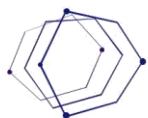


Informe De Implementación Final SERINGTEC - Casa de Bolsa

19 de noviembre de 2019
Presentado Por: SOFTMATSERVICES SAS



SOFTMAT

Services SAS

NIT 901111352-2

Contenido

INTRODUCCIÓN	3
1- ALCANCE.	3
2- ACTIVIDADES REALIZADAS	3
3- TECNOLOGIAS INVOLUCRADAS	3
4- EQUIPOS INSTALADOS	3
5- TOPOLOGÍA	6
6- CONFIGURACIÓN WLAN	7
7- FIREWALL INFORME DE IMPLEMENTACIÓN.....	10
8- ACCESOS.....	22

INTRODUCCIÓN

Este documento tiene por objetivo presentar un informe detallado del desarrollo del proyecto de la implementación de la red inalámbrica y configuración del firewall perimetral.

1- ALCANCE.

Los alcances de este proyecto incluyen exponer el uso y funcionamiento de la infraestructura de Aruba Networks, cisco y la plataforma de seguridad Sophos.

2- ACTIVIDADES REALIZADAS

Las tareas realizadas fueron las siguientes:

- Configuración de los Access Point de Aruba Networks y Cisco de acuerdo con las necesidades de la institución.
- Integración de la solución con la LAN y los servicios con los que se cuentan en el sitio.
- Configuración del firewall perimetral.

3- TECNOLOGIAS INVOLUCRADAS

Se configuro una controladora 2500, la cual presenta una arquitectura centralizada para la solución cisco, de igual manera se configuro una red anillo de la solución Aruba Networks, y se instala el firewall Sophos el cual es el cerebro de la red.

4- EQUIPOS INSTALADOS

En la siguiente sección se presenta una descripción de los equipos que conforman la solución implementada a Seringtec:

Controladora cisco 2500



Una controladora opción ideal para redes más pequeñas y sucursales, el controlador inalámbrico de la serie 2500 crece con su negocio. Se escala a 75 puntos de acceso y 1000 dispositivos cliente. También ofrece acceso inalámbrico seguro para invitados. Con la tecnología integrada Cisco CleanAir, este controlador ejecuta una red de autocuración y optimización.

Cisco Aironet 1040



La serie 1040 es un punto de acceso 802.11n de nivel empresarial de nivel de entrada diseñado para satisfacer las necesidades de conectividad inalámbrica de las pequeñas y medianas empresas.

Business Ready 802.11n Rendimiento Con la tecnología 2x2 de entrada y salida múltiples (MIMO) que proporciona al menos seis veces el rendimiento de las redes 802.11a/g existentes, la serie Cisco Aironet 1040 ofrece la ventaja de rendimiento de la calidad de clase empresarial 802.11n a un precio básico para pequeñas y medianas empresas.

Aruba IAP 305



Los puntos de acceso de la serie básica 300 Wave 2 de Aruba ofrecen un alto rendimiento y una soberbia experiencia de usuario para entornos de media densidad.

Estos puntos de acceso Wave 2 proporcionan ClientMatch con capacidad MIMO multiusuario (MU-MIMO) para aumentar la eficiencia de la red y respaldar la creciente demanda de densidad en su red.

La serie 300 también dispone de un Aruba Beacon Bluetooth integrado que simplifica la gestión remota de una red de Aruba Beacons de larga escala alimentados por batería, proporcionando a su vez ubicación y guía en interiores avanzadas, además de capacidades de notificaciones automáticas basadas en proximidad.

