Technical Guide

Unified Threat Management (UTM) Offload

Feature Overview and Configuration Guide

Introduction

This guide describes the AlliedWare Plus™ feature known as UTM Offload. This feature is available on the AR4050S from software version 5.4.8-1.1 onwards.

UTM Offload is beneficial when there is a business need to maintain a high level of security, in conjunction with high forwarding performance when using multiple stream-based features.

UTM Offload improves network forwarding performance by offloading some of the advanced security features to a second physical or virtual machine that is automatically managed by the AR4050S.

This second machine is known as the **offload** device, and the AR4050S is referred to as the **forwarding** device.

With the offload device performing security packet processing functions, additional CPU cycles are available on the forwarding device (AR4050S), which in turn increases packet forwarding rates.

Features that have been offloaded are presented on the forwarding device (AR4050S) as if they are running locally. The AR4050S also functions as a PXE boot server. PXE is short for Pre-Boot Execution Environment, pronounced pixie. PXE allows a workstation to boot from a server on a network.

- The AR4050S network boots the offload device using PXE, configures the offload device, and then configures itself to send packets to the device.
- The AR4050S then uses the extra memory and CPU resources on the offload device to reduce its load, thereby increasing its performance.

Products and software version that apply to this guide

This guide applies to the AR4050S, running software version **5.4.8-1.1** or later.

For more information, see the following documents:

- The product's Datasheet
- The product's Command Reference

These documents are available from the above links on our website at alliedtelesis.com.

Licensing

- UTM Offload requires an AT-FL-UTM-OFFLOAD-xYR subscription license. Select from the 1, 3, or 5 year options.
- The UTM Offload feature is installed on the forwarding device (the AR4050S), rather than the offload device.
- Licenses for the UTM features (IP Reputation, URL Filtering and Malware Protection) are installed on the forwarding device. There is no need to get new licenses for the same feature on the offload device.

Content

How does UTM Offload work?

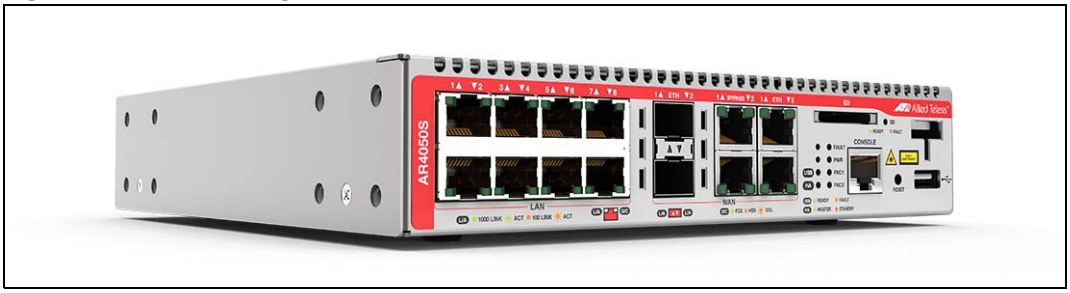
UTM Offload enables some security and threat protection features (IPS, IP Reputation, Malware Protection, and URL Filtering) to be offloaded to a secondary physical or virtual machine that is automatically managed by the AR4050S.

UTM Offload can up to double WAN connection throughput when using these features for real-time threat protection.

The forwarding device - AR4050S:

- boots and manages the offload device.
- configures the offload device.
- presents the status of all features, whether being processed locally on the AR4050S, or on the offload device.
- uses Service Function Chaining (SFC) methodology to send received traffic to the offload device for processing.
- gets the result of that processing back from the offload device and continues packet processing as normal.

Figure 1: The forwarding device - AR4050S



What Features can be Offloaded?

Security features are configured as normal on the AR4050S device, but whenever UTM Offload is enabled, the following advanced threat protection features are all offloaded, if they are configured:

- IPS
- IP Reputation
- Malware Protection
- URL Filtering

The AR4050S automatically manages the offload device for you. You don’t need to configure the offload device, as configuration and the status of all features is presented the same whether offloaded or not.

Setting up UTM Offload

These are the steps required to set up UTM Offload.

- Purchase, download, and install the UTM Offload license on the AR4050S
- Enable UTM Offload on the AR4050S (the forwarding device)
- Set up the offload device

These steps are described in more detail below:

Purchasing, downloading, and installing the UTM Offload license

You only require a UTM Offload subscription license on the AR4050S, you do not need a license on the offload device as well. For information on purchasing, downloading, and installing the UTM Offload subscription license, see the Licensing Feature Overview Guide.

Enabling UTM Offload on the AR4050S

To enable UTM Offload on the AR4050S, you must have a direct Ethernet connection between the offload device and the AR4050S, i.e. from the Gigabit eth1 or eth2 port on the AR4050S to an Ethernet port on the offload device. The Ethernet connection must support a MTU of 1588 or higher. For more detail, see "Setting up the offload device" on page 6.

As an example, to enable UTM Offload and configure interface eth2 and subnet 192.168.100.0/24 to boot and communicate with, and manage the offload device, use the following commands:

```
awplus#configure terminal
awplus(config)#utm-offload interface eth2 subnet 192.168.100.0/24
```

To disable UTM Offload, use the following command:

```
awplus(config)#no utm-offload
```

Configuration notes

The MTU of the UTM Offload device interface is set to 1582 to support the overhead required for the standard Ethernet frames. You can not change this setting.

