

VPN Gateway Virtual Appliance (VGVA) for L2 VPN Installation Guide March 2020





Table of Contents

Introduction	2
Overview of Solution	2
Document Control	3
Network Schematic	3
VPN Gateway Virtual Appliance Server Prerequisites	3
Deploying VMWare Infrastructure	4
Initial Configuration and License Activation	6
Create VGVA in ExtremeCloud IQ	7
Configure Layer 2 VPN	7
Step 1: Create a L2 IPsec VPN Object	8
Step 2: Create or edit a Network Policy	10
Step 3: Verify the IPsec Tunnel	12
Step 4: Verify Client Connectivity	14
Summary	14

Introduction

This document has been created to provide a configuration walkthrough guide to allow technical staff to deploy Extreme Networks' VPN Gateway Virtual Appliance (VGVA) software in a VMWare environment and remote devices to provide Layer 2 VPN.

This document focuses on the creation of a Layer 2 VPN solution, deployed between an access point running IQ Engine (AP305C, AP510C, AP410C, AP30, AP150W, AP122, AP630, AP230, AP130) and a VGVA.

The document describes the configuration steps to prepare the VMWare environment for deployment of the VGVA, installation of VGVA software, Layer 2 VPN policy creation and its deployment to the VGVA and wireless access points.

Overview of Solution

The solution comprises of three elements; ExtremeCloud[™] IQ Management Platform, remote access point network devices and VGVA software.

The ExtremeCloud IQ management platform is used to create configuration policies, distribute policies to network devices, and monitor connected devices and clients. The remote access point is used to provide local wireless services and initiate Layer 2 VPN tunnels to the VGVA software that runs as a virtual machine on VMWare ESX hosts. It is used to terminate Layer 2 VPNs and forward traffic from remote sites into the head office network and forward remote outbound traffic in VPN from the head office to the remote sites.

Document Control

Version Number	Date	Description	Author
1.0	February 2020	Configuration Guide - VPN Gateway Virtual Appliance (VGVA) for L2 VPN	Marko Tisler, Glyn Brice, Stuart Farmer

Network Schematic

The Layer 2 VPN solution requires the ability for the remote access point to create a Layer 2 VPN from the remote site to the centrally hosted VGVA. Figure 1 shows a typical deployment of the solution.

The remote access point is connected to the home router which provides IP addressing information. The VGVA software logically connects on EthO, the host server is connected to the upstream firewall in a DMZ. The two ExtremeCloud IQ devices are configured and managed by the ExtremeCloud IQ instance.

The access point provides wireless connectivity to local devices, based on the configuration the traffic is forwarded in the VPN tunnel between the access point and the VGVA.

The head end firewall is configured to allow VPN traffic from the Internet, the data is decrypted by the VGVA and forwarded to the firewall from

the same interface, the firewall controls traffic to the internal network. The traffic once decrypted can be tagged with VLAN information to provide segregation.

The traffic from the head end follows the reverse path, forwarded by router to firewall, inspected and forwarded by firewall to VGVA, encrypted and forwarded across the Internet to the access point where it is decrypted and forwarded to wireless client.



Figure 1 - Layer 2 VPN Solution

VPN Gateway Virtual Appliance Server Prerequisites

This section of the document describes the VMWare server requirements that are required to install and run VGVA, managed by ExtremeCloud IQ.

The VGVA software will require Internet access (http/https) for the purposes of license verification. This can also be achieved using a HTTP proxy server configured as a part of the initial configuration. The administrator will be prompted to enter the proxy server during the initial configuration wizard and will access to a DNS server.

If the intention is to place clients onto VLANs other the its management VLAN, you will need to configure the VM to support trunking inside the vSphere environment. This is achieved by setting the associated port group configuration with VLAN label 4095. Also make sure your network infrastructure is correctly configured with the required VLAN and trunk settings. You can learn more <u>here</u>.

rts Netwo	ork Adapters				
Configuratio	on ch gement VLAN	Summary 120 Ports Virtual Machine	Port Group Properties Network Label: VLAN ID:	CVG Trunk All (4095)	
CVG V VM Ne Mana	/LAN 203 etwork gement Net	Virtual Machine Virtual Machine vMotion and IP	Effective Policies Security		
VG 1	Trunk	Virtual Machine	Promiscuous Mode: MAC Address Changes: Enroed Transmits:	Accept Accept	

