

Base de Conhecimentos > Products > Classic Firewalls > How to set up a VPN connection between EAGLE20 and the LANCOM Advanced VPN Client (NCP client) ?

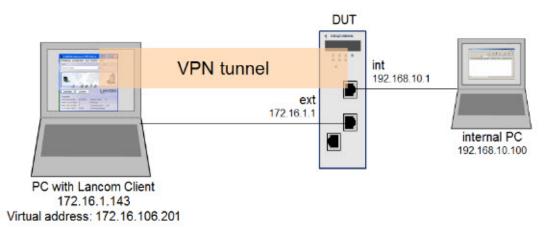
How to set up a VPN connection between EAGLE20 and the LANCOM Advanced VPN Client (NCP client) ?

- 2024-03-08 - Classic Firewalls

This lesson describes how to configure a VPN using Hirschmann EAGLE20 and the LANCOM Advanced VPN Client.

Used software versions: EAGLE20 firmware v5.2.00 Lancom Advanced VPN Client v2.30 Build 146

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.

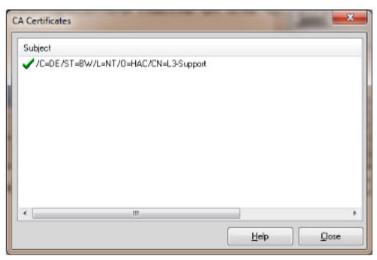
Import Certificates

		 Advanced VPN Client + CaCerts 		ch CaCerts		2
Organize 🔻 Inclu	de in li	brary Share with Burn	New folder	# ▪		
🔆 Favorites	-	Name	Date modified	Туре	Size	
Desktop	-	L3CA.pem	06.07.2012 16:38	PEM File		1
\rm Downloads	11	ANCOM_Client.p12	06.07.2012 16:39	Personal Informati		3
🔛 Recent Places						
词 Libraries						
Documents						
al Music						
Pictures	+ 4					100

Copy the PEM export of the CA (in our example L3CA.pem) and the PKCS#12 export of the LANCOM Client certificate (in our example LANCOM_client.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

	LANCOM Advanced VPI	N Client
	Connection Configuration	Log View Help
	Profile: AFF650_x509	
ertificates		
Certificate configuration		
Name Standard certificate configuration	User Certificate PKCS#12 file	
		c): 0 sec
	Certificates	LAN
Add Edit	Name: Standard certificate	e configuration Certificate Renewal
	Certificate:	from PKCS#12 file
	Seject Certificate:	1
-	PKCS#12 Filename:	C:\Program Files (x86)\LANCOM\Advanced VPN
	Contract Date	
	Certificate Path:	C:\Program Files (x86)\LANCOM\Advanced VPN
	Egitinicate Paint	

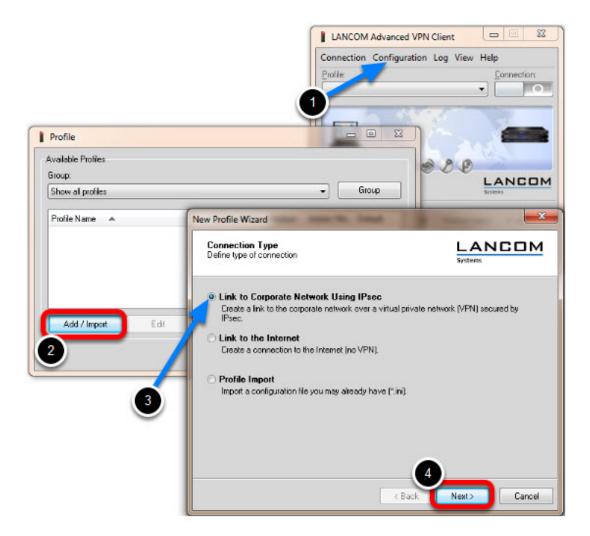
Highlight the Standard certificate configuration and click Edit.

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

Click OK.