Firewall Sophos

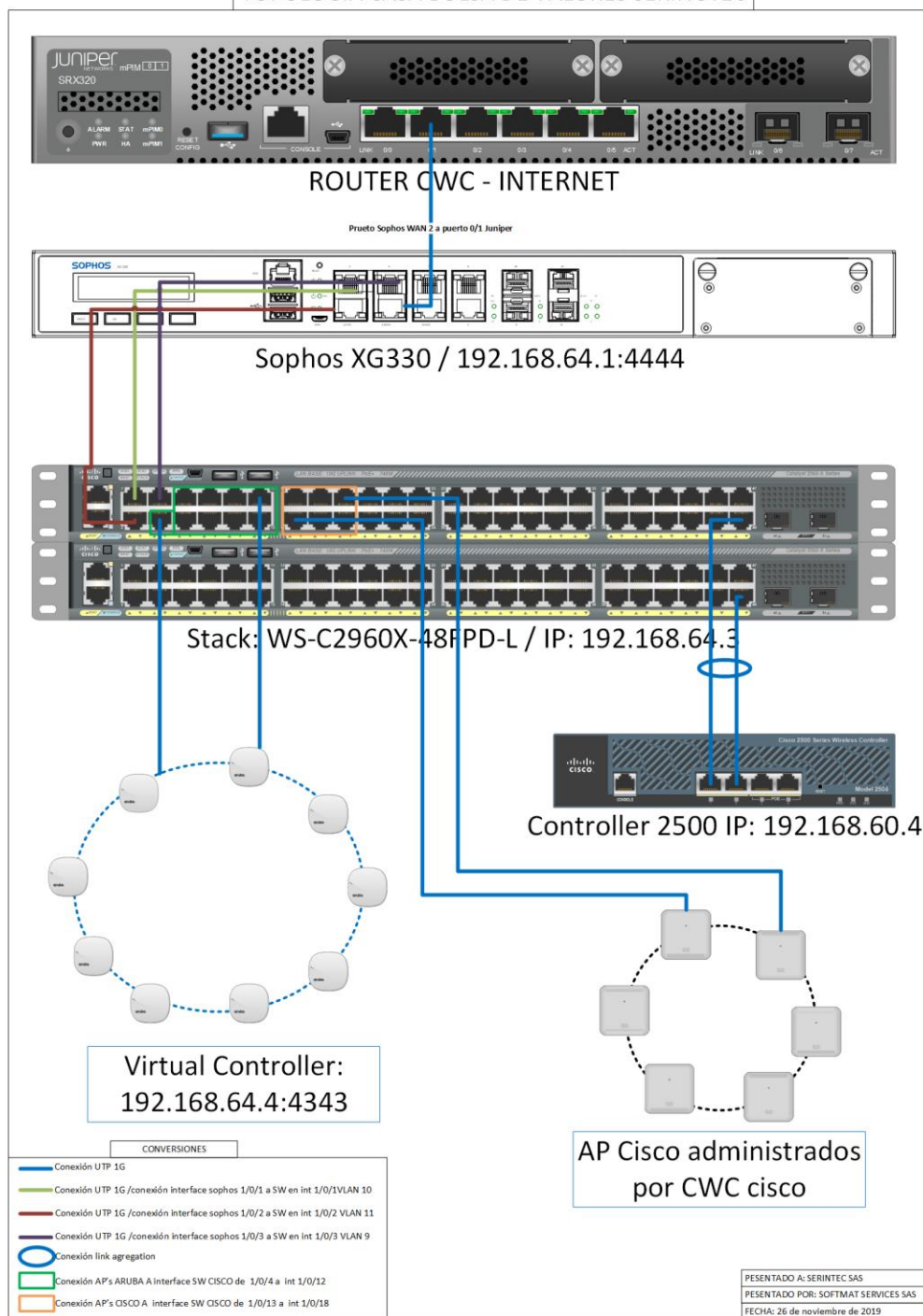


El dispositivo **Sophos XG330** está diseñado para proporcionar el equilibrio óptimo entre rendimiento y protección: para diversos

Entornos de TI. Estos escritorios de nivel de entrada los cortafuegos son la opción ideal para el presupuesto pequeñas empresas conscientes, minoristas y pequeñas u oficinas en el hogar.

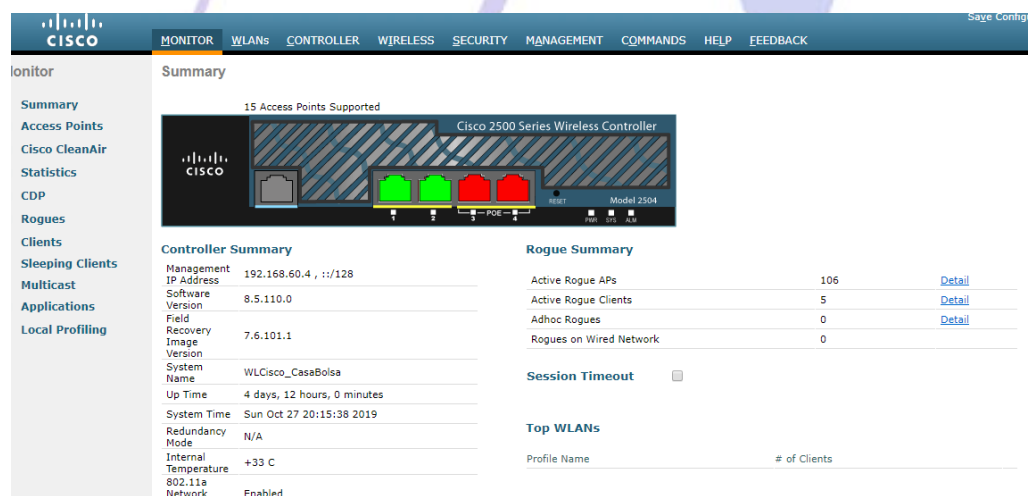
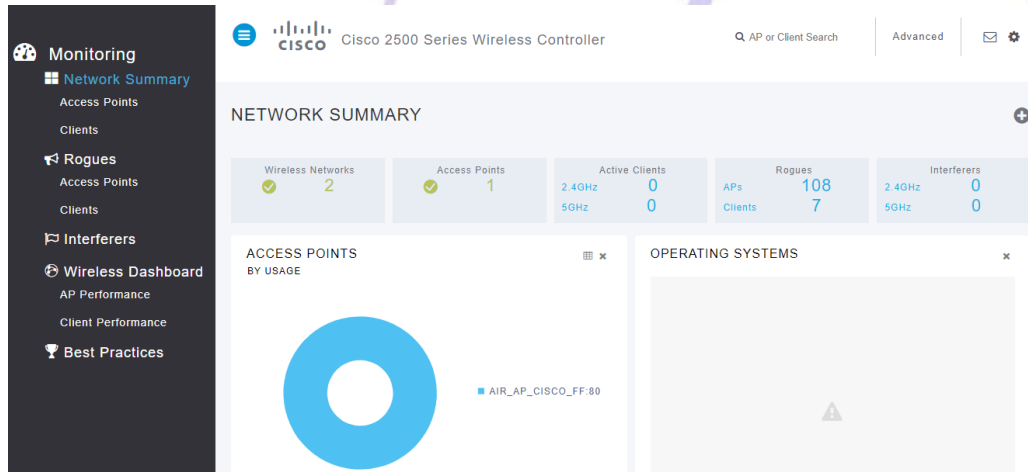
5- TOPOLOGÍA

