



Configuring RADIUS and Remote Authentication Servers using FortiAuthenticator and BuyPass Code

Shanaz Khan SE Fortinet Norway

Topology

FortiAuthenticator configured as a RADIUS server and connected to LDAP and FortiGate.



Figure 1 Sample topology

The configuration discussed in this document was tested with the following setup for users, groups, and, memberships:

Group	Member	Resource
IT	dollyduck	Esxi Server (10.188.10.10)
HR	donaldduck	FAZ (10.188.2.5)
Marketing	mickeymouse	FML (10.188.100.10)

Table 1 Users' access to resources

Software versions

The configuration discussed in this document was tested with the following firmware versions:

- FortiAuthenticator GA 6.0.1
- FortiGate 6.2.0
- Windows Server 2016
- Windows 10
- BuyPass Code Service Connector
- BuyPass Code token App for mobile phone

Prerequisites

This documentation is based on BuyPass Service Connector already installed on MS LDAP server as well as the necessary users and groups defined in customer's AD domain structure.

FortiAuthenticator basic setup

1) Configure IP and DNS on the FortiAuthenticator

Configure Remote Auth. Servers (LDAP)

- 1) Go to Authentication -> Remote Authentication Servers -> LDAP and select Create New
- 2) Enter the remote LDAP server information

and some	24								
ystem	,	Edit LDAP Server							
Unentication	~	Name:	Prilab_server						
User Account Policies	,	Primary server name/IP:	10.188.2.15	Port:	389				
Oser Management	``	 Use secondary server 							
Guest Portals	,	Base distinguished name:	OU=Disney,DC=prilab,DC=no						
Remote Auth Servers	,	Bind type:	Simple Regular						
General		Username:	prilab\Administrator Password:		•••••				
LDAP		• Add supported domain names (used only if this is not a Windows Activ	e Directory server)					
RADIUS		Ouery Elements							
OAUTH SAMI		Pre-defined templates:	Please select a template 🔻	Apply					
RADIUS Service	,	User object class:	person						
LDAP Service	>	Username attribute:	sAMAccountName						
Soluth Service	>	Group object class:	group						
SAML IdP	>	Obtain group memberships from:	User attribute Group attrib	oute					
FAC Agent	>	Group membership attribute:	memberOf						
ortinet SSO Methods	>	• Force use of administrator acco	unt for group membership lookups						
Ionitor	>	Secure Connection							
ertificate Management	>	• Enable							
ogging	>	Windows Active Directory Domain	Authentication						
		C Enable							
		Remote LDAP Users							
		Username			Token	Actions			
		sa-bpcode-t				2 H			
		sa-bpcode				2 H			
		nassenøff				2.8			
		mickeymouse				2.8			
		Increymouse donalddark							

3) You should able to see the LDAP users replicated under Remote Users

System	> Import	🛆 Export Users 📋 Delete 🖉 Edit 🖉 Re-Enable			Search for remote L	DAP users T	LDAP users RADIUS users SAML u	
Authentication	Ť 🛛	Username	Remote LDAP server	Admin	Status	Token	Token Requested	
User Management		donaldduck	Prilab_server (10.188.2.15)	0	0		0	
Local Users Remote Users Remote User Sync Rules Social Login Users Guest Users	0	mickeymouse	Prilab_server (10.188.2.15)	0	0		0	
		nassenøff	Prilab_server (10.188.2.15)	•	0		0	
		sa-bpcode	Prilab_server (10.188.2.15)	•	0		0	
		sa-bpcode-t	Prilab_server (10.188.2.15)	•	0		0	

Create User Group

- 1) Go to User Management -> User Groups -> Create New
- 2) Select Type Remote LDAP
- 3) User retrieval: Specify an LDAP filter
- 4) Remote LDAP: Select a remote LDAP server
- 5) LDAP filter: specify a filter and Test Filter to verify the correct user(s) in the group
- 6) Radius Attributes -> Add Attribute. Vendor: Fortinet, Attribute ID: Fortinet-Group-Name.
 Value: HR (repeat the above steps for the all necessary groups, in this case HR, IT, Marketing SSLVPN)

