You can group patterns to require users to meet certain criteria, as provided by the group membership of the external authentication server (e.g., CN=vpnusers*). You can also define conditions to be met by the certificate (e.g., **O(Organization)**) must be the company name).

Setting	Description
Mandatory Client Credentials	Select the credentials required for client authentication: • **X.509 Certificate** – Client certificate authentication mandatory. • **External Authentication** – User password authentication mandatory. • **IPsec needs Xauth** – Select to allow only IPsec clients that support Xauth. Select **Login must match AltName in Certificate** if certificate lookup is done by Alternative Name.
Authentication Scheme	Select an authentication scheme from the list to be used by all client-to-site VPN connections.
Default Authentication Scheme	The default or fallback authentication scheme used to authenticate VPN clients. Select the **Ras Login permission required checkbox** if Remote Access login is required. As soon as **RAS Log permission required** is activated, only a MSAD user with this option can connect. Users in other authentication databases, for example, LDAP, do not have this option as default and will not be able to connect. As a workaround, the user can be assigned a Boolean attribute with the name msNPAllowDialin in the directory. The VPN server itself does not distinguish between directories when querying.
Server	(Optional) Select the server certificate used by the VPN server to authenticate to the VPN client, or use the default server certificate configured in the VPN settings.
Server Protocol Key	Select your X.509 server certificate.
Used Root Certificate	(Optional) Select the root certificate used to validate client certificates.
X509 Login Extraction Field	Extract the username from the selected client certificate field. The X.509 Login Extraction Field is only used for pre-authentication.
IP Attribute Name	Set the VPN client IP address to the attribute configured in the LDAP, MSAD, or RADIUS server.

VPN Group Policy Name Attribute	Name of the attribute field on the authentication server that contains group information. The VPN group policy is pinned to the value returned by the LDAP, MSAD, or RADIUS server.
Preauthentication Scheme	Attributes from LDAP / MSAD / RADIUS or TACPLUS authentication schemes are used to determine the default authentication scheme for the user. As soon as only a username is used, the configured default authentication scheme will be used. The username must also exist in LDAP (or the corresponding authentication scheme) or the option **Alternative Login Name Field** must be used. • **Authentication Selector Field** – Enter the attribute name (e.g., `memberof` for group memberships in MSAD/LDAP etc.) where the authentication scheme for the user is stored. Example: ngflocal, msad, etc. ◦ **Value Pattern/Scheme Name** – Right-click and select **New name to Scheme Mapping**. Then, enter LDAP `Pattern=AuthScheme` (for example: `HQ=msad2,` if MSAD was chosen as additional authentication scheme) and click **OK**. A user is checked for an existing attribute, e.g., output of group membership information (memberof). If **vpnallow** is configured in the transmitted USER group membership field, MSAD2 is used. The Value pattern field also accepts special characters: '-', '_', ',' (comma), '=', ' ' (space). • **(optional) Alternative Login Name Field** – Enter the attribute name where an alternative username can be stored if an additional username should be used for a user with the same password. • **IP Address Field** – IP attribute name without pre-authentication: Enter the attribute name where the IP address for the VPN client is stored. The field must exist in LDAP/MSAD and return the desired IP address as value. A combination consisting of fixed and dynamic IP addresses in the same VPN Client is not recommended. In this case, consider using two VPN Client networks instead. To avoid IP collisions, you could also generate Barracuda VPN Lic File entries. This would exclude IP addresses from being assigned dynamically. • **VPN Group Field** – Enter the attribute name where the VPN group policy name is stored. The VPN group policy name attribute lets you assign a VPN group policy directly to the client, without a pre-authentication scheme. Example: If the LDAP field `NGVPNGROUPPOLICY` for a user contains `iOS`, the user gets the corresponding group policy assigned. • **Group Information** – Select the source of the user group information. ◦ **From Preauthentication** – Use group information from the pre-authentication scheme. ◦ **From Authentication** – Use group information from the default authentication scheme.

Group Policy Settings

Common Settings

Setting	Description
Name	Enter a name for the policy. For example, `Group Policy`. • The **Common Settings** field is automatically updated with this name, and the check box is automatically selected as soon as you fill in the details. • This name is also used on native VPN clients on iOS and Android
Statistic Name	Enter a name to better allocate statistics entries.
Network	Select the VPN client network the group policy applies to.
DNS	Enter the IP address of the DNS server used for the clients.
WINS	If applicable, enter the IP address of the WINS server.
Network Routes	Add all networks that should be reachable by the VPN clients. Enter `0.0.0.0/0` for all traffic to be sent through the client-to-site VPN.
Access Control List (ACL)	Add an Access Control List.
Group Policy Condition	Right-click the **Group Policy Condition** field and select **Create New Policy**.