TOPOLOGIA CASA BOLSA DE VALORES SERINGTEC

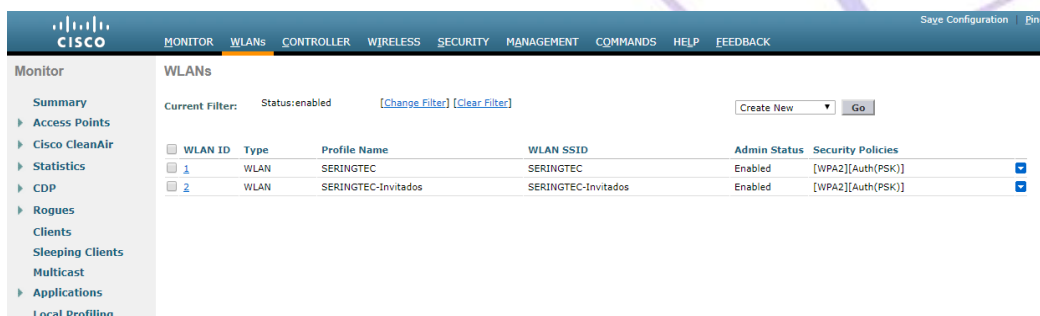


6- CONFIGURACIÓN WLAN

Cisco



SSID'S



WLANs

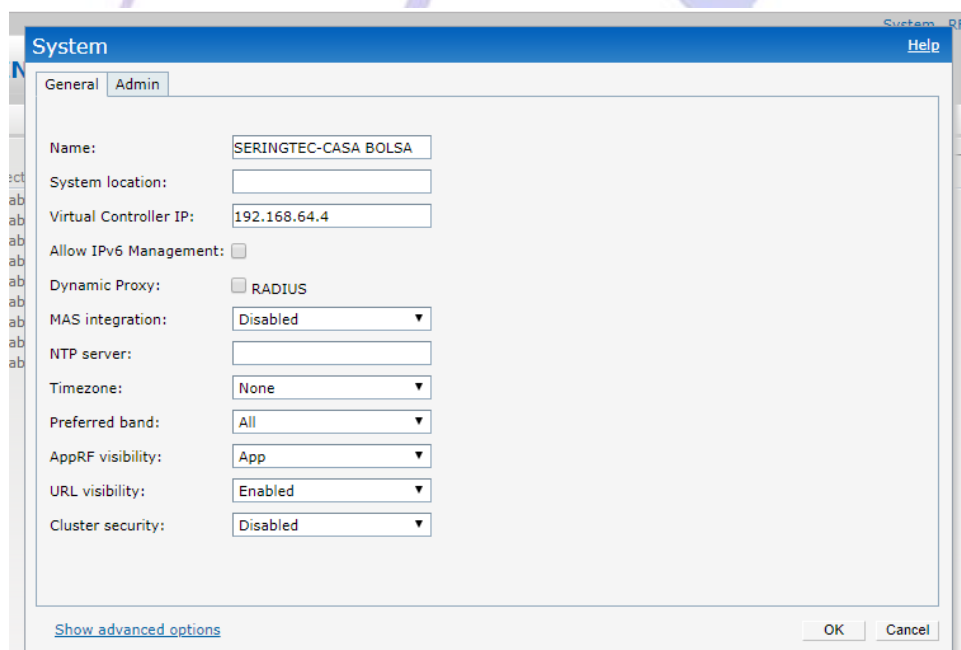
Current Filter: Status:enabled [\[Change Filter\]](#) [\[Clear Filter\]](#) [Create New](#) [Go](#)

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	SERINGTEC	SERINGTEC	Enabled	[WPA2][Auth(PSK)]
2	WLAN	SERINGTEC-Invitados	SERINGTEC-Invitados	Enabled	[WPA2][Auth(PSK)]

Inventario

MAC AP	REFERENCIA
d4:8c:b5:b0:30:de	AIR-LAP1041N-A-K9
d4:8c:b5:b0:30:8e	AIR-LAP1041N-A-K9
70:70:8b:b5:65:90	AIR-AP1815I-B-K9
70:70:8b:b5:5d:90	AIR-AP1815I-B-K9
70:70:8b:b5:59:88	AIR-AP1815I-B-K9
70:70:8b:b5:5d:68	AIR-AP1815I-B-K9
70:70:8b:b5:62:50	AIR-AP1815I-B-K9
70:7d:b9:cc:66:b8	AIR-AP1815I-B-K9
00:56:2b:53:c0:d0	AIR-AP1815I-B-K9

Aruba Networks



The screenshot shows the 'System' configuration window in the Aruba Networks management interface. The 'General' tab is selected, and the 'Name' field is set to 'SERINGTEC-CASA BOLSA'. Other fields include 'System location', 'Virtual Controller IP' (192.168.64.4), 'Allow IPv6 Management' (unchecked), 'Dynamic Proxy' (unchecked), 'MAS integration' (Disabled), 'NTP server', 'Timezone' (None), 'Preferred band' (All), 'AppRF visibility' (App), 'URL visibility' (Enabled), and 'Cluster security' (Disabled). The 'Show advanced options' link is visible at the bottom left, and 'OK' and 'Cancel' buttons are at the bottom right.

Maintenance [Help](#)

About Configuration Certificates Firmware Reboot Convert

a Hewlett Packard
Enterprise company

Name: Aruba Operating System Software
 Type: 305
 Build Time: 2017-10-19 18:44:44 PDT (build 61959) by p4build
 Version: 6.5.4.3
 Website: <http://www.arubanetworks.com>
 Legal: (c) Copyright 2017 Hewlett Packard Enterprise Development LP.
 Cloud Activation Key: CADCCCLL

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:
 (1) This device may not cause harmful interference.
 (2) This device must accept any interference received, including interference that may cause undesired operation.

FCC Info:
 105 FCC ID: Q9DAP105SDR
 92 FCC ID: Q9DAP9293SDR
 93 FCC ID: Q9DAP9293SDR
 175P FCC ID: Q9DAP175SDR
 175AC FCC ID: Q9DAP175SDR
 175DC FCC ID: Q9DAP175SDR

[Close](#)

RF [Help](#)

ARM

Band steering mode: Force 5Ghz ▼
 Airtime fairness mode: Preferred Access ▼
 Client match: Disabled ▼

[Show advanced options](#) [OK](#) [Cancel](#)

SSID'S

3 Networks									
Name	Clients	Type	Band	Authentication Method	Key Management	IP Assignment	Zone	Active	
SERINGTEC	187	Employee	All	None	WPA2-AES	Default VLAN	-	Yes	
SERINGTEC-Invitados	8	Employee	All	None	WPA2-AES	VLAN 9	-	Yes	
soporte	0	Employee	All	None	WPA2-AES	NAT Mode	-	Yes	edit x
New									

Inventario

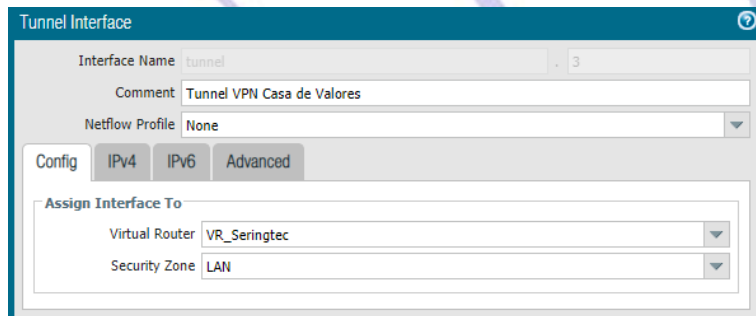
ALA_DERECHA_PI...	192.168.64.11	Access	Disabled	37	305(ind.. M
ALA_IZQUIERDA_...	192.168.64.13	Access	Disabled	35	305(ind.. M
AP_1_piso12	192.168.64.8	Access	Disabled	25	305(ind.. M
AP_2_piso12	192.168.64.6	Access	Disabled	32	305(ind.. M
AP_3_piso12	192.168.64.7	Access	Disabled	13	305(ind.. M
AP_4_piso12	192.168.64.5	Access	Disabled	12	305(ind.. M
AP_5_piso12	192.168.64.9	Access	Disabled	3	305(ind.. M
CAFETERIA_PISO_...	192.168.64.10	Access	Disabled	8	305(ind.. M
RECEPCION_PISO...	192.168.64.12	Access	Disabled	32	305(ind.. M

7- FIREWALL INFORME DE IMPLEMENTACIÓN.