Ensure that the port group in vSphere allows promiscuous mode. If disabled L2 VPN clients may not be able to receive an IP address or pass any traffic. You can access these settings on your host > Configuration > Networking > <your vSwitch>.

orts	Network Adapters				
Conf	iguration	Summary	Port Group Properties -		
-	vSwitch	120 Ports	Network Label:	CVG Trunk	
	Management VLAN	Virtual Machine	VLAN ID:	All (4095)	
ō	CVG VLAN 203	Virtual Machine			
0	VM Network	Virtual Machine	Effective Policies		
0	Management Net	vMotion and IP	Security		
0	CVG Trunk	Virtual Machine	Promiscuous Mode:	Accept	
			MAC Address Changes:	Accept	
			Forged Transmits:	Accept	
			Traffic Shaping		
			Average Bandwidth:	-	
			Peak Bandwidth:		
			Burst Size:	-	
			Failover and Load Bala	ncing	
			Load Balancing:	Port ID	
			Network Failure Detection	n: Link status only	
			Notify Switches:	Yes	
			Failback:	Yes	
			Active Adapters:	vmnic0	
			Standby Adapters:	None	

Deploying VMWare Infrastructure

1. Once the VGVA firmware .ova file has been downloaded from the Extreme Networks' support portal, open the vSphere client. Go to File > Deploy OVF Template and locate the downloaded .ova file

Ø		vcenter2 - vSphere Client		-	D X
File Edit View Inventory Admin	Ø	Deploy OVF Template	_ 0 X		
This (55) Vois Interface All to be and	Server Select the source location.	Depicy GVF Template Depicy GVF Template Depicy from a file or UR. Classrichdreate after Torrelated Art (Sorthand) (Sorth Art and Sorthand) The Star SLE, bedowska after start for Of package from the Demonship after and the	Browse e, or drive, a	h Inventory	9
Recent Tasks Name Target				c • Completed Time	Clear
	Help	< Back	Vext > Cancel		

2. Click Next. Click next again on the following screen.

0		Deploy OVF Template		- • ×
OVF Template Details Verify OVF template details.				
Source OVF Template Details Hame and Location Di Host / Cluster Resource Pool Dick Format Ready to Complete	Product: Version: Vendor: Publisher: Download size: Size on disk: Description:	Aerohive HiveOS Virtual Applance HiveOS 6.21 Aerohive Networks, Inc. No certificate present 28.9 MB 23.3 MB (fm provisioned) 256.1 MB (fmkk provisioned)	,	
Help			< Back Next >	Cancel

3. Give the virtual machine a name and select the inventory location.

Ø	Deploy OVF Template
Name and Location Specify a name and loca	ation for the deployed template
Source OVF Template Details Name and Location II host / Cluster Resource Pool Disk Format Ready to Complete	Name: <u>faredware Hover05 Virtual Applance</u> The name can contain up to 80 characters and it must be unique within the inventory folder. Inventory Location: Venter2 Lob2
Help	< Back Next > Cancel

4. Select the host server.

0	Deploy OVF Template	- • ×
Host / Cluster On which host or duster	do you want to run the deployed template?	
Source OVE Tendate Details Name and Location Details (Cluster Specific Host Resource Pool Disk Format Ready to Complete		
Help	< Back Next	> Cancel

5. Select the datastore that will host the virtual machine.

Storage Where do you want to sto Source QVF Temolate Details Name and Location Host / Cluster Storage Disk Format Network Mapping Ready to Complete	Select a destination sto VM Storage Profile: Name Data2-RAIDI datastore1	s? Prive Type Drive Type Non-SSD Non-SSD	al machine files: Capacity Provisioned 418.00 GB 910.99 GB 413.25 GB 362.41 GB	Free Type 66.53 G6 VMFS3 91.44 G8 VMFS3	Thin Pro Support Support
Source QVF Tennolate Details Name and Location Host / Cluster Storage Disk Format Network Mapping Ready to Complete	Select a destination sto VM Storage Profile: Name Data2-RAID1 datastore1	Drive Type Drive Type Non-SSD	Capachy Provisioned 418.00 GB 910.99 GB 413.25 GB 362.41 GB	Free Type 66.63 GB VMFS3 91.44 GB VMFS3	Thin Pro Support Support
Usante articultation Host / Cluster Storage Disk Format Network Mapping Ready to Complete	Name Data2-RAID1 datastore1	Drive Type	Capacity Provisioned 418.00 GB 910.99 GB 413.25 GB 362.41 GB	Free Type 66.63 GB VMFS3 91.44 GB VMFS3	Thin Pro Support
Storage Disk Format Network Mapping Ready to Complete	Data2-RAID1	Non-SSD Non-SSD	418.00 GB 910.99 GB 413.25 GB 362.41 GB	66.63 GB VMFS3 91.44 GB VMFS3	Support
Disk Format Network Mapping Ready to Complete	datastore1	Non-SSD	413.25 GB 362.41 GB	91.44 GB VMFS3	Support
	5				
	Disable Storage D	RS for this virtual	machine		>
	Select a datastore:				
	Name	Drive Type	Capacity Provisioned	Free Type	Thin Prov
	5				د
	1.1				
Help			< Back	Next >	Cancel

