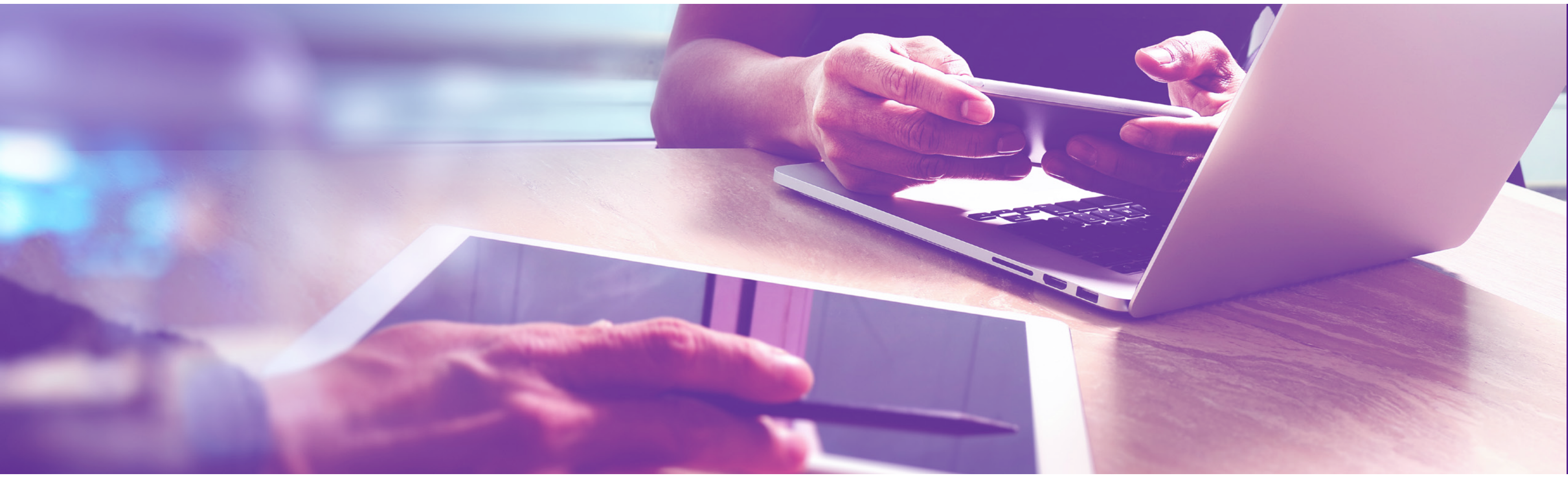

The Smart Approach to Networking for Enhanced Agency Cybersecurity

Increasingly sophisiticated internal and external cybersecurity threats require defense in depth with multi-faceted solutions and next generation networking technology.

The Cybersecurity Imperative

Every minute of every day Federal agencies face cyberattacks—from lone-wolf hackers and disgruntled employees to organized crime networks and nation state actors. Although their motives vary, their objective is clear--to disrupt operations and steal sensitive information collected and generated by government organizations. Consequently, threat identification and mitigation is more critical than ever for those responsible for the integrity, resiliency, and availability of agency networks, data, and systems. Conventional network defense at the perimeter is no longer sufficient to combat increasingly sophisticated attack sources and methods. Today, the smart approach to confront the complex threat landscape must rely on a network architecture that enables multi-layered threat prevention, detection, and response.

Extreme Cybersecure Networking

Extreme delivers government agencies a smart alternative to the conventional, outdated techniques and technologies that are proving largely ineffective to address digital age threats. At the foundation is a next-generation network virtualization technology that naturally compartmentalizes traffic.

Extreme Fabric Connect automatically partitions traffic, by community of interest, into virtual containers and maintains this separation end-to-end across the network. In addition to delivering highly efficient connectivity, this approach has the important, added benefit of denying unauthorized intruders the “node-hop” opportunities that borderless access affords. By reducing the attack surface available, agencies can take a significant step towards immediate improvement in their overall enterprise security posture.

Extreme Fabric Connect is an enhanced implementation of the next-generation network virtualization standard, and is significantly more powerful than conventional approaches.

Extreme Fabric Connect integrates an enterprise-class access control solution–Identity Engines–and seamlessly complements multi-layered threat detection and protection technologies. Extreme Fabric Connect redefines responsible networking in an age when the next cyberattack is a never-present reality.

The Technical Benefits

Built natively as a series of isolated virtual networks that interconnect only specifically-provisioned endpoints, Extreme Fabric Connect handles traffic forwarding in a fundamentally different way. Traffic that belongs to a specific service is encapsulated with the appropriate header at the Edge, remains isolated from all other traffic, and is opaque to intermediate network nodes. This transmission strategy mitigates the risk of traffic blurring between VLANs or seeping through generic routing tables. Many cyberattacks are conducted by relatively unsophisticated players, using tools shared or purchased from the Dark Web. An Ethernet-centric Extreme Fabric Connect network creates a topology that is invisible from an IP perspective; there are no contiguous hop-by-hop IP paths to trace, therefore the network topology cannot be traced using remote IP-based hacking tools. In some recent cases, hackers initially have focused on the government agency websites as potential attack launch points. By exploiting known nor unknown vulnerabilities to gain entry and by using the borderless nature of the internal network, attackers have been able to simply roam at will until data of sufficient value has been found and extracted. The Extreme Fabric Connect approach isolates individual end-points and services from each other, delivering a true ships-in-the-night capability that is called “stealth networking.”

This unique capability complements defense-in-depth and specialist overlay services and is designed to support data-driven protection strategies.

Deployed in concert with an enterprise-class access control broker, such as Identity Engines, Fabric Connect leverages fine-grained authentication to create an especially effective policy enforcement point; no connectivity is provided without the hosts first authenticating themselves. Failed or suspect hosts are completely isolated and can be mapped to quarantined or remediation zones.

The Extreme Approach

Extreme enables a more manageable, cost-effective enterprise network that delivers end-to-end simplicity from the datacenter to the network edge. Embedding automation and integration delivers a more agile network where applications, devices, and users view the network as a simple connectivity utility that automatically reconfigures itself when changes occur. Extreme makes it possible for the network to handle once-manual functions automatically, reducing the potential for error, and accelerating time-to-service. An automated core takes advantage of a single, network-wide Ethernet Fabric to remove the need for manual configuration at each network hop. This approach empowers the network to quickly respond to changing business and operational equirements with precision and flexibility.

Learn More

For more information, please contact your Extreme Networks Account Manager or Authorized Partner and visit www.extremenetworks.com.

Extreme®
Connect Beyond the Network

http://www.extremenetworks.com/contact / Phone +1-408-579-2800