SecurITy made in Germany

Trust Seal
www.teletrust.de/itsmig

NCP
SECURE COMMUNICATIONS

Whitepaper

Friendly Net Detection

Friendly Net Detection Updated: March 2022

1. Disclaimer

The information contained in this document is subject to change without notice and does not constitute an obligation on the part of NCP engineering GmbH. NCP engineering GmbH reserves the right to make changes in line with technical progress.

2. Trademarks

All products named are registered trademarks of the respective organizations.

Friendly Net Detection – Definition and Description

Friendly Net Detection (FND) is a technology designed for automatically detecting "Known Networks", also known as "Friendly Networks". The technology aims to guarantee maximum security for company networks in remote access virtual private networks (VPNs) while enabling the user to work seamlessly in the company network or in trusted environments. In this scenario, a solution that delivers end-to-end security is needed – protecting the end device while being smart enough to let the user work unhindered in friendly networks. This whitepaper sets out to describe the requirements and functions of Friendly Net Detection.

Friendly Networks – Scenario

The integrated personal firewall in the NCP Secure Clients enables firewall rules to be configured in a highly flexible way. Rules can also be defined that are based on a locked setting (deny all connections that are not explicitly permitted). Based on this rule, network packets are filtered according to specific criteria.

By way of example, these include:

- Sender/recipient address
- Protocol (IP, UDP, ICMP, etc.)
- Application program

These criteria, which are set in the security policy, define very precisely what a user may and may not do from their device on a certain network (for example intranet, central company network, Internet). This security policy is usually created and maintained by the network administrator.

To prevent a user from circumventing this security policy by deleting or changing firewall rules, the NCP Secure Client allows configuration parameters to be locked. This also prevents users who have administrator rights for the operating system from changing the configuration, providing protection that is independent of the system environment.

However, this creates a problem for mobile users who use a wide variety of networks, e.g., in airports, hotels, at home and in their company or office network. Administrators must then define a firewall policy that meets the security requirements of these different locations. For example, a company may require that a mobile user can only download their e-mails from the company server, and prohibit them from accessing the internet, for security reasons.

But what if the mobile user connects their computer to the company network? They are now in a secure environment protected by central security measures (firewall, virus scanner, etc.). The user might also need to access certain client/server applications that require communication via preset TCP/IP or UDP ports. Personal firewalls then become superfluous to the requirements within the company network, so they would need to be disabled for the user to work effectively on the company network. For this type of scenario, static firewalls that only allow rules to be activated or deactivated would block the user's access to the network completely. The user would have to switch firewall rules manually depending on their location. However, this contradicts the overall security policy and the principle of end-to-end security.

To solve this problem, networks are divided into two groups:

1. Friendly networks that include the company network and any other networks that the administrator trusts.
2. All other networks are either called "Unfriendly Networks" or "Unknown Networks", which have the same meaning.

In order to define firewall rules that are dependent on the location or current network of the user, NCP Secure Clients offer the option of assigning dynamic firewall rule(s) based on these network groups. As a result, the firewall rule is only active if the user is in a network designated as either a friendly or unfriendly network.

Friendly Net Detection – Analysis

The advantage of Friendly Networks (FNs) is that the administrator must only define firewall rules once for the entire system environment, and then these rules are applied by the personal firewall in the client software accordingly. However, this is only generally possible with a static network structure. As described above, intranets or extranets of companies and organizations are characterized by permanent changes that are based on, among other things, the needs of remote users and business partners. This would mean, administrators would be faced with the task of keeping the list of friendly networks permanently up to date and ensuring compliance with the different firewall rules.

This problem is avoided and solved by Friendly Net Detection – which is built into the dynamic personal firewall within the NCP Secure Client. It allows the remote client to automatically and seamlessly detect whether it is in a FN, without having to change the entire configuration. Nevertheless, before providing a more detailed functional description of how this is accomplished, a further problem associated with Friendly Networks needs to be considered. This problem being that not every company has an IP address range from the public IP address space.

Many companies use private IP addresses, such as 10.x.x.x/8, 172.16.x.x/16 or 192.168.x.x/24, and network address translation (NAT) or proxy servers. A problem could be that in permanently configured FNs, for example, employees work with the same network address used in the Friendly Net at their home location. Another problem scenario might occur if a sales representative connects their notebook to another network, i.e., to a customer who uses the same IP address space as their company network.

