IT@Intel-Whitepaper

Intel IT
Employee Hotspot
März 2014

„Mobile Employee Hotspot“ für die Konsumerisierung der IT

Sanjay Rungta
Senior Principal Engineer, Intel IT

Manish Dave
Staff Engineer, Intel IT

Roy Beiser
Network Specialist, Intel IT

Kurzübersicht

Die Konsumerisierung der IT und der geschäftliche Bedarf an breiter gefächerten Zugangsmöglichkeiten zum Netzwerk sind für Intel IT eine ständige Herausforderung. Die zunehmende BYOD-Verbreitung (Bring Your Own Device) bringt zusätzliche Probleme mit sich, da die Auswahl im Konsumsegment wächst, wie auch die Erwartungen der Mitarbeiter bezüglich der Netzwerkunterstützung.

Das „Employee Hotspot“-Wi-Fi-Netzwerk war anfangs hauptsächlich ein Vorteil für die Beschäftigten, hat sich jedoch als signifikanter Nutzen für das Unternehmen mit höherer Produktivität der Mitarbeiter und abnehmenden Kosten herausgestellt.

2005 implementierte Intel IT ein „Guest Internet Access Wi-Fi*“-Netzwerk, das es externen Mitarbeitern und Besuchern an den Standorten von Intel ermöglichte, mit ihren eigenen Geräten aus geschäftlichen Gründen auf das Internet zuzugreifen. Ende 2007 erlebte die Mobilgerätebranche mit den ersten Touchscreen-Smartphones einen grundlegenden Wandel und bis 2009 waren Smartphones unter den Mitarbeitern weit verbreitet, jedoch war mit ihnen kein Zugang zum firmeneigenen Wi-Fi-Netzwerk möglich. 2010 nahm Intel IT dann einen Hotspot-Dienst für Mitarbeiter („mobile Employee Hotspot“) in Betrieb, um deren private Mobilgeräte für den Internetzugang einzubinden. Was als Vorteil für die Beschäftigten begann, hat sich jedoch als signifikanter Nutzen für das Unternehmen mit höherer Produktivität der Mitarbeiter herausgestellt.

Wir gehen davon aus, dass die Mitarbeiter in Zukunft mehrere Mobilgeräte haben werden und dass die weitere technische Entwicklung bei den Geräten den Bedarf an Bandbreite und Vernetzungsmöglichkeiten erhöhen wird. Um dieser Nachfrage zuvorzukommen, haben wir den gesamten Employee-Hotspot-Dienst mit einem Overlay-Netz neu strukturiert, was die Umsetzung mit geringeren Kosten erleichtert. Beim neuen Overlay-Netz wird virtuelle Routing- und Forwarding-Technik verwendet, weshalb unsere bestehende Netzwerkinfrastruktur ohne zusätzliche Hardware genutzt werden kann. Die Vorteile dieses Konzepts sind:

- **Verbesserte Sicherheit und Skalierbarkeit:** Durch zusätzliche Ressourcen wie Application-Layer-Gateways, Cloud-basierte Proxys und Mobile Security können wir Bedrohungen schneller erkennen bzw. darauf reagieren und die Skalierbarkeit bei hoher Auslastung erhöhen.
- **Verbesserte Benutzerfreundlichkeit:** Nach der Einrichtung eines neuen Hotspot-Account-Managementsystems können die Mitarbeiter mühelos Mobilgeräte hinzufügen oder löschen und schnell ihre Passwörter aktualisieren.
- **Verbesserte Produktivität:** Dadurch, dass neue Funktionen für die Netzwerksicherheit hinzukamen, können wir den Zugang zu geschäftlichen Anwendungen wie Collaboration-Tools gestatten.
- **Reduzierte Kosten:** Durch die Nutzung unserer bestehenden Netzwerkinfrastruktur mithilfe des Overlay-Netzes sind keine eigenen Router erforderlich.

Mit der weiteren Anpassung unserer Strategie an die real stattfindende Konsumerisierung der IT wollen wir uns genauer ansehen, ob andere Dienste im Unternehmensnetzwerk und der Employee Hotspot in einem „konvergierten“ Overlay-Netz zusammengeführt werden können, um die Infrastrukturkosten weiter zu senken. Außerdem suchen wir nach Möglichkeiten, zur Steigerung der Produktivität von Mitarbeitern mehr Zugriff auf geschäftliche Anwendungen und Daten zu bieten und nach Wegen, die Sicherheit insgesamt und die Benutzerfreundlichkeit zu verbessern.

Inhaltsverzeichnis

IT@INTEL

Das IT@Intel-Programm bringt IT-Fachleute in aller Welt mit ihren Kollegen bei Intel zusammen, um Erfahrungen, Vorgehensweisen und Strategien auszutauschen. Unser Ziel: Darstellung bewährter Methoden und Strategien von Intel IT, die geschäftlichen Nutzen bringen und die IT des Unternehmens zu einem Wettbewerbsvorteil machen. Besuchen Sie www.intel.com/IT oder wenden Sie sich an Ihren Ansprechpartner bei Intel, wenn Sie mehr erfahren möchten.