6. Select the disk format.

Note: Thick provisioning will reserve all the disk space needed by the virtual machine while thin provisioning will reserve the minimal amount and increase it later if needed.

Ø	Dep	loy OVF Template	_ _ ×
Disk Format In which format do you	want to store the virtual disks?		
Source OvEr Template Datalis Vanne and Location Hotor / Cluster Startine Disk Format Network Mapping Ready to Complete	Datastore: Available space (GB): (© Thick Provision Lazy Z C Thick Provision Eager C Thin Provision	Data2-RAID1 66.6 eroed Zeroed	
Help			<back next=""> Cancel</back>

7. Select the network for the virtual machine's EthernetO interface. This will be the network for the management interface of the virtual appliance (VA). In this case, we are connecting the VA to a Network called CVG-WAN.

2	Deploy OVF	Template	>
Network Mapping What networks shoul	d the deployed template use?		
Source OVF Template Details Name and Location	Map the networks used in this OVF	template to networks in your inventory	
Host / Cluster	Source Networks	Destination Networks	
Storage Didu Formation	Ethernet0	CVG-WAN	
Network Mapping Ready to Complete			
Help		< Back Nex	t > Cancel

8. Review your settings and click Finish.

)	Deploy OV	/F Template
Ready to Complete Are these the options	you want to use?	
Source gviF Template Details Name and Location Hold / Cluster Storace Disk Format Network Nacons Ready to Complete	When you dick Finish, the deploy Deployment settings: OVF file: Download state: Size on disk: Name: Folder: Host/Cluster: Datastore: Disk provisioning: Network Mapping: Network Mapping:	nent task will be started. C:\Users\Administrator\Downloads\AH_VG-VA.ova 28.9 MB 32.3 MB Acrohive HiveOS Virtual Applance Lab2 10.5.1.4 Data2-RAID1 Thin Provision "Ethernet" to "CVG-WAN" "Ethernet1" to "Drop"
Heln	✓ Power on after deployment	cBack Earth Convol

Initial Configuration and License Activation

Open the console access to the VGVA virtual machine in the vSphere client. Login using the username admin and password aerohive.



You will be greeted by the initial Virtual Appliance Wizard. Start with configuring the network settings (option 1).





Configure either static or DHCP configuration for the IP address of the eth0 interface of the virtual appliance.

Note: eth0 interface will be used for the initial connectivity between the VGVA and ExtremeCloud IQ. It will be necessary to set the actual management interface settings for the VGVA from ExtremeCloud IQ once the VGVA is connected to it. After the management interface is configured from ExtremeCloud IQ, the eth0 interface will no longer have an IP address and will only be used for bridging traffic. The mgt0 interface IP settings will be used for all further communication including GRE and IPsec tunnels.

Note: For ease of use it is recommended to configure the ethO interface IP settings using DHCP during this initial stage and set the static settings from within ExtremeCloud IQ once the VGVA is connected to ExtremeCloud IQ.



Once network settings have been entered manually and confirmed,

press "Enter" to start the connectivity test. The VA will then perform the following tests:

- Ping the default gateway
- Resolve a FQDN using the provided DNS server
- Try to contact the licensing server

Note: The management VLAN that the virtual machine is the untagged VLAN.