FortiAuthenticator v6.0	0-Ь	uild0034 FAC-VMTM180030	172				Le
System	>	Edit User Group					
Authentication	~	Name	110				
& User Account Policies	>	ivame.	PIR Local				
🐸 User Management	*	Туре:	Remote LDAP				
Local Users			Remote RADIUS				
Remote Users			Remote SAML MAC				
Remote User Sync Rules			© Creatify on LDAD 6hor				
Social Login Users		User retrieval:	 Sector an LDAP niter Set a list of imported remote LDAP users 				
Guest Users							
User Groups		Remote LDAP:	Prilab_server (10.188.2.15) *				
Usage Profile		LDAP filter:	(memberOf=cn=HR,ou=Disney,dc=prilab,dc=no)		Test Filter		
Realms		Usage Profile	[Please Select] 🔻				
FortiTokens		RADIUS Attributes					
MAC Devices		Attribute		Value		Vendor	Actions
Self-service Portal	>	Fortinet-Group-Name		HR		Fortinet	/ 8
🔹 Guest Portals	>	Add Attribute					
Remote Auth. Servers	>						
RADIUS Service	>				OK Cancel		

Note – the Value for this attribute (HR in the above example) is the attribute sent with every user member of the LDAP group specified, and this is what FortiGate uses to match users against its local group.

A Ikke sikker https://10.	188.2.8/ldap/browser-filter/?_po	oup=1&remote_ld	ap=1&filter=(memberOf%3Dcr	%3DHR%2Cou%3DI	
Test LDAP Filter					
LDAP server:	10.188.2.15:389				
Filter:	(memberOf=cn=HR,ou=Disney,dc=prilab,dc=no)				
	Арріу	Clear			
Filter child nodes an	d show number of children				
🗀 CN=Donald Duck					
Organization:	[Please Select] 🔻				
		Use Filter	Cancel		

FortiAuthenticator v6.00-build0034 FAC-VMTM18003072								
System	>	Create New Clit Delete						
Authentication	~		Name	Туре	Remote server			
User Account Policies	>							
😁 User Management			HR	Remote LDAP	LDAP: Prilab_server (10.188.2.15)			
Local Users			т	Remote LDAP	LDAP: Prilab_server (10.188.2.15)			
Remote Users			Marketing	Remote LDAP	LDAP: Prilab_server (10.188.2.15)			
Remote User Sync Rules			SSLVPN	Remote LDAP	LDAP: Prilab_server (10.188.2.15)			
Social Login Users Guest Users		4 user groups						

Remote Authentication Servers

- 1) Go to Remote Auth. Servers -> RADIUS -> Create New
- 2) Give it a suitable new, in this sample configuration we'll call it BuyPass_TokenServer
- 3) **Preferred auth. method**: select appropriate method (must be same as in RADIUS configuration on Fortigate)
- 4) **Servername/IP**: IP address of the server where the BuyPass Code Service Connector is running (in this sample configuration, BPSC is running on the Domain Controller)
- 5) Port: 1812, Secret: must be same as in RADIUS configuration on Fortigate)

FortiAuthenticator v6.00-build0034 FAC-VMTM18003072							
System	>	Edit RADIUS Server					
Authentication User Account Policies User Management Self-service Portal	* * *	Name: Preferred auth. method: Timeout:	Buypass_TokenServer PAP				
General	~	Secret:	10.188.2.15	Port:	1812		
RADIUS OAUTH SAML		Secondary Server (Optional Redu User Migration	ndancy)				
RADIUS ServiceLDAP Service	> >				OK Cancel		

Realms

- 1) Go to Authentication -> User Management -> Realms -> Create New
- 2) Create a new realm pointing to your LDAP server.
- 3) Chained token authentication with remote RADIUS server: select the RADIUS server created in previous step (Remote Auth.Servers)

FortiAuthenticator v6	.00-bı	uild0034 FAC-VMTM18003072
System	>	Edit Realm
Authentication	~	Manual II. II.
晶 User Account Policies	>	Name: Idap-radius
😁 User Management	~	User source: Prilab_server (10.188.2.15)
Local Users		C Chained token authentication with remote RADIUS server Buypass_TokenServer (10.188.2.15)
Remote Users		Only for members of these LDAP groups
Remote User Sync Rules		
Social Login Users		OK Cancel
Guest Users		
User Groups		
Usage Profile		
Organizations		
Realms		

Configuring RADIUS client

- 1) Go to Authentication -> RADIUS Services -> Clients
- 2) **Client name/IP**: the IP address of the FortiGate
- 3) Secret: The RADIUS passphrase that the FortiGate unit will use

