Leading in Cybersecurity Solutions

Company brochure

+31 (0)20-7881030

info@networking4all.com

https://www.networking4all.com

NETWORKING4ALL

LEADING IN CYBERSECURITY SOLUTIONS

About Networking4all

Networking4all is a professional and service-focused supplier of SSL certificates, penetration tests, vulnerability scans, endpoint protection | detection | response, security awareness training, social engineering services and other internet security products. Besides our cybersecurity advice, we also offer managed security services, with which we unburden our clients from their cybersecurity. Via this security service, we monitor workstations, servers and network traffic for suspicious activities, and are available for incident response and forensics. We also work on vulnerability management proactively with reports about progress and occured incidents.

With 21 years' experience, Networking4all is a Platinum Elite Partner for most SSL brands, including Digicert, Thawte, Geotrust, and GlobalSign. Additionally, we have collaborated with a number of known security suppliers such as Qualys and F-Secure. We are also part of Cyberveilig Nederland (Cyber-secure Netherlands). We strive to find the best solution for the specific online security needs for every client.

ISO 27001 & ISO 9001

The ISO 9001 certification is the internationally recognised norm for quality management. This includes procedures with which we are continuously working to improve customer satisfaction. With the ISO 27001 certification, we show how important we consider information security to be. These processes are continuously monitored, captured, guarded and improved. These ISO-certifications are judged and issued annually by KIWA, an internationally recognised institute.

CCV certification for pentests

Companies are dealing with an increasing number of cyber threats such as ransomware attacks and data leaks. The call for trustworthy pentests is growing louder. In collaboration with a large number of parties, the Centre of Crime Prevention and Safety (CCV) created a certification for pentests in April of 2021. The certification came about via a close collaboration with the Cybersecurity Stakeholders Committee. This committee consists of the following parties: VNO-NCW / MKB Nederland, CIO Platform, Dutch Association of Insurers, Police, Cyberveilig Nederland, NLdigital, Digital Trust Center and Online Trust Coalition.

Owners of this certificate are periodically audited for upholding the norms, expertise and quality of penetration tests. During this audit, employees are checked whether they are OSCP (Offensive Security Certified Professional) certified.

Certificate number: K108753/01
Issued on: 15-08-2021
Valid until: 15-08-2024
Certification scheme Cybersecurity Pentest version 1.0

For more information about the CCV certification click here. (Dutch)

Active partner of sector organisations

To strengthen our mission we are an active partner within relevant industry organisations that share the same vision. Networking4all is a partner of both Cyberveilig Nederland (Cybersecure Netherlands) and the Dutch Cloud Community.

Cyberveilig Nederland

Cyberveilig Nederland is committed to increasing quality and transparency in the cybersecurity sector. We share our knowledge and expertise and show that cyber security is not only a risk, but also an opportunity in the development of new products and services. We do all this for and with our members: service providers in the field of cyber security.

Dutch Cloud Community

DCC's mission is to create the preconditions for a healthy Dutch hosting-, cloud-, and internet sector and to contribute to an open, safe and free internet. This fits perfectly with the vision of Networking4all. In January 2021, the Dutch Cloud Community was created from the merger of ISPConnect and DHPA, the two sector organisations of the sector. More than one hundred prominent companies are affiliated with DCC. Together we represent the digital infrastructure sector.

Balance between People, Process and Technology

Security should be a balance between technology and organisational culture. Our products and services focus on the three information security pillars of people, process and technology.

People
Continue to educate your employees on cyber security skills and the dangers of cyber attacks. Provide tools to act appropriately. Keep Security Awareness top of mind through various ongoing awareness activities.

Process
Provide a coherent structure and modus operandi to mitigate risks or address threats in real time. This by including information security in processes/culture within the organisation.

Technology
Provide the right technological tools to identify vulnerabilities and respond quickly and appropriately to threats and attacks.