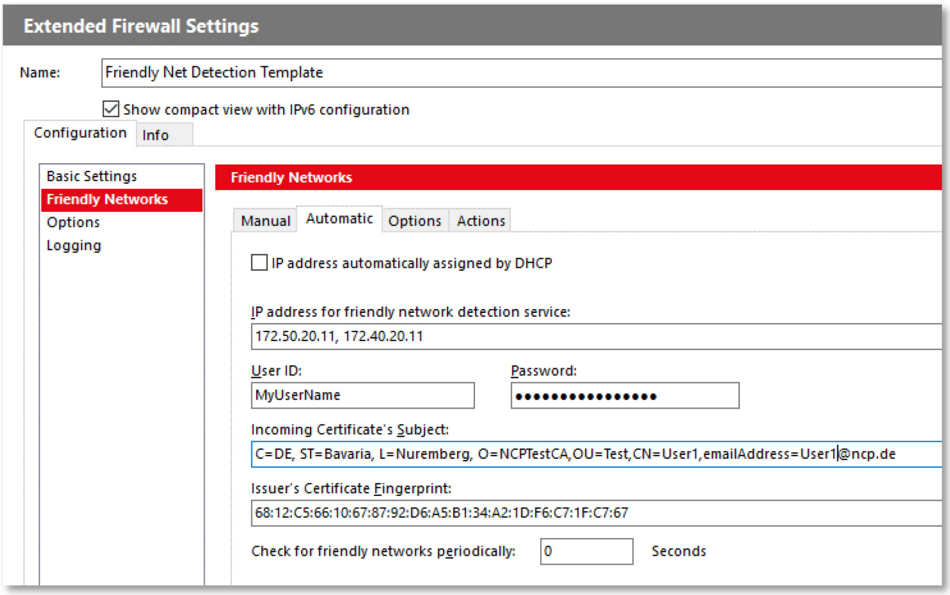
In either case, the result is the same: The security policy is either disabled or relaxed, meaning that firewall rules, which are intended to protect the client and are therefore only applied in "Friendly Networks", are now activated. Friendly Net Detection alleviates the need for administrators or users to configure and keep track of friendly networks and their associated firewall rules by doing this for them.

NCP Friendly Net Detection – Feature Description

Friendly Net Detection (FND) is a client/server application. The Friendly Net Detection server (FNDS) is a service to be installed separately, and completely independent of the VPN Gateway, it can be installed on any computer within, or with access to, the known company network. The Friendly Net Detection client (FNDC) is part of the NCP Secure Client Suite and can be configured within its firewall settings. FND is based on Extensible Authentication Protocol (EAP) via User Datagram Protocol (UDP) in various modifications or via Transport Layer Security (TLS).

This ensures the security of the system and avoids problems that occur more frequently in proprietary solutions. A prerequisite for implementing FND is the installation of the FNDS in a network that has been declared as FN. This service must then be accessible from all network access points and changes must be made to the router settings if necessary. When an employee connects their device to the company network, the FNDC attempts to contact the configured FNDS. If the connection is successful and authenticated, the FN status is confirmed, and the firewall rules of the NCP Secure Client are automatically switched accordingly for internal networks.

The authentication procedure is as follows: The procedure is based on the standardized authentication protocols EAP (RFC2284) and EAP-TLS (RFC2716) or TLS (RFC5246), whereby only the server is authenticated by the client. In the case of EAP, a username and password are stored on the server, which must match the password stored by the client. This approach also allows grouping of clients (definition of group-specific FNs).



Extended Firewall Settings

Name: Friendly Net Detection Template

☑ Show compact view with IPv6 configuration

☐ IP address automatically assigned by DHCP

IP address for friendly network detection service: 172.50.20.11, 172.40.20.11

User ID: MyUserName

Password: •••••••••••••••

Incoming Certificate's Subject: C=DE, ST=Bavaria, L=Nuremberg, O=NCPTestCA,OU=Test,CN=User1,emailAddress=User1@ncp.de

Issuer's Certificate Fingerprint: 68:12:C5:66:10:67:87:92:D6:A5:B1:34:A2:1D:F6:C7:1F:C7:67

Check for friendly networks periodically: 0 Seconds

Figure 1 Dialog for FND configuration

For EAP-TLS, the issuer certificate or all certificates that are necessary for the validation of the FNDS certificate must be stored on the client machine. Furthermore, the fingerprint of the issuer certificate and the subject of the FNDS certificate can also be configured within the client or strictly in the central management system. This prevents an experienced user from replicating a FN in an unauthorized environment such as a home network. Only the VS-GovNet connector uses a different authentication method.

