

Cisco Firepower Firewall with Profitap Bypass TAP for In-Line Protection



In today's rapidly evolving digital landscape, network security has become a critical concern for organizations of all sizes. To combat the increasing complexity and sophistication of cyber threats, it is essential to deploy robust security solutions that offer comprehensive protection. This solution brief presents a combined solution integrating Cisco Firepower Firewall with Profitap Bypass TAP to provide enhanced in-line protection for high-availability network infrastructures.

By leveraging the advanced features of both technologies, organizations can achieve increased security, improved performance, and greater operational efficiency.

Benefits Summary

- No more single point of failure for in-line security tools.
- Increased security in case of in-line appliance failure with the Profitap Bypass TAP heartbeat feature.
- Eliminate network interruptions for updates, service, or troubleshooting.
- Ensure optimum availability and security for your networks with Profitap Bypass TAPs and Cisco Firepower firewalls.

Cisco Firepower Firewall

Cisco Firepower Firewall is a next-generation firewall that integrates advanced threat intelligence, application visibility, and control features. It provides granular traffic inspection, intrusion prevention, and web filtering capabilities, enabling organizations to enforce security policies effectively. By leveraging its contextual awareness and threat intelligence, Firepower Firewall can identify and block sophisticated attacks in real time, preventing data breaches and minimizing network downtime.

Profitap Bypass TAP

Profitap Bypass TAP is a network access technology that provides a reliable and fail-safe method for integrating security appliances into the network infrastructure. Using passive fiber optic tapping, Profitap Bypass TAP ensures seamless traffic flow even during hardware failures or power outages. It enables easy deployment and maintenance of security devices without interrupting network connectivity, providing uninterrupted protection.

Use Case 1: Manual Bypass Mode

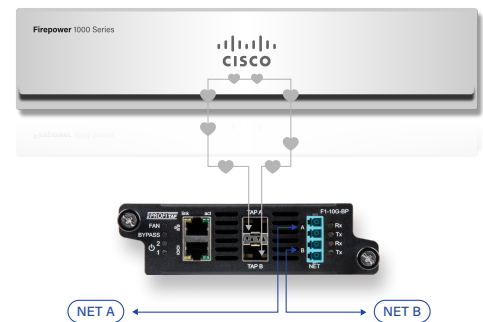
Challenge: Keep the network fully operational during maintenance and troubleshooting.

Answer: Integrating a Profitap Bypass TAP into the network allows in-line appliances to be accessed at any time, for instance to add, remove, or upgrade firewalls, without affecting network uptime or security. This is done by activating the manual bypass feature in the BP-Manager software. This way, traffic is no longer forwarded to the in-line appliance so the device can be freely accessed. The bypass mode can be turned off after maintenance, making the in-line appliance active. This feature makes troubleshooting or planned maintenance easy and can be done without affecting the operational stability of the network.

Use Case 2: Heartbeat Functionality

Challenge: Actively check the operational status of the in-line appliance.

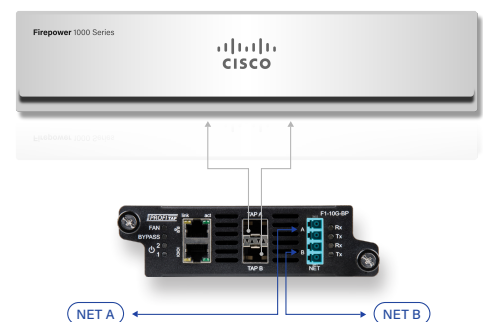
Answer: To actively track if the in-line appliance connected to the Profitap Bypass TAP is operational, the TAP uses bidirectional, configurable heartbeat packets with the data stream that, in turn, the in-line appliance must forward. If the in-line appliance is compromised, these packets will not return to the bypass TAP. In this event, the TAP will enable bypass mode to ensure the critical network link stays up.



Use Case 3: Out-of-Band Mode

Challenge: Maintain out-of-band monitoring.

Answer: The Profitap Bypass TAP can be set up in out-of-band mode with no need to rewire, allowing network traffic to be forwarded to intrusion detection systems or other out-of-band appliances.



Combined Solution Benefits

Enhanced Security: The combined solution leverages the advanced threat detection capabilities of the Cisco Firepower Firewall to identify and block malicious activities. By tapping into network traffic through the Profitap Bypass TAP, Firepower Firewall can inspect packets in real time, enabling proactive threat mitigation and preventing unauthorized access to sensitive information.

Improved Performance: Integrating the Cisco Firepower Firewall with Profitap Bypass TAP ensures optimal network performance. With the hardware bypass functionality, the TAP allows network traffic to flow seamlessly, even if the security appliance experiences power loss or failure. This eliminates any single points of failure and minimizes network latency, ensuring uninterrupted connectivity and maintaining business continuity.

Operational Efficiency: The combined solution offers simplified deployment, management, and maintenance processes. Profitap Bypass TAPs enable quick and hassle-free installation, reducing configuration time and effort. Different bypass modes offer great flexibility both in monitoring and maintenance scenarios.

Conclusion

In-line protection is vital to network security, enabling real-time threat detection and prevention. The combined solution of the Cisco Firepower Firewall with Profitap Bypass TAP offers a powerful defense mechanism that enhances network security while ensuring uninterrupted connectivity and operational efficiency. By implementing this solution, organizations can strengthen their security posture, mitigate risks, and safeguard critical assets from evolving cyber threats.