Technical Guide

Firewall

FEATURE OVERVIEW AND CONFIGURATION GUIDE

Introduction

This guide describes AlliedWare Plus™ Firewall and its configuration.

AlliedWare Plus Firewall is a Next-Generation Firewall (NGFW) that offers security, flexibility and ease of use. Unlike a traditional firewall, it will keep pace with rapid changes in Internet-based applications, enabling enterprises to see the benefits of web-based technology without costly security issues.

Contents

AlliedWare Plus™ OPERATING SYSTEM

Products and software version that apply to this guide

This Guide applies to AlliedWare Plus™ Firewall, running version **5.4.5** or later.

To see whether a product supports AlliedWare Plus Firewall, see the following documents:

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

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

Feature support may change in later software versions. For the latest information, see the above documents.

What Is AlliedWare Plus Firewall?

A firewall, at its most basic level, controls traffic flow between a trusted network (such as a corporate LAN) and an untrusted or public network (such as the Internet). The most commonly deployed firewalls nowadays are port-based or packet filtering. These traditional firewalls determine the allowed traffic versus the disallowed traffic based on many characteristics of the packets, including their destination and source IP addresses and TCP/UDP port numbers. However, traditional network security solutions have failed to keep pace with changes to applications, threats, and the network landscape.

AlliedWare Plus Firewall is designed for the challenges facing modern networks. In contrast to traditional firewalls that lack the intelligence to discern network traffic in a world where network boundaries are disintegrating and Internet applications are exploding, AlliedWare Plus Firewall no longer talks about packets, IP addresses and ports. Instead it focuses on applications, users and content. It classifies traffic by the application's identity in order to enable visibility and control of all types of application.

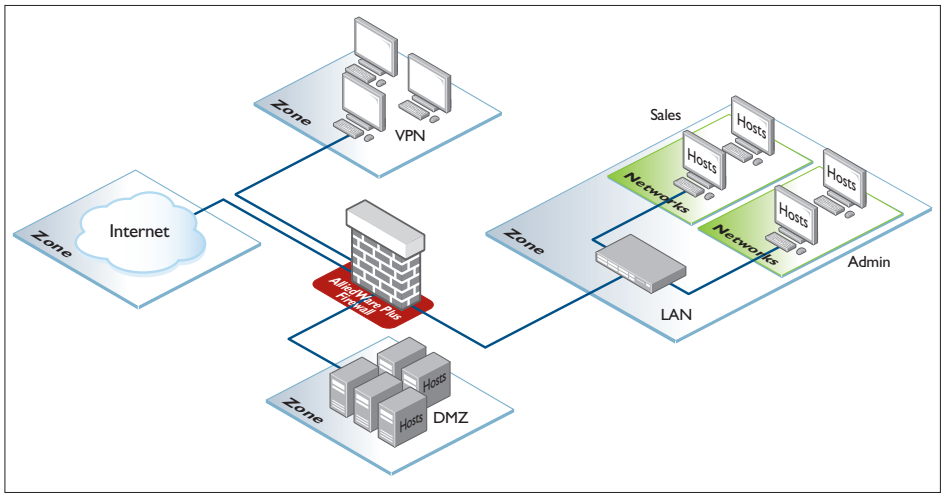
AlliedWare Plus Firewall views the physical network in terms of zones, networks and hosts. Firewall rules can be applied to any level of this hierarchy, as shown in Figure 1, "AlliedWare Firewall," on page 3. See "What is Entity?" on page 4 for entity definitions and usage.

When AlliedWare Plus Firewall is enabled, its default policy is to drop all applications from anywhere to anywhere. If no rule is explicitly configured, all traffic moving through the firewall is blocked.

AlliedWare Plus Firewall filters traffic by identifying applications. The application-centric traffic classification identifies specific applications flowing across the network regardless of the port and protocol in use.

AlliedWare Plus Firewall identifies applications through a database of regularly updated application signatures. Deep Packet Inspection (DPI) is used by the firewall to match packets against these signatures and provide layer 7 filtering for firewall rules. See "What is Application?" on page 4 for application definition and usage.

