

Aus der Reihe

OctoGate in der Praxis

Der Einsatz einer WLAN-Lösung

SecurITy

Trust Seal
www.teletrust.de/itsmig

made
in
Germany

Inhaltsverzeichnis

OctoGate Schulfirewall	Seite 4
Firewall und WLAN in der Schule	Seite 5
Warum Firewall und WLAN?	Seite 6
Gäste-Netz	Seite 8
Virtuelle Access Points	Seite 9
Datenschutz und Netztrennung	Seite 10
Infrastruktur	Seite 12
Firmware-Updates	Seite 13
WLAN-Managementfunktionen	Seite 14
Steuerung des WLAN-Zugangs durch den Lehrer	Seite 16
Anbindung von Schul-Außenstellen	Seite 17
Service	Seite 18



Die OctoGate Schulfirewall

WLAN mit OctoGate ist

- ... einfach und robust.
- ... maßgeschneidert für Schulen.
- ... preislich attraktiv.
- ... gesetzeskonform.
- ... Jugendschutz.
- ... kinderleicht zu installieren.

Die OctoGate Schulfirewall ist ein eigenständiges Produkt zum aktiven Schutz des Schulbetriebes vor schadhaften Inhalten aus dem Internet. Die OctoGate Schulfirewall beinhaltet einen Email-Server, eine Plattform zum Team-Dokumentenaustausch, einen Virens Scanner und vieles mehr.

Durch eine bereits große Anzahl an Installationen in Deutschlands Schulen und Schnittstellen zu Klassenraum-Managementsystemen wie paedML, snv und INiS haben wir einen hohen Bekanntheitsgrad erlangt.

Weiteres Leistungsmerkmal unserer OctoGate Schulfirewall ist die Bereitstellung von WLAN-Funktionalitäten, die genau auf die Bedürfnisse einer Schule abgestimmt sind. Wir liefern auch die WLAN-Hardware. Die dazugehörige Management-Lösung ist bereits in unserer OctoGate Schulfirewall enthalten.

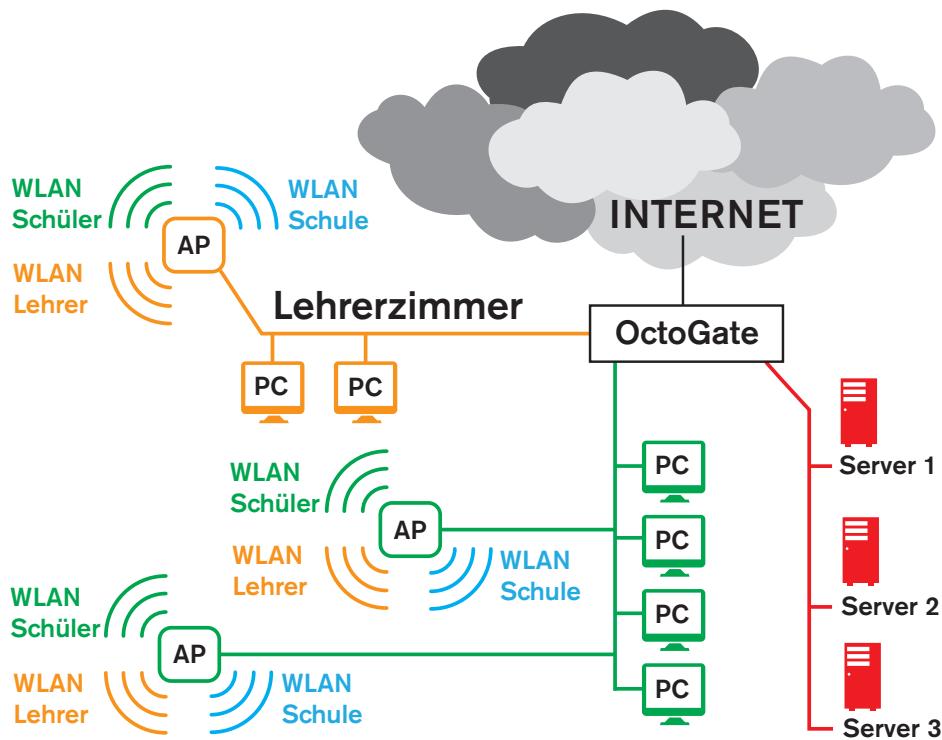
In unserer Reihe „OctoGate in der Praxis“ beleuchten wir die Vorteile, Einsatzszenarien und praktischen Hintergründe unserer Produkte in verschiedenen Bereichen.

