White Paper

Deploying Network TAPs for Improved Security

Companies are continuously improving their network security infrastructure to combat both internal and external threats. The efficacy and cost of network security solutions are under constant assessment. This white paper describes how a combination of network security probes and network TAPs can improve visibility and redundancy, while reducing solution complexity and cost.

Table of contents

FLUKE networks

Traditional network security

Network security professionals are tasked with securing the data traversing networks and saved on servers. These professionals utilize specialized probes, or intrusion detection systems (IDS), to monitor and analyze network traffic for potential threats. It is not always technically or financially feasible to place multiple probes throughout the network. In addition, managing a large number of security probes and the alarm information that they produce can be overwhelming. A more practical approach is to determine where the most confidential information exists within the organization's network, where the network vulnerabilities lie, and place safeguards around that information and the devices where it is stored. Consider the following figure that illustrates a common network physical topology.

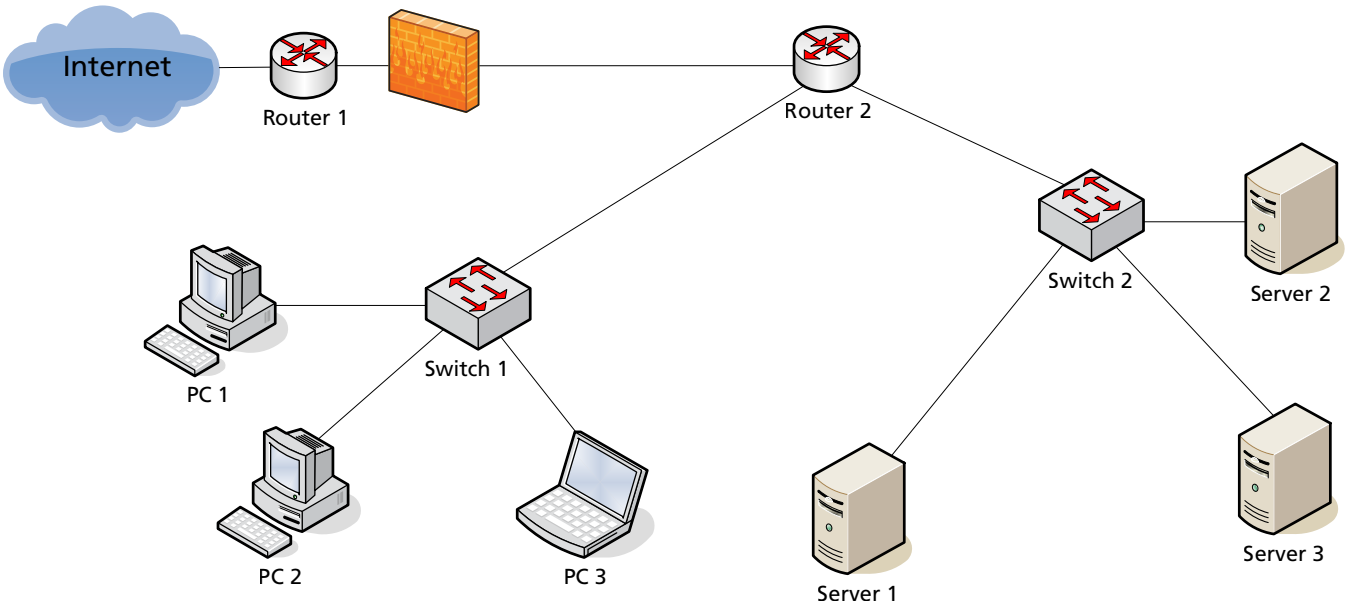

Figure 1: Typical network topology

External threats from unauthorized users have traditionally been the primary concern for security professionals. A security probe is placed at points of external network egress, between the firewall and router 2 in the above figure. The probe monitors and analyzes incoming and outgoing traffic, and intercepts malicious traffic just inside the firewall.

Today security professionals are also concerned about internal threats from authorized users. Authorized users can gain access to the network via a VPN connection which is usually terminated beyond the firewall. The deployment of security probes inside the network is required to address these internal threats.