Figure 1: AlliedWare Firewall



AlliedWare Plus Firewall provides the following features:

- Stateful inspection maintains the status of active connections through the firewall to dynamically allow inbound replies to outbound connections.
- Robust application identification and inspection enables granular control of the flow of sessions through a firewall, based on the specific applications that are being used.
- Rules allow specified traffic to be matched and the appropriate action applied.
- Network Address and Port Translation permits multiple hosts on a LAN to be mapped to a single public IP address and hides details of the internal network.
- OpenVPN integration provides secure remote access to intranet resources.
- Application Layer Gateway (ALG) inspects the application layer payload of a packet and understands the application control messages, and performs Network Address Translation processing if necessary. AlliedWare Plus Firewall currently supports FTP ALG that provides connection tracking and NAT for FTP, TFTP ALG that provides connection tracking and NAT for TFTP and SIP ALG that provides connection tracking for SIP and related RTP connections.
- Categorized websites prevents unauthorized access to inappropriate content.
- Logs allow retrieval of all event details for later analysis.
- Reports of network usage and statistics give network managers the information they need to effectively manage their networks.

What Is Application?

Application is a high level abstraction of application packets being transported by network traffic. Traffic matching for applications can be achieved through the firewall by using several techniques, for example, matching packets to port numbers or searching for application signatures in flows of packets. You can configure source port, destination port, protocol, ICMP code and ICMP type for the application. Application is invalid if its protocol, source or destination are not properly configured, for example, application has no protocol configured, or, source and destination ports are applied to protocols that are not TCP, UDP or SCTP.

There are 40 predefined applications with protocols, source and destinations ports. You can use the **show application** command to show the detail of these applications.

What Is Entity?

AlliedWare Plus NGFW supports application and entity based security policies. For example, firewall and Network Address Translation (NAT) rules are applied to applications among different zone entities.

Entity is a high level abstraction of a network device, a group of networks or subnets. It is the instance that firewall and NAT policy can be applied to. There are three types of entity:

- Zone
- Network
- Host

Zone is a high level abstraction for a logical grouping or segmentation of physical networks. This is the highest level of partitioning that firewall and NAT policy can be applied to. Zone establishes the security border of your networks. A zone defines a boundary where traffic is subjected to policy restrictions as it crosses to another region of your networks. The minimum zones normally implemented would be a trusted zone for the private network behind the firewall and a untrusted zone for the Internet. Other common zones are a Demilitarized Zone (DMZ) for publicly visible web servers and a Virtual Private Network (VPN) zone for remote access users or tunnels to other networks.

A network is a high level abstraction of a logical network in a zone. This consists of the IP subnets and interfaces over which it is reachable. Subnets are grouped into networks to apply a common set of rules among the subnets.

Host is a high level abstraction of a single node in a network. This is commonly used if a particular device, for example a server, has a static IP address that needs to be specified in a firewall policy.

What Is NAT?

A router can act as an agent between the Internet and a local network. When you use NAT, you assign private IP addresses to hosts on the private side of the router. When those hosts send traffic, the router translates the private addresses to one or more public and valid addresses before routing the traffic. When the router receives traffic that is destined for those hosts, it translates the public addresses back to the appropriate private addresses.

NAT, defined in RFC 1631, provides a solution to one of the major problems facing the Internet—IP address depletion. IP address space is limited and obtaining a large block of registered addresses is difficult. Although you can use private IP address (RFC 1918) in your internal network, private IP addresses are not routable through the Internet.

The router supports:

- Port Forwarding: To provide public access to internal servers, the firewall is used in conjunction with NAT and the firewall must be able to forward traffic received on an interface to those servers. Port Forwarding redirects any traffic from the specified entity to a specific host address regardless of the original destination of the traffic. The most common application for this is to forward HTTP traffic to an internal web server.
- NAT with IP Masquerade: It is a case where all or a range of addresses are mapped to a singe address with source port translation to identify the association. This singe address masquerades as the public source address for the private addresses.

