Services Publication

2019

Table of Contents

Cloud PBX Overview

NetFortris' Cloud PBX is a hosted, managed enterprise communications service. This fully managed service includes routing, POE switching, IP phones, metered access to local, long distance, and toll-free calling, and an end-user administration portal. For an additional charge, optional add on services include: hosted firewall, internet access, Wi-Fi, contact center applications, and MPLS connectivity. Cloud PBX is available in four packages: Business Basic Voice, Business Standard, Business UC and Business Collaboration.

Business Basic Voice

NetFortris Business Basic Voice includes auto-attendant, authorization codes, call waiting, call transfer, call hold/resume, call park/pickup, call forwarding, ad hoc conferencing, and extension dialing.

Business Standard

NetFortris Business Standard includes all components of Basic Business Voice, and includes a voicemail box and an end user web portal. The portal is used for managing calls, line preferences, call forward variants, voicemail notifications, voicemails to email options, and message waiting indication.

Business UC

NetFortris Business Unified Communications (UC) includes the components of Business Standard package and also includes UC features. This includes Instant Messaging (IM), Presence, Group Chat/IM, video calling from a personal computer via an integrated softphone.

Business Collaboration

NetFortris Business Collaboration includes the components of Business UC and adds desktop, file, and application sharing along with multi-point voice and video conferencing.

Mobile Clients

iOS/Android smartphone and iOS/Android tablet clients are available on any Cloud PBX Package. However, mobile clients only support full UC functionality when deployed with the Business UC or Business Collaboration packages. Supported devices include any Android (4.1 or later) or iOS mobile device and iOS tablets (iOS 7 or later).

Total Control WAN Overview

Total Control WAN is a managed network service utilizing customer premises equipment, core network components and a centralized management platform, hosted and provided by NetFortris. The service provides a secure WAN overlay, connecting branch locations together and providing access to enterprise applications and the internet.

Customers can use the management platform to monitor traffic flowing to and from their WAN while providing advanced visibility, application control, and enhanced cloud delivery. The premises equipment can aggregate multiple WAN links and dynamically select the best path for passing traffic. Customer premises equipment selection is site-specific, and is based on port requirements and total aggregated throughput at each location.

Components

NetFortris Total Control WAN service is made up of the following components:

a) Customer premises equipment, designed to support the bandwidth throughput and business profile at your branch location.
b) Access to NetFortris core gateways, for cloud services optimization, last mile optimization, and interconnection between MPLS and broadband networks.
c) Access to cloud management portal for profile changes and network analytics.
d) One read-only administration account for network management
e) One custom network profile that determines application priorities, VPN and firewall settings for all connected equipment.
f) Wi-Fi radios used for CPE activation by NetFortris or approved IT staff only.
g) Fully managed service, email alerting, 24x7 phone support, and two-factor authentication capabilities.

Pre-Installation

The Total Control WAN System Design sheet is intended to map out specific customer network settings. A NetFortris representative will work with the customer to complete this document. Once a design document is filled, NetFortris will be able to set up profiles and start the implementation process.

Network access

The customer premises equipment can aggregate up to 3 WAN links, which can be provided by NetFortris or by a 3rd party. Connection to the WAN must be done via Ethernet, or USB for 3G/4G connectivity. Compatible WAN connections include: fiber, Ethernet over Copper, T1 or bonded T1s, Cable, DSL, and 3G/4G wireless. When using a 3rd party circuit, NetFortris is not responsible for the troubleshooting or maintenance of that service, outside of the scope of the Total Control WAN overlay.

Configuration of TCW service and installation

Total Control WAN is configured through a cloud management portal and distributes profiles to all activated devices. Customers may access this cloud portal to view network analytics or make minor changes to individual components of their network. Configurations to the profile may include VPN and firewall settings, application prioritization, network topology, LAN, DNS, DHCP, and Wi-Fi settings.

When equipment is shipped to a site for installation, instructions can be given on how to set up the device and activate it. If the customer opts to have a tech perform the installation portion, applicable T&M rates will apply.

CPE and other components that make up the Total Control WAN service are based on the total aggregated throughput to each location. If customer bandwidth and traffic throughput increases during the contract period for Total Control WAN, new service tiers and potentially CPE may need to be applied and swapped to support increased traffic. If the Total Control WAN service does require a service upgrade, the customer will be billed according to new bandwidth requirements.

NetFortris Deployment & Support Policies for Managed Services

Equipment provided by NetFortris as a part of the Managed Service does not include shipping charges. The customer will be billed for all shipping charges incurred. In the event Customer terminates an individual Service or other element for which NetFortris generates a fee, other than the last day of the then current billing cycle, Customer will remain responsible for all fees and charges through the end of the applicable billing cycle (should Customer request that NetFortris port a number to another carrier the Service for that number shall be terminated upon completion of the porting process). Customer shall remain liable for all usage and recurring charges through the end of the then current billing cycle.

If applicable, NetFortris will install IP phones, POE switch(es), router(s), Uninterruptible Power Supply (UPS), conference phone(s), IAD(s) and ATA(s).

By way of example #1: A system with twenty (20) SIP phones are deployed with a **managed** 24-port switch. The customer wants to add another six (6) SIP phones; NetFortris will deploy another 24-port switch or replace the 24-port switch with a 48-port switch, at the sole discretion of NetFortris.

