Network Smarter with Native Stealth Capabilities

Avoiding the conventional hooks that enable most cyber-attacks, native stealth capabilities deliver a reduced attack profile and can help organizations avoid the risk or fallout of a hack.

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 reduce the network's attack profile. By reducing their exposure, businesses can mitigate the chances of a cyber-attack being successful or even launched. Limiting the available points in ingress, and obscuring those that remain, significantly lessens the attack surface available for potential hackers to exploit.

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 a double-edged sword 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.

> *"One ought to design systems under the assumption that the enemy will immediately gain full familiarity with them."*
>
> **Shannon's Maxim**

In an effort to control what is, in effect, global any-to-any reachability – 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.

- 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

Native Stealth: Security by 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.

Extreme delivers a distinctly new 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.

Fabric Connect leverages a MAC-layer service identifier, the Virtual Service Network ID, and this enables an IP-free approach to traffic forwarding decision-making. This 24-bit identity uniquely defines a particular service; delivering hyper-scalability 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; 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 hop-by-hop to end-to-end; configuration is vastly simplified and change is de-risked.

- Connectivity is typically defined a series of hop-by-hop forwarding decisions
- But, being IP-centric, this means that network attacks can be launched from any point
- Businesses often chose to lock-down connectivity to selective paths so that any-to-any doesn't simply become a conduit used by attackers
- However, these measures can be expensive and are always complex to plan, deploy, and maintain
- By contrast, limiting visibility of the network and hardened that which remains visible goes a long way to reducing attack opportunities
- Proactively obscuring the network minimizes the exposure profile and helps with defense-in-depth

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.

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.

- Fabric Connect offers a prospective hacker with little to exploit, being free of the hooks that make conventional networks vulnerable
- Being Ethernet-centric, Fabric Connect is invisible from an IP perspective, making it untraceable using remote IP-based tools
- Fabric Connect leverages a MAC-layer technique for traffic forwarding enabling an IP-free
- Traffic belonging to a specific service remains isolated from every other service/traffic, and opaque to intermediate nodes
- Edge-only provisioning completely removes any need for service-specific configuration in the Core, further limiting opportunities for potential attackers
- By reducing, obscuring, or even avoiding the conventional pitfalls, organizations can mitigate their exposure and focus their specialist security efforts on those areas that do must public

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.

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.

> By natively embedding stealth capabilities into the fabric of their network, organizations can significantly reduce their exposure to and risk of cyberattack. Avoiding many of the conventional hooks, and obsoleting the typical tools, that hackers seek to exploit, businesses can reduce their exposure and more tightly focus their specialist security efforts.

It has been said that there are two types of organization: those that have been hacked and know it, and those that have been hacked but do not know it. Hackers leverage common IP-based tools and techniques in order to gain entry and extract assets. Information-age organizations can significantly reduce their exposure to and risk of cyber-attack by ensuring that their network has a strong foundation of native stealth capabilities. By reducing, obscuring, or even avoiding the conventional pitfalls, businesses can mitigate their exposure and focus their specialist security efforts on those areas that do must public. Native stealth capabilities deliver a reduced attack profile and can help organizations avoid the risk or fallout of a hack.

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