# Assuring Secure Collaboration for High-Performance Computing with a Science DMZ

Networking strategies for effective and secure Science DMZ computing environments

### Challenge

Federal agencies and research and education institutions need to collaborate securely using analytics, data visualization, and high-performance computing. The challenge is to meet the needs of these data-intensive applications without compromising performance or security.

### Solution

Juniper Networks Science DMZ solutions, include:

- EX Series Ethernet Switches
- MX Series 3D Universal Edge Routers
- SRX Series Services Gateways

### Benefits

- Enable data-intensive scientific and research collaboration while minimizing security risks
- Support very large data flows without impacting other application traffic
- Mitigate the risk of attacks on a Science DMZ while ensuring network availability

The research and education community has long needed to move massive data sets to collaborate. A growing number of public and private sector organizations also depend on big data, high-performance computing, and other data-intensive efforts that require moving very large amounts of data for analytics, data visualization, or other collaborative efforts. These initiatives are characterized by very large, long-lived data flows, also known as "elephant flows." The challenge is to meet the needs of data-intensive science applications without compromising performance or security.

## The Challenge

Several years ago, researchers at ESnet, the Energy Sciences Network, created the concept of a Science DMZ to facilitate data-intensive scientific collaboration. According to ESnet, a "Science DMZ is a portion of a network, built at or near the campus or laboratory's local network perimeter, that is designed such that the equipment, configuration, and security polices are optimized for high-performance scientific applications rather than for general purpose business systems or enterprise computing."

While the use of Science DMZs has typically been limited to the high-end research and education community, federal agencies are increasingly building Science DMZs to support analytics, high-performance computing, and other collaborative initiatives that require very large data flows across and between organizations.

For more information on Science DMZ architecture and services, please see http://fasterdata.es.net/science-dmz/.

## The Juniper Networks Science DMZ Solution

Juniper Networks has developed a Science DMZ solution that can support the demands of very large data flows while mitigating security risks in high-performance computing environments. Juniper products deliver the operational and security capabilities needed to optimize and fortify Science DMZ operations, including:

- Flexible routers and switches that leverage the robust features of Juniper Networks® Junos® operating system, which is recognized for stability, dependability, and performance
- Carrier-grade reliability that is service provider tested for 99.999% availability with service layering that does not impact line-rate performance
- Ability to handle very large data flows at 100 Gbps and 40 Gbps without compromising performance
- Security controls that can be implemented to mitigate the impact of operating without the protection of a firewall

## Science DMZ

Juniper Networks offers customized, high-performance, bundled solutions to meet specific Science DMZ requirements.

For organizations that need high-performance edge routing and switching for a Science DMZ, the Juniper Networks EX9200 line of Ethernet switches provides an SDN-ready, programmable, flexible, and scalable solution. EX9200 switches deliver carrier-class reliability and wire-speed performance even at high 40GbE and 100GbE port densities. The EX9200 Science DMZ Platform Package with special pricing features a Juniper Networks EX9200 Ethernet Switch, which supports various interfaces, including 100GbE (see Figure 1).

Organizations that require high-performance edge routing and switching as well as a full Internet routing table for the Science DMZ can leverage Juniper Networks MX Series 3D Universal Edge Routers. SDN-ready MX Series routers provide industry-leading system capacity, density, and performance to scale in bandwidth, subscribers, and services. With the MX Series, organizations can build a scalable Science DMZ that scales from 20 Gbps to 80 Tbps with unparalleled reliability and outstanding operational efficiency. Science DMZ Platform Packages with special pricing are available for the Juniper Networks MX240, MX480, MX960, MX2010, and MX2020 3D Universal Edge Routers (see Figure 2).

