MACMON VLAN MANAGER

Mehr Schutz durch Netzwerksegmentierung: statische und dynamische VLANs

VLANs (Virtual Local Area Networks) bieten die Möglichkeit, das Netzwerk unabhängig von der physischen Struktur zu segmentieren. Eine Netzwerkunterteilung verringert die Broadcast-Last in den einzelnen Segmenten und unterstützt auch Sicherheitskonzepte, indem sie die verschiedenen Bereiche voneinander abschottet. Egal ob MAC- oder 802.1X-basiert, kommen so erhebliche Vorteile zum Tragen.

Arbeitsgruppen und Zuordnung

Über VLANs gebildete Arbeitsgruppen können so unabhängig von ihrer örtlichen Verteilung uneingeschränkt kommunizieren, als ob sie zum selben LAN gehören. Sensible Ressourcen können auf diesem Wege vor dem allgemeinen Zugriff geschützt werden.

VLANs lassen sich entweder statisch, das heißt durch feste Zuordnung der einzelnen Switchports zu bestimmten VLANs oder dynamisch bilden. Die dynamische Zuordnung kann auf der Basis der MAC-Adresse (Layer-2-VLAN) oder auf Basis einer höheren Protokollschicht, wie auch über 802.1X erfolgen.

Key facts

- ✓ Schneller und kontrollierter Netzwerkzugang für Gäste und deren mobile Geräte wie Laptop, iPhone oder Android ins LAN und WLAN.
- ✓ Gewährleistung der Sicherheit der IT-Infrastruktur und die Übersicht und Nachvollziehbarkeit von Netzwerkzugängen.
- ✓ Unterstützung der VLAN-Konzepte auf Layer 2- und auf 802.1X-Basis sowie in Mischumgebungen.
- ✓ Plug & Play Betrieb durch das einzigartige automatische Regelwerk.
- ✓ Rasend schnelle Reaktion durch die vollständig neu entwickelte macmon Horizon Engine.

Besucher oder Quarantäne-VLAN

Nicht vertrauenswürdige Geräte können von macmon, sobald sie im Netzwerk erscheinen, in ein Besucher- oder Quarantäne-VLAN geschaltet werden. Hierbei kann es sich um mobile Arbeitsplätze von reisenden Mitarbeitern, um Systeme von Dienstleistern oder fremde Geräte von Besuchern handeln. macmon kann anhand der Gruppenzugehörigkeit oder aufgrund eines Einzelvermerks das Gerät als weniger vertrauenswürdig einstufen und dann reagieren.

Wenn das Gerät vom Netz genommen wird, wird der Switchport von macmon wieder seinem ursprünglichen VLAN zugeordnet. Aufgrund des flexibel zu gestaltenden Regelwerks kann dies auf bestimmte Switches, Netzwerksegmente oder Bereiche eingeschränkt werden während für die meisten Fälle das automatische Regelwerk breits alle Anforderungen erfüllt und umsetzt.

Sollen beispielsweise Geräte vom Typ „Besucher" nur in ausgewiesenen Räumlichkeiten in einem „Besucher-VLAN" erlaubt, in anderen Bereichen aber gänzlich verboten sein, so lässt sich diese Forderung mit dem macmon VLAN Manager flexibel und einfach umsetzen. Auch Geräte, die lange nicht im Netz gesehen wurden oder nach einem „Compliance-Check" als unsicher eingestuft werden, können bis zur Klärung des Status in einem Quarantäne-Netz gehalten werden. Hier haben diese zwar den Zugriff auf die aktuellen Sicherheits-Patches und den aktuellen Virenscanner, können aber andere Dienste nicht sehen und damit keinen Schaden anrichten.

Die VLAN-Management-Technologie kommt auch in der Kopplung mit anderen Herstellern bzw. Sicherheitsprodukten zum Einsatz. Nutzt ein Technologiepartner, wie EgoSecure macmon, um Systeme ereignisgesteuert in Quarantäne zu verschieben, so erfolgt dies in der Regel durch einen Befehl an macmon mit dem Inhalt, das betroffene System in ein anderes VLAN umzuschalten. Auch der macmon eigene Antivirus Connector isoliert auf diese Weise infektiöse Systeme.

Dynamische VLANs auf MAC-Layer Schicht (Layer-2-VLANs)

Bei den dynamischen Layer-2-VLANs erfolgt eine Zuordnung zu einem Netzsegment über das Endgerät, wobei das Gerät anhand der MAC-Adresse identifiziert wird. Der Vorteil eines solchen Konzeptes ist, dass der Anwender, egal wo ein Gerät betrieben wird, immer nur Zugang zu dem Netzwerkbereich hat, den er für seine Arbeit benötigt. Auch nach einem Umzug oder bei der Nutzung mobiler Arbeitsmittel landet der Benutzer im richtigen Segment und es ist keine Nachkonfiguration im Bereich des Netzes nötig. Die gleiche Funktionalität ist auch beim Einsatz von 802.1X-basierten Authentifizierungen möglich.