When configured, the interface of the forwarding device, which connects to the UTM Offload device, is automatically assigned an IP address which is the lowest usable address in the subnet. The interface is reserved for communication with the UTM Offload device and you should not manually configure this interface. The configured IP subnet used for UTM Offload is visible in the **show utm-offload** command, However the assigned IP address is not visible.

The AR4050S manages the offload device and offloads traffic automatically.

Setting up the offload device

The offload device can be any physical computer or virtual machine (VM). To use the UTM Offload feature, there must be a direct Ethernet connection from the forwarding device (AR4050S) to the offload device. The offload device must be configured to PXE boot (network boot) from the forwarding device.

Virtual machine

For instructions on setting up a virtual machine as an offload device, see "Configuring UTM Offload on VMware ESXi Server" on page 8.

Physical computer

If you want to set up a physical computer as an offload device, then the computer must:

- have a serial port, even if nothing is connected to that serial port.
- have a direct Ethernet connection between itself and the AR4050S, i.e. from the Gigabit eth1 or eth2 port on the AR4050S to an Ethernet port on the offload device. The Ethernet connection must support a MTU of 1588 or higher.
- be configured to network boot from the AR4050S. This will usually be done by changing the BIOS settings on the offload device and enabling PXE boot.
  - PXE boot does not currently support IPv6, therefore the Ethernet interface used for off loading is configured with IPv4.
  - The PC vendors website will have information about how to enable PXE boot. For example, to enable PXE Boot for Intel Desktop Boards, see Intel Support.

Specifications

The offload device must have the following minimum specifications:

UTM Offload Device Specifications
■ Multi-core 64-bit x86 processors
■ i5 CPU with 4 cores and 2.3-2.8GHz clock speed
■ 2GB of RAM
■ 4GB of Flash/HDD
■ VMware ESXi Hypervisor 6.x (Note: VMware is the only supported hypervisor if UTM Offload is not run directly on the offload device.)
■ A network card (NIC). Supported models: ■ Intel e1000 ■ Intel e1000e ■ Intel igb ■ VMware vmxnet3
■ At least one non USB storage device
■ Storage devices: Devices that support AHCI mode. ■ If using a SATA HDD, the SATA controller (which the SATA drive connects to) needs to support AHCI

About the Offload Image

The Allied Telesis Next Generation Firewall Appliance (AFA) software release is the image that is automatically downloaded and installed into the UTM Offload device.

The offload image is downloaded from the Update Server by the forwarding device and used to network boot the offload device. The forwarding device automatically downloads a compatible offload image version from the Update Server. Offload image version numbering aligns with other AlliedWare Plus software versions.

For example, an AR4050S running 5.4.8-1.1 downloads the 5.4.8-1.1 version of the AFA image. This process is automatically managed by the Update Server which ensures the correct version is offered to the AR4050S. You do not have to worry about getting the right version of AFA image to match your AlliedWare Plus software release. It is not possible for the forwarding device to boot the offload device with the wrong release.

Checking for image updates on the offload device

New offload device images are automatically downloaded by the forwarding device when detected.

The **default** interval used to detect offload image updates is 60 minutes. You can manually change this setting.

For example:

To change the time interval to 12 hours, use the following commands:

```
awplus#configure terminal
awplus(config)#utm-offload update interval hours 12
```

Figure 2: The **utm-offload update-interval** command parameters

```
awplus#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
awplus(config)#utm-offload update-interval ?
  days     Interval in days
  hours    Interval in hours
  minutes  Interval in minutes
  never    Never update the resource
  weeks    Interval in weeks
awplus(config)#utm-offload update-interval hours 12
```

The offload device image is downloaded from the resource server. The offload resource is tied to the release of software that the AR4050S is running. For more information on the AlliedWare Plus Update Manager, see the Update Manger Feature Overview and Configuration Guide.

Note: Configuring the update interval to **never** and upgrading the forwarding device to a later release without using the command **update afa_offload now** may result in the offload device not working.

Configuring UTM Offload on VMware ESXi Server

Many enterprises today have bare-metal hypervisor technology such as VMware ESXi Server running on powerful server hardware locally, to provide business critical applications and resources. This is a great use case for UTM Offload as businesses can utilize already existing hardware, simply by creating a new VM instance (virtual machine) to provide throughput improvements with the AR4050S while using the Advanced Threat Protection feature set.

There must be a direct Ethernet connection from the forwarding device (AR4050S) to the virtual machine. The virtual machine must be configured to PXE boot (network boot) from the forwarding device.

The PXE boot process make it very easy to setup UTM Offload in ESXi, in addition to the basic UTM Offload requirements for the AR4050S:

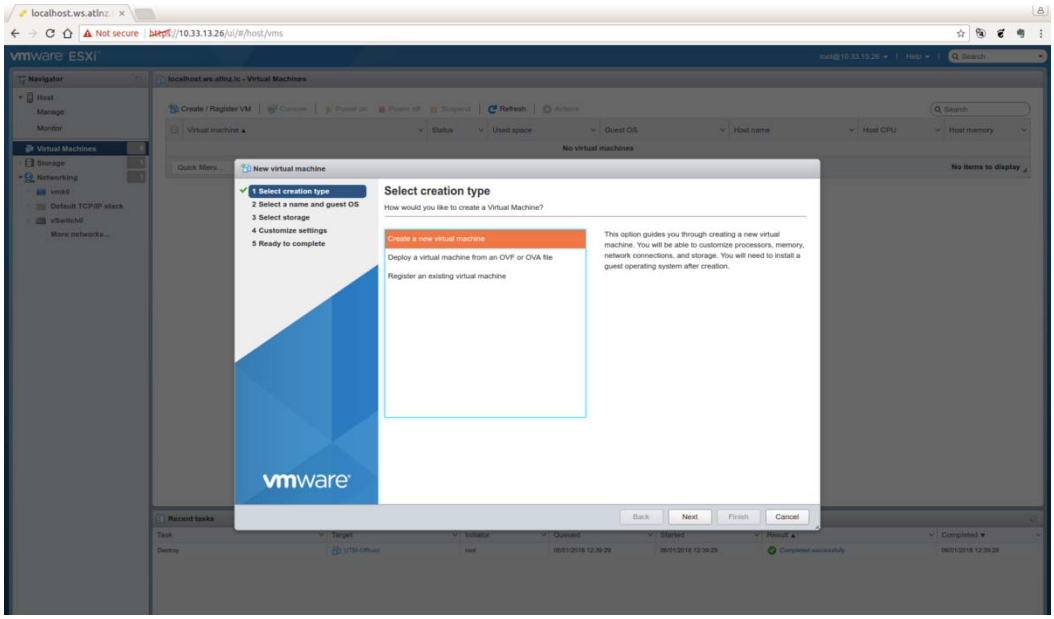
- UTM Offload licence (loaded on to the AR4050S)
- Internet access
- DNS server configuration
- Single UTM Offload configuration command on the ESXi

Simply follow the VMware configuration wizard as shown below, set the MTU of your virtual machine to be at least 1600 bytes, and click **Play**.

Using the configuration wizard

Open the VMware ESXi application, and perform the following steps:

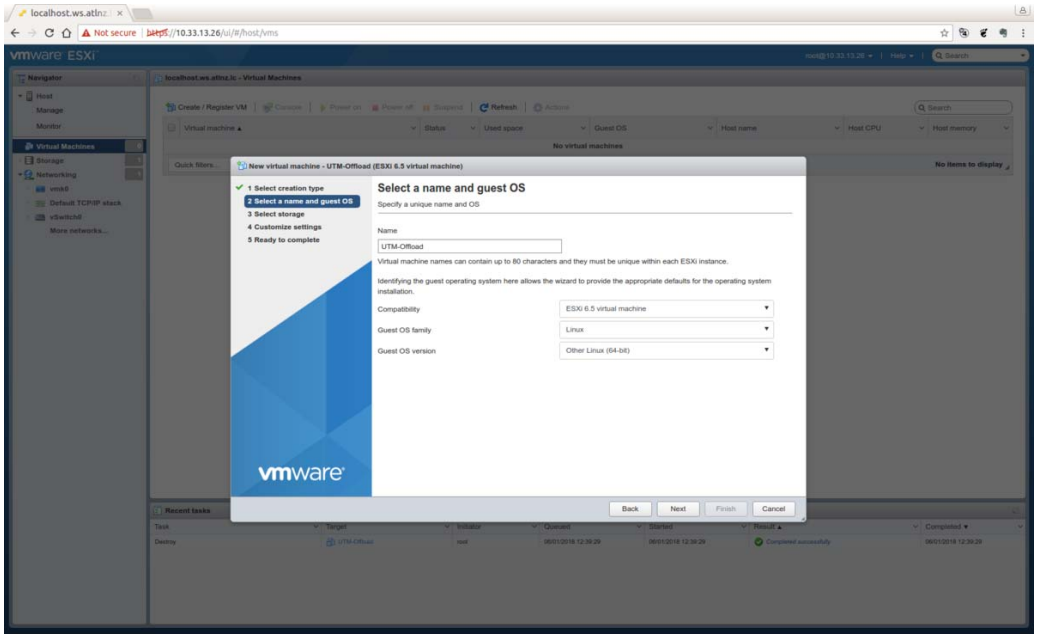
1. From the left side menu, select **Virtual Machines**
2. From the top tabs, select **Create/Register VM** to start the Wizard.



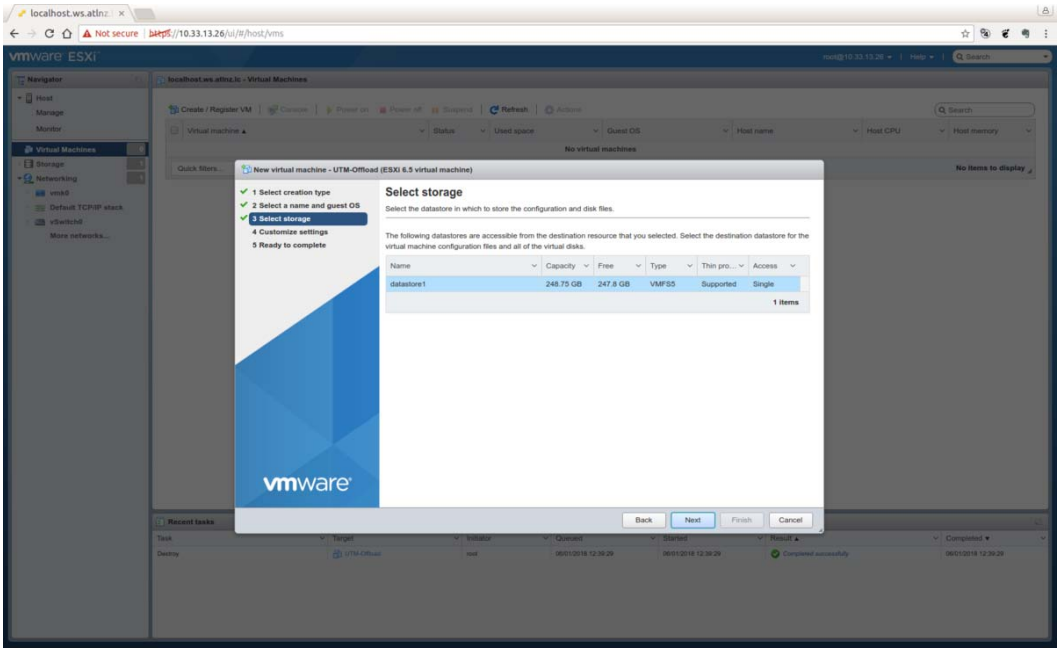
Note: The offload device must have an unused serial port.

