LANCOM Systems und ARP-Guard kooperieren im Bereich Network Access Control (NAC)

Die LANCOM Systems GmbH ist ein europäischer Anbieter moderner Netzwerkinfrastrukturkomponenten (WAN, LAN, WLAN, Firewalls), virtueller Netzwerkkomponenten sowie eines Cloud-basierten Systems zur zentralen Steuerung des gesamten Netzwerkportfolios. Mit dem Produktportfolio von LANCOM können verschiedene Netzwerkszenarien abgebildet werden. Kunden sind vor allem Wirtschaftsunternehmen unterschiedlichster Größenordnung sowie Verwaltungen, Universitäten und Schulen.

Zur Abrundung des Angebots im Bereich der Verhinderung unberechtigter Zugriffe auf das Netzwerk arbeitet LANCOM mit dem NAC-Anbieter ISL Internet Sicherheitslösungen GmbH und dessen Produkt ARP-Guard zusammen, die seit 1999 herstellerunabhängige Lösungen für den Schutz vor unberechtigtem Zugriff auf heterogene Netzwerke anbietet.

Ein schlagkräftiges Duo

Der Vorteil der Zusammenarbeit besteht darin, dass die Lösungen beider Anbieter sehr gut aufeinander abgestimmt sind. Alle ISL ARP-Guard NAC-Funktionen arbeiten perfekt mit LANCOM Netzwerkkomponenten und ihren integrierten Sicherheitsfunktionen zusammen. Für die Kunden garantiert das ein hohes Maß an Sicherheit. Durch die Kooperation der beiden deutschen Hersteller wird Network Access Control (NAC) zum integrierten Bestandteil der LANCOM Netzwerklösungen.

Wie arbeitet ARP-Guard NAC?

ARP-Guard NAC scannt zunächst alle Switches und die angeschlossenen Endgeräte und bietet anschließend eine vollständige Übersicht über die im Netzwerk befindlichen Geräte und wo diese sich befinden. Das stellt sicher, dass keine dem Netzwerkmanagement fremden Geräte das (W)LAN nutzen, sondern nur berechtigte Geräte. Sobald sich unbekannte Geräte im Netzwerk anmelden, findet eine sofortige Alarmierung statt und Gegenmaßnahmen können automatisch eingeleitet werden. Für die Kontrolle der Zugänge setzt ARP-Guard einen reaktiven Ansatz per SNMP oder einen proaktiven Ansatz über IEEE 802.1X (RADIUS) ein.

Beachten Sie, dass NAC-SNMP nicht zusammen mit der LANCOM Management Cloud betrieben werden darf. Hierbei würden die beiden Management-Systeme sich gegenseitig behindern und die jeweils zuletzt geschriebene Konfiguration verwendet werden. Verwenden Sie daher diese Methode nur zusammen mit Standalone-Switches.

Wir empfehlen daher die Verwendung von NAC über RADIUS, da dieses sowohl mit Standalone-Switches als auch mit der LANCOM Management Cloud betrieben werden kann. Zusätzlich verwendet es dabei deutlich hochwertigere Authentifizierungsmethoden und bietet einige Vorteile gegenüber NAC-SNMP.