For TLS authentication, certificates are used rather than a username and password. The CA certificate, i.e., the certificate of the FND server, is also stored on the client machine. If a TLS connection to an FND server is successfully established, the client detects the FN as a result. Pure TLS authentication is supported by the FND server from version 4.0 and in the client from GovNet v2.10. The previous versions only support EAP or EAP-TLS.

After the authentication parameters have been set up, the IP address of the FNDS must be configured. To increase reliability, a maximum of ten IPv4 or IPv6 addresses may be added. Alternatively, the FNDS IP address can also be distributed to the FNDC via DHCP, which supports any number of FNDS addresses.

Summary

Friendly Net Detection is an important feature of the NCP Secure Client Suite for universal use in any remote access and secure communication environment. The rules of the integrated personal firewall for internal use in the known network and external use in the unknown network are specified centrally by the administrator and cannot be manipulated or switched off by the user. Users can continue to access the company network in any scenario without hindrance in their network connection or compromising on security.

For managing the configuration of NCP Secure Clients centrally, NCP optionally offers Secure Enterprise Management (SEM) as a single point of administration.

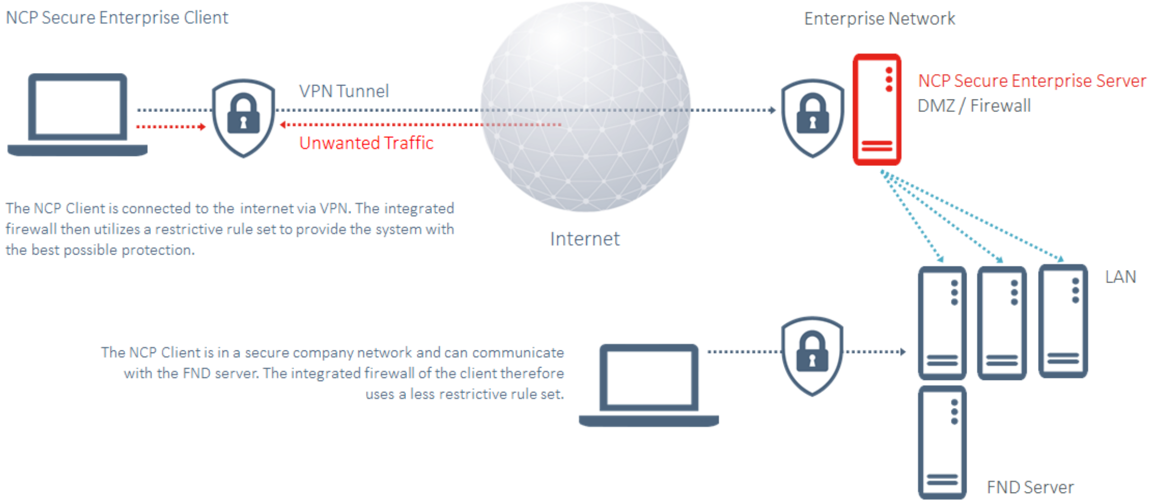

NCP Secure Enterprise Client
VPN Tunnel
Unwanted Traffic
Enterprise Network
NCP Secure Enterprise Server
DMZ / Firewall
The NCP Client is connected to the internet via VPN. The integrated firewall then utilizes a restrictive rule set to provide the system with the best possible protection.
Internet
LAN
The NCP Client is in a secure company network and can communicate with the FND server. The integrated firewall of the client therefore uses a less restrictive rule set.
FND Server

Figure 2 Scenario including Friendly Net Detection

SECURE COMMUNICATIONS

NCP engineering GmbH
Dombuehler Str. 2
90449 Nuremberg, Germany

Phone: +49 911 9968 0
sales@ncp-e.com
www.ncp-e.com