Schedule B20 – Service Description
Universal Threat Management

1. Service Name:

UTM

2. Service Term

All services under this schedule shall individually each be on a 5 year term from the date of installation. Upon each expiration, the term shall renew automatically for an additional term equal to the Service Term listed herein (each a "Renewal Service Term") unless the Service is terminated at the end of the Service Term or at the end of any Renewal Service Term by a Party notifying the other in writing of such intention no later than ninety (90) days prior to the end of the Initial Service Term or Renewal Service Term, as the case may be. At the end of each Renewal Service Term, an additional Renewal Service Term will commence unless the Service is terminated in accordance with the foregoing.

3. Service Summary:

Comwave Universal Threat Management ("UTM") is a solution that encompasses the Comwave UTM Controller and the optional Comwave UTM Analytics. Both services are monthly subscription based for customers with eligible Comwave Services. UTM has multiple advanced network security functions that provide superior visibility and protection over traditional firewalls. Commonly referred to as Unified Threat Management, features include Intrusion Prevention (IPS), Application Control, Anti-Virus and Anti-Spyware protection, Web Content Filtering, and more. The service is continuously updated based on the latest threat signatures.

The UTM platform is in the Comwave core and is currently powered Fortinet. These firewall appliances reside at the edge of Comwave's core network and inspect traffic inbound or outbound from the Internet, applying the configured security policies.

All equipment is housed in one of Comwave's secure data centers, with redundant Internet connections, high availability internal switching fabric, dual battery/diesel backup power. These premises are restricted by card key access to authorized employees only, and are under continuous 24x7 video surveillance.

4. Service Specifications:

Comwave reserves the right to change these Service Specifications to accommodate new or upgraded hardware and UTM, changes in vendor-recommended best practices, or other operational concerns. If any such change should materially diminish the quality or capability of the service, Comwave shall promptly provide written notice to Customer of such change, and Customer may elect to terminate the contract within 30 days of such notice.

UTM Basic: Allows you to choose one of three pre-defined profiles to protect your company. The profile selected is used to protect all your sites. All profiles include IPS, Anti-Virus/Anti-Malware, Botnet prevention, Automatic Updates.

Profile Name	Content Filter
Strictly Business	No Adult, No Social, No video.
Business Casual	No Adult content
Open	No web filtering

UTM Enhanced: Includes IPS, Anti-Virus/Anti-Malware, Botnet prevention, category-based website blocking & phishing URLs, Safe Search, Custom Web Filtering, Application Control, Email Alerts, Self-Service Web Portal, Up to 5 Custom Profiles, and automatic updates. UTM Enhanced is managed through the Comwave UTM Controller portal.

Schedule B20 – Service Description
Universal Threat Management

UTM Enhanced Edge: Includes IPS, Anti-Virus/Anti-Malware, Botnet prevention, category-based website blocking & phishing URLs, Safe Search, Custom Web Filtering, Application Control, Email Alerts, Self-Service Web Portal, Up to 5 Custom Profiles, and automatic updates. UTM Enhanced Edge is managed through the an on-site FortiGate appliance.

Features:

- **IPS:** Intrusion Prevention Service provides real-time detection and filtering of network and application attacks by continuously monitoring your network for malicious traffic. It uses a database of more than 8000 known threats to stop attacks that evade conventional firewall defenses. It also provides behavior-based heuristics, enabling the system to recognize threats for which no signature has yet been developed.
- **Anti-Virus:** Scan email and web traffic for virus signatures. The anti-virus service employs advanced virus, spyware, and heuristic detection engines to prevent both new and evolving threats from gaining access to your network and its valuable content and applications.
- **Anti-Malware, Block Malicious Websites/Phishing URLs, Botnet Prevention:** Blocks known botnets, malicious websites and phishing URLs using extensive and continuously updated FortiGuard signature database.
- **Application Control:** Ability to control discrete functions lets you define and enforce policies for thousands of applications running across the network regardless of port or the protocol used for communication.
- **Web Content Filtering:** Allows Customer to control the types of web content a user may view. Customize the web content filtering engine specifically to your company's needs using multiple pre-defined categories.
- **Email Alerts:** The UTM can be configured to send notification of anti-virus and IPS security events to one email address of choice.
- **Automatic Updates:** Continuously updated protection. FortiGuard Labs' global research team continuously monitors the evolving threat landscape. They deliver rapid product updates and detailed security knowledge, providing protection from the latest threats. See http://www.fortiguard.com/ for more information.

Important Notes:

1. Encrypted traffic
   Network traffic that is encrypted cannot be scanned, however Comwave supports SSL certificate inspection, which inspects the header information of the packets. It is used to verify the identity of web servers to help ensure HTTPS protocol isn't used as a workaround to access sites you have blocked using web filtering.

2. Off-Net Internet Access/Split Tunneling

   Off-net Internet access services do not connect to the Comwave network and therefore, traffic does not pass through the UTM. The exception is for subscribers of VPN services, where off-net traffic is typically routed back to the Comwave core network using VPN and can then pass through the UTM. If split-tunneling is enabled at the site router, traffic destined for the Internet will not VPN back to the Comwave core network, and therefore will not be scanned by the UTM.

