Datasheet

Netgard™ Privileged Gateway

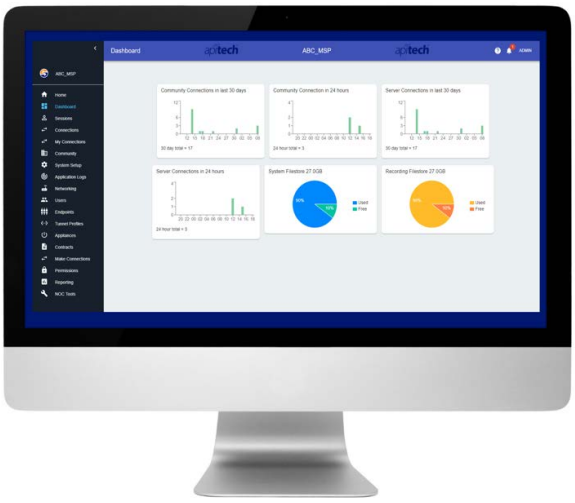
Every Remote Connection Matters

NetGard™ Privileged Gateway Solution

Netgard Privileged Gateway from ION™ Networks enables Managed Service Providers (MSP's), equipment manufacturers and Enterprises (3rd party medium to large organizations) to control secure access to critical voice and data networks via a common gateway platform, minimizing the risk of cross-domain intruders.

With an extensive set of security features Netgard Privileged Gateway controls network access, real time vulnerability monitoring, and forensic auditing. Flexibility, enabling futureproof access and monitoring of virtually any platform, is at its core. This ensures support for a wide range of systems (voice, data, facilities etc) and diverse set of users (internal, MSP, or 3rd party OEM vendors).

At the same time Netgard Privileged Gateway allows MSPs to deliver the broadest range of high revenue services.



Netgard Privileged Gateway dashboard view

Specifications

- Federated (bridged) connection builds a trust relationship between the MSP and Enterprise network, meeting all parties' technical and security needs.
- One solution to secure all 3rd party access as well as internal Privileged Users and credentials.
- Enhanced control facilities for Privileged Users.
- Real Time monitoring and event/ data analysis.
- A scalable, plug and play, easily deployed solution.
- Meets stringent industry recognized standards such as FIPS, HIPPA, SOX, PCI
- Granular Access Control of 3rd party connectivity.
- Bolt on integration with key SOC applications such as Splunk, Snort, AAA, for greater visibility, control, and monitoring of Privileged Session Management.

Most importantly, it provides a federated (bridged) connection that can build a trust relationship between the MSP and Enterprise network meeting all parties' technical and security needs.

This federation of access requires each side to agree the baseline security methodologies (i.e. encryption, key strength, hashing), then once established, the two parties define which users have access and which endpoints will be exposed to each user.

The virtual service contract defines:

- Secure Connection (Crypto, keys, authentication strength
- Who is allowed access
- When access is permitted
- Which devices can be accessed
- Whether per connection authorization is required

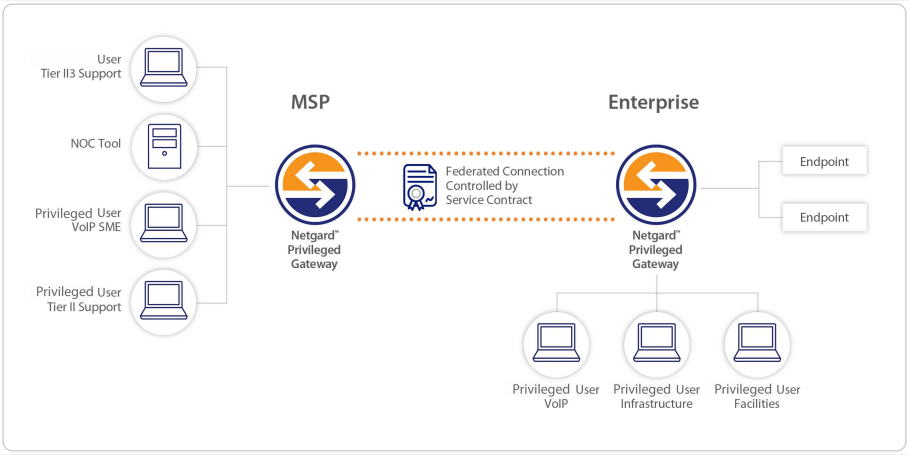


Diagram 1: A Privileged User Gateway (PUG) service contract controls the connection between federated privileged user gateways

The Federated Requirement

The Enterprise CISO, CTO, and CFO must provide a broad range of privileged users with access to a complex network of distributed IT assets. But traditional network security falls short in meeting the demands of Privileged Session Management for remote users, vendors and systems.

In addition, MSPs and equipment manufacturers need their own set of tools to deliver a robust set of services and maintain systems inside the Enterprise network or Cloud. These include the typical IT or VoIP systems, as well as mission critical systems like HVAC, Security Monitoring Applications, and core systems such as medical or lab equipment. The primary goal of the MSP's service delivery tool set is to enable services without any concern for security.