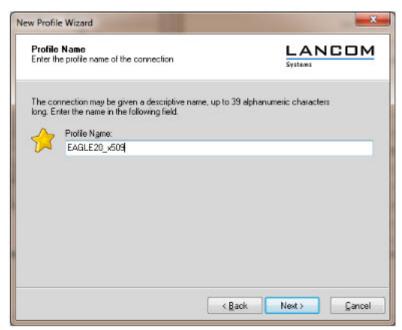
Close the Certificates configuration window.

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



Enter a Profile Name Click Next

Communication Medium

Communication Medium Select the media type of the connecti	on.	
Determine how the connection to the to be used via modem, set the commu-		
appropriate modern.		
Communication Media:	LAN (over IP)	•

Select LAN (over IP) as communication media Click Next

VPN Gateway Parameters

	iateway Parameters ch VPN gateway should the connection be hed?	
the VPI Using B	he DNS name (i.e. vpnserver.domain.com) or the offic N gateway you want to connect to. Extended Authentication (XAUTH) you can enter the u tication. If no authentication data are entered they will tion.	eser ID and password for the
C	Gateway (Tunnel Endpoint): 172.16.1.1	
22	Extended Authentication (AUTH)	
	UserID:	
	Password: Pas	sword (contirm):

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

IPsec Configuration



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

Local Identity (IKE)

	ared Key n Secret for /	Authentication	
identica	ily configure	d on both sides (VPN clie s value for the IKE ID acc Key	cording to the selected ID type.
0	<u>s</u> hared se	cier:	Confirm Secret:
	Localiden	tity (IKE)	
	Type:	ASN1 Distinguished	IName 👻
	ID:	/C=DE/ST=BW/L=	NT/0-HAC/CN-LANCOMClien
	ID:	/C=DE/ST=BW/L=	NT/O-HAC/CN-LANCOMClien

Delete the pre-shared keys

Set the Type to ASN1 Distinguished Name

Using the test certificates, copy the DN

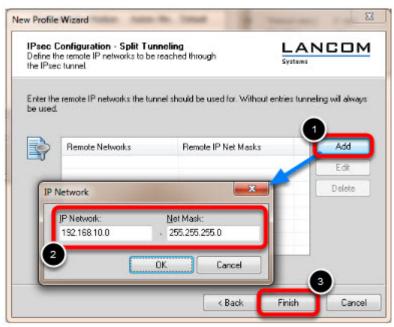
/C=DE/ST=BW/L=NT/O=HAC/CN=LANCOMClient in the ID field Click Next

IPsec Configuration - IP Addresses

	Configuration - IP Addresses ng the IP address to the client	
client's	which IP address the client is going IP address is dynamically assigned by more, define where the DNS / WINS IP Address <u>Assignment</u> Manual IP Address	
2000	Manual IP Address	
	172.16.106.201	
0	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



Define the remote IP network to be reached through the IPsec tunnel. In our example 192.168.10.0/24. Click Finish.

Profile Window

Available Profiles Group:	
<new (1)="" group=""></new>	▼ Group
Profile Name EAGLE 20_x509	Communication Medium Default
Add / Import	Copy <u>D</u> elete <u>Export</u>

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

Profile Settings

Basic Settings Line Management IPsec General Settings Advanced IPsec Options Identities	IPsec Ge	neral Settings <u>G</u> ateway (Tunn 172.16.1.1	el Endpoint):	
IPsec Address Assignment Spit Tunneing Certificate Check Link Firewall	Policies	<u>I</u> KE Policy: IP <u>s</u> ec Policy: Exch. <u>M</u> ode: <u>P</u> FS Group:	automatic mode automatic mode main mode (IKEv1) DH-Group 2 (1024 Bit)	•
			DH-Group 2 (1024 Bit) Policy Lifetimes Policy Editor	

Highlight **IPsec General Settings** in the left pane. Click **Policy Editor**

IKE Policy Settings

Psec Configuration	1	
 37 IKE Polic 37 Press 37 RSA 37 IPsec Polic 37 IPsec Polic 37 ESP 	hared Key Signatur	
	Edit	Copy Delete

