Securing the Everywhere Perimeter

IoT, BYOD, and Cloud have fragmented the traditional network perimeter. This revolution necessitates a new approach that is comprehensive, pervasive, and automated.

Businesses need an effective strategy to differentiate critical applications and confidential data, partition user and devices, establish policy boundaries, and reduce their exposure.

Leveraging Extreme Networks technology, organizations can hide much of their network and protect those elements that remain visible. Borders are established that defend against unauthorized lateral movement, the attack profile is reduced, and highly effective breach isolation is delivered. This improves the effectiveness of anomaly scanning and the value of specialist security appliances. Redundant network configuration is rolled back, leaving an edge that is "clean" and protected from hacking. Businesses avoid many of the conventional hooks and tools that hackers seek to exploit. Additionally, flipping the convention of access-by-default, effective access control policy enforcement denies unauthorized connectivity.

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 important areas for attention are the ability to isolate traffic belonging to different applications, to reduce the network's exposure and attack profile, and to dynamically control connectivity to network assets.

In addition to all of the normal challenges and demands, businesses are also starting to experience IoT. This networking phenomenon sees unconventional embedded system devices appearing, seemingly from nowhere, requiring connectivity.

IoT is being positioned as the enabling technology for all manner of "Smart" initiatives.

The pervasive consumerization of technology is also driving IoT into businesses. What's crucial for success is the agility, scalability, and robustness of the underlying information technology infrastructure.

Securing the Everywhere-Perimeter: Deploying an IoT-ready Architecture

The Securing the Everywhere-Perimeter program formalizes a series of capabilities that seek to address both traditional and emergent networking requirements with an innovative approach to protecting critical applications and confidential data.

The three key emerging challenges – implementing scalable segmentation, managing the double-edged nature of IP reachability, and securing edge configuration and attachment – are addressed by the three pillars of the Extreme Securing the Everywhere-Perimeter:

- Hyper-Segmentation
- Native Stealth
- Automatic Elasticity

Security experts agree: the expanded use of network segmentation is an invaluable tool in thwarting cyber-attacks[1]. It is a recommendation that has obvious merit. Segmentation can severely limit lateral movement, thereby helping to protect essential applications and confidential data. Additionally, wide-spread use of segmentation complements traditional security technologies.

The world is on the verge of an unprecedented surge in networked connectivity. For this evolution to hyper-connectivity to be successful managed, both in terms of efficiency of delivery and protection against cyber-attack, networks need a foundation that seamlessly integrates scalability, security, and automation.

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

Effective network segmentation enables organizations to separate essential applications, protect confidential data. Separate virtual networks, each tuned to meet specific application requirements, 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.

[1] Rob Joyce, Chief of Tailored Access Operations, US National Security Agency: "Disrupting Nation State Hackers", USENIX Enigma, January 2016.

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.

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 Networks, however, enables organizations to easily and seamlessly create networkwide 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.

For hyper-connectivity to be successful, networks need a foundation that seamlessly integrates scalability, security, and automation.

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.

Native Stealth: Security Through Designed Obscurity

Limiting how much of the network is visible, and hardened that which is, goes a long way to reducing the opportunities presented to cyber-attackers. Proactively obscuring the network, at and between access nodes, minimizing the exposure profile and helps with defense-in-depth.

These characteristics combine to offer a prospective hacker with little to exploit. Much of the network is hidden, and that which remains visible is free of the hooks that make conventional networks vulnerable.

Conventional networking has progressively evolved, due to a number of factors, to where is has essentially become a collapsed, routed backbone with multiple virtual interfaces that provide connectivity to a variety of user segments. In practice, this is configured as multiple Virtual LANs (VLANs) that support groups of users, each with a routed interface (terminating on Virtual Routers).

The Layer 3 engines at the heart of the network populate tables with all known routes, facilitating interconnectivity and creating a situation where any-to-any communication is the necessary default behavior.

In larger networks, end-to-end connectivity is, in fact, a series of hop-by-hop forwarding decisions. Being IP-centric, the conventional network topology is very easily and quickly mapped; this is good for network management purposes but is double-edged insofar as it also presents an effective attack platform for hackers. Being IP-centric, attacks can be launched from any point within or external to the network.

In an effort to control the default any-to-any behavior – rarely practical in and of itself – businesses often chose to lock-down connectivity to selective paths so that any-to-any doesn't simply become a conduit used by attackers. Options include using Access Control Lists (ACLs) or distributed physical or virtual state-aware firewalls to limited, for example, users-to-application, not users-to-users. These measures can be expensive and are always complex to plan, deploy, and maintain.