Neuros cuent ne: For nt address: in	r IP/Hostname © Subnet © R IB821 C Accept guest portal requests fro for usage enforcement for Frofile name: Description: C Apply this profile based on R EAP types: Description: C Modewatcaston Description: Description: C Modewatcaston Description:	Range mr related Ac Default IADIUS attrib P P P P P P	cess Points utes. APGTC APFTLS EAP APFTLS				
ne: por rt address: int st portal: Accept RADIUS acounting message Support RADIUS Disconnect message Podes uit x New Profile	e IP/Hostname Subnet R I IP/Hostname i IP/Hostname Subnet R I I I I I I I I I I I I I I I I I I	Range mrrelated Ac Default ADIUS attrib O P O P	cess Points utes. AP-GTC AP-GTC AP-TLS AP-TLS AP-TLS				
nt address: 10. ret: 10. set portal: Accept RADIUS accounting message Support RADIUS Disconnect message Number Profile	IP/Hostname Subnet R IP/Hostname Subnet IP/Hostname Accept guest portal requests from Accept guest portal requests from s for usage enforcement ess Profile name: Description: Apply this profile based on R EAP types:	Default Default MADIUS attrib O E O E	cess Points utes. AP-GTC AP-TLS EEAP AP-TLS				
101 ext. 101	18821 Accept guest portal requests from for usage enforcement fees Profile name: Description: Apply this profile based on R EAP types: Description:	Default Default MADIUS attrib C E C P C E	cess Points utes. APGTC APFTLS EAP APFTLS				
ret:	Accept guest portal requests from s for usage enforcement ges Profile name: Description: Apply this profile based on Re EAP types: Description: Des	Default Default ADIUS attrib E E E E E E	cess Points utes. AP-GTC AP-TLS EAP AP-TLS EAP AP-TTLS				
st portal: Accept RADIUS accounting message Support RADIUS Disconnect message Indiana Unit X New Profile	Accept guest portal requests from s for usage enforcement. es Profile name: Description: Apply this profile based on R EAP types: Desca Addresidation Description: Descriptio	Default Default ADIUS attrib	utes. AP-GTC AP-TLS EAP AP-TLS EAP AP-TLS				
es poliair. Support RADIUS accounting message Support RADIUS Disconnect message Indéa Uit X New Profile	s for usage enforcement es Profile name: Description: Apply this profile based on R EAP types: Deute Authentication	Default ADIUS attrib E E E E E E E E E E	utes. AP-GTC AP-TLS EEAP AP-TLS				
Accept RADIUS accounting message support RADIUS Disconnect message publics https://www.polifie New Profile	s for usage enforcement jes Profile name: Description: Apply this profile based on Ri EAP types: Deute Authentication Of 100 Education to Description	Default tADIUS attrib E O P O E	utes. AP-GTC AP-TLS EAP AP-TTLS				
Putiles Putiles uit X New Profile	Profile name: Description:	Default ADIUS attrib DE DE DE DE DE DE DE DE DE DE AUTOR	utes. AP-GTC AP-TLS EAP AP-TTLS				
Proties ult X New Profile	Profile name: Description:	Default ADIUS attrib	utes. AP-GTC AP-TLS E&P AP-TTLS				
ult x	Description: Apply this profile based on R EAP types: Device Authentication	ADIUS attrib	utes. IAP-GTC JAP-TLS F&P JAP-TTLS				
New Profile	Apply this profile based on Ri EAP types: Device Authentication	ADIUS attrib	utes. IAP-GTC IAP-TLS IEAP IAP-TTLS				
New Profile	EAP types: Device Authentication		AP-GTC AP-TLS ÆAP AP-TTLS				
	Device Authentication		AP-TLS PEAP AP-TTLS				
	Device Authentication	O F	AP-TTLS				
	Device Authentication						
	I Delant And Delant Line of the Property Sector	(MAR)					
	AD machine authentication	(
	MAC device filtering						
	User Authentication						
	Authentication method:	 Enf App Pas For 	orce two-factor authentication bly two-factor authentication if available (auth sword-only authentication (exclude users with tToken-only authentication (exclude users wit	enticate any user) out a password) hout a FortiToken)			
	Enable Token Mobile push no	otifications au	uthentication				
	Username input format:	 use real real 	rname@realm lm\username lm/username				
	Realms:	Default	Realm	Allow local users to override remote users	Use Windows AD domain authentication	Groups 🛛	Delete
		٠	Idap-radius Prilab server (10.188.2.15)	٩	0	C Filter: HR. IT. Marketing. SSLVPN (Edit) C Filter local users: (Edit)	0
		Add a re	alm				
les will be applied in top-to-bottom order d on matching RADIUS attributes. If the lie has no attributes to match, that profile always be applied before any beneath it.				Save			
ile de alv	s will be applied in top-to-dottom order on matching RADUS attributes. If the have no attributes to match, that profile any be applied before any beneath II.	Viername input format: Realms: will be applied in task-to Rection order on must here RRADUS attributes. If the part of the RADUS attributes at the Real may be applied for the RADUS attributes.	will be applied in top-to-bettom order on read top: ADUS attributes, 11 bettom of the provide applied in top-to-bettom order on read top: ADUS attributes, 11 bettom of the provide applied in top-to-bettom order on read top: ADUS attributes, 11 bettom of the provide applied in top-to-bettom order on read top: ADUS attributes, 11 bettom of the provide applied in top-to-bettom order on read top: ADUS attributes, 11 bettom of the provide applied in top-to-bettom order on read top: ADUS attributes, 11 bettom of the provide applied in top-to-bettom order on read top: ADUS attributes, 11 bettom of the provide applied in top-to-bettom order on read top: ADUS attributes, 11 bettom of the provide applied in top-to-bettom order on read top-top-top-top-top-top-top-top-top-top-	Username input format: e username@realm e realm/username e real	will be upded in top-to-bottom order on multiple ADUS stributes. If the har no attribute shows that produces and the stribute shows that produces and the shows that produces and t	Vesmane input format:	Viername input format: * username@realm 0 realm/username Realms: * with De agglied in top-to-doction or der or with the agglied in top-to-doction or der * with De agglied in top-to-doction or

