



Network Critical

The Window to your Network™

How to Raise Your FISMA SCORES

Federal Data Centers can benefit from
Smart Data Access Technology

Fall 2011



Smart Data Access Technology

The data center is command central for any Federal organization. It is where the applications and associated data negotiate the network infrastructure 24x7, providing critical services to both internal and external customers. Today's data centers are increasingly complex with many different vendors and technologies working together at faster speeds than ever before.

The need for security, accountability and compliance is paramount. One of the results of more and more monitoring tools being deployed in a given network is that practices such as utilization of SPAN and VACL ports are proving to be unacceptable solutions. In order to guarantee and certify that the data in your network is secure and complies with FISMA, CALEA and other lawful intercept rules and regulations, the network administrator must have access to all the data, not just what a SPAN or VACL network link can deliver to the monitoring tools. The TAP solution deployed in the network allowing access to network traffic being sent to the monitoring tools must be secure; ensuring the packets of data running through them cannot be compromised.

Network Critical's Smart Network Access (SmartNA) System provides all the security required to keep data safe from prying eyes while allowing the traffic going through it to be delivered to the monitoring tools. Whenever a tool is placed into the network, a new point of failure is introduced. Downtime in the data center can cost Federal Agencies thousands of dollars in lost productivity. To ensure the efficient operation of the data center, reduce bottlenecks, prevent outages and maintain security, it is vital for IT to carefully monitor and analyze all the data in the data center. It is not only absolutely necessary to have failsafe access, but secure access as well, and complete visibility of the Federal Agency's most important asset – data. To achieve this goal, Federal Agencies must augment their architecture to include Smart Data Access Technology.

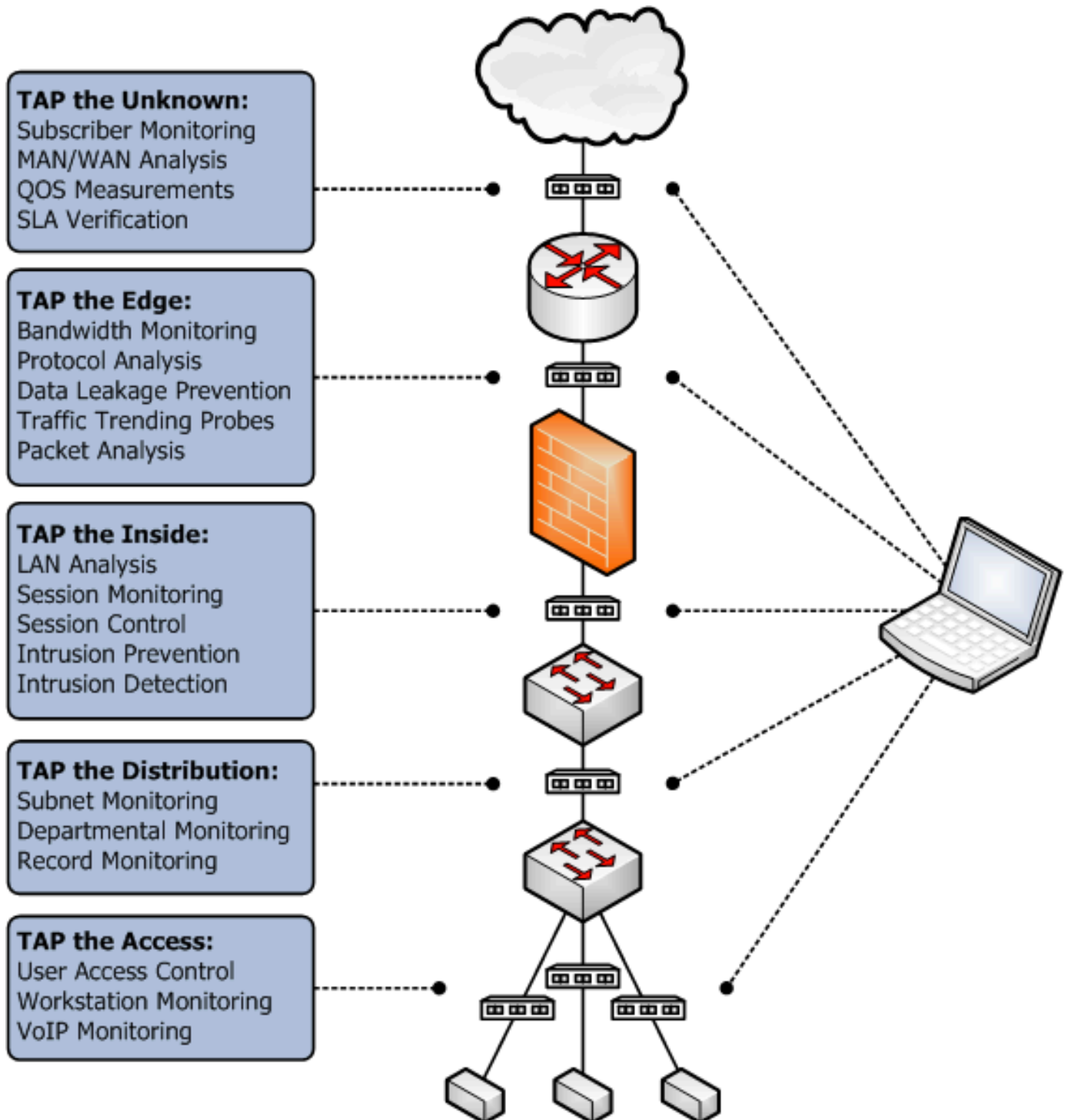
Building a Secure Smart Data Access Technology Network

