

## BRUKERVEILEDNING

## **INTEGRASJONSGUIDE – BP CODE** Check Point R75.x – R76

ÅPEN

Versjon: 1.2 Versjonsdato: 30.07.2013

Fax: +47 23 14 59 01

E-mail: kundeservice@buypass.no VAT: NO 983 163 327

# Endringshistorie

Versjon	Dato	Status	Beskrivelse/Endringer
1.0	11.03.2013	Final	Opprettelse og ferdigstillelse av dokument
1.1	30.05.2013	Final	Små justeringer
1.2	30.07.2013	Final	Små justeringer

## Bidragsytere

Firmanavn	Navn
EVRY	Asmer Helez
Buypass	Espen Sammerud

# Innholdsfortegnelse

1	Kon	figurere Check Point med Buypass Code 2-faktor autentisering	4
	1.1	Forutsetninger	4
	1.2	Fremgangsmåte	4

# 1 Konfigurere Check Point med Buypass Code 2-faktor autentisering.

### 1.1 Forutsetninger:

- a. BPC GW er installert i nettverket og kan kommunisere med LDAP server på TCP port 389 (Idap).
- b. Servicekonto som skal brukes for å lese AD er opprettet.
- c. Oversikt over ip-adresser for BP Code GW, PoA (Point of Access).
- d. Velg LDAP stien. Skal man bruke hele AD, bestemt OU eller flere OU's?

### 1.2 Fremgangsmåte

2. Logg på ditt brukersted med admin-bruker. https://www.buypass.no/bpcode/merchants/DINMERCHANTKODE/

buypass

3. Definer LDAP server og LDAP sti under meny LDAP.

Oversikt og varsling Hendelseslogg Auditeringslogg	LDAP konfiguras	jon			
Administrasjon <u>Brukere</u> <u>Brukersted</u>	URL:*	ldap://192.168.171.15 f.eks. «Idap://idap.domene.no»	?	IP addr. til LDAP server/domene kontroller	
Konfigurasjon LDAP Radius	Brukernavn:* Passord:*	bpc_svc_ldap	?	Service konto med lese tilgang til LDAP/AE og passord	
>ålogget:	Tel.nr. attribut:* App.id. attribut:	mobile	?	Attribut i LDAP/AD	
Rolle: SUPERUSER	Beskrivelse: LDAP lockout varighet:	LDAP BPLAB01 0	?	Beskrivelse for enklere oversikt hvos flere	
For brukersted: <b>Fest Redundans</b> <u>(Loga ut)</u>	Aktiv	Tilbake Lagre     * betyr at feltet må være utfylt			

### LDAP sti(er).

	URL		Brukernavn	Tel.nr. attribut	App.id. attribut	Beskrivelse	
-	Idap://192.168.171.15		bpc_svc_ldap	mobile		LDAP BPLAB01	
Prioritet LDAP sti							
	1 basedn[ou=Users,ou=BPCode,dc=BPLAB01,dc=local(*)],filter[samAccountName=#USER#]			x slett			
	3	basedn[ou=Users2,o	u=BPCode,dc=BPLAB	01,dc=local(*)],filter[samAcc	countName=#USERS	#] x slett	
	2	basedn[ou=Users2,o	u=BPCode,dc=BPLAB	01,dc=local(*)],filter[samAcc	countName=#USER#	] x slett	

Man kan definere en eller flere LDAP stier. Hvis man ønsker å liste alle undermapper så bruker man (\*) bak siste DC= (i vårt eksempel ,dc=local(\*))

4. Definer RADIUS klient (Konfigurasjon  $\rightarrow$  Radius  $\rightarrow$  Ny konfigurasjon).

Oversikt og varsling Hendelseslogg	RADIUS konf	igurasjon				
Auditeringslogg Administrasjon				LAN in til CP		
Brukere	IP-adresse:*	192.168.171.1	?			
Administrator	Shared secret:*	•••••	? 🧹	Shared secret		
Konfigurasjon	NAS identifikator:		?	•		
Radius	NAS IP:		?			
- 0.	Beskrivelse:	CheckPoint R75.30	? <	📁 🛛 Beskrivelse		
Palogget: Rolle:	Tilbake         Lagre           = betyr at feltet må være utfylt.					
Oversikt og varsling Hendelseslogg	RADIUS konf	igurasjon				
Auditeringslogg Administrasjon	Oversikten viser inforr Code.	nasjon brukerstedet trenger for å sette opp	en RADIUS-klient for	autentifisering med henhold		
Brukere Brukersted	IP-adresse	NAS identifikator	NAS IP	Beskrivelse		
Administrator						
LDAP						
Radius	± 192.168.171.37			MS UAG 2010		
	192.168.171.1			CheckPoint R75.30		
Pålogget:	Ny konfiguracion					

- 5. Logg på Check Point SmartDashboard.
- 6. Definer ny Host for BP Code GW.



Skriv inn navn på Host, IP-adresse og beskrivelse, og klikk OK.