HINTERGRUND

Die Konsumerisierung der IT und der geschäftliche Bedarf an breiter gefächerten Zugangsmöglichkeiten zum Netzwerk sind für Intel IT eine ständige Herausforderung. In der Vergangenheit konnten wir der Nachfrage mit dem Guest Internet Access (GIA) nachkommen, wobei externe Mitarbeiter und Besucher Zugang erhielten, solange sie sich am Standort aufhielten. Dem fügten wir ein „Employee Hotspot"-Wi-Fi*-Netzwerk hinzu, um Mitarbeitern den Zugang zum Internet mit ihren privaten Mobilgeräten zu ermöglichen. Die zunehmende BYOD-Verbreitung (Bring Your Own Device) wirft zusätzliche Probleme auf, da die Auswahl im Konsumsegment wächst, wie auch die Erwartungen der Mitarbeiter bezüglich der Netzwerkunterstützung.

Was ursprünglich als Vorteil für die Beschäftigten begann, nämlich beim Zugriff auf Dienste und Daten selbst wählen zu können, hat sich seither dank Kosteneinsparungen und höherer Produktivität der Mitarbeiter als signifikanter Vorteil für das Unternehmen erwiesen.

Guest Internet Access

Die 2003 eingeführte Intel® Centrino® Prozessortechnologie machte Mobile Computing mit umfassendem Netzwerkzugang möglich und weckte Erwartungen an eine konsistente Netzwerkanbindung privater, für geschäftliche Tätigkeiten genutzter Geräte. Intel hatte mehr als 30 000 externe Mitarbeiter, die im Lauf der Zeit Netzwerk- und Internetzugang brauchten, um ihre Aufgaben zu erledigen, sodass wir es zur Steigerung der Produktivität für notwendig hielten, sicheren Zugriff auf Onlineressourcen zu gestatten.

Um dieser entscheidenden geschäftlichen Notwendigkeit nachzukommen, richteten wir 2005 den „GIA" ein. Die Architektur für die Netzwerksicherheit, die das Netzwerk vor böswilligen Aktivitäten schützt, war damals nicht dafür ausgelegt, unbekannten, nicht registrierten Endgeräten den Zugang zu ermöglichen. Dieser Einschränkung begegneter wir unter anderem mit folgenden Maßnahmen:

- **Rechtliche Haftung:** Alle Besucher müssen die Nutzungsbedingungen und Richtlinien für den Umgang mit vertraulichen Daten (Acceptable Use Policy) akzeptieren, bevor sie Zugang erhalten.
- **Authentifizierung und Einrichtung von Benutzerkonten:** Ein neuer zentraler Dienst ermöglicht es den Gastgebern bzw. Verantwortlichen, temporäre, von selbst verfallende Benutzerkonten für Besucher anzulegen.
- **Zugangskontrollen:** Besucher erhalten über das Netzwerk Zugriff auf das Internet und VPN-Zugang zu ihren eigenen Standorten, aber nicht zum Intranet von Intel. Die Einhaltung von Vorgaben wie spezifischen Antivirus-DAT-Dateien und Patch-Versionen werden ebenfalls vor der Gewährung des Zugangs geprüft.

Während der ersten 24 Monate nach der Bereitstellung wurde „GIA" hauptsächlich für Auftragnehmer aktiviert, die den Werksausbau begleiteten. Dabei reisen die Außendienstmitarbeiter verschiedener Auftragnehmer zu einer einzelnen Intel-Anlage, um im ständigen Kontakt mit Technikerteams Zulassungen für Werkzeuge zu besorgen. Vor der GIA-Bereitstellung kehrten die Außendienstmitarbeiter häufig in ihre Hotels zurück oder nutzten öffentliche Angebote für den Internetzugang, um auf die Intranetdienste ihrer Firmenzentralen zuzugreifen, was einen Produktivitätsverlust bedeutete. Nach der GIA-Einrichtung berichteten 98 % der Außendienstmitarbeiter über Zeitersparnisse durch den vom Reinraum aus möglichen Zugriff auf ihre Intranet-Sites.

Mitarbeiter von Intel Sales and Marketing nutzten GIA auch, um die Wi-Fi-Fähigkeiten neuer Notebooks mit Intel Centrino Prozessortechnologie zu demonstrieren, die in den Sales-and-Marketing-Niederlassungen zur Verfügung standen.

Employee-Hotspot-Wi-Fi-Netzwerk 1.0

Nach der Einrichtung von GIA bemerkten wir einen wachsenden Bedarf an einem möglichen Internetzugang mit privaten Mobilgeräten. In den Jahren 2009 und 2010 stellten wir fest, dass die Zahl der Handheldgeräte, mit denen auf Dienste des Unternehmens zugegriffen wurde, um 94 % anstieg, und als Reaktion auf diesen zunehmenden geschäftsspezifischen Bedarf stellten wir den Employee Hotspot bereit.

Anders als bei GIA, bei dem es darum ging, Besuchern einen befristeten Zugang zu verschaffen, sollte der Employee Hotspot im Sinne von Intels „Great Place to Work"-Philosophie den Mitarbeitern den Vorteil eines persönlichen Internetzugangs mit Mobilgeräten bieten. Doch was als reine „nice-to-have"-Leistung für die Mitarbeiter begann, hat sich in eine Lösung verwandelt, die signifikante Produktivitätsvorteile für das gesamte Unternehmen ermöglicht.

