AMF Security Controller

SDN Controller for Enterprise Networks

The Allied Telesis AMF-Sec Controller enables state-of-the-art network security. It provides exactly what enterprises need—reduced management costs, increased security and an improved end-user experience.

Overview

Allied Telesis Autonomous Management Framework™ (AMF) simplifies and automates network management. AMF-Sec adds a powerful security component with an intelligent, fully featured SDN controller. It reduces manual effort and cost in two ways: First, it works with security appliances to instantly respond to malware alerts, and block the movement of threats within a wired or wireless network. And second, it automates network access control, only allowing authenticated users to access online resources and applications.

Intelligent Isolation Adapter automatically blocks threats

AMF-Sec works with best-of-breed UTM Firewalls to identify threats, then the intelligent Isolation Adapter engine built into our AMF–Sec controller responds immediately to isolate the affected part of the network, and quarantine the suspect device. Remediation[1] can be applied so the user device can re-join the network with minimal disruption. This helps organizations avoid lost time and unnecessary disruption to network services.

Protect the network edge

Most security solutions are only capable of blocking suspicious traffic as it passes through the firewall from the Internet, so only external threats can be detected and blocked—this is the traditional “secure border” model. However, AMF-Sec can isolate traffic anywhere in the network, so it can prevent threats not only at the border, but also inside the network through USB drives, BYOD, and more. AMF-Sec is an innovative solution that can monitor traffic entering and traversing the local network, without introducing latency or bottlenecks.

Automated network access control

Remove the need to manually setup each user device as part of rolling out a network security solution. With AMF-Sec, new user devices are automatically authenticated by the AMF-Sec controller when they attempt to access the network. Non-authenticated devices are blocked, protecting digital business information.

Open and flexible SDN solution

AMF-Sec works seamlessly with Allied Telesis OpenFlow capable switches and wireless APs[2], and with a range of physical and virtual firewall products. AMF-Sec also integrates with AMF, which can be used to deliver instructions to network devices, and so does not have to rely on the OpenFlow protocol. The AMF Application Proxy enables the AMF-Sec controller to communicate securely with the AMF master when a threat is detected, so it can take action to block the threat at source by quarantining the infected device.

This provides flexible deployment, with the option of using either OpenFlow or AMF as the security communication protocol.

Simplified security management

Ease the burden of security management with a powerful solution to automate threat protection and network access control. AMF-Sec enables management flexibility with the ability to set up administrators to manage specific groups of devices. Comprehensive logging provides a clear audit trail for easy threat management review.

AMF-Sec is integrated with the Vista Manager EX network management and monitoring tool, which provides administrators with visual alerts of any threats that have been dealt with, and clear visibility of network connectivity status.

AMF-Sec is an innovative SDN solution. It removes duplication and reduces network operating costs, by constantly monitoring for threats to protect the network, and automating user access control. AMF-Sec delivers true business value, all day, every day.

Key Features

- Suitable for both wired and wireless networks[2]
- Integrates with security appliances to detect threats
- Automatically blocks threats and quarantines suspect devices
- Automates network access control of user devices
- OpenFlow v1.3 compatible
- AMF Application Proxy
- Visual alerts provided to Vista Manager EX
- Flexible management with administrator/device groups
- Security logs for a clear audit trail

[1] Remediation is managed by the network administrator

[2] Coming soon on TQ5403 series wireless APs

Key Solution

Block threats at the source

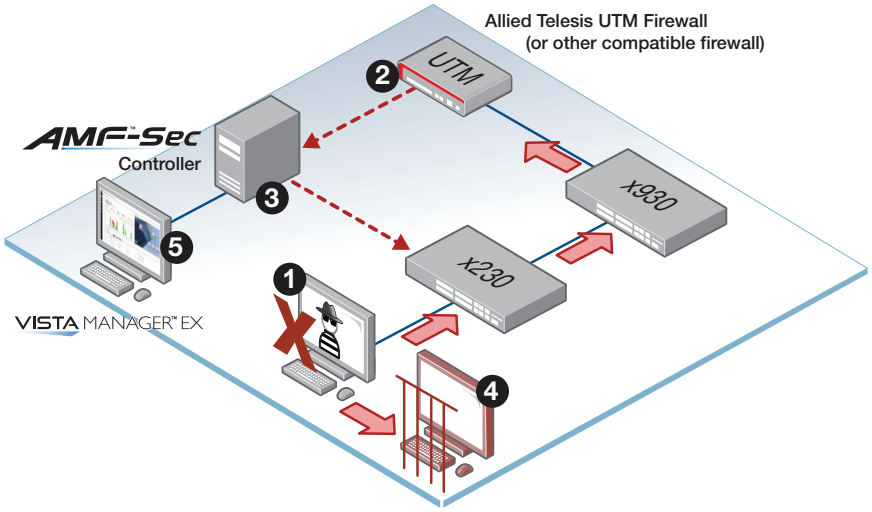
Most threat protection solutions are only capable of blocking suspicious traffic as it passes through the firewall from the Internet, so only external threats can be detected and blocked—this is the traditional "secure border" model.

