



The Secure Path to Scalable WAN Acceleration

Silver Peak's Secure Content Architecture™

Enterprises are increasingly investing in server centralization and/or business continuity initiatives as a means of protecting critical business information. By consolidating resources into purpose-built data centers, enterprises can physically protect critical information and more easily track vital assets. In addition, data can be backed up more easily and with consistent regularity, minimizing the ongoing risk of exposure.

CIOs are turning to Wide Area Network (WAN) acceleration as a key enabler for these strategic IT initiatives. By overcoming common WAN obstacles, such as limited bandwidth, network congestion, and high latency, these devices ensure that consolidation does not come at the expense of application performance.

Ironically, however, WAN acceleration can actually introduce new security challenges if not implemented properly. For example, deploying a WAN acceleration appliance with unencrypted drives can actually create risk where none previously existed.

Silver Peak products are built on a Secure Content Architecture™ that enables enterprises to deploy WAN acceleration with complete confidence. The Silver Peak solution incorporates the latest in encryption technology to protect data at all times – at rest and in transit across the WAN. In addition, Silver Peak makes it easy to configure, enforce, and monitor security policies from a central location through the Silver Peak Global Management System (GMS), and employs mechanisms to ensure that security does not come at the expense of network performance or scalability. The result is end-to-end secure WAN acceleration.

Secure Content Architecture

Silver Peak's Secure Content Architecture assures security and privacy of information at both the data plane layer and the control plane layer.

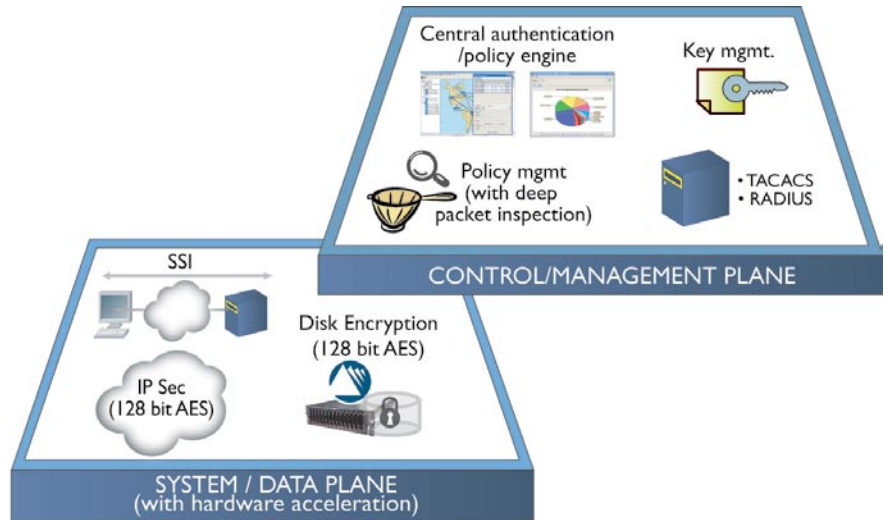


System/Data Plane Protection:

Silver Peak protects data at all times – when residing on system hardware and when traversing the WAN. Data security and privacy are achieved with the following techniques:

- **Disk encryption:** Disk encryption is required on any WAN acceleration device that stores information locally – from disk based data reduction to file caching (e.g., WAFS). It is the only fail-safe way of protecting information in the event that an entire device (or individual hard drive) are compromised. In addition, it is the most secure way of ensuring that company sensitive data that may reside in the data store cannot be accessed in the event that an appliance changes hands – i.e. is transferred between locations, returned to a supplier for repair, returned after an evaluation period, etc.

Disk encryption also protects WAN acceleration appliances from unauthorized access. Without encryption, it is possible to pull useful information out of the data store. Even if data is “scrambled” through the course of operations and stored in a proprietary fashion, it is still possible that large pieces of information are stored on the appliance as contiguous blocks. These blocks can be large enough to store “useful” information to a hacker, such as



a name, social security number, and credit card information. If someone gains access to the device, simple commands can be used to extract this data. By encrypting the local data store, this risk is eliminated.

Silver Peak uses 128 bit AES encryption to thoroughly protect all information stored within NX appliances. With dedicated processors for hardware acceleration, disk encryption takes place at line rate, ensuring that data privacy does not come at the expense of performance and scalability.

- **Secure Transport (IPsec):** IPsec is often used to ensure data remains secure and private when transferred over the WAN. Industry best practices recommend that a 128 bit encoding scheme (or higher), such as AES or 3DES, be used in conjunction

with IPsec to perform encryption. Older methods, such as 56 bit DES, are easily broken, which is why industry leaders no longer use 56 bit keys.

