February 8, 2006

Cranite SafeConnect: A New Twist on VPNs

By David Strom
Founding Editor-in-Chief of *Network Computing Magazine*

Table of Contents:

If you absolutely need total control over your remote users, and need to run the widest possible range of applications, then the Cranite Systems Inc. SafeConnect VPN software should be in your short list of products to consider. SafeConnect is neither fish nor fowl, and sits squarely between SSL VPN and IPsec products, combining the ease of use of the SSL crowd with end-to-end applications interoperability of IPsec.

We took a close look at the various components that make up the Cranite SafeConnect v1.1 solution. This includes the SafeConnect Client v1.1, the SafeConnect Access Controller v1.1, and the Cranite Management System v1.1 software. We tested the product on a series of laptops and compared how it worked with SSL VPNs from Juniper, Nokia, and other major manufacturers. Overall, the product stood up well in these tests. We were able to support more applications than the SSL VPNs, owing to the fact that SafeConnect owns the entire connection and handles the protocol translation flawlessly.

Cranite takes some of the advantages from both approaches, and goes beyond the fledgling network-extension efforts that characterize the SSL space. SafeConnect will prevent eavesdropping over the remote connection no matter where and how your users connect, and it is easily setup in a few hours. It will support a wider range of applications and do so without any additional configuration required. It delivers extremely high file transfer throughput, way beyond any of the SSL VPN products. Finally, it is priced attractively at about a third to a half of what competitive SSL VPN products with equivalent feature sets would cost.

Cranite is like the Check Point SSL in that it comes as a software-only product. You need to install the gateway piece on any dedicated Intel-based PC -- it runs its own Linux-derivative OS. The only caveat is that you’ll need to have a machine with two network adapters. You will also need to install the client piece on each remote user’s machine.

Setup took us about two hours, and most of that time was spent understanding the lab network environment where we were doing the tests. The most complicated part of the whole process is choosing which authentication and authorization servers will be used in conjunction with SafeConnect product.

Currently, the company only supports Windows XP and 2000 users. Plans are in the works for Mac, Windows Mobile/CE and Linux clients. If you have a more heterogeneous network than XP/2000, this is not the product for you now.

There are several other things the product doesn’t do. It can’t and doesn’t try to compete with the SSL products for unmanaged remote users, since its client must be installed on each remote desktop or laptop. It doesn’t provide the level of client endpoint integrity checking that a Nokia, Juniper or F5 SSL product provides.

We liked the fact that once you were connected, your remote connection was solid and bullet-proof from man-in-the-middle attacks. We tried to break the connection by sending malformed packets with a bad MAC address – something that would bring down any SSL VPN connection – but SafeConnect kept on going without any problems. About the only way to tear down the connection would be to fill the pipe with a denial of service attack or if we lost the line entirely from our ISP.

SafeConnect has three major deficiencies: First, it doesn't prevent users with duplicate credentials from concurrently connecting to the network, and it doesn't report on these circumstances either. This puts a burden on your IT department to keep track of their client credentials. Second, there is no auditing ability, which we discuss more completely below. Finally, while the product comes with its own LDAP and RADIUS servers, if you do decide to use these pieces you will have to configure them via their separate command line interfaces. Cranite should integrate these into its own graphic configuration screens.

Let's look at eight major areas and see how the product stacks up against the leading SSL VPN players in terms of ubiquitous application access, security features, ease of use, performance and how it is used from various desktops and locations.

I. AUTHENTICATION

As we said earlier, SafeConnect comes with its own Open LDAP and Free RADIUS servers that can be used respectively for authorization and authentication. The SSL VPN products can use one or the other, but with SafeConnect, you must use both servers. However, you can substitute your own servers in the place of the two supplied by Cranite, but they must share a common set of user names between them for the product to work, of course.

Included in the base software install are five sample users that are useful for evaluation purposes. We had some trouble getting all the right parameters specified for our test network, and wished that Cranite had the same high-quality debugging tools that Nokia offers on its SSL VPN product to track down common configuration mistakes. Cranite does not support native Windows Active Directory Kerberos connections, you will need to setup a RADIUS intermediary.

