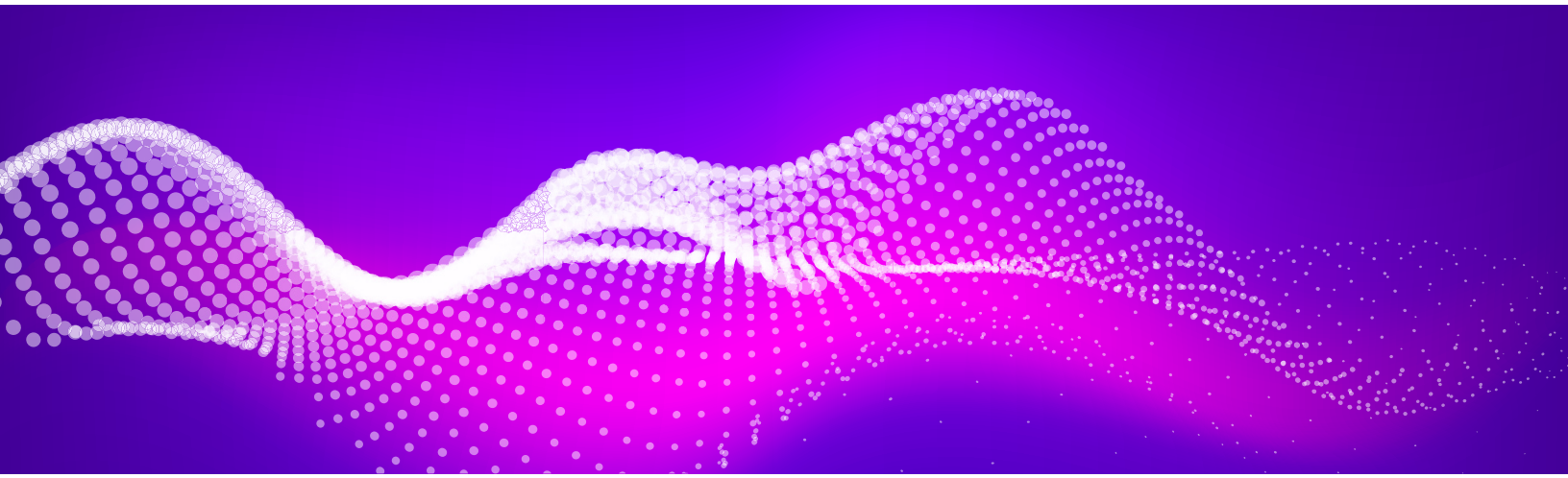

End-to-End Hyper-Segmentation for Smarter Networking

Supplanting legacy protocols, hypersegmentation delivers scale-out service separation and seamlessly traverses the entire organization, from device to data center.

With hyper-segmentation, organizations can establish borders to defend against unauthorized lateral movement, reduce their attack profile, deliver highly effective breach isolation, improve the effectiveness of anomaly scanning, and greatly improve the value of specialist security appliances.

The Business Imperative

As businesses undertake the digital transformation, the trends of cloud, mobility, and IoT converge. Organizations need to take a holistic approach to protecting critical systems and data, and an important area for attention is the ability to isolated traffic belonging to different applications. Effective network segmentation enables the organization to deliver separate virtual networks, each tuned to meet specific requirements. Doing so separates essential applications, protects confidential data and serves as the foundation for a sound security strategy.

The most literal approach to network segmentation is to run separate physical networks. However, this method isn't just costly, but simultaneously maintaining multiple networks is time-consuming in the extreme; a burden that could easily cripple most IT departments.

Traditional VLANs have been popular given that they can be used to create logical domains that can span multiple physical LAN segments. However, VLANs require significant manual configuration and do not easily scale beyond the edge of the network.

A carrier-focused service like MPLS is another option, although this form of traffic separation is typically only used by large enterprises, and then normally only for wide-area connectivity. It requires a significant investment in complex networking equipment, and a highly trained staff to provision the network and maintain the configuration.

Hyper-Segmentation: End-to-End Separation Needs to be the New Normal

The Data Center trend for micro-segmentation or macro-segmentation (depending upon marketing preferences) that delivers finely tuned connectivity between virtual machine hypervisors is certainly a step in the right direction. It is, however, by definition only a partially solution to a much broader problem: application traffic traverses the entire network, and is not contained within the confines of the Data Center.

