reinhold.leitner@applicgate.com

2021-02-16

VPN Client with ApplicGate

1 Introduction

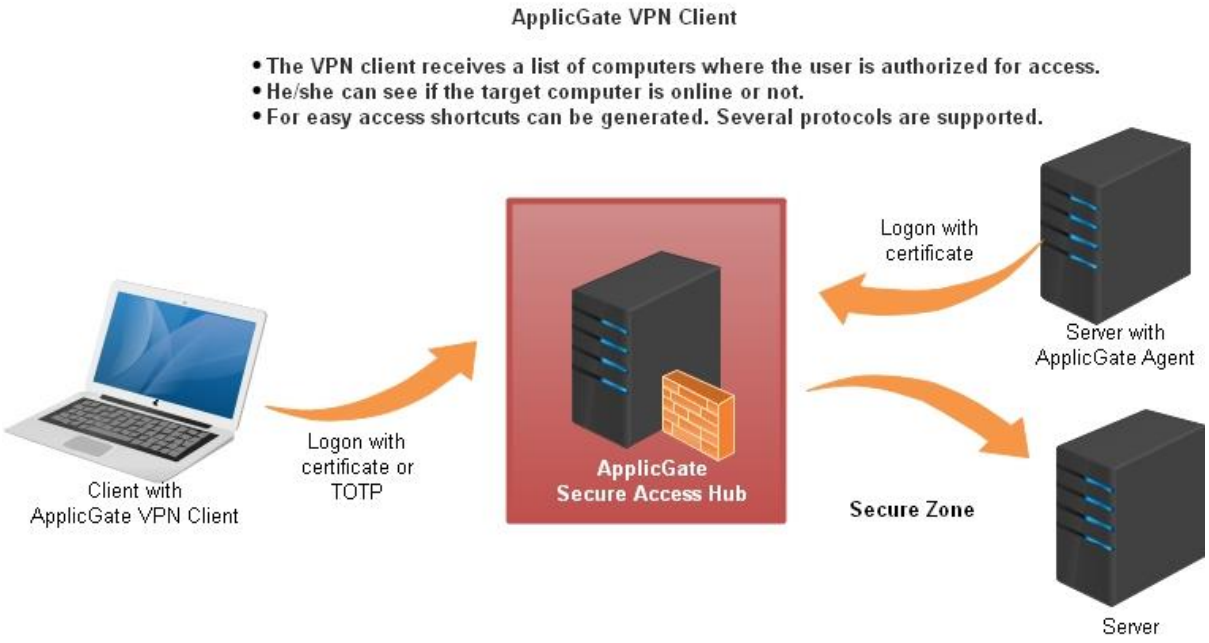
The goal is to secure access from the Internet to servers located in the Intranet or any cloud site using **strong authentication** (certificates or TOTP).

The advantages of this solution:

- The VPN client receives a list of computers where the user is authorized for access and an indication if the target computer is online or not.
- For easy access shortcuts can be generated. Several protocols are supported.
- The VPN client can use a web proxy to connect to the Internet.
- All protocols (RDP, CIFS etc.) are tunnelled through encrypted connections.
- Access can be controlled by timers (date, hours, and weekdays).

This document shows some examples how to configure ApplicGate as a VPN client and how to configure the corresponding ApplicGate VPN server.

2 Network Schema



The ApplicGate VPN server acts as a Secure Access hub.
Only authenticated users are allowed to access the server within the Intranet.

Remark:
The “ApplicGate VPN Server” role can be installed at the “Intranet Server”. So there is no need for an additional server.

3 Prerequisites

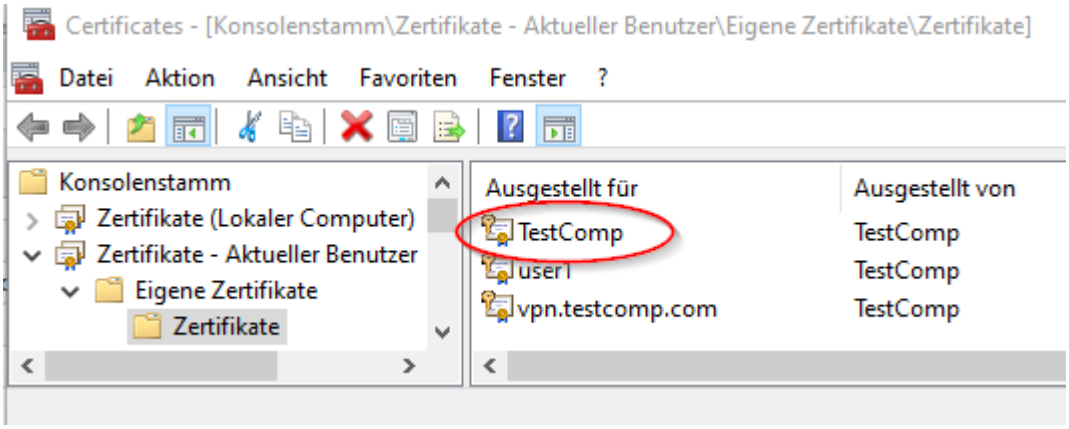
- A computer with a public IP address where the ApplicGate VPN server feature can be configured:
  Any Windows or Linux (e.g. latest version of Debian or Raspbian) machine
- Windows 10 for the ApplicGate VPN client
- ApplicGate software, see www.applicgate.com
- Certificates (see also chapter “Certificates for Authentication and Encryption” below).
  As an alternative TOTP can be used for authentication.