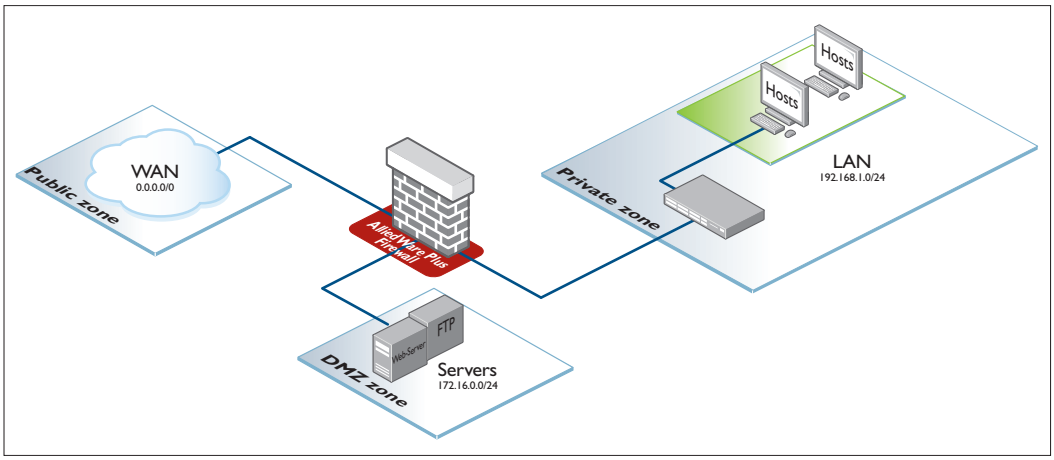
By default, NAT is disabled. You can use the **enable (NAT)** command to explicitly enable this functionality. If firewall protection is enabled, you need to configure firewall rules that allow the application matching its source and destination entities to pass through the firewall. Portfwd rules (actions) are applied before any other firewall rules and masq rules (actions) are applied after any other firewall rules. To configure NAT rules, you can use the **rule (NAT)** command.

Configuration Example

Configuring Firewall and NAT rules for entities

The following example shows you how to configure an AlliedWare Plus Firewall. The figure below shows the network topology and zone partition used by the example.

Figure 2: Network topology and zone partition



Step 1: Configure DMZ zone.

```
awplus#configure terminal
awplus(config)#zone dmz
awplus(config-zone)#network servers
awplus(config-network)#ip subnet 172.16.0.0/24 interface eth1
awplus(config-host)#host ftp
awplus(config-host)#ip address 172.16.0.2
awplus(config-host)#host web-server
awplus(config-host)#ip address 172.16.0.10
```

Step 2: Configure private zone.

```
awplus(config-host)#zone private
awplus(config-zone)#network lan
awplus(config-network)#ip subnet 192.168.1.0/24 interface vlan1
```

Step 3: Configure public zone.

```
awplus(config-host)#zone public
awplus(config-zone)#network wan
awplus(config-network)#ip subnet 0.0.0.0/0 interface eth2
```

Step 4: Configure application.

```
awplus(config)#application ping
```

```
awplus(config-application)#protocol icmp
awplus(config-application)#icmp-type 8
awplus(config-application)#icmp-code 0
```

Step 5: Configure firewall rules.

```
awplus(config)#firewall
awplus(config-firewall)#rule 100 permit ping from public to private
awplus(config-firewall)#rule 200 permit ping from public to dmz
awplus(config-firewall)#rule 300 permit ping from private to dmz
awplus(config-firewall)#rule 400 permit ping from dmz to private
awplus(config-firewall)#rule 500 permit ftp from public to
dmz.servers.ftp
awplus(config-firewall)#rule 600 permit http from public to
dmz.servers.web-server
awplus(config-firewall)#rule 700 permit any from private to private
awplus(config-firewall)#rule 800 permit any from dmz to dmz
awplus(config-firewall)#rule 900 permit any from private to public
awplus(config-firewall)#rule 1000 permit any from dmz to public
```

Step 6: Enable firewall protection.

Enable firewall protection and apply the firewall rules. This also ensures that the network administrator is not prematurely locked out of the device.

```
awplus(config-firewall)#protect
```

Step 7: Configure Network Address Translation (NAT) rules.

```
awplus(config)#nat
awplus(config-nat)#rule 10 masq any from private to public
awplus(config-nat)#rule 20 masq any from dmz to public
awplus(config-nat)#rule 30 masq any from private to dmz
awplus(config-nat)#rule 40 portfw ftp from public with dst
dmz.servers.ftp
awplus(config-nat)#rule 50 portfw http from public with dst
dmz.servers.web-server
awplus(config-nat)#rule 60 portfw ftp from private with dst
dmz.servers.ftp
awplus(config-nat)#rule 70 portfw http from private with dst
dmz.servers.web-server
```