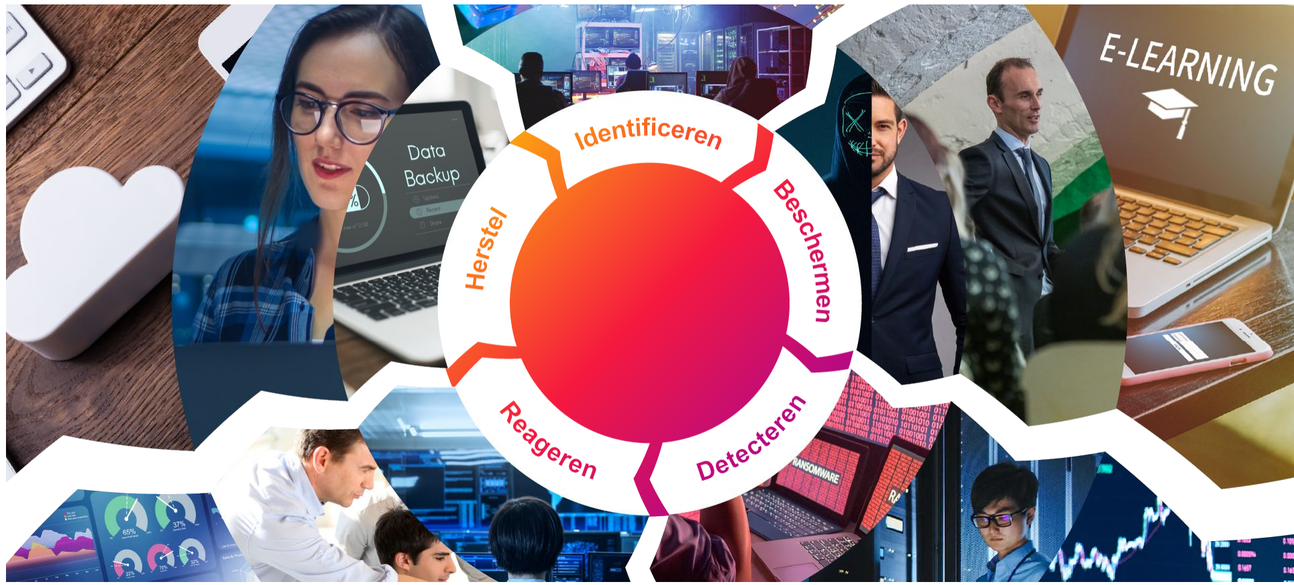
Deploying technological measures undoubtedly increases the level of defence. However, only proper implementation of the information security pillars people, process technology will actually lead to a reduction in risks.

Ask about ZERO measurement capabilities on Employee Awareness, IT infrastructure vulnerabilities and information security in your processes.

We offer Cybersecurity Total Solutions

We work with our own cybersecurity framework in which we have divided all our services into five phases. The five phases of a holistic cybersecurity programme. In an ideal world, you as a company, have all five facets of your business safeguarded with one or more services. These five phases include:

- Identificeren
- Beschermen
- Detecteren
- Reageren
- Herstel



Central to our framework is our SOC/SIEM, to which we connect and monitor customers' systems and networks 24/7, complemented by our in-house incident response team. Whether you are in the market for identifying weaknesses in your network, improving employee awareness or a combination of several, we can unburden you within all facets.

Our services focus on the following pillars:

- SOC/SIEM Managed Security Monitoring Your organisation has insight into its attack surface/threat landscape at all times, enabling better anticipation.
- Ethical Hacken including Pentest | Pentest as a Service | Bug Bounty | Red Teaming | Wifi/Bluetooth Audit.
- Awareness as a Service including Social Engineering (Phishing, Vishing, Mystery Guest, Usb drop) Awareness E-learning, Class-based Awareness Training (Online, onsite).
- ISO 27001 Assessment including checking the degree of information security in terms of people, process and technology using the ISO 27001 Controls.
- SSL/Signing including SSL , Codesigning, Email signing and PDF signing certificates.

Managed Security Monitoring

The advantages of Managed Security Monitoring | SOC SIEM are::

- Your IT infrastructure is continuously monitored for threats, vulnerabilities and cyber-attacks
- We alert your organisation and advise on countermeasures
- Your organisation has insight into its attack surface / threat landscape at any time, allowing for faster anticipation
- Scalable and suitable for both large and small companies
- Fast onboarding through smart vendor connections
- Monitor agreements & SLA recorded in an agreement
- Customer data never leaves the customer's environment
- Quality | ISO 27001 | ISO 9001 | CCV Pentest Quality Mark

Included services:

- 24/7 Active monitoring & alerting
  - Monitoring of external threat
  - Monitoring of internal threat
- 24/7 incident response (8/5 also possible)
- Implementation & onboarding
- Patch advice
- Fast response times
- Security specialist on site, on request
- Real-time reporting including app and own access
- Dedicated phone number | direct line to our security specialists

Security Operations Center | SOC

We take care of the daily defence of your IT infrastructure by using cyber security technologies through managed security services. These are monitored 24/7 from our Security Operations Centre by our certified security specialists.

Security Information and Event Management | SIEM

Security Information and Event Management (SIEM) is used to detect, prevent and help resolve cyber security incidents by centralising information about security events across a network. In other words, through our SIEM tools, we help businesses identify cyber security vulnerabilities and threats before they can have a major negative impact on operations and the delivery of products or services.

