EdgeCorp’s ADN Deployment Scenario

EdgeCorp, the leader in widget technologies, is an international organization based in Atlanta, Georgia, USA. With over 2800 employees in 39 offices worldwide, their Information Technologies (IT) staff is always seeking ways to provide better end-user service at lower costs. As part of this, they have embarked on a full review of all network uses and architecture. Initial focus will be on the sales offices (3 major, 30 minor locations) with a goal of reducing on-site IT managed equipment.

By consolidating remote servers from sales offices back to EdgeCorp’s headquarters in Atlanta, the IT department expects to save dozens of on-site repair visits per year as well as allow better local regulatory compliance. Today, each office has a Microsoft Exchange server which is running outdated software versions on undersized hardware, requiring it be upgraded or replaced. This same server also acts as a file share and software patch repository for all PCs on the local network. A key requirement is that removing these servers – to reduce IT costs – cannot increase the time required to perform typical tasks; any decreased productivity in these sales locations directly impacts corporate revenue. Following lab evaluations, EdgeCorp has decided to deploy Blue Coat ProxySG appliances as part of the server consolidation project.
Future projects leveraging Blue Coat ProxySG’s will investigate:

- enhancing the security of Internet access against spyware/malware
- optimizing data transfers to the backup data center
- addressing data sharing between the research offices
- a streaming video project to be used for corporate news updates and manufacturing training

**EdgeCorp’s ADN Design**

**Atlanta Headquarters Deployment**

Based on the architecture of EdgeCorp’s network the Atlanta Headquarters ProxySG will be deployed out-of-path like a server. This design was selected over the alternatives to minimize the network infrastructure changes necessary. The proxies in Atlanta need only to be configured with basic network settings, joined to the ADN, and configured with the IP addresses/subnets of the servers to be optimized.

As the ADN grows, additional ProxySG appliances can be added to Atlanta as needed. Each device that advertises the same IP addresses/subnets becomes a load-balanced member automatically, allowing the cluster of ProxySG appliances optimizing traffic from branch offices to scale infinitely.

---

**Atlanta Headquarters with a ProxySG**

**Atlanta Headquarters with two ProxySG appliances**
**Branch Office Deployment**

In each branch office, the proxies can be placed inline during the next network maintenance window. Once physically installed with basic network configuration, the branch office proxies will be remotely configured to join the ADN and traffic interception enabled at which point optimization will begin.

**EdgeCorp’s ADN Configuration**

EdgeCorp’s ADN will primarily optimize traffic between branch offices and the Atlanta Headquarters. The ProxySG’s in Atlanta will be deployed “out-of-path” to avoid network redesigns. This type of deployment requires that the ProxySGs be configured with basic IP address information via the serial console (or appliance front-panel) before the Web-based setup wizard can be used. The serial console may be accessed using the provided null-modem cable:

For inline network designs such at the EdgeCorp branch offices, steps one through six can be skipped by browsing to a special URL [https://proxysg.bluecoat.com:8083/](https://proxysg.bluecoat.com:8083/) through a bridged interface on the unconfigured ProxySG

1. Connect the provided serial cable (null modem, DB9) between a PC and the ProxySG to be configured
2. Use the following settings with a terminal emulator program:
   a. 9600 baud
   b. 8 bits
   c. No parity
   d. 1 stop bit
   e. No flow control
Press the “enter/return” key three times to activate the SGOS serial console

Select “W” to perform enough configuration for the web setup wizard to be accessible

Configure the proxy’s IP address, subnet mask, and default gateway on the interface to be connected to the network

After confirming the IP data, switch to the Web Setup Wizard by browsing to https://<configured_ip>:8083/
The Web setup Wizard will walk through the basic configuration, including reconfirming the IP information and security settings (username, password, etc).

Enable ADN
ADN Manager Configurations

- Each ADN will have a ProxySG acting as Primary Manager (and optionally another acting as Backup Manager) - during the basic setup each ProxySG will be configured with the IP addresses or "self" based on its role in the ADN

  a. For the first Atlanta ProxySG, which will be primary ADN Manager, choose "self" as the Primary ADN Manager and enter the New York ProxySG's IP as the Backup Manager

  b. For the New York proxy choose "self" for the Backup Manager and enter the first Atlanta ProxySG as Primary Manager

  c. For all other ProxySG appliances (including other proxies in Atlanta) configure the IP addresses of the Primary and Backup ADN Managers

Here the configuration of branch and Headquarters ProxySGs begin to differ. It is suggested that ProxySG appliances nearest the servers be configured first. For inline deployments these steps may be skipped. However in EdgeCorp’s design the Atlanta proxies are out-of-path, thus step #10 is necessary for ADN traffic from branch office ProxySGs to reach the Atlanta ProxySG appliances.
Wizard Differences in Atlanta Headquarters ProxySGs

1. When the ProxySG is deployed out-of-path and will be acting as the server-side of the ADN communication, advertise the server subnets to be accelerated.

2. As server-side only ProxySG appliances, the Atlanta proxies do not need to intercept any traffic.

3. Configuration of the Atlanta ProxySG appliances is now complete. Click “next” through all remaining menus and confirm the settings to be applied.
Wizard Differences in Branch Office ProxySG

1. Branch office ProxySG appliances are inline; there are no server subnets to advertise.

2. Client-side ProxySGs should intercept traffic so that it flows through the ADN. EdgeCorp therefore, will intercept HTTP for Web browsing, CIFS for file-shares, and Email traffic in the branch offices.

3. ProxySG appliances can provide both an Application Delivery and a Network Security solution. This step will modify the default settings of the device to suit the primary use - select "MACH5 defaults".

4. Configuration of the branch ProxySG is now complete and traffic optimization will begin occurring for all new connections on intercepted protocols.