Forcepoint NGFW
Sidewinder Application-Level Proxy

Forcepoint Next Generation Firewall (NGFW), with its built-in Sidewinder application proxy technology, provides an unmatched level of security for application-level network traffic. This technology mediates access and data flows between users and the servers running mission-critical applications, isolating them from transport- and application-layer attacks over SSH/SFTP, HTTP/HTTPS, FTP, TCP, and UDP.
Executive summary

Modernizing your network, improving capacity and availability, and gaining full visibility into your networks and policies—while maintaining the highest level of security across your entire network—is vital. For government agencies and organizations, Forcepoint Sidewinder proxy firewalls have played a pivotal role in securing the most sensitive, mission-critical environments.

Today, the best of Sidewinder’s application proxy technology is now incorporated into Forcepoint NGFW. With it, organizations can leverage next generation capabilities without sacrificing the application-level security you rely on to protect your data. With this integration, you can extend this functionality at a scale and speed not previously possible.

With Forcepoint NGFW, you can deploy and manage thousands of firewalls, IPSs, VPNs, and SD-WANs with built-in clustering for load balancing for high availability—in minutes, all from a single console. Processes can quickly become strong, accurate controls that stop ransomware and other intrusions, while letting you properly handle encrypted traffic.

Application-layer proxy

While stateful inspection firewalls are capable of monitoring open connections, they are incapable of inspecting application-layer traffic. Stateful firewalls allow external sources to make direct connections with internal servers. This direct exchange of packets between external clients and internal application servers could compromise security.

For example, if you were to allow HTTP traffic through your firewall, a stateful inspection firewall would not prevent an HTTP-based attack. With an application-layer proxy, on the other hand, there is no direct communication between client and internal servers. Instead, the connection is split in two. The client opens a connection with the firewall, and the firewall opens a separate connection to the server on the client’s behalf (see Figure 1). The client interprets the firewall as the server (Transaction 1), and the server interprets the firewall as the client (Transaction 2).

Transaction is split in two: to client, firewall appears to be the server (transaction #1); to server, firewall appears to be the client (transaction #2)

Figure 1: Application-Layer Proxy functionality
**Forcepoint NGFW Sidewinder proxies**

For years, Forcepoint has been protecting mission-critical applications in some of the most sensitive networks around the world. Forcepoint proxies (SSH, HTTP/HTTPS, FTP/SFTP, TCP, and UDP) can provide network-level proxies, protocol validation, and configurable application-level protocol filtering and translation. These software-based module proxies are primarily intended for users in high assurance environments such as government or financial institutions. In these environments, Forcepoint NGFW is not only able to inspect the traffic, but also control which commands can be issued from within the encrypted data stream. In other words, in addition to being a network segmentation, it can split connections between front-end servers and back-end servers. As shown in Figure 2, the firewall doesn’t forward the original packet from one end to the other—only the data from the original packet is forwarded.

**The benefits of using Forcepoint Sidewinder application-layer proxies:**

- **More extensive attack prevention:** prevent most attacks that involve modifying IP, TCP, or UDP headers to evade detection. These kinds of attacks cannot always be detected using signature-based detection alone.
- **Covert channel prevention:** prevent attempts to covertly send data in the header bits of IP, TCP, or UDP packets.
- **More detailed control of application protocols:** take more granular control of application protocols, e.g., using the SSM HTTP proxy for detailed HTTP header filtering and control.

![Figure 2: Forcepoint NGFW Sidewinder Application-Layer Proxy](image-url)
Forcepoint NGFW Sidewinder SSH proxy example

The Forcepoint NGFW Sidewinder SSH proxy allows you to restrict the types of traffic and the commands that can be used with SSH connections. The firewall is establishing an SSH tunnel between the firewall and the client and an SSH tunnel between the firewall and the server, with the firewall functioning as a proxy. As traffic flows between the client and the server, the firewall is able to distinguish whether the SSH traffic is being routed normally or if it is using SSH tunneling (port forwarding).

Using this type of proxy means you can enforce policies that allow only reads and no writes to the server or can block deleting or renaming files on the server. A simple packet filtering policy rule or a pass-through rule with generic proxy is not able to control the communication between client and server.

USE CASE: ACCESSING PCI SERVERS

One important use of the proxies is in a PCI-DSS compliant environment. To securely transmit data from Point-of-Sale terminals to PCI servers rather than batch-transferring data through unsecure application layers, you can enforce endpoints to use SFTP proxy service on an encrypted path.

As seen in the policy rule shown in Figure 4, only authorized endpoints and terminals can access PCI servers via SFTP proxy service. In this example, you are not only able to inspect the traffic, but also control commands that can be used from within the encrypted data stream.

To make this more secure, you can apply a policy allowing only read and write capabilities and blocking any deleting, renaming, or changing of the files.
You can also enforce encryption strength for the connections. In the Protocol Parameters, you can separately specify the key type and key length for each side of the connection. The Client Advanced Settings define settings for connections between the Forcepoint SSH Proxy and the client; the Server Advanced Settings define settings for connections between the Forcepoint SSH Proxy and the server.
SUMMARY

The Forcepoint NGFW built-in Sidewinder application proxy technology offers an unmatched level of security for mission-critical, application-level network traffic. The technical differentiators and customer benefits include:

- Adding capabilities of inspecting application layer of traffic with the benefits of an NGFW
- Mediating access and data flow between users and the servers on which mission-critical applications run
- Preventing attempts to covertly send data in the header bits of IP, TCP, or UDP packets
- Inspecting traffic while controlling which commands can be issued from within the encrypted data stream
- Assisting in meeting PCI-DSS and other compliance requirements

To learn more, visit forcepoint.com/NGFW