Der Einsatz einer WLAN-Lösung in einer Schule ist vielfältig und beinhaltet nicht nur die Bereitstellung der Funk-Infrastruktur. Alle WLAN-Geräte müssen auch verwaltet und gesichert werden. Die dazugehörige Firewall sollte den Internetverkehr von Viren und Erwachsenen-Inhalten säubern und dafür sorgen, dass einzelne Geräte die Internet-Verfügbarkeit der anderen nicht stören.

Der Schulbetrieb muss durchgängig gesichert sein. Unsere langjährige Erfahrung im Schulsektor zahlt sich auch beim Service für Sie aus. Unser Supportteam ist schnell und kompetent für Sie da. Selbstverständlich erhalten Sie bei Bedarf einen Geräte-Vorabaustausch.



Firewall und WLAN in der Schule



Die Abbildung zeigt das Beispiel einer Schule mit installierter OctoGate Schulfirewall. Die abgebildete Lösung beinhaltet ein Schülernetz mit mehreren PCs und zwei WLAN Access Points (grün) sowie ein Netz für das Lehrerzimmer mit einem WLAN Access Point (orange). Zusätzlich existiert ein weiteres separates Netz für die Server der Schule (rot). Die OctoGate Schulfirewall sitzt zentral zwischen physikalisch getrennten Netzen und kontrolliert sämtlichen Datenverkehr, welcher zwischen den Netzen fließt. Vor allem die Daten aus dem Internet werden sorgfältig gefiltert – Spam, Viren, Trojaner oder Erwachsenen-Inhalte. Selbstverständlich ermöglichen wir Lehrern auch einen sicheren Zugriff von zu Hause aus auf Inhalte der Schule über das Internet. Dieses geschieht durch VPN (Virtuelles Privates Netzwerk) und andere Technologien. Alle WLAN Access Points werden zentral von der OctoGate Schulfirewall gesteuert, konfiguriert und überwacht. Mit OctoGate erhalten Sie ein Rundum-sorglos-Paket für die ganze Schule!

OctoGate Schulfirewall

- unterstützt mehrere Netzwerke: Server, Schüler, Lehrer.
- filtert Viren, Trojaner, Spam und Erwachsenen-Inhalte.
- bietet sicheren Zugriff von außen via VPN.
- verfügt über eine zentrale Steuerung der WLAN Access Points.
- bietet eine kinderleichte Installation des WLANs.

Warum Firewall und WLAN?

Steht eine Schule vor der Aufgabe der Installation einer WLAN-Lösung, wird meistens nur die Komponente Funk-Infrastruktur betrachtet und das Augenmerk auf das Ausleuchtungsgutachten und die Gebäude-Infrastruktur (Strom- und Netzwerkleitungen) gerichtet. Außerdem wird das Thema einer eigenen Kabel-Infrastruktur für die WLAN Access Points und eines VLAN-Konzeptes (Virtuelle Netzwerke auf demselben Kabel mit speziellen Hardware-Switches) fokussiert. Die Notwendigkeit einer Firewall wird dabei oft nicht gesehen.

Dazu folgendes Beispiel: Eine Schule mit 1.200 Schülern setzt ein WLAN-Gäste-Netz ein. Einige Wochen nach der Installation meldet sich die Schulleitung beim OctoGate Support mit der Meldung: „Internet-Komplettstörung“. Des Rätsels Lösung: Fünf Android Geräte verschiedener Schüler hatten sich einen Virus außerhalb der OctoGate-Umgebung eingefangen. Dieser Virus versuchte nun je Gerät 200 Mal pro Sekunde seine Server im Internet zu erreichen. Das war zu viel für die Außenanbindung. Da die Schule nicht nur WLAN, sondern auch eine OctoGate Schulfirewall einsetzt, war es einfach, das Problem zu beheben und die betroffenen Server im Internet sowie die WLAN-Geräte zu sperren.

Fazit: Neben der Betrachtung der Funk-, Gebäude- und Kabel-Infrastruktur für ein gut funktionierendes WLAN ist auch die Absicherung über eine zentrale Firewall zwingend notwendig.

