

Base de Conhecimento > Products > HiSecOS > VPN with LANCOM Advanced VPN Client

VPN with LANCOM Advanced VPN Client

- 2024-07-31 - HiSecOS

This lesson describes how to configure a VPN using Hirschmann EAGLE20/30 and the LANCOM Advanced VPN Client using x.509 certificates.

Software versions used: EAGLE20/30 firmware v02.0.01 Lancom Advanced VPN Client v3.00 Build 21499

Network plan



Install and start LANCOM Advanced VPN Client



The LANCOM Client with a 30 day evaluation period can be downloaded from

http://www.lancom-systems.de

After installation start the LANCOM VPN Client.

Import Certificates

Organize • Include in library •	Sh	are with		(81	• 01
	*	Name	Date modified	Туре	Size
Desktop	-	Cacert.pem	14.04.2015 15:38	PEM File	2
Libraries	1	pnclient-cert.p12	14.04.2015 15:47	Personal Information Exchange	4

Copy the PEM export of the CA (in our example **cacert.pem**) and the PKCS#12 export of the LANCOM Client certificate (in our example **vpnclient-cert.p12**) in the CaCerts directory:

C:\Program Files (x86)\LANCOM\Advanced VPN Client\CaCerts

Note: The file extension of the CA export must be **.pem** otherwise the LANCOM Client will not find the CA.

CA Certificates



To verify if the LANCOM Client could load the CA, select **Connection** -> **Certificates** -> **Display CA Certificates** from the menu.

The distinguished name of the CA should be displayed, marked with a green checkmark. Click **Close**.

Certificates Configuration



Select **Configuration -> Certificates** from the menu.

Certificate Selection

	Connection Conf	liguration View Help
	Connection Profile	Connection:
utificates		X shed
Certificate configuration	and the second sec	
Centineate configuration		
Name	User Certificat	LANCOM
Standard certificate configuratio	in PKC3#12 IIIe	
		0.500
	Cartificator	
	Certificates	
		and the second se
	Name: Standard certific	cate configuration
	Name: Standard certific	cate configuration
	Name: Standard certific User Certificate PIN Policy	cate configuration
	Name: Standard certific User Certificate PIN Policy Certificate:	cate configuration y Certificate Renewal from PKCS#12 file
Add Edit	Name: Standard certific User Certificate PIN Policy Certificate: Select Certificate:	cate configuration y Certificate Renewal from PKCS#12 file 1
Add	Name: Standard certific User Certificate PIN Policy Certificate: Seject Certificate:	cate configuration y Certificate Renewal from PKCS#12 file 1
Add	Name: Standard certific User Certificate PIN Policy Certificate: Select Certificate: PKCS#12 <u>F</u> ilename:	cate configuration y Certificate Renewal from PKCS#12 file 1 C:\Program Files (x86)\LANCOM\Advance
Add Edit	Name: Standard certific User Certificate PIN Policy Certificate: Select Certificate: PKCS=12 <u>F</u> ilename: Enable Certifica	cate configuration y Certificate Renewal from PKCS#12 file 1 C:\Program Files (x86)\LANCOM\Advance ste Selection
Add	Name: Standard certific User Certificate PIN Policy Certificate: Select Certificate: PKCS#12 <u>Fi</u> lename: Enable Certifica C <u>g</u> rtificate Path:	cate configuration y Certificate Renewal from PKCS#12 file 1 C:\Program Files (x86)\LANCOM\Advance ate Selection
Add	Name: Standard certific User Certificate PIN Policy Certificate: Select Certificate: PKCS#12 <u>Filename</u> : Enable Certifica C <u>g</u> rtificate Path:	cate configuration y Certificate Renewal from PKCS#12 file 1 C:\Program Files (x86)\LANCOM\Advance ate Selection
Add	Name: Standard certific User Certificate PIN Policy Certificate: Seject Certificate: PKCS#12 Eilename: Enable Certifica Cgrtificate Path:	cate configuration y Certificate Renewal from PKCS#12 file 1 C:\Program Files (x86)\LANCOM\Advance ate Selection Connection
Add	Name: Standard certific User Certificate PIN Policy Certificate: Select Certificate: PKCS#12 Eilename: Enable Certifica Cgrtificate Path: PiN Request at each	cate configuration y Certificate Renewal from PKCS#12 file 1 C:\Program Files (x86)\LANCOM\Advance ate Selection Connection

Highlight the Standard certificate configuration and click Edit.

