Traversal of the Customer Edge with NAT-Unfriendly Protocols

Petri Leppäaho, Nicklas Beijar, Raimo Kantola, Jesús Llorente Santos
Department of Communications and Networking
Aalto University
Helsinki, Finland
{petri.leppaaho, raimo.kantola, nicklas.beijar, jesus.llorente.santos}@aalto.fi

***Abstract*—Customer Edge Switching (CES) provides policy based reachability to hosts in a private network without the disadvantages caused by traditional mechanisms for traversing Network Address Translators (NAT). Although most protocols traverse the customer edge correctly, we identify a few protocols that require special processing because of the IP addresses carried in the user data. This paper first presents the results of protocol compatibility testing with CES and selects two protocols, SIP and FTP, for further study. The paper then reports the implementation of Application Layer Gateways for these two protocols and gives guidelines for processing other protocols. The solution enables transparent communication across address realms without keep-alive signalling and application layer code in end systems as required by the current recommended approach to NAT traversal. The proposed approach significantly cuts the session establishment delays typical in SIP and improves security. The presented work is a part of a larger project that proposes the Customer Edge Switching to replace NATs and form collaborative firewalls for protecting customer networks.**

Keywords—Application Layer Gateway; Session Initiation Protocol; File Transfer Protocol; NAT traversal; Customer Edge Switching; collaborative firewall.

I. INTRODUCTION

In the current Internet, the availability of IPv4 addresses has become an increasing problem. IPv6 would provide a sufficient number of addresses but adopting IPv6 is difficult, as it requires hosts, applications and network equipment to be updated. Network Address Translation (NAT) [1] has prolonged the use of IPv4 by allowing the reuse of certain address blocks in several networks simultaneously. Unfortunately, NATs cause problems to several protocols. To overcome these problems, application developers are required to implement NAT traversal mechanisms, which use various tricks to allow traffic through the NAT. However, NAT traversal comes with several drawbacks. The application is required to send traffic periodically forcing a mobile device to wake up and drain its battery. Each application must separately implement its NAT traversal mechanism. NAT traversal introduces security concerns as the NAT and firewall is bypassed in an uncontrolled way. Finally, the mechanisms introduce a significant delay in session setup.

Customer Edge Switching (CES) [2] aims to provide an alternative to NATs. A CES device transfers traffic between the customer and the provider networks according to policies specified by the customer. When only one endpoint is behind a CES, the CES integrates a Private Realm Gateway (PRGW) [3] enabling inbound connections to the private address space. Thus, in addition to address translation on the client side, CES performs server side address translation. The full advantage of CES is obtained when the networks of both communicating endpoints contain a CES, whereas the traffic is tunnelled between the CES devices through the public network. In this setting, both CES devices can negotiate in order to take the policies of both networks into account.

Protocols that behave in an expected way can traverse the CES in both directions without any NAT traversal algorithms. These protocols are required to (1) address the endpoint with a Fully Qualified Domain Name (FQDN) instead of an IP address, and (2) perform a DNS query to map the FQDN to an IP address, which is used for communication. Most protocols behave in this way. However, we are aware that certain protocols do not follow this procedure. The first aim of this paper is to identify the protocols and applications that are not following the above scheme.

Our second aim is to show that protocols that are not as such compatible with CES can still operate in a CES enabled network. Contrary to NAT traversal, where the application is adapted to the NAT, we take the opposite approach, where the NAT is adapted to applications through Application Layer Gateways (ALGs). In our philosophy, application code should not be cluttered with network layer code taking care of reachability. ALGs are primarily intended as a mechanism to make the currently existing protocols work with CES. We recommend that new protocols should be designed following the above principles, i.e. address the destination using FQDN instead of assuming a global IP address. Compared to NATs, the use of CES allows an easy way to accept inbound connections without NAT traversal mechanisms or ALGs.

The contribution of this paper is to present the results of compatibility testing of protocols, concentrating on interactive protocols operating directly between clients. Further, this paper presents the implementation of ALGs for two selected protocols that were found incompatible with the CES: the Session Initiation Protocol (SIP) [4] and File Transfer Protocol (FTP) [5]. The paper finally summarizes our evaluation of the ALGs, which shows that the developed ALGs were highly successful, and gives guidelines for future development of ALGs.