4 Configuration of ApplicGate VPN Server

4.1 Trusted Root

The VPN server has to trust the client certificate.
If you have generated the certificates as defined below proceed as follows:

- On your Windows computer export the signing certificate (the CA certificate) using mmc certificates to TestCompCA.crt (without public key, Base64 encoded):



- At the ApplicGate VPN Server define the CA certificate as trusted:
  For Linux e.g. (depends on Linux version):
  sudo cp TestCompCA.crt /usr/local/share/ca-certificates
  sudo update-ca-certificates
  For Windows:
  use mmc certificates and
  import the certificate TestCompCA.crt into “Trusted Root Certification Authorities, Certificates”

If you have other certificates you have to ensure the trust if not done already (similar procedure as above).

4.2 Configuration Files

We need two configuration files for the ApplicGate VPN Server: **routing.csv** and **groups.csv**

For detailed information see https://help.applicgate.com or the local help built-in ApplicGate.

4.2.1 Example for Routing.csv

Connections to the target computers (Computer 1 and Computer 2) are forwarded directly in this example (as for the server at the bottom in the schema above). Another configuration option you can see in a chapter “Server Logon to ApplicGate”.

```
SourceIP   ;GatewayIP;GatewayPort;GatewayIP2;DestinationIP;DestinationPort;Expiration ;Type                ;UID                              ;Comment                    ;eMail
*          ;*        ;99   ;manage      ;300       ;30    ;* ;SSL:vpn.testcomp.com.pfx/vpntest, REFRH:5,TINT:5,LOG:1, GRPUPD,RTUPD, DELLOG:20, LGS, LGTIME, FLG:yes, BPRI:AboveNormal;MGMT;;
*          ;*        ;442  ;reverselogon;client|mgmt;     ;* ;SSL:vpn.testcomp.com.pfx/vpntest, CCR:*@testcomp.com, ISS:"CN=TestComp, O=Test Company", CHKCC; VPNS; VPN Server;
VPNclients1;*        ;3391 ;*          ;10.0.0.20 ;3389  ;* ;UIDN:"VPN myComp!VPNclients1", LDAC:yes      ;VPN.1~Computer1.RDP            ;RDP to Computer 1          ;admin@testcomp.com
VPNclients1;*        ;445  ;           ;10.0.0.20 ;*     ;  ;LDAC:yes                                    ;VPN.1f~CIFS.bat                ;Fileshare Computer 1       ;admin@applicgate.com
VPNclients1;*        ;3392 ;*          ;10.0.0.21 ;3389  ;* ;LDAC:yes                                    ;VPN.2~Computer2.RDP            ;RDP to Computer 2          ;admin@testcomp.com
```

Detailed description:

- The first entry defines the **manage**ment interface:
  Accessible via all network interfaces via TCP port 99.
  In this case (manage) 300 defines the maximum number of connections allowed and 30 defines the default TTL in minutes.
  The Type field defines the server certificate via the keyword SSL, REFRH sets the refresh timer for the home page to 5 seconds, TINIT defines the internal timer interval with 5 seconds, GRPUPD and RTUPD allow updates of group.csv and routing.csv via the web interface, DELLOG defines the number of days to delete old log files, LGS enables logging of sessions (one line per session with start time, duration etc.), LGTIME enables insertion of date/time in front of each log message, FLG enables logging to the general log file, BPRI sets the priority of ApplicGate.
  This entry must be modified to allow only authorized access, e.g.:
  Specify SourceIP, GatewayIP (e.g. 127.0.0.1 for local access only) or the keywords CCR and ISS to check client certificates.
- The **reverselogon** entry defines how the clients log on to the ApplicGate VPN server:
  Accessible via all network interfaces via TCP port 442.
  The field DestinationIP defines the supported functions: client (download rules to the client) and mgmt (optional, allow management of the client).
  The Type field defines the server certificate, the keyword CCR requests client certificates (all certificates with email address ending with @testcomp.com are allowed) and the certificate issuer must match as defined in the keyword ISS.