Unsere OctoGate Schulfirewall bietet allen Schulen ein Rundum-sorglos-Paket:

- Verwendung von PoE-Technologie zur Stromversorgung der WLAN Access Points über das Netzkabel. Es sind keine Elektrikerarbeiten notwendig.
- automatische Kalibrierung der WLAN Access Points, Lastverteilung zwischen den Geräten und zeitgesteuerte Reduzierung der Sendeleistung: In der Regel entfällt somit das Ausleuchtungsgutachten.
- sichere Verbindung zwischen WLAN Access Point und Firewall. Automatisch und ohne Konfigurationsaufwand. Somit kein VLAN-Konzept oder physikalisch eigenständiges Netzwerk für WLAN Access Points notwendig.
- OctoGate Schulfirewall zusammen mit den OctoGate WLAN Access Points: Kinderleichte Installation. Einstecken – geht.

OctoGate Schulfirewall

- einfach zu installierende Lösung, keine Zusatzadministration.
- kein schulweites WLAN ohne Firewall.
- mit PoE ist die Nachrüstung von WLAN einfach.



Gäste-Netz

Die OctoGate Schulfirewall kann sogenannte Gäste-Netze zur Verfügung stellen, sowohl im WLAN als auch im kabelgebundenen Netz. Wie beim WLAN-Zugang im Hotel wird ein einmaliger Voucher Code benötigt. Dieser kann beispielsweise im Sekretariat oder über den Klassenlehrer an die Schüler ausgegeben werden. Anders als im Hotel kann so ein Code durchaus mehrere Jahre seine Gültigkeit behalten und nur im Bedarfsfall früher über das zentrale Management der OctoGate Schulfirewall gelöscht werden.

Die ausgegebenen Voucher Codes binden die Hardware-Erkennung eines WLAN-Gerätes an das Berechtigungskonzept der OctoGate Schulfirewall. Bei der ersten Anmeldung des Gerätes im WLAN-Netz wird dieser Code einmalig vom System abgefragt. Bei der Generierung der Voucher Codes wird eine Laufzeit definiert – diese Laufzeit startet mit der ersten Anmeldung auf der Abfrage-Webseite.

Dabei sollte die Schule nachhalten, welcher Code an welchen Schüler ausgegeben wurde. Die OctoGate Schulfirewall protokolliert alle Aktionen eines WLAN-Gerätes datenschutzkonform. Beide Datenbestände zusammen können im Fall eines Missbrauchs den jeweiligen Schüler identifizieren und gegebenenfalls sperren.



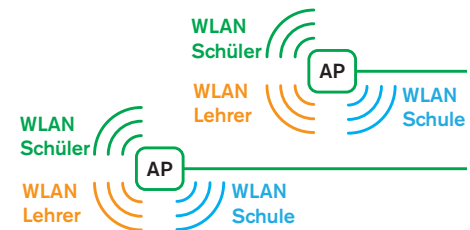
OctoGate Schulfirewall

- Voucher Codes mit individuellen Laufzeiten.
- Laufzeit beginnt erst nach der ersten Anmeldung.
- lückenloses Reporting der Aktionen eines Gerätes.
- nachträgliche Löschung ausgegebener Codes möglich.

Virtuelle Access Points

Im Gesamt-Schaubild auf Seite 5 sehen wir drei WLAN Access Points. Jeder für sich hat drei virtuelle Access Points und strahlt somit ein Netz für Gäste, ein Netz für Lehrer-PCs und ein Netz für schuleigene Geräte aus. Jeder WLAN Access Point strahlt die gleichen Netze aus – somit kann ein WLAN-Gerät, welches sich über das Schulgelände bewegt, ohne Konfigurationsänderung mit allen WLAN Access Points kommunizieren.

Die beispielhafte Konfiguration des Gesamt-Schaubildes soll alle Möglichkeiten und Features der Lösung aufzeigen. Somit wurden drei Netze mit unterschiedlichen Möglichkeiten konfiguriert:



- **Gäste-Netz – für Schüler oder schulfremde Geräte**

Dieses WLAN-Netz ist offen konfiguriert. Ein neuer Gast bekommt zunächst eine Anmeldeseite und muss sein Gerät einmalig mit einem individuellen Voucher Code identifizieren.