This work was partially supported by the European Celtic MEVICO project.

The rest of the paper is organized as follows. Section II briefly presents Customer Edge Switching. Section III reports the result of our compatibility testing. Sections IV and V describe the ALGs for SIP and FTP, respectively. Section VI presents the evaluation of the ALGs and Section VII describes guidelines for developing new ALGs. Finally, Section VIII refers to some related work and Section XI concludes.

II. Customer Edge Switching

Customer Edge Switching develops the NAT/Firewall into a device that is an integral part of the Internet architecture. CES devices are located at the edges of the customer networks and they are connected to the public network, as depicted in Figure 1. CES makes protocol choices in the public and private networks independent from each other, and allows an easy way to introduce new technologies such as IPv6 and routed Ethernet [6]. The addressing and routing of the networks are separate: IP addresses from the private networks are not revealed to the public network. To identify hosts, various types of IDs can be used, including domain names, operator assured IDs and temporary IDs.

CES significantly alleviates the IPv4 address depletion problem by making it sufficient to allocate only a private address to hosts. This is feasible if inbound connectivity can be provided efficiently. In networks served by CES, reachability is the responsibility of the network functions and access is interrupt driven. As a result, CES provides an alternative to the currently recommended methods of NAT traversal: Session Traversal Utilities for NAT (STUN) [7], Traversal Using Relays around NAT (TURN) [8] and Interactive Connectivity Establishment (ICE) [9]. The improvement compared to state-of-the-art is that sending keep-alive signalling is not needed, which saves power in mobile devices. Applications do not need to include code for NAT traversal. Session setup is faster than in case of typical NATs because of avoiding the delay caused by ICE trying to find the optimal NAT traversal method.

In the *CES-CES* scenario, packets are tunnelled between the CES devices using the Customer Edge Traversal Protocol (CETP) [10]. The tunnelling header carries the source and target communication identifiers. In addition to the data plane functions, CETP carries control type-length-value (TLV) elements that allow the inbound edge to make an informed decision on flow admission. Due to these control TLV-elements, the CES box acts as a collaborative firewall. The *CES-Local* scenario is a special case of the CES-CES scenario, with both endpoints served by the same CES.

In the *CES-Legacy* scenario, CES includes a Private Realm Gateway (PRGW) [3] that operates similarly to a NAT for outbound connections. For inbound connections, the PRGW integrates a Domain Name System (DNS) leaf node and identifies the destination node by mapping the requested FQDN with the traffic. This scenario provides an upgrade path allowing the deployment of CES one network at a time.

The CES concept uses the FQDN as the global address. Each connection must be initialized by performing a DNS lookup of the FQDN of the destination. This provides the host with an IP address, which can be used to reach the destination.

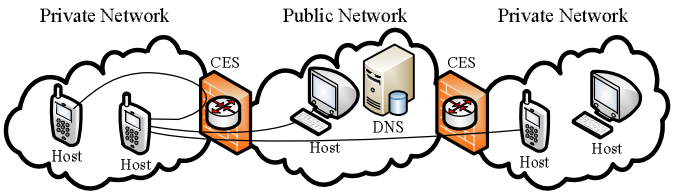

Fig. 1. CES architecture

The IP address is connection specific and is valid for the initializing host only. In order to indicate an address to another host, e.g. in a protocol message, the FQDN must be used instead of the IP address. Most client-server protocols adhere to this way of operation. However, CES must provide an alternative solution for the remaining protocols. Instead of requiring applications to be aware of the CES, we solve the compatibility issues in the CES device itself by using ALGs.

III. Compatibility Testing

We tested a set of common applications in order to examine how they operate in the presence of a CES. As client-server protocols such as HTTP and SSH earlier have been proved successful, the focus is now on applications establishing connections directly between users. Such applications are used for messaging, voice/video calls and file transfer. At the same time, these applications are the ones that are most interesting from a mobile perspective and the applications that are expected to be challenging for a CES network. Applications were tested on the Linux (Ubuntu) and Windows platforms.