Palo Alto Firewall

Crear Interface Tunnel

- Network > Interface > Tunnel



Tunnel Interface

Interface Name: tunnel

Comment: Tunnel VPN Casa de Valores

Netflow Profile: None

Config: IPv4 | IPv6 | Advanced

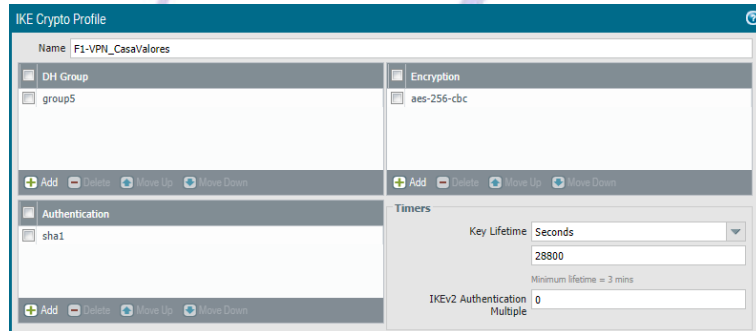
Assign Interface To:

Virtual Router: VR_Seringtec

Security Zone: LAN

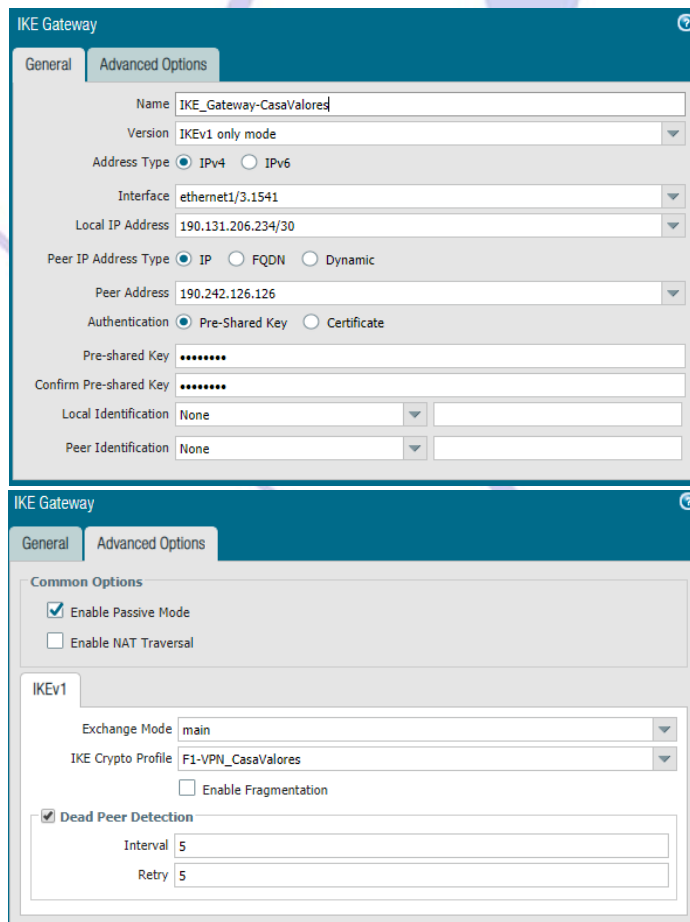
Configurar Gateway IKE - Fase 1 (Parámetros)

- Network > IKE Crypto > F1-VPN_CasaValores



The screenshot shows the 'IKE Crypto Profile' configuration window. The 'Name' field is 'F1-VPN_CasaValores'. Under 'DH Group', 'group5' is selected. Under 'Encryption', 'aes-256-cbc' is selected. Under 'Authentication', 'sha1' is selected. The 'Timers' section shows 'Key Lifetime' set to 'Seconds' with a value of '28800' and 'Minimum Lifetime' set to '3 mins'. 'IKEV2 Authentication' is set to 'Multiple'.

- Network > IKE Gateway > IKE_Gateway-CasaValores

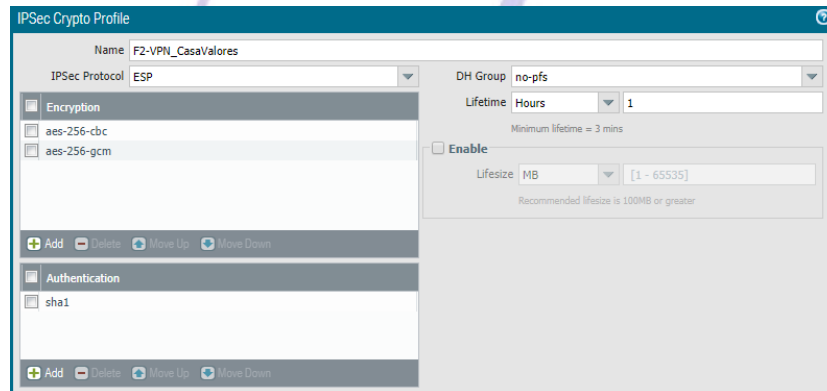


The first screenshot shows the 'General' tab of the 'IKE Gateway' configuration window. The 'Name' is 'IKE_Gateway-CasaValores'. The 'Version' is 'IKEv1 only mode'. The 'Address Type' is 'IPv4'. The 'Interface' is 'ethernet1/3.1541'. The 'Local IP Address' is '190.131.206.234/30'. The 'Peer IP Address Type' is 'IP'. The 'Peer Address' is '190.242.126.126'. The 'Authentication' is 'Pre-Shared Key'. The 'Pre-shared Key' and 'Confirm Pre-shared Key' fields are masked with dots. The 'Local Identification' and 'Peer Identification' are both set to 'None'.