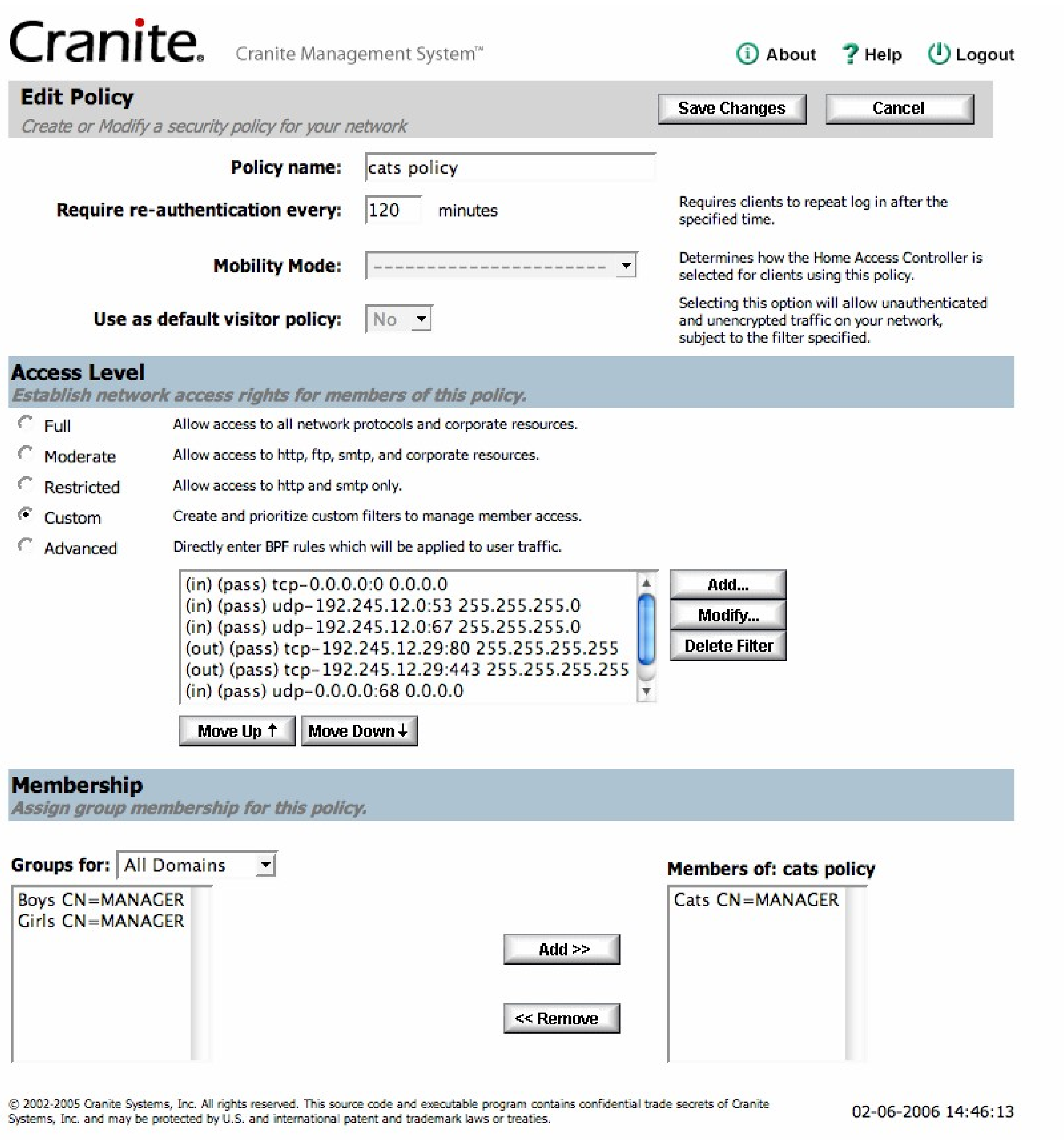
Obviously anyone doing this must have the network permissions and skills to set this up properly. As we mentioned earlier, if you do decide to use the supplied servers, you will need to set them up with separate command line utilities, outside of the graphical configuration screens.