In most organizations, confidential information is stored on particular servers. Confidential information includes company financial data, employee passwords, employee Social Security numbers, customer contact information, and customer credit card data. The servers saving this information are usually found at the network core. Figure 2 depicts where security probes can be placed within the network to secure the network from external and internal threats.

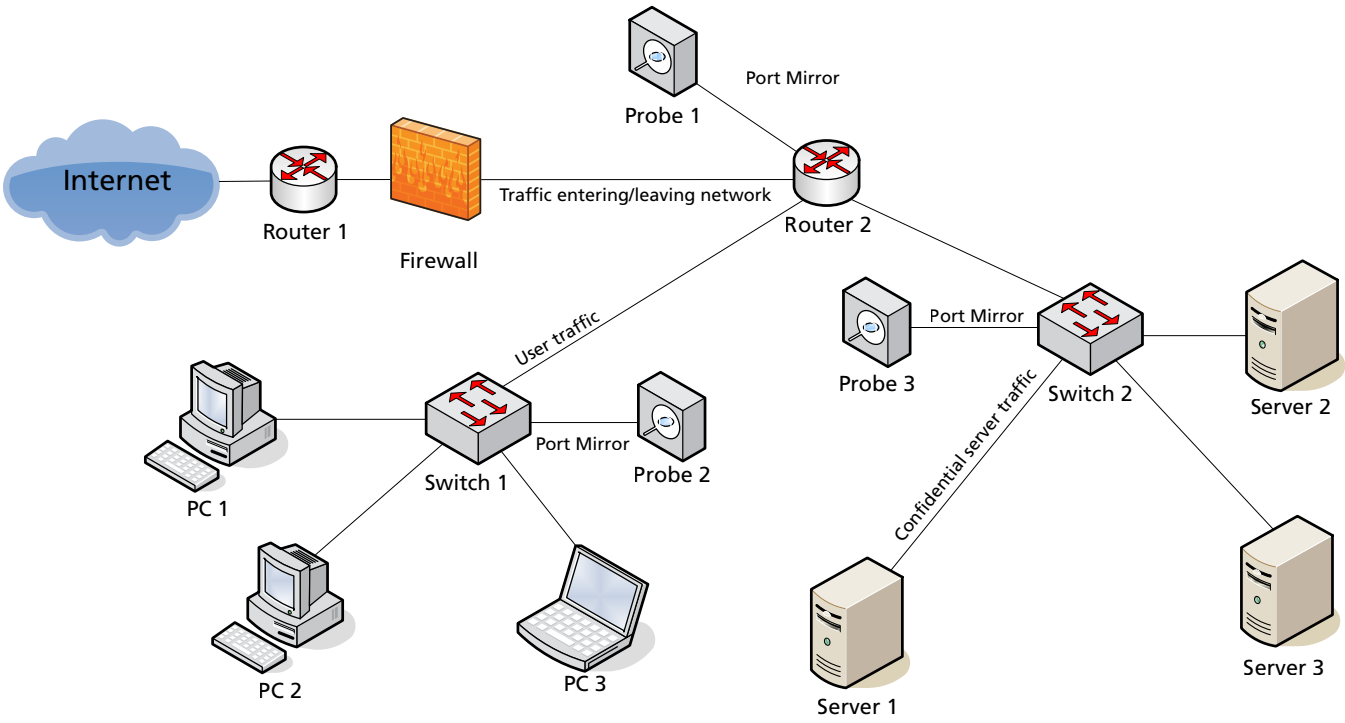

Figure 2: Probe deployment using port mirrors

In this example, security probe 1 monitors traffic entering and leaving the network via router 2 and the firewall. Probe 2 monitors user traffic between switch 1 and router 2. Probe 3 monitors the traffic from server 1. In this example server 1 is where the most confidential company information is stored.

In this example, the security probes access network traffic via "port mirrors." A port mirror is a software based connection that is created inside a network device, most commonly an Ethernet switch or router. The port mirror makes copies of traffic coming from a specific port(s) on the Ethernet switch and copies the traffic to the port mirror. When a security probe is connected to the port mirror, in theory it will see all the traffic coming from the designated ports.