The second screenshot shows the 'Advanced Options' tab of the same 'IKE Gateway' configuration window. Under 'Common Options', 'Enable Passive Mode' is checked and 'Enable NAT Traversal' is unchecked. Under 'IKEv1', the 'Exchange Mode' is 'main', the 'IKE Crypto Profile' is 'F1-VPN_CasaValores', and 'Enable Fragmentation' is unchecked. The 'Dead Peer Detection' section is checked, with 'Interval' and 'Retry' both set to '5'.

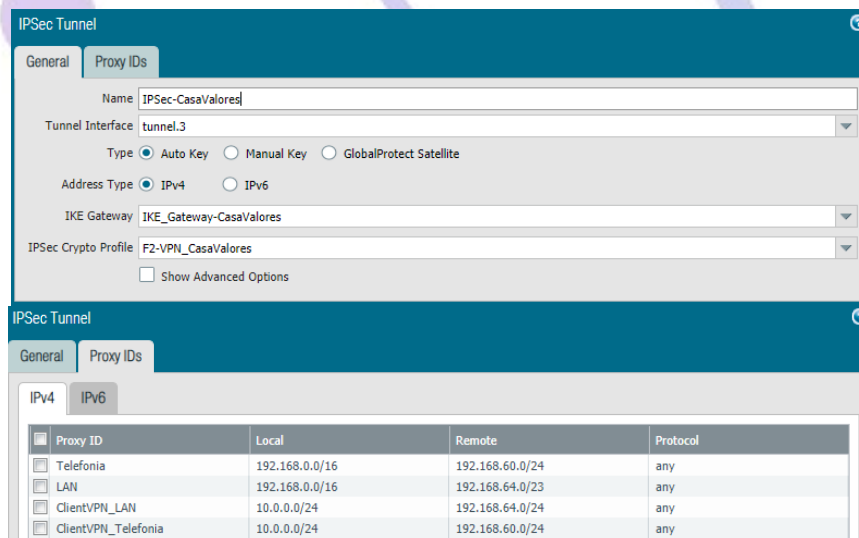
Configurar IPSec - Fase 2 (Parámetros)

- Network > IPSec Crypto



Configurar Tunnel IPSec VPN

- Network > IPSec Tunnel



Proxy ID	Local	Remote	Protocol
Telefonia	192.168.0.0/16	192.168.60.0/24	any
LAN	192.168.0.0/16	192.168.64.0/23	any
ClientVPN_LAN	10.0.0.0/24	192.168.64.0/24	any
ClientVPN_Telefonia	10.0.0.0/24	192.168.60.0/24	any

Crear Ruta para tráfico VPN

- Virtual Router (VR_Seringtec) > Static Routes > IPv4

Virtual Router - VR_Seringtec

Router Settings

Static Routes

Redistribution Profile

RIP

OSPF

OSPFv3

BGP

Multicast

IPv4 IPv6

6 items

Name	Destination	Interface	Type	Value	Admin Distance	Metric	Route Table
Default-ETB	0.0.0.0/0	ethernet1/1	ip-address	186.155.2...	default	50	unicast
Default_CWC	0.0.0.0/0	ethernet1...	ip-address	190.131.2...	default	10	unicast
Telefonia-Cucuta	192.168.41.0/24	tunnel.2			default	10	unicast
LAN-Cucuta	192.168.40.0/24	tunnel.2			default	10	unicast
Telefonia-CasaValores	192.168.60.0/24	tunnel.3			default	10	unicast
LAN-CasaValores	192.168.64.0/23	tunnel.3			default	10	unicast

Add Delete Clone

Sophos XG Firewall

Crear Política VPN IPSec para Fase 1 y Fase 2

- Configure > VPN > IPSec policies (Seringtec)

General settings

Name: Seringtec

Description: Description

Key exchange: ☒ IKEv1 ☐ IKEv2

Authentication mode: ☒ Main mode ☐ Aggressive mode

Aggressive mode is insecure

Key negotiation tries: 3

Re-key connection: ☒

Pass data in compressed format: ☐

SHA2 with 96-bit truncation: ☐

Phase 1

Key life: 28800 Seconds

Re-key margin: 120 Seconds

Randomize re-keying margin by: 0 %

DH group (key group): 2 selected

Encryption: AES256

Authentication: SHA1

You can add up to 3 different algorithm combinations

Phase 2

PFS group (DH group) None ⚠ Key life 3600 Seconds

Encryption AES256 ⚙ Authentication SHA1 ⚠

+ You can add up to 3 different algorithm combinations

Dead Peer Detection

☒ Dead Peer Detection

Check peer after every 5 Seconds Wait for response up to 5 Seconds When peer unreachable Re-initiate ⚙

Configurar IPSec Connection

- Configure > VPN > IPSec policies (IPSecSeringtec)

General settings

Name IPSecSeringtec ⚙ IP version IPv4 IPv6 ⚙ ☐ Activate on save ☐ Create firewall rule

Description Description ⚙ Connection type Site-to-site ⚙

Gateway type Initiate the connection ⚙

Encryption

Policy Seringtec ⚙ Authentication type Preshared key ⚙

[Change preshared key](#)

Gateway settings

Local gateway

Listening interface Port2 - 190.242.126.126 ⚙

Local ID type Select local ID ⚙

Local ID ⚙

Local subnet Telefonia ⚙ ⚙ LAN ⚙ ⚙ Add new item

☐ Network Address Translation (NAT)

Remote gateway

Gateway address 190.131.206.234 ⚙

Remote ID type Select remote ID ⚙

Remote ID ⚙

Remote subnet Seringtec ⚙ ⚙ VPNSeringtec ⚙ ⚙ Add new item

Activar IPSec Connection

- Configure > VPN > IPSec Connections (Status - Active – Connections)

IPsec connections

Show additional properties

Add Delete Wizard

Name	Group name	Policy	Connection type	Status	Active	Connection	Manage
IPSecSeringtec	-	Seringtec	Site-to-site	●	●	1	

