



Die besten Vorgehensweisen bei der Einrichtung eines sicheren Wireless-Netzwerks

INHALT	
Einleitung	2
Aktuelle Sicherheitsanforderungen	2
Zielsetzung	2
Technische Grundlagen	3
Aktuelle Problemstellung	4
Die wichtigsten Sicherheitsanforderungen an integrierte Netzwerke	4
Die führende Stellung von SonicWALL	6
Zusammenfassung	8

Einleitung

Die Wireless-Technologie verändert die Arbeitsabläufe in Unternehmen grundlegend. Unabhängig von ihrem jeweiligen Standort im Unternehmen können die Mitarbeiter unmittelbar auf unternehmenskritische Anwendungen und Informationen zugreifen, um Anfragen von Kunden sowie Kollegen in Echtzeit zu bearbeiten. Dies erhöht die Produktivität und verbessert den Kundenservice. Folglich versteht man unter „Arbeit“ immer weniger einen konkreten Ort als vielmehr eine Aktivität, die unabhängig vom Standort ausgeführt werden kann.

Wireless-Netzwerke bergen jedoch erhebliche Sicherheitsrisiken, da sie die physischen Grenzen des Netzwerks aufheben. Kein Unternehmen kann es sich leisten, die Sicherheit seines Netzwerks durch den Komfort eines Wireless-Netzwerks zu gefährden. Das vorliegende Dokument beschreibt mögliche Risiken eines Wireless-Netzwerks und die beste Vorgehensweise, um das volle Potenzial eines solchen „drahtlosen“ Netzes ohne Kompromittierung der Sicherheit auszuschöpfen.

Aktuelle Sicherheitsanforderungen

Das alte Bild von Netzwerken – der drahtgebundene Benutzer geht dorthin, wo sich die Daten befinden – ist längst überholt. Vielmehr kommen durch die wachsende Beliebtheit des Wireless LAN die Daten zum Benutzer, der auf diese Weise produktiver und effizienter arbeiten kann. Innerhalb der Reichweite eines Wireless-Netzwerks kann ein mobiler Benutzer von überall und jederzeit auf das Netzwerk zugreifen. Trotz dieser eindeutigen Vorteile haben Unternehmer und Netzwerkadministratoren auch berechtigte Sorge, wenn es um die Implementierung und Verwaltung des drahtlosen Zugriffs auf das Netzwerk geht. Wireless-Netzwerke bergen eine Reihe schwerwiegender Sicherheitsrisiken, die den Einsatz strenger und umfassender Sicherheitsmaßnahmen zur Eindämmung dieser Risiken erforderlich machen.

Zielsetzung

Im vorliegenden Dokument werden Faktoren vorgestellt, die für die Sicherung eines Wireless-Netzwerks erforderlich sind. Mit Hilfe dieser Informationen können Unternehmer und Netzwerkadministratoren vermeiden, dass durch eine unzureichende Implementierung unnötige Kosten und Risiken entstehen. Des Weiteren sind Hintergrundinformationen und Leitlinien zur Bewertung der derzeit verfügbaren Wireless-Lösungen sowie ein Überblick über die zentralisierte Verwaltung von kabelgebundenen und Wireless-Netzwerken enthalten.

Die Verantwortlichen im Unternehmen möchten sich für eine Kerntechnologie entscheiden, die am besten auf ihre Branche und ihre Geschäftsanforderungen zugeschnitten ist. Denn Unternehmen benötigen Lösungen, die bereits heute kosteneffektiv sind, sich aber auch an wachsende zukünftige Anforderungen anpassen. Als weitere Entscheidungshilfe enthält das Dokument einen Überblick über die Gesamtbetriebskosten (TCO) und die Skalierbarkeit der jeweiligen Lösung.

Die erörterten Sicherheitslösungen kombinieren kabelgebundene und drahtlose Netzwerke miteinander und sind in einer Vielzahl von Konfigurationen verfügbar, so dass sie den Erfordernissen unterschiedlich großer Unternehmen der verschiedensten Branchen genügen. Alle beschriebenen Lösungen erfüllen die zentralen Bewertungskriterien für einen sicheren, kosteneffektiven, effizienten und skalierbaren Netzwerkbetrieb.

Technische Grundlagen

Das drahtgebundene LAN eines Unternehmens befindet sich innerhalb des Gebäudes, wobei die Daten nur über Leitungen übertragen werden und nur autorisierten Benutzern mit physischen Verbindungen zu diesen Leitungen zugänglich sind. Jedes Netzwerk – sei es ein kabelgebundenes oder ein Wireless-Netzwerk – ist jedoch anfällig für Sicherheitsrisiken. Zu diesen Risiken gehören Bedrohungen der physischen Sicherheit eines Netzwerks, unautorisierter Zugriff oder Abhören bis hin zu Angriffen aus dem Netzwerk selbst seitens der (autorisierten) Benutzer.

