Abstract

This document discusses multi-homing considerations for Distributed-Denial-of-Service Open Threat Signaling (DOTS).

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].

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 December 23, 2017.

Copyright Notice

Copyright (c) 2017 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.
1. Introduction

In many deployments, it may not be possible for a network to determine the cause for a distributed Denial-of-Service (DoS) attack [RFC4732], but instead just realize that some resources seem to be under attack. To fill that gap, the IETF is specifying an architecture, called DDoS Open Threat Signaling (DOTS) [I-D.ietf-dots-architecture], in which a DOTS client can inform a DOTS server that the network is under a potential attack and that appropriate mitigation actions are required. Indeed, because the lack of a common method to coordinate a real-time response among involved actors and network domains inhibits the effectiveness of DDoS attack mitigation, DOTS protocol is meant to carry requests for DDoS attack mitigation, thereby reducing the impact of an attack and leading to more efficient defensive actions.

Table of Contents

1. Introduction .................................................. 2
2. Terminology .................................................... 3
3. Multi-Homing Scenarios ....................................... 3
   3.1. Residential CPE ........................................... 4
   3.2. Multi-homed Enterprise: Single CPE, Multiple Upstream ISPs ........................................... 4
   3.3. Multi-homed Enterprise: Multiple CPEs, Multiple Upstream ISPs ........................................... 5
   3.4. Multi-homed Enterprise with the Same ISP ............... 6
4. DOTS Deployment Considerations ................................ 6
   4.1. Residential CPE ........................................... 7
   4.2. Multi-homed Enterprise: Single CPE, Multiple Upstream ISPs ........................................... 8
   4.3. Multi-homed Enterprise: Multiple CPEs, Multiple Upstream ISPs ........................................... 10
   4.4. Multi-homed Enterprise: Single ISP ...................... 11
5. Security Considerations ....................................... 12
6. IANA Considerations ......................................... 12
7. Acknowledgements ............................................. 12
8. References ...................................................... 12
   8.1. Normative References .................................... 12
   8.2. Informative References ................................... 12
Authors’ Addresses ................................................ 13
[I-D.ietf-dots-use-cases] identifies a set of scenarios for DOTS; almost all these scenarios involve a CPE.

The basic high-level DOTS architecture is illustrated in Figure 1 ([I-D.ietf-dots-architecture]):

```
+-----------+            +-------------+
| Mitigator | ~~~~~~~~~~ | DOTS Server |
+-----------+            +-------------+

+---------------+        +-------------+
| Attack Target | ~~~~~~ | DOTS Client |
+---------------+        +-------------+
```

Figure 1: Basic DOTS Architecture

[I-D.ietf-dots-architecture] specifies that the DOTS client may be provided with a list of DOTS servers; each associated with one or more IP addresses. These addresses may or may not be of the same address family. The DOTS client establishes one or more DOTS signaling sessions by connecting to the provided DOTS server(s) addresses.

DOTS may be deployed within networks that are connected to one single upstream provider. It can also be enabled within networks that are multi-homed. The reader may refer to [RFC3582] for an overview of multi-homing goals and motivations. This document discusses DOTS multi-homing considerations.

2. Terminology

This document makes use of the terms defined in [I-D.ietf-dots-architecture] and [RFC4116].

IP refers to both IPv4 and IPv6.

3. Multi-Homing Scenarios

This section briefly describes some multi-homing scenarios that are relevant to DOTS. In the following sub-sections, only the connections of border routers are shown; internal network topologies are not elaborated hereafter.
3.1. Residential CPE

The scenario shown in Figure 2 is characterized as follows:

- The home network is connected to the Internet using one single CPE (Customer Premises Equipment).
- The CPE is connected to multiple provisioning domains (i.e., both fixed and mobile networks). Provisioning domain (PvD) is explained in [RFC7556].
- Each of these provisioning domains assign IP addresses/prefixes to the CPE. These addresses/prefixes are said to be Provider-Aggregatable (PA).
- The CPE is provided by each of these provisioning domains with additional configuration information such as a list of DNS servers, DNS suffixes associated with the network, default gateway address, DOTS server's name.
- Because of ingress filtering, packets forwarded by the CPE to a given provisioning domain must be sent with a source IP address that was assigned by that network [RFC8043].

![Diagram of typical multi-homed residential CPE](image)

Figure 2: Typical Multi-homed Residential CPE

3.2. Multi-homed Enterprise: Single CPE, Multiple Upstream ISPs

The scenario shown in Figure 3 is characterized as follows:

- The enterprise network is connected to the Internet using one single router.
That router is connected to multiple provisioning domains (i.e. managed by distinct administrative entities).

