Default Perimeter Identification
draft-kline-default-perimeter-00

Abstract

Automatic, simple identification of when traffic is crossing a perimeter is highly desirable for a variety of home network uses. This document proposes a set of default tests to be applied to traffic scheduled for forwarding, which can be used collectively to identify this perimeter in some (but not all) environments.

Status of this Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on January 30, 2013.

Copyright Notice

Copyright (c) 2012 IETF Trust and the persons identified as the document authors. All rights reserved.

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. Introduction ............................................. 3
   1.1. Requirements Language ................................. 3
2. Terminology .............................................. 3
3. Fundamental recommendations ............................... 4
   3.1. Network node default security practices .............. 4
   3.2. State changes and logging ............................ 5
4. Useful perimeter signals ................................... 5
   4.1. Product-defined interface purposes .................... 6
   4.2. Routing adjacency ...................................... 6
   4.3. Links requiring subscriber information ................ 6
   4.4. Links requiring existing network-layer connectivity ... 7
   4.5. Links that are fundamentally point-to-point in nature .. 7
5. IP over Ethernet ........................................... 7
   5.1. DHCPv6 PD, if and only if............................. 8
   5.2. Other tricks? .......................................... 8
6. Additional considerations ................................... 8
   6.1. Physical vs virtual interfaces ......................... 8
   6.2. Mixed zone next-hops on the same interface ............ 9
   6.3. Perimeter and protocol version ........................ 9
7. Acknowledgements .......................................... 9
8. IANA Considerations ....................................... 9
9. Security Considerations .................................... 10
10. References ............................................... 10
    10.1. Normative References ................................. 10
    10.2. Informative References ............................... 10
Appendix A. Additional Stuff ................................ 10
Author's Address ............................................ 10
1. Introduction

Automatic, simple identification of when traffic is crossing a perimeter is highly desirable for a variety of home network uses. This document proposes a set of default tests to be applied to traffic scheduled for forwarding, which can be used collectively to identify this perimeter.

Of note are limitations introduced by the ubiquitous use of IP over Ethernet (IPoE) Internet access methods. By design these architectures make it difficult (at best) to distinguish any difference between a LAN port in an enterprise and a home Internet connection.

Nevertheless, where practical, an automated mechanism of perimeter discovery permits home devices to define default definitions of the "interior", i.e. the home, and the "exterior", usually the greater Internet. Once indentified, a device could apply default security policies to traffic transiting the perimeter.

Specifying the default policy that should be applied to traffic crossing this perimeter is out of scope of this document. Implementors should remain mindful of recommended practices, e.g. RFC 4864 [RFC4864], et cetera.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2. Terminology

In order to address perimeter identification at a manageable scale the scope has been limited to discussing concepts of "interior", "exterior", and "perimeter". Working definitions in use by this document are as follows.

Interior

The interior is broadly defined to include the collection of interfaces (physical or virtual), nodes, and forwarding next-hops collectively under the control of a single logical administrative domain.
Exterior
The exterior is broadly defined to include all interfaces (physical or virtual), nodes, and forwarding next-hops collectively NOT under the control of any single logical administrative domain and specifically NOT under the control of the administrative domain which defines the interior.

Perimeter
The perimeter is taken to be the collection of all ephemeral demarcations within the collection of interior nodes which forward traffic such that any IP packet transiting that demarcation can be said to be crossing either from the interior toward the exterior or from the exterior toward the interior. This is independent of whether or not such traffic is permitted by policy to complete its transiting from one zone to the other.

Expressly not discussed herein are architectures having multiple interior networks, nor the relationships between them as separate from their relationship to their common exterior or any common perimeter. The architectures under discussion have a single interior, single exterior, and a single logical perimeter between them.

The definition of perimeter is such that, for example, an IP packet arriving on a NAT device’s interior interface that is "hairpinned" and retransmitted out the interior interface is not considered to have touched nor crossed the perimeter.

The definition of perimeter as written technically permits traffic being forwarded over an interface to be classified as transiting a perimeter or not based on the classification of the next-hop. The implications of this are discussed in a later section.

3. Fundamental recommendations
The application of security policies at the perimeter and possible relaxation of security policies within the interior are apt to have administrative consequences. Some fundamental recommendations for nodes operating in this environment follow.

3.1. Network node default security practices
By default all network nodes SHOULD follow best current security practices. Any node may at times find itself in a hostile environment. This is obviously true of mobile nodes when, for instance, connecting to a variety of public "Wi-Fi" networks. In
such environments mobile nodes cannot be sure that there is any network device acting in the mobile node's own best security interests with respect to others on the local network.

