

Network Masking:

Securing Your Network at Layers 2 & 3

Industry Problem

Network technology trends are exposing organizations to increasing Layer 2 security threats throughout networks as they become “borderless.” These threats include unauthorized network mapping, traffic analysis across segments, denial of service, and man-in-the-middle attacks. Layer 2 attacks are typified by low level probing to gather information, followed by a targeted attack. In a recent solicitation, one U.S. government agency commented:

“The first stage in a cyber attack is to perform reconnaissance on the target network. The attacker’s goal is to identify targets that either contain the desired information or are critical to network traffic. Following that step, the attacker will determine what is exploitable on the targeted network devices. If the information gathered above is incorrect, the attackers will waste time and resources attempting to exploit systems and services that may or may not exist, which will result in more time for the defenders to take the appropriate response.”

These attacks typically exploit a Layer 2 network protocol weakness; the “MAC” address of a device is fixed by the manufacturer and may be decoded using publicly available tools. Firewall, switch and IDS vendors consistently warn customers about the threats to their networks at Layer 2 and Layer 3. “White Hat” security auditors use Layers 2 and 3 exploits to gain access for penetration testing; however, until now they could not offer a mitigation strategy.

This had been viewed as a perimeter problem in the past, but government and commercial network technology trends, such as cross-domain interoperability, switch-oriented topologies, virtualization, and cloud computing, are exposing organizations to Layer 2 threats throughout networks as they become “borderless.”

VLANS, transparent firewalls, and port security are all attempts to secure Layer 2 and Layer 3. These only indirectly address the problem, restrict functionality and increase the configuration management burden. A new approach is needed.



A New Approach: Network Masking

Masking Networks has pioneered “network masking” to address these Layer 2 and Layer 3 threats by masking the identity and presence of firewalls, servers, LAN segments, and other devices. Effective network masking maintains full network interoperability and performance without increasing the network configuration management burden.

Network masking at Layer 2 includes methods for generating a proxy MAC address for the protected device, using that proxy to mask the device at wire speed, and hiding the device’s network hops. This also forms the essential foundation for network masking at Layer 3 as well as implementing secure higher layer applications.

The most urgent customer demand is driven by requirements to isolate and segment networks. Examples of network segmentation include government-contractor interfaces, industrial and IT networks, and places of converging network traffic. Network masking prevents or greatly hinders node hopping, traffic analysis, and other vulnerabilities in these situations.

Business enterprise networks have similar segmentation compliance requirements, particularly for energy, finance and healthcare markets. These include isolating a SCADA network from the utility IT network, protecting privacy information and financial transactions, as well as network segmentation for trade and export compliance. Network masking also provides small and medium businesses with an easy due care option to maintain a reasonable security posture without adopting a large configuration management burden.

In summary, network masking addresses the business requirement to segment networks as well as the information assurance requirement to secure Layer 2 and Layer 3.

Alternatives to Network Masking

Network device vendors have acknowledged the threat and tried to address Layer 2 security in their own products. Cisco whitepapers and customer training consistently warn of Layer 2 threats to their switches and recommend port security and VLANs as part of the answer. With port security, only pre-configured MAC addresses are recognized by the switch, and VLANs logically segment the switch traffic to virtual subnets. These steps only indirectly address the Layer 2 threat and also add a



significant audit and management burden for the network administrator. For example, while VLANs and port security do address a foreign device connecting to the network, they do not address the threat of a foreign bot infecting an authorized device and mapping the network. They are also not effective in protecting against perimeter attacks and do not prevent node hopping by an attacker. Port security and VLANs are indirect partial measures while network masking directly addresses the Layer 2 threat.

Many firewall and IDS vendors offer “transparent” modes of operation and so validate the concept of network masking at the network perimeter. However, their implementations typically result in limiting the switching features of the firewall, making it generally impractical to use in a multiport configuration. What is needed is a network masking implementation that covers fully configured firewalls and IDS.

Masking Networks’ Solution

Masking Networks, with its patent pending Masking Shunt technology, is focused on network masking solutions to fully address Layer 2 and Layer 3 security and provide a secure foundation for applications at upper layers.

First Generation – MS 100 (Masking Shunt)

The MS 100 was recognized for “Top Three” performance at the Coalition Warrior Interoperability Demonstration (CWID) 2005 and was referred to as “*invaluable in mitigating potential attacks to DoD, DHS, and coalition networks*” and a “*formidable security tool.*” The MS 100 is in production, has been through functional and compatibility testing by the US Department of Defense, and is available for government purchasing.

The MS 100 is designed to operate at full wire speed, be fully compatible, easy to install, and highly resistant to attack. It has no MAC address of its own and no web interface or operating system, making it virtually invisible on the network. As a pass through device, The MS 100 is simply installed covering the firewall or other device it is masking. The protected device continues to operate as before.



Next Generation – MS 101 and MS 200 Family Product Line

The next generation MS 200 product line scales linearly in three important ways. First, it is implemented using switch fabric to cover a broader set of network applications and price points. Second, the semiconductor components scale in performance - from 100 Mbps to 10 Gbps and above. Third, the MS 200 system architecture supports higher layer functionality, including Layer 3 masking, load balancing, and loadable application modules.

The MS 101 is the entry level in this new roadmap. Based on the MS 200 architecture, it is a cost-reduced, more flexible, and higher performance replacement for the MS 100. As the flagship product, the MS 200 incorporates switch fabric with the network masking core to support four or more devices. The MS 200 also supports loadable software modules and other advanced features. Finally, in order to expand the addressable market even further, the MS 200 architecture is also designed to be integrated with 3rd party network devices.

Become a Partner

Masking Networks is looking for integration and reseller partners to expand our business in government and commercial markets. Masking Networks offers the MS 100 and MS 200 series network masking products, integration services to add network masking to 3rd party network devices, packaged and custom software, maintenance services, training, and support. Contact us at inquiries@maskingnetworks.com for more information about becoming a partner.

About Masking Networks

Masking Networks is a US corporation headquartered in Reston, Virginia. It was founded in 2006 to commercialize network masking technology to secure military networks. Our primary customer has been the U.S. Department of Defense. For more information about Masking Networks or our products, please visit www.maskingnetworks.com.