By way of example #2: A system with twenty (20) SIP phones are deployed with a 24-port **customer-owned** switch. The customer has other customer-owned devices (e.g., printers, servers, etc.) that the customer wants to connect to this switch, and the number of devices exceeds the number of available switch ports, the customer must purchase a NetFortris certified switch (price varies by switch model) from the table below.

NetFortris Certified CPE – Cloud PBX

Equipment Type	Model Number/ Description
Polycom IP Phone	VVX Series: 300, 310, 311, 400, 410, 411, 500, 501, 600, 601, Camera, & Expansion module
Yealink IP Phone	T Series: T23G, T28P, T42G, T46G, T48G, Expansion module Cordless Phones: W52P/H, W56P/H, W60P
Conference Station	Polycom: IP 6000, IP 5000, IP 7000
Routers	Cisco routers: 871, 877, 881, 887, 891, 897, 3725, 3745, 1941, 3845, 3945
POE Switch	Cisco (all POE GigE): 3560G-24PS (24 ports), SG300-10MP (8 ports), SG300-10MPP, SG300-28P (28 ports), SG300-28MP (28 ports), SG300-52MP (52 ports),
WIC (WAN Interface Cards)	WIC-DS1-T1-V2, VWIC2-2-MFT-T1/E1
Phone ATA (Analog Telephone Adapter - Lines)	Cisco: SPA112, SPA8000
Fax ATA (Analog Telephone Adapter – Fax)	Audiocodes MP202B
IAD (Integrated Access Device)	Cisco: 2435 (8 FXS), 2431 (T1/E1/PRI)
UPS (Uninterrupted Power Source)	APC BR 1300 LCD

NetFortris Certified CPE – Total Control WAN

Equipment Model Number/Type	Description
Edge 510	4 GE Ports; maximum 100Mbps throughput. Desktop appliance.
Edge 520	10 GE Ports; maximum 200Mbps throughput. Desktop appliance.
Edge 540	10 GE Ports; maximum 1Gbps throughput. Desktop appliance.
Edge 840	6 GE Ports; maximum 1Gpbs throughput. 1-RU Rack unit.
Edge 2000	8 GE Ports; maximum 5Gbps throughput. 1-RU Rack unit.
Wall Mount	Mounting Units for 5x0 Models
Rack Mount	2U Mounting Units for 5x0 Models

Site Surveys

If requested by the customer, NetFortris can send a technician to the customer site to perform a site survey at NetFortris standard time and materials plus trip charge rates. The survey will identify the requirements for delivery of services and devices.

Emergency Service (911)

Customer acknowledges that VoIP 911 Emergency Service may not connect to Public Service Access Points ("PSAPs") or may improperly ring to a PSAP administrative line, which may not be staffed or include trained 911 emergency operators. The 911 emergency service is based on the geographical location that Customer provides to NetFortris. The customer is responsible for updating any address change with NetFortris. In some cases, the VoIP 911 call may not automatically transmit the end-user's location. VoIP service may not work during a power outage or when the internet connection otherwise fails or is interrupted. NetFortris is not responsible for any third parties involved in the 911 emergency service or response or for Customer's failure to supply the correct geographical location.

Circuits

For NetFortris provided circuits/broadband access, NetFortris will extend the circuit from the customer MPOE riser feeder to the applicable CPE, up to fifty (50) feet and up to two (2) hours of technician time. Any additional technician time and any extension beyond fifty (50) feet will be charged at NetFortris standard time and materials rates. If a riser feeder is not available from the MPOE, NetFortris will install such cable at the NetFortris standard time and materials rate and bill the customer directly.

If Building Management requires a third party riser company to extend the circuit, the third-party riser company may invoice Customer directly. In the event the third party riser company invoices NetFortris, NetFortris will bill the Customer for this expense.

Circuit Utilization

NetFortris circuits may be used dynamically for IP voice and data, however, a customer must subscribe to these IP voice and data services in order to receive them. The customer may not exceed a maximum circuit utilization of seventy percent (70%) of total circuit capacity.

OTT services may not function properly if more than 70% of total circuit capacity, including without limitation all types of traffic being carried over the customer's circuits, is utilized.

Internet Protocol/IPSEC Bandwidth

Quoted circuit speed indicates the maximum speed provisioned to the Customer premises equipment. Private Internet Protocol (IP) services which are routed via the NetFortris core network shall operate at the maximum provisioned speed, except that the maximum speed may be limited by factors such as circuit overhead, packet encryption overhead, Customer network management factors, Customer device capabilities, Customer infrastructure, and any other factors that are not within the control of NetFortris. For clarity, this guarantee does not apply to publicly routed (internet) based circuits.

Over-The-Top (OTT) Deployments

In an Over-The-Top (OTT) deployment, the customer has obtained broadband access services from a provider other than NetFortris. NetFortris does not provide any circuits or access transport in case of OTT deployments, however, NetFortris may still provide a managed service including without limitation enterprise telephony, UC, Wi-Fi, and Security. If Customer connects their SIP phone from outside the NetFortris network, by way of example connecting over a home broadband connection, this shall also be considered an OTT deployment. Voice quality may be compromised on a purely OTT connection. The customer is responsible for all local firewall, router, and switch settings. NetFortris support is available for an additional fee.

