



INFINIGATE
.... Adding Value to Distribution

TechServices

Support Services

Knowledge Base

Sophos Connect Client 2.0

Sophos
XG 18.0 MR3



Inhaltsverzeichnis

1 Allgemeines	3
2 Beschreibung	3
3 Vorbereitung	3
4 Notwendige Schritte	3
4.1 Grundlegende Funktionen des Sophos Connect Client.....	3
4.1.1 Allgemeine Informationen.....	3
4.1.2 Profilverwaltung IPSEC.....	4
4.1.3 Profilverwaltung SSLVPN	5
4.1.4 Verbinden eines Profils	7
4.1.5 Status der Verbindung	7
4.1.6 Ereignisübersicht und VPN-Protokoll.....	9
4.2 Sophos Connect Admin.....	10
4.2.1 Split-Tunnel und Security Heartbeat	10
4.2.2 Benutzerkennwort und 2-Faktor.....	11
4.2.3 Auto-Connect Tunnel	12
4.2.4 DNS-Suffix und Domänen-Logon-Skript	12
4.3 IPSEC Konfiguration auf der XG Firewall	12
4.3.1 Konfiguration des Dienstes und Authentifizierung	12
4.3.2 Relevante Konfigurationen für den Client und Konfigurationsexport	15
4.3.3 Firewallregel	16
4.3.4 Benutzer statische IP zuweisen.....	16
4.3.5 Mehrfaktorauthentifizierung.....	17
4.4 SSLVPN Konfiguration auf der XG Firewall	18
4.4.1 Konfiguration des Dienstes und der Authentifizierung	18
4.4.2 Erweiterte Konfigurationen für den SSL VPN Dienst	19
4.4.3 Firewallregel	20
4.4.4 Mehrfaktorauthentifizierung	20
4.5 Update des Sophos Connect Client.....	21
5 weitere Unterstützung	21



1 Allgemeines

Mit der sogenannten Knowledge Base stellt das TechServices Team im Rahmen des Supports für Partner kostenlose Anleitungen zu häufig gestellten Fragestellungen bereit. Anhand dieser werden die Partner in die Lage versetzt, die im jeweiligen Eintrag beschriebenen Problemstellungen schnell selbst lösen zu können.

2 Beschreibung

Der Sophos Connect Client bietet Remote-Anwender eine einfache und schnelle Möglichkeit einen VPN Tunnel aufzubauen. Ab der Version 2.0 wurden beide VPN Technologien (SSL und IPSEC) in einem Client vereint. Derzeit ist der Connect Client 2.0 nur für Windows und der Sophos XG v18 verfügbar.

3 Vorbereitung

Zur Umsetzung des KB ist eine vorkonfigurierte XG Installation mit WAN-Verbindung notwendig. Optional kann auch eine Identitätsquelle wie Active Directory eingerichtet werden, um entsprechende Benutzer für die VPN-Verbindung authentifizieren zu können.

Eine Softwareverteilung für das MSI-Paket des „Sophos Connect Client“ ist von Vorteil. Im KB-Artikel <https://community.sophos.com/kb/en-us/133555> von Sophos wird eine Möglichkeit zur automatisierten Ausrolung des Clients per AD-Gruppenrichtlinien beschrieben.

4 Notwendige Schritte

4.1 Grundlegende Funktionen des Sophos Connect Client

4.1.1 Allgemeine Informationen

Der Sophos Connect Client 2.0 basiert auf StrongSwan 5.8.0 (IPSEC), der auf die Charon IKE-Implementierung aufsetzt. Es werden IKEv1 als auch IKEv2 unterstützt. Die umfangreiche Unterstützung von Verschlüsselungs- und Hash-Algorithmen gewährleistet einen hohen Sicherheitsstandard. Weitere Informationen zu StrongSwan sind unter <https://wiki.strongswan.org/projects/strongswan> zu finden.

Der Sophos Connect Client ab Version 2.0 beinhaltet nun auch eine SSLVPN Unterstützung basierend auf OpenVPN 2.5 (SSLVPN), auch hier können verschiedene umfangreiche Verschlüsselungs- und Hash-Algorithmen genutzt werden. Weitere Informationen zu OpenVPN sind unter <https://community.openvpn.net/openvpn/wiki/HOWTO> zu finden.

SOPHOS		
Connections		Events
Occurred	Description	Clear events
✓ 2020-12-1 6:40:26 AM	SECTION	
✓ 2020-12-1 6:40:29 AM	Sophos Connect version: 2.0.34.0910	
✓ 2020-12-1 6:40:29 AM	strongSwan version: 5.8.0	
✓ 2020-12-1 6:40:29 AM	OpenVPN version: 2.5.0.0	

Abbildung 1



4.1.2 Profilverwaltung IPSEC

Der Client kann mehrere Profile importieren, welche jeweils auf der XG-Firewall erstellt wurden. Es ist jedoch nur eine aktive Verbindung möglich.

Der Import erfolgt über die 3 Punkte dem Kontextmenü (Abb.2) „Verbindung importieren“.