Mit Ausnahme des physischen Kabels verfügt ein Wireless LAN (WLAN) über die gleichen Eigenschaften und Sicherheitsrisiken wie ein drahtgebundenes LAN. Daher gelten für Wireless LANs die gleichen Sicherheitsmaßnahmen wie für drahtgebundene LAN-Umgebungen, um die Datenintegrität und -sicherheit zu gewährleisten. Bei Wireless LANs fallen jedoch weitere spezifische Sicherheitsfaktoren an. Naturgemäß ermöglichen Wireless-Netzwerke innerhalb ihrer Reichweite den Zugriff durch Dritte, z.B. durch Personen außerhalb der physischen Sicherheitsumgebung des Netzwerks. Obwohl die Reichweite eines Wireless LANs begrenzt ist, können drahtlose Signale häufig noch mehrere Hundert Meter außerhalb der physischen Begrenzung eines Gebäudes empfangen werden. In größeren Unternehmen mit mehreren Wireless LAN Access Points, an denen sich drahtlose Benutzer in die drahtgebundenen Netze einwählen, stellt daher jeder Access Point zugleich eine Eindringmöglichkeit in das interne Netzwerk dar.

Mittlerweile gibt es viele verschiedene Arten von Wireless-Sicherheitslösungen unterschiedlicher Hersteller, um diese Sicherheitsrisiken und -probleme zu bekämpfen. Die meisten Wireless-Sicherheitslösungen lassen sich einer der drei im Folgenden beschriebenen Kategorien zuordnen.

Eigenständige Access Points

In den Anfängen der Wireless-Technologie wurden eigenständige Access Points, sog. Standalone Access Points, kurz APs, eingesetzt. Diese dienten hauptsächlich dazu, den 802.11-konformen drahtlosen Datenverkehr zu sammeln. Zum einen fehlte eine zentrale Verwaltung; zum anderen war es schwierig, auch in einem größeren, verteilteren Wireless-Netzwerk den Roaming-Benutzern konstante Leistung zu bieten. Auch die Skalierbarkeit war ein Problem, da jeder AP lokal verwaltet werden musste. Der gravierendste Nachteil war jedoch, dass bei eigenständigen Access Points keine zentralen Sicherheitsrichtlinien eingesetzt werden können. Durch die minimale integrierte Sicherheit – üblicherweise WEP (Wired Equivalent Privacy) oder zunehmend WPA (Wi-Fi Protected Access) mit einem Pre-Shared-Key – wogen sich die arglosen Benutzer in einer falschen Sicherheit. Und verständlicherweise sorgten sich die Netzwerkadministratoren, dass ihre Netzwerke durch solche Produkte für Backdoor-Angriffe, wie Dictionary-Attacks (Einbruch durch Erraten der Kennwörter) und Man-in-the-Middle-Attacks (Angriffsart, bei dem der Angreifer zwei Kommunikationspartnern den jeweils anderen Partner vorspielt), angreifbar wurden.

Sichere Wireless-Gateways

Einige Hersteller entwickelten als Reaktion auf die zunehmenden Sicherheitsrisiken sog. sichere Wireless-Gateways (eigenständige Geräte, die in das vorhandene Netzwerk integriert werden können). In Verbindung mit den APs anderer Hersteller setzen Sicherheits-Appliances auf Gateway-Ebene Sicherheits- und Verwaltungsrichtlinien im gesamten WLAN-Datenverkehr durch. Die APs werden jedoch nicht vom Gateway verwaltet, sondern Firmware-Upgrades oder die Einstellung der Funkfrequenz muss an jedem AP einzeln durchgeführt werden: Dies erfordert mehr Ressourcen als eine zentral verwaltete Lösung.

Kombination von Switches und Access Points

Die neueste Entwicklung in diesem Bereich stellt die Kombination eines Wireless-Switches mit verwaltbaren APs durch einen einzigen Hersteller dar. Diese Lösungen bieten eine zentrale Verwaltung der APs sowie des WLAN-Datenverkehrs, die Durchsetzung von Wireless-Sicherheitsrichtlinien und eine detaillierte Kontrolle der Funkfrequenzen.

Die Nachteile dieser Lösungen liegen auf der Kostenseite und im Verwaltungsaufwand, da ein zusätzlicher wireless-spezifischer Switch mit einem eigenen WLAN-Verwaltungssystem nötig ist, das neben der vorhandenen LAN-Verwaltungsplattform des Unternehmens betrieben wird. Folglich müssen die Unternehmer nach wie vor mit zwei parallelen Netzwerken arbeiten. Eine Lösung diesen Typs wäre noch immer anfällig für schwer einzugrenzende und dynamische Bedrohungen durch Malware wie Viren, Spyware, Würmer und Phishing-Angriffe, die sich über die Anwendungsebene verbreiten.