Disadvantages of port mirroring

While port mirrors have the advantage of being integrated into the network device and are able to show traffic crossing the Ethernet switch backplane, they have drawbacks.

Many security professionals use port mirrors but are unaware that less than 100% of the traffic may be sent to the mirror port. Since the port mirror is a software implementation, traffic destined for the mirror port may be dropped if the Ethernet switch becomes congested. If traffic is dropped, the security probe has incomplete visibility into the network and security can be compromised.

Port mirrors are configured using the Ethernet switch software. An incorrectly configured port mirror can create additional network congestion, or worse a port mirror can be accidentally, or intentionally, turned off. The ability to remotely turn off the traffic feeding a network security probe is a concern.

Often there are several different departments and groups within a company needing access to the same network traffic. The IT department may want to monitor network traffic to help troubleshoot network and application issues. The compliance group may need to provide access to network traffic to auditors to verify financial, HIPAA or PCI compliance. Since Ethernet switches and routers support only a limited number of port mirrors, there may not be mirror ports available to the security team.

Tapping the network

A network TAP (Test Access Point) makes a copy of network traffic available to security probes and other devices. A network TAP replaces a mirror port and eliminates the associated mirror port limitations: dropping traffic due to switch congestion, misconfigured mirror ports, and disabled mirror ports. A TAP is designed so that it does not become a point of network failure. Traffic on the network link will continue to flow even if the TAP loses power. A TAP can aggregate half duplex traffic onto a single monitor port to feed a single-port security probe, while providing buffering capability to handle traffic utilization surges.

TAPS are placed wherever access to network traffic is needed. Referring back to the earlier example, TAPs would be placed between the firewall and router 2 to access traffic entering and leaving the network, between switch 1 and router 2 to access user traffic, and between server 1 and switch 2 to access confidential traffic from the server. Security probes are then connected to the taps. See Figure 3.

