Authentication, Encryption, and Transport

https://campus.barracuda.com/doc/41116174/

VPN clients must authenticate themselves to the VPN server. A valid certificate is required for the client to verify the identity of the VPN server. To meet the security needs of your network, you can define username/password authentication and strict certificate requirements.

The Barracuda NG Firewall supports multiple encryption algorithms for VPN connections. For TINA VPNs, multiple transport types are also available.

In this article:

VPN Authentication Certificates

X.509 certificates are used by IPsec, L2TP/IPsec, and TINA (the Barracuda proprietary transport protocol). The certificates contain the following information:

- Public key.
- Some data signed by the private key for verification.
- Identity of the the CA.
- Identity of the owner.
- Key usage. Depending on what type of VPN and which clients you use, certain X.509 extensions might be required when creating the certificate.

For PPTP VPNs, external certificates are not needed because certificates are generated by the server at runtime.

Special settings might be required when creating the following types of certificates:

- L2TP/IPsec VPN service certificates. For more information, see How to Configure a Client-to-Site L2TP/IPsec VPN.
- Certificates for iOS devices used as a VPN client. For more information, see How to Configure Apple iOS Devices for Client-to-Site VPN Connections.

Certificate CA (PKI) Options

With the Barracuda NG Control Center (C610,VC610, or VC820), the Barracuda Trust Center, a full-featured public key infrastructure (PKI) for self-signed certificates, is included.

For Barracuda NG Firewalls that are standalone or managed with a Barracuda NG Control Center C400 or VC400, use an external CA (PKI).

Depending on the certificate, you must export it in one of the following formats after it is created and signed:

Certificate	File Format
Root Certificate	PEM or CER
Server Certificate	PKCS12, CER, or CRT
Service Certificate/Key	PEM
Client Certificate (if needed)	PEM

Example Certificates for IPsec, L2TP, and iOS Clients

If you encounter any problems with your certificates, compare your settings to those of the example certificates. Especially verify the **X509 Basic Constraints** and **X509v3 Key Usage** settings.

Root Certificate

Tab	Setting	Value
Status	**Signature Algorithm**	sha1WithRSAEncryption
Subject	**RFC 2253**	emailAddress=support@barracuda.com,OU=documentation,O=Barracuda Networks,L=Innsbruck,ST=Tirol,C=AT
	Hash	7b6d2374
Extensions	**X509v3 Basic Constraints**	CA:TRUE
	X509v3 Key Usage	Digital Signature, Key Agreement, Certificate Sign

Server Certificate

Tab	Setting	Value

Status	**Signature Algorithm**	sha1WithRSAEncryption
Subject	**RFC 2253**	emailAddress=support@barracuda.com,OU=docu,O=Barracuda Network AG,L=Innsbruck,ST=Tyrol,C=AT
	Hash	cc0460b5
Issuer	**RFC 2253**	emailAddress=support@barracuda.com,OU=documentation,O=Barracuda Networks,L=Innsbruck,ST=Tirol,C=AT
	Hash	7b6d2374
Extensions	**X509v3 Key Usage**	Digital Signature, Key Agreement, Certificate Sign
	X509v3 Subject Alternative Name	DNS:vpnserver.yourdomain.com

Client Certificate

Tab	Setting	Values
Status	**Signature Algorithm**	sha1WithRSAEncryption
Subject	**RFC 2253**	emailAddress=support@barracuda.com,OU=documentation,O=Barracuda Networks,L=Innsbruck,ST=Tyrol,C=AT
	Hash	c2b06d20
Issuer	**RFC 2253**	emailAddress=support@barracuda.com,OU=documentation,O=Barracuda Networks,L=Innsbruck,ST=Tirol,C=AT
	Hash	7b6d2374
Extensions	**X509v3 Key Usage**	Digital Signature

Supported Encryption Algorithms

The Barracuda NG Firewall supports the following encryption algorithms for TINA, IPsec, and L2TP/IPsec VPN connections:

Algorithm	Description
AES256	Advanced Encryption Standard with 256-bit encryption.
AES	Advanced Encryption Standard with 128-bit encryption. AES is often chosen because it provides a good performance and security ratio.

3DES	Triple DES. This algorithm is considered most secure but results in high system loads and lower VPN performance.
Blowfish	A keyed, symmetric block cipher developed to replace DES.
CAST	A 128-bit block cipher created by Carlisle Adams and Stafford Tavares.
DES	Digital Encryption Standard. DES is the only export restricted algorithm available. DES is not recommended because it is considered unsafe.
NULL	No encryption.

TINA Transport Protocols

For TINA VPNs, the following transport types are available:

Transport Protocol	Description
UDP	Stateless protocol that is best used for response-optimized tunnels. UDP is not recommended for unstable internet connections.
TCP	Stateful protocol that is used if the tunnel runs over a proxy server. Higher protocol overhead limits the response time. TCP is preferred for unstable Internet connections.
UDP & TCP	Hybrid mode that creates two transport tunnels. To compensate for the weakness of both protocols, UDP is used for TCP connections and TCP is used for stateless connections.
ESP	The tunnel uses ESP (IP protocol 50). ESP is best for performance-optimized tunnels, but it does not work if NAT routers must be traversed.