It is equally true of more traditionally "fixed" nodes: any compromised neighbor nodes ("fixed" or mobile) may be used as a conduit for further compromise. Indeed, one study of a captured "botnet" ([TORPIG], section 5.2.4) found that roughly 78.9% of infected hosts had RFC 1918 [RFC1918] addresses, commonly used in IPv4 NAT deployments.

3.2. State changes and logging

Devices conforming to this and other homenet documents MUST continuously evaluate the interior, exterior, and perimeter classifications of interfaces and traffic. These may change at any time, for example if new devices are added into the network or a power event causes all equipment to reset, and specific ordering of device bring-up within a homenet network MAY NOT be assumed.

Nodes compliant with this and other homenet documents SHOULD administratively log the perimeter classification of interfaces (both physical and virtual), the reason(s) for such classification, and times at which such classifications are made or changed.

4. Useful perimeter signals

This is a non-trivial task as it is tantamount to automated discovery of administrative boundaries.

Many architectures fundamentally make it difficult or impossible to detect administrative boundaries and rely on various mechanisms of user or administrator invention to create or modify such boundaries. Other hints about administrative boundaries may be insecure, unreliable, operationally impractical, or may place arbitrary requirements upon the architectural where previously no such requirement existed.

Nevertheless there are some signals that may be useful. Which signals are available and useful vary with the access architecture, and in some cases there may be virtually no reliable information to securely determine a perimeter. An physically or cryptographically authenticated routing protocol may be the highest fidelity signal for determining the interior, and thereby the exterior and perimeter.
4.1. Product-defined interface purposes

Many products come with interfaces labeled with their intended use. Examples include home routers with RJ-45 ports labeled "WAN" and "LAN", or perhaps with symbols indicating "The Internet" and "inside the home". Other examples include wireless routers with defined separate WLAN and "Guest" ESSIDs. In such cases where interior and exterior are clearly delineated a homenet device SHOULD by default consider traffic forwarded between interfaces of differing regions as traversing a boundary.

4.2. Routing adjacency

Some networks may employ a physically or cryptographically secure routing protocol. Within such networks, traffic received from and scheduled to be forwarded to next-hops with whom an adjacency has been formed SHOULD by default be classified as interior and not considered to be transiting a perimeter.

Similarly, traffic forwarded to or received from next-hops with whom no adjacency has been formed SHOULD by default be classified as exterior. A next-hop with whom no adjacency has been formed but which nevertheless constitutes the next-hop for a learned or configured route SHOULD by default be considered exterior.

If (and only if?) an interface has only interior next-hops then traffic originating from nodes on links on that interface SHOULD by default be considered to be interior... Discuss: [two routers each sharing a hub with two upstreams on it]. HELP: need more thought to clarify forwarding traffic to on-link destinations versus to next-hops for further forwarding. Don’t want to accidentally classify interior on-link nodes as exterior because no adjacency is formed.

HELP: much more thought is required here. What about bring-up order? What about an interior node attempting and failing to start an authenticated adjacency: it’s a problem if the interface flips into exterior classification.

HELP: find language that doesn’t, for example, define interior to be the entire Internet when RPKI is in use.

4.3. Links requiring subscriber information

One obvious administrative boundary is a link that requires subscriber credentials in order for that link to successfully forward and receive general traffic. Examples include authenticated PPPoE sessions, 3G/LTE PDP contexts (requiring a SIM card associated with a customer account), and authenticated VPN links. By default, all
traffic traversing such a link SHOULD be considered to be traversing a perimeter.

4.4. Links requiring existing network-layer connectivity

By default, all traffic traversing any interface that encapsulates (decapsulates) its payload in a layer higher than or equal to the network (IP) layer in order to forward (receive) traffic SHOULD be considered to be traversing a perimeter. Examples of such interfaces include: Teredo, 6to4, 6rd, 4rd, PPTP and L2TP tunnels, et cetera.

In cases where the exact layer of encapsulation is not necessarily clearly defined or agreed upon, e.g. MPLS interfaces, traffic traversing such interfaces SHOULD also by default be considered to be traversing a perimeter.

In the absence of default perimeter classification, such links would provide a mechanism to breach an otherwise existing perimeter and generally complicate the definition and discovery of the interior. In cases where such interfaces are desired to be classified as part of the interior, and traffic traversing them also classified as interior traffic, another means MAY use to re-classify accordingly.