- **Lehrer-Netz – für private Geräte der Lehrer**

In diesem Netz wird der Zugang, wie gewohnt, durch ein Passwort gewährt. Ein Zugang zu den geschützten Bereichen der Schulserver (personen-gebundene Daten) ist somit gewährleistet. Natürlich wird auch hier der Datenverkehr der PCs von der Schulfirewall protokolliert und von Viren und Erwachsenen-Inhalten befreit.

- **Schuleigene Geräte-Netz – für schuleigene Geräte**

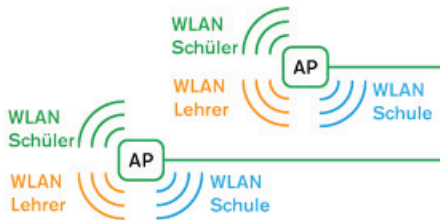
In diesem Netz wird die Zugangskontrolle nicht durch eine Passwortabfrage geregelt, sondern durch ein gesichertes X509-Zertifikat. Hintergrund: WLAN Passwörter sind unter Umständen abfragbar. Somit könnten Schüler den Zugang zu diesen Geräten im Rahmen des Unterrichts erhalten und eigenen Geräten den Zugang erlauben.

Bei einer Authentifizierung durch X509-Zertifikate (Datei, welche von der Windows-Domäne verteilt wird) kann das nicht passieren.

OctoGate Schulfirewall

- beliebig viele virtuelle Access Points (VAP) konfigurierbar.
- jeder Hardware Access Point strahlt alle virtuellen Access Points aus.
- jeder virtuelle Access Point hat ein eigenes Netz mit eigenen Sicherheitsregeln und Zugängen.
- Trennung der Netze und einzelnen Geräte eines Netzes voneinander.

Datenschutz und Netztrennung



Im Schaubild sind die zwei WLAN Access Points in drei Netzen vertreten. Die Aufgabe der WLAN Access Points ist es nun, diese Netze voneinander zu isolieren und alle Daten dieser Netze nur zur OctoGate Schulfirewall zu transportieren. Diese entscheidet dann, ob die Netzwerkanfrage des betreffenden Users bearbeitet werden darf oder abgelehnt wird.

Weiterhin muss natürlich ein Übergang zwischen den virtuellen Netzen unterbunden werden (z. B. WLAN Gäste -> WLAN schuleigene Geräte). Darüber hinaus muss eine Kommunikation der WLAN-Geräte untereinander verhindert werden, so dass unter den Schülern kein Austausch illegaler Inhalte ohne Kontrolle durch die Schulfirewall stattfinden kann.

Die Trennung des Gesamtsystems in drei Netze (orange, grün, rot) hat einen rechtlichen Hintergrund – personenbezogene Daten dürfen kein Netzwerk passieren, in dem Schüler Zugang zu PCs oder zur Infrastruktur erlangen können. Bestimmte, auf den Servern gespeicherte Personendaten, dürfen nur durch die PCs oder durch die WLAN Access Points im Lehrerzimmer abgerufen werden. Die WLAN Signalstärke des WLAN Access Points im Lehrerzimmer wird entsprechend angepasst, so dass das Signal den Raum nicht verlassen kann. Weiterhin wird der WLAN Access Point durch starke Verschlüsselung und Authentifizierung abgesichert.

Datenschutz wird bei uns groß geschrieben. Die OctoGate Schulfirewall protokolliert jegliche Nutzerinteraktion mit dem Netz, um später im Missbrauchsfall aussagefähig zu sein. Da es sich hier um personenbezogene Daten handelt (z. B. welcher Nutzer welche Webseite besucht hat) werden dem „normalen“ Administrator der OctoGate Schulfirewall die Nutzernamen nicht angezeigt. Einzig ein zweiter User, dessen Passwort nur dem Datenschutzbeauftragten übergeben wird, ist in der Lage, die kompletten Daten einzusehen. Auch eine Bereinigung dieser Daten kann individuell konfiguriert werden.

OctoGate Schulfirewall

- Trennung der virtuellen Access Point Netze.
- Isolierung der Clients innerhalb der virtuellen Access Points voneinander.
- Schutz personenbezogener Daten.
- lückenlose Protokollierung und Datenbereinigung.