Extreme, however, enables organizations to easily and seamlessly create network-wide virtual segments. These segments utilize a shared, independent control plane that is abstracted from network hardware elements, and can be implemented end-to-end, from device to data center. This capability is called hyper-segmentation.

Extreme's hyper-segmentation technology, enabled by the Extreme Fabric Connect technology, helps secure the network by virtually segregating traffic according to enterprise-specific requirements: for example, by business unit or for a compliance-driven application such as a payment card financial transactions. Uniquely, these hyper-segments can span the entire network. They are established using a simplified edge-only provisioning capability, and automatic attachment is supported thereby improving time-to-service and reducing the operational burden. Hyper-segments can also be dynamically triggered by users, endpoint devices, applications, servers, networking nodes, and business policy. The underlying technology's programmatic nature allows for seamless integration with workflow platforms.

"There are only two types of companies: those that have been hacked, and those that will be."

US Federal Bureau of Investigation

Service Separation

Fabric Connect handles traffic forwarding in a fundamentally unique way, building connectivity as a series of isolated virtual networks that interconnect specifically-provisioned end-points only. Traffic belonging to a specific service is encapsulated with the appropriate header at the Edge, and remains isolated – end-to-end across the network – from unconnected service traffic and is also opaque to intermediate network nodes.

Uniquely, Fabric Connect isolates foreign services from each other, delivering a true "ships-in-the-night" capability. This mitigates the need for intra-network ACLs and Firewalls; VSNs are oblivious to each other, as are hosts on different VSNs, and there is no risk of traffic blurring between VLANs or seeping via generic routing tables.

- The megatrends of cloud, mobility, and IoT are converging
- Protecting mission - critical systems and data is becoming increasingly important
- Businesses can mitigate the chances of being a cyber-attack victim by reducing their attack profile
- Limiting points in ingress and obscuring those that remain significantly lessens the potentially exploitable attack surface
- Conventional networking is very easily mapped: good for connectivity and network management, but double-edged as it also presents a well-understood attack platform for hackers

End-to-End Reach

Unlike VLAN tagging, domain stitching, or using MPLS within the enterprise, Fabric Connect allows hyper-segmentation to natively extend end-to-end across the network; from device to data center. Contrary to conventional topology-specific technologies such as VLANs and MPLS, network-wide segmentation ensures that traffic belonging to specific to a group of users or a particular application remains isolated for the entirety of its transmission from source to destination.

With end-to-end segmentation there is no point where traffic flows belonging to different applications is allowed to mix. Everyday examples of how this might be implemented include Guest WLAN access that is isolated from normal corporate traffic and only permitted to connect to the Internet; IP Telephony sessions from handsets to call server are partitioned from other applications; all traffic associated with a payment card service is isolated as it traverses a shared infrastructure.

This has the combined benefits of contiguous end-to-end service delivery and reducing complexity and operational burden. Network-wide segments are seamless and created with simplified configuration commands at the network edge. Service configuration is then automatically distributed throughout the network. Organizations are now able to add new services or make changes to existing services in minutes rather than days, weeks, or months.

The Fabric Connect control plane also offers flexibility in network design: any logical or physical topology can be created – whether it is Ring, Tree, Hierarchical, or Layer 2 or Layer 3, or any combination – anywhere there is Ethernet connectivity. This eliminates traditional design constraints and offers the freedom to build protected service segmentation on demand, wherever and whenever it is needed.

- Segmentation trends in the Data Center deliver finel tuned connectivity between virtual machine hypervisors
- By definition, however, it is only a partially solution to a much broader problem
- Application traffic traverses the entire network and is not contained within the Data Center

- By contrast, Extreme enables organizations to easily and seamlessly create network-wide virtual segments.
- Implemented end-to-end, from device to Data Center is the Extreme capability known as hyper-segmentation.

Lateral Borders

Antiquated policy and an over-reliance upon conventional perimeter defense can leave companies ill-prepared to face digital-age threats. In some recent cases, attackers have been known to initially focused on the external corporate website, seeking to leverage this as a launch point. Exploiting unrecognized or unpatched vulnerabilities to gain entry, and taking advantage of the borderless nature of the internal network, has permitted attackers to simply roam at will until data of sufficient value has been found, mined, and extracted.