Aktuelle Problemstellung

Netzwerk- und Sicherheitsadministratoren suchen nach einer Möglichkeit, kabellose Netzwerke mit derselben Zuverlässigkeit vor den gleichen Bedrohungen wie kabelgebundene Netzwerke zu schützen. Der mögliche Verlust der Datensicherheit wird von den Unternehmen als Hauptgrund dafür angegeben, dass kein Wireless LAN implementiert wird. Es ist kein Zufall, dass der nicht autorisierte Zugriff auf vertrauliche Daten und Lauschangriffe auf das Netzwerk auch bei der Implementierung kabelgebundener Netzwerke die größten Sicherheitsproblemen darstellen. Ähnlich wie bei der Übertragung von Daten aus dem Internet, kann man auch bei drahtlosen Daten nicht sicher sein, woher sie stammen, da sie durch Wände und Gebäude in das Netzwerk gelangen. Daher muss das Wireless-Netzwerk genau wie Daten aus dem Internet als nicht vertrauenswürdig angesehen und vom internen Netzwerk getrennt werden.

Die drei oben beschriebenen Produktkategorien sind auf aktuelle Wireless-Anforderungen und -Probleme zugeschnitten. Sie ignorieren jedoch, dass die Netzwerkadministratoren nach einer sicheren und praktikablen Methode suchen, um für das Wireless-Netzwerk ein ebenso robustes Sicherheitsniveau wie für das drahtgebundene Netzwerk zu gewährleisten, ohne ein paralleles WLAN und ein zusätzliches Verwaltungssystem einzurichten. Mit zunehmender Komplexität der Sicherheitsbedrohungen sind für den entsprechenden Schutz immer mehr Ressourcen erforderlich. Allein aus diesem Grund ist es nicht zweckmäßig, einfach ein weiteres Verwaltungssystem für das Wireless-Netz zu verwenden, sondern das Sicherheitsmanagement für beide Netze zu kombinieren.

Die wichtigsten Sicherheitsanforderungen an integrierte Netzwerke

Grundlagen

Eine zuverlässige Sicherheitsstrategie für Wireless-Netzwerke sollte nach den folgenden Richtlinien erstellt werden:

- Im Wireless-Netzwerk gelten die gleichen Sicherheitsrichtlinien wie in jedem anderen nicht vertrauenswürdigen Netzwerk.
- Der Sicherheitsansatz wird in Schichten implementiert. Er beginnt mit einer robusten Firewall (basierend auf einer konfigurierbaren, hochperformanten Deep-Packet-Inspection-Engine), auf die eine dynamisch aktualisierte Datenbank mit Tausenden von Angriffs- und Schwachstellensignaturen folgt.
- Dieser Schichtenansatz ermöglicht eine vollständige Sicherheitslösung, die das Netzwerk vor einer Reihe dynamischer Bedrohungen schützt, wie z.B. Viren, Würmern, Trojanern, Software-Schwachstellen (z.B. Pufferüberläufe); Peer-to-Peer- und Instant Messenger-Anwendungen, Backdoor-Angriffen und anderem böartigem Code.
- Für Wireless-Clients, die sich über das Wireless-Netzwerk in das Netzwerk einwählen, gelten die gleichen Sicherheitsrichtlinien wie für Remote-Benutzer, die sich über das Internet mit dem internen vertrauenswürdigen Netzwerk verbinden.

Eine solche Sicherheitsstrategie erfordert eine wohl überlegte Planung. Zur Gewährleistung von Sicherheit, Zuverlässigkeit, skalierbarer Leistungsstärke und benutzerfreundlicher zentraler Verwaltung sollte proaktiv vorgegangen werden.

Bewährte Sicherheit

Jeder Benutzer, der die Verbindung zu einem internen Netzwerk über ein nicht vertrauenswürdiges Netzwerk herstellt, muss auf seinem Computer, Laptop, privaten Computer oder an seinem Arbeitsplatz in einer Niederlassung die IPSec-VPN-Client-Software verwenden. IPSec ist seit vielen Jahren bewährter Standard und hat sich vom VPN-Zugriff über das Internet bis hin zur sicheren Kommunikation bei Geldgeschäften als stabil und zuverlässig erwiesen. Der VPN-Client verwendet den internen Netzwerk-Gateway zur Authentifizierung und Verschlüsselung des Datenverkehrs.