Extreme Networks delivers a distinctly different administrative and operational experience. Being Ethernet-centric, the Fabric Connect network topology is invisible from an IP perspective; there are no inherent hop-by-hop IP paths to trace, therefore the network topology cannot be traced using remote IP-based tools.

Stealth networking makes the infrastructure invisible from an IP perspective, making the topology untraceable using remote IP-based tools.

Fabric Connect leverages a MAC-layer service identifier, the Virtual Service Network ID, and this enables an IP-free approach to traffic forwarding decisionmaking. This 24-bit identity uniquely defines a particular service; delivering hyperscalability that exceeds 16 million entities. It is part of the IEEE 802.1ah Header that encapsulates the standard 802.3 Header and datagram. The Header and identity are applied at the edge of the domain. Intermediate nodes base their forwarding decisions upon the shortest path/s to the destination node, through a shared understanding of the network topology, using the Destination Edge Bridge's MAC Address (again, part of the 802.1ah Header) as the directing data point.

Traffic belonging to a specific service is encapsulated with the appropriate header at the Edge, and remains isolated from every other service/traffic, and opaque to intermediate nodes. This mitigates the need for intra-network ACLs and Firewalls; Virtual Service Networks (VSNs) are oblivious to each other, as are hosts on different VSNs, and there is no risk of traffic blurring between VLANs or seeping through generic routing tables.

Therefore, rather than conventional any-to-any, the entire basis of connectivity becomes one-to-one or a series of multiple ones-to-ones. In its simplest form – two devices communicating with each other over the backbone – connectivity is established by both being configured, only at the Fabric Edge, as members of the same VSN. Services, Layer 2 and Layer 3 VSNs, are a function of explicit provisioning, and communication between different services is blocked unless specifically enabled.

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 configuration appears on only these two nodes, nowhere else, regardless of the network topology or size. This completely revolutionizes the configuration and change paradigm, from hopby- hop to end-to-end; configuration is vastly simplified and change is de-risked.

Automatic Elasticity: When Denial-of-Service is a Good Thing

Minimizing the amount of network segment configuration that is needlessly distributed to the network edge provides a further layer of protection. Obscuring unrequired segment configuration unless and until specifically required by authenticated and authorized user/device connectivity reduces the profile presented for a potential attack.

Elasticity simplifies and expedites provisioning, but crucially, it has the added benefit of reducing a network's exposure and attack profile.

The original approach to support network segmentation was to statically provision application or departmental VLANs – for example, "Data" and "Voice", or "Operations", "Engineering" and "Research" – on all edge nodes, and configure physical Switch ports to support one or more of the segments. While static configuration is technically valid, it is increasingly seen as sub-optimal. Even if the environment is accurately documented and the record keeping was scrupulously maintained, there remains a risk of exposure. When VLANs are statically configured at the network edge, and no additional user or device evaluation, authentication, and authorization is invoked, the network is essentially open.

Extreme Networks has pioneered the concept of "automated network elasticity" that mitigates the need for manual configuration. This capability automatically stretches the required segment to the edge of the network only as and when required, seamlessly integrating with hyper-segmentation. As applications terminate, or end-point devices close-down or disconnect, the now-redundant networking services are automatically retracted from the Edge. This elasticity as two obvious benefits: it simplifies and expedites provisioning for the ever-increasing number of network devices, but crucially it has the added benefit of reducing a network's exposure and attack profile. To use an everyday analogy: people don't walk around with their wallet or purse out, open, and their cash exposed, rather, they keep it hidden and produce it only when it is safe and appropriate to do so.

The first thing to say, it's neither feasible nor desirable to attempt to pre-provision every possible network segment at every Edge node. The business environment never achieves finality, there's never a point at which evolution stops, and so it's unrealistic to declare a "final" network configuration. Equally, such as configuration would be extremely complex, prone to error, difficult to troubleshoot.

Crucially, it would expose every network segment at every network Edge node, and doing so would be a highly undesirable act. In a variation on the time-honored "need to know" maxim, network access should be elastic, only extended to the Edge as required, and retracted once the genuine need has passed. Replacing static network device configuration with dynamic programming reduces overall complexity in the network and has a corresponding benefit in reducing the risk of outage due to misconfiguration or attack.

In the context of the Internet of Things (IoT), end-point devices – more often than not, unattended devices – need to be deployed in real-time, without IT intervention or manual configuration, via a centralized policy engine that defines and enforces compliance with the business policy. Extreme's award-winning Identity Engines is an ideal solution, providing enhanced user and/or device authentication and policy control.

