The Volkswagen of America (VWoA) and Cisco VPN Solution: **Drivers Found**

VOLKSWAGEN, A.G., IS A GLOBAL INDUSTRIAL POWERHOUSE. BASED IN WOLFSBURG, GERMANY, VWAG IS THE THIRD LARGEST AUTOMAKER IN THE WORLD AND ITS PRODUCTS ARE THE TOP SELLERS IN EUROPE TODAY. THE VW GROUP INCLUDES SOME OF THE MOST IMPORTANT AND EXCITING AUTOMOBILE LEGENDS IN THE WORLD—FROM LUXURY RIDES LIKE BENTLEY AND ROLLS ROYCE AND THE EXOTIC HIGH-PERFORMANCE CAPABILITIES OF PORSCHE, LAMBORGHINI AND BUGATTI, TO THE GREAT GLOBAL PEOPLE MOVERS, AUDI, VW, AND VW TRUCKS.

While VW cars are the driving choice for millions throughout the world, what drives VW is information. To stay in the business forefront, to get the right products to market, and to maintain a highly successful global organization, VWAG has created a wholly-owned, world-wide subsidiary to meet its IT needs: gedas. Owned and grown out of the VW family, gedas is the center for VW's global information needs.

Secure and Cost-effective Communications: the gedas, Inc. North America Challenge

gedas was founded in 1983, and has 3400 employees in 36 locations worldwide. gedas, Inc. was formed in the US in June, 1999, is the newest member of the gedas family. Because of VW's global, extended nature, one of the first challenges that gedas, Inc., needed to solve for Volkswagen of America (VWoA) was that of secure remote business access.

> **"We were providing 800 services for our dial-up users, and it is horrendously expensive."**
>
> ***Elliot Zeltzer***
>
> ***Telecommunications and Network Services Manager***
>
> ***gedas, Inc.***

Business Drivers and Technical Challenges

VWoA's success ushered in a whole new set of communication demands from a growing user and vendor base. In the end, gedas, Inc., had to reconstruct, and actually deconstruct, their infrastructure from the bottom up.

The RAS Question

The base of corporate remote users, historically supported by a costly 800-number remote access system (RAS), was growing geometrically. Anyone on the corporate staff who had a laptop could call in—members of the sales force, management, account executives, remote regional managers—constituting a fast-growing remote user community.

To meet the needs of the remote community, gedas knew they had to increment capacity, but every increment to RAS capacity, including modems and network services, requires additional capital investment. Growing numbers of modem banks also incur additional management and headcount to support frequent software changes and correct configurations. But all of this investment and effort couldn't meet the demands of the remote community. Users continued to experience problems with modem speeds and disconnects. Managing the dial environment had become a significant strain on VW resources.

Elliot Zeltzer, Telecommunications and Network Services Manager for gedas, Inc., explained it this way: "Anything outside the building is also outside of our control

and we needed to re-gain control! What forced us to look at dial was this: we just couldn't keep chasing modem capacity and cost. We were providing 800 services for our dial-up users, and it is horrendously expensive. And as user quantities continued to grow, and as connect times got longer, we just couldn't sustain the cost of connecting these folks and then leaving them connected for eight hours. So, one of our most significant challenges was the high cost of RAS: scaling the remote users, the lead time for added capacity, the added hardware, and getting the ISDN lines configured."

The Need to Connect to Vendors—Flexibly

One of VWoA's most important business resources is the extranet that communicates with their growing pool of vendors and suppliers. But VWoA found that building extranet connections required a separate infrastructure of firewalls, and all of the other nuances of adding additional resources into an enterprise network.

VWoA, like any other business, found many issues to resolve when connecting separate, outside businesses. Along with the long lead times to set up each new partner, at the end of the vendor relationship, each custom connection needed to be disconnected. The infrastructure investment would be lost.

Security Challenges

Because of VWoA's prominence in the marketplace, and the fact that they understand the value of their internal communications and intellectual properties, all network sessions had to be protected from the dangers of hacking. To meet this need, and the requirements of internal auditors, they had used a variety of cumbersome encryption mechanisms that forced additional capital investment and additional management layers onto the network infrastructure.

Many Challenges: A Single Solution—VWoA's Virtual Private Network

Mr. Zeltzer, and his team of network designers, looked at the challenges they faced: a growing remote user base, the high cost of scaling remote infrastructure, the difficulty of adding and separating external vendors from their private infrastructure, and the encrypted communications requirements. A virtual private network (VPN) looked like it could solve all of the problems at the same time.

The VPN solution promised many benefits: no more modems (!) and connecting through local ISPs would greatly reduce the complexity of remote access. Migrating to an Internet-based solution would drive down the costs of both 800 number access and the creation of additional private infrastructure. At the same time, they could provision vendor connectivity anytime, anywhere—connecting and disconnecting external vendors became fast and easy. Bandwidth could be driven by the applications running over the VPN connection—and VPNs can run over a broad variety of transport mediums: analog, ISDN, T1, Digital Subscriber Line (DSL), and cable modem.

Picking the Winning Solution and Provider

After analysis, the gedas team identified what applications, groups, services and technologies the VPN had to support: remote users, vendor partners, encryption of remote links and sessions, and internal pools of interest (internal groups with a need for closed networked communications—for example, consultants or departments.) Broadband connectivity support, including DSL and cable, was also important.