URSPRÜNGLICHE EMPLOYEE-HOTSPOT-IMPLEMENTIERUNG

Merkmale der ursprünglichen Implementierung waren:

- **Infrastruktur:** Für die erste Implementierung des „Employee Hotspot" wurde eine Netzwerkarchitektur verwendet, die der von GIA ähnelte und uns folgende Möglichkeiten bot:
  - Isolierung des Hotspot-Datenverkehrs mittels VLAN-Technik
  - Strenge Sicherheitskontrolle
  - Nutzung der vorhandenen WAN-, DMZ- (Demilitarized Zone) und ISP-Netzwerkinfrastruktur

  VLANs wurden auf bestimmte Hotspot-SSIDs (Service Set Identifications) abgebildet und von einem eigenen Router am Ort des Hotspots über Generic-Routing-Encapsulation-Tunnel zum zentralen DMZ geroutet, wie in Abb. 1 gezeigt.
- **Sicherer Zugang:** Um den Schutz vor Schadsoftware und schädlichem Datenverkehr zu erhalten, filterten wir den Netzwerkdatenverkehr durch einen transparenten Proxy, der als Bridge zwischen DMZ-Hub-Router und der externen Firewall diente. Unter Verwendung eines modularen Zugangsmodells verbanden sich die Endgeräte mit dem Hotspot und führten die erforderliche Authentifizierung durch. Application-Gateways sorgten für die richtigen Profile auf Basis von Zugriffsebene und Steuerungsregeln.
- **Registrierung von Endgeräten und Benutzern:** Wie bei der GIA-Benutzerauthentifizierung benötigten wir von den Mitarbeitern eine Anmeldung und die Bereitstellung eines Netzwerk-Benutzerkontos für ihre privaten Geräte – ein Vorgang, bei dem sie rechtliche Bedingungen für den Netzwerkzugang akzeptieren mussten. Nachdem die Netzwerk-Benutzerkonten bereitgestellt waren, konfigurierten die Mitarbeiter die Wi-Fi-Profile auf ihren Geräten, worauf sich das jeweilige Gerät immer automatisch mit jedem Hotspot verband, sobald es in seiner Reichweite war. So konnten sich die Mitarbeiter automatisch an jedem Intel-Standort weltweit mit dem Netzwerk verbinden.

Diese drei Komponenten waren ein guter Anfang, doch neue Anwendungsfälle und die technische Weiterentwicklung brachten einige Probleme mit sich.

EMPLOYEE HOTSPOT 1.0 – PROBLEME

Als Mitarbeiter die IT-Umgebung durch neue Mobilgeräte erweiterten, stieg auch der Bedarf an Tools für geschäftliche Anwendungen auf diesen Geräten. Mitarbeitern den Zugriff auf entsprechende Dienste zu gestatten, kann dem Unternehmen Kosteneinsparungen und Produktivitätsvorteile bringen. Das ursprüngliche Employee-Hotspot-Design hatte Probleme und Beschränkungen, die seine Fähigkeit, künftigen Anforderungen zu genügen, beeinträchtigten:

- **Sicherheit:** Bei der ersten Implementierung stand die Bereitstellung von Internetzugang im Mittelpunkt und die Möglichkeiten, sicheren Zugriff auf interne Dienste des Unternehmens zu gewähren, zum Beispiel auf Social-Collaboration-Tools, die eine weitere Steigerung der Produktivität und der allgemeinen Nutzung des Angebots bewirken konnten, war begrenzt.
- **Benutzerfreundlichkeit:** Die Benutzer mussten sich ein Mal täglich authentifizieren und weil Benutzernamen oft Unterstriche enthalten, war das Einloggen mit manchen Geräten ein frustrierendes Unterfangen.
- **Skalierbarkeit.** Die lokalen dedizierten Router am Ort der Hotspots waren in ihrer Bandbreite begrenzt. Das Bandbreitenmanagement der älteren Infrastruktur, die ursprünglich für GIA eingerichtet und später dann für den Employee Hotspot verwendet wurde, war statischer Natur und konnte den Bandbreitenbedarf nicht dynamisch an den zu erwartenden Anstieg der Benutzung privater Endgeräte anpassen.
- **Agilität:** Neue Hotspot-Standorte mit dem ursprünglichen Modell online zu bringen, war zeitraubend, weil dort dann eine neue Netzwerkinfrastruktur nur für den Internetzugang installiert werden musste.
- **Aufwand:** Die dedizierte Netzwerktechnik an 120 Hotspot-Standorten erreichte das Ende ihrer Nutzungsdauer und erforderte neue Investitionen, wobei wir immer versuchen, unsere Netzwerkprojekte möglichst „Nullbudget" abzuwickeln.

Wir schauten uns jeden dieser Bereiche an und suchten nach Verbesserungsmöglichkeiten, wobei wir sofort die Probleme in puncto Sicherheit und Benutzerfreundlichkeit in Angriff nahmen. Um die im Betrieb auftretenden Probleme bezüglich Skalierbarkeit, Agilität und Kostenaufwand zu überwinden, begannen wir mit einer Überarbeitung der Lösung zum Employee Hotspot 2.0 (siehe unten).

