Smarter Networking with Automatic Elasticity

A Holistic Approach to Protecting Critical Systems and Data

Integrated elasticity delivers multiple benefits to the information-centric organization: service agility is enhanced, access control can be effectively enforced, any unused or redundant configuration is rolled back, leaving the network edge "clean". Flipping the convention of access-by-default, automatic elasticity obscures even the hint of network configuration, let alone connectivity, unless and until successful authentication.

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 dynamically control connectivity to network assets. Being able to automatically extend connectivity to valid users and devices, aids more than just business agility, it establishes a paradigm where the default condition is more secure than what conventional networking delivers.

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.

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.

Extreme has pioneered the concept of "network elasticity", and we're uniquely positioned – by virtue of our differentiated technologies – to deliver solutions that make this a reality. The capability stretches network services to the Edge, only as required and only for the duration of a specific application session. As applications terminate, or end-point devices close-down or disconnect, the now-redundant networking services retract from the Edge. This elasticity as two obvious benefits: it simplifies and expedites provisioning for the ever-increasing number of network devices, and it has the added benefit of reducing a network's exposure and attack profile. To use an everyday analogy: people don't walk about with their wallet or purse out, open, and their cash exposed; no, they keep it hidden and produce it only when specifically needed.

> *"The 'Art of War' teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable."*
>
> **Sun Tzu**

- The megatrends of cloud, mobility, and IoT are converging
- Protecting mission-critical systems and data is becoming increasingly important
- While static configuration is technically valid, it is increasingly seen as sub-optimal
- Without strong and universal authentication and authorization, statically configuring VLANs at the edge exposes the network to risk
- Minimizing the needless distribution of network segment configuration provides a further layer of protection
- It's neither feasible nor desirable to pre-provision every possible application segment at every Edge node
- In a variation on "need to know", network access should be elastic, extended only when required and then retracted
- Dynamic programming reduces complexity and reduces the risk of attack or misconfiguration
- In the context of IoT, often unattended end-point devices need to be deployed in real-time, without IT intervention or manual configuration
- Obscuring unrequired segment configuration reduces the profile presented for a potential attack

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

The first thing to say, it's neither feasible nor desirable to attempt to pre-provision every possible application segment at every Edge node. The business environment never achieves finality, there's never a point at which evolution stops. Therefore, it's unrealistic to declare a "final" network configuration, for universal deployment, to every Access Switch. 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 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 that leverage the Session Initiation Protocol (SIP). Extreme is uniquely positioned, given our ability to support the huge scalability demands that IoT will potentially make, to accelerate the deployment of these solutions.

- It's neither feasible nor desirable to pre-provision every possible application segment at every Edge node.
- In a variation on "need to know", network access should be elastic, extended only when required and then retracted.
- Dynamic programming reduces complexity and reduces the risk of attack or misconfiguration.

- In the context of IoT, often unattended end-point devices need to be deployed in real-time, without IT intervention or manual configuration.
- Obscuring unrequired segment configuration reduces the profile presented for a potential attack.

Auto-Attach and 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.

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.

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.

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 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 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.

- Extreme has pioneered the concept of “network elasticity”, stretching services to the Edge, only as required and for the duration of a specific session.
- With Fabric Attach, all network segment configuration remains absent from the network edge unless and until authorized.
- As sessions terminate, or end-point devices close-down or disconnect, the now-redundant networking services retract from the Edge.
- Two obvious benefits: simplifying and expediting the provisioning of network devices and reducing a network’s exposure and attack profile.

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 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.

To be effective and remain competitive, a modern business needs to have a high degree of service agility. However, IT struggles with the challenge of being responsive while also trying to maintain some sense of order; eventually, something has to give and traditionally this has been regulation network access. With the added dimension of IoT, the risk levels are only going to increase, and exposure of the network – and, by extension, the business – makes do-nothing an option that is no longer credible.

Static edge configuration and access-by-default are workarounds that have had their day. By contrast, automatic elasticity establishes an environment where edge configuration is dynamically extended and retracted, where user and device access has to be authenticated and authorized, and where automation provides the necessary scale and agility. It is a ground truth that networks are safer when access has to be explicitly earned rather than implicitly assumed.

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.

Extreme™
Customer-Driven Networking

http://www.extremenetworks.com/contact