 $\label{eq:Highlight} \textbf{RSA Signature} \text{ in the IKE Policy}$

Click **Edit**

Name:	RSA Signatur			
Authentication	Encryption	Hash	DH Group	_
RSA-Signature	AES 128 Bit	SHA	DH-Group 2 (1024	Bit)
withentication:	BSA-Signat	Je		ådd
Authentication:	RSA-Signatu	ute		≜dd
-	RSA-Signatu AES 128 Bit			<u>A</u> dd
Authentication: Encryption: Hagh:				

Set Encryption to AES 128 Bit. Set Hash to SHA. Set DH Group to DH-Group 2 (1024 Bit)

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

IPsec Policy Settings

Psec Configuration	<u> </u>		
 IKE Policy Pre-sh 			
oi Piesa			
4 ST IPsec Poli			
T ESP4		_	
Add	Edit	Ссру	Delete

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

		an 111 a	
CI	ICK	Edit.	

Name:	ESP-AES128-SHA		
Protocol	Encryption	Authentication	
ESP	AES 128 Bit	SHA	
	_		
Protocolt	ESP	v	Ādd
Protocol: Encryption	ESP AES 128 BR	•	<u>A</u> dd

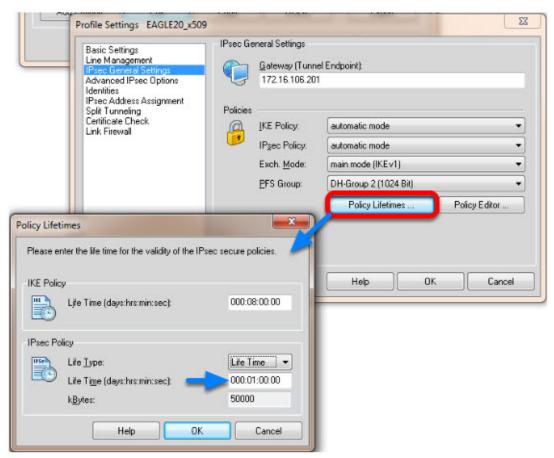
Change the Name to ESP-AES128-SHA. Set Encryption to AES-128 Bit. Set Authentication to SHA. Click OK. Close the IPsec Configuration window.

Select IKE and IPsec Policy

Basic Settings Line Management IFsec General Settings Advanced IPsec Options Identities IPsec Address Assignment	Management <u>Cleaneral Settings</u> noced IPsec Options titles	rel Endpoint);
Split Tunneling Certificate Check Link Firewall	Policies IKE Policy: IPgec Policy: Exch. <u>Mode</u> : <u>P</u> FS Group:	RSA Signatur ▼ (ESP-AES128-SHA ▼ main mode (IKEv1) ▼ DH-Group 2 (1024 Bit) ▼ Policy Lifetimes Policy Editor
]	Help QK Gan

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 **IPsec Policy Life Time** to **1 hour**. Click **OK**.

Profile Settings - Identities

Basic Settings Line Management IPsec General Settings Advanced IPsec Options (denthins) IPsec Address Assignment Split Tunneling Certificate Check Link Firewall	Identities Local Identity (IKE)	
	Tupe	ASN1 Distinguished Name
	ID:	/C-DE/ST-BW/L-NT/O-HAC/CN-LANCOM
	Pre-shared Key Shared Secret Certico Secret Certico Secret	Standard cartificate configuration
	configuration:	
	Diser ID:	(weith)
	Eassword:	
	from the configura	ation above

Navigate to Identities.

Select Standard certificate configuration.

Click **OK.**

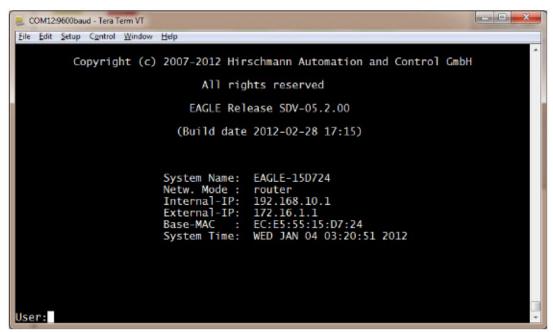
Click **Ok** to close the **Profile** Window.