Unlike the previous scenario, two sub-cases can be considered for an enterprise network with regards to assigned addresses:

1. **Provider Independent (PI) addresses**: The enterprise is the owner of the IP addresses/prefixes; the same address/prefix is then used for communication placed using any of the provisioning domains.

2. **PA addresses/prefixes**: Each provisioning domain assigns IP addresses/prefixes to the enterprise network.

   ```plaintext
   +------+
   | ISP1 |
   +------+
   +------+
   | ISP2 |
   +------+
   |       |
   |       |
   |       |
   +-------+
   Service Providers
   +---------++---------+
   |                    |     Service Providers
   | +-----------------++--+
   | |   +------------++-
   | |     |       |  rtr
   | |     |       |   +--+
   | |     |       |     ... (Internal Network)
   | |     |       |   +-----+
   | |     |       |
   | |     |       |   +----+
   | |     |       |   +----+
   | |     |       |   +----+
   +------++------+
   Enterprise Network
   ``

   Figure 3: Multi-homed Enterprise Network (Single CPE connected to Multiple Networks)

### 3.3. Multi-homed Enterprise: Multiple CPEs, Multiple Upstream ISPs

This scenario is similar to the one in Section 3.2; the main difference is that dedicated routers are used to connect to each provisioning domain.
Figure 4: Multi-homed Enterprise Network (Multiple CPEs, Multiple ISPs)

3.4. Multi-homed Enterprise with the Same ISP

This scenario is a variant of Section 3.2 and Section 3.3 in which multi-homing is provided by the same ISP (i.e., same provisioning domain).

4. DOTS Deployment Considerations

Table 1 provides some sample (non-exhaustive) deployment schemes to illustrate how DOTS agents may be deployed for each of the scenarios introduced in Section 3.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>DOTS client</th>
<th>DOTS gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>Residential CPE</td>
<td>CPE</td>
<td>N/A</td>
</tr>
<tr>
<td>Single CPE, Multiple provisioning domains</td>
<td>internal hosts or CPE</td>
<td>CPE</td>
</tr>
<tr>
<td>Multiple CPEs, Multiple provisioning domains</td>
<td>internal hosts or all CPEs (rtr1 and rtr2)</td>
<td>CPEs (rtr1 and rtr2)</td>
</tr>
<tr>
<td>Multi-homed enterprise, Single provisioning domain</td>
<td>internal hosts or all CPEs (rtr1 and rtr2)</td>
<td>CPEs (rtr1 and rtr2)</td>
</tr>
</tbody>
</table>

Table 1: Sample Deployment Cases
These deployment schemes are further discussed in the following subsections.

4.1. Residential CPE

Figure 5 depicts DOTS signaling sessions that are required to be established between a DOTS client (C) and DOTS servers (S1, S2) in the context of the scenario described in Section 3.1.

The DOTS client MUST resolve the DOTS server’s name provided by a provisioning domain using the DNS servers learned from the same provisioning domain. The DOTS client MUST use the source address selection algorithm defined in [RFC6724] to select the candidate source addresses to contact each of these DOTS servers. DOTS signaling sessions must be established and maintained with each of the DOTS servers because the mitigation scope of these servers is restricted. The DOTS client SHOULD use the certificate provisioned by a provisioning domain to authenticate itself to the DOTS server provided by the same provisioning domain. When conveying a mitigation request to protect the attack target(s), the DOTS client among the DOTS servers available MUST select a DOTS server whose network has assigned the prefixes from which target prefixes and target IP addresses are derived. For example, mitigation request to protect target resources bound to a PA IP address/prefix cannot be honored by an provisioning domain other than the one that owns those addresses/prefixes. Consequently, Typically, if a CPE detects a DDoS attack on all its network attachments, it must contact both DOTS servers for mitigation. Nevertheless, if the DDoS attack is received from one single network, then only the DOTS server of that network must be contacted.

The DOTS client MUST be able to associate a DOTS server with each provisioning domain. For example, if the DOTS client is provisioned with S1 using DHCP when attaching to a first network and with S2 using Protocol Configuration Option (PCO) when attaching to a second network, the DOTS client must record the interface from which a DOTS server was provisioned. DOTS signaling session to a given DOTS server must be established using the interface from which the DOTS server was provisioned.
4.2. Multi-homed Enterprise: Single CPE, Multiple Upstream ISPs

Figure 6 illustrates a first set of DOTS associations that can be established with a DOTS gateway is enabled in the context of the scenario described in Section 3.2. This deployment is characterized as follows:

- One of more DOTS clients are enabled in hosts located in the internal network.
- A DOTS geteway is enabled to aggregate/relay the requests to upstream DOTS servers.

When PA addresses/prefixes are in used, the same considerations discussed in Section 4.1 are to be followed by the DOTS gateway to contact its DOTS server(s). The DOTS gateways can be reachable from DOTS client using a unicast or anycast address.

Nevertheless, when PI addresses/prefixes are assigned, the DOTS gateway MUST sent the same request to all its DOTS servers.
An alternate deployment model is depicted in Figure 7. This deployment assumes that:

- One or more DOTS clients are enabled in hosts located in the internal network.

- These DOTS clients communicate directly with upstream DOTS servers.

If PI addresses/prefixes are in use, the DOTS client can send the mitigation request for all its PI addresses/prefixes to any one of the DOTS servers. The use of anycast addresses is NOT RECOMMENDED.

If PA addresses/prefixes are used, the same considerations discussed in Section 4.1 are to be followed by the DOTS clients. Because DOTS clients are not located on the CPE and multiple addresses/prefixes may not be assigned to the DOTS client (IPv4 context, typically), some complications arise to steer the traffic to the appropriate DOTS server using the appropriate source IP address. These complications discussed in [RFC4116] are not specific to DOTS.
Another deployment approach is to enable many DOTS clients; each of them responsible to handle communication with a specific DOTS server (see Figure 8). Each DOTS client is provided with policies (e.g., prefix filter) that will trigger DOTS communications with the DOTS servers. The CPE MUST select the appropriate source IP address when forwarding DOTS messages received from an internal DOTS client. If anycast addresses are used to reach DOTS servers, the CPE may not be able to select the appropriate provisioning domain to which the mitigation request should be forwarded. As a consequence, the request may not be forwarded to the appropriate DOTS server.

4.3. Multi-homed Enterprise: Multiple CPEs, Multiple Upstream ISPs

The deployments depicted in Figure 7 and Figure 8 apply also for the scenario described in Section 3.3. One specific problem for this scenario is to select the appropriate exit router when contacting a given DOTS server.

An alternative deployment scheme is shown in Figure 9:

- DOTS clients are enabled in hosts located in the internal network.
- A DOTS gateway is enabled in each CPE (rtr1, rtr2).
- Each of these DOTS gateways communicate with the DOTS server of the provisioning domain.
When PI addresses/prefixes are used, DOTS clients can contact any of the DOTS gateways to send a DOTS message. DOTS gateway will then relay the request to the DOTS server. Note that the use of anycast addresses is NOT RECOMMENDED to establish DOTS signaling sessions between DOTS client and DOTS gateways.

When PA addresses/prefixes are used, but no filter rules are provided to DOTS clients, these later MUST contact all DOTS gateways simultaneously to send a DOTS message. Upon receipt of a request by a DOTS gateway, it MUST check whether the request is to be forwarded upstream or be rejected.

When PA addresses/prefixes are used, but specific filter rules are provided to DOTS clients using some means that are out of scope, these later MUST select the appropriate DOTS gateway to be contacted. The use of anycast is NOT RECOMMENDED to reach DOTS gateways.