Obwohl für WLAN-spezifische Verschlüsselung hauptsächlich der Standard IEEE802.11i verwendet wird, bietet IPSec VPN mehr Flexibilität und kann sozusagen „zweifach“ verwendet werden: die Mitarbeiter haben immer dieselben Benutzerberechtigungen, auch wenn sie sich nicht in ihrem Büro befinden, sondern beispielsweise eine Wireless-Verbindung in einem Besprechungsraum nutzen. Der Zugriff auf das interne LAN-Netzwerk erfolgt über denselben VPN-Client, der auch von unterwegs, zuhause oder in Niederlassungen für den Remote-Zugriff auf das Netz verwendet wird. Die Administratoren müssen pro Benutzer lediglich ein Konto für den Zugriff auf WLAN-Standorte einrichten. Dies macht den sicheren Netzzugriff kostengünstiger und effizienter. Eine sichere Lösung für den Zugriff auf Wireless-Netzwerke sollte so flexibel gestaltet sein, dass sie sowohl den IPSec-VPN-Zugriff über das WLAN unterstützt als auch mit WLAN-Verschlüsselungsstandards wie z.B. IEEE 802.11i kompatibel ist.

Zentral verwaltete Sicherheitsprodukte zur Implementierung von Wireless-Sicherheit müssen darüber hinaus zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken unterscheiden und Sicherheitsrichtlinien für den gesamten Datenverkehr im Netz durchsetzen können. Im Unternehmen sollte eine Benutzer-Datenbank eingesetzt werden, mit der Verbindungsanfragen und deren Rückfragen abgeglichen werden können. Hierbei bietet sich eine gemeinsam von den kabelgebundenen und kabellosen Netzwerken verwendete Datenbank an, damit der Netzwerkadministrator nicht zwei Datenbanken verwalten muss.

Bekämpfung von neuen Bedrohungen und Produktivitätsproblemen

Netzwerkangriffe werden immer zahlreicher und komplexer. Stateful-Packet-Inspection-Firewalls und VPN-Lösungen sind daher zwar notwendig, aber längst nicht mehr ausreichend, um Netzwerkintegrität und umfassende Sicherheit garantieren zu können. Sogar herkömmliche Desktop-Antiviren-Clients haben sich bei der Blockierung der neuesten Varianten von Viren, Würmern und Trojanern als nicht effektiv genug erwiesen. Unabhängig von der Art des Netzwerks (kabelgebunden oder kabellos), ist es für Unternehmer und Netzwerkadministratoren zwingend erforderlich, die notwendigen Sicherheitsmaßnahmen zum Schutz vor kombinierten Angriffsmethoden zu ergreifen. Diese Angriffsarten werden per E-Mail, in Attachments, über Websites oder Peer-to-Peer-Anwendungen eingeschleust. Deshalb sind Sicherheitslösungen wie Gateway-Virenschutz, Anti-Spyware, Intrusion Detection und Intrusion Prevention erforderlich, um diese kombinierten Angriffsarten zu bekämpfen. Die zentralisierte Sicherheitslösung sollte zusammen mit herkömmlichen Firewall- und VPN-Regeln den gesamten Datenverkehr innerhalb des Netzwerks und zwischen den einzelnen Netzwerksegmenten sichern.

Rogue-AP-Detection

Mit der Rogue-AP-Detection wird gewährleistet, dass das Hinzufügen eines nicht autorisierten APs in das Netzwerk keine Backdoor-Schwachstellen verursacht. Hierfür müssen manuell und zeitgesteuert Virensuchläufe in der Reichweite der Funkfrequenz (RF) durchgeführt werden, um APs in der näheren Umgebung ausfindig zu machen, sie zu erfassen und die Netzwerkadministratoren darüber zu informieren.

Benutzerfreundliche Verwaltung/Gesamtbetriebskosten

Werden Wireless- und drahtgebundene Sicherheit in einer Plattform integriert, muss auch die Konfiguration und Verwaltung der jeweiligen Netzwerke ermöglicht werden, sowie die Durchsetzung der unternehmensweiten Sicherheitsrichtlinien in den Netzwerken von einer einzigen, zentralen Verwaltungsschnittstelle aus. Der Schulungsaufwand für die Administratoren wird erheblich geringer, da sie sich nicht mehr mit einer Vielzahl von

Plattformen auseinandersetzen müssen; redundante Verwaltungsaktivitäten entfallen. Die Protokollierung und Berichterstellung von Netzwerkaktivitäten, die für die Rechnungsprüfung erforderlich sind, sollte zentral gesteuert werden.

