

iQuila Deployment Guide for iQuila Bridge in Microsoft Azure

iQ22059r3

This Document Applies to: iQuila Enterprise Microsoft Azure

www.iQuila.com

Bridge Deployment Guide

Overview

iQuila Enterprise is a powerful tunnelling platform allowing you to extend your corporate network across multiple locations while keeping the tightest of security across your network, using iQuila enterprise bridges you can easily link in remote branch offices around the world and home workers at ease. The advance AI manages the multicast traffic over your network, and the security policy centre allows you to control what data can travel to what destination you select over your network.

This Deployment Guide will guide you through setting up the iQuila Enterprise Bridge Appliances along with the iQuila Enterprise windows client software.

Deploying the Enterprise Server / Bridge

×

Cancel

From the iQuila Manager login to the iQuila server you have just deployed, the first time you login you will be prompted with a wizard, select the 1st option iQuila Server Default and click next.

You must create one Virtual Switch on the iQuila Enterprise Server

OK

as a minimum. Please choose your Virtual Switch Name.

Setup Wizard - Please choose your Virtual Switch Name

Virtual Switch Name: Default

ď

You will then be asked to create a default Virtual Switch. Enter a name of choice then select ok.

If your service includes the VEN AI Edge Processing, you can enable it here. If your subscription does not include this feature, please select Disable VEN AI Edge Processing and click ok.

The wizard will now ask you to create user accounts.

User accounts are used for Authenticating Server, Bridge devices along with client software connections.

To create your users select create users.





Copyright iQuila Ltd © 2020

The Auth type is defined, by Security Permissions from the dropdown list.

First, we will go through setting up a bridge user account.

Under username enter the name of your choice, for this bridge device in this scenario we will choose the username Bridge1. In the full name section enter the name of the location of the bridge that will be located. In this scenario we chose New York.

Now select the authentication type you would like, there are 6 different types of authentications in this scenario. We will use Individual certificate authentication.

Next, select the create certificate button.

The *create new certificate* window will show

Fill out the relevant information and *select the strengthens bits from the dropdown field.* then *select OK.*

You will now be asked to select the format, and protection for your certificate, in this scenario we will select Save as PKCA#12

Then, select *set passphrase* and enter a strong passphrase to protect the certificate.

Click save and save the certificate with a name that will identify it later e.g. Bridge1 New York.

ave Certifica	te and Private Key	×
Select the m	ethod to save the certificate and private key.	
Sa <u>v</u> e Meth	od:	
O Save a:	s X509 Certificate (.CER) and Private Key File (.KEY) Saving by splitting into two files: a standard Base 64-encoded and a private key file.	certificate file
Save a:	s <u>PKCA#12 File (P12)</u>	
Ra	Saving as a PKCS#12 (Public Key Cryptography Standard #12) f You can store both certificate and private key in a single PKCS#	le. 12 file.
O Write t	o <u>S</u> mart Card	
I	When a smart card is connected to this computer, you can writ and private key to a smart card.	e the certificate
	Select Which Smart Card to Use	
	Select which smart card device to use.	
Private Key	Protection:	
R .	When saving the private key, you can set a passphrase to encrypt. Y equired to enter the passphrase when loading it.	ou will be
	Set Passphrase	
	Passphrase:	
	Confirm:	
	OK	Cancel