Relevant links

Managed Security Monitoring

Cyber security per sector

SSL Portfolio & Management

Networking4all offers an extensive SSL (TLS) portfolio with several major brands such as Digicert and solutions, from one comprehensive portal. In addition, we have dedicated account managers and security specialists at your service for clear and straightforward advice during, before and after SSL requests. With our self-developed and award-winning portal, you can save time, reduce risks and respond immediately to any vulnerabilities. We also offer an attractive own (white label) SSL line.

Our SSL certificates are available at three different validation levels:

Domain validation | DV
Domain validation (DV) is suitable for non-public websites. It verifies that the applicant has management of the domain for which the certificate is requested. DV certificates are widely used for personal, non-commercial websites, or private domains used for testing purposes.

Organisation validation | OV
For a public website with no commercial objective or government function, an Organisation Validation (OV) certificate often offers a solution. In addition to controlling the management of the domain, the applicant's business details are checked. The company details are included in the certificate and can be easily checked in most browsers by querying the certificate details.

Extended validation | EV
A certificate with Extended Validation (EV) is suitable for commercial websites such as web shops and banks, but also for government bodies. For this type of validation, the company details are extensively checked using a public register, such as the trade register of the Chamber of Commerce. As a result, the company details are displayed in the certificate details in the browser.

In addition to SSL Certificates, we also offer solutions for:

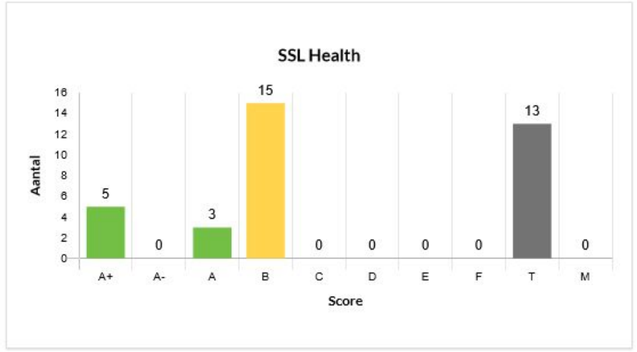
- Code signing
- Email & ID signing
- PDF signing

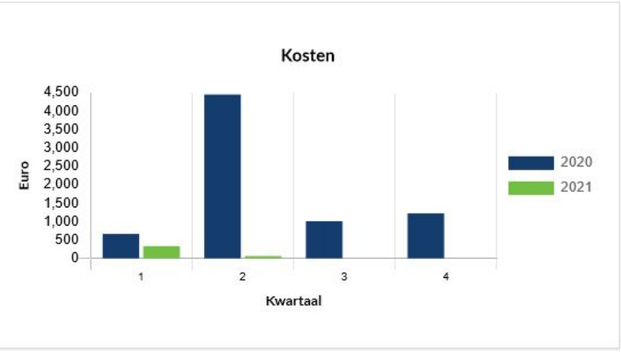
SSL Portfolio & Management

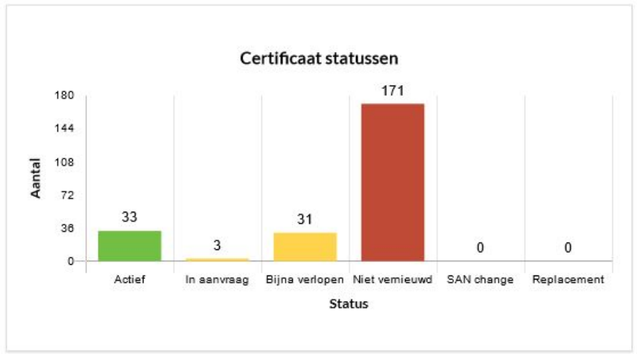
Our revamped management panel for SSL Certificates won the International Innovation Award from Digicert when it was launched in 2019. Unique because you can configure the management as you wish. You can apply for SSL certificates, reissue them, add domain names and even monitor installation and configuration. In addition, you can configure reminders and set standards to make your SSL request even faster.