- The last three entries define the rules that are transmitted to the client if the client has the proper authorization:
  VPNclients is a group with a list of email addresses, e.g. user1@testcomp.com and so on, that are allowed to access these entries.
  GatewayIP can be * or a local address, DestinationIP and DestinationPort define where to forward the connection request.
  Each routing entry should have a unique identification (UID). It consists of a main part separated from a sub part by ".".
  The keyword UIDN defines a long text for all UID entries with same main part (in this case "VPN myComp", used to generate the UID list), defines the access to this list (in this case the group VPNclients) and optionally a path where shortcuts can be stored.
  The keyword LDAC:yes enables download of this entry to the clients.
  Optionally via the field UID the name of a shortcut may be specified (see next chapter)

This is the view of the routing entries via ApplicGate:

ID	Listening	Source IP	Gateway IP	Gateway Port	Gateway IP2	Destination IP	Destination Port	Expiration	Type	UID	Comment	eMail
12	true	*	*	99	manage	300	30	*	SSL:vpn.testcomp.com.pfx/vpntest, REFRH:5,TINT:5,LOG:1, GRPUPD,RTUPD, DELLOG:20, LGS, LGTIME, FLG:yes, BPRI:AboveNormal	MGMT	Manage	admin@testcomp.com
13	true	*	*	442	reverselogon	client	*	*	SSL:vpn.testcomp.com.pfx/vpntest, CCR:*@testcomp.com, ISS:"CN=TestComp, O=Test Company", CHKCC	VPNS	VPN Server	
14	true	VPNclients1	*	3391	*	10.0.0.20	3389	*	UIDN:"VPN myComp!VPNclients1! https://vpn.testcomp.com:441/VPN", LDAC:yes	VPN.1 ~Computer1.RDP	RDP to Computer 1	admin@testcomp.com
15	true	VPNclients1	*	445	*	10.0.0.20	*	*	LDAC:yes	VPN.1f ~CIFS.bat	Fileshare Computer 1	admin@applicgate.com
16	true	VPNclients1	*	3392	*	10.0.0.21	3389	*	LDAC:yes	VPN.2 ~Computer2.RDP	RDP to Computer 2	admin@applicgate.com

4.2.2 Shortcuts

Shortcut files are generated by ApplicGate locally and executed by ApplicGate.

Shortcuts depending on file name and/or type:

- *.RDP … Remote Desktop
- *.VNC … UltraVNC
- *-R.VNC … RealVNC
- *.bat … map a network share via CIFS (SMB)
- *webdav.bat … map a network share via WebDAV

After initial creation these files may be changed:
Username/password and other parameters can be changed and saved to these files.
These shortcut files will not be overwritten except the local address/port is incorrect.

Remark: When the switch **scsh** is specified at start of the VPN client and the server transmits a path (defined in the keyword UIDN) to the client the files are not generated. They will be retrieved by ApplicGate using this path.

Shortcut commands:

- cmd: ... The command will be executed; the strings %ip% and %port% will be replaced with the actual value. e.g. shortcut to start PuTTY:
  cmd:putty -P %port% %ip%
  Start RDP:
  mstsc /v:%ip%:%port%
- cmdb: ... The command will be inserted into a temporary .bat file and then the .bat file will be executed. The string %ip% and %port% will be replaced with the actual value.
  At the end of the .bat file the command pause will be inserted. This allows the user to see the result of the command. E.g. shortcut to map a network share:
  cmdb:net use * \\%ip%*share* * /User:*domain**user*

4.2.3 Example for groups.csv

```
GroupName  ;IPranges                                  ;Comment ;eMail  ;Expiration
License    ;* mycomputer mycompany 0KO1b...8UjCsaNTu ;License ;       ;*
Title      ;ApplicGate VPN Server                     ;        ;       ;*
VPNclients1;user1@testcomp.com                        ;        ;       ;*
```

Detailed description:

- **The license entry defines the license which can be obtained via www.applicgate.com .**
- Title defines the title for the management interface.
- VPNclients1 is used for access control as shown above.

4.3 Installation of ApplicGate at the VPN Server

Before you start the installation you have to copy the files routing.csv and groups.csv to the installation directory.

For installation on Windows see: https://help.applicgate.com/helpmeST.htm
For installation on Linux see: https://help.applicgate.com/helpmeSX.htm

5 Configuration of the ApplicGate VPN Client

Supported for Windows, e.g. Windows 10.

Ensure that the DNS name vpn.testcomp.com can be resolved at the client (via DNS server or local hosts file).

If access to network shares via CIFS will be configured:
The Server service must be disabled at the VPN client. Don't forget to reboot after the service has been disabled,

5.1 Install user certificate

Double-click the file user1@testcomp.com.pfx to install the certificate or use any other certificate (in this case authorization must be adapted at the VPN server).

5.2 Installation of ApplicGate at the VPN Client

For the following two installation options currently there are no client licenses necessary.