- 4) Keep **Default** profile. **User Authentication** -> **Authentication method**: *Apply two-factor authentication if available (authenticate any user)*
- 5) Realms
 - I. Select the remote realm we created in **Realms**

- II. Groups: enable filter and select the local group(s) we created in User Groups (<u>no need</u> to enable Allow local users to override remote users + Use Windows AD domain authentication)
- III. Groups: enable filter and select the local group we created in User Groups. Save -> OK



Configure the FortiGate for RADIUS authentication

• Go to User & Device -> RADIUS Servers and select Create New

- **Name**: the FortiAuthenticator, in this case called FAC. Specify Authentication method and IP address of the FortiAuthenticator (FAC).
- Secret: same passphrase as specified for RADIUS Client configuration on FortiAuthenticator.
- **Test Connectivity**: verify the connection between FortiGate and FortiAuthenticator.

User Groups

We need to create local groups on Fortigate, corresponding to the groups created on FortiAuthenticator (HR, IT, Marketing, SSLVPN)

- 1) User & Device -> User Groups and select Create New
- 2) Name: Give it a suitable name
- 3) Type: Firewall
- 4) Remote Groups -> Add and select the remote RADIUS Server created previously (fac).
- 5) **Groups: Specify** and give it a name (corresponding to FortiAuthenticator group name)

Note – By default this value is '*Any*', and with this value, FortiGate will ignore radius attributes received. So in order to match attribute HR, instead of *Any*, select HR.

FortiWiFi 61E FW	/F61E4Q1	6000306			Add Course Market		
20 Dashboard	>				Add Group Match		
🔆 Security Fabric	>				Remote Server	🍰 FAC	-
K FortíView	>		radius_group_HR		Groups	any Specify	
+ Network	>	Туре				HR	0
System	>	Members	+				
Policy & Objects	>	Remote Gr					
Security Profiles	>						
므 VPN	>	+ Add	A Edit 📋 Delete				
User & Device	~			Remote Server			
User Definition		島 FAC					
User Groups	☆						

Now every user that arrives with e.g. an attribute 'HR' will be matched against *radius_group_HR* group.

FortiWiFi 61E FWF61E4Q16000306										
🚯 Dashboard	>	+ Create New & Edit To Clone Delete Search	Q							
🔆 Security Fabric	>	Group Name A	Group Tupo 🌢	Mombors *						
🖿 FortiView	>	Group Name 🖤	Group Type +	Members •						
Network	>	FortinetSSO	🕸 Fortinet Single Sign-On (FSSO)		0					
System	>	Guest-group	Firewall	🛔 guest	0					
📕 Policy & Objects	>	SSL-VPN-users	Firewall	shanazkhan	3					
Security Profiles	>			SIII38						
U VPN	>	SSO_Guest_Users	Fortinet Single Sign-On (FSSO)		1					
Luser & Device	~	radius-group_IT	E Firewall	🖧 FAC	2					
User Definition		radius_group_HR	Firewall	lo FAC	2					
User Groups	☆	radius_group_Marketing	Firewall	S FAC	2					
Guest Management		radius_group_SSLVPN	E Firewall	S FAC	3					
Device Inventory		vpn-group	E Firewall		4					

Repeat the above steps for all necessary groups (in this case, HR, IT, Marketing, SSLVPN)

SSL VPN Settings

VPN -> SSL-VPN Settings

- Specify Listen on Interface(s) in this case wan1 + Listen on port 10443
- **Restrict Access**: Allow access from any host
- **Tunnel Mode Client settings** -> Address Range: Automatically assign addresses
- Specify DNS Server(s)
- Authentication/Portal Mapping: Create New, select the necessary group(s), keep default realm and assign portal tunnel-access

