Network Working Group
Internet Draft
Expiration Date: November 2003
File Name: draft-white-sobgp-bgp-deployment-01.txt
June 2003

Russ White
(editor)
Cisco Systems

Deployment Considerations for Secure Origin BGP (soBGP)
draft-white-sobgp-bgp-deployment-01.txt

Status of this Memo

1. Contributors

A large number of people contributed to this draft; we've tried to include all of them here (but might have missed a few): James Ng, Tim Gage, Alvaro Retana, Dave Cook, Brian Weiss, and Iljitsch van Beijnum.

2. Abstract

There is a great deal of concern over the security of routing systems within the Internet, particularly in relation to the Border Gateway Protocol [BGP], which is used to provide routing information between autonomous systems. This draft addresses various deployment scenarios and options using the extensions to BGP outlined in [SOBGP-BGP] in conjunction with [SOBGP-CERTIFICATE] (which is not yet completed or published) and [SOBGP-RADIUS]. Each section of this draft discusses a different deployment situation or deployment option. The final section discusses how private key rollovers can be accomplished with no loss of routing information within soBGP deployments.

3. Overview of the Deployment Scenarios

Each section below discusses a possible deployment option for soBGP; each could be seen as a separate deployment option, or they could be seen as a set of incremental steps from a very simple soBGP deployment in a small network to a large soBGP deployment across an internetwork.

4. Deploying soBGP within Single Devices Along Autonomous System Edges

In it's simplest form, soBGP can be deployed entirely within BGP speakers at the edge of an Autonomous System (AS).

```
+-(eBGP)-+           +-(eBGP)-+
|        |           |        |
v        v           v        V

A--------B-----C-----D--------E

         ^           ^
         |           |
         +--(iBGP)---+
```

In this network, A is sending all the certificates it has learned from other sources to B using the SECURITY message type. It is passing these certificates to D via iBGP, and D is passing these certificates to E via eBGP.

5. Deploying soBGP with Certificate Distribution Within the BGP Protocol and Reflection within an AS

A slightly more complex deployment would continue to distribute the certificates through the BGP protocol, using the SECURITY message type outlined in [SOBGP-BGP], but would offload the work of validating the information to a locally reachable server running RADIUS.

```
          +--(iBGP)--+
+-(eBGP)-+|          |+-(eBGP)-+
|        ||          ||        |
v        vv          vv        V

A--------B-----C-----D--------E
          \         /
         ^ \       / ^
         |  \     /  |
         |   +-F-+   |
         |  (Server) |
         |   ^   ^   |
         |   |   |   |
      (iBGP)-+   +-(iBGP)
```

In this network, A is sending soBGP certificates towards B, along with routing updates and other information. While B is peering through iBGP with D, it is not sending soBGP certificates through this iBGP session; it does not negotiate sending the SECURITY message type to D. B is peering through iBGP to F, a server, but only negotiates carrying the SECURITY message type along this session, so that F only receives soBGP certificates, and no routing updates. F reflects these soBGP certificates to D, which then transmits them to E.

It is also possible to bypass the edge routers in distributing the soBGP certificates within the SECURITY message type.

```
          +--(iBGP)--+
+-(eBGP)-+|          |+-(eBGP)-+
|        ||          ||        |
v        vv          vv        V

A--------B-----C-----D--------E
          \         /
^          \       /          ^
|           \     /           |
|            +-F-+            |
|           (Server)          |
```

```
|            ^   ^            |
|            |   |            |
+-----(eBGP)-+   +-(eBGP)-----+
```

Here, A and B are peering using eBGP, but are only exchanging route information, and not the SECURITY message type. A and F are peering over a multihop eBGP session, and exchanging only the SECURITY message type. B and D no longer have any security information at all; they request information on the validity of any received route from F using the method described in [SOBGP-RADIUS].

Since F is relying only on the interior routing within the local AS to reach the edge of the AS (to reach the link between A and B), the eBGP multihop session is not relying on routes learned from BGP itself to secure BGP.

The eBGP session which F is learning from could also be multihop to another soBGP server in an adjacent AS, rather than to an edge router.

```
   +-(iBGP)-+          +--(iBGP)--+
   |        |+-(eBGP)-+|          |+-(eBGP)-+
   |        ||        ||          ||        |
   v        vv        vv          vv        V

   G---------A--------B-----C-----D--------E
   |                   \         /
   |                    \       /          ^
   H                     \     /           |
(Server)                  +-F-+            |
   ^                     (Server)          |
   |                      ^   ^            |
   |                      |   |            |
   +---------------(eBGP)-+   +-(eBGP)-----+
```

Now, H, A, B, C, D, and E are all exchanging NLRI information only, while F and G are exchanging only SECURITY messages. In this case, B must be manually configured to trust the route to G learned from A, and A must be manually configured to trust the route to F learned from B (or they must use static routing, or some sort of temporary acceptance of the learned routes until the SECURITY messages are all exchanged), to prevent the circularity problem mentioned above. This is more complex than the previous deployment options discussed above.

