Die neuen
Securepoint Network Access Controller

NAC 100, NAC 200 und NAC 400

Die Securepoint Network Access Controller sind für wenige bis hin zu tausenden gleichzeitiger Benutzer und zur Integration in kleine bis große, komplexe Netzwerk- und Sicherheitsinfrastrukturen geeignet.

Securepoint bietet folgende Produktlinien an: Securepoint NAC 100 und NAC 200 sind einfach einzusetzen und zu bedienen und eignen sich für kleine und mittlere Unternehmen, sowie für private und öffentliche Hotspots. Securepoint NAC 400 wird zur Abstimmung der Integrations-, Leistungs- und Verfügbarkeitsanforderungen von mittleren bis großen Unternehmen eingesetzt. Für noch größere Infrastukturen können auch mehrere Network Access Controller kombiniert eingesetzt werden.

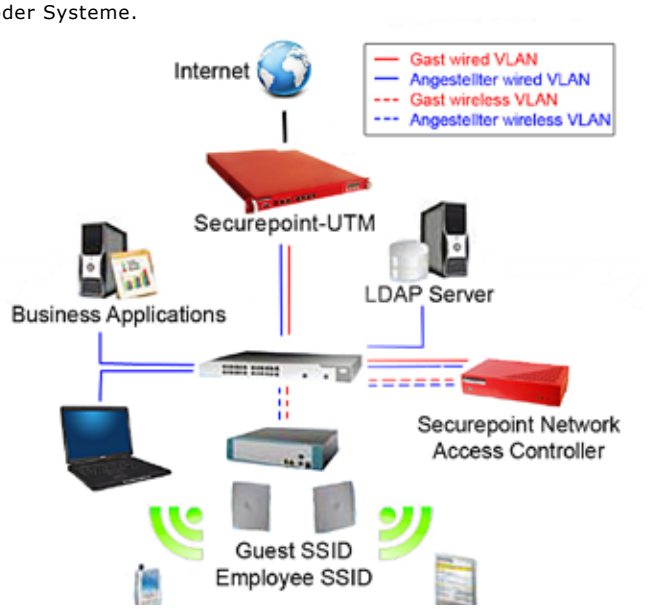
Alle Securepoint Network Access Controller lassen sich dank des unkomplizierten und benutzerfreundlichen graphischen Administration Interface besonders schnell installieren und problemlos in vorhandene Infrastrukturen implementieren.

Securepoint Network Access Controller:
Business Class Secure Mobility

Der Securepoint Network Access Controller ist positioniert zwischen einem Unternehmens-LAN und einem drahtgebundenen (Ethernet, DSLAM, CPL) oder drahtlosen Zugangsnetzwerk.

Der gesamte eingehende und ausgehende Datenverkehr läuft über den Securepoint Network Access Controller, um die absolute Sicherheit der Daten zu gewährleisten, LAN-Integration zu vereinfachen, Verwaltung zu erleichtern und die Benutzerfreundlichkeit zu verbessern.
Die Securepoint Network Access Controller sind je nach Modell in der Lage tausende Benutzer gleichzeitig zu handhaben und lässt sich innerhalb der Netzwerkstruktur unkompliziert installieren.

Alle Securepoint-Lösungen lassen sich dank des unkomplizierten und benutzerfreundlichen graphischen Administration Interface besonders schnell installieren und implementieren.
Securepoint Network Access Controller beinhalten sämtliche für den Betrieb notwendigen Module (LDAP-Directory, RADIUS-Server, DHCP-Server usw.) und benötigen keine zusätzlichen Tools oder Systeme.



Einfache Selbstregistrierung des Benutzers auf dem Securepoint-Portal mit Verbindungseinstellung per SMS auf das Handy.

Neu: Securepoint bietet die Produktlinien Securepoint **NAC 100, NAC 200 und NAC 400** an. Diese WLAN und Network Access Controller lassen sich leicht einsetzen und verwalten; sie erfüllen alle Anforderungen im Hinblick auf firmeninterne Sicherheit sowie Mobilität der Mitarbeiter und Besucher.

Securepoint Network Access Controller richten sich vor allem an Hotels, Kommunal- und Regierungsbehörden, Einrichtungen im Gesundheits- und Bildungswesen, Firmen und Einzelhandelsunternehmen.

Firmeninterne Sicherheit

Konfigurationsfreier mobiler Zugang

Die PCs oder PDAs der Benutzer sind nicht immer so konfiguriert, dass eine Verbindung mit dem Zugangsnetzwerk hergestellt werden kann. Securepoint Network Access Controller ermöglichen den Benutzern das Einwählen und den Zugang zu Netzwerk-Ressourcen ohne vorherige Konfiguration oder Installation und ohne dass sie technischen Support benötigen. IP-Addressierung, Internet-Proxies, E-Mail usw. werden automatisch gehandhabt.
Die Benutzerfreundlichkeit wird wesentlich verbessert und der technische Support auf ein Minimum reduziert.