Extreme delivers businesses a smart alternative to conventional, outdated techniques and technologies that are proving largely ineffective to digital-age threats. Solutions created using Fabric Connect leverage, at their foundation, a next-generation network virtualization technology that naturally compartmentalizes traffic. This unique capability is very complementary to defense-in-depth and specialist overlay services, supporting data protection for security-conscious organizations.

Complementary Security

Hyper-segmentation is very complementary to defense-in-depth and specialist security service overlays, enhancing data protection for security-conscious companies. Leveraging Fabric Connect, it becomes easy to implement additional layers of security, such as state-aware firewall and intrusion detection. These can then be configured to focus on a very narrow profile of that traffic which is acceptable and a normal baseline, versus what is potentially anomalous. In other words, establishing narrowed connectivity and information flow domains allows for known-good traffic patterns to be baselined, and anomalies to be more easily and quickly detected. Therefore, when suspect behaviors are identified, they can be signaled to reporting platforms for detailed examination and corrective action.

Leveraging the dynamic network segmentation capabilities of Fabric Connect, individual anomalous devices, or entire end-to-end systems, can be moved to separate logical segments. This allows for specialist analysis to be conducted, in real-time, while minimizing exposure to a potential threat. Rather than only being able to block a suspect device, and therefore potentially over-reacting to a false positive, organizations can also choose to adopt a "wait and see" approach; essentially a half-way house between normal application access and complete isolation.

In cases where malicious activity has passed a defined threshold, offending systems can be swiftly quarantined, and forensics tools brought to bear.

Additionally, when deployed in concert with an Enterprise-class access control broker such as Extreme Identity Engines, Fabric Connect leverages fine-grained authentication and authorization to create very effective policy enforcement points; no connectivity is provided without users and/or devices first proving themselves.

- Fabric Connect builds connectivity as a series of isolated virtual segments that deliver a true "ships-in-the-night" capability
- Network-wide segmentation ensures that traffic remains isolated for the entirety of its transmission from source to destination
- Fabric Connect naturally compartmentalizes traffic and counters the borderless nature of conventional networking
- Leveraging narrowed information domains allows for known-good traffic patterns to be baselined and anomalies to be more easily and quickly detected
- Created only at the Edge, networkwide segments are automatically distributed throughout the network, eliminating error-prone and time-consuming manual configuration practices.
- Fabric Connect's programmatic nature allows for subject-specific private networks to be established without manual provisioning.

Edge-Only Provisioning

Network-wide segments are seamless, created with simplified configuration commands on an Edge node. Fabric Connect automatically permeates the configuration throughout the network, eliminating error-prone and time-consuming network-wide manual configuration practices. Organizations are now able to add new services or make changes to existing services in minutes rather than days, weeks, or months.

Edge-only provisioning completely removes any need for service-specific configuration in the Core, or any other intermediate Fabric Connect node; if a service is present on just two nodes, then the necessary onfiguration appears on only these two nodes, nowhere else, regardless of the network topology or size. This completely revolutionizes the configuration and change paradigm, from hop-by-hop to end-to-end; configuration becomes vastly simplified and change is de-risked.

Fabric Attach facilitates the automatic attachment of authenticated end-point devices directly into their appropriate VSNs. Equally beneficial at both the Wiring Closet and Data Center edges, Fabric Attach supports dynamic service creation and removes the delays and risks associated with manually configuring conventional networks.

Massive Scalability

Many conventional networks, including those offering virtualization capabilities, remain constrained by the original VLAN specification that limits the number of unique services to just over four thousand. This number may have been sufficient when segmentation was applied only very coarsely, but, in an age of IoT, mass segmentation will be crucial to delivering both effective scalability and isolation-based security.

Thankfully, Fabric Connect delivers a distinctly different operational experience. Simply put, communication is established between two or more devices by all being configured as members of the same Virtual Service Network (VSN). This configuration is applied only at the Fabric Edge, using one of 16 million unique Service IDs, and creates a virtual segment that can span end-to-end across the network. Crucially, the core of the network does not need to be re-configured to support a new or changed VSN, allowing services to be dynamically provisioned without introducing risk.