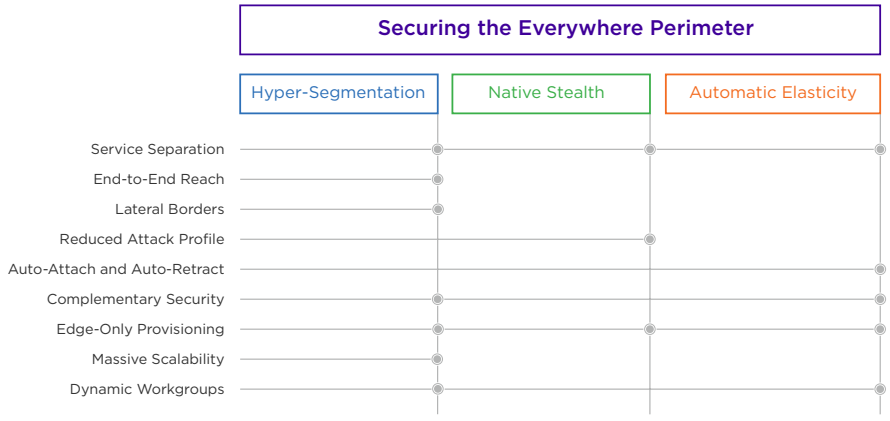
Leveraging a variety of existing techniques for recognition, authorization, and authentication – i.e. MAC- and/or RADIUS-based, 802.1X, and 802.1AB– users or devices request application-specific network assignment during start-up and/or connection. Network connectivity – VLAN, QoS, Policy, whatever characteristics are needed to deliver the required service – is then dynamically extended to the Edge. Any particular networking session may last only minutes or hours, or perhaps days. Regardless, the key attribute is that service is automatically provisioned – "spun-up" if you will – without manual intervention or pre-configuration. Similarly, once the session terminates, the same-said networking configuration is then automatically undone, removed from the Access node, and consigned to history.

In addition to supporting the flexible deployment of obvious network end-points such as IP Phones, Wireless APs, and IP CCTV Cameras, network elasticity plays a crucial role in facilitating IoT solutions. Including those that leverage the Session Initiation Protocol (SIP).

Securing the Everywhere-Perimeter Capabilities

The individual pillars deliver a series of key enabling capabilities. In some cases, these capabilities are common to two or all of the pillars, alternatives they may be unique to one specific pillar.

Service Separation

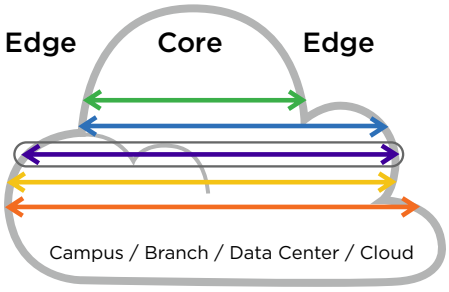


Fabric Connect handles traffic forwarding in a fundamentally unique way, building connectivity as a series of isolated virtual networks that interconnect specificallyprovisioned end-points only. Traffic belonging to a specific service is encapsulated with the appropriate header at the Edge, and remains 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,

Traffic is encapsulation at the Edge, and separation is maintained end-to-end accross the network. Delivering a true "ships-in-the-night" capability.

Mitigates the need for intra-network ACLs and Firewalls. No risk of traffic blurring between VLANs or seeping via generic routing tables.



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.

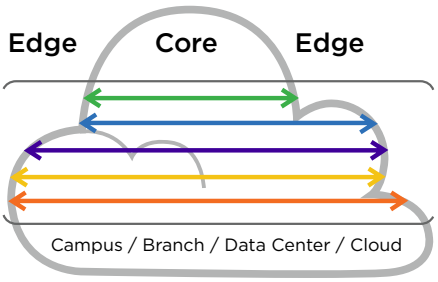
Hyper-segmentation helps organizations secure their network by virtually segregating traffic according to enterprise-specific requirements.

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 specific to a group of users or a particular application remains isolated for the entirety of its transmission from source to destination.

Unlike other technologies, hyper-segmentation natively extends end-to-end across the entire network.

Delivers contiguous virtual segments; all the way from Device to Data Center, from Brand to Cloud.



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.