We tested authentication using the RSA SecureID server and key fobs and it worked flawlessly, once we had set up the correct groups and configuration parameters on the Cranite server.

II. ACCESS AND POLICY CONTROL

Cranite's setup screens are less complex than Juniper's or Nokia's, and also less capable: for example, you can't restrict access by time of day for SafeConnect as you can with the two SSL VPNs. It is fairly easy to setup groups and access right lists. The trouble comes when you want to attempt to handle more fine-grained policy controls for particular applications. The design of the product is to allow a client complete access to the corporate network and its resources. Unlike SSL VPNs, which also must run some proprietary network extension client to have the same level of interoperability, with Cranite, once you are inside, you have access to everything that a local client would have.

Setting up policy controls is difficult and requires detailed understanding of firewall rules, protocols, and ports. A sample screen shot shows how you would handle the relatively simple case of restricting access to a particular HTTP server as an example: this required setting a series of separate rules and it took us several attempts to get it right.



Edit Policy

Create or Modify a security policy for your network

Policy name: cats policy

Require re-authentication every: 120 minutes — Requires clients to repeat log in after the specified time.

Mobility Mode: ---------------------- — Determines how the Home Access Controller is selected for clients using this policy.

Use as default visitor policy: No — Selecting this option will allow unauthenticated and unencrypted traffic on your network, subject to the filter specified.

Access Level

Establish network access rights for members of this policy.

○ Full	Allow access to all network protocols and corporate resources.
○ Moderate	Allow access to http, ftp, smtp, and corporate resources.
○ Restricted	Allow access to http and smtp only.
● Custom	Create and prioritize custom filters to manage member access.
○ Advanced	Directly enter BPF rules which will be applied to user traffic.

```
(in) (pass) tcp-0.0.0.0:0 0.0.0.0
(in) (pass) udp-192.245.12.0:53 255.255.255.0
(in) (pass) udp-192.245.12.0:67 255.255.255.0
(out) (pass) tcp-192.245.12.29:80 255.255.255.255
(out) (pass) tcp-192.245.12.29:443 255.255.255.255
(in) (pass) udp-0.0.0.0:68 0.0.0.0
```

Membership

Assign group membership for this policy.

Groups for: All Domains

Boys CN=MANAGER
Girls CN=MANAGER

Members of: cats policy

Cats CN=MANAGER

© 2002-2005 Cranite Systems, Inc. All rights reserved. This source code and executable program contains confidential trade secrets of Cranite Systems, Inc. and may be protected by U.S. and international patent and trademark laws or treaties.

02-06-2006 14:46:13

As we said earlier, you are not restricted to how many times you can connect from a single user ID, unlike Juniper and other SSL products that can enforce this access control. We tested this using the RSA key fobs providing our password for our user ID at two different laptops that were logged in concurrently. We think this a major drawback, and at the very least Cranite should report the multiple logins if not prevent the situation.

III. MANAGEMENT

We found the management screens of SafeConnect fairly easy to navigate and understand. There is no native SNMP support. Also, SafeConnect is just available in an English-language version only and the company does not plan on offering any additional language support. The configuration and management screens are accessed through a Web browser and are less confusing with fewer options than either the Nokia or Juniper SSL servers' equivalent screens.

IV. LOGGING AND AUDITING

SafeConnect's log is a simple affair. It lists all events by default, and while you can search and filter events, it isn't easy to do so and is there mostly for a debugging tool. There is no auditing capability in the product, but perhaps this is less important since it will be used in situations where all the remote users are managed by a central IT staff.

V. CLIENT SUPPORT

Like many of the network extension SSL products, you will need administrative rights to install the SafeConnect client. (Permeo/Blue Coat is one major exception to this.) However, once installed, it can be run from the user's individual account. As we said, only Windows 2000/XP clients are currently supported. We tested on both versions with no problems. The only issue was the built-in Windows XP SP2 firewall for testing the SSL products – but obviously Cranite was fine with this situation, along with supporting Zone Alarm as a firewall. And since it isn't an SSL product, it supports whatever browser configuration on the client you want to use.

