

Application connectivity

Even for the smallest company, accessing applications and data over the Internet is a routine procedure. When looking for an easy-to-use and secure remote access solution, Giritech's G/On system provides an innovative alternative to VPNs.

English translation of product review made by German magazine, LanLine (www.lanline.de) published in March 2009 issue. Translation by Giritech.

Typically, connections from home offices or mobile devices to the company's network are established using VPNs (Virtual Private Network) based on IPSec or SSL. This means that a direct connection between the nodes is created. Significantly, the technical and administrative operative expenses required to setup a VPN environment with DMZ, firewall, authentication server, certificate server, IPSec VPN terminator, SSL VPN applications and possibly intrusion detection systems (IDS) are high and require specialized skills. Also, because so much functionality is required, the DMZ degenerates into a secondary network, even though higher security criteria are in place.

Another problem when using IPSec VPNs is the installation of the clients themselves. Usually, administrative rights are required for setup, which means that they cannot be used instantly on any PC. Although installation efforts when using SSL VPNs are reduced to only setting up browser plug-ins, standard users are not always able to obtain these privileges. The G/On product by Danish company Giritech tries to elegantly avoid the setup problems of VPN accesses with their patented EMCADS technology (Encrypted Multipurpose Content and Application Deployment System).

G/On is server-based software which accepts requests from clients over a secure connection via only one single open port and passes them on similarly to a proxy server. Typically, the client software is launched from a USB key holding all the

required applications. What is so special about G/On is the connection itself. Instead of a classical VPN-/TCP connection, access is established in the application layer.

Easy installation

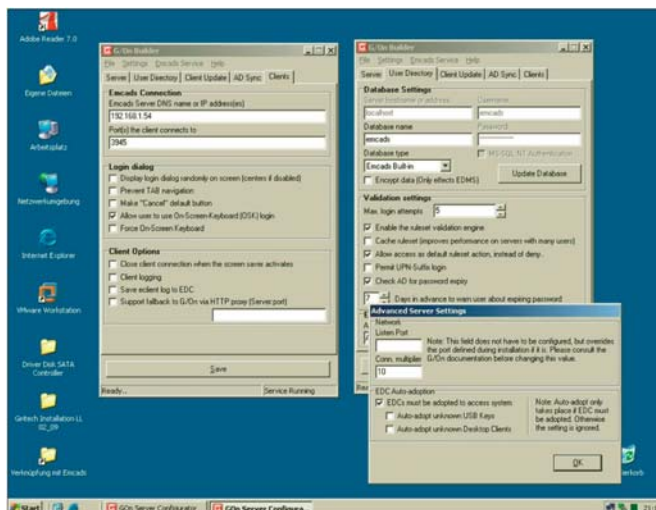
The testing package consisted of two 1 GB USB sticks, a German quick guide, one installation CD and a license key which was sent by email. All the material would easily fit into a box the size of a network card. The foundation for G/On is a Microsoft Windows server-2000-SP4 or Server 2003-SP1 server installation on typical standard hardware. The manufacturer recommends installation on a dedicated server - or on a proxy or terminal server. However it is not recommended to install the system on a domain controller or web server. The hardware recommendations describe a 3

GHz single core Pentium system with 512 Mbyte RAM for a maximum of 100 users and a dual core system with 3 GHz and 2 GB RAM for 500 users being active at the same time. Depending on the method of installation, a USB Token is required on the server side – we did however use a “tokenless installation”.

Setup itself was finished nearly instantly. Configuration and basic application setup took only just about half an hour during our test. The G/On admin dialog windows are largely self-explanatory and all one needs to do is go through the register tabs from left to right. Unfortunately, the user is not prevented from making faulty insertions – if one misses entering for example the public IP address of the G/On server, the software does not stop the user from finishing the configuration process. German G/On support however could narrow down to this particular problem within a few minutes during a phone session and after that, we could use the software as planned. All data such as access attempts, connection details or settings are stored in an included database. By request, it is possible to use an already existing MySQL or Microsoft SQL installation. Configuration starts with the creation of a private and public key. These can either be entered manually on the keyboard or –much easier – automatically created with a dedicated button. After that, general settings such as the administration account for G/On, destination paths and active directory access details are defined.

Synchronization with the active directory is optional and simplifies the availability in environments with a large number of users.