Set the **PKCS#12 Filename** in our example C:\Program Files (x86)\LANCOM\Advanced VPN Client\CaCerts\vpnclient-cert.p12.

Click OK.

Close the **Certificates** configuration window.

Creating a new profile



- 1. Select from the menu **Configuration** -> **Profiles**
- 2. Click Add / Import to create a new profile
- 3. Select Link to Corporate Network Using IPsec
- 4. Click Next

Profile Name

ew Profile Wizard	×
Profile Name Enter the profile name of the connection	LANCOM Systems
The connection may be given a descriptive name, up characters long. Enter the name in the following fit	p to 39 alphanumeric Eld.
EAGLE30_x509	
	Rade Markan
<	gate Next > Cancel

Enter a **Profile Name** Click **Next**

Communication Medium

w Profile Wizard	
Communication Medium Select the media type of the connect	tion.
Determine how the connection to t internet is to be used via modem, so select the appropriate modem.	he corporate network should be established. If the at the communication media to "modem" and then
Communication Media:	LAN (over IP)
	e Back Next > Cancel

Select LAN (over IP) as communication media Click Next

VPN Gateway Parameters

New Profil	e Wizard	— ×—
VPN G To whi establi	ateway Parameters ch VPN gateway should the connect shed?	tion be
Enter t 212.10 Using auther establi	he DNS name (i.e. vpnserver.domain 17.29) of the VPN gateway you wan Extended Authentication (XAUTH) yo trication. If no authentication data a shing the connection. <u>G</u> ateway (Tunnel Endpoint):	.com) or the official IP address (i.e. t to connect to. iu can enter the user ID and password for the are entered they will be requested when
	55.1.2.2 Extended Authentication @AU	TH)
	User ID:	
	Password:	Password (con <u>f</u> irm):
		< Back Next > Cancel

Enter the **Gateway** to which the connection should be established. Could be an IP address or DynDNS name.

IPsec Configuration

w Protil	e Wizard	
IPsec (Config	Configuration ure the basic IPsec parameters	
The bar "autom In the o defined	sic IPsec parameters can be specified here. The satic mode" which are pre-defined (default) pro event that uniquely defined IKE- / IPsec policie d and assigned using the policy editor under I Exchange Mode: main mode (IKEv1)	Provide the second seco
	PFS Group:	
	DH-Group 2 (1024 Bit)	•
	IPsec Compression IPsec over HTTPS* (LANCOM VPN router with operating syst	tem LCOS 8.0 or higher required)
	based on receiver you rath rinder technoic	ogy.

Set the Exchange Mode to main mode (IKEv1) Set PFS Group to DH-Group 2 (1024 Bit) Click Next

Local Identity (IKE)

lew Profil	e Wizard		×
Pre-sh Commo	ared Key on Secret fo	r Authentication	LANCOM Systems
A share be ider Enter t	ed secret or ntically conf he appropri Pre-share Shared Se	pre-shared key is use igured on both sides ate value for the IKE I d Key coret:	d to encrypt the connection. This then needs to (VPN client and VPN gateway). D according to the selected ID type. Confirm Secret:
	Local Iden	ntity (IKE)	
0	Type:	ASN1 Distinguis	hed Name 🔹
	ID:	/C=DE/ST=BW/O	=Hirschmann/OU=L3-Support/CN=VPNCLIENT
			< Back Next > Cancel