Network Settings
The Hive®S Virtual Appliance wast be able to conwanicate with hosts on the Internet in order to process your activation code and be configured by HiveManager.
Choose the ∺ethod for configuring the eth8 interface settings: 1. Use DHCP to obtain the interface IP address, net⊨ask, gateway, and DNS server IP address 2. Manually configure the interface settings Enter option {(1) or 2>:1
Do you want to apply the change?<[yes];no>;yes
Testing the connection between the HiveOS Virtual Appliance and license server (Press Enter to start)_ $\!\!\!$

Enter the activation code and the system will create a Serial Number this will be entered into ExtremeCloud IQ in order to add the device for management.



Create VGVA in ExtremeCloud IQ

In order to add the VGVA, login to the ExtremeCloud IQ instance. If you are using the Local Cloud (VA) version of ExtremeCloud IQ this step can be skipped as the VGVA will try to locate the Local Cloud using the normal discovery mechanisms (DHCP, DNS, redirector).

In order to add the VGVA to the ExtremeCloud IQ instance as a new device click "Add" while in the Manage/Devices tab. This workflow allows the administrator to assign location and a Network Policy, that will be automatically assigned once the device connects to ExtremeCloud IQ.

ADD 🛃	5 17 10							Utilities	Actions	Update Devices		fault View 👻
Device Type Real Simulate	Device Make ed Aerohive Dell	Entry Type Manual CSV	Extreme Networ (Separated by co . 025017052101	ks omma) E.g Ade 01	I Location .ter >> 16 Spring Gardens >> F	iloor 1 🕞	Add Policy G * ADD	DEVICES CANCEL				
Enter Hostna		Serial # SEAR	ICH							Showing 2 of 2	0 Selected I Se	lect: All Pages, None
Status	Host Name	Uptime	Clients	MAC	Location		Serial #	Model	IQ Eng	ine Updated	 Polic 	y MGT IP Address
- •	AH-795080	0d 3h 19m	0	885BDD795080	aerohive >> Dorchester >> 1	6 Spring Gard	01301604120755	AP130	8.4r4	2020-03-18 15:17:55	GB-L2- Remote	192.168.0.124
- •	AH-2d8680	0d 1h 38m	0	F4EAB52D8680	Assign		60018082400107	XR600P (L2 VPN Gateway	r) 10.0r7a	2020-03-18 17:12:19	GB-L2- Remote	192.168.85.1
10 20	50 100											H 4 1 - H GO

Once the VGVA contacts and connects to your ExtremeCloud IQ instance, click on the device name while in the Manage/Device tab, and assign a static IP address.

Configure the management IP address depending on your environment. By default, the management IP address needs to come from the untagged (native) VLAN. This can be overridden. Once done click "Save".

IPv4		
Static Address		
IPv4 Address*	10.5.2.120	
Subnet Mask*	255.255.255.0	
Default Gateway	10.5.2.1	
 Dynamic Address Config 	aration (DHCP)	
fanagement VLAN	(1-4054)	
lative VLAN		

Next, you will need to decide what you are using the VGVA for. It could either be to terminate GRE tunnels for guest tunneling or IPsec tunnels from wireless access points acting as VPN clients.

Configure Layer 2 VPN

The configuration steps to deploy the Layer 2 VPN is completed within the Network Policy of ExtremeCloud IQ and deployed to the VGVA and wireless access points.

Requirements

- The VPN is created between access point(s) and the VGVA .
- The access points and VGVA are managed by the same ExtremeCloud IQ instance.
- The IP address assignment, L3 routing and firewalling is done by other network devices located at head end.
- The VGVA uses static IP addressing for the mgtO interface. This is required in order to properly configure NAT on the firewall and forward the traffic coming from the AP to the correct IP address. Alternatively, you can create a static assignment on your DHCP server.
- All port forwarding/port mapping is configured on the local firewall/router.
- The firewall is configured to perform Network Address Translation and UDP forwards traffic to ports 4500 and 500 to the internal mgt0 (management interface) IP address of the VGVA.
- The VGVA HiveOS version is 6.9rx or later.



Step 1: Create a L2 IPsec VPN object

In ExtremeCloud IQ create a new L2 IPSec VPN object under Configuration > Common Objects > Network > Layer 2 IPSec VPN. Click "Add".