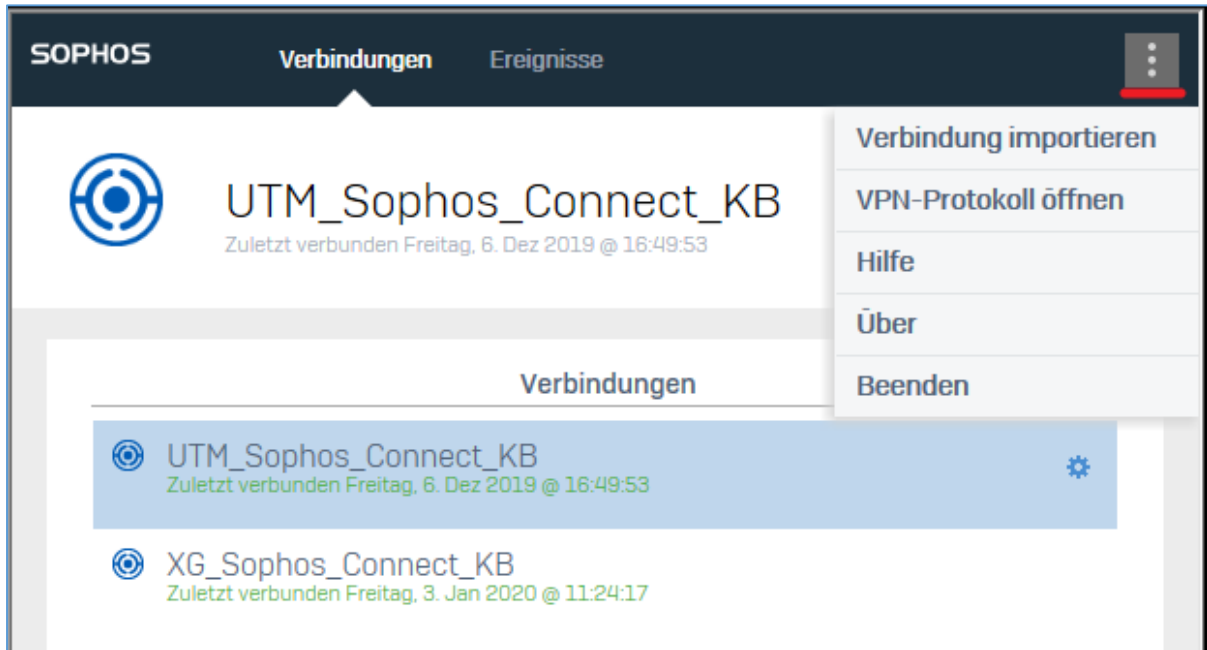


Abbildung 2

Wird eine IPSEC-Remote-Verbindung mit Benutzerzertifikat verwendet, muss dieses im Benutzerportal heruntergeladen und im Client importiert werden. Die Aufforderung erfolgt automatisch beim Import eines entsprechenden Profils.

Das im Benutzerportal festgelegte PKCS#12-Kennwort muss eingegeben und die Datei per „PKCS#12“-Datei importieren“ (Abb. 3) geladen werden.



Abbildung 3



4.1.3 Profilverwaltung SSLVPN

Der Import von SSLVPN Verbindung kann nur über einen Automatischen Import mit Hilfe des User Portals durchgeführt werden. Vorteil zum älteren Sophos SSL Client: Änderungen an der SSL VPN Konfiguration werden durch den Sophos Connect Client 2.0 automatisch erkannt und angewendet.

Dabei muss eine Provisionierungsdatei (*.PRO) erstellt werden, welche man durch einen Doppelklick ausführt oder durch Kopieren in den Ordner „C:\Program Files (x86)\Sophos\Connect\import“ dem Sophos Connect Client zur Verfügung stellen kann.

Bei älteren Sophos Connect Clients der Version 2 kann es vorkommen, dass das User Portal Capture noch nicht unterstützt wird. Hierzu kann das Capture beim Zugriff auf das User Portal über die Firewall Console deaktiviert werden. Siehe hierzu Abbildung 4.1

```
# console> system captcha_authentication_global disable
```

```
Sophos Firmware Version SFOS 18.0.1 MR-1-Build396

console> system captcha_authentication_global disable

Captcha authentication serves as an extra security defense against scripted automated login attempts.

Are you sure you want to disable captcha for the webadmin and user portal? (Y/N): Y
Captcha authentication for the webadmin and user portal is turned off.
console>
```

Abbildung 4.1

Hinweis: ein automatisches Update des Sophos Connect Clients ist bisher noch nicht integriert!

Hier in Abbildung 4.2 kann man eine Beispiel Provisionierungsdatei (sslvpn.pro) mit zwei SSLVPN Verbindungen sehen.

```
[
{
  "display_name": "SSL_demo1_infinigate_de",
  "gateway": "demo1.infinigate.de",
  "user_portal_port": 1443,
  "otp": false,
  "can_save_credentials": true,
  "check_remote_availability": false,
  "run_logon_script": false
},
{
  "display_name": "SSLDemo2_infinigate_de",
  "gateway": "demo2.infinigate.de",
  "user_portal_port": 443,
  "otp": false,
  "can_save_credentials": true,
  "check_remote_availability": true,
  "run_logon_script": false
}
]
```

Abbildung 4.2



Folgende Schalter kann eine Provisionierungsdatei für den SSL VPN Tunnel enthalten (Abb. 4.3).

Schalter	Beschreibung
"display_name": "<Enter Connection name>"	Name der Verbindung im Sophos Connect Client (Pflichtfeld)
"gateway": "<Enter Your Gateway hostname or ip>"	WAN IP-Adresse der Firewall (Pflichtfeld)
"gateway_order":	Gibt an, wie die XG-Firewall den Datenverkehr ausgleicht, wenn mehrere Gateways konfiguriert sind. distributed: Wählt ein Gateway nach dem Zufallsprinzip aus, wenn eine Verbindung versucht wird. latency: Wählt ein Gateway danach aus, wie schnell es auf eine TCP-Verbindungsanforderung antwortet. in_order: Versucht zuerst das erste Gateway in der Liste, wenn das fehlschlägt, wird das nächste Gateway in der Liste versucht.
"user_portal_port": 443	User Portal Port Einstellung der betroffenen XG Firewall (Default ist 443)
"otp": false	Ist für diese VPN Verbindung eine 2FA Authentifizierung aktiviert (Default ist false)
"auto_connect_host": ""	Automatischer Verbindungsaufbau der VPN Verbindung, wenn ein Client aus den „Remote LAN Networks“ vom Client angesprochen wird (Default ist kein Wert)
"can_save_credentials": true	User und Password können im Sophos Connect Client gespeichert werden (Default ist true)
"check_remote_availability": false	Führt beim Verbindungsstart eine Remote-Verfügbarkeitsprüfung durch, um nicht reagierende Clients zu eliminieren. (Default ist false)
"run_logon_script": false	Führt das vom Domänencontroller bereitgestellte Anmeldeskript aus, nachdem der VPN-Tunnel aufgebaut wurde. (Default ist false)

Abbildung 4.3



4.1.4 Verbinden eines Profils

Per Doppelklick eines Profils die Verbindung aufgebaut. Wird SSLVPN und IPsec mit XAUTH (Abb. 4.4) verwendet müssen die entsprechenden Benutzerangaben zur Authentifizierung eingegeben werden.

