

Operational Security Capabilities  
for IP Network  
Infrastructure  
Internet-Draft  
Intended status: BCP  
Expires: September 2, 2010

J. Kristoff  
Team Cymru  
M. O'Reirdan  
Comcast  
F. Gont  
UTN/FRH  
March 1, 2010

**Port Filtering Considerations**  
**draft-kristoff-opsec-port-filtering-00.txt**

Abstract

This document provides advice and technical guidance for ISP port filtering.

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/ietf/1id-abstracts.txt>.

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

This Internet-Draft will expire on September 2, 2010.

Copyright Notice

Copyright (c) 2010 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 BSD License.

This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.



## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">3</a>
<a href="#">2.</a>	Perimeter-based Security . . . . .	<a href="#">4</a>
<a href="#">3.</a>	Filter Placement . . . . .	<a href="#">5</a>
<a href="#">4.</a>	Ingress Edge Host Shielding . . . . .	<a href="#">6</a>
<a href="#">5.</a>	Ingress Shielding Rate Limits . . . . .	<a href="#">7</a>
<a href="#">6.</a>	Performance Considerations . . . . .	<a href="#">8</a>
<a href="#">7.</a>	Support Considerations . . . . .	<a href="#">9</a>
<a href="#">8.</a>	Filter Rule Design . . . . .	<a href="#">10</a>
<a href="#">9.</a>	Future Considerations . . . . .	<a href="#">11</a>
<a href="#">10.</a>	Opt In / Opt Out . . . . .	<a href="#">12</a>
<a href="#">11.</a>	Email filtering . . . . .	<a href="#">13</a>
<a href="#">12.</a>	Security Considerations . . . . .	<a href="#">14</a>
<a href="#">13.</a>	Normative References . . . . .	<a href="#">15</a>
<a href="#">Appendix A.</a>	Shielding Filter Example, Cisco IOS . . . . .	<a href="#">16</a>
	Authors' Addresses . . . . .	<a href="#">20</a>



## **1. Introduction**

Many networks have implemented a variety of mechanisms to prevent or limit certain types of network traffic from traversing their networks or reaching certain classes of systems. This activity, which we generically refer to simply as "filtering" can take many forms and be instituted for a number of purposes. "Port filtering" is a specific class of stateless Internet packet filtering based on the port number fields found in the protocols that provide an interface between the Internet Protocol (IP) below and application layers above. Common protocols that implement these port identifiers include the transmission control protocol (TCP), user datagram protocol (UDP), stream control transmission protocol (SCTP) and the datagram congestion control protocol (DCCP). We aim to offer high-level guidance to networks who are currently or are considering utilizing port filters.

Filtering policies are often a contentious issue and can spark lengthy debates. We avoid rehashing those discussions. We do highlight architectural and technical issues where particular filtering policies have shown noteworthy side effects from practical experience. Others have published extensively on architectural principles that are worthy of the reader's attention [TODO: ref to Salzer, Clark and Reed paper, IETF [RFC 1958](#), IETF [RFC 2775](#), IETF [RFC 3439](#), what credible anti-transparency or pro-filtering references are there?].

The rest of this document is organized as follows. The first section outlines problems that can arise from port filtering, and where appropriate discusses how to mitigate them. The remainder of the document outlines from a high-level, common port filtering scenarios are being widely implemented.

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 [[RFC2119](#)].



## **2. Perimeter-based Security**

The point in the network where port filtering is applied results in a defined perimeter, or delineation of a good "inside" and bad "outside" [ref [RFC 3631](#) 3.11]. Systems common to a particular area or "side" share an implicit trust relationship. As the number of systems in an area grows, the number of implicit trust relationships in that area may grow exponentially. With port filtering, in practice this only occurs if all systems are sharing a common set of applications and ports. Likewise, as the number of systems in an area or side decreases, implicit trust relationships in shared applications and ports decline. For large networks, filters may need to be applied throughout the infrastructure to be effective, yet may become an increasingly difficult distributed management challenge.