The data center is part of a network ecosystem that drives the work of any size Agency. It is comprised of switches, routers, firewalls, application servers, IP services (DNS, RADIUS, and LDAP), virtualized applications, and storage area networks. Monitoring the actual network data is extremely important to the security of the agency. Federal Agencies will typically implement networks with countless numbers of monitoring and security tools for defense but find out that it is not efficient or cost effective to have a tool connected on every critical data path. The key to improved secure access and better visibility is to build a Smart Data Access Technology network that can filter, aggregate, consolidate and replicate data to the monitoring and security tools that are already found in the data center.



Smart Data Access Technology

How Smart Data Access Technology can be architected into the network





Smart Data Access Technology

The key to secure access is to TAP inline between major network devices found in the data center. This includes core switch-to-switch links, switch-to-router and switch-to-server links. TAPs can also be deployed in passive network connections that copy data from the link to the monitoring and analyzing devices. Network Critical designed the SmartNA™ as a modular product. The modular design provides secure access of the data, allowing greater flexibility that can accommodate the different media types typically present. The chassis and module architecture allows an agency's data center to save costly "rack" space by housing several different modules to perform filtering, aggregating and regeneration all in the same chassis. By moving beyond the fixed-function chassis, Federal agencies will benefit the data center with reduced power consumption and a smaller footprint. Many of these benefits provide "Day One improved efficiencies."

They include:

- **Reduced Monitoring Burden and Increased Effectiveness of Existing Tools -**

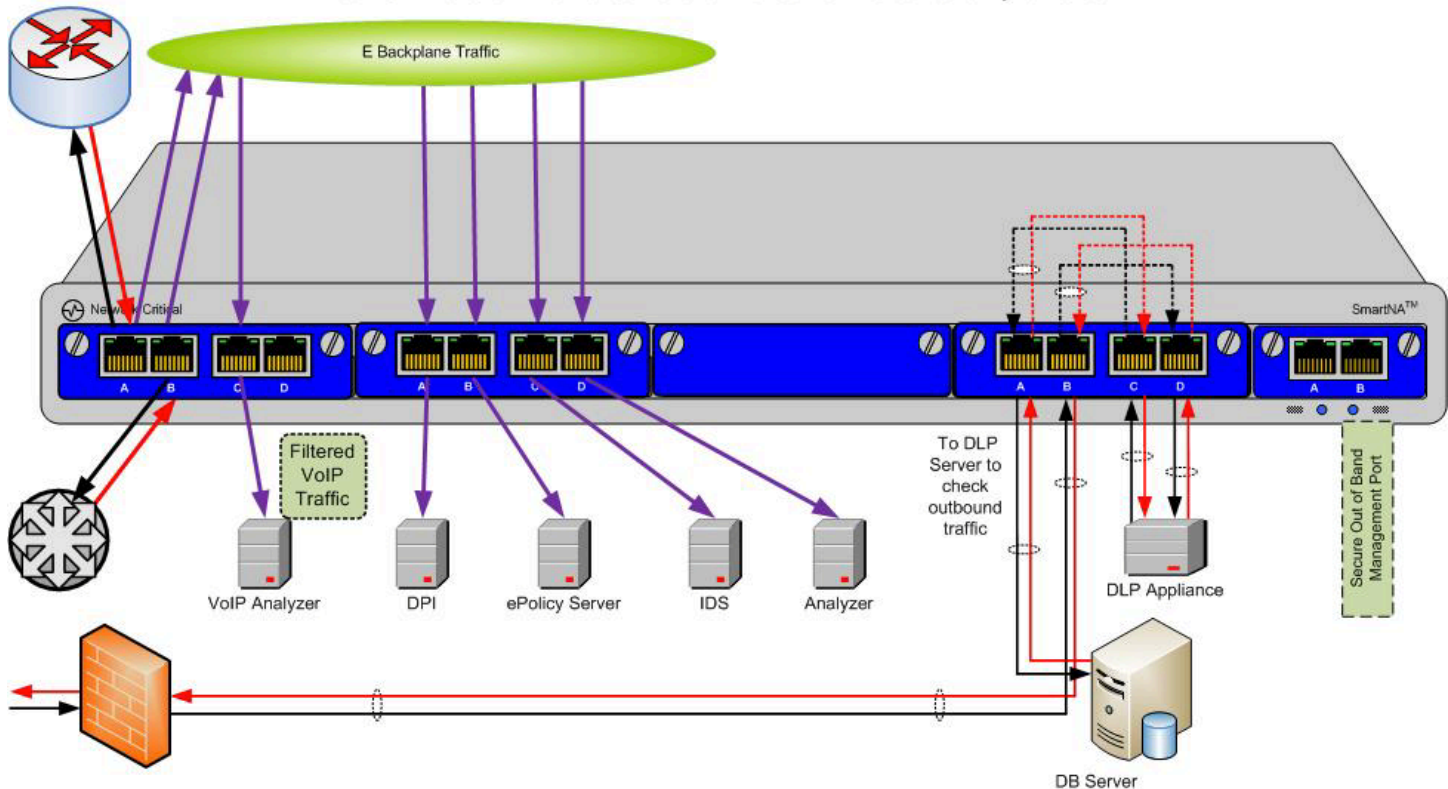
Often a Federal Agency will experience a tool overburdened by the amount of data sent to it or difficulty monitoring higher speed connections with lower speed tools. Smart Data Access Technology like the SmartNA™ System will diminish these problems using filtering functionality. Filtering allows the 10G traffic or aggregated traffic to be throttled down to less than 1G and sent to the 1G tool that the Agency already owns. With filtering, users can reduce the amount of data being sent to a tool so the tool will only see the data it needs instead of processing voluminous amounts of unnecessary data. This improves efficiency and saves budget dollars.

- **Eliminated SPAN/Port Monitor Contention -** Most switch and router manufacturers such as Cisco, Brocade, HP, and Juniper have a use limitation of only two ports for SPAN/Port Mirroring connections. Because of this limitation, users have reduced visibility into data because all packet capture/data recorder, application monitoring and security tools cannot access the data they need to see. By using Network Critical SmartNA TAPs, users can connect these same SPAN/Port Mirroring connections to the routers and switches and easily replicate the data to multiple tools at the same time.



Smart Data Access Technology

The possibilities are almost endless – Here we replicate traffic on a Critical Link to four different tools, filter VoIP traffic to a VoIP analyzer and check outbound DataBase traffic for breach of policy and we still have another slot for future expansion.



- **Easily Add New Tools and Monitor New Applications** – Data centers are continuously evolving, adding new applications or services and new monitoring tools. When all monitored data is routed through Smart Data Access Technology, users can easily connect new tools or monitor new applications using the SmartNA™ System’s modular technology by quickly sending data to new tools without disturbing existing monitoring connections. All of this can be accomplished without having to wait for lengthy change management processes because no downtime is incurred and all data is passively accessed and distributed by the SmartNA™ System.

- **Secured Monitored Data** – Another important consideration when monitoring or capturing data is controlling access to that data to ensure only authorized users capture or see it. The Network Critical SmartNA™ System secures data by offering many different security options: user-based port locking to ensure only authorized users access specific ports; packet slicing, which slices the payload of application data; SNMP traps which are triggered when a device is unplugged or a new device is plugged into an empty port; data masking which hides the contents of sensitive information; and user- and group-based centralized authentication using RADIUS/TACACS. Additionally, all out-of-band management functions use secure access technologies such as SSH and HTTPS.



