

# Government IT Agency Balances Security with High Availability

nGenius packet flow switches ensure flawless rollout of active inline security deployment

## OVERVIEW

### Industry

Government

### Business Challenges

- Ensure security and privacy of citizens' data
- Provide highest possible availability of services
- Prevent single points of failure in its active inline security defenses

### Solution Requirements

- Guarantee 99.999 percent uptime
- Provide instant failover capabilities
- Load balance across two IPS systems

### Business Value

- Inline IPS deployment without worries about potential network downtime
- Automatic failover guarantees availability even in the event of a system failure



### Customer Profile

This government agency manages IT infrastructure for the country's Ministry of finance. The agency is responsible for hosting online tax services, and processes tax returns for the country's population. The agency runs two redundant data centers to ensure highest availability of services.

### Security Challenges

The organization maintains sensitive data on the entire population of the country and thus must provide highest levels of security. At the same time, availability of services is critical as the network must be online around the clock for such a high profile application, where every citizen can potentially be affected by a downtime. The agency must carefully balance security and privacy of citizens' data with meeting the high standards the government has set in serving its taxpayers.

The agency was in process of deploying the McAfee IPS (intrusion prevention system) but was concerned about the potential for the security system to bring the entire network down, and with that, the reputation of the Ministry, let alone the disruption this may cause to the national economy.

### Security Visibility Solution

Because the agency wanted to maintain redundancy, its IT managers needed a solution that could provide the automatic failover and availability that it required. They explored multiple packet aggregation and management solutions and found that the NETSCOUT packet flow switches were the only systems that would help secure the network, without putting its functionality at risk. The key considerations for the agency were:

- **No single point of failure:** The system must support high-availability in the case of a security system's failure and must ensure that in such a case the IPS can be bypassed or that traffic can be forwarded to another device. The NETSCOUT nGenius® Packet Flow Switches themselves have zero impact on the network in the event of power outage, with their fail-safe functionality.

- **Policy-based triggers:** The system must ensure that the IPS do not introduce unacceptable latency into the network and perform as expected at all times. The packet flow switches from NETSCOUT allow for a set latency to trigger an action, such as routing around the IPS device or failing over to a redundant tool, to ensure that security does not become a single point of failure or a bottleneck.
- **Both positive and negative health checks:** These health checks fully exercise a tool's application stack, and not just via a heartbeat or yes/no response. This is a vital capability to ensure that the link is operative and the security applications are working as they should, inspecting and blocking traffic as required. NETSCOUT provided the unique capability to perform these health checks in a production environment.
- **Automated management:** The NETSCOUT systems included preset workflows that can be easily customised to match the security policies of the agency, allowing to fine tune the network performance in a variety of scenarios.
- **Active inline aggregation and load balancing:** Packet flow switches from NETSCOUT provided the agency with active network traffic aggregation and disaggregation. The aggregation was scaled across two redundant sites allowing the IT team the flexibility to direct traffic to one or both instances of the IPS in the event of especially heavy traffic during the tax season.

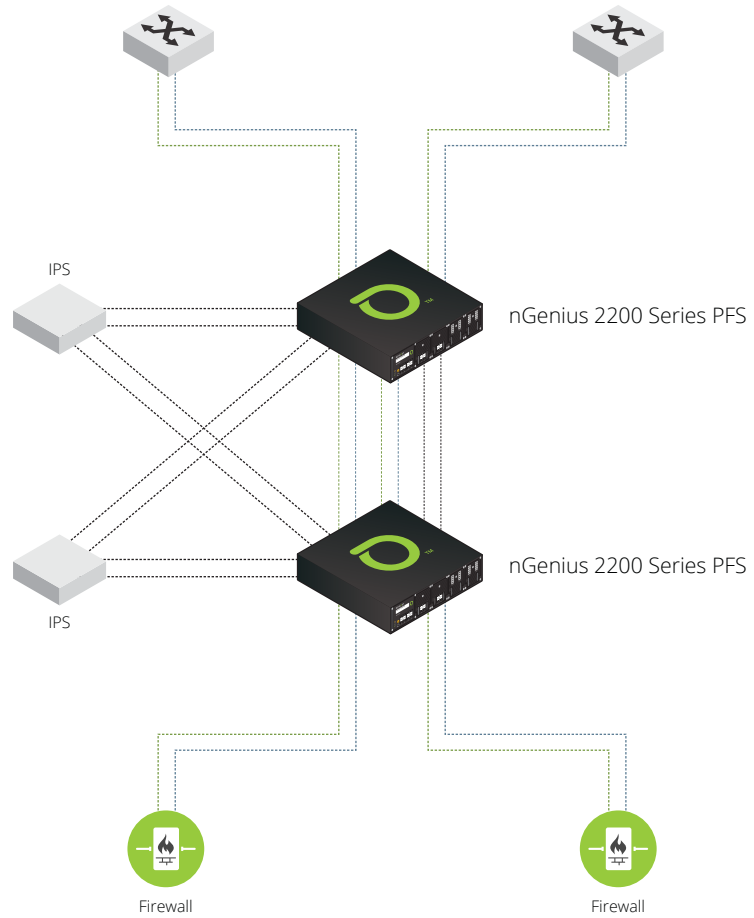


Figure 1: High-availability for inline security systems with nGenius PFS.

## Business Results

The customer deployed two NETSCOUT 2200 series packet flow switches, one each in its two data centers. The IPS deployment went flawlessly, with the two redundant McAfee IPS systems now live on the agency's network.

The IT managers chose to deploy the NETSCOUT packet flow switches because no other vendor could guarantee that combined solution would not affect the network in the event of a system outage.

The packet flow management deployment added network aggregation capabilities, session-based/flow-aware load balancing, inline tool bypass option with policy-based event triggering and custom health check functionality. The NETSCOUT systems load balance the traffic in case of a period of heavy utilization, especially during tax time.

With NETSCOUT, the agency can not only check that the McAfee IPS appliance is passing traffic, but also be sure the software is functional and blocking malicious packets.

Combining nGenius 2200 series PFS with McAfee IPS enables the customer to validate that the IP appliances are up and ready to perform at their highest competency and capacity – thus gaining optimal network intelligence.

For more information, visit [www.netscout.com/pfs](http://www.netscout.com/pfs).

**NETSCOUT**

### Corporate Headquarters

NETSCOUT Systems, Inc.  
Westford, MA 01886-4105  
Phone: +1 978-614-4000  
[www.netscout.com](http://www.netscout.com)

### Sales Information

Toll Free US: 800-309-4804  
(International numbers below)

### Product Support

Toll Free US: 888-357-7667  
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: [www.netscout.com/company/contact-us-2/](http://www.netscout.com/company/contact-us-2/)