Unterschiede zwischen NAC-SNMP und NAC über RADIUS

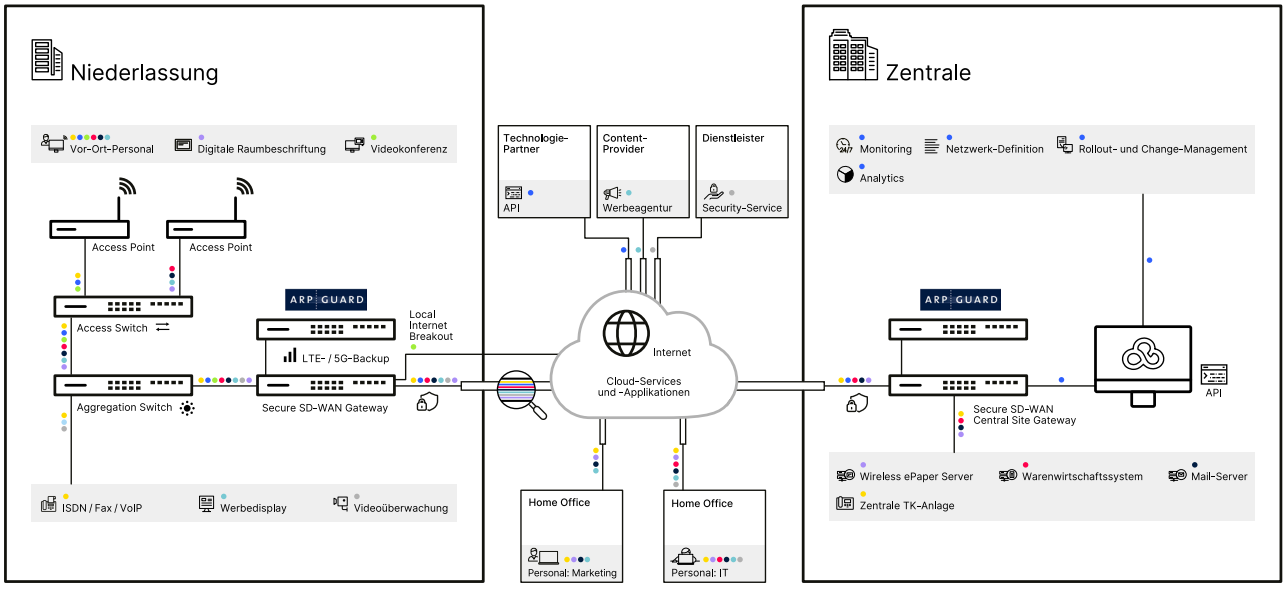
Bei NAC-SNMP werden die MAC-Adressen am Switch-Port gelernt, wobei dem jeweiligen Switch-Port genau ein VLAN zugewiesen werden kann. Wenn an diesem Port ein weiterer unmanaged Desktop-Switch mit mehreren Teilnehmern angeschlossen wird, läuft ein Fingerprinting ab, welches weitere Parameter wie Portfreigaben und SSH-Keys scannt und dann das VLAN mit Berechtigungen setzt. Bei nicht eindeutigen Ergebnissen des Fingerprintings kann in diesem Fall keine gute Entscheidung für die dedizierten Berechtigungen und damit das Ziel-VLAN erreicht werden.

Bei NAC über RADIUS ist es neben einer Authentifizierung per EAP-Methode über den Benutzernamen mit Passwort oder einem Zertifikat, auch möglich die MAC-Adresse als solche zum Kriterium zu machen (MAC-Fallback / MAC Authentication Bypass). Zusätzlich kann nicht nur auf Port-Ebene sondern auch auf Session-Ebene eine VLAN-Zuweisung passieren, sodass auch mehr als ein Endgerät mit individueller VLAN-Schaltung pro Port angeschlossen werden kann.

Damit die RADIUS-Schaltung am Port nicht durch die von der LANCOM Management Cloud geschriebene Konfiguration gestört wird, sollten Sie in der LANCOM Management Cloud grundsätzlich alle VLANs an den Ports erlauben. Per RADIUS wird dann geregelt, welches VLAN jeweils genutzt wird.

Zusätzlich erlauben oder unterbinden einheitliche und automatisch anwendbare Sicherheitsregeln den Zugriff auf die Unternehmensnetzwerkinfrastruktur. Dies ist in Zeiten steigender Benutzer-Geräte-Zahlen wie insbesondere auch einer wachsenden Anzahl an cyber-physischen Geräten wie IoT- (Internet of Things) und OT-Geräten (Operational Technology) besonders wichtig. Alle Geräte im Netzwerk werden ständig auf Richtlinienkonformität geprüft. Weicht ein Gerät von einer zuvor definierten Richtlinie ab, z. B. wenn der Virenscanner nicht aktuell oder die Firmware eines Clients nicht auf dem neuesten Stand ist, kann der Client in Quarantäne genommen werden. Erst wenn die Updates installiert und der Gerätestatus den definierten Richtlinien entspricht, wird dem Client der Zugang wieder gewährt.

Abbildung 1:
NAC mit ARP-Guard



Durch diesen zweifachen Schutzmechanismus ist sichergestellt, dass innerhalb des Netzwerkes nur bekannte Endgeräte zum Einsatz kommen und dass diese alle Anforderungen der Sicherheitsrichtlinie erfüllen. Das verhindert das Eindringen unberechtigter Geräte ins Netzwerk, indem diese die Einfallstore des WLAN oder einer freien Netzwerkdose nutzen. Zusätzlich wird die menschliche Sicherheitslücke in Form der Mitarbeiter geschlossen, die aus Unachtsamkeit oder gar vorsätzlich die Sicherheitsrichtlinien für Geräte im Netzwerk nicht beachten.

