SONICWALL

5-Point Checklist to Enhance Your Defense with Network Segmentation

Rethink How to Secure and Control Access to Critical Assets

In the event of a breach, network segmentation can make the difference between major complication and complete catastrophe. An essential part of any proactive cybersecurity strategy, network segmentation works to divide the various parts of your network, reducing the attack surface of any given piece and helping to contain breaches when they do occur. With infection limited to one segment, IT security teams can respond more quickly, isolating and remediating just that piece of the network. This helps to minimize damage and disruption as well as reduce recovery time.

Network segmentation doesn't just control the movement of malware, however — it also controls access and movement of data. Within each segment, organizations can define custom access and security controls based on risk and criticality, which can safeguard sensitive data from both external actors and insider threats.

For those considering this method to provide a more secure network environment, we've created this checklist as a quick reference as you begin crafting your network segmentation strategy:

Identify and Classify Assets: Analyze and catalog the types of assets that exist within your network (such as servers, workstations and IoT devices). Then assign them to different segments based on their level of criticality and vulnerability.

Understand Communication Patterns: Determine how the various assets communicate with one another within your network, and use this information to segment your network in a way that isolates sensitive assets and limits the spread of malware.

Implement Access Controls: Restrict access to sensitive assets and segments by implementing access controls, such as firewalls and VPNs. This will help prevent unauthorized access and limit the potential impact of a security breach.

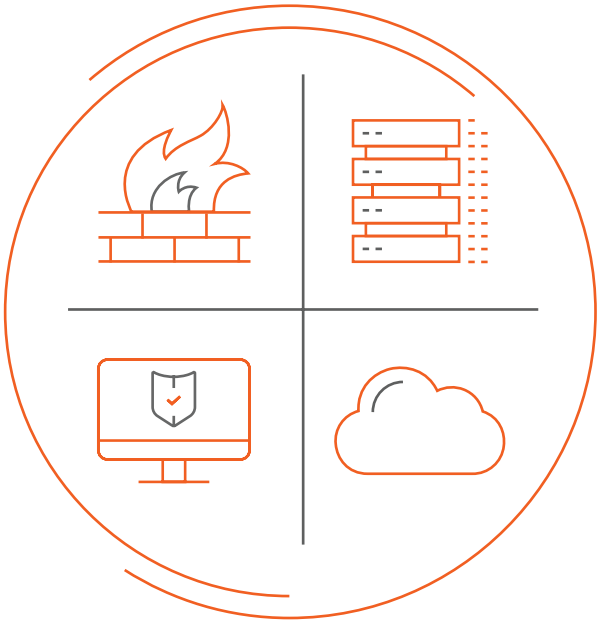
Monitor Network Activity: Implement network monitoring and logging to detect unusual or malicious activity within the network. Doing so will help identify potential security threats and allow you to respond more quickly to mitigate them

Conduct Regular Reviews: Periodically review and update your network segmentation strategy to ensure it remains effective in light of new security threats and changes to network infrastructure. This helps ensure that the network remains secure and that vulnerabilities are identified and addressed in a timely manner.

Network segmentation is a crucial part of any proactive security strategy or business continuity plan. Implementing network segmentation not only makes it more difficult for attackers to gain access to your network, it also helps ensure that access for employees, contractors and others is limited to only what's necessary. If a breach does occur, network segmentation can also speed recovery time and can greatly contain any resulting damages.

SonicWall's award-winning hardware and advanced technologies include NGFWs, Secure Mobile Access and Cloud App Security. These solutions are designed to allow any network — from small businesses to large enterprises, from the datacenter to the cloud — to segment and achieve greater protection with SonicWall.

To learn more about implementing an effective and comprehensive network segmentation strategy, contact your SonicWall representative today.



About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era and a work reality where everyone is remote, mobile and unsecure. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide. For more information, visit www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

SONICWALL®

© 2023 SonicWall Inc. ALL RIGHTS RESERVED.
SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners. The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. Except as set forth in the terms and conditions as specified in the license agreement for this product, SonicWall and/or its affiliates assume no liability whatsoever and disclaims any express, implied or statutory warranty relating to its products including, but not limited to, the implied warranty of merchantability, fitness for a particular purpose, or non- infringement. In no event shall SonicWall and/or its affiliates be liable for any direct, indirect, consequential, punitive, special or incidental damages (including, without limitation, damages for loss of profits, business interruption or loss of information) arising out of the use or inability to use this document, even if SonicWall and/or its affiliates have been advised of the possibility of such damages. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

Misc-SEG_Checklist-JK-8338