	Name: Bridge1	Security Policy
Bull	Name: New York	1001 Distraction and and
	Hote:	Security Policy
Auth Type	S Anonymous Authentication	Croup Name Browse Groups
	Individual Certificate Authentication Signed Certificate Authentication RADIUS Authentication PJ NT Domain Authentication	Individual Certificate Authentication Settings:
		allowed or denied connection depending on whether the SSL clien certificate completely matches the certificate that has been set for the user beforehand.
assword Authenticat	tion Settings:	
assword Authenticat	Ebssword:	
Assword Authenticat	Ensword:	Specify CentificateCreate Centificate
Addius or NT Doma	Ion Settings:	Signify Cestilicate Igners Centilicate Cestilicate
ADIUS or NT Doma	In Authentication Settings	Signity Certificate provide Certificate Certificate Signed Certificate Automatication Settings Workshold and
ADIUS or NT Doma	In Authentication Settings	togety Certitude jour Certitude Create Certitude -Signed Certitude Automation Settinget Controlleget of a context to give a context to give a context of a
ADIUS or NT Doma	In strags	Signity Certificate grew Certificate Create Certificate • Signed Certificate Autoentication Mutility
RADIUS or NT Doma RADIUS or NT Doma MADIUS or NT Doma MADIUS or NT Domai BADIUS or NT Domail BADIUS server	In a strange	Signet Cestitute Ignet Cestitute Create Cestitute Signet Cestitute Automation Settings Automation Settings Automation of Automation Settings Automation Settings Automation Settings Automation of Automation Settings Automation Settings Automation Settings Automation of Automation Settings Automation Settings Automation Settings
RADIUS or NT Doma RADIUS or NT Doma RADIUS or NT Doma RADIUS or NT Doma RADIUS serv RADIUS serv RADIUS serv Socity Userv Socity Userv	In Attraction Settings	Signal Certificate Device Certificate Create Certificate Signal Certificate Automations Mettigate Workstate Automations Mettigate Signal Certificate for a strateging of the second of

reate New Certificate

ertificate and Private Key for Signing:	Load Certificate and Private Key
	Click 'Load Certificate and Private Key' to specify the X509 Certificate and RSA Private Key that will user a new certificate signature.
Common Name (CN):	Bridge1
Organization (O):	Compasny Name
Organization Unit (OU):	
Country (C):	kG
State (ST):	New York
Locale (L):	US
Serial Number: (Hexadecimal)	
Expires in:	3650 Days Strengthness: 4096 vits
To manage certif software such as	kates and certificate authorities on a large scale, you should use eithe OpenSSL, or commercial CA (certificate authority) software.

You can easily create certificates which is signed by self or other certificates

Once the certificate has been saved, the user window will be displayed, you can add further users accounts now or they can be added later.

Once you have finished adding users click Exit

-										
ser Name	full Name	Group Name	Description	Auth Method	Num Logins	Last Login	Expiration Date	Transfer Dytes	Transfer Packets	
bridge1	New York			Individual Certif.	0	(None)	No Expiration	0	0	

This will return you back to the easy setup wizard.

Under Step 3 *select the dropdown* and *select the network adaptor* you would like to bridge, normally this will be a different adaptor to the adaptor used for management, once selected *select Close.*



If you are using a Virtual Environment, a Notification window will be displayed.

It is important for iQuila to function correctly promiscuous mode is set to accept on virtual infrastructure.

Please make the necessary changes and *click ok.*

Instructions for Local Bridge on VM	×
飅 Using Local Bridge Function on VM	
It has been detected that the VEN Server might be running on a VM (Virtual Machine) suchlike VMware or Hyper-V. Read the following instructions carefully. If you are not using a VM, please ignore this message.	•
Instructions	
Some VMs prohibit the "Promiscuous Mode" (MAC Address Spoofing) on the network adapters by	
default.	
If the Promiscuous Mode (MAC Address Spoofing) is administratively disabled, the Local Bridge function between a Virtual Switch on the VEN Server and a physical network adapter on the physical computer does not work well. You should allow the Promiscuous Mode (MAC Address Spoofing) by using the configuration tool of the VM.	
For details please refer the documents of your VM. If it is a shared-VM and administrated by other person, please request the administrator to permit the use of the Promiscuous (MAC Address Spoofing) Mode to your VM.	
QK	

j	iver loca	most				censed to	b: iQuila		IO LICEN	ise	25 days r	emaining		
Switch / Hub Settings	v	'irtual Switch Name	Status	Type	Users	Groups	Sessions	MAC Tables	IP Tables	Num Logins	Last Login	Last Communication	Transfer Bytes	Transfer Packets
Manage Virtual Sw	tch	C Default	Online	Standalone	. 1	0		0	0	0	2021-01-05 14:56:53	2021-01-05 14:56:53	0	0
<u>O</u> nline														
Offline														
View <u>S</u> tatus														
Create a Virtual Sw	tch													
Propgrties														
Delete														
and Routing														
Local <u>B</u> ridge Setti	g													
Layer <u>3</u> Switch Sett	ng													
IPsec / L2TP Settin	9													
OpenVPN / MS-SS	ſP													
k And Encryption														
Encryption and Net	ork													
		VEN Server Infe	ormation				Manag	ement of <u>L</u> isten	ers:			iQuila Artificial Intelligenci		
ustering		± ↓ ↓		⊻iew Server Stat	tus		C	reate Pr	ort Number	Status		(<u>)</u> v	EN AI Setting	
Clustering Configura	tion	101		E <u>d</u> it Config			D	elete	TCP 443	Listening	_			
		.946.						Start	TCP 1194	Listening				