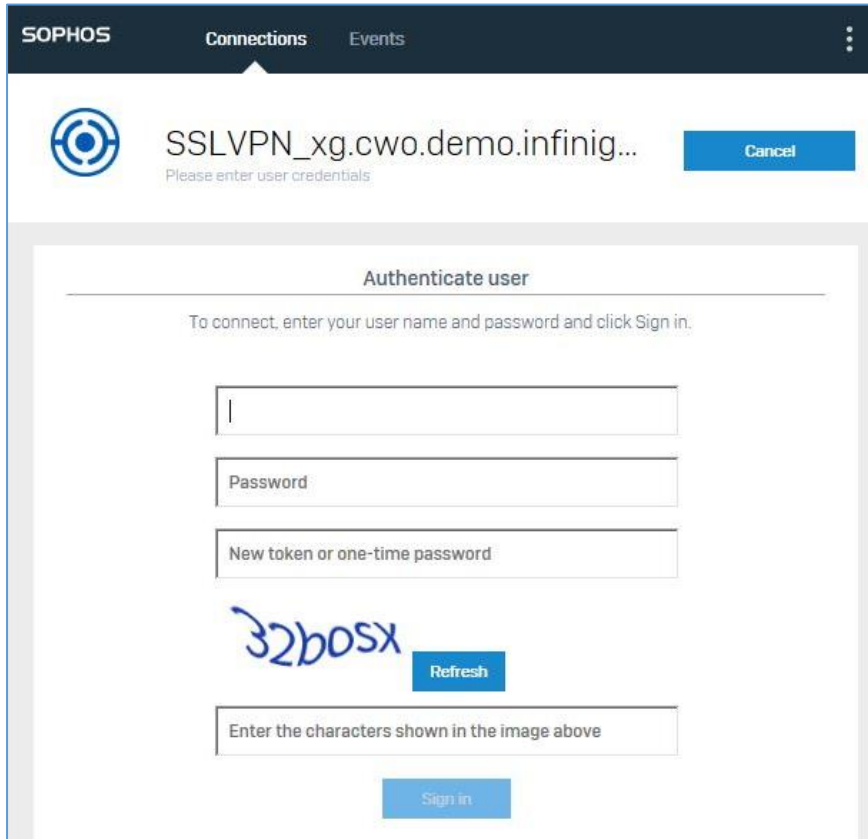


Abbildung 4.4

4.1.5 Status der Verbindung

Nach Verbindungsaufbau bietet der Client eine Übersicht relevanter Informationen. Abbildung 5 zeigt den Verbindungsaufbau und Zielgateway am Beispiel IPsec.



Abbildung 5



In Abbildung 6 werden zusätzlich die zugewiesene IP für den Tunneladapter, DNS und Routen, die über den Tunnel gehen, angezeigt. In diesem Fall wird der komplette IPv4-Traffic (0.0.0.0/0) über den Tunnel geroutet.

Verbindung überwachen		
Lokale IP	10.	: 51919
Gateway-IP	10.4	: 4500
Virtuelle IP-Adresse	192.168.101.10	
DNS-Server	172.16.16.16	
Entferntes Netzwerk	0.0.0.0/0	
Erhaltene Bytes	6563426	
Übertragene Bytes	4672960	
Empfangene Pakete	15725	
Übertragene Pakete	14818	

Abbildung 6

Abbildung 7.1 für IPSec und Abbildung 7.2 für SSLVPN bietet eine Übersicht der Sicherheitseinstellungen.

Verbindung überwachen	
<u>IKE</u>	
Verschlüsselungsalgorithmus/Schlüssel...	AES_CBC / 256
Integritätsalgorithmus	HMAC_SHA2_256_128
Pseudozufallsfunktion	PRF_HMAC_SHA2_256
Diffie-Hellman-Gruppe	MODP_2048
Nächster Rekey	4 Stunden 7 Minuten 42 Sekunden
<u>IPsec</u>	
Verschlüsselungsalgorithmus/Schlüssel...	AES_CBC / 256
Integritätsalgorithmus	HMAC_SHA2_256_128
Diffie-Hellman-Gruppe	MODP_2048
Nächster Rekey	42 Minuten 35 Sekunden

Abbildung 7.1

Monitor connection	
<u>SSL VPN</u>	
Encryption algorithm	AES-128-CBC
Integrity algorithm	SHA256
Compression	True

Abbildung 7.2



4.1.6 Ereignisübersicht und VPN-Protokoll

Der Reiter Ereignisse bietet ein verkürztes Protokoll mit Informations-, Warnungs- und Fehlermeldungen.

Aufgetreten	Beschreibung
2020-1-3 11:29:00 AM	Sophos-Connect-Version: 1.4.45.1015
2020-1-3 11:29:00 AM	strongSwan-Version: 5.8.0
2020-1-3 11:29:00 AM	Verbindung Sophos_Connect_KB hergestellt
2020-1-3 11:29:39 AM	Verbindung Sophos_Connect_KB wird deaktiviert
2020-1-3 11:29:46 AM	Verbindung Sophos_Connect_KB deaktiviert
2020-1-3 11:47:39 AM	Verbindungsname bearbeitet [UTM_user_certificate]
2020-1-3 1:56:09 PM	Geben Sie die Benutzer-Anmeldeinformationen ein
2020-1-3 1:56:15 PM	Benutzerauthentifizierung abgebrochen
2020-1-3 1:56:32 PM	Verbindungsname bearbeitet [XG_Sophos_Connect_KB]
2020-1-3 1:56:49 PM	Verbindungsname bearbeitet [UTM_Sophos_Connect_KB]
2020-1-3 1:59:23 PM	Geben Sie die Benutzer-Anmeldeinformationen ein
2020-1-3 1:59:45 PM	Verbindung UTM_Sophos_Connect_KB wird hergestellt
2020-1-3 1:59:54 PM	Benutzerauthentifizierung fehlgeschlagen. Bitte versuchen Sie es
2020-1-3 2:00:04 PM	Benutzerauthentifizierung abgebrochen
2020-1-3 2:00:04 PM	Verbindung UTM_Sophos_Connect_KB wird deaktiviert

Abbildung 8

Ein ausführliches Log kann im Kontextmenü „VPN-Protokoll öffnen“ (erreichbar über die 3 Punkte, siehe Abb. 2) eingesehen werden.