It is the customer's responsibility to ensure that the broadband connectivity needed for their deployment has been procured, provides sufficient bandwidth and Quality of Service (QoS) control, and is available at the applicable CPE location prior to NetFortris service turn-up.

All NetFortris managed services require one or more broadband Internet connections to function properly. Dial-up, standard wireless, or satellite Internet connections do not provide sufficient bandwidth and will negatively impact the delivery of NetFortris managed voice services.

Each NetFortris voice call requires a minimum of 90 kbps of synchronous bandwidth. The following table indicates required bandwidth for various levels of concurrent voice calls.

Concurrent Calls	Required Bandwidth
10	900 kbps
50	4.5 Mbps

Concurrent Calls	Required Bandwidth
100	9.0 Mbps
1000	90.0 Mbps

For example, a typical T1 (1.5 Mbps or 1,500 kbps) connection can support up to 18 concurrent calls or approximately 5 video calls.

If service performance is adversely impacted by circuit related issues and Customer requests or requires remote troubleshooting support, NetFortris will invoice Customer at standard time and material rates. In the event a NetFortris technician is dispatched to the customer site, one trip charge per day per technician will apply in addition to the NetFortris standard rates.

Customer-Owned CPE Settings for QoS

- If the customer's network connection does not have sufficient bandwidth to support all data traffic needs and concurrent voice or video calls, quality of service will be affected.
- The customer shall configure their network router to prioritize voice traffic over data traffic.

Routers and Switches

All on-premises hardware and network devices require a business-grade router to function properly. Power over Ethernet (PoE) switches are highly recommended, as they eliminate the need for individual power adapters for each end point and also allow for centralized power redundancy. The following protocols should be installed and available on the network router:

- **DHCP:** Devices should receive an internal IP address assignment via Dynamic Host Configuration Protocol (DHCP)
- **NAT:** All Network Address Translation (NAT) connections must be left open for at least 60 seconds
- **QoS:** In a converged network, Quality of Service (QoS) must be applied to prioritize voice and video traffic over all other traffic types
- **Public IP Addresses:** Some HD video devices may require public IPs to function properly

To avoid voice quality issues caused by voice and data competing for the same bandwidth over the customer's network connection, the customer must configure the router's Quality of Service (QoS) settings to the NetFortris default QoS settings to optimize and prioritize voice packets on the Wide Area Network (WAN) connection.

- AUDIO RTP: DSCP 46(ef) [COS1, IP Precedence 5, Priority 1 Queue]
  - UDP
    - 1024-65355, actual ranges depending on phone make and model.
    - 9000-20000 range
    - 2000-3000 range

- 5000-5499 range
- VIDEO RTP: DSCP 34(af41) [COS2(V), IP Precedence 4, Priority 2 Queue]
  - UDP
    - 1024-65355, actual ranges depending on phone make and model.
    - 9000-20000 range
    - 2000-3000 range
    - 5500-6000 range
- SIP: DSCP 26(af31) [COS2, IP Precedence 3, Priority 3 Queue]
  - UDP 5060
  - TCP 5060
  - TLS
  - TCP 5061

Firewalls

Firewalls shall be configured to allow NetFortris end points to access HTTP, HTTPS, and UDP traffic on the network. NetFortris end points must be allowed to both send and receive TCP and UDP packets on arbitrary ports and to arbitrary IP addresses. Some network ports may need to be opened manually. Firewalls should be configured with the following settings for optimal functionality:

- **Persistent NAT Connections** NAT keep-alive requests must be allowed every 30 seconds.
- **HTTP** HTTP over port 80 must be enabled.
- **SIP** Multiple UDP connections must be allowed on ports 5060 and 5061.
- **RTP** Internally-initiated UDP requests must be allowed on ports 10,000-65,536 for audio and video.
- **NTP** UDP traffic must be allowed on port 143 for Network Time Protocol (NTP). Contact NetFortris Support for more information on firewall configuration.

TCP/UDP SERVICES/PORTS
- AUDIO RTP (74.85.29.0/25 West, 207.232.92.0/25 East)
  - UDP (30sec timeout)
    - 1024-65355, actual ranges depending on phone make and model, NO NAT:
    - 9000-20000 range
    - 2000-3000 range
    - 5000-5499 range
- VIDEO RTP
  - UDP (30sec timeout)
    - 1024-65355, actual ranges depending on phone make and model, NO NAT:
    - 9000-20000 range
    - 2000-3000 range
    - 5500-6000 range
- SIP (74.85.29.0/25 West, 207.232.92.0/25 East)
  - UDP 5060-5064 (360 second timeout)
  - TCP 5060 (360 second timeout)
- DNS: (69.28.97.4 and 69.28.104.5)

- UDP 53: domain
- Some service providers block third part DNS Servers; you can use you providers DNS.
- TIME: (time.netfortris.com)
  - UDP 123: ntp
- PROVISIONING TCP:80, 443, 8443
  - (spprov.netfortris.com) 74.85.29.30
    TCP:80, 443, 8443
  - (gvpp-edp.netfortris.com) 74.85.29.16
    TCP:80, 443, 8443
- SERVICES, PORTAL, REPORTING TOOLS, CONTACT CENTER
  - (pa.netfortris.com) 74.85.104.12
    TCP 443: https
  - (gvpp-edp.netfortris.com) 74.85.29.16
    TCP 443: https
  - (commandcenter.netfortris.com) 69.170.184.158
    TCP 443: https

Cabling

The customer is responsible for meeting the minimum cabling requirements, as defined by NetFortris in its sole discretion. Unless other stated, all cable work shall be charged at NetFortris standard time and material rates. In addition, any cable work requested on the day of installation will be charged at NetFortris standard time and material Overtime Labor Rates. All cable work will be charged a two (2) hours minimum. In addition to standard time and material charges, a trip charge will be applied for each deployment of a technician.