Crear LAN-VPN Reglas de Firewall

- PROTECT > Firewall

Firewall

How-to guides Log viewer Help admin

IPv4 IPv6 Enable filter Add firewall rule

ID	Name	Source	Destination	What	Action	Features
2	Valores-Seringtec	LAN, TELEFONIA, Any host	VPN, Any host	Any service	Accept	
9	Permit_Destiny_Hos...	LAN, WIFI, Any host	WAN, FQDN_Permit	Any service	Accept	
5	Network_Policy_WIE...	WIFI, Any host	WAN, Any host	Any service	Accept	
6	Internet_Full	LAN, POLICE_SIN_RES TRICION	WAN, Any host	Any service	Accept	
7	Internet_IT	LAN, POLICE_INTERNE T_TI	WAN, Any host	Any service	Accept	
8	Internet_Youtube	LAN, POLICE_YOUTUB E	WAN, Any host	Any service	Accept	
1	Internet_General	LAN, Any host	WAN, Any host	Any service	Accept	
3	Seringtec-Valores	VPN, Any host	LAN, TELEFONIA, Any host	Any service	Accept	

Configurar interfaces de red para LAN, WAN, WiFi Visitantes y Telefonía















- CONFIGURE > Network > Interfaces

Network

How-to guides Log viewer Help admin

Interfaces Zones WAN link manager DNS DHCP IPv6 router advertisement Cellular WAN IP tunnels Neighbors (ARP-NDP) Dynamic DNS

Interface	Status/Interface speed	IP address	Misc
GuestAP DMZ Wireless protection	Unplugged Auto-negotiated	10.255.0.1/255.255.255.0 Static	
Port1 LAN Physical	Connected 1000 Mbps - Full Duplex Auto-negotiated	192.168.64.1/255.255.254.0 Static	
Port10 Unbound Physical	Disabled Auto-negotiated	N/A	
Port11 Unbound Physical	Disabled Auto-negotiated	N/A	
Port12 Unbound Physical	Disabled Auto-negotiated	N/A	
Port2 WAN Physical	Connected 1000 Mbps - Full Duplex Auto-negotiated	190.242.126.126/255.255.255.252 Static	

 Port3 Unbound Physical	Disabled Auto-negotiated	N/A	
 Port4 Unbound Physical	Disabled Auto-negotiated	N/A	
 Port5 WiFi Physical	Connected 1000 Mbps - Full Duplex Auto-negotiated	192.168.62.1/255.255.255.0 Static	
 Port6 TELEFONIA Physical	Connected 1000 Mbps - Full Duplex Auto-negotiated	192.168.60.1/255.255.255.0 Static	
 Port7 Unbound Physical	Disabled Auto-negotiated	N/A	
 Port8 Unbound Physical	Disabled Auto-negotiated	N/A	
 Port9 Unbound Physical	Disabled Auto-negotiated	N/A	







Configurar zonas de tráfico común para las reglas de Firewall (LAN, WAN, VPN, WiFi Visitantes y Telefonía)

- CONFIGURE > Network > Zones

Network How-to guides Log viewer Help admin Serratec S.A.S.

Interfaces **Zones** WAN link manager DNS DHCP IPv6 router advertisement Cellular WAN IP tunnels Neighbors (ARP-NDP) Dynamic DNS

☐ ☐ Add Delete

<input type="checkbox"/>	Name	Members	Type	Device access	Description	Manage
<input type="checkbox"/>	LAN	Port1	LAN	Ping/Ping6, HTTPS, SSH		
<input type="checkbox"/>	WAN	Port2	WAN	SSL VPN, User Portal		
<input type="checkbox"/>	DMZ	GuestAP	DMZ	HTTPS, SSH		
<input type="checkbox"/>	LOCAL		LOCAL			
<input type="checkbox"/>	VPN		VPN	Ping/Ping6, HTTPS, SSH		
<input type="checkbox"/>	WiFi	Port5	LAN	Ping/Ping6, HTTPS, SSH		
<input type="checkbox"/>	TELEFONIA	Port6	LAN	Ping/Ping6, HTTPS, SSH		 

Configurar servicio de DHCP para zonas de Telefonía, LAN y WiFi Visitantes

- CONFIGURE > Network > DHCP

Network How-to guides Log viewer Help admin ▾
Seringtec S.A.S.

Interfaces Zones WAN link manager DNS **DHCP** IPv6 router advertisement Cellular WAN IP tunnels Neighbors [ARP-NDP] Dynamic DNS

Server

Add Delete

<input type="checkbox"/>	Name	Interface	Lease detail Dynamic	Static	IP version ▾	Status	Manage
<input type="checkbox"/>	<u>DHCP-TELEFONIA</u>	Port6 - 192.168.60.1	192.168.60.50 - 192.168.60.200	-	IPv4	On	
<input type="checkbox"/>	<u>DHCP-LAN</u>	Port1 - 192.168.64.1	192.168.64.50 - 192.168.65.250	View detail	IPv4	On	
<input type="checkbox"/>	<u>DHCP-GUEST</u>	Port5 - 192.168.62.1	192.168.62.10 - 192.168.62.254	-	IPv4	On	

Configurar perfil de Traffic Shapping para limitar BW sobre la red de WiFi de Visitantes

- CONFIGURE > System services > Traffic Shapping (Limit-WiFi Visitantes)

System services How-to guides Log viewer Help admin ▾
Seringtec S.A.S.

High availability Traffic shaping settings **RED** Malware protection Log settings Data anonymization **Traffic shaping** Services

Edit traffic shaping (QoS) policy

Name *

Policy association ☐ Users ☒ Rules ☐ Web categories ☐ Applications

Rule type ☒ Limit ☐ Guarantee

Limit upload/download separately ☒ Disable ☐ Enable

Priority *

Limit * KB/s [2 - 2560000]

Bandwidth usage type ☐ Individual ☒ Shared

Description

Configurar perfiles de control de aplicaciones para los perfiles de usuarios Generales y Youtube.

- PROTECT > Applications > Application filter (Block APP General y Block APP Youtube)

Applications How-to guides Log viewer Help admin Seringtec S.A.S.