FortiWiFi 61E	FWF61E4Q1	6000306				
🚯 Dashboard	>	SSL-VPN Settings		Edit Authenticat	ion/Portal Mapping	
🔆 Security Fabric	>			Users/Groups	radius-group_IT	×
E FortiView	>		You are using a default built-in certificate, which will not be ab your server's domain name (your users will see a warning). It is		radius_group_HR	×
+ Network	>		recommended to purchase a certificate for your domain and u		radius_group_Marketing	×
System	>		usu,		+	
Policy & Objects	>		Click here to learn more	Realm	Default realm Specify	
Security Profiles	>			Portal	tunnel-access	
	~	Require Client Certificate				

All the necessary groups will now show up in the Authentication/Portal Mapping window:

VPN	~				
Overlay Controller VPN	Tunnel Mode Client Settings 🚯				
IPsec Tunnels IPsec Concentrator IPsec Wizard IPsec Tunnel Templates	Address Range	Automatically assign a Tunnel users will reco 10.212.134.210	ddresses Specify cu	stom IP ranges 10.212.134.200 -	
SSL-VPN Portals	DNS Server	Same as client system	DNS Specify		
SSL-VPN Settings	DNS Server #1	185.83.167.68			
SSL-VPN Realms	DNS Server #2	185.83.167.4			
VPN Location Map	Specify WINS Servers	Þ			
User & Device	> Allow Endpoint Registration	Þ			
' WiFi & Switch Controller Log & Report Monitor	 Authentication/Portal Mapping Create New Edit 	0 Delete			
	User	s/Groups	Realm	Portal	
	SSL-VPN-users		1	tunnel-access	
	 radius_group_SSLVPN radius-group_IT 		1	tunnel-access	
	 radius_group_HK radius_group_Marketing 				
	 radius_group_HR radius_group_Marketing All Other Users/Groups 		1	web-access	
	и radius_group_нк и radius_group_Marketing All Other Users/Groups		1	web-access	

SSL-VPN Portals

- Edit tunnel-access, make sure that Tunnel mode is enabled
- **Enable Split Tunneling:** when enabled, only traffic that matches the destination address in the respective policy will be routed through the tunnel. (In this case, split tunneling is not enabled as I wish my test users to also access Internet through the tunnel).
- **Source IP Pools:** select SSLVPN_TUNNEL_ADDR1 (automatically created in the tunnel mode client settings)

Firewall Policies

• Create policies to grant access to your users connecting though SSLVPN. This is also where we grant users access to resources based on their group membership.