NetFortris will provide two (2) Category 5 cables, one (1) five-foot cable to use from the IP Phone to the user's computer and one (1) three-foot cable to connect the switch to the Patch Panel. If additional cables or longer cables are required, NetFortris will bill customer the standard material rate.

In the event that no Category 5 cabling is available at the customer location then installation shall not proceed until the necessary equipment has been installed by the customer, at customer cost, in a manner sufficient to make the local network suitable for carrying multimedia traffic.

Rack/Cabinet Space

The customer is responsible for providing an adequate rack or cabinet space for NetFortris-provided equipment including without limitation the proper Switch, Router, IAD, and UPS. The equipment should be located in a dust-free environment with suitable temperature and humidity control.

Additional Add-On Services

Analog Integration

NetFortris will configure and install the appropriate Analog Terminal Adapter (ATA) device to support analog device integration to the Cloud PBX solution. Voice (i.e., phone line) ATA devices can support up to (2) or eight (8) analog line ports, depending on the device selected. Analog services that can be integrated include a modem, overhead paging, door phone, door opener and standard analog phones. If the customer will be utilizing its own switch to support this integration, the customer is responsible for the programming of the switch port. Analog Facsimile is supported via a dedicated 2-port Facsimile ATA. Therefore, in the event customer selects to support both analog voice lines and Facsimile lines, separate ATAs will be deployed.

Unified Communications Clients

The NetFortris Unified desktop applications for Windows or MAC, are available exclusively for Business UC or Business Collaboration customers. These desktop applications can be downloaded directly from a NetFortris provided web portal. UC applications for Android and iOS mobile devices are available for customers who have purchased the optional mobility feature and can be downloaded from the Google Play or iOS app store, respectively. Users must meet all minimum system requirements for applicable clients to operate correctly. The customer is responsible for all charges associated with using the mobile application. These charges include, without limitation voice, SMS/text, and data services.

Unlimited Calling

Fair Usage and Overage Charges: Services that include unlimited calling plans shall remain within the bounds of Reasonable traffic. For the purpose of this section, "Reasonable" shall be defined as no more than an average of 1500 minutes of outbound local and long distance usage per user per month, within the lower U.S. 48 states only. Any usage in excess of this amount will be billed at the current standard rate. NetFortris shall provide reasonable advance written notice of any changes to NetFortris' standard rates.

Subject to the Fair Usage clause above, unlimited calling excludes Alaska, Hawaii, U.S. territory, and International, which is available for additional fees.

Subject to the Fair Usage clause above, unlimited calling packages may only be used for normal business use. A combination of factors is used to determine abnormal use, including but not limited to: trunking or forwarding your NetFortris number to another number(s) capable of handling multiple simultaneous calls, spamming and blasting calls. NetFortris reserves the right upon prior notice to suspend or cancel unlimited calling service if NetFortris determines abnormal use behavior exist.

Contact Center

NetFortris Enterprise Contact Center solution is offered as a base package with additional optional features. The base Contact Center package contains all core functionality of the contact center, including skills-based routing, intelligent queueing, auto-attendants, and reporting. Optional features include supervisor listen and view, call/screen recording, custom reports, agent surveys/scorecards, PCI compliance, and multimedia queue channels such as social media, email, or web chat.

Call Recording

Call recording is provided as an 'always-on' service. Recordings are managed through a browser-based web portal and can be accessed by the end user, supervisor or administrator. Users can view, listen, and download calls from the end user portal. Supervisors with the appropriate permissions can listen to and view other users recorded calls. Administrators can define their user's permissions and create users within the call recording system, as well as run reports from the portal.

NetFortris is not supplying any legal advice nor does it profess the accuracy of the information provided in regards to call recording. If you have questions concerning legal implications and how these laws apply in particular states or the legal ramifications of the use of this product, you should contact an attorney for advice. NetFortris is not legally responsible for any misinterpretation, lack of understanding or lack of knowledge regarding the use of call recording or the use of its products by a purchaser or other party whether legal or illegal. It is your responsibility to acquaint yourself with the proper knowledge for legal use of this product. There are both federal and state statutes governing the use of call recording. It is the responsibility of you, the Customer, to understand and know the statutes that apply and what the rights and responsibilities are when recording and disclosing communications.

Voicemail Transcription

The optional NetFortris Voicemail-to-Text solution allows voicemail messages to be transcribed into text. The transcribed text message will be delivered via email to the end-user. If the transcribed message was emailed, a copy of the actual audio voicemail message will be attached in a .wav format as part of the email. The end-user will not receive voicemail transcriptions if the recipient has an incorrect or non-working email address.

The transcribed message is based on reasonable efforts and some messages may not be transcribed due to poor diction/dictation, noisy environment, poor phone connection, language, or other issues beyond the control of NetFortris. NetFortris is not liable for any indirect loss or for loss of profits, goodwill, time use, data or other intangible losses due to the use of this service.

