



## **Maestro Features And Benefits**

## **Server Side Optimization Features**

<b>Feature</b>	<b>Connection Consolidation</b>
<b>Description</b>	<ul style="list-style-type: none"> <li>• The CN-5000 terminates all TCP connections from the clients.</li> <li>• The CN-5000 maintains a small number of permanent, persistent connections with the server.</li> <li>• The CN-5000 acts as a true TCP termination point:               <ul style="list-style-type: none"> <li>○ It terminates and owns all client-side TCP connections.</li> <li>○ It initiates and owns all server-side TCP connections.</li> </ul> </li> <li>• All user requests from the many client-side connections are sent to the servers over the few persistent connections.</li> </ul>
<b>Benefits</b>	<ul style="list-style-type: none"> <li>• The server is relieved of 3 major points of TCP-related burden/overhead:               <ul style="list-style-type: none"> <li>○ The number of TCP setup/teardown operations is dramatically reduced.</li> <li>○ The number of simultaneous connections a server needs to deal with is drastically reduced.</li> <li>○ All TCP connections to the server are LAN-based. The server thinks that the clients are on the same LAN as the server:                   <ul style="list-style-type: none"> <li>▪ The server can transmit data at the maximum speed allowed by the network.</li> <li>▪ The server does not have to spend any resources on delivering data over slower, more problematic WAN-based client sessions.</li> </ul> </li> </ul> </li> <li>• CPU resources are freed up for the server. Now, instead of dealing with network-related issues, the server can dedicate its resources to actual application processing.</li> <li>• The server can serve data in a truly optimized network environment. Content serving is with minimum overhead and maximum speed.</li> </ul>

<b>Feature</b>	<b>Intelligent Connection Management Algorithm</b>
<b>Description</b>	<ul style="list-style-type: none"> <li>• The number of connections opened to each server is based on the server OS and the ratio between requests for static vs. dynamic content</li> <li>• The connection profile is dynamically adjusted according to the load of the server.</li> </ul>
<b>Benefits</b>	<ul style="list-style-type: none"> <li>• The best performance can be gleaned from a server since the optimal number of connections is opened to each server according to the type of server.</li> <li>• Dynamic content (which usually takes longer to serve) never interferes with serving of static content (which usually takes shorter). Users requesting small, static files are never hampered by users requesting larger, dynamic files (the phenomenon is commonly referred to as "Head of Line Blocking").</li> </ul>

<b>Feature</b>	<b>Request Buffering</b>
<b>Description</b>	<ul style="list-style-type: none"> <li>• User requests are only passed to the server after they're received by the CN-5000 in their entirety.</li> </ul>
<b>Benefits</b>	<ul style="list-style-type: none"> <li>• The server does not spend resources/buffers waiting for the user request to complete over a slower WAN-connection. This is an important</li> </ul>

	<p>overhead pain point, especially if the request is long (long URL, long cookie header, HTTP POSTs, etc.).</p> <ul style="list-style-type: none"> <li>• The longer the user connection, the more chance of it arriving in multiple packets, which means there's a possibility of packets arriving out of order or the session being subjected to retransmissions. Because the CN-5000 buffers the request and sends it to the server as a LAN client, the server is never exposed to these anomalies. Therefore, the server is shielded from these conditions and can operate in a truly optimized environment.</li> </ul>
--	---

<b>Feature</b>	<b>Response Buffering</b>
<b>Description</b>	<ul style="list-style-type: none"> <li>• The CN-5000 buffers responses from the server, on their way to the client.</li> <li>• Responses are received from the server at maximum LAN speed, and then sent to the client according to the speed of the client's connection.</li> </ul>
<b>Benefits</b>	<ul style="list-style-type: none"> <li>• Again, this is another mechanism that truly shields the server from slower client connections.</li> <li>• The server is capable of sending data at maximum LAN speed, with no regard to what speed the client can receive the data at. The CN-5000 becomes the intermediary that will deal with the slower client connections. The server can serve content quickly (at Gigabit speeds) and move on to the next request.</li> </ul>

<b>Feature</b>	<b>SSL Acceleration / Secure Connection Processing</b>
<b>Description</b>	<ul style="list-style-type: none"> <li>• The CN-5000 terminates all SSL sessions from the clients at multi-gigabit speeds.</li> <li>• The requests arriving from the clients over these secure connections are sent to the server in one of two ways: <ul style="list-style-type: none"> <li>○ Over clear text HTTP</li> <li>○ Over server-side SSL connections that are done through lighter encryption schemes and last permanently</li> </ul> </li> </ul>
<b>Benefits</b>	<ul style="list-style-type: none"> <li>• SSL handshakes are massively CPU-consuming. The server is completely offloaded with dealing with the many SSL session setups that client environment would require.</li> <li>• A fully secure request/response chain can still be maintained (secure requests arriving at the CN-5000 through SSL connections and being sent to the server through SSL connections). However, even though the server needs to deal with SSL connections from the CN-5000, the overhead of drastically minimized: <ul style="list-style-type: none"> <li>○ The secure connections to the server are established through lighter security schemes using shorter encryption keys. Computational resources for setting up these sessions are significantly less.</li> <li>○ The secure connections between the CN-5000 and the server are permanent. So, there is no need for the server to continually deal with SSL session setup.</li> </ul> </li> </ul>