12 Dashboard > 1 12 Security Fabric > 14 FortiView > 15 System > 16 System > 17 Policy 1 17 Authentication Rules > 17 Authentication Rules > 17 Addresses > Wildcard FQDN Addresses > Internet Service Database > Schedules > Virtual IPs > IP Pols >	Edit Policy Name ① Incoming Interface A Outgoing Interface Source Destination Schedule Service Action Inspection Mode	Access HR SSLVPN tunnel interface (ssl.root * SSLVPN_TUNNEL_ADDR1 radius_group_HR FAZ ACCEPT Ø DENY w based Proxy-based	X X X X X X X X X X X X X X X X X X X			
X Security Fabric > M FortiView > T Network > IPotiDigs > > IPotiDigs > > IPotiDigs Objects ~ IPot Policy IPot Policy IPot Policy Addresses Wildcard FQDN Addresses Internet Service Database Schedules Virtual IPs IP Pols Protocol Octions Pools Pools	Name 1 Incoming Interface Outgoing Interface Source Destination Schedule Service Action Inspection Mode	Access, HR SSL-VPN tunnel interface (ssl.root * SSLVPN, TUNNEL_ADDR1 radius_group_HR * FAZ * ACCEPT Ø DENY w based Proxy-based	× × × ×			
 ▶ FortiView > > ♦ Network > ♦ System > Policy & Objects Poly Policy Authentication Rules IPv4 DoS Policy Addresses Wildcard FQDN Addresses Internet Service Database Services Schedules Virtual IPs IP Polos Bersteral Octions 	Name 0 Incoming Interface Outgoing Interface Source Destination Schedule Service Action Inspection Mode	Access HR SSL-VPN tunnel interface (ssl.root SSL-VPN tunnel interface (ssl.root SSL-VPN tunnel interface (ssl.root SSL-VPN tunnel ADDR1 SSL-VPN tunnel ADDR1 SSL-VPN tunnel ADDR1 FaZ FaZ Accept Paxet Proxy-based Proxy-based	× × ×			
Hetwork System System Policy & Objects Policy & Objects Policy & Objects Pov4 Policy Policy Policy Policy Authentication Rules IPv4 DoS Policy Addresses Internet Service Database Services Schedules Virtual IPs IP Polos Porols Porols	Incoming Interface Outgoing Interface Source Destination Schedule Service Action Inspection Mode Fig	SSL-VPN tunnel interface (sslroot SSL-VPN tunnel interface (sslroot SSLVPN_TUNNEL_ADDR1 radius_group_HR FAZ FAZ ALL ALL VACCEPT ODENY webased Proxy-based	X X X X X X X X X X X X X X X X X X X			
System System Policy & Objects ' IPv4 Policy Ivy A Policy Authentication Rules IPv4 DoS Policy Addresses Wildcard FQDN Addresses Internet Service Database Services Schedules Virtual IPs IP Pools Pools Pools	Outgoing Interface Source Destination Schedule Service Action Inspection Mode	Serv-Int SSLVPN_TUNNEL_ADDR1 radius_group_HR FAZ FAZ ACCEPT OLENY w-based Proxy-based	× × × × ×			
Policy & Objects IPv4 Policy Authentication Rules IPv4 DoS Policy Addresses Internet Service Database Services Schedules Virtual IPs IP Pools Portoeol Octions	Source Destination Schedule Service Action Inspection Mode	+ SSLVPN_TUNNEL_ADDR1 radius_group_HR radius_group_HR FAZ A A A A A A A A A A A A	X X X X X X X X X X X X X X X X X X X			
IPv4 Policy ☆ Authentication Rules IPv4 DoS Policy IPv4 DoS Policy Addresses Midcard FQDN Addresses Internet Service Database Services Schedules Virtual IPs IP Pools Perstonal Octions Schedules	Source Destination Schedule Service Action Inspection Mode	SSLVPN_TUNINEL_ADDR1 SSLVPN_TUNINEL_ADDR1 SSLVPN_TUNINEL_ADDR1 STATUS FAZ FAZ FAZ FAZ FAZ FAZ FAZ FAZ FAZ FA	x x x x x x x x x x x x x x x x x x x			
Authentication Rules IPv4 DoS Policy Addresses Wildcard FQDN Addresses Internet Service Database Services Schedules Virtual IPs IP Pools Personal Octions	Destination Schedule Service Action Inspection Mode		×			
IPv4 DoS Policy Addresses Wildcard FQDN Addresses Internet Service Database Services Schedules Virtual IPs IP Pools Personal Octions	Destination Schedule Service Action Inspection Mode	FAZ ACCEPT Ø DENY w-based Proxy-based	×			
Addresses Wildcard FQDN Addresses Internet Service Database Services Schedules Virtual IPs IP Pools Personal Octions	Schedule Service Action Inspection Mode	ACCEPT Ø DENY w-based Proxy-based	×			
Wildcard FQDN Addresses Internet Service Database Services Schedules Virtual IPs IP Pools Protocol Octions	Schedule Service Action Inspection Mode	Image: Contract of always Image: Contrest of always	×			
Internet Service Database Services Schedules Virtual IPs IP Pools Protocols	Service Action Inspection Mode	ALL ACCEPT Ø DENY w-based Proxy-based	×			
Services Schedules Virtual IPs IP Pools Perford Options	Action Inspection Mode Flo	ACCEPT Ø DENY w-based Proxy-based				
Schedules Virtual IPs IP Pools Protocol Options	Action Inspection Mode Flo	ACCEPT O DENY w-based Proxy-based				
Virtual IPs IP Pools Protocol Options	Inspection Mode Flo	w-based Proxy-based				
IP Pools Protocol Ontions	inspection mode	Proxy-based				
Protocol Ontions						
Trococor opcions	Firewall / Network Opti	ions				
Traffic Shapers Traffic Shaping Policy Traffic Shaping Profile	NAT O Protocol Options	efault 👻	1			
Security Profiles	Security Profiles					
2 VPN	AntiVirus 🔾)				
User & Device	Web Filter)				
♥ WiFi & Switch Controller >	DNS Filter)				
M Log & Report	Application Control					
	IPS 🔘)				
- Monitor	SSL Inspection	sst no-inspection •				
	Logging Options					
	Log Allowed Traffic	Security Events All Sessions				
	Comments Write a c	comment				
	Enable this policy 🔘					

 Create a separate policy for each group, with the same Incoming Interface – SSLVPN tunnel interface (ssl.root). The differentiator will be the source groups we add in addition to SSLVPN_TUNNEL_ADDR1