Dynamic Workgroups

Some organizations maintain a need for additional levels of separation to be applied, either temporarily or in the long term. Examples include were "Chinese Walls" are created for projects or ongoing joint-venture operations. However, the individuals and devices involved in such activities can often need to move between these sensitive functions and their more routine roles.

This desire to selectively apply enhanced protection can present something of a challenge as many organizations have enacted policies that forbid the use of encryption technologies for communications and storage. This is as a result of these technologies becoming closely associated with the use of the "Dark Web" and nefarious activities such as organized crime and terrorism. Law enforcement agencies argue against the uncontrolled availability and wide-spread use of this technology, and it is often blocked at security demarcation points.

This dichotomy makes life difficult for those organizations that wish to responsibly apply enhanced levels of protection for particularly sensitive applications and data but need to ensure that they do not become an unwitting third party to serious illegal activity.

Extreme is able to provide a solution to this requirement through a combination of unique technologies. Teams, being people and/or devices, can be dynamically created, automatically relocated to a new and unique network segment, and additional levels of protection can be applied. The programmatic nature of Fabric Connect allows for these subject-specific private networks to be established without the need to involve manual configuration or provisioning. Leveraging an Extreme Breeze-powered workflow, users can self-provision the required connectivity and services: private network segmentation, IP Address re-assignment, and access to restricted implementations of applications such as unified communications, video conferencing, and file sharing. The private network is available only to authorized personnel and is active only as required.

Imagine the scenario where a project team working on M&A activity has a weekly call: a single click on the meeting link would automatically trigger a series of background provisioning changes that form this group on individuals, and their relevant devices, into a separate private network. All of the normal Fabric Connect stealth capabilities apply, and through a partnership that Extreme has established with security innovator Senetas, it is also possible to selectively add end-to-end encryption. Therefore, organizations can dynamically deliver a genuinely private – and secure – workgroup networking capability.

- IoT and Smart infrastructures are driving an unprecedented expansion in networked connectivity
- Organization cannot afford to ignore the importance of protecting access to its network, applications, and information
- Without proper controls, a breach of one device could provide a hacker with the virtual keys to the castle
- Extreme helps to significantly reduce the level of network exposure and avoid the chinks that are normally used for an exploit

The Extreme Difference

The world is on the verge of an unprecedented expansion in networked connectivity, driven by the combined forces of the Internet of Things and Smart infrastructures. No organization can afford to ignore the importance of protecting access to its network, applications, and information. Without proper controls, a breach of one device could provide a hacker with the virtual keys to the castle.

Hyper-segmentation delivers scale-out service separation and seamlessly spans the entire organization, from device to data center. Critical applications and confidential data can be easily and automatically compartmentalized, users and devices partitioned, and policy boundaries established. Extreme provides the networking attributes that are fundamental for businesses operating in the age of IoT.

With hyper-segmentation, organizations can establish borders to defend against unauthorized lateral movement, reduce their attack profile, deliver highly effective breach isolation, improve the effectiveness of anomaly scanning, and maximize the value of specialist security appliances.

Lateral movement is regulated and this helps defend the greater network should one element be subject to attack; breach isolation is an important aspect of defense-in-depth. Intelligently segmenting applications and content enables more effective baselining and anomaly scanning.

Extreme delivers technologies that help secure the everywhere-perimeter. Organizations can significantly reduce the level of network exposure and they can avoid the chinks that are normally used for an exploit.

Empowering businesses to differentiate their critical application and confidential data, to efficiently and with massive scale partition the essential, and to obscure and harden the network, provides a comprehensive security foundation in an epoch of cyber-attack and IoT.

Extreme delivers is a solution set of next-generation capabilities that address the challenges of the everywhere-perimeter. It provides a foundational layer for the specialist security services employed today, enabling their effectiveness to be maximized. Extreme leverages a shared control plane that seamlessly manages hyper-segmentation, native stealth, and automatic elasticity across the organization. Using software-defined and identity technologies to automate onboarding and access from users, devices, networking nodes, and servers, Extreme makes protecting and managing everywhere-access practical.

Learn More

To learn more about Extreme Networking, and to obtain additional information such as white papers and case studies, please contact your Extreme Account Manager or Authorized Partner or visit us at www.extremenetworks.com.