Es enthält wichtige Informationen zum Dienst. Konfiguration, TUN-Device, Plugins müssen ohne Fehlermeldung geladen sein. Ist dies nicht der Fall kann ein Tunnel nicht aufgebaut werden. Zu Problemen kann es kommen, wenn der Dienst mangels Berechtigungen nicht korrekt starten kann.

Bei einem Verbindungsaufbau werden die Informationen hier am Beispiel IPSec (Abb. 9) für das zugehörige Verbindungsprofil ausgegeben.

```

2020-01-03 09:58:21AM 00[DMN] Starting IKE service charon-svc (strongSwan 5.8.0, Windows Client 6.2.9200 (SP 0.0))
2020-01-03 09:58:21AM 00[LIB] TAP-Windows driver version 1.0 available.
2020-01-03 09:58:23AM 00[LIB] opened TUN device: {3FDA2529-1017-429A-99C7-4FE33616CD88}
2020-01-03 09:58:24AM 00[LIB] loaded plugins: charon-svc nonce x509 pubkey pkcs1 pkcs7 pkcs8 pkcs12 pem openssl kernel-libipsec kernel-iph socket-w
2020-01-03 09:58:24AM 00[JOB] spawning 16 worker threads
2020-01-03 11:16:15AM 16[CFG] loaded IKE shared key with id 'Sophos_Connect_KB-psk-id' for: '%any'
2020-01-03 11:16:15AM 11[CFG] loaded EAP shared key with id 'Sophos_Connect_KB-user-id' for: 'sophos.connect'
2020-01-03 11:16:15AM 16[CFG] added wici connection: Sophos_Connect_KB
2020-01-03 11:16:16AM 10[CFG] wici initiate CHILD_SA 'Sophos_Connect_KB-tunnel-1'
2020-01-03 11:16:16AM 15[IKE] <Sophos_Connect_KB|1> initiating Main Mode IKE_SA Sophos_Connect_KB[1] to 10.49.15.133
2020-01-03 11:16:16AM 15[ENC] <Sophos_Connect_KB|1> generating ID_PROT request 0 [ SA V V V V V ]
2020-01-03 11:16:16AM 15[NET] <Sophos_Connect_KB|1> sending packet: from 10.49.15.133 [51918] to 10.49.15.133 [51918] (180 bytes)
2020-01-03 11:16:16AM 13[NET] <Sophos_Connect_KB|1> received packet: from 10.49.15.133 [5000] to 10.49.15.133 [51918] (180 bytes)
2020-01-03 11:16:16AM 13[ENC] <Sophos_Connect_KB|1> parsed ID_PROT response 0 [ SA V V V V V ]
2020-01-03 11:16:16AM 13[IKE] <Sophos_Connect_KB|1> received XAuth vendor ID
2020-01-03 11:16:16AM 13[IKE] <Sophos_Connect_KB|1> received DPD vendor ID
2020-01-03 11:16:16AM 13[IKE] <Sophos_Connect_KB|1> received Cisco Unity vendor ID
2020-01-03 11:16:16AM 13[IKE] <Sophos_Connect_KB|1> received FRAGMENTATION vendor ID
2020-01-03 11:16:16AM 13[IKE] <Sophos_Connect_KB|1> received NAT-T (RFC 3947) vendor ID
2020-01-03 11:16:16AM 13[CFG] <Sophos_Connect_KB|1> selected proposal: IKE:AES_CBC_256/HMAC_SHA2_256/PRF_HMAC_SHA2_256/MODP_2048
2020-01-03 11:16:16AM 13[ENC] <Sophos_Connect_KB|1> generating ID_PROT request 0 [ KE No NAT-D NAT-D ]
2020-01-03 11:16:16AM 13[NET] <Sophos_Connect_KB|1> sending packet: from 10.49.15.133 [51918] to 10.49.15.133 [5000] (396 bytes)
2020-01-03 11:16:16AM 12[NET] <Sophos_Connect_KB|1> received packet: from 10.49.15.133 [5000] to 10.49.15.133 [51918] (396 bytes)
2020-01-03 11:16:16AM 12[ENC] <Sophos_Connect_KB|1> parsed ID_PROT response 0 [ KE No NAT-D NAT-D ]
2020-01-03 11:16:16AM 12[IKE] <Sophos_Connect_KB|1> faking NAT situation to enforce UDP encapsulation
2020-01-03 11:16:16AM 12[ENC] <Sophos_Connect_KB|1> generating ID_PROT request 0 [ ID HASH ]
2020-01-03 11:16:16AM 12[NET] <Sophos_Connect_KB|1> sending packet: from 10.49.15.133 [51919] to 10.49.15.133 [4500] (92 bytes)
2020-01-03 11:16:16AM 11[NET] <Sophos_Connect_KB|1> received packet: from 10.49.15.133 [4500] to 10.49.15.133 [51919] (92 bytes)
2020-01-03 11:16:16AM 11[ENC] <Sophos_Connect_KB|1> parsed ID_PROT response 0 [ ID HASH ]
2020-01-03 11:16:16AM 13[NET] <Sophos_Connect_KB|1> received packet: from 10.49.15.133 [4500] to 10.49.15.133 [51919] (92 bytes)
2020-01-03 11:16:16AM 13[ENC] <Sophos_Connect_KB|1> parsed TRANSACTION request 14708282 [ HASH CPRQ(A_U2R_X_PWD) ]

```

Abbildung 9



4.2 Sophos Connect Admin

Der Sophos Connect Admin bietet die Möglichkeit die exportierte Konfigurationsdatei anzupassen. Über „open“ kann die exportierte Konfigurationsdatei geladen werden.

Hinweis: Dies gilt nur für IPSEC Verbindungen, SSL VPN Verbindungen werden im Punkt 4.4 separat betrachtet.

