

Data Leakage Prevention Systems Deployment Case

Data leakage prevention refers to tools designed to detect and prevent the unauthorized transmission of data to outside sources. These tools are used by organizations that process highly classified or sensitive information, such as government agencies or banking and insurance companies.

Why do you need to use an access technology solution with your DLP?

Because these tools need to be installed in-line, they can become a source of network downtime. When the device fails or needs to have maintenance performed on it, the entire network needs to be brought down to perform these fixes.

Gaining access to 100% of network traffic is essential for successful data leakage prevention. SPAN ports may not provide 100% of network traffic if they are over-subscribed or they may not be available for use when necessary. It may also be necessary to monitor multiple network segments simultaneously and aggregate the data to your data leakage prevention tools or to replicate the data to more than one network tool at the same time.

Network Critical solutions for DLP

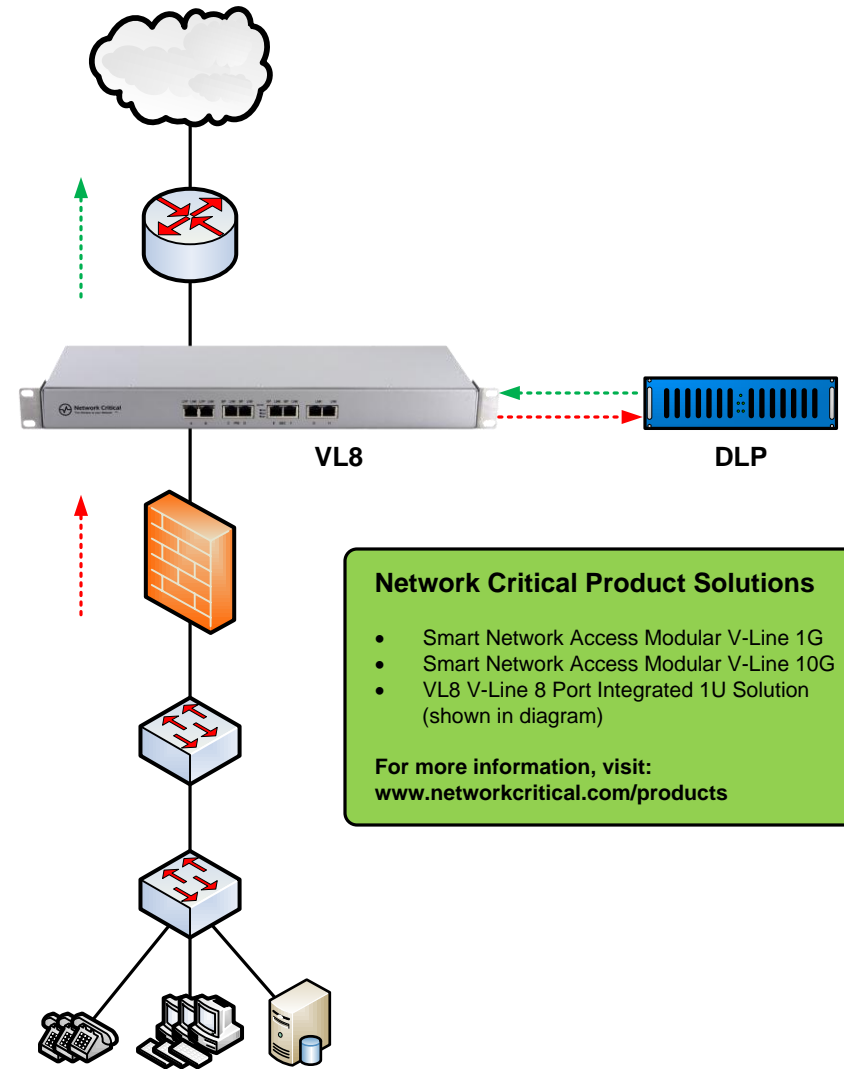
By using virtually inline or V-Line taps in a network, system administrators can isolate appliance failures and inherited appliance software issues by deploying their otherwise inline network tools using a hardened traffic access point. V-Line taps actively monitor the directional flow of data through a network appliance in both directions, and allow the tap to maintain live network continuity while having the option to actively bypass an inline appliance, should the device lose network link or traffic flowing in either direction through the inline appliance.

In the event of an inline appliance failure, V-Line traffic access points detect these occurrences while maintaining live network link, and will actively bypass the faulty appliance. Similarly, if traffic ceases flowing in either direction through an inline appliance, V-Line taps can detect such an anomaly and actively bypass inline appliance software failures.

Network Critical works with the following vendors that sell DLP products:

AlarmPoint	Code Green Networks	NetWitness	Symantec
Blue Coat	Forescout	Nitro Security	TrendMicro
CA Technologies	Fortinet	RSA	TrustWave
Check Point	McAfee	Sonicwall	Verdasys

www.networkcritical.com



Network Critical Product Solutions

- Smart Network Access Modular V-Line 1G
- Smart Network Access Modular V-Line 10G
- VL8 V-Line 8 Port Integrated 1U Solution (shown in diagram)

For more information, visit:
www.networkcritical.com/products