However, the AMF-Sec controller can isolate traffic anywhere in the network, and automatically block malware threats, such as those introduced inadvertently by staff with USB sticks, BYOD and so on. Suspect devices and quarantined to protect the network.

This makes AMF-Sec an innovative security solution that can monitor traffic entering and traversing the local network, without introducing latency or bottlenecks.

AMF-Sec is closely integrated with Vista Manager EX, and visual alerts on the network map make finding the suspect device simple, so remediation can be applied.

1. Targeted attack inside the network! Threat information is seen upline
2. Firewall sends threat notification
3. AMF-Sec instructs switch to shut down threat source
4. Infected device sent to quarantine
5. Security alert shown on Vista Manager EX



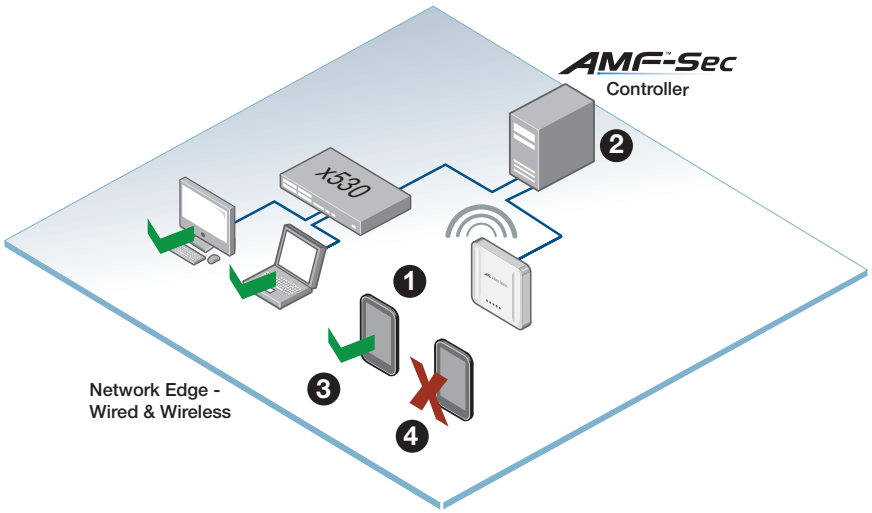
Automate network access control

Remove the need to manually setup each new user device as part of rolling out a network security solution.

With AMF-Sec, new user devices are automatically authenticated when they attempt to access the network, as their MAC addresses are checked against a database on the AMF-Sec controller.

Non-authenticated devices are blocked, protecting the network and digital business information.

1. New devices attempt to join the network
2. New device MAC address checked against authentication database
3. Authenticated device is granted access
4. Non-authenticated device is blocked



