

UserGate in Banks – Full-Scale Protection of Affiliated Corporate Networks from External Threats



Information protection is a number one priority for the modern banking system: confidential information leaks, data destruction and garbling, misappropriation funds from clients' personal accounts and failures of computer systems are threats caused by viruses, malicious software and hackers' attacks. In view of this, full-scale Internet access control and protection of financial organizations' corporate local area networks have become vitally important.

The vulnerability of banks' computer systems is confirmed by daily incidents of misappropriation of bank card details followed by illegal financial operations, more frequent attacks on Internet banking systems, etc. It is also demonstrated by the substantial financial damage caused to banks by viruses and instances of unauthorized access. Analysts report that the annual amount of such damages comprises billions of dollars.

According to Panda Security¹, Trojans posed the most serious threat for banks in 2008. The main purpose of this software is the theft of victims' bank details to obtain access to their accounts.

According to Panda Security¹, Trojans posed the most serious threat for banks in 2008. The main purpose of this software is the theft of victims' bank details to obtain access to their accounts.

Scrupulous management of employees who access Internet resources through corporate LANs plays an important role in full-scale bank information protection management. Research indicates that more than 80% of the world's leading financial organizations seek ways to control the actions of their employees to avoid the abuse of a company's resources and prevent possible information leaks and potential insider activity.

Information networks of banking organizations have a special nature due to the need for permanent-protected Internet access, required for the online exchange of confidential information between the bank's branches. Another aspect is the use of specific Internet applications for interbank operations, access to shared resources, data collection and processing, clients' online access to their accounts, and many other tasks.

Stable and Protected Internet Access

Banks need uninterrupted and stable Internet access to maintain quality operation, as the client services of banks largely depend on the Internet channel. As a rule, to ensure continuous operations, banks simultaneously use services of several Internet providers that can guarantee the required data transfer speed and quality of access.

However, to avoid potential network failures, loss of information and delays in the operation of banking applications when switching from provider to provider, banks need reliable software that permit the trouble-free transfer of the bank's operations and services from one Internet channel to another.

¹ Panda Security 2008, http://www.pandasecurity.com/resources/pro/02dw_Annual_Report_Pandalabs_2008.pdf

The UserGate Proxy & Firewall software solution offered by Entensys Corporation is a tool for Internet access management that permits work with two or more providers simultaneously. If more than one Internet connection is available, the Backup Channel function can be used.

This function allows the automatic transfer of all users to an alternative Internet connection if the main Internet channel fails. Connection to the main channel is restored automatically as soon as it comes back online, which enables uninterrupted Internet access for the bank's employees and the stable operation of all banking services.

Besides, multiple channel support function provides the capability to grant Internet access to different users via different providers' channels. This helps optimize LAN loading and ensure the proper distribution of web resources among the bank's employees.

System administrators may choose one of the available anti-virus modules or enable both modules for maximum protection. Anti-virus modules examine all incoming HTTP, FTP, SMTP and POP3 traffic. UserGate anti-virus protection can be also complemented by a third virus scan software protecting the file system on a local PC.

The next step of Internet access security management is anti-virus filtering and protection of a bank's servers from possible hacker attacks and the unauthorized access to confidential information.

UserGate's built-in firewall ensures protection of a bank's LAN from unauthorized access from outside networks and at the same time, provides the capability to access local resources, such as mail server, web-server or VPN-server in the local area network.

Anti-virus traffic protection is the key to ensure the safe operation of banking communications. UserGate proposes a double-gate virus check of all traffic by means of integrated anti-virus modules from Kaspersky Laboratory and Panda Security.

System administrators may choose one of the available anti-virus modules or enable both modules for maximum protection. Anti-virus modules examine all incoming HTTP, FTP, SMTP and POP3 traffic. UserGate anti-virus protection can be also complemented by a third virus scan software protecting the file system on a local PC.

This approach guarantees full-scale protection of a bank's LAN from virus activity and common network attacks and provides total security of local corporate resources and confidential information possessed by financial organizations.