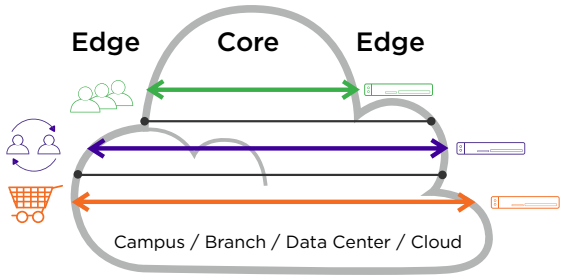
The Fabric Connect control plane also offers flexibility in network design: any logical or physical topology can be created – whether it is Ring, Tree, Hierarchical, or Layer 2 or Layer 3, or any combination – anywhere there is Ethernet connectivity. This eliminates traditional design constraints and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

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.

In boredless networks, a successful exploit of one device, host, or segment places the entire network at risk.

Creating a defined border prevents within the network prevents attackers from roaming at will.



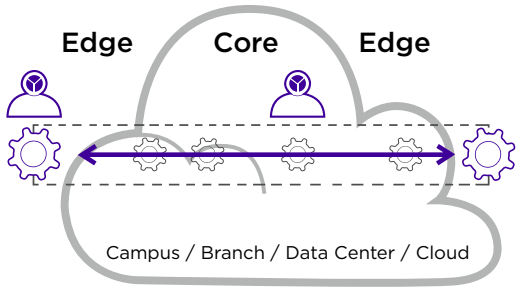
Extreme Networks delivers businesses a smart alternative to conventional, outdated techniques and technologies that are proving largely ineffective to digital-age threats. Solutions created using Fabric Connect leverage, at their foundation, a nextgeneration network virtualization technology that naturally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

Reduced Attack Profile

Cyber-attacks can originate from a variety of source: ranging from nation-state players to the relatively unsophisticated using tools shared or purchased via the Dark Web. However, a Fabric Connect network, being Ethernet-centric, operates a topology that is invisible from an Internet/IP perspective; there are no contiguous hop-by-hop IP paths to trace, therefore the network topology cannot be mapped using IP-based hacking tools. This is a function of specific design intent, delivering more than simple “security-through-obscurity”, but conscious obfuscation of the network topology, reachability, and services.

The Ethernet-centric technology is invisibile from an Internet/IP perspective.

There are no contiguous hop-by-hop IP paths to trace, therefore the network topology cannot be mapped using IP-based hacking tools.



Network management is fully supported – indeed, additional Layer 2 tools are delivered – however, individual devices will only ever see, at most, the other hosts on their specific virtual segment. Individual Fabric Connect networking nodes are not, by default, visible to any host on any VSN; if enabled, ICMP would only show the VSN Edge nodes, but nothing of the inner network.

It is neither feasible nor desirable to pre-provision every possible application segment at every Edge node. Because individual networking sessions may last only minutes, hours, or perhaps days, Fabric Attach empowers network connectivity – VLAN, QoS, Policy, et al – to be dynamically extended to the Edge. What's pertinent, in this scenario, is that service is automatically provisioned – "spun-up" if you will – without manual pre-configuration or intervention. Similarly, once a session terminates, the now-redundant networking configuration is automatically undone, removed from the Access node, and consigned to history.

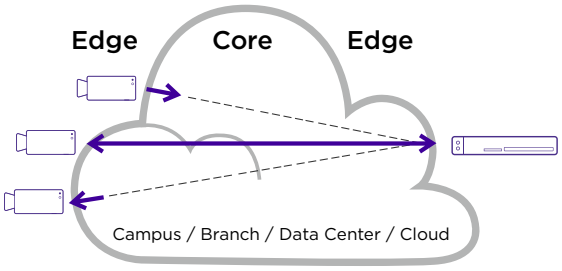
These characteristics combine to offer a prospective hacker with little to exploit. Much of the network is hidden, and that which remains visible is free of the hooks that make conventional networks vulnerable.

Auto-Attach & Auto-Retract

Auto-Attach, pioneered by Extreme as "Fabric Attach" and being standardized by the IEEE (as the 802.1Qcj standard). It leverages a secure signaling exchange to automate connectivity and network segment assignment. It works by enabling Auto-Attach Clients (or Proxies, typically Ethernet Switches, operating on their behalf) to present connection request to nodes on the edge of the Fabric Connect domain. There are a number of deployment options, providing flexibility to accommodate the vagaries of Auto-Attach device capabilities, Fabric Connect topologies, and whether Identity Engines is part of the solution.

Auto-Attach Clients present connection request to Fabric Connect edge nodes,

Network segement configuration is absent from the network edge pre-Attach and post-Attach



Clients – end-point devices – requesting either specific or non-specific network assignment are both supported. The Client can present a particular VLAN identity or alternatively nothing, and the actual network assignment decision is made with reference to administrator-defined criteria and policy. This enables devices such as video surveillance cameras or building automation sensors that leverage their factory-configured, application-specific VLAN identity, enabling them to be easily discriminated and subsequently associated with the appropriate network segment that supports their application.