Eine effektive Wireless-Sicherheitslösung gibt dem Netzwerkadministrator die Möglichkeit, mit Hunderten von Access Points zu kommunizieren, ohne dass er sich mit jedem AP einzeln befassen muss. Eine zentrale Sicherheitsverwaltung kann über eine zentrale Verwaltungsschnittstelle alle Access Points konfigurieren und verwalten. Updates der Sicherheitsrichtlinien werden jedem Access Point automatisch zugestellt.

Einfache Einrichtung eines Wireless-Guest-Internetzugangs

Bei einer Wireless-Sicherheitslösung sollte problemlos ein Gastzugang eingerichtet werden können. So können auch kurzzeitige Benutzer auf öffentliche Ressourcen wie das Internet zugreifen, ohne dass der Zugang auf vertrauenswürdige Netzwerkressourcen, wie z.B. das kabelgebundene LAN, freigegeben werden muss.

Die Herausforderung liegt darin, ohne zusätzliches paralleles Netzwerk einem vertrauenswürdigen Benutzer den Wireless-Zugang auf Netzwerkressourcen zu ermöglichen, während gleichzeitig ein Besucher über ein Gastkonto ungehindert auf das Netzwerk zugreift. Dafür muss die Sicherheitslösung sowohl über Gastzugangs-Services mit Authentifizierungsmechanismen verfügen, um die Gastbenutzer von vertrauenswürdigen Wireless-Benutzern zu unterscheiden, als auch je nach Benutzer und Nutzungsrichtlinien des Unternehmens verschiedene Zugangsebenen aufweisen.

Die problemlose Einrichtung eines Gastzugangs ist ein wichtiger Faktor. Dazu muss die Sicherheitslösung eine einfache Methode für den temporären Zugriff bieten, ohne dass die Netzwerkintegrität kompromittiert wird.

Möglichkeit zur Erweiterung

Eine Wireless-Sicherheitslösung muss leicht einzurichten und zu skalieren sein. Der Übergang von Legacy-Wireless-Netzwerken muss effizient möglich sein.

Besonders wichtig ist die Skalierbarkeit. Unternehmen mit ausgedehnten Arealen benötigen möglicherweise mehrere Hundert Access Points. Wireless-Sicherheitslösungen können die Einrichtung vereinfachen, indem die anfängliche Bereitstellung der Access Points sowie umfangreiche Veränderungen, wie z.B. die Verteilung neuer Firmware und Konfigurationen, automatisiert wird. Mit einer Wireless-Sicherheitslösung sollten so viele zulässige Access Points wie nötig problemlos verbunden und ihr Betrieb automatisiert werden.

Außerdem sollten Wireless-Sicherheitslösungen dem Benutzer Transparenz bieten, ohne dass unhandliche, komplizierte untergeordnete Software oder andere Änderungen an ihren Geräten unbedingt erforderlich sind.

Abschätzung der Benutzererfahrung

Aus der Perspektive des Benutzers muss eine Wireless-Sicherheitslösung ungeachtet seines Standortes innerhalb des Unternehmens eine konstante Netzwerkverbindung ohne Unterbrechungen gewährleisten. Dies ist für den Benutzer eine grundlegende Voraussetzung, um die Vorteile des Wireless-Netzwerks vollständig nutzen zu können.

Der Benutzer fordert einen transparenten und unterbrechungsfreien Netzwerkbetrieb. Gleichzeitig ist es die Aufgabe des Netzwerkadministrators, im gesamten Unternehmen einen sicheren Wireless-Zugriff und einen vollständigen Schutz des Netzwerks zu garantieren. Diese Ebene des unterbrechungsfreien Service wird stetig verbessert, ebenso wie Erweiterungen zur Unterstützung von Streaming Audio- und Streaming Video-Anwendungen. Daher sollte bei der Wahl eines Anbieters von Wireless-Lösungen besonders darauf geachtet werden, dass dieser neue Standards und Innovationen in diesen Bereichen durch zeitnahe und leicht zu implementierende Updates der Access-Point-Firmware einhält.

Einhaltung standardbasierter Architektur

Für eine erfolgreiche Implementierung müssen Wireless-Lösungen auf einem Standard basieren, um ihren Betrieb in einer bereits vorhandenen Wireless- und Sicherheitsinfrastruktur zu gewährleisten. Zu diesen Standards gehören der IEEE 802.11a/b/g-Standard für drahtlose Netzwerke, der Power-over-Ethernet-Standard IEEE 802.3af (PoE), der IEEE 802.11d-Standard, IPSec-Verschlüsselung für sicheren Wireless LAN-Zugang, WPA und der IEEE 802.11i-Standard. Darüber hinaus müssen solche Lösungen auf die jeweilige Hardware zugeschnitten sein, damit sie kurzfristig erweiterte Sicherheitsrichtlinien durch ein einfaches Firmware-Upgrade übernehmen können.