You will now be displayed the main iQuila Management window.

Encryption Setup

Select Encryption and Network button, this will display the Encryption and Network settings window.

Under Encryption and Algorithm *select the Appropriate encryption algorithm*, in this case for strong encryption we will select the algorithm.

ECDHE-RSA-AES256-GCM-SHA384



Once selected *click OK*

From the main management window under Management of Listeners, *select any additional ports* you may like the server to listen on and communicate with. The default port for communication from clients and bridges is TCP port 443.

If you are locating the iQuila Enterprise Device behind a firewall. Please read the iQuila Enterprise Firewall pdf

/lanagement of	Listeners:	
C <u>r</u> eate	Port Number	Status
	IIII TCP 443	Listening
Dele <u>t</u> e	1 TCP 992	Listening
	🖷 TCP 1194	Listening
Start	🖷 TCP 5555	Listening
Sto <u>p</u>		

Configuring a Bridge Device

Bridge Device Management is configured on TCP Port 5555, configure your iQuila enterprise manager to the IP of the bridge device and connect, when you first connect to an iQuila Device it will ask you to create a password.

When you connect to the iQuila Bridge for the first time you will be presented with the iQuila Bridge configuration window.

Click Next.

iQuila Enterprise Server Configuration	Wizard	
🧃 iQuila Enterprise Se	rver Configuration Wizard	
ly using this wizard, you can easily configu	e the iQuila Enterprise Server for your requirements.	
elect the type of VEN server you would lik	e to build.	
Quila Server Default Configuration.		
IQuila Enterprise Server Accepts, IQuil (default).	a Clients, Mobile Devices and Bridge Connections.	
Quila Server Site to Site Configuration	on.	
iQuila Enterprise Server Creates Layer	2 connections between sites.	
Please select the Role of the Server :		
iQuila Server Accepts inbound 8	ridge connections (Center)	
VEN Bridge at Each Site		
Advanced Configuration of iQuila E	nterprise Server	
Please select this option if you are pl	anning to build a iQuila Enterprise Server that supports dustering	
lick Next to start Setup. Click Close if you	want to exit the setup and manually configure all settings.	
	<u>N</u> ext > ⊆lose	

As Bridge devices do not require users this section is not avaliable, so please *proceed to step 2* configure connection setting

a User to Accept VEN Connection In this logistic finite prior is scored to a control access VEN, or becomes the central in this logistic finite prior is server that accepts connections from other sites, create users to pt the VEN connection. Create Users Consection to Realization VEN Conser
In this loads Entreprise Sense accepts a remote access VEN, or becomes the central to be the loads Entreprise sense that accepts connections from other sites, create users to pt the VEN connection. Create Users - Conservice to Restinction VEN Conser
Create Users
a Connection to Destination VEN Server
Configure Connection Setting
al Bridge an site-to-site VEN, use the Local Bridge Function to connect a bridge between the virtual met segment on the VEN side and the physical Ethernet segment on the local side. Select an
ing Ethernet device (Network Adapter) that will be provide the bridge connection to the VEN.
ct the Ethernet device to establish the bridge connection.

The Connection setting window will show

Under Setting name, *enter a name of the connection setting* e.g., Head Office

Host Name: *enter the host name or IP addres*s of the iQuila Enterprise server.

Port Number: unless you have configured different port numbers on the iQuila Enterprise server the port number can be left as default Port 443.



The virtual Switch name should be auto populated (unless you have disabled this function on the iQuila Server) if this function is **disabled** then manually *enter the Virtual Switch name*.