Delete the pre-shared keys

Set the Type to **ASN1 Distinguished Name**

Using the test certificates, copy the DN /C=DE/ST=BW/O=Hirschmann/OU=L3-

Support/CN=VPNCLIENT in the ID field

Click Next

IPsec Configuration - IP Addresses

w Profi	e Wizard	
IPsec Assign	Configuration - IP Addresses ing the IP address to the client	LANCOM Systems
Specify the clic Furthe	which IP address the client is g ent's IP address is dynamically as rmore, define where the DNS / \ IP Address <u>A</u> ssignment	oing to use. By selecting "Use IKE Config Mode" signed by the VPN gateway. VINS servers (if used) can be found.
ADK	Manual IP Address	•
	IP Address:	
	172-16-106-201	
e	DNS / WINS Servers	
U	DNS Server:	WINS Server:
	0.0.0.0	0.0.0.0

Set the IP Address Assignment to Manual IP Address.

IPsec Configuration - Split Tunneling

Enter the remote			
will always be use	IP networks the ed.	tunnel should be used for. W	Vithout entries tunneling
Remote	e Networks	Remote IP Net Masks	1 Add Edit
IP N	letwork		Delete
2	[P Network: 10.2.0.0	<u>N</u> et Mask: - 255.255.255.0	
		OK Canc	e

Define the remote IP network to be reached through the IPsec tunnel. In our example 10.2.0.0/24. Click Finish.

Profile Window

how all profiles		-	Group
Profile Name 🔺	Communication	Medium Default	
AGLE30_X509	LAN		

The new profile is created and displayed in the **Profile** window Highlight the profile and click **Edit.**

Profile Settings

Basic Settings Line Management IPrec General Settings Advanced IPsec Options Identities	IPsec General Settings <u>Gateway</u> (Tunnel El 55.1.2.2	ndpoint):	
IPsec Address Assignment Spiti Tunneling Certificate Check Link Firewall	Policies Exch. Mode: [KE Policy: IKE <u>D</u> H Group: IP <u>s</u> ec Policy: <u>P</u> FS Group:	main mode (IKEv1) automatic mode DH-Group 2 (1024 Bit) automatic mode DH-Group 2 (1024 Bit) Policy Lifetimes Polic	v v v v ty <u>E</u> ditor
		Help OK	<u>C</u> ancel

Highlight IPsec General Settings in the left pane.

Click Policy Editor

IKE Policy Settings

IPsec Configuration	
Add Edit	Copy Delete

Highlight **RSA Signature** in the IKE Policy

Click **Edit**

Authentication	Encryption	Hash	
RSA-Signature	AES 128 Bit	SHA	
uthentication:	RSA-Signature		Add
uthentication:	RSA-Signature AES 128 Bit		<u>A</u> dd

Set Encryption to AES 128 Bit. Set Hash to SHA.

Note: The specified encryption and hash algorithms must correspond to the settings in the EAGLE

IPsec Policy Settings

sec Configuration	1		x
- 3T IKE Policy 3T Pre-sh 3T RSA S - 3T IPsec Polic 3T ESP-A	ared Key Ignatur IY ES128-MD5		
Add	Edit	Copy Delete	
			ose

Highlight the entry **ESP-AES128-MD5** in the **IPsec Policy** tree. Click **Edit.**

IPSec Policy

lame:	ESP-AES128-SHA	
Protocol	Encryption	Authentication
ESP	AES 128 Bit	SHA
rotocol:	ESP	- Add
rotocol: incryption	ESP AES 128 Bit	✓ Add Remove

Change the Name to ESP-AES128-SHA.

Set Encryption to AES-128 Bit.

Set Authentication to SHA.

Click OK.