The tested applications for the protocols are the following:

- *SIP*: Kamailio, 3CX servers; Ekiga, Twinkle, 3CX clients.
- *FTP*: vsftpd server and ftp client (Unix).
- *XMPP*: Google Talk, Empathy, Psi, Pidgin, Tkabber.
- *IRC*: Empathy, Konversation, Xchat, IRSSI.
- *Microsoft Notification Protocol (MSN)*: Windows Live Messenger, aMSN, Pidgin, Emesene.
- *Skype*: Skype
- *Oscar*: AIM, Pidgin, Empathy, Kopete.
- *ICQ*: ICQ, Pidgin, Empathy, Kopete.
- *YMSG*: Yahoo! Messenger, Pidgin, Empathy, Kopete.

For the protocols allowing installation of a server on a private network, we tested the CES-CES scenario. The other protocols were tested using the server on the public Internet, whereas the client was located behind a CES.

Additionally, we tested web-based access to the communication services with Ebuddy (supporting MSN, Yahoo, AIM, Google Talk, and ICQ), Imo IM (supporting MSN, Skype, Yahoo Messenger, AIM, Google Talk, and ICQ) and Meebo (supporting MSN, Yahoo, and AIM).

Each test resulted in one of three outcomes: (1) the protocol worked perfectly, (2) the protocol requires an ALG, and (3) the protocol failed but ALGs are difficult or impossible to implement due to encryption. For a few protocols, the outcome was dependent of which client was used. In those cases, some of the clients utilized TURN to bypass the CES. In the CES-Legacy scenario, applications supporting TURN work

TABLE I. APPLICATION TEST RESULTS IN CES-CES SCENARIO

Protocol	Operation	Outcome	Problems
SIP	Calls	ALG required	Private IP used
FTP	File transfer	ALG required	Private IP used
XMPP	Messaging	Success	
	File transfer	Fail / ALG required	Private IP used, encryption
IRC	Messaging	Success	
	File transfer	ALG required	

TABLE II. APPLICATION TEST RESULTS IN CES-LEGACY SCENARIO

Protocol	Operation	Outcome	Problems
SIP	Calls	ALG required	Private IP used
FTP	File transfer	ALG required	Private IP used
MSN	Messaging	Success	
	File transfer	Success	
Skype	Messaging	Success	
	Calls	Success	
XMPP	Messaging	Client dependent [1)]	Private IP used
	File transfer	Client dependent [1)]	Private IP used
Oscar	Messaging	Success	
	File transfer	Client dependent [2)]	Private IP used
ICQ	Messaging	Success	
	File transfer	Client dependent [3)]	Private IP used
	Calls	Client dependent [3)]	Private IP used
Yahoo	Messaging	Success	
	File transfer	Client dependent [4)]	Private IP used
	Calls	Client dependent [4)]	Private IP used
Web interface	Messaging	Success	

1) Google Talk and Empathy successful. Kopete and Pidgin require ALG.
2) AIM Windows successful. Empathy, Kopete, and Pidgin require ALG.
3) ICQ Windows successful. Empathy, Kopete, and Pidgin require ALG.
4) Yahoo messenger successful. Empathy, Kopete, and Pidgin require ALG.

with inbound connections since TURN enables traversal through a CES in a similar manner as through a NAT.

The results are summarized in Table I for the CES-CES scenario and in Table II for the CES-Legacy scenario. Other protocols that are broken by NATs [11] are expected not to work with CES either.

In the CES-CES scenario, all communication requires inbound connections (through one of the CES devices). In the CES-Legacy scenario, the applications typically establish an outbound connection to the server, over which messaging is performed. Outbound connections are always successful. However, for file transfers and calls, the clients communicate directly with each other, whereas one of the clients must be able to receive an inbound connection.

Protocols may fail to work because of the following reasons. (1) The client establishes a connection to an IP address without a preceding DNS query, leading to failure in a CES-CES scenario. (2) The client sends its private address in protocol messages, but this address cannot be used outside the private network. (3) Additional mapping is required for the data connection leading to failure in the CES-Legacy scenario.

