On the Design and Implementation of Structured P2PVPNs

David Isaac Wolinsky, Kyungyong Lee,
Yonggang Liu, P. Oscar Boykin, Renato
Figueiredo
University of Florida
{davidiw, klee, yonggang, boykin,
renato}@acis.ufl.edu

Linton Abraham
Clemson University
labraha@clemson.edu

ABSTRACT

In recent years, P2P VPNs have become quite popular by allowing users to connect directly with each other bypassing the overhead of communicating through a third party proxy. These P2P VPNs still require connecting to a central server for authentication, NAT traversal, and proxying in the off chance NAT traversal fails. While this significantly improves upon classical, centralized VPNs, this approach now requires ether maintenance of all-to-all connections during run-time or the involvement of a centralized authentication entity for each live connection attempt. For this solution, we propose a completely run-time decentralized P2P model based upon a structured P2P system. In this paper, we will describe the components of this model and describe and evaluate our reference implementation. A decentralized P2PVPN has an intuitive and simplistic setup, reduces the requirements for connectivity, offers better proxy selection in lieu of NAT traversal, and provides an opportunity for more intuitive trust solutions. For evaluation, we will compare system and networking overheads of the different VPN technology focusing on latency, bandwidth, CPU, and memory.

1. INTRODUCTION

A Virtual Private Network (VPN) provides the illusion of a Local Area Network (LAN), namely direct communication, over a wide area network such as the Internet while guaranteeing secure and authenticated communication amongst participants. Common uses of VPNs include accessing company or academic network resources while traveling abroad, playing LAN based video games over the Internet, connecting distributed resources from multiple sites, and securing your Internet traffic while in unsecure locations.

In the context of this paper, the focus will be on VPNs that provide connectivity between individual resources and so all resources that need symmetric connectivity will need to be configured to the VPN. While traditional VPNs enable such distributed connectivity they do so at the cost of maintaining a central server, which becomes the conduit for all traffic, becoming a performance bottleneck and potentially removing end-to-end security.

To that end, there have been three directions 1) support for multiple VPN servers for a single VPN [5], 2) the use of P2P connections for bypassing central communication that rely on run-time central authentication [3, 4], and 3) the use of unstructured P2P networks to form VPNs based upon shared secrets without user authentication and limitations on network size [2, 1]. In this paper, we present a novel approach to forming VPNs supporting large VPN systems with user authentication through the use of Structured P2P systems that have no reliance on centralized systems after initialization. Structured P2P technology enables users to communicate directly with all users without knowing anything beyond their virtual IP bypassing the need for centralization while providing all-to-all communication without maintaining all-to-all connectivity with participants. Interesting possibilities of P2P include efficient wide area multicast, data distribution, storage, chat applications, and even IP connectivity.

Current generation P2PVPNs do not provide features such as full-tunneling of network traffic, such as forwarding Internet traffic, nor do they have efficient mechanisms for multicast or broadcast. P2PVPNs rely on direct connectivity and in general will not work if NAT (Network Address Translation) traversal between peers is unsuccessful.

The problems we seek to address with our P2PVPN model include:

- reducing the role of centralization for user authentication in a VPN
- supporting full-tunneling of Internet traffic in a P2P system
- handling relay selection in lieu of unsuccessful NAT traversal
- supporting multicast and broadcast communication

A rudimentary overview of our solutions to the above problems follows and will be covered in depth in the rest of this paper. To provide fully decentralized run-time connectivity, we use an automated certificate authority based upon the use of user groups. In the case of full-tunneling, P2PVPNs introduce significantly more complexity since a simple routing table swap as done in central VPNs no longer work, as such we investigate three different mechanisms for tunneling all Internet traffic to our full-tunnel endpoint(s) besides our P2P traffic. When nodes cannot directly communicate, they seek to connect to peers that are mutually physically close to each other and use them to relay communication. For efficient multicast and broadcast communication, we rely on the use of bootstrapping a private P2P system whose members are only participants of the VPN.

Explicitly, our contributions made in this paper are:

- automated group-based certificate authority
- three different approaches to configuring full-tunneling

SC09 November 14-20, 2009, Portland, Oregon, USA
(c) 2009 ACM 978-1-60558-744-8/09/11 $10.00.

- intelligent selection of relays
- use of a private P2P VPN system bootstrapped of a general P2P system

The rest of this paper is organized as follows. Section II gives an overview of current VPN technologies and the efforts to decentralized. Section III introduces P2P structures and our previous work IPOP (IP over P2P). Section IV describes the contributions of this paper, namely a feature-full P2PVPN. In Section V, we discuss our implementation and present evaluation comparing centralized, P2P, and our VPN. Finally, we give some concluding remarks in Section VI.

2. VIRTUAL PRIVATE NETWORKS

3. STRUCTURED PEER-TO-PEER SYSTEMS

4. COMPONENTS OF A P2PVPN

5. EVALUATING VPN MODELS

6. CONCLUSIONS

7. REFERENCES

[1] L. Deri and R. Andrews. N2N: A layer two peer-to-peer vpn. In *AIMS '08: Proceedings of the 2nd international conference on Autonomous Infrastructure, Management and Security*, pages 53–64, Berlin, Heidelberg, 2008. Springer-Verlag.

[2] W. Ginolas. P2PVPN. `http://p2pvpn.org`, August 2009.

[3] LogMeIn. Hamachi. `https://secure.logmein.com/products/hamachi/vpn.asp`, July 2008.

[4] K. Petric. Wippien. http://wippien.com/, August 2009.

[5] J. Yonan. OpenVPN. `http://openvpn.net/`, March 2007.