SPECIFICATION			
Server			
Processor	CPU 2.5GHz or faster, 64bit x86 processors		
RAM	4GB or larger		
Disk Space	80GB or larger		
Physical Requirements	Network Interface GbE × 1, Optical drive DVD drive (bootable)		
Virtualization	VMware vSphere ESXi 5.5 (Hypervisor) VMware vSphere ESXi 6.0 (Hypervisor) VMware vSphere ESXi 6.5 (Hypervisor) Microsoft Windows Server 2012 R2/2016 Hyper-V		
Management			
Browser	Microsoft Internet Explorer 11 Google Chrome Mozilla Firefox		
AMF-Sec mini	AMF-Sec controller built into the Device GUI running on an AR4050S UTM Firewall		
Allied Telesis Switch for AMF Application Proxy (AMF Master)	AMF Cloud[3] SwitchBlade x8106[3] x950 Series	SwitchBlade x8112[3] SwitchBlade x908 GEN2[3] x930 Series	
Allied Telesis Switch for AMF Application Proxy (AMF Member)	SwitchBlade x8112 SwitchBlade x8106 SwitchBlade x908 GEN2 x950 Series x930 Series x550 Series x530 Series x530L Series x510/x510L Series	x320 Series x310 Series XS900MX Series GS900MX Series x230 Series x220 Series GS980M Series FS980M Series IE510-28GSX	IE340 Series IE300 Series IE200 Series IE210L Seires AR Series
Allied Telesis Switch for OpenFlow	SwitchBlade x908 GEN2 x950 Series x930 Series x550 Series x530 Series	x530L Series x510/x510L Series x310 Series x230 Series IE510-28GSX	IE340 Series IE300 Series IE210L Series
AMF Master	Max: 4		
AMF Member Management	Max: 510 AMF members for network access control. 600 AMF members for threat protection		
OpenFlow Switch Management	Max : 510		
Device Management	Max MAC Address : 5000		
Policy Management	Max Policy : 5000		
User Management	Max User : 5000 (*Up to 255 MAC Address and 8 policy per user)		
Location Management	Max : 510		
VLAN	0 ~ 4094		
Features			
Administration Interface	Web GUI Backup and restore configuration Update firmware Manage licenses		
Network Actions (AMF Application Proxy)	Block access based on MAC address, Quarantine, Log activity. Take link down Use IP filter to block or redirect		
Network Actions (OpenFlow)	Block access based on MAC address, Quarantine, Log activity		
Log	Syslog Device authentication result OpenFlow controller	OpenFlow packets GUI operation Trap monitor	
Mail Notification	Under OpenFlow control	Device authentication, Blocking, Isolating, Rogue device access, Changing database synchronization	
	Under AMF Application Proxy control	Device authentication, Blocking, Isolating, Rogue device access	
Redundancy	Max : 2 controllers - one active and one standby		
Scalability	AMF Application Proxy	Additional SESC License[3], AMF Master, AMF Member	
	OpenFlow	Additional SESC License[3], OpenFlow License on each Switch[4]	
System Version	1.8.0		

[3] These products include the AMF Application Proxy license

[4] Please refer to "Ordering Information"

Ordering Information

AT-FL-SESC-BASE-(1YR/5YR)
Base software including 10 node license for 1 or 5 years

Additional Licenses

AT-FL-SESC-ADD10-(1YR/5YR)
License for an additional 10 nodes for 1 or 5 years

AT-FL-SESC-ADD50-(1YR/5YR)
License for an additional 50 nodes for 1 or 5 years

AT-FL-SESC-ADD100-(1YR/5YR)
License for an additional 100 nodes for 1 or 5 years

AT-FL-SESC-ADD200-(1YR/5YR)
License for an additional 200 nodes for 1 or 5 years

Related AMF Licenses

AT-FL-x950-AAP-(1YR/5YR)
x950 Series AMF Application Proxy license for 1 or 5 years

AT-FL-x930-AAP-(1YR/5YR)
x930 Series AMF Application Proxy license for 1 or 5 years

AT-FL-AR4-ASEC-(1YR/5YR)
AMF-Sec mini license, with AMF Application Proxy operating on an AR4050S UTM Firewall

Related OpenFlow Licenses

AT-FL-GEN2-OF13-(1YR/5YR)
SBx908 GEN2 OpenFlow license for 1 or 5 years

AT-FL-x950-OF13-(1YR/5YR)
x950 Series OpenFlow license for 1 or 5 years

AT-FL-x930-OF13-(1YR/5YR)
x930 Series OpenFlow license for 1 or 5 years

AT-FL-x550-OF13-(1YR/5YR)
x550 Series OpenFlow license for 1 or 5 years

AT-FL-x530-OF13-(1YR/5YR)
x530 Series OpenFlow license for 1 or 5 years

AT-FL-x530L-OF13-(1YR/5YR)
x530L Series OpenFlow license for 1 or 5 years

AT-FL-x510-OF13-(1YR/5YR)
x510 Series OpenFlow license for 1 or 5 years

AT-FL-x310-OF13-(1YR/5YR)
x310 Series OpenFlow license for 1 or 5 years

AT-FL-x230-OF13-(1YR/5YR)
x230 Series OpenFlow license for 1 or 5 years

AT-FL-IE5-OF13-(1YR/5YR)
IE510-28GSX OpenFlow license for 1 or 5 years

AT-FL-IE34-OF13-(1YR/5YR)
IE340(L) Series OpenFlow license for 1 or 5 years

AT-FL-IE3-OF13-(1YR/5YR)
IE300 Series OpenFlow license for 1 or 5 years

AT-FL-IE2-OF13-(1YR/5YR)
IE210L Series OpenFlow license for 1 or 5 years

© 2020 Allied Telesis, Inc. All rights reserved.

617-000626 RevF