3. Whitelists not permitted

   Static URL Filtering is designed to complement category based filtering. Any website exceptions to the general rules laid out though category filtering are entered using this field. The Static URL Filter should not be used to create a whitelist. It is critical to performance to block content using the specific content categories in UTM Controller, rather than creating a whitelist that only allows sites you want to allow. Due to the dynamic source content of modern websites, whitelists can very quickly become cumbersome to manage, and can impact network performance.

4. On-Net to On-Net Traffic

   By default, traffic passing between on-net locations on the secure network does not pass through the UTM and is not scanned. It can however be configured as an option, if required.

Schedule B20 – Service Description
Universal Threat Management

UTM Analytics

This Service provides IT and security professionals with an online reporting engine with insightful data of what is being attacked and where possible vulnerabilities exist. UTM Analytics may be purchased an as optional add-on on eligible plans.

Monthly Plan

The rate is based on the quantity of log data being processed in GB per day, with up to 30 days of analytics. If the allocated storage quota (GB/day x 30 days) is used up before 30 days, then the logs will rollover and the oldest logs will be overwritten. Plan overages are billed in GB increments.

Includes:

- Up to 30 days of analytics
- Daily Log allocation in GB, as specified by the subscription plan
- Storage quota in GB of 30 days x Daily Log allocation
- Reports are kept for 3 months
- 3 administrator accounts. Additional accounts may be purchased.

Please refer to Quick Start Guide for additional details. Reports are subject to change from time-to-time

5. Standard Pricing:

Monthly Recurring Charges

The Standard Pricing set forth here shall apply to any items not explicitly set forth in the Service Order. These are the current rates for these services and are subject to change without notice.

The Monthly Recurring Charges ("MRC") shown below shall apply to all UTM services required by Customer for each internet or private connection. Monthly Recurring Charges shall be billed in advance for each following month.

Charges for services or add-ons added during a billing period shall be prorated to the start of the next billing period for that Customer, and subsequently billed in advance. No refunds or credits will be given for services terminated during a billing period.

Item	Monthly Fee per site	Setup
UTM BASIC	Tier 1 $15 up to 50Mbps Tier 2 $30 up to 100Mbps Tier 3 $80 up to 100-250Mbps Tier 4 $375 up to 1GB	$250
UTM Enhanced (Requires Controller)	Tier 1 $20 up to 50Mbps Tier 2 $40 up to 100Mbps Tier 3 $110 up to 100-250Mbps Tier 4 $500 up to 1GB	$500

Controller for UTM Enhanced

Item	Monthly Fee	Overage	Setup
UTM Controller	$40		$250
UTM Analytics	$500 1 GB of Log Data	$100/GB	$500

Schedule B20 – Service Description
Universal Threat Management

Schedule B20 – Service Description
Universal Threat Management

Service Charges

Service Change	Fee
Labour	$150/hour
Order cancellation within 24 hours of this Service Order	No Charge

6. Service Responsibilities:

Comwave Shall:

- Supply, house, power, and maintain the UTM Equipment located in its data center infrastructure.
- Maintain UTM infrastructure properly, applying any firmware or other patches as required to ensure appropriate security.
- Apply all appropriate upgrades as may be required from time-to-time
- Assist Customer's Technical Contact(s) in resolving problems with the UTM. This responsibility extends to Comwave contacting the infrastructure vendor to identify and resolve issues.

Customer Shall:

- Be responsible for ensuring the correct UTM profile and filtering has been activated.
- Monthly validation testing
- Be responsible for the effects of any security policy it implements on the UTM.
- Be aware that UTM functions can have unintended adverse effects on application use. Troubleshooting on particular application issues will be subject to Professional Services fees.
- Agree that the UTM service is designed to reduce the risk of a security breach. Comwave does not warrant that the service will be error-free or completely secure.

7. Disclaimer:

COMWAVE UTM IS PROVIDED "AS IS" AND COMWAVE MAKES NO REPRESENTATIONS OR WARRANTIES, AND COMWAVE DISCLAIMS ALL REPRESENTATIONS, WARRANTIES, AND CONDITIONS, ORAL OR WRITTEN, EXPRESS OR IMPLIED, ARISING FROM COURSE OF DEALING, COURSE OF PERFORMANCE, OR USAGE IN TRADE, OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY, QUALITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, OR SYSTEMS INTEGRATION. WITHOUT LIMITING THE FOREGOING, COMWAVE MAKES NO WARRANTY, REPRESENTATION, OR GUARANTEE AS TO THE UTM'S USE OR PERFORMANCE AND DOES NOT WARRANT, REPRESENT, OR GUARANTEE THAT THE OPERATION OF THE UTM WILL BE FAILSAFE, UNINTERRUPTED, OR FREE FROM ERRORS OR DEFECTS OR THAT THE UTM WILL PROTECT AGAINST ALL POSSIBLE THREATS.