Support for mission critical applications was paramount in their minds. When substituting a RAS solution with a dial connected VPN solution, they still had to support mission critical applications. To do that, they contracted with the same vendor already providing their Internet service, to ensure the same level of service-level agreement (SLA)— and, to ensure that what had to get done (payroll, for example) would get done, no matter what.

They also determined their criteria for the right VPN partner and solution. The right partner had to be a "tier 1" supplier. That supplier had to have a solution that would terminate all tunnel types, including Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (LT2P), L2TF and IPsec. The solution also had to support TACACS+ and Radius, and had to supply a graphic user interface (GUI) administrative interface. Complete fault tolerance and high performance (wire speed was the minimum) were also on the list of "must-haves."

Lastly, VWoA needed to be ISP independent. Whatever VPN solution they put in place needed to be self-contained and transport independent, to give VWoA the broadest set of communications options and the flexibility they needed to respond to many different needs.

In short, the supplier of the VPN solution had to have it all—and more!

The Cisco VPN Solution

In the end, there was only one provider and one solution that met all of VWoA's needs: Cisco, and the Cisco VPN 3000 Series Concentrator. VWoA chose the Cisco VPN 3060 model. The 3060 provided scalable aggregation for enterprise-class deployment and central site aggregation of single user and remote office connections—the right solution for both individual users and vendors. VWoA required termination of up to 5000 concurrent sessions, and the Cisco VPN 3060 Concentrator could meet those needs—without impacting performance. "Even running triple DES encryption," according to Mr. Zeltzer, "we have found no performance penalty running the Cisco VPN solution."

The other half of the Cisco VPN 3000 solution is an integrated VPN client that guarantees secure, end-to-end, encrypted traffic capabilities. Any party—remote individuals, remote offices, or vendor partners—needs only to install the software client to become part of VW's extended, secure infrastructure. Policy dictates access and privileges. Each session is secure, and once a session is over, there are no traces left—no infrastructure or modem pool to support. Tunneling over the public Internet takes the place of expensive RAS and private network infrastructure solutions.

The Cisco VPN 3000 also offers a Web-based, management architecture by providing GUI-based tools for simplified installation, configuration and monitoring. Mr. Zeltzer added: "The installation was so easy, that we had our 3000s up and running in just three hours!"

Over the public Internet, or over a variety of other network links, including a dial solution over the Public Switched Telephone Network (PSTN), the VPN client connects users to the VW infrastructure, securely, enabling them to do their jobs.

Cisco VPN Benefits for VWoA

VWoA's VPN strategy has brought tremendous benefits. Migrating from a RAS, 800 number solution to a low-cost IPS-based solution with encrypted tunnels has dropped the price of remote connectivity by 88 percent. Scaling this solution is infinitely simpler, because it relies on a software client, and is connection medium-neutral, accepting DSL, cable, and dial.

Sending VPN client software over the network means that bringing suppliers in on very short notice is a snap. All they need is an Internet connection. At the end of the vendor relationship, VWoA can disconnect by taking their privileges away. No more slow, infrastructure-heavy, VLAN connections. The VPN solution gives VWoA greater agility than ever before.

From an audit perspective, the Cisco VPN solution meets its security needs. All sessions are triple DES encrypted—safely extending VWoA's infrastructure wherever it needs to be to meet business needs.

Cisco VPN Is the Right Solution for Growing Enterprises

VWAG is a growing global enterprise, and a prominent member of the Fortune Global 20. It needs flexible, 21st century communications solutions to maintain its competitive advantage, and the secure VPN solution from Cisco is one of them.

But enterprises of all sizes can benefit from Cisco know-how and the 3000 series of VPN concentrator and remote access solutions. If you want to know more about how VPN solutions and the Cisco 3000 series can meet your business's remote access and security challenges, visit http://www.cisco.com/go/evpn

Turbonium: Securing the Newest Element on the Planet

Sources in the scientific community have recently reported the discovery of the newest addition to the periodic table of elements: turbonium. Turbonium's significant properties include its speed and its green color. These properties are especially evident in the newest VW Beetle. Members of the scientific community have communicated the news about turbonium through the turbonium Web site: www.turbonium.com. Not only can visitors learn about this important new element, but they can configure and purchase their new turbonium VW Beetle, on line, at the same time!

Because VWoA is supported by a Cisco Enterprise Network, the turbonium Web site, along with the rest of VWoA's Web site and eCommerce infrastructure are protected by the award-winning Cisco Secure PIX Firewall. The Cisco Secure PIX monitors all Web traffic for appropriate controls, guaranteeing security for both VW and the customers who choose to visit and to shop on their site. Remember, while your turbonium VW Beetle mileage may vary, your www.vw.com experience will be secure.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems Europe
11, Rue Camille Desmoulins
92782 Issy Les Moulineaux
Cedex 9
France
www.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems Australia, Pty., Ltd
Level 17, 99 Walker Street
North Sydney
NSW 2059 Australia
www.cisco.com
Tel: +61 2 8448 7100
Fax: +61 2 9957 4350

Cisco Systems has more than 190 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the Cisco.com Web site at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Canada • Chile • China • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE
Finland • France • Germany • Greece • Hong Kong • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia
Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Singapore
Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela

08/00 BW6532