LiveView Monitoring

The NetFortris LiveView Monitoring solution provides standards-based monitoring of NetFortris-managed network devices, services or applications on TCP/IP and Windows networks via a web portal.

Paperless Fax

NetFortris Paperless Fax solution provides inbound and outbound facsimile service. For inbound facsimile service, all incoming faxes are converted to PDF format and are downloadable via a customer portal. Subscribers are notified of incoming facsimile via email. Incoming faxes will reside on the NetFortris system for ninety (90) days. After ninety (90) days all data will be automatically deleted.

Outbound facsimile service is accessible through a customer portal or outgoing email. Compatible documents include DOC, DOCX, XLS, XLSX, PPT, PPTX, PNG, PDF. Outbound facsimile documents must be in black and white.

The facsimile transmission and receipt will not operate correctly in the event of incorrect or non-working email addresses. Further, NetFortris is not responsible for errors associated with third party systems.

Meet-Me Conference Calling

Meet-Me conference calling service is available for Cloud PBX customers. A 25-port conference calling service is included for Business UC and Business Collaboration customers and is an optional add-on feature for Business Basic Voice and Business Standard customers. Each Meet-Me conference user will be given a local dial-in number, along with one (1) conference access code. Additional conference access codes may be purchased. Conference moderators can adjust their moderator PIN and conference preferences through their web portal.

Passwords and Security

For security and protection purposes, the customer is required to change all user and administrative passwords set by NetFortris. If applicable, NetFortris will set the initial default password for the following: Voicemail, Web Portal, Call Recording, Administration Portal and LiveView Monitoring.

Customer hereby agrees and acknowledges that fraudulent use of the Services, including but not limited to DISA, auto-attendant, voice mail, 800 and 900 services and 10xxx, is possible. NetFortris does not maintain or control the customer's PBX. The customer is completely responsible for the security of their PBX. The customer is responsible for all charges incurred via their PBX.

Training

For a fee, NetFortris offers training for Administrative users, End-Users, Receptionists, and Contact Center agents or supervisors. Training is delivered remotely via online screen sharing technologies. The training provided to the customer is intended to serve a "train the trainer" model so the customer is responsible for ensuring that relevant personnel is included in the training session. On-site training is also available for an additional fee.

NetFortris Provided CPE Support Policy

Customer may not connect any devices to NetFortris provided equipment without receiving prior consent from NetFortris.

In all cases, the customer is responsible for obtaining a Return Merchandise Authorization (RMA) from NetFortris before shipping any defective CPE to NetFortris.

NetFortris is not responsible for manufacturer defects. Within the first 30 days after installation, if NetFortris-provided CPE is defective or damaged due to NetFortris employee negligence, NetFortris will replace or repair the defective part(s) at its cost. NetFortris will not be responsible for any defect or damage resulting from mishandling, abuse, misuse, improper storage, accident, negligence, theft, vandalism, fire, water or other peril beyond the control of NetFortris. Additionally, NetFortris is not responsible for conditions outside of the environmental specifications, including and not limited to wiring, electrical power, temperature, humidity or dust, or causes other than normal use, or improper installation by someone other than NetFortris employees. If such damage is incurred, the customer shall remit payment for the CPE at the then defined NetFortris rates. NetFortris is not responsible for the replacement of disposable batteries used in cordless devices, due to normal usage. In the event there is a defect with a SIP Phone that cannot be resolved through remote phone support, NetFortris will ship a replacement via UPS ground. Expedited shipping of the SIP phone will be billable to the customer. If the defective phone is not returned within five (5) business days, the customer will be billed, and pay, for the replacement SIP Phone.

If the customer prefers onsite troubleshooting support or installation of the CPE, NetFortris will invoice Customer at standard time and material rates. In the event a NetFortris technician is dispatched to the customer site and the problem did not stem from NetFortris-provided CPE, Customer will be billed at NetFortris standard labor rates plus trip charge.

Customer Owned CPE Support Policy

NetFortris can assist with configuring and installing customer-provided CPE at NetFortris' then-current time and materials rate. Customer must provide configurations and passwords for their customer owned CPE. NetFortris is not responsible for hardware provided by the customer during configuration or installation. Customer CPE must qualify as NetFortris Certified CPE.

NetFortris is not responsible for any defective part(s) or damage to the customer-owned equipment. In the event customer-provided CPE causes degradation in service or needs technical assistance by NetFortris, then NetFortris will invoice Customer at then-current time & materials rates. Any resulting degradation in service shall not be considered a NetFortris outage or breach of contract.

Any remote or onsite troubleshooting and support will be billed at the NetFortris standard time and material rates for a minimum of one (1) hour. In the event a NetFortris technician is dispatched to the customer site, one trip charge per day per technician will apply in addition to the NetFortris standard rates.

Service Implementation

NetFortris Responsibilities

- Provide a single point of contact during installation and an Account Manager for ongoing support.
- Schedule kickoff meeting (conference call) to verify the scope of work, confirm preliminary information and gather high-level requirements pertaining to your system.
- If applicable, schedule a technical site-visit to identify network equipment and confirm customer site meets Category 5 standard or higher.
- Conduct System Design Specification (SDS) session to determine and document customer's detailed phone and network design.
- Confirm deployment timeline with the customer.
- Schedule two (2) hours of technician time for installation at the customer location.
- Test and verify full operation of the system.
- If applicable, deliver online end-user training on phone, voicemail and portal features. Training will also be provided for Receptionist Console if the application is part of the solution.
- Provide Project Closeout Document after installation which will include NetFortris Customer Support information.

