

INTERNET-DRAFT

Intended Status: Informational
Expires: April 24, 2018

N. Elkins
Inside Products
M. Ackermann
BCBS Michigan
October 21, 2017

Common Network Architecture for Brick and Mortar Enterprises
draft-elkins-brickmortar-architecture-00

Abstract

The network architecture and topology for "brick and mortar" enterprises differ in significant aspects from those of Internet-based companies. This has implications for protocol implementations.

By and large, the network connects to sites spread throughout a geographic region. The architecture is not flat. There may be multiple hops - routers, middle boxes and the like. There may also be multiple carriers or ISPs involved (including internally built infrastructure). The number, nature and amount of applications also dictate a complex topology which then dictates a complex protocol implementation. Lastly, a number of these enterprises are in industries which are regulated. Such regulations impact the nature of network design. These considerations are discussed in this document.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at
<http://www.ietf.org/lid-abstracts.html>

The list of Internet-Draft Shadow Directories can be accessed at
<http://www.ietf.org/shadow.html>

Copyright and License Notice

Copyright (c) 2017 IETF Trust and the persons identified as the document authors. All rights reserved.

IETF Trust Legal Provisions of 28-dec-2009, Section 6.b(i), paragraph 3: This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1	Background	3
1.1	Middle Box Usage	3
1.2	Routing and Other Protocols Used	4
1.3	"Home-grown" Infrastructure	4
1.4	Connections to Business Partners	4
2	Regulatory Requirements	4
2.1	End-to-End Encryption	4
3	Applications	4
4	Security Considerations	5
5	IANA Considerations	5
6	References	5
6.1	Normative References	5
6.2	Informative References	5
7	Acknowledgments	5
	Authors' Addresses	6

1 Background

The network architecture and topology for "brick and mortar" enterprises differ in significant aspects from those of Internet-based companies. This has implications for protocol implementations. By and large, the network connects to sites spread throughout a geographic region. The architecture is not flat. For example, for an oil and gas company, the network may connect refineries, gas stations, storage depots, oil fields, and the like. The architecture is not flat.

Within the data center as well as to the end location, there will be multiple hops - routers, firewall, load balancers and the like. Often multi-homing is done for fall back and disaster recovery. Hence, multiple carriers or ISPs will be involved. Thus, the architecture is inherently complex -- some have routes with 10, 15 or even over 50 hops.

The number, nature and amount of applications also dictate a complex topology which then dictates a complex protocol implementation. Lastly, a number of these enterprises are in industries which are regulated. This means that some of the control over their architecture is not in their own hands.

1.1 Middle Box Usage

Such large enterprises use Content Delivery Networks (CDNs) and NATs. One might wish that IPv6 was used to avoid NAT but this is not likely

to be the case inside the enterprise for many years.

Other type of middle boxes are frequently used by the data center infrastructure. This includes firewalls, load balancers, web servers, app servers, and middleware servers. A multi-tiered route is very common.

1.2 Routing and Other Protocols Used

Within the data center, such enterprises often use OSPF, EIGRP, BGP, and even RIP and static routes.

1.3 "Home-grown" Infrastructure

What is "home-grown"? For the "brick and mortars", if they do anything on their own, it will be to put up hardware infrastructure. For example, the connectivity in the swamps (which may have oil) or mining locations may be quite bad. Some companies put up, for example, their own microwave towers throughout the region.

What such enterprises do NOT do was to rewrite the code for the routers, middle boxes, etc.

1.4 Connections to Business Partners

Some of the most critical connections of large enterprises are to their business partners or regulatory bodies. For example, many financial institutions in the United States connect to the Federal Reserve; many insurance companies connect to the Medicare or Social Security systems.

2 Regulatory Requirements

Many of the "brick and mortar" enterprises are regulated by various legal structures such as HIPAA or PCI. These have an impact on the type of architecture which can be supported.

2.1 End-to-End Encryption

At times, there are regulatory requirements which enforce end-to-end encryption. For diagnostic and security purposes, it is important to be able to have visibility into the packets, routing and otherwise, so as to be able to manage the network.

If there is a protocol which does not allow for visibility, this can be quite problematic.

3 Applications

One of the advantages that large brick and mortar enterprises had in the dawn of the computer age is that they began to computerize early. Forty or fifty years later, what was once a competitive advantage now carries with it some burdens.

The number and nature of applications has multiplied greatly. Hundreds, if not thousands, of different applications are used. These range from the Stone Age (of computing) to the Space Age (of computing). That is, applications from those written in the 1960's to those using the most current technology must be supported.

Change can come at a glacial pace.

Having said that, many brick and mortars still see technology as their competitive advantage and are trying to keep pace.

4 Security Considerations

There are no security considerations.

5 IANA Considerations

There are no IANA considerations.

6 References

6.1 Normative References

6.2 Informative References

7 Acknowledgments

The authors would like to thank Steve Fenter for his comments.

Authors' Addresses

Nalini Elkins
Inside Products, Inc.
36A Upper Circle
Carmel Valley, CA 93924
United States
Phone: +1 831 659 8360
Email: nalini.elkins@insidethestack.com
<http://www.insidethestack.com>

Michael S. Ackermann
Blue Cross Blue Shield of Michigan
P.O. Box 2888
Detroit, Michigan 48231
United States
Phone: +1 310 460 4080
Email: mackermann@bcbsm.com
<http://www.bcbsm.com>