4.5. Links that are fundamentally point-to-point in nature

Most home networking technology supports more than two nodes on the same logical link communicating directly. By default, traffic traversing from such a "shared access" link which is classified as interior to one which is fundamentally point-to-point in nature (e.g. PPPoE, PPPoA, or some other future link type) SHOULD be considered as transiting a perimeter.

Additionally, traffic transiting a homenet device from such a "shared access" link which is classified as interior to one on which no on-link neighbor discovery and/or communication is permitted by configuration of the node itself, e.g. an 802.11 SSID on which the node acting as an infrastructural access point forbids direct neighbor communications, SHOULD be considered as crossing a perimeter.

HELP: what does this mean for 6lowpan networks inside the home?

5. IP over Ethernet

The ubiquity of IPoE undoubtedly greatly simplifies network architectures and node requirements for connecting to such networks. However, it can be difficult at best for a homenet device to
determine if it is fully in the interior of a network or part of the perimeter.

5.1. DHCPv6 PD, if and only if...

DHCPv6 PD is at this time the most common method for supplying "SoHo" networks with a routable prefix block. If (and only if) a means of distributing prefixes among interior routers is devised that does NOT use DHCPv6 Prefix Delegation, then a link on which DHCPv6 PD succeeded SHOULD be considered an administrative boundary and traffic traversing this interface SHOULD be considered to be traversing a perimeter.

If DHCPv6-PD is to be used within the interior then this signal is not useful.

5.2. Other tricks?

(TBD) If you’re DHCPv6-setting-up-the-reverse-DNS then that interface SHOULD be considered part of the perimeter.

(TBD) If DHCPv4’ing an RFC 1918,6598,... address? What other prefixes and updates will be required as we run out of IPv4?

6. Additional considerations

Everything herein needs more thought and work.

6.1. Physical vs virtual interfaces

In certain configurations it may be desirable that the perimeter defined on a virtual interface also be extended to include the physical interface(s) over which such traffic is forwarded/received. For example, consider a router configured with a PPPoE virtual interface on a physical 802.3 interface. In such a configuration, the security policy applied to traffic transiting the PPPoE interface should most likely also be applied to non-PPPoE traffic transiting the physical interface. If not, the "interior" region would otherwise be logically extended to include the upstream access link. As there is no guaranteed of administrative boundary XXX, a default configuration SHOULD consider the physical interface a perimeter.

By way of contrast, consider an entirely interior router which also has a VPN interface, through which traffic may be passed to, say, a resident’s company network. While a VPN virtual interface SHOULD be considered a logical demarcation point, the physical interface through which VPN-encapsulated traffic is transmitted need not
necessarily be classified as such. Instead, what may be desired is that traffic to/from interfaces that are interior to this VPN-enabled router may pass through either the VPN interface or any "upstream" interfaces, but traffic originating from "upstream" interfaces may be default DENIED transit through the VPN interface. While this situation may be far from the norm for networks, it nevertheless affords the maintenance of a simple mental model of a hierarchical network.

To address these uses, by default the physical interface(s) through which a virtual interface’s traffic is forward should also be considered a perimeter, unless other means determine that it is in fact an interior interface. Note that in all cases such a virtual interface is considered a perimeter.

Discuss: applying the policy to the entire interface for some "infrastructural" connections (e.g. PPPoE). Virtual link versus physical link, virtual interface versus physical interface.

6.2. Mixed zone next-hops on the same interface

By default, if one then all. TBD: explain.

6.3. Perimeter and protocol version

In cases where one IP version’s perimeter might be determined to differ in some way from another IP version’s identified perimeter, the potential for confusion and misconfiguration, and therefore security risk, increases. In the interests of simplicity, and in keeping with the principle of least surprise, traffic transiting links or forwarding to (received from) next-hops which would transit a perimeter in one protocol version SHOULD be considered as transiting a perimeter for traffic of all protocol versions.

7. Acknowledgements

The author gratefully acknowledges the constructive input and criticism of Lorenzo Colitti, Mark Townsley, and Ole Troan.

Thanks also must go to pleasant, peaceful and productive trips on the Japan Rail (JR) Shinkansen ("bullet train").

8. IANA Considerations

This memo includes no request to IANA.
9. Security Considerations

All drafts are required to have a security considerations section. See RFC 3552 [RFC3552] for a guide.

10. References

10.1. Normative References


10.2. Informative References


Appendix A. Additional Stuff

This becomes an Appendix.

Author’s Address

Erik Kline
Google Inc.
Roppongi 6-10-1, 26th Floor
Minato, Tokyo  106-6126
JP

Phone: +81 03 6384 9000
Email: ek@google.com