```
+---+
|    |
+---+    +---+    +---+    +---+    +---+
|S2|-----|G2|-----|C3|-----|G1|-----|S1|
|    +---+    +---+    +---+    +---+
|    +---+    +---+    +---+    +---+
|    |    |
+---+    +---+    +---+
```

Figure 9: Multiple DOTS Clients, Multiple DOTS Gateways, Multiple DOTS Servers

4.4. Multi-homed Enterprise: Single ISP

The key difference of the scenario described in Section 3.4 compared to the other scenarios is that multi-homing is provided by the same ISP. Concretely, that ISP can decided to provision the enterprise network with:

1. The same DOTS server for all network attachments.

2. Distinct DOTS servers for each network attachment. These DOTS servers needs to coordinate when a mitigation action is received from the enterprise network.

In both cases, DOTS agents enabled within the enterprise network may decide to select one or all network attachments to place DOTS mitigation requests.
5. Security Considerations

DOTS-related security considerations are discussed in Section 4 of [I-D.ietf-dots-architecture].

TBD: In Home networks, if EST is used then how will the DOTS gateway (EST client) be provisioned with credentials for initial enrolment (see Section 2.2 in RFC 7030).

6. IANA Considerations

This document does not require any IANA.

7. Acknowledgements

To be completed

8. References

8.1. Normative References


8.2. Informative References


Authors’ Addresses

Mohamed Boucadair
Orange
Rennes  35000
France

Email: mohamed.boucadair@orange.com

Tirumaleswar Reddy
McAfee, Inc.
Embassy Golf Link Business Park
Bangalore, Karnataka  560071
India

Email: TirumaleswarReddy_Konda@McAfee.com