Discover and Manage Your Network Perimeter

A publication of Lumeta Corporation
www.lumeta.com

Executive Summary

If your network consists of more than a dozen routers or more than a few hundred hosts, chances are good that you do not know exactly where your network ends and other networks – such as the networks of your current and past business partners, suppliers, customers, outsourcers, divestitures and acquisitions – begin. You are not alone; most enterprises and government agencies are finding it increasingly difficult to determine and manage their ever-changing network perimeter.

A network can be thought of as an IP address space that is connected by routes between forwarding devices like routers, multi-layer switches, firewalls and multi-homed servers and desktops. The challenge is to find out how all other address spaces connect to your address space. There can be hundreds or even thousands of routes that get injected into your network though numerous devices, some of which you know about but many of which you may not. Finding all of the routes or connections presents a significant challenge to securing a network. Most network management and security organizations acknowledge that this is a problem, but they do not have a feasible way to maintain an accurate definition of the true network connectivity.

Business Trends Contributing to the Elusive Network Perimeter

Years ago, it was easier to determine the extent of a corporation's network. In the early nineties, most networks were designed, at least in theory, in accordance with a "crunchy shell-gooey center" model. In this model, the boundary of an enterprise's network was protected by firewalls at each connection point to the outside world, but little additional network access control was provided inside of the network. The network perimeter could, therefore, be defined and understood by maintaining an accurate list of the firewalls and understanding the policies implemented by the firewalls.

However, for most organizations, the "crunchy shell-gooey center" model quickly proved to be inadequate, given the types of business activities the network needed to support. Many leading analysts suggest that networks are now "boundaryless," meaning that the perimeter changes so frequently that a single layer of defensive measures at the edge of a network is no longer sufficient to protect critical business information. Because the boundaries of the networks of today's organizations need to be significantly more fluid, the network perimeter is much more elusive.

Some of the business imperatives fueling the rapid changes in network boundaries include:

- More organizations are connecting their networks with those of their business partners, including customers, suppliers and joint ventures – and companies change partners more rapidly to meet the needs of the market with agility.

- Outsourcing has dramatically increased, as companies seek ways to maintain cost competitiveness and focus on their core strengths. With outsourcing comes the “bleeding” of one network into another. If an outsourcer mis-configures the perimeter of one or more networks, outsiders suddenly have direct visibility into your network.

- Merger and acquisition activity continues to be a significant part of global business. The acquiring and acquired companies often have very different policies regarding network security and management. Nevertheless, in an attempt to demonstrate the much-sought-after synergies that motivate the acquisitions, most companies need to connect the networks rapidly, despite the lack of clarity about the acquired company’s network reach.

- Divestitures also create substantive network change. Because there is not usually a one-to-one correspondence between the organization(s) that is spunout and the parent company’s network resources, such as the address blocks used by the spinout, it is often difficult to determine whether the networks were actually disconnected as intended in accordance with the new business structure.

- Many organizations are moving from a centralized model of corporate control toward a distributed model, in which each division has more control over the business. Consequently, an increasing number of network connectivity decisions are made by people distributed across the network and around the globe. Unfortunately, in this type of environment usually no single person, organization, or system has an enterprise-wide understanding of the network.

Effects of Unknown and Undocumented Perimeters

Not knowing exactly how your network connects to other networks has serious implications for both network security and network management:

