A TLC srl
Via 1° Maggio, 26 / 60131 Ancona (Italy)
Phone +39 071 250651 / Fax +39 071 2506518
www.aethra.com - info@aethra.com

All-in-One Device

NGFW is a VNF (Virtual Network Function) software feature optionally integrated in selected Aethra Telecommunications Routers, providing cost-saving benefits by combining router and firewall functions on a single device.

Fully Intel Based x86 Compute Power

All the solutions are based on Intel x86 architecture, with 4, 8 and up to 16 cores to ensure maximum flexibility and performance up to 5Gbps aggregated.

OPNSense Based

Aethra Telecommunications Next Generation Firewall (NGFW) solution is based on the widely adopted OPNSense architecture.

APPLICATION BRIEF

Aethra Telecommunications® NGFW Next Generation Firewall

Aethra Telecommunications Next Generation Firewall (NGFW) is a security solution available for XV Series Business Routers and Universal CPEs.

It is deployed as a Virtual Network Function (VNF) in the service chain by allocating dedicated resources on an XV Series uCPE.

The router and the NGFW act as autonomous entities jointly defining the full service. The resource allocation between the router and the NGFW allows full segregation and always guarantees deterministic performances: NGFW does not impact routing performances, provided that the correct number of CPU cores are available for both the router and the NGFW subsystems.

NGFW complements the advanced business router features present in the ATOS operating system, enabling XV Series CPEs to be deployed as a complete and integrated access and security solution for Small and Medium Enterprises.

ADVANTAGES OF AN ON-PREMISES APPROACH

Integrating NGFW and access router in a single hardware platform reduces space and power consumption.
The on-premises solution also assures significant cost savings compared to cloud computational resources and bandwidth.

WEB BASED USER INTERFACE

The Next Generation Firewall is fully integrated with the router and, at the same time, is configured as a separate entity with its own dedicated WEBGUI.

Access to the WEBGUI can be limited with different privileges levels so that Communication Service Providers (CSPs) can offer Next Generation Security Solutions to their customers without the need to give them access to the router itself (Figure 1).

MANAGEMENT AND SOFTWARE UPDATES

NGFW core application updates are entirely managed via the router using ATOS software bundles and are completely independent from the XV Series ATOS release. The NGFW can be updated without impacting the router software release.

Any core application or plugin update is

A TLC srl
Via 1° Maggio, 26
60131 Ancona (Italy)
Phone +39 071 250651
Fax +39 071 2506518
www.aethra.com
info@aethra.com

completely under control of the CSP, who is able to decide what to deploy and when.

On the other hand, NGFW rules and definitions (for example for IPS / IDS, Antivirus and Web Proxy, which need to be kept constantly refreshed) can be updated directly from the WEBGUI without the need for a dedicated package.

Regular automatic updates can be easily configured as well by the CSP or even directly the end user (Fig. 3).

HIGH AVAILABILITY

Scenarios requiring redundancy are supported and can be setup with two XV Series uCPEs configured in VRRP and running two instances of NGFW configured in HA (one on each Universal CPE).

Thanks to CARP (Common Address Redirection Protocol), multiple NGFW instances can share a single IP address and provide redundancy in case one of the NGFWs fails. pfSync synchronizes the state of multiple firewalls, ensuring that all the ones in the high availability cluster have the same configuration and firewall rules.

The VRRP (Virtual Router Redundancy Protocol) of the Aethra Telecommunications router allows for total redundancy of routers / firewalls system and provides automatic failover and seamless switchover, ensuring that there are no interruptions to the network services.

MODULAR SOLUTION

Next Generation Firewall is a modular solution, which includes:

- Stateful Firewall
- Intrusion Detection and Intrusion Prevention System (IPS / IDS)
- VPN
- WEB Proxy
- Captive Portal
- Antivirus

Single modules can be enabled or disabled according to the CSPs business model and the service that they want to offer to their customers.