но	st Node - BuypassLode	GW Contraction of the second	<u> </u>
[	General Properties	Host Node - General Properties	
	NAT	Machine	
	Other	Name: BuypassCodeGW	Color: 📕 Black 💌
		IP Address: 192.168.171.24 Resolve from Name	
		Comment: BPLABBPC01	
		Products:	
		Configure Servers	

7. Klikk på "Servers and OPCSEC Applications" (1). Høyre klikk på RADIUS og velg New RADIUS (2).



8. Fyll inn: Name, Comment, velg Host fra pkt 6, velg service "UDP NEW-RADIUS", skriv inn shared secret fra pkt 4, velg RADIUS Ver.2.0 og PAP. Klikk OK.

RADIUS Server Properties - BPC-RADIUS						
General Accou	unting					
Name:	BPC-RADIUS					
Comment:	BPC Radius server					
Color:	Black -					
Host:	BuypassCode - New					
Service:	UDP NEW-RADIUS					
Shared Secret:	•••••					
Version:	RADIUS Ver. 2.0 Compatible					
Protocol:	PAP 👻					
Priority:	1 🔄 (1 is highest)					
	OK Cancel					

- 9. Det er flere måter å sette opp en VPN brukertilgang i Check Point på. Brukere kan autentiseres direkte, med LDAP mot AD, SecurID eller ved å bruke RADIUS. Vi skal vise hvordan man konfigurerer alle eksterne brukere til å benytte BP Code Radius Gateway ved autentisering.
- 10. Gå til Manage → Users and Administrators → New → External User Profile → Match all users Dette lager en bruker med navn generic\*

🎬 192.168.171.1 - Check Point SmartDashboard R75.30 - Standard							
<u>File E</u> dit <u>V</u> iew <u>M</u> anage <u>R</u> ule	es <u>P</u> olicy	SmartWor	rkflow	<u>S</u> earch	<u>W</u> indow	Help	
፤ 🖬 Ə 🛛 🌡 🖻 🛅 🗄	№ № #	ð : 🗉	;		<b>-</b> 1	<b>⇒</b> × ‡	ų
두 숙 🔍 🕒 🗚	8		×	Mobile A	Access	1 🖻	А
🖃 🐣 Users and Administrators	•			Firew	all		5 N
🕀 🔂 Access Roles			No	Name		So	
		I		TT GILLO		00	
🕀 📃 Administrators		I		Firewa	all manag	jement	(F
- External User Profiles			1			-	-
🕀 🚰 LDAP Groups	New Ext	ernal User	Profile	Ma	itch by doi	main	
🕀 🔒 Templates	Edit			Ma	itch all use	rs	

11. Fyll inn Comment, velg RADIUS som "Authentication Scheme" og velg BPC Radius server definert under pkt 8. Klikk OK.

External User Profile Proj	perties ? 🗙
General Properties Groups Authentication Location Time Encryption	General Properties         This External User Profile will apply to all users which are not defined in the internal User Database or any known LDAP Account Unit and do not match any other External User Profile.         External User Profile name:       generic*         Comment:       All external users         Expiration Date       \$1.12.2030         Expiration Date:       \$1.12.2030
Futernal User Profile Pre	nation 2V
External oser Frome Fro	
General Properties Groups Location Time Encryption	Authentication Authentication Scheme: RADIUS Settings: Select a RADIUS Server or Group of Servers: BPC-RADIUS

12. Opprett en ny VPN gruppe (User Group)



Skriv inn navn på gruppen og legg til generic\* i "Selected Members" (ble opprettet under pkt 11). Klikk OK.

Group Properties - RA	DIUS-VPN-USERS	? ×
Name:	RADIUS-VPN-USERS	
Comment:		
Color:	Black 💌	
Mailing List Address:		
Available Members:	Selected Members:	
asmhel     BPC-LDAP-GRP     de     grp_sec_ypn     grp_usertest     infopulse     infopulse     ioov     ioov     mikon	▲ Add > Add > Add >	
Show: All	View expanded group.	,
	OK Car	ncel

13. Klikk på VPN communities, høyreklikk på Remote Access, velg Participating Gateways og legg til Check Point firewall objektet hvis det ikke er der fra før.

🎬 192.168.171.1 - Check Point SmartDashboard R75.30 - Standard
<u>Eile Edit View M</u> anage <u>R</u> ules <u>P</u> olicy SmartWorkflow <u>S</u> earch <u>Wi</u> ndow <u>H</u> elp
:日 つ I X 四 四   🍓 極 奥 ぬ   三   三 = = = = = = = = = = = = = = = =
🖳 🗣 🗣 🕲 🔍 📵
🖃 🖓 VPN Communities 🛛 🗰 Firewall 👘 NAT 🚔 IPS 💡
🔁 🔯 Site To Site
Remote Access
General Participating Gateways
Participating Gateways
Participant User Group     All the connections between the Gateways below and the     Participants Users Groups will be encrupted
Paticipant Cateways
👔 dgffw01lb
Add Edit Remove

Klikk på Participant User Groups og legg til (Add) gruppen som ble opprettet under pkt 12. Klikk OK to ganger.