Secure Communication between Branches

A bank's geographically remote branches need to use a well-tuned and protected communication system that enables prompt information exchange and shared access to corporate resources. VPN connection is a perfect solution for this purpose as it allows remote-protected access through web channels to database, FTP and mail servers. Essentially, the technology is capable of protecting web traffic of any intranet and extranet information systems, audio and video conferences and electronic commerce systems.

UserGate supports data transmission via PPTP and L2TP protocols to enable communication between a VPN-server and VPN clients within a given LAN. Besides, there is a capability to share network resources, which allows remote access to a VPN-server.

In summary, this technology can help build a system of information exchange between a bank's remote offices, provide protected access to shared client bases, financial reports and other confidential internal corporate information, as well as enable remote external access of the bank's employees to the bank's servers and information stored in the LAN.

Control of Employee Actions

Prosperity, reputation and success of any bank are based on the work of its employees. User action control and restriction systems have been long employed by banks and other financial organizations in the management of their local area

networks. The need for their use is primarily conditioned by certain aspects of the banking system's security concept and the plans to reduce a bank's direct and indirect costs associated with the use of web resources and the employees' working hours.

Traffic filtering has become an important trend in controlling bank employees' work. It helps deny access to non-work-related and potentially dangerous web sites that can cause infection of a bank's LAN, excessive consumption of traffic and abuse of the budget allotted for the Internet.

UserGate offers an advanced approach to the filtering of bad sites by letting system administrators block entire categories of undesirable web sites, such as "Online Dating," "Social Networks," "Travelling," etc. Filtering tools employed by UserGate lets an administrator use a constantly updated database containing over 450 million web sites on all the world's languages grouped into 70 categories.

The major disadvantage of primitive traffic filtration by URL or domain name addresses is that you need to know the addresses of the sites you want to restrict or block access to, as well as constantly update and replenish the lists of blocked sites manually.

UserGate offers an advanced approach to the filtering of bad sites by letting system administrators block entire categories of undesirable web sites, such as "Online Dating," "Social Networks," "Travelling," etc. Filtering tools employed by UserGate lets an administrator use a constantly updated database containing over 450 million web sites on all the world's languages grouped into 70 categories.

This traffic filtering system is focused on covering Russian-language web sites, which makes it a perfect choice for Russian banks and other financial organizations.

The next stage of managing Internet access from a bank's LAN is focused on controlling active Internet applications. UserGate lets the administrators create a bank's corporate policies governing the work of particular applications accessing the Web. For example, the use of ICQ or P2P networks at workplaces can be banned or restricted unless they are required for effective work. Additionally, UserGate has a capability to deny the use of older versions of applications: the administrator may choose to deny the use of Internet Explorer versions older than IE8.

Setting these flexible restrictions and denials, a bank can guarantee that its employees accessing Internet via the bank's LAN will use web resources for the right purposes.

Reduction of Internet-Related Costs

Internet-related costs are fairly high for banks and many other organizations. The use of traffic statistics and billing systems can help save substantial amounts of money on Internet access. Traffic statistics tools are a way to know which web resources users visit and which files they download and help determine which part of the traffic is not related to work and should be restricted.

UserGate contains tools that help analyze the visited and downloaded web resources and present complete reports in tables and diagrams.

Billing systems, in their turn, help create different plans of Internet access, set the allowable cost of traffic and assign flexible limits of maximum costs, both in money terms and traffic size.

UserGate's integrated billing system allows creating plans based on a provider's rates or depending on the specifics of work: administrators can set the allowable cost of traffic based on such criteria as the time of day, day of week, public holidays, etc.

Banks that use UserGate Proxy & Firewall solution show a 40% reduction of Internet-related costs.



Conclusion

Only comprehensive and full-scale solutions can guarantee the proper security of Internet access for a bank's employees. Full-scale security software is a convenient tool because in addition to ensuring the total security of your local area network and reducing traffic costs, it gives you a full picture of employees' Internet activity through a variety of reports, which makes personnel management and labor productivity development so much simpler.