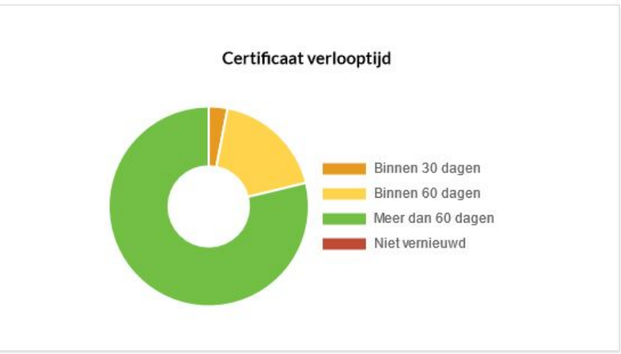
You can also add existing certificates (not purchased from us) and set reminders for timely renewals so you can work and anticipate from a single portal. We will also scan these certificates using our SSL Health (monitor installation and configuration) service.

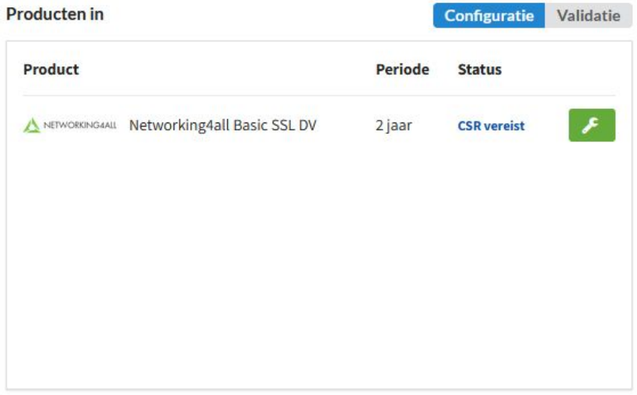
Through our visually powerful validation process, you will know exactly which step the process is at. Manage your contacts, end customers and locations. You also have a clear overview of your certificates, orders, price lists, invoices and can login securely with 2FA.

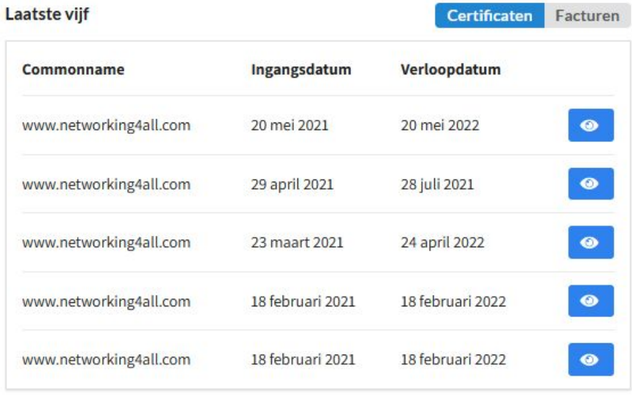












What is Certificate as a Service?

Networking4all takes care of your entire SSL Portfolio management. Based on a structured process, we relieve you of the entire process from application to issuance. You will only have to install the certificate. We also provide advice based on our SSL Best Practices. Mutual agreements and processes are laid down in a contract.

Problems that we often encounter:

- People don't know exactly which SSL certificates they have
- No overview who ordered which SSL (different departments)
- No certificate ordering policy
- No best-practices are used, which makes them more vulnerable
- A poor/incomplete configuration of the certificate / back-end server

With Certificate as a Service, we offer a one-stop solution for your SSL management.

Automatic deployment of S/MIME email certificates

Optionally, we also offer a solution to deploy S/mime certificates very easily. Requesting, implementing and configuring in a few minutes. This concerns an automated roll-out of S/MIME certificates so that you are digitally signed by default when sending email.

The use of S/MIME is recommended by the Standardisation Forum.
If an email message is signed with an S/MIME certificate, the recipient knows in any case

- That the sender of the email has been verified by his digital signature.
- That the message could not be changed after sending because of the digital 'seal' of the S/MIME certificate.

Features:

- Very easy rollout to employee clients.
- Radiates confidence | extra layer of security.
- The decision to send digitally signed emails throughout the organisation considerably reduces the chance of Business Email Compromise.

Collaborations

By working closely with our partners and our suppliers, we add valuable information and knowledge to the market. We do not always deliver our services alone. In addition to our own services and products developed in-house, we also often work with partners. These can be the suppliers we work closely with, but also parties we do business with in order to provide even better services for you as a customer. We cooperate with them because we trust them, and they with us for exactly the same reason. Good cooperation is based on mutual trust.

We also cooperate with interest groups within the cyber security industry. Our objective is to achieve a safer digital world for both the business world and end users.