 $\label{eq:close} \textbf{Close} \text{ the IPsec Configuration window.}$

Select IKE and IPsec Policy

asic Settings ine Management Sec General Settings dvanced IPsec Options Sentities Sec Address Assignment	IPsec General Settings Gateway (Tunnel Ei 55.1.2.2 Pallician	ndpoint):	
Psec Address Assignment plit Tunneling ertificate Check ink Firewall	Exch. Mode: JKE Policy: IKE DH Group: IPSec Policy:	main mode (IKEv1) RSA Signatur DH-Group 2 (1024 Bit) ESP-AES128-SHA	• • • •
	<u>r</u> . 3 0100p.	Policy Lifetimes	Policy <u>E</u> ditor

Set the IKE Policy to **RSA Signature** Set the IPsec Policy to **ESP-AES 128-SHA**

Policy Lifetimes



Click the button **Policy Lifetimes.**

Change the **IKE Policy Life Time** to 8 hours Change the **IPsec Policy Life Time** to **1 hour**. Click **OK**.

Profile Settings - Identities

Basic Settings Line Management	Local Identity (IKE)	
Advanced IPsec Options	Type:	ASN1 Distinguished Name 👻
entities sec Address Assignment	jD:	/C=DE/ST=BW/O=Hirschmann/OU=L3-Sup
alit Tunneling	Pre-shared Key	
ink Firewall	Shared Secret:	
	Confirm Secret:	
	Certificate configuration:	Standard certificate configuration
	Extended Authentication	(XAUTH)
	C User ID:	
	Password:	
	from the configur	ation above 👻

Navigate to Identities.

Select Standard certificate configuration.

Click **OK.**

Click **Ok** to close the **Profile** Window.

LANCOM Client configured



The LANCOM Client configuration is finished

EAGLE20 Configuration



- 1. Set IP addresses of the router interfaces accordingly.
- In our example: Int1/3 10.2.0.2/24; Int1/4: 55.1.2.2/24
- 2. Switch the EAGLE30 into router mode

Starting from a default configuration the CLI commands to configure the device via serial connection are:

!*(EAGLE)>enable

!*(EAGLE)#configure

!*(EAGLE)(Config)#interface 1/3

!*(EAGLE)((Interface)1/3)#ip address primary 10.2.0.2 255.255.255.0

!*(EAGLE)((Interface)1/3)#ip routing

!*(EAGLE)((Interface)1/3)#exit

!*(EAGLE)(Config)#interface 1/4

!*(EAGLE)((Interface)1/4)#ip address primary 55.1.2.2 255.255.255.0

!*(EAGLE)((Interface)1/4)#ip routing

!*(EAGLE)((Interface)1/4)#exit

!*(EAGLE)(Config)#ip routing

3. Login to the webinterface of the EAGLE30 from the int1/3 (IP 10.2.0.2)

VPN Configuration Web Interface



- 1. Navigate in the web interface tree to **Virtual Private Network -> Connections**.
- 2. Open the Wizard

VPN - Basic Settings

1 Create or Select Entry 2 Authentication	VPN Index	VPN Descri	VPN Active	Authentication Type	Startup	Operational Status	Remote Host
2 Authentication 3 Endpoint and Traffic Selectors 4 Advanced Configuration	ngex		Active	туре		2080,9	
	Create/Edit Index 1	Description	LANCOMCIent				

Specify the index and description of the VPN connection. Click Next

Upload Certificate/Key

Pre-sh Commo	shared Key mon Secret for Authentication		L 515	ANCOM
A share be iden Enter ti	d secret or itically conf ne appropri Pre-share Shared Se	pre-shared key is used igured on both sides (ate value for the IKE ID d Key cret:	to encrypt the connection. /PN client and VPN gateway according to the selected IE C <u>o</u> nfirm Secret:	This then needs to).) type.
8	Local Ider Type: [D:	ASN1 Distinguish /C=DE/ST=BW/O=	ed Name Hirschmann/OU=L3-Suppo	•) rt/CN=VPNCLIENT[
			< <u>B</u> ack Next	>Cancel

- 1. Select **Certificate Bundle (PKCS12)** from the Authentication Method drop-down box.
- 2. Click on Upload certificate/key

3. Specify the location of PKCS12 file and passphrase. The passphrase of the test certificate

- is 'vpnclient'.
- 4. Click OK

Upload successful



If the certificate file was uploaded successfully you see a confirmation message. Click ok.

