

## BRUKERVEILEDNING

## **INTEGRASJONSGUIDE – BP CODE** Cisco ASA 8.3x – 9.1x

ÅPEN

Versjon: 1.1 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	30.05.2013	Final	Opprettelse og ferdigstillelse av dokument
1.1	30.07.2013	Final	Små justeringer

## Bidragsytere

Firmanavn	Navn
Buypass	Espen Sammerud

# Innholdsfortegnelse

1	Kon	nfigurere Cisco ASA med Buypass Code 2-faktor autentisering	4
1	1.1	Forutsetninger	4
1	1.2	Fremgangsmåte	4

## 1 Konfigurere Cisco ASA 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 BPC 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 Ide	ntifisering			buypass
Identifiser	med Buypa	ss Co	de	
	Brukernavn*: Engangskode*:		Logg på	

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

Hendelseslogg	LDAP konfigurasj	on		
Administrasjon				
Brukere	URL:*	ldap://192.168.171.15	?	IP addr. til LDAP server/domene kontroller
<u>Brukersted</u> Administrator		f.eks. «Idap://Idap.domene.no»		
Konfigurasjon	Brukernavn:*	bpc_svc_ldap	?	Service konto med lese tilgang til I DAP/AD
LDAP Radius	Passord:*	•••••	?	og passord
	Tel.nr. attribut:*	mobile	?	Attribut i LDAP/AD
>ålogget:	App.id. attribut:		?	
Rolle:	Beskrivelse:	LDAP BPLAB01	?	Beskrivelse for enklere oversikt byos flere
SUPERUSER	LDAP lockout varighet:	0	?	beskinelse for enkiele oversikelitos here
For brukersted:	Aktiv	8		
Fest Redundans		Tilbake Lagre		
[Logg_ut]		* betyr at feltet må være utfylt	t.	

#### 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=BPLAB0	1,dc=local(*)],filter[samAcco	ountName=#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[samAc	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(\*))

 Definer RADIUS klient (Konfigurasjon → Radius → Ny konfigurasjon). Skriv inn "inside" IP på Cisco ASA'n, shared secret og en beskrivelse. Velg LDAP(er) som skal benyttes og deretter "lagre".