Customer Responsibilities

- Designate a single point of contact to support the installation process. Such person should have detailed knowledge of the network, broadband access, and current phone system and act as a decision maker on behalf of the customer. NetFortris recommends a backup for the designated single point of contact.
- Ensure NetFortris-requested information or documentation needed for the installation be delivered within the agreed timeframe. For example, installation address, network diagram, floor plan, phone bills, and user information, etc.
- Provide rack or cabinet space for NetFortris-provided Switch, Router, IAD, and UPS.
- Confirm minimum cabling requirement of Category 5 or higher. Customer must provide one home run Cat 5 cable per End User location to a single Telco closet. If customer location does not have sufficient cabling for each workstation where an IP phone will be placed, or has multiple Telco closets, NetFortris can provide cabling work at NetFortris standard time and material rate.
- Provide a secure staging room for NetFortris-provided equipment delivered prior to installation date. Staging room should be secure with proper environmental conditions, to include appropriate levels of temperature, humidity, and dust.

- Provide access to facilities including any security clearances and required coordination with building management to allow necessary access for service installation.
- Review and approve final System Design Specification (SDS) within five (5) business days of receiving the document from NetFortris. Failure to respond within five days shall be considered customer approval. If there is a requested change for installation date after the final SDS document has been approved, Customer will be billed and shall pay Change of Critical Date fee.
- Meet minimum equipment and system requirements for all applicable software applications.
- Coordinate internal users for End-User training.
- Verify system functionality and operation of the system.

Pricing Guide

The tables below outline the Cloud PBX rates, standard time and material rates, as well as other related fees.

Third Party Fees

Miscellaneous charges and fees imposed by any third party carrier or underlying service providers, whether charged to or against NetFortris, will be payable by Customer, in addition to a twenty percent (20%) markup ("Recovery Charge"), provided that any cost Recovery Charge shall represent an accurate, demonstrable charge to or against NetFortris as associated with the provisioning, maintenance or termination of Service by Customer.

NetFortris Time and Material Rates	Hourly (US $)	Trip Charge (US $)
Standard Rate (Up to 8 hours) M-F 8am-5pm	175.00	85.00
Standard Rate (Over 8 hours) M-F 8am-5pm	125.00	85.00
Over-Time Rate M-F, 5pm-Midnight, Sat. 8am-5pm	262.50	85.00
Double/Over Time Rate M-Sat. Midnight-8am, Saturday 5pm- Midnight, All day Sunday	350.00	85.00

Circuit Expedites	Fee (US $)
California: AT&T/SBC Main Territory	500.00
California: Verizon 722/730 Territory	750.00
Other	2,500.00

*Note: Expedite Fee does not guarantee earlier installation date than Firm Order Confirmation date.

Change of Critical Dates	Fee (US $)
Final signed SDS not received by NetFortris five (5) business days prior to installation date	1,500.00
Customer-requested change to install date after schedule has been approved	1,500.00

Number Porting	Fee (US $)
Number Port	(Any 3rd party pass-through fees apply)
Porting Expedite	(Any 3rd party pass-through fees apply)
Change of port date	(Any 3rd party pass-through fees apply)

Professional Services	Rate (US $)
Technical Site Survey (excludes Travel & Expenses)	1000.00 / day
IVR/Auto-Attendant revisions/programming	150.00 / hour
Hunt Group revisions/customization	150.00 / hour

Professional Services	Rate (US $)
Customized Music-on-Hold	150.00 / hour
Active Directory integration to Fortinet Firewall	150.00 / hour
Active Directory integration to Cloud PBX	150.00 / hour
Salesforce integration to Cloud PBX (requires customer to have purchased relevant licenses from Salesforce)	250.00 / hour
Microsoft Lync 2013 integration (supported for on-premise Lync server deployments only)	250.00 / hour
SIP Trunk inter-operability testing/configuration for connecting customer IP-PBX to NetFortris core network	1000.00 / PBX
Tenant/User administration including Moves, Adds, Changes, Deletes (MACD)	150.00 / hour
Remote diagnostics/trouble-shooting for over-the-top (OTT) deployments	250.00 / hour
In-person, onsite diagnostics/trouble-shooting for OTT deployments (excludes T&E)	2500.00 / day
NetFortris Managed CPE (firewall, router, switch, phone) configuration at customer request, post installation	175.00 / hour
Customer-Owned CPE (firewall, router, switch, phone) configuration & support	275.00 / hour
Customer-Owned network and CPE (OTT) configuration and support for firewall, router, switch, phone, etc.	275.00 / hour

Training	Rate (US $)
Remote, online web-based training (3-hour session for phone, soft-client, user portal)	500.00 / session
In-person, onsite training (excludes Travel & Expenses)	1500.00 / day