42	Access_IT		SRV_mngt	SSLVPN_TUNNEL_ADDR1	<pre>esxi_server</pre>	o always	ALL	✓ ACCEPT	8 Disabled
44	Access_HR	SSL-VPN tunnel interface (ssl.root)	Serv-Int	SSLVPN_TUNNEL_ADDR1	🗐 FAZ	lo always	ALL	✓ ACCEPT	Oisabled
45	Access_Marketing	SSL-VPN tunnel interface (ssl.root)	Serv-IntFML-Management	SSLVPN_TUNNEL_ADDR1	📮 FML	lo always	ALL	✓ ACCEPT	Disabled

Testing

• Once you've completed the above configuration, you can test connecting a user to SSL-VPN, e.g. our test user dollyduck:

FortiClient The Security Fabric Agent		– 🗆 X
File Help		
dollyduck ~	0	
X FABRIC TELEMETRY		
() MALWARE PROTECTION		-
🚱 WEB FILTER		
CALING APPLICATION FIREWALL	VPN Name Test-SSL	Ŧ
🛞 VULNERABILITY SCAN	Username dollyduck	
	Token	
Notifications	OK	ocel
C Settings		
🖽 About		

The test user is asked for Token after username/password. BuyPass token code is typed and the test user connects successfully, as shown in FortiAuthenticator logs

Fortiauthenticator Logs

• FortiAuthenticator logs shows successful connection.

FortiAuthenticator vé	5.00-ы	uild0034	FAC-VMTM18003072								Lagged in as admin	0 🕩
System	>	C Refr	esh 🗅 Download Raw Log	Log Type I	Reference	✿ Debug Report ►					Search for k	ug records
Authentication Fortinet SSO Methods	,	ID	Timestamp	Level	Category	Sub category	Type id	Action	Status	Source IP	Short message	User
Monitor	,	5689	Tue Jul 30 17:52:08 2019	information	Event	Authentication	20001	Authentication	Success	10.188.2.1	Remote LDAP user authentication with chained radius auth successful	dollyduck
Certificate Management	,	5688	Tue Jul 30 17:51:47 2019	information	Event	Authentication	20299	Authentication	Pending	10.188.2.1	Remote RADIUS user authentication partially done, remote server expecting challenge response	dollyduck

• View log details. The detailed logs may also be useful for troubleshooting

System	>	C Refre	sh Download Raw Log	E Log Type F	Reference	Debug Report -							Search for I	log records	
Authentication	>	ID	Timestamp	Level	Category	Sub category	Type id	Action	Status	Source IP	Short message		Deta	ails	>
Monitor	,	5689	Tue Jul 30 17:52:08 2019	information	Event	Authentication	20001	Authentication	Success	10.188.2.1	Remote LDAP user authentication with chained radius auth successful	ID I	Log Record I	Detail	
Certificate Management	,	5688	Tue Jul 30 17:51:47 2019	information	Event	Authentication	20299	Authentication	Pending	10.188.2.1	Remote RADIUS user authentication partially done, remote server expecting challer	Timestamp	Tue Ju	a 30 17:51:4	7 201
Logging	~	5687	Tue Jul 30 17:50:34 2019	error	Event	System	30910				NTPD no server suitable for synchronization found/error repeated 29 times in the past	Level	inform Auctor	nation	
Log Access		5686	Tue Jul 30 16:49:49 2019	error	Event	System	30910				NTPD no server suitable for synchronization found/error repeated 29 times in the past	Status	Pendi	ing	
Logs		5685	Tue Jul 30 15:49:04 2019	error	Event	System	30910				NTPD no server suitable for synchronization found/error repeated 29 times in the past	Source IP	10.18	8.2.1	
🕼 Log Config	>	5684	Tue Jul 30 15:33:15 2019	information	Event	Authentication	20320	Authentication	Failed	10.188.2.1	Remote LDAP user authentication with no token failed: user not found	Message	Remot hentic remot	te RADIUS u cation partial te server exp	yer au ly don acting
Audit Reports	> 5	> 5683 Tue	Tue Jul 30 15:19:51 2019	information	Event	Authentication	20320	Authentication	Failed	10.188.2.1	Remote LDAP user authentication with no token failed: user not	User	hallen	ge response duck	
		5682	Tue Jul 30 14:48:19 2019	error	Event	System	30910				NTPD no server suitable for synchronization found/error repeated 29 times in the past		Log Typ)e	
		5681	Tue Jul 30 14:45:27 2019	information	Event	Admin Configuration	10003	Delete			Deleted User Group: Remote LDAP	Type Id	20299	2	
		5680	Tue Jul 30 14:31:47 2019	information	Event	Authentication	20994	Login	Success	10 188 6 101	Web access granted to 'admin'	Name	Authe	e RADIUS CH	sting alleng
		5470	T . 1 100 44 04 17 0040		E	A double double	00004	Login	6	10.100.0.101		Sub Category	Autho	antication	
		56/9	106 301 30 14:31:47 2019	information	Event	Autrentication	20994	Login	Success		Local administrator autnentication with no token successful	Category	Event		
		5678	Tue Jul 30 13:47:35 2019	error	Event	System	30910				NTPD no server suitable for synchronization found/error repeated 29 times in the past	Description	Authorization	ntication po e RADIUS se	į
		5677	Tue Jul 30 12:46:50 2019	error	Event	System	30910				NTPD no server suitable for synchronization found/error repeated 29 times in the past		ocong	/ cnascrige re	1004

