Datasheet

Enabling a Remote Workforce

How to battle the strain on your networks with VPN

Forcepoint Next Generation Firewall (NGFW) combines fast, flexible networking (multi-link VPN) with industry-leading security to connect and protect people and the data they use throughout diverse, evolving enterprise networks. Forcepoint NGFW provides consistent security, performance, and operations across physical, virtual, and cloud systems. It's designed from the ground up for high availability and scalability, as well as centralized management with full 360° visibility.

Keep pace with changing security needs

- A unified software core enables Forcepoint NGFW to handle multiple security roles in dynamic business environments, from firewall/VPN to IPS to layer 2 firewall. Forcepoint NGFWs can be deployed in a variety of ways (e.g., physical, virtual, cloud appliances), all managed from a single console.
- Forcepoint uniquely tailors access control and deep inspection to each connection in order to provide high performance and security. We combine granular application control, intrusion prevention system (IPS) defenses, built-in virtual private network (VPN) control, and mission-critical application proxies into an efficient, extensible, and highly scalable design. Our powerful anti-evasion technologies decode and normalize network traffic before inspection and across all protocol layers to expose and block the most advanced attack methods.

Scale site-to-site connectivity with on-demand VPNs

For organizations with site-to-site connectivity, or a distributed remote workforce, connecting all of the sites and users together is called a mesh—and at scale it can be expensive, time consuming, and difficult to administer. With Forcepoint, customers can take full advantage of our VPN Client, which can be deployed easily and without any additional costs to the consumer.

New architectures built for this kind of scale are reinventing how VPNs are set up. The connectivity among the sites is designed so they can dynamically determine how to connect to each other. With on-demand VPNs, organizations can:

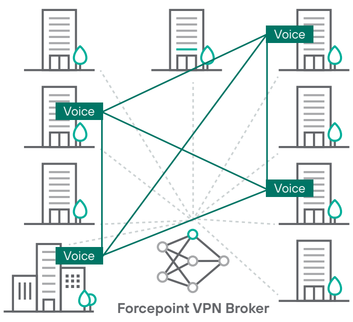
→ Configure VPNs centrally and update dynamically

→ Connect sites directly without creating bottlenecks due to backhauling

→ Scale to thousands of sites

→ Use public and private links seamlessly

This is important because it allows neighboring organizations to communicate more effectively. Instead of manually configuring every location, connectivity becomes dynamic. This allows a smaller equipment footprint at each site, with less complexity. Overall, this reduces cost as well as risk of network outages.



Forcepoint NGFW use case – N51

Introduction

Forcepoint can help our Global Government Customers and Systems Integrators combat the overload and strain on the network caused by increased usage of VPN connectivity by an expanded remote workforce. A small desktop firewall can be configured with either policy-based or rule-based protocols and distributed to remote emplyees for a full VPN mesh architecture. Due to the nature of our customer's organizations and missions, we recognize there is often a need for added security, and a VPN Client may not suffice.

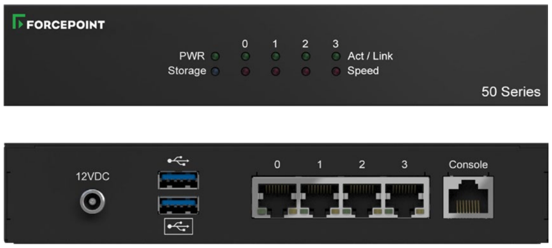


Figure 1: Forcepoint NGFW N51 & N51LTE Appliances

Potential challenges facing customers

→ Complex VPN management

→ A lack of or inefficient one-to-many device provisioning

→ New time-consuming firewall deployments

→ Maintaining policy consistency across firewalls

→ Deploying software updates at a large scale

→ Having a unified view of all firewalls and VPN tunnels

Potential challenges facing customers

→ Less planned maintenance & fewer unplanned outages

→ Fewer cyberattacks and breaches

→ Faster deployment times

→ Lower Total Cost of Ownership

→ End-user internet performance improvement

→ Planned maintenance & unplanned outages reduced from days to hours

→ Incident response time reduced from days to hours

PERFORMANCE	N51 & N51LTE
NGFW/NGIPS throughput (HTTP 21kB payload)	200 Mbps
Max firewall throughput (UDP 1518 byte)	1.9 Gbps
Max inspection throughput (UDP 1518 byte)	900 Mbps
TLS 1.2 inspection performance (HTTP 21kB payload)	100 Mbps
IPsec VPN throughput AES-GCM-256	1 Gbps
Concurrent IPsec VPN tunnels	1,000
Mobile VPN clients	Max 25
Concurrent inspected TCP connections	100,000
Max concurrent inspected HTTP connections	40,000
VLAN taggingt	Unlimited

NETWORK INTERFACES	N51	N51LTE
Fixed ethernet interfaces	4x GE RJ45	
Wireless	-	LTE
Connectors	2x USB, 1x serial	

PHYSICAL	N110	N115
Form factor	Desktop	
Dimensions W x H x D	180 x 37 x 131 mm 5.36 x 1.5 x 5.16 in	
Net weight	0.65 kg 1.43 lbs	0.70 kg 1.54 lbs
AC power supply	100-240 VAC 50-60 Hz, 24 W	
Typical power consumption	9 W	14 W
Max power consumption	12 W	17 W
Max BTU/Hour	58	
MTBF (hours)	150,000 hours	
Operating temperature	5° - 40° C, 41° - 104° F	
Storage temperature	-20° - 70° C, -4° - 158° F	
Relative humidity non-condensing	10% - 90%	
Safety certification	CB, UL/EN60950, NOM	
EMI certification	FCC Part 15, CE, EN55022, EN55024	

forcepoint.com/contact