Some specialized settings such as disconnection of the data connection as soon as the screen saver goes active on the client PC can be selected using checkboxes. On the network side, only one important adjustment is required: one single



Before a secure connection between Client and server can be established, a configuration is required as usual. Contrary to VPN products, this is completed with G/On in about half an hour.

port, standard 3945, must be forwarded on the firewall to the G/On Server. This eliminates the need to position the server in the DMZ. It is even possible to utilize a dynamic DNS address in conjunction with

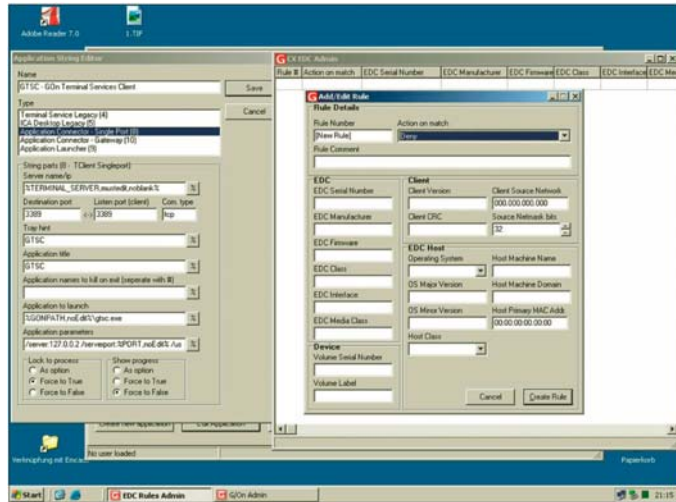
the company network, the USB stick can hold “portable applications” such as the Firefox browser. The stick we had for testing did offer sufficient space for additional applications with 1 GByte of memory.

The G/On client works with any computer running Windows 2000 SP4, XP, 2003 or Vista. Besides this, the client can be run on x64 Windows - not as native 64-bit application but as 32-bit WOW task. The development roadmap includes a client for Mac OS in the near future. Windows XP Embedded on Thin

software. Since the read only partition is used there is no possibility on the client PC to apply changes – neither for the user nor for applications. Tampering is revealed based on hash values of the files. Before any client can establish a connection with the server, an activation is required. This process is known as “adopt”. Unchangeable attributes of the client, or the worldwide unique serial number on the USB stick are used as identifiers. After the activation, which took only one minute in our test, the G/On Client establishes a connection to the G/On Server in order to identify the user by username and password.

So even a lost stick which was accidentally found, does not represent a security risk without knowing the access credentials. Furthermore, client installations as well as sticks can be deactivated with a single click on the server. In the Windows client tray, near the clock, a menu with the red letter “G” is displayed. Depending on the encountered zone, the predefined applications show up in this menu.

The entire communication is 256 Bit AES encrypted and is handled through one single port – virtually a port multiplexing. On the company’s network side, the G/On server – as a Proxy – takes care of the



Instead of a network connection, the client gains access to previously activated applications. Rules can be setup for groups or individual clients.

G/On. With this configuration, the setup of the server using “G/On Builder” is completed. The private and public keys should be stored in a safe location, because this information is – in conjunction with a special backup – required in order to restore G/On on a backup server.