LANCOM Client configured



The LANCOM Client configuration is finished

EAGLE20 Configuration



1. Switch the EAGLE20 into router mode

2. Set IP addresses of internal and external interface accordingly.

In our example: Internal Interface 192.168.10.1/24; External Interface: 172.16.1.1/24

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

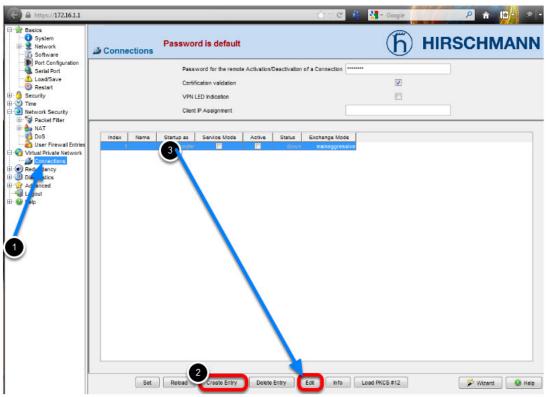
(Hirschmann Eagle) #network mode router

(Hirschmann Eagle) #network router param int ip-address 192.168.10.1

(Hirschmann Eagle) #network router param ext ip-address 172.16.1.1

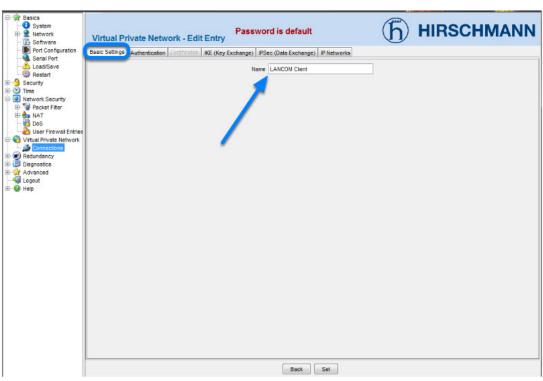
3. Login to the webinterface of the EAGLE20 from the internal network (192.168.10.0/24)

VPN Configuration Web Interface



- 1. Navigate in the web interface tree to **Virtual Private Network -> Connections**.
- 2. Create a new Entry.
- 3. Highlight the new entry and click Edit

VPN - Basic Settings



Name the VPN connection.

Change to next tab Authentication.

VPN - Authentication - Import Certificate

Basics System System System System Software Port Configuration Load/Save Load/Save Secart Software Software	Password is det Virtual Private Network - Edit Entry Basic Setting Authentication certificates KE (Key Exchange) IPSec (Data Exc Key Info Method x509 Pre-Shared Key 2	Icchange) P Networka
Connectons Connectons	Copy from PC Certificates Fie D:VemploertEAGLE1.p12 Password test	ack Set

- 1. Select **x509rsa**.
- 2. Click on **Load PKCS#12**

3. Specify location of the AFF certificate and password. The password of the test certificates is 'test'.

4. Click Copy from PC

Identities

Change the **Remote Type** to **asn1dn**.

Copy the distinguished name of the LANCOM Client certificate n the field **Remote ID**. In our example /C=DE/ST=BW/L=NT/O=HAC/CN=LANCOMClientChange to the next tab **Certificates**.