Under the section User and authentication setting, change the Auth Type to Client Certificate authentication and enter the username created with the certificate, in this scenario we will use Bridge1.

Select the Option, *specify client certificate*, select the *Certificate we made previously Bridge1 New York*, you will be prompted for the Security Phrase, once entered *press Ok*.

The certificates name an expiry date will be displayed.

Click ok

The cascade connection window is displayed the status of the connection to the server.

Select Exit

Cascade Cor either local o Before Usin Cas inco	nnection can make a layer or remote VEN Server. g Cascade Connection cade Connection creates orrectly configured, an infi	-2 Ethernet-level links between this a Layer 2 Bridge between multiple V nity loop could inadvertently be cre	Virtual Switch and other Virtual Sw /irtual Switches. But if the connectic ated. When using a Cascade Conne	itch which is located or in is ction function
etting Name	Status	Established at	Destination VEN Server	Virtual Switch
Head Office	Connecting	(None)	10.10.10.1	

On Step 3 of the wizard *select the drop down* and *select the network adaptor* you would like to bridge and *select close*.

🐢 ¹	o complete the setup of this iQuila Server / iQuila Bridge, you must complete the following tasks
Step 1. C	reate a User to Accept VEN Connection
2	When this iQuila Enterprise Server accepts a remote access VEN, or becomes the central site-to-site iQuila Enterprise server that accepts connections from other sites, create users to accept the VEN connection.
	Create Users
Step 2. D	efine a Connection to Destination VEN Server When this (Quils Enterprise Server is installed on a particular site (edge) of a site-to-site VEN y have to specify the address of the content VEN Server that accepts the connections, and establis connection to that central VEN Server.
Step 2. D	efine a Connection to Destination VEN Server When this iQuils Enterprise Server is installed on a particular site (edge) of a site-to-site VEN y have to specify the address of the center VEN Server that accepts the connections, and establis connection to that central VEN Server. <u>Configure Connection Setting</u>
Step 2. D	efine a Connection to Destination VEN Server When this (Quils Enterprise Server is installed on a particular site (edge) of a site-to-site VEN years to specify the address of the center VEN Server that accepts the connections, and establis connection to that central VEN Server. Configure Connection Setting et Local Bridge For an site-to-site VEN, use the Local Bridge Function to connect a bridge between the virtual
itep 3. So	Effine a Connection to Destination VEN Server When this (Quile Enterprise Server is installed on a particular site (edge) of a site-to-site VEN years to specify the address of the center VEN Server that accepts the connections, and establis connection to that central VEN Server. Configure Connection Setting Et Local Bridge For an site-to-site VEN, use the Local Bridge Function to connect a bridge between the virtual Ethemed segment on the VEN site and the bryksical Ethemed segment on the local Side, Sector existing Ethernet device (Network Adapter) that will be provide the bridge connection to the VEN



Ma	nage VEN Bridge "	localhost"			Li	censed t	0:				-1 days rer	maining		
yer2 Su	hth / Hub Settings	Value Sector Name	Mater	here	lbers.	Denses	fangeren.	Mat Lotes	P tables	New Jones.	Last Incom	Los Communications	hanke Bdes	Dansler Back
-32	Manage Virtual Switch	SERIOGE	Dation	Standalone	0	0	1	99	\$1	0	2021-01-05160640	2021-01-05 163253	28,459,015	907,687
÷.														
۳.	Denne													
	Office													
ē.	Were Status													
	Create a Virtual Switch													
2	hupples													
	Delete													
¢=														
	Court groupe setting													
	Layer gowild/octing Theo/LgtP Setting Open/PN/MS-SSTP													
	Later programming Layer (SwitchSetting Hases / 2019 Setting Diserving MCSSTP	_												
tvort A	Later programming Layer (SwitchSetting Have 7, g77 Setting Demonstry, MCSETP Interview, MCSETP													
tvert A	Under granden of the second se		mater				- Marag	ement of Listener	14			a-to Anti-Golf Meth Geno	e	
	uside supporting Upper (Smithing) (Hase/UpP Sating Deerver(VMCSST# and Encyption Stopption and National Stopption and National	- UN Sources	musico	View Server Stat	hs		Maring	enset of kiene	P62			ga ta Ari Kosi Metagero Que a se a	e EN AJ Setting	
	Laber () = Hyperboling Laber () = Hubboling (Habby / 2011 Sattage Developing / 455 - 6519 and Encyption and Nativent Encyption and Nativent encyption	VIN Group and	vru¥56	View Server Stat	hs		Maring	enerit of kiteee	ts L Number TEP 5555	Shituo]	ga ta Ari Kosti Meti gero Que	e EN AI Setting	
	Luce 1 projectoring Luce 1 Sel ADISCI (Fig 1946 / 277 Setting Diservice) Set 6578 of Encyption and National Second Second Second Custoring Configuration Custoring Configuration	- UR Generation	20145100	View Server Stat Esit Cardig	tus.		N3100	enerit of ideae police Para eletre	to 1.7Aunitor 1729 1995	Slatua Detering]	al la Ari Scal Met gero Que	e EN Al Sering	