Select Local Certificate

Create or Select Entry Authentication	Authentication Type Method	Certificate Bundle (PKCS12)
Endpoint and Traffic Selectors Advanced Configuration	Pre-shared key (PSK) Pre-Shared Key Confirm Pre-Shared Key Certificate Certificate	Choose
	Local Certificate Encrypted Private Passphrase (PKCS Confirm Passphras	Choose X Choose X / Change V / Change Upload certificate/key

Click **choose** and select the local certificate.

Uncheck Set/Change Passphrase

1 Create or Select Entry 2 Authentication	Authentication Type Method	Certificate	Bundle (PKCS12)
Endpoint and Traffic Selectors Advanced Configuration	Pre-shared key (PSK) Pre-Shared Key Confirm Pre-Shared Key		Change
	Certificate Certificate Authority		Choose
	Local Certificate	EAGLE20-cert.p12	Choose
	Encrypted Private Key		Choose
	Passphrase (PKCS12) Confirm Passphrase		Est / Change
			Upload certificate/key
			_2

- 1. uncheck Set/Change
- 2. click **Next**

Endpoint and Traffic Selectors

Create or Select Entry Authentication Endpoint and Traffic Selector	Endpoints Specifies the hostname or IP address of the security gateway.				
Advanced Configuration	Local Gateway	55.12.2			
	Remote Gateway 55.1.2.143				
	Traffic Selectors				
	Index Description Source Address (CDR) So	surce Restrictions Destination Address (CIDR) Destination Res			
(
Add Traffic Selector					
Index	1				
Description	2				
Source Address (CD)	R) 10.2.0.0/24				
Source Restrictions	for second as con-				
Destination Restriction	1/2/16/106/201/34				
	OK Cancel				
C					

1. Specify local and remote gateway addresses.

In our example

Local Gateway: 55.1.2.2

Remote Gateway 55.1.2.143

2. Add Traffic Selector with

Source Address (CIDR): 10.2.0.0/24

Destionation Address (CIDR): 172.16.106.201/32 (virtual address)

Advanced Configuration

Create or Select Entry	General		
2 Authentication	Margintine (s)	150	
Advanced Configuration	IKE/Key-Exchange		
	Version	KEv1	
	Startup	responder	•
	IKE Local Identifier Type	id	• 🔶
	KE Local D	Support/CN=EAG	
	Remote Identifier Type	d	• 🔶
	IKE Remote ID	upport/CN=VPNCL	емт —
	IKE Exchange Mode	main	•
	Key agreement	modp1024	•
	integrity (MAC)	hmacsha1	•
	Encryption	aes128	•
	DPD Timeout [s] Lifetime [s]	120	
		28800	
	PSec/Data-Exchange		
	Key agreement	modp1024	•
	Integrity (MAC)	hmacsha1	•
	Encryption	aes128	•
	Lifetime [s]	3600	

Set IKE Version 1 and specify the local and remote IDs (ASN1 DN of the certificates -see certindex.txt)

Version: **IKEv1**

IKE Local Identifier Type: id

IKE Local ID: /C=DE/ST=BW/O=Hirschmann/OU=L3-Support/CN=EAGLE20

IKE Remote Identifier Type: id

IKE Remote ID: /C=DE/ST=BW/O=Hirschmann/OU=L3-Support/CN=VPNCLIENT

Click Finish

Activate the VPN Connection



Activate the VPN connection

Click Set

Initialize Tunnel Setup



1. Move the Connection slide to the right to initialize the tunnel setup.

You will get prompted to enter the certificate's pin. In our example 'test'

2. The connection should be established successfully.

LANCOM Advanced VPN Client - Log



Select Log -> Logbook

VPN Overview



In the EAGLE20/30 web interface navigate to **Virtual Private Network - Overview** to check if the VPN connection is up.