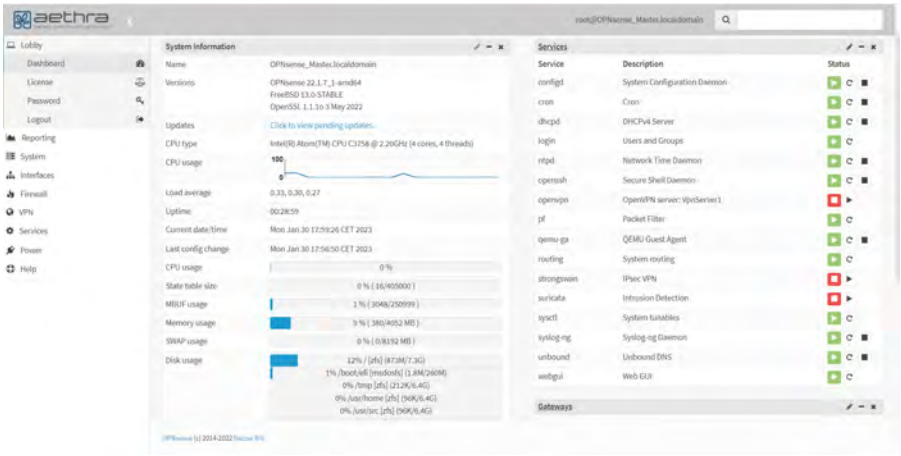

Fig. 1: Next Generation Firewall dashboard.

Stateful Firewall

The stateful firewall module includes support for TCP, UDP, ICMP, and other protocols, as well as advanced options for managing and filtering incoming and outgoing traffic like GeoIP.

GEOIP SUPPORT

Using a vast database of IP addresses and their corresponding geographical locations, the GeoIP feature allows to easily block or restrict access from specific regions, countries, or even cities.

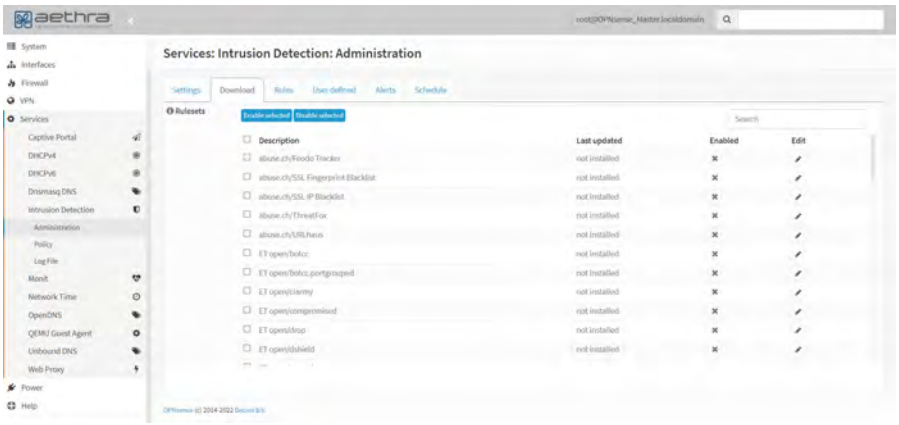

Fig. 2: IPS / IDS Rulesets Management.

CONTENT FILTERING

NGFW inspects packets at the application layer of the TCP/IP stack and can identify applications to control access to predefined lists of sites in specific categories, such as social, adult, music, sports sites and more.

NGFW Stateful Firewall module use cases include for example securing networks for schools and colleges: it can be configured to block access to inappropriate or harmful websites, ensuring students and faculty have access to safe and appropriate content.

IDS / IPS

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) scan network traffic for signatures that match known cyber attacks. The use of this module prevents the delivery or circulation of malicious packets to stop the attack.

DEEP PACKET INSPECTION

IPS uses Deep Packet Inspection technology to identify if traffic destined to the network is malicious or not.

The IPS rulesets are updated periodically via the ETOpen / ETPro rule lists (Fig. 2).

SSL INSPECTION

Aethra Telecommunications NGFW supports proxy SSL inspection to detect hidden malware, ransomware and other HTTPS-borne attacks.

MULTITHREADED ARCHITECTURE

The multithreaded architecture of IPS takes full advantage of the XV Series uCPEs multicore architecture by splitting forwarding traffic into multiple threads and running them on different CPU cores.