VPN - Certificates

Basics System System Software	Virtual Private Network - Edit Entry	(h) HIRSCHMANN
Port Configuration	Basic Settings Authentication Sertificates IKE (Key Exchange) PSec (Data Exchange) IP Networks	
Port Configuration Co	Basic Settings Authentication Pertificates (KE (Key Exchange) PSec (Data Exchange) (P Networks) Key Info Method x500rsa Pre-Shared Key Load PKCS #12 Kentiles Local Type defauit Local ID Remote D IST-BW/L-INT/O-HIAC/CN-LAN/COM/Clent Remote D ST-BW/L-INT/O-HIAC/CN-LAN/COM/Clent Back Set	
	Data Sei	

c Settings Authentica		c (rey exchange) [In	Sec (Data Exchange) P Networks
		l.	Load PKCS #12
			Show PKCS #12 file from PC
		Local	
		Certificate	YZrPz4HuUVowFBGVdKYGbDOA5ka * 9m7T79+Guq7mG4HHshGoVyk0/7alla/5 plsF+QzT3RQkIDF97o8PYhLq/SPw7mi END CERTIFICATE *
		Password	< <u>ــــــــــــــــــــــــــــــــــــ</u>
	\hookrightarrow	Private Key	*******
		Certification Authority	y (CA)
		Certificate	dqx/BwYdH6WQCHt2PcOSzuruaYvKC prwJAhzwBni07xG0y9HOWPHHxVS A0ym3V02y8+SpMXEhFocw== END CERTIFICATE < III +
		Remote	
		Certificate (optional)	

After successfully imported the certificate in the previous step you'll get the content of the PKCS#12 file displayed here.

Change to the next tab **IKE (Key Exchange)**

VPN - IKE (Key Exchange)

asic Settings	Authentication	Certificates	IKE (Key Exchange) PSec	(Data Excha	nge) IP Networks			
			Mode Protocol	auto		•]		
			Startup as	responder		•]		
			DPD Timeout	120				
			Lifetime	28800				
			Compatibility Mode	¢				
			Ha		modp1024 v sha1 v hmacsha1 v aes128 v			
			Peers (Endpoints)		_			
			Local IP Address	172.16.1.1				
			Remote IP Addres	s 172.16.1.1	43			
				Back	Set		 	

1. Set Startup as to responder.

2. The **Lifetime** should correspond to the LANCOM Client settings (8 hours) but is entered here in seconds.

3. Set the encryption **algorithms** accordingly in our example:

Key Agreement: modp1024

Hash: **sha1**

Integrity: hmacsha1

Encryption: aes128

4. Set the Local IP Address to 172.16.1.1

5. Set the **Remote IP Address** to **172.16.1.143**

Change to the next tab **IPsec (Data Exchange)**

VPN - IPsec (Data Exchange)

Basic Settings Authentication Certificates IKE (Key	Exchange PSec (Data Exchange) P Networks
-	Mode Encapsulation tunnel • Force NAT-T [11] Lifetime 3600
	Algorithms Key Agreement modp1024 Integrity hmacsha1 Encryption acs128
	Back Set

The **Lifetime** in seconds should correspond with the settings of the LANCOM Client (1 hour) Set the encryption **algorithms** accordingly.

In our example:

Key Agreement: **modp1024**

Integrity: hmacsha1

Encryption: aes128

Change to the next tab **IP Networks**

VPN - IP Networks

Basic Settings	Authentication Certifi	cates KE (Key	Exchange) IPSec (Data Excl	hange) (IP Network						
Index	Source Address (CIDR)	Source Port	Destination Address (CIDR)	Destination Port	Policy	Protocol	Description	Mapped Source Address	Mapped Destination Address	Active
1 19	2.168.10.0/24	any	172.16.106.201/32	any	require	any				1
4				1 Create Entry Back	m Delete Set	Entry				•

1. Create a new Entry

Enter the following values:

Source Address: 192.168.10.0/24 (internal network EAGLE20)

Destination Address: 172.16.106.201/32 (virtual Address of LANCOM Client)

Policy: **require** (traffic is not routed if tunnel is down)

2. Click **Set** to write the changes on all tabs in the device

Click **Back**

Activate VPN Connection



Activate the created VPN connection.

Click Set

Initialize Tunnel Setup



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'
 The connection should be established successfully.