Die Einführung eines solchen Konzeptes ist mit dem macmon VLAN Manager einfach, indem Sie über eine WEB-GUI jedem Gerät ein VLAN zuordnen. Wenn Sie die VLAN-Zuordnung über die macmon-Gruppen steuern, verringert sich der Betriebsaufwand nochmal erheblich.

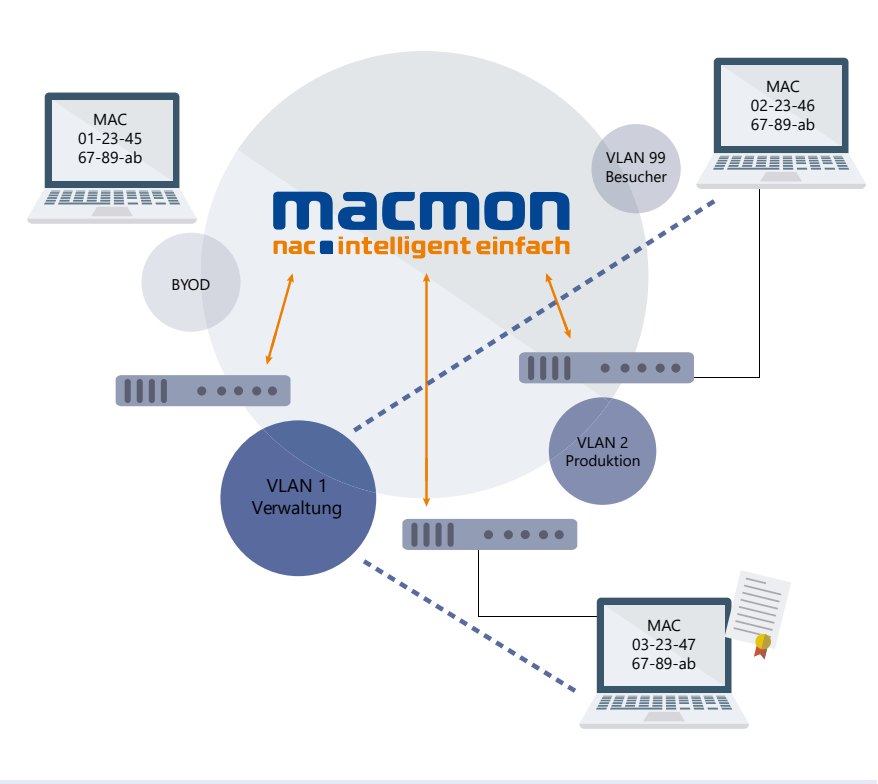
macmon überwacht laufend, ob die Switchports, an denen die Geräte betrieben werden, sich im richtigen Netzwerk befinden. Falls hier eine Veränderung stattgefunden hat, die Einfluss auf die Autorisierung hat wird der entsprechende Switchport automatisch umkonfiguriert.

Schutz aller ungenutzten Switchports vor Missbrauch

Sie wollen sicherstellen, dass nicht zugelassene Geräte auch nicht im Netzwerk lauschen können? Das können Sie mit macmon erreichen. macmon sorgt dafür, dass alle Switchports, an denen kein Gerät aktiv betrieben wird, einem VLAN zugeordnet wird, in dem keine Dienste angeboten werden. Wird nun ein Gerät angeschlossen, wird es von macmon erkannt sobald es ein Datenpaket sendet. Es wird je nach Wunsch und Status dem zugewiesenen Netzwerk, dem Gäste-VLAN oder, wenn es lange nicht mehr im Netz gesehen wurde, einem Remediation-VLAN zugeordnet.

Geräte, die ans Netz angeschlossen werden und die keine Daten austauschen, bleiben so lange im „No-Go-Netz", bis sie sich melden. So können auch „Lauschangriffe" verhindert werden.

Der macmon VLAN Manager ist Bestandteil des Network Bundles. Er umfasst die VLAN-Verwaltungsmodule, die Switch spezifischen Steuermodule und die Erstellung lösungseigener Skripte. Der macmon VLAN Manager unterstützt bereits eine Reihe von Switch-Typen. Da die VLAN-Steuerung sich herstellerabhängig unterscheidet, kann eine Anpassung der VLAN-Steuermodule an die von Ihnen eingesetzten Switches nötig sein – wozu dann der temporäre Zugang zu einem solchen Switch erforderlich ist.



Kontakt

macmon secure GmbH
Alte Jakobstraße 79-80 | 10179 Berlin
Tel.: +49 30 2325777-0 | nac@macmon.eu | www.macmon.eu