NCP

SECURE COMMUNICATIONS

Branch Office Networking

Technical Paper

high security remote access

Network
Communications
Products engineering

USA:

NCP engineering, Inc.
444 Castro Street, Suite 711
Mountain View, CA 94041
Tel.: +1 (650) 316-6273
Fax: +1 (650) 251-4155

Germany:

NCP engineering GmbH
Dombuehler Str. 2
D-90449 Nuremberg
Tel.: +49 (911) 9968-0
Fax: +49 (911) 9968-299

Internet

http://www.ncp-e.com

Email

info@ncp-e.com

Support

NCP offers support for all international users by means of Fax and Email.

Email Addresses

helpdesk@ncp-e.com	(English)
support@ncp-e.com	(German)

Fax

+1 (650) 251-4155	(USA)
+49 (911) 9968-458	(Europe)

When submitting a support request, please include the following information:

- exact product name
- serial number
- version number
- an accurate description of your problem
- any error message(s)

Copyright

While considerable care has been taken in the preparation and publication of this manual, errors in content, typo-graphical or otherwise, may occur. If you have any comments or recommendations concerning the accuracy, then please contact NCP. NCP makes no representations or warranties with respect to the contents or use of this manual, and explicitly disclaims all expressed or implied warranties of merchantability or suitability of use for any particular purpose.
Furthermore, NCP reserves the right to revise this publication and to make amendments to the contents, at any time, without obligation to notify any person or entity of such revisions or changes. This manual is the sole property of NCP and may not be copied for resale, commercial distribution or translated to another language without the express written permission of NCP engineering GmbH.
All trademarks or registered trademarks appearing in this manual belong to their respective owners.

© 2014 NCP engineering GmbH, All rights reserved.

What is required for secure and efficient networking of branch offices and the company headquarters?

A site-to-site VPN is used to connect independent networks, for example, for branch office networking. In most cases this means that the branch office networks are connected to the network of the company headquarters. Another possibility is machine-to-machine (M2M) networking. In this case it is machines that communicate with the central gateway. In all cases VPN gateways are used. They establish a connection to the Internet, then they encode and authenticate the IP user data for transmission and tunnel it through the Internet. IPsec is the VPN protocol that is most frequently used for these types of connection.

This article discusses aspects of branch office networking that are frequently disregarded during planning or extending site-to-site VPNs. However, these aspects cause problems none the less.

Types of networks

Meshed or star-shaped networks are the two options for branch office networking. With meshed networks, the branch offices are not only connected to the headquarters but also amongst each other. With star-shaped networks, however, all communication between the branch offices is channeled through one central VPN gateway. This results in higher latency in communication between the branch offices. However, a clear advantage of star-shaped networks is that IT administrators control the whole network via one central monitoring system. Hence, star-shaped networks allow for real time detection and locating communication faults between the branch offices. However, this requires a central VPN management system. Should communication faults occur in the crosslinks of a meshed network, however, locating them is much more difficult. If a network, for example, contains 100 branch offices, controlling this network would cause substantial extra effort.

