Call-Back Security Helps Prevent Unauthorized Access

Perle’s 833AS Access Server Replaces Cisco at Dutch Hospital

The Challenge:
The CUSTOMER:
St. Radboud University Hospital, in Holland, operates as a patient care facility and a very successful medical research and education faculty. Closely associated with the University of Nijmegen, St. Radboud has earned a reputation for the newest and most advanced treatments given in fields, such as bone marrow transplant, microsurgery and child care.

THE CHALLENGE:
Until recently, St. Radboud relied on a Cisco Access Server, with analog modem support, to provide hospital staff with remote dial-in access. This service, which depended on the University of Nijmegen’s network, gave employees access to the Internet and the hospital’s LAN from home offices. As more staff started to use this service, it became increasingly apparent that the Cisco Access Server was not a long-term solution. Henk Coenen, head of St. Radboud’s Computer and Communications Department, wanted to make use of the Cisco server’s call-back facility in combination with ISDN support but, despite repeated efforts, the University IT department was unable to configure the server to provide a reliable call-back service. Call-back was particularly important to Coenen because patient information needed to be kept confidential and could not be jeopardized as a result of providing remote user access.

The Solution:
The CUSTOMER:
St. Radboud University Hospital, in Holland, operates as a patient care facility and a very successful medical research and education faculty. Closely associated with the University of Nijmegen, St. Radboud has earned a reputation for the newest and most advanced treatments given in fields, such as bone marrow transplant, microsurgery and child care.

THE CHALLENGE:
Until recently, St. Radboud relied on a Cisco Access Server, with analog modem support, to provide hospital staff with remote dial-in access. This service, which depended on the University of Nijmegen’s network, gave employees access to the Internet and the hospital’s LAN from home offices. As more staff started to use this service, it became increasingly apparent that the Cisco Access Server was not a long-term solution. Henk Coenen, head of St. Radboud’s Computer and Communications Department, wanted to make use of the Cisco server’s call-back facility in combination with ISDN support but, despite repeated efforts, the University IT department was unable to configure the server to provide a reliable call-back service. Call-back was particularly important to Coenen because patient information needed to be kept confidential and could not be jeopardized as a result of providing remote user access.

The Solution:
As a result of a cold call from Perle, Henk Coenen discovered the Perle 833AS Access Server; a scalable solution that could provide the reliable call-back he was looking for, as well as both ISDN and analog/DSP modem support.

Security & Accountability
The call-back user authentication feature on the Perle 833AS requires a dial-in user to type a log-on ID and password. The connection is then broken and the user is automatically called back at a pre-configured number. This added security measure helps prevent unauthorized access, even if an individual’s log-on ID and password have been stolen. The feature would also allow Coenen to track individual dial-in usage and attribute the running costs of Internet access to the appropriate hospital departments.

The Benefits:
The comprehensive and robust call-back security offered by the Perle 833AS means that confidential patient information is protected from unauthorized remote access.

The Challenge:
St. Radboud had relied on a Cisco Access Server, with analog modem support, for remote dial-in access but this solution proved unable to deliver reliable call-back security in conjunction with new ISDN connections that were being implemented.

The Solution:
The University Hospital chose the Perle 833AS Access Server as a scalable solution to provide reliable call-back as well for both ISDN and analog/DSP modem users.

The Benefits:
The comprehensive and robust call-back security offered by the Perle 833AS means that confidential patient information is protected from unauthorized remote access.

THE CUSTOMER:
St. Radboud University Hospital, in Holland, operates as a patient care facility and a very successful medical research and education faculty. Closely associated with the University of Nijmegen, St. Radboud has earned a reputation for the newest and most advanced treatments given in fields, such as bone marrow transplant, microsurgery and child care.

THE CHALLENGE:
Until recently, St. Radboud relied on a Cisco Access Server, with analog modem support, to provide hospital staff with remote dial-in access. This service, which depended on the University of Nijmegen’s network, gave employees access to the Internet and the hospital’s LAN from home offices. As more staff started to use this service, it became increasingly apparent that the Cisco Access Server was not a long-term solution. Henk Coenen, head of St. Radboud’s Computer and Communications Department, wanted to make use of the Cisco server’s call-back facility in combination with ISDN support but, despite repeated efforts, the University IT department was unable to configure the server to provide a reliable call-back service. Call-back was particularly important to Coenen because patient information needed to be kept confidential and could not be jeopardized as a result of providing remote user access.

THE SOLUTION:
As a result of a cold call from Perle, Henk Coenen discovered the Perle 833AS Access Server; a scalable solution that could provide the reliable call-back he was looking for, as well as both ISDN and analog/DSP modem support.

www.perle.com