SonicWALL als Marktführer

SonicWALL Inc. ist einer der führenden Anbieter von Internet-Sicherheitslösungen im Bereich mehrschichtiger Sicherheitslösungen für Netzwerke aller Größen. Seine breitgefächerte fachliche Kompetenz im Bereich Netzwerksicherheit setzt SonicWALL ein, um wireless-spezifische Sicherheitsprobleme zu lösen.

Die Baureihen SonicWALL SOHO TZW, TZ 170 Wireless und TZ 150

Im Jahre 2003 leistete SonicWALL Pionierarbeit und entwickelte die erste Single-Point-Lösung, die sowohl für kabelgebundene als auch für Wireless-Netzwerke Sicherheit und Verwaltungsfunktionen bot. Nach dem überragenden Erfolg dieser ersten Version führte SonicWALL die Produkte TZ 150 Wireless und TZ 170 Wireless ein. Hierbei handelte es sich um sichere Wireless-Gateways, die sichere, 802.11b/g-konforme, Deep-Packet-Inspection-Firewall- und VPN-Technologien in einer einzigen und benutzerfreundlichen Lösung integrierten. Durch die VPN-Verschlüsselung im Wireless LAN gewährleisten sowohl TZ 150 Wireless als auch TZ 170 Wireless lückenlose Wireless-Sicherheit; sie tragen den Sicherheitsanforderungen der IT-Administratoren einerseits und den Wünschen der Benutzern nach einem Wireless-Netzwerk in kleinen Unternehmen andererseits Rechnung. TZ 150 und TZ 170 sind mit dem SonicWALL Global VPN Client und dem Global Security Client kompatibel und gewährleisten so einen sicheren Wireless- und Remote-Zugriff auf das Unternehmensnetzwerk. Für das Wireless-Netzwerk werden zusätzliche Sicherheitsebenen durch Rogue-AP-Detection und moderne Wireless Intrusion Detection Services bereitgestellt – Standardfunktionen, über die alle SonicWALL Wireless-Lösungen verfügen. Netzwerkadministratoren schaffen sowohl für drahtgebundene und drahtlose Mitarbeiter als auch für Wireless-Gastbenutzer zahlreiche Zugangsbereiche, zusammen mit einem beispiellosen Maß an Steuerung und Flexibilität, ohne Kompromisse bei der Netzwerksicherheit eingehen zu müssen.

Sichere, verteilte Wireless-Lösung von SonicWALL

Aufbauend auf den innovativen Single-Point-Wireless-Lösungen ist die SonicWALL Secure Distributed Wireless Solution auf die Anforderungen größerer Netzwerke zugeschnitten. Diese Lösung beinhaltet eine SonicWALL-Sicherheits-Appliance der Baureihe TZ 170 oder PRO (PRO 1260, 2040, 3060, 4060 oder 5060) unter dem Betriebssystem SonicOS Enhanced 2.5 oder höher und ist kombiniert mit SonicPoints. SonicPoints sind IEEE 802.11a/b/g- sowie 802.11b/g-konforme und voneinander abhängige Access Points, die Benutzern im Netzwerk eine sichere Wireless LAN-Verbindung gewährleisten.



Abbildung 1: Secure Distributed Wireless Solution – Sicherheits-Appliances der Baureihe PRO und SonicPoints (APs)

Die SonicWALL-Appliance der Baureihe TZ 170 bzw. PRO bietet zentrale Verwaltung von kabelgebundenen sowie Wireless LANs. Mit Hilfe des SonicWALL Discovery Protocol (SDP) erkennt die Sicherheits-Appliance sofort, wenn SonicPoints zum Netzwerk (Ebene 2) hinzugefügt werden. Nach der Erkennung der SonicPoints nutzt die Sicherheits-Appliance über das SonicWALL Simple Provisioning Protocol (SSPP) automatische Bereitstellungsfunktionen, um auf allen APs automatisch eine vordefinierte Konfiguration zu installieren. Durch die Verwendung des SonicWALL-Betriebssystems SonicOS Enhanced kann jede Appliance der SonicWALL-Baureihen TZ 170 bzw. PRO die SonicWALL Secure Distributed Wireless Solution nutzen.

Im Gegensatz zu anderen Wireless-Sicherheitslösungen löst die SonicWALL Secure Distributed Wireless Solution nicht nur wireless-spezifische Sicherheitsprobleme, sondern ermöglicht auch die Durchsetzung von Sicherheitsrichtlinien und eine zentrale Verwaltung von kabelgebundenen sowie kabellosen LANs. Während Ihr Netzwerk mit anderen Wireless-Lösungen immer noch anfällig für Viren, Software-Schwachstellen, Würmer und bösartigen Datenverkehr ist, bietet SonicWALL eine integrierte Sicherheitslösung, die Firewall-Regeln für den gesamten Netzwerkverkehr und Sicherheitsdienste, wie z.B. Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service, sowohl für den kabelgebundenen als auch den kabellosen Datenverkehr durchsetzt.

