What is a Transparent ADN?

When a WAN optimization solution is deployed, it typically consists of one or more core locations which are accessed by a number of edge sites (or branches). When a ProxySG appliance at the edge communicates with a ProxySG appliance at the core, the communication takes place over a connection called an ADN tunnel. If the core ProxySG appliance(s) have been deployed inline and transparent ADN tunnels have been configured, the communication will appear transparent in the network; both the destination IP address and port of the original client request will be preserved. If the Blue Coat SGOS feature “reflect-client-ip” is enabled, the source IP of the connection will also be preserved.

Why should I implement a Transparent ADN?

The key benefit to implementing a Transparent ADN is to preserve transport and connection information across the WAN that can be critical in providing visibility into the traffic on the network. The alternate solution, an ADN that utilizes explicit ADN tunnels, results in all WAN traffic between the edge and the core appliance being sent to a fixed port, with the source and destination IP addresses appearing as that of the appliances. While acceptable for many deployments, many customers have network management tools that require visibility into IP and port information in traffic flows (Netflow, etc.) or have network policy that is specifically enforced solely by IP or destination port (security, routing, traffic shaping). Vendors only offering an explicit tunneling solution, therefore, are at a distinct disadvantage. In a Transparent ADN, this information is preserved, allowing administrators to seamlessly deploy into an existing network with no additional changes.

Another benefit of a Transparent ADN is that it eliminates the need to configure ADN routing information on each peer in the network. Instead, ProxySG appliances participating in a Transparent ADN are able to take advantage of auto-discovery of ADN peers. ADN nodes must still register with the ADN Manager, however, to establish membership in the ADN.

How does a Transparent ADN work?

In order to take advantage of a Transparent ADN, the core ProxySG appliance(s) must be deployed physically inline, or virtually inline (such as with WCCP). This allows requests destined for servers behind the core ProxySG appliance(s) to be transparently intercepted. The key feature of a Transparent ADN is the ability to maintain the source IP of the client as well as the destination IP and port of the server. This is accomplished with transparent ADN tunnels and a feature called “reflect-client-ip”. To preserve the source IP, edge ProxySG appliances must have the “reflect-client-ip” option enabled. The “reflect-client-ip” feature results in the ProxySG appliance preserving the source IP address of the client when sending its server-side request. This feature is independent of the Transparent ADN solution. For transparent ADN tunnels to preserve the destination IP and port, these connections must implement a unique way of identifying themselves as ADN connections; this is achieved using a...
TCP option flag during connection setup. When an edge ProxySG appliance initiates a connection to the core ProxySG appliance, it inserts a TCP option flag into the SYN packet which contains its own peer ID. This allows the core ProxySG appliance to verify the ADN membership of the edge ProxySG appliance and, therefore, identify the connection as an ADN connection. If the ProxySG appliance sending the SYN is not part of the same ADN as the receiving ProxySG appliance, an ADN tunnel is not established; the core ProxySG appliance treats the connection as a standard forward-proxy (non-ADN) connection. If they are part of the same ADN, the core ProxySG appliance sends a SYN ACK in return which contains a TCP option flag that identifies itself with its own peer ID. After the edge ProxySG appliance verifies ADN membership of the core ProxySG appliance, it completes the TCP handshake by responding with an ACK. Both appliances have identified themselves at this point. The next step in utilizing the ADN tunnel is to exchange protocol, byte cache dictionary version, and other information. This is done over the ADN tunnel just established.

The TCP option flag that is used to establish the ADN tunnel and negotiate dictionary size is only recognized by those peers in the ADN. If, for some reason, a packet with the TCP option flag is received by an origin server or any other appliance that is not part of the ADN, it is ignored.

Blue Coat Difference

Transparent, Authenticated, and Secure ADN Tunnels

Blue Coat transparent ADN tunnels provide a simple, scalable mechanism for accessing ADN content. For added security, Blue Coat ProxySG appliances support mutual authentication, and authentication for the users and servers whose traffic they accelerate. We are also the only vendor that offers secure ADN tunnels that encrypt communications between appliances with SSL. This combination allows Blue Coat to provide a unique solution that removes the historic trade-off between security, visibility, and performance.

Ease of Deployment

A Transparent ADN minimizes the configuration necessary to deploy an ADN while also allowing current network management tools and policies to continue to function. Because ADN network traffic is visible, administrators can deploy ProxySG appliances into the existing network infrastructure with minimal impact. This translates to faster roll-outs which can be a critical success factor when deploying hundreds of appliances.