GHOSTSENTRY™

Product Information

Who needs GhostSentry?

If a vendor remotely manages site equipment, but site staff is responsible for restricting or logging remote access, GhostSentry can help. Other solutions are difficult to manage for site personnel and vendors. GhostSentry is plug-and-play simple.

What's the benefit? What do you get out of it?

GhostSentry can help you comply with policies and regulations that require logging network access. With GhostSentry, your staff can easily track access to your site, with a simple approval workflow, and a clear log of activity. GhostSentry allows end-users to request access in-line, and administrators to immediately manage that request from anywhere, even a smartphone.

What makes us unique?

Our simple cloud-based administration and log make deploying and managing very easy. Two technical factors make GhostSentry different. Our technology allows us to place the device inline and accomplish user authentication, without any IP addresses on the protected network. Second, it works just fine with overlapping IP addresses, so a single piece of hardware can handle networks with identical IP address ranges and still work great. You gain important compliance logs without complicated setup.

Features

- Controls access by username
- Allows on-demand access request
- Allows scheduled access request
- Secure inline authentication
- Logs user access
- MICS compliant standard reporting
- Requires "Reason for Access" prior to access (per MICS)
- Controls access of independent networks
- Compatible with secure or isolated vendor networks
- Requires no IP address changes on vendor network
- Controls existing vendor-maintained circuits
- Does not require an agent on the vendor PC
- Does not require an agent on the destination server
- Requires "Description of Work Performed" at entry (per MICS)

F&C CPAs

GHOSTSENTRY™

Product Information

Deep dive

In the GhostSentry appliance, pairs of interfaces are configured as a bridge (we call the pair a “gate”), so that all packets coming from side A initially travel unobstructed to side B, and vice versa. Then, a transparent firewall is activated to block all traffic except ARP, and optionally DNS, DHCP, and ICMP, or other protocols the administrator wants or needs to allow. No IP addresses are assigned to the bridge, and the specific addresses of the traffic traversing the bridge are irrelevant to the process. When an end-user wishes to pass from a device on side A to a device on side B (with an IP address of B1.B1.B1.B1), the procedure is to open a web browser and point to the destination with the URL http://B1.B1.B1.B1:142. When the TCP session attempts to pass through to destination port 142, GhostSentry redirects the traffic to a captive portal screen on the authentication web server. This redirection happens through a full translation of the source and destination IP address and MAC address. Regardless of where the packet originated, the packet reaches the authentication server with a privately assigned address, and valid internal MAC address. After the end-user completes successful authentication and authorization, and for his source IP address, future traffic is allowed and logged.

In GhostSentry, controls have been created for the site administrator, so that an end-user can request access through their in-line connection for a specific daily time-slot, on defined days of the week. The request also contains the intended purpose of the connection, and can include additional information such as licensing numbers, or procedural steps. The request is passed to the administrative web interface, and to the administrator’s email address so that approval can be performed from a smart-phone or other internet connected device. Further, the administrator can create and approve special rules that allow traffic for automated systems such as WAP, WABC, or health monitoring. In this way, SNMP or other health monitoring can be automated, but still approved and logged.

Note that the entire GhostSentry process works perfectly without the client network(s) being exposed to the Internet at all. Since the device is in-line with their secure network, no access can circumvent their physical or logical network security. Only end-users actually on side A of the network can authenticate and reach side B. This is an important factor in implementation, since many NOCs have a “closed” network, and isolate their workstations to their own private address space. Each of the port pairs (collectively called “gates”) is isolated so that end-user traffic on the physical gate 1 cannot mix with gate 2. Even if the IP addresses overlap between clients connected to the physical gates, the process works properly, because only the physical port is used for directing traffic.

F&C CPAs