Infrastruktur

Die OctoGate WLAN Access Points sind mit einem PoE-System ausgestattet. PoE bedeutet „Power over Ethernet“ – somit wird mit dem Netzkabel auch die Stromversorgung für das Gerät angeliefert. Dieses vereinfacht die nachträgliche Installation in einer Schule ungemein, denn somit werden keine zusätzlichen Steckdosen an der Decke oder Wand benötigt. Die Installation eines WLAN Access Points ist damit durchaus durch schuleigenes Personal zu bewältigen.

Achtung: Normalerweise besitzt ein Netzwerk-Switch keine Unterstützung für PoE-Geräte. Hier gibt es zwei Lösungsmöglichkeiten: Entweder wird der Switch durch einen PoE-fähigen Switch ersetzt oder der im Lieferumfang enthaltene PoE-Injector wird verwendet. Hierbei handelt es sich um ein Gerät, das nachträglich eine Netzwerkdatenleitung PoE-fähig macht ohne, dass ein Austausch des Switches erforderlich ist.



Die zentrale Anschaffung eines PoE-fähigen Switches hat einen weiteren Vorteil: Man kann zeitgesteuert oder per Software sämtliche WLAN Access Points ein- oder ausschalten. Das spart zusätzlich Energie.

OctoGate Schulfirewall

- PoE-Stromanschluss über das Netzkabel.
- einfache Installation – keine zusätzliche Strominfrastruktur notwendig.
- Wand-/Deckenhalterung inbegriffen.

Firmware-Updates

Uns als Firewall-Hersteller ist es ungemein wichtig, unsere Module immer auf den aktuellsten Stand der Technik zu bringen. DAS nehmen wir bei der OctoGate Schulfirewall sehr ernst – denn die Hacker schlafen nicht. Gleiches gilt natürlich auch für die WLAN Access Points. Angenommen: Sie haben in einer Schule 20 WLAN Access Points verschiedener Consumer-Hersteller ohne zentrales Management installiert. In diesem Fall wäre es unmöglich, die WLAN Access Points ständig auf dem neuesten Sicherheitsstandard zu halten. Es wäre nicht auszudenken, was passieren würde, wenn jemand von außen über eine bekannte Schwachstelle an schulinterne Daten gelangt oder z. B. die Heizungssteuerung manipuliert.

Bei den OctoGate WLAN Access Points kann das nicht passieren. Unsere OctoGate Schulfirewalls werden regelmäßig auf den neuesten Stand gebracht. Mit jedem neuen Firmware-Update der OctoGate Schulfirewall kommt automatisch auch ein neues Betriebssystem für unsere WLAN Access Points.



OctoGate Schulfirewall

- alle WLAN Access Points erhalten automatisch Updates von der OctoGate Schulfirewall.
- Sicherheitsrisiko Consumer Access Points vermeiden!
- unsere Access Point Firmware ist speziell gehärtet gegen Hacker.

WLAN-Managementfunktionen

Lastverteilung: Ziel einer schulweiten WLAN-Lösung sollten natürlich nicht nur die drei WLAN Access Points sein, wie im Beispiel auf Seite 5 zu sehen, sondern eine flächendeckende Ausleuchtung der gesamten Schule. In der Aula oder in Versammlungsräumen dürfen es dann auch ein paar mehr WLAN Access Points sein, um allen Geräten ausreichend Kapazität zu bieten. Unsere Empfehlung ist hier 25-30 Nutzer pro WLAN Access Point, was in etwa einer Schulklasse entspricht.

Doch gerade in Räumen mit einem hohen Menschenandrang, wie z. B. einer Aula, kommen Sie ohne eine automatische Nutzer- bzw. Lastverteilung nicht mehr aus. Die OctoGate Schulfirewall muss automatisch erkennen, wenn sich zu viele Geräte auf einem WLAN Access Point angemeldet haben und die Geräte umsortieren. Auch eine lastabhängige Verteilung ist hier sinnvoll. Geräte mit hohem Bandbreitenbedarf sollten isoliert auf einem Kanal zusammengefasst werden.