Smart Data Access Technology

An Example of a Security Solution

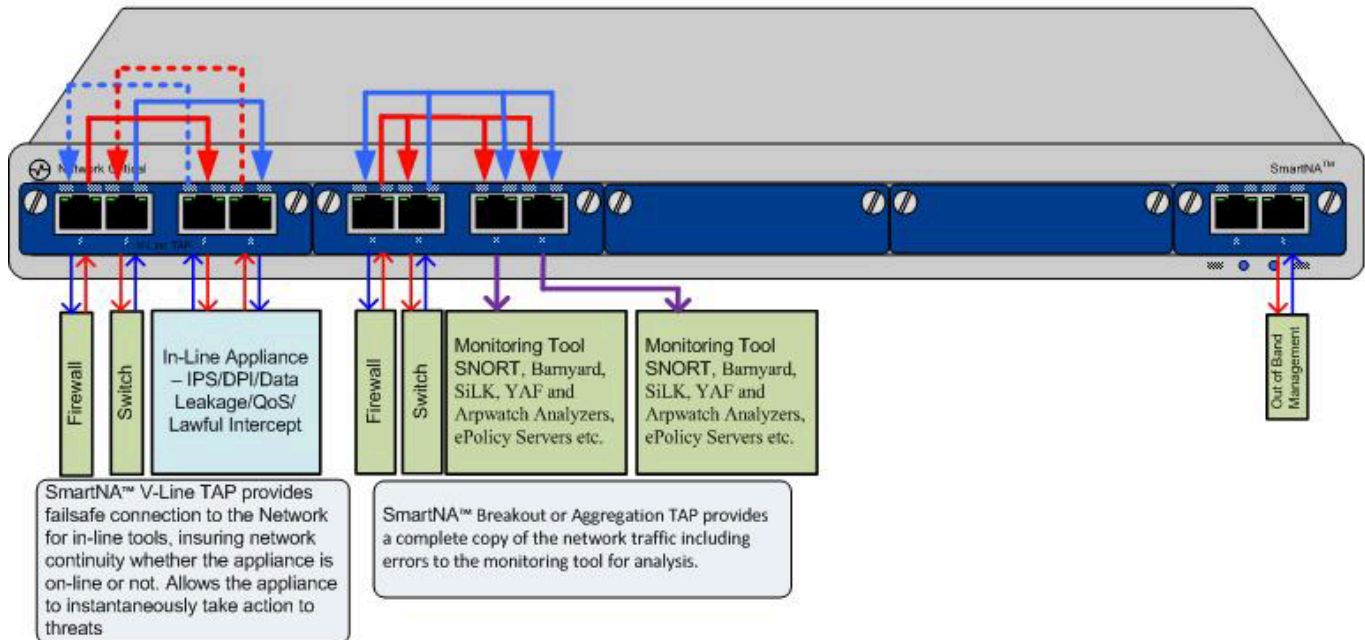
The Network Security Solution consists of five complementary open-source applications: Snort®, YAF, Barnyard, SiLK, and Arpwatch. These applications may be used individually, or they may be used in conjunction with each other to create a compelling suite of security services. Can solve In-Line or Monitor only configurations

Module 1

is a V-Line TAP module that provides the live link continuity in the event that the appliance goes off-line.

Module 2

is an Aggregating TAP and can provide the tools attached to it with all of the traffic or filter out all but the traffic that the tool needs to see.



In both cases, the live traffic is always assured to be failsafe because of the TAP. No matter what happens to the Appliance, tool or TAP the traffic will continue. The SmartNA™ system is designed to protect the traffic path for links that are connected to it. Because the TAP is a layer 1 device, it passes all the traffic that is presented to it. This is an important requirement when the traffic may become evidence in a court of law. The only way to be certain that the traffic is analyzed properly is if all the traffic is presented to the analysis equipment.



Smart Data Access Technology

Summary:

Introducing comprehensive Smart Data Access Technology solutions such as Network Critical's SmartNA™ System within Federal data centers will provide secure access and complete visibility into all mission critical data 24x7. With complete visibility and secure access, Agencies will reduce downtime and time-to-resolution of complex data center issues, benefiting all internal and external users. Network Critical Smart Data Access Technology resolves many issues such as SPAN/Mirror port contention, monitoring 10Gbps connections with lower speed capable tools, configuration and change order management and other obstacles that normally require a significant amount of time and resources. With thousands of units deployed and the uncompromised attention Network Critical clients receive; network administrators will realize greater efficiency, improved productivity and most importantly, the security of their most important asset – information.

About Network Critical

Network Critical, the creator of the network TAP solution, provides lab-certified, innovative, carrier-grade TAP solutions which allow complete access to network traffic. Network Critical TAPs are used with network intrusion detection systems, network intrusion protection systems, network traffic monitoring and more to provide 100% network visibility with zero packet loss 24 hours a day, 365 days a year.

The organization's commitment to uncompromised attention provides customers with an involved, attentive and hands-on experience that will meet their needs of today and exceed their expectations for tomorrow. Network Critical is a global access technology solution provider with operations based in Buffalo, NY USA; Reading, Berkshire UK; and Amsterdam, the Netherlands. For more information, visit www.networkcritical.com.