Group Policy Condition

Right-click the **Group Policy Condition** field and select **New Rule**. In the **X509 Certificate Conditions** section of the **Group Policy Condition** window, set filters for the certificate. For each certificate condition, select the certificate field from the drop-down list, enter the required value, and click **Add/Change**.

Setting	Description
External Group	Define the groups on the authentication server that will be assigned the policy. E.g., `CN=vpnusers*` or * for everybody
Client	Enter the IP address of the client network.
X509 Subject	To let everyone with a valid certificate log on, click **Edit/Show** and add the following condition to the Subject field: `CN=*`. Certificate condition entries are case insensitive and can contain the quantification patterns ? (zero or one) and * (zero or more).
Cert Policy / OID	(Optional) Enter an OID to allow only certificates with a specific key usage. E.g., Client Authentication (1.3.6.1.5.5.7.3.2)
Peer	Enter the IP address of the peer network.

Barracuda Tab - Barracuda Settings

Setting	Description
Enforce Windows Security Settings	Enforce Windows security features for Network Access Clients to allow VPN connections. • **Network Firewall** – A personal firewall must be enabled. • **Windows Update** – MS Windows Automatic Update must be enabled. • **User Account Control** – User Account Control must be enabled. • **Virus Protection** – An antivirus product must be enabled. • **Spyware Protection** – An anti-spyware product must be enabled. • **Internet Security Settings** – Internet Security Settings must be enabled.
VPN Client Network	Configure additional settings for the VPN client network. • **DNS Suffix for VPN** – Appends a specific DNS suffix. • **ENA** – Active ENA (Exclusive Network Access) prevents access to networks the client is not directly connected to. • **Always On** – If disabled, users cannot disconnect manually from the VPN.
Firewall Rules	Additional client firewall settings and assignment of online/offline firewall rules. • **VPN Client NAC** – You can use online/offline firewall rules or SSL VPN, if available. Required to allow only clients with enabled and functional NAC feature. For more information, see Barracuda Network Access and VPN Client . • **VPN** – Assigns an online ruleset configured in the **VPN FW** tab. • **Offline** – Assigns an offline ruleset configured in the **Offline FW** tab. • **Firewall Always On** – The Network Access Client's firewall needs to be enabled for successful VPN connections.
Login Message	Welcome messages can be used to display customized messages to welcome users to the corporate network, inform them about security policies, or display administrator contact details. • **Message** – Create a custom welcome message in the **Message** tab of the **Client-to-Site** page, and then select the message in this section. • **Bitmap** – Upload a 150x80 pixel, 256 color BMP bitmap in the **Pictures** tab of the **Client-to-Site** page, and then select the custom bitmap in this section.

Ciphers	The encryption algorithms that the VPN server will offer. You can select one of the following options: • **AES | AES256** – The Advanced Encryption Standard (default). AES works with 128-bit key length, and AES256 works with 256-bit key length. With AES 256, the security of the encrypted data is increased, but more CPU capacity is required. Only use AES256 when required. Represents a very good compromise between key length and encryption speed. AES encryption speed can also be improved with hardware acceleration. (Recommended.) • **CAST** – Algorithm similar to DES with a key length of 128-bit. • **Blowfish** – Works with a variable key length up to 128-bit. • **DES** – Digital Encryption Standard. Because DES is only capable of a 56-bit key length, it cannot be considered safe any longer. (Not recommended.) • **3DES** – Further development of DES encryption. Three keys each having a 56-bit length are used sequentially, providing a key length of 168-bit. (Not recommended.) Try to avoid using 3DES because this algorithm works very slowly and only offers acceptable performance with the help of special hardware acceleration cards. • **Null** – No encryption.
Advanced	• **Registry** – Checks the VPN client for MS Windows registry keys configured in the **Registry** tab. If the configured key and value match, an implicit 'allow' is assumed. In case of a mismatch, the action 'warning' or 'termination' will be executed. • **Key Time Limit** – The period of time after which the re-keying process is started. • **Key Traffic Limit** – The keys of the VPN tunnel are renewed after this amount of traffic. • **Tunnel Probing** – The interval between tunnel probes. If probes are not answered in the time period specified by the Tunnel Timeout setting, the tunnel is terminated. You can select Silent (no probes are sent), 1 sec, 10 secs, 20 secs, 30 secs (default), or 60 secs. • **Tunnel Timeout** – The length of time in seconds in which tunnel probes must be correctly answered before the tunnel is terminated. If, for some reason, the enveloping connection breaks down, the tunnel must be re-initialized. This is extremely important in setups with redundant possibilities to build the enveloping connection.

