

SICHERUNG VON NETZWERKEN MIT VLAN-TAGGING IN MANAGED SWITCHES

HIGHLIGHTS

- ✓ Viele Unternehmen führen VLANs ein, um die Sicherheit ihrer Netzwerkinfrastruktur zu erhöhen. Dies erfordert jedoch fortschrittliche Netzwerk-Switches, die eine granulare Kontrolle bis hin zu den Endgeräten ermöglichen.
- ✓ Managed Switches sind die ideale Lösung für diese Herausforderungen. Mit ihnen können Netzwerkadministratoren mehrere VLANs einrichten, um Unternehmensabteilungen effektiv voneinander zu trennen und gleichzeitig eine optimale Erreichbarkeit für jedes Endgerät zu gewährleisten.
- ✓ Zusätzlich zum VLAN-Tagging bieten Managed Switches wie der TSW202 und der TSW212 QoS- und Scheduling-Funktionen, die eine priorisierte Verwaltung des Datenflusses von mehreren Endpunkten ermöglichen und Aufgaben wie das regelmäßige Herunterfahren von Ports automatisieren, um das Netzwerkmanagement weiter zu verbessern.

DIE HERAUSFORDERUNG - WEIT MEHR ALS NUR KONNEKTIVITÄT UNTERSTÜTZEN

Der Aufbau einer neuen Netzwerkinfrastruktur erfordert in jedem Unternehmen, unabhängig von seiner Größe, die Maximierung der Effizienz und Sicherheit jeder einzelnen Abteilung. Dies ist von entscheidender Bedeutung, da niemand seine wertvollen Daten in die Hände von Hackern geben möchte, die mit jedem Datenleck einen durchschnittlichen Schaden von [weltweit durchschnittlich 4,45 Millionen Dollar](#) verursachen.

Angesichts des unvermeidlichen Austauschs sensibler Daten zwischen verschiedenen Abteilungen ist die Gewährleistung der Datensicherheit in Ihrem Unternehmen ebenfalls von entscheidender Bedeutung. Dazu muss sichergestellt werden, dass der Datentransfer und Datenzugriff streng kontrolliert und sicher sind, manchmal sogar vor den Augen anderer Abteilungen des Unternehmens.

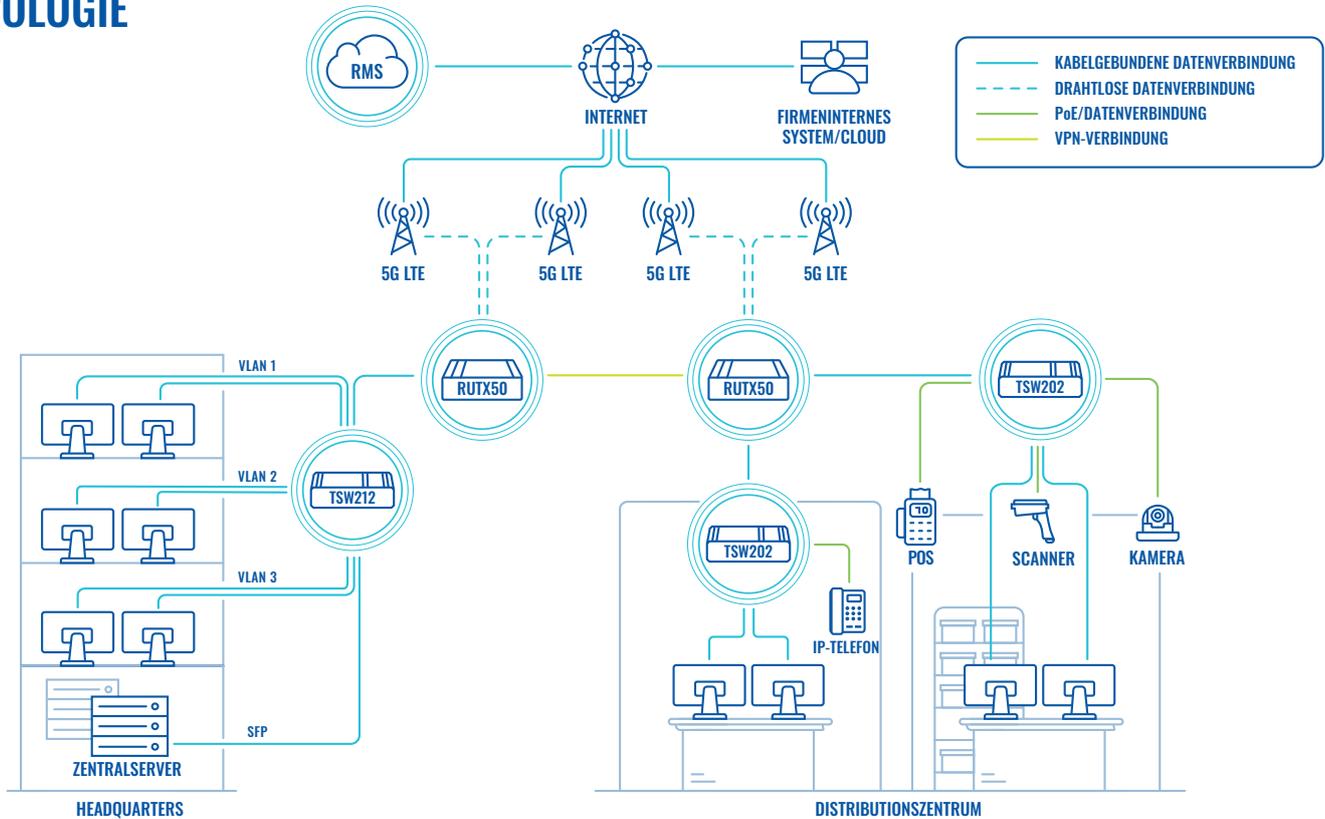
Um diesen Herausforderungen zu begegnen, entscheiden sich viele für die Einrichtung separater [virtueller lokaler Netzwerke](#) (VLANs) für jede Abteilung, was relativ kostengünstig und einfach zu implementieren ist. VLANs in Netzwerken isolieren Abteilungen wirksam voneinander und verhindern, dass sie auf Daten zugreifen, die nicht für sie bestimmt sind.