You will now be presented with the main management windows for Bridges.

Packet Filtering & Data Prioritisation

iQuila Enterprise Packet Filtering and Data Prioritisation enables you to secure your network whilst prioritising your important data, depending on your Licensing, up to 4,096 entries can be defined in a Virtual Switch. Packet Filtering is a function which either passes or discards IP packets passing through network devices according to designated rules commonly referred to as packet filtering rules, rules are processed on the priority number assigned to each rule, the lower the priority number set the more important the rule. Multiple rules can be created for both IPv4 and IPv6

Data which can be Defined by Packet Filtering Entries.

The following data can be defined by the access list registered in the Virtual Switch. Data which can be Defined by Packet Filtering Entries

Basic Setting

Access List Memo.

Enter a description of the access list entry. This entry enables the setting of an arbitrary character string to clarify the entry for the Virtual Switch Administrator, and its contents has no effect on packet filtering operation.

Action.

Designates how an IP packet is treated when a matching entry definition is found in the access list. Sets to [Pass] or [Discard].

Priority.

Designates the priority of an entry within the access list as an integer. The lower the integer, the higher the priority the packet has over the VEN connection. If there are access list entries with the same priority, it is undefined as to which is applied first.

Filtering Option for IP Headers

Source IP address.

Designates the sending IP address as the packet's matching criteria. It is also possible to designate a subnet range including multiple IP addresses by designating the network address and subnet mask. All, sending IP addresses match when no range is designated.

Destination IP address.

Designates the destination IP address as the packet's matching criteria. It is also possible to designate a subnet range including multiple IP addresses by designating the network address and subnet mask. All destination IP addresses match when no range is designated.

Protocol Type.

Designates the protocol number of that IP packet as the packet's matching criteria. It is possible to match all IP protocols. The numbers which can be designated can be entered as integers although 6 (TCP/IP), 17 (UDP/IP) and 1 (ICMP) are already defined.

Source / destination port number range.

The minimum or maximum source port and destination port numbers can be designated as the packet's matching criteria when TCP/IP or UDP/IP is selected as the protocol type. All port numbers are regarded as matching when no values are designated.

Filtering Options for User and Groups

Source username.

A username can be designated as the packet's matching criteria when wishing to match only those packets sent by a specific user (strictly speaking, it is the packet sent by the VEN session of a specific username). Sending usernames are not checked when no name is designated.

Destination username.

A username can be designated as the packet's matching criteria when wishing to match only those packets to be received by a specific user (strictly speaking, it is the packet intended to be received by the VEN session of a specific username). Destination usernames are not checked when no name is designated.

Access List Entries Match

When none of the Access List Entries Match.

When multiple access lists are registered on a Virtual Switch and the IP packet does not match any of the entries contained therein, a [Pass] action is decided by default.

Adding, Deleting & Editing Access List Entries.

To add, delete or edit entries in the access list, click on the [Manage Access lists] button in the iQuila Server Manager. Next click on the [Add], [Delete] or [Edit] buttons. Be sure to click the [Save] button after completing any changes to the access list, as changes are not applied to the Virtual Switch unless saved. Furthermore, the access list is enabled from the instant it is set (also applies to iQuila VEN sessions which are already connected.