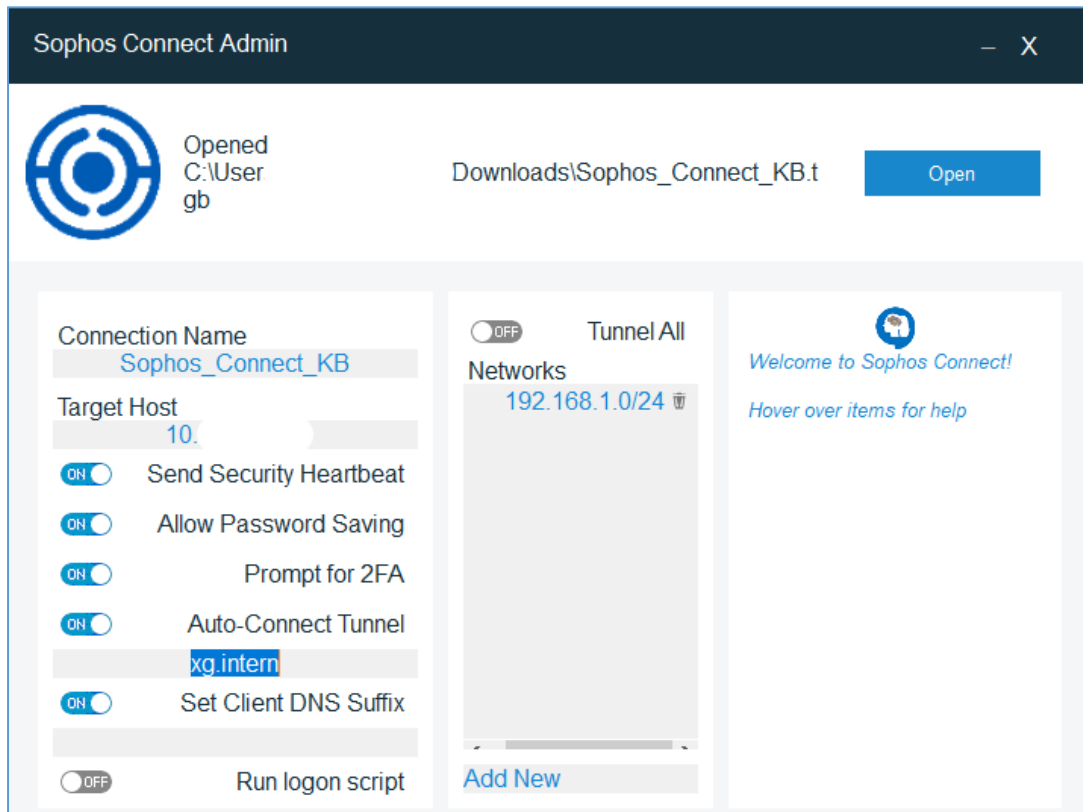


Abbildung 10

4.2.1 Split-Tunnel und Security Heartbeat

Standardmäßig wird bei einer IPsec Verbindung der komplette Clienttraffic über den Tunnel gesendet. Durch Hinzufügen eines Subnetzes wird nur dieses über den Tunnel geroutet. Bei Verwendung des Security Heartbeats auf der XG muss dies aktiviert werden, damit der HB-Traffic durch den Tunnel geroutet wurde. Optional kann auch die Heartbeat-IP, die der heartbeat.xml im Verzeichnis des Central Clients zu entnehmen ist, in Networks hinzugefügt werden.



4.2.2 Benutzerkennwort und 2-Faktor

Das Speichern des Benutzerkennworts kann in der Konfigurationsdatei mit „Allow Password Saving“ aktiviert werden. Dies ist Voraussetzung, damit „Auto-Connect Tunnel“ ohne Kennwortaufforderung funktioniert.

Zusätzlich kann die 2-Faktor-Authentifizierung verwendet werden, hierzu ist entsprechend auf der Firewall OTP zu konfigurieren. Im Admin-Tool kann für den Sophos Connect Client ein Eingabefeld für das OTP durch „Prompt for 2FA“ aktiviert werden.

Dies gewährleistet, dass bei Speicherung von Benutzername und Kennwort nach der Eingabe im Sophos Connect Client (Abb. 11) das Kennwort ohne OTP gespeichert wird und bei Wiederverbindung (Abb. 12) nur die Eingabeaufforderung für das OTP erfolgt.

Die Einrichtung von OTP auf der Sophos XG wird im Abschnitt [4.3.5 Mehrfaktorauthentifizierung](#) erklärt.

SOPHOS Verbindungen Ereignisse

Sophos_Connect_XG_OTP Abbrechen
Geben Sie die Benutzer-Anmeldeinformationen ein

Benutzer authentifizieren

Zum Anmelden geben Sie Ihren Benutzernamen und Ihr Kennwort ein und klicken Sie auf „Anmelden“.

sophos.connect

.....

|

Benutzername und Kennwort speichern

Anmelden

Abbildung 11

Benutzer authentifizieren

|

Anmelden

Abbildung 12



4.2.3 Auto-Connect Tunnel

Ist die Option „Auto-Connect Tunnel“ aktiv, wird nach dem OS-Login versucht, die letzte aktive Verbindung aufzubauen. Es kann ein DNS-Suffix eingetragen werden, damit der Client anhand dessen erkennen kann ob, es sich um ein bekanntes oder fremdes Netz handelt.

Bitte Punkt [4.2.2 Benutzerkennwort und 2-Faktor](#) beachten.

4.2.4 DNS-Suffix und Domänen-Logon-Skript

Wird die Option „Set Client DNS Suffix“ aktiviert und entsprechend eingetragen, erhält der Client nach erfolgreicher Verbindung das entsprechende Suffix. Zusätzlich kann mit „Run logon script“ das Domänen-Logon-Skript ausgeführt werden.

4.3 IPSEC Konfiguration auf der XG Firewall

4.3.1 Konfiguration des Dienstes und Authentifizierung

Die XG Firewall muss ein konfiguriertes WAN-Interface und mindestens ein LAN-Netz besitzen. Unter dem Punkt „Configure -> VPN“ den Reiter „Sophos Connect Client“ wählen.

Den Dienst mit „Sophos Connect Client“ aktivieren und ein WAN-Interface wählen.

Als Authentifizierung können „Preshared key“ (Abb. 13.1) und „Digital certificate“ (Abb. 13.2) gewählt werden. Bei PSK ein sicheres Kennwort angeben. Die ID-Zuordnung kann auf Standard gelassen werden, sollte sich die Firewall hinter einer NAT befinden, diese manuell festlegen.

Unter „Allowed users and groups“ werden Benutzer hinzugefügt, die sich verbinden dürfen. Ab der Sophos XG Version 18MR3 können auch Gruppen verwendet werden. Die Authentifizierung der Benutzer erfolgt per XAUTH.