ExtremeCloud	Pilot ONBOARD CONFIGURE	MANAGE ML INSIGHTS	CLOUD VIEW	/ A3	Q	۹ 🖗	glyn brice Aerohive - INTL Partner Account
201107	Layer 2 IPsec VPN Services P New Laye	r 2 IPsec VPN Service					
POLICY	New Layer 2 IPsec VPN	Service					
BASIC							
SECURITY	Name *						
QOS	Description						
MANAGEMENT			h				
NETWORK	During VDN Comment During						
Access Consoles	 Device VPN Server and Device 	e VPN Client Settings					
ALG Services	Single Device VPN Server	Redundant Device VPN Server	rs				
LLDP/CDP Profiles	Device VPN Server*	Select One	*				1
IP Tracking Groups	Server Public IP Address						2
Layer2 IPsecVPNServices							
Location Servers	Server MGT0 IP Address						
Management Options	Server MGT0 Default Gateway						
Tunnel Policies	Client Turnel IP Address Paol Start *						
sFlow Receivers	Contra Factorial Procession Contra						
Network Services	Client Tunnel IP Address Pool End *						
Subnetwork Space	Client Tunnel IP Address Pool Netmask*						
VPN Services							
Firewalls	Device VPN Client DNS Server *		ک + ۵	7			
AUTHENTICATION	Note: A VPN Gateway Virtual Appliance su	pports up to 1024 VPN clients, and	an AP supports up	a to 128VPN clients.			
AAA Server Settings							

Name the VPN object e.g. L2-VPN and select a VPN server from the Device VPN Server dropdown menu. Up to two servers can be configured for redundancy purposes.

Add VPN Services Layer2			×
Name *			
L2-VPN			
Description			
li li			
Device VPN Server and Device	e VPN Client Settings		
Single Device VPN Server	Redundant Device VPN Se	ervers	
Device VPN Server *	AH-00ad00	~	
Server Public IP Address	86.138.76.234		
Server MGT0 IP Address	192.168.85.1		
Server MGT0 Default Gateway	172.18.21.225		
Client Tunnel IP Address Pool Start *	192.168.3.1		
Client Tunnel IP Address Pool End *	192.168.3.101		
Client Tunnel IP Address Pool Netmask *	255.255.255.0		
Device VPN Client DNS Server *	Google-DNS	¥ ≓ + ⊡∕	
Note: A VPN Gatewav Virtual Appliance su	noorts up to 1024 VPN clients. a	and an AP supports up to 128VPN clients.	
		CAN	DEL

ExtremeCloud IQ will automatically determine the server's public IP address which will be used as the L2 IPsec VPN tunnel destination by the L2 VPN clients. Dedicate a non-existent IP Address Pool to be used for L2 VPN tunnel. These addresses will be used to create tunnel interfaces on the VPN clients.

Scroll down on the same screen, the administrator is presented with the User Profiles for Traffic Management. This selects the user profiles which should have their traffic tunneled across the VPN tunnel. In this case we selected the traffic for the user profile "GB-L2-Remote-UP" to be tunneled back to the VPN server.

Click Save.

Add VPN Services L	_ayer2
User Profiles for Tra	affic Management
Available User Profiles	VPN Tunnel Mode
GB-PCG-Owner-KB-UP	Enabled
GB-PCG-Guest-KB-UP	Enabled
GB-Test-1X-C	Enabled
Remote-Working	Enabled
GB-L2-Remote-UP	Enabled
GB-Remote-L2-UP	Enabled
Optional Settings	
IPsec VPN Certificate	Authority Settings
+ Server-Client Credent	lials
Advanced Server Opt	ions
+ Advanced Client Optic	ons

Step 2: Create or Edit a Network Policy

The next step is to create a Network Policy which will use this L2 IPsec VPN object. Create an SSID and select the appropriate authentication method. Example below uses WPA2-Personal.

😎 ExtremeCloud I	Pilot onboard <u>configure</u> man	AGE ML INSIGHTS CLOUD VIEW	A3		Q 📜 🕚 よ glyn brice Aerohive - IN	TL Partner Account					
Network Policies > GB-L2-Remote >	All SSIDs > GB-Remote-L2										
Policy Details Wireless Networks Device Templates Reuter Settings Additional Settings Deploy Policy											
CONFIGURATION GUIDE	Wireless Network										
Policy Name GB-L2-Remote User Profile @ GB-L2-Remote-UP	Name (SSID)* GB-Remote-L2 Broadcast SSID Using GB-Remote-L2 WRF0 Radio (2.4 GHz or 5 GHz) Re-UP WRF1 Radio (5 GHz orly)										
SSID Usage SSID Authentication MAC Authentication											
	OP Enterprise WPA/WPA2/WPA3	Personal WPA/WPA2/WPA3	B Private Pre-Shared Key	Copen	?						
	Key Management WPA2-	WPA2 Personal)-PSK *									
	Encryption Method CCMP	AES) *									
	Key Type ASCII F	ey 👻									
	Enable Captive Web Portal										