Problem (1) cannot be easily solved without client modifications, but this problem did not appear in our testing. Problem (2) is resolved by using an ALG to translate between private addresses and public addresses, or to FQDNs where applicable. Problem (3) is solved by an ALG creating additional mappings on demand. Thus, most problems can be solved using an ALG. However, this solution only works for unencrypted protocols.

TABLE III. NOTATION

Element	Definition
FQDN{*s,d,m*}	Fully Qualified Domain Name of the source, destination and media
IP{*s,d,o,m*}	The IP address for the source, destination and public realm and media content
P{*s,d,o,m*}	The port number for the source, destination, public realm and media content
IP*pd*	The proxy IP address for connecting with the destination host
*	Creation of additional mapping in the forwarding table for incoming connections

In order to demonstrate how difficult protocols can traverse a CES, we implemented ALGs for two selected protocols (SIP and FTP).

IV. APPLICATION LAYER GATEWAY FOR SIP

SIP [4] is a text-based protocol for setting up and controlling media sessions. SIP consists of request and response messages and shares some similarities with Hypertext Transfer Protocol (HTTP). The messages contain a method, various headers and occasionally a body field with Session Description Protocol (SDP) for the media information. The SIP headers and the SDP content carry IP addresses and port numbers of the end hosts as well as third-party relay nodes if available. SIP is transported in Transmission Control Protocol (TCP) or User Datagram Protocol (UDP). This paper focuses on the UDP implementation of the protocol.

A. Design Choices

The underlying premise when designing an ALG is that it has to provide seamless and transparent operations that ensure successful communication without requiring any changes in the hosts involved. On that premise, we implemented a stateless solution that includes two different sets of algorithms which modify messages by either (1) adapting the scope of the addresses and ports in the messages between private and public networks, or (2) replacing the addresses according to the assigned FQDN. The former case applies to CES-Legacy scenarios, whereas the latter is used in CES-CES scenarios.

We found that using IP addresses instead of FQDNs in CES-CES communications requires temporary state information and a certain level of heuristic in the ALG. The state information aggregates addresses and port numbers of the hosts, state and ID of the call as well as inferred third-party SIP servers; eventually leading to a stateful ALG. The operation is highly complex because it requires the allocation of multiple connections in CES until the endpoints are identified and the media connection is established. The computational and memory requirements also grow larger in this approach. Therefore, this solution is not presented in this paper, despite it has been proved working. Instead, we use FQDNs in the CES-CES scenario. Further details about the solutions can be found in [12].

$$\begin{matrix} Source: \\ Destination: \\ [Media]: \end{matrix} \begin{bmatrix} IPs:Ps \\ IPd:Pd \\ IPm:Pm \end{bmatrix} \rightarrow \begin{bmatrix} FQDNs:Ps \\ FQDNd:Pd \\ FQDNm:Pm \end{bmatrix}$$

Fig. 2. Function #1 - Translation in CES-Local scenario

$$\begin{matrix} Source: \\ Destination: \\ [Media]: \end{matrix} \begin{bmatrix} IPs:Ps \\ IPd:Pd \\ IPm:Pm \end{bmatrix} \rightarrow \begin{bmatrix} FQDNs:Ps \\ FQDNd:Pd \\ FQDNm:Pm \end{bmatrix}$$

Fig. 3. Function #2 - Outbound translation in CES-CES scenario

$$\begin{matrix} Source: \\ Destination: \\ [Media]: \end{matrix} \begin{bmatrix} FQDNs:Ps \\ FQDNd:Pd \\ FQDNm:Pm \end{bmatrix} \rightarrow \begin{bmatrix} FQDNs:Ps \\ FQDNd:Pd \\ FQDNm:Pm \end{bmatrix}$$

Fig. 4. Function #3 - Inbound translation in CES-CES scenario

$$\begin{matrix} Source: \\ Destination: \\ [Media]: \end{matrix} \begin{bmatrix} IPs:Ps \\ IPd:Pd \\ IPm:Pm \end{bmatrix} \rightarrow \begin{bmatrix} IPo:Po \\ IPd:Pd \\ IPmo:Pmo* \end{bmatrix}$$