5.2.1 Local Installation

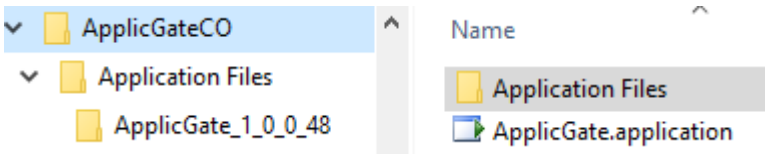
- Create a new directory and store ApplicGate.exe into this directory
- Start the ApplicGate VPN Client via following command:
  applicgate.exe "/ClickOnce?server=vpn.testcomp.com:442&sslcc=Prompt:user1@testcomp.com&title=VPNclient&cifs"
- For definition of parameters see https://help.applicgate.com/helpmeCO.htm

5.2.2 Network Installation via ClickOnce

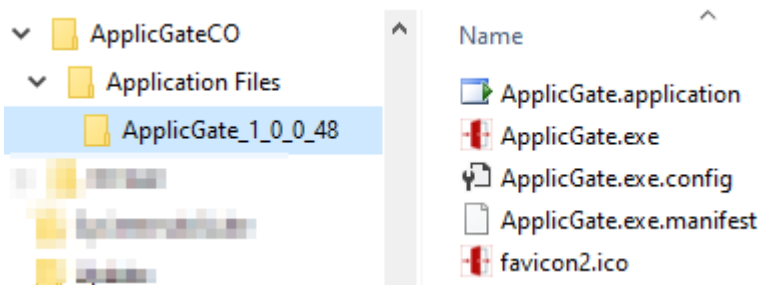
The advantage of this option is the easy installation and update of ApplicGate.
See also https://help.applicgate.com/helpmeCO.htm

ClickOnce is supported by the web browsers IE and Edge. For other browsers add-ins are available.
When using Edge for an initial installation, ClickOnce must be enabled: Enter
edge://flags/#edge-click-once
into the address field of Edge.

Following files must be offered at a web server, e.g. https://www.mycomp.com/ApplicGateCO :



The file ApplicGate.application references to the files stored in ApplicGate_1_0_0_48 or the current version of ApplicGate.



Now installation and start at the client is done via entering following URL into e.g. the Edge browser:
https://www.mycomp.com/ApplicGateCO/ApplicGate.application?server=vpn.testcomp.com:442&sslcc=Prompt:user1@testcomp.com&title=VPNclient&cifs

An entry in the start menu will be generated.

5.2.3 Start Parameters for the ApplicGate VPN Client

Required parameter:

- server=*node:port*... IP address or DNS name and port of the central ApplicGate server

For authentication one of these two parameters is required:

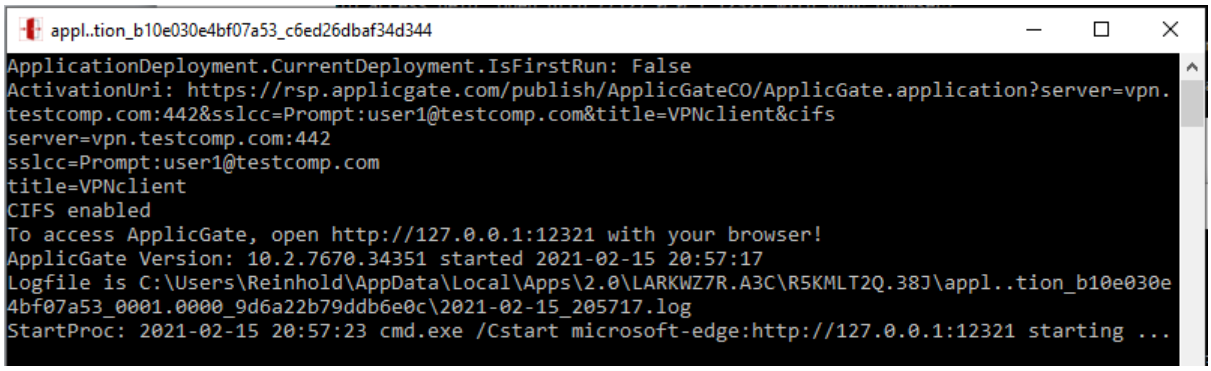
- sslcc=*sslccparameter* ... certificate selection, same parameter as for keyword SSLCC.
  If totp is not specified: default is sslcc=Prompt:*
- totp=[email][!SecurityID] ... use TOTP and specify optional default values, same parameter as for keyword TOTP

Optional parameters:

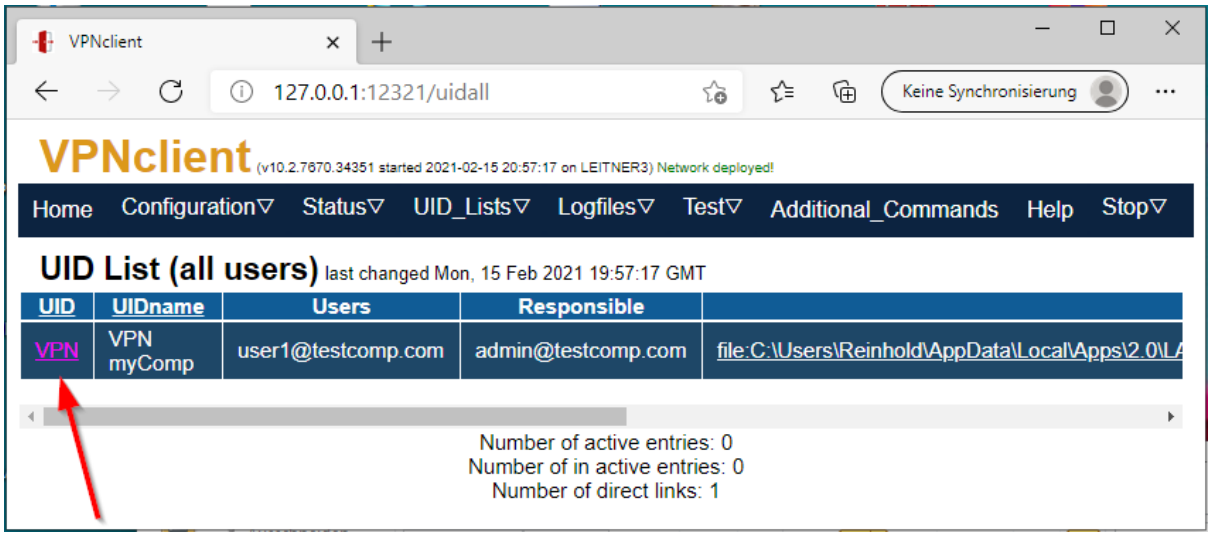
- browser=*browsername* ... start web browser: IE, Edge or Firefox (default is Edge)
- cifs ... same as keyword CIFS: Do not ignore rules with CIFS (IP port 445)
- defcmd=*command* ... default for sslcc is uidall (to see the uid list), default for totp is rouaum (to start the autologon session)
- log=*logvalue* ... one digit log level (0-4), if negativ: log will be shown in start window also and timestamps will be written (default is 1)
- manage=*ipaddress:port* ... address to manage ApplicGate, default is 127.0.0.1:12321
- proxy=*node:port* ... web proxy for connection
- rulenet=*rulenet* ... same as keyword RULENET: Used to construct first part of local IP addresses.
- scsh ... same as keyword SCSH: Use shortcuts from share, if path is defined (do not generate local shortcuts).
- title=*title* ... Title to display at the management interface

5.3 The ApplicGate VPN Client

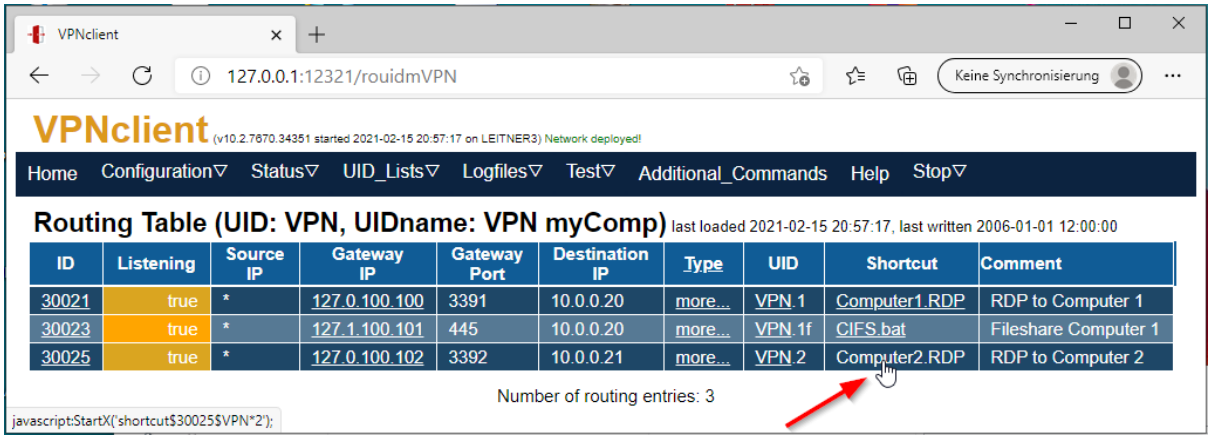
If the ApplicGate VPN client has been started as mentioned above a command window like this will show up:



Microsoft Edge will be started and following window will be shown:
Note: Microsoft IE and Firefox are supported also.



If you click “VPN” you will see all routing entries in detail:



To access the remote computer via RDP: click the Computer1.RDP or Computer2.RDP.
To map a network share of Computer 1: click CIFS.bat.

Remark: All shortcuts are generated automatically and are stored locally.

5.4 Start of ApplicGate VPN Client after Installation

Additional starts can be done via a start menu item or via the link as above.

To change the start parameters start the ApplicGate VPN client via the URL.

5.5 Stop of ApplicGate VPN Client

Use the Stop command in the Stop menu or terminate the command window.

5.6 ClickOnce Logging

For ClickOnce debugging turn on ClickOnce logging by definition of following registry keys:

To set a custom log file location:
1. Open Regedit.exe.

2. Navigate to the node
HKCU\Software\Classes\Software\Microsoft\Windows\CurrentVersion\Deployment
3. Set the string value LogFilePath to the full path and filename of your preferred custom log location.
This location must be in a directory to which the user has write access. For example create the following folder structure and set LogFilePath to
C:\Users\<username>\Documents\Logs\ClickOnce\installation.log.