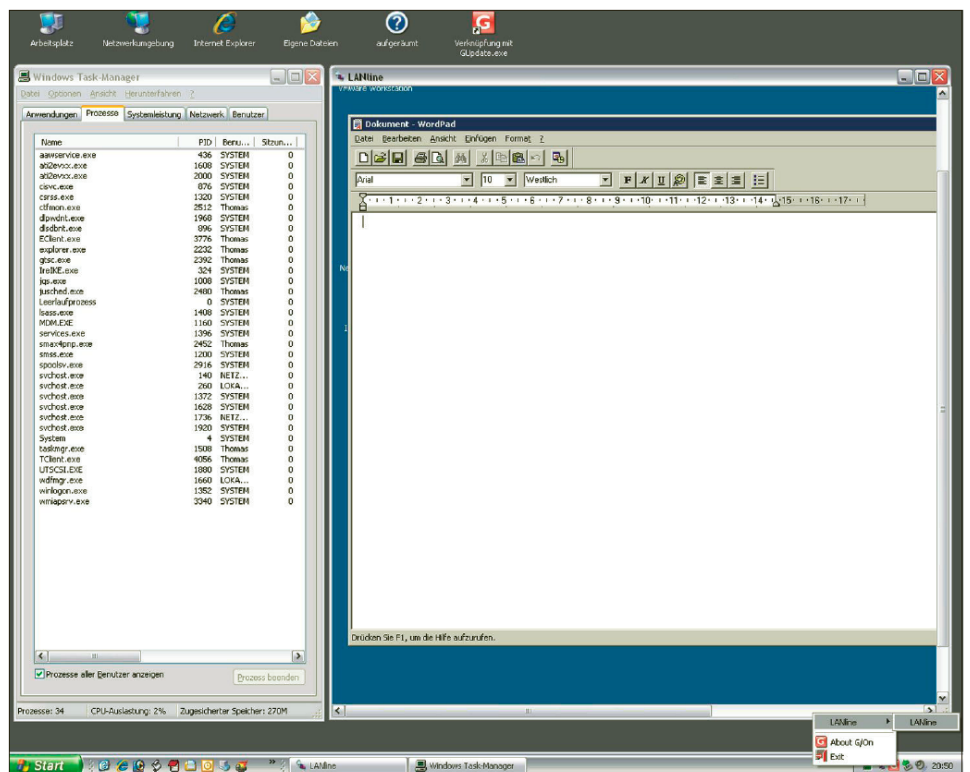
Unlike traditional VPN methods, G/On is a remote access solution with application connectivity. Respectively, applications such as terminal sessions for Microsoft RDP or Citrix ICA, browser connections to the intranet, Outlook, Navision, SAP, CRM or MS Dynamics must be approved in the menu structure of the “G/On Admin”. Depending on the use, it is also possible to assign individual ports for clients to specified target machines. In order to configure the applications one must know the required port and IP addresses or DNS names of the targets. Since the primary objective of the solution is to use the client on the USB stick, additional zone management can be found in the management console. Based on IP addresses, vendor- or server information, the software client can determine if it was activated in a “trusted” or “untrusted” network. This can then result in a different set of menu options.

Secure access via USB stick

Apart from the applications which are communicating over the connection with

Clients is already supported today, but devices from Hewlett Packard or Igel do require an administrative activation of the USB Token. Wyse Thin Clients support G/On without any configuration changes right out of the box.

The G/On client software can either be installed directly on the computer or on the dedicated G/On USB Stick. This stick, manufactured by Hagiwara, normally holds an invisible “read only” partition filled with the ISO image of the client



G/On Terminal session on the client computer: All required applications are stored on a special USB stick. The network connection is encapsulated for the individual application.

distribution of the data packages required by the applications.

The G/On Client is deliberately developed as a monolithic application. There are no DLLs, external files or registry information used from the client computer. Malware trying to take advantage of exploits is consequently unable to compromise the security of G/On. Additionally, the client software is compressed and encrypted to avoid reverse engineering. The client does not even rely on the memory and task allocation of Windows through the Microsoft Memory Manager but uses its own dedicated memory management.

The applications launched on the client via G/On communicate exclusively on the local loopback adapter of the machine with standard IP address 127.0.0.2. Therefore the client PC is never a member of the network which it is accessing. The G/On software only allows data packets to pass through the loopback in the direction of the G/On Server which originate from the desired and launched applications – “lock to process”. In our test it was for instance possible to access the test intranet in the LAN over <http://127.0.0.2> if the browser was launched from the G/On menu. If another browser instance is opened, trying to access the address, it only sees port 80 of the client PC.

Many internet connections are implemented using proxy servers. The latest G/On version supports “TCP over HTTP” and is therefore prepared for interaction with servers such as Microsoft ISA or JANA2 Proxy. Various optional modules, such as Wake on LAN for remote PCs, remote access or a connector for Novell eDirectory are available on demand.

Conclusion

It is really difficult not to get addicted to the charm of the red USB sticks. The fact that the EMCADS encryption and communication engine developed by Giritech is FIPS 140-2 certified does increase the sense of security even more. Price for one Business license for small and mid-sized companies starts at 835 Swiss Francs. One client license is offered for 238 SFrs and the USB Access Key is priced at 112 SFrs. Thomas Bär/wj

Giritech ist offizieller Partner von

T-City Friedrichshafen

Ein Gemeinschaftsprojekt der
Deutschen Telekom und der Stadt Friedrichshafen

GIRITECH®

Giritech GmbH

- Deutschland · Österreich · Schweiz -

Mariabrunnstrasse 123 · 88097 Eriskirch

Tel. +49 (0) 75 41 / 97 10 99-0

Mail: info@giritech.de

www.giritech.de