🎇 192.168.171.1 - Check Point SmartDas	hboard R75.30 - Standa	dard	
<u>File Edit View Manage Rules Policy</u>	SmartWorkflow Search	Window Help	_/
i 🔚 つ l X फ फ 👔 i 🏭 起 🦸	note Access Communit	ity Properties - RemoteAccess	×
목 숙 🔍 🕼 🗚 🔒 📔	General	Participant User Groups	
VPN Communities      Site To Site	Participating Gateways Participant User Group	Add Participants Users Groups Remote Access User I	?>
Remote Access		grp_sec_ypn     grp_sec_ypn     grp_sec_ypn     grp_sectest     grp_sect	cel
		Add Edit Remove	F

14. Opprett firewall regel (om nødvendig) som tillater udp/1812 (new-radius) trafikk fra firewall til BPC GW.



15. Klikk på "Install Policy" og deretter OK.



Installation Taxaba	Marian	Mahurah Casuitu	0.0	Desister Consulty
dalfw01lb	B75 30	Verifuing	405	Desktop Security
- gumono	1110.00	<ul> <li>Follying</li> </ul>		Though the second se
	_			
Show Errors				
Show Errors	- Standard			Minimize
Show Errors tallation Process stallation	- Standard			Minimize
Show Errors tallation Process stallation nstallation Targets	- Standard	Network Security	QoS	Minimize
Show Errors callation Process stallation nstallation Targets dglfw01lb	Standard Version R75.30	Network Security	QoS	Minimize
Show Errors tallation Process stallation installation Targets digfw01lb	- Standard Version R75.30	Network Security	QoS	Minimize
Show Errors	- Standard Version R75.30	Network Security	QoS	Minimize
Show Errors	- Standard	Network Security	QoS	
Show Errors	- Standard Version R75.30	Network Security	QoS	Minimize  Desktop Security @K
Show Errors	- Standard Version R75.30	Network Security	QoS	Minimize
Show Errors	- Standard Version R75.30	Network Security	QoS	Minimize
Show Errors	Version R75.30	Network Security	QoS	Minimize Desktop Security OK
Show Errors	- Standard Version R75.30	Network Security	QoS	Minimize
Show Errors	- Standard Version R75.30	Network Security	QoS	Minimize
Show Errors	- Standard	Network Security	QoS	Minimize
Show Errors  tallation Process istallation installation Targets digliw01b installation comp installation comp installation comp installation comp	- Standard	Network Security	QoS	Minimize

16. Konfigurer Check Point klienten til å bruke RADIUS ved pålogging (Sites – Properties – Settings)..

Det skal velges "Username and Password" for "Authentication Method".

Endpoint Security <sup>.</sup>
Sites Advanced A site represents the organization you want to connect
BP lab
Properties of BP lab
Details       Settings         Always-Connect       Enable Always-Connect to allow the client to connect automatically to your active site when possible.         Image: Enable Always-Connect       Pril tunneling         When connected, all outbound traffic is encrypted and sent to the gateway but only traffic directed at site resources is passed.         Image: Encrypt all traffic and route to gateway
Authentication Method: Username and Password v
OK Cancel Help

17. Tast inn brukernavn og engangskode fra Buypass Code App'n og klikk Connect.

😚 Check Point Endpoi	nt Security	
Endpoint S	ecurity <sup>.</sup>	
Site: Authentication	BP lab 💌	
Username: Password:	bp_asmhel	1
Connect	Cancel Help	

#### 18. VPN koblet

😚 Connecting to BP lab		×
Endpoint Sec	urity <sup>.</sup>	Check Point SOFTWARE TECHNOLOGIES LTD.
	Loading virtual network adapter	75%
	Cancel Close	<< Details
Detecting Proxy Configural Resolving site name Betrieving site information	ion	•
Checking if a client update Connecting to site User bp_asmhel authentic	is available ated by Radius authentication	=
Enforcing firewall policy		
Endpoint Sec	urity <sup>.</sup>	Check Point SOFTWARE TECHNOLOGIES LTD.
	Connection succeeded	100%
	Disconnect Close	Details >>

19. Vi kan sjekke i loggen på BP Code Manager om påloggingen var vellykket eller ikke.

🗢 buypass <sup>.</sup>	
Oversikt og varsling Hendelseslogg Aufteringslogg Administrasjon Briskers Briskersker Konfigurasjon LDA2 Raduus	Hendelseslogg       Oversikten viser hendelser siste uken. Bruk søkefunksjonen hvis du ønsker å se en bestemt tidsperiode, hendelser for en bestemt bruker, og/eller for en bestemt hendelsestype.       Fre kl.:     00:00 • • • • • • • • • • • • • • • • •
Pålogget:	06.03.2013 ACCESS_GRANTED bp_asmhel User authenticated CN=bp_asmhel, OU=Users, OU=BPCode, 14:03:19 DC=BPLAB01, DC=local and NAS 192.168.171.1

Brukers' plassering i AD må være i samsvar med LDAP stien som ble konfigurert i BP Code Manager i pkt 3.