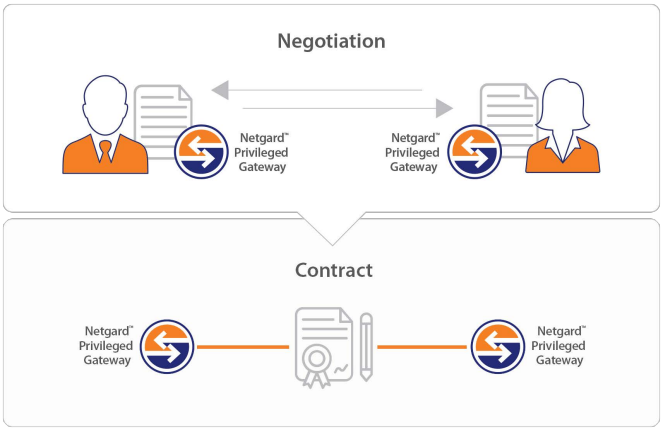


Diagram 2: The federated connection is defined by a service contract between both parties

By using its unique federated connection, Netgard Privileged Gateway adopts a zero trust approach to user access.

The problems facing MSPs when forced to use a customer's secure access solution (VPN) are that:

- It limits the efficiency of the service they can deliver, which in turn reduces revenue. A side effect is the excessive time to provide delivery of services since the technical staff must set up the specific access for these types of customers.
- It incurs a higher cost to deliver services to support unique access channels for multiple customers.
- Changing passwords when personnel leave or vendors change creates a huge admin overhead for Enterprises.

The 2 key reasons the Enterprise is reluctant to provide the MSP dedicated access are:

- Additional costs to vet and approve a one-off access method for each MSP.
- Multiple dedicated MSP access paths create multiple vectors of attack.

For both the MSP and their Enterprise customers there is a need for a secure access method that meets the challenges for robust service delivery with an elevated set of security features. The federated connection is defined by a 'Service Contract', which dictates access rights and controls. Beyond the Service Contract there needs to be a way to provide a complete recording of privileged user activity for root cause analysis, data analytics, or security forensics. These requirements must be coupled with evolving MSP customer (Enterprise) Privileged Session Management security techniques. Netgard Privileged Gateway provides the easily deployable solution to solve these complex problems, and removes the risk of inconsistent service delivery.

These features and benefits are shown in Table 1 below.

Feature	Benefit	Detail
Audit	Record who accessed the system and when, with detailed analysis and monitoring of activity	• System Changes • Tracking who went where, when • Tracking duration of session • Data feed to Snort • Session Recording
User Tunnels	Easily extend secure access to third parties (i.e. equipment manufacturers and consultants) to resolve system issues quickly and eliminate the need for VPN and/or Jump host access	• Easy-deployment model • Secure method to bring third- party into PRIISMS without other VPN solutions • Supports SHA512, TLS 1.2, 2048 • RSA keys
Negotiated Connection	Federation of access, with each Party agreeing the baseline security methodologies (i.e. encryption, key strength, hashing), and defining which users have access and which endpoints will be exposed to the users.	• Customer selectable PKI • Negotiated encryption controls • Negotiated access controls • Negotiated artefact collection • Negotiated NOC tools connection
Granular User Access Control	Manage users and logins from within the Netgard Privileged Gateway system or through external LDAP connections	• Single logon for all endpoints • Access controls based on time, equipment, role or user defined attributes
High Availability	The Netgard Privileged Gateway 'Community' feature enables two or more Netgard Privileged Gateway servers to act as one system sharing a database & licenses.	• Ability to self-replicate the database • Share changes and capabilities • Shared license • Redundancy and scalability

Table 1: Features and Benefits

Minimum Requirements:

- **Host:** VMWare host (ESXI/6.5 or 6.7 or Workstation/14), HyperV (near future)
- **Resources:** 4 (minimum) cores, 8Gb RAM, 2 volumes of 40 GB (minimum) each HD Space, 1 or more virtual NICs

About ION™ Networks

A trusted name in remote device management and secure access, ION Networks provides remote access solutions that enable customers to securely manage, monitor, and maintain high quality of service for critical voice and data network infrastructures. Customers include MSPs, enterprises, equipment manufacturers, and government and military agencies.

ION Network's solutions include:

- Netgard Privileged Gateway for Managed Service Providers
- Netgard Privileged Gateway for Enterprise
- ION PRIISMS
- ION Service Access Point
- ION Secure Appliance
- Avaya Secure Access Link Appliance
- ION Secure Modem
- Netgard MFD follow-me print solutions

ION Networks is a division of APITech with a 30+ year pedigree in security, access and connectivity solutions, and global reach.

Contact Us

USA
Tel: +1 908-546-3900
Email: sales.ion@apitech.com

Canada
Tel: +1 613-270-9009

UK & Europe
Tel: +44 (0) 1452 557 237