Fig. 5. Function #4 - Outbound translation in CES-Legacy scenario

$$\begin{matrix} Source: \\ Destination: \\ [Media]: \end{matrix} \begin{bmatrix} IPs:Ps \\ IPo:Po \\ IPm:Pm \end{bmatrix} \rightarrow \begin{bmatrix} IPs:Ps \\ IPd:Pd \\ IPm:Pm \end{bmatrix}$$

Fig. 6. Function #5 - Inbound translation in CES-Legacy scenario

In CES-Legacy scenarios, the SIP ALG adapts the scope of the IP addresses and port numbers conveyed in the SIP messages when the communication involves a private and a public host. Additionally, the solution may create mappings dynamically for the media and media control connections.

In CES-CES scenarios, the SIP ALG does not need to create additional mappings or modify the port numbers due to the transparent nature of the CES architecture regarding the transport layer. In this case, the IP addresses are replaced by FQDNs of the associated hosts so that the end hosts issue new DNS queries that allocate state in CES thus enabling communication.

B. Operations

The designed solution is compatible with the CES-CES, the CES-Legacy and the CES-Local scenarios. The ALG comprises five different operations for address translation and creation of additional mapping if necessary. The operations are described in Figures 2 - 6. The notation used in the figures is explained in Table III.

Figure 2 represents the transformation performed over a CES-Local connection. The IP addresses of the source, destination and media are replaced by their respective FQDN ensuring CES compatibility. The port numbers are not affected. Figure 3 represents the transformation performed over an outbound connection in the CES-CES scenario. The operation is the same as with local connections. Figure 4 reveals that inbound connections in CES do not require any transformation and the contents are already translated due to a previous outbound operation.

Figure 5 represents the transformation performed over an outbound connection in the CES-Legacy scenario. The source address and port are translated to the outbound scope according to the connection state information. If media content is found, the addresses and ports are also translated and additional

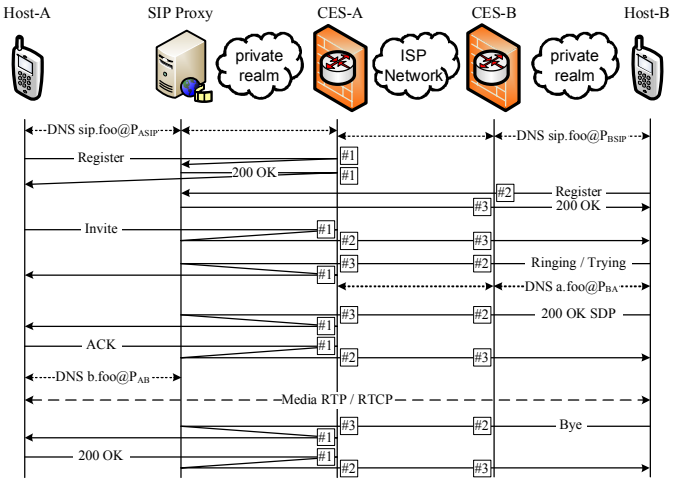

Fig. 7. SIP example in CES-CES scenario

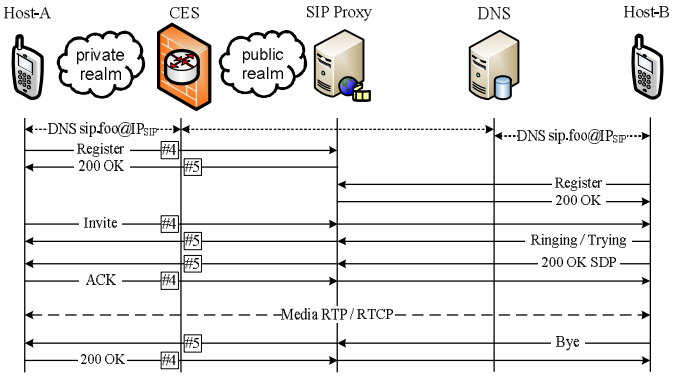

Fig. 8. SIP example in CES-Legacy scenario

mappings are created thus allowing incoming connections towards the private host. Figure 6 shows that inbound connections in the CES-Legacy scenario only require to change the destination address and port with the private address and port of the host. The media content is not altered in any way and no additional mappings are required.