3. From the **Select a name and guest OS** page, enter a unique **Name**

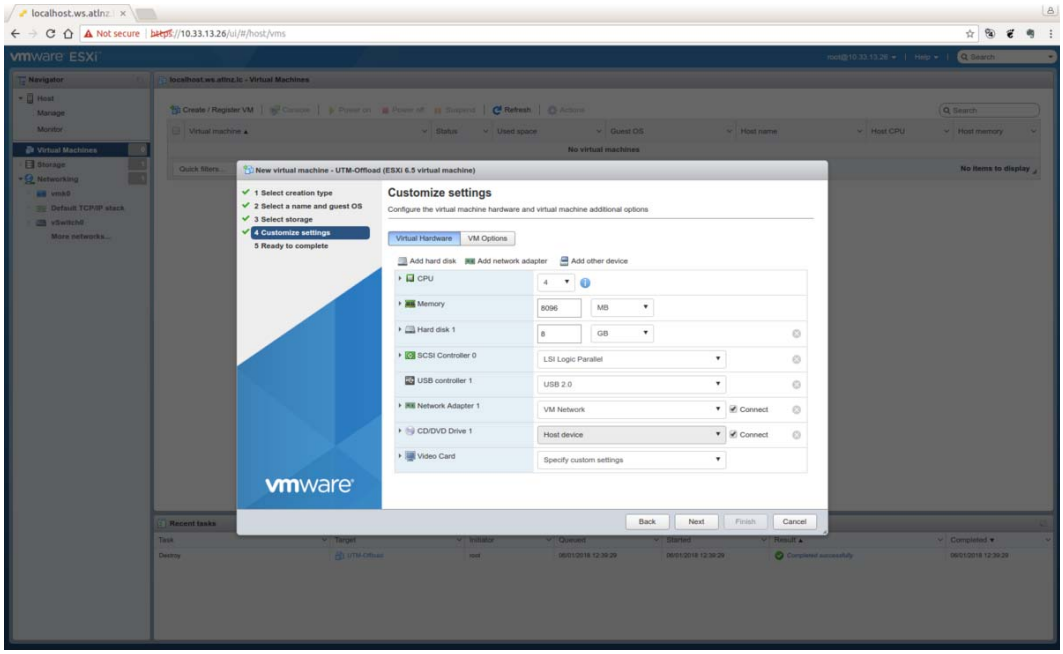
4. Use the drop down boxes to select, **Compatibility**, **Guest OS family**, and **Guest OS version**.



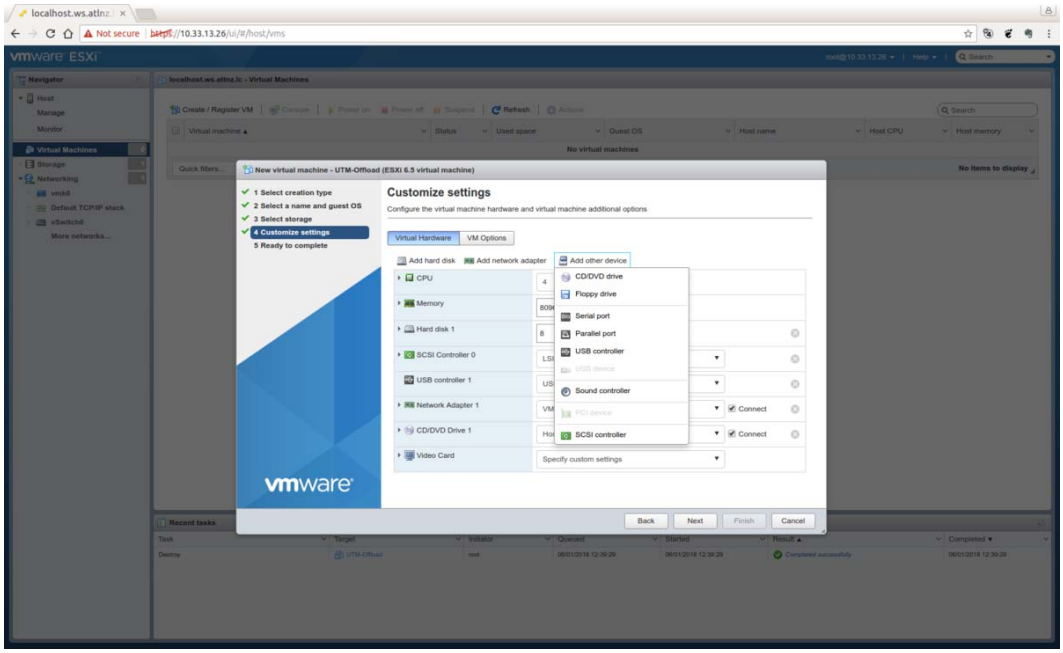
5. From the **Select storage** page, select the **datastore** for your configuration.