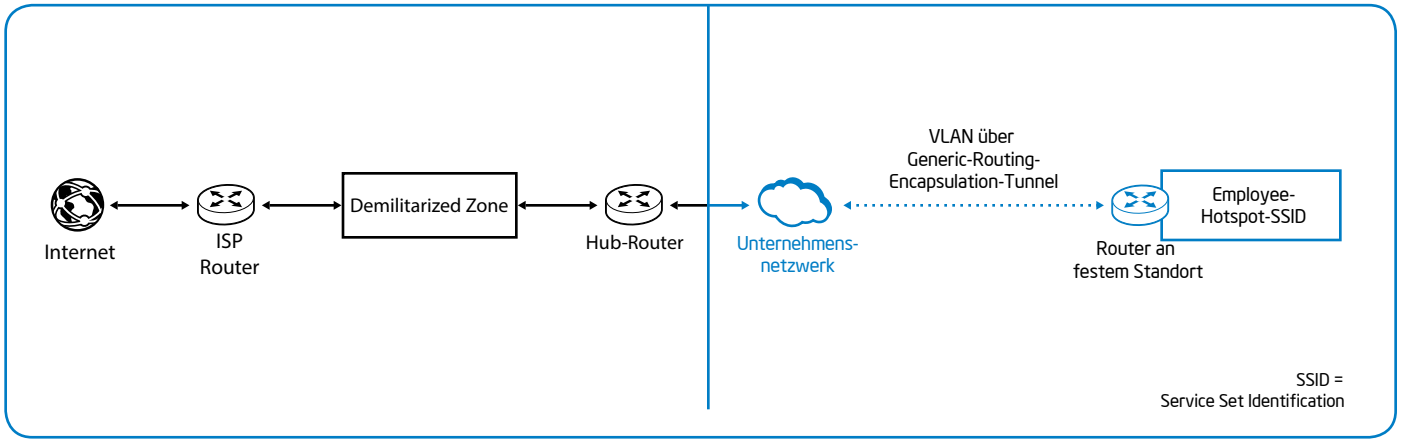

Abbildung 1: Bei der ursprünglichen Implementierung des Employee-Hotspot-Netzwerks wurde der Hotspot-Datenverkehr mittels VLAN-Technik und eigenen Routern am Ort der Hotspots isoliert.

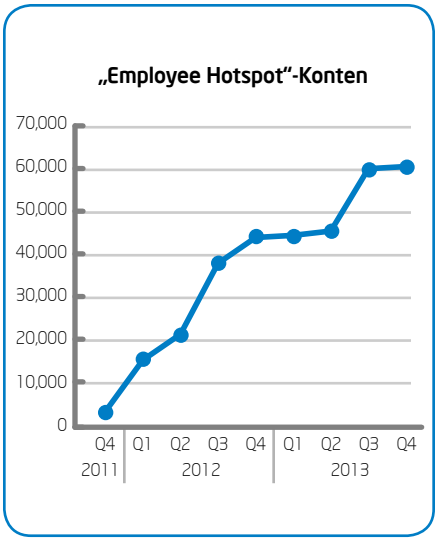

Abbildung 2: Die Zahl der Employee-Hotspot-Benutzerkontenstieg von 2011 bis 2013 signifikant.

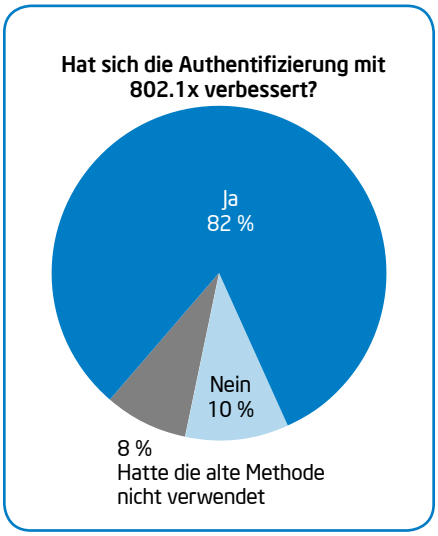

Abbildung 3: 82 % der befragten Nutzer gaben in der zweiten Umfrage der verbesserten Authentifizierung den Vorzug.

EMPLOYEE HOTSPOT 1.0 – VERBESSERUNGEN FÜR DIE AUTHENTIFIKATION UND DIE BENUTZERFREUNDLICHKEIT

Mit dem Ziel, die Nutzung des Angebots und Produktivität zu steigern, wollten wir die Benutzerfreundlichkeit des Employee-Hotspot-Dienstes und die Zufriedenheit der Mitarbeiter mit diesem Service insgesamt verbessern. Um das zu erreichen, nahmen wir mehrere Änderungen an den Prozessen für den Zugang mit Mobilgeräten vor, zum Beispiel durch Verbesserungen beim Rücksetzen des Passworts, die den Vorgang von einigen Stunden auf Minuten verkürzten. Ein neues System für die Verwaltung von Hotspot-Benutzerkonten präsentierte den Mitarbeitern ein einziges Portal für die Anmeldung, das Einloggen und das Verwalten des Lebenszyklus ihrer Mobilgeräte und der Dienste, die sie in Anspruch nehmen.