To modify the access list with the command line utility, use the [AccessAdd], [AccessList], [AccessDelete], [AccessEnable] and [AccessDisable] commands.

The following section is a brief insight to adding Packet Filtering Rules.

Iocalhost (TI	his server) - iQuila Server Manager													- 🗆 ×
🧒 Mar	nage iQuila Server	"localhost"			Li	icensed t	o: iQuila	Ltd Test	License	•	0 days rem	aining		
Layer2 Swit	ch / Hub Settings	Virtual Switch Name	Status	Type	Users	Groups	Sessions	MAC Tables	IP Tables	Num Logins	Last Login	Last Communication	Transfer Bytes	Transfer Packets
- 22	Manage Virtual Switch	DEFAULT	Online	Standalone	0	0	0	0	0	0	2023-03-09 125805	2023-03-09 12:58:05	0	0
æ_	Online													
2	Offine													
	View Status													
	Create a Virtual Switch													
1	Properties													
×	Delete													
Bridging an	d Routing													
++	Local Bridge Setting													
	Layer 3 Switch Setting													
	IPsec / L2TP Setting													
2	iQuila Mobile													
Network Ar	Encryption and Network													
**		VEN Server Info	ormation				Mana	pement of Listene	5		K	uila Artificial Intelligenc		
VEN Cluste	ring	4 ⁰		View Server Sta	tus							Q	EN AI Setting	
	Clustering Configuration	â.		Edit Config				Create Po	rt Number TCP 443	Status Listening				
-	Clustering Status	:Ö:		can comp				Start .	TCP 992 TCP 1194	Listening				
1	Connections List	₽ j ₽		About this iQuila	Server			Stop	N.F 3300	Lotenig			0.4	

To navigate to Packet Filtering select the switch and click Manage Virtual Switch.

Select Manage Packet Filtering.

ge	ment of Security Database:	Secure NA	l Settings	Current Status of this Virtual Switch:	
	Manage Users			Item	Value
	Manage your users. Create, Edit and Delete.	(D)	Virtual NAT and Virtual DHCP Server	Sector Contract Contract Manage	DEFAULT
				and Status	Oeliee
			Network Address Translation (NAT) is available on this Virtual Switch. You	I Tree	Chandelese
			can conligure virtual test and virtual DHCP.	a type	Standarone
				W NAI	Disabled
	Manage Groups		Virtual NAT may conflict with you network, please check before enabling	Sessions	0
		<u> </u>	virtual root may connect with you retwork, please check before endoring.	Access Lists	0
	Add, delete or edit groups.			a Users	0
				Groups	0
				MAC Tables	0
AC				(IP Tables	0
		VEN Sess	ions Management:	Num Logins	0
	Manage Packet Filtering			Last Login	2023-03-09 12:58:05
	managerackermenng	\bigcirc	Manage Sessions	Last Communication	2023-03-09 12:58:05
	Add or delete Packet filtering rules and apply			Created at	2023-03-09 12:58:05
	Data prioritisation.		Manage Active VEN Sessions on this Virtual Switch.	Outgoing Unicast Packets	0 packets
				Outgoing Unicast Total Size	0 bytes
				Outgoing Broadcast Packets	0 packets
				Outgoing Broadcast Total Size	0 bytes
				Uncoming Unicast Packets	0 packets
15	witch Settings:	VEN Certr	hcates	Uncoming Unicast Total Size	0 bytes
		_		Incoming Broadcast Packets	0 packets
5	Switch Properties		Trusted CA Certificates Revoked Certs	Incoming Broadcast Total Size	0 bytes
	congae and theat agest smean		Manage trusted CA certificates for you Virtual Switch and Users.		Refresh
	Authentication Server Setting	VEN Sessi	ors Management: Manage Cascade Connections	VEN Log Files	Log File Lis
ţ	Use external RADIUS authentication server for user authentication.		Establish Cascade Layer2 Bridge Connection to Switches on local or remote VEN Servers.	Configure settings of log s	aving function.

The Action List for rule creation.

