# Checklist in 5 punti per potenziare le difese con la segmentazione della rete

## Un nuovo approccio per proteggere e controllare l'accesso alle risorse critiche

Nel caso di una violazione, la segmentazione della rete può fare la differenza tra un danno grave e una catastrofe completa. La segmentazione della rete, un elemento essenziale di qualsiasi strategia di cybersecurity proattiva, consente di separare le varie parti della rete in modo da ridurre la superficie di attacco di ogni singola sezione, permettendo di contenere eventuali violazioni. Limitando l'infezione a un solo segmento, il personale addetto alla sicurezza IT può reagire più rapidamente, isolando e intervenendo solo su quella parte della rete. In questo modo è possibile ridurre al minimo i danni, le interruzioni dei servizi e i tempi di ripristino.

La segmentazione della rete non controlla solo il movimento del malware, bensì anche l'accesso e il movimento dei dati. Per ogni segmento, le aziende possono definire controlli di sicurezza e di accesso personalizzati in base a rischi e criticità, in modo da proteggere i dati sensibili sia da attacchi esterni che da minacce interne.

Per le aziende che stanno valutando questo metodo per garantire un ambiente di rete più sicuro, abbiamo creato questa checklist come riferimento iniziale per iniziare a creare una strategia di segmentazione della rete:

---

**Individuare e classificare le risorse:** analizzate e catalogate i tipi di risorse presenti nella vostra rete (ad es. server, workstation e dispositivi IoT) e assegnatele a segmenti diversi in base al loro livello di criticità e vulnerabilità.

**Comprendere i modelli di comunicazione:** stabilite in che modo le varie risorse comunicano tra loro all'interno della rete e, in base a queste informazioni, segmentate la rete in modo da isolare le risorse sensibili e limitare la diffusione del malware.

**Implementare il controllo degli accessi:** limitate l'accesso a risorse e segmenti sensibili implementando controlli di accesso, come firewall e VPN. Questo vi permetterà di prevenire accessi non autorizzati e limitare il potenziale impatto di una violazione di sicurezza.

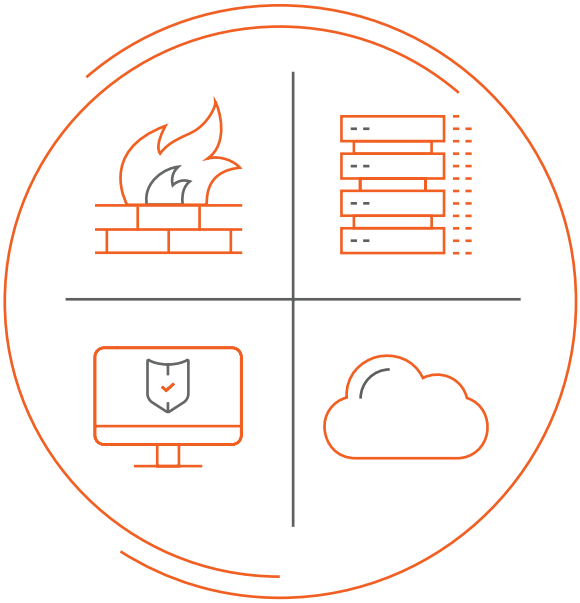
**Monitorare le attività di rete:** implementate un sistema di monitoraggio e logging della rete per rilevare attività insolite o dannose all'interno della vostra rete. In questo modo sarete in grado di identificare potenziali minacce alla sicurezza e di reagire più rapidamente per eliminarle.

**Eseguire controlli regolari:** esaminate e aggiornate periodicamente la vostra strategia di segmentazione della rete per assicurarvi che rimanga efficace nonostante la comparsa di nuove minacce ed eventuali modifiche all'infrastruttura di rete. Ciò permette di garantire che la rete sia sempre sicura e che le vulnerabilità vengano identificate e risolte in modo tempestivo.

La segmentazione della rete è un elemento cruciale di qualsiasi strategia di sicurezza proattiva o piano di continuità aziendale. Implementare la segmentazione della rete non solo rende più difficile ai cybercriminali accedere alla vostra rete, ma vi aiuta anche a garantire che dipendenti, fornitori e altri possano accedere solo alle risorse necessarie. Se si verifica una violazione, la segmentazione della rete può anche velocizzare i tempi di ripristino e contenere notevolmente eventuali danni.

L'hardware pluripremiato e le tecnologie avanzate di SonicWall includono firewall di nuova generazione (NGFW), Secure Mobile Access e Cloud App Security. Queste soluzioni sono progettate per consentire la segmentazione di qualsiasi rete – dalle piccole imprese alle grandi aziende fino ai data center e al cloud – e ottenere una maggiore protezione con SonicWall.

Per maggiori informazioni su come implementare una strategia di segmentazione della rete efficace e completa, contattate subito il vostro rappresentante SonicWall.



## SonicWall

SonicWall fornisce soluzioni di cybersecurity innovative per la nuova normalità iperdistribuita, in una realtà lavorativa in cui tutto è all'insegna del telelavoro, della mobilità e in cui la sicurezza dei dati rappresenta un elemento fondamentale. Con la sua capacità di individuare le minacce più elusive e offrendo una visibilità in tempo reale, SonicWall rende possibili economie innovative e colma le lacune della cybersecurity per aziende, enti pubblici e PMI in ogni parte del mondo. Per maggiori informazioni visitare www.sonicwall.com.

**SonicWall, Inc.**
1033 McCarthy Boulevard | Milpitas, CA 95035
Per maggiori informazioni consultare il nostro sito web.
**www.sonicwall.com**

SONICWALL®



Misc-SEG_Checklist-A4-JK-8338