Reliable VPN Solutions in M2M Environments

As the Internet of Things weaves its way into the fabric of everyday life, enterprises and security professionals are left with the challenge of protecting the communications between millions of devices. ATMs, vending machines, kiosks, cars and trucks, warehousing equipment, shipping and asset tracking devices—the list of IoT applications and M2M (machine-to-machine) environments continues to grow.

How do you manage a secure VPN when there isn't a human being interfacing with the endpoint machine? If you don't have reliable solutions in place—particularly for business-critical systems—you risk lost revenue, disgruntled customers or users, and the expense of restoring operations. And in the case of systems that involve sensitive information, it may be crucial to be in compliance with PCI, SOX, or HIPAA requirements.

How many M2M connections?
Analyst forecasts vary widely, but the growth rate is undeniable. Predictions range from 12 billion to 50 billion devices connected by 2020, up from just 1 billion in 2010.*

There are different ways to connect a machine to your network. Providing a private wireless connection or using an appliance for the connection usually requires additional hardware and services. The easiest and most secure way to connect a machine via VPN to your network is to use a VPN client on the machine. This solution fits easily into your infrastructure and doesn't require additional hardware, such as routers, modems, and SIM cards. In addition, since the traffic is secured right from the operating machine instead of from the private wireless connection or router, no unencrypted traffic ever leaves the machine.

Of course, different environments demand different measures. This paper introduces three areas to think about when setting up a VPN in an M2M environment.

Connections — How to make sure the machine connects when it's supposed to.
Authentication — How to make sure the machine is authenticated in a secure way.
Management — How to manage the VPN to fit with your organization's security policies.

*Source: digitalresearch.eiu.com/m2m/report/section/executive-summary.

Americas: NCP engineering, Inc. · 444 Castro Street, Suite 711 · Mountain View, CA 94041 · Phone: +1 (650) 316-6273 · www.ncp-e.com
Others: NCP engineering GmbH · Dombuehler Str. 2 · 90449 Nuremberg · Germany · Phone +49 911 9968-0 · Fax +49 911 9968-299

Establishing the Connection

Depending on the machine's application, your VPN may need to be connected all the time (as with a surveillance camera) or only on demand (as when someone swipes a credit card at a POS terminal). In either case, the VPN client needs to be able to establish a reliable VPN session. Your main focus will be on choosing a connection method that fits your requirements.

Automatic, or always on

One approach is for the VPN client to connect to the VPN automatically and remain connected. If a disconnect occurs—due to network issues, for example—the VPN client will attempt to reestablish the session, ensuring that the VPN is active again as soon as the data connection is available. In a seamless roaming scenario, the VPN client establishes the connection automatically and will hold the session if a disconnect occurs, preventing session loss of the machine's running application until the VPN session can be reestablished.

Command line

If you prefer to control the VPN directly and only establish a VPN session on demand, you can use a command-line tool to manage interactions between the machine's application software and the VPN client. Typically, a command-line tool supports basic functionalities, such as connect/disconnect, entering username/password, and starting/stopping the VPN client.

API

An API (application programming interface) is a more powerful approach, allowing you to fully control the VPN client from the machine's application software. In addition to the functionalities of a command-line tool, an API can be used to change the VPN profile, to connect to a different gateway, enter a PIN for the use of certificates, get software/connection/authentication status, or change specific settings.

Authenticating the Connection

In most M2M environments, you don´t have humans who enter their credentials or PINs. Instead, to provide the same level of security, the machine—or the VPN "user"—needs to be able to perform authentication steps as it establishes the VPN connection. Depending on the security requirements of the application and the policies of your enterprise, you can choose among the following methods.

Username/Password

You can store a username/password in the VPN client configuration on the machine. The username/password may be information about the machine, such as its hostname. You may also have human users with discrete username/password combinations, such as with multiple users of a company car.

Certificates (PKI – public key infrastructure)

To provide stronger authentication using asymmetric encryption, you can implement your choice of certificates. You can also combine certificates with username/password authorization for a higher level of security, or even two-factor authentication. Some certificates are software-based, while others work in conjunction with the machine, with a smartcard, or with a chip that's built into the machine.

- **Soft certificates,** or user certificates, are files that can be copied from one machine to another—that is, they're not tied to a given machine (which can be an advantage or a disadvantage, depending on your requirements). You can use a common .p12 file, or you can use soft certificates that are stored in the operating system (for example, Microsoft Certificate Store). Depending on the VPN configuration, the certificate may require a PIN.

- **Machine/Hardware certificates** are user/soft certificates that rely on a fingerprint of the machine to bind it to that unique machine—which means they cannot be used with any other machine.

- **Smartcards** are cards (like credit cards) with embedded integrated chips. A soft certificate is stored on the chip—and therefore can´t be exported. Smartcards provide another layer of security, since you need the physical, external smartcard for authentication. This method requires that a smartcard reader be built into, or plugged into, the machine.