Kanalverteilung: Im Wireless Bereich für 2.4 GHz und 5 GHz gibt es eine Vielzahl von Funkkanälen, welche im europäischen Raum erlaubt sind. Unsere WLAN Access Points erkennen hier automatisch, wenn sich andere WLAN Access Points in der Nähe befinden und belegen automatisch andere Funkkanäle. Somit erübrigt sich, durch die beiden genannten Features, in der Regel die Erstellung eines WLAN-Ausleuchtungsgutachtens. Dadurch sparen Sie Kosten und Zeit.

Leistungsregelung: Unsere WLAN Access Points regeln ihre Leistung selbstständig herunter, wenn sich im Umfeld viele WLAN Access Points befinden. Auch eine uhrzeitgesteuerte Abschaltung oder Verminderung der Sendeleistung der WLAN Access Points ist möglich. Das ist ein wichtiger Punkt, der nicht außer Acht gelassen werden darf. Denn auch, wenn physikalische Emissionen deutlich weniger schädlich als Mobilfunk-Emissionen sind, sollten Sie in der Schule die elektromagnetische Belastung so gering wie möglich halten.

Abwärtskompatibilität: Unsere WLAN Access Points unterstützen selbstverständlich auch ältere Wireless Standards. Des Weiteren existieren Mechanismen, die WLAN-Clients, welche sich nicht korrekt an die Standards halten, daran hindern, andere Systeme zu steuern („beacon timeouts“).

OctoGate Schulfirewall

- Verteilung der Last (Anz. der Geräte) auf erreichbare WLAN Access Points.
- automatische Aushandlung der Funkkanäle – kein Ausleuchtungsgutachten.
- Leistungsregelung: Reduzierung der elektromagnetischen Belastung.
- Abwärtskompatibilität.



Steuerung des WLAN-Zugangs durch den Lehrer

Die OctoGate Schulfirewall hat ausgezeichnete Schnittstellen zu den verschiedenen Klassenraum-Managementsystemen wie zum Beispiel paedML, snv oder INiS, welche es dem Lehrer ermöglichen, den Internetzugang der einzelnen PCs oder der schülereigenen Geräte genau zu regeln und zu überwachen.

Beispielsweise kann in der paedML Lösung des Landes Baden-Württemberg der Lehrer im Unterricht die eigenen, selbstgestellten Firewallregeln und die erreichbaren Webseiten der Schüler PCs steuern.

Ähnliches gilt für den Schulnetzverwalter snv der INL AG – hier können WLAN-Gäste gezielt gesteuert, abgeschaltet oder WLAN Access Points der einzelnen Klassenräume deaktiviert werden.

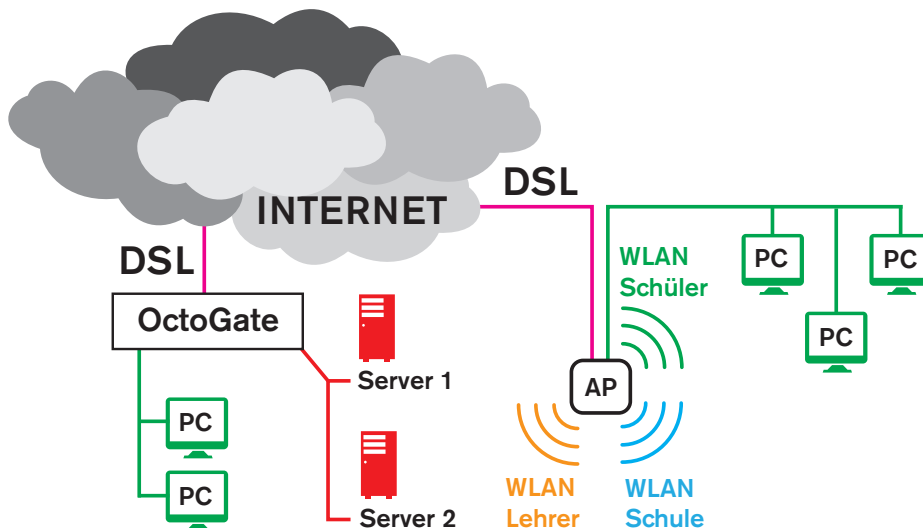
Die Steuerung dieser Features, beispielsweise das Versetzen eines Klassenverbundes in den „Klausurmodus“ (erreichbar ist beispielsweise nur noch Wikipedia), erfolgt innerhalb des Systems, welches der unterrichtende Lehrer permanent benutzt: Die Bedienkonsole des Klassenraum-Managementsystems. Dieses überträgt die Konfiguration zur Firewall, wo die Regeln sofort aktiviert werden. Die Benutzeroberfläche der OctoGate Schulfirewall wäre hier im Praxiseinsatz viel zu komplex und wird durch die komfortable Schnittstelle ersetzt.