- Over 15 years of experience in IT security
- In-house innovation
- Active with own investigations

Dutch Cloud Community

CYBERVEILIG NEDERLAND

ICTRECHT

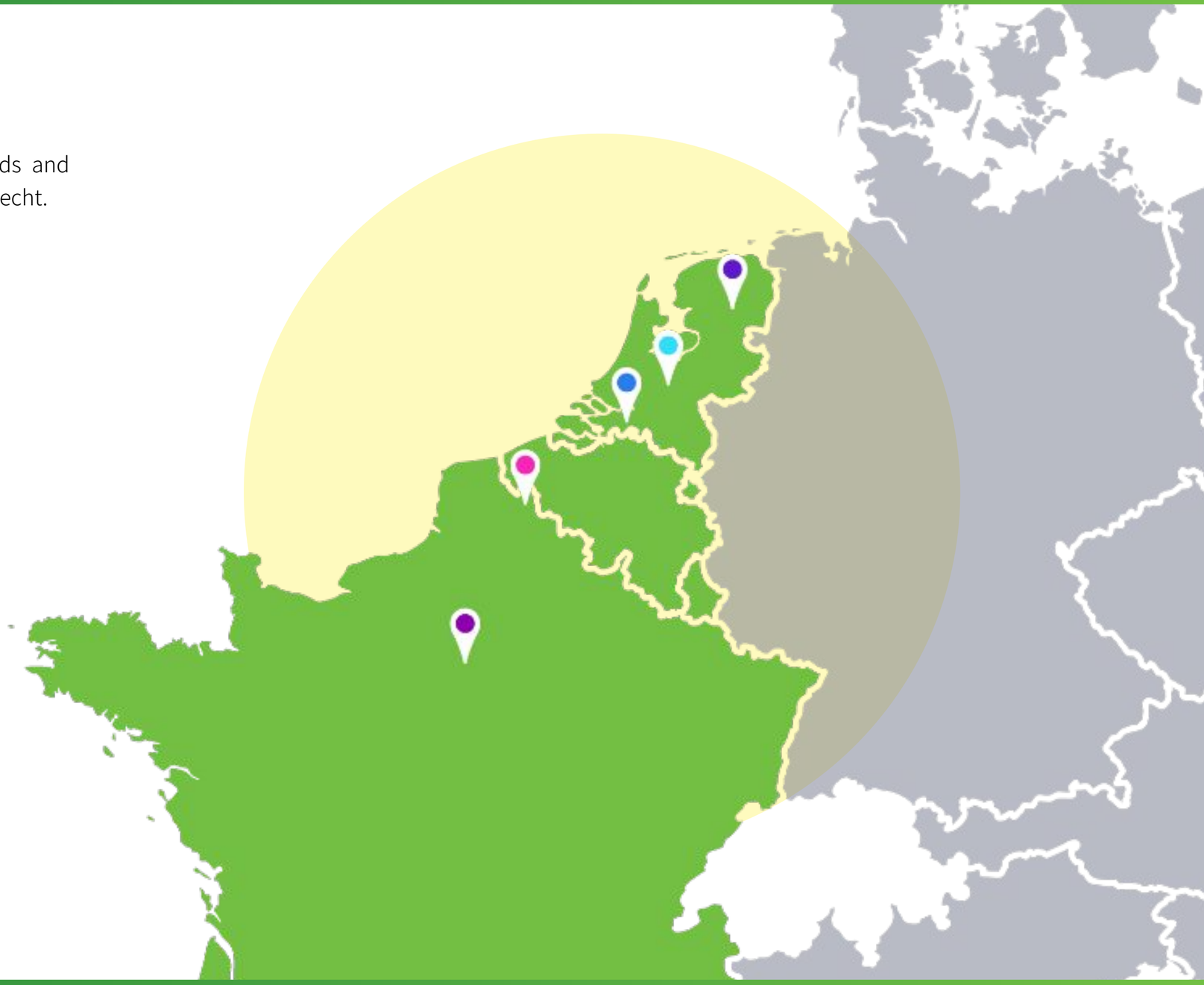
APEX SECURITY

Stepco®

Our European offices

Networking4all is located in different places in the Netherlands and France with our headquarters in the Netherlands in De Meern, Utrecht.

- NL | De Meern, Utrecht | Headquarters
- NL | Zevenbergen, Noord-Brabant
- NL | Assen, Drenthe
- FR | Paris
- FR | Lille



De Meern, Utrecht | Headquarters

Would you like an informal and exploratory conversation with us to see what we can do for you, or possibly for each other, over a cup of coffee or tea? Please contact us for an appointment on location.

"Secure internet for all"

We would be happy to discuss the possibilities with you without any obligation.

Please contact us via:
+31 (0)20 788 10 30

"Safety and security are fundamental needs."

+31 (0)20-7881030

info@networking4all.com

https://www.networking4all.com

NETWORKING4ALL