6. Multihoming Deployment

Multihoming presents a special challenge to the deployment of soBGP within a large scale internetwork.

```
  (---------)            (---------)
 (  AS65401  )          (  AS65402  )
(             )        (             )
 (           )          (           )
   (---A---)              (---B---)
       |                      |
        \                    /
         \-----+      +-----/
               |      |
            (--C------D--)
           (              )
            (   No AS    )
             (----------)
```

Assume No AS has obtained a block of addresses, 10.1.1.0/24, from AS65401, and would like to advertise that same block of addresses through AS65402. Since NOAS has no AS number, it cannot generate any soBGP certificates, and must rely on its upstream providers to work out the security impact in some way. The simplest solution would be, of course, for NOAS to obtain an AS number, and fully participate in soBGP, but barring that, what other solutions are there?

AS65401 could issue a certificate allowing AS65402 to originate just the prefix in question, 10.1.1.0/24, or AS65401 could simply list AS65402 in the certificate covering 10.1.1.0/24 as an authorized originator for this address space (as multiple authorized originators are allowed).

Proxy Advertisement of Certificates

Note there is no requirement for a given entity which originates routes into the routing system to actually originate the corresponding certificates required for the correct origination of the route to be validated, and the AS Path attached to the route to be verified.

```
          (-----------------)
         ( Other Third Party )
           (---------------)
            /             \
           /               \
  (---------)            (---------)
 (  AS65401  )          (  AS65402  )
```

```
   (             )       (             )
    (           )         (           )
      (---A---)             (---B---)
          |                     |
           \                   /
            \-----+      +-----/
                  |      |
               (--C------D--)
              (              )
               (  AS65403   )
                (----------)
```

In this case, AS65401, AS65402, or some other third part may actually advertise the certificates necessary for AS65403 to originate validated routes.

7. Certificate Generation and Private Key Protection

There is only one private/public key pair per entity; certificates are generated as determined by local policy and as required to account for changes in the network. Since the entity's private key is not used in any part of the operations verifying received information, or in generating information to transmit to other devices, these certificates could be generated on some secure central system in the AS, and the results, containing only public keys, can be transmitted throughout the network.

Securing the private key of each entity should be relatively easy in this environment, since the location of the private key can be carefully constrained; no device other than the system which generates the required certificates needs use of the private key.

8. Impact on Performance and Memory Utilization

Very little to no research has been done on the actual performance and memory utilization characterisitics of soBGP as outlined in this and other documents. However, as this is an important area of consideration, we present some suggested analysis below. (In other words, this is a guess).

In terms of memory, each device running sobGP will need to store:

- o Each of the Entitycerts Received. The maximum number of Entitycerts within the routing system would be the number participating autonomous systems multiplied by the number of outstanding Entitycerts from each autonomous system.

This will probably be, at most, three Entitycerts per AS, with a current maximum of 65,000 autonomous systems.

- o Each of the ASPolicycerts (and Their Fragments) Received. The number of ASPolicycerts within the system will probably be similar to the number of Entitycerts within the system, possibly twice as many, given there is only one Policycert valid for any given AS at any time.

- o Each of the PrefixPolicycerts Received. The number of PrefixPolicyCerts within the system will depend on the number of address blocks each participant in the routing system advertises, and will double during key rollover. This could grow to some large number, possibly eight or ten times the number of autonomous systems participating in the routing system.

Performance will depend on the amount of cryptographic work required and the amount of validation which is done on each route checked. If all the steps taken in validating the various certificates are taken during network convergence, it would slow down convergence, possibly significantly.

However, it is possible to deploy soBGP in various other modes, such as:

- o Receive and prebuild all information needed to validate incoming routes before any routes are received, so that no cryptographic operations need to take place when receiving routes.

- o Receive and accept all routes, then receive and build the validation information required to check that the information received was accurate.

- o Allow some secondary device to perform all cryptographic functions, building the validation information needed as convergence is taking place. Check the validity of prefixes after convergence has occured.

Assuming that some combination of optimizations are used, such as precalculating the authorization data, and performing all validation checks after network convergence has occured. Because there are no cryptographic functions which need to be performed while transmitting routes, we anticipate that there will be very little impact on network performance through the adoption of these drafts.

9. References

[BGP]Rekhter, Y., and T. Li, "A Border Gateway Protocol 4 (BGP-4)", RFC 1771, March 1995.

[SOBGP-BGP]
Ng J (editor), "Extensions to BGP to Support Secure Origin BGP (soBGP)", Draft-ng-sobgp-deployment-01.doc, November 2002

10. Editor's Address

Russ White
Cisco Systems
7025 Kit Creek Road
Research Triangle Park, NC 27709
riw@cisco.com