### **3. Filter Placement**

Mechanisms exist in current Internet systems that perform filtering at almost any point in communications path. In ISP networks, port filters are most often set in router configurations. These routers also perform the route selection and packet forwarding duties of transit traffic. In some cases, ISPs use specialized devices generically referred to as firewalls that inspect or intercept packets as they traverse the path. Firewalls often reside next to or in some cases may be integrated into routing devices. These devices are dedicated to filtering and related duties, but do not generally perform the routing and forwarding functions of the traditional routing system.



#### **4. Ingress Edge Host Shielding**

Edge networks consisting of only end hosts and are used primarily for client-based applications have been successfully put behind &shielding& filters and rate limits. If it is known that these hosts will require limited stable server processes, the goal is to limit their exposure to server processes and minimize their ability to generate abusive traffic. A balance between protection, support and transparency is a delicate balance. Care must be taken to avoid preventing access to current or future client-based services through the use of filters.



## **5. Ingress Shielding Rate Limits**

Rate limits artificially constrain the amount, optionally by type, of traffic that may be sourced by an edge host. It is common for typical client-based hosts on the Internet to use TCP for the bulk of the source traffic, particularly for high-speed transfers and where a congestion-avoidance friendly protocol is desired. Therefore, rate limits for other protocol types to an acceptable rate that leave the bulk of the available capacity to the TCP or TCP-like packets have been used.

## **6. Performance Considerations**

## **7. Support Considerations**

TODO: troubleshooting and diagnosis issues, documentation



## **8. Filter Rule Design**

TODO: order and anomalies with rules

## **9. Future Considerations**

TODO: future app support, flexibility, new protocols

[10.](#) **Opt In / Opt Out**

## **11. Email filtering**

## **12. Security Considerations**

None.

### **13. Normative References**

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.