Step 8: Enable NAT to apply the NAT rules.

```
awplus(config-nat)#enable
```

Step 9: Configure interfaces.

```
awplus(config)#interface eth2
awplus(config-if)#ip address 128.0.0.1/24
```

```
awplus(config-if)#interface eth1
awplus(config-if)#ip address 172.16.0.1/24
awplus(config-if)#exit
awplus(config)#vlan database
awplus(config-vlan)#vlan 1
awplus(config-vlan)#exit
awplus(config)#interface vlan1
awplus(config-if)#ip address 192.168.1.1/24
```

Step 10: Verify Firewall configuration.

```
awplus#show running-config firewall
```

Output 1: Below is an example output from the console:

```
awplus#show running-config firewall
firewall
 rule 100 permit ping from public to private
 rule 200 permit ping from public to dmz
 rule 300 permit ping from private to dmz
 rule 400 permit ping from dmz to private
 rule 500 permit ftp from public to dmz.servers.ftp
 rule 600 permit http from public to dmz.servers.web-server
 rule 700 permit any from private to private
 rule 800 permit any from dmz to dmz
 rule 900 permit any from private to public
 rule 1000 permit any from dmz to public
 protect
!
```

Step 11: Verify Entity configuration.

```
awplus#show entity
```

Output 2: Below is an example output from the console:

```
awplus#show entity
Zone:         dmz
 Network:     dmz.servers
  Subnet:     172.16.0.0/24 via eth1
  Host:       dmz.servers.ftp
   Address:   172.16.0.2
  Host:       dmz.servers.web-server
   Address:   172.16.0.10

Zone:         private
 Network:     private.lan
  Subnet:     192.168.1.0/24 via vlan1

Zone:         public
 Network:     public.wan
  Subnet:     0.0.0.0/0 via eth2
```

Step 12: Verify NAT configuration.

```
awplus#show nat rule
```

Output 3: Below is an example output from the console:

```
awplus#show nat rule

[* = Rule is not valid - see "show nat rule config-check"]
  ID     Action  App        From          To            With
Hits
-------------------------------------------------------------------------
-----------
* 10     masq    any        private       public        -
0
  20     masq    any        dmz           public        -
0
* 30     masq    any        private       dmz           -
0
  40     portfw  ftp        public        -
dmz.servers.ftp

0
  50     portfw  http       public        -
dmz.servers.web-server

0
* 60     portfw  ftp        private       -
dmz.servers.ftp

0
* 70     portfw  http       private       -
dmz.servers.web-server

0
```

Configuring Firewall rules to interact with Update Manager

The Update Manager is a tool to enable an AlliedWare Plus device to be kept up to date with the latest available software components and resources. When Firewall protection is enabled, you need to create Firewall rules to permit the Update Manager traffic to be sent. Fore more information about the Update Manager, see the Update Manager Feature Overview and Configuration Guide.

Step 1: Configure network entity.

You can create a network entity for the Update Manager which is located on the Internet assuming that the Internet is reachable over interface ETH1.

```
awplus#configure terminal
awplus(config)#zone WAN
awplus(config-zone)#network INTERNET
awplus(config-zone)#ip subnet 0.0.0.0/0 interface eth1
```

Step 2: Configure entity for the Update Manager source traffic.

You can create an entity for the Update Manager source traffic which is from the interface that connects to the Internet.

```
awplus(config)#zone ROUTER
awplus(config-zone)#network WAN
awplus(config-network)#ip subnet 192.168.52.0/24 interface eth1
awplus(config-host)#host WAN_INT
awplus(config-host)#ip address 192.168.52.20
```

Step 3: Configure Firewall rules.

The Update Manager traffic uses HTTPS protocol. You can create a Firewall rule to allow HTTPS application.

```
awplus(config-host)#end
awplus#configure terminal
awplus(config)#firewall
awplus(config-firewall)#rule permit https from ROUTER.WAN.WAN_INT
to WAN
```

Similarly, you can create a rule to allow DNS resolution of the Update Server's URL if the DNS server is reachable via the WAN interface.

```
awplus(config-firewall)#rule permit dns from ROUTER.WAN.WAN_INT to
WAN
```

C613-22012-00 REV B

Allied Telesis the solution : the network

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