



Making IP Multicasting Secure

IP multicasting is an efficient way to deliver feeds, but it also poses a number of security risks

August 2003



Where the source of multicast services is external, it will dynamically open holes within the firewall. Whilst the shared model avoids this, it does allow the multicast to move across internal subnet boundaries and may also compromise the corporate intranet. If your company has different access levels and degrees of protection, your security policy could end up looking like Swiss Cheese.

Using an IP network for the real-time transmission of information has become increasingly popular over the last few years. The commoditisation of bandwidth has seen prices fall dramatically and become extremely competitive compared with leased lines, while the development of protocols such as Resource Reservation Protocol (RSVP) means that true quality of service (QoS) can be implemented. It has now become an ideal transport mechanism for all manner of feeds which are needed “on-tap,” such as news and financial information. Furthermore, improvements in both performance and security mean that it can also be used for software updates and distributing corporate information.

But however fat your pipe is, you still have to be prudent as to how much bandwidth you use. An IP unicast, in which the feed is sent to one person, may be the best method if only one person has subscribed. However, services such as news and financial feeds tend to have rapidly increasing subscription bases, and a unicast to fifty people in a company means that the same feed – and bandwidth usage – multiplied fifty times.

An alternative is an IP broadcast: the feed is only sent once but is available to everybody, whether they want it or not. But this is even more bandwidth hungry, because the feed must cover the entire network, which means crossing subnet boundaries and eating up processing time on routers and switches.

Perhaps the most efficient method is an IP multicast. The feed is sent to a multicast address within the network, and those users who wish to receive it simply “tune in” to that address.

Unfortunately, there is a downside to the technology, and unsurprisingly, this is the security aspect. With a unicast or broadcast, the network administrator can ensure a secure, policed gateway through the corporate firewall. They know the recipient if it is unicast and can track the progress, behaviour and content of the feed at every point across the network. Even where the feed is routed multiple times, the administrator can ensure safe and secure updates of all routing tables, and in a multi-zoned firewall environment, grant the necessary access privileges. With IP broadcasting the situation is similar, if a little more time consuming.

With multicasting, the position becomes far more complex. Multicasting works by creating a distribution tree through the target network. Where the source of the information is external to the network, it will navigate the shortest route through the network, via a single branch for each user, to recipients’s in-boxes. Although this is fast, it is also heavy on network resources, so a sharing model can be set up instead to eliminate this problem. Sharing relies on an rendezvous point set up within the network which directs incoming traffic to users by the most efficient route.

However, the network administrator doesn’t actually have any control over who joins the multicast if the source is within the network. Users are

effectively setting their own security access – and also affecting the security access of the multicast. Where the source of multicast services is external, it will dynamically open holes within the firewall. Whilst the shared model avoids this, it does allow the multicast to move across internal subnet boundaries and may also compromise the corporate intranet. If your company has different access levels and degrees of protection, your security policy could end up looking like Swiss Cheese.

Even if the multicast is harmless – and the chances are if it comes from a trusted source, such as Reuters or Bloomberg – there are two vitally important security considerations. Firstly, it makes a mockery of the enforcement of the corporate security policy. This isn't just a matter of personal or professional pride: it can have serious implications for any security or quality accreditation that your company has, and may possibly require to do business with other companies.

Secondly, as these holes open and close, there is a risk – and with today's scanning tools, a very high risk – that something or someone else may piggy-back the multicast and gain access to your network. And by this time, the multicast, believing itself secure behind the firewall, may have compromised your internal network security as well, leaving corporate data there for the taking. And if you are a financial organisation, the penalties for such information getting out can be severe indeed.

This is clearly a situation where having a firewall simply isn't sufficient. The majority of firewalls effectively become transparent if multicasting is in progress. So what options do you have? Since banning all forms of multicasting completely is hardly realistic, one way is to forbid dynamic multicasting; that is, stop users from adding themselves to multicast distribution lists without authority. By confining your network to static multicasting, the responsibility for maintaining and monitoring the router tables once again falls under the control of the administrator. The multicast's direction tree can be kept under control and guided away from those subnets that contain sensitive information. This also has the added attraction of allowing fine-tuning of network performance, since the tree can be banned from overworked areas of the network.

But this also has its disadvantages. In a large company, constantly updating the routing tables and access privileges can quickly become a full-time job, which isn't really viable. And it also depends on the source of the multicast remaining the same: if the IP address of the source is dynamic, ensuring transparent yet secure access at the firewall becomes virtually impossible. The situation becomes a complete nightmare if you factor in clustered firewalls with multiple ISPs – at this point the administrator will probably give up and walk away!

But while security will obviously be an issue for some time to come, if you take a few basic steps, the risks can be minimised. By only accepting feeds from trusted – and static – sources, policing access to the feed, and ensuring that you have a firewall which can be carefully managed, you can enjoy the benefits of IP multicasting without the fear of a security breach.

About the Stonesoft Corporation

Stonesoft Corporation, founded in 1990, is a worldwide software company, with international headquarters in Helsinki, Finland; Americas headquarters in Atlanta, Georgia; and Asia Pacific regional headquarters in Singapore. Stonesoft provides enterprise-level network security and high availability clustering technology for companies deploying business-critical network applications on Internet and mobile servers. Stonesoft's StoneGate is a firewall and VPN solution providing advanced security, dynamic load balancing and high availability. StoneBeat® clustering products provide the same functionality for third-party firewalls, Web, content scanning, domain name and cache servers in wired and wireless environments. All of Stonesoft's solutions are designed to *Enable the Secure, Highly Available Enterprise*™.

Trademarks and Patents

StoneGate is a trademark of Stonesoft Corporation. Multi-link technology, multi-link VPN, and the StoneGate clustering technology as well as other technologies included in StoneGate are protected by pending patent applications in the U.S. and other countries. All other trademarks are property of their respective owners.

Copyright and Disclaimer

Copyright © 2000-2002 Stonesoft Corporation. All rights reserved. This documentation and related products are protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this document or related products may be reproduced in any form, or by any means without written authorization of Stonesoft Corporation. All rights, title, and interest in the product shall remain with Stonesoft and its licensors. The information in this document is subject to change without notice. If you find any problems with the documentation, please report them to us in writing. Stonesoft Corporation does not warrant that this document is free of errors. Statements contained in this text, other than historical information, include forward-looking statements, are based on current expectations, and involve risks and uncertainties.

International Headquarters

Stonesoft Corp.
Itälahdenkatu 22 A
FIN-00210 Helsinki
Finland
+358-9-4767 11 tel
+358-9-4767 1234 fax

US Headquarters

Stonesoft, Inc.
115 Perimeter Center Place
South Terraces, Suite 1000
Atlanta, Georgia 30346
+1-770-668 1125 tel
+1-770-668 1131 fax

United Kingdom

Stonesoft
Wyvols Court, Swallowfield
Reading, Berkshire RG7 1WY
UK
+44-118 988 0270 tel
+44-118 988 0369 fax