Zeitgemäßes Client-Management und BYOD durch den Einsatz von NAC

Die Kombination der LANCOM Infrastruktur mit der ARP-Guard NAC-Lösung bietet zudem überall dort exzellente Anwendungsmöglichkeiten, wo Nutzern ein BYOD (bring your own device)-Angebot gemacht wird – beispielsweise im Falle separierter Netzwerke für Schüler und Lehrer in Schulen. Nutzer können somit ihre Smartphones oder Tablets in das WLAN der Organisation (z. B. der Schule) einloggen, und ARP-Guard Network Access Control schafft anschließend eine Übersicht, welche Geräte sich im Netzwerk befinden. Die Netzwerkzugriffe der „fremden Geräte“ können somit von den organisationsinternen Netzwerkbereichen, z. B. der Verwaltung und den darin berechtigten Geräten wie beispielsweise PCs, Drucker oder Laptops, separiert werden. Jeder unbefugte Versuch eines Zugriffs wird sofort identifiziert, effizient überwacht und ggf. unterbunden. Geräte von organisationsfremden Personen können stattdessen auf einen separaten Gästebereich zugreifen. Der Zugriff auf die geschäftskritischen Netzwerksegmente bleibt somit den Mitarbeitergeräten vorbehalten. Privaten Geräten von Mitarbeitern oder Schülern (BYOD) können unter bestimmten Umständen (Richtlinienerfüllung) Zugangsberechtigungen auf bestimmte interne Bereiche gewährt werden.

Netzwerkdosen als Einfallstore von Netzwerken

Ebenfalls sind frei zugängliche Netzwerkdosen in Firmen- oder Klinikgebäuden eine Achillesferse eines Netzwerkes. Wichtig ist dabei, dass alle Netzwerkdosen mit LANCOM Access-Switch-Ports gepatcht sind. Mit der LANCOM Management Cloud (LMC) und SD-LAN können die gewünschten Netze und VLANs bequem auf definierte Ports aller Switches an allen verwalteten Standorten global ausgerollt werden. Eine lokale Konfiguration auf dem jeweiligen Switch ist selbstverständlich genauso möglich. Der Cloud-Ansatz ist dabei beim NAC über SNMP nur für die initiale Konfiguration empfehlenswert, da die Kommunikation mit den Switches genauso wie ARP-Guard über SNMP-Abfragen stattfindet und sich so beide Systeme gegenseitig stören. Bei Nutzung von NAC über RADIUS sollten in der LMC grundsätzlich alle VLANs an den Port erlaubt sein. Nach dieser angesprochenen Basiskonfiguration können über die ARP-Guard NAC-Lösung individuelle Anpassungen für einzelne Nutzer, Geräte oder Projekte vorgenommen werden: Wird ein fremdes Gerät im Netzwerk erkannt, erteilt das NAC-System dem jeweiligen Switch einen Befehl zur Umkonfiguration des Netzwerk-Ports.

Wird also ein unbekanntes Gerät angeschlossen und erkannt, wird der Netzwerk-Port abgeschaltet und das Gerät verliert sofort die Netzwerkverbindung.

Flexible Gestaltung von Arbeitsplätzen und Zugangsberechtigungen

NAC bietet zudem die Möglichkeit, Netzwerk-Ports nicht wie zuvor beschrieben zu sperren, sondern umzuleiten: Meldet sich ein fremder Client im Netzwerk an, erfolgt dann keine vollständige Trennung vom Netzwerk. Stattdessen kann er zur Anmeldeseite des Gästebereichs umgeleitet werden, wo er sich registrieren kann, um Zugriff auf das Internet zu erhalten. Diese Funktion kann neben dem Sicherheitsaspekt auch für eine komfortable Steuerung der VLANs für Mitarbeitergeräte eingesetzt werden. In diesem Fall kennt ARP-Guard das zum Endgerät (und zum Port) gehörende VLAN und stellt dem Mitarbeiter automatisch alle von ihm benötigten Ressourcen zur Verfügung, egal an welchem Ort er sein Endgerät anschließt. Gerade in Unternehmen, die keine feste Zuordnung von Büros und Arbeitsplätzen mehr kennen, ist dies ein exzellenter Mehrwert.

Sprechen Sie uns gerne an und heben Sie Ihre Netzwerksicherheit auf die nächste Stufe! Kontaktieren Sie hierzu gerne den LANCOM Vertriebs-Innendienst Deutschland.

Telefon: +49 (0)2405 49936 333

LANCOM Systems GmbH
A Rohde & Schwarz Company
Adenauerstr. 20/B2
52146 Würselen | Deutschland
info@lancom.de | lancom-systems.de