Hjem Logger Administrasjon	F	RADIUS kon	figurasjon			
LDAP	1	(P-adresse:*	192.168	171.151	<b>←</b>	
<u>Radius</u> Brukersted	5	Shared secret:*	•••••	•••	←	
		NAS identifikato	r:			1
Pålogget:		NAS IP:				
essa Rolle:	E	Beskrivelse:	Cisco AS	A 5505 8.3(	1)6 🗕	
Superbruker For brukersted: Test Redundans [Logg ut]		Tilgjengelige L Idap://192.16	DAPs 8.171.32	<- -> <<	Valgt LDAPs  dap://192.168.171.19	gre
	1				* betyr at feltet må v	være utfylt.
Hjem Logger Administrasjon Konfigurasjon LDAP Radius Brukersted	<b>RADIU</b> Oversikte Buypass (	<b>IS konfigurasj</b> e n viser informasjon b Code.	D <b>N</b> rukerstedet trenger for å	sette opp en RA	* betyr at feltet må v	være utfylt.
Hjem Logger Administrasjon Konfigurasjon LDAP <u>Radius</u> Brukersted	RADIU Oversikte Buypass (	<b>IS konfigurasj</b> e n viser informasjon b Code. a <b>dresse</b>	D <b>N</b> rukerstedet trenger for å NAS identifikator	sette opp en RA NAS I	* betyr at feltet må v DIUS-klient for autentisering me P Beskrivelse	være utfylt.
Hjem Logger Administrasjon Konfigurasjon LDAP Radius Brukersted Pålogget: essa	RADIU Oversikte Buypass ( IP-r B 192	<b>JS konfigurasj</b> e n viser informasjon b Code. adresse .168.171.24	D <b>N</b> rukerstedet trenger for å NAS identifikator	sette opp en RA NAS I	* betyr at feltet må v DIUS-klient for autentisering me P Beskrivelse Gw	være utfylt.
Hjem Logger Administrasjon LDAP Radius Brukersted Pålogget: essa Kolle:	RADIU Oversikte Buypass ( 192 192 192 192	IS konfigurasjo n viser informasjon b Code. adresse .168.171.24 .168.171.35	DN rukerstedet trenger for å NAS identifikator httptest	sette opp en RA NAS I	* betyr at feltet må v DIUS-klient for autentisering me P Beskrivelse Gw http	være utfylt.
Hjem Logger Administrasjon Konfigurasjon LDAP Radius Brukersted Pålogget: essa Rolle: Superbruker	P-ri P-ri ■ 192 ■ 192 ■ 192 ■ 192	JS konfigurasje n viser informasjon b Code. adresse .168.171.24 .168.171.35 .168.171.32	DN rukerstedet trenger for å NAS identifikator httptest idaptest	sette opp en RA NAS I	* betyr at feltet må v DIUS-klient for autentisering me P Beskrivelse Gw http Tomcat	være utfylt.
Hjem Logger Administrasjon Konfigurasjon LDAP Radius Brukersted Pålogget: essa Rolle: Superbruker	IP           * 192           * 192           * 192           * 192           * 192	<b>IS konfigurasj</b> o n viser informasjon b Code. 	DN rukerstedet trenger for å NAS identifikator httptest idaptest	sette opp en RA NAS I	* betyr at feltet må v DIUS-klient for autentisering me P Beskrivelse Gw http Tomcat Cisco ASA 5505 8.3(1)	e the second sec
Hjem Logger Administrasjon LDAP Radius Brukersted Pålogget: essa Rolle: Superbruker For brukersted: Test Redundans	RADIU Oversikte Buypass ( 192 192 192 192 192 192 192 192	Adresse adresse 168.171.24 168.171.35 168.171.32 1.168.171.151 AP URI D:://192.168.171.15	DN rukerstedet trenger for å NAS identifikator httptest idaptest	sette opp en RA NAS I Be	* betyr at feltet må v DIUS-klient for autentisering me Gw http Tomcat Cisco ASA 5505 8.3(1) skrivelse AP BPLAB01	6
Hjem Logger Administrasjon Konfigurasjon LDAP Radius Brukersted Brukersted Pålogget: essa Rolle: Superbruker For brukersted: Test Redundans	P-P- P-P- P-P-P- P-P-P-P-P-P-P-P-P-P-	IS konfigurasje           n viser informasjon b           Code.           adresse           .168.171.24           .168.171.35           .168.171.32           .168.171.151           AP URI           p://192.168.171.15           Rediger	DN rukerstedet trenger for å NAS identifikator httptest idaptest	sette opp en RA NAS I Be LD	* betyr at feltet må v DIUS-klient for autentisering me P Beskrivelse Gw http Tomcat Cisco ASA 5505 8.3(1) skrivelse AP BPLAB01	6
Hjem Logger Administrasjon LDAP Radius Brukersted Pålogget: essa Rolle: Superbruker For brukersted: Test Redundans [Loga_ut]	IP         IP      <	Adresse adresse .168.171.24 .168.171.35 .168.171.151 AP URI .://192.168.171.151 Rediger .168.171.37	DN rukerstedet trenger for å NAS identifikator httptest idaptest	sette opp en RA NAS I Be	* betyr at feltet må v DIUS-klient for autentisering me Gw http Tomcat Cisco ASA 5505 8.3(1) skrivelse AP BPLAB01 MS UAG 2010	6
Hjem Logger Administrasjon LDAP Radius Brukersted Pålogget: essa Rolle: Superbruker For brukersted: Test Redundans [Logg ut]	IP-1           © Versikte           Buypass (I           Buypass (I           192           192           192           192           Ig           192           192           192           192           192           Ig           Idap           Ig	JS konfigurasje           n viser informasjon b           Code.           adresse           .168.171.24           .168.171.35           .168.171.32           .168.171.151           P URI           o://192.168.171.15           Rediger           .168.171.37           .168.171.37	DN rukerstedet trenger for å NAS identifikator httptest Idaptest Slett	sette opp en RA NAS I LD	* betyr at feltet må v DIUS-klient for autentisering me Gw http Tomcat Cisco ASA 5505 8.3(1) skrivelse AP BPLAB01 MS UAG 2010 Check Point (SPLAT) R75	6 4.30

5. Logg på Cisco ASA med Cisco ASDM

6. Opprett en ny AAA Server Group under meny "Configuration – Remote Access VPN"

Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups



Klikk på "add" på høyre side i "AAA Server Groups" oversikten.

Add

Gi gruppen et navn, for eksempel "bpcode". Velg protokoll "RADIUS".

Resten av parameterne kan stå urørt. Klikk deretter på "OK".

付 Add AAA Server (	Group		×
Server Group: Protocol: Accounting Mode:	bpcode  RADIUS Simultaneous	▼	
Reactivation Mode:	Oppletion	🕤 Timed	
Dead Time: 10	minutes		
Max Failed Attempts:	3 counting update		
VPN3K Compatibi	lity Option		*
ОК	Cancel	Help	

Co	Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups					
A	AAA Server Groups					
	Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts
	LOCAL	LOCAL				
	bpcode	RADIUS	Single	Depletion	10	3

7. Legg til en server ("add" på høyre side) i den nylig opprettede gruppen (i feltet "Servers in the Selected Group").

Velg interface "inside". Skriv inn ip-adressen til BP Code GW'n. Endre "Server Authentication Port" til 1812. Endre "Server Accounting Port" til 1813. Skriv inn "Server Secret Key" (fra punkt 4). Fjern haken fra "Microsoft CHAPv2 Capable". Resten av parameterne kan stå urørt. Klikk deretter på "OK".