- **TPM (Trusted Platform Module)** is a smartcard that's built into the machine. This low-cost, low-performance, and low-capacity crypto chip is soldered onto the motherboard, making implementation somewhat more challenging than other authentication

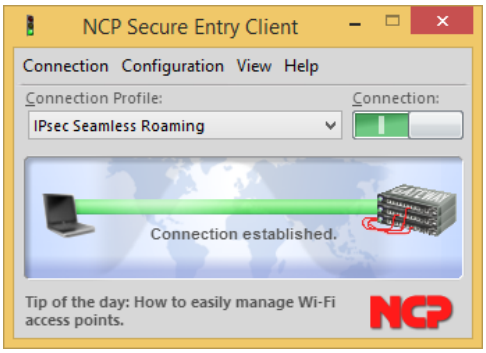
methods. The chip has the same capabilities as the chip on a smartcard, but adds root-of-trust security. The TPM certificate can be used with or without a PIN.

Authentication methods at a glance

Authentication method	Resources/ Time	Flexibility	Security	Encryption	Comments
Username/ Password	Low	High	*	Symmetric	A user directory infrastructure (e.g., LDAP, Active Directory, RADIUS) must already be in place.
Soft Certificates	Low	Medium	***	Asymmetric	Usually a CA (Certificate Authority), such as Microsoft CA or Entrust, is already in place.
Hardware/ Machine Certificates	Low	Low/ Medium	****	Asymmetric	Encryption works in conjunction with the machine hardware.
Smartcards	High	Low	*****	Asymmetric	Soft certificates are deployed on (external) smartcards. Additional hardware and third-party vendor are required.
TPM	High	Low	*****	Asymmetric	Certificate is stored on an encrypted chip on the machine. Third-party vendor is required.

Americas: NCP engineering, Inc. · 444 Castro Street, Suite 711 · Mountain View, CA 94041 · Phone: +1 (650) 316-6273 · www.ncp-e.com
Others: NCP engineering GmbH · Dombuehler Str. 2 · 90449 Nuremberg · Germany · Phone +49 911 9968-0 · Fax +49 911 9968-299

Managing the VPN Client



The VPN makes it possible to securely connect each machine to your network. If the VPN doesn´t work, the machine may not be able to fulfill its purpose. That's why you need to make sure you have a VPN management tool in place—whether for updating the configuration, updating software, or managing certificates. Without centralized management, you'll need to roll out configurations manually, via a memory stick or a CD, and physically access every machine, every time you need to make a change.

Rollout

In a system image or software distribution system, the VPN client comes with an initial configuration to establish the connection. As soon as it contacts the management server, it can automatically download customized configurations, certificates (if necessary), licenses, and software updates (if necessary).

Configuration and software updates

The VPN client contacts the management system periodically to check for any new configurations or software, which will install automatically onto the client—without requiring any physical interaction with the machine.

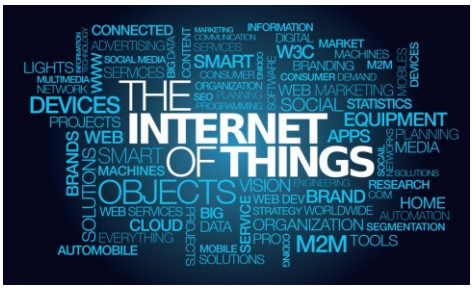
VPN management

As your M2M environment expands and the number of endpoint machines increases, central management ensures that your network never becomes too complex to operate securely and efficiently. A single point of administration provides the flexibility to scale up and down automatically, according to business demands.

Authentication management

If you use certificates for authentication, a PKI management tool can help you roll out, issue, revoke, and renew certificates—again, without needing to touch the endpoint devices.

Americas: NCP engineering, Inc. · 444 Castro Street, Suite 711 · Mountain View, CA 94041 · Phone: +1 (650) 316-6273 · www.ncp-e.com
Others: NCP engineering GmbH · Dombuehler Str. 2 · 90449 Nuremberg · Germany · Phone +49 911 9968-0 · Fax +49 911 9968-299



Conclusion

If you don't have reliable VPN connections in your M2M environment, your machines are at risk of interruption or failure—resulting in headaches and, oftentimes, lost revenue. In the case of machines that are distributed over distant geographies, it may be difficult, time-consuming, and expensive to access them physically; and in all cases, it's a major chore. A reliable VPN connection forms the basis for all communication between the machine and the enterprise network. Make sure you have VPN software—such as from NCP—that can scale up to managing thousands of machines on the network and their interaction with the data center.

About Julian Weinberger

Julian Weinberger, CISSP, is Director of Systems Engineering for NCP engineering. He has ten years of experience in the networking and security industry, as well as expertise in SSL-VPN, IPsec, PKI, and firewalls. Based in Mountain View, CA, Julian is responsible for developing IT network security solutions and business strategies for NCP engineering. He also provides the company's key accounts with pre- and post-sales technical support for their remote access security solutions.

About NCP engineering

Since its inception in 1986, NCP engineering has delivered innovative software that allows enterprises to rethink their secure remote access and to overcome the complexities of creating, managing, and maintaining network access for their staff.

Headquartered in the San Francisco Bay Area, NCP engineering serves 35,000+ customers worldwide throughout the healthcare, financial, education, and government markets, as well as many Fortune 500 companies. In addition, the company has established a network of national and regional technology, channel, and OEM partners to serve its customers.

For more information about NCP's remote access VPN solutions, visit www.ncp-e.com. You can also reach us on our blog, VPN Haus, or on Twitter at @NCP_engineering.