OctoGate Schulfirewall

- Schnittstellen zu paedML, snv und INiS.
- Steuerung der Geräte einzelner Schüler oder ganzer Klassen.
- Steuerung des Internetzugangs und des WLANs.

Anbindung von Schul-Außenstellen



Die OctoGate WLAN Access Points können auch an Standorten verwendet werden, welche nur über das Internet mit den Schulsystemen verbunden sind. Sei es eine Außenstelle, in der PCs und ein WLAN Access Point benötigt werden, oder eine entfernte Turnhalle, in der eine Heizungsanlage aus der Ferne gesteuert werden muss. Unsere WLAN Access Points sorgen für eine sichere VPN-Verbindung zur OctoGate Schulfirewall und Ihren Servern in der Schule.

Die Systeme suchen sich automatisch einen Weg über das Internet zu Ihrer eigenen OctoGate Schulfirewall und versorgen auf Wunsch WLAN-Geräte mit einer Verbindung.

Durch das eingebaute Quality of Service Modul (QoS) kann die VPN-Verbindung zu Ihrer eigenen OctoGate Schulfirewall auch für IP-Telefonie oder Terminalserver-Dienste genutzt werden. Es wird automatisch erkannt, ob das zu transportierende Datenpaket Priorität hat oder nicht.

OctoGate Schulfirewall

- VPN-Technologie: Anbindung von Außenstellen.
- Quality of Service / IP Telefonie.
- WLAN in der Außenstelle genauso wie in der Schule.
- Anbindung weiterer kabelgebundener PCs möglich.

Service

Komplizierte Technologie, die Hektik des Schulalltages und die Tatsache, dass ein Lehrer nicht immer gleichzeitig ein IT-Fachmann ist, machen den Einsatz moderner WLAN-Lösungen in Schulen nicht unbedingt einfacher. Wir können durch ein gutes Servicekonzept helfen – unserem OctoGate Managed Service.

Als Firewall-Hersteller in der IT-Branche unterhalten wir ein eigenes, kompetentes Supportteam, welches telefonisch oder per E-Mail jederzeit bei Fragen rund um die Themen Internet, Firewall, Netzwerk und WLAN Rede und Antwort steht.

Grundkonzept unseres Supports ist der direkte Zugriff per Fernwartung auf die Firewall und alle dahinterliegenden WLAN Access Points – schnell, effizient und möglichst schon gleich während des Erstkontaktes mit dem Support-Kunden.

Die Schulen funktionieren anders als Geschäftskunden. Wir haben langjährige Erfahrung mit 1.300 deutschen Schulen. Haben Sie sich auch schon gefragt: „Was tun, wenn...? Mit dem Firewall-Support ein Gespräch führen während ich eine Klasse unterrichte? Nein. Irgendwann im Laufe des Tages von einem Supporter zurückgerufen werden und dann sofort am schadhaften PC eine komplizierte Konfigurationen durchführen? Geht nicht. Während der Abiturprüfungen einen Firewall-Ausfall wegen Einspielung eines Updates? Darf nicht.“

Wir von OctoGate verstehen das und haben unseren kompletten Support auf den Schulalltag und die speziellen Bedürfnisse des Bildungssektors ausgerichtet, um solche Negativbeispiele von vornherein auszuschließen.

OctoGate **Schulfirewall**

- Managed Service: Sie rufen an – wir kümmern uns.
- Support optimiert auf die Bedürfnisse des Schulalltags.
- direkter Support vom Hersteller – schnell und mit datenschutzrechtlich abgesichertem Fernzugriff bis zum WLAN Access Point.





OctoGate

OctoGate IT Security Systems GmbH
Friedrich-List-Str. 42
33100 Paderborn

Telefon: +49 5251 18040-70

E-Mail: vertrieb@octogate.de

Web: www.octogate.de