LANCOM Advanced VPN Client - Log

	Connection Configuration Log View H	Help
	Profile:	Connection:
	EAGLE20 x500	•)
Log Book		-
20.09.2012 14:19:45	IPSec: Created an IPSEC SA with the following characteristics -	
20.09.2012 14:19:45	lpSrcRange=[172.16.106.201-172.16.106.201]JpDstRange=[192.168.10.0-192.168.10.255]JpProt=0,	i i i i i i i i i i i i i i i i i i i
20.09.2012 14:19:45	IPSec: connected: LifeDuration in Seconds = 2520 and in KiloBytes = 0	ANCO
20.09.2012 14:19:45	IPSec: Connected to EAGLE20_x509 on channel 1.	1
20.09.2012 14:19.45	PPP(lpcp): connected to EAGLE20_x509 with IP Address: 172.16.106.201	
20.09.2012 14:19:45	SUCCESS: IpSec connection ready	0.500
20.09.2012 14:20:09	Ike: NOTIFY : EAGLE20_x509 : RECEIVED : NOTIFY_MSG_R_U_HERE : 36136	out
20.09.2012 14:20:09	Ike: NOTIFY : EAGLE20_x509 : SENT : NOTIFY_MSG_R_U_HERE_ACK : 36137	LAN
20.09.2012 14:20:34	Ike: NOTIFY : EAGLE20_x509 : RECEIVED : NOTIFY_MSG_R_U_HERE : 36136	
20.09.2012 14:20:34	Ike: NOTIFY : EAGLE20_x509 : SENT : NOTIFY_MSG_R_U_HERE_ACK : 36137	-
20.09.2012 14:20:57	Ike: NOTIFY : EAGLE20_x509 : RECEIVED : NOTIFY_MSG_R_U_HERE : 36136	
20.09.2012 14:20:57	Ike: NOTIFY : EAGLE20_x509 : SENT : NOTIFY_MSG_R_U_HERE_ACK : 36137	
20.09.2012 14:21:21	Ike: NOTIFY : EAGLE20_x509 : RECEIVED : NOTIFY_MSG_R_U_HERE : 36136	
20.09.2012 14:21:21	Ike: NOTIFY : EAGLE20_x509 : SENT : NOTIFY_MSG_R_U_HERE_ACK : 36137	
20.09.2012 14:21:24	PPP(Lcp): Disconnect cause - INACTIVITY TIMEOUT:	
20.09.2012 14:21:24	IPSec: Disconnecting from EAGLE20_x509 on channel 1.	
20.09.2012 14:21:24	IPSec: Disconnecting from EAGLE20_x509 on channel 1.	
	IPSec: Disconnected from EAGLE20_x509 on channel 1.	

Select Log -> Logbook

EAGLE20 - Logfile

Network Software Port Configuration	Event Log		
Serial Port Load/Save Restart		AI	None
urity	Show		Description
e work Security	Show	Category	operating system kernel messages (reserved by RFC 3164)
ual Private Network	7	System	system (user-level) messages, e.g. startup/shutdown, task monitoring, event handling, LEDs (reserved by RFC 3164)
Connections	7	Auth	system (deenever) messages, e.g. standponddown, task monitoring, event handing, LEDs (reserved by RFC 3164) security/authorization messages (reserved by RFC 3164)
undancy	7	Svalog	messages generated internally by sysiog (reserved by RFC 3164)
phostics		P-Stack	P protocol stack
Events		a -ordon	
E Event Log		Psec	Psec data exchance (ESP/AH protocol)
Svalog Server	7	VPN	Paec key exchange (KE) and VPN control
Events Settings	100		
Advanced Settin	7	PPPoE	point-to-point protocol over ethernet
Ports	7	RADIUS	remote authentication dial in user service protocol
Topology Discovery	7	SSH	secure shell protocol
Device Status	9	SSL	secure sockets layer protocol
Signal Contact	7	Firewall	frewall
Alarms (Traps)	1	DHCP-D	dynamic host configuration protocol daemon
Report	1	DHCP-C	Pv4 dynamic host configuration protocol client
MAC Firewall List	2	WEB-S	WEB server
IP Firewall List	1	IP-Net	P network and interfaces
Configuration Check	V	(S)NTP	(simple) network time protocol
Ping	1	DHCP-S	Pv4 dynamic host configuration protocol server
anced	V	SNMP	simple network management protocol
out		DHCP-R	dynamic host configuration protocol relay
p i i i i i i i i i i i i i i i i i i i	V	Eth-F	ethernet network and interfaces
	V	ppp	point-to-point protocol
	V	TCP	transmission control protocol
	1	Config	configuration handling
	V	HiDiscovery	discovery of devices
		LLDP	ink layer discovery protocol
		User-Mgmt	user management
	V	Crypto-HW	cryptographic hardware interface
	V	Redundancy	redundancy protocols