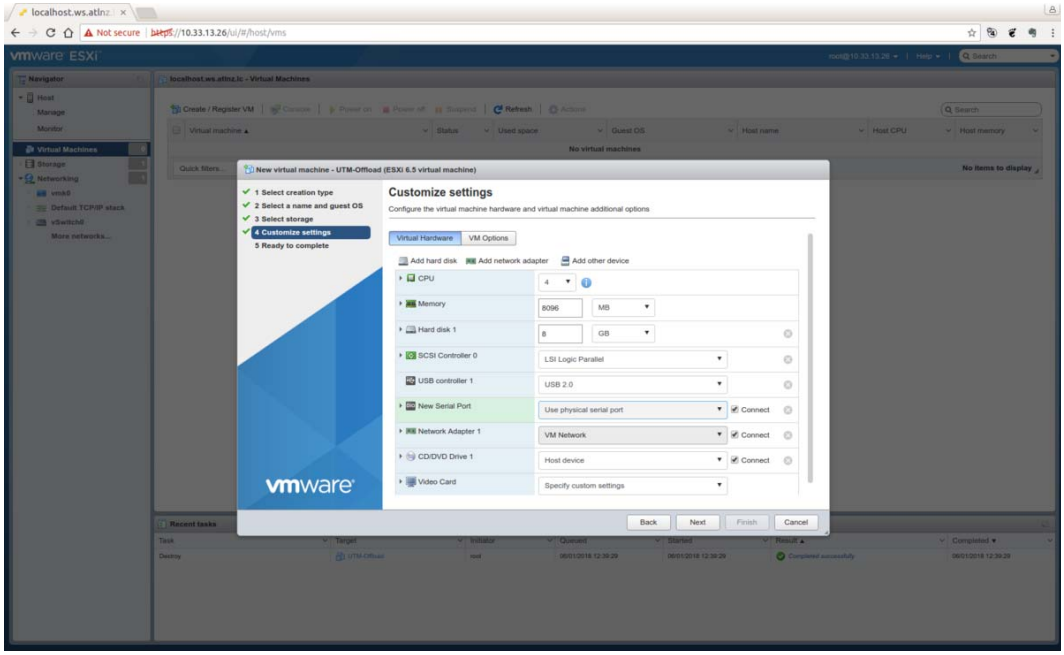
6. From the **Customize settings** page, configure the **Virtual Hardware** and **VM Options**.



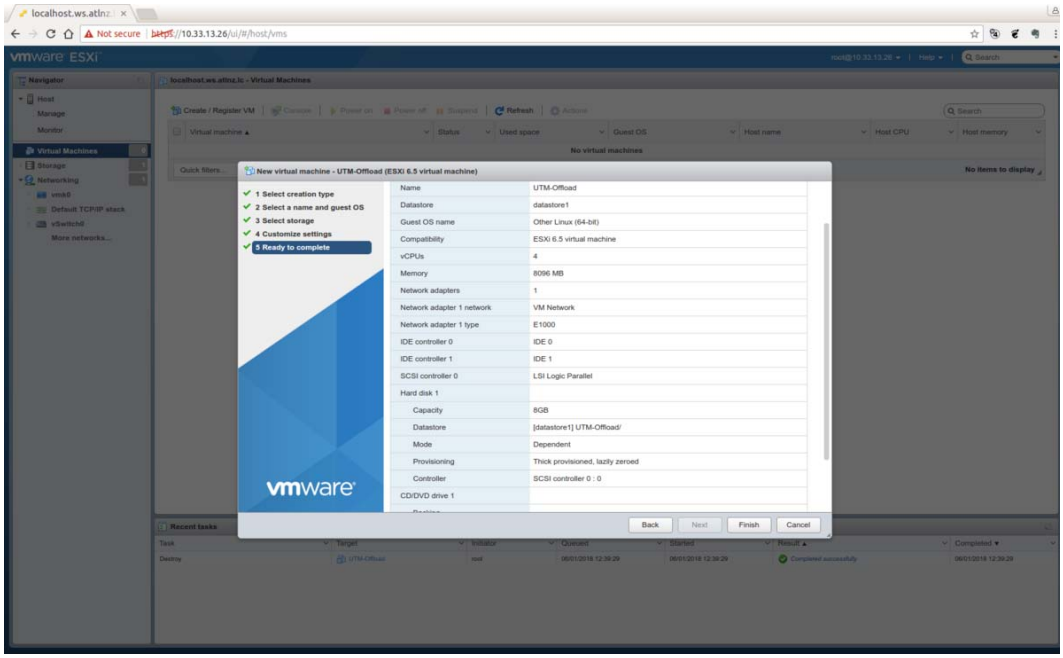
- Select **Serial port**.



