MCNC®

Connecting North Carolina's Future Today

Network Security for today's North Carolina

Introducing MCNC and NCREN

MCNC is a broadband non-profit organization that owns and operates the North Carolina Research and Education Network (NCREN). For more than three decades, MCNC has been a leader in Internet technology growth, development, and deployment on a world-class, 2,600-mile fiber network. Today, NCREN helps create unprecedented opportunities for North Carolina citizens where they live, access education, seek economic gain, participate in their governance, and access health care. With constantly emerging technologies in networking also comes with great responsibility for MCNC and customers on NCREN.

Keeping North Carolina connected and protected

Security is an essential part of today's technology-driven society. Securing an organization's networking infrastructure requires employees and institutions alike to proactively manage and protect personal and organizational assets. MCNC manages security threats and responses in the context of business risks and is strengthening its ability to rapidly detect and respond to security threats on the NCREN network. MCNC also continues to develop important relationships with federal, state and local law enforcement and other agencies to maintain awareness of potential threats and techniques to appropriately mitigate them.

Managing Security Risk

MCNC is a proactive business partner and technology enabler with a structured approach to risk management. MCNC has established its Enterprise Risk Management Committee (ERMC) as a way to identify, catalog, and analyze risk issues facing the organization. It is comprised of key decision makers from each business vertical within the organization that formally review security concerns and decide how best to respond. This process ensures that potential consequences of security events are analyzed in terms of their potential impact on the organization and customers. Once the potential consequences are understood, responses are crafted to match the risk. Improving MCNC's risk management and overall security posture remains a top priority for the organization.

Identify, track and prioritize DDoS attacks

The last three years have seen a surge in the effective use of Distributed Denial of Service, or DDoS, as a weapon of cyberattack. No longer only the domain of elite attackers, today's DDoS attacks can be easily launched by those with limited technical skills, and the results can seriously the impair business operations of the victim. MCNC's Enterprise Risk Management Committee has identified DDoS as an elevated priority for MCNC customers and has prioritized investments in expanding and strengthening the organization's ability to mitigate the negative effects of these attacks on NCREN.

Defending against DDoS is a cost of doing business

Expanded protection capabilities greatly enhance MCNC's ability to repel DDoS attacks and will provide customers the tools to address certain attack types that cannot be easily mitigated today. While heightened capabilities will not eliminate all negative effects of DDoS attacks, they should improve attack response times and strengthen MCNC's ability to protect customer networks.

P.O. Box 12889 • 3021 E. Cornwallis Road • Research Triangle Park, N.C. 27709-2889 • 919.248.1900 • www.mcnc.org

www.twitter.com/mcnc | www.facebook.com/mcnc-ncren | www.linkedin.com/company/mcnc | www.youtube.com/MCNCvideos

Did You Know?

- ✓ Today's DDoS attackers can send hundreds of Gbps of malicious traffic to their targets in seconds.
- ✓ MCNC has prioritized investments in strengthening the organization's ability to mitigate DDoS attacks.
- ✓ MCNC scrubbing centers provide technical capabilities to mitigate attacks without impairing traffic flow.
- ✓ MCNC is compliant with Service Organization Control (SOC 2) data center standards.
- ✓ Data backups are provided by the IBM TSM system. MCNC provides backup to disks and synchronous transmissions to disks in Winston-Salem.
- ✓ MCNC's system monitoring is performed with Nagios and Cacti.

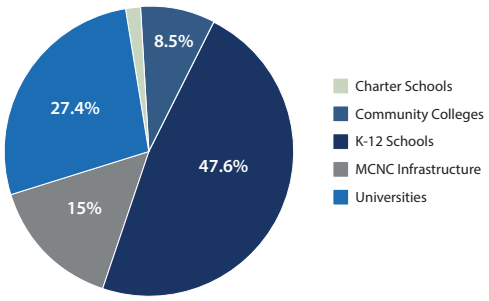
"MCNC has prioritized investments in security and risk management solutions that mitigate the negative effects of cyberattacks on NCREN. New internal security methodologies working in concert with scrubbing center technology and configurations layered into the NCREN architecture is helping keep mission-critical applications and information safe behind and beyond firewalls with no additional costs to customers."

Chris Beal
Director of MCNC Security & Chief Security Architect

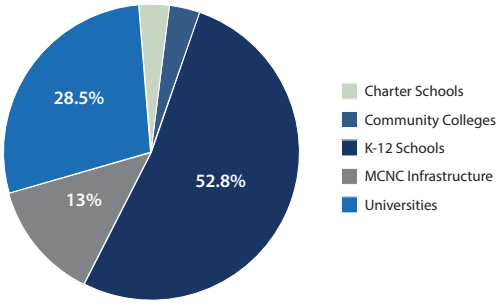
**All data and information provided herein was recorded as of May 2016.*

Contact us today by calling 919.248.1900
visit www.mcnc.org

DDoS Attacks on NCREN By Number of Attacks



DDoS Attacks on NCREN By Volume (Gbps)



Network security through transparent flow modification

DDoS attackers now can send gigabits of malicious traffic to their targets in seconds. MCNC has designed and implemented network "scrubbing centers" on NCREN for explicitly removing network scans and attacks at various protocol layers - including a TCP scrubber to eliminate insertion and evasion attacks. MCNC's scrubbing center solution offers an effective ability to mitigate cyberattacks without impairing normal TCP/IP protocol services for customers under attack. It offers fine-grained inspection capabilities for all attack traffic while providing a number of mitigation techniques that can be utilized for various attack types. This solution provides a surgical response to address attack traffic.

Putting a stop to large, strong DDoS attacks

DDoS attacks are growing bigger and more complex. As attackers evolve and refine their techniques, having options for addressing attacks is a priority for MCNC. A major benefit of the scrubbing center solution is access to real-time research and incident response professionals. These teams are constantly updating the platform's mitigation capabilities in response to attack patterns seen across the global Internet. Having access to this threat information will significantly strengthen MCNC's ability to respond to and mitigate attack traffic. Some attack patterns are capable of being effectively mitigated via filtering at a port/protocol level. Some highly-damaging attack patterns cannot be effectively mitigated in this manner. Over time, MCNC's scrubbing centers should reduce the time it takes to mitigate potential DDoS attacks. In some cases, they may also help automate the mitigation of certain types of DDoS attacks, further reducing the impact on MCNC constituents.

Identity and access management as a service

MCNC offers centralized web security services by utilizing Zscaler's Security as a Service platform. This service features web content filtering, advanced threat protection, and real-time analytics. Community members utilizing this service can get protection across every user, location and device, including laptops, smartphones, and tablets.

Commitment to operational excellence

MCNC is guided by values in innovation, economic development, relationships with state and local government, thought leadership, and security solutions. MCNC's expanded security portfolio builds upon these values to continue offering further differentiation from commercial service providers. By taking a risk management approach to security – thoughtfully analyzing and making decisions based on risk levels as well as enterprise impacts – MCNC will continue to strengthen its security posture for NCREN customers for years to come as MCNC remains committed to Connecting North Carolina's Future Today.