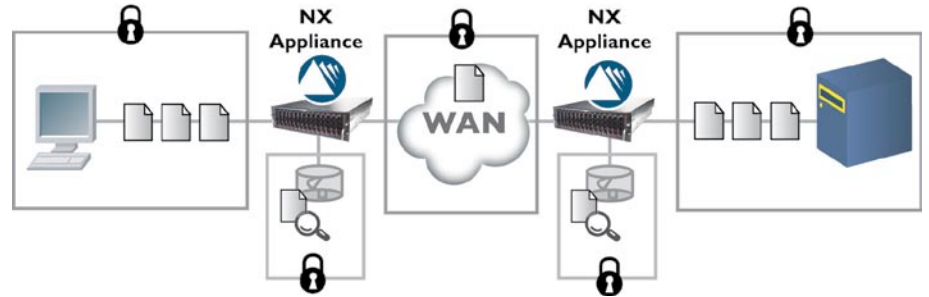
IPsec can be performed outside of the WAN acceleration appliance. But, if it occurs upstream of this device, the appliance must terminate the IPsec session, perform its acceleration functions, and then re-establish its own IPsec session across the WAN. Doing IPsec downstream of the appliance, such as in a WAN router, can result in poor performance due to the processor-intensive nature of this function. For these reasons, it is often desirable to perform IPsec directly within the WAN acceleration appliances.



Silver Peak supports 128 bit IPsec (using AeS for encryption.) Dedicated hardware ensures that the IPsec encryption process does not adversely impact the performance of Silver Peak appliances. This paves the way for additional encryption technologies that can be used to secure transmission across the WAN in the future.

- **Secure Socket Layer (SSL):** SSL delivers end-to-end security on a per-session basis between two peers, such as a web browser and a server in the data center. It is fairly straightforward to perform basic acceleration techniques on SSL traffic, including Quality of Service (QoS) and TCP acceleration. It is more complicated, however, to perform data reduction and compression. These techniques require that the WAN acceleration appliance securely become part of the trusted security domain, “terminate” the SSL traffic, decrypt the SSL streams, optimize the traffic, then re-encrypt (or “re-terminate”) the SSL traffic.

The above process presents a security hole if the data is stored in-the-clear within the acceleration appliance. As a result, encrypting data at rest is a co-requisite when providing full acceleration techniques and data reduction on SSL traffic streams. To avoid introducing jitter and latency during the process of “terminating” and



“un-terminating” the SSL traffic, fast authentication and high speed encryption and decryption is also required within the WAN acceleration appliance. This is achieved with hardware acceleration.

By offering 128 bit disk encryption with hardware acceleration, Silver Peak delivers a hardware platform that is ideally suited for accelerating SSL traffic. This includes Quality of Service (QoS) and TCP acceleration support today, with future support for key and certificate management, compression, and data reduction via a seamless software upgrade.

Management/Control Plane Protection:

Silver Peak employs a variety of methods to control the manner in which traffic traverses the WAN. These include:

- **Fine grained policy management:** Silver Peak’s NX appliances make intelligent policy decisions in real-time to improve the security and performance of WAN

traffic. For example, they can determine which WAN acceleration techniques should be applied to individual flows of traffic to optimize performance, or if no techniques should be applied at all. In addition, Silver Peak NX appliances can dynamically enforce Quality of Service (QoS) parameters on this traffic, including real-time bandwidth allocation. Furthermore, the Silver Peak solution can choose to prioritize traffic based upon pre-established security policies. For example, IT staff can rate limit music/video sharing, instant messaging, or other traffic deemed “undesirable” from traversing the WAN.

Silver Peak NX appliances employ stateful deep packet inspection to make intelligent acceleration decisions when handling applications that use ephemeral (i.e. temporary) ports, such as Voice over IP (VoIP) and FTP. This is in addition to port and flow based filtering schemes, providing granular control and applicability across the widest breadth of enterprise applications.



By leveraging a variety of hardware and software components, Silver Peak provides the highest level of data protection today, while ensuring seamless support of future security technologies tomorrow.

- **Centralized control:** Silver Peak's Global Management System (GMS) enables Access Control Lists (ACLs) and other advanced authentication policies to be centrally configured and enforced. This includes "device authentication", whereby only valid Silver Peak appliances are allowed on the network, and "connection authentication", whereby connectivity can only be established between trusted Silver Peak devices (with approved IP addresses). These features protect a Silver Peak network from session hijacking or man-in-the-middle (MiM) types of attacks.

IPsec parameters can easily be configured between appliances for secure transport across the WAN. With the Silver Peak solution, network administrators can also manage passwords and access rights on each appliance and set logging parameters for granular control and detailed auditing capabilities.

- **Secure Access:** Access to all Silver Peak devices is tightly controlled using TACACS+ and/or RADIUS. This ensures complete AAA protection, including user tracking and auditing per-command authorization, and group based authentication privileges. Enterprises can use their existing AAA / security infrastructure, eliminating the need to maintain separate databases for administrative passwords, credentials, and other security privileges.

- **Visibility:** By exporting Netflow statistics, Silver Peak provides IT managers with detailed visibility into traffic behavior for rapid problem identification and resolution. In addition, Netflow information can be sent to Intrusion Detection/Protection Systems (IDS/IPS) and other security tools for advanced data protection. These devices can in turn provide dynamic policy updates that can be used to block a particular host from using the WAN.

Conclusion

Silver Peak's Secure Content Architecture provides complete protection of enterprise traffic – at rest and across the WAN. Security policies are easy to configure, enforce, and monitor, and hardware acceleration ensures that security does not adversely impact network performance or scalability.

The Silver Peak solution was designed from the ground up with secure acceleration in mind. By leveraging a variety of hardware and software components, Silver Peak provides the highest level of data protection today, while ensuring seamless support of future security technologies tomorrow.

Security. Scalability. Performance. Ease of Use. With Silver Peak's WAN acceleration appliances, you can have it all.