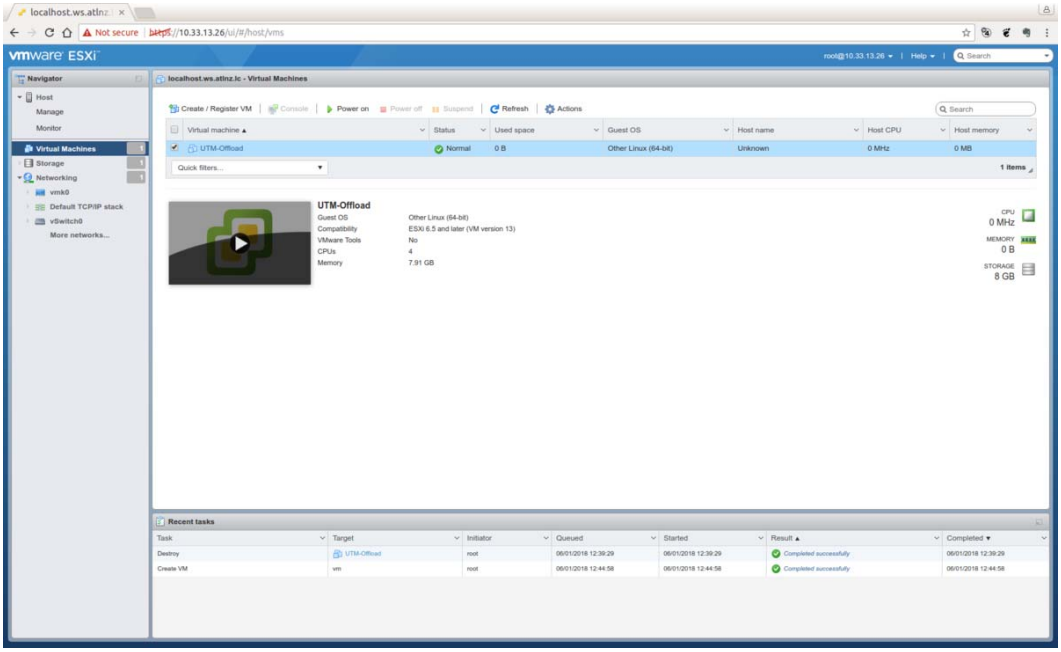
- Select **Connect**

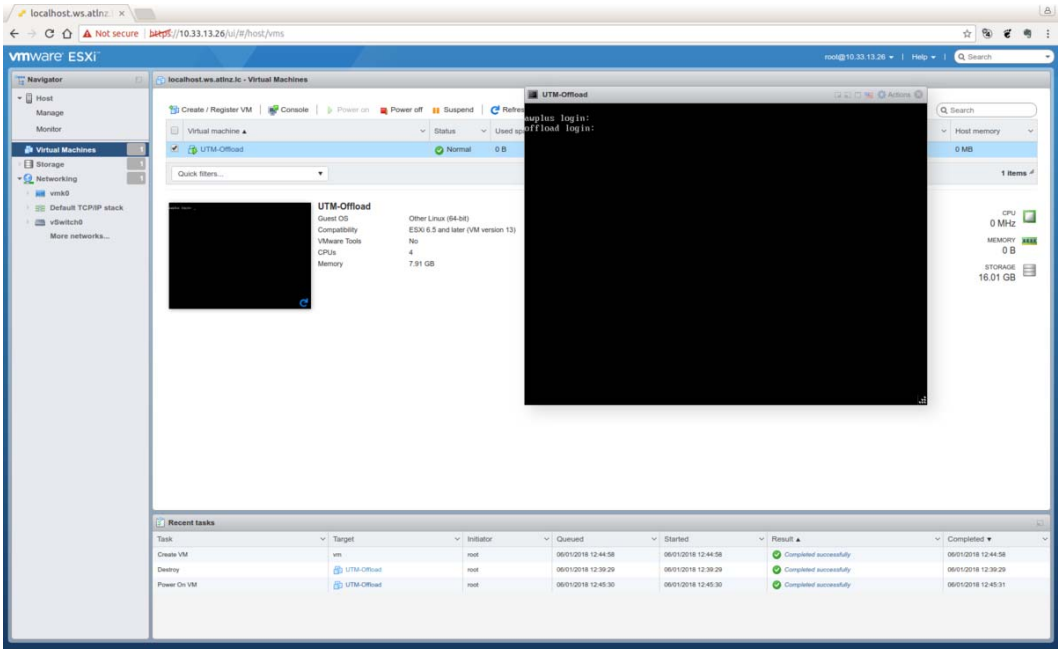


- Check the settings and click **Finish**.