Application filter	Synchronized Application Control	Cloud applications	Application list	Traffic shaping default
<input type="checkbox"/> Block filter avoidance apps	Allow		Drops traffic from applications that tunnels other apps, proxy and tunnel apps, and from apps that can bypass firewall policy. These applications allow users to anonymously browse Internet by connecting to servers on the Internet via encrypted SSL tunnels. This, in turn, enables users to bypass network security measures.	
<input type="checkbox"/> Block generally unwanted apps	Allow		Drops generally unwanted applications traffic. This includes file transfer apps, proxy & tunnel apps, risk prone apps, peer to peer networking (P2P) apps and apps that causes loss of productivity.	
<input type="checkbox"/> Block high risk (Risk Level 4 and 5) apps	Allow		Drops traffic that are classified under high risk apps (Risk Level- 4 and 5).	
<input type="checkbox"/> Block peer to peer (P2P) networking apps	Allow		Drops traffic from applications that are categorized as P2P apps. P2P could be a mechanism for distributing Bots, Spywares, Adware, Trojans, Rootkits, Worms and other types of malwares. It is generally advised to have P2P application blocked in your network.	
<input type="checkbox"/> Block very high risk (Risk Level 5) apps	Allow		Drops traffic that are classified under very high risk apps (Risk Level- 5).	
<input type="checkbox"/> Block_APP_General	Allow			
<input type="checkbox"/> Block_APP_YouTube	Allow			
<input type="checkbox"/> Deny All	Deny		Deny All Policy.	

Configurar perfiles de filtrado Web (Full, IT, Youtube y General)

- PROTECT > Web > Policies/User activities

Web How-to guides Log viewer Help admin Seringtec S.A.S.

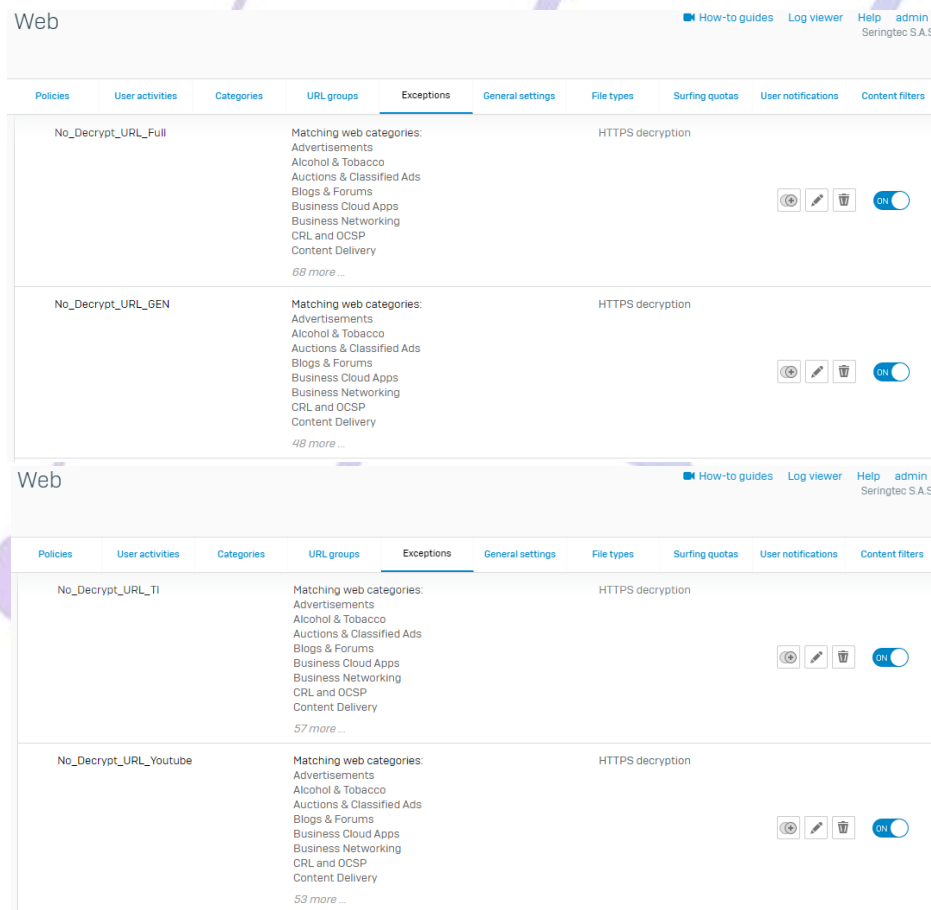
Policies	User activities	Categories	URL groups	Exceptions	General settings	File types	Surfing quotas	User notifications	Content filters
No Web Mail		Deny access to web mail sites					0		
No Web Mail or Chat		Deny access to web mail and online chat sites					0		
No web uploads		Restrict users from uploading content to any site					0		
Policy_Web_Full							2		
Policy_Web_General							1		
Policy_Web_IT							1		
Policy_Web_YouTube							1		

Web How-to guides Log viewer Help admin Seringtec S.A.S.

Policies	User activities	Categories	URL groups	Exceptions	General settings	File types	Surfing quotas	User notifications	Content filters
Name		Contains							
Bandwidth-heavy Browsing		Download Freeware & Shareware, Live audio, Live video, Peer-to-peer & torrents, Radio & A...							
Block_URL_Full		Anonymizers, Command & Control, Controlled substances, Criminal Activity, Dynamic DNS...							
Block_URL_General		Anonymizers, Command & Control, Controlled substances, Criminal Activity, Dynamic DNS...							
Block_URL_IT		Anonymizers, Command & Control, Controlled substances, Criminal Activity, Dynamic DNS...							
Block_URL_YouTube		Anonymizers, Command & Control, Controlled substances, Criminal Activity, Dynamic DNS...							
Community, Education and Religion		Educational Institutions, General Business, Government, NGOs & Non-Profits, Political Org...							

Configurar exclusiones para inspección de tráfico Web encriptado (Full, IT, Youtube y General)

- PROTECT > Web > Exceptions



The screenshot displays the 'Web' configuration page in the PROTECT console, specifically the 'Exceptions' tab. The page shows a list of exceptions that have been configured for web traffic inspection. Two exceptions are visible:

- No_Decrypt_URL_Full**: This exception is configured for 'HTTPS decryption'. It lists matching web categories: Advertisements, Alcohol & Tobacco, Auctions & Classified Ads, Blogs & Forums, Business Cloud Apps, Business Networking, CRL and OCSP, and Content Delivery. The exception is currently enabled (toggle switch is on).
- No_Decrypt_URL_GEN**: This exception is also configured for 'HTTPS decryption'. It lists the same matching web categories as the first exception. It is also currently enabled.

Each exception entry includes a list of matching web categories and a toggle switch to enable or disable the exception. The interface also includes navigation tabs for Policies, User activities, Categories, URL groups, Exceptions, General settings, File types, Surfing quotas, User notifications, and Content filters.

Configurar Settings generales para la configuración del escaneo de contenido-malware sobre tráfico Web y y escaneo y descripción de tráfico HTTPS

- PROTECT > Web > General settings

Web How-to guides Log viewer Help admin Seringtec S.A.S.

