DATACOM SYSTEMS INC

Deploying Network Taps for improved security

A guide to improving security visibility

A DATACOM SYSTEMS WHITE PAPER

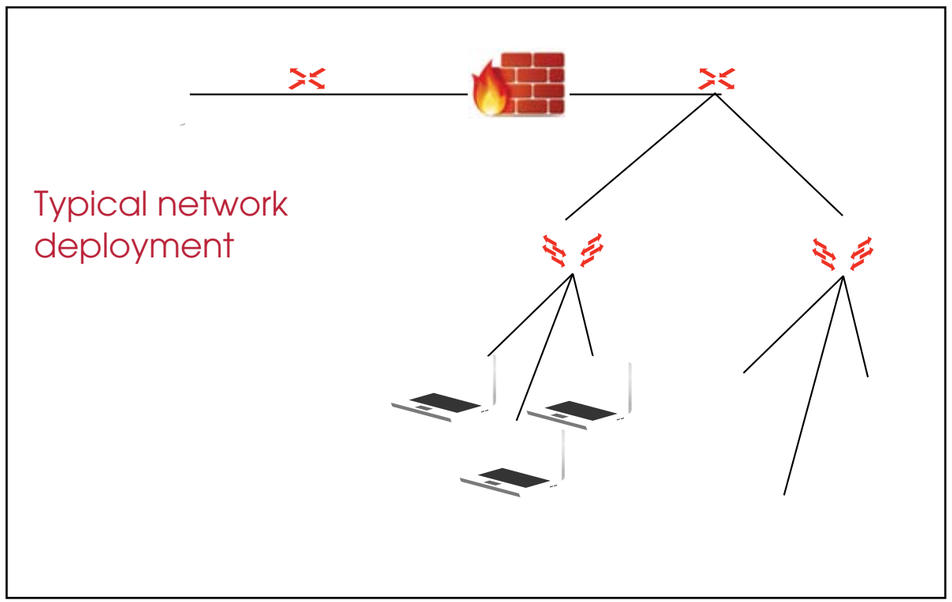
Improve Visibility

Companies are continuously improving their security infrastructure to combat both internal and external threats. The deployment and resources required to improve security are under constant assessment. Improved methods to monitor and troubleshoot security problems can have a significant impact on uptime and customer satisfaction.

A network security detection and prevention scheme using a combination of network taps and aggregation devices can improve visibility and redundancy, reduce system complexity and diminish initial and continuing costs for implementation.

Placing security monitoring solutions in multiple locations around the network is not always technically or financially feasible. Managing a large number of devices and the alarm information that they produce can be overwhelming. A more practical approach is to determine the most desirable information that exists in the company, and begin placing safeguards around that information or the devices where it is stored. Consider the following figure that demonstrates a common network physical topology.

Managing a large number of devices and the alarm information that they produce can be overwhelming. A more practical approach is to determine the most desirable information that exists in the company, and begin placing safeguards around that information or the devices where it is stored.



A network security detection and prevention scheme using a combination of network taps and aggregation devices can improve visibility and redundancy, reduce system complexity and diminish initial and continuing costs for implementation.

The most common location for a security probe is at external points of egress. This architecture evaluates incoming and outgoing traffic and intercepts malicious traffic just inside the firewall. External threats have traditionally been the primary concern for security professionals.

Currently, internal threats from existing employees with authorized accounts represent a major security threat. Authorized accounts can gain access via a VPN, wireless or wired connection which is usually terminated beyond the firewall. The deployment of security devices and probes inside the network to combat these internal threats is becoming increasing common.

Certain critical servers hold information that should be strictly prohibited. Critical records include company financial data, customer information, and employee passwords or Social Security numbers. The servers with this information are often found at the core of the network and connected to high-availability network devices. Protecting this information is the primary goal of strong security protection architectures. The following figure depicts these typical locations of security probes within the network. The dashed lines represent the links that the probes are receiving data from, for their analysis. While this is a perfectly valid solution, there are additional details that should be considered when designing this type of security system.