VI. INTEROPERABILITY AND APPLICATIONS SUPPORT

Cranite supported more applications and did so more easily than any of the SSL VPN products, which is to be expected since they did not use the same proxy technology that these products use and can own the entire protocol stack from end-to-end. Still, testing these was almost a non-event, because there wasn't much to do – the applications just worked.

For example, we were able to get the SIP phone VoIP application X-Lite to work the first time without any specific configuration, which was problematic for the Fortinet SSL

VPN product and would only work with the SSL VPN products with their associated network extension clients.

SafeConnect was the only product to support IP v6 and did so with flying colors, without any additional configuration, other than adding v6 protocol support to our Windows client. None of the SSL VPN vendors can do this currently.

Finally, SafeConnect supported multicast networks without any specialized configuration. We used the Iperf client to pass multicast packets between two PCs, proving that companies looking to support multicast applications such as video servers could do so with ease with this product. We summarize the types of applications supported in the table below.

Supported applications:

	Cranite	SSL VPN products
Terminal services	Supported 100%	Requires network extension client or port forwarding
SSH	Supported 100%	Requires network extension client or port forwarding
Full SMB access	Supported 100%	Requires network extension client
Web Services	Supported 100%	Requires proxy
Citrix services	Supported 100%	Requires network extension client or port forwarding
KVM over IP	Supported 100%	Requires network extension client
VoIP/SIP telephony	Supported 100%	Requires network extension (except Fortinet)
IP v6 support	Supported 100%	Not supported
Multicast support	Supported 100%	Not supported

VII. END POINT SECURITY

What Cranite excels at is maintaining the remote connection no matter what a hacker might try to do to interrupt, snoop, or confuse the situation. A single malformed packet can bring down any of the SSL VPN connections, but SafeConnect is more robust.

Once SafeConnect is loaded and logged in to the network, it provides end-to-end security for the connection. However, one of the issues for corporate IT administrators is keeping track of where their laptops have been and the possibility of infection when they are outside of the corporate network. Cranite does a great job of protecting them from infection when their client is running and connected to the corporate network, but once disconnected, anything goes and the laptop is vulnerable. Unlike many of the SSL products, SafeConnect does not scan the client for some minimum set of security software such as anti-virus and anti-span before allowing a connection. F5 in particular has the greatest end-point security enforcement policies, and we wish that Cranite would adopt a similar visual policy editor type of model.

We used NMAP to search for open ports on the remote client. When SafeConnect was running, it not only masked all open ports and blocked any attempts at showing any services, but didn’t even show that the remote PC was connected to the network. This is a unique advantage for Cranite and something that neither the IPsec clients nor SSL VPN products offer.

VIII. PERFORMANCE

We tested FTP transfers on SafeConnect and compared them to several SSL clients and found it to have exceptional performance and without any special configuration required to support FTP too. The F5 client includes their own compression algorithms for FTP, Nokia and Nortel use standard TCP FTP transfers, and Juniper uses the IPsec ESP protocols for the transfer. We used a standard Windows FTP command line session to move a single file between server and remote user for both an uncompressed text file and a binary compressed file of 10 MB. As you can see from the results below, the Cranite solution was about ten times faster than any of its competitors in moving data through its connection.

File Transfer Performance

Test Description	Text Transfer (kB/s)	Binary Transfer (kB/s)
F5 TCP/FTP get (with compression)	200	200
F5 TCP/FTP put (with compression)	559	560
Nokia TCP/FTP get	155	156
Nokia TCP/FTP put	127	125
Nortel TCPP/FTP get	89	82
Nortel TCP/FTP put	52	51
Juniper ESP/FTP get	111	110
Juniper ESP/FTP put	52	52
Cranite TCP/FTP get	3365	3392
Cranite TCP/FTP put	3301	3234

BIO:

David Strom is the former editor-in-chief of Network Computing and Tom’s Hardware, has written two books and thousands of magazine articles for technical and general interest publications and Web sites. He runs his own network consultancy in Santa Monica, Calif. and can be reached at david@strom.com. This review was sponsored by Cranite Systems and represents an independent analysis of the product.