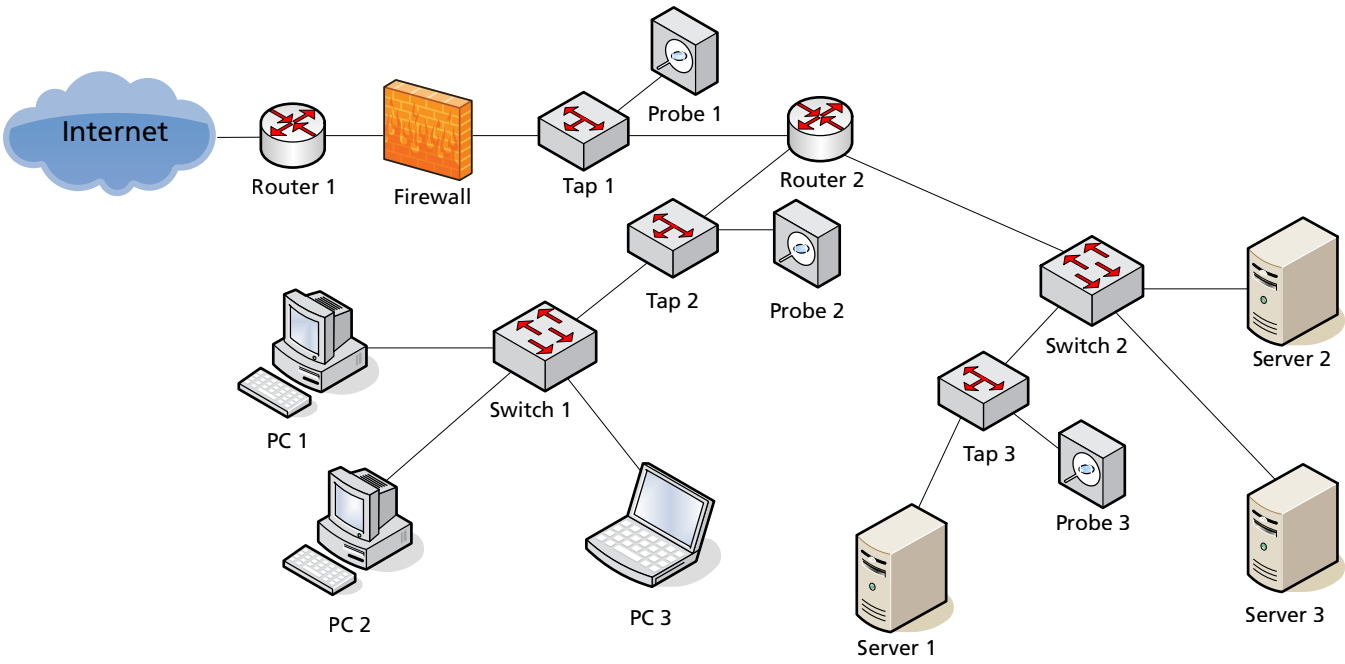

Figure 3: Probe deployment using network TAPs

Minimize the number of security probes using an aggregation TAP

An aggregator, also called an aggregation TAP, is a device that combines many inputs into a single output. Aggregators can eliminate the use of multiple security probes by merging together the inputs of several inline TAPs. One probe being fed an aggregated stream of traffic can replace several dedicated link probes. Aggregators are deployed where the sum of the inputs is less than the capacity of the output. TAPs and aggregators are cost effective solutions for organizations with low link utilization. One probe can monitor traffic gathered from multiple locations throughout the network, maximizing the value of the probe and minimizing overall probe costs.

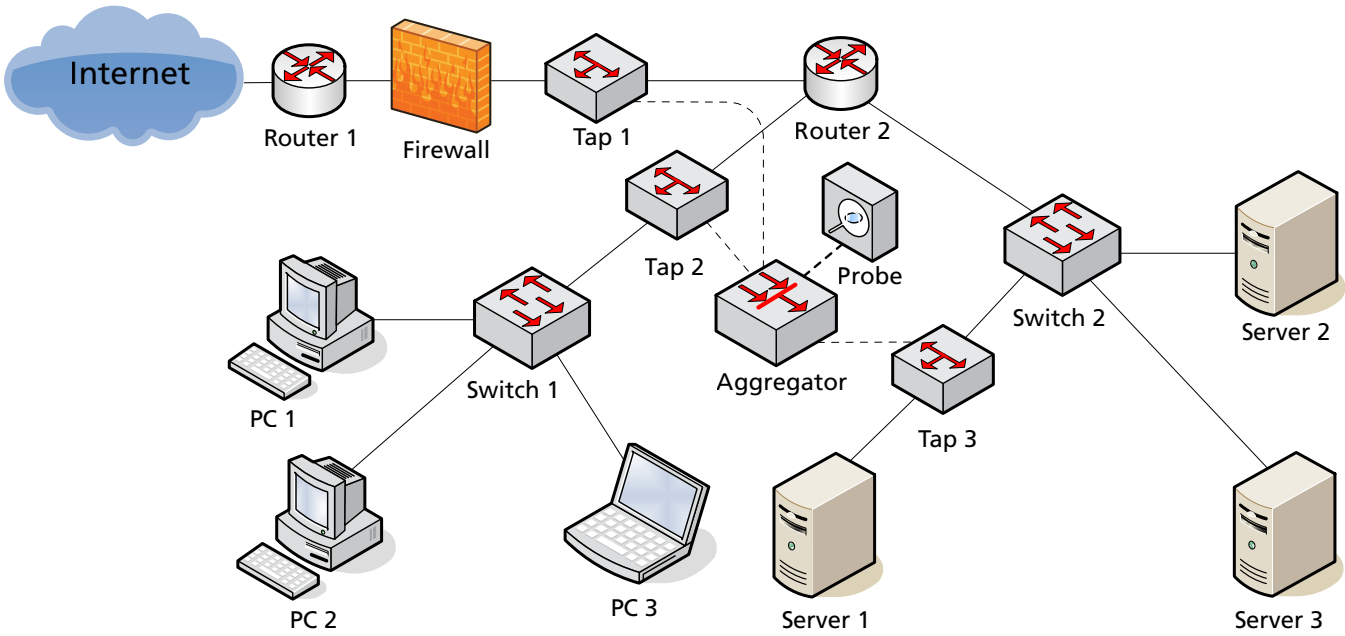

Figure 4: Aggregation of traffic from multiple TAPs to a single Probe

Span TAPs provide redundancy

A Span TAP, or regeneration TAP, creates identical copies of traffic so that multiple probes can all access the same data. Span TAP applications include deployment of redundant security probes. Should one probe fail, the back-up probe seamlessly takes over the security task. Span TAPs are also useful when additional devices need access to the same traffic: network monitors, application analyzers, packet recorders, etc. Each device can get access to the traffic it needs without compromising Ethernet switch resources or other devices , as illustrated in Figure 5.

