Accelerated IPSec

Frequently Asked Questions (FAQ)

1. What is an IPSec VPN?

Internet Protocol Security (IPSec) is a standard set of protocols describing how to ensure the authenticity, privacy, and integrity of data in transit. A Virtual Private Network (VPN) secures traffic between locations as well as if the traffic was within a location.

2. What is Accelerated IPSec?

Accelerated IPSec combines the best of site-to-site VPN security with the performance and ease-of-use of WAN acceleration. Any protocol can now be as secure and perform as well across the Internet as across the LAN.

3. Who can benefit from Accelerated IPSec?

Accelerated IPSec's performance and usability makes it well suited for networking and storage teams. **Storage teams** can now encrypt and accelerate site-to-site replication traffic without having to configure or install networking equipment. **Networking teams** can use Accelerated IPSec to address the performance and security problems of any protocol within the organization.

4. Why is Silver Peak introducing Accelerated IPSec now?

Silver Peak has long offered IPSec as one of its tunneling mechanisms. In light of recent concerns around potential wiretaps and security breaches, many organizations are looking to better protect their data in transit. Instead of purchasing a new IPSec VPN and then having to grapple with the performance challenges, Silver Peak is offering its Accelerated IPSec.

5. What challenges does IPSec face today?

Applications running across IPSec tunnels face a number of engineering challenges. Packet loss, out-of-order packets and other network congestion problems common to today's wide area networks (WANs) and Internet, require packets to be resent and reordered, adding delay to an application. Distance adds latency in TCP and CIFS/SMB exchanges. Bandwidth limitations constrain the amount of data sent over the WAN. Packet fragmentation, always a problem for network, commonly results with IPSec and delays security processing on the receiving firewall accompanying the VPN.

6. How does packet fragmentation impact firewall performance?

Firewalls filter traffic flows using the TCP/UDP port and protocol information normally contained in the initial packet. Packet fragmentation pushes some of this information into later packets, forcing the

firewall to delay its filtering process. IPSec often leads to packet fragmentation as the protocol must append data to each packet, often exceeding the maximum message transfer unit (MTU) size. The sending host or intervening devices, such as the routers, must then fragment the outgoing packets.

7. How does Accelerated IPSec address the loss, latency and bandwidth problems of running applications across IPSec VPNs?

Network congestion problems, such as packet loss and out-of-order packets, are eliminated or reduced through several technologies. *Adaptive Forward Error Correction (FEC*) reconstitutes lost packets at the far end of a WAN link, avoiding delays that come with multiple round-trip retransmissions. *Real-time Packet Order Correction (POC)* resequences incoming packets across all IP flows, avoiding retransmission and processing delays that occur when packets arrive out of order. *Traffic shaping and QoS* mechanisms ensure applications receive the necessary bandwidth on congested networks. *Dynamic Path Control* can send applications across least congested path between locations.

Bandwidth problems are overcome through byte-level, real-time data deduplication for any enterprise application not just TCP-based applications. Even applications or protocols based on UDP or a proprietary IP-based protocol benefit from deduplication. Data is fingerprinted and compressed the first time it is sent across WAN. Subsequent requests are fulfilled from the local Silver Peak instance

Latency problems are overcome by accelerating CIFS and TCP protocols. Packet coalescing re-packages multiple smaller packets into a single larger one while still factoring in the maximum MTU-size that can be accommodated by the IPSec VPN without fragmentation. Dynamic Path Control selects the fastest IPSec path or the fastest unencrypted path, if that's preferred, to a remote location. Overall, application performance is made more consistent through traffic shaping and quality of service (QoS) mechanisms.

8. How does Accelerated IPSec address the performance problems that undermine regular IPSec VPNs?

Silver Peak's Auto-MTU algorithms automatically determine the maximum Message Transfer Unit (MTU) that can be used for a path before intermediate routers fragment packets. In fact, packet fragmentation can only occur through gross misconfiguration or the complete inability to reduce the size of the incoming packet. Typically, Silver Peaks are deployed behind the firewall. Ports are opened through the firewall, avoiding the issue. Where organizations cannot open a port or need to place Silver Peak infront of their firewalls, as in the case of a demilitarized zone (DMZ),

9. How much can I save with Accelerated IPSec?

While Accelerated IPSec can reduce capital expenditures for organizations looking for IPSec VPNs and WAN optimization, the real value to Accelerated IPSec is gaining the fastest, most secure applications performance possible. Numerous independent head-to-head tests have shown Silver Peak to offer the best performance of any WAN optimization platform. In fact, Silver Peak's Accelerated IPSec often out performs unencrypted WAN optimization platforms.