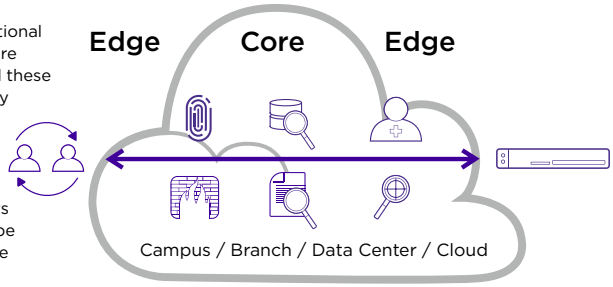
The crucial advantage is that all network segment configuration remains absent from the network edge unless and until valid user and/or device connectivity has been requested and authorized. This provides a further layer of protection by obscuring currently unrequired network segments and reducing the attack profile.

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.

It becomes easy to implement additional layers of security, such as state-aware firewall and intrusion detection, and these can be configured to focus on a very narrow baseline of acceptable and normal traffic.

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.



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.

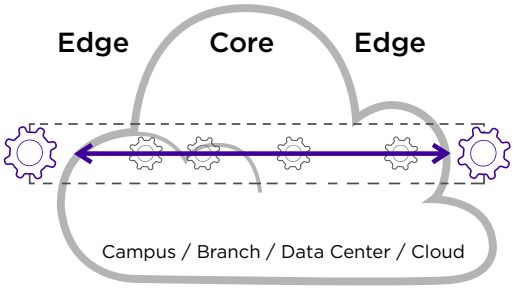
Additionally, when deployed in concert with an Enterprise-class access control broker, Fabric Connect leverages fine-grained authentication and authorization to create very effective policy enforcement points; no connectivity is provided without users and/or devices first proving themselves.

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.

Completely removes any need for service-specific configuration in the Core, or any other intermediate node.

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.



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 configuration appears on only these two nodes, nowhere else, regardless of the network topology or size. This completely revolutionizes the configuration and change paradigm, from hopby- hop to end-to-end; configuration becomes vastly simplified and change is de-risked.

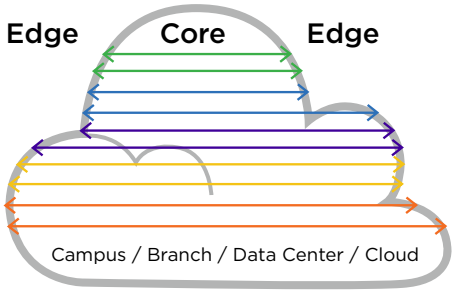
Fabric Attach facilitates the automatic attachment of authenticated end-point devices directly into their appropriate VSNs. Equally beneficial at both the Wiring Closet and Data Center edges, Fabric Attach supports dynamic service creation and removes the delays and risks associated with manually configuring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

Original VLAN technology may have been sufficient when segmentation was applied only very coarsely.

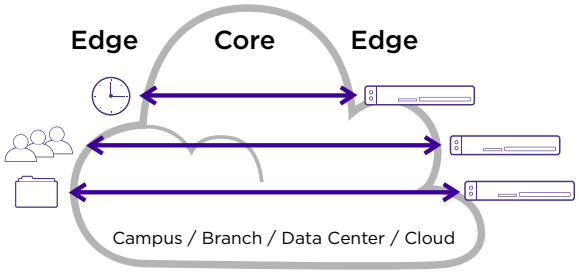
But, in an age of IoT, mass segmentation will be crucial to delivering both effective scalability and isolation-based security. Now, Fabric Connect delivers end-to-end scalability that scales up to 16 million unqiue Service IDs.



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.

Teams can be dynamically created, automatically pre-provisioned to a new and unique network segment, and additional levels of protection applied.

Programmatic capabilities enable these subject-specific private networks to be established without the need to involve manual configuration or provisioning.



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.

Extreme Networks 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.

Crucially, the edge of the network is purged of default access and redundant configuration. Implementing robust authenticated and authorized access control, in concert with a dynamic auto-attachment capability, ensures that the network's attack profile is further reduced. Forcing every user and device to positively justify connectivity establishes a strong first line of defense and a presents a significant obstacle to would-be hackers.

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.

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 Networks 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 hypersegmentation, 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 Networks 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.

Extreme networks

http://www.extremenetworks.com/contact