Weiterhin wechselten wir bei der Authentifizierung zu 802.1x, einem IEEE-Standard (Institute of Electrical and Electronics Engineers) für die Port-basierte Steuerung des Netzwerkzugangs mit einem Authentifizierungsmechanismus für Endgeräte, die an ein LAN oder WLAN angebunden werden müssen. Der Wechsel von der Web-basierten Authentifizierung zu 802.1x gestattete den Mitarbeitern, ihre Zugangsdaten in einem Wi-Fi-Profil auf jedem registrierten Endgerät zu speichern und sich im gesamten Unternehmen mit stets automatischer Verbindung zum Netzwerk zu bewegen.

Nachdem wir diese Änderungen vorgenommen hatten, befragten wir die Benutzer und erhielten positive Reaktionen. Außerdem wurde dieser Zugang nun häufiger genutzt (Abb. 2). Mehr als 93 % der Befragten gaben an, den Dienst weiter benutzen zu wollen. Weiterhin stellten wir fest, dass es keine negativen Auswirkungen auf die bestehende WLAN-Infrastruktur geben und sich die Belastung des dedizierten Netzwerks innerhalb akzeptabler Grenzen halten würde.

Eine zweite Umfrage kam zu folgenden Ergebnissen:

- Mehr als 95 % der Befragten sagten, sie würden den Dienst weiterhin benutzen.
- 82 % gaben der verbesserten Authentifizierung den Vorzug, wie in Abb. 3 gezeigt.
- Weniger als 1 % der Mobilgeräte wurden nicht unterstützt, wobei es sich hauptsächlich um ältere E-Reader handelte.

Diese vielversprechenden Ergebnisse zeigten uns, dass wir auf dem richtigen Weg waren und die Mitarbeiter den Hotspot-Service schätzten.

Neue Nutzungsmodelle

Nachdem die Zahl der privaten 2in1-Geräte und Tablets als Zweitgeräte für den Zugriff auf Unternehmens- wie auch auf persönliche Daten innerhalb des Unternehmens weiterhin steigt, gehen wir davon aus, dass die Mitarbeiter das Employee-Hotspot-Angebot immer häufiger nutzen werden. Während wir Verbesserungen vorsehen, um die bereits genannten betrieblichen Probleme bezüglich Skalierbarkeit, Agilität und Aufwand anzugehen, haben wir auch folgende aufkommende Nutzungsmodelle erkannt:

- **Mehrere Endgeräte pro Mitarbeiter:** Wir beobachten seit 2010 eine Zunahme von durchschnittlich 1,1 auf 1,4 Endgeräte pro Mitarbeiter und gehen davon aus, dass sich dieser Anstieg fortsetzen wird. Die Mitarbeiter möchten Geräte mühelos hinzufügen, ersetzen und verwalten können, und wir müssen dabei weiterhin die Netzwerksicherheit sicherstellen und dafür sorgen, dass die Netzwerkkapazität die Anforderungen mit effektiver Benutzerkontenverwaltung und -authentifizierung erfüllt.
- **Für das Geschäft benutzte private Geräte:** Dass private Endgeräte für den Zugriff auf Geschäftsdaten, wie Collaboration-Tools, Kalender, Sprachnachrichten und Video benutzt werden, bringt dem Unternehmen durch die erhöhte Produktivität der Mitarbeiter direkte Vorteile. Gegenwärtig erfolgt der Zugriff auf diese Anwendungen über das Internet durch die DMZ, was nicht so effizient funktioniert wie die Benutzung des Employee Hotspot.
- **Modernste Anwendungen für private Endgeräte.** Wir erwarten, dass neue Generationen von Endgeräten, wie Tablets und 2in1- Computer, im Gegensatz zum aktuellen Smartphone-Modell, bei dem offline gearbeitet wird und die Daten später synchronisiert werden, Verbindungen mit voller Bandbreiter gestatten. Der Employee Hotspot muss sich in diesem Szenario dynamisch an Spitzenauslastungen der Bandbreite anpassen können, ohne den vorhandenen geschäftlichen Datenverkehr zu unterbrechen.

Diese aufkommenden Nutzungsmodelle werden uns veranlassen, die Architektur weiter auszubauen.

ANPASSUNG UNSERES EMPLOYEE-HOTSPOT-WI-FI-NETZWERKS AN BYOD-TRENDS

Der Bedarf, für die Arbeit genutzte private Geräte (BYOD) mit dem Netzwerk zu verbinden, steigt und deshalb müssen wir unsere Netzwerkdienste weiterentwickeln. Mit einer neu entwickelten Architektur stellen wir Netzwerkfähigkeiten bereit, die den Mitarbeitern nicht nur geschäftlichen Nutzen bringen, sondern uns auch helfen, auf die nächste Welle der IT-Konsumerisierung vorbereitet zu sein und die Kosten zu begrenzen.