Action	Status	Priority	Memo	Contents	New (IPv4)
					New (IPv6)
					Edit
					Delete
					Clone
					Enable
					Direble
					UISAD/E
					Henr with biols
					priority appear l
					11.02.055

A	Action	Status	Priority	Memo	Contents	New (IP
						New (IP
						Edit
						Delete
						berete
						-
						Clone
						Enable
						Disable
						Items with high priority appear
						in the list.

To create new rules in the Access list select New (IP4or IP6) on the right.

All rules start with Basic Settings.

asic seconds		Filtering Options for IP He	aders				
Memo:		Source IP Address:	Applies to All Sour	ce Addresses			
Action:	Pass O Discard	IP	v4 Address:				
Priority:	(Smaller number has higher priority.)	Su	bnet Mask:				
iltering Options for Users	or Groups		(255.255.255.255)	means a single host)			
This access list will specific users, grou	be applied only to the packets that for ps send or receive.	Destination IP Address: [Applies to All Dest	ination Addresses			
Source Name:	Brows	se	bnet Mask:				
Destination Name:	Brows	;e (2	55.255.255.255 mean	s Specified host only)			
Leave these nor group r	fields blank if you don't specify user nar name.	ne Protocol Type:	All IPv4 / IPv6 Protor	cols ~			
iltering Options for MAC H Source MAC Address:	leaders Applies to any Source Addresses	Specify IP Protocol:					
M	AC Address:	Filtering Options for TCP H	eaders and UDP Hea	ders Jaximum			
-		Source Port:	*				
Destination MAC Address:	Applies to any Destination Addresse	S Destination Port:					
M	AC Address:	The blank port number f It will apply to packets th minimum value is specifie	The blank port number field matches any ports. It will apply to packets that match only the minimum value when the minimum value is specified but the maximum value is not.				
You can use hexadecimal without the separators.	number with two separators, "-" or ":", a	nd Verify TCP Connec	ction State (Only TCP I	Packets)			

The first recommended rule to be applied a Discard ALL rule. This will drop all packets to the switch and should be set for IP4 and IP6.

In this example.

Set the Memo (Rule frendly name) to Discard ALL. Set Action to Discard. Discard drops the packet.

Set Priority to 1000. Sets the priority position of the rule.

All other section leave on their default setting then click OK to save the rule.

sic Settings	Filtering Options for IP Headers
Memo: Dicard ALL	Source IP Address: 🗹 Applies to All Source Addresses
Action: O Pass	IPv4 Address:
Priority: 1000 (Smaller number has	Subnet Mask:
ering Options for Users or Groups	(255.255.255 means a single host)
This access list will be applied only to the packets that for	Destination in Address Mannies to All Destination Addresses
specific users, groups send or receive.	IPv4 Address:
Source Name: Browse	Subset Marke
Destination Name: Browse	(255.255.255.255 means Specified host only)
Leave these fields blank if you don't specify user name nor group name.	Protocol Type: All IPv4 / IPv6 Protocols 🗸
ering Options for MAC Headers Source MAC Address: 🗹 Applies to any Source Addresses	Specify IP Protocol:
MAC Address:	Filtering Options for TCP Headers and UDP Headers
Mask:	Minimum Maximum
Destination MAC Address: Applies to any Destination Addresses	
MAC Address	Destination Port:
Mac Aduress:	The blank port number field matches any ports. It will apply to packets that match only the minimum value when th minimum value is specified but the maximum value is not.
fou can use hexadecimal number with two separators, "-" or "(", \sim and without the separators.	Verify TCP Connection State (Only TCP Packets)

The rule will be displayed in the Action List

	Action	Status	Priority	Memo	Contents	New (IF
1	Discard	Enable	1000	Dicard ALL	(ether) *	New (IF
						Edit
						Delet
						Ción
						Enabl
						Direk
						DISAD
						Items with hig priority appea
						in the list.

Filtering by MAC address.

Set the Basic Settings first.

The default setting for MAC filtering is set to Apply to any source address. Untick the source/destination box to enter a specific MAC address. Select OK to add the rule.