To specify verbose log files
1. Open Regedit.exe.
2. Navigate to the node
HKCU\Software\Classes\Software\Microsoft\Windows\CurrentVersion\Deployment.
3. If necessary, create a new string value named LogVerbosityLevel.
4. Set the LogVerbosityLevel value to 1

6 Server Logon to ApplicGate

In this configuration there is no direct forwarding to the server.

The Intranet server has to log on to the ApplicGate VPN server to allow connections from the VPN client, like the server at the top in the schema above.

The VPN client can see the status of the Intranet server.

6.1 VPN Server

The routing entries have been change as follows:

ID	Listening	Source IP	Gateway IP	Gateway Port	Gateway IP2	Destination IP	Destination Port	Expiration	Type	UID	Comment
14	true	*	*	444	reverselogon	R2|R6	*	*	SSL:vpn.testcomp.com.pfx/vpntest, CCR:server*@testcomp.com, ISS:"CN=TestComp, O=Test Company", CHKCC	RSP	RSP Server
15	true	VPNclients1	*	3391	forward	server1@testcomp.com:R6%LEITNER4	*	*	UIDN:"VPN myComp!VPNclients1! https://vpn.testcomp.com:441/VPN", LDAC:yes	VPN.1 ~Computer1.RDP	RDP to Computer 1
17	true	VPNclients1	*	445	forward	server1@testcomp.com:R2%LEITNER4	*	*	LDAC:yes	VPN.1f ~CIFS.bat	Fileshare Computer 1
19	true	VPNclients1	*	3392	forward	server2@testcomp.com:R6%SERVER2	*	*	LDAC:yes	VPN.2 ~Computer2.RDP	RDP to Computer 2

The first routing entry allows the logon of the servers where the certificate matches server*@testcomp.com.

Rules R2 and R6 offered by the servers are accepted.

The next entries forward the connections from the client to the target computer (if logged on).

In this example SERVER2 (red) did not log on.

6.2 Intranet Server

Here are the corresponding routing entries (management entry is not listed):

ID	Listening	Source IP	Gateway IP	Gateway Port	Gateway IP2	Destination IP	Destination Port	Expiration	Type
20	true	autologon	R2|R6	*	*	10.0.0.3	444	*	LOG:1,TTL:6,SSLTARGET:vpn.testcomp.com, SSLCC:server1@testcomp.com.cer, RETRY:2
21	true	incoming	R2	*	*	127.0.0.1	445	*	*
22	true	incoming	R6	*	*	127.0.0.1	3389	*	*

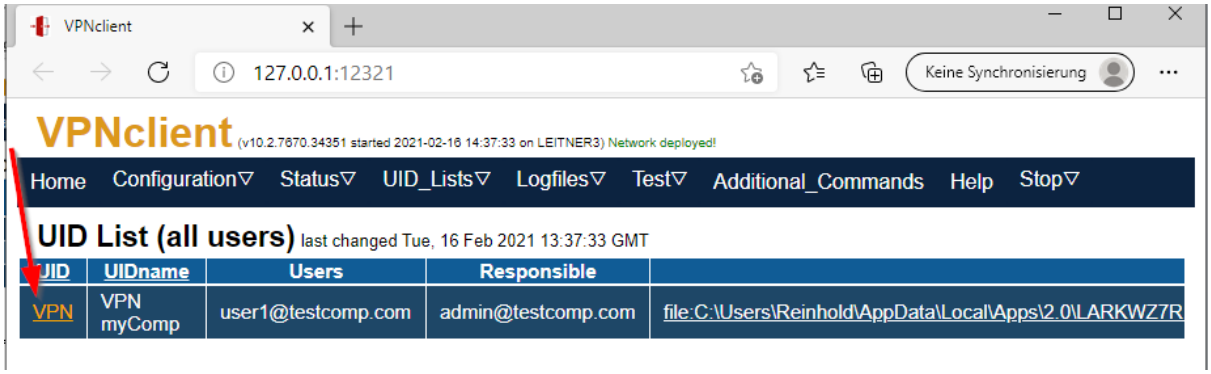
Via the first entry the Intranet Server logs on to the VPN Server and identifies itself using a certificate.

The other two entries implement the rules R and R6. In this case the incoming connections are forwarded to a local TCP port.