User Access Settings Configure your QoS, VLAN, Firewall policies, and Traffic Tunneling
Default User Profile GB-L2-Remote-UP +
Apply a different user profile to various clients and user groups.
Additional Settings 4 Configure your Availability Scheduling, Security Controls, Optional Settings, and Client Monitoring

In this case we have created an SSID called GB-Remote-L2 utilizing a user profile called "GB-Remote-L2-UP". The user profile ties the L2 IPSec VPN tunneling rules to this SSID. Save the Network Policy.

Note: The user is mapped to VLAN 1 in this case. To place the connected client device in a different VLAN, make sure the VG VA virtual machine Ethernet 0 interface is configured as a trunk port in vSphere and that VLANs are actually being passed to the ESXi server.

Click "Save" and go to the "Additional Settings" section. This is where we will assign a VPN Service to this network policy.

ayer 2 IPsec VPN Services				
Wireless Networks	Device Templates	Router Settings	Additional Settings	Deploy Policy
Layer 2 IPsec VPN Services				
Layer 2 IPsec VPN Service	ON			
Layer 2 IPsec VPN Settings	+ 5			
Selected VPN Service Layer 2	GB-L2-Remote			

First, turn the Layer 2 IPsec VPN feature on. Then click to select the VPN Service we created under the Common Objects section. Click "Select" and click "Save". Finally, upload this Network Policy to both the VGVA and the access point which will serve as the VPN Client.

Network Policies 🤌 GB-L2-Remote 🎽 La	yer 2 IPsec VPN Services	Layer 2 IPsec VPN Service	×		
Policy Details	Wireless Networks			Additional Settings	Deploy Policy
MANAGEMENT SERVER	Layer 2 IPsec VPN Services	II Name			
DNS Server	Layer 2 IPsec VPN Service	GB-L2-Remote			
NTP Server	Layer 2 IPsec VPN Settings	10 20 50 500	н « 1 » н 🗌 🚥		
Syslog Server	Selected VPN Service Layer 2		CANCEL		
POLICY SETTINGS					
ACSP Logging					
Bonjour Gateway Settings					
Device Credentials					
Device Data Collection And Monitoring					
Device Time Zone					
HIVE					

Click "Select" and click "Save". Finally, upload this Network Policy to both the VGVA and the access point which will serve as the VPN Client.

Apply the network policy to selected devices Orly store devices that are: Image: Constraint of the selected	Apply the network policy to selected devices Origination Opyload devices that are: Image: Topology and the set of the s	
Orly show devices that are: Image: Constraint of the original state of	Ordyretine Hind In Filde Filde Filde Filde Filde Serial # / Serials # / S	
Bithus Device Nome Device Model IP Address MAC Address Serial # / Service Tag Last Updated On Image: Comparison of the Co	Status Device Name Device Model IP Address MAC Address Serial # / Service Tag Last Upd V I AH 795680 AP130 192 168.0.124 8650D795000 01301604120753 2020-034 V I AH 205680 XR600P 192 168.1.221 F4EA85206600 60016082400107 2020-034 10 20 50 100 X	
Image: Control Contro Control Contron Control Control Control Control Control Control C	Image: 1 A4755600 AP130 192 168.1.24 885800755680 01301604120755 2020403 Image: 1 A4426860 X9600P 192 168.1.221 F4EA85206680 6001602240107 2020403 Image: 1 A14-06160 X9600P 192 168.1.221 F4EA85206680 6001602240107 2020403 Image: 1 X9600P 192 168.1.221 F4EA8520680 6001602240107 2020403 Image: 1 X9600P 192 168.1.221 F4EA8520680 1900P 1900P Image: 1 X960P 190 P 190 P 190 P 190 P 190 P	ted On
Att-2x3660 XR600P 192.168.1.221 F4EA85206680 60018052400107 2020-03-181840-45 10 20 60 100 10<	Image: Part Add Scale Sca	15:17:55
10 20 50 100 R (1) H (0	10 20 00 100 () () () () () () () () () () () () ()	18:40:45
		н 🔤 😡

Step 3: Verify the IPsec tunnel

To verify that the IPSec tunnel has been successfully established, navigate to the Monitor tab and select the Access Point. Click Manage > Tools > Utilities > Device Diagnostics.