High Availability

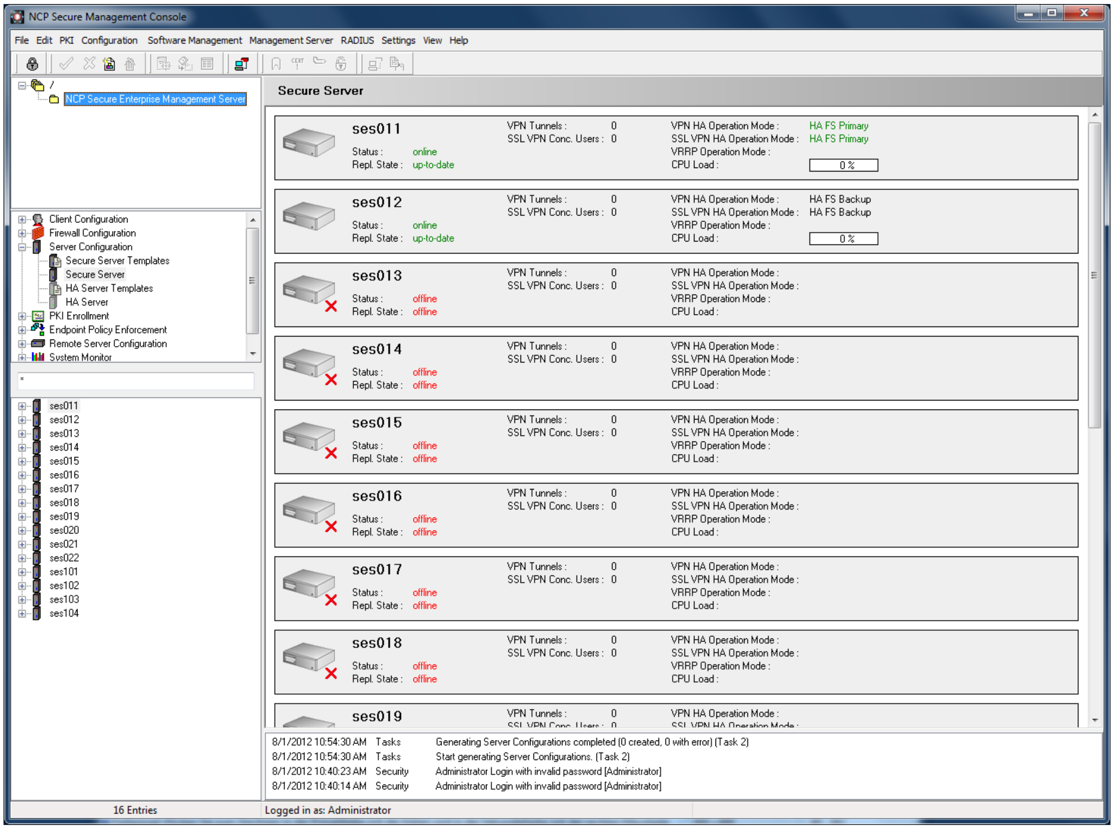
The criteria of availability differ, depending on which branch offices are connected to the main network. This means high availability has to be guaranteed for branch offices which must not break down; common examples are branch offices of banks and their ATM's or checkout systems of retail chains. In order to guarantee high availability, professional VPN systems support several backup systems.

Monitoring the VPN connection is a basic requirement for being able to carry out backups. One method of connection monitoring is DPD (Dead Peer Detection- RFC). On top of that, the VPN gateway of the branch office should support several alternative media types (communication mediums) for Internet dial up. The VPN solution should be able to automatically recognize a communication fault with a remote side. If it does, the VPN gateway disconnects the standard connection automatically a sets up an alternative backup link. Most modern VPN software solutions support infinite backup connections. With these solutions, the restricting factor is the number of communication mediums the hardware supports.

Central Management

A central VPN management system is required for effective networking of branch offices. Even if there are only a few branch offices, the time and money that has to be spent on local network administration is out of proportion. With M2M, such kind of administration this is hardly possible.

Central management automates management of remote / branch office VPN gateways. The more VPN relevant systems the central management contains, the simpler and more manageable the network becomes for administrators. Apart from configuration and software update management the following tasks should be included into the management software, too: management of digital software or hardware certificate (CA) rollout, an LDAP console for identity and rights management as well as security monitoring of the end-devices (Network Access Control / Endpoint Security).



ses011
Status : online
Repl. State : up-to-date
VPN Tunnels : 0
SSL VPN Conc. Users : 0
VPN HA Operation Mode : HA FS Primary
SSL VPN HA Operation Mode : HA FS Primary
VRRP Operation Mode :
CPU Load : 0 %

ses012
Status : online
Repl. State : up-to-date
VPN Tunnels : 0
SSL VPN Conc. Users : 0
VPN HA Operation Mode : HA FS Backup
SSL VPN HA Operation Mode : HA FS Backup
VRRP Operation Mode :
CPU Load : 0 %

ses013
Status : offline
Repl. State : offline
VPN Tunnels : 0
SSL VPN Conc. Users : 0
VPN HA Operation Mode :
SSL VPN HA Operation Mode :
VRRP Operation Mode :
CPU Load :

ses014
Status : offline
Repl. State : offline
VPN Tunnels : 0
SSL VPN Conc. Users : 0
VPN HA Operation Mode :
SSL VPN HA Operation Mode :
VRRP Operation Mode :
CPU Load :