VLAN kann auch eine zusätzliche Sicherheitsebene gegen Bedrohungen von außen bieten: Wenn beispielsweise in einer Abteilung ein Datenleck auftritt, sind andere Abteilungen, die zu anderen VLANs gehören, nicht betroffen.

Größere Unternehmen, die Produkte vertreiben und über mehrere Distributionszentren in verschiedenen Städten oder Ländern verfügen, stehen jedoch vor einer zusätzlichen Herausforderung, da die Übertragung von Daten von diesen Standorten an die Zentrale eine weitere Ebene von Sicherheitsbedenken aufwirft.

Angesichts der Bedeutung der Verwaltung von Daten von mehreren Endpunkten wird deutlich, dass Komponenten wie Netzwerk-Switches für den Aufbau einer komplexen Netzwerkinfrastruktur unerlässlich sind. Sie haben die Aufgabe, die zentrale Verwaltung des Datenflusses zu erleichtern und sicherzustellen, dass nur autorisiertes Personal wie Systemadministratoren sicher auf die Daten zugreifen können.

TOPOLOGIE



DIE LÖSUNG - MANAGED SWITCHES FÜR MAXIMALE KONTROLLE

Managed Switches wie der TSW202 und der TSW212 von Teltonika Networks sind die ideale Lösung für derartige Herausforderungen. Sie bieten eine robuste Netzwerkkonnektivität über verschiedene Abteilungen hinweg und ermöglichen eine granulare Kontrolle über die gesamte Netzwerkinfrastruktur bis hin zu den Endgeräten.

Der TSW212 Managed Switch mit 8 Ports, der über ein Ethernet-Kabel mit unserem RUTX50 5G-Router verbunden ist, erweitert die Konnektivität über SFP-Ports zum Server in der Zentrale. Darüber hinaus verbindet er mehrere Computer in verschiedenen Abteilungen über Gigabit-Ethernet-Ports, um eine Datenübertragung mit hohem Durchsatz an allen Endpunkten zu ermöglichen.

Das Potenzial für anspruchsvollere Konfigurationen kann durch eine hervorragende Konnektivität ausgeschöpft werden. Der TSW212 Managed Switch unterstützt VLAN-Tagging-Konfigurationen, so dass jede Abteilung in separaten VLANs arbeiten kann.

Diese Funktion ermöglicht ein effizientes Datenverkehrsmanagement, als ob die Abteilungen in getrennten Netzwerken arbeiten würden. Netzwerkadministratoren können so die gesamte Netzwerkinfrastruktur und den Datenverkehr aller Abteilungen zentral verwalten und überwachen.

Darüber hinaus unterstützt der TSW212 Managed Switch Quality of Service (QoS), mit dem bestimmte Arten von Datenverkehr priorisiert werden können. Beispielsweise können Vertriebsdaten gegenüber Buchhaltungsdaten priorisiert werden, um sicherzustellen, dass bei einer Überlastung der Netzwerkinfrastruktur die Daten der Vertriebsabteilung zuerst die entsprechenden Endpunkte erreichen.

Mit Funktionen wie QoS und VLAN-Tagging kann ein sicheres Netzwerk und eine nahtlose Datenübertragung für maximale Effizienz gewährleistet werden.

Die gleiche Netzwerkpriorisierung kann mit dem TSW202 Managed Switch auch in entfernten Distributionszentren angewendet werden, so dass POS-Terminals eine höhere Priorität als datenintensive Kamera-Feeds erhalten, um jederzeit die größtmögliche Genauigkeit der Bestandsdaten zu gewährleisten.

Und da der TSW202 ein [PoE+](#)-Switch ist, kann er mit POS-Systemen, Kameras, Scannern und IP-Telefonen verbunden werden, um diese Endgeräte mit Netzwerkkonnektivität und Strom zu versorgen.

Managed Switches zeichnen sich in diesem Szenario auch durch Funktionen wie der Zeitsteuerung aus, mit der Endgeräte automatisch ein- und ausgeschaltet werden können und die Priorisierung nur für bestimmte Zeiträume aktiviert werden kann. Da sie mit [RMS](#)-kompatibel sind, können Sie das RMS-Management und sein Multikonfigurationstool verwenden, um diese Verfahren für alle Geräte in einer einzigen Sitzung remote durchzuführen.

Da sowohl die Zentrale als auch die Distributionszentren miteinander kommunizieren müssen, um Bestände, Zahlungsinformationen etc. abzurufen, muss dies über eine sichere Remote-Verbindung erfolgen. Aus diesem Grund wird eine VPN-fähige Verbindung benötigt. Ein VPN ermöglicht es den Administratoren, die Zentrale zu erreichen und Daten sicher abzurufen.

Managed Switches wie der TSW202 und der TSW212 sind in komplexen Netzwerkinfrastrukturen besonders wertvoll, da sie mehrere Protokolle unterstützen. Sie sind mit den Protokollen STP und RSTP kompatibel, die Netzwerkschleifen und Broadcast-Störungen verhindern und eine schnelle Wiederherstellung nach Änderungen der Netzwerktopologie ermöglichen, was für die Aufrechterhaltung der Netzwerkverfügbarkeit von entscheidender Bedeutung ist.