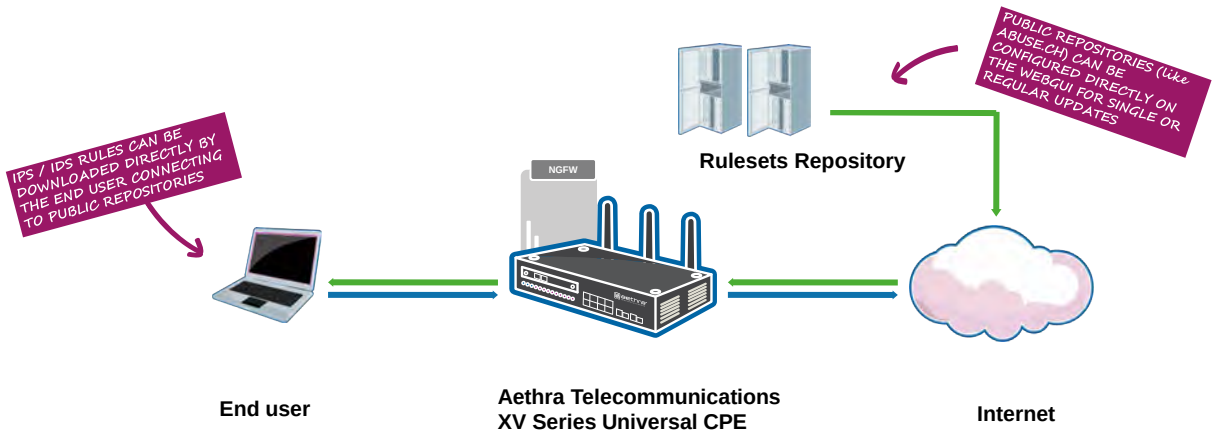

Fig. 3: IPS / IDS Rulesets and signatures.

VPN

NGFW supports a wide range of VPN technologies, from SSL VPNs to IPsec. The use of IPsec allows high throughput performance leveraging Intel AES-NI technology (Fig. 4).

REMOTE-ACCESS AND ROADWARRIOR

NGFW supports both site-to-site VPN tunnels (to allow multiple users traffic to flow through each VPN tunnel) and roadwarrior architectures.

Remote-access and roadwarrior VPN are both performed over SSL VPN or IPsec.

TWO-FACTOR AUTHENTICATION AND OTP

NGFW supports Two-Factor Authentication (2FA) for its users: when connecting to a corporate network, users must first enter their RADIUS or Active Directory credentials, followed by a time-based one-time password (OTP).

This OTP (a digital code) is displayed on a dedicated smartphone application such as Google Authenticator (Fig. 5).

Web Proxy

The Web Proxy module includes a caching proxy that reduces bandwidth usage and improves response times by caching and reusing frequently-requested web pages.

CATEGORY BASED WEB FILTERING

Web proxy supports category based web filtering. It is designed to increase network security by inspecting traffic using the built-in proxy cache and one of the freely available or commercial blacklists.

HTTPS TRANSPARENT PROXY

NGFW intercepts and inspects encrypted HTTPS traffic, such as browsing activities. It acts as a "man-in-the-middle" between the client and the server and can be used

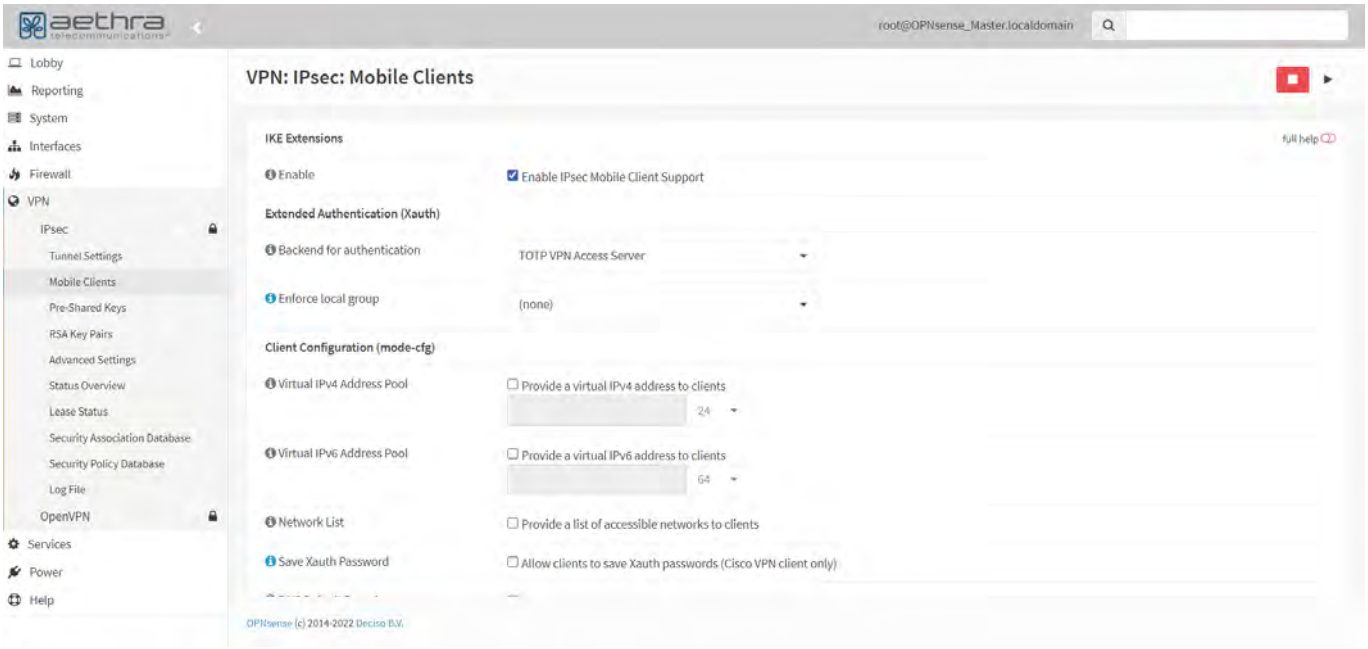

Fig. 4: VPN Configuration for IPsec Mobile Clients.

to monitor, filter and control Internet access.