On the FortiGate, Monitor \rightarrow Firewall User Monitor displays our test user as connected:

dollyduck	radius-group_IT	11 second(s)	10.212.134.200	0 B	Le Firewall

Test user may now access network resources according to defined security policies. In our sample configuration, test user dollyduck belongs to AD Group IT. Our FortiGate policies grant group IT access to the essi server only:



The test user is not allowed to access e.g. FortiMail (10.188.100.10)

Windows 10					🖪 🏠 Actio	ins 🗵
🛃 Log in - VMware ESXi 🛛 🗙 🔿	10.188.100.10	×	+	-	٥	×
\leftrightarrow \rightarrow X (i) https://10.188.100.10/	/admin			T	2	:
ED.						
Dette nettstedet er ik	ke tilgjengelig					
10.188.100.10 brukte for lang tid	på å svare.					
Prøv dette:						
Sjekk tilkoblingen						
 Sjekk proxy-tjeneren og br Kjør Windows Nettverksdia 	annmuren agnose					
	- <u>j</u>					
ERR_CONNECTION_TIMED_OUT						
Last inn på pytt				Deta	lier	
Kobler til						
Kobler til						

ex. Ledetekst

Microsoft Windows [Version 10.0.17763.615] (c) 2018 Microsoft Corporation. Med enerett.
C:\Users\dollyduck>ping 10.188.11.10
Pinging 10.188.11.10 with 32 bytes of data: Request timed out. Request timed out. Request timed out. Request timed out.
Ping statistics for 10.188.11.10: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss), C:\Users\dollyduck>ping 10.188.10.10
Pinging 10.188.10.10 with 32 bytes of data: Reply from 10.188.10.10: bytes=32 time=2ms TTL=63 Reply from 10.188.10.10: bytes=32 time=1ms TTL=63 Reply from 10.188.10.10: bytes=32 time=1ms TTL=63 Reply from 10.188.10.10: bytes=32 time=1ms TTL=63
Ping statistics for 10.188.10.10: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 1ms, Maximum = 2ms, Average = 1ms

Let's test with a user belonging to another group, e.g. mickeymouse \rightarrow group Marketing.

As with test user donalduck, this test user is asked for buypass token in addition to username/password.

FortiClient The Security Fabric Agen		-	×
File Help			
mickeymouse ~	0		
X FABRIC TELEMETRY			
() MALWARE PROTECTION			
🕀 WEB FILTER	_		
APPLICATION FIREWALL	VPN Name Test-SSL v		
HIN VULNERABILITY SCAN	Username mickeymouse		
	Password ······		
Notifications			
C Settings	OK Cancel		
About			

FortiAuthenticator verifies successful login

information	Event	Authentication	20001	Authentication	Success	10.188.2.1	Remote LDAP user authentication with chained radius auth successful	mickeymouse
information	Event	Authentication	20299	Authentication	Pending	10.188.2.1	Remote RADIUS user authentication partially done, remote server expecting challenge response	mickeymouse

FortiGate, Monitor \rightarrow Firewall User Monitor, displays our test user as connected.

FortiWiFi 61E	WF61E4Q1	6000306				>	[] 🛛 • 🗘 🛛 🕗 admin
B Dashboard	>	2 Refresh 🕞 Deauthenticate	Show all FSSO Logons Search	Q			
Security Fabric	>	User Name ≑	User Group ≑	Duration ≑	IP Address ≑	Traffic Volume ≑	Method \$
+ Network	, ,	mickeymouse	Radius_group_Marketing	10 minute(s) and 51 second(s)	10.212.134.200	372.39 kB	Firewall

Once connected, Test user mickey mouse has access to FortiMail, as per firewall policies.

Windows 10					🖨 Actio	ons 🛞
🖻 🖅 🗖 FortiMail	× + ~		10		٥	×
\leftarrow \rightarrow O \textcircled{a}	Sertifikatfeil https://10.188.100.10/admin	□ ☆	∱≡	h	È	

Please Login	
Name	
Password	
Remember me	
Log In	