Als Identitätsquelle kann die lokale Datenbank oder eine externe Quelle wie LDAP oder Active Directory verwendet werden. Bei Verwendung einer konfigurierten externen Quelle muss der Server unter „Configure -> Authentication -> Services -> VPN (IPsec/L2TP/PPTP) authentication methods“ (Abb. 13.3) hinzugefügt werden.

IPsec connections	SSL VPN (remote access)	SSL VPN (site-to-site)	Sophos Connect client	L2TP (remote access)	Clientless access	Bookmarks	Bookmark groups	PPTP (remote access)
General settings								
Sophos Connect client		<input checked="" type="checkbox"/> Enable						
Interface *		PortB - 193. i						
Authentication type *		Preshared key i						
Preshared key *		***** Change Preshared key Show preshared/PSK key						
Local ID		Select local ID i						
Remote ID		Select remote ID i						
Allowed users and groups *		VPN-Group -						
		Add new item						

Abbildung 13.1



Für die Zertifikatsauthentifizierung die Zertifikate zuordnen. Es können dabei selbstsignierten Zertifikate verwendet werden.

Authentication type *	Digital certificate	<i>i</i>
Local certificate *	ApplianceCertificate	
Remote certificate *	sophos.connect	
Local ID	DER ASN1 DN [X.509]	/C=DE/ST=NA/L=NA/O=Infinigate Deutschland Gm <i>i</i>
Remote ID	IP address	1111 <i>i</i>

Abbildung 13.2

Die „Remote ID“ muss mit der „Certificate ID“ übereinstimmen. Abbildung 13.2 zeigt ein Beispiel für ein selbstsigniertes Zertifikat (sophos.connect).

VPN (IPsec/L2TP/PPTP) authentication methods

Set authentication methods same as firewall

Authentication server list	Selected authentication server
<input type="text" value="type to search..."/>	dc01 <i>x</i>
<input type="checkbox"/> Local	
<input type="checkbox"/> nas01	
<input checked="" type="checkbox"/> dc01	

drag to change priority

Abbildung 13.3



Das Zertifikat kann unter „System -> Certificates -> Certificates -> Generate self-signed certificate“ erstellt werden.

Name *	<input type="text" value="sophos.connect"/>
Valid from *	<input type="text" value="2020-01-03"/>
Valid until *	<input type="text" value="2021-01-03"/>
Key type *	<input checked="" type="radio"/> RSA <input type="radio"/> Elliptic curve
Key length *	<input type="text" value="2048"/> ▼
Secure hash *	<input type="text" value="SHA - 256"/> ▼
Key encryption	<input type="checkbox"/> Enable
<u>Certificate ID *</u>	<input type="text" value="IP address"/> ▼ <input type="text" value="1111"/>

entification attributes

Country name *	<input type="text" value="Germany"/> ▼
State *	<input type="text" value="NA"/>
Locality name *	<input type="text" value="NA"/> (eg. city name)
Organization name *	<input type="text" value="Infinigate Deutschland GmbH"/> (eg. company name)
Organization unit name *	<input type="text" value="OU"/> (eg. department name)
Common name *	<input type="text"/> (eg. server's hostname)
Email address *	<input type="text" value="sophos.connect@xg.intern"/>

Abbildung 14



4.3.2 Relevante Konfigurationen für den Client und Konfigurationsexport

Ein Subnetz, aus dem der Client eine IP erhält, muss eingetragen werden. Die IP kann auch von einem RADIUS-Server zugewiesen werden. Optional kann für den Tunneladapter noch ein DNS-Server konfiguriert werden.

Client information

Name *

Assign IP from * -

Allow leasing IP address from RADIUS server for L2TP, PPTP and Sophos Connect client ⓘ

DNS server 1

DNS server 2

Sophos Connect Client Contains Sophos Connect client installers (Windows and macOS) and admin tool (Windows)

Abbildung 15

Per „Download“ können die MSI-Pakete für den Client und das Admin-Tool heruntergeladen. Die MSI-Pakete können auch per Gruppenrichtlinien verteilt werden.

In den „Advanced Settings“ wird festgelegt, ob die Verbindung getrennt wird, falls der Client über den festgelegten Zeitraum im Feld „Idle session time interval“ inaktiv ist.

Advanced settings

Disconnect when tunnel is idle Enable

Idle session time interval Seconds (between 120-999)

Abbildung 16

Mit „Apply“ die Konfiguration speichern und die VPN starten. „Reset“ setzt die Konfiguration auf Standard zurück.

Die Konfigurationsdatei, welche eine tgb-Endung enthält, wird mit „Export connection“ heruntergeladen. Diese enthält alle Informationen. Im Falle einer PSK-Authentifizierung diesen in Klartext und bei Zertifikatsauthentifizierung die Zertifikatskette Base64 enkodiert.

Abbildung 17

Die Konfigurationsdatei muss im Client vom Benutzer als Verbindungsprofil importiert werden.



4.3.3 Firewallregel

Das virtuelle IPsec-Interface des „Sophos Connect Client Dienstes“ wird automatisch der Zone VPN hinzugefügt. Damit erfolgen die Verbindungen der „Sophos Connect Client“ über die VPN-Zone. Entsprechend müssen die Regeln erstellt werden. Im Beispiel Abbildung 18 dürfen die Benutzer uneingeschränkt im Internet surfen.

Source zones *

LAN
VPN
Add new item

Source networks and devices *

Any
Add new item

During scheduled time

All the time
Select to apply the rule

Destination and services

Select the destination zones, networks, devices, and services.
The rule applies to traffic to these destinations.

Destination zones *

WAN
Add new item

Destination networks *

Any
Add new item

Services *

Any
Add new item

Services are traffic type

Abbildung 18

4.3.4 Benutzer statische IP zuweisen

Es gibt die Möglichkeit einem Benutzer für die Verbindung eine statische IP zuzuweisen, um Adresskonflikte zu vermeiden oder ein bestimmter Dienst erfordert dies. Dies erfolgt unter „Configure -> Authentication -> Users“. Den entsprechenden Benutzer editieren und die IP im Punkt „Sophos Connect Client“ eintragen.