6.3 VPN Client

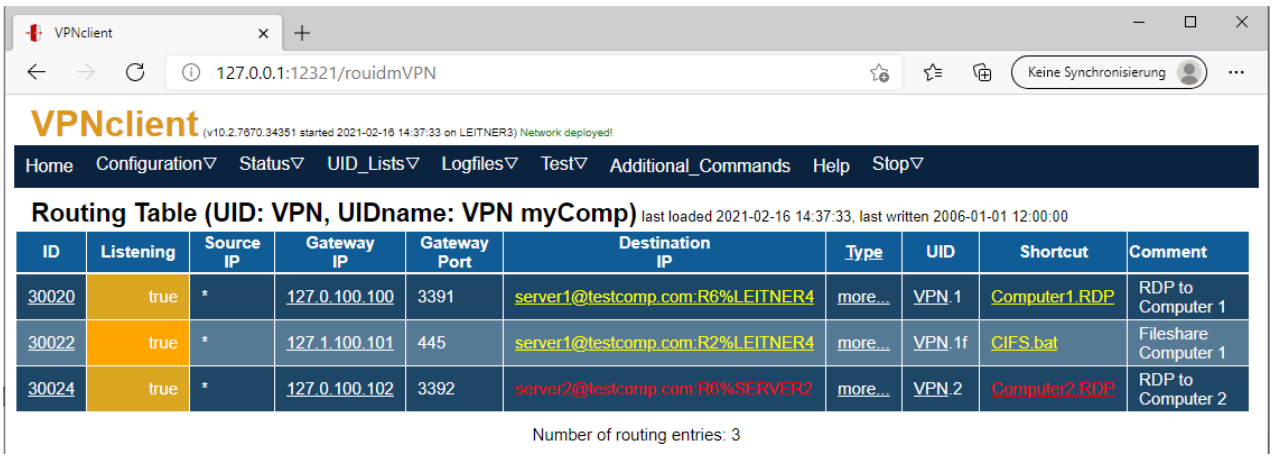
The advantage is now: The UID colour shows the status of the target computer:

- Magenta … Status unknown (direct link, e.g. site-to-site tunnel)!
- Yellow … All links are active!
- Orange … Some links are inactive!
- Red … No links are active



The colour of Destination IP and Shortcut shows the status of the target computer:

- Yellow … ready
- Red … inactive



7 Shortcuts with cmd and cmdb

The ApplicGate VPN client executes the specified commands locally.

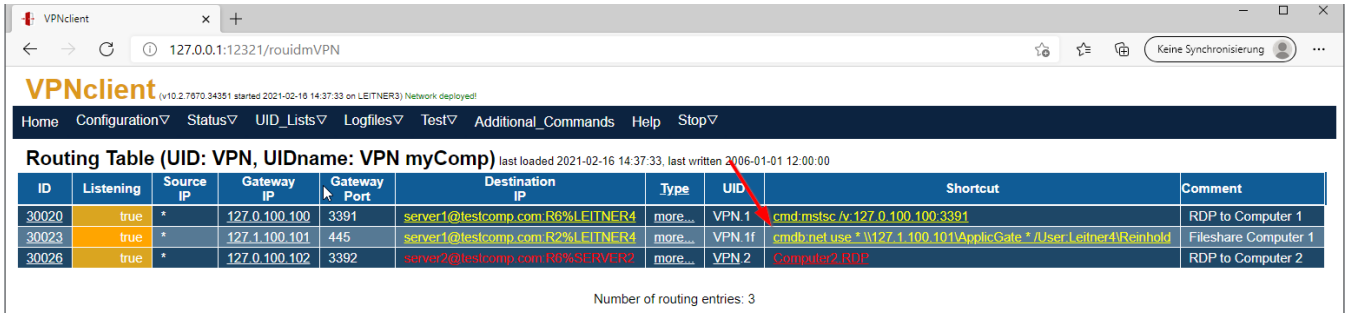
7.1 VPN Server

UID field with cmd and cmdb shortcuts to start RDP and map a network share:

- VPN.1~cmd:mstsc /v:%ip%:%port%
- VPN.1f~cmdb:net use * \\%ip%\ApplicGate * /User:Leitner4\Reinhold

7.2 VPN Client

IP address and TCP port are resolved:



UID	Shortcut	Comment
VPN.1	cmd:mstsc /v:127.0.100.100:3391	RDP to Computer 1
VPN.1f	cmdb:net use * \\127.1.100.101\ApplicGate * /User:Leitner4\Reinhold	Fileshare Computer 1
VPN.2	Computer2.RDP	RDP to Computer 2

8 Certificates for Authentication and Encryption

Any software certificate or smartcard is supported. Certificates can be obtained from various certificate authorities (CAs) or you can generate certificates of your own using e.g. OpenSSL or PowerShell scripts. See also https://help.applicgate.com/helpmeCE.htm .

8.1 Example to Generate Certificates using the PowerShell

- On Windows 10 Professional create a new directory.