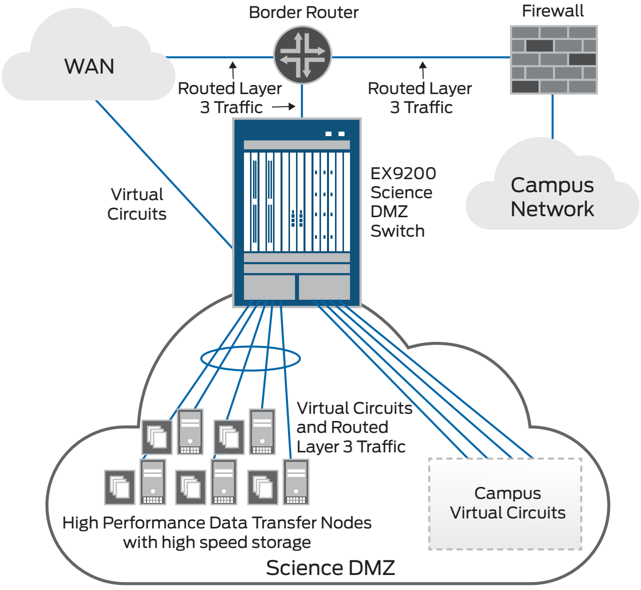

Figure 1. EX9200 Science DMZ

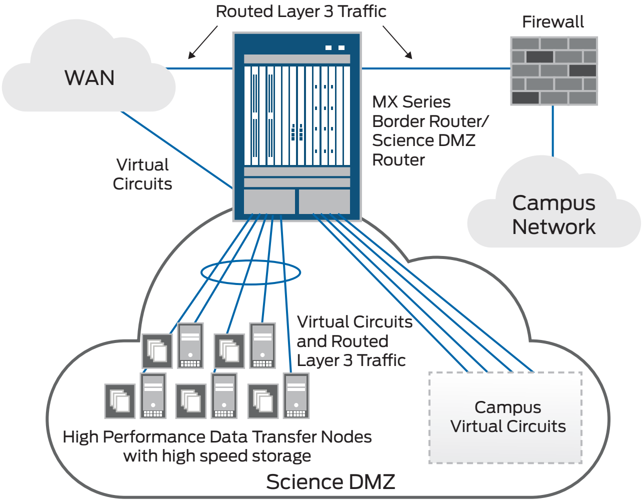
Routed Layer 3 Traffic
Firewall
WAN
MX Series Border Router/ Science DMZ Router
Virtual Circuits
Campus Network
Virtual Circuits and Routed Layer 3 Traffic
Campus Virtual Circuits
High Performance Data Transfer Nodes with high speed storage
Science DMZ

Figure 2. MX Series Science DMZ

## Science DMZ Security Controls

The Juniper Science DMZ solution delivers a number of security controls.

### Transit Filtering

- **Firewall Filters**—examines the Layer 3 and Layer 4 headers on a packet-by-packet basis. Based on configured rules, a firewall filter decides whether the router forwards or drops the packet.
- **Filter-Based Forwarding (Policy-Based Routing)**—controls the next-hop selection for traffic by defining input packet filters that examine the fields in a packet's header. If a packet satisfies the match conditions of the filter, the packet is forwarded using the routing instance specified in the filter action statement.
- **J-Flow Monitoring**—enables flow record management using J-Flow, Juniper Networks' flow monitoring implementation. Juniper switches and routers generate summarized flow records for sampled packets from the Packet Forwarding Engine (PFE). Flow records can be exported in a NetFlow-compliant standard packet format to an external flow information collector for analysis.

### Network-Wide Security Measures

- **Remotely Triggered Black Hole (RTBH) Routing**—mitigates denial-of-service (DoS) attacks. Once an attack has been detected, BGP can be used to modify route tables to specifically drop attack traffic before it enters the Science DMZ.
- **BGP FlowSpec (RFC-5575)**—mitigates DoS attacks with more granularity and control. FlowSpec uses the BGP network layer reachability information to selectively drop traffic flows based on Layer 3 and Layer 4 information.

### Routing Engine Protection

- **Firewall Filters for the Routing Engine**—focuses on the defense of the router itself.
- **Policers for Host-Bound Exception Traffic**—restricts Routing Engine access to only those authorized to communicate with the router and limits the amount of data that they are allowed to send to the router. This approach helps defend the router from distributed denial of service (DDoS) attacks and effectively provides a security curtain for one of the devices that is protecting the Science DMZ.

## Secure Science DMZ with SRX Series Services Gateways

A Science DMZ is located outside (in front of) an organization's firewall. This strategy was developed to work around the fact that traditional firewalls are not capable of supporting high-speed data transfer flows. Placing the Science DMZ outside the firewall overcomes this limitation, but it also introduces security concerns and leaves the Science DMZ more vulnerable to attacks. Now that 100-Gbps-capable firewalls such as Juniper Networks SRX Series Security Gateways are available, network engineers are considering how these firewalls can contribute to the security of their existing Science DMZs.

Organizations that need consistent high performance and must meet more stringent cybersecurity requirements can use Juniper Networks SRX5400, SRX5600, or SRX5800 Services Gateways in their Science DMZ (see Figure 3.) The SRX Series delivers high-performance security with integrated threat intelligence, delivered on the industry's most scalable and reliable platform. It is designed with separate data and control planes, so that when the network is under attack, the administrator maintains management access to modify policies and block bad traffic so that the network stays up.

The SRX Series gateway can be used to offer separate levels of firewall service for high-bandwidth data transfers (elephant flows) and other Internet traffic (mice flows). The SRX Series ASIC-based Express Path technology enables line-rate performance for elephant flows of 100 Gbps and 40 Gbps. With Express Path, organizations can support large data flows while ensuring that their security posture is well matched to their high-performance science applications. In addition, the service processor-based Fast Path on the SRX Series gateway enables support for additional firewall functions for other Internet traffic.