Sophos Connect client * Enable Disable IP address 192.168.101.10

Abbildung 19



4.3.5 Mehrfaktorauthentifizierung

Die XG Firewall unterstützt für IPsec-Remoteverbindungen Mehrfaktorauthentifizierung per OTP. Dies muss unter „Configure -> Authentication -> One-time password -> Settings“ konfiguriert werden.

OTP kann für alle Benutzer oder nur für selektierte Benutzer und Gruppen aktiviert werden. Unter dem Punkt „Enable OTP for facilities“ muss „User portal“ und „IPsec remote access“ aktiviert werden.

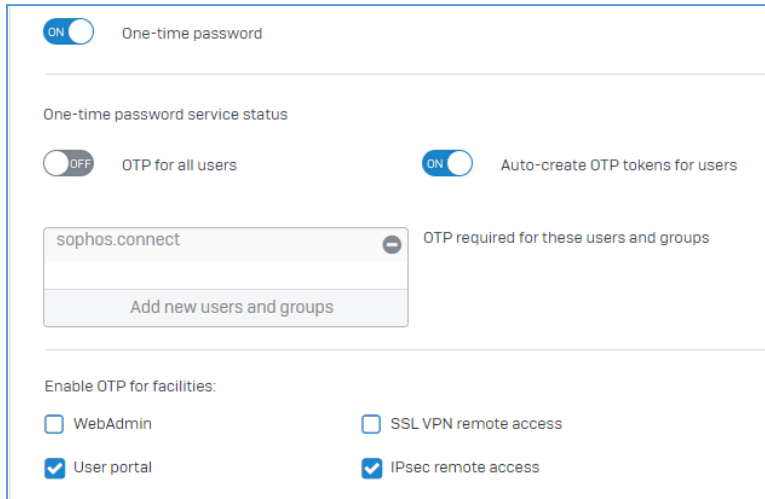


Abbildung 20

Zur Generierung des OTP-Tokens muss sich jeder Benutzer im Benutzerportal anmelden und den Schlüssel dem verwendeten OTP-Authenticator hinzufügen. Empfehlenswert sind FreeOTP oder der Sophos Authenticator für Android und iOS. Diese erlauben das Abscannen des QR-Codes sowie die Verwaltung mehrerer Schlüssel.

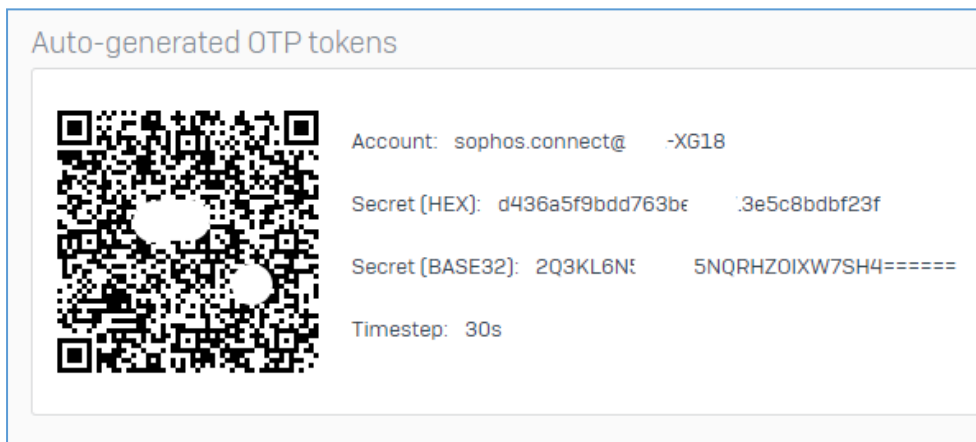


Abbildung 21



4.4 SSLVPN Konfiguration auf der XG Firewall

4.4.1 Konfiguration des Dienstes und der Authentifizierung

Die XG Firewall muss ein konfiguriertes WAN-Interface und mindestens ein LAN-Netz besitzen. Unter dem Punkt „Configure -> VPN“ den Reiter „SSL VPN (remote access)“ wählen. Hier ein neues VPN Profil über „Add“ erstellen.

Als Name kann eine individuelle Profil Bezeichnung gewählt werden (Abb.22).

The screenshot shows the configuration page for an SSL VPN profile. The 'General settings' section contains two input fields: 'Name *' with the value 'SSL_xg_cwo_demo_infinigate_de' and 'Description' with the placeholder 'Enter description'.

Abbildung 22

Bei Identity werden die entsprechenden Userkonten hinterlegt, welche dieses Profil nutzen sollen. Hier können nicht nur User sondern auch Gruppen genutzt werden. Als Identitätsquelle kann die lokale Datenbank oder eine externe Quelle wie LDAP oder Active Directory verwendet werden. Bei Verwendung einer konfigurierten externen Quelle muss der Server unter „Configure -> Authentication -> Services -> SSL VPN authentication methods“ hinzugefügt werden (Abb.23).

The screenshot shows the 'Identity' configuration page. Under the 'Policy members' section, there is a dropdown menu with 'VPN-Group' selected and an 'Add new item' button below it.

Abbildung 23

Unter Tunnel Access werden die internen Netzwerk Ressourcen angegeben, welche in Form von automatischen Routen am Sophos Connect Client hinterlegt werden. Hierbei kann man einmal den Punkt „Use as default gateway“ oder einzelne Netzwerk Ressourcen in Form von ganzen Netzen oder einzelnen Host Objekte auswählen. Bei der Wahl von „Use as default gateway“ wird nach dem Verbindungsaufbau der komplette Client Traffic über den VPN Tunnel von der Firewall betrachtet und verarbeitet.

The screenshot shows the 'Tunnel access' configuration page. The 'Use as default gateway' toggle is turned OFF. The 'Permitted network resources [IPv4]' section shows a dropdown menu with 'Netz_LAN' selected and an 'Add new item' button below it. The 'Permitted network resources [IPv6]' section also has an 'Add new item' button.

Abbildung 24



Über den Punkt „Disconnect idle clients“ kann bei Inaktivität der VPN Tunnel automatisch getrennt werden. Hier ist der Standard Wert 15 Minuten (Abb. 25).

Idle time-out

Disconnect idle clients OFF

Override global time-out (Default 15 Minutes) Minutes [15-60]

Abbildung 25

4.4.2 Erweiterte Konfigurationen für den SSL VPN Dienst

Unter dem Punkt „Configure -> VPN“ den Reiter „Show VPN Settings“ und SSL VPN können sie weitere Einstellungen des SSL VPN Dienstes durchführen (Abb.26).