📑 Edit AAA Server		x
Server Group:	bpcode	
Interface Name:	Inside 🗸 🗸	←
Server Name or IP Address:	192.168.171.24	
Timeout:	10	seconds
RADIUS Parameters		
Server Authentication Port	: 1812 -	
Server Accounting Port:	1813 🔶	
Retry Interval:	10 seconds 🗸	
Server Secret Key:	•••••	
Common Password:		
ACL Netmask Convert:	Standard 👻	
Microsoft CHAPv2 Capable	: 🔲 🛶	
SDI Messages		
Message Table		8
OK	Cancel Help	

Se	rvers in the Selected Group	
	Server Name or IP Address	Interface
	192, 168, 171, 24	inside

Klikk deretter på "Apply" nederst i konfigurasjonsvinduet.

Fra det samme vinduet kan man nå teste autentiseringen (klikk på knappen "Test" på høyre side) for å sjekke at oppsettet er korrekt.

Velg "Authentication".

Skriv inn brukernavn (må finnes i LDAP/AD).

Skriv inn engangskode fra Buypass Code App'n og klikk deretter på "OK".

🔂 Test AAA Server	-192.168.171.24				
To test the following AAA server enter a username and password.					
AAA Server Group:	bpcode (RADIUS)				
Host:	192.168.171.24				
Authorization	Authentication				
Username:	essa_2 🔶				
Password:	****** •				
	OK Cancel				

information	n	×
į	Authentication test to host 192. 168. 171. 24 is successful.	
	OK	

Den samme konfigurasjonen kan gjøres fra CLI og ser da slik ut:

aaa-server	bpcode	protocol	radiu	JS
aaa-server	bpcode	(inside)	host	192,168,171,24
key *****				
authentica	ation-po	ort 1812		
accounting	g-port 1	1813		
no mschap\	/2-capak	ole		

8. Konfigurer "Clientless SSL VPN Access" til å bruke BP Code (RADIUS). I dette tilfellet benyttes standardprofilen (DefaultWEBVPNGroup)



Dobbelklikk på "DefaultWEBVPNGroup".

Configuration > Remote Access VP	N > Clientless SSL VPN	Access > Connect	ion Profiles
Access Interfaces			
Enable interfaces for clientless SSL VP	N access.		
Interface	Allow Access		
outside			
inside			
Access Port: 443			
Click here to Assign Certificate to Inte	erface.		
Login Page Setting			
Allow user to select connection pro	ofile, identified by its alias.	on the login page. (	)therwise, DefaultWebVPNGroup
	· · · ·	on the login pager o	and macy benaarmed in her dap
Allow user to enter internal passw	ord on the login page.		
Connection Profiles			
Connection profile (tunnel group) spec	ifies how user is authentic	ated and other para	meters.
🖶 Add 📝 Edit 🏢 Delete			
Name	Enabled	Aliases	Authentication Method
DefaultRAGroup	$\checkmark$		AAA(LOCAL)
DefaultWEBVPNGroup	<b>V</b>		AAA(LOCAL)

Velg "Authentication Method" AAA og deretter AAA Server Group fra pkt.6 Fjern eventuelt hake fra "Use LOCAL if Server Group fails"

Basic	Name: DefaultWEBVPNGroup	
Advanced	Aliases:	
	Authentication	
	Method:	
	AAA Server Group: bpcode	✓ Manage
	Use LOCAL if Server Group fails	
	DNS	
	Server Group: DefaultDNS	▼ Manage
	(Following fields are attributes of the DNS server group selected	above.)
	Domain Name:	
	Group Policy	Manage
	Bittarpi bitcy	• Hanagerri

#### Klikk OK

Connection Profiles			
Connection profile (tunnel group) specifies how user is authenticated and other parameters.			
🖶 Add 🗹 Edit 📋 Delete			
Name	Enabled	Aliases	Authentication Method
DefaultRAGroup	<b>V</b>		AAA(LOCAL)
DefaultWEBVPNGroup	<b>V</b>		AAA(bpcode)

Klikk deretter "Apply" nederst i vinduet.

Den samme konfigurasjonen kan gjøres fra CLI og ser da slik ut:

tunnel-group DefaultWEBVPNGroup general-attributes
 authentication-server-group bpcode

9. Pålogging på Clientless SSL VPN Access (browser-based VPN access)

Skriv inn brukernavn (må finnes i LDAP/AD). Skriv inn engangskode fra Buypass Code App'n og klikk deretter på "Login".

Login
Please enter your username and password.
USERNAME: essa_2 PASSWORD: •••••
Login