EAGLE20/30 Event Log

In Course of Carlos		
(P 233) (W/W	-	
c Settings	The second second	
System	U System Log	U
Sature	1	
Load/Save	System Log	
External Memory	, , , , , , , , , , , , , , , , , , , ,	
/ort		
Asstat	110000-000000000000	
1	System Information	
ce Security	Product	EAGLE20
rank Security	Release	Hi8ec08-02.0.01-RC2
ALL PRIVATE Righwork	Hardware version:	00
(mag	aera number	83/59/005050101127
coalica.	Annuale Software release (PUM)	MISECUS-02 0.01-MC2 2015-01-16 15:33
Status Configuration	Elemente toffertes mintre (El 2041)	UD442.0 014652
System	Armiel software orienan (ELASED	GUA2.0.01-RC2
Sysiop	Bootogie software release (FLASH)	HiBoxt9-01-2-03-2014-05-23-07-22
Ports	P address (management)	03.00
LDP	MAC address (Range 80)	EC E5 55 01 2A ED
Asport	Bystem Name	EAGLE ECE555012AE0
Gitteal	System Up Time	0 days Ditra 50 mins 15 secs
Persistent Loggi	System Date and Time (local time zone)	2015-04-16 08:21:40
System Log	System operating hours	15 days 1 hrs 40 mms 42 secs
Audt Trail	Powert	OK
anted	Power2	DEFECTIVE
	Terrip Conference along the second as to bit to	
	Comparation state (ranning to rever)	out of another
	Service street scattery status	114040
	Secondary threadward for high reviewing harffor	
	second dramatics for tight howey carried	- a sing
	174: Notine Apr 16 2015	08-21-12 ISEMPTEAP swand 0x002300141 Tran 'hm2NabLowinSurgessTran' was sent.
	(hm2NeblastloginUserName.0 = adai	n. hn2WeblastLoginInetAddressType.0 = 1, hn2WeblastLoginInetAddress.0 = 55,1,2,143)
	173+ Metter Apr 16 2015	08-21-12 Instants overmore (m0022005a) Lonin via uch interface successful for user
	famint, role fadministratort.	to the second contract of the second processes of the
	177: Notice Apr 16 2015	00:17:17 UNDAME searcher Su00200201 Longer via unb interface successful for user
	"amin" with "administration"	martiers insume machait awaysaaral walkas era ana reservore awageagers ent medi
	171. Harian her 16 2016	AB.12.13 INDUCTION and SubDitional Free Participations and
	Cheffichiant Constitution and a site	and a second succession of the second s
	170. Metion her 16 2015	AD. 11.55 Interrete and Auto1200241 Page Include anti-
	1701 NOLLOS APE 16 2015	opinite [pushines aunde exceptions] tieb unstaurodonerreb, wes send:
	(nausalastiopoletastase.0 = Ads	AN ILLER DER sie destanden die Lemme nie der enteren fet fer eren betreit erte
	1691 NOTION ADD 16 2015	contribe for our decorrect) cut redont are antoesaint for neet ,egarg,' tote
	"Administrator" from 55.1.2.143 b	ecause of timeout exceed.
	'Administrator' from 55.1.2.143 b 160: Notice Apr 16 2015	ecsuse of timeout exceed. 08:11:34 [SNMFTRAP snapd 0x00230014] Trap 'hm2VpnUpTrap' was sent. (hm2VpnConnIndex = 2,
	'Administrator' from 55.1.2.143 b 160: Notice Apr 16 2015 hm2VpmConndperStatus = 1)	ecsuse of timeout exceed. 08:11:34 [SNAFTRAP stopd 0x00230014] Trap 'bm2VpnUpTrap' was sent. (bm2VpnConnIndex = 2,