## [Appendix A](#). Shielding Filter Example, Cisco IOS

These examples assume [BCP 38](#)/84 are in effect, but are not shown for brevity.

```
interface FastEthernet0/0
  ip address 192.0.2.0 255.255.255
  ip access-group shield-filter-in in
  ip access-group shield-filter-out out
  ! 2 Mb/s source ICMP limit for entire edge net
  rate-limit input access-group 2000 20000000 375000 750000
  conform-action transmit exceed-action drop
  ! 10 Mb/s source UDP (non-multicast) limit for entire edge net
  rate limit input access-group 2001 10000000 1875000 3750000
  conform-action transmit exceed-action drop
  ! 10 Mb/s source IP/UDP multicast limit for entire edge net
  rate limit source access-group 2002 10000000 1875000 3750000
  conform-action transmit exceed-action drop
  ! 2 Mb/s source IGMP limit for entire edge net
  rate limit input access-group 2003 20000000 375000 750000
  conform-action transmit exceed-action drop
  ! 10 Mb/s source IPsec limit for entire edge net
  rate-limit input access-group 2004 10000000 1875000 3750000
  conform-action transmit exceed-action drop
  ! 10 Mb/s source GRE limit for entire edge net
  rate-limit input access-group 2005 10000000 1875000 3750000
  conform-action transmit exceed-action drop
  ! 10 Mb/s source limit for all other non-TCP-friendly protocols
  rate-limit input access-group 2500 10000000 1875000 3750000
  conform-action transmit exceed-action drop

access-list 2000 remark ICMP - for edge ingress rate limit
access-list 2000 permit icmp any any
access-list 2000 deny ip any any

access-list 2001 remark UDP (non-multicast) - for edge ingress
rate limit

access-list 2001 deny udp any 224.0.0.0 15.255.255.255
access-list 2001 permit udp any any
access-list 2001 deny ip any any

access-list 2002 remark IP/UDP multicast - for edge ingress
rate limit

access-list 2002 permit udp any 224.0.0.0 15.255.255.255
access-list 2002 deny ip any any
```





```
access-list 2003 remark IGMP - for edge ingress rate limit
access-list 2003 permit igmp any 224.0.0.0 15.255.255.255
access-list 2003 deny ip any any
```

```
access-list 2004 remark IPsec - for edge ingress rate limit
access-list 2004 permit ahp any any
access-list 2004 permit esp any any
access-list 2004 deny ip any any
```

```
access-list 2005 remark GRE - for edge ingress rate limit
access-list 2005 permit gre any any
access-list 2005 deny ip any any
```

```
access-list 2500 remark default - for edge ingress rate limit
access-list 2500 deny icmp any any
access-list 2500 deny igmp any any
access-list 2500 deny udp any any
access-list 2500 deny tcp any any
access-list 2500 deny ahp any any
access-list 2500 deny esp any any
access-list 2500 deny gre any any
access-list 2500 permit ip any any
```

```
ip access-list extended shield-filter-in
  remark [subnet description] (full shielding) - inbound
  !
  ! allow high numbered TCP source ports
  permit tcp any gt 1023 any
  !
  ! allow high numbered UDP source ports
  permit udp any gt 1023 any
  !
  ! allow GRE (required for PPTP)
  permit gre any any
  !
  ! allow IPsec (next 3 lines)
  permit esp any any
  permit udp any eq isakmp any
  permit ahp any any
  !
  ! allow UDP limited broadcasts
  permit udp any host 255.255.255.255
  !
  ! allow UDP multicast
  permit udp any 224.0.0.0 15.255.255.255
  !
  ! allow DHCP clients
  permit udp host 0.0.0.0 host 255.255.255.255 eq bootps
```



```
!  
! allow NTP (some clients use 123 for both src and dst port)  
permit udp any eq ntp any eq ntp  
!  
! allow TCP source port 113 (IDENT)  
permit tcp any eq ident any  
!  
! allow IGMP  
permit igmp any 224.0.0.0 15.255.255.255  
!  
! allow ICMP echo messages (PING)  
permit icmp any any echo  
!  
! allow ICMP echo response messages (PONG)  
permit icmp any any echo-reply  
!  
! allow ICMP parameter problem messages  
permit icmp any any parameter-problem  
!  
! allow ICMP TTL exceeded messages  
permit icmp any any time-exceeded  
!  
! allow ICMP unreachable messages  
permit icmp any any unreachable  
!  
! deny everything else by default and log it  
deny ip any any log-input  
  
ip access-list shield-filter-out  
remark [subnet description] (full shielding) - outbound  
!  
! allow high numbered TCP destination ports  
permit tcp any any gt 1023  
!  
! allow high numbered UDP destination ports  
permit udp any any gt 1023  
!  
! allow GRE (required for PPTP)  
permit gre any any  
!  
! allow IPSec (next 3 lines)  
permit esp any any  
permit udp any any eq isakmp  
permit ahp any any  
!  
! allow UDP multicast  
permit udp any 224.0.0.0 15.255.255.255  
!
```



```
! allow NTP (some clients use 123 for both src and dst port)
permit udp any eq ntp any eq ntp
!
! allow TCP destination port 113 (IDENT)
permit tcp any any eq ident
!
! allow IGMP
permit igmp any 224.0.0.0 15.255.255.255
!
! allow ICMP echo messages
permit icmp any any echo
!
! allow ICMP echo response messages
permit icmp any any echo-reply
!
! allow ICMP parameter problem messages
permit icmp any any parameter-problem
!
! allow ICMP TTL exceed messages
permit icmp any any time-exceeded
!
! allow ICMP unreachable messages
permit icmp any any unreachable
!
! deny everything else by default and log it
deny ip any any log-input
```

Figure 1



Authors' Addresses

John Kristoff  
Team Cymru  
16W361 S. Frontage Road  
Suite 100  
Burr Ridge, IL 60527  
US

Phone: +1 630 230-5400  
Email: [jtk@cymru.com](mailto:jtk@cymru.com)  
URI: <http://www.team-cymru.org>

Michael O'Reirdan  
Comcast

Fernando Gont  
Universidad Tecnologica Nacional / Facultad Regional Haedo  
Evaristo Carriego 2644  
Haedo, Provincia de Buenos Aires 1706  
Argentina

Phone: +54 11 4650 8472  
Email: [fernando@gont.com.ar](mailto:fernando@gont.com.ar)  
URI: <http://www.gont.com.ar>