In the EAGLE20 web interface navigate to **Diagnostics -> Events -> Event Log.**

Make sure that **all** events or at least the **category IPsec** and **VPN VPN** is checked, then click **Show Events**

EAGLE20 Event Log

Event Log

Hirschmann EAGLE Security Device

System software: EAGLE SDV-05.2.00 2012-02-28 17:15 RAM: SDV-05.2.00 2012-02-28 17:15 BAK: SDV-05.1.00 2011-06-07 11:27 Network operation mode: Router Mode Network internal interface IP address: 192.168.10.1 MAC address: ec:e5:55:15:d7:24 Network external interface IP address: 172.16.1.1 MAC address: ec:e5:55:15:d7:25 System name: EAGLE-1SD724 System uptime: 0 days 0 hours 16 minutes 26 seconds System local time: 2012-09-20 14:33:43

Entrynumber: Time [Taskname, Severity, Facility, Errorcode] Eventinformation

1: 2012-09-20 14:21:43 [tSnmpTrapTask, NOTICE, SNMP, 0x01FB0036] SNMP trap - send vpnDown trap done.

2: 2012-09-20 14:21:43 [tVpnMain, NOTICE, VPN, 0x020000A3] VPN connection 1 is 'DOWN'

3: 2012-09-20 14:21:40 [tHmLog, NOTICE, Syslog, 0x01F60003] There were 1 additional message(s) of the last entry

4: 2012-09-20 14:21:16 [tHmLog, NOTICE, Syslog, 0x01F60003] There were 1 additional message(s) of the last entry

5: 2012-09-20 14:20:52 [tHmLog, NOTICE, Syslog, 0x01F60003] There were 1 additional message(s) of the last entry

6: 2012-09-20 14:20:08 [ipcom_syslogd, NOTICE, VPN, 0x01F60001] OS-Log "VPN-1 received notification R-U-THERE-ACK"

7: 2012-09-20 14:19:45 [tSnmpTrapTask, NOTICE, SNMP, 0x01FB0035] SNMP trap - send vpnUp trap done.

8: 2012-09-20 14:19:45 [tVpnMain, NOTICE, VPN, 0x020000A2] VPN connection 1 is 'UP'

9: 2012-09-20 14:19:44 [ipcom_syslogd, NOTICE, VPN, 0x01F60001] OS-Log "VPN-1 quick mode exchange done in 235 ms (peer: 172.16.1.143, message ID: 44889698)"

2012-09-20 14:19:44 [ipcom_syslogd, NOTICE, VPN, 0x01F60001] OS-Log "New exchange started (QUICK_MODE with Message ID: 1149803416)"
 2012-09-20 14:19:44 [ipcom_syslogd, NOTICE, VPN, 0x01F60001] OS-Log "VPN-1 Main mode exchange done in 520 ms (peer: 172.16.1.143, Message ID: 0)"

12: 2012-09-20 14:19:44 [ipcom_syslogd, NOTICE, VPN, 0x01F60001] OS-Log "VPN-1 received notification INITIAL-CONTACT"

13: 2012-09-20 14:19:43 [ipcom_syslogd, NOTICE, VPN, 0x01F60001] OS-Log "New exchange started (ID_PROT with Message ID: 0)"

14: 2012-09-20 14:19:37 [tSnmpd. NOTICE, VPN. 0x0200000C1 VPN connection 1 activated successfully

Back Reload Search Save

0.0