In some situations, the length of the modified packet may exceed the Maximum Transmission Unit (MTU) of the link due to lengthy FQDNs. In order to avoid unnecessary fragmentation, the SIP ALG can use temporary short FQDNs.

C. Case Examples

Let us introduce case examples for SIP communications in the CES-CES and CES-Legacy scenarios where two hosts are able to register in a SIP server and successfully establish a call.

Figure 7 represents CES-CES communication. The private hosts query the CES in order to create a connection with the SIP server. The SIP messages between Host-A and SIP server are modified by CES-A following the local transformation according to Figure 2. The SIP messages between Host-B and SIP server are modified by CES-B following the outbound transformation according to Figure 3. The media parameters are transformed to FQDN so that the hosts are required to issue a new DNS query in order to establish the media connection. No additional mapping is created.

Figure 8 represents CES–Legacy communication. The SIP messages between Host-A and SIP server are modified by

$$\text{Offset} = \text{Length}_{\text{new}} - \text{Length}_{\text{original}} + \Delta\,\text{Offset}$$
$$\text{ACK}_{\text{new}} = \text{ACK}_{\text{current}} - \text{Offset}$$
$$\text{SEQ}_{\text{new}} = \text{SEQ}_{\text{current}} + \text{Offset}$$

Fig. 9. FTP ALG equations

$$\begin{array}{rccc} \textit{CES Local}: & [\text{IPs}] & \rightarrow & [\textit{IPpd}] \\ \textit{CES Outbound}: & [\text{IPs}] & \rightarrow & [\text{FQDNs}] \\ \textit{CES Inbound}: & [\text{FQDNs}] & \rightarrow & [\textit{IPpd}] \\ \textit{Legacy Outbound}: & [\text{IPs}] & \rightarrow & [\textit{IPo}]* \\ \textit{Legacy Inbound}: & - & \rightarrow & - \end{array}$$

Fig. 10. FTP ALG address translation

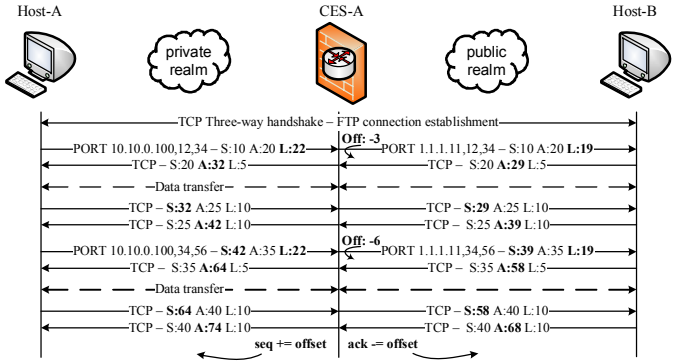

Fig. 11. FTP ALG case example

CES-A following the outbound and inbound transformation according to Figure 5 and Figure 6, respectively. The addresses and ports conveyed in the SIP messages are translated according to the destination realm. If the ALG detects media information originating from a private host, the addresses and ports are adapted to the public scope; additional mappings are created for the incoming RTP and RTCP connections. If the media does not match a private host, it remains unchanged without further actions.

V. Application Layer Gateway for FTP

FTP follows the client-server architecture and establishes separate control and data connections over TCP. The control messages carry information related to the IP address and port of the host serving the data connection. The purpose of these messages is to indicate the remote host where the data is to be fetched from (passive mode) or sent to (active mode).

The FTP ALG modifies the user data conveyed in the FTP control messages and creates additional mapping in the forwarding table for incoming connections. Because the FTP control messages are in text format, the translation of the IP address may result in a change in the size of the packet. The FTP connection must remain undisrupted regardless of these changes. The ALG is stateful; it stores and keeps updated the offset introduced for a given connection as a result of the address translation. The offset is used for adjusting the subsequent packets of the FTP transaction. The acknowledgment number is modified while forwarding an outbound packet and the sequence number while forwarding an inbound packet [1][3][12]. The offset calculation and the TCP field modifications are described in Figure 9. The operations are represented in Figure 10.