↓ CONNE	CTION STATUS	i Online / 9 O	fline	↓ TOTAL A	PPS 12		CLI	ENTS 1	USERS 0		ALARMS 0 I 4 I 0		SECURITY 0 Rogue A	Ps I 0 Rogue Clients
	Client Monitor	Diagnosis	Utilities	Packet Capture										
▼₀ ►	Device Di	agnostics												
			ddr o s	how Log									0 17	
	Status	Host N	lame S	how Version	ptime	MGT IP Address	Clients	MAC	Location	Serial #	Model	IQ Engine	Updated	
	🖸 🖷 🗊	AH-79	5080 S	how Running Config	d 0h 26m	192.168.0.124	0	8858DD795080	aerohive >> Dorchester >> 16 Spring Ga	rdi 01301604120755	AP130	10.0r8	2020-03-19 11:38:	
	- •	AH-2d	8680 S	how Startup Config	d 0h 12m	192.168.1.221	0	F4EAB52D8680	Assign	60018082400107	XR600P (L2 VPN Gateway)	10.0r7a	2020-03-19 11:38:	
			s	how MAC Routes										
			s	how ARP Cache										
			s	how Roaming Cache										?
			s	how DNXP Neighbors										
			s	how DNXP Cache										
			s	how AMRP Tunnel										
			s	how GRE Tunnel										
			s	how IKE Event										
			s	how IKE SA										
			s	how IPsec SA										
			s	how IPsec Tunnel										
			s	how CPU										
			s	how Memory										

This will display successfully established VPN tunnels. The following commands can be used to verify the VPN tunnels have been successfully created.

Show IKE SA

Show IKE SA						>	<
1: phase 1 start;							
2: msg 1 received;							
3: msg 1 sent;							
4: msg 2 recived;							
5: msg 2 sent;							
6: msg 3 received;							
7: msg 3 sent;							
8: msg 4 received;							
9: phase 1 establishe	ed;						
10: phase 1 expired;							
S=Side(I=Initiator;R=F	Responder):V=Version:E=Etype						
Created=ISAKMP SA crea	ated time;Phase2=Counter of phase 2	rekey					
Destination	Cookies	ST S	V	E Created		Phase2	Tu
nnel-ID							
86.153.11.253[4500]	96882a08a02c4b0e:c39be48ac0f48b1b	9 I	10	M 2020-03-20	19:14:56	1	
9							

Show IPsec SA

Show IPsec Tunnel

IPsec Tunnel Duration:									
Scurce	Destination	Created		Duration					
192.168.1.221[4500]	82.26.25.241[1065]	2020-03-20	19:14:56	0 days 0 hours 3 minutes 30 seconds					
Total IPsec Tunnel Sess	ions: 1								
Tunnel Statistic Inform	ation::								
Src IP	Dst IP	Pkts	Bytes	Auth-Err	Other-Err	SPI	Remaining-Lifet	ime	
192.168.1.221[4500]	82.26.25.241[1065]	22	1628	0	0	0x03111d08	1584734473(s)	expir	
e									
82.26.25.241[1065]	192.168.1.221[4500]	25	1863	0	0	0x0bacb864	1584734473(s)	expir	
e									

×

 \times

Step 4: Verify Client Connectivity

You can now connect the WLAN client to the SSID you created and configure for L2 IPSec VPN. The client should get its IP address from the LAN subnet behind the VGVA. The VLAN can be different than the one used by the VGVA and the VLAN ID is defined by the User Profile object.

Summary

This solution provides a method to quickly and easily deploy a layer 2 VPN between the Virtual Gateway Appliance (VGVA) and a wireless access point. Once deployed, the solution will extend the head office network to remote locations and provide remote wireless users the abilituy to access head office based applications.



http://www.extremenetworks.com/contact

©2020 Extreme Networks, Inc. All rights reserved. Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries. All other names are the property of their respective owners. For additional information on Extreme Networks Trademarks please see http://www.extremenetworks.com/company/legal/trademarks. Specifications and product availability are subject to change without notice. 30018-0420-09