SonicWALL's Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service wehrt mit Hilfe einer leistungsstarken, intelligenten Scan Engine, die das Unternehmensnetzwerk in Echtzeit nach Viren, Würmern und anderen Internetbedrohungen durchsucht, dateibasierte Viren und bösartigen Code ab. Diese einzigartige Lösung sorgt bereits am Sicherheits-Gateway für Schutz vor Bedrohungen, indem sie Download- oder E-Mail-Dateien mit einer umfangreichen und dynamisch aktualisierten Signaturdatenbank besonders bedrohlicher Viren abgleicht. Aufgrund der täglich neuen und meist unvorhersehbaren Bedrohungen wird die Deep-Packet-Inspection-Architektur ständig aktualisiert. So kann der weitest mögliche Schutz vor sich ständig verändernden Bedrohungen gewährleistet werden.

SonicWALL Gateway Anti-Virus überprüft E-Mail-, Internet-, Dateiübertragungs- und eine Vielzahl von streambasierten Protokollen (einschließlich SMTP, POP3, IMAP, HTTP, FTP und NetBIOS) und durchsucht Instant-Messaging- und Peer-to-Peer-Anwendungen, wodurch Netzwerkviren umfassend abgewehrt werden. Als zusätzliche Sicherheitsschicht schützt Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service vor Angriffen über die Anwendungsschicht nicht nur vor externen Bedrohungen, sondern auch vor Bedrohungen aus dem eigenen Netzwerk.

Im Unterschied zu anderer Sicherheitssoftware analysiert der Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service Dateien jeder Größe in Echtzeit, ohne dass kostspielige Laufwerke oder Speichermedien zusätzlich angeschafft werden müssen. Dieser Sicherheits-Service ist damit eine grundlegende Voraussetzung für einen lückenlosen Sicherheitsschutz und außerdem eine der wichtigsten Bestandteile der SonicWALL-Strategie zur Erzielung einer skalierbaren und mehrschichtigen Sicherheit für Netzwerke aller Größen.

Die SonicWALL Secure Distributed Wireless Solution verfügt über einige erweiterte Funktionen, wie Wireless Guest Services (Internetzugang für Gast-Benutzer ohne die Sicherheit des vertrauenswürdigen Netzwerks zu gefährden), IPSec VPN für einen sicheren Zugriff auf das Wireless LAN, Rogue-AP-Detection und kabelgebundene sowie kabellose Sicherheits- und Konfigurationsrichtlinien, die über die Benutzeroberfläche der Sicherheits-Appliance zentral konfiguriert werden.

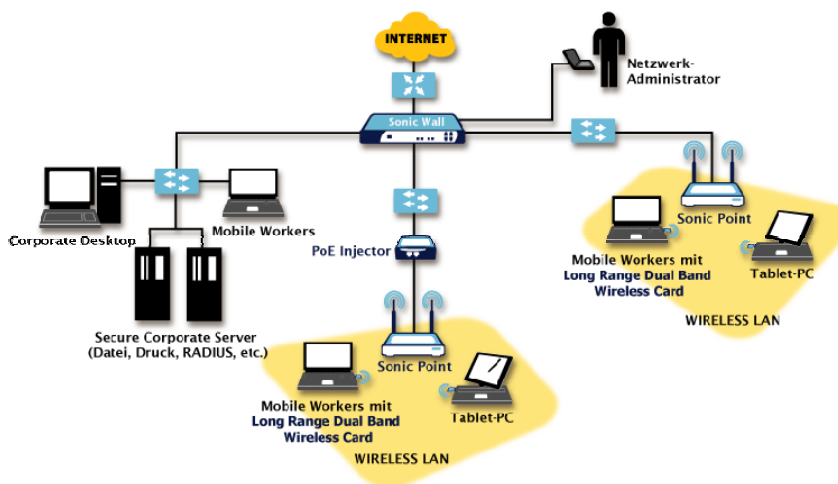


Abbildung 2: Secure Wireless Deployment

SonicPoints

SonicPoints sind IEEE 802.11a/b/g- bzw. 802.11b/g-konforme, Access Points, die Benutzern im Netzwerk eine sichere Wireless LAN-Verbindung ermöglichen. Der SonicPoint ist ein Tri-Mode-, Dual-Band- und Dual-Radio-fähiger und IEEE 802.11a/b/g-konformer Access Points. Für Kunden, die auf eine hohe Flexibilität bei der Implementierung angewiesen sind, ist der SonicPoint G als Dual-Mode-, Single-Band- und IEEE 802.11b/g-konformer Access Point mit mobilen Hochleistungsantennen besonders geeignet. Die Hochleistungsfunkwellen der SonicPoints unterstützen Benutzer mit den Standards 802.11a bzw. 802.11b/g. Beim Einsatz der SonicWALL Long Range Dual Band Wireless Card unterstützen SonicPoints außerdem den 108 Mbit/s-Turbo-Modus der Standards 802.11a bzw. 802.11g.