[Policies](#) [User activities](#) [Categories](#) [URL groups](#) [Exceptions](#) [General settings](#) [File types](#) [Surfing quotas](#) [User notifications](#) [Content filters](#)

XG Firewall protects you by scanning HTTP and HTTPS traffic for unwanted content or malware. Use this page to modify protection settings, as well as settings for the proxy and web cache.

Protection

Malware and content scanning

Scan engine selection: Scanning mode: ☐ Block potentially unwanted applications

Single scan engine is set to [Sophos](#).
Sandstorm and content filters require use of the Sophos engine, either as the single scan engine or in dual engine mode.

Action on malware scan failure: Do not scan files larger than: MB

Files that cannot be fully scanned because they are encrypted or corrupted may contain undetected threats.

Authorized PUAs:

[Advanced settings](#)

[Policies](#) [User activities](#) [Categories](#) [URL groups](#) [Exceptions](#) [General settings](#) [File types](#) [Surfing quotas](#) [User notifications](#) [Content filters](#)

Search engine enforcement

Can now be configured per policy. Go to Web > Policies and edit a policy to configure search engine enforcement.

HTTPS decryption and scanning

HTTPS scanning certificate authority (CA):
The scanning CA is used to secure scanned HTTPS connections.

☒ Block unrecognized SSL protocols
Stop traffic that avoids HTTPS scanning by using invalid SSL protocols.

☒ Block invalid certificates
Ensure HTTPS traffic is secure by connecting only to sites with a valid certificate.

For errors and block/warn policy actions on HTTPS connections when Decrypt & Scan is disabled:

- ☒ Display user notifications
Browsers may show certificate warnings if the HTTPS CA is not installed.
- ☐ Drop connections without a user notification
Browsers may show connection failure messages.

Configurar exclusiones para inspección de tráfico Web encriptado (Full, IT, Youtube y General)

- PROTECT > Intrusion prevention > IPS policies (LAN TO WAN)

Intrusion prevention

How-to guides Log viewer Help admin 
Seringtec S.A.S.

DoS attacks
IPS policies
Custom IPS signatures
DoS & spoof protection

Name *
Description

A default IPS policy template to scan the traffic flowing from LAN to WAN, primarily intended to secure LAN-based clients

Save
Cancel

Name	Signatures	Signature filter criteria	Action
Browsers_Officetools_Multi... and Instant Messaging	All	Category = browser-ie, browser-... Severity = All Severity Platform = All Platform Target = Client	Recommended
Operating System and Services	All	Category = os-windows, indicato... Severity = All Severity Platform = All Platform Target = Client	Recommended
ERP System	All	Category = misc Severity = All Severity Platform = All Platform Target = All Target	Recommended
Industrial Control System	All	Category = protocol-scada, brow... Severity = All Severity Platform = All Platform Target = All Target	Recommended
Malware communication	All	Category = malware-cnc, exploit... Severity = All Severity Platform = All Platform Target = Client	Recommended
Reconnaissance	All	Category = scan Severity = All Severity Platform = All Platform Target = Client	Recommended
All windows clients	All	Category = All categories Severity = All Severity Platform = Windows Target = Client	Recommended
All Linux clients	All	Category = All categories Severity = All Severity Platform = Linux Target = Client	Recommended
All Clients	All	Category = All categories Severity = All Severity Platform = All Platform Target = Client	Recommended

Configurar reglas de Firewall para permitir el tráfico desde la red Interna hacia Internet para los distintos tipos de perfiles de usuarios (Full, IT, Youtube, WiFi Visitantes y General). En cada regla se asocian los perfiles de seguridad para el control Web, de Aplicaciones, de Prevención de Intrusos, y de Traffic Shaping. Además de los correspondientes NAT para poder salir a navegar a Internet.

- PROTECT > Firewall

Firewall


How-to guides Log viewer Help admin
 Seringtec S.A.S.

IPv4 IPv6 Enable filter + Add firewall rule


ID	Name	Source	Destination	What	Action	Features
2	Valores-Seringtec in 6.77 GB, out 1.26 GB	LAN, TELEFONIA, Any host	VPN, Any host	Any service	Accept	AV WEB APP QoS HB RT NAT LOG IPS
9	Permit_Destiny_Hos... in 5.27 MB, out 220.00 KB	LAN, WiFi, Any host	WAN, FQDN_Permit	Any service	Accept	AV WEB APP QoS HB RT NAT LOG IPS
5	Network_Policy_WIF... in 6.27 GB, out 697.28 MB	WiFi, Any host	WAN, Any host	Any service	Accept	AV WEB APP QoS HB RT NAT LOG IPS
6	Internet_Full in 5.13 GB, out 1.05 GB	LAN, POLICE_SIN_RES TRICCION	WAN, Any host	Any service	Accept	AV WEB APP QoS HB RT NAT LOG IPS
7	Internet_IT in 3.71 GB, out 150.98 MB	LAN, POLICE_INTERNE T_TI	WAN, Any host	Any service	Accept	AV WEB APP QoS HB RT NAT LOG IPS
8	Internet_YouTube in 3.34 GB, out 437.59 MB	LAN, POLICE_YOUTUB E	WAN, Any host	Any service	Accept	AV WEB APP QoS HB RT NAT LOG IPS
1	Internet_General in 162.34 GB, out 97.75 GB	LAN, Any host	WAN, Any host	Any service	Accept	AV WEB APP QoS HB RT NAT LOG IPS
3	Seringtec-Valores in 161.14 MB, out 159.80 MB	VPN, Any host	LAN, TELEFONIA, Any host	Any service	Accept	AV WEB APP QoS HB RT NAT LOG IPS

8- ACCESOS.


ARUBA

Title: Icon: 


User name:


Password: 

CONTROLLER CISCO


Title: Icon: 

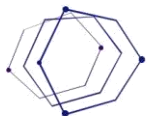
User name:

Password: 

Title: Icon: 

User name:

Password: 



SOFTMAT
Services SAS

NIT 901111352-2

SOPHOS XG 330

Title: Icon: 

User name:


Password: 

Title: Icon: 

User name:

Password: 

PRESHARE KEY VPN SITE TO SITE 106 – CASA DE BOLSA

Title: Icon: 

User name:

Password: 