Basic Settings	Filtering Options for IP Headers
Memo:	Source IP Address: 🗹 Applies to All Source Addresses
Action: Pass Discard	IPv4 Address:
Priority: (Smaller number has higher priority.)	Subnet Mask:
iltering Options for Users or Groups	(255.255.255.255 means a single host)
 This access list will be applied only to the packets that for specific users, groups send or receive. 	Destination IP Address: Applies to All Destination Addresses
Source Name: Browce	IPv4 Address:
biowse	Subnet Mask:
Destination Name: Browse	(255.255.255.255 means Specified host only)
Leave these fields blank if you don't specify user name nor group name.	Protocol Type: All IPv4 / IPv6 Protocols 🗸 🗸
iltering Options for MAC Headers Source MAC Address: Applies to any Source Addresses	Specify IP Protocol:
MAC Address:	Filtering Options for TCP Headers and UDP Headers
Mask:	Minimum Maximum Source Port: -
Destination MAC Address: Applies to any Destination Addresses	Destination Port:
MAC Address: Mask:	The blank port number field matches any ports. It will apply to packets that match only the minimum value when the minimum value is specified but the maximum value is not.
without the separators.	Verify TCP Connection State (Only TCP Packets)
(FF-FF-FF-FF-FF means a specified host)	O Established Basket O Userstablished Basket

Filter Option for IP Headers is the main rules to set based on source/destination address and protocal type. Default setting allows any source or destination IP address and All IP4/IP6 protocol types

isic Settings		Filtering Options for IP Headers
Memo:		Source IP Address: Applies to All Source Addresses
A stilling		IPv4 Address:
Action:		Subnet Macky
Priority:	higher priority.)	
tering Options for Users o	or Groups	(255.255.255.255 means a single host)
This access list will b	e applied only to the packets that for	Destination IR Address: Applies to All Destination Addresses
specific users, group	is send of receive.	
Source Name:	Browse	
	StottSc	Subnet Mask:
Destination Name:	Browse	(255.255.255.255 means Specified host only)
Leave these nor group na	fields blank if you don't specify user name ame.	Protocol Type: All IPv4 / IPv6 Protocols V
tering Options for MAC H	eaders	All IPv4 / IPv6 Protocols
Source MAC Address:	Applies to any Source Addresses	6 (TCP/IP Protocol)
MA	C Address:	Filtering Options for TCP H 1 (ICMPv4 Protocol)
	Mask:	58 (ICMPv6 Protocol)
		Source Port: Specify the IP Protocol Number
Destination MAC Address:	Applies to any Destination Addresses	Destination Port:
MA	C Address:	The blank port number field matches any ports.
	Mask:	It will apply to packets that match only the minimum value when the minimum value is specified but the maximum value is not.
You can use hexadecimal and without the separate	number with two separators, "-" or ";", ors.	Verify TCP Connection State (Only TCP Packets)
(FF-FF-FF-FF-FF-FF mean:	s a specified host)	

Protocal Type allows you to select a custom protocol by selecting the Specify the IP Protocal number option from the list. The dropdown list contains the standard 4 protocol types by default. The Filtering options for TCP/UDP headers are the same as as used in all firewalls for traffic routing.

sic Settings	Filtering Options for IP Headers
Memo:	Source IP Address: Applies to All Source Addresses
Action: Pass Discard	IPv4 Address:
Priority: (Smaller number has	Subnet Mask:
tering Options for Users or Groups	(255.255.255.255 means a single host)
This access list will be applied only to the packets that for specific users, groups send or receive.	Destination IP Address: Applies to All Destination Addresses
	IPv4 Address:
Source Name: Browse	Subnet Mask:
Destination Name: Browse	(255.255.255 means Specified host only)
Leave these fields blank if you don't specify user name nor group name.	Protocol Type: 6 (TCP/IP Protocol) V
tering Options for MAC Headers Source MAC Address: ☑ Applies to any Source Addresses	Specify IP Protocol:
MAC Address:	Filtering Options for TCP Headers and UDP Headers
Mask:	Minimum Maximum Source Port:
Destination MAC Address: 🗹 Applies to any Destination Addresses	Destination Port: -
MAC Address:	The blank port number field matches any ports.
Mask:	ni will apply to packets that match only the minimum value when the minimum value is specified but the maximum value is not.
You can use hexadecimal number with two separators, "-" or "\",	Varify TCD Connection State (Only TCD Deckets)