



## Is your Virtual Private Network really private?

Modern organizations are increasingly spread out geographically with the offices around the globe, employees working from their homes and travelling around. This has given rise for a need to provide efficient remote access methods to the company's information systems. Virtual Private Networks (VPNs) are usually used for this purpose because of their cost-effectiveness and support for mobility. VPNs carry data over the public Internet, and as such, are cheaper and more flexible compared to private physical lines. With VPN technologies, a secure tunnel across Internet is created from the client computer into the internal network of the company and communication is typically encrypted for further privacy.

**As attractive as a VPN may be, it is also a big security challenge for an organization.** VPNs are often used for accessing the services of internal network and the data carried over it can be highly sensitive. A breach in security can go unnoticed for a long time since attacker may appear to be a legitimate user. Furthermore, the protocols comprising typical VPN implementations are many and complex, giving a lot of opportunities for implementation and configuration errors.

**It has been estimated that as many as 90% of remote-access VPN's have exploitable vulnerabilities**

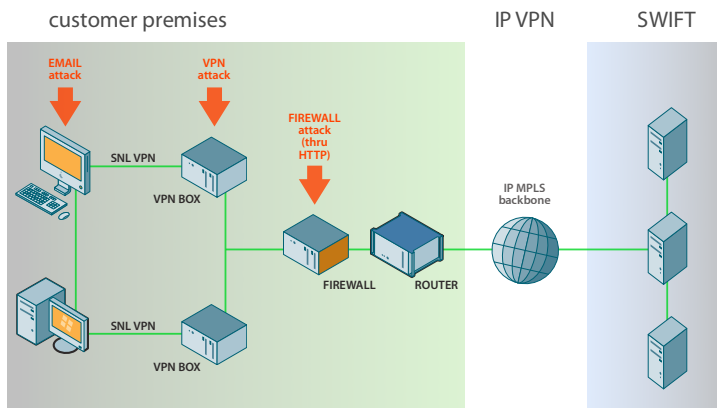
(<http://esj.com/security/article.aspx?EditorialSID=1291>). A common method of attack is to craft a malformed protocol message that will cause unwanted behavior like buffer overflows or denial of service in firewalls, VPN servers or other security devices. During past couple of years several vulnerabilities of this type have been found from VPN related protocols like IKE/ISAKMP, SSH and SSL (<http://xforce.iss.net/xforce/alerts/id/163>, <http://secunia.com/advisories/22091>, <http://xforce.iss.net/xforce/alerts/id/168>). One example of vulnerabilities in this category is an ISAKMP-related buffer overflow in a particular VPN server product (<http://xforce.iss.net/xforce/alerts/id/163>). **Remote attackers could exploit this vulnerability to completely compromise the security of the affected product and gain super-user level privileges.**

As a summary of the potential threats, chances are that what should be the strongest link in organizations information security can, in fact, be the weakest one.

**Codonomicon DEFENSICS provides automated black-box robustness testing tools for finding and preventing the reliability and security problems.** The DEFENSICS testing methodology is based on systematic simulation of possible attacks. The system under test is subjected to protocol messages that are automatically mutated based on heuristics that have been proven to find flaws from different failure categories. Codonomicon tools include the complete simulation of the tested protocols, which enables full state coverage, not just testing of the initial messages. Full state coverage combined with the automatic mechanism for crafting malformed messages guarantees maximum breadth and depth in testing.

VPN servers can terminate various protocols, including ISAKMP/IKE, IKEv2, L2TP, PPTP and IPSec. Should there be a vulnerability that allows the exploitation beyond the denial of service, the whole protected network could be exposed for an unauthorized access. Codonomicon covers test solutions for over 100 interfaces and the DEFENSICS VPN testing solution includes testing facilities for all aforementioned protocols and also for SSH1, SSH2 and TLS/SSL. With the DEFENSICS VPN test solution, vulnerabilities related to the VPN implementations can be found and eliminated proactively. For example, the VPN server vulnerability discussed earlier could have been detected with DEFENSICS VPN tests.

A practical example of highly critical system where VPN security plays a big role is on SWIFTnet, a network commonly used in banking industry to handle messaging and transactions. As the picture below illustrates, a compromised VPN box (while not the only potential attack surface) would pave a way to the very core of protected network. Running DEFENSICS test suites against the potential attack surfaces is the efficient way to ensure the security of a VPN system prior to deployment.



One possible SWIFTnet configuration

CODENOMICON Ltd.

Tutkijantie 4E  
FIN-90570 OULU  
FINLAND  
+358 424 7431

101 Metro Drive  
Suite 660  
San Jose, CA 95110  
UNITED STATES  
+1 408 392 9000

info@codenomicon.com  
www.codenomicon.com