Ausgehend von den neuen Nutzungsmodellen beurteilten wir, inwiefern unsere gegenwärtige Netzwerkinfrastruktur Möglichkeiten bietet, Einrichtungen und Ressourcen mehrfach zu nutzen. Wie bei unseren früheren Installationen bot sich ein Overlay-Netz als beste Methode an, um die Kosten zu begrenzen. Wie zuvor baut auch unser neues Design auf der bestehenden WAN-Infrastruktur auf, benötigt jedoch keine eigenen Router mehr, was uns zusätzlich den Vorteil bietet, neue Hotspot-Standorte und Außenstellen schnell einrichten zu können.

Employee-Hotspot-Wi-Fi-Netzwerk 2.0

Momentan sind wir dabei, ein neues Modell umzusetzen, bei dem die GIA- und Employee-Hotspot-Dienste mit der vorhandenen LAN/WAN-Infrastruktur mittels eines Overlay-Netzes zusammengeführt werden. Mit einer neuen Routing- und Forwarding-Technik können wir die LAN- und -WAN-Router des Firmenstandorts verwenden und die bislang speziell für das GIA- und das Employee-Hotspot-1.0-Netzwerk eingesetzten Router entfernen. Abb. 4 illustriert die Overlay-Technik.

Dieser Ansatz bietet entscheidende Vorteile:

- **Reduzierte Kosten:** Dadurch, dass wir unser vorhandenes mehrschichtiges privates LAN/WAN nutzen können, entfällt die Notwendigkeit zusätzlicher Hardware an jedem Hotspot-Standort.
- **Möglichkeit, schnell neue Hotspots einzurichten:** Weil keine neuen Router benötigt werden, können wir neue globale Hotspot-Standorte in erheblich kürzerer Zeit online bringen.
- **Erhöhte Sicherheit:** Mit einer von Cloud-Dienstleistern bereits vielfach verwendeten Technik, die Netzwerkrouting-Instanzen voneinander isoliert, können wir die Sicherheit und die Trennung der Netze voneinander verbessern.
- **Verbesserte Ausfallsicherheit.** Wir verwenden zwei Netzwerkpfade von jedem Hotspot aus zu den zwei DMZ-Hubs, was eine Ausfallsicherung im Falle des Versagens eines DMZ-Hubs oder eines Endpunkts für den ausgehenden Internet-Datenverkehr darstellt.

Die folgenden beiden Abschnitte behandeln die Lösungsarchitektur und unseren Ansatz für die IT-Sicherheit genauer.

ARCHITEKTUR

Bei der neuen Architektur kommt eine virtuelle Routing- und Forwarding-Technik (VRF) zum Einsatz, um das Hotspot-Netzwerk den LAN- und WAN-Unternehmensnetzwerken zu überlagern, was eigene Router überflüssig macht. VRF ist eine Internetprotokoll-Technik (IP-Technik), die es ermöglicht, dass mehrere Instanzen einer Routingtabelle zur selben Zeit auf demselben Router existieren. Diese Methode bietet den zusätzlichen Vorteil höherer Sicherheit durch die vollständige Trennung der Routing-Instanzen, was in etwa dem entspricht, dass durch die Virtualisierung in Rechenzentren mehrere virtuelle Maschinen auf einem einzelnen Server unterstützt werden. Durch die Einrichtung mehrerer VRF-Instanzen auf den WAN- und LAN-Routern können wir sowohl den GIA- als auch den Employee-Hotspot unterstützen und dabei die sichere Isolation zwischen den Netzwerken aufrechterhalten.