WITHOUT LIMITING ANYTHING ELSE, COMWAVE HAS NO RESPONSIBILITY FOR, AND YOU WILL INDEMNIFY AND HOLD HARMLESS COMWAVE FROM, ALL CLAIMS, SUITS, DEMANDS, AND PROCEEDINGS ALLEGING, CLAIMING, SEEKING, OR ASSERTING, ANY LIABILITY, LOSS, OBLIGATION, RISK, COST, DAMAGE, AWARD, PENALTY, SETTLEMENT, JUDGMENT, FINE, OR EXPENSES (INCLUDING ATTORNEYS FEES) ARISING FROM OR IN CONNECTION WITH YOUR USE OF THE UTM.

UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER IN TORT, NEGLIGENCE, CONTRACT OR OTHERWISE, SHALL EITHER PARTY BE LIABLE TO THE OTHER UNDER THIS AGREEMENT OR IN CONNECTION WITH ITS SUBJECT MATTER FOR ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, EXEMPLARY, CONSEQUENTIAL, OR EXTRA-CONTRACTUAL DAMAGES OF ANY KIND, LOSS OF GOODWILL, LOSS OF PERSONNEL SALARIES, LOST PROFITS

OR REVENUE, DAMAGES DUE TO WORK STOPPAGE AND/OR COMPUTER FAILURE OR MALFUNCTION, AND/OR COSTS OF PROCURING SUBSTITUTE UTM OR SERVICES, WHETHER OR NOT FORESEEABLE, EVEN IF THE EXCLUSIVE REMEDIES PROVIDED BY THIS AGREEMENT FAIL OF THEIR ESSENTIAL PURPOSE AND EVEN IF EITHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OR PROBABILITY OF SUCH DAMAGES. b) REGARDLESS OF WHETHER THE CLAIM FOR SUCH DAMAGES IS BASED IN CONTRACT, TORT AND/OR ANY OTHER LEGAL THEORY, IN NO EVENT SHALL EITHER PARTY'S AGGREGATE LIABILITY TO THE OTHER PARTY FOR DIRECT DAMAGES UNDER THIS AGREEMENT OR IN CONNECTION WITH ITS SUBJECT MATTER EXCEED THE AMOUNT OF SIX (6) MONTHS MONTHLY FEES PAID UNDER THIS SCHEDULE DURRING TWELVE (12) MONTHS IMMEDIATLEY PREECEEDING SUCH CLAIM. FOR THE SERVICES DESCRIBED HEREIN, THE TERMS OF THIS SCHEDULE SHALL PREVAIL IN THE EVENT OF A CONFLICT WITH ANY OTHER TERMS IN THIS AGREEMENT. PRODUCT SPECIFICATIONS ARE SUBJECT TO CHANGE WITHOUT NOTICE. SOME FEATURES LISTED HEREIN REQUIRE ADDITIONAL HARDWARE, PACKAGES AND FEES.

8. Activation and Installation:

Within approximately ten (10) business days of receipt of Customer's order, Comwave shall provision the requested UTM and provide administrative access to the online management portal to Customer.

If Customer requests that Comwave complete the initial configuration with customized policies, allow (5) additional business upon final determination of the policies required.

After initial activation, within two (2) business days of receipt of Customer's request to modify a policy, Comwave shall make the requested change and inform Customer when it has been implemented. Customer may also make changes at any time via the self-service web portal.

9. Service Level Objectives:

Support Response

- Server Not Responding: Some problem with the UTM or its environment that is causing a complete interruption of service.
  9am-5pm EST: under 30 minutes to respond and begin troubleshooting
  After Hours: under 90 minutes
- Administration Issues: A problem or question regarding the use or configuration of the UTM
  9am-5pm EST: Under 120 minutes to respond to query

Chronic Outages

Comwave commits that the UTM Service will continue to function without Chronic Outages after its acceptance. If the UTM Service suffers from Chronic Outages, then Customer may cancel the Service without incurring any Early Termination penalty for that Service.

Chronic Outages are defined as five or more Service Interruptions, each lasting two hours or more, within any calendar month. A Trouble Ticket must be opened for each Service Interruption while the interruption is occurring, and Customer contact must provide reasonable assistance while the Comwave technicians attempt to resolve the problem. Customer must give notice of intent to cancel within 7 calendar days after the last Service Interruption. Comwave shall then have 30 calendar days to cure the problem. Comwave shall be deemed to be unable to cure the problem if there are more than two Service Interruptions of two hours or more each during the last 10 calendar days of the cure period.

Modifications

Comwave reserves the right to modify any of the above Service Level Commitments upon 30 days written notice to Customer. These modifications may apply both to new and existing services ordered under this Agreement. If these modifications reduce the future levels of committed Service Delivery for existing services, then Customer may cancel these services. Unless Customer provides notice of intent to cancel existing services within 30 days after written notice was issued by Comwave, Customer is deemed to have accepted the Service Level Commitment modifications for all services ordered under this Agreement.