IPsec IKEv1 Tab - IPsec IKE1 Phase II Settings

Setting	Description
Disable	Clear the check box, and then select **Group Policy Name (Create New)**.
Edit Phase 1	Click to edit the **Phase 1** settings.
Encryption	The data encryption algorithm.
Hash Meth	The hash algorithm.
DH-Group	The Diffie-Hellman Group that specifies the type of key exchange. DH Group1 to Group18 are supported.
Time	The re-keying time in seconds that the server offers to the partner.

Minimum	The minimum re-keying time in seconds that the server accepts from its partner.
Maximum	The maximum re-keying time in seconds that the server accepts from its partner.

IPsec IKEv2 Tab - IPsec IKE1 Phase I Settings

Configure the same settings for IPsec Phase I that you selected for IPsec Phase II.

Rules Tab

The **Rules** tab lets you edit the group VPN settings. For parameters, see the **Group Policy Tab** section above. To create a rule, right-click in the window and select **New Rule**.

Setting	Description
Assigned VPN Group	Select the VPN group the rule should apply to.
Group Pattern	Enter the group pattern, or click **Lookup** to perform an AD lookup and search for the group pattern.
Subject	Click **Edit/Show** to open the **Certificate Condition** window. Configuration may contain patterns (*,?). Equal keys are slash delimited: To match for DC=foo, DC=bar, you have to enter DC=bar/foo. The order of the distinguished name parts is reversed.
Certificate Policy	Enter the certificate policy (OID 2.5.29.32). It will be checked if the transmitted certificate contains the certificate policies extension (OID 2.5.29.32) and if one of the contained values matches the configuration. For more information, see http://oid-info.com/get/2.5.29.32.
Generic v3 OID / Content	Enter an OID to allow only certificates with a specific key usage. E.g., Client Authentication (1.3.6.1.5.5.7.3.2). You can enter an OID of an arbitrary X.509 v3 extension that will then be searched in the extensions of the transmitted certificate and checked against the value configured in the **Content** field. V_ASN1_IA5STRING and V_ASN1_OCTET_STRING entries can be entered as value, entries of another type will be configured as hexadecimal DER-encoded chain: e.g., for presence of the attribute `clientAuth` in the **Extended Key Usage** extension, the OID 2.5.29.37 with the value 300A06082B06010505070302 must be searched.
Peer Condition	Select the check boxes for the client types used by the peer. • **Barracuda Client** – Barracuda VPN Client or Barracuda Network Access Client including CudaLaunch for Android and iOS. • **IPsec Client** – IPsec clients such as the native Windows, Android, or iOS IPsec VPN clients. • **Transparent Agent (SSL-VPN)** – The legacy SSL VPN transparent VPN client.

Peer Address/Network	Click **Add** to add the IP address of the peer network.

Common Tab

See **Common Settings** section above.

Barracuda Tab

Setting	Description
Name	Enter a name for the Barracuda Client connection.
Enable VPN Client NAC	Enables the Barracuda Network Access Client. For more information, see Barracuda Network Access and VPN Client.
ENA	Active ENA (Exclusive Network Access) prevents access to networks the client is not directly connected to. Select **Split Tunnel On...**
VPN Rules	Assigns an online ruleset configured in the **VPN FW** tab.
Offline Rules	Assigns an offline ruleset configured in the **Offline FW** tab.
Message	Welcome messages can be used to display customized messages to welcome users to the corporate network, inform them about security policies, or display administrator contact details. Create a custom welcome message in the **Message** tab of the **Client to Site** page, and then select the message in this section.
Bitmap	Upload a 150x80 pixel, 256 color BMP bitmap in the **Pictures** tab of the **Client-to-Site** page, and then select the custom bitmap in this section.
Firewall Always ON	The Network Access Client's firewall needs to be enabled for successful VPN connections.
VPN Always ON	If disabled, users cannot disconnect manually from the VPN.
Key Time Limit	The period of time after which the re-keying process is started.
Key Traffic Limit	The keys of the VPN tunnel are renewed after this amount of traffic.
Tunnel Probing	The interval between tunnel probes. If probes are not answered in the time period specified by the **Tunnel Timeout** setting, the tunnel is terminated.
Tunnel Timeout	The length of time in which tunnel probes must be correctly answered before the tunnel is terminated. If, for some reason, the enveloping connection breaks down, the tunnel must be re-initialized. This is extremely important in setups with redundant possibilities to build the enveloping connection.
Accepted Ciphers	The ciphers that can be used to establish the connection.

Enforce Windows Security Settings	Enforce Windows security features: • **Network Firewall** – A personal firewall must be enabled. • **Windows Update** – MS Windows Automatic Update must be enabled. • **User Account Control** – User Account Control must be enabled. • **Virus Protection** – An antivirus product must be enabled. • **Spyware Protection** – An anti-spyware product must be enabled. • **Internet Security Settings** – Internet Security Settings must be enabled.

IPsec Tab

See **IPsec IKEv1 Tab - IPsec IKE1 Phase II Settings** section above.