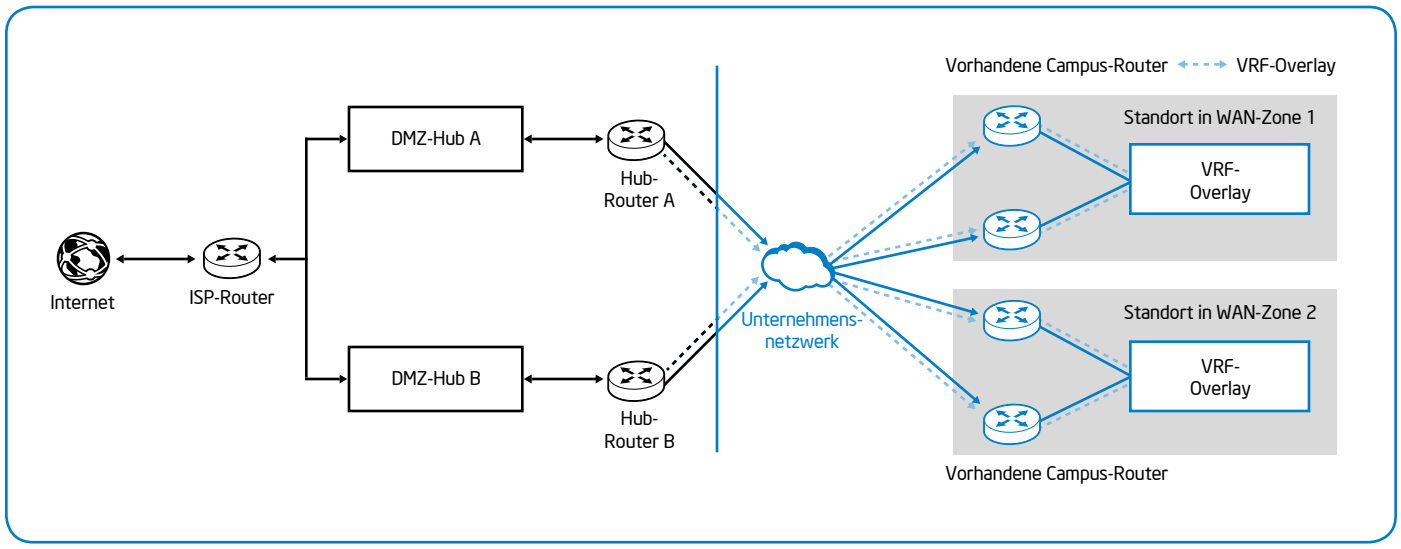

Abbildung 4: Für das Overlay-Netz mit virtuellem Routing und Forwarding (VRF) werden je zwei Netzwerkpfade zu zwei DMZs (Demilitarized Zones) genutzt, was die Ausfallsicherheit erhöht.

Entsprechend wird bei dieser Technik auch die vorhandene Infrastruktur für die Datenübertragung des neuen Netzwerkdiensts genutzt. Darüber hinaus werden mit dem neuen Design auch die DHCP-Server des Standorts (Dynamic Host Configuration Protocol) zur Verwaltung der Client-IP-Adressen von extern und intern bereitgestellten Diensten genutzt.

SICHERHEIT

Das neue Design bietet nun sichere Möglichkeiten, den Zugriff auf intern bereitgestellte Dienste zu gestatten, was die Produktivität für Mitarbeiter mit privaten Geräten verbessert. Ein modulares, zentrales Verwaltungssystem für Sicherheitsereignisse ermöglicht unserem Security-Operations-Team, Sicherheitsvorfälle schneller zu erkennen und zu bearbeiten (Abb. 5).

- Application-Layer-Gateways: Eingehender Datenverkehr wird durch feiner abgestufte Zugangskontrollen über anwendungsabhängig arbeitende Gateways wie Web-Application-Firewalls, Sicherheits-Gateways für Webdienste und Webportale für VPN-Verbindungen gefiltert.
- Cloud-basierte Proxys: Damit mehr Endgeräte und Anwendungen mit hohem Bandbreitenbedarf unterstützt werden, können Cloud-basierte Proxy-Filter die Dienste entsprechend skalieren, um die Anforderungen zu erfüllen. Dies gestattet außerdem die Einrichtung von Hotspot-Diensten an Stellen, von denen aus keine Backhaul-Verbindung zur DMZ besteht und der Hotspot-Datenverkehr stattdessen über einen lokalen ISP zum Cloud-Proxy-Dienst weitergeleitet wird.
- Mobile Security: Funktionen mit einem abgestuften Vertrauensmodell („Granular Trust") für die Verwaltung und Sicherheit von Mobilgeräten und mobilen Anwendungen legen in Abhängigkeit von der Person, die den Zugang anfordert, vom benutzten Endgerät, vom Standort und vom Zeitpunkt eine Reihe von strenger werdenden Einschränkungen fest.
- Voice over IP (VoIP) und Zusammenarbeit: Als Verbesserungen planen wir unter anderem, mit privaten Endgeräten VoIP und Lösungen für die Zusammenarbeit wie Videokonferenzen zu ermöglichen.

FAZIT

Das „Employee Hotspot"-Wi-Fi-Netzwerk war anfangs hauptsächlich ein Vorteil für die Beschäftigten, hat sich jedoch als signifikanter Nutzen für das Unternehmen mit höherer Produktivität der Mitarbeiter und abnehmenden Kosten herausgestellt.

Ausgehend von der GIA-Implementierung zur Verbesserung der Produktivität für Besucher und externe Mitarbeiter, die am Standort tätig sind, bis zur Einführung des Employee Hotspot, der den Mitarbeitern konsistenten Internetzugang mit ihren Mobilgeräten bietet, haben wir unsere Netzwerkarchitektur ständig weiterentwickelt, um den Anforderungen nachzukommen.

Das neue VRF-Overlay-Netz bietet den Mitarbeitern bessere Zugriffsmöglichkeiten auf Dienste mit privaten Endgeräten, erhöht die Sicherheit und Skalierbarkeit und gestattet uns, ein breiteres Spektrum von Diensten für geschäftliche Anwendungen anzubieten, die produktiveres Arbeiten ermöglichen. Overlay-Netze zu verwenden, erlaubt uns außerdem, die sowieso schon vorhandene Netzwerkhardware zu benutzen, was die Kosten auf ein Minimum beschränkt.

Das neue Design und die Pilotinstallation befinden sich in der Endphase und wir werden das GIA- und Employee-Hotspot-Zugangsnetz im gesamten Unternehmen auf das Overlay-Netz umstellen. Wir gehen von einem Abschluss des Vorhabens noch in diesem Jahr aus und werden in den kommenden Monaten Sprach- und Videodienste für die elektronische Zusammenarbeit über den neuen Employee Hotspot bereitstellen und Mitarbeitern gestatten, Endgeräte ihrer Wahl für mehr geschäftliche Anwendungen als bisher zu verwenden.