ses015
Status : offline
Repl. State : offline
VPN Tunnels : 0
SSL VPN Conc. Users : 0
VPN HA Operation Mode :
SSL VPN HA Operation Mode :
VRRP Operation Mode :
CPU Load :

ses016
Status : offline
Repl. State : offline
VPN Tunnels : 0
SSL VPN Conc. Users : 0
VPN HA Operation Mode :
SSL VPN HA Operation Mode :
VRRP Operation Mode :
CPU Load :

ses017
Status : offline
Repl. State : offline
VPN Tunnels : 0
SSL VPN Conc. Users : 0
VPN HA Operation Mode :
SSL VPN HA Operation Mode :
VRRP Operation Mode :
CPU Load :

ses018
Status : offline
Repl. State : offline
VPN Tunnels : 0
SSL VPN Conc. Users : 0
VPN HA Operation Mode :
SSL VPN HA Operation Mode :
VRRP Operation Mode :
CPU Load :

ses019
VPN Tunnels : 0
SSL VPN Conc. Users : 0
VPN HA Operation Mode :
SSL VPN HA Operation Mode :

```
8/1/2012 10:54:30 AM   Tasks      Generating Server Configurations completed (0 created, 0 with error) (Task 2)
8/1/2012 10:54:30 AM   Tasks      Start generating Server Configurations. (Task 2)
8/1/2012 10:40:23 AM   Security   Administrator Login with invalid password [Administrator]
8/1/2012 10:40:14 AM   Security   Administrator Login with invalid password [Administrator]
```

16 Entries
Logged in as: Administrator

Image 1: Multiple VPN Management Console

A VPN system secures all data transfers in an encrypted tunnel. However, sealing of the communication has to take place as early as Internet dial up, which is the most frequent point of vantage of hacker attacks. The core problem is how the branch offices authenticate towards the central gateway. One possibility for authentication are pre-shared keys, another is the use of certificates. For security reasons certificates are the better option, because they can be adapted. This means old certificates can be locked and new ones can be issued.   Certificate handling has to be organized; i.e. if one certificate expires, the VPN management should offer automatisms that request and issue new certificates.

At times, a further security requirement is simply overlooked: The firewall must only allow IPsec connections. Usually branch offices connect to the Internet via a DSL router. This router protects the VPN gateway. Some VPN gateways also support the communication medium PPPoE. This means, the gateway can directly be used for DSL dial-up and a DSL router becomes obsolete. In this case, too, the firewall must only allow IPsec connections. Maintenance of the branch offices' VPN gateway can also be possible by direct dial up via ISDN - not via the Internet.

Masking

Administrators frequently demand access to all end-devices. They either want to access them from the headquarters or from the management system. Their demand is legitimate from their point of view. On the other hand it is easier to exclude the branch offices' IP networks and to mask them for communication with the headquarters. Masking means, they are hidden behind an address. However, these two demands contradict each other.

If administrators have to access all branch office networks transparently, it is essential that each branch office network receives its own, unique IP address range (if it does not have one, yet). At the same time, this means that all installed routers and end-devices have to be configured again. This might be feasible for small networks, however, in larger network environments time and money IT administrators have to spent on this task is enormous. The administrator has to take care that the corresponding routes are known at the central side. Some VPN gateways dynamically publish the routing information, when a connection is set up.

If transparent access is not absolutely essential, masking the IP addresses via Network Address Translation (NAT) is a viable solution. This means, the IP address is changed into a VPN tunnel IP address, which the host or the central VPN management system recognizes and automatically allocates to the branch office – not to the end-device. This significantly reduces time and money spent on configuration and rollout.