Probes and port mirrors

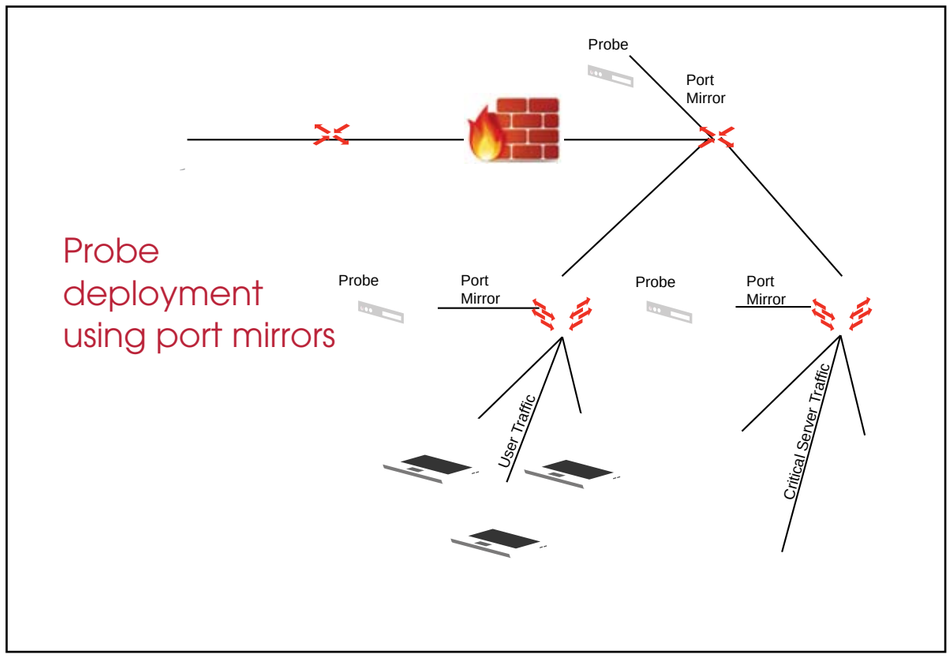
A network device can support a restricted number of port mirrors. This limitation is increasingly important as more security and analysis devices try to access the same data.

Security probes or Intrusion Detection Systems (IDS) use a variety of algorithms to analyze potential threats. While each manufacturer has their own unique way of analyzing, categorizing and reporting potential threats they are only as effective as the information that they receive.

Many security devices receive data via methods that do not provide them complete information on the traffic traveling on a network link. 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 specific port(s) on the Ethernet switch and copies the traffic to the port mirror. When a security device is connected to the port mirror in theory, it will see the traffic coming from the designated ports.

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 some drawbacks. Many security professionals use port mirrors but are unaware that less than 100% of the traffic will be sent to the mirror port. Since the port mirror is a software implementation, traffic destined to the mirror may be dropped if the Ethernet switch becomes congested.

The port mirror makes copies of traf c coming from speci c port(s) on the Ethernet switch and copies the traf c to the port mirror. When a security device is connected to the port mirror in theory, it will see the traf c coming from the designated ports.



A network device can support a restricted number of port mirrors. This limitation is increasingly important as more security and analysis devices try to access the same data. A variety of groups and departments are also creating and maintaining their own monitoring solutions, independent of the IT (Information Technology) Group. Providing network access to these additional departments is another challenge faced by the maintainers of corporate communication systems and drives the need for greater network visibility.

Port mirrors are configured using the Ethernet switch software. Port mirrors can be accidentally or intentionally turned off. The ability to remotely turn off the traffic feeding a network security device gives security and audit personnel cause for alarm.

Curing a critical event, the last thing a network engineer needs to worry about is taking time and care to setup a port mirror, and ensure that the appropriate traffic is copied to recording or analysis tools. An incorrectly created port mirror can create additional network congestion or shutdown required ports.

Tapping the link

A network TAP (Test Access Point) makes a copy of information in a network connection. The TAP is designed so that it does not become a point of failure in the network. TAPs are designed so that traffic on the network link continues to flow, even if the TAP loses power. TAPs also minimize latency between the network link and the monitor port on the TAP. TAPs will aggregate duplex traffic onto a single output port, while providing buffering capability to handle traffic utilization surges. TAPs can also provide identical copies of traffic so that multiple tools all see the same data. These "regeneration" TAPs are deployed when redundant probes or security tools need to have 24X7 visibility to a network segment. The failure of one security device does not create an issue, since the other security device sees the same network data from the TAP.

Placement of TAPs is typically in the locations with the most critical information in the network. TAPs will provide continuous monitoring on links where critical information travels, or on links leading to servers or storage devices where the data resides. TAPs are designed around a hardware-based architecture that minimizes latency, so their deployment can be made anywhere in the network.

Similar to security probes, some common locations for TAPs include inside the firewall, network trunks or links to or from critical servers.