## **Client and Network Side Optimization Features**

<b>Feature</b>	<b>Content Compression</b>
<b>Description</b>	<ul style="list-style-type: none"> <li>• The content served from the servers is compressed at the CN-5000 before it's sent to the client.</li> <li>• Standard-based compression, supporting both Gzip and Deflate, which are compatible with all popular browsers.</li> <li>• Compression is performed at rates up to 1 Gbps. Compression ratio is the same as the fastGzip algorithm.</li> </ul>
<b>Benefits</b>	<ul style="list-style-type: none"> <li>• Depending on the content of the site, outbound bandwidth for a site can be reduced by 50%, reducing the number of bits that traverse the link from the data center to the client:               <ul style="list-style-type: none"> <li>○ Data center bandwidth utilization is reduced lowering prices and delaying the need for additional bandwidth.</li> <li>○ The client experiences improved response time since the compressed content arrives faster than the non-compressed version.</li> </ul> </li> <li>• Servers are also capable of compressing content themselves. But, compression has associated overhead. By offloading the task to the CN-5000, the server is relieved of this burden.</li> </ul>

<b>Feature</b>	<b>Fast TCP</b>
<b>Description</b>	<ul style="list-style-type: none"> <li>• Client connections typically go through a "slow start" period as the two TCP end-points try to determine the optimal transmission speed for the TCP session.</li> <li>• The CN-5000 learns optimal transmission speeds per client IP address and stores them for future connections from this client. Therefore, the slow start process is bypassed on subsequent connections from this user.</li> <li>• On the server side, all TCP connections operate at maximum LAN speed.</li> </ul>
<b>Benefits</b>	<ul style="list-style-type: none"> <li>• Client TCP connections reach optimal transmission levels quickly. The client will notice faster response times since data is sent to the client from the CN-5000 at optimal/maximum speeds.</li> <li>• Server-side connections operate at maximum network speed, allowing the server to transmit data at the highest rates allowed by the network.</li> </ul>

## **Security and Protection Features**

<b>Feature</b>	<b>Denial of Service Protection</b>
<b>Description</b>	<ul style="list-style-type: none"> <li>• Protection against DoS and DDoS attacks at L4 and L7               <ul style="list-style-type: none"> <li>○ L4: The robust system architecture inherently protects against L4 attacks such as SYN Flood, TCP Flood, and Open/Close attacks.</li> <li>○ L7: The L7 DDoS feature protects against URL attacks, where requests for legitimate URLs are made in massive volumes through drone machines on the Internet. The CN-5000 can use an advanced algorithm to differentiate between real human clients and malicious robotic drones.</li> </ul> </li> <li>• Protection against (D)DoS attacks based on SSL handshakes.</li> </ul>

	<ul style="list-style-type: none"> <li>○ SSL handshakes are huge burdens for the CPU. An attacker can kill a server by continuously establishing new SSL sessions.</li> <li>○ The CN-5000 is the termination point for all SSL connections. Its massive scale allows it to handle large number of SSL handshakes and control the rate at which they're opened.</li> <li>○ If the CN-5000-&gt;Server communication is encrypted, all handshakes are managed by the CN-5000. No malicious attacker can get to the server directly to open an SSL session.</li> </ul>
<b>Benefits</b>	<ul style="list-style-type: none"> <li>• DoS attacks at L4 and L7 can kill CPUs and TCP stacks. By acting as a true TCP termination point before the servers, these high level attacks can be stopped by the CN-5000.</li> <li>• The robust TCP processing engine of the CN-5000 is not susceptible to the same attacks that can cause harm to TCP stacks on the servers. Additional internal mechanisms ensure that the CN-5000 protects itself and the servers from these attacks.</li> <li>• URL attacks at L7 are incredibly difficult to identify since they are for legitimate URLs. The CN-5000 uses an advanced mechanism to differentiate between real (human) users and brainless machines that act as DDoS attack points. This way, only real users can get to the servers.</li> <li>• Since all SSL sessions are terminated at the CN-5000, the server is never exposed to any SSL sessions originating from the Internet or any other malicious sources. <ul style="list-style-type: none"> <li>○ The CN-5000 controls all client-bound SSL traffic. If there is any SSL traffic to the server, it's controlled fully by the CN-5000.</li> <li>○ For server-side encryption, the number of handshakes between the CN-5000 and the server is minimal, so the CN-5000 does not put any extraneous unnecessary burden on the server.</li> </ul> </li> </ul>

<b>Feature</b>	<b>Peak Load Protection</b>
<b>Description</b>	<ul style="list-style-type: none"> <li>• Peak load conditions are harmful to servers because when peak loads are reached, the clients don't slow down. Therefore, the servers are simply overwhelmed and cannot deal with the massive client load</li> <li>• Internal buffering on the CN-5000 (both for requests and responses) control the flow of traffic between the clients and the servers. The servers operate to their maximum ability, without being overloaded.</li> <li>• Essentially, the CN-5000 allows the servers to work as hard as they can without overloading them.</li> </ul>
<b>Benefits</b>	<ul style="list-style-type: none"> <li>• In cases where the client load would normally overwhelm a server, the CN-5000's buffering mechanisms shield the server from the requests that it could not handle.</li> <li>• The CN-5000 allows the server not to be overloaded. The server can work to its peak potential, and new requests will only be sent to the server if there's an idle connection and the server can handle the request.</li> </ul>