CORE
MANAGED & HOSTING SERVICES

HIPAA & HEALTHCARE **SECURITY**

COMPLIANCE, SECURITY, VISIBILITY

Every doctor's office, pharmacy, and health care provider in the U.S has to adhere to HIPAA compliance. HIPAA forces healthcare providers to protect patient health data. The most important requirement is to reduce the risk and vulnerabilities associated with the electronic data. To remain compliant, healthcare service providers require network security tools.

Core IT understands the technology challenges that health services providers face as well as the basics of IT security and how to manage HIPAA compliance in the most cost efficient manner.

HIPAA and UTM Firewall

For healthcare services providers, Core IT has come up with UTM Firewall which not only guarantees network security but also complies with selected administrative and technical safeguards required by HIPAA

164.308(a)(1)(ii)(B) Risk management

Required: Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

Our UTM firewall protects the complete network and gives the ability for health services providers to monitor and control every type of traffic, whether coming from the Internet, internal employee systems or network devices.

The single-click port forwarding and outbound traffic filtering allows easy control of traffic in and out of the network.

Healthcare services providers with UTM Firewall email filtering for spam and viruses can control employee Web surfing with access policies and monitoring. The inbuilt intrusion detection and prevention system ensures detection and blocking of attacks.

Connections to remote branch offices, hospitals, and billing and insurance services can be easily established with perfect encryption over IPSec VPNs.

Employees away from the office can connect securely to the network through SSL VPN that provides mutual certificate-based authentication and encrypts traffic between the employee's remote machine and the office network.

164.308(a)(4)(i) Standard: Information access management

Required: Implement policies and procedures for authorizing access to electronic protected health information.

UTM Firewall simplifies data security by allowing healthcare services providers to establish secure network zones for critical data and systems restricting access to health data. With minimal technical knowledge, a security zone can be designated for storing health information and limiting access to specified machines.

Moreover, the UTM firewall architecture can be provisioned to physically segregate network interface cards (NICs) and LANS and helps in reducing improper configurations.

164.308(a)(4)(ii)(A) Isolating health care clearinghouse functions

Required: If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronically protected health information of the clearinghouse from unauthorized access.

UTM Firewall logically segregates clearinghouse servers from the larger network and control the traffic they receive. It's easy to block any number of desired connections from the Internet.

164.308(a)(4)(ii)(B) Access Authorization

Addressable: Implement policies and procedures for granting access to electronic protected health information, for example, access to a workstation, transaction, program, process or other mechanism.

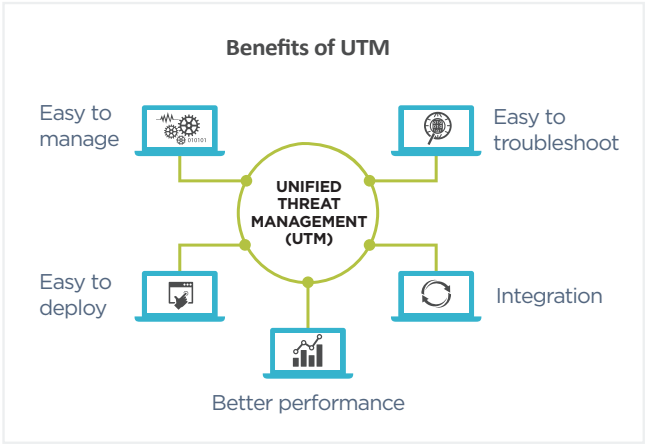
With UTM Firewall traffic that tries to reach or leave a specific machine, server, application or service can be easily restricted or allowed.

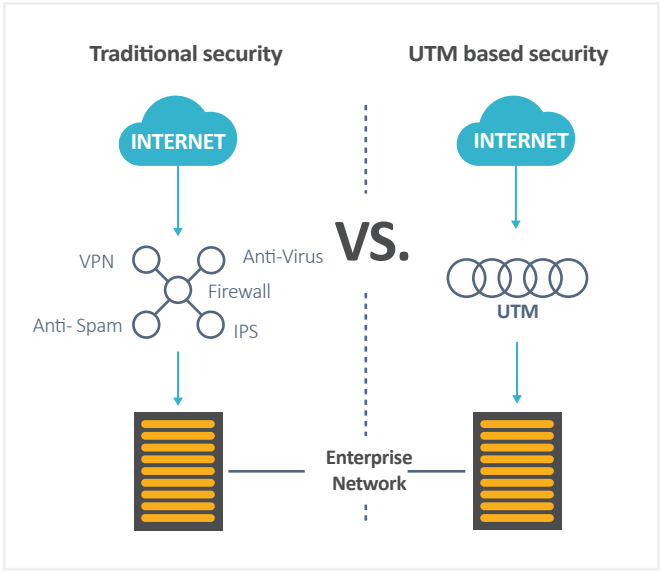
164.308(a)(5)(ii)(B) Protection from malicious software

Addressable: Procedures for guarding against, detecting, and reporting malicious software.

The inbuilt antivirus system scans emails and attachments for viruses and malware. The internal intrusion detection and prevention provides additional safeguards.

PDF reports of security events can be configured to be sent automatically to a desired set of recipients.





164.308(a)(5)(ii)(D) Password management

Addressable: Procedures for creating, changing, & safeguarding passwords.

Each UTM Firewall device has a unique, randomly generated password that can be changed for each administrator of the device. If required, remote access management can be easily disabled or limited to specific source IP addresses.

164.312(a)(2)(iii) Automatic logoff

Addressable: Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

UTM firewall administrator can preset the allowed idle time duration before re-authentication is required.

164.312(a)(2)(iv) Encryption and decryption

Addressable: Implement a mechanism to encrypt and decrypt electronic protected health information.

The patient data is encrypted during the transit between the system by using industry-leading cryptographic algorithms.

MAKING **HIPAA COMPLIANCE EASIER**

Risk Management
Implement security measures to reduce risks & vulnerabilities.

Information Access Management
Implement policies & procedures for authorizing access to electronic protected data

Healthcare Clearinghouse
The clearinghouse must implement policies & procedures that protect the data

Access Authorization
Implement policies & procedures for granting access to protected data

Protection From Malicious Software
Procedures for guarding detecting, & reporting malicious software.

Password Management
Procedures for creating, changing, & safeguarding passwords.

Automatic Logoff
Implement auto logoff after predetermined time of inactivity.

Encryption & Decryption
Implement a mechanism to encrypt & decrypt electronic protected data.

E: info@coreitx.com • **W:** www.coreitx.com

1.212.271.8732 (**USA**) +91 22 4006 5252 (**India**) +971-554506553 (**Dubai**)