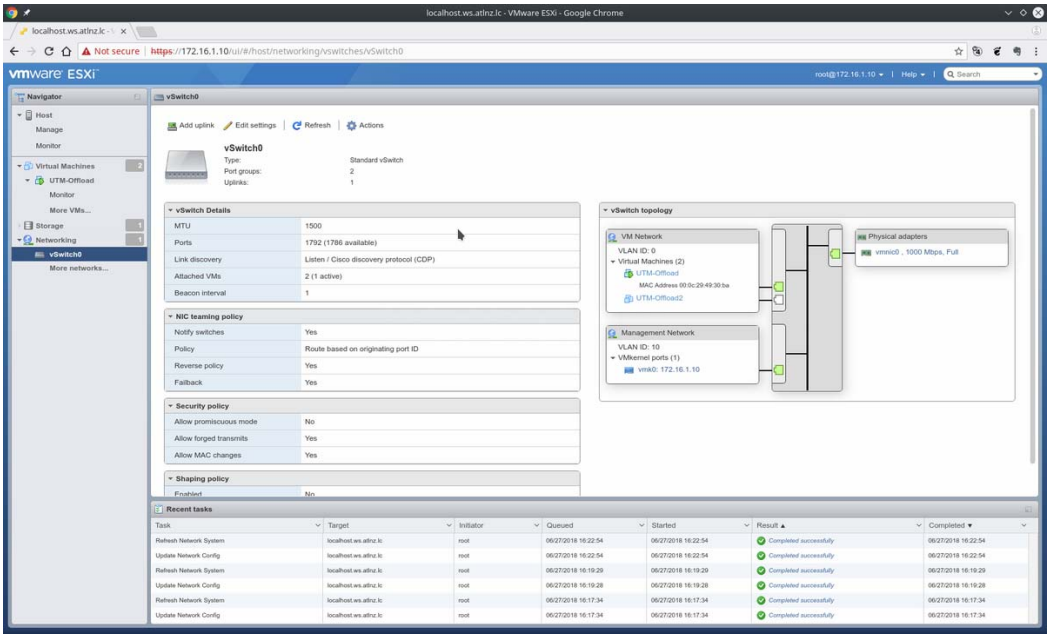


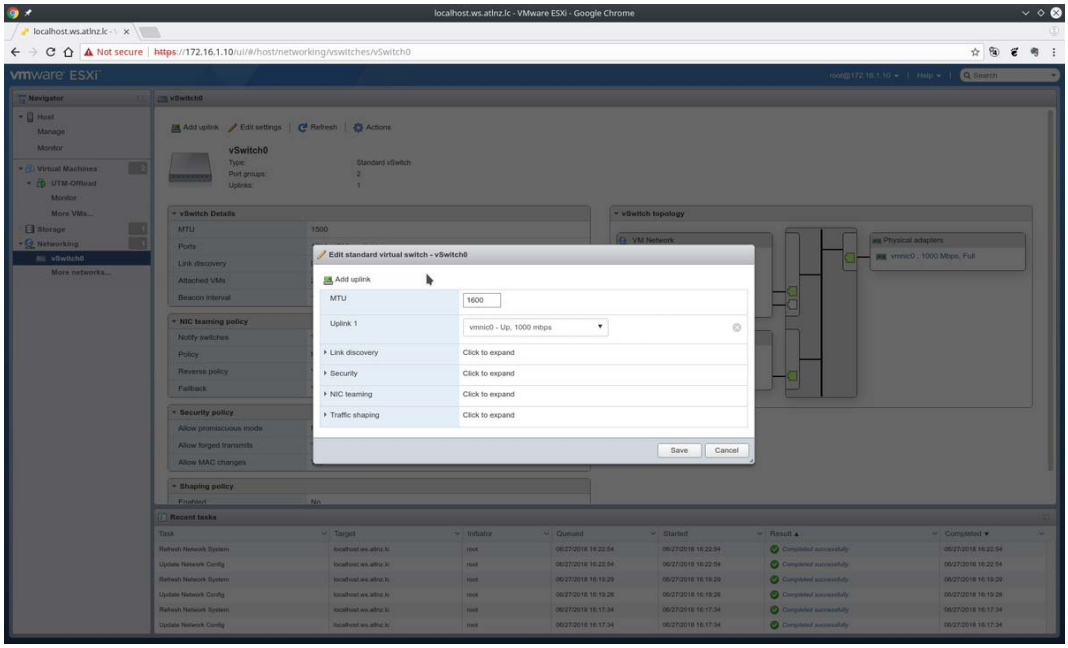
- Click **Play**


vmware ESXi
Navigator
Host
Manage
Monitor
Virtual Machines
Storage
Networking
vmk0
Default TCP/IP stack
vSwitch0
More networks...
localhost.ws.atlnz.lc - Virtual Machines
Create / Register VM
Console
Power on
Power off
Suspend
Refresh
Actions
Virtual machine
Status
Used space
Guest OS
Host name
Host CPU
Host memory
UTM-Offload
Normal
0 B
Other Linux (64-bit)
Unknown
0 MHz
0 MB
Quick filters...
1 items
UTM-Offload
Guest OS
Other Linux (64-bit)
Compatibility
ESXi 6.5 and later (VM version 13)
VMware Tools
No
CPUs
4
Memory
7.91 GB
CPU
0 MHz
MEMORY
0 B
STORAGE
8 GB
Recent tasks
Task
Target
Initiator
Queued
Started
Result
Completed
Destroy
Create VM


vmware ESXi
Navigator
Host
Manage
Monitor
Virtual Machines
Storage
Networking
vmk0
Default TCP/IP stack
vSwitch0
More networks...
localhost.ws.atlnz.lc - Virtual Machines
UTM-Offload
Create / Register VM
Console
Power on
Power off
Suspend
Virtual machine
Status
Host memory
UTM-Offload
Normal
0 MB
Quick filters...
1 items
UTM-Offload
Guest OS
Other Linux (64-bit)
Compatibility
ESXi 6.5 and later (VM version 13)
VMware Tools
No
CPUs
4
Memory
7.91 GB
CPU
0 MHz
MEMORY
0 B
STORAGE
16.01 GB
Recent tasks
Task
Target
Initiator
Queued
Started
Result
Completed
Create VM
Destroy
Power On VM

7. Expand the **Networking** drop down menu and select the vSwitch that attaches to the UTM Offload device and set the **MTU** to be **1600 bytes**.