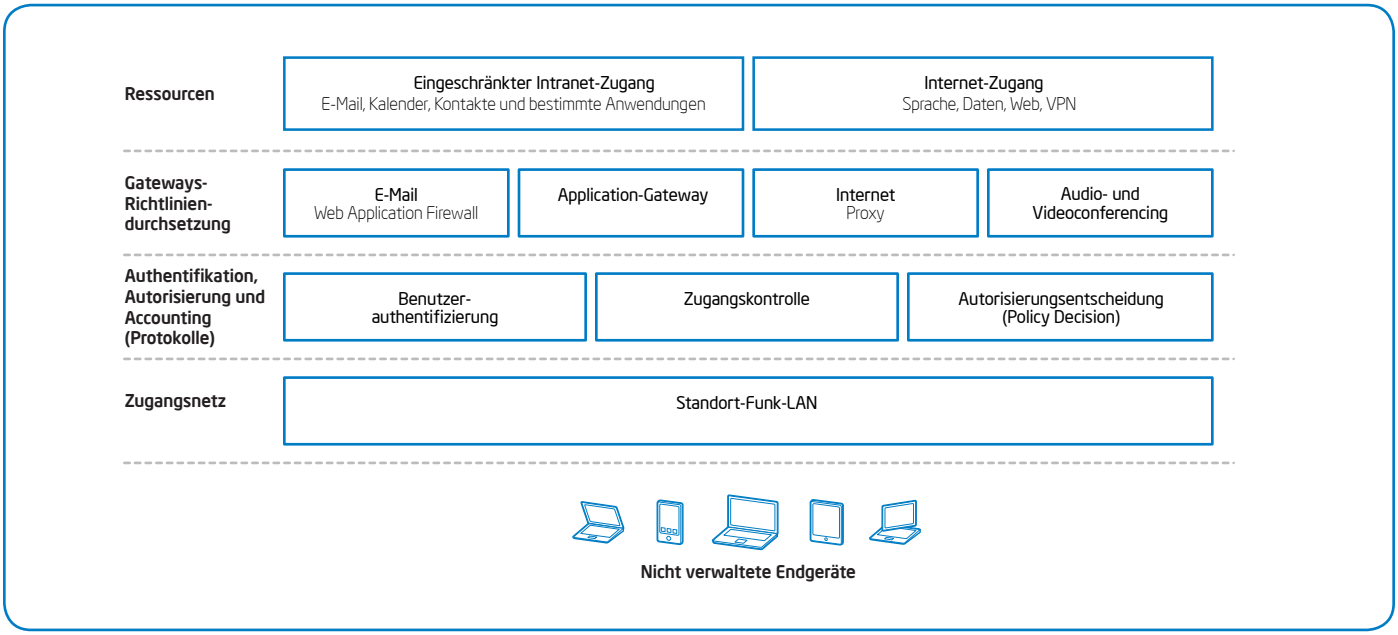

Abbildung 5: Die modulare Architektur der Zugangskontrolle ermöglicht den sicheren Zugriff auf geschäftliche Daten.

Im Zuge der Weiterentwicklung unserer Strategie und um uns der Realität einer Konsumerisierung der IT zu stellen, werden wir uns damit befassen, ob andere Dienste im Unternehmensnetzwerk und der Employee Hotspot in einem „konvergierten" Overlay-Netz zusammengeführt werden können, um die Infrastrukturkosten weiter zu senken. Wir werden auch in Zukunft Möglichkeiten wahrnehmen, zur Steigerung der Produktivität von Mitarbeitern mehr Zugriff auf geschäftliche Anwendungen und Daten zu bieten und beim weiteren Voranschreiten der „Konsumerisierung" in unserer IT-Umgebung die Sicherheit insgesamt und die Benutzerfreundlichkeit zu verbessern.

WEITERE INFORMATIONEN

Auf www.intel.com/IT finden Sie Inhalte zu verwandten Themen:

- „Eine Roadmap für die Verbindung von Smartphones mit dem Intel-Wi-Fi*-Netzwerk"
- „Neun Dinge, die Sie im Bereich eines Wi-Fi-Hotspots vermeiden sollten"

Mehr über Erfolgsmodelle von Intel IT erfahren Sie unter www.intel.com/IT.

VERFASSER

Todd Butler
Product Line Manager

Chandra Chitneni
Staff Network Engineer

Neil Doran
Program Manager

Dick Freeman
Senior Network Engineer

Avigail Garti
Network Engineer

Kevin Heine
Senior Network Engineer

Chris Steenkolk
Network Engineer

ABKÜRZUNGEN

BYOD	Bring Your Own Device
DMZ	Demilitarized Zone
FSE	Vertriebsingenieur Außendienst (Field Sales Engineer)
GIA	Guest Internet Access (Internet-Gastzugang)
IP	Internetprotokoll
ISP	Internet-Service-Provider
SSID	Service Set Identification/ Identifier
VoIP	Voice over IP
VRF	Virtual Routing and Forwarding

Look Inside.™