TABLE IV. SIP ALG Evaluation

CES-CES and CES-Local scenarios			
Host-A	**Host-B**	**SIP server**	**Outcome**
Network-A	Network-A	Network-A	Success
Network-A	Network-A	Network-B	Success
Network-A	Network-B	Network-A	Success
CES-Legacy scenarios			
Host-A	**Host-B**	**SIP server**	**Outcome**
Network-A	Network-A	Internet	Success
Network-A	Internet	Network-A	Success
Network-A	Internet	Internet	Success
CES-CES and CES-Legacy scenarios			
Host-A	**Host-B**	**SIP server**	**Outcome**
Network-A	Internet	Network-B	Fail / Stateful ALG required

TABLE V. FTP ALG Evaluation

Client	**Server**	**Scenario**	**Outcome**
Network-A	Network-A	CES-Local	Success
Network-A	Network-B	CES-CES	Success
Network-A	Internet	CES-Legacy	Success
Internet	Network-A	CES-Legacy	Success

Figure 11 illustrates a private host establishing an FTP active connection with a server located in the public realm, the introduced offset and how the TCP fields are adjusted.

VI. Experimental Evaluation

In order to verify the operation of the SIP and FTP ALGs, we integrated them within the CES prototype which contains an implementation of the PRGW and the CETP protocol. The operations of the ALGs are triggered based on the port number and the transport protocol (TCP/UDP).

The test scenarios for the SIP ALG result in the combination of the different networks where the hosts and the server can be located, also including some unlikely scenarios. The results summarized in Table IV reveal that only one rare scenario is unsuccessful and requires a stateful ALG for enabling end-to-end media whereas the SIP signalling worked in all cases. Additional rare scenarios are presented in [10].

The test cases for the FTP ALG comprise CES-CES, CES-Local and CES-Legacy scenarios. The results presented in the Table V reveal that the FTP ALG operates successfully in all cases with passive and active FTP mode.

VII. Design Guidelines

A set of guidelines are defined to help developing new ALGs for other protocols in CES enabled networks.

A. Addressing

The scope of the IP addresses must be adapted to the realm to which the packet is forwarded. For example, private addresses are replaced with public addresses for outbound connections and public addresses with private addresses for inbound connections. Additionally, we recommend using FQDN instead of IP addresses for host identification if the protocol specifications allow.

B. Connection State

Some protocols require maintaining additional protocol specific information in addition to the information that CES keeps for all ongoing connections. This leads to a stateful ALG. For example, a TCP based protocol must keep track of the introduced offset as a result of the changes in length of the packets after modification. The ALG must modify the sequence and acknowledgement numbers in the TCP header based on the offset. ALGs for UDP based protocols can be built stateless.

Similarly to FTP and SIP, a protocol may use a control connection to negotiate the establishment of additional data connections. As a consequence, the ALG must analyse these messages and create connection state in CES for the data connections.

VIII. Related Work

In [13] NAT traversal solutions for SIP, including static routes, Universal Plug And Play (UPnP), STUN, ICE Session Border Controllers and ALGs are compared. Application layer gateways for SIP and FTP are used in several firewall and NAT products. In [14] a basic stateful ALG for SIP is presented, which adjust the Contact and Via headers of forwarded messages. In [15] a SIP ALG is complemented with functionality for the Message Session Relay Protocol (MSRP). An ALG for FTP is proposed in [16] for gateways connecting IPv6 and IPv4 networks. In [17] an ALG is described for DNS servers located in private networks.

IX. Conclusions

Customer Edge Switching provides an easy way to accept inbound connections to a host with a private address provided that the application uses FQDNs for establishing the connection. However, we identified a set of protocols that are problematic for CES. These protocols assume that the hosts have a globally reachable IP address and therefore convey IP address and port information in the payload, which is known to cause problems also with NATs. We propose the use of Application Layer Gateways instead of developing host based traversal methods for CES.

To prove the concept, we extended a CES prototype with ALGs for the SIP and FTP protocols. The prototype demonstrates the feasibility of developing transparent ALGs for hosts and applications therefore enabling these protocols in CES. We evaluated different combinations of CES and Legacy scenarios for the developed ALGs that returned promising results. The guidelines for creating ALGs were formed accordingly. However, the development of ALGs is not always possible due to secure protocols and encrypted messages.