Managed Cloud PBX Solution	MRC (US $)
Business Basic Voice (per seat)	9.99
Business Standard (per seat)	14.99
Business UC (per seat)	24.99
Business Collaboration (per seat)	54.99
Auto Attendant (per single level)	5.00
MeetMe Audio Conferencing (25 participants)	1.00
MeetMe Audio Conferencing (100 participants)	5.00
Unlimited Calling (per seat)	8.00
Contact Center License	55.00
Multimedia Queuing for contact center	10.00
Hunt Groups (per group)	18.00

Unified Mobile Client with Call Grabber	6.00
Indicated Call Park	9.99
Voicemail Box	5.00
Voicemail Transcription (per user)	5.00
Call Recording (per user, plus per hour storage fee)	9.99
Call Recording Storage Fee (per user, per hour)	5.00
Emulated Analog Line (SPA112/SPA8000 required)	9.99
SIP ATA (SPA112/SPA8000) for Analog Line	9.00
Analog Fax Service (requires MP-202B SIP ATA)	9.99
SIP ATA (MP-202B) for Analog Fax Service	9.00
Paperless Fax 500	9.99
Paperless Fax 1500	17.99
Paperless Fax 5000	45.99
Paperless Fax Enterprise	Custom Quote
LiveView Standard Monitoring (per site)	4.95
LiveView Pro Monitoring (per site)	29.95
Local Forward Only Number	19.00
Reserved Number/DID	0.50
Toll Free Number (plus usage)	5.00

Miscellaneous Equipment	Included	MRC (US $)	NRC (US $)
UPS (BR1300LCD or equivalent)	(1) Per Site	15.00	0.00
3 Foot Patch Cable	(1) Per Station		3.95
5 Foot Patch Cable	(1) Per Station		3.95
7 Foot Patch Cable			4.95
14/15 Foot Patch Cable			7.95
25 Foot Patch Cable			14.95
12 Patch Panels			149.50
24 Patch Panels			195.50
48 Patch Panels			308.33
Floor Racks			262.50
Wall Mount Rack			462.50
Rack Shelves			193.53
Faceplates			2.88
Biscuits			3.38
Jacks			7.82
Wall Mount Jacks			9.95

Security Responsibilities

Overview

Published February 2019

The detailed Security Responsibilities are defined in the "PCI DSS Responsibility Matrix" located on the NetFortris website (https://www.netfortris.com/legal) and hereby incorporated by reference.

Introduction

Trustwave conducted an assessment and found NetFortris to be compliant with PCI DSS 3.2. This responsibility matrix has been created to illustrate and clarify the PCI compliance responsibilities for NetFortris and the customers of NetFortris services. As part of the assessment Trustwave analyzed an array of both customer-facing and internal infrastructure services.

Overview

NetFortris offers their customers Infrastructure as a Service (IaaS) solutions, which their customers may use to process, or transmit cardholder data. IaaS offerings include physical plants and data center facilities, networking firewalls/security, and servers and storage.

Customer facing services including Identity and Access Management, Compute, Networking, Web & Mobile, Analytics, Management & Security, and Hybrid Integration were included within the assessment. Additionally, Trustwave assessed NetFortris' internal infrastructure services including Network Infrastructure and Tools, Security Services and Tools, Remote Access, Incident Management System, Identity and Access Management Infrastructure, Release Management, and Account and Subscription Management.

Responsibility

Customers of NetFortris are ultimately responsible for their own PCI DSS compliance. The following tabs describe the various responsibilities of NetFortris, their customers, or both to achieve PCI DSS compliance. In all assessments, proper scoping is key to success. For cloud deployments, reading the PCI requirements to understand their intent, and correlating this Responsibility Summary will aid customers in planning ahead for a successful assessment.

As a Level 1 Service Provider, NetFortris allows for their customers to satisfy specific PCI DSS requirements cited herein through usage of their Attestation of Compliance. This reliance is dependent on which NetFortris services are being leveraged and how they are being implemented by the customer.

Most requirements, however, require an understanding of the distribution of responsibilities between NetFortris and their customers to fully meet PCI DSS compliance. In addition, some requirements are fully the responsibility of NetFortris customers to implement to meet PCI DSS compliance.

In general, responsibilities can be understood as follows:

IaaS instances: very little difference from traditional self-hosted servers, with NetFortris providing the datacenter networking compliance.

Attestation of Compliance

NetFortris's PCI DSS Attestation of Compliance can be requested as need to comply with customer compliance efforts.

Responsibility Summary

ver 2-21-2019	Customer	NetFortris	NetFortris exception	Exception description
Requirement 1 - Install and maintain a firewall configuration to protect cardholder data		Partial	1.3.4 n/a	No cardholder data network for which NetFortris is responsible
		Partial	1.3.6 n/a	NetFortris does not store cardholder data
Requirement 2 - Do not use vendor-supplied defaults for system passwords and other security parameters		Partial	2.1.1 n/a	No wireless environments connected to the in-scope environment
		Partial	2.2.3 n/a	NetFortris does not run any insecure services, daemons or protocols.
		Partial	2.6 n/a	NetFortris is not a shared hosting provider.