With that said, there are cost savings depending on the specifics of the environment. Eliminating a branch VPN solution, for example, can save about half the cost of the WAN acceleration platform. Management and deployment costs are also lower with Silver Peak than many platforms .

10. Why not just run IPSec tunnels on my routers?

While many routers are IPSec capable they do not address the congestion, latency and bandwidth problems that undermine today's applications. Tunnel configuration can also be painstaking process with many routers, particularly when there are many tunnels. Silver Peak holds a number of patents simplifying the construction, deployment and management of tunnels. Routing performance may also suffer as IPSec processing consumes CPU cycles.

11. Why not just configure a Cisco ISR with Cisco WAAS for WAN optimization?

Silver Peak software can run within the Cisco ISR and outperform Cisco WAAS, a fact confirmed by numerous independent tests. There are also numerous problems with the Cisco WAAS architecture. Only TCP applications can be optimized by the platform, there is no support for UDP or other IP-based applications. There is also no compensation for network congestion issues, which are prevalent in IPSec VPNs. Connection count is limited forcing upgrades as more users or new applications are deployed. Because of these and other limitations, Silver Peak has constantly outperformed Cisco WAAS in independent testing.

12. How many IPSec clients can you support?

Silver Peak's Accelerated IPSec is a site-to-site solution. IPSec clients are not provided by Silver Peak.

13. How do Silver Peak devices authenticate with one another?

Silver Peak devices algorithmically create private keys, which are exchanged during the tunnel creation process. This saves the cost and time process of creating and maintaining certificates and supporting a Certificate Authority (CA). Once exchanged, private keys can be changed through the CLI or GUI at any point of time and manual key change could be automated through a shell script, if desired. We currently do not use PFS.

14. What happens if the authentication fails?

If the Silver Peak software cannot create the necessary Security Associations then the Silver Peak tunnel will not become active. Customers can determine whether to drop the traffic, send the traffic in the clear (shaped or unshaped), or continue to look for an alternative path to send traffic.

15. What encryption method does Silver Peak use to protect data?

Silver Peak's uses the standard for strong encryption, Advanced Encryption Standard-256 (AES-256). AES was finalized as a Federal Information Processing Standard (FIPS)-approved cryptographic algorithm and

uses keys with 128, 192, or 256 bits. Encryption is further enhanced by regularly regenerating the security key used for encrypting and decrypting data. Currently, the rekey interval is fixed at 12 hours, though it can be modified by a security engineer.

16. What are the authentication transforms that are used?

SHA-1

17. What is the strength of the IPSec key and what hash do we use?

Silver Peak generates 256-bit AES keys with SHA-1 hash authentication, which is a 160-bit hash.

18. What crypto hardware / software does Silver Peak use?

Silver Peak's IPSec implementation is based on standard RedHat Linux IPSec kernel, and Racoon (Internet Key Exchange (IKE) daemon for automatically keying IPSec connections.

19. Is there a chart comparing your software encryption using Intel cryptographic function to a hardware encryption device/chipset?

No. We originally employed the Broadcom 5840 device chipset and found our software encryption to be faster. We have not seen any significant degradation in performance between IPSec and clear processing in our performance across all platforms. Great steps have been taken to allocate CPU resources for IPSec tasks separate from standard data path CPU processes.

20. Does the WAN accelerator have exposed memory cards or hard drives that can be stolen? If stolen, can the data on them be retrieved? What is the exposure?

No memory cards or hard drives are exposed on any appliance. There is no front panel network configuration. All data at rest on the appliance hard drives are encrypted with 256-bit AES encryption, minimizing any exposure.

21. What about SSL?

Silver Peak optimizes SSL traffic using a variety of techniques, including Quality of Service (QoS) to prioritize this traffic, TCP acceleration to overcome latency, and Network Integrity to minimize the impact of dropped/out of order packets. In addition, Silver Peak has the ability to terminate (and re-establish) SSL sessions so that Network Memory compression and deduplication techniques can be performed on SSL encrypted traffic.

22. Is network access protected in the Silver Peak software?

Access to all Silver Peak products is tightly controlled using TACACS+ and RADIUS. This ensures complete AAA protection, including user tracking and auditing per-command authorization, and group based authentication privileges. Enterprises can use existing databases to facilitate administration and avoid potential security holes. CLI access is provided only via SSH (telnet is not available). The appliance manager can access the system using HTTP or HTTPS. (HTTP can be disabled if desired.)