The adoption of ALGs instead of NAT Traversal mechanisms enables faster connection setup, direct communication between endpoints and it does not require the costs and administrative burden of third-party relays. It simplifies the application development and decreases the bandwidth consumption, which is especially beneficial for mobile hosts and wireless networks. The security is enhanced by removing third-party elements such as STUN/TURN servers and relays, which reduces the risk for man-in-the-middle attacks.

Although the ALGs have been successfully proven for enabling challenging protocols through CES, we believe that future applications should rely on FQDN for host identification rather than IP addresses. All NAT-friendly [11] applications that resolve FQDNs with DNS queries instead of using IP addresses for establishing a communication are supported by CES. Replacing NATs with CES enables policy based communications and enhanced security without the disadvantages of current NAT Traversal mechanisms.

Acknowledgment

The authors wish to thank Sarantorn Bisalbutra for carrying out the application compatibility experiments.

References

[1] P. Srisuresh and K. Egevang, *Traditional IP Network Address Translator (Traditional NAT)*, RFC 3022, Jan. 2001.

[2] R. Kantola, "Implementing Trust-to-Trust with Customer Edge Switching,", *AMCA in connection with AINA 2010*, Perth, Australia, April 2010.

[3] J. Llorente, *Private Realm Gateway*, M.Sc. Thesis, Aalto University, Helsinki, Finland, Sep. 2012.

[4] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley and E. Schooler, *SIP: Session Initiation Protocol*, RFC 3261, June 2002.

[5] J. Postel and J. Reynolds, *File Transfer Protocol (FTP)*, RFC 959, Oct. 1985.

[6] R. Kantola, M. Luoma and J. Manner, "Future Internet is by Ethernet," in *World Computer Congress*, Brisbane, Australia. Sep. 2010.

[7] J. Rosenberg, R. Mahy and P. Matthews, *Session Traversal Utilities for NAT (STUN)*, RFC 5389, Oct. 2008.

[8] R. Mahy, P. Matthews and J. Rosenberg, *Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)*, RFC 5766, April 2010.

[9] J. Rosenberg, *Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols*, RFC 5245, April 2010.

[10] R. Kantola, N. Beijar, Z. Yan and M. Pahlevan, *Customer Edge Traversal Protocol (CETP)*, Work in progress, Sep. 2012, Available: http://www.re2ee.org/.

[11] M. Holdrege and P. Srisuresh, *Protocol Complications with the IP Network Address Translator*, RFC 3027, Jan. 2001.

[12] P. Leppäaho, *Design of Application Layer Gateways for Collaborative Firewalls*, M.Sc. Thesis, Aalto University, Helsinki, Finland, May 2012.

[13] W. Chen, Y. Huang and H. Chao, "NAT traversing solutions for SIP applications," in *EURASIP Journal on Wireless Communications and. Networking*, vol. 2008, no. 4, pp. 1-9, Jan. 2008.

[14] J. Han, W. Hyun, S. Park, I. Lee, M. Huh, S. Kang, "An application level gateway for traversal of SIP transaction through NATs," in *Proc. 8th Int. Conf on Advanced Communication Technology, ICACT 2006*, Phoenix Park, South Korea, Feb. 2006.

[15] H. Yang, H. Lin, J. Li and W. Lei, "The Design and Implementation of an Enhanced SIP ALG to Support MSRP Sessions," in *Proc. 9th Int. Conf. on Hybrid Intelligent System, HIS '09*, Vol.2, pp. 289-292, Shenyang, China, Aug. 2009.

[16] J. Lee, M. Shin, H. Kim, "Implementation of NAT-PT/SIIT, ALGs and consideration to the mobility support in NAT-PT environment," in *Proc. IEEE 59th Vehicular Technology Conf., VTC 2004*, Los Angeles, CA, USA, May 2004.

[17] P. Srisuresh, G. Tsirtsis, P. Akkiraju and A. Heffernan, *DNS extensions to Network Address Translators (DNS_ALG),* RFC 2694, Sep. 1999.