Zusätzlich zu IPSec VPN over WLAN können WPA und 802.11i auf allen SonicPoints konfiguriert werden. SonicPoints sind mit den IEEE 802.3af-Standards kompatibel. Dadurch unterstützen die SonicPoints Power-over-Ethernet (POE) und lassen sich einfach an Wand oder Decke montieren, da keine elektrischen Leitungen verlegt werden müssen. Da SonicPoints über die Verwaltungsschnittstelle der Sicherheits-Appliance vollständig konfiguriert und verwaltet werden können, ist keine dedizierte Verwaltung erforderlich. Und schließlich werden unterstützte Benutzer durch 802.11d-konformes, internationales Roaming angewiesen, ihre Einstellungen (wie z.B. Leistung und Betriebskanal) zur Erfüllung regionaler Auflagen automatisch anzupassen.

Verwaltung

Die SonicWALL Secure Distributed Wireless Solution ermöglicht Netzwerkadministratoren die zentrale Verwaltung und Konfiguration aller SonicPoints. Für Niederlassungen bzw. Benutzer, die weit voneinander entfernt sind, können Netzwerkadministratoren über das SonicWALL Global Management System (GMS) kabelgebundene und drahtlose Netzwerksicherheitsrichtlinien für Hauptstellen, Zweigstellen und mobile Benutzer global verwalten und durchsetzen. Die Sicherheitslösung lässt sich von einigen wenigen Büros bis hin zu Tausenden verteilter Netzwerke skalieren.

Zusammenfassung

Unabhängig davon, ob es sich um ein kabelgebundenes oder ein Wireless-Netzwerk handelt, sollten Maßnahmen zum Schutz der Netzwerksicherheit und der Netzwerkintegrität ergriffen werden. Da der wichtigste Sicherheitsansatz darin liegt, ein Wireless-Netzwerk als ebenso wenig vertrauenswürdig wie das Internet anzusehen, sollte eine Gateway-Sicherheits-Appliance eingesetzt werden, die die Sicherheit der kabelgebundenen und der Wireless-Netzwerke zentral verwaltet und durchsetzt, sowie das nicht vertrauenswürdige Netzwerk vom internen Netzwerk trennt.

Auch wenn den neuesten Wireless-Sicherheitsstandards derzeit viel Aufmerksamkeit geschenkt wird, empfehlen wir die Verwendung bewährter Sicherheitstechniken und -verfahren, wie z.B. IPSec VPN. Denn die ausgereifte und bewährte Sicherheit von IPSec VPN garantiert Ihnen eine nachhaltige Investition in die Wireless-Sicherheit. Bei den neuen Sicherheitsstandards gibt es jedoch keine Garantie. Sie müssen sich im Laufe der Zeit erst noch bewähren.

Eine umfassende Firewall-Appliance mit zahlreichen integrierten Sicherheitsfunktionen und integrierter Wireless-Funktionalität ist die effektivste und effizienteste Möglichkeit, sowohl ein kabelgebundenes wie auch ein Wireless-Netzwerk absolut zuverlässig zu schützen. Diese Lösung bietet den größtmöglichen Schutz durch die Integration einer Firewall, VPN, Gateway-Virenschutz, Intrusion Detection, Intrusion Prevention und Content Filtering-Funktionen in einer einzigen Plattform.

Voneinander getrennt verwaltete, unabhängige kabelgebundene bzw. Wireless-Netzwerke wird es wohl nicht mehr lange geben. Wireless-Sicherheit muss sich in eine neue Richtung entwickeln – mit Lösungen, die kabelgebundene und Wireless-Netzwerke in einer kosteneffektiven, effizienten und hochsicheren Plattform vereinen. Nur derartig umfassende Lösungen können den Bedürfnissen und Anforderungen aller Netzwerkbenutzer und Netzwerkadministratoren gerecht werden.

©2005 SonicWALL, Inc. ist eine eingetragene Marke von SonicWALL, Inc. Andere in diesem Dokument erwähnte Produktnamen können Marken und/oder eingetragene Marken ihrer jeweiligen Hersteller sein. Spezifikationen und Beschreibungen können sich ohne vorherige Ankündigung ändern. wp_wireless_0805