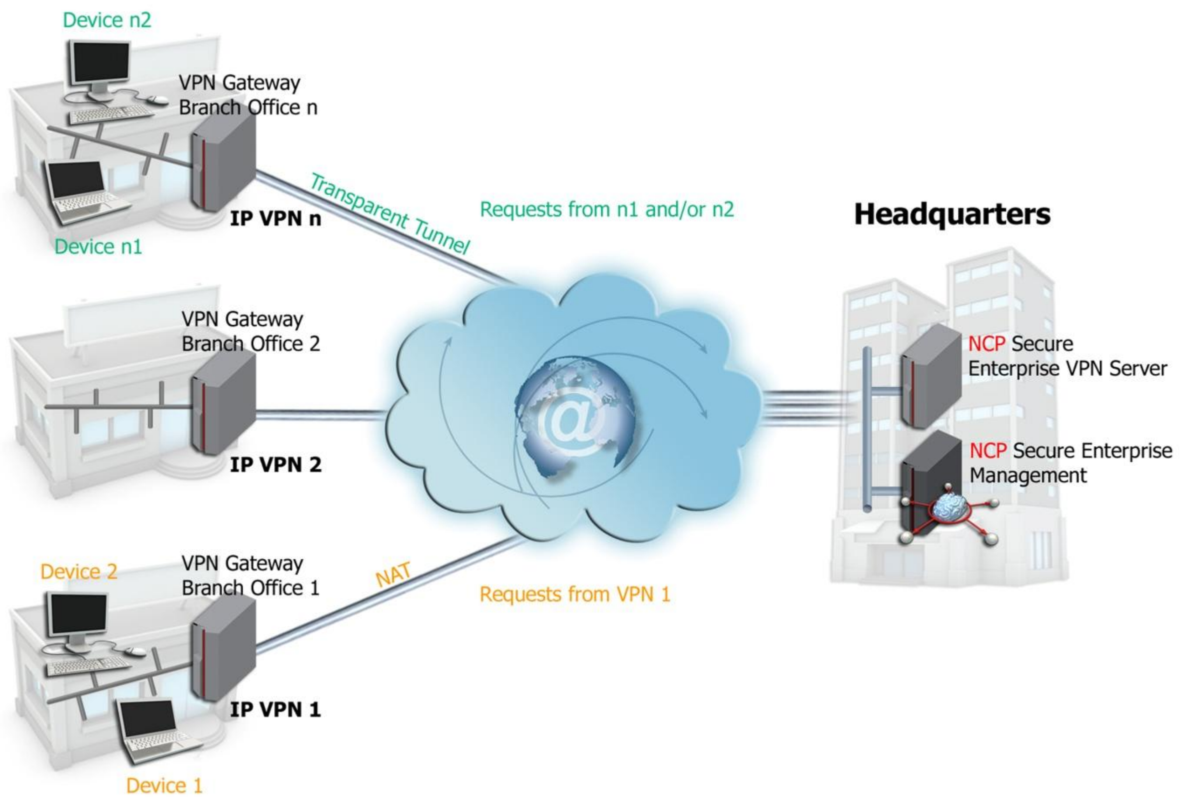


Image 2: Masking (NAT) or transparent branch office access

This means, companies have to choose between masking and access to all end-devices. The latter comes with increased administration effort for the branch offices. Of course, mixed operation is possible, too.

Fragmenting and Maximum Transmission Unit (MTU)

A further problem, which occurs, is the size of the data packets when communicating via different Internet dial-up media. For example, DSL allows for packet sizes of 1492 Byte. Frequently VPN data packets, which the branch office VPN gateway sends to the router via DSL, are larger than 1492 Byte. This results in fragmented VPN IPsec data packets as default. However, this fragmentation has a negative effect at IP level, since various routers do not accept fragmented IPsec packets. They do not forward such data packets and the data is lost.

This problem can be combated with pre-fragmentation. This process does not fragment the IPsec packets but fragments the data packets prior to tunneling, which means, the IPsec tunnel header is added after fragmentation. With this method, the system only sends non-fragmented data packets that the Internet router / firewall accepts.

Modern professional VPN solutions provide this intelligent method of dynamic reduction of the MTU. Such VPN gateways are able to automatically adapt the packet size of TCP connections to the defined size prior to connection set up.

Enforced 24h disconnect for DSL connections

24h disconnect is immaterial for site-to-site VPNs. However, during "peak times" a permanent connection has to remain established. Most providers automatically carry out the enforced 24h disconnect 24 hours after the first connection setup. This means that the administrator has to pay attention as early as VPN installation that the VPN gateway offers a feature that allows the administrator to set the time of the enforced 24h disconnect.

Branch office structure is decisive

All aspects discussed above should be taken into consideration when implementing a site-to-site VPN installation. In most cases it is only details that make branch office networking become difficult, even if it has been in place for years. Most VPN gateways are suitable for simple standard networks, however, administration and management tools separate the wheat from the chaff.