## Features and Benefits

The Juniper secure Science DMZ solution delivers:

- Separate levels of service for high-bandwidth data transfers (elephant flows) and other Internet traffic (mice flows)
- An ASIC-based Express Path for elephant flows with support for full stateful firewall service and security screens for IP address sweeps, port scans, DoS attacks, Internet Control Message Protocol (ICMP), UDP, and SYN floods
- A services processing unit-based Fast Path with support for additional firewall functions such as intrusion prevention system (IPS), antivirus, antispam, Web, and content filtering that can be used for mice flows

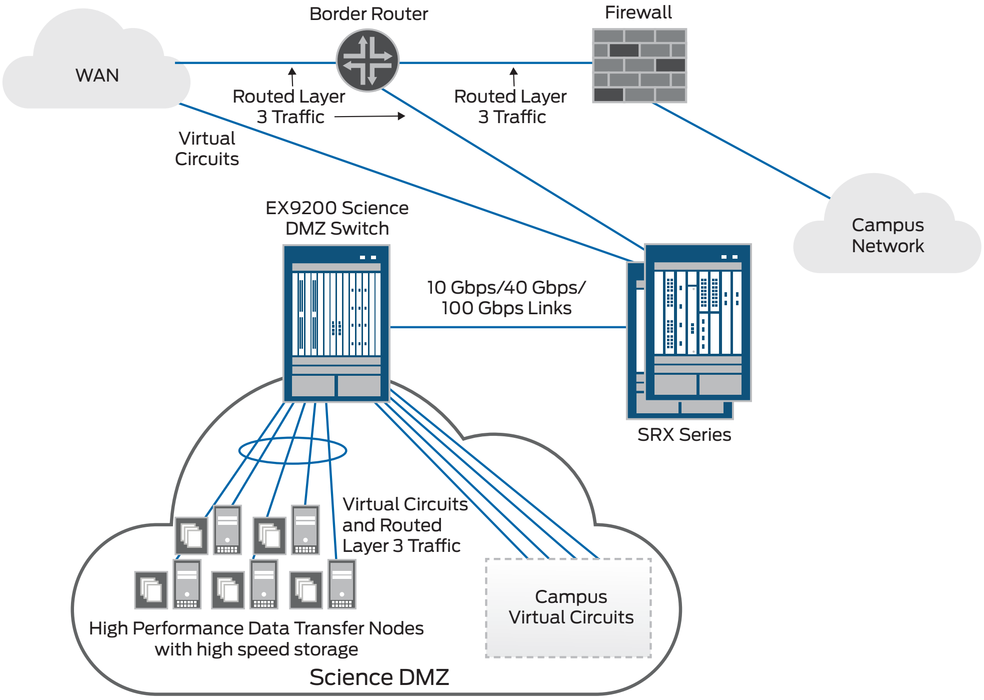
Border Router
Firewall
WAN
Routed Layer 3 Traffic
Routed Layer 3 Traffic
Virtual Circuits
EX9200 Science DMZ Switch
10 Gbps/40 Gbps/ 100 Gbps Links
Campus Network
SRX Series
Virtual Circuits and Routed Layer 3 Traffic
Campus Virtual Circuits
High Performance Data Transfer Nodes with high speed storage
Science DMZ

Figure 3. Secure Science DMZ

## Solution Components

| Solution | Customer's Requirement | Base Solution |
|---|---|---|
| Science DMZ | High-performance edge routing and switching | EX9200 line of Ethernet switches |
| | • High-performance edge routing and switching<br>• Full Internet routing table | MX Series 3D Universal Edge Routers |
| Secure Science DMZ | • Security at scale<br>• Line-rate security at 40GbE or 100GbE<br>• High-performance edge routing and switching<br>• Optional support for a Full Internet routing table | SRX5400, SRX5600, or SRX5800 Services Gateways and EX9200 line of Ethernet switches or MX Series 3D Universal Edge Routers |

## Summary—Explore Your Science DMZ Options with Juniper

Internationally recognized research institutions and government agencies rely on Science DMZ environments enabled by Juniper Networks. They partner with Juniper for the peace of mind that allows researchers to focus on the Science DMZ architectures they are implementing, not whether the network will perform as promised.

## Next Steps

Juniper Networks stands ready to discuss your Science DMZ requirements and how optimized configurations and specially priced technology bundles for Science DMZ switch/router security controls can work in your computing environment. For more information and to review your specific requirements, please contact your Juniper Networks account team.

## About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at www.juniper.net.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701

JUNIPer NETWORKS