8.1.1 Generate Server Certificate

- Download the PowerShell Script from https://help.applicgate.com/helpmePS.htm to this directory with name e.g. _NewServerCertificate.ps1
- Execute this script with PowerShell:
  The first time you will be prompted to enter the Subject and the Organization to generate a signing certificate (the CA certificate).
  Then enter the name of the server and the organization (domain).
  To export the certificate you have to enter a password.

```
*******************************************************
*            Generate server certificate              *
*                                                     *
```

```
* Example:                                              *
*   Input:                                               *
*     Server:  www                                       *
*     Company: test                                      *
*   Generates a certificate for server www.test.com      *
*                                                        *
* Hint:                                                  *
*  Server may be * to generate a wildcard certificate    *
*                                                        *
*    If the signing certificate could not be found:      *
*      A new signing certificate will be created.        *
*                                                        *
*     ApplicGate Network Security (C) January 2020       *
**********************************************************
Try to read saved hash of signing certificate from file CAsavedHash.txt ...
Saved hash of CA cannot be found or certificate not found. Generate new CA certificate? [Y/N]: Y
Generating CA certificate in certificate store CurrentUser ...
Enter Subject: TestComp
Enter Organization: Test Company
Following certificate will be used for signing:

   PSParentPath: Microsoft.PowerShell.Security\Certificate::CurrentUser\My

Thumbprint                                Subject
----------                                -------
E0C8203C48BE83A0633CC74BD7680446BA2C5B34  CN=TestComp, O=Test Company

Please enter following data to generate the user certificate:
Servername: vpn
Company: testcomp
Generating certificate for vpn.testcomp.com in certificate store CurrentUser\My ...

Following certificate has been generated:
5ACE52AF822F8901921EE38C6B9407EF734CB25A  CN=vpn.testcomp.com
Export server certificate? [Y/N]: y
Enter password for .pfx file: vpntest
Exporting  vpn.testcomp.com.pfx  ...

LastWriteTime : 31.03.2020 21:21:39
Length        : 2910
Name          : vpn.testcomp.com.pfx

Exporting  vpn.testcomp.com.cer  ...

LastWriteTime : 31.03.2020 21:21:39
Length        : 1090
Name          : vpn.testcomp.com.cer

Enter Return to exit:
```

- Note: The file CAsavedHash.txt contains the hash of the signing certificate so that it can be used later.

8.1.2 Generate Client Certificate

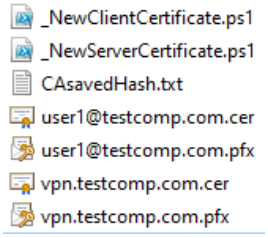
- Download the PowerShell Script from https://help.applicgate.com/helpmePC.htm to this directory with name _NewClientCertificate.ps1
- Execute this script with PowerShell:
  Then enter the name of the user and the organization (domain).
  To export the certificate you have to enter a password.

```
**********************************************************
```

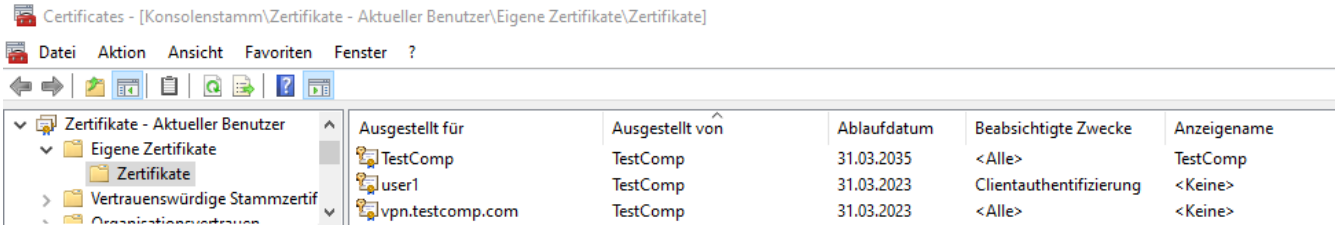
```
*             Generate user certificates               *
*                                                      *
*    If the signing certificate could not be found:    *
*      A new signing certificate will be created.      *
*                                                      *
*     ApplicGate Network Security (C) January 2019     *
********************************************************
Try to read saved hash of signing certificate from file CAsavedHash.txt ...
Following certificate will be used for signing:

   PSParentPath: Microsoft.PowerShell.Security\Certificate::CurrentUser\My

Thumbprint                                Subject
----------                                -------
E0C8203C48BE83A0633CC74BD7680446BA2C5B34  CN=TestComp, O=Test Company

Please enter following data to generate the user certificate:
Username: user1
Company: testcomp
Generating certificate for E=user1@testcomp.com,CN=user1,O=testcomp in certificate store
CurrentUser\My ...
TextExtension 2.5.29.17={text}Email=user1@testcomp.com&UPN=user1@testcomp.com

Following certificate has been generated:
336386629E3046709DA8A6ED7B3ED4F0C19CE576  E=user1@testcomp.com, CN=user1, O=testcomp
Export user certificate? [Y/N]: y
Enter password for .pfx file: userpw$
Exporting  user1@testcomp.com.pfx  ...

LastWriteTime : 31.03.2020 21:34:29
Length        : 3014
Name          : user1@testcomp.com.pfx

Exporting  user1@testcomp.com.cer  ...

LastWriteTime : 31.03.2020 21:34:29
Length        : 1194
Name          : user1@testcomp.com.cer

Enter Return to exit:
```

8.1.3 Generated Files

Content of directory:



Certificates in Microsoft certificate store (seen via mmc certificates):



9 Table of Contents