ver 2-21-2019	Customer	NetFortris	NetFortris exception	Exception description
Requirement 3 - Protect stored cardholder data	X	Partial	3.3 n/a	No PAN is in possession of NetFortris. PAN is responsibility of customers, if present.
	X	Partial	3.4 n/a	PAN Storage is NetFortris' customer responsibility. NetFortris has no CHD storage
		Partial	3.4.1 n/a	Full disk encrpytion is not used
	X	Partial	3.5 n/a	This requirement, if present is the responsibility of NetFortris' customer. NetFortris does not store CHD
	X	Partial	3.5.1 n/a	This requirement, if present is the responsibility of NetFortris' customer. NetFortris does not store CHD
	X	Partial	3.5.2 n/a	This requirement, if present is the responsibility of NetFortris' customer. NetFortris does not store CHD
	X	Partial	3.5.3 n/a	This requirement, if present is the responsibility of NetFortris' customer. NetFortris does not store CHD
	X	Partial	3.5.4 n/a	This requirement, if present is the responsibility of NetFortris' customer. NetFortris does not store CHD
		Partial	3.6 n/a	NetFortris does not share keys with their customers for the purpose of encrypting cardholder data

		Partial	3.6.1 n/a	NetFortris does not generate keys for its customers for the purpose of encrypting cardholder data.
		Partial	3.6.2 n/a	NetFortris does not distribute keys for its customers for the purpose of encrypting cardholder data
		Partial	3.6.3 n/a	NetFortris does not store keys for its customers for the purpose of encrypting cardholder data.
		Partial	3.6.4 n/a	NetFortris does not have a definied crypto-period for its customers for the purpose of encrypting cardholder data
		Partial	3.6.5 n/a	NetFortris does not retire or destroy keys for its customers for the purpose of encrypting cardholder data
		Partial	3.6.6 n/a	NetFortris does not use manual clear-text key management for its customers for the purpose of encrpyting cardholder data
		Partial	3.6.7 n/a	NetFortris does no substitute keys for its customers for the purpose of encrypting cardholder data
		Partial	3.6.8 n/a	NetFortris does not have key custodians for cardholder data

ver 2-21-2019	Customer	NetFortris	NetFortris exception	Exception description
Requirement 4 - Encrypt transmission of cardholder data access open, public networks		Partial	4.1.1 n/a	NetFortris does not use wireless networks to transmit CHD
Requirement 5 - Protect all systems against malware and regularly update anti-virus software or programs		X		
Requirement 6 - Develop and maintain secure systems and applications		Partial	6.3 n/a	NetFortris does not provide development services or develop custom code in use in the in-scope environment, or to store, transit or forward CHD
		Partial	6.3.1 n/a	NetFortris does not provide development services or develop custom code in use in the in-scope environment, or to store, transit or forward CHD
		Partial	6.3.2 n/a	NetFortris does not provide development services or develop custom code in use in the in-scope environment, or to store, transit or forward CHD
		Partial	6.4.3 n/a	NetFortris does not handle PAN in any form, including as testing data
		Partial	6.5 n/a	NetFortris does not develop custom code.
		Partial	6.6 n/a	NetFortris has no public-facing web applications in use in the in-scope environment

ver 2-21-2019	Customer	NetFortris	NetFortris exception	Exception description
Requirement 7 - Restrict access to cardholder data by business need to know		X		
Requirement 8 - Identify and authenticate access to system components		Partial	8.1.5 n/a	NetFortris does not provide remove vendor access
		Partial	8.5.1 n/a	NetFortris does not access customer premises POS or servers
		Partial	8.7 n/a	NetFortris maintains no databases containing CHD

ver 2-21-2019	Customer	NetFortris	NetFortris exception	Exception description
Requirement 9 - Restrict physical access to cardholder data		Partial	9.1.2 n/a	Netfortris (and its collocated data center providers) have no network jacks located in public areas
		Partial	9.5.1 n/a	NetFortris does not store media backups containing CHD
		Partial	9.6 n/a	NetFortris has no media which contains CHD stored, no any CHD on paper media
		Partial	9.6.1 n/a	NetFortris has no media which contains CHD stored, no any CHD on paper media

		Partial	9.6.2 n/a	NetFortris has no media which contains CHD stored, no any CHD on paper media
		Partial	9.6.3 n/a	NetFortris has no media which contains CHD stored, no any CHD on paper media
		Partial	9.8.1 n/a	NetFortris has no hard-copy materials containing CHD
		Partial	9.8.2 n/a	NetFortris has no hard-copy materials containing CHD
		Partial	9.9 n/a	NetFortris maintains no devices that capture cardholder data
		Partial	9.9.1 n/a	NetFortris maintains no devices that capture cardholder data
		Partial	9.9.2 n/a	NetFortris maintains no devices that capture cardholder data
		Partial	9.9.3 n/a	NetFortris maintains no devices that capture cardholder data

ver 2-21-2019	Customer	NetFortris	NetFortris exception	Exception description
Requirement 10 - Track and monitor all access to network resources and cardholder data		Partial	10.2.1 n/a	NetFortris has no cardholder data it manages
		Partial	10.5.4 n/a	NetFortris has no external-facing technologies in the in-scope environment
Requirement 11 = Regularly test security systems and processes		X		
Requirement 12 - Maintain a policy that addresses information security for all personnel		X		
Appendix A1 - Additional PCI DSS Requirements for Shared Hosting Providers			n/a	NetFortris is not a shared hosting provider
Appendix A2 - Additional PCI DSS Requirements for Entities using SSL / early TLS			n/a	NetFortris is not using SSLv3 or TLS v1.0 or v1.1