Settings Close VPN settings

SSL VPN L2TP

SSL VPN settings

Protocol * TCP UDP [Select UDP for better performance]

SSL server certificate *

Override hostname

Port * [1-65535]

IPv4 lease range * - (Should be from private IP ranges. First 2 IPs in the range will be used by the server.)

Subnet mask *

IPv6 lease (IPv6/prefix) * /

Lease mode *

IPv4 DNS

IPv4 WINS

Domain name

Disconnect dead peer after * Seconds [60 - 1800]

Disconnect idle peer after * Minutes [15 - 60]

Abbildung 26

Hier können Sie das genutzte Protokoll, den Netzwerk Port, das Dienst Zertifikat sowie den Hostnamen der externen WAN Verbindung der XG Firewall hinterlegen.

Hinweis: der SSL Port (TCP/443) kann nicht gemeinsam mit der Webserver Protection (WAF) genutzt werden!

Weiterhin können Sie den IP-Range der, nach erfolgreicher VPN Verbindung, zugewiesenen IP-Adressen anpassen.

Sie haben die Möglichkeit hier für die SSL VPN Verbindung einen internen DNS-Server sowie ein DNS-Suffix anzugeben, welcher nach erfolgter Verbindung genutzt werden soll.

Hinweis: Änderungen in den Erweiterten SSL VPN Eigenschaften haben auch auf den Site-to-Site SSL VPN Tunnel Auswirkungen!



4.4.3 Firewallregel

Das virtuelle SSL VPN-Interface des „Sophos Connect Client Dienstes“ wird automatisch der Zone VPN hinzugefügt. Damit erfolgen die Verbindungen der „Sophos Connect Client“ über die VPN-Zone. Entsprechend müssen die Regeln erstellt werden. Im Beispiel Abbildung 27 dürfen die Benutzer uneingeschränkt im Internet surfen.

The screenshot shows a Firewall Rule configuration interface. It is divided into several sections:

- Source zones ***: A list containing 'LAN' and 'VPN', each with a minus sign icon. Below the list is an 'Add new item' button.
- Source networks and devices ***: A list containing 'Any' with a minus sign icon. Below the list is an 'Add new item' button.
- During scheduled time**: A dropdown menu set to 'All the time' with the text 'Select to apply the rule' below it.
- Destination and services**: A heading with the instruction 'Select the destination zones, networks, devices, and services. The rule applies to traffic to these destinations.'
- Destination zones ***: A list containing 'WAN' with a minus sign icon. Below the list is an 'Add new item' button.
- Destination networks ***: A list containing 'Any' with a minus sign icon. Below the list is an 'Add new item' button.
- Services ***: A list containing 'Any' with a minus sign icon. Below the list is an 'Add new item' button. A note at the bottom right says 'Services are traffic type'.

Abbildung 27

4.4.4 Mehrfaktorauthentifizierung

Die XG Firewall unterstützt für SSL VPN-Remoteverbindungen Mehrfaktorauthentifizierung per OTP. Dies muss unter „Configure -> Authentication -> One-time password -> Settings“ konfiguriert werden.

OTP kann für alle Benutzer aktiviert werden, oder nur für selektierte Benutzer und Gruppen. Unter dem Punkt „Enable OTP for facilities“ muss „User portal“ und „SSL VPN remote access“ aktiviert werden (Abb.28).

The screenshot shows the 'One-time password' settings interface. It includes the following elements:


- One-time password**: A toggle switch that is turned ON.
- One-time password service status**:
 - OTP for all users**: A toggle switch that is turned OFF.
 - Auto-create OTP tokens for users**: A toggle switch that is turned ON.
- OTP required for these users and groups**: A list containing 'cwolter@cwo.test' with a minus sign icon. Below the list is an 'Add new users and groups' button.
- Enable OTP for facilities**:
 - WebAdmin**: A checkbox that is unchecked.
 - User portal**: A checkbox that is checked.
 - SSL VPN remote access**: A checkbox that is checked.
 - IPsec remote access**: A checkbox that is checked.
- Timestep**:
 - Default token timestep in seconds**: A text input field with '30' and 'Seconds [10 - 300]'.
 - Maximum passcode offset steps**: A text input field with '3' and '[0 - 10]'.
 - Maximum initial passcode offset steps**: A text input field with '10' and '[0 - 600]'.

Abbildung 28



Zur Generierung des OTP-Tokens muss sich jeder Benutzer im Benutzerprotal anmelden und den Schlüssel dem verwendeten OTP-Authenticator hinzufügen. Empfehlenswert sind FreeOTP oder der Sophos Authenticator für Android und iOS. Diese erlauben das Abscannen des QR-Codes sowie die Verwaltung mehrerer Schlüssel.

Auto-generated OTP tokens



Account: sophos.connect@ -XG18

Secret (HEX): d436a5f9bdd763be .3e5c8bdbf23f

Secret (BASE32): 2Q3KL6N! 5NQRHZOIXW7SH4=====

Timestep: 30s

4.5 Update des Sophos Connect Client

Ein Update des Sophos Connect Clients von der Version 1 auf die Version 2 ist problemlos möglich. Dabei werden auch die entsprechenden IPSEC Verbindungsprofile mit übernommen.

Hinweis: Der Sophos Connect Client 2.0 überprüft, ob ein Sophos SSL VPN Client am System installiert ist. Wenn ja, wird die Installation abgebrochen, da der Sophos SSL VPN Client vorab manuell deinstalliert werden muss. Hierbei werden keine SSLVPN Verbindungsprofile übernommen, diese müssen anschließend, wie in Punkt [4.1.3 Profilverwaltung SSLVPN](#) beschrieben aktiviert werden.

5 weitere Unterstützung

Bei Rückfragen zu diesem Knowledge Base Artikel oder anderen Themen steht Ihnen unser Partner Support gerne zur Verfügung, den Sie unter support@infinigate.de erreichen können.

Beim Aufbau eines vertiefenden Wissens unterstützen wir mit individuellen Schulungen oder Zertifizierungstrainings; alle Information dazu jederzeit aktuell unter www.infinigate.de/akademie oder akademie@infinigate.de