The https transparent proxy decrypts, inspects and then re-encrypts the traffic. The end-user is unaware of the interception. This provides organizations with visibility and control over encrypted traffic while also maintaining privacy and security for the users.

Captive Portal

The Captive Portal module is designed to provide secure authentication for users via HTTPS or splash-only portal. It supports multiple authentication sources, including LDAP, RADIUS and local user manager.

VOUCHER MANAGER

The platform also offers the possibility to generate Vouchers and Tickets for guest users. Vouchers can be exported to a csv file and merged with a template for a professional handout.

With timeouts and "welcome back" options, it is possible to set idle and hard timeouts, allowing users to resume their session without having to re-authenticate.

Antivirus

The Antivirus moduled is based on an ICAP (Internet Content Adaptation Protocol) server that implements virus scanning and content filtering in the transparent HTTP proxy caches.

NGFW scans incoming HTTP traffic for viruses and malware, blocking and cleaning infected content before they reach the end user.

For more info

For more info on the Aethra Telecommunications XV Series routers and Universal CPEs and on the Next Generation Firewall solutions, please visit www.aethra.com or contact your sales representative.

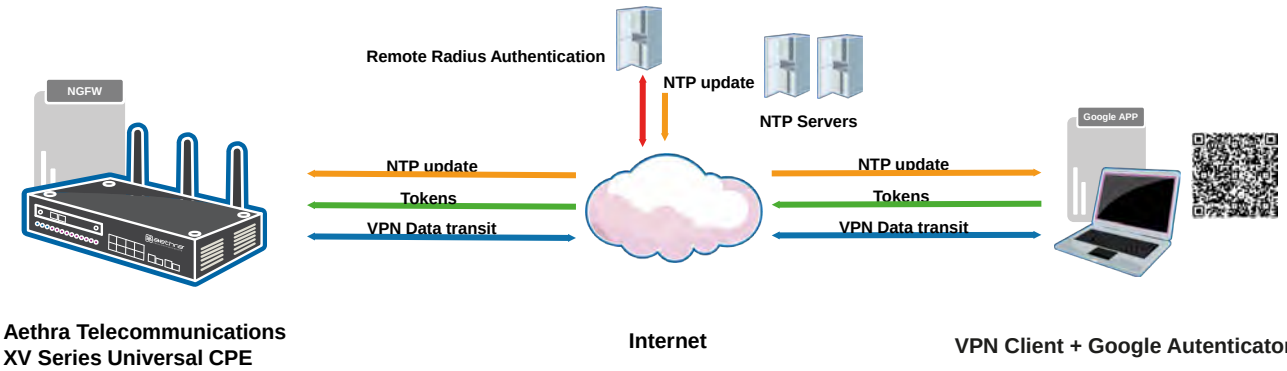

Fig. 5: Two Factor Authentication and OTP.

XV Series Universal CPE	Scenario	# cores for NGFW	IMIX410 IPS / IDS off	IMIX410 IPS / IDS on	1500byte IPS / IDS off	1500byte IPS / IDS on
XV8800-4C8R120D **XV8800-VE2-4C8R120D**	• Connectivity w/ WAN FTTH up to 1G • Connectivity w/ WAN FTTC VDSL2	2	1.2Gbps aggregated	300Mbps aggregated	2Gbps aggregated	600Mbps aggregated
XV8800-8C16R120D **XV9421-8C16R120D**	• Connectivity w/ WAN FTTH 1G • Connectivity w/ WAN FTTH 2.5G	4	1.7Gbps aggregated	1.3Gbps aggregated	3Gbps aggregated	3Gbps aggregated
XV9440-16C16R128D	• Connectivity w/ WAN FTTH up to 10G (ex. XGSPON)	8	Up to 5Gbps[1] aggregated			

NOTES

[1] Performances in 10G scenarios are highly related to the specific configuration of both the router and the NGFW.

Table 1: Next Generation Firewall Performance Figures.

Fig. 6: Aethra Telecommunications XV8800 / XV8800plus, XV9421 and XV9440 routers and Universal CPEs.

071073106GB Rev.2 (23/02)