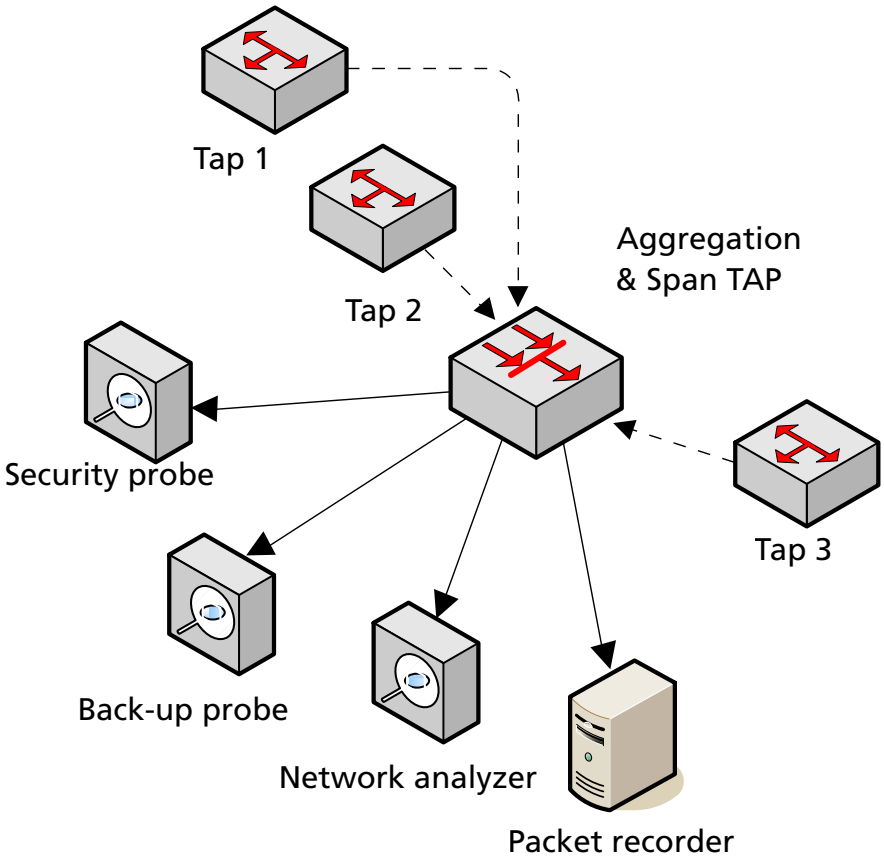

Figure 5: Same traffic copied to multiple devices

Summary

Keeping network traffic secure from external and internal threats is important to every organization. Using security probes in conjunction with network TAPs to monitor and analyze traffic is one method currently being employed by IT security professionals. TAPs are reliable, always on, easy to setup, and do not exhibit the limitations of port mirrors. TAPs whose outputs are aggregated together can also effectively simplify and reduce the cost of the security solutions. Span TAPs facilitate security probe redundancy and access to the same network traffic by multiple devices to serve the needs of various intra-company departments.

For more information about Fluke Networks Tap Solutions, **visit www.flukenetworks.com/taps**

Contact Fluke Networks: Phone **800-283-5853** (US/Canada) or **425-446-4519** (other locations). **Email: info@flukenetworks.com**.

NETWORKSUPERVISION

Fluke Networks
P.O. Box 777, Everett, WA USA 98206-0777

Fluke Networks operates in more than 50 countries worldwide. To find your local office contact details, go to **www.flukenetworks.com/contact**.

Printed in U.S.A. 1/2010 3624794A