- Unknown and rapidly changing network perimeters leave the network vulnerable to attack and misuse. Both the severity and frequency of network attacks have increased dramatically in the past ten years. Even more distressing is the fact that the cost of recovering from an attack is large and growing rapidly year after year. Exposed devices are the first point of entry for attacks. Attacks are now an expected occurrence in business.
- Without clearly managing the network perimeter, companies may be wasting network resources. For instance, after a spin-off, unauthorized connections between the parent company and the spin-off often persist for years. Once these connections are disabled, the network resources, such as Wide Area Network (WAN) links, router interfaces and router capacity can be reallocated to support authorized business activities or eliminated.
- When a security breach occurs, it is difficult to prioritize response efforts without an accurate understanding of the network perimeter. If the perimeter is well documented, network managers can identify areas for remediation that will get the most critical and largest areas of the network operational quickly and will provide the best protection against re-infection.
- Without a complete set of network facts, network and security managers cannot ensure that their security policies are implemented across the network as a whole. For instance, the firewalls for a particular division may be properly configured to protect the network resources of that division. However, a firewall in a different division may allow traffic in a way that is consistent with that division's security policy, but which may cause a significant network exposure to the first division.
- Most companies do not know the most effective places to deploy security tools such as Intrusion Detection System (IDS) and Vulnerability Assessment (VA) solutions. With a clearly defined network perimeter, companies can identify key locations in the network to focus their IDS and VA products. They need to know where traffic can enter and leave the network so they can be sure to monitor those flows. Traffic capture tools such as IDS products depend on finding the attacker's traffic flows. If you miss a door into the network, you miss the attack. It is also critical to know which devices are exposed through the perimeter and monitor these devices closely, since they are most likely the first points of attack.

What Should You Do?

If your network perimeter is eluding you, here are concrete steps for effectively managing this issue:

1. Identify and clearly document and maintain a list of the routers, firewalls, and end systems that have connections to outside networks.

2. Establish a process for tracking the authorized business partners that should be connected to your network. Update this list over time.

3. Periodically send traffic to both current and former partners and each divestiture network to verify that only authorized connectivity is maintained and that unwanted connections have been eliminated as planned. Be sure to send this traffic from multiple points within the network to ensure that routes to ex-partners and divestitures have been properly disconnected throughout the entire network.

4. Send traffic to every network address block that is part of your network to identify those divisions or remote offices that may have added unauthorized connections to the Internet, customers, competitors, or past or present business partners. To increase the accuracy and completeness of the test, be sure to send this traffic from at least three points within the network.

Due to the dynamic nature of network perimeters, automate this process wherever possible. Stale information about the changing network boundary leaves your network vulnerable and means portions of the network perimeter are no longer being managed and protected in accordance with your policies.

Best Practices in Global Network Visibility

Organizations require a solution that provides the information necessary to discover, document and manage your network perimeter. It supplies a clear list of the routers and firewalls that form the network perimeter. Companies need to see who owns the routers that are the first hop beyond the perimeter so that they can quickly determine the organizations to which their network is connected.

In addition to listing the routing devices that comprise the perimeter, organizations should maintain a complete set of network facts on an ongoing basis. In other words, scan data should be examined on a periodic basis to understand the evolving states of network connectivity and defense configuration. A simple risk scorecard at each assists organizations in reporting the current state of network risk to senior management and becomes a benchmark to measure future network risk profiles.

Conclusion

Managing the network perimeter is a complex problem that companies must address to manage and secure their network effectively. Although most network security and network management teams recognize this as a critical issue, very few have a complete understanding of their network perimeter. This gap between the desired knowledge and actual knowledge about the perimeter is primarily due to a lack of tools to automate the process and the speed with which the perimeter changes.

Lumeta can discover your network perimeter, identify who owns the networks connected to your network, and automatically map the network perimeter. No other solution provides network perimeter management with the degree of comprehensiveness and accuracy of Lumeta IPsonar and Lumeta ESI.

One other important thing to remember is that discovering and managing the network perimeter is part of a bigger picture. To create a fully secure network, organizations must have a full range of network facts so in addition to understanding the true perimeter, they can:

- Make a baseline of network information
- Discover all unknown connectivity and unknown assets
- Shore up all leaks
- Handle rouge wireless devices

Lumeta's Network Situational Awareness solution addresses dangerous gaps produced in risk management processes as rapid network change causes organizational security policy and network defense configuration to become misaligned. With the implementation of a comprehensive Network Situational Awareness program, organizations can qualify risk from a network perspective, based on this comprehensive set of network facts. Using Network Situational Awareness, companies can also prioritize remediation efforts based on a complete view of connectivity and risk. This is a critical requirement for managing the network perimeter and keeping your entire network secure.