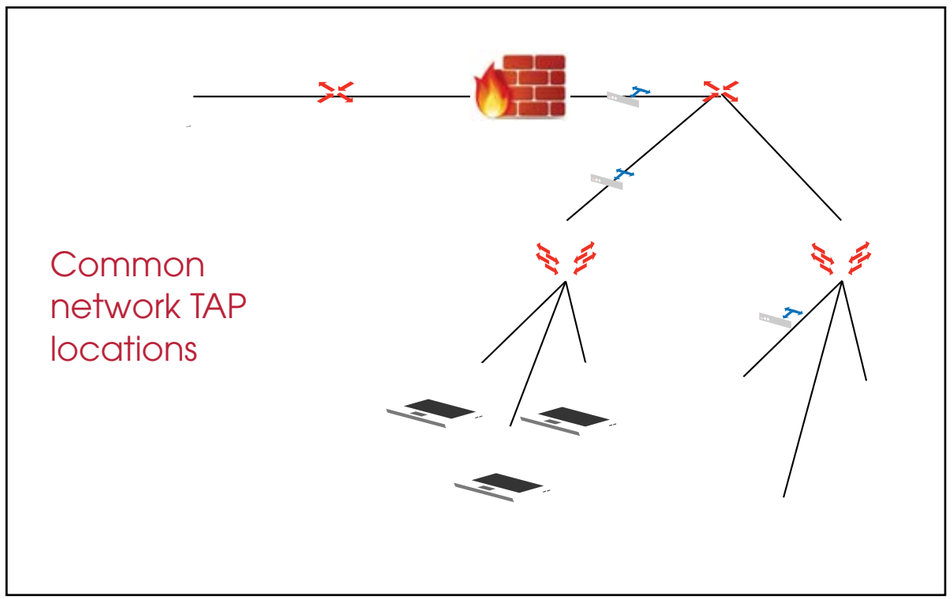
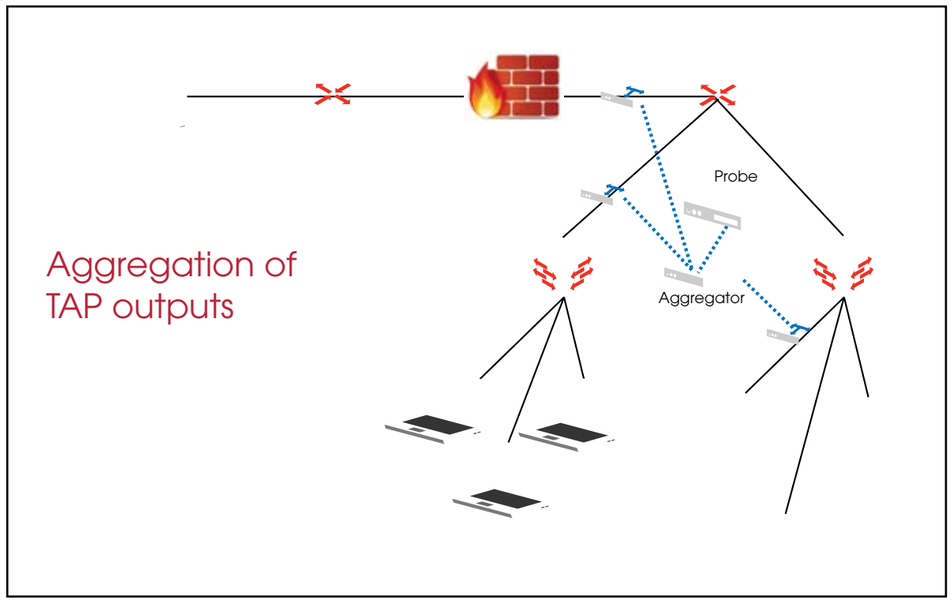
Deploying a combination of network TAPs and probes is an alternative method to placing security probes throughout the network. The passive nature of TAPs, ensure that network communication is maintained. Combining TAP outputs with the use of an aggregation device means greater visibility for the network probe.

An aggregator is a device that combines many inputs into a single output. Aggregators can eliminate the use of multiple probes by merging outputs from several TAPs together. Aggregators are deployed where the sum of the inputs is less than the capacity of the output. Many aggregators have an added benefit of creating multiple outputs, where each output is identical to the other. Since the aggregator sends identical traffic to its' output ports, all probes on an aggregator see the same traffic. If one probe fails, the other is able to continue securing the network. TAPs and Aggregators are a cost effective solution to an organization that is starting to do security analysis with low utilization on their links.

Improved security visibility using network TAPs to monitor and troubleshoot security problems is one method currently being employed by most Fortune 500 companies. They are always on, and eliminate the time to setup, configure and troubleshoot port mirrors. TAPs whose outputs are aggregated together can also effectively simplify and reduce the cost of the security solution. TAPs can provide an improved method of network access over port mirrors. TAP deployment is a proven and secure mechanism for improved visibility and redundancy.

Aggregators can eliminate the use of multiple probes by merging outputs from several TAPs together.

Placement of TAPs should be in accordance with the location of the most critical information in the network.



Combining TAP outputs with the use of an aggregation device means greater visibility for the network probe.