Gastzugang

Securepoint stellt mit dem NAC Lösungen zu den Themen sicherer Gastzugang, konfigurationsfreier Zugang und Verwaltung der Benutzer-Accounts bereit.
Besuchern des Netzwerks steht ein unkompliziertes und benutzerfreundliches Web-Tool zur Verfügung. Dieses anpassbare Delegation Feature kann genutzt werden, um die Aufgabe des delegierten Administrators im Voraus festzulegen. Eine autorisierte Person kann mit dem NAC einen temporären Account erstellen und diesem ein vordefiniertes Profil mit einem Zeitfenster und/oder Zeitguthaben zuordnen. Ein Connection Ticket wird generiert und dem Benutzer übergeben. Zusätzlich zu diesem Visitor Hosting Tool ermöglichen die Securepoint Network Access Controller die Selbstregistrierung des Benutzers auf dem NAC-Portal. Dabei ist ein Eingreifen Dritter nicht erforderlich, denn die Benutzer erhalten ihre Verbindungseinstellungen per SMS auf ihre Mobiltelefone oder erwerben online Zeit, die z. B. per Kreditkarte abgerechnet wird.

Zonen-Management

Mit dem NAC lassen sich Zonen wie z. B. der Empfangsbereich oder Büros in einem Betrieb, das Foyer oder die Zimmer eines Hotels etc. definieren.
Abhängig von der Zone, aus der sich ein Benutzer einwählt, zeigt der NAC das passende Authentisierungsportal – kostenlos oder kostenpflichtig, mit oder ohne Zeitguthaben.
Der Administrator kann entscheiden, den Zugang von bestimmten Zonen aus zu sperren, z. B. für Besucher ist die Verbindung zu Bürobereichen gesperrt. Eine Zone ist mit einem oder mehreren VLANs verbunden. NAC stellt die Verwaltungs-, Konfigurations- und Überwachungsfunktionen über ein einfaches intuitives Web-Interface zur Verfügung.
Der NAC ermöglicht insbesondere die Echtzeitanzeige der verbundenen Benutzer und der verwendeten Applikationen.

Strikte Verwaltung der Zugangsrechte

Jeder Benutzer erhält ein Profil, welches die Rechte des betreffenden Nutzers (Internet, E-Mail, firmeninterne Anwendungen) je nach Zeit, Standort und Funktion des Benutzers im Unternehmen genau beschreibt.
Die Anwendung der Profile erfolgt dynamisch, immer wenn Benutzer eingeloggt sind.
Der NAC ist in der Lage, den ausgehenden Datenverkehr je nach Profil des Benutzers zu einem bestimmten VLAN und den Internet-Datenverkehr umzuleiten. Dies ermöglicht die Begrenzung verschiedener Benutzergruppen und somit die Durchsetzung der Security Policy des Unternehmens. NAC ist fähig, mehrere Profile, Portale und Ebenen der Datenvertraulichkeit zu bewältigen: Der NAC entspricht dem in den Terminals vorhandenen und durch IEEE 802.11i standardisierten Verschlüsselungsmechanismus (TKIP, AES).

Verbindungsdatenprotokolle

Wen ein Unternehmen in seinem Netzwerk Besucher zulässt, ist es gesetzlich dazu verpflichtet, die Verbindungsdaten der Besucher des Netzwerks zu speichern (europäische Richtlinie 24/2006/EG). NAC erfüllt diese Anforderungen durch Verwaltung der Sitzungsprotokolle (wer hat sich wann eingeloggt) und der Aktivitätsprotokolle. Diese Daten werden in einer Datenbank gespeichert und können bei Bedarf flexibel analysiert werden.

Benutzer-Authentisierung

NAC bietet einen vollständigen RADIUS-Server zur User-Authentisierung, der die Identität der Benutzer über ein Web-Portal überprüft.
Die Authentisierung über das Web-Portal eignet sich aufgrund der einfachen Bedienung besonders für Besucher. Durch die Verwendung eines RADIUS-Servers, kann der NAC ein hohes Maß an Sicherheit für Mitarbeiter gewährleisten. NAC können mit jeder Art Directory (LDAP oder Active Directory) verbunden werden.
Die Verwaltung der Authentisierungsverfahren ist sehr einfach und erfolgt über ein sicheres Web-Interface.

Securepoint Network Access Controller
Mehr Kontrolle, mehr Sicherheit.

Vorteile von Securepoint:

SICHERHEIT IM UNTERNEHMEN
- Authentisierung, Vertraulichkeit, Rückverfolgbarkeit, Begrenzung
- Zugangskontrolle nach Profil (Mitarbeiter, Besucher)
- gemeinsame Nutzung drahtgebundener und drahtloser Netzwerke

MOBILITY MANAGEMENT
- Kunden, Lieferanten, Subunternehmer, Partner
- Konferenz- und Schulungsräume
- Beschaffung, Sicherheit, gesetzliche Verpflichtungen

EINFACHE NUTZUNG, IMPLEMENTIERUNG UND VERWALTUNG
- gut gestaltete Web-Interfaces für die Verwaltung
- konfigurationsfrei

SECUREPOINT
SECURITY SOLUTIONS

Securepoint GmbH
Salzstraße 1
21335 Lüneburg
Germany

fon: ++49 (0) 41 31 / 24 01-0
fax: ++49 (0) 41 31 / 24 01-50

mail: info@securepoint.de
web: www.securepoint.de