Security Considerations

In all use cases UTM Offload should be deployed on a physically secured network because data traffic between the forwarding device and offload device has no additional security applied. LAN and WAN traffic are exposed on the offload network. UTM Offload does not increase the vulnerability of the forwarding device, as long as the physical link from the forwarding device to the offload device is secure.

Configuring Firewall and NAT allowing UTM Offload on the AR4050S

The following is a simple configuration for firewall and NAT allowing UTM Offload.

Configuration notes

- Rule 30 will allow the device to access the Update Manager.
- You need to configure a DNS Server address to allow communication with the update manager.
- The offload device synchronizes the time from the forwarding device. This ensures log messages are correctly time-stamped. Therefore, NTP is configured on the forwarding device (AR4050S).

```
!
zone private
  network lan
  ip subnet 192.168.10.0/24 interface vlan1
network offload
  ip subnet 192.168.100.0/24 interface eth2
!
zone public
 network all
  ip subnet 0.0.0.0/0 interface eth1
 host router
  ip address dynamic interface eth1
!
firewall
 rule 10 permit any from private to private
 rule 20 permit any from private to public
 rule 30 permit any from public.all.router to public
 protect
!
nat
 rule 10 masq any from private to public
 enable
!
ntp server <URL>
!
utm-offload interface eth2 subnet 192.168.100.0/24
!
ip name-server <x.x.x.x>
!
interface vlan1
 ip address 192.168.10.1/24
!
interface eth1
 ip address dhcp
!
```

UTM Offload Logging

The following UTM Offload items are logged:

- Change in state of the offload device.
- Communication failure between the AR4050S and the offload device.
- Existing UTM feature log messages appear in the AR4050S log transparently.
- Other general log messages generated by the offload device appear in the AR4050S log transparently
- Messages from the offload device appearing in the AR4050S log have the offload device's IP address, the timestamp for when the message was generated and the string "offload" inserted.

When the AR4050S detects the offload device is no longer present it will:

- output a log
- stop sending packets to the offload device for processing
- install a rule to block traffic from being forwarded across the forwarding device (this allows management of the forwarding device to continue, but continues to protect the user)

Checking the UTM offload status

To see the status of the offload device, use the command:

```
awplus#show utm-offload
```

Figure 3: Output from **show utm-offload**

```
awplus#show utm-offload
Status:       Enabled (Booted)
Interface:    eth2
Subnet:       192.168.100.0/24
Resource update interval: 1 hour

awplus#show resource
-------------------------------------------------------------------------------
Resource Name          Status       Version   Interval  Last Download
                                                        Next Download Check
-------------------------------------------------------------------------------
dpi_procera_app_db     Sleeping     dpi_procera_app_db_v66
                                              1         None
                                              hour      Sun  1 Jul 2018 21:58:54
afa_offload            Sleeping     afa_main_offload_v51
                                              1         None
                                              hour      Sun  1 Jul 2018 21:47:41
iprep_et_rules         Sleeping     iprep_et_rules_v8582
                                              1         Mon  2 Jul 2018 04:05:06
                                              hour      Mon  2 Jul 2018 06:05:03
```

Glossary

- **Forwarding device (AR4050S)**

  The device that intercepts packets, sends them to the offload device for processing and finally forwards the packets when they return. It also manages the configuration of the offload device.

- **Offload Device**

  The headless device that provides UTM packet processing offload for the forwarding device. A headless device is a device that does not have a user-facing User interface.

- **Offload Image**

  Full software release that runs on the offload device. The offload image is downloaded from the Update Server by the forwarding device and used to network boot the offload device.

- **PXE Boot**

  Pre-boot Execution Environment (PXE) is the standard method used to boot off the shelf hardware across a network without first needing to install software on that hardware. The forwarding device functions as a PXE boot server to boot the offload device using the offload image.

- **Service Function Chaining (SFC)**

  SFC is a standardized mechanism for how network service functions are applied to packets. Packets are classified and matched by local policy to a configured Service Function Path (SFP).
  Those packets are then forwarded by the Service Function Forwarder (SFF) to each Service Function (SF) in the order specified in the path. SFC is used internally in UTM Offload as the underlying mechanism for offloading packets to the remote UTM engine.

- **UTM**

  In the context of UTM Offload, consists of one or more of the following security features:

  - **IDS/IPS**. Detects packets/flows that may threaten the network and when run in inline mode, prevents that threat.
  - **IP Reputation**. Categorizes public hosts based on their global reputation so that undesirable traffic can be blocked.
  - **URL Filtering**. Blocks access to websites that are known to contain resources that could potentially cause harm to endpoints.
  - **Malware Protection**. Scans traffic byte streams for signatures of common Malware and prevents that Malware from entering the network.

- **Bare-Metal Hypervisor**

  A hypervisor or virtual machine monitor (VMM) is computer software, firmware or hardware that creates and runs virtual machines. A bare-metal hypervisor, also known as a Type 1 hypervisor, is virtualization software that has been installed directly onto the computing hardware and does not require the installation of an additional underlying operating system.

C613-22108-00 REV C

Allied Telesis NETWORK SMARTER

North America Headquarters | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
EMEA & CSA Operations | Incheonweg 7